Alma Mater Studiorum - Università di Bologna

Scuola di Scienze

Corso di Laurea in Informatica

Analisi e confronto tra ZeroTier e OpenVPN: analisi di configurazione e applicazioni di due soluzioni VPN

Relatore:
Prof. Andrea Melis

Presentata da:
Marco Milani

Sessione Unica
Anno Accademico 2023/2024

Introduzione

L'obiettivo di questa tesi è analizzare e confrontare le caratteristiche di ZeroTier e OpenVPN, due soluzioni VPN. Le VPN sono strumenti fondamentali per garantire la sicurezza delle connessioni e la protezione dei dati nel contesto di reti aziendali e non solo, specialmente nella nostra epoca in cui la connettività globale e il lavoro remoto sono in costante crescita. Con l'introduzione e la nascita di nuove tecnologie, risulta fondamentale valutare l'efficacia delle VPN sia in termini prestazionali che di sicurezza.

L'obiettivo principale di questo lavoro è fornire un confronto basato su parametri come la latenza, il throughput, la scalabilità e la sicurezza delle due soluzioni. Oltre a questo, sono state analizzate anche le varie difficoltà che si possono riscontrare durante l'installazione e configurazione di entrambe le tecnologie, in quanto per determinati utenti può essere un fattore molto influente nella scelta della soluzione migliore, ad esempio in contesti aziendali. L'intento è quello di comprendere quale possa risultare più efficiente in contesti d'uso specifici, offrendo così uno studio utile per chi ha necessità di scegliere tra le due tecnologie.

Le conclusioni di questo studio puntano a fornire una visione chiara e sintetica sui punti di forza e le criticità di ciascuna soluzione, con l'obiettivo di guidare il lettore verso una scelta informata basata sui dati raccolti.

Indice

Elenco delle figure

Elenco delle tabelle

1. Stato dell'arte

1.1 Introduzione alle Reti Private Virtuali (VPN)

Una VPN (Virtual Private Network) è un sistema che consente di creare una rete privata utilizzando tecniche di tunneling [1] o crittografia attraverso Internet, che è una rete pubblica. Il termine "Network" indica un insieme di dispositivi interconnessi, come computer, router o stampanti, che comunicano tra loro utilizzando vari protocolli e tecnologie. Questi dispositivi possono trovarsi in località geografiche diverse e utilizzano metodi diversi per scambiarsi dati. Il termine "Private" implica un certo livello di segretezza nelle comunicazioni tra due o più dispositivi. Solo i partecipanti alla rete privata sono a conoscenza dei dati trasmessi, mentre gli estranei non possono accedere o conoscere il contenuto delle comunicazioni. Questo concetto di privacy è legato anche alla sicurezza, poiché i dati devono essere protetti da eventuali interferenze o intercettazioni. Il termine "Virtual" si riferisce a qualcosa che simula o replica una realtà fisica. Nel caso delle VPN, una rete "virtuale" simula una rete privata all'interno di un'infrastruttura di rete condivisa, come Internet. Le comunicazioni virtuali vengono isolate attraverso partizioni logiche, garantendo che solo i partecipanti autorizzati abbiano accesso, nonostante l'infrastruttura sottostante sia condivisa da molteplici utenti o organizzazioni. Quindi, una VPN è una rete privata costruita su un'infrastruttura pubblica, dove l'accesso è limitato a una specifica comunità di interesse. La rete è protetta e segmentata virtualmente da altri utenti che condividono la stessa infrastruttura, permettendo così comunicazioni sicure e riservate. [13]

[1] Il tunneling è una tecnologia che consente a una rete di inviare i propri dati tramite le connessioni di un'altra rete. Il tunneling funziona incapsulando un protocollo di rete all'interno di pacchetti trasportati dalla seconda rete. [8]

Motivazioni dell'utilizzo della VPN: Le VPN nascono dall'esigenza di virtualizzare le comunicazioni di un'organizzazione, rendendole invisibili a osservatori esterni, pur sfruttando infrastrutture comuni. Il vantaggio economico principale risiede nel ridurre i costi, raggruppando più servizi di comunicazione su una singola rete, invece di gestire reti separate. Tuttavia, è necessario mantenere un livello di isolamento per proteggere la privacy e l'integrità dei dati. La sicurezza varia in base alle esigenze: da semplici meccanismi di oscuramento a forti misure crittografiche. Storicamente, uno dei precursori delle VPN è stato il Public Data Network (PDN, rete pubblica di trasmissione dati), che include Internet. Tuttavia, l'uso di una rete pubblica non garantisce la riservatezza, e per questo molte organizzazioni preferiscono utilizzare VPN per proteggere la comunicazione tra sedi geograficamente distanti, garantendo privacy, integrità dei dati e qualità del servizio.

1.2 Sistemi OT (e IT) e dispositivi IoT/IIoT

I sistemi OT (Operational Technology) e IT (Information Technology) rappresentano due domini tecnologici distinti, ma sempre più integrati grazie alla diffusione dell'Internet of Things (IoT) e dell'Industrial Internet of Things (IIoT).

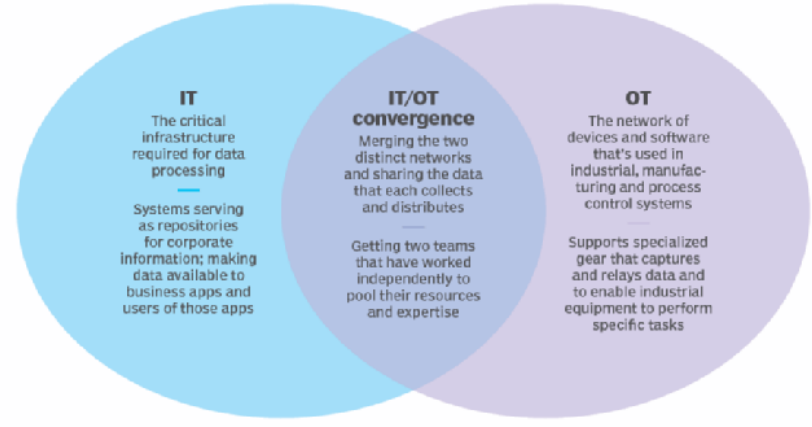

Figura 1.1: Diagramma introduttivo sui sistemi IT e OT. [7]

La tecnologia operativa (OT) si riferisce all'impiego di dispositivi hardware e software per il monitoraggio e il controllo di processi fisici, spesso legati a impianti industriali. I sistemi OT sono ampiamente utilizzati in settori che richiedono molte risorse e svolgono compiti che spaziano dal controllo delle infrastrutture critiche alla gestione di robot in ambienti di produzione. Questa tecnologia trova applicazione in vari settori industriali, tra cui la produzione, il petrolio e il gas, la generazione e distribuzione di energia elettrica, l'aeronautica, il trasporto marittimo e ferroviario, e i servizi pubblici.

I sistemi IT, invece, si focalizzano sulla gestione delle informazioni digitali, come server, reti e applicazioni, utilizzati per raccogliere, elaborare e archiviare dati. Storicamente, OT e IT erano separati, ma l'emergere di tecnologie come l'IIoT ha reso necessaria una maggiore integrazione tra i due ambiti. L'IIoT si riferisce all'applicazione dei principi IoT in contesti industriali, consentendo ai dispositivi OT di connettersi a reti IT per migliorare l'efficienza operativa, l'analisi dei dati e la manutenzione predittiva.

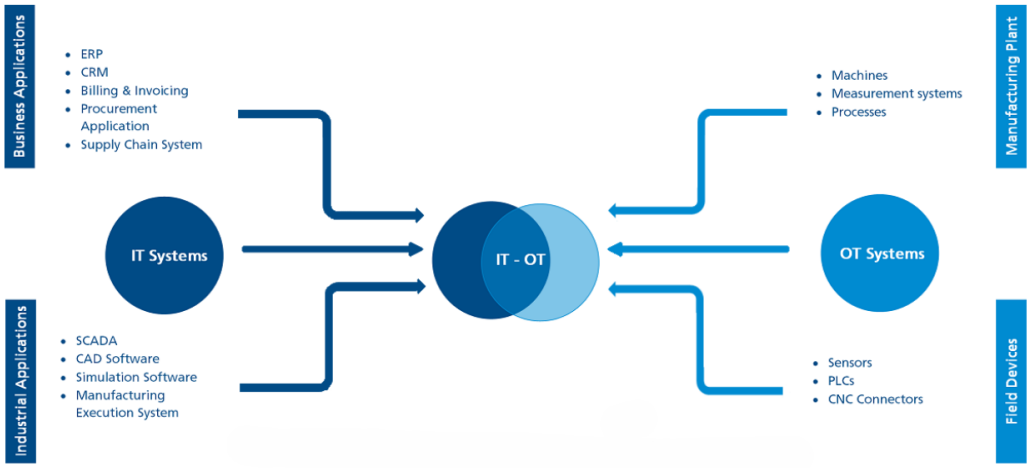

Figura 1.2: Convergenza tra IT e OT: l'unione tra infrastrutture IT per la gestione dei dati e sistemi OT per il controllo dei processi industriali. [16]

L'Internet of Things (IoT) è una rete costituita da dispositivi interconnessi che integrano sensori e altre tecnologie per raccogliere, trasmettere e

ricevere dati. Questi dispositivi, che possono includere sensori ambientali, elettrodomestici, dispositivi indossabili e dispositivi industriali (IIoT), sono in grado di comunicare tra loro con sistemi centralizzati, scambiando informazioni in tempo reale. Grazie all'IoT, i dispositivi possono essere monitorati e controllati da remoto, consentendo l'automazione e l'ottimizzazione di una vasta gamma di processi, dai contesti industriali e produttivi fino alle applicazioni domestiche e smart city. Questo paradigma tecnologico permette una gestione intelligente delle risorse, migliora l'efficienza operativa e favorisce lo sviluppo di nuovi servizi basati sui dati raccolti da questi dispositivi interconnessi.

L'integrazione dei dispositivi IIoT nelle operazioni industriali è un processo strategico che richiede un'attenta pianificazione e il software giusto. L'obiettivo è stabilire un sistema sicuro, affidabile ed efficiente che raccolga e analizzi i dati in modo continuo, offrendo importanti informazioni per il progresso delle attività.

Proprio per questo motivo, le soluzioni VPN possono essere molto rilevanti, poiché con l'integrazione di OT e IT, la necessità di proteggere le comunicazioni tra dispositivi industriali e i sistemi centrali diventa fondamentale. Le VPN possono fornire una connessione sicura tra diverse reti, inclusi ambienti industriali remoti, consentendo ai dispositivi OT di connettersi a reti aziendali IT senza compromettere la sicurezza.

Le VPN, quindi, sono utilizzate per garantire la sicurezza delle comunicazioni tra i dispositivi IoT e IIoT e i sistemi centrali, evitando potenziali attacchi e intrusioni esterne in ambienti sensibili come le fabbriche o le infrastrutture critiche.

1.3 Soluzioni VPN Open Source

Le soluzioni VPN open source offrono numerosi vantaggi, come la trasparenza del codice sorgente, la possibilità di personalizzazione e il supporto di una comunità attiva di sviluppatori e utenti. Tuttavia, presentano anche alcune criticità. Il supporto tecnico, infatti, dipende spesso dalla comunità o da

fornitori terzi, a differenza delle opzioni commerciali che offrono assistenza diretta da parte dall'azienda produttrice. Inoltre, la documentazione potrebbe non risultare sempre completa e aggiornata. Tra le principali soluzioni VPN open source si annoverano ZeroTier, Tailscale, Pritunl, Tinc, NetMaker e OpenVPN. Ciascuna di queste piattaforme si distingue per caratteristiche specifiche che la rendono adatta a differenti contesti d'uso:

- ZeroTier si contraddistingue per la sua ampia compatibilità, facilità di configurazione e la capacità di creare reti private su invito.
- Tailscale pone enfasi sulla semplicità d'uso e l'integrazione con Active Directory, risultando una scelta ideale per le aziende che ne fanno uso per la gestione degli utenti.
- Nebula offre un maggiore controllo sull'infrastruttura di rete e una soluzione self-hosted.
- Pritunl vanta una sicurezza avanzata e supporta diversi protocolli VPN.
- Tinc eccelle per la sua flessibilità e scalabilità.
- NetMaker utilizza il protocollo WireGuard per offrire reti ad alta velocità e scalabilità.
- OpenVPN offre una configurazione altamente flessibile, sicurezza avanzata con protocolli di crittografia robusti e una vasta disponibilità su diverse piattaforme, rendendolo una soluzione popolare da vent'anni, ma a discapito della complessità e dei costi di manutenzione.

La scelta della soluzione più adatta dipende dalle esigenze specifiche dell'azienda, considerando fattori come budget, complessità della rete, requisiti di sicurezza e facilità d'uso. Nei capitoli successivi verranno principalmente approfonditi il confronto tra ZeroTier e OpenVPN e le relative caratteristiche.

1.4 ZeroTier

ZeroTier è una piattaforma open source progettata per facilitare la creazione di reti virtuali sicure e distribuite su scala globale, particolarmente adatta per dispositivi IoT. Il suo principale punto di forza risiede nella capacità di connettere dispositivi provenienti da reti diverse in modo semplice e rapido, riducendo la complessità tipica delle configurazioni di server VPN tradizionali e della gestione di certificati.

ZeroTier supporta numerose piattaforme, tra cui Linux, macOS, Windows, iOS/iPadOS, Android e FreeBSD, rendendolo una soluzione versatile e facilmente integrabile in ambienti eterogenei. Inoltre, offre un piano gratuito per uso personale, che consente di testare la piattaforma senza costi iniziali.

1.4.1 Architettura

A livello architetturale, ZeroTier non si appoggia su protocolli VPN esistenti, ma utilizza il proprio protocollo di rete, sviluppato internamente e basato sullo User Datagram Protocol (UDP)[2]. Questo protocollo permette di stabilire comunicazioni dirette tra dispositivi, superando le problematiche legate a configurazioni complesse di rete e a distanze geografiche. ZeroTier adotta una tecnica chiamata NAT traversal, che consente di superare le limitazioni imposte dal NAT (Network Address Translation). In una rete standard, i dispositivi utilizzano un indirizzo IP privato, che non corrisponde all'indirizzo IP pubblico visibile su Internet. Questo processo di traduzione è gestito da un dispositivo chiamato "router NAT", il cui compito è tradurre gli indirizzi. Il NAT è stato introdotto per affrontare la carenza di indirizzi IPv4, lo standard ancora ampiamente utilizzato su Internet, che ha uno spazio di indirizzamento limitato. Il suo successore, IPv6, risolve questo problema offrendo un numero significativamente maggiore di indirizzi IP. ZeroTier, tramite il NAT traversal, permette ai dispositivi dietro router NAT di

[2]Lo User Datagram Protocol (UDP) è uno dei principali protocolli di rete della suite di protocolli Internet. È un protocollo di livello di trasporto a pacchetto, usato di solito in combinazione con il protocollo di livello di rete IP. [3]

essere accessibili direttamente dall'esterno della rete locale, garantendo una comunicazione fluida e senza interruzioni. [14]

Le reti mesh [3] ZeroTier sono composte da tre principali componenti:

- Dispositivi finali: eseguono il software client zerotier-one, che permette loro di unirsi e abbandonare le reti esistenti.
- Controller di rete: gestiscono l'aggiunta di nuovi membri, la gestione dei certificati e la sincronizzazione della configurazione tra i membri partecipanti nella mesh.
- Root: si occupano della scoperta e della creazione della connessione tra i nodi partecipanti e possono anche inoltrare il traffico quando non è possibile una connessione peer-to-peer diretta tra i nodi mesh.

Sia i controller di rete che le root sono gestiti da ZeroTier, con la possibilità di configurarli su un'infrastruttura privata. Mentre ospitare un controller di rete personalizzato è un processo ben documentato e semplice, impostare una root personalizzata risulta meno intuitivo. [5]

1.4.2 Descrizione generale e funzionalità

Un aspetto distintivo di ZeroTier è la capacità di creare "reti private" su invito. In questo modello, il nodo controller, gestito dall'amministratore della rete, deve approvare ogni dispositivo che intende unirsi alla rete, aggiungendo un ulteriore livello di sicurezza. Questa funzionalità contribuisce a mantenere la rete sicura e ben controllata.

ZeroTier può essere utilizzato come servizio SaaS[4] e offre anche la possibilità di essere eseguito su infrastrutture self-hosted, ovvero organizzazioni che ospitano e gestiscono internamente il proprio software e i propri servizi.

[3] Una rete mesh è una topologia di rete locale in cui i nodi si collegano direttamente, in modo dinamico e non gerarchico, al maggior numero possibile di altri nodi. Questi nodi collaborano per instradare i dati in modo efficiente da e verso i client.[6]

[4] SaaS si riferisce a un modello di distribuzione software, in cui il software viene fornito tramite Internet come servizio.

Per quanto riguarda il relaying del traffico (ovvero l'inoltro del traffico di rete attraverso un intermediario), ZeroTier supporta il relay su TCP tramite una rete di relay distribuiti globalmente (dispositivi che agiscono come intermediari).[5]

1.4.3 Caratteristiche principali

Tra le principali caratteristiche di ZeroTier si evidenziano:

- Velocità: configurazione rapida, con distribuzione remota e automatizzata.
- Flessibilità: emulazione Ethernet Layer 2 con funzionalità multipath, multicast e bridging.
- Sicurezza: la soluzione Zero Trust di ZeroTier offre una sicurezza scalabile con crittografia end-to-end a 256 bit.
- Semplicità di installazione: l'installazione è di tipo "one-click", semplice e rapida.
- Nessuna complessità di certificati: non è necessario creare o gestire certificati complicati.
- Interfaccia intuitiva: rispetto alla complessità di OpenVPN, ZeroTier offre un'interfaccia grafica più semplice.
- Nessuna installazione di client: non c'è bisogno di installare client aggiuntivi sui dispositivi.
- Nessuna apertura di porte: non è necessario aprire porte sul router per consentire la connessione.

ZeroTier gode di un'ampia diffusione a livello globale, con oltre 3 milioni di dispositivi connessi, 12.700 stelle su GitHub, una comunità di oltre 350.000 membri e una presenza in più di 220 paesi e territori. [11]

1.5 OpenVPN

OpenVPN è un software open source sviluppato da James Yonan nel 2001 con l'obiettivo di fornire una soluzione VPN sicura e versatile per connettere dispositivi attraverso reti non fidate, come Internet. Nel corso degli anni, OpenVPN è diventato uno dei protocolli VPN più popolari, grazie alla sua flessibilità, sicurezza e capacità di funzionare su molteplici piattaforme, tra cui Windows, macOS, GNU/Linux, Android, Solaris e FreeBSD. A differenza di altri protocolli come IPsec o PPTP, OpenVPN sfrutta il protocollo SSL/TLS [5] per la crittografia e l'autenticazione. [18]

1.5.1 Architettura

OpenVPN è noto per la sua struttura flessibile e modulare, che permette di realizzare diverse configurazioni di rete, tra cui accesso remoto, collegamento di sedi distanti e superamento delle restrizioni geografiche.

1.5.2 Sicurezza e Crittografia

Come già accennato, OpenVPN sfrutta i consolidati meccanismi SSL/TLS, utilizzando la libreria OpenSSL. La libreria OpenSSL integra vari protocolli che assicurano il tunneling, fornendo cifratura e sicurezza. Per la crittografia, supporta algoritmi come AES (considerato uno dei più robusti), Blowfish e Camellia. In termini di hashing, si avvale del protocollo SHA, mentre per la crittografia a chiave pubblica utilizza Diffie-Hellman; infine, per l'autenticazione, si affida nuovamente al protocollo SHA [4]. Questo garantisce che il traffico trasmesso attraverso il tunnel VPN sia completamente sicuro e protetto, conferendo un'elevata protezione dei dati e una gestione efficace delle chiavi crittografiche.

Inoltre, la piattaforma supporta diversi metodi di autenticazione, tra i quali:

[5] Secure Socket Layer (SSL) e Transport Layer Security (TLS) sono protocolli utilizzati per fornire servizi di sicurezza affidabili a livello del protocollo di trasporto.

- Chiavi private condivise (PSK[6]) grazie al protocollo Diffie-Helmann.
- Certificati digitali.
- Autenticazione, che può avvenire tramite username e password o attraverso il protocollo SHA.

Questa flessibilità consente agli amministratori di rete di scegliere il metodo di autenticazione più adatto alle proprie esigenze, aumentando così il livello complessivo di sicurezza.

1.5.3 Vantaggi

Sicurezza e affidabilità OpenVPN è noto per essere una delle soluzioni VPN più sicure disponibili, grazie al protocollo SSL/TLS e alle librerie che utilizza per la crittografia. Questo lo rende meno vulnerabile rispetto a molte altre implementazioni VPN.

Adattabilità multi-piattaforma OpenVPN è compatibile con una vasta gamma di piattaforme e sistemi operativi. Questo lo rende una scelta versatile, consentendo di stabilire connessioni VPN sicure da qualsiasi luogo e dispositivo.

Flessibilità e Configurabilità OpenVPN offre grande flessibilità e possibilità di configurazione, permettendo agli amministratori di rete di adattare le impostazioni alle esigenze specifiche dell'infrastruttura. Ciò comprende la possibilità di configurare parametri come crittografia, autenticazione, routing e altre opzioni, per assicurare una connessione VPN efficiente e sicura.

[6]Pre Shared Key (PSK): utilizza una chiave segreta condivisa che è stata scambiata precedentemente tra due utenti utilizzando un canale di comunicazione sicuro. Questo sistema utilizza quasi sempre un algoritmo di crittografia a chiave simmetrica. PSK è un metodo molto efficace, ma se utilizzato per un gruppo di utenti molto vasto può generare dei problemi di scalabilità poiché la chiave individuale dev'essere condivisa con ogni singolo utente.[1]

1.5.4 Limiti

Nonostante i numerosi vantaggi, OpenVPN presenta alcune limitazioni. Il principale svantaggio è legato alla complessità del protocollo SSL/TLS, che può rendere OpenVPN più difficile da configurare rispetto ad altre soluzioni VPN, soprattutto in contesti specifici o avanzati. Una configurazione errata o non ottimizzata potrebbe compromettere sia la sicurezza che le prestazioni del sistema. La gestione di OpenVPN richiede spesso tempo e competenze tecniche avanzate per essere eseguita correttamente. Inoltre, sebbene OpenVPN sia open-source e gratuito, l'implementazione e la gestione su larga scala possono comportare costi significativi, come l'acquisto di hardware e software, la formazione del personale e il supporto tecnico necessario per il corretto funzionamento dell'infrastruttura.

1.6 ZeroTier vs OpenVPN

Prima di procedere con un'analisi approfondita dell'implementazione dei due sistemi, sono state condotte ricerche basate sulle documentazioni ufficiali di entrambe le piattaforme, al fine di offrire una panoramica preliminare. Le principali caratteristiche confrontate tra i due sistemi sono riassunte nella tabella seguente.

	ZeroTier	**OpenVPN**
OpenSource	Sì.	Sì.
Facilità d'uso	Semplice ma può richiedere maggiore configurazione.	Nonostante disponga di grande flessibilità, la configurazione di OpenVPN può risultare molto complessa.

	ZeroTier	**OpenVPN**
Prezzo	Ha una versione base gratuita con opzioni di abbonamento.	Ha una versione gratuita e diversi piani a pagamento per le aziende con prezzo per connessione.
Protocollo VPN	Protocollo proprietario (ZTP).	OpenVPN protocol.
Supporto multi-piattaforma	Linux, macOS, Windows, iOS, Android, FreeBSD.	GNU/Linux, xBSD, macOS, Solaris, iOS, Android e Windows.
Self-Hosted option [7]	È possibile eseguire un piano di controllo self-hosted, sebbene senza un'interfaccia web ufficiale.	OpenVPN può essere implementato in un ambiente self-hosted.
Access control (gestione degli accessi autorizzati)	Sì.	Sì.
Integrazione con identity provider per SSO (Single Sign-On) [8]	No, non è una funzionalità nativa di ZeroTier ma si può configurare in seguito.	Sì, gli utenti vengono gestiti con nomi utente e password.

[7] Una VPN Self-Hosted è gestita internamente dall'organizzazione, senza dipendere da servizi VPN esterni. L'infrastruttura, come server e software, viene installata e configurata su hardware e rete propri.

[8] L'integrazione con un identity provider per SSO significa che il sistema può essere configurato per autenticare gli utenti utilizzando un servizio esterno di gestione delle identità consentendo agli utenti di accedere al sistema una sola volta utilizzando le stesse credenziali, senza dover inserire password diverse per ogni servizio.

	ZeroTier	**OpenVPN**
Peer-to-peer network [9]	Sì.	No, OpenVPN è basato su un modello client-server, in cui un server centrale media la connessione tra i client.
Crittografia end-to-end	Sì.	No.
Anno di nascita	2011.	2001.

Tabella 1.1: Tabella di confronto delle caratteristiche di ZeroTier e OpenVPN.

[9]Una peer-to-peer network è una rete in cui ogni dispositivo può agire sia come client che come server, scambiando direttamente dati con altri nodi senza bisogno di un server centrale.

2. Analisi progettuale

2.1 Obiettivi del progetto

L'obiettivo principale di questa studio è confrontare le caratteristiche delle due soluzioni VPN ampiamente utilizzate: OpenVPN e ZeroTier. Il fine di interesse è valutare quale delle due possa risultare più efficiente e adatta a specifiche esigenze aziendali. Questo lavoro si propone quindi di analizzare le due soluzioni e di presentare un confronto dettagliato in merito alle seguenti aree chiave:

- prestazioni di rete,
- scalabilità,
- semplicità di installazione, configurazione e manutenzione, e
- sicurezza.

2.1.1 Prestazioni di rete

Uno degli obiettivi principali è analizzare le prestazioni di rete offerte da OpenVPN e ZeroTier. Per esaminare questo parametro si affronterà la valutazione di:

Latenza: il tempo che intercorre tra l'invio di un pacchetto dati e la sua ricezione da parte del destinatario.

Throughput: la quantità di dati trasferiti attraverso la rete in un determinato intervallo di tempo.

Questi due aspetti sono correlati ma non necessariamente dipendenti uno dall'altro: la latenza è associata alla prontezza con cui i dati raggiungono la destinazione, mentre il throughput misura il volume di dati che può essere trasferito.

2.1.2 Scalabilità

Un altro obiettivo importante è quello di esaminare la capacità di scalare in ambienti con un numero crescente di dispositivi collegati. Un'analisi a riguardo è utile per valutare come le due soluzioni si comportano in un contesto multi-device, dove possono variare le esigenze in termini di gestione delle risorse e mantenimento delle prestazioni.

2.1.3 Semplicità di installazione, configurazione e manutenzione

Verrà analizzato quanto sia semplice configurare e mantenere attive le due soluzioni. Questo aspetto è particolarmente rilevante per utenti meno esperti o per realtà che richiedono un basso impatto operativo. Verranno esaminate le seguenti aree:

Facilità d'uso: come avviene l'installazione e la configurazione delle due piattaforme.

Gestione dei certificati e autenticazione: le procedure necessarie per garantire sicurezza e autenticazione all'interno della rete.

Accessibilità: l'usabilità delle interfacce grafiche (se presenti) e la possibilità di gestire configurazioni da remoto.

2.1.4 Sicurezza

La sicurezza è un fattore centrale in qualsiasi implementazione VPN. Di seguito verranno confrontate le caratteristiche di sicurezza di OpenVPN e ZeroTier, considerando aspetti quali:

Crittografia: il livello di crittografia utilizzato dalle due soluzioni, valutando la loro adeguatezza in contesti che richiedono elevati standard di protezione.

Controllo degli accessi: la gestione dei permessi e il livello di granularità offerto per consentire l'accesso a utenti e dispositivi.

Modello di autenticazione: il confronto dei meccanismi di autenticazione supportati, inclusi quelli basati su certificati o integrazioni con servizi di autenticazione esterni (SSO, LDAP, etc.).

3. Implementazione

3.1 Installazione e configurazione di ZeroTier

Il processo di installazione e configurazione di ZeroTier si articola in pochi passaggi che permettono la creazione di una rete virtuale in modo intuitivo. La piattaforma richiede inizialmente la registrazione a un account, fondamentale per la gestione centralizzata delle reti. L'account non è richiesto per i dispositivi che desiderano connettersi alla rete, tuttavia ogni dispositivo deve installare il proprio client per poter accedere alla rete creata.

Dopo aver completato la registrazione sul sito ufficiale di ZeroTier, il primo passo consiste nel creare una rete tramite il comando specifico "Create Network".

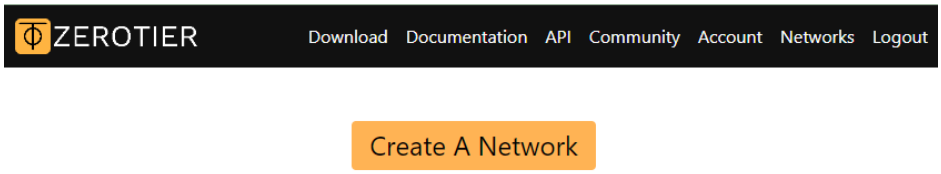

Figura 3.1: Download ZeroTier: "Create A Network".

Questo dà origine a una rete virtuale la cui gestione e configurazione avviene interamente attraverso l'interfaccia web. L'utente ha la possibilità di assegnare un nome alla rete, inserire una descrizione e personalizzare una serie di impostazioni avanzate. Tra queste impostazioni, vi è la scelta degli indirizzi IP da assegnare dinamicamente ai dispositivi connessi, la configurazione di IPv6, e l'eventuale utilizzo di un DNS personalizzato.

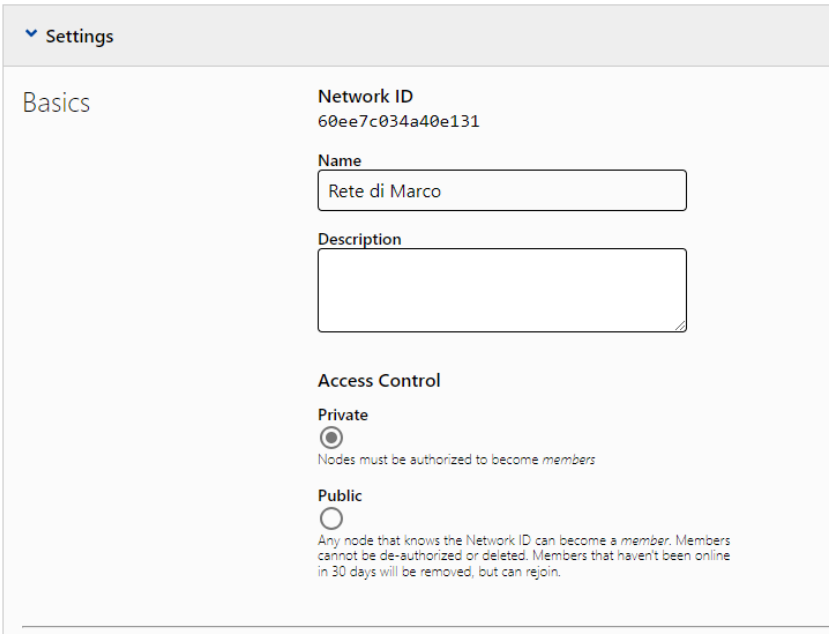

Figura 3.2: Interfaccia di configurazione: nome della rete, descrizione e Access Control.

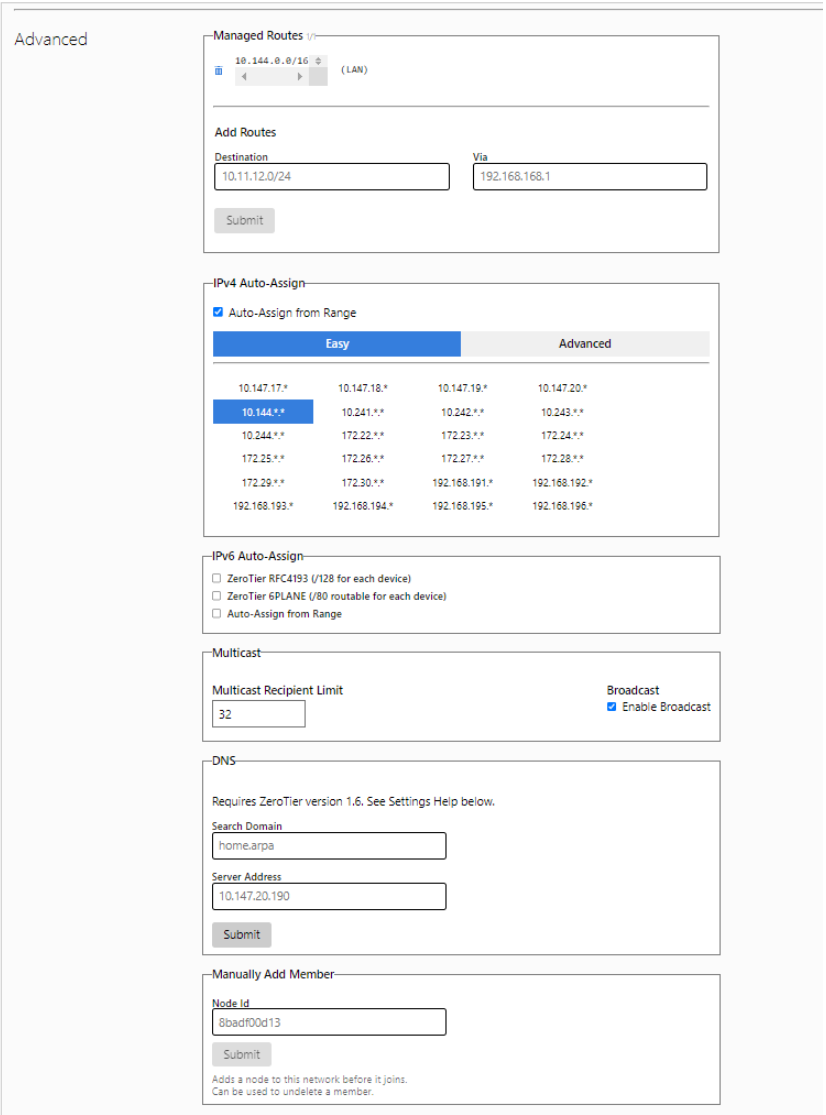

Figura 3.3: Interfaccia di configurazione: impostazioni avanzate.

Un elemento importante della configurazione riguarda il controllo degli accessi. ZeroTier permette di definire se la rete deve essere pubblica o privata. Nel caso di una rete privata, ogni nuovo dispositivo che tenta di connettersi alla rete deve essere preventivamente autorizzato dall'amministratore. Questa operazione avviene tramite un ID di rete univoco, che ogni client deve inserire per richiedere l'accesso. L'amministratore ha poi il compito di appro-

vare manualmente ciascuna richiesta prima che il dispositivo possa accedere alla rete e comunicare con gli altri membri.

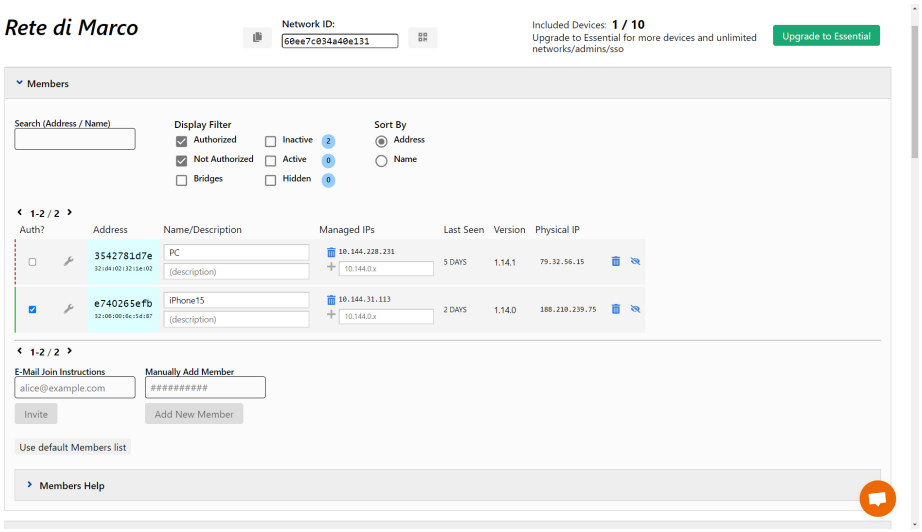

Figura 3.4: Interfaccia di controllo degli accessi di ZeroTier.

La versione gratuita di ZeroTier consente la creazione di al più tre reti, ciascuna delle quali può connettere un massimo di dieci dispositivi. Una volta connessi, i dispositivi possono comunicare tra loro utilizzando gli indirizzi IP assegnati all'interno della sottorete ZeroTier.

Questo sistema permette una rapida configurazione di base, che può essere implementata senza particolari difficoltà tecniche.

Tuttavia, la configurazione di base di ZeroTier presenta alcune limitazioni. Una di queste è la necessità di installare il client su ogni dispositivo che intenda connettersi alla rete. Questa esigenza può rappresentare un problema in quei contesti in cui l'installazione di un software aggiuntivo non è possibile, come nel caso di telecamere di sorveglianza all'interno di una sottorete. In simili scenari, l'unica soluzione praticabile consiste nell'installare un server dedicato all'interno della rete. Questo server fungerà da nodo intermedio, instradando tutte le connessioni verso i dispositivi della rete ZeroTier, eliminando così la necessità di installare il client su dispositivi non compatibili.

3.2 Installazione e configurazione di OpenVPN

L'installazione e la configurazione di OpenVPN su Windows richiede una serie di passaggi fondamentali per garantire il corretto funzionamento di un server VPN.

3.2.1 Installazione di OpenVPN Server su Windows

Il primo passo consiste nel scaricare e installare il pacchetto OpenVPN Server. Il software è disponibile gratuitamente sul sito ufficiale di OpenVPN.

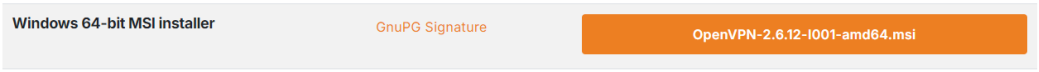

Figura 3.5: Dowload OpenVPN.

Una volta completato il download, è sufficiente eseguire l'installer e seguire le istruzioni fornite, accettando i termini di utilizzo e completando l'installazione nel percorso predefinito.

3.2.2 Creazione di certificati e chiavi per il server

Dopo aver installato OpenVPN, è necessario configurare la PKI (Public Key Infrastructure)[1] per garantire la sicurezza delle connessioni. Questo processo include la creazione delle chiavi e dei certificati sia per il server che per i client.

1. Aprire il Prompt dei Comandi con privilegi di amministratore.

[1]In crittografia una infrastruttura a chiave pubblica, in inglese public key infrastructure (PKI), è un insieme di processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un utente, oltre che di associare una chiave pubblica a un utente, normalmente per mezzo di software distribuito in modo coordinato su diversi sistemi. Le chiavi pubbliche tipicamente assumono la forma di certificati digitali.[2]

2. Spostarsi nella directory Easy-RSA.

3. Eseguire lo script ‘Easy-RSA-Start.bat‘ per iniziare la configurazione. Questo script avvia l’ambiente Easy-RSA, utile per la gestione delle chiavi.

4. Eliminare eventuali configurazioni predefinite, in modo da preparare un nuovo ambiente PKI personalizzato.

5. Inizializzare il database e la struttura della directory per la PKI utilizzando il comando fornito dallo script Easy-RSA.

6. Generare un’Autorità di Certificazione (CA) utilizzando Easy-RSA. Questo passaggio crea il certificato principale necessario per firmare le chiavi.

7. Creare certificati e chiavi specifici per il server OpenVPN.

8. Generare i parametri di Diffie-Hellman, utilizzati per lo scambio sicuro delle chiavi.

Una volta completati questi passaggi, le chiavi e i certificati necessari per il server sono pronti.

3.2.3 Configurazione del server OpenVPN

Con i certificati e le chiavi pronte, è il momento di configurare il server OpenVPN. La configurazione prevede la creazione di un file di configurazione che istruisca OpenVPN su come gestire le connessioni.

1. Creare una nuova cartella ”Server-Config-Files” sul Desktop e copiare al suo interno i certificati e le chiavi generate.

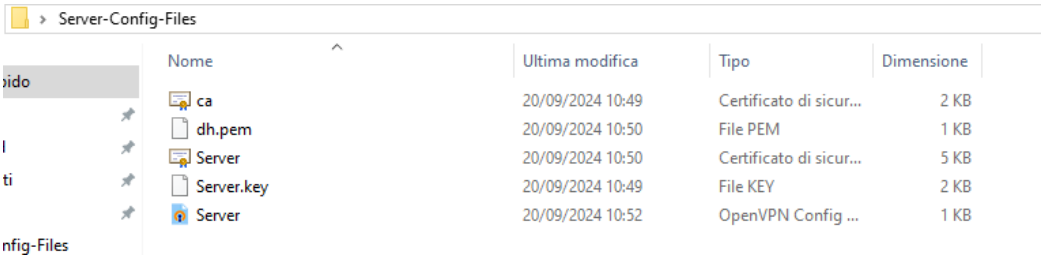

Figura 3.6: Cartella Server-Config-Files.

2. Creare un file di configurazione per il server chiamato ‘server.ovpn‘, contenente i parametri di base per il funzionamento della VPN, come la porta da utilizzare (di solito la porta 1194 con il protocollo UDP).

3. Abilitare l'opzione "IPEnableRouter" per consentire ai client VPN di accedere alla rete locale interna.

4. Configurare la condivisione della connessione internet tra la rete locale e il tunnel VPN.

5. Assicurarsi che il firewall del sistema sia configurato correttamente per consentire il traffico attraverso la porta 1194/UDP.

A questo punto, la configurazione del server è completata e pronta per essere utilizzata.

3.2.4 Creazione di un profilo client

Per consentire ai client di connettersi alla VPN, è necessario generare dei certificati e delle chiavi per ogni client.

1. Utilizzando Easy-RSA, generare un certificato e una chiave per un client, ad esempio denominato "Client1".

2. Copiare i file necessari per la connessione del client (certificato, chiave, configurazione) in una nuova cartella "Client-Config-Files" sul Desktop.

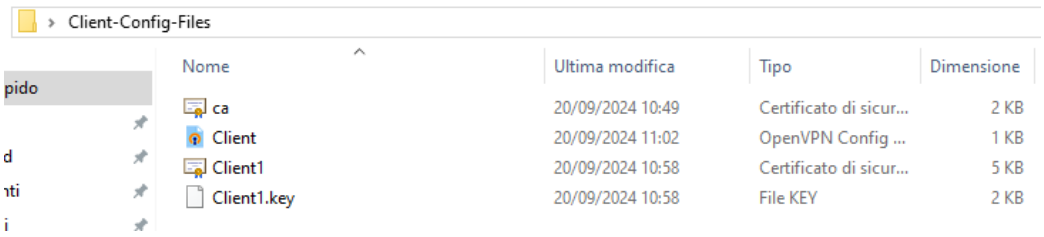

Figura 3.7: Cartella Client-Config-Files.

3.2.5 Configurazione del client OpenVPN

Ora è necessario configurare il client OpenVPN per connettersi al server:

1. Copiare i file di configurazione dal server alla macchina client.
2. Scaricare e installare OpenVPN sul client, seguendo la stessa procedura utilizzata per il server.
3. Creare un file di configurazione per il client che includa i certificati e le chiavi forniti dal server.
4. Copiare tutti i file nella cartella di configurazione di OpenVPN sul client
5. Configurare il firewall del client per consentire il traffico attraverso la porta 1194/UDP.

A questo punto, è possibile testare la connessione per assicurarsi che il client possa connettersi correttamente al server.

4. Analisi

In questo capitolo si andrà ad analizzare le differenze strutturali e funzionali che emergono tra ZeroTier e OpenVPN e in che modo queste possano influenzare l'uso di ciascuna tecnologia in specifici ambiti.

4.1 Architettura e modello di comunicazione

ZeroTier adotta un modello peer-to-peer (abbreviato: P2P) che permette la comunicazione diretta tra client, bypassando, nella maggior parte dei casi, la necessità di un server centrale. Ciò lo rende ideale per scenari in cui due dispositivi, come un PC e uno smartphone, devono comunicare tra loro senza una configurazione di rete complessa. OpenVPN, invece, si basa su un'architettura client-server, in cui tutti i client devono passare attraverso un server centrale per comunicare. Questo modello è più orientato all'accesso a risorse centralizzate, come stampanti o file server, in un'infrastruttura aziendale.

Per quanto riguarda l'applicazione in rete, ZeroTier è particolarmente utile per connettere dispositivi remoti senza richiedere la configurazione specifica della rete locale, facilitando la gestione di reti eterogenee. Per esempio, permette di collegare più punti (come casa, ufficio e dispositivi mobili) senza dover configurare dettagli come subnet o routing statico. OpenVPN, d'altro canto, richiede una configurazione di rete predefinita. Le reti che si vogliono connettere tramite OpenVPN devono avere classi IP differenti per evitare conflitti, rendendo la configurazione più tecnica e impegnativa.

ZeroTier è un sistema che lavora con IP dinamici e riesce a superare alcuni degli ostacoli tipici delle reti VPN tradizionali, come la necessità di configurare port forwarding o IP statici. OpenVPN, invece, lavora con IP statici e talvolta è necessario configurare un DNS (Domain Name System), ovvero un sistema dei nomi di dominio che traduce nomi in indirizzi IP. In questo modo, anche se si ha un indirizzo IP dinamico, il DNS può comunicare sempre l'indirizzo IP di un determinato dispositivo nonostante i cambiamenti

dinamici di IP. Nonostante l'utilizzo di un DNS, la latenza che esso comporta può essere considerata trascurabile.

4.2 Sicurezza

In termini di sicurezza, entrambi i sistemi offrono solide implementazioni di crittografia. Di seguito verranno analizzate la crittografia, l'autenticazione, la gestione delle chiavi e il firewall e la traversata NAT.

4.2.1 Crittografia

OpenVPN sfrutta principalmente il protocollo SSL/TLS per lo scambio di chiavi e la protezione dei dati, e utilizza algoritmi di crittografia avanzati come AES-256 (cifrario estremamente vantaggioso in termini di semplicità e rapidità, e con un elevato livello di sicurezza) per il traffico dati. La sua configurabilità permette di scegliere tra diversi protocolli di sicurezza (come TCP o UDP). Queste caratteristiche lo rendono noto per la sua robusta sicurezza crittografica,

ZeroTier adotta una crittografia a 256 bit end-to-end per il traffico tra nodi. La chiave privata di ciascun nodo è conosciuta solo dal nodo stesso, garantendo che ogni comunicazione sia sicura e privata. ZeroTier implementa un'architettura a chiave pubblica decentralizzata.

4.2.2 Autenticazione

Come visto precedentemente, OpenVPN supporta diverse modalità di autenticazione: certificati digitali, autenticazione tramite password e l'uso di hardware token. L'autenticazione a due fattori (2FA) può essere integrata per migliorare ulteriormente la sicurezza.

ZeroTier, invece, utilizza chiavi crittografiche per l'autenticazione dei nodi, e ogni dispositivo ottiene una chiave privata che viene usata per autenticarsi all'interno della rete. Inoltre, offre anche la possibilità di aggiungere nodi alle reti private solo su invito, riducendo il rischio di accessi non autorizzati.

4.2.3 Gestione delle chiavi

La gestione delle chiavi di OpenVPN è centralizzata e richiede la configurazione manuale e distribuzione dei certificati SSL.

ZeroTier gestisce le chiavi in modo automatico: le chiavi pubbliche e private vengono generate al momento dell'installazione del nodo e sono automaticamente riconosciute e utilizzate per la crittografia e l'autenticazione.

4.2.4 Firewall e NAT Traversal

OpenVPN necessita di una configurazione appropriata dei firewall e, in alcuni casi, può richiedere il forwarding delle porte. Tuttavia, supporta tecniche come l'uso di UDP per attraversare NAT e firewall.

ZeroTier è altamente efficiente nell'attraversamento di NAT e firewall senza bisogno di particolari configurazioni, grazie al suo utilizzo di tecniche avanzate di NAT traversal. Questo lo rende particolarmente sicuro e versatile in ambienti con firewall restrittivi o complessi, riducendo il rischio di configurazioni vulnerabili.

Entrambe le soluzioni VPN, OpenVPN e ZeroTier, offrono una sicurezza elevata, ma utilizzano approcci diversi. OpenVPN è altamente configurabile e offre flessibilità avanzata per chi desidera avere controllo sulla sicurezza, grazie alla sua architettura SSL/TLS e alla gestione manuale dei certificati. ZeroTier, invece, presenta una gestione delle chiavi automatizzata e crittografia end-to-end, riducendo il rischio di errori nella configurazione.

4.3 Scalabilità

Per valutare la scalabilità delle due soluzioni VPN, si sono presi in considerazione dei test discussi nella conferenza "Scalability evaluation of VPN technologies for secure container networking" [12] volti a determinare quanto bene un software VPN può gestire grandi quantità di connessioni e chiamate di servizio. Il relativo articolo ne spiega i risultati in modo da valutare

la scalabilità di diverse soluzioni VPN tra cui appunto OpenVPN e ZeroTier. Essi sono stati condotti utilizzando l'infrastruttura di IDLab Virtual Wall, con macchine aventi lo stesso hardware e situate nella stessa posizione geografica. Ogni macchina era equipaggiata con due processori Intel E5520 Quad-core a 2,2 GHz e 12 GiB di RAM. Un totale di 8 macchine, configurate con Ubuntu 16.04 e Docker 18.06, sono state utilizzate per creare un cluster Kubernetes [1] v1.11, composto da un nodo master e 7 nodi worker. Kubernetes è stato scelto per facilitare la distribuzione di numerosi container client VPN, simulando una rete con molti client indipendenti. Ogni test prevedeva la distribuzione di un certo numero di "pod" (che varia da 50 a 750, in incrementi di 100), ciascuno contenente un container con un client VPN e uno script configurabile per testare la connettività. I pod inviavano richieste REST ogni 250 ms per 15 minuti, senza corpo, e ricevevano una risposta con codice HTTP 200 (il codice HTTP 200 indica che la richiesta del client è stata accolta ed elaborata con successo). Questo approccio, caratterizzato da messaggi brevi, emula il traffico tipico dei sensori IoT, spesso presente nelle reti edge. I risultati del test sono stati aggregati e analizzati per determinare come i tempi di risposta e i tassi di errore variano con una quantità crescente di pod.

[1] Kubernetes è una piattaforma portatile, estensibile e open-source per la gestione di carichi di lavoro e servizi containerizzati, in grado di facilitare sia la configurazione dichiarativa che l'automazione.

4.3.1 Tempo di risposta

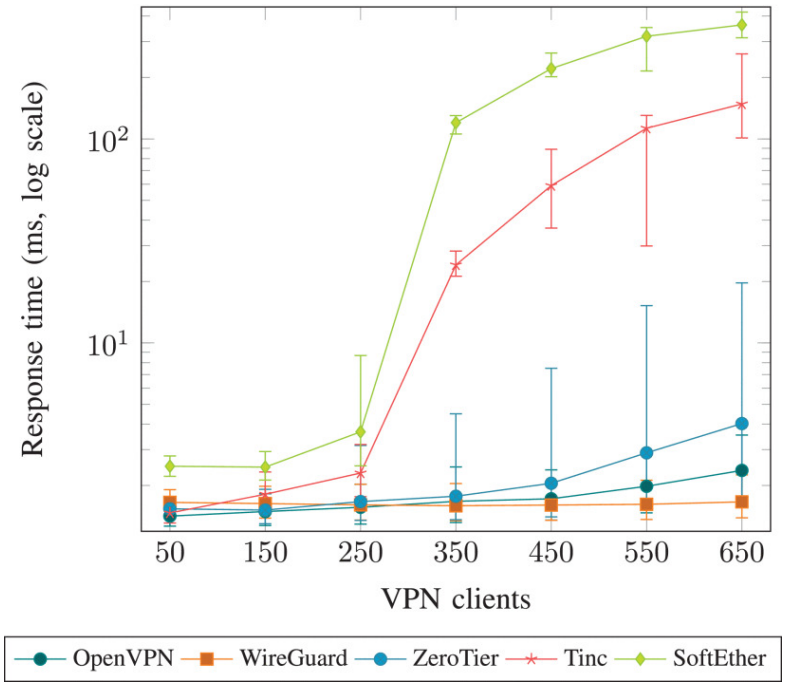

Figura 4.1: Evoluzione del tempo di risposta per un numero crescente di client VPN, rappresentato su scala logaritmica.

Nel test di scalabilità, i risultati (figura 4.1) evidenziano comportamenti distinti a seconda del numero di client connessi. Fino a 450 client, entrambi i protocolli mostrano prestazioni simili in termini di tempi di risposta. ZeroTier inizia a mostrare un incremento rapido nei tempi di risposta massimi già attorno ai 250 client, suggerendo un impatto crescente con l'aumento del traffico. Per quanto riguarda OpenVPN, si osserva un aumento dei tempi di risposta che, pur inizialmente lineare, diventa evidente in una curva quadratica quando si superano i 450 client, mostrando un degrado progressivo delle prestazioni con l'aumentare del numero di utenti. ZeroTier segue una curva quadratica fin dall'inizio, con i tempi di risposta più lenti che si distaccano rapidamente dai risultati ottimali. Mentre OpenVPN riesce a mantenere un buon livello di prestazioni con un numero moderato di client, ZeroTier risente

di un aumento del carico più significativo già con un numero relativamente basso di connessioni.

4.3.2 Tasso di fallimento

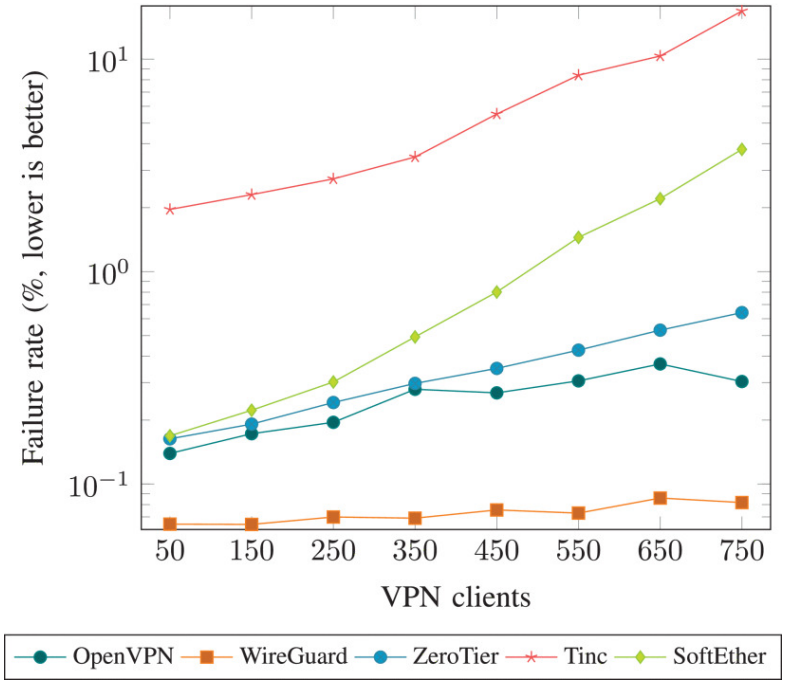

Figura 4.2: Evoluzione del tasso di errore per un numero crescente di client VPN.

Nel test relativo ai tassi di fallimento (figura 4.2) durante la scalabilità di OpenVPN e ZeroTier, i risultati mostrano un andamento simile ai tempi di risposta osservati in precedenza. Entrambi iniziano con tassi di errore relativamente bassi, paragonabili fino a circa 450 client. Tuttavia, come per i tempi di risposta, ZeroTier inizia a manifestare un deterioramento più rapido, con un aumento degli errori oltre tale soglia. OpenVPN, invece, mostra un andamento più lineare nei tassi di fallimento. Tuttavia, anche OpenVPN subisce un aumento degli errori, seppur in modo meno pronunciato rispetto a ZeroTier.

In conclusione, per quanto riguarda la scalabilità, emerge che entrambe le soluzioni sono valide e presentano prestazioni simili entro un certo numero di client; dopo una certa soglia mostrano comportamenti distinti. OpenVPN mantiene una crescita più lineare sia nei tempi di risposta che nei tassi di errore, offrendo maggiore stabilità nelle reti di dimensioni più elevate. ZeroTier, sebbene inizialmente alla pari con OpenVPN, subisce un degrado più rapido nelle prestazioni con una crescita sia di tempi di risposta che di tassi di errore quando i client aumentano significativamente. Nonostante comunque le ottime prestazioni, ciò lo rende meno adatto, rispetto ad OpenVPN, in scenari di utilizzo su larga scala.

4.4 Semplicità di implementazione

In questa sezione verranno analizzati la semplicità di installazione e la configurazione e gestione della rete per le due soluzioni VPN.

4.4.1 Semplicità di installazione

ZeroTier, come si è visto nei capitoli precedenti, si distingue per la sua procedura di installazione estremamente intuitiva, che richiede pochi e semplici passaggi per creare una VPN. Dopo la registrazione a un account sul sito ufficiale e l'installazione del client su ogni dispositivo, l'utente può facilmente configurare la rete tramite un'interfaccia web. Questa interfaccia consente di gestire le impostazioni avanzate, come l'assegnazione degli indirizzi IP e il controllo degli accessi, rendendo il processo di configurazione accessibile anche a utenti con competenze tecniche limitate. Inoltre, l'amministrazione della rete è trasparente: l'interfaccia utente permette di visualizzare i dispositivi autorizzati e quelli attualmente raggiungibili, semplificando la gestione della rete. Tuttavia, il controllo basato sui dispositivi richiede l'autorizzazione manuale di ciascun dispositivo, il che può risultare macchinoso in reti con un numero elevato di client, causando un'interfaccia meno reattiva.

OpenVPN, d'altra parte, presenta un'installazione più complessa. Dopo il download e l'installazione del pacchetto, è necessario configurare una PKI

(Public Key Infrastructure), un processo che include la creazione e gestione di certificati e chiavi di crittografia. La configurazione di un server OpenVPN richiede una conoscenza preliminare dei concetti di rete e crittografia, e prevede una serie di passaggi come la generazione dei parametri di Diffie-Hellman, la gestione dei file di configurazione e la configurazione di firewall e porte di rete. Questo processo, pur garantendo un elevato livello di sicurezza, è più impegnativo e meno immediato rispetto a ZeroTier.

4.4.2 Configurazione e gestione della rete

La configurazione di OpenVPN richiede la gestione di certificati e chiavi per ciascun client. Ogni dispositivo deve avere i propri certificati e chiavi, che devono essere generati e distribuiti manualmente dall'amministratore. Questa gestione manuale offre un controllo più granulare sulle connessioni, ma rende la soluzione meno immediata da configurare.

ZeroTier, invece, offre una maggiore semplicità grazie a una gestione centralizzata della rete tramite un'interfaccia web. La configurazione dei dispositivi avviene in modo automatico una volta installato il client, e l'amministratore deve solo autorizzare l'accesso alla rete. L'interfaccia utente fornisce informazioni utili su ogni dispositivo, come lo stato di connessione e l'indirizzo IP assegnato.

In sintesi, ZeroTier è una soluzione VPN ideale per chi cerca un'implementazione rapida e una gestione semplificata. OpenVPN, invece, offre un maggior controllo e una configurabilità più avanzata, ma richiede competenze tecniche superiori.

4.5 Prestazioni di rete

In questa sezione verranno analizzate le prestazioni di rete di OpenVPN e ZeroTier. Prima di entrare nei dettagli, è importante sottolineare che le prestazioni possono variare a seconda della posizione geografica, delle restrizioni della rete e di altri fattori, rendendo i risultati specifici alle condizioni di utilizzo.

4.5.1 Latenza

OpenVPN tende ad avere una latenza inferiore rispetto a ZeroTier, poiché utilizza un server centralizzato per gestire le connessioni. Questo riduce la necessità di routing aggiuntivo o nodi intermedi. ZeroTier, in alcuni casi, può avere latenza più alta, specialmente quando i client si connettono tramite un "relayer" esterno per gestire la comunicazione diretta tra i nodi, costruendo tunnel crittografici per proteggere il traffico.

4.5.2 Throughput

Per quanto riguarda il throughput, è stato preso in considerazione un articolo, pubblicato da ZeroTier stesso, in cui presenta un benchmark tra ZeroTier 1.2.4, OpenVPN 2.4.1 e Linux IPSec [15].

La configurazione di benchmark in questione è composta da due macchine virtuali Linux single-core (CentOS 7) su un processore Core i7 a 2,8 GHz. La virtualizzazione è stata gestita tramite VMWare Workstation, ed entrambe le macchine virtuali risiedevano sullo stesso host fisico. I test sono stati eseguiti usando iperf3, uno strumento che misura la velocità di trasferimento dei dati in modalità TCP, con 1 GB di dati casuali.

Questo test si concentra esclusivamente sulle limitazioni della CPU, non essendo coinvolta una rete fisica reale, e quindi il benchmark riflette il carico generato dalla gestione della VPN e dalle procedure di crittografia/compressione.

La tabella dei risultati mostra le velocità di trasferimento ottenute con diverse configurazioni:

Software	Crittografia / Configurazione	Velocità
Nessuna (VMWare bridge)	-	4760 Mbps
IPSec / Linux 3.10.0	AES-128-CBC / Nessuna	497 Mbps
ZeroTier 1.2.3	Salsa20 / LZ4 (predefinito)	484 Mbps
OpenVPN 2.4.1	AES-256-CBC / Nessuna	309 Mbps
OpenVPN 2.4.1	AES-256-CBC / LZO	290 Mbps
OpenVPN 2.4.1	Blowfish-CBC / Nessuna	234 Mbps
OpenVPN 2.4.1	Blowfish-CBC / LZO	221 Mbps

Tabella 4.1: Tabella di benchmark del throughput tra ZeroTier, OpenVPN e IPSec su Linux.

Come si può notare dalla tabella le prestazioni di OpenVPN sono notevolmente inferiori rispetto a ZeroTier, con velocità che variano tra 221 e 309 Mbps a seconda della crittografia/compressione utilizzata. Questo è in linea con quanto già discusso precedentemente nel confronto tra ZeroTier e OpenVPN: OpenVPN richiede più risorse di elaborazione per la gestione del traffico crittografato, e la sua velocità può risentirne. Risulta più lento a causa del maggiore overhead nella gestione delle connessioni e della crittografia più pesante (come AES-256-CBC).

Conclusioni

Dalla presente analisi e confronto tra OpenVPN e ZeroTier, è emerso che le due soluzioni offrono approcci diversi alla creazione e gestione di reti private virtuali (VPN), con vantaggi e svantaggi specifici a seconda dell'ambiente di applicazione.

OpenVPN rappresenta una soluzione più tradizionale e consolidata, ideale per contesti aziendali che richiedono un elevato livello di controllo e sicurezza. La sua architettura basata su un modello client-server consente di implementare configurazioni avanzate e personalizzabili, ma questo implica una maggiore complessità nelle fasi di configurazione e gestione. Il fatto che la sicurezza sia gestita direttamente dall'organizzazione, senza affidarsi a infrastrutture esterne, garantisce un controllo completo sui dati, rendendolo particolarmente adatto in ambienti dove la protezione delle informazioni è fondamentale. Tuttavia, la necessità di mantenere un server centrale può portare a costi aggiuntivi in termini di infrastruttura e manutenzione.

D'altra parte, ZeroTier si distingue per la sua semplicità d'uso e per la capacità di creare reti peer-to-peer. La sua architettura distribuita elimina la necessità di un server centrale per le comunicazioni tra dispositivi, rendendola una soluzione leggera e adatta a piccole reti o a contesti come l'Internet of Things. La configurazione è estremamente intuitiva e automatizzata, riducendo il margine di errore umano. Tuttavia, la dipendenza da server esterni (in cloud) può rappresentare un punto debole, soprattutto per le aziende che gestiscono informazioni sensibili e che necessitano di un controllo diretto e costante sulla propria infrastruttura.

Dal punto di vista prestazionale, OpenVPN tende a garantire latenze più basse, grazie alla sua architettura client-server, mentre ZeroTier potrebbe risultare più lento in determinati scenari a causa della necessità di passare attraverso un punto di intermediazione per la crittografia. In termini di throughput, ZeroTier sembra offrire velocità superiori rispetto a OpenVPN.

Oltre alle prestazioni e alla facilità di configurazione, un altro fattore critico da considerare è la scalabilità, soprattutto quando queste soluzioni vengono applicate in ambienti con un numero elevato di client o dispositivi, come nel caso di reti aziendali di grandi dimensioni o infrastrutture IoT. Dai test esaminati si evince che OpenVPN e ZeroTier si comportano in modo simile, con tempi di risposta ragionevoli e prestazioni accettabili. Tuttavia, quando il numero di client supera un certo limite, emergono differenze: ZeroTier mostra un incremento nei tempi di risposta, ciò suggerisce che la sua architettura può iniziare a incontrare difficoltà nella gestione di volumi elevati di traffico. Questo effetto si accentua man mano che aumentano le connessioni, con un impatto particolarmente evidente sui tempi di risposta massimi, che seguono una curva quadratica fin dalle prime fasi del test. Mentre, OpenVPN riesce a mantenere prestazioni più stabili con un numero moderato di client, mostrando un degrado delle prestazioni meno pronunciato con l'aumentare delle connessioni. Nonostante ciò, è da ricordare che, in presenza di carichi estremamente elevati, anche OpenVPN non risulta immune a un calo delle prestazioni. Questo rende più adatto il sistema di OpenVPN in contesti in cui si richiede una maggiore robustezza e capacità di scalare in modo più efficiente.

In conclusione, la scelta tra OpenVPN e ZeroTier dipende strettamente dalle esigenze specifiche dell'ambiente in cui vengono implementate. OpenVPN risulta essere la scelta ideale per organizzazioni che necessitano di configurazioni flessibili e di un maggiore controllo sulla sicurezza, mentre ZeroTier offre una soluzione pratica e veloce per reti distribuite e comunicazioni peer-to-peer. La decisione finale dovrebbe tenere conto delle dimensioni della rete, delle risorse disponibili e della criticità dei dati trattati.

Bibliografia

[1] Gen. 2016. URL: https://it.wikipedia.org/wiki/Pre-Shared_Key.

[2] Lug. 2022. URL: https://it.wikipedia.org/wiki/Infrastruttura_a_chiave_pubblica.

[3] Feb. 2024. URL: https://it.wikipedia.org/wiki/User_Datagram_Protocol.

[4] Lug. 2024. URL: https://it.wikipedia.org/wiki/OpenSSL.

[5] Set. 2024. URL: https://onlinelibrary.wiley.com/doi/full/10.1002/spe.3329.

[6] Set. 2024. URL: https://en.wikipedia.org/wiki/Mesh_networking.

[7] S. J. Bigelow e B. Lutkevich. "What is IT/OT convergence? Everything you need to know". In: *IT Operations* (apr. 2024). URL: https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence.

[8] CSRC Content Editor. *Tunneling - glossary: CSRC*. URL: https://csrc.nist.gov/glossary/term/tunneling.

[9] Markus Feilner et al. *Open VPN: Building and integrating virtual private networks: Learn how to build secure VPNs using this powerful open source application*. Birmingham, UK, 2006.

[10] A. F. Gentile et al. *A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment*. Set. 2022. URL: https://www.mdpi.com/1999-5903/14/9/264.

[11] *Getting Started with ZeroTier*. URL: https://docs.zerotier.com/.

[12] T. Goethals et al. *Scalability evaluation of VPN technologies for secure container networking*. Retrieved October 25, 2019. 2020. URL: https://ieeexplore.ieee.org/abstract/document/9012673/authors#authors.

[13] Geoff Huston e Paul Ferguson. *What is a VPN?* Apr. 1998.

[14] Adam Ierymenko. *The state of NAT Traversal.* Accessed: 2024-04-23. Apr. 2024. URL: https://www.zerotier.com/blog/the-state-of-nat-traversal/.

[15] G. Limberg. *Benchmarking ZeroTier vs. OpenVPN and Linux IPSec.* Apr. 2024. URL: https://www.zerotier.com/blog/benchmarking-zerotier-vs-openvpn-and-linux-ipsec/.

[16] Mindtree. *Converging IT & OT Systems: Accelerating Digital Transformation For Manufacturers.* n.d. URL: https://www.mindtree.com/insights/blog/converging-it-ot-systems-accelerating-digital-transformation-manufacturers.

[17] Rok Vidmar e Andrej Kos. *Vrednotenje rešitve za navidezno zasebno omrežje ZeroTier v primerjavi s konkurenčnimi rešitvami: Magistrsko delo: Magistrski študijski program druge stopnje Elektrotehnika.* Master's thesis. Ljubljana, Slovenia, 2022.

[18] James Yonan. *Reference manual for openvpn 2.4.* Dic. 2023. URL: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/.