Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Studio delle Tecnologie Zero Trust, ZeroTier, VPN IPsec, OpenVPN, WireGuard e gestione accesso mediante micro servizi finalizzato alla progettazione di un ambiente Zero Trust.

Antonio Francesco Gentile, Davide Macrì, Emilio Greco

RT-ICAR-CS-24-01 **Aprile 2024**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 8-9C, 87036 Rende, Italy, URL: *www.icar.cnr.it*
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: *www.icar.cnr.it*
– Sezione di Palermo, Via Ugo La Malfa, 153, 90146 Palermo, URL: *www.icar.cnr.it*

Sommario

Introduzione

La Zero Trust Architecture (ZTA) è un nuovo approccio cruciale per garantire la sicurezza delle infrastrutture informatiche aziendali, poiché abbandona il tradizionale concetto di "perimetro da difendere". Questo cambiamento è motivato dalla complessità crescente delle reti aziendali, che includono reti interne, uffici remoti, connessioni mobili e servizi cloud, rendendo obsolete le tecniche di protezione basate sul perimetro. La ZTA, invece, pone l'enfasi sulla verifica continua degli utenti, dei dispositivi e delle applicazioni che cercano l'accesso alle risorse aziendali, richiedendo una revisione delle politiche di sicurezza e l'implementazione di controlli granulari sull'accesso. Questo nuovo modello implica l'utilizzo di tecnologie come l'autenticazione continua, l'autorizzazione basata sul ruolo e la crittografia del traffico, riducendo il rischio di compromissione e attacchi informatici. Infine, il documento esegue un'analisi comparativa delle tecnologie ZTA e delle VPN tradizionali, valutandole in base a criteri come sicurezza, scalabilità e affidabilità.

Questo documento fornisce un'analisi comparativa delle tecnologie Zero Trust, ZeroTier e delle VPN tradizionali come IPsec, OpenVPN, WireGuard E Cloudflared. Ogni tecnologia viene esaminata in base a criteri chiave quali sicurezza, scalabilità, facilità d'uso, approccio ai micro servizi, performance e affidabilità.

Riferimenti architetturali: NIST Special Publication 800-207

Il concetto di Zero Trust (ZT) rappresenta una serie dinamica di approcci nella sicurezza informatica, che sposta l'attenzione da difese tradizionali basate su perimetri fissi della rete, verso una focalizzazione sugli utenti, gli asset e le risorse. L'architettura a Zero Trust (ZTA) implementa questi principi per progettare infrastrutture e flussi di lavoro, sia in ambito industriale che aziendale. In pratica, ciò significa eliminare la fiducia implicita in asset o account utente basandosi esclusivamente sulla loro posizione fisica o rete di appartenenza. L'autenticazione e l'autorizzazione sono fasi distinte prima che l'accesso a una risorsa aziendale sia consentito. Questo approccio è una risposta alle sfide attuali delle reti aziendali, come utenti remoti, dispositivi personali (BYOD) e asset basati su cloud, che non si trovano più entro perimetri di rete tradizionali.

L'infrastruttura aziendale tipica è diventata più complessa nel tempo, con diverse reti interne, uffici remoti, individui mobili e servizi cloud. Questa complessità ha reso obsoleti i tradizionali metodi di sicurezza basati sui perimetri di rete, poiché non esiste più un unico perimetro identificabile per l'azienda. L'approccio ZT, invece, parte dal presupposto che un attaccante sia già presente nell'ambiente aziendale e che l'ambiente stesso non sia più affidabile di uno esterno. Pertanto, si basa sulla continua valutazione dei rischi e sull'attuazione di protezioni mirate.

L'architettura a Zero Trust (ZTA) è progettata per prevenire violazioni dei dati e limitare il movimento laterale all'interno dell'azienda, utilizzando principi di autenticazione e autorizzazione rigorosi. Questo approccio richiede una valutazione del rischio aziendale e non può essere implementato con una semplice sostituzione tecnologica, ma piuttosto attraverso un processo graduale che integra principi ZT nei flussi di lavoro e nelle operazioni aziendali.

Per essere efficace, ZT richiede la completa integrazione con pratiche di sicurezza informatica esistenti, gestione delle identità e degli accessi, monitoraggio continuo e migliori pratiche. Le organizzazioni dovrebbero implementare gradualmente questi principi per proteggere i loro asset e le funzioni aziendali, considerando che molte opereranno in una modalità ibrida tra Zero Trust e approcci basati su perimetri.

Concetti fondamentali dell'approccio Zero Trust

Il concetto di Zero Trust (ZT) è una filosofia di sicurezza informatica che si basa sull'idea di non concedere fiducia implicita, ma valutarla costantemente per proteggere le risorse. L'architettura Zero Trust (ZTA) rappresenta un approccio completo alla sicurezza delle risorse e dei dati aziendali, includendo aspetti come identità, credenziali, gestione degli accessi e dispositivi terminali.

Tradizionalmente, le organizzazioni si sono concentrate sulla difesa del perimetro, consentendo agli utenti autenticati di accedere a una vasta gamma di risorse una volta all'interno della rete interna. Tuttavia, questo approccio ha portato a problemi come il movimento laterale non autorizzato all'interno dell'ambiente.

Le Connessioni Internet Attendibili (TIC) e i firewall di perimetro hanno fornito una protezione robusta contro gli attacchi dall'Internet, ma sono meno efficaci nel rilevare e bloccare gli attacchi dall'interno della rete e non possono proteggere soggetti al di fuori del perimetro aziendale.

Zero Trust (ZT) si propone di ridurre l'incertezza nell'applicare decisioni di accesso e privilegi minimi nei sistemi e nei servizi informativi in un contesto di rete considerato compromesso. L'architettura Zero Trust (ZTA) è il piano di sicurezza informatica di un'azienda che utilizza questi concetti e include componenti, flussi di lavoro e politiche di accesso.

Un'azienda adotta Zero Trust come strategia principale e sviluppa un'architettura Zero Trust come piano creato con i principi di Zero Trust in mente, implementandola per creare un ambiente Zero Trust utilizzato dall'azienda.

Questo approccio si concentra sull'autenticazione, sull'autorizzazione e sulla riduzione delle zone di fiducia implicita, mantenendo nel contempo la disponibilità e minimizzando i ritardi temporali nei meccanismi di autenticazione. Le regole di accesso sono create il più dettagliate possibile per imporre i privilegi minimi necessari per eseguire l'azione richiesta.

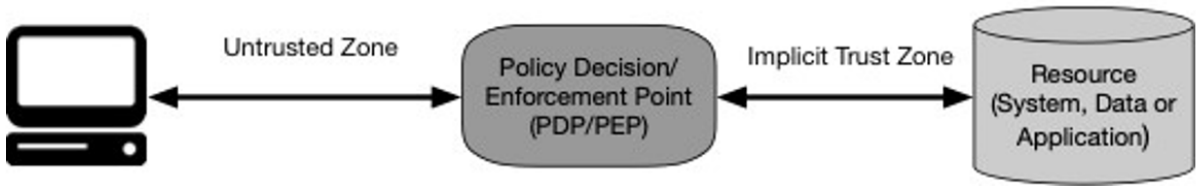


Figure 1: Zero Trust Access

Il sistema deve garantire sia l'autenticità del soggetto che la validità della richiesta, permettendo al soggetto di accedere alla risorsa solo dopo una valutazione accurata da parte del PDP/PEP. Questo evidenzia l'importanza di due aspetti fondamentali nel concetto di zero trust: l'autenticazione e l'autorizzazione.

Le imprese devono sviluppare politiche dinamiche basate sul rischio per l'accesso alle risorse, garantendo l'applicazione coerente di tali politiche per ogni richiesta di accesso. Questo significa che non dovrebbero fare affidamento su una fiducia implicita dopo il superamento di un livello base di autenticazione.

La "zona di fiducia implicita" rappresenta un'area in cui tutte le entità sono considerate affidabili almeno al livello dell'ultimo punto di controllo PDP/PEP. Ridurre al minimo questa zona è cruciale per garantire che il PDP/PEP possa applicare controlli specifici e che tutto il traffico oltre il PEP abbia lo stesso livello di affidabilità.

Il concetto di Zero Trust fornisce un approccio per avvicinare i PDP/PEP alla risorsa, con l'obiettivo di autenticare e autorizzare esplicitamente tutti i soggetti, gli asset e i flussi di lavoro aziendali.

Zero Trust: Principi

Numerose definizioni e discussioni su Zero Trust (ZT) enfatizzano la rimozione delle difese perimetrali a ampia area, come i firewall aziendali, come elemento chiave. Tuttavia, molte di queste definizioni continuano a fare riferimento ai perimetri in qualche modo, come la micro-segmentazione o i micro perimetri, come parte delle capacità operative di un'architettura Zero Trust (ZTA). Di seguito, cerchiamo di definire ZT e ZTA in termini di principi fondamentali che dovrebbero essere inclusi anziché ciò che viene escluso. Questi principi rappresentano l'obiettivo ideale, anche se va riconosciuto che non tutti i principi possono essere completamente realizzati nella loro forma più pura per una data strategia. Un'architettura a Zero Trust è concepita e implementata con il rispetto dei seguenti principi fondamentali di Zero Trust:

- Tutte le comunicazioni devono essere crittografate, indipendentemente dalla loro posizione nella rete, poiché la posizione non implica automaticamente fiducia. È necessario proteggere e autenticare tutte le comunicazioni utilizzando i metodi più sicuri disponibili.
- L'accesso alle risorse aziendali è concesso sulla base di sessioni valutate secondo i privilegi minimi richiesti. L'autenticazione e l'autorizzazione non garantiscono automaticamente l'accesso a risorse diverse.
- L'accesso alle risorse è regolato da politiche dinamiche che considerano lo stato osservabile dell'identità del cliente, dell'applicazione/servizio e dell'asset richiedente, oltre ad altri attributi comportamentali e ambientali.
- L'azienda monitora costantemente l'integrità e la sicurezza degli asset posseduti e associati. Nessun asset è considerato intrinsecamente affidabile e la sicurezza degli asset viene valutata durante ogni richiesta di risorse.
- Tutta l'autenticazione e l'autorizzazione delle risorse sono dinamiche e rigorosamente applicate prima dell'accesso. L'azienda dovrebbe disporre di sistemi di gestione delle identità e degli accessi in grado di monitorare e gestire l'accesso alle risorse in modo continuo.
- L'azienda raccoglie informazioni sullo stato corrente degli asset, dell'infrastruttura di rete e delle comunicazioni per migliorare la sua postura di sicurezza e le sue politiche.
- Questi principi mirano a essere neutrali rispetto alla tecnologia e si applicano sia al lavoro interno di un'organizzazione che alla collaborazione con altre organizzazioni, ma non ai processi aziendali rivolti al pubblico o ai consumatori in modo anonimo. Un'organizzazione non può imporre politiche interne agli attori esterni, ma può implementare politiche basate su Zero Trust su utenti non aziendali con una relazione speciale con l'organizzazione.

Una Prospettiva Zero Trust della Rete

- Nella progettazione e nell'attuazione della rete, ci sono alcune assunzioni di base per la connettività di qualsiasi organizzazione che adotti la Zero Trust Architecture (ZTA). Alcune di queste assunzioni riguardano l'infrastruttura di rete di proprietà dell'azienda, mentre altre riguardano le risorse

aziendali che operano su infrastrutture di rete non di proprietà dell'azienda, come reti Wi-Fi pubbliche o fornitori di servizi cloud pubblici. Queste premesse guidano la creazione di una ZTA. La rete di un'azienda che implementa una ZTA dovrebbe essere sviluppata seguendo i principi fondamentali delineati in precedenza e basandosi su tali assunzioni.

1. L'intera rete privata aziendale non è considerata una zona di fiducia implicita, pertanto, gli asset devono operare sotto l'assunzione che un attaccante possa essere presente sulla rete aziendale. Di conseguenza, tutte le comunicazioni devono avvenire in modo sicuro, includendo l'autenticazione di tutte le connessioni e la crittografia del traffico.
2. I dispositivi sulla rete potrebbero non essere di proprietà o configurabili dall'azienda. Visitatori o servizi esterni potrebbero includere risorse non di proprietà dell'azienda che richiedono l'accesso alla rete per svolgere le proprie funzioni. Questo può includere politiche "porta il tuo dispositivo" (BYOD) che permettono ai dipendenti di utilizzare dispositivi personali per accedere alle risorse aziendali.
3. Nessuna risorsa è considerata affidabile per definizione. Ogni asset deve essere valutato sulla base della sua postura di sicurezza tramite un punto di decisione della policy (PEP) prima che l'accesso a una risorsa aziendale venga concesso. Tale valutazione deve essere continua durante tutta la sessione e le credenziali dei soggetti non sono sufficienti per l'autenticazione del dispositivo.
4. Non tutte le risorse aziendali risiedono su infrastrutture di proprietà dell'azienda. Queste risorse possono includere soggetti aziendali remoti o servizi cloud. Gli asset aziendali potrebbero dover utilizzare reti non aziendali per la connettività di base e i servizi di rete.
5. I soggetti aziendali remoti e gli asset non devono fidarsi completamente delle proprie connessioni di rete locali. Devono presumere che la rete locale sia ostile e che tutto il traffico possa essere monitorato o modificato. Pertanto, tutte le richieste di connessione devono essere autenticate e autorizzate, e tutte le comunicazioni devono essere protette al massimo.
6. Gli asset e i flussi di lavoro devono mantenere una politica di sicurezza coerente quando si spostano tra infrastrutture aziendali e non aziendali. Questo significa che devono conservare la loro postura di sicurezza quando si spostano tra reti aziendali e non aziendali o tra data center locali e istanze cloud non aziendali.

Elementi Concettuali dell'Architettura Zero Trust

L'implementazione della Zero Trust Architecture (ZTA) in un'azienda comprende diversi elementi concettuali, gestibili sia come servizio in loco che tramite un servizio basato su cloud. Il modello concettuale mostrato nella Figura 2 illustra le relazioni di base tra questi elementi e le loro interazioni. È essenziale notare che questo modello è ideale e mette in evidenza gli elementi concettuali e le loro connessioni. Dal diagramma in Figura 1, il punto decisionale delle policy (PDP) è diviso in due componenti logici: il motore delle policy e l'amministratore delle policy (come definito di seguito). Gli elementi concettuali della ZTA utilizzano un piano di controllo separato per la comunicazione, mentre lo scambio dei dati delle applicazioni avviene attraverso un piano dati.

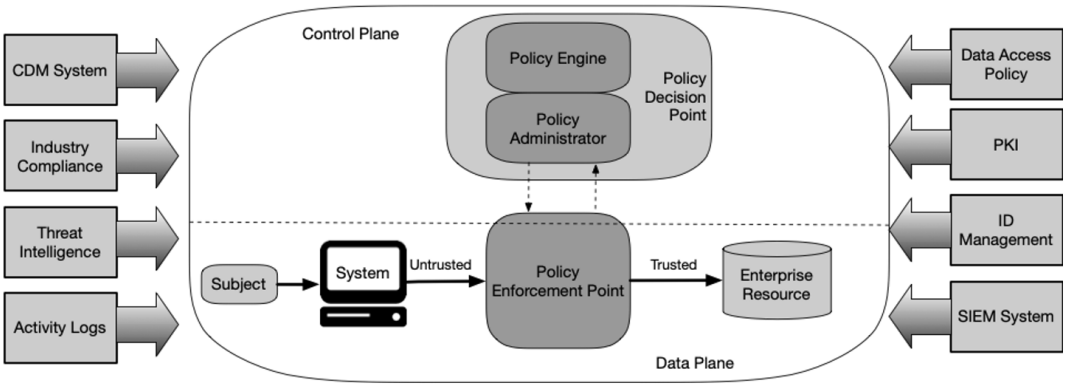


Figure 2: Core Zero Trust Logical Components

Le descrizioni dei componenti:

- Il motore delle policy (PE) è responsabile della decisione finale sull'accesso, utilizzando regole aziendali e input esterni per determinare se concedere, negare o revocare l'accesso.
- L'amministratore delle policy (PA) gestisce le connessioni tra soggetto e risorsa, creando token di autenticazione specifici della sessione e collaborando con il PE per autorizzare o negare l'accesso.
- Il punto di applicazione delle policy (PEP) regola le connessioni, comunicando con il PA per ricevere aggiornamenti delle policy e può essere suddiviso in lato client e lato risorsa o essere un componente singolo.

Oltre a questi, sorgenti esterne forniscono input al motore delle policy:

il Sistema di diagnosi e mitigazione continua (CDM) raccoglie informazioni sugli asset aziendali, il sistema di conformità settoriale garantisce la conformità alle normative, i feed di intelligence sulle minacce forniscono informazioni sugli attacchi, i registri di attività di rete monitorano la sicurezza, le politiche di accesso ai dati definiscono le regole di accesso, la PKI gestisce i certificati, il sistema di gestione delle identità gestisce gli account utente e il SIEM raccoglie dati per monitorare e prevenire gli attacchi.

Varianti delle Approcci all'Architettura Zero Trust

Esistono diverse modalità per implementare un'Architettura Zero Trust (ZTA) all'interno di un'organizzazione, ognuna con i propri componenti e fonti principali di regole di policy. Questi approcci includono la governance avanzata dell'identità, la microsegmentazione logica e la segmentazione basata sulla rete, tutti basati sui principi del Zero Trust. Mentre una soluzione completa includerà elementi di tutti e tre gli approcci, la scelta tra di essi dipende dal caso d'uso specifico e dalle policy esistenti dell'organizzazione. Ad esempio, un'organizzazione potrebbe trovare che un certo approccio si adatta meglio alle sue esigenze e alla sua infrastruttura attuale, anche se altri approcci potrebbero essere altrettanto validi ma richiederebbero modifiche più significative.

3.1.1 ZTA Utilizzando una Governance dell'Identità Potenziata

L'approccio della governance avanzata dell'identità per lo sviluppo di un'Architettura Zero Trust (ZTA) si concentra sull'identità degli attori come componente chiave per la definizione delle policy di accesso alle risorse aziendali. Le policy si basano sull'identità e sugli attributi assegnati ai soggetti, con l'accesso alle risorse determinato principalmente dai privilegi di accesso assegnati a ciascun soggetto. Fattori aggiuntivi come il dispositivo utilizzato, lo stato dell'asset e le condizioni ambientali possono influenzare il livello di fiducia e quindi l'autorizzazione di accesso finale. Questo approccio è spesso utilizzato in ambienti con reti aperte o con dispositivi non aziendali frequenti, ma richiede un monitoraggio costante per mitigare potenziali rischi, come attività malevole sulla rete. Tuttavia, funziona bene con vari modelli aziendali, inclusi i servizi basati su cloud che potrebbero non supportare pienamente le soluzioni di sicurezza aziendali.

3.1.2 ZTA Utilizzando la Micro Segmentazione

Un'azienda potrebbe scegliere di implementare una ZTA basata sulla collocazione di risorse su segmenti di rete unici protetti da dispositivi gateway di sicurezza. Questi dispositivi, come switch intelligenti, router o firewall di nuova generazione, agiscono come PEP per proteggere le risorse, concedendo dinamicamente l'accesso solo alle richieste autorizzate. Questo approccio può anche includere la microsegmentazione basata sull'host utilizzando agenti software o firewall sugli endpoint. I dispositivi gateway fungono da componenti PEP e possono essere gestiti insieme come parte di un programma di governance dell'identità (IGP). La chiave di questo approccio è la gestione efficace dei dispositivi PEP, in grado di reagire prontamente alle minacce e ai cambiamenti nel flusso di lavoro, garantendo la sicurezza delle risorse aziendali.

3.1.3 ZTA Utilizzando l'Infrastruttura di Rete e i Perimetri Definiti dal Software

L'ultimo approccio per implementare una ZTA sfrutta l'infrastruttura di rete, utilizzando una rete sovrapposta che potrebbe operare a livelli più bassi dello stack di rete OSI o a livello 7. Questi approcci, spesso chiamati Software Defined Perimeter (SDP), incorporano concetti di Software Defined Networking (SDN) e Intent-Based Networking (IBN). In questo scenario, il PA funge da controller di rete, adattando la configurazione della rete in base alle decisioni prese dal PE. I clienti continuano a richiedere l'accesso attraverso i PEP, i quali sono gestiti dal componente PA.

Varianti Implementative dell'Architettura Astratta

Tutti i componenti sopra elencati sono componenti concettuali. Non è necessario che siano sistemi distinti. Un singolo asset potrebbe svolgere le funzioni di più componenti concettuali, e allo stesso modo, una componente concettuale potrebbe comprendere più elementi hardware o software per eseguire le operazioni. Ad esempio, una PKI gestita internamente potrebbe consistere in un singolo componente responsabile dell'emissione di certificati per i dispositivi e un altro componente utilizzato per rilasciare certificati agli utenti finali, entrambi utilizzando certificati intermedi emessi dalla stessa autorità di certificazione radice interna all'azienda. In alcune soluzioni ZT attualmente disponibili sul mercato, i componenti PE e PA sono integrati in un unico servizio.

Esistono diverse varianti nella distribuzione dei componenti selezionati dell'architettura, le quali sono descritte nelle sezioni seguenti. A seconda della configurazione della rete aziendale, possono essere utilizzati più modelli di implementazione ZTA per diversi processi aziendali all'interno della stessa azienda.

3.2.1 Implementazione Basata su Agente Dispositivo/Gateway

In questo modello di implementazione, il PEP è diviso in due parti: una risiede direttamente sulla risorsa stessa, mentre l'altra è posizionata di fronte ad essa come componente separato. Ad esempio, ogni dispositivo aziendale dispone di un agente software installato per gestire le connessioni, mentre ogni risorsa è associata a un componente, come un gateway, posizionato di fronte ad essa. In questo modo, la risorsa comunica solo con il gateway, che funge da proxy per essa. L'agente software instrada il traffico verso il PEP appropriato per la valutazione delle richieste. Il gateway gestisce la comunicazione con l'amministratore delle policy e consente solo le comunicazioni approvate configurate da quest'ultimo.

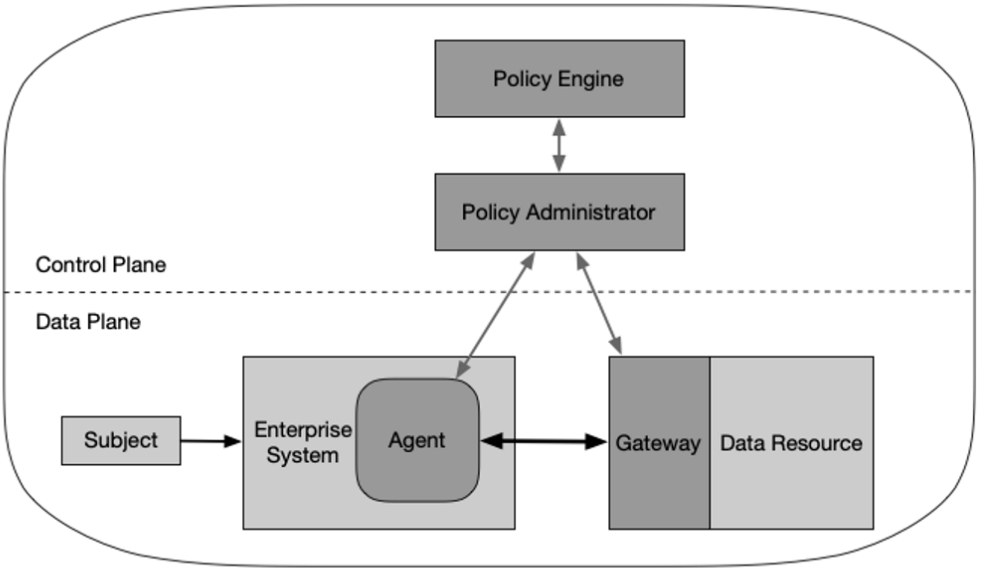


Figure 3: Device Agent/Gateway Model

In uno scenario comune, un dipendente con un laptop aziendale desidera accedere a una risorsa aziendale, come un'applicazione o un database delle risorse umane. L'agente software locale gestisce la richiesta di accesso e la inoltra all'amministratore delle policy, che può essere situato internamente o ospitato su cloud. Successivamente, l'amministratore delle policy sottopone la richiesta al motore delle policy per la valutazione. Se la richiesta viene autorizzata, viene configurato un canale di comunicazione tra l'agente dispositivo e il gateway della risorsa pertinente tramite il piano di controllo. Questo processo include l'assegnazione di informazioni come indirizzo IP, porta, chiave di sessione, o altri dati di sicurezza. Una volta stabilita la connessione, inizia lo scambio crittografato dei dati dell'applicazione o del servizio. La connessione viene interrotta quando il flusso di lavoro è completato o in caso di eventi di sicurezza, come il timeout della sessione o il fallimento dell'autenticazione. Questo modello è particolarmente adatto per le aziende che gestiscono in modo efficace dispositivi e risorse che possono comunicare con il gateway. Per le aziende che utilizzano ampiamente i servizi cloud, questa implementazione riflette l'Approccio al Perimetro Definito dal Software (SDP) della Cloud Security Alliance (CSA), in una configurazione client-server. È anche una scelta appropriata per le aziende che preferiscono non adottare politiche BYOD, poiché l'accesso è consentito solo tramite l'agente dispositivo installato su dispositivi di proprietà aziendale.

3.2.2 Implementazione Basata su Enclave

In questa variante del modello di implementazione, i componenti del gateway non sono necessariamente collocati sugli asset o davanti a singole risorse, ma sono posizionati al confine di un insieme di risorse, come ad esempio un data center locale. Queste risorse generalmente supportano una specifica funzione aziendale o potrebbero non avere la capacità di comunicare direttamente con un gateway, come nel caso di sistemi legacy senza un'interfaccia di programmazione delle applicazioni adatta per la comunicazione con un gateway. Questo approccio potrebbe essere vantaggioso per le aziende che utilizzano microservizi basati su cloud per processi aziendali specifici, come le notifiche agli utenti o la gestione delle buste paga. In questo modello, l'intero cloud privato è posto dietro il gateway.

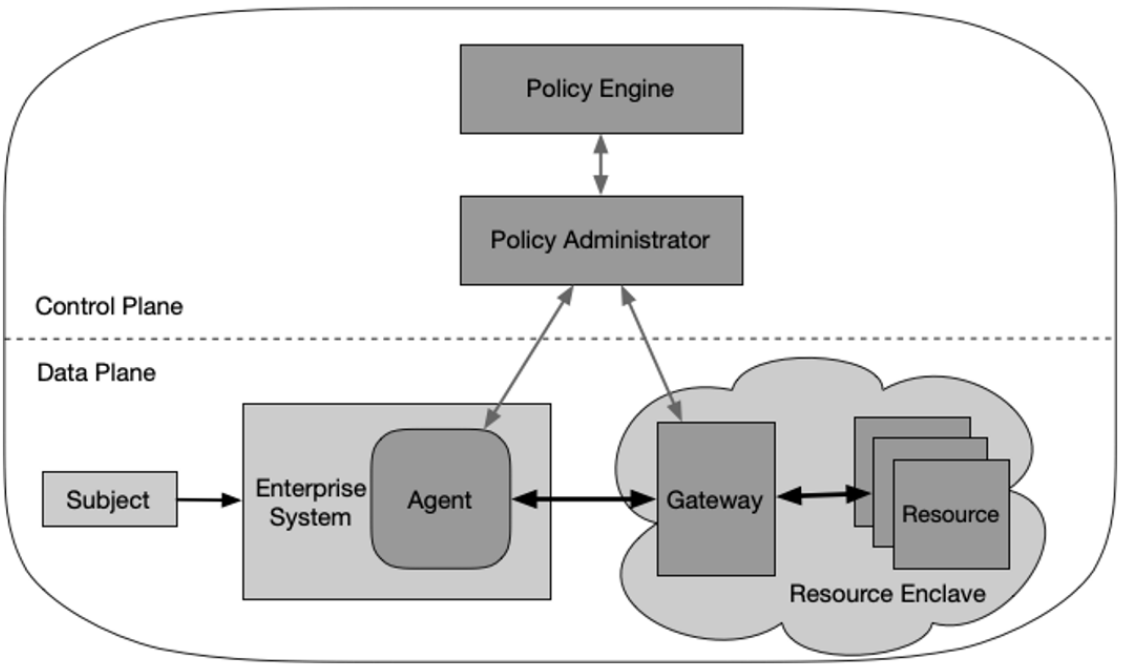


Figure 4: Enclave Gateway Model

Questo modello potrebbe rappresentare una fusione tra il modello di agente dispositivo/gateway e altre forme di implementazione. In questa configurazione, gli asset dell'azienda sono dotati di un agente dispositivo che agevola la connessione ai gateway dell'enclave. Tuttavia, le connessioni e il processo di gestione sono simili a quelli del modello di base di agente dispositivo/gateway. Questo approccio si adatta bene alle aziende con applicazioni legacy o data center locali che non possono avere gateway individuali per ogni risorsa. È necessario un solido programma di gestione degli asset e delle configurazioni per installare e configurare gli agenti dispositivo. Tuttavia, il limite di questo modello è che il gateway protegge una raccolta di risorse, il che potrebbe non garantire la protezione di ciascuna risorsa individualmente. Inoltre, potrebbe consentire ai soggetti di visualizzare risorse alle quali non hanno i privilegi di accesso.

3.2.3 Implementazione Basata su Portale delle Risorse

In questo modello di implementazione, il PEP assume il ruolo di un unico gateway che gestisce le richieste provenienti dai soggetti. Tale gateway può essere dedicato a una singola risorsa o a un'area protetta che ospita una collezione di risorse utilizzate per una specifica funzione aziendale. Un esempio concreto potrebbe essere un portale gateway situato in un cloud privato o in un data center, contenente applicazioni legacy, come illustrato nella Figura 5.

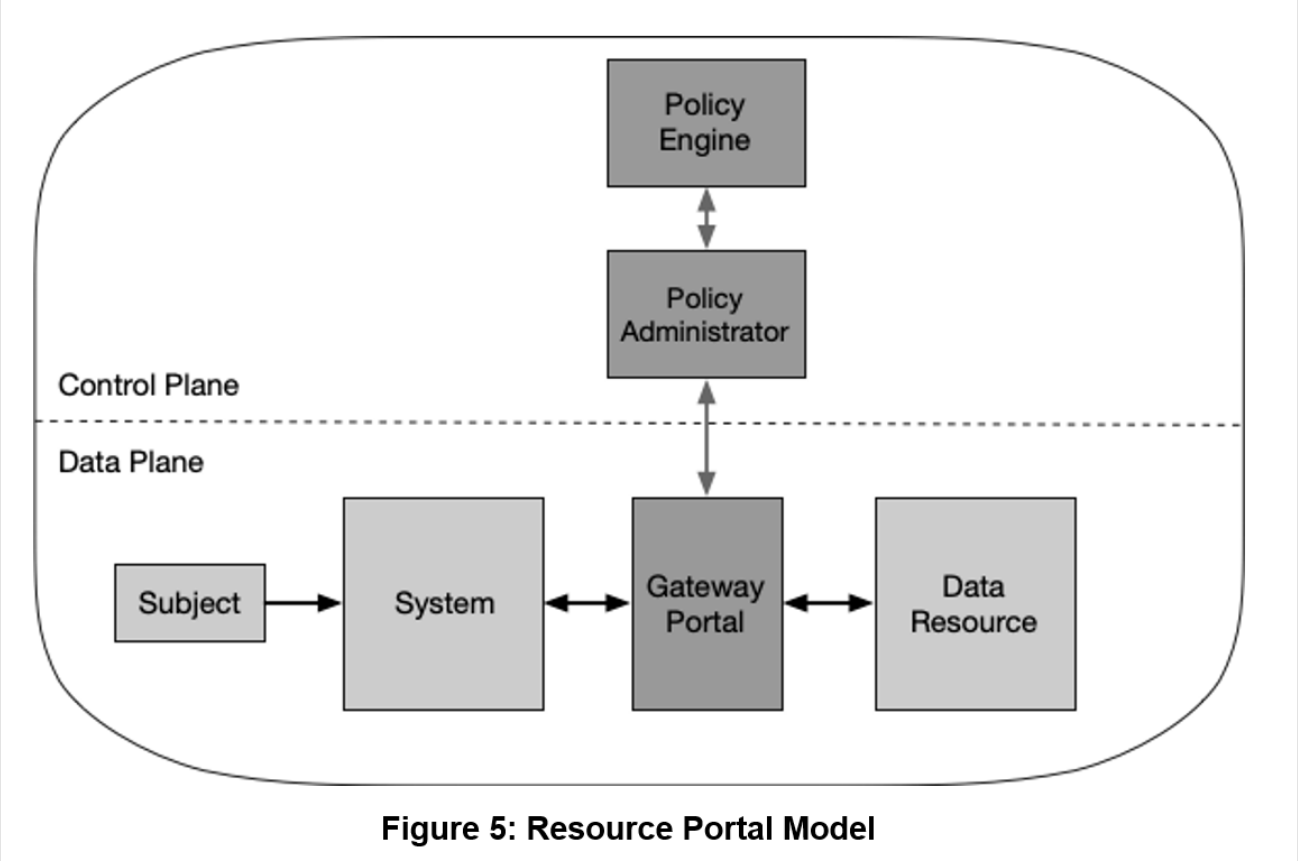


Figure 5: Resource Portal Model

In questo modello, il principale vantaggio rispetto agli altri è che non è necessario installare un componente software su tutti i dispositivi client. Questo aspetto rende il modello più flessibile per le politiche BYOD e le iniziative di collaborazione tra organizzazioni. Gli amministratori aziendali non devono preoccuparsi di garantire che ogni dispositivo sia dotato dell'agente dispositivo corretto prima dell'utilizzo. Tuttavia, ciò significa anche che le informazioni disponibili sui dispositivi che richiedono l'accesso sono limitate. Il modello può analizzare solo gli asset e i dispositivi una volta connessi al portale PEP, e potrebbe non essere in grado di monitorarli costantemente per malware, vulnerabilità non aggiornate e configurazioni adeguate. Una differenza chiave di questo modello è l'assenza di un agente locale che gestisca le richieste, il che significa che l'azienda potrebbe non avere una visione completa o un controllo diretto sugli asset, in quanto può osservarli o analizzarli solo quando si collegano al portale. Ciò potrebbe comportare la perdita di visibilità sugli asset tra le sessioni. Inoltre, questo modello potrebbe rendere possibile per gli attaccanti individuare e tentare di accedere al portale o eseguire attacchi di denial-of-service (DoS) contro di esso. Di conseguenza, i sistemi del portale devono essere adeguatamente protetti per garantire la disponibilità contro attacchi DoS o interruzioni della rete.

3.2.4 Sandboxing delle Applicazioni sui Dispositivi

In un'altra versione del modello di distribuzione agente/gateway, le applicazioni o i processi approvati vengono eseguiti in compartimenti separati sugli asset. Questi compartimenti possono essere costituiti da macchine virtuali, container o altre implementazioni simili, ma l'obiettivo è sempre lo stesso: proteggere l'applicazione o le sue istanze da un host eventualmente compromesso o da altre applicazioni in esecuzione sull'asset.

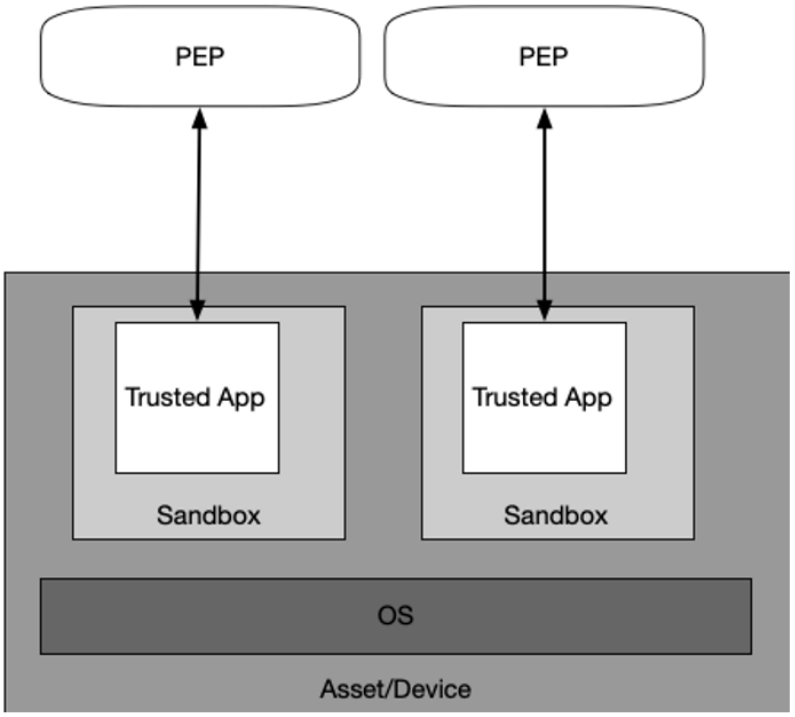
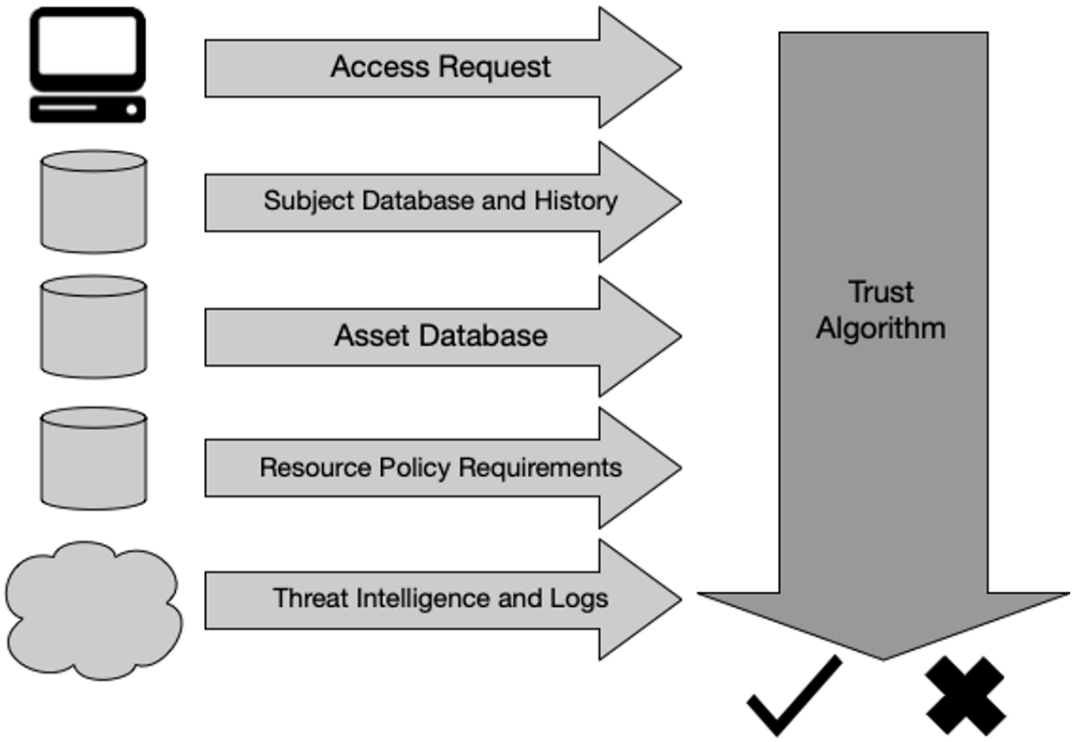


Figure 6: Application Sandboxes

Nella Figura 6, il dispositivo soggetto esegue applicazioni approvate e verificate in un ambiente chiamato sandbox. Le applicazioni possono comunicare con il PEP per richiedere l'accesso alle risorse, ma il PEP respingerà le richieste provenienti dalle altre applicazioni presenti sull'asset. In questo modello, il PEP potrebbe essere un servizio locale all'interno dell'azienda o un servizio basato su cloud. Il principale vantaggio di questa variante del modello è che le singole applicazioni sono isolate dal resto dell'asset. Ciò significa che se l'asset viene compromesso, le singole applicazioni sandbox possono essere protette da eventuali infezioni da malware presenti sull'host. Tuttavia, uno svantaggio di questo modello è che le aziende devono gestire e mantenere le applicazioni sandbox per tutti gli asset e potrebbero non avere una visione completa sugli asset client. Inoltre, l'azienda deve garantire che ogni applicazione sandbox sia sicura, il che potrebbe richiedere maggiori sforzi rispetto al semplice monitoraggio dei dispositivi.

Algoritmo di Fiducia

Nel contesto dell'adozione della Zero Trust Architecture (ZTA) da parte di un'organizzazione, il motore delle policy svolge il ruolo analogo a quello del cervello, mentre l'algoritmo di fiducia del PE agisce come il suo processo decisionale principale. L'algoritmo di fiducia è il meccanismo mediante il quale il motore delle policy determina se consentire o negare l'accesso a una risorsa. Il motore delle policy riceve dati da diverse fonti, come il database delle policy che contiene informazioni sugli attributi e i ruoli dei soggetti, i modelli storici di comportamento dei soggetti, le fonti di intelligence sulle minacce e altri metadati. Questo processo può essere suddiviso in categorie ampie e visualizzato graficamente, come mostrato nella Figura 7.



Nella figura, gli input forniti all'algoritmo di fiducia possono essere categorizzati in diverse categorie:

1. Richiesta di accesso: Questa categoria include informazioni sulla richiesta effettuata dal soggetto, come la risorsa richiesta e le informazioni sul richiedente, come la versione del sistema operativo e il software utilizzato. Queste informazioni sono utilizzate per valutare se concedere o negare l'accesso alla risorsa.
2. Database dei soggetti: Questo database contiene informazioni sugli attributi e i privilegi dei soggetti che richiedono l'accesso alle risorse. Include identità logiche, risultati di autenticazione e altri attributi come tempo e geolocalizzazione. Queste informazioni costituiscono la base per le policy di accesso.
3. Database degli asset (e stato osservabile): Questo database contiene lo stato conosciuto di ogni asset aziendale, come la versione del sistema operativo, il software e la sua integrità, la posizione di rete e la geolocalizzazione. Queste informazioni vengono confrontate con lo stato dell'asset che effettua la richiesta per determinare se concedere o negare l'accesso.
4. Requisiti delle risorse: Questo insieme di policy definisce i requisiti minimi per l'accesso alle risorse, come i livelli di sicurezza dell'autenticatore e la sensibilità dei dati. Questi requisiti sono sviluppati dai responsabili dei dati e dei processi aziendali.
5. Intelligence sulle minacce: Questo flusso di informazioni fornisce informazioni sulle minacce generali e attive su Internet. Include anche informazioni su comunicazioni sospette dal dispositivo. Queste informazioni sono utilizzate per valutare il rischio associato all'accesso alle risorse. Il peso di ciascuna fonte di dati può essere determinato da un algoritmo proprietario o configurato dall'azienda per riflettere l'importanza della fonte di dati. La determinazione finale viene quindi passata al PA per l'esecuzione delle decisioni. Il PA è responsabile di configurare i PEP necessari per abilitare la comunicazione autorizzata e può mettere in pausa o terminare una connessione in base alla policy.

Varianti dell'Algoritmo di Fiducia

Esistono diverse modalità di implementazione della Zero Trust Architecture (ZTA), ognuna con caratteristiche distintive che possono essere adattate in base alle esigenze e alle priorità dell'organizzazione. Queste caratteristiche includono come vengono valutati i fattori decisionali e come le richieste di accesso vengono valutate rispetto al contesto dell'utente, dell'applicazione o del dispositivo.

1. Basato su criteri o punteggio: Un TA basato su criteri applica criteri predefiniti che devono essere soddisfatti prima che sia consentito l'accesso a una risorsa. Questi criteri possono variare per ogni risorsa e l'accesso viene concesso solo se tutti i criteri sono rispettati. Al contrario, un TA basato su punteggio calcola un livello di fiducia basato sui dati forniti da varie fonti e sui pesi configurati dall'azienda. Se il punteggio supera una soglia predefinita, l'accesso viene concesso.
2. Singolare o contestuale: Un TA singolare valuta ogni richiesta di accesso individualmente, senza considerare la storia del soggetto. Al contrario, un TA contestuale tiene conto del comportamento passato del soggetto o dell'applicazione quando valuta le richieste di accesso. Questo consente di rilevare più facilmente comportamenti anomali o attacchi interni. Idealmente, un TA contestuale offre un controllo degli accessi più dinamico e adattabile, ma potrebbero esserci limitazioni dovute alla disponibilità di infrastrutture o risorse. È importante bilanciare la sicurezza con l'usabilità e l'efficienza dei costi durante l'implementazione di algoritmi di fiducia. La fase iniziale di implementazione richiede test e regolazioni per garantire che le politiche siano applicate correttamente senza compromettere i processi aziendali.

Componenti di Rete/Ambiente

In un ambiente basato sulla Zero Trust Architecture (ZTA), è cruciale separare i flussi di comunicazione utilizzati per controllare e configurare la rete dai flussi di comunicazione dell'applicazione o del servizio che effettivamente svolgono le attività dell'organizzazione. Questa separazione, che può essere sia logica che fisica, è comunemente realizzata tramite la distinzione tra un piano di controllo e un piano dati. Il piano di controllo è responsabile per la gestione e la configurazione delle risorse di rete, l'assegnazione degli accessi e l'attuazione delle politiche di sicurezza. Viene utilizzato da vari componenti infrastrutturali, sia interni all'azienda che forniti da terze parti, per stabilire e mantenere i percorsi di comunicazione tra le risorse. D'altro canto, il piano dati gestisce la comunicazione effettiva tra i componenti software. Prima che un percorso di comunicazione possa essere stabilito attraverso il piano dati, deve essere configurato e autorizzato tramite il piano di controllo. Ad esempio, il piano di controllo può essere utilizzato da componenti come Policy Engine (PA) e Policy Enforcement Point (PEP) per stabilire il percorso di comunicazione tra i soggetti e le risorse aziendali, mentre il carico di lavoro delle applicazioni o dei servizi utilizzerà il percorso del piano dati una volta stabilito.

Requisiti di Rete per Supportare ZTA

Gli asset aziendali sono dotati di una connettività di base alla rete, che può includere un routing di base e l'infrastruttura di servizi come il DNS, sia su reti locali (LAN) controllate dall'azienda o meno. Tuttavia, gli asset aziendali remoti potrebbero non utilizzare tutti i servizi di infrastruttura disponibili.

- È fondamentale che l'azienda sia in grado di distinguere gli asset di sua proprietà o sotto il suo controllo, nonché di valutare la postura di sicurezza attuale di tali dispositivi, utilizzando credenziali autenticate anziché informazioni non autenticate come gli indirizzi MAC di rete.
- L'azienda ha la capacità di osservare tutto il traffico di rete, registrando i pacchetti visti sul piano dati e filtrando i metadati sulla connessione per aggiornare dinamicamente le politiche di accesso e informare i componenti come il Policy Enforcement Point (PEP).
- Le risorse aziendali non sono raggiungibili senza passare attraverso un PEP, il quale configura percorsi di comunicazione personalizzati e autorizzati solo dopo che un client è stato autenticato e

autorizzato. Questo protegge le risorse da scansioni e attacchi DoS e impedisce l'accesso non autorizzato.

- Il piano di controllo e il piano dati sono logicamente separati, con il primo utilizzato per la gestione delle risorse di rete e l'assegnazione degli accessi, mentre il secondo per la comunicazione effettiva tra i componenti software.
- Gli asset aziendali possono accedere al PEP tramite varie modalità come un portale web, un dispositivo di rete o un agente software, facilitando l'accesso alle risorse aziendali.
- Il PEP è l'unico componente che accede all'amministratore delle politiche, stabilendo connessioni per la gestione dei percorsi di comunicazione tra i client e le risorse aziendali.
- Gli asset aziendali remoti dovrebbero poter accedere alle risorse aziendali senza dover attraversare necessariamente l'infrastruttura di rete aziendale, ad esempio utilizzando servizi ospitati da provider di cloud pubblico senza richiedere una VPN.
- L'infrastruttura per il processo decisionale ZTA deve essere scalabile per gestire variazioni del carico di lavoro, garantendo che i componenti come PE, PA e PEP possano gestire il flusso di lavoro aziendale in modo efficiente.
- Alcuni asset aziendali potrebbero non essere in grado di raggiungere determinati PEP a causa di fattori di politica o osservabili come la posizione geografica o il tipo di dispositivo, che possono influenzare l'accesso alle risorse in base a criteri specifici.

Scenari di Implementazione/Casi d'Uso

Ogni organizzazione può adottare i principi del zero trust nell'ambiente aziendale, poiché la maggior parte delle aziende ha già implementato alcuni aspetti di questo approccio o sta lavorando verso tale implementazione attraverso politiche di sicurezza informatica e pratiche di resilienza. Ci sono diversi scenari di implementazione e casi d'uso che si prestano naturalmente a un'architettura di zero trust. Ad esempio, il concetto di ZTA si adatta particolarmente bene alle organizzazioni con una distribuzione geografica ampia o con una forza lavoro altamente mobile. Tuttavia, qualsiasi tipo di organizzazione può trarre vantaggio dall'adozione di un'architettura di zero trust. Nei seguenti casi d'uso, il concetto di ZTA potrebbe non essere esplicitamente menzionato poiché è probabile che l'azienda abbia sia infrastrutture basate sul perimetro che elementi di ZTA già in funzione. Come discusso precedentemente, è comune che un'organizzazione attraversi un periodo in cui coesistono sia i componenti di ZTA che quelli basati sul perimetro nella propria infrastruttura di rete.

Azienda con Sedute Satellite

In uno scenario comune, un'azienda con una sede centrale e sedi remote sparse geograficamente non collegate da una rete fisica di proprietà dell'azienda deve consentire ai dipendenti delle sedi remote di accedere alle risorse aziendali. Tuttavia, potrebbero non esistere collegamenti di rete adeguati per indirizzare tutto il traffico verso la sede centrale, e i dipendenti potrebbero essere in telelavoro o in località remote utilizzando dispositivi personali o aziendali. In questa situazione, l'azienda potrebbe desiderare di concedere l'accesso a risorse come il calendario o l'email, ma limitare o negare l'accesso a risorse più sensibili come il database HR. In questo contesto, il PE/PA(s) spesso risiede come servizio cloud, offrendo una maggiore disponibilità e consentendo ai lavoratori remoti di accedere alle risorse cloud senza dipendere interamente dall'infrastruttura aziendale. Gli asset finali, sia dispositivi aziendali che personali, possono essere dotati di un agente installato o possono accedere a un portale delle risorse. In alternativa, ospitare il PE/PA(s) sulla rete locale dell'azienda potrebbe non essere la soluzione più efficiente, poiché richiederebbe agli uffici remoti e ai lavoratori di instradare tutto il traffico verso la rete aziendale per raggiungere le applicazioni e i servizi basati su cloud.

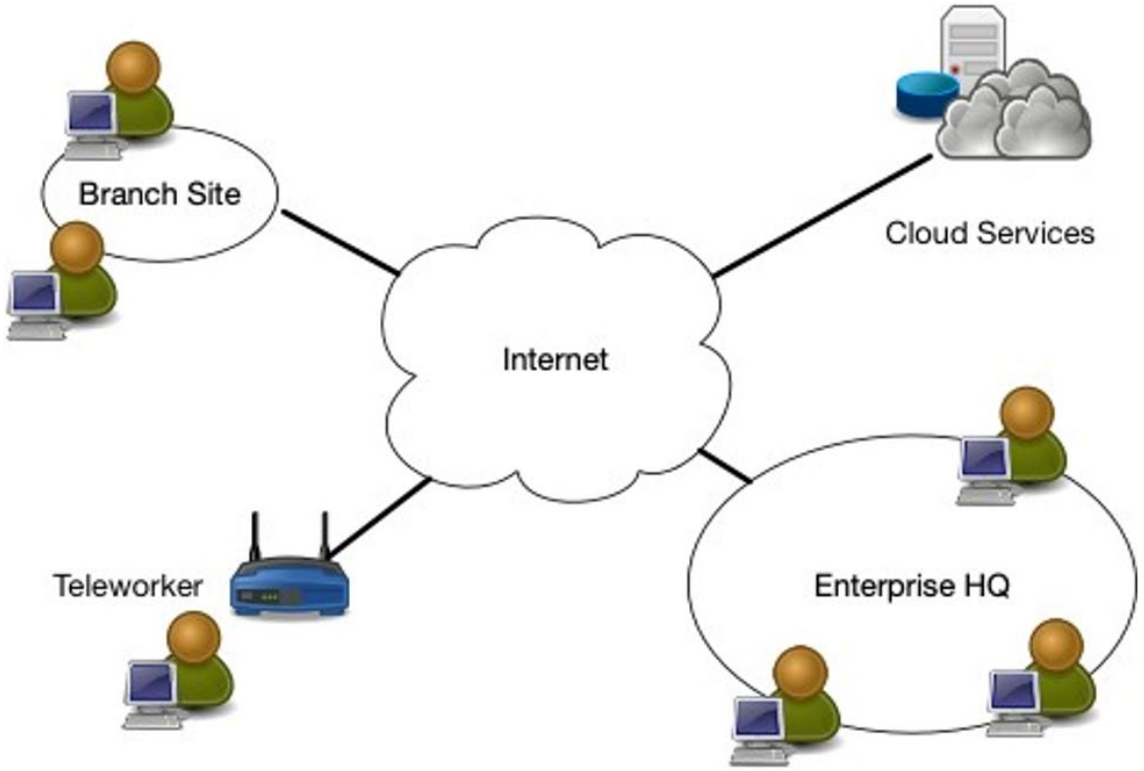


Figure 8: Enterprise with Remote Employees

Azienda Multi-Cloud/Cloud-to-Cloud

Un caso d'uso sempre più comune per l'implementazione di una Zero Trust Architecture (ZTA) è rappresentato da un'azienda che sfrutta più fornitori di servizi cloud. In questo scenario, l'azienda dispone di una rete locale ma utilizza due o più fornitori di servizi cloud per ospitare le proprie applicazioni, servizi e dati. Talvolta, l'applicazione o il servizio risiede su un servizio cloud diverso rispetto alla fonte dei dati. Per garantire prestazioni ottimali e semplificare la gestione, l'applicazione ospitata nel Fornitore di Servizi Cloud A dovrebbe essere in grado di connettersi direttamente alla fonte dei dati ospitata nel Fornitore di Servizi Cloud B, anziché essere obbligata a instradare il traffico attraverso la rete aziendale.

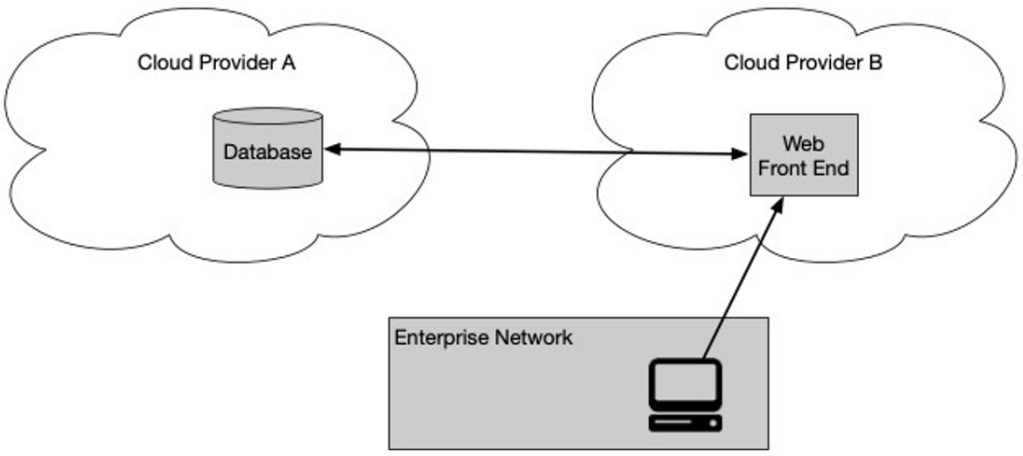


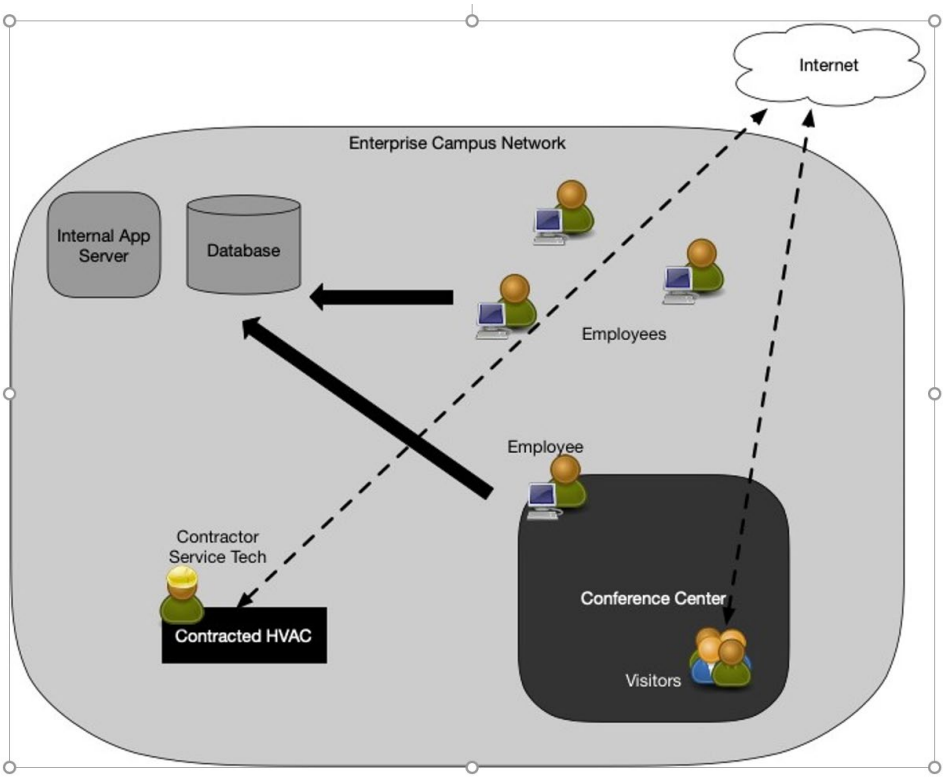
Figure 9: Multi-cloud Use Case

Questo caso d'uso rappresenta l'implementazione della specifica del Perimetro Definito dal Software (SDP) della CSA per la comunicazione tra server. Con l'evolversi delle aziende verso l'utilizzo di applicazioni e servizi basati su cloud, diventa sempre più evidente che fare affidamento esclusivamente sul perimetro aziendale

per la sicurezza comporta rischi. La Zero Trust Architecture (ZTA) affronta questa sfida considerando che non dovrebbe esserci differenza tra l'infrastruttura di rete gestita dall'azienda e quella di qualsiasi altro fornitore di servizi. Pertanto, l'approccio zero trust all'uso multi-cloud consiste nel posizionare i PEP ai punti di accesso di ogni applicazione, servizio e fonte di dati, indipendentemente dal provider cloud. Il PE e il PA possono essere implementati come servizi situati sia nel cloud che su un terzo provider di cloud. I clienti, attraverso un portale o un agente installato localmente, accedono direttamente ai PEP, consentendo all'azienda di gestire l'accesso alle risorse anche quando sono ospitate al di fuori della propria infrastruttura. Tuttavia, una sfida consiste nel fatto che i diversi fornitori di cloud possono implementare funzionalità simili in modi unici, richiedendo agli architetti aziendali di essere consapevoli di come implementare la ZTA aziendale con ciascun fornitore di cloud utilizzato.

Azienda che include visitatori in loco e/o fornitori di servizi

In un altro scenario comune, un'azienda ospita visitatori in loco e/o fornitori di servizi contrattati che richiedono un accesso limitato alle risorse aziendali per svolgere il proprio lavoro. Ad esempio, l'azienda dispone di applicazioni, servizi interni e risorse, compresi servizi appaltati a fornitori esterni che potrebbero richiedere accesso occasionale in loco per la manutenzione di sistemi come quelli di riscaldamento e illuminazione intelligenti. In un contesto di zero trust, l'azienda potrebbe consentire a questi dispositivi e ai tecnici di servizio in visita l'accesso a Internet, mentre protegge e oscura le risorse aziendali. Ad esempio, considerando un centro conferenze dell'azienda dove i visitatori interagiscono con i dipendenti, un'architettura ZTA basata su SDP può differenziare i dispositivi e i soggetti dei dipendenti, consentendo loro di accedere solo alle risorse aziendali appropriate. I visitatori del campus potrebbero essere limitati ad accedere solo a Internet, senza possibilità di accedere alle risorse aziendali. Inoltre, potrebbero essere prevenuti dal rilevare i servizi aziendali attraverso scansioni di rete attive, mantenendo così la sicurezza della rete aziendale.



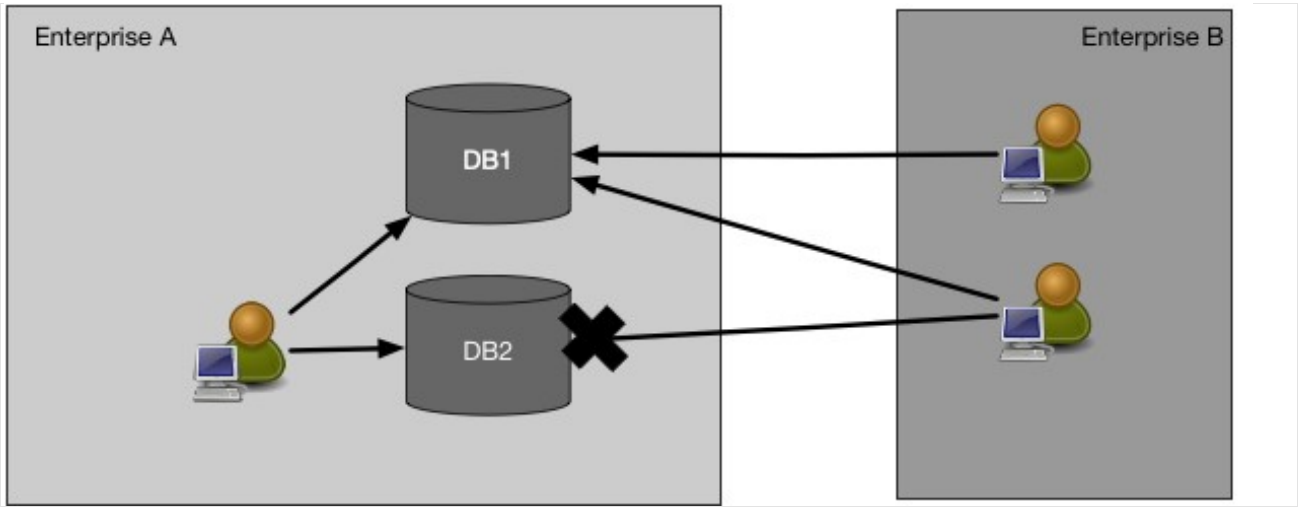
In questo scenario, i PEP e i PA possono essere ospitati sia come servizio cloud sia sulla LAN, a seconda dell'utilizzo dei servizi cloud. Gli asset aziendali possono essere dotati di un agente installato o accedere alle risorse tramite un portale. I PA garantiscono che gli asset non aziendali, che potrebbero non avere agenti

installati o non possono connettersi a un portale, non possano accedere alle risorse locali, ma possano accedere a Internet.

Aziende diverse con confini aziendali

In questo caso d'uso, si tratta della collaborazione tra aziende attraverso i confini aziendali, coinvolgendo due entità separate, come Azienda A e Azienda B. Questa collaborazione potrebbe riguardare progetti congiunti o scambi di dati tra le organizzazioni. Ad esempio, Azienda A potrebbe ospitare un database critico per un progetto e deve consentire l'accesso a determinati dati a dipendenti specifici di Azienda B.

Una soluzione per gestire questa collaborazione in modo efficiente è l'implementazione di un sistema di gestione delle identità federate. Questo permette alle due organizzazioni di stabilire rapidamente relazioni di trust e autorizzare l'accesso ai dati pertinenti senza compromettere la sicurezza. Utilizzando i PEP delle rispettive organizzazioni, i soggetti possono essere autenticati attraverso una comunità di identità federata, garantendo che solo gli utenti autorizzati abbiano accesso ai dati necessari. Questo approccio semplifica la gestione degli account e delle autorizzazioni, migliorando allo stesso tempo la sicurezza e la facilità d'uso nell'ambito della collaborazione tra aziende.



In entrambi i casi, sia nel Caso d'uso 1 (Sezione 4.1) sia nell'attuale scenario, si affronta la sfida di consentire l'accesso alle risorse aziendali da parte di dipendenti o soggetti esterni, senza la necessità di una connessione fisica alla rete aziendale. Questo può implicare l'accesso a risorse ospitate all'interno dell'ambiente aziendale o nel cloud.

Nel contesto di questa situazione, l'implementazione di un approccio Zero Trust significa che non ci si basa su regole di firewall o liste di controllo degli accessi (ACL) per autorizzare l'accesso. Invece, un PE e un PA possono essere ospitati come servizio cloud, consentendo l'accesso alle risorse senza la necessità di stabilire una VPN o soluzioni simili.

Per i dipendenti dell'Azienda B, potrebbe essere richiesto l'installazione di un agente software sui loro dispositivi o l'accesso alle risorse dati attraverso un gateway web, a seconda delle politiche di accesso e delle tecnologie adottate.

Inoltre, per quanto riguarda i servizi rivolti al pubblico, come pagine web pubbliche o servizi accessibili senza la necessità di credenziali, i principi della Zero Trust non si applicano direttamente. In questi casi, l'azienda potrebbe non avere il controllo completo sugli asset richiedenti e non richiedere credenziali per accedere a risorse pubbliche anonime.

Azienda con Servizi Rivolti al Pubblico o ai Clienti.

Le aziende possono stabilire politiche specifiche per gli utenti pubblici registrati, come i clienti con una relazione commerciale o utenti speciali come i familiari dei dipendenti. Queste politiche possono includere requisiti riguardanti la sicurezza delle credenziali, come la lunghezza delle password e il ciclo di vita delle stesse, oltre alla possibilità di richiedere l'autenticazione a più fattori (MFA) come opzione o requisito.

Tuttavia, è importante notare che le aziende sono limitate nelle politiche che possono implementare per questa categoria di utenti. Possono utilizzare le informazioni sulle richieste in ingresso per determinare lo stato del servizio pubblico e rilevare eventuali attività sospette. Ad esempio, un aumento improvviso delle richieste di accesso da parte di browser web sconosciuti o versioni obsolete potrebbe indicare un attacco automatizzato, e l'azienda potrebbe prendere misure per limitare l'accesso da questi clienti identificati.

Inoltre, le aziende devono essere consapevoli di eventuali leggi o regolamenti riguardanti la privacy e la raccolta di informazioni sugli utenti e sugli asset richiedenti. È importante rispettare tali normative e garantire che le politiche implementate siano conformi alle stesse.

Minacce Associate all'Architettura a Zero Trust

Nessuna azienda può eliminare completamente il rischio informatico. Tuttavia, quando integrata con le politiche esistenti di sicurezza informatica, la gestione delle identità e degli accessi, il monitoraggio continuo e l'igiene informatica generale, una ZTA correttamente implementata e mantenuta può contribuire a ridurre il rischio complessivo e proteggere contro molte minacce comuni.

È importante notare che alcune minacce possono presentare caratteristiche uniche quando si implementa una ZTA. Ad esempio, l'approccio zero trust richiede una rigorosa autenticazione e autorizzazione per ogni richiesta di accesso, il che può ridurre il rischio di accessi non autorizzati. Tuttavia, questa stessa natura rigorosa può anche portare a una maggiore complessità operativa e potenzialmente a un aumento dei falsi positivi, richiedendo un'attenzione particolare nella gestione delle politiche e nella configurazione dei sistemi. Inoltre, la decentralizzazione delle decisioni di accesso può rendere più difficile la rilevazione di attività sospette o di accessi anomali, poiché le azioni devono essere valutate in base al contesto e alla storia dell'utente o del dispositivo.

In definitiva, mentre una ZTA offre numerosi vantaggi nella gestione del rischio informatico, è essenziale riconoscere e affrontare le sfide uniche che possono emergere durante la sua implementazione e mantenimento.

5.1 Subversione del Processo Decisionale della ZTA

Nella Zero Trust Architecture (ZTA), il motore e l'amministratore delle politiche rappresentano componenti chiave per l'intera azienda. Ogni comunicazione tra le risorse aziendali avviene solo se approvata e, eventualmente, configurata dal Policy Engine (PE) e dal Policy Administrator (PA). Pertanto, è cruciale che questi componenti siano correttamente configurati e mantenuti.

Il rischio di manipolazioni non autorizzate o errori che potrebbero interrompere le operazioni aziendali è presente quando gli amministratori aziendali hanno accesso alla configurazione delle regole del PE. Allo stesso modo, un PA compromesso potrebbe consentire l'accesso a risorse non autorizzate, come un dispositivo personale compromesso.

Per mitigare questi rischi, è fondamentale garantire che i componenti PE e PA siano configurati e monitorati correttamente. Ogni modifica alla configurazione deve essere registrata e soggetta ad audit per garantire la conformità e la sicurezza dell'ambiente aziendale.

5.2 Denial-of-Service o Disruzione della Rete

Nella Zero Trust Architecture (ZTA), il Policy Administrator (PA) è un componente critico per il controllo dell'accesso alle risorse aziendali. Senza il consenso del PA e eventuali azioni di configurazione, le risorse aziendali non possono comunicare tra loro. Pertanto, qualsiasi interruzione o negazione dell'accesso ai PEP o al PA può avere un impatto negativo sulle operazioni aziendali. Le aziende possono mitigare questa minaccia posizionando l'applicazione delle politiche di sicurezza in un ambiente cloud protetto o replicandola in diverse posizioni seguendo le linee guida sulla resilienza cibernetica.

Tuttavia, queste misure mitigative non eliminano completamente il rischio. Attacchi come quelli della botnet Mirai dimostrano la capacità di produrre massicci attacchi DoS che possono interrompere i servizi Internet per milioni di utenti. Inoltre, un attaccante potrebbe intercettare e bloccare il traffico verso un PEP o un PA da parte di una parte o di tutti gli account utente all'interno di un'azienda, causando problemi solo a una parte dei soggetti aziendali. Questo rischio non è unico per la ZTA ed è anche presente nelle VPN remote legacy.

Esiste anche il rischio di interruzioni involontarie, ad esempio, se un fornitore di hosting mette offline un PE o un PA basato su cloud per un errore operativo. Le interruzioni dei servizi cloud, sia IaaS che SaaS, sono accadute in passato e potrebbero impedire a un'intera azienda di funzionare se il motore o l'amministratore delle politiche diventano inaccessibili.

Infine, c'è il rischio che le risorse aziendali non siano raggiungibili dal PA, anche se l'accesso viene concesso a un soggetto. Questo potrebbe accadere a causa di un attacco DDoS o di un utilizzo imprevisto e intenso, impedendo al PA di configurare il percorso di comunicazione dalla rete. Questo scenario è simile a qualsiasi altra interruzione di rete in cui alcuni o tutti i soggetti aziendali non possono accedere a una risorsa particolare a causa della sua non disponibilità.

5.3 Credenziali Rubate/Minaccia Interna

Una corretta implementazione della Zero Trust Architecture (ZTA), insieme alle politiche di sicurezza delle informazioni, alla resilienza e alle migliori pratiche, può notevolmente ridurre il rischio che un attaccante ottenga un ampio accesso tramite credenziali rubate o attacchi interni. Il principio fondamentale della ZTA, che implica la mancanza di fiducia implicita basata sulla posizione della rete, significa che gli attaccanti devono compromettere un account o un dispositivo esistente per ottenere un punto d'appoggio all'interno di un'azienda.

Nel contesto della ZTA, un'implementazione efficace dovrebbe impedire a un account o a un asset compromesso di accedere a risorse al di fuori del suo normale ambito di competenza o modelli di accesso. Ciò significa che gli account con politiche di accesso alle risorse che interessano agli attaccanti sarebbero i bersagli principali. Gli attaccanti possono utilizzare varie tecniche, come phishing o ingegneria sociale, per ottenere credenziali di account preziosi, che possono essere considerati preziosi a seconda della loro motivazione, come ad esempio l'accesso a risorse finanziarie o di pagamento.

L'implementazione di autenticazione multifattoriale (MFA) per le richieste di accesso può ridurre il rischio di perdita di informazioni da un account compromesso. Tuttavia, è importante notare che un attaccante con credenziali valide o un insider malintenzionato potrebbe comunque essere in grado di accedere a risorse per le quali l'account ha ottenuto l'accesso.

La ZTA riduce il rischio e impedisce a tutti gli account o asset compromessi di muoversi lateralmente all'interno della rete. Se le credenziali compromesse non sono autorizzate ad accedere a una particolare risorsa, continueranno a essere negate l'accesso a quella risorsa. Inoltre, l'utilizzo di un algoritmo di fiducia contestuale è più probabile che rilevi e risponda rapidamente a questo tipo di attacco rispetto a una rete legacy basata su perimetri. Il contesto può rilevare modelli di accesso che si discostano dal comportamento normale e negare all'account compromesso o alla minaccia interna l'accesso alle risorse sensibili.

5.4 Visibilità sulla Rete

L'azienda potrebbe non essere in grado di ispezionare in profondità il traffico crittografato sulla rete, ma potrebbe ancora raccogliere metadati su questo tipo di traffico e utilizzarli per identificare potenziali minacce. I metadati includono informazioni come gli indirizzi di origine e destinazione, la dimensione dei pacchetti, i tempi di trasmissione e altre informazioni di base sulle comunicazioni. Questi metadati possono essere analizzati per rilevare pattern anomali o comportamenti sospetti che potrebbero indicare un attacco o un comportamento dannoso.

Inoltre, le tecniche di apprendimento automatico possono essere utilizzate per analizzare il traffico crittografato e categorizzarlo come valido o potenzialmente dannoso. Questo approccio consente all'azienda di identificare eventuali anomalie nel traffico crittografato e prendere misure correttive o di mitigazione di conseguenza.

Anche se l'azienda non può esaminare direttamente il contenuto crittografato, può ancora sfruttare i metadati e le tecniche di apprendimento automatico per rilevare e rispondere a potenziali minacce sulla rete. Questo approccio consente una forma di analisi dei dati che può essere efficace anche in presenza di traffico crittografato.

5.5 Archiviazione di Informazioni di Sistema e Rete

Una minaccia correlata al monitoraggio e all'analisi del traffico di rete è rappresentata dal rischio associato al componente di analisi stesso. Se i dati raccolti durante le scansioni del monitoraggio, il traffico di rete e i metadati vengono conservati per scopi come la creazione di politiche contestuali o l'analisi forense successiva, tali dati diventano un obiettivo per gli attaccanti. Analogamente ai diagrammi di rete e ai file di configurazione, queste risorse devono essere protette poiché forniscono informazioni sull'architettura aziendale e possono essere utilizzate per identificare asset vulnerabili per ulteriori attacchi.

Un'altra fonte di informazioni che un attaccante potrebbe sfruttare in un'azienda Zero Trust è lo strumento di gestione utilizzato per definire le politiche di accesso. Questo componente contiene le regole di accesso alle risorse e può rivelare agli attaccanti quali account sono più preziosi da compromettere, come ad esempio quelli che hanno accesso alle risorse critiche.

Per proteggere questi dati preziosi, è essenziale implementare adeguate protezioni per prevenire l'accesso non autorizzato e gli attacchi. Le risorse critiche dovrebbero avere politiche di accesso rigorose e essere accessibili solo da account amministrativi designati o dedicati, garantendo così un livello aggiuntivo di sicurezza.

5.6 Affidamento su Formati Dati o Soluzioni Proprietari

La Zero Trust Architecture (ZTA) si basa su diverse fonti di dati per prendere decisioni di accesso, inclusi dati sul soggetto richiedente, sugli asset utilizzati, intelligence aziendale ed esterna, e analisi delle minacce. Tuttavia, spesso gli asset utilizzati per memorizzare e processare queste informazioni non seguono uno standard aperto e comune per l'interoperabilità. Ciò può causare problemi quando un'azienda è bloccata con

un sottoinsieme di fornitori a causa di problemi di compatibilità. Se un fornitore ha un problema di sicurezza o subisce un'interruzione, un'azienda potrebbe avere difficoltà a migrare verso un nuovo fornitore senza costi estremi o un lungo periodo di transizione. Questo rischio non è unico per la ZTA, ma data la sua dipendenza dall'accesso dinamico alle informazioni, la disruzione può influenzare gravemente le funzioni aziendali principali. Per mitigare questi rischi, le aziende dovrebbero valutare i fornitori di servizi in modo olistico, considerando non solo i controlli di sicurezza, ma anche i costi di commutazione aziendale e la gestione del rischio della catena di approvvigionamento, oltre ai fattori più tradizionali come le prestazioni e la stabilità.

5.7 Uso di Entità Non-persona (NPE) nell'Amministrazione della ZTA

L'intelligenza artificiale e altri agenti software vengono sempre più utilizzati per affrontare problemi di sicurezza nelle reti aziendali, spesso interagendo con i componenti di gestione della Zero Trust Architecture (ZTA) al posto degli amministratori umani. Tuttavia, l'autenticazione di questi componenti in un'implementazione ZTA presenta sfide aperte. Si presume che tali sistemi tecnologici automatizzati utilizzino un qualche mezzo per autenticarsi quando si interfacciano con i componenti delle risorse tramite API.

Il rischio principale nell'uso della tecnologia automatizzata per configurare e applicare le politiche è la possibilità di falsi positivi (azioni innocue erroneamente identificate come attacchi) e falsi negativi (attacchi erroneamente identificati come attività normali), che potrebbero compromettere la sicurezza aziendale. Tuttavia, questo rischio può essere mitigato con regolari analisi e ottimizzazioni per migliorare il processo decisionale.

Un'altra preoccupazione è che un attaccante potrebbe indurre o costringere un agente software a eseguire compiti non autorizzati. Poiché tali agenti potrebbero avere livelli di autenticazione inferiori rispetto agli utenti umani, ad esempio, utilizzando chiavi API anziché autenticazione multifattore (MFA), potrebbero essere più vulnerabili all'inganno. L'accesso alle credenziali di tali agenti potrebbe anche consentire agli attaccanti di impersonarli, aumentando il rischio di compromissione della sicurezza.

Migrare verso un'Architettura a Zero Trust

L'implementazione della Zero Trust Architecture (ZTA) rappresenta un percorso evolutivo piuttosto che una sostituzione radicale dell'infrastruttura e dei processi esistenti. Le organizzazioni dovrebbero adottare gradualmente i principi della zero trust, apportando modifiche ai processi e adottando soluzioni tecnologiche che proteggano i dati di maggior valore. Molte aziende continueranno a operare in un ambiente ibrido che combina elementi della zero trust e del modello basato sul perimetro, investendo contemporaneamente in iniziative di modernizzazione dell'IT. Un piano di modernizzazione dell'IT che integri i principi della ZT può facilitare la migrazione graduale dei flussi di lavoro su piccola scala.

Il percorso di transizione di un'azienda verso una strategia basata sulla zero trust dipende dalla sua attuale postura in termini di sicurezza informatica e operazioni. Prima di poter implementare un ambiente significativo focalizzato sulla ZT, un'azienda deve raggiungere un livello di competenza di base. Ciò include l'identificazione e la catalogazione di asset, soggetti, processi aziendali, flussi di traffico e la mappatura delle dipendenze per l'azienda. Queste informazioni sono essenziali per sviluppare un elenco di processi aziendali candidati e per comprendere i soggetti e gli asset coinvolti in tali processi.

Architettura a Zero Trust Pura

In un contesto greenfield, dove si parte da zero senza vincoli di infrastruttura esistente, è possibile progettare e costruire un'architettura a zero trust sin dall'inizio. Identificando le applicazioni, i servizi e i flussi di lavoro necessari, l'azienda può creare un'architettura basata sui principi della zero trust per gestire tali flussi di lavoro. Una volta definiti i flussi di lavoro, si possono identificare i componenti necessari e mappare le

interazioni tra di essi. Da qui, inizia un processo di ingegnerizzazione e organizzazione per la costruzione dell'infrastruttura e la configurazione dei componenti, che potrebbe richiedere anche cambiamenti organizzativi.

Tuttavia, è importante notare che questa opzione è di solito impraticabile per organizzazioni con una rete esistente, come le agenzie federali. Tuttavia, ci sono situazioni in cui un'organizzazione potrebbe essere incaricata di una nuova responsabilità che richiede la costruzione di una nuova infrastruttura. In questi casi, è possibile introdurre concetti di zero trust nella progettazione della nuova infrastruttura. Ad esempio, un'agenzia potrebbe ricevere l'incarico di sviluppare una nuova applicazione o servizio e potrebbe progettare l'infrastruttura attorno ai principi della zero trust, implementando controlli come la valutazione della fiducia dei soggetti prima di concedere l'accesso e la creazione di micro-perimetri attorno alle nuove risorse. Tuttavia, il successo di tale approccio dipende dalla dipendenza della nuova infrastruttura dalle risorse esistenti, come i sistemi di gestione delle identità.

Architettura ibrida ZTA e basata su perimetro

È improbabile che qualsiasi azienda di dimensioni significative possa adottare completamente la zero trust in un'unica transizione tecnologica. È più probabile che vi sia un periodo di transizione in cui i flussi di lavoro della zero trust convivono con quelli non basati su tale approccio. La migrazione verso la zero trust potrebbe avvenire gradualmente, un processo aziendale alla volta. L'azienda deve garantire che gli elementi fondamentali, come la gestione delle identità, la gestione dei dispositivi e la registrazione degli eventi, siano sufficientemente flessibili da funzionare in un'architettura di sicurezza ibrida che combina elementi della zero trust e del perimetro tradizionale. Gli architetti aziendali potrebbero preferire soluzioni di zero trust che possano integrarsi facilmente con i componenti esistenti. La migrazione di un flusso di lavoro esistente verso la zero trust probabilmente richiederà una ridisegnazione parziale o completa. Durante questo processo, le aziende potrebbero cogliere l'opportunità per adottare pratiche di ingegneria dei sistemi sicure, se non lo hanno già fatto per i loro flussi di lavoro.

Passaggi per introdurre la ZTA in una rete architettata basata su perimetro

Migrare verso la Zero Trust Architecture (ZTA) richiede una conoscenza dettagliata degli asset, dei soggetti e dei processi aziendali all'interno dell'organizzazione. Questa conoscenza è essenziale perché il Punto di Esecuzione (PE) possa valutare correttamente le richieste di risorse. Se manca una comprensione completa, il processo aziendale rischia di fallire poiché il PE potrebbe negare le richieste a causa di informazioni insufficienti. Questo rischio è particolarmente elevato se ci sono implementazioni di "shadow IT" non riconosciute all'interno dell'organizzazione. Prima di intraprendere azioni per introdurre la ZTA in un'azienda, è necessario condurre un'attenta identificazione degli asset, dei soggetti, dei flussi di dati e dei flussi di lavoro. Questa consapevolezza costituisce il fondamento essenziale che deve essere stabilito prima di procedere con l'implementazione della ZTA. Un'azienda non può determinare quali nuovi processi o sistemi devono essere implementati senza una chiara comprensione dello stato attuale delle sue operazioni. Questi processi di identificazione possono essere eseguiti parallelamente, ma entrambi sono strettamente legati all'analisi dei processi aziendali dell'organizzazione. Questi passaggi possono essere mappati ai processi del Framework di Gestione del Rischio (RMF), poiché l'adozione della ZTA è un processo finalizzato alla riduzione del rischio per le funzioni aziendali. Il percorso per implementare la ZTA può essere visualizzato e organizzato seguendo i passaggi illustrati nella Figura 12.

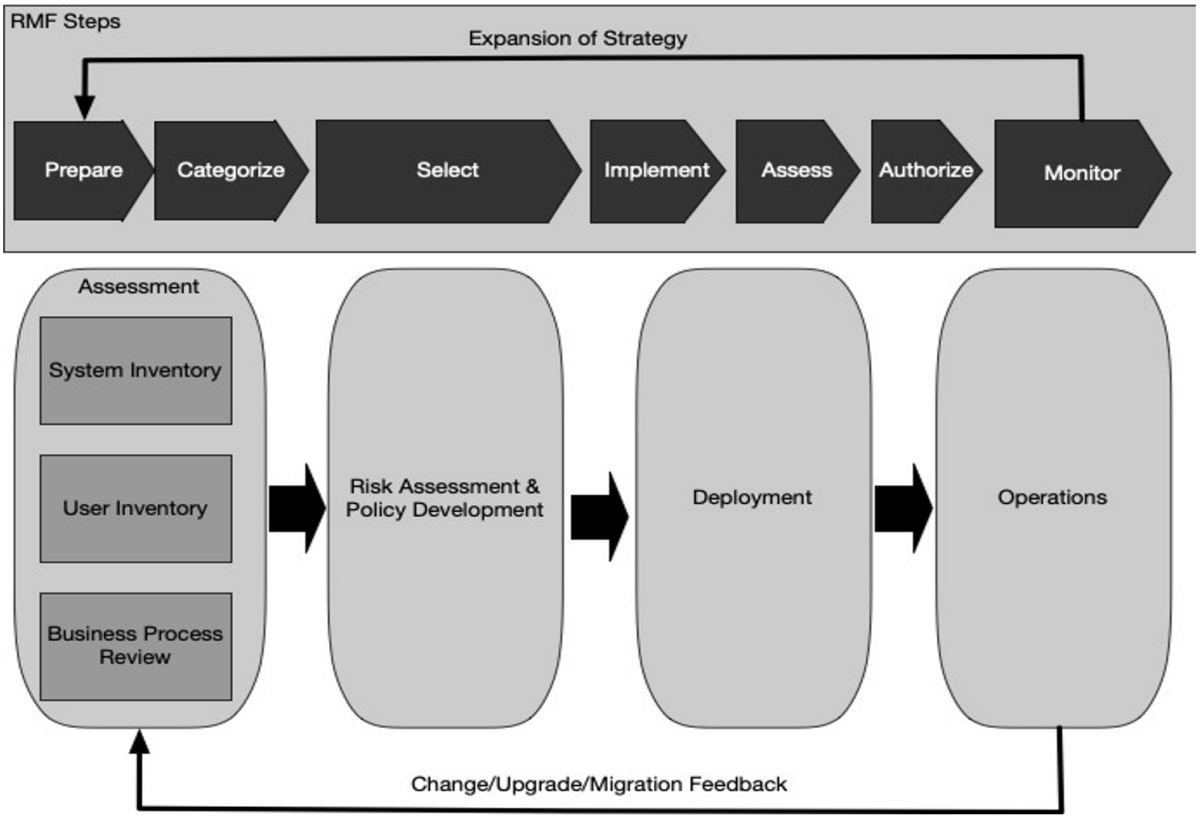


Figure 12: ZTA Deployment Cycle

Dopo la creazione dell'inventario iniziale, è essenziale stabilire un ciclo regolare di manutenzione e aggiornamento. Questo ciclo può comportare modifiche che influenzano direttamente o indirettamente i processi aziendali e, pertanto, è necessaria un'attenta valutazione di tali impatti. Ad esempio, anche un cambiamento apparentemente minore, come il passaggio a nuovi fornitori di certificati digitali, potrebbe avere conseguenze significative che vanno oltre la superficie. Queste conseguenze potrebbero coinvolgere la gestione dello store di certificati radice, il monitoraggio dei log di Certificate Transparency e altri aspetti che richiedono un'analisi approfondita per essere compresi appieno. Pertanto, è fondamentale condurre valutazioni approfondite dei processi aziendali durante ogni fase di manutenzione e aggiornamento per garantire che le modifiche apportate non compromettano l'integrità e l'efficienza complessiva delle operazioni aziendali.

Identificare gli Attori nell'Azienda

Affinché un'azienda operi con successo secondo i principi della zero trust, è essenziale che il Punto di Emissione (PE) abbia una comprensione approfondita dei soggetti aziendali. Questi soggetti possono includere sia individui umani che entità non personali (NPE), come gli account di servizio utilizzati per interagire con le risorse aziendali. Gli utenti con privilegi speciali, come gli sviluppatori o gli amministratori di sistema, richiedono un'attenzione particolare quando si assegnano attributi o ruoli in un'architettura di sicurezza basata sulla zero trust. In molte architetture legacy, questi account possono disporre di autorizzazioni generalizzate per accedere a tutte le risorse aziendali, il che rappresenta un rischio significativo per la sicurezza. La zero trust Architecture (ZTA) dovrebbe consentire agli sviluppatori e agli amministratori di avere una flessibilità sufficiente per soddisfare i requisiti aziendali, utilizzando registri e azioni di audit per identificare i modelli di comportamento di accesso. Le implementazioni della ZTA possono richiedere agli amministratori di soddisfare criteri di fiducia o rigorosi standard di sicurezza come quelli indicati nel documento NIST SP 800-63A, Sezione 5. Questo approccio garantisce che l'accesso alle risorse sia concesso

in base a una valutazione continua del rischio e della fiducia, riducendo così il rischio di violazioni della sicurezza.

Identificare gli Asset di Proprietà dell'Azienda

Di seguito si evidenzia l'importanza dell'identificazione e della gestione degli asset nell'implementazione della Zero Trust Architecture (ZTA). Questo comprende sia dispositivi di proprietà dell'azienda che quelli non di proprietà che possono accedere alle risorse aziendali. È essenziale catalogare e monitorare accuratamente questi asset, compresi hardware, account utente, e applicazioni. Inoltre, l'azienda deve essere in grado di valutare rapidamente i nuovi asset scoperti sulla propria infrastruttura. Queste informazioni influenzano le decisioni di accesso alle risorse da parte del Punto di Emissione (PE). In particolare, il testo sottolinea la necessità di gestire il "shadow IT", le risorse aziendali non ufficialmente riconosciute e gestite. Le agenzie federali hanno iniziato a identificare gli asset aziendali, spesso attraverso programmi come HWAM e Software Asset Management (SWAM). È essenziale che i processi aziendali siano progettati considerando la ZTA, e i programmi devono essere flessibili per adattarsi ai cambiamenti nell'azienda nel tempo.

Architettura dei Servizi Zero Trust e Provider di riferimento:

Il servizio Zero Trust si basa su componenti chiave per creare un ambiente di sicurezza robusto:

- L'autenticazione Multi-Fattore (MFA) richiede più metodi di autenticazione per verificare l'identità dell'utente, migliorando la sicurezza rispetto alle tradizionali password.
- L'autorizzazione Granulare definisce politiche di accesso basate su ruoli, privilegi e altri attributi, permettendo solo l'accesso a risorse specifiche necessarie.
- La Microsegmentazione suddivide la rete in segmenti più piccoli, limitando le aree di attacco e impedendo il movimento laterale degli attaccanti.
- Il Monitoraggio Continuo analizza costantemente il traffico di rete e il comportamento degli utenti per individuare minacce o anomalie e rispondere prontamente.

Principali Provider e Servizi Zero Trust:

1. Microsoft Azure Active Directory (Azure AD)
    a. Costi: Azure AD offre una varietà di piani di licenza, che possono includere funzionalità di Zero Trust come MFA e Conditional Access. I costi variano in base al numero di utenti e alle funzionalità desiderate.
    b. Benefici: Integrazione nativa con altri servizi Azure, ampio supporto per l'autenticazione basata su standard come OAuth e OpenID Connect, e strumenti avanzati per la gestione delle identità e degli accessi.
2. Okta
    a. Costi: Okta offre piani di licenza basati sul numero di utenti e sulle funzionalità desiderate. I costi possono variare a seconda del livello di servizio e delle opzioni di supporto.
    b. Benefici: Ampia compatibilità con un'ampia gamma di applicazioni SaaS e servizi cloud, supporto per l'integrazione con Active Directory e altre fonti di identità, e strumenti avanzati per la gestione degli accessi e la conformità.
3. Zscaler Private Access
    a. Costi: Zscaler offre piani di licenza basati sul consumo, calcolati in base al volume di traffico e al numero di utenti. I costi possono variare in base alle opzioni di configurazione e alle funzionalità aggiuntive desiderate.
    b. Benefici: Accesso sicuro alle risorse aziendali senza la necessità di una VPN tradizionale, capacità di implementare politiche di Zero Trust per il controllo granulare degli accessi, e riduzione dei rischi di sicurezza associati alla connettività diretta alla rete aziendale.
4. Cisco Zero Trust Security

a. Costi: I costi variano in base alle esigenze specifiche dell'organizzazione e alla configurazione del servizio. Cisco offre una gamma di soluzioni e pacchetti personalizzati per soddisfare le esigenze di sicurezza di diverse organizzazioni.
b. Benefici: Ampia suite di prodotti e servizi per la sicurezza Zero Trust, compresi firewall, soluzioni per l'accesso remoto sicuro e strumenti per la protezione degli endpoint, oltre a un'ampia rete di partner e supporto per la gestione e l'integrazione.

Considerazioni sui Costi e sui Benefici:

In sintesi, i servizi Zero Trust comportano costi variabili basati sulle esigenze specifiche dell'organizzazione, l'implementazione e le funzionalità richieste, compresi licenze, implementazione, manutenzione, supporto e costi operativi. Tuttavia, offrono benefici significativi come una maggiore sicurezza delle risorse digitali e delle reti aziendali, una riduzione del rischio di violazioni della sicurezza e perdite di dati, il miglioramento della conformità normativa, un aumento della visibilità e del controllo degli accessi, e il supporto per modelli di lavoro flessibili come il lavoro remoto e la mobilità aziendale. In ultima analisi, sebbene i costi possano variare, i benefici della protezione dei dati e della riduzione dei rischi di sicurezza possono essere sostanziali per le organizzazioni che operano in un ambiente sempre più complesso e minaccioso.

1. Microsegmentazione:

In sintesi, la microsegmentazione è una pratica cruciale nell'architettura Zero Trust che prevede la suddivisione della rete in microsegmenti distinti. Questo approccio isola e protegge ciascuna parte della rete da potenziali minacce, limitando il movimento laterale degli attaccanti anche in caso di compromissione di un segmento.

2. Autenticazione Multi-Fattore (MFA):

L'autenticazione multi-fattore è essenziale nell'architettura Zero Trust. Oltre alle credenziali tradizionali, richiede prove aggiuntive di identità, come token generati da app mobili o codici SMS. Questo livello extra rende più difficile per gli attaccanti accedere alle risorse anche se hanno ottenuto le credenziali di accesso.

3. Autorizzazione Granulare:

Nell'architettura Zero Trust, l'autorizzazione è granulare e basata sul principio del "least privilege", il che significa che gli utenti ottengono solo l'accesso alle risorse e alle funzionalità di cui hanno effettivamente bisogno per svolgere il proprio lavoro. Le politiche di accesso sono definite in modo preciso e possono essere regolate in base al ruolo dell'utente, al contesto dell'accesso e ad altri fattori.

4. Monitoraggio Continuo:

Il monitoraggio continuo è essenziale per l'architettura Zero Trust. Tutte le attività di rete e di accesso vengono costantemente monitorate e analizzate per individuare eventuali comportamenti sospetti o anomalie. Le soluzioni di sicurezza Zero Trust utilizzano analisi comportamentale avanzate e machine learning per rilevare e rispondere rapidamente alle minacce in tempo reale.

5. Sicurezza a Livello di Applicazione:

L'architettura Zero Trust si concentra anche sulla sicurezza a livello di applicazione. Questo significa che ogni applicazione e servizio deve essere protetto indipendentemente dalla sua posizione all'interno della rete, che si trovi nel data center aziendale, nel cloud o su dispositivi remoti. Le politiche di sicurezza vengono applicate direttamente alle applicazioni stesse, piuttosto che alla rete circostante.

6. Isolamento dei Dati Sensibili:
I dati sensibili vengono isolati e protetti in modo rigoroso nell'architettura Zero Trust. Le tecnologie di crittografia e di gestione delle chiavi vengono utilizzate per proteggere i dati in transito e a riposo, riducendo il rischio di compromissione da parte di attaccanti o insider malintenzionati.

In sintesi, l'architettura Zero Trust si basa su principi come microsegmentazione, autenticazione multi-fattore, autorizzazione granulare, monitoraggio continuo, sicurezza a livello di applicazione e isolamento dei dati sensibili per garantire una protezione completa delle reti e delle risorse digitali. Questo approccio è proattivo e mira a ridurre al minimo il rischio di violazioni della sicurezza, indipendentemente dalla posizione degli utenti o delle risorse nella rete.

Architettura di ZeroVPN:
L'architettura ZeroVPN non è un concetto o una tecnologia standard definiti come Zero Trust o le VPN tradizionali come IPsec, OpenVPN o WireGuard. Ecco una descrizione di come potrebbe funzionare un sistema VPN che si ispira ai principi di Zero Trust, cercando di eliminare le tradizionali "reti fidate" e adottando un approccio di "never trust, always verify" per l'accesso alla rete.

1. Autenticazione e Autorizzazione Forte:
ZeroVPN inizia la sessione con un rigoroso processo di autenticazione multi-fattore (MFA) per ogni utente che tenta di accedere alla rete. Questo può includere l'uso di credenziali utente, certificati digitali, token generati dinamicamente e altri metodi di autenticazione. Prima di concedere l'accesso, il sistema verifica l'identità dell'utente e applica politiche di autorizzazione granulari basate sui suoi privilegi e ruoli definiti.

2. Microsegmentazione della Rete:
La rete ZeroVPN è suddivisa in microsegmenti più piccoli e distinti, ognuno dei quali è isolato e protetto da potenziali minacce. Ogni segmento può contenere risorse specifiche, come server, applicazioni o servizi, e l'accesso a ciascun segmento è controllato in modo rigoroso in base alle politiche di sicurezza stabilite.

3. Crittografia End-to-End:
Tutto il traffico all'interno della rete ZeroVPN è crittografato end-to-end per garantire la privacy e la sicurezza dei dati in transito. Viene utilizzata una crittografia robusta per proteggere le comunicazioni tra i dispositivi e i server, impedendo a potenziali attaccanti di intercettare o manipolare il traffico di rete.

4. Monitoraggio Continuo e Rilevamento delle Minacce:
Un componente chiave della rete ZeroVPN è il monitoraggio continuo delle attività di rete e l'analisi comportamentale per individuare comportamenti sospetti o anomalie. Questo sistema di rilevamento delle minacce utilizza tecnologie avanzate come machine learning per identificare e rispondere rapidamente alle potenziali minacce alla sicurezza.

5. Sicurezza a Livello di Applicazione:
Oltre alla protezione della rete, ZeroVPN si concentra anche sulla sicurezza a livello di applicazione. Le applicazioni e i servizi sono protetti indipendentemente dalla loro posizione nella rete, che si trovino nel data center aziendale, nel cloud o su dispositivi remoti. Le politiche di sicurezza vengono applicate direttamente alle applicazioni stesse, garantendo una protezione completa delle risorse digitali.

6. Gestione Centralizzata delle Politiche di Sicurezza:
Tutte le politiche di sicurezza e di accesso sono gestite centralmente tramite un pannello di controllo unificato. Questo consente agli amministratori di definire e applicare in modo coerente le politiche di

sicurezza in tutta la rete ZeroVPN, semplificando la gestione e garantendo una protezione uniforme delle risorse digitali.

In conclusione, l'architettura ZeroVPN adotta un approccio di "never trust, always verify" per la sicurezza delle reti, combinando principi come autenticazione e autorizzazione forti, microsegmentazione della rete, crittografia end-to-end, monitoraggio continuo delle minacce, sicurezza a livello di applicazione e gestione centralizzata delle politiche di sicurezza. Questo approccio proattivo mira a garantire una protezione completa delle risorse digitali, riducendo al minimo il rischio di violazioni della sicurezza.

Architettura di Tailscale

Tailscale è una soluzione di rete privata virtuale (VPN) che offre una connettività sicura e semplice tra dispositivi e reti distribuite. La sua architettura è progettata per fornire un accesso affidabile e sicuro alle risorse di rete, sfruttando tecnologie moderne e principi di sicurezza avanzati. Di seguito viene presentata una descrizione dell'architettura di Tailscale:

1. Modello di Connessione Peer-to-Peer:

- Tailscale utilizza un modello di connessione peer-to-peer, in cui ogni dispositivo connesso alla rete Tailscale costituisce un nodo peer autonomo.
- Questo modello semplifica la configurazione e la gestione della rete, eliminando la necessità di server intermedi per la connessione VPN.

2. Crittografia e Sicurezza:

- Tailscale utilizza crittografia forte e sicura per proteggere le comunicazioni tra dispositivi, incluso l'utilizzo di Curve25519 per gli scambi di chiavi e ChaCha20 per la crittografia del traffico.
- Questo garantisce la privacy e la protezione dei dati in transito, riducendo il rischio di intercettazioni o manipolazioni da parte di terze parti.

3. Autenticazione e Gestione delle Identità:

- Ogni dispositivo Tailscale è associato a un'identità unica, che viene utilizzata per autenticare e autorizzare le connessioni alla rete.
- Tailscale utilizza un sistema di autenticazione basato su chiavi pubbliche e private per verificare l'identità dei dispositivi e garantire l'accesso sicuro alla rete.

4. Connessioni Sicure tramite Tunnelling:

- Tailscale utilizza il tunnelling per instradare il traffico attraverso connessioni sicure tra i dispositivi.
- Il protocollo di tunnelling utilizzato da Tailscale è basato su WireGuard, un protocollo VPN moderno e performante noto per la sua efficienza e sicurezza.

5. Gestione Centrale e Controllo degli Accessi:

- Tailscale offre una console di gestione centralizzata che consente agli amministratori di configurare e monitorare la rete Tailscale.
- Gli amministratori possono definire e applicare in modo coerente le politiche di accesso e sicurezza, gestire le identità dei dispositivi e monitorare l'attività di rete attraverso un'interfaccia utente intuitiva.

6. Integrazione con Ambienti Cloud e Locali:

- Tailscale offre integrazioni con ambienti cloud e reti locali, consentendo ai dispositivi Tailscale di comunicare in modo sicuro sia all'interno di reti locali che attraverso Internet.
- Questa flessibilità consente alle organizzazioni di estendere facilmente la loro infrastruttura di rete e fornire accesso sicuro ai dipendenti e ai dispositivi remoti.

7. Monitoraggio e Diagnostica Avanzati:

- Tailscale fornisce strumenti avanzati per il monitoraggio e la diagnostica della rete, inclusi report sull'attività di rete, monitoraggio delle prestazioni e notifiche di sicurezza.
- Questi strumenti consentono agli amministratori di identificare e risolvere rapidamente eventuali problemi di rete e mantenere elevati standard di sicurezza e affidabilità.

Conclusioni:

L'architettura di Tailscale è progettata per offrire un'esperienza di rete sicura, affidabile e facile da usare per organizzazioni di qualsiasi dimensione. Utilizzando un modello di connessione peer-to-peer, crittografia avanzata, autenticazione basata su chiavi pubbliche, tunnelling sicuro e una console di gestione centralizzata, Tailscale semplifica la connettività tra dispositivi e reti distribuite, consentendo alle organizzazioni di estendere facilmente la loro infrastruttura di rete e garantire un accesso sicuro alle risorse aziendali.

Architettura Tailscale Zero Trust

Tailscale Zero Trust è una implementazione dei principi Zero Trust all'interno dell'architettura di Tailscale, una soluzione di rete privata virtuale (VPN). Tailscale Zero Trust mira a fornire un accesso sicuro e granulare alle risorse di rete, applicando controlli di sicurezza basati sull'identità e sul contesto dell'accesso. Di seguito viene presentata una relazione tecnica sull'architettura Tailscale Zero Trust:

1. Architettura Peer-to-Peer:

- Tailscale Zero Trust utilizza un modello di connessione peer-to-peer, in cui ogni dispositivo connesso alla rete Tailscale costituisce un nodo peer autonomo.
- Questo modello elimina la necessità di un server centrale per la gestione delle connessioni VPN, riducendo i punti di vulnerabilità e semplificando la gestione della rete.

2. Crittografia e Sicurezza:

- Tailscale Zero Trust utilizza crittografia forte e sicura per proteggere le comunicazioni tra dispositivi, inclusa l'autenticazione basata su chiavi pubbliche e private.
- Tutte le comunicazioni tra i nodi Tailscale sono crittografate utilizzando il protocollo WireGuard, garantendo la privacy e la sicurezza dei dati in transito.

3. Autenticazione e Autorizzazione Granulare:

- Ogni dispositivo Tailscale è associato a un'identità unica, che viene utilizzata per autenticare e autorizzare le connessioni alla rete.
- Tailscale Zero Trust implementa un modello di autorizzazione granulare, consentendo agli amministratori di definire e applicare politiche di accesso basate sull'identità, sul ruolo e sul contesto dell'accesso.

4. Segmentazione della Rete e Isolamento delle Risorse:

- Tailscale Zero Trust supporta la segmentazione della rete e l'isolamento delle risorse, consentendo agli amministratori di suddividere la rete in segmenti più piccoli e controllare l'accesso alle risorse in base ai requisiti di sicurezza.
- Questo approccio riduce la superficie di attacco e limita il movimento laterale degli attaccanti all'interno della rete.

5. Monitoraggio Continuo e Analisi Comportamentale:

- Tailscale Zero Trust offre funzionalità avanzate di monitoraggio continuo e analisi comportamentale per individuare e rispondere prontamente alle minacce alla sicurezza.

- Gli amministratori possono monitorare l'attività di rete, raccogliere dati sul comportamento degli utenti e dei dispositivi e identificare potenziali anomalie o attività sospette.

6. Gestione Centralizzata delle Politiche di Sicurezza:

- Tailscale Zero Trust fornisce una console di gestione centralizzata che consente agli amministratori di definire e applicare politiche di sicurezza in modo coerente in tutta l'organizzazione.
- Gli amministratori possono configurare regole di accesso, autorizzazioni e controlli di sicurezza attraverso un'interfaccia utente intuitiva.

7. Integrazione con Ambienti Cloud e Locali:

- Tailscale Zero Trust offre integrazioni con ambienti cloud e reti locali, consentendo ai dispositivi Tailscale di comunicare in modo sicuro sia all'interno di reti locali che attraverso Internet.
- Questa flessibilità consente alle organizzazioni di estendere facilmente la loro infrastruttura di rete e garantire un accesso sicuro alle risorse aziendali, indipendentemente dalla posizione dei dispositivi.

Conclusioni:

L'architettura di Tailscale Zero Trust combina i principi Zero Trust con le funzionalità avanzate di Tailscale per offrire un'esperienza di rete sicura, affidabile e facile da usare. Utilizzando un modello peer-to-peer, crittografia avanzata, autenticazione basata su chiavi pubbliche, autorizzazione granulare e segmentazione della rete, Tailscale Zero Trust consente alle organizzazioni di proteggere efficacemente le loro risorse di rete e garantire un accesso sicuro ai dipendenti e ai dispositivi remoti.

Architettura di Headscale

Headscale è un progetto open-source che offre una soluzione per la gestione centralizzata di reti Tailscale. Si basa sul protocollo Tailscale per fornire una connettività sicura e semplificata tra dispositivi, consentendo agli amministratori di gestire in modo centralizzato le identità, le autorizzazioni e le politiche di accesso. Di seguito viene presentata una relazione tecnica sull'architettura di Headscale:

1. Componenti Principali:

- Server Headscale: Il cuore di Headscale è rappresentato dal server, che gestisce le operazioni di autenticazione, autorizzazione e gestione delle identità dei dispositivi e degli utenti.
- Database: Headscale utilizza un database per memorizzare in modo sicuro le informazioni sull'infrastruttura di rete, inclusi gli utenti, i dispositivi e le autorizzazioni.
- Interfaccia Utente: Una interfaccia utente web consente agli amministratori di configurare e monitorare l'infrastruttura di rete, definire e applicare politiche di accesso e gestire le identità dei dispositivi e degli utenti.

2. Architettura Serverless:

- Headscale utilizza un'architettura serverless, in cui la maggior parte delle operazioni di gestione e controllo della rete sono delegate ai client Tailscale.
- Questo approccio riduce la complessità e i costi operativi, consentendo agli amministratori di concentrarsi sulla configurazione e sul monitoraggio dell'infrastruttura di rete.

3. Comunicazioni Crittografate:

- Tutte le comunicazioni tra i dispositivi Tailscale e il server Headscale sono crittografate utilizzando protocolli sicuri.
- Headscale utilizza crittografia forte e sicura per proteggere la privacy e la sicurezza delle informazioni scambiate tra i dispositivi e il server.

4. Gestione Centralizzata delle Identità e delle Autorizzazioni:

- Headscale offre una gestione centralizzata delle identità e delle autorizzazioni, consentendo agli amministratori di definire e applicare in modo coerente le politiche di accesso in tutta l'organizzazione.
- Gli amministratori possono configurare regole di accesso basate sul ruolo, definire gruppi di utenti e dispositivi e monitorare l'attività di rete attraverso un'interfaccia utente intuitiva.

5. Scalabilità e Affidabilità:

- Headscale è progettato per essere altamente scalabile e affidabile, consentendo la gestione di grandi flotte di dispositivi e utenti distribuiti in diverse sedi geografiche.
- L'architettura serverless e la distribuzione su cloud provider come AWS o Google Cloud consentono di scalare dinamicamente risorse in base alle esigenze di utilizzo.

6. Integrazione con Ambienti Esistenti:

- Headscale può essere integrato con ambienti di rete esistenti, consentendo agli amministratori di estendere facilmente la loro infrastruttura di rete e garantire un accesso sicuro alle risorse aziendali.
- L'architettura aperta e flessibile di Headscale consente l'integrazione con servizi e applicazioni di terze parti attraverso API e connettori personalizzati.

Conclusioni:

L'architettura di Headscale offre una soluzione flessibile e scalabile per la gestione centralizzata delle reti Tailscale. Utilizzando un'architettura serverless, comunicazioni crittografate, gestione centralizzata delle identità e delle autorizzazioni e un'interfaccia utente intuitiva, Headscale semplifica la configurazione, il monitoraggio e la gestione dell'infrastruttura di rete, consentendo alle organizzazioni di proteggere efficacemente le loro risorse e garantire un accesso sicuro ai dipendenti e ai dispositivi remoti.

Architettura di Headscale Zero Trust

Headscale Zero Trust è un'implementazione dei principi Zero Trust all'interno dell'architettura di Headscale, una soluzione per la gestione centralizzata di reti Tailscale. Attraverso l'applicazione dei principi Zero Trust, Headscale mira a garantire un accesso sicuro e granulare alle risorse di rete, limitando l'affidamento su reti affidabili e utilizzando controlli basati sull'identità e sul contesto dell'accesso. Di seguito viene presentata una relazione tecnica sull'architettura di Headscale Zero Trust:

1. Architettura Basata su Zero Trust:

- Headscale Zero Trust adotta un approccio di "never trust, always verify", in cui ogni richiesta di accesso è considerata non affidabile e richiede una verifica rigorosa prima di concedere l'accesso.
- Questo approccio si basa su controlli granulari sull'accesso, autenticazione multi-fattore (MFA), autorizzazione basata sul ruolo e monitoraggio continuo per garantire la sicurezza delle connessioni e delle risorse di rete.

2. Gestione Centralizzata delle Identità e delle Autorizzazioni:

- Headscale Zero Trust offre una gestione centralizzata delle identità e delle autorizzazioni, consentendo agli amministratori di definire e applicare in modo coerente le politiche di accesso in tutta l'organizzazione.
- Gli amministratori possono configurare regole di accesso basate sul ruolo, definire gruppi di utenti e dispositivi e monitorare l'attività di rete attraverso un'interfaccia utente intuitiva.

3. Segmentazione della Rete e Isolamento delle Risorse:

- Headscale Zero Trust supporta la segmentazione della rete e l'isolamento delle risorse, consentendo agli amministratori di suddividere la rete in segmenti più piccoli e controllare l'accesso alle risorse in base ai requisiti di sicurezza.
- Questo approccio riduce la superficie di attacco e limita il movimento laterale degli attaccanti all'interno della rete.

4. Monitoraggio Continuo e Analisi Comportamentale:

- Headscale Zero Trust offre funzionalità avanzate di monitoraggio continuo e analisi comportamentale per individuare e rispondere prontamente alle minacce alla sicurezza.
- Gli amministratori possono monitorare l'attività di rete, raccogliere dati sul comportamento degli utenti e dei dispositivi e identificare potenziali anomalie o attività sospette.

5. Scalabilità e Affidabilità:

- Headscale Zero Trust è progettato per essere altamente scalabile e affidabile, consentendo la gestione di grandi flotte di dispositivi e utenti distribuiti in diverse sedi geografiche.
- L'architettura serverless e la distribuzione su cloud provider consentono di scalare dinamicamente risorse in base alle esigenze di utilizzo.

6. Integrazione con Ambienti Esistenti:

- Headscale Zero Trust può essere integrato con ambienti di rete esistenti, consentendo agli amministratori di estendere facilmente la loro infrastruttura di rete e garantire un accesso sicuro alle risorse aziendali.
- L'architettura aperta e flessibile di Headscale Zero Trust consente l'integrazione con servizi e applicazioni di terze parti attraverso API e connettori personalizzati.

Conclusioni:

Headscale Zero Trust offre una soluzione completa e scalabile per l'implementazione dei principi Zero Trust all'interno dell'architettura di Headscale. Utilizzando un'architettura serverless, comunicazioni crittografate, gestione centralizzata delle identità e delle autorizzazioni, segmentazione della rete, monitoraggio continuo e analisi comportamentale, Headscale Zero Trust consente alle organizzazioni di proteggere efficacemente le loro risorse di rete e garantire un accesso sicuro ai dipendenti e ai dispositivi remoti.

Attualmente, Headscale non è direttamente compatibile con WireGuard. Headscale utilizza il protocollo Tailscale per gestire le connessioni VPN tra i dispositivi e il server Headscale. Tuttavia, WireGuard è il protocollo VPN sottostante utilizzato da Tailscale per stabilire connessioni sicure tra i dispositivi. Pertanto, anche se Headscale stesso non supporta direttamente WireGuard, i dispositivi che utilizzano Headscale possono ancora beneficiare delle caratteristiche di sicurezza e prestazioni offerte da WireGuard.

Tailscale è un servizio VPN che semplifica la connettività tra dispositivi in una rete. Utilizza WireGuard come protocollo sottostante per stabilire connessioni sicure e crittografate tra i dispositivi. Ecco come avviene l'integrazione:

1. Configurazione Semplificata: Tailscale semplifica notevolmente il processo di configurazione di una VPN. Quando un dispositivo si unisce alla rete Tailscale, viene generata automaticamente una coppia di chiavi crittografiche pubbliche e private per quel dispositivo. Queste chiavi vengono utilizzate per autenticare il dispositivo e crittografare le comunicazioni.
2. Distribuzione delle Chiavi: Una volta che un dispositivo si unisce alla rete Tailscale, le sue chiavi pubbliche vengono distribuite a tutti gli altri dispositivi nella rete. Questo avviene tramite i server di coordinamento Tailscale.
3. Comunicazioni Crittografate: Quando un dispositivo deve comunicare con un altro dispositivo sulla rete Tailscale, utilizza le rispettive chiavi pubbliche per stabilire una connessione sicura tramite il

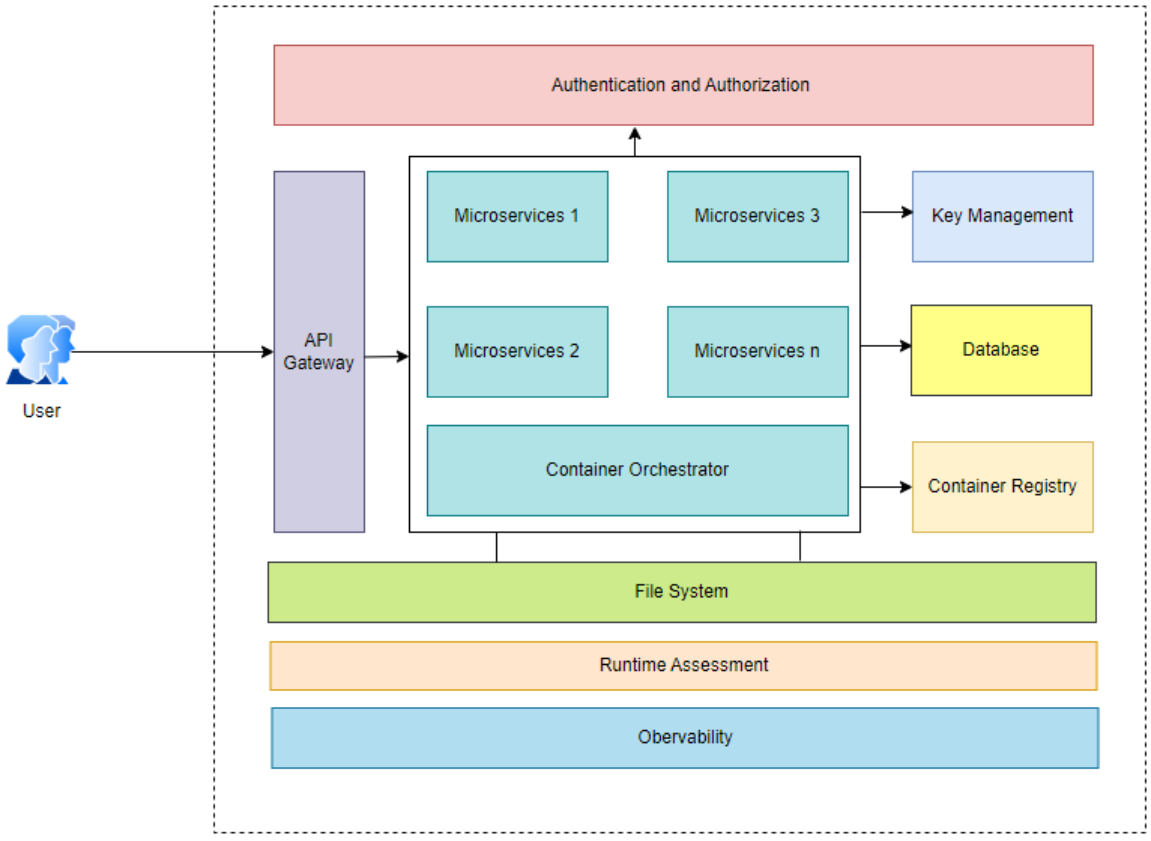
protocollo WireGuard. WireGuard offre un tunnel crittografato punto a punto tra i dispositivi, garantendo la privacy e la sicurezza delle comunicazioni.

4. Gestione delle Connessioni: Tailscale gestisce dinamicamente le connessioni tra i dispositivi sulla rete, mantenendo solo le connessioni necessarie in base alle esigenze di comunicazione. Questo aiuta a ottimizzare le prestazioni della rete e a garantire che le connessioni siano sempre sicure.

In sintesi, l'integrazione di WireGuard in Tailscale consente ai dispositivi di comunicare in modo sicuro e crittografato all'interno della rete Tailscale. WireGuard fornisce il tunnel VPN sicuro tra i dispositivi, mentre Tailscale semplifica la configurazione e la gestione di questa rete VPN, rendendola adatta per l'uso in ambienti aziendali e personali.

Proteggere i Microservizi nei Cloud Provider con un Approccio di Zero Trust

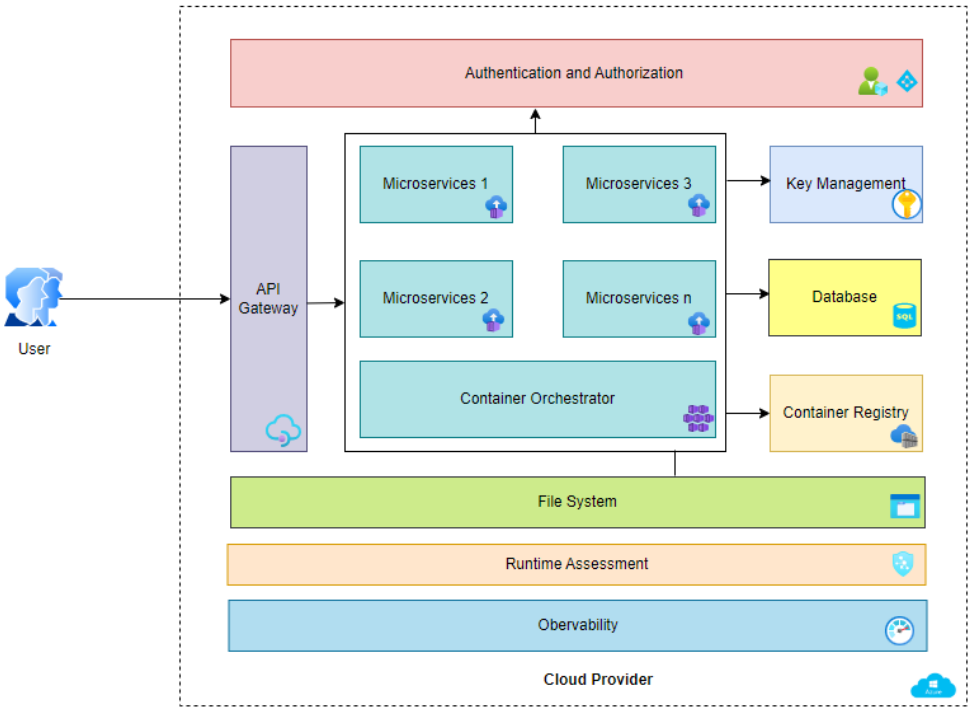
Nell'attuale panorama delle applicazioni cloud-native, i microservizi hanno assunto un ruolo predominante, diventando lo standard per lo sviluppo di applicazioni. Anche le applicazioni basate sull'IA si affidano sempre più a questa architettura. Tuttavia, con la diffusione degli iperscalatori e la tendenza dei clienti a distribuire i propri microservizi su più fornitori di cloud, la sicurezza diventa una priorità cruciale. In questo contesto, la Sicurezza Zero Trust emerge come un elemento essenziale per garantire il funzionamento sicuro dei microservizi nel cloud. Questo approccio si basa sui principi di "non fidarsi mai, sempre verificare", assumendo che tutto possa essere potenzialmente ostile. Attraverso l'assunzione di ostilità, la verifica esplicita e l'attuazione di politiche di accesso minime, la Sicurezza Zero Trust mira a ridurre la superficie di attacco complessiva e a limitare il potenziale danno in caso di violazione della sicurezza, offrendo un livello avanzato di protezione per i microservizi nell'ambiente cloud.



Zero Trust Security per Micro Servizi

Per applicare la Sicurezza Zero Trust all'ambiente dei microservizi, occorre considerare diverse considerazioni cruciali:

1. Autenticazione e autorizzazione continua: Ogni componente dei microservizi deve essere autenticato e autorizzato continuamente, con una valutazione costante delle identità e la revoca delle identità compromesse. Strumenti come Azure AD e AWS IAM gestiscono l'autenticazione e l'accesso in modo sicuro.
2. Crittografia delle comunicazioni: È essenziale crittografare tutte le comunicazioni tra i microservizi utilizzando HTTPS e mTLS. Azure Key Vault e AWS KMS sono utili per gestire le chiavi di crittografia.
3. Controllo dell'accesso tramite gateway API: Le entità esterne devono accedere ai microservizi tramite un gateway API che convalida l'identità dell'utente. Azure API Management e Amazon AWS API Gateway sono opzioni valide.
4. Classificazione e protezione dei dati: È necessario classificare e proteggere i dati in base al livello di riservatezza. Strumenti come Azure Key Vault e AWS Secrets Manager gestiscono segreti e chiavi API in modo sicuro.
5. Sicurezza dell'infrastruttura con l'IaC: Utilizzare l'infrastruttura come codice per provvisionare e mantenere i componenti. Azure Resource Manager e AWS CloudFormation sono strumenti per definire e distribuire l'infrastruttura in modo coerente.
6. Sicurezza dei contenitori e dei cluster: Verificare e utilizzare solo immagini dei contenitori firmate e privi di vulnerabilità. Azure Container Registry e Amazon ECR sono soluzioni per memorizzare e gestire immagini di container.
7. Valutazione continua della sicurezza del runtime dei microservizi: Valutare l'ambiente di runtime per compromessi di sicurezza e fermarli immediatamente. Strumenti come Microsoft Defender for Cloud e AWS GuardDuty forniscono valutazioni della sicurezza in tempo reale.
8. Osservabilità e monitoraggio continuo: Monitorare continuamente i microservizi per individuare potenziali problemi e vulnerabilità. Strumenti come AWS X-Ray e Azure Application Insights forniscono osservabilità continua per garantire la sicurezza dell'ambiente dei microservizi.



Implementare la sicurezza Zero Trust per proteggere i Micro servizi utilizzando i servizi offerti da Azure.

Per implementare la Sicurezza Zero Trust in un'applicazione di microservizi che gestisce dati finanziari sensibili, è fondamentale considerare tutto il traffico di rete, gli utenti e i servizi come potenzialmente ostili. Ciò implica la verifica esplicita dell'identità di tutti gli utenti e dei servizi, limitando il loro accesso solo a ciò che è strettamente necessario per i loro ruoli. Azure Active Directory è utile per gestire l'autenticazione e l'autorizzazione degli utenti, mentre un gateway API come Azure API Management controlla l'accesso ai microservizi e convalida l'identità dell'utente prima di consentire l'accesso. La crittografia di tutte le comunicazioni tra servizi, API e altri componenti utilizzando HTTPS e mTLS è essenziale per garantire una comunicazione sicura. Azure Key Vault gestisce in modo sicuro le chiavi di crittografia. Per classificare e proteggere i dati in base al livello di riservatezza, è necessario mantenere un registro dei dati e archiviare segreti, certificati e chiavi API in modo sicuro in un vault di controllo degli accessi alle chiavi, come Azure Key Vault. La valutazione continua dell'ambiente di esecuzione per compromessi di sicurezza e la correzione immediata possono essere ottenute utilizzando Microsoft Defender for Cloud, prevenendo così attacchi e garantendo un funzionamento sicuro dei microservizi. In conclusione, l'architettura dei microservizi è diventata predominante nello sviluppo di applicazioni cloud-native. Con la distribuzione sempre più diffusa dei microservizi su più fornitori di cloud, implementare misure di sicurezza robuste è diventato essenziale. La Sicurezza Zero Trust offre un approccio efficace per proteggere i microservizi e la loro infrastruttura in un ambiente di Hyperscaler, assumendo che tutto sia potenzialmente ostile e applicando il principio del privilegio minimo. Azure e AWS forniscono una gamma di servizi utili per implementare efficacemente la Sicurezza Zero Trust, inclusi Azure Active Directory, AWS IAM, API Gateway e Key Vault.

Differenze Architetturali tra VPN IPsec e Servizi Zero Trust

Le VPN IPsec (Internet Protocol Security) e i servizi Zero Trust rappresentano due approcci differenti alla sicurezza delle reti aziendali, ciascuno con le proprie caratteristiche architetturali e implementative. Di seguito viene presentata una relazione tecnica sulle differenze architetturali tra VPN IPsec e servizi Zero Trust:

VPN IPsec:

Tunneling di Livello di Rete:

1. Le VPN IPsec creano tunnel crittografati a livello di rete per instradare il traffico tra dispositivi o reti remote.
2. L'architettura è basata su protocolli di tunneling IPsec che offrono crittografia e autenticazione per il traffico in transito.
3. Accesso di Tipo "Tutto o Niente":
4. Le VPN IPsec tendono ad offrire un accesso binario, in cui gli utenti o i dispositivi hanno accesso completo alla rete una volta autenticati tramite la VPN.
5. Questo approccio non fornisce un controllo granulare sull'accesso alle risorse di rete e può aumentare il rischio di esposizione della rete a minacce interne.
6. Relativa Complessità di Configurazione:
7. L'implementazione e la configurazione di VPN IPsec possono essere complesse, richiedendo competenze tecniche avanzate e configurazioni dettagliate dei dispositivi di rete.
8. Limitata Visibilità e Controllo:
9. Le VPN IPsec possono offrire una visibilità limitata sul traffico di rete e sulle attività degli utenti, rendendo difficile il monitoraggio e il controllo delle minacce alla sicurezza.

Servizi Zero Trust:

1. Architettura Basata sul Principio di "Never Trust, Always Verify":
2. I servizi Zero Trust si basano su un approccio di "never trust, always verify", in cui ogni richiesta di accesso è considerata non affidabile e richiede una verifica rigorosa prima di concedere l'accesso.

3. L'architettura è basata su controlli granulari sull'accesso, autenticazione multi-fattore (MFA), autorizzazione basata su ruoli e monitoraggio continuo.
4. Microsegmentazione e Isolamento delle Risorse:
5. I servizi Zero Trust utilizzano la microsegmentazione per suddividere la rete in segmenti più piccoli e isolati, riducendo la superficie di attacco e limitando il movimento laterale degli attaccanti all'interno della rete.
6. Questo approccio offre un controllo granulare sull'accesso alle risorse e una maggiore protezione contro le minacce interne.
7. Gestione Centralizzata delle Politiche di Sicurezza:
8. I servizi Zero Trust offrono una gestione centralizzata delle politiche di sicurezza, consentendo agli amministratori di definire e applicare in modo coerente le politiche di accesso e sicurezza in tutta l'organizzazione.
9. Monitoraggio Continuo e Risposta alle Minacce:
10. I servizi Zero Trust includono funzionalità avanzate di monitoraggio continuo e analisi comportamentale per individuare e rispondere prontamente alle minacce alla sicurezza.

Conclusioni:

Le principali differenze architetturali tra VPN IPsec e servizi Zero Trust risiedono nella natura del controllo degli accessi, nella visibilità e nel monitoraggio del traffico di rete, nonché nella complessità di configurazione e gestione. Mentre le VPN IPsec offrono una connessione sicura tra reti remote, i servizi Zero Trust vanno oltre, fornendo un controllo granulare sull'accesso, una protezione più efficace contro le minacce interne e una gestione centralizzata delle politiche di sicurezza. La scelta tra i due dipenderà dalle esigenze specifiche dell'organizzazione, dalla complessità dell'ambiente di rete e dalla strategia di sicurezza complessiva dell'azienda.

Implementazione dei Servizi Zero Trust tramite VPN IPsec

L'implementazione di servizi Zero Trust tramite VPN IPsec richiede un approccio che integri i principi di Zero Trust con le funzionalità fornite dalle VPN IPsec. Sebbene le VPN IPsec siano tradizionalmente utilizzate per creare tunnel crittografati tra reti remote, è possibile utilizzare alcuni concetti e pratiche di Zero Trust per migliorare la sicurezza all'interno di questi tunnel. Di seguito viene presentata una relazione tecnica su come implementare i servizi Zero Trust tramite VPN IPsec:

1. Segmentazione del Traffico VPN:

- Implementare una segmentazione del traffico VPN tramite VPN IPsec per instradare il traffico solo verso le risorse autorizzate.
- Utilizzare politiche di routing e access control list (ACL) per limitare il traffico VPN solo alle risorse specifiche all'interno della rete aziendale.

2. Autenticazione Multi-Fattore (MFA):

- Configurare l'autenticazione multi-fattore (MFA) per gli utenti che accedono alla VPN IPsec.
- Utilizzare soluzioni MFA integrate o di terze parti per richiedere prove aggiuntive di identità oltre alle tradizionali credenziali di accesso.

3. Autorizzazione Granulare:

- Implementare politiche di accesso granulari sulla VPN IPsec per consentire l'accesso solo alle risorse e alle applicazioni necessarie per il lavoro degli utenti.
- Utilizzare gruppi di sicurezza o altri meccanismi per definire e applicare politiche di autorizzazione basate sul ruolo dell'utente o sul contesto di accesso.

4. Monitoraggio Continuo e Analisi Comportamentale:

- Configurare sistemi di monitoraggio continuo per analizzare il traffico VPN e rilevare eventuali anomalie o comportamenti sospetti.
- Utilizzare strumenti di analisi comportamentale per identificare potenziali minacce o attività anomale all'interno dei tunnel VPN.

5. Gestione Centralizzata delle Politiche di Sicurezza:

- Utilizzare una soluzione di gestione centralizzata delle politiche di sicurezza per definire e applicare in modo coerente le politiche di accesso e sicurezza sulla VPN IPsec.
- Garantire che le politiche di sicurezza siano aggiornate e coerenti in tutti i dispositivi e le reti coinvolti nella VPN IPsec.

6. Protezione dei Dispositivi Terminali:

- Assicurarsi che i dispositivi terminali che si connettono alla VPN IPsec siano adeguatamente protetti da minacce come malware, ransomware e altre vulnerabilità di sicurezza.
- Utilizzare soluzioni di endpoint protection per monitorare e proteggere i dispositivi terminali da potenziali minacce.

Conclusioni:

L'implementazione di servizi Zero Trust tramite VPN IPsec richiede un approccio integrato che combini le funzionalità di sicurezza delle VPN IPsec con i principi di Zero Trust. Integrando pratiche come la segmentazione del traffico, l'autenticazione multi-fattore, l'autorizzazione granulare, il monitoraggio continuo e la gestione centralizzata delle politiche di sicurezza, è possibile migliorare la sicurezza della VPN IPsec e ridurre i rischi di accesso non autorizzato e violazioni della sicurezza all'interno della rete aziendale. Tuttavia, è importante tenere presente che mentre questa implementazione può migliorare la sicurezza complessiva, non elimina completamente i rischi associati alle VPN IPsec e richiede un'attenta pianificazione e configurazione per garantire una protezione efficace dei dati e delle risorse aziendali.

Differenze Architetturali tra VPN OpenVPN e Servizi Zero Trust

Le VPN OpenVPN e i servizi Zero Trust rappresentano due approcci differenti alla sicurezza delle reti aziendali, ciascuno con le proprie caratteristiche architetturali e implementative. Di seguito viene presentata una relazione tecnica sulle differenze architetturali tra VPN OpenVPN e servizi Zero Trust:

VPN OpenVPN:

1. Tunneling di Livello Applicativo:
2. OpenVPN utilizza un modello di tunneling a livello applicativo, in cui il traffico VPN è incapsulato in protocolli di trasporto come TCP o UDP.
3. L'architettura si basa su un client-server model, con un server OpenVPN che fornisce connessioni VPN sicure ai client.
4. Accesso basato su Tunneling VPN:
5. OpenVPN offre accesso ai servizi e alle risorse aziendali attraverso il tunnel VPN, consentendo agli utenti di connettersi alla rete aziendale come se fossero localmente connessi.
6. Autenticazione e Crittografia:
7. OpenVPN supporta diversi metodi di autenticazione e crittografia per garantire la sicurezza delle connessioni VPN, inclusi certificati digitali, autenticazione username/password e crittografia a chiave pubblica/privata.
8. Limitata Granularità di Controllo:
9. OpenVPN offre un controllo relativamente limitato sull'accesso e sulle politiche di sicurezza, con opzioni di configurazione predefinite per la gestione delle connessioni VPN.

Servizi Zero Trust:

1. Architettura Basata sul Principio di "Never Trust, Always Verify":
2. I servizi Zero Trust adottano un approccio di "never trust, always verify", in cui ogni richiesta di accesso è considerata non affidabile e richiede una verifica rigorosa prima di concedere l'accesso.
3. L'architettura è basata su controlli granulari sull'accesso, autenticazione multi-fattore (MFA), autorizzazione basata sul ruolo e monitoraggio continuo.
4. Microsegmentazione e Isolamento delle Risorse:
5. I servizi Zero Trust utilizzano la microsegmentazione per suddividere la rete in segmenti più piccoli e isolati, riducendo il rischio di movimento laterale degli attaccanti all'interno della rete.
6. Politiche di Sicurezza Centralizzate e Gestione:
7. I servizi Zero Trust offrono una gestione centralizzata delle politiche di sicurezza, consentendo agli amministratori di definire e applicare in modo coerente le politiche di accesso e sicurezza in tutta l'organizzazione.
8. Monitoraggio Continuo e Risposta alle Minacce:
9. I servizi Zero Trust includono funzionalità avanzate di monitoraggio continuo e analisi comportamentale per individuare e rispondere prontamente alle minacce alla sicurezza.

Conclusioni:

Le principali differenze architetturali tra VPN OpenVPN e servizi Zero Trust risiedono nella natura del controllo degli accessi, nella visibilità e nel monitoraggio del traffico di rete, nonché nella complessità di configurazione e gestione. Mentre OpenVPN offre un accesso sicuro tramite tunnel VPN e opzioni di crittografia, i servizi Zero Trust vanno oltre, fornendo un controllo granulare sull'accesso, una protezione più efficace contro le minacce interne e una gestione centralizzata delle politiche di sicurezza. La scelta tra i due dipenderà dalle esigenze specifiche dell'organizzazione, dalla complessità dell'ambiente di rete e dalla strategia di sicurezza complessiva dell'azienda.

Implementazione dei Servizi Zero Trust tramite VPN OpenVPN

L'implementazione dei servizi Zero Trust tramite VPN OpenVPN richiede un approccio che integri i principi di Zero Trust con le funzionalità fornite da OpenVPN. Sebbene OpenVPN sia tradizionalmente utilizzato per creare tunnel VPN sicuri, è possibile utilizzare alcuni concetti e pratiche di Zero Trust per migliorare la sicurezza delle connessioni VPN e limitare l'accesso alle risorse aziendali. Di seguito viene presentata una relazione tecnica su come implementare i servizi Zero Trust tramite VPN OpenVPN:

1. Autenticazione Multi-Fattore (MFA):

- Configurare l'autenticazione multi-fattore (MFA) per gli utenti che accedono alla VPN OpenVPN.
- Utilizzare soluzioni MFA integrate o di terze parti per richiedere prove aggiuntive di identità oltre alle tradizionali credenziali di accesso.

2. Autorizzazione Granulare:

- Implementare politiche di accesso granulari sulla VPN OpenVPN per consentire l'accesso solo alle risorse e alle applicazioni necessarie per il lavoro degli utenti.
- Utilizzare gruppi di sicurezza o altri meccanismi per definire e applicare politiche di autorizzazione basate sul ruolo dell'utente o sul contesto di accesso.

3. Crittografia e Sicurezza dei Certificati:

- Configurare OpenVPN per utilizzare crittografia forte e certificati digitali per garantire la sicurezza delle connessioni VPN.
- Utilizzare una infrastruttura a chiave pubblica (PKI) per generare e gestire i certificati digitali utilizzati per l'autenticazione e la crittografia.

4. Monitoraggio Continuo:

- Configurare sistemi di monitoraggio continuo per analizzare il traffico VPN e rilevare eventuali anomalie o comportamenti sospetti.
- Utilizzare strumenti di analisi comportamentale per identificare potenziali minacce o attività anomale all'interno dei tunnel VPN.

5. Gestione Centralizzata delle Politiche di Sicurezza:

- Utilizzare una soluzione di gestione centralizzata delle politiche di sicurezza per definire e applicare in modo coerente le politiche di accesso e sicurezza sulla VPN OpenVPN.
- Garantire che le politiche di sicurezza siano aggiornate e coerenti in tutti i dispositivi e le reti coinvolti nella VPN OpenVPN.

6. Protezione dei Dispositivi Terminali:

- Assicurarsi che i dispositivi terminali che si connettono alla VPN OpenVPN siano adeguatamente protetti da minacce come malware, ransomware e altre vulnerabilità di sicurezza.
- Utilizzare soluzioni di endpoint protection per monitorare e proteggere i dispositivi terminali da potenziali minacce.

Conclusioni:

L'implementazione dei servizi Zero Trust tramite VPN OpenVPN richiede un approccio integrato che combini le funzionalità di sicurezza di OpenVPN con i principi di Zero Trust. Integrando pratiche come l'autenticazione multi-fattore, l'autorizzazione granulare, la crittografia e la sicurezza dei certificati, il monitoraggio continuo e la gestione centralizzata delle politiche di sicurezza, è possibile migliorare la sicurezza della VPN OpenVPN e ridurre i rischi di accesso non autorizzato e violazioni della sicurezza all'interno della rete aziendale. Tuttavia, è importante tenere presente che mentre questa implementazione può migliorare la sicurezza complessiva, non elimina completamente i rischi associati alle VPN OpenVPN e richiede un'attenta pianificazione e configurazione per garantire una protezione efficace dei dati e delle risorse aziendali.

Differenze Architetturali tra VPN WireGuard e Servizi Zero Trust

Le VPN WireGuard e i servizi Zero Trust rappresentano due approcci distinti alla sicurezza delle reti, ciascuno con le proprie caratteristiche architetturali e implementative. Di seguito viene presentata una relazione tecnica sulle differenze architetturali tra VPN WireGuard e servizi Zero Trust:

VPN WireGuard:

1. Protocollo Leggero e Performante:
2. WireGuard è noto per la sua semplicità e leggerezza, offrendo un protocollo VPN veloce e performante con un codice base ridotto rispetto ad altre soluzioni.
3. L'architettura di WireGuard è progettata per essere efficiente in termini di risorse, riducendo l'impatto sulle prestazioni del sistema.
4. Approccio Kernel-based:
5. WireGuard è implementato a livello di kernel, integrandosi direttamente con il sistema operativo dell'host. Questo permette una maggiore efficienza e velocità rispetto a soluzioni basate su user-space.
6. Connessioni Peer-to-Peer:
7. WireGuard supporta connessioni peer-to-peer, in cui ogni dispositivo connesso alla rete VPN costituisce un nodo peer autonomo.
8. L'architettura peer-to-peer semplifica la configurazione e la gestione delle connessioni VPN, eliminando la necessità di un server centrale.
9. Crittofrafia Moderna e Sicura:
10. WireGuard utilizza crittografia moderna e sicura basata su Curve25519 per gli scambi di chiavi e ChaCha20 per la crittografia del traffico.

11. Questo garantisce una protezione efficace dei dati in transito e una resistenza alle minacce di crittanalisi.

Servizi Zero Trust:

1. Approccio Basato su "Never Trust, Always Verify":
2. I servizi Zero Trust adottano un approccio di "never trust, always verify", in cui ogni richiesta di accesso è considerata non affidabile e richiede una verifica rigorosa prima di concedere l'accesso.
3. L'architettura è basata su controlli granulari sull'accesso, autenticazione multi-fattore (MFA), autorizzazione basata sul ruolo e monitoraggio continuo.
4. Microsegmentazione e Isolamento delle Risorse:
5. I servizi Zero Trust utilizzano la microsegmentazione per suddividere la rete in segmenti più piccoli e isolati, riducendo il rischio di movimento laterale degli attaccanti all'interno della rete.
6. Politiche di Sicurezza Centralizzate e Gestione:
7. I servizi Zero Trust offrono una gestione centralizzata delle politiche di sicurezza, consentendo agli amministratori di definire e applicare in modo coerente le politiche di accesso e sicurezza in tutta l'organizzazione.
8. Monitoraggio Continuo e Risposta alle Minacce:
9. I servizi Zero Trust includono funzionalità avanzate di monitoraggio continuo e analisi comportamentale per individuare e rispondere prontamente alle minacce alla sicurezza.

Conclusioni:

Le principali differenze architetturali tra VPN WireGuard e servizi Zero Trust risiedono nella natura della connessione VPN e nel controllo dell'accesso. Mentre WireGuard offre un protocollo VPN leggero e performante con connessioni peer-to-peer, i servizi Zero Trust forniscono un approccio completo alla sicurezza della rete, con controlli granulari sull'accesso, microsegmentazione, gestione centralizzata delle politiche di sicurezza e monitoraggio continuo. La scelta tra i due dipenderà dalle esigenze specifiche dell'organizzazione, dalla complessità dell'ambiente di rete e dalla strategia di sicurezza complessiva dell'azienda.

Implementazione dei Servizi Zero Trust tramite VPN WireGuard

- L'implementazione dei servizi Zero Trust tramite VPN WireGuard richiede un approccio che integri i principi di Zero Trust con le funzionalità fornite da WireGuard. Mentre WireGuard offre una connettività VPN leggera e efficiente, i servizi Zero Trust vanno oltre, fornendo un controllo granulare sull'accesso, la microsegmentazione della rete e il monitoraggio continuo. Di seguito viene presentata una relazione tecnica su come implementare i servizi Zero Trust tramite VPN WireGuard:

1. Autenticazione Multi-Fattore (MFA):

- Configurare l'autenticazione multi-fattore (MFA) per gli utenti che accedono alla VPN WireGuard.
- Utilizzare soluzioni MFA integrate o di terze parti per richiedere prove aggiuntive di identità oltre alle tradizionali credenziali di accesso.

2. Autorizzazione Granulare:

- Implementare politiche di accesso granulari sulla VPN WireGuard per consentire l'accesso solo alle risorse e alle applicazioni necessarie per il lavoro degli utenti.
- Utilizzare gruppi di sicurezza o altri meccanismi per definire e applicare politiche di autorizzazione basate sul ruolo dell'utente o sul contesto di accesso.

3. Crittografia e Sicurezza:

- Configurare WireGuard per utilizzare crittografia forte e sicura per garantire la privacy e la protezione dei dati in transito.
- Utilizzare Curve25519 per gli scambi di chiavi e ChaCha20 per la crittografia del traffico per garantire una protezione efficace dei dati.

4. Microsegmentazione e Isolamento delle Risorse:

- Suddividere la rete in segmenti più piccoli e isolati utilizzando WireGuard per ridurre la superficie di attacco e limitare il movimento laterale degli attaccanti.
- Utilizzare tunnel WireGuard separati per diverse categorie di risorse o utenti per migliorare la sicurezza e il controllo.

5. Monitoraggio Continuo:

- Configurare sistemi di monitoraggio continuo per analizzare il traffico VPN WireGuard e rilevare eventuali anomalie o comportamenti sospetti.
- Utilizzare strumenti di analisi comportamentale per identificare potenziali minacce o attività anomale all'interno dei tunnel VPN.

6. Gestione Centralizzata delle Politiche di Sicurezza:

- Utilizzare una soluzione di gestione centralizzata delle politiche di sicurezza per definire e applicare in modo coerente le politiche di accesso e sicurezza sulla VPN WireGuard.
- Assicurarsi che le politiche di sicurezza siano aggiornate e coerenti in tutti i dispositivi e le reti coinvolti nella VPN WireGuard.

Conclusioni:

L'implementazione dei servizi Zero Trust tramite VPN WireGuard richiede un approccio integrato che combini le funzionalità di sicurezza di WireGuard con i principi di Zero Trust. Integrando pratiche come l'autenticazione multi-fattore, l'autorizzazione granulare, la crittografia e la sicurezza, la microsegmentazione e il monitoraggio continuo, è possibile migliorare la sicurezza della VPN WireGuard e ridurre i rischi di accesso non autorizzato e violazioni della sicurezza all'interno della rete aziendale. Tuttavia, è importante tenere presente che mentre questa implementazione può migliorare la sicurezza complessiva, non elimina completamente i rischi associati alla VPN WireGuard e richiede un'attenta pianificazione e configurazione per garantire una protezione efficace dei dati e delle risorse aziendali.

Architetture reali a confronto col concetto di base

Zero Trust

Descrizione: Zero Trust è un modello di sicurezza che non si fida automaticamente di nessuna entità interna o esterna e richiede una verifica rigorosa di tutte le persone e dei dispositivi cercanti di connettersi alle risorse.

Architettura: Basata sulla microsegmentazione, autenticazione multi-fattore (MFA), autorizzazione granulare e monitoraggio continuo.

Vantaggi: Riduzione dei rischi di sicurezza, maggiore controllo sull'accesso alle risorse.

Zero Tier

1. Descrizione: ZeroTier è una rete privata virtuale a livello di software che consente di collegare dispositivi, server e reti in un'unica rete.
2. Architettura: Basata su un modello peer-to-peer decentralizzato.
3. Vantaggi: Facilità di configurazione, scalabilità, compatibilità multi-piattaforma.

VPN IPsec

1. Descrizione: VPN IPsec (Internet Protocol Security) è un protocollo per stabilire connessioni sicure su Internet.
2. Architettura: Utilizza tunneling IPsec per crittografare il traffico.
3. Vantaggi: Ampiamente supportato, sicurezza robusta, prestazioni elevate.

OpenVPN

1. Descrizione: OpenVPN è un software open-source per l'implementazione di VPN.
2. Architettura: Utilizza SSL/TLS per crittografare il traffico.
3. Vantaggi: Flessibilità, facilità di configurazione, supporto multi-piattaforma.

WireGuard

1. Descrizione: WireGuard è un protocollo VPN leggero e veloce.
2. Architettura: Progettato per essere semplice ed efficiente.
3. Vantaggi: Prestazioni superiori, codice pulito e auditabile, bassa latenza.

2. Sicurezza

- Zero Trust: Basato su un approccio di "never trust, always verify", con controlli rigorosi e autenticazione multi-fattore.
- ZeroTier: Crittografia end-to-end per la privacy dei dati e autenticazione basata su chiave.
- VPN IPsec: Utilizza algoritmi crittografici robusti per garantire la sicurezza dei dati in transito.
- OpenVPN: Crittografia SSL/TLS per proteggere le comunicazioni.
- WireGuard: Utilizza crittografia moderna e algoritmi avanzati per garantire la sicurezza.

3. Scalabilità

- Zero Trust: Scalabile, ma richiede una pianificazione accurata per l'implementazione su larga scala.
- ZeroTier: Scalabile, con la capacità di aggiungere facilmente nuovi dispositivi e reti.
- VPN IPsec: Scalabile, ma richiede una configurazione complessa per gestire grandi reti.
- OpenVPN: Può essere scalato, ma potrebbero sorgere limitazioni in termini di prestazioni e complessità.
- WireGuard: Considerato altamente scalabile grazie alla sua architettura leggera e efficiente.

4. Prestazioni

- Zero Trust: Le prestazioni dipendono dalla complessità dell'ambiente e delle politiche di sicurezza implementate.
- ZeroTier: Buone prestazioni, anche se possono variare in base alla topologia di rete.
- VPN IPsec: Prestazioni solide, ma possono essere influenzate dalla complessità della configurazione e dalla larghezza di banda disponibile.
- OpenVPN: Prestazioni accettabili, anche se potrebbero essere inferiori rispetto a soluzioni più moderne come WireGuard.
- WireGuard: Conosciuto per le prestazioni elevate e la bassa latenza, ideale per applicazioni sensibili alle prestazioni.

5. Facilità d'Uso

- Zero Trust: Richiede una pianificazione e una configurazione iniziali dettagliate, ma può offrire un'esperienza utente semplificata a lungo termine.
- ZeroTier: Facile da configurare e gestire, con un'interfaccia utente intuitiva.
- VPN IPsec: Potrebbe richiedere una competenza tecnica più avanzata per la configurazione e la gestione.
- OpenVPN: Relativamente facile da configurare e utilizzare, con molte risorse disponibili per la guida e il supporto.
- WireGuard: Progettato per essere semplice da configurare e gestire, con un set di opzioni ridotto per semplificare l'utilizzo.

6. Affidabilità

- Zero Trust: L'affidabilità dipende dalla corretta implementazione delle politiche di sicurezza e dalla disponibilità dei servizi di autenticazione e autorizzazione.
- ZeroTier: Affidabile, ma la connettività potrebbe essere influenzata da problemi di rete o di connessione.
- VPN IPsec: Affidabile se configurato correttamente, ma può essere soggetto a interruzioni in caso di problemi di connettività o configurazione.
- OpenVPN: Affidabile, ma la stabilità potrebbe essere influenzata da fattori esterni come la qualità della connessione Internet.
- WireGuard: Considerato altamente affidabile grazie alla sua architettura semplice e robusta.

7.Conclusione

Ogni tecnologia ha i propri vantaggi e svantaggi. La scelta migliore dipende dalle esigenze specifiche dell'organizzazione, comprese considerazioni come sicurezza, prestazioni, facilità d'uso e scalabilità. Prima di adottare una tecnologia, è consigliabile condurre una valutazione dettagliata per garantire che soddisfi i requisiti specifici dell'ambiente di utilizzo.

L’approccio Cloudflared

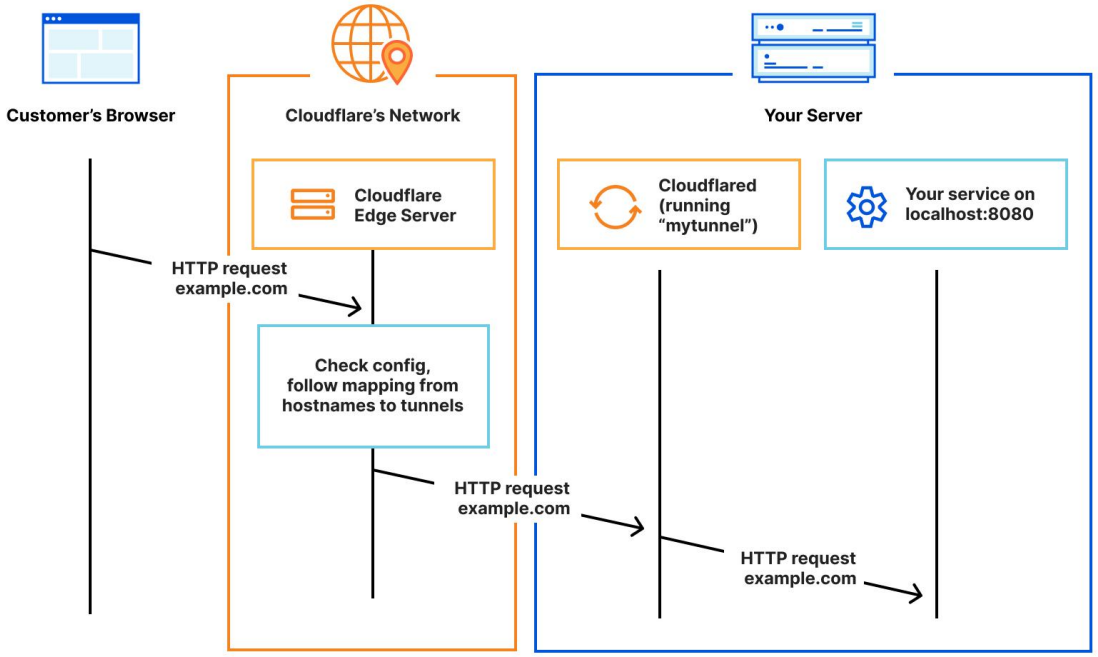
Cloudflare Tunnel, che utilizza l'applicazione Cloudflared, è una tecnologia che consente di stabilire connessioni sicure e private tra i dispositivi degli utenti e l'infrastruttura di Cloudflare attraverso Internet pubblico. Questo permette agli utenti di accedere a risorse all'interno di reti private o dietro firewall senza esporre direttamente tali risorse alla rete pubblica. Ecco come funziona:

1. Agente Cloudflared: L'utente installa e avvia l'applicazione Cloudflared sul proprio dispositivo client. Cloudflared funge da agente che gestisce la connessione sicura con l'infrastruttura di Cloudflare.
2. Connessione TLS: Cloudflared stabilisce una connessione sicura TLS con l'infrastruttura di Cloudflare, garantendo la confidenzialità e l'integrità del traffico.
3. Autenticazione e Autorizzazione: Cloudflare autentica l'agente Cloudflared e autorizza l'accesso alle risorse specifiche nell'infrastruttura. Questo può includere la verifica delle credenziali e l'applicazione di politiche di accesso definite dall'utente.
4. Tunneling: Cloudflared crea un tunnel crittografato attraverso Internet pubblico tra il dispositivo client e l'infrastruttura di Cloudflare, permettendo il trasferimento sicuro del traffico.
5. Accesso alle Risorse Private: Attraverso il tunnel, il dispositivo client accede alle risorse protette all'interno della rete privata o dietro firewall, con Cloudflare che agisce come intermediario per instradare il traffico in modo sicuro.
6. Gestione e Monitoraggio: Cloudflare fornisce strumenti per configurare, gestire e monitorare i tunnel Cloudflared attraverso il suo pannello di controllo, consentendo agli amministratori di controllare l'accesso alle risorse e monitorare l'utilizzo e le prestazioni dei tunnel.

Concetti del Tunnel Cloudflare

Il Tunnel Cloudflare offre un modo sicuro per collegare le risorse a Cloudflare senza esporre un indirizzo IP pubblicamente raggiungibile. Utilizzando il demone leggero 'cloudflared', il Tunnel crea solo connessioni in uscita alla rete globale di Cloudflare, consentendo di connettere in modo sicuro server web HTTP, server SSH, desktop remoti e altri protocolli a Cloudflare. Questo permette alle tue origini di servire il traffico attraverso Cloudflare senza rischiare gli attacchi che aggirano la sicurezza di Cloudflare. Cloudflared stabilisce connessioni in uscita (tunnel) tra le tue risorse e la rete globale di Cloudflare, con i tunnel che sono oggetti persistenti che dirigono il traffico verso i record DNS. Puoi eseguire diversi processi 'cloudflared' (connettori)

all'interno dello stesso tunnel, ognuno dei quali stabilirà connessioni con Cloudflare e invierà il traffico al data center Cloudflare più vicino.



Use Cases

Connessione tramite SSH attraverso il Tunnel Cloudflare

Il Protocollo Secure Shell (SSH) consente agli utenti di accedere remotamente ai dispositivi tramite la riga di comando. Con Cloudflare Zero Trust, puoi rendere il tuo server SSH disponibile su Internet senza il rischio di aprire porte in ingresso sul server. Cloudflare Zero Trust offre due soluzioni per fornire accesso sicuro ai server SSH:

- Instradamento della subnet privata con Cloudflare WARP verso il Tunnel
- Instradamento del nome host pubblico con accesso a cloudflared

Connessione al desktop remoto tramite Tunnel Cloudflare

Il Protocollo Desktop Remoto (RDP) fornisce un'interfaccia grafica per consentire agli utenti di connettersi a un computer in remoto. L'RDP è comunemente utilizzato per facilitare un semplice accesso remoto a macchine o postazioni di lavoro a cui gli utenti non possono accedere fisicamente. Tuttavia, ciò rende anche le connessioni RDP soggette ad attacchi frequenti, poiché una configurazione errata può consentire involontariamente l'accesso non autorizzato alla macchina. Con Cloudflare Zero Trust, puoi godere della comodità di rendere il tuo server RDP disponibile su Internet senza il rischio di aprire porte in ingresso sul tuo server locale. Cloudflare Zero Trust offre due soluzioni per fornire accesso sicuro ai server RDP:

- Instradamento della subnet privata con Cloudflare WARP verso il Tunnel
- Instradamento del nome host pubblico con accesso a cloudflared

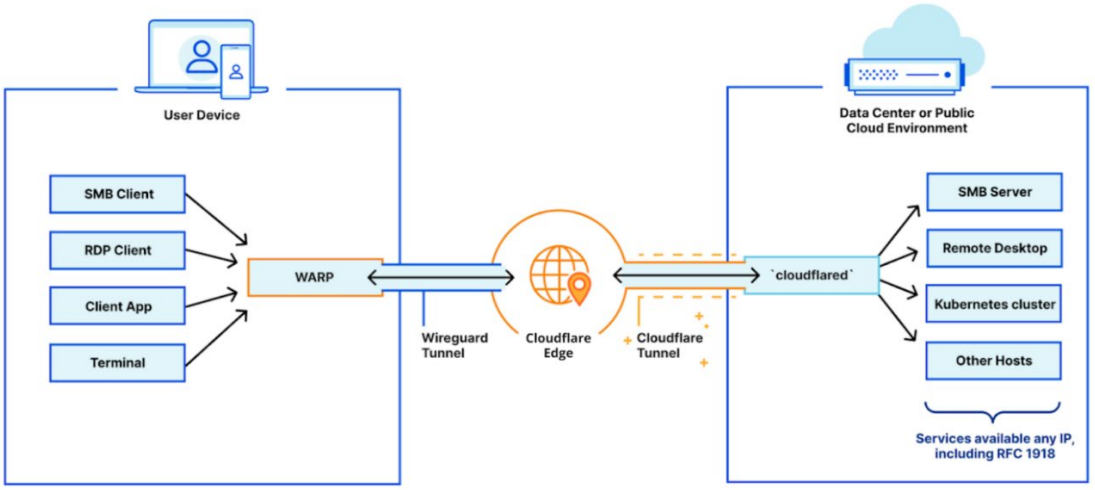
Accedi ad unità SMB tramite Tunnel Cloudflare

Il protocollo Server Message Block (SMB) consente agli utenti di leggere, scrivere e accedere a risorse condivise su una rete. A causa dei rischi per la sicurezza, firewall e provider di servizi Internet di solito bloccano le connessioni pubbliche a una condivisione di file SMB. Con Cloudflare Tunnel, puoi fornire accesso SMB sicuro e semplice agli utenti al di fuori della tua rete. Cloudflare Zero Trust offre due soluzioni per la connessione ai server SMB:

- Instradamento della subnet privata con Cloudflare WARP verso il Tunnel
- Instradamento del nome host pubblico con accesso a cloudflared

Connettere reti private

Una rete privata ha due componenti principali: il server e il client. L'infrastruttura del server (sia che si tratti di un'applicazione singola, di più applicazioni o di un segmento di rete) è collegata alla rete globale di Cloudflare tramite il Tunnel Cloudflare. Ciò viene fatto eseguendo il demone cloudflared sul server. Dal lato del client, gli utenti finali si connettono alla rete globale di Cloudflare utilizzando il client Cloudflare WARP. Il client WARP può essere distribuito a tutta la tua organizzazione in pochi minuti utilizzando gli strumenti MDM interni. Quando gli utenti si connettono a un IP reso disponibile tramite il Tunnel Cloudflare, WARP invia la loro connessione attraverso la rete di Cloudflare al tunnel corrispondente.



Creare reti private con WARP-to-WARP

Con Zero Trust di Cloudflare, è possibile creare una rete privata tra due o più dispositivi che eseguono Cloudflare WARP. Ciò significa che è possibile avere una rete privata tra il telefono e il laptop senza mai dover essere connessi alla stessa rete fisica. Se hai già un'implementazione Zero Trust esistente, puoi anche abilitare questa funzionalità per aggiungere la connettività dispositivo-dispositivo alla tua rete privata con un semplice clic. Ciò ti consentirà di connetterti a qualsiasi servizio che si basa su protocolli basati su TCP, UDP o ICMP tramite la rete di Cloudflare. Gli utenti della tua organizzazione possono raggiungere questi servizi iscrivendosi all'account Zero Trust della tua organizzazione. Una volta iscritti, a ogni dispositivo viene assegnato un indirizzo IP virtuale nell'intervallo 100.96.0.0/12 che consentirà agli utenti o ai sistemi di indirizzare direttamente questi dispositivi. Gli amministratori saranno quindi in grado di creare politiche di Zero Trust per determinare chi all'interno della tua organizzazione può raggiungere quegli indirizzi IP virtuali. Questa guida copre come:

- Abilitare la connettività WARP-to-WARP per stabilire una rete privata tra i tuoi dispositivi.
- Gestire le preferenze di Split Tunnel per il client WARP per determinare quale traffico deve essere instradato verso la rete globale di Cloudflare.
- Creare politiche di sicurezza Zero Trust per limitare l'accesso.

- Connettersi agli spazi IP virtuali dai dispositivi WARP senza alcuna modifica alla configurazione lato client.

Configurare il Connettore WARP

Il Connettore WARP di Cloudflare è un software che consente la connettività site-to-site, bidirezionale e mesh senza richiedere modifiche all'infrastruttura di routing di rete sottostante. Il Connettore WARP stabilisce una connessione sicura di livello 3 tra una rete privata e Cloudflare, consentendoti di:

- Connettere due o più reti private tra loro.
- Collegare dispositivi IoT che non possono eseguire software esterni, come stampanti e telefoni IP.
- Filtrare e registrare il traffico avviato dal server, come il traffico VoIP e SIP.
- Applicare politiche di sicurezza Zero Trust basate sull'indirizzo IP di origine della richiesta.

Reti virtuali

Le reti virtuali ti consentono di connettere reti private che hanno intervalli di indirizzi IP sovrapposti senza creare conflitti per utenti o servizi. Ad esempio, un'organizzazione potrebbe voler esporre due reti private virtuali distinte che considera "produzione" e "staging". Tuttavia, se le due reti private ricevessero casualmente la stessa assegnazione di indirizzi IP RFC 1918, potrebbero esserci due risorse diverse con lo stesso indirizzo IP. Creando due reti virtuali separate, è possibile instradare in modo deterministico il traffico verso indirizzi privati duplicati come 10.128.0.1/32 staging e 10.128.0.1/32 produzione. Queste reti virtuali appariranno come opzioni selezionabili dall'utente all'interno dell'interfaccia grafica del client WARP. Casi d'uso Ecco alcuni scenari in cui le reti virtuali possono rivelarsi utili:

- Gestire ambienti di produzione e staging che utilizzano lo stesso spazio degli indirizzi.
- Gestire acquisizioni o fusioni tra organizzazioni che utilizzano lo stesso spazio degli indirizzi.
- Consentire ai servizi professionali IT di accedere alla rete dei propri clienti per vari scopi di amministrazione e gestione.
- Consentire agli sviluppatori o agli utenti homelab di instradare in modo deterministico il traffico attraverso la propria rete domestica per imporre ulteriori controlli di sicurezza.
- Garantire ulteriore segmentazione (oltre alla sola applicazione di politiche) tra reti e risorse per motivi di sicurezza, mantenendo tutta la configurazione all'interno di un singolo account Cloudflare.

DNS privato

Per impostazione predefinita, il client WARP invia le richieste DNS a 1.1.1.1, il risolutore DNS pubblico di Cloudflare, per la risoluzione. Con Cloudflare Tunnel, puoi connettere un risolutore DNS interno a Cloudflare e utilizzarlo per risolvere domini non pubblicamente instradati.

Conclusioni

In conclusione, l'architettura Cloudflare Tunnel basata su Cloudflared offre un modo sicuro e privato per consentire agli utenti di accedere alle risorse protette all'interno di reti private o dietro firewall. Utilizzando connessioni TLS crittografate e tunneling sicuro attraverso Internet pubblico, Cloudflare Tunnel protegge le risorse dall'esposizione diretta e offre un livello aggiuntivo di sicurezza e controllo per le organizzazioni.