



UNIVERSITÀ DEGLI STUDI ROMA TRE

Dipartimento di Ingegneria
Corso di Laurea in Ingegneria Informatica

Tesi Di Laurea

Realizzazione di un sistema di
cyber-defense: utilizzo delle VPN per un
accesso remoto sicuro a risorse interne

Laureando

Filippo Visconti

Matricola 547344

Relatore

Prof. Maurizio Patrignani

Correlatore

Federico Lommi

Anno Accademico 2021/2022

Questa è la dedica

Ringraziamenti

Questi sono i ringraziamenti.

Introduzione

In questa tesi, si andranno a studiare i funzionamenti delle reti private virtuali, delle necessità che portano alla loro installazione e si andrà a misurare le performance ottenute con diverse soluzioni software. Prima di cominciare, è necessario fare un breve excursus definendo termini e concetti di base, fondamentali per comprendere i capitoli seguenti.

Concetti di base

Server

Un server è una macchina, un computer in grado di erogare servizi di ogni genere agli utenti (detti *client*). Tendenzialmente, hanno potenze di calcolo superiori di vari ordini di grandezza rispetto ai dispositivi comunemente utilizzati, e fanno della ridondanza e dell'affidabilità pilastri fondamentali.

Tipologie di reti

Parlando di una rete di calcolatori, si intende una rete a cui sono connessi due o più computer tramite cui è possibile condividere dati, dispositivi, connessione a internet, e via dicendo.

Esistono varie tipologie di reti di calcolatori, distinte in base al loro target, che consiste nell'estensione della rete. In base a questo parametro, è possibile distinguere le reti in Local Area Network, Metropolitan Area Network e Wide Area Network. Tutte e tre le tipologie sono relative a una rete fisica.

Un altro tipo di reti è composto dalle reti private virtuali, o Virtual Private Networks, che consiste in una rete di calcolatori le cui connessioni tra i nodi utilizzano reti

pubbliche (WAN) come fondamenta su cui realizzare una rete virtuale. Questo tipo di reti permette di realizzare collegamenti privati tra location geograficamente anche molto distanti senza la necessità di posare cavi fisici, ma avvalendosi dell'infrastruttura esistente, garantendo comunque integrità e cifratura dei dati, controllo degli accessi e confidenzialità.

Il modello OSI

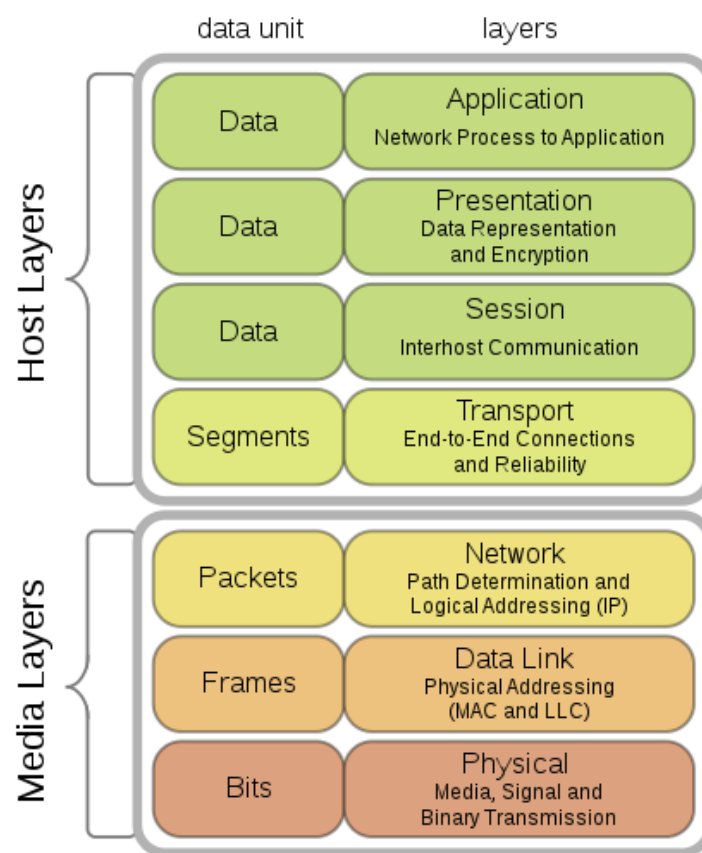


Figura 1: Modello OSI a strati

La pila ISO OSI è uno strumento estremamente efficace nel modellare il funzionamento di una rete di calcolatori. Si basa su 7 livelli, ognuno dei quali svolge il proprio lavoro utilizzando un'interfaccia standard offerta dal livello inferiore e offrendo a sua vol-

ta un'interfaccia al livello superiore. Tutti e 7 i livelli collaborano per rendere possibile il funzionamento della rete.

I compiti dei sette livelli sono, in breve, i seguenti:

1. Livello fisico: è composto dall'infrastruttura fisica - cavi in rame, fibra ottica, ponti radio - e dai componenti hardware che codificano e decodificano i bit
2. Livello data-link: si occupa di effettuare controlli sul livello fisico, specialmente sull'integrità dei dati
3. Livello di rete: è il regno del protocollo IP, pilastro delle reti di calcolatori, che si occupa dello smistamento dei pacchetti e di portarli a destinazione; di particolare interesse sono gli indirizzi IP, che identificano in modo univoco un dispositivo collegato in rete
4. Livello di trasporto: astrae il funzionamento del protocollo IP, offrendo alle applicazioni vari protocolli che si occupano della comunicazione tra due host, indipendentemente da come sono collegati o da quanto sono distanti; può garantire il recapito corretto delle informazioni
5. Livello di sessione, livello di presentazione, livello di applicazione: sono gli strati più prossimi all'utente finale, e si occupano di gestire la comunicazione dei processi utilizzati dall'utente con il livello di trasporto

Pericoli di esporre un server su Internet

Rendere accessibile un server dalla rete Internet, affinché sia possibile sfruttare i servizi che offre dovunque nel mondo ci si trovi, porta con sé una serie di rischi e problematiche concrete e decisamente rilevanti. Infatti, i servizi pubblicati saranno esposti sia a utenti corretti che a malintenzionati, che potrebbero andare alla ricerca di vulnerabilità informatiche (ma non solo) col fine di ottenere accesso alle macchine e disporne a loro piacimento.

Necessità di un'infrastruttura di rete sicura

L'architettura di sicurezza del Modello OSI considera 5 classi principali di servizi di sicurezza. Tra queste si hanno: autenticazione, controllo degli accessi, confidenzialità, integrità e non ripudio. In particolare, questi servizi sono definiti come segue:

- autenticazione - il servizio di autenticazione verifica l'identità di un utente o di un sistema
- controllo degli accessi - il servizio protegge le risorse di sistema da utenti non autorizzati
- confidenzialità - il servizio protegge i dati da rivelazioni non autorizzate
- integrità - il servizio protegge i dati da modifiche, aggiunte o rimozioni non autorizzate
- non ripudio *a.k.a non-repudiation* - il servizio assicura che il mittente dell'informazione abbia una notifica di consegna e il destinatario riceva una prova di identità del mittente, in modo tale che nessuno dei due possa successivamente negare di aver processato tali dati

Organizzazione dei capitoli

I capitoli che seguono sono sviluppati come segue.

Nel capitolo 1, vengono discussi i requisiti del sistema che andranno rispettati nello svolgimento della tesi.

Nel capitolo 2, si discute lo stato dell'arte, illustrando dal punto di vista teorico i protocolli e i software che si andranno a utilizzare.

Nel capitolo 3, viene illustrata la realizzazione dell'ambiente di test, compresa l'installazione e la configurazione dei servizi scelti.

Nel capitolo 4, si analizzano le misure ottenute durante i test.

Nel capitolo 5, si presentano i principali problemi di sicurezza a cui si potrebbe andare incontro.

Indice

Introduzione	iv
Concetti di base	iv
Pericoli di esporre un server su Internet	vi
Necessità di un'infrastruttura di rete sicura	vii
Organizzazione dei capitoli	vii
Indice	viii
Elenco delle figure	xii
1 Requisiti	1
1.1 Caratteristiche della rete aziendale	1
1.1.1 Diagramma di rete	1
1.1.2 Descrizione dei componenti fondamentali	2
1.1.3 Servizi offerti all'esterno	3
1.1.4 Servizi offerti all'interno	4
1.2 Necessità degli utenti	6
1.2.1 Accesso ai servizi interni senza esposizione all'esterno	6
1.3 Requisiti di sicurezza	6
1.3.1 Controllo del traffico	6
1.3.2 Trasmissione sicura dei dati	7
1.3.3 Controllo dei dispositivi	7
1.3.4 Compatibilità	7

2	Stato dell'arte	8
2.1	Virtual Private Networks	8
2.1.1	Architetture disponibili	8
2.1.2	Perché soddisfano i requisiti	9
2.1.3	Soluzioni principali	9
2.2	Internet Protocol Security	10
2.2.1	Panoramica	10
2.2.2	Transport mode vs Tunnel mode	10
2.2.3	Protocolli utilizzati	11
2.2.4	Cifratura	13
2.2.5	Autenticazione	14
2.2.6	Implementazioni	14
2.2.7	Considerazioni	14
2.3	PPTP	14
2.3.1	Panoramica	14
2.3.2	Protocolli utilizzati	15
2.3.3	Cifratura	15
2.3.4	Autenticazione	15
2.3.5	Considerazioni	16
2.4	OpenVPN	16
2.4.1	Panoramica	16
2.4.2	Protocolli utilizzati	16
2.4.3	Tunnel TCP vs UDP	18
2.4.4	Cifratura	18
2.4.5	Autenticazione	19
2.4.6	Misure di sicurezza aggiuntive	19
2.4.7	Considerazioni	19
2.5	WireGuard	20
2.5.1	Panoramica	20
2.5.2	Protocolli utilizzati	20
2.5.3	Cifratura	21

2.5.4	Autenticazione	21
2.5.5	Considerazioni	21
3	Realizzazione	22
3.1	Virtualizzatore	22
3.1.1	Caratteristiche e funzionamento	22
3.1.2	VirtualBox	23
3.1.3	VMWare ESXi	23
3.1.4	Installazione e configurazione dei servizi VPN	23
3.2	Installazione e configurazione di IPSec - tunnel mode	24
3.2.1	Aggiunta dell'interfaccia di rete virtuale	24
3.2.2	Installazione di strongSwan	24
3.2.3	Configurazione di strongSwan	25
3.2.4	Creazione del certificato per un client	25
3.3	Installazione e configurazione di OpenVPN over TCP	26
3.3.1	Installazione di OpenVPN	26
3.3.2	Certificati	27
3.3.3	Configurazione del profilo VPN per un client	27
3.4	Installazione e configurazione WireGuard	27
3.4.1	Configurazione del profilo VPN per un client	27
3.5	Configurazione del Firewall	28
4	Testing	29
4.1	Modalità di esecuzione dei test	29
4.1.1	Panoramica di iPerf3	29
4.1.2	Panoramica di mtr	29
4.1.3	Criteri di valutazione	31
4.1.4	Scelta della configurazione di test	33
4.2	Misure senza VPN	33
4.3	Misure con IPSec e IKEv2	34
4.4	Misure con OpenVPN over TCP	35
4.5	Misure con WireGuard	35

4.6	Analisi delle misure	36
5	Security concerns	38
5.1	Principali problematiche di sicurezza	38
5.2	Attacchi mirati agli utenti	38
5.2.1	Furto di credenziali	39
5.2.2	Social Engineering	40
5.3	Attacchi mirati al sistema	41
5.3.1	Versione non aggiornata	42
5.3.2	Exploit di vulnerabilità zero-day	42
5.4	Multi-factor authentication	42
5.4.1	Certificato	43
5.4.2	Username e password	44
5.4.3	One Time Password	44
	Conclusioni e sviluppi futuri	45
	Quale è uscito vincitore	45
	Come migliorare le misure	45
	Test di VPN Peer-To-Peer	46
	Zero Tier	46
	PAM vs VPN	47
	Bibliografia	48

Elenco delle figure

1	Modello OSI a strati	v
1.1	Diagramma di rete	1
2.1	Modello logico di connessione con e senza VPN	9
2.2	Transport mode vs Tunnel mode diagram	10
2.3	Authentication Header packet formats	11
2.4	Encapsulating Security Payload packet formats	12
2.5	Dettaglio di un pacchetto OpenVPN	17
3.1	Installazione fisica vs Installazione virtuale	23
3.2	Dettagli interfaccia virtuale strongswan0	24
3.3	Architettura di installazione di WireGuard	28
4.1	Esempio di output di iPerf3	30
4.2	Esempio di output di mtr	30
4.3	Throughput senza VPN su 300 secondi	33
4.4	mtr senza VPN	34
4.5	IPSec Throughput su 300 secondi	34
4.6	mtr su IPSec	34
4.7	OpenVPN Throughput su 300 secondi	35
4.8	mtr su OpenVPN	35
4.9	WireGuard Throughput su 300 secondi	35
4.10	mtr su WireGuard	36
4.11	Confronto dei throughput grezzi	36

4.12	Confronto dei throughput raffinati	37
4.13	Confronto di latenza media e di packetloss	37
5.1	MFA	43

Capitolo 1

Requisiti

1.1 Caratteristiche della rete aziendale

La rete su cui siamo stati chiamati a lavorare è illustrata nel diagramma seguente.

1.1.1 Diagramma di rete

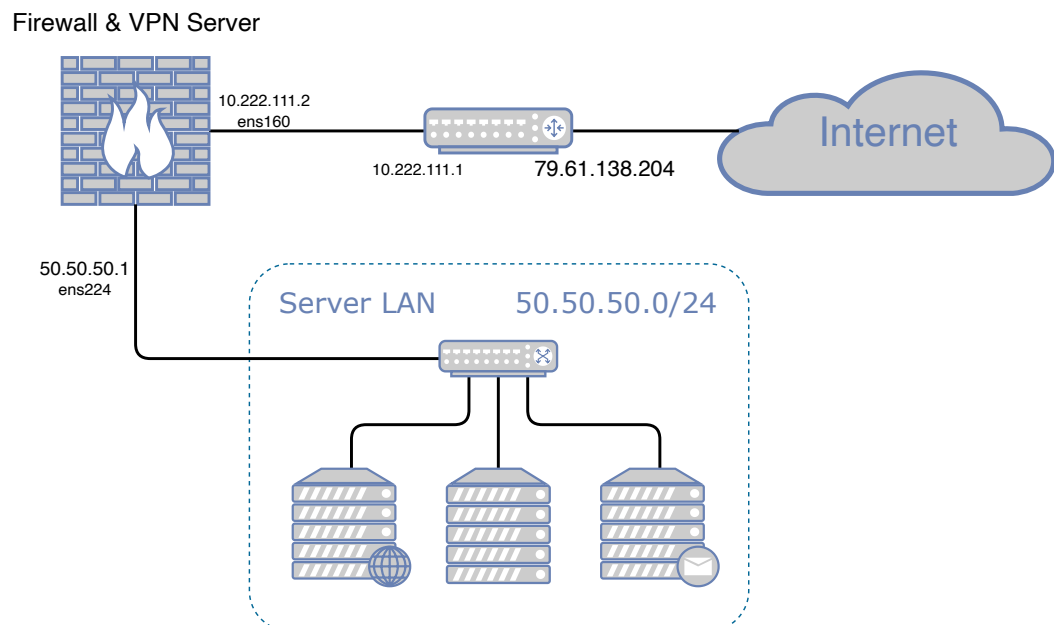


Figura 1.1: Diagramma di rete

La porzione di diagramma che rappresenta l'infrastruttura di rete dell'azienda è quella sinistra della nuvola. La porzione destra raffigura, invece, un'altra sottorete, che per fini di testing immaginiamo sia la rete casalinga di un dipendente dell'azienda. La nuvola sta a rappresentare tutta la rete Internet.

1.1.2 Descrizione dei componenti fondamentali

1.1.2.1 Router

Un componente essenziale all'interno dell'infrastruttura di rete è il router. Il router è un dispositivo di rete che lavora al livello 3 del modello OSI e che permette e gestisce l'instradamento dei pacchetti tra sottoreti diverse. Le tabelle d'instradamento, salvate nella memoria interna del router, contengono informazioni che riguardano come raggiungere gli altri nodi della rete e sono lo strumento che permette al router di instradare correttamente i pacchetti. Queste tabelle associano il prefisso IP [Pos81, RFC0791] e relativa maschera della sottorete di destinazione con il *next-hop*, l'indirizzo IP del prossimo router a cui deve essere destinato al pacchetto affinché si avvicini alla sua vera destinazione, e l'interfaccia di rete del router da cui il pacchetto deve essere inoltrato affinché possa raggiungere il *next-hop*. Generalmente la funzione di routing è svolta da un componente hardware dedicato, che, se di fascia alta, permette di raggiungere prestazioni pari alla velocità della linea - ossia, spedisce i pacchetti alla stessa velocità alla quale li riceve. Tuttavia, è possibile il compito venga svolto da server generici, a patto che siano dotati di un numero adatto di schede di rete, su cui gira un software apposito.

1.1.2.2 Firewall

In entrambi i casi, è comune che il router abbia un firewall [Fre00] integrato. Un firewall è un dispositivo fisico, o un software, che ha come obiettivo la regolazione del traffico di una rete. Ciò avviene applicando una serie di regole che coinvolgono lo stato, la porta e il protocollo dei pacchetti che lo attraversano. L'amministratore di rete ha la responsabilità di inserire regole appropriate al contesto, affinché, tutto ciò che non è strettamente necessario, non venga fatto passare. Un esempio di Firewall software molto conosciuto in ambienti UNIX, è `iptables`. Il seguente comando mostra una

regola che *consente* il passaggio di un pacchetto in entrata sul firewall dalla scheda di rete `eth0`, destinato alla porta 22 TCP, e che sia il primo di una comunicazione, o faccia parte di una comunicazione già instaurata.

```
iptables -A INPUT -p tcp --dport 22 -i eth0 \  
-m state --state NEW,ESTABLISHED -j ACCEPT
```

Il sistema a disposizione avrà un router/firewall installato su un server, che ha come sistema operativo CentOS 7 [Cen] - la versione gratuita di Red Hat Enterprise Linux [Lin].

1.1.2.3 Le LAN utilizzate

Nella configurazione della rete aziendale corrente è presente soltanto una sottorete, denominata LAN dei server, dove risiedono esclusivamente i server che erogano servizi all'esterno dell'azienda. Tutti i servizi per uso interno, destinati a una ulteriore LAN, in questo esempio sono erogati dal router/firewall stesso.

1.1.3 Servizi offerti all'esterno

L'azienda ha necessità di pubblicare

- un sito web, il cui hosting è effettuato sul web server interno;
- un mail server, che si occupa di inviare e ricevere i messaggi di posta elettronica

1.1.3.1 Web servers

Il sito web è servito in HTTP sulla porta 80 e in HTTPS sulla porta 443, e la pubblicazione è affidata a un noto servizio, *Apache httpd* [Apa].

1.1.3.2 Mail servers

L'azienda ha un mail server che si occupa di inviare, ricevere e archiviare i messaggi di posta dei dipendenti dell'azienda.

1.1.4 Servizi offerti all'interno

1.1.4.1 DHCP server

Il Dynamic Host Configuration Protocol [Dro97, RFC2131] è un protocollo ausiliario che permette l'assegnazione automatica degli indirizzi IP e altri parametri di configurazione ai dispositivi connessi alla rete usando una architettura client-server. Il DHCP offre un servizio non connesso e utilizza UDP come protocollo di trasporto. Il server ascolta le richieste (che saranno broadcast, destinate per convenzione all'IP 255.255.255.255) sulla porta 67 UDP, e inoltra le risposte al client sulla porta 68 UDP. Altri parametri di configurazione che comunemente accompagnano l'appena assegnato indirizzo IP sono i server DNS [Moc87, RFC1034] di default, l'indirizzo IP del default gateway, e la durata per il quale l'IP assegnato è valido.

1.1.4.2 DNS server

Il Domain Name System è il sistema di assegnazione gerarchico e decentralizzato dei nomi che identificano gli host in rete. Un'analogia che aiuta a comprendere la funzione del DNS è quella della rubrica telefonica. Infatti, come nella rubrica telefonica viene mantenuta un'associazione tra un nome - facile da ricordare per una persona - e il relativo numero di telefono - più difficile da ricordare, e facile da confondere -, così il DNS conserva dei *resource records* composti da un nome - **example.com** - associato a un indirizzo IPv4 o IPv6 - **93.130.23.53**. Si tratta di un protocollo di livello 7, che generalmente comunica sulla porta 53 UDP, ma potrebbe sfruttare anche VPN o tunnel, TLS, HTTPS, Tor. È una potenzialità interessante, in quanto le richieste non sono crittate e si potrebbe andare incontro a problemi di sicurezza. Il DNS è in grado di memorizzare anche altre informazioni riguardanti un certo dominio, tra cui:

- i *name servers* che sono autorità per quel dominio - coloro che a loro volta memorizzano i resource records dei vari sottodomini;
- gli indirizzi IP dei mail exchanger di riferimento per quel dominio;
- degli alias, ossia un'associazione tra due nomi di dominio.

Nella configurazione corrente, il server DNS, che gira sullo stesso server su cui è in esecuzione il Firewall, lavora come relay e il suo IP viene distribuito a tutti i client della rete interna via DHCP come DNS resolver. Ciò significa che tutti gli host della rete, nel momento in cui devono risolvere un nome, inviano una richiesta al server DNS interno, che si occuperà lui di risolverlo e, una volta ottenuto il risultato, lo restituisce al richiedente. Questo comporta diversi vantaggi, tra cui:

- la comunicazione verso l'esterno per la risoluzione dei nomi avviene da un unico punto della rete;
- si può fare caching, ossia mantenere in memoria per un certo periodo di tempo (che viene specificato nella risposta ricevuta dal server DNS) le risposte delle varie risoluzioni, cosicché, se di una richiesta si era già trovata la risposta, non dovrà essere fatta di nuovo la risoluzione;
- si possono implementare dei filtri per bloccare la risoluzione di nomi a cui si vuole limitare l'accesso;
- si possono facilmente tracciare le varie richieste.

1.1.4.3 Web app interne

All'interno della rete locale dell'azienda, sono accessibili degli applicativi che permettono la gestione di alcuni sistemi, ad esempio degli apparati di rete.

1.1.4.4 File servers

Affinché i dipendenti autorizzati possano collaborare e accedere a file condivisi, è stato predisposto un file server, a cui si può accedere con protocolli quali FTP [PR85, RFC0791] e SFTP. Tuttavia, i file in questione possono contenere dati sensibili. Per questo motivo, è necessario che la risorsa sia adeguatamente protetta, non esposta alla rete esterna e che l'accesso sia regolamentato.

1.1.4.5 Database servers

Similmente al file server, c'è anche un database server a disposizione dei dipendenti, le cui necessità di sicurezza rispecchiano quelle del file server.

1.2 Necessità degli utenti

1.2.1 Accesso ai servizi interni senza esposizione all'esterno

Per quel che riguarda i dipendenti dell'azienda, hanno necessità di poter lavorare in modo autonomo da casa. Dunque devono poter accedere in maniera sicura a tutte le risorse disponibili all'interno della rete privata da qualsiasi parte del mondo.

1.2.1.1 Remote work

Lavorare da remoto è un qualcosa che sta prendendo sempre più piede nel mondo di oggi. Specialmente con la pandemia da Covid-19, si è visto come sia fondamentale offrire strumenti adeguati ai dipendenti per svolgere le proprie mansioni indipendentemente dalla loro posizione. Tutto ciò, tuttavia, non deve avvenire a discapito della sicurezza.

1.3 Requisiti di sicurezza

Tra i requisiti principali di sicurezza, si ha: la possibilità di controllare il traffico, di avere una trasmissione sicura dei dati, di effettuare un controllo dei dispositivi aziendali.

1.3.1 Controllo del traffico

1.3.1.1 Proxy interno obbligatorio

Un valido strumento per effettuare controllo del traffico e tenerne traccia tramite log è rappresentato dai proxy. Un proxy è un server che si pone come intermediario tra la LAN interna e la rete esterna, generalmente per le comunicazioni che avvengono sulle porte TCP 21, 80 e 443, ossia quelle che utilizzano i protocolli FTP, HTTP e HTTPS. Utilizzando un server proxy, i client, anziché comunicare direttamente con l'host di destinazione, inviano la richiesta al proxy, che si occupa di comunicare con

l'host di destinazione e di restituire la risposta ottenuta all'iniziatore della richiesta. Con questo tipo di intermediazione, è triviale registrare tutta l'attività che avviene e filtrare richieste ritenute non opportune. Il filtraggio in questione è noto come URL filtering. Il funzionamento si basa su delle blacklist (o whitelist, nel caso inverso), contenenti URL a cui si vuole impedire ai client di accedere. Quando arriva una richiesta al server proxy, questa passerà e verrà inoltrata solo nel caso l'URL della richiesta non sia contenuto nella blacklist.

1.3.2 Trasmissione sicura dei dati

Come è possibile immaginare, per un'azienda è fondamentale poter contare su di un'infrastruttura che garantisca che i dati che transitano su di essa non vengano compromessi.

1.3.2.1 Evitare intercettazioni

Vedi Cina con il Great Firewall

Senza la garanzia di una trasmissione sicura dei dati, dove "sicura" si riferisce a tutte le diverse sfaccettature dell'ambito, si è esposti a "eavesdropping attacks". Questi attacchi consistono nell'ascoltare, senza farsi notare, le comunicazioni altrui, tramite strumenti di *sniffing* posti a vari livelli. Un'analogia esplicativa è quella delle *cimici* posizionate all'interno dell'abitazione di un indagato, per registrare le sue comunicazioni.

1.3.3 Controllo dei dispositivi

L'azienda ha bisogno di poter controllare e gestire i dispositivi concessi in uso ai suoi dipendenti, affinché il software installato sia sempre e solo quello autorizzato, e le loro configurazioni siano quelle più adatte agli elevati standard di sicurezza richiesti.

1.3.4 Compatibilità

Il sistema da realizzare deve garantire compatibilità con le ultime versioni dei tre sistemi operativi per desktop principali - macOS, Windows e le distribuzioni principali Linux - e dei due sistemi operativi principali per mobile - iOS e Android.

Capitolo 2

Stato dell'arte

2.1 Virtual Private Networks

Una rete privata virtuale consiste in una rete il cui accesso è regolamentato, che si appoggia a un protocollo di trasporto pubblico e condiviso, e che consente di garantire confidenzialità della comunicazione, accesso solo previa autenticazione, integrità dei dati e protezione da alcuni tipi di attacchi, ad esempio Man-in-the-middle o attacco replay.

2.1.1 Architetture disponibili

Una rete VPN può realizzare diversi tipi di collegamenti, per soddisfare esigenze diverse. Nei paragrafi successivi, si andranno ad analizzare i 3 tipi di architetture più comuni:

- Gateway-to-Gateway
- Host-to-Host
- Host-to-Gateway

2.1.1.1 Gateway-to-Gateway

Consiste in una VPN che connette in maniera stabile due reti. Questa configurazione permette ad esempio di estendere una rete privata tra diverse location geograficamente separati e distanti a piacere, oppure di garantire a una serie di uffici un accesso sicuro a un data center.

2.1.1.2 Host-to-Host

Questa configurazione è la meno comune. Consiste nello stabilire una comunicazione diretta tra due host, in cui uno fa da server VPN e l'altro da client VPN. Un caso d'uso potrebbe essere un amministratore di sistema che deve fare gestione remota di un apparecchio.

2.1.1.3 Host-to-Gateway

In questa modalità, il risultato che si ottiene è lo stesso che si avrebbe connettendo un host alla rete locale in cui risiede il server VPN. È usata principalmente per offrire un accesso sicuro da remoto alla rete. Quando l'host vuole instaurare una connessione VPN con il server, gli viene richiesto di autenticarsi.

2.1.2 Perché soddisfano i requisiti

Una VPN in configurazione Host-to-Gateway si prospetta come la soluzione più pratica e funzionale per soddisfare le necessità dell'azienda e dei suoi dipendenti, garantendo loro la possibilità di accedere alle risorse interne attraverso un canale di comunicazione privato, ad accesso controllato, criptato e dove è assicurata l'integrità dei dati.

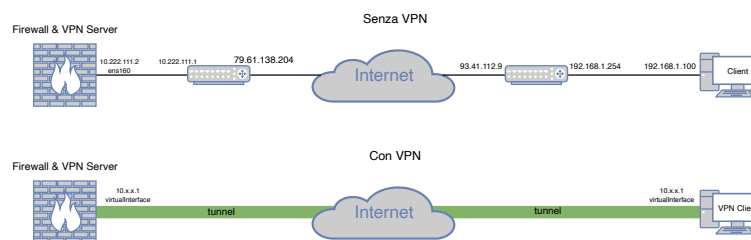


Figura 2.1: Modello logico di connessione con e senza VPN

2.1.3 Soluzioni principali

Tra le soluzioni VPN più comuni troviamo:

- Point-to-Point Tunneling Protocol
- Internet Protocol Security

- OpenVPN
- Wireguard

2.2 Internet Protocol Security

2.2.1 Panoramica

IP Security è una suite di protocolli il cui obiettivo è rendere sicura la comunicazione tra due computer attraverso una rete IP. Contiene protocolli per la mutua autenticazione degli host e per la negoziazione delle chiavi di cifratura da usare durante la sessione. In molti contesti, rendere sicuro il livello di rete (L3 OSI) è una soluzione migliore rispetto a rendere sicuro il livello di trasporto (L4 OSI) o di presentazione (L7 OSI), in quanto offre un ulteriore punto di controllo per gli amministratori e più flessibilità nell'analizzare, e gestire, ogni singolo pacchetto IP. IPsec supporta l'autenticazione a livello di rete, autenticazione del mittente, integrità dei dati, cifratura, e protezione dagli attacchi replay, protezione dall'analisi del traffico e controllo degli accessi.

2.2.2 Transport mode vs Tunnel mode

The IPsec protocols AH and ESP can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

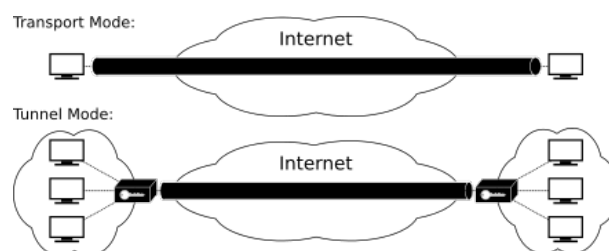


Figura 2.2: Transport mode vs Tunnel mode diagram

2.2.2.1 Transport mode

In transport mode, generalmente solo il payload del pacchetto IP è cifrato o autenticato. L'indirizzamento non cambia, dato che l'header IP non è né modificato né cifrato;

tuttavia, quanto si usa il protocollo Authentication Header - approfondito in seguito - l'indirizzo IP non può essere modificato da Network Address Translation, in quanto una modifica al campo invaliderebbe l'hash. Il livello di trasporto e di applicazione sono sempre certificati da un hash, quindi il loro contenuto non può essere modificato in alcun modo, ad esempio utilizzando una traduzione dei numeri delle porte. Un superamento delle problematiche causate dall'attraversamento di NAT è definito dalle RFC che descrivono il meccanismo NAT-T, ma che va oltre gli scopi di questa tesi.

2.2.2.2 Tunnel mode

In tunnel mode, l'intero pacchetto è cifrato e autenticato. È dunque incapsulato all'interno di un nuovo pacchetto IP con un nuovo header IP. Generando un nuovo header IP, non si incontra nessuna difficoltà nell'attraversamento di NAT.

2.2.3 Protocolli utilizzati

IPSec utilizza i seguenti protocolli per stabilire una connessione sicura. Sia AH che ESP, descritti in seguito, possono lavorare in tunnel mode o in transport mode.

2.2.3.1 Authentication Header

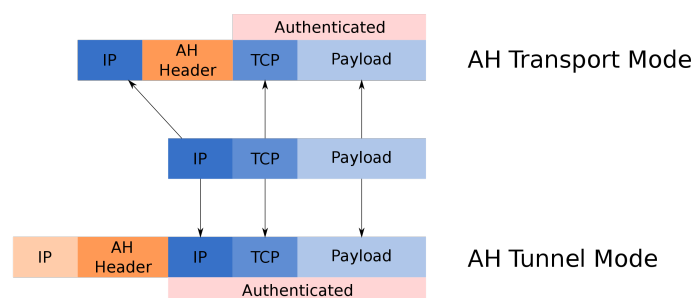


Figura 2.3: Authentication Header packet formats

Authentication Header [Ken05a, RFC4302] garantisce integrità per tutti gli header dei pacchetti, ad eccezione di alcuni campi dell'header IP, e autenticazione del mittente. Se configurato, è anche possibile utilizzarlo per offrire protezione dagli attacchi replay.

AH si interfaccia direttamente con IP, utilizzamndo il protocollo IP numero 51. AH autentica l'intero datagramma, ad eccezione dei campi variabili. Tuttavia, le informazioni contenute nel datagramma sono trasferite in chiaro e, dunque, leggibili da uno sniffer. Per questo motivo, AH non soddisfa i requisiti di sicurezza richiesti.

2.2.3.2 Encapsulating Security Payload

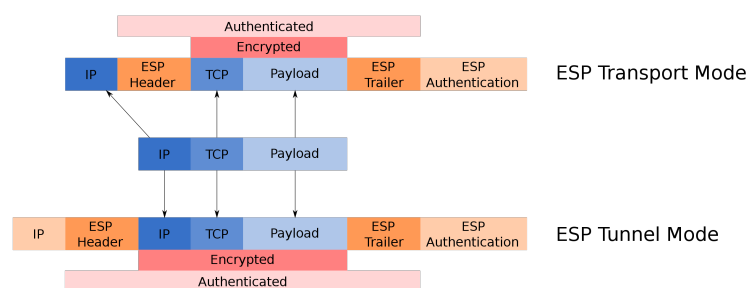


Figura 2.4: Encapsulating Security Payload packet formats

Encapsulating Security Payload [Ken05b, RFC4303] offre confidenzialità dei dati, autenticazione del mittente, controllo di integrità e protezione da attacchi relay. In Transport mode, non autentica né cifra l'header IP: cioè potrebbe esporre le informazioni contenute a potenziali attacchi mentre il pacchetto è in transito. Tuttavia, la Transport mode necessita di meno potenza computazionale, ottenendo un overhead minore della tunnel mode, rinunciando a una maggior sicurezza.

In Tunnel mode, viene creato un nuovo header IP e usato come header esterno del pacchetto, eguito dall'header ESP e poi il pacchetto originale (sia header IP che payload originale). L'ESP Trailer e gli opzionali dati di autenticazione sono aggiunti dopo il payload. Quando si usano cifratura e autenticazione contemporaneamente, ESP protegge completamente il pacchetto originale, perché diventa il payload del nuovo pacchetto ESP. Da notare è che non viene protetto il nuovo header IP. Un gateway deve necessariamente usare ESP in Tunnel mode.

2.2.3.3 Internet Key Exchange v2

Ancora del testo—IKE è un acronimo per Internet key exchange ed è il protocollo usato per stabilire una security association nella suite di protocolli IPsec. Questo protocollo è definito in RFC 4306. —

Internet Key Exchange [Kau05, RFC4306] è un protocollo che svolge la funzione di negoziazione, gestione e creazione delle Security Associations. Una SA è un insieme di regole necessarie a definire le funzionalità e i sistemi di sicurezza per stabilire una connessione IPSec. Può essere definita manualmente, anche se non scala dovutamente con VPN di grandi dimensioni. Un metodo più comune è quello di usare una delle cinque possibili modalità di scambio: main, aggressive, quick, informational e group. Le modalità sono differenti per velocità e l'uso di funzioni di cifratura. IKEv2 è la versione più recente di IKE e migliora il protocollo rendendolo più semplice, garantendo affidabilità nel recapito dei messaggi, protezione contro attacchi di tipo DenialOfService e migliora l'uso di IKE su gateways NAT. È un protocollo di livello applicazione e utilizza il protocollo UDP come protocollo di trasporto; la porta su cui viene stabilita la connessione è 500.

2.2.4 Cifratura

IPSec supporta diversi protocolli di cifratura, tra cui AES, Blowfish, Triple DES, ChaCha e DES-CBC. Inoltre, usa due tipi di cifratura: simmetrica e asimmetrica. In una codifica simmetrica, una chiave è condivisa tra gli utenti, mentre una asimmetrica fa affidamento su entrambe le chiavi pubbliche e private. La codifica asimmetrica è considerata più sicura: molti utenti condividono la chiave pubblica, ma la sicurezza fa affidamento sulla chiave privata - protetta a tutti i costi - che non ha bisogno di essere condivisa con nessuno (a differenza di una chiave simmetrica). IPSec usa la cifratura asimmetrica per instaurare una connessione sicura, per poi sfruttare quella simmetrica per migliorare la velocità di collegamento. Per quello che riguarda il collegamento, è compatibile sia con UDP che con TCP.

2.2.5 Autenticazione

L'autenticazione a chiave pubblica e privata assicura che mittenti e destinatari stiano effettivamente comunicando con il giusto partner. IPsec supporta molteplici sistemi di autenticazione, tra cui: HMAC-SHA1/SHA2, certificate authorities (CAs), RSA, ECDSA, e pre-shared key (PSK). Ogni tipologia ha i suoi pregi e difetti e casi d'uso in cui è preferibile. Ogni protocollo punta a garantire che i dati rimangano sicuri e affidabili attraverso il loro tragitto.

2.2.6 Implementazioni

StrongSwan è una implementazione open-source di IPsec per Linux. Supporta funzionalità come IPv6, certificati X.509 a chiave pubblica, liste di certificati revocati, storage di chiavi RSA private su smartcard e implementazione completa del protocollo IKEv2.re.

2.2.7 Considerazioni

Questa suite di protocolli consente di implementare una soluzione VPN accademicamente perfetta, robusta dal punto di vista della sicurezza ed efficace. L'unico impedimento che ha è che richiede l'utilizzo di due porte dedicate e i due protocolli ausiliari utilizzati (AH/ESP e IKE), che potrebbero rendere l'utilizzo più difficoltoso in ambienti con firewall molto limitanti.

2.3 PPTP

2.3.1 Panoramica

Si tratta di uno dei più vecchi protocolli VPN in uso ancora oggi, ma in quanto tale ha alcune gravi criticità date dall'età. Ad esempio, la crittografia a 128 bit e il protocollo usato per l'autenticazione (MS-CHAP) contenente note vulnerabilità lo rendono ormai un protocollo insicuro, da evitare se le informazioni che transitano sono sensibili. Tuttavia, è estremamente semplice da configurare e il più veloce dal punto di vista prestazionale, il che lo rende ideale per usi quali streaming video o l'utilizzo di VPN su terminali con potenze di calcolo estremamente limitate. È stato sviluppato da Microsoft

nel 1999 [HPV⁺99, RFC2637] e lavora instaurando un canale di controllo tra i due peers sulla porta 1723 TCP e un tunnel GRE su cui transitano effettivamente i dati.

2.3.2 Protocolli utilizzati

2.3.2.1 Generic Routing Encapsulation

GRE è un protocollo di tunneling sviluppato da Cisco Systems che può incapsulare un'ampia varietà di protocolli di livello di rete all'interno di collegamenti Point-to-Point o Point-to-Multipoint virtuali su una rete IP.

2.3.3 Cifratura

Con PPTP, è possibile usare Microsoft Point-to-Point Encryption (MPPE) per instaurare una connessione cifrata, ma PPTP di base non usa cifratura. MMPE usa l'algoritmo RC4 con chiavi da 40 o 128-bit. Tutte le chiavi sono derivate dalla password in chiaro dell'utente. Tuttavia, la RFC7465 proibisce l'uso di RC4 in quanto non robusto a sufficienza.

2.3.4 Autenticazione

Per quel che riguarda l'autenticazione degli utenti, PPTP può usare uno dei seguenti protocolli:

- Extensible Authentication Protocol (EAP),
- Microsoft Challenge Handshake Authentication Protocol (MSCHAP) version 1 and version 2,
- Challenge Handshake Authentication Protocol (CHAP),
- Shiva Password Authentication Protocol (SPAP),
- Password Authentication Protocol (PAP).

MSCHAP version 2 e EAP-Transport Layer Security (TLS) sono protocolli migliori rispetto agli altri supportati perché offrono mutua autenticazione, dove sia il client che il server verificano l'identità dell'altro. Se un client si autentica attraverso uno degli altri

protocolli, il server verifica l'identità del client, ma il client non ha modo di verificare quella del server.

2.3.5 Considerazioni

Non offrendo una cifratura adeguata, PPTP non è una soluzione ritenuta accettabile per il caso d'uso in questione.

2.4 OpenVPN

2.4.1 Panoramica

OpenVPN è una VPN SSL che permette di incanalare tutto il traffico di una sottorete attraverso una unica porta UDP o TCP, e fa affidamento su OpenSSL. Come le altre soluzioni VPN, OpenVPN servizi essenziali di sicurezza quali autenticazione, cifratura, integrità dei dati e controllo degli accessi. Supporta due modalità di lavoro, routing e bridging:

Routing consiste nell'interconnessione di due sottoreti indipendenti, dove il server VPN (generalmente installato sul router) inoltra i pacchetti all'indirizzo IP specificato in fase di configurazione. Si tratta quindi di un collegamento a livello 3 del modello OSI.

Bridging è una modalità che lavora esclusivamente all'interno di una sottorete; il funzionamento è analogo a quello di uno switch ethernet fisico.

OpenVPN è una soluzione che lavora in user space, dunque l'overhead generato è maggiore in quanto sono necessarie molteplici copie dei pacchetti affinché siano trasferiti dal kernel space allo user space. Supporta l'intero insieme delle funzionalità di TLS, necessitando di una ampia code base, mostrando un maggior potenziale a soffrire di vulnerabilità.

2.4.2 Protocolli utilizzati

Come precedentemente accennato, OpenVPN usa la libreria di OpenSSL, che implementa il protocollo Transport Layer Security, progettato per offrire una connessione

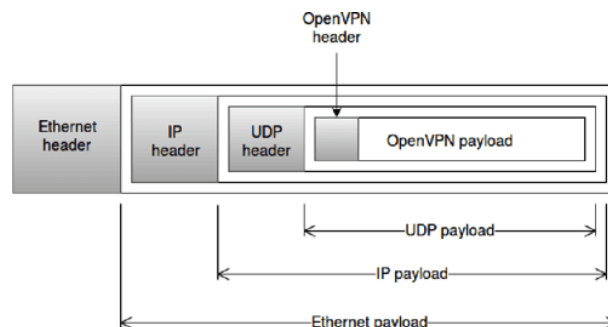


Figura 2.5: Dettaglio di un pacchetto OpenVPN

sicura attraverso una rete non sicura. A differenza del puro TLS, OpenVPN offre all'utente la possibilità di utilizzare una pre-shared key per generare quel che è noto come HMAC firewall, che autentica tutta la sequenza di handshake TLS.

Essendo UDP un protocollo non connesso, i pacchetti IP criptati e firmati che sono incanalati tramite UDP, non hanno nessuna garanzia di affidabilità. L'affidabilità necessaria per una sicura autenticazione è garantita, però, dal protocollo TLS che utilizza TCP come protocollo di trasporto. È importante notare che il canale dati e il canale di controllo transitano all'interno dello stesso tunnel UDP (o TCP). L'incapsulamento dei pacchetti è descritto dal seguente diagramma.

La struttura mostrata si applica a tutti i pacchetti OpenVPN; tuttavia, differenti pacchetti avranno differenti payloads.

2.4.2.1 Secure Socket Layer/Transport Layer Security VPNs

Il protocollo Transport Layer Security, originariamente noto come Secure Socket Layer, è un protocollo progettato per garantire una connessione sicura attraverso una rete non sicura. TLS permette autenticazione di client e server, integrità dei dati e confidenzialità. Per l'autenticazione usa i certificati X.509 [CSF⁺08, RFC5280] con una crittografia asimmetrica e si occupa di negoziare una chiave di sessione simmetrica. Un vantaggio delle VPN SSL rispetto a quelle basate su IPsec è che riescono a lavorare anche in reti protette da firewall molto stringenti, in quanto la maggior parte delle aziende non filtra il traffico TCP sulla porta 443, essendo normalmente usato dai dipendenti per accedere a Internet. OpenVPN di default utilizza la porta 1194 UDP, ma, nel caso quella porta

fosse chiusa, può utilizzare la 443 TCP.

2.4.3 Tunnel TCP vs UDP

Premesso che attraverso i tunnel VPN passa traffico sia TCP che UDP, anche i tunnel stessi possono essere realizzati con connessioni TCP o UDP.

Il protocollo TCP utilizza notevoli algoritmi per assicurare un recapito corretto dei dati al destinatario. Avere due connessioni TCP una dentro l'altra forzerà gli algoritmi di entrambe le connessioni a lavorare in parallelo. Non essendo TCP progettato per lavorare in quella condizione, si potrebbe andare incontro a problemi quali il *retransmission problem*, *TCP meltdown* e doppia ritrasmissione. Questi problemi potrebbero verificarsi nel momento in cui entrambe le connessioni stanno tentando di ritrasmettere pacchetti.

Tutto ciò non vale per il protocollo UDP, che come descritto precedentemente, è un protocollo non connesso senza nessuna garanzia che il messaggio raggiunga correttamente il destinatario. A discapito dell'affidabilità, si possono ottenere velocità di trasmissione notevolmente superiori.

TCP potrebbe rivelarsi la scelta migliore solo nel caso in cui si debba creare un tunnel che passi attraverso una rete instabile, o attraverso una rete che applica forti censure.

2.4.4 Cifratura

OpenVPN utilizza un protocollo di sicurezza personalizzato e SSL/TLS per lo scambio delle chiavi. Usa OpenSSL per la cifratura, dunque è disponibile un ampio numero di algoritmi di cifratura, in particolare basati su AES [BMM04, RFC3826]. Quello di default è AES-256-GCM, che garantisce un ottimo livello di sicurezza, specialmente riguardo confidenzialità, autenticazione dell'origine e integrità dei dati. OpenVPN supporta la Perfect Forward Secrecy, un meccanismo che garantisce che le chiavi di cifratura vengano cambiate automaticamente ad intervalli regolari. Dunque, se anche una chiave venisse compromessa, soltanto una piccola porzione di dati verrebbe esposta.

2.4.5 Autenticazione

A differenza della modalità Preshared Static Key, la modalità TLS (preferita) usa il protocollo TLS per autenticare, instaurare una connessione sicura ed effettuare lo scambio delle chiavi simmetriche di sessione tra i peers. L'uso di TLS non solo offre un metodo automatico e sicuro per la distribuzione delle chiavi simmetriche, ma anche un modo per rinnovare tali chiavi in qualsiasi momento della comunicazione. Questo aspetto della modalità TLS offre ciò che è chiamato Perfect Forward Secrecy, che non è presente nella modalità PSK. I due step principali del protocollo TLS, a grandi linee, sono:

1. Negoziazione della connessione TLS: entrambi i lati della connessione si autenticano scambiandosi i certificati e verificando i certificati del lato opposto; se l'autenticazione ha successo, il protocollo procede allo step due; altrimenti, la connessione viene terminata.
2. Le chiavi di sessione sono negoziate attraverso il canale TLS sicuro appena stabilito.

2.4.6 Misure di sicurezza aggiuntive

OpenVPN offre diverse funzionalità di sicurezza: cifratura fino a 256-bit attraverso la libreria OpenSSL, anziché supportare IKE; lavora in user space, senza quindi necessità di effettuare operazioni sullo stack IP, e quindi operazioni kernel; ha la possibilità di far cadere i privilegi di root; entrare in una *chroot jail* dopo l'inizializzazione; applicare un SELinux context dopo l'inizializzazione; offre supporto alle smartcard attraverso i token basati su PKCS 11.

2.4.7 Considerazioni

Si tratta di una soluzione per VPN matura e flessibile, con supporto a meccanismi di sicurezza all'altezza.

2.5 WireGuard

2.5.1 Panoramica

In IPsec, si ha una separazione netta tra il livello che si occupa dello scambio dati (IKE) e il livello di trasformazione (AH/ESP). Seppure sia una saggia separazione del punto di vista semantico, e decisamente corretta da un punto di vista di rete, ha lo svantaggio di aumentare la complessità implementativa. WireGuard, anziché implementare questa separazione, crea un'interfaccia di rete virtuale che può essere amministrata con le utility standard `ip` e `ifconfig`. Dopo aver configurato questa interfaccia con una chiave privata (e opzionalmente una PSK) e le varie chiavi pubbliche dei peers con cui dovrà comunicare in maniera sicura, la connessione è pronta ad essere instaurata. Scambio di chiavi, connessioni, disconnessioni e via dicendo avvengono dietro le quinte, e l'amministratore non deve configurare nessuno di questi aspetti. Le regole di firewalling possono essere configurate usando i tool standard, con la garanzia che i pacchetti che provengono da un'interfaccia di WireGuard saranno autenticati e cifrati. Per la sua semplicità, WireGuard è apparentemente meno incline a errori di configurazione rispetto ad IPsec.

WireGuard è in grado di instaurare esclusivamente tunnel di livello 3. Con questo approccio è infatti più semplice assicurare autenticità e origine dei pacchetti. Supporta sia IPv4 che IPv6 e può incapsulare sia v4-in-v6 che v6-in-v4.

WireGuard si concentra sulla semplicità e su una codebase facilmente ispezionabile, essendo allo stesso tempo estremamente performante e adatto a diversi ambienti. Combinando lo scambio di chiavi e la cifratura a livello 3 in un unico meccanismo e utilizzando un'interfaccia di rete virtuale anziché un livello di trasformazione, WireGuard rompe con la tradizione per perseguire una soluzione ingegneristicamente solida apparentemente più pratica e sicura.

A partire dalla versione 5.6 del kernel Linux, WireGuard verrà incluso nel kernel stesso.

2.5.2 Protocolli utilizzati

Nell'implementazione di WireGuard, sono utilizzati i seguenti protocolli:

ChaCha20 per cifratura simmetrica, autenticata con Poly1305, utilizzando AEAD, come specificato in [NL15, RFC7539]

Curve25519 come Elliptic-curve Diffie-Hellman, un protocollo per la negoziazione delle chiavi

BLAKE2s per hashing e hashing con chiave, descritto in [SA15, RFC7693]

SipHash24 come chiavi per hashtable

HKDF come funzione per la derivazione delle chiavi, come spiegato in [KE10, RFC5869]

2.5.3 Cifratura

Dal punto di vista della cifratura utilizzata da WireGuard, rompe la tradizione delle altre soluzioni. Infatti, è intenzionalmente privo di flessibilità per quel che riguarda la scelta dei cifratori e dei protocolli utilizzati. Se vengono trovate falle in quelli scelti in fase di progettazione, tutti i terminali avranno bisogno di essere aggiornati. Come dimostrato dalla continua scoperta di vulnerabilità all'interno del protocollo TLS, dare la possibilità di scegliere quale cifrario usare aumenta enormemente la complessità.

2.5.4 Autenticazione

Per la distribuzione delle chiavi, WireGuard si ispira a OpenSSH, dove i due peers si scambiano le proprie chiavi pubbliche statiche. Il meccanismo con cui lo scambio avviene è basato sull'handshake **Noise IK** di Noise [Noi]. Dopo lo scambio delle chiavi, il peer che non ha iniziato la connessione deve aspettare ad usare la sessione fino a che non riceve un pacchetto cifrato dall'iniziatore, che dà conferma delle chiavi. Le chiavi pubbliche sono lunghe 32 bytes e possono essere facilmente rappresentate con una codifica Base64 in 44 caratteri, che semplifica il trasferimento di esse attraverso vari mezzi. È supportata anche la Perfect Forward Secrecy, illustrata precedentemente.

2.5.5 Considerazioni

La semplicità di installazione è sicuramente un fattore che in ambienti piccoli ha la sua rilevanza; insieme alle prestazioni elevate, la rendono una soluzione da valutare al momento di installare un servizio VPN.

Capitolo 3

Realizzazione

3.1 Virtualizzatore

Un virtualizzatore è un software che si occupa di astrarre le risorse hardware di un computer/server, facendo da intermediario tra esse e il software che deve girarci sopra. Astraendo le risorse, è possibile distribuirle in maniera agile e ottimizzata tra i vari software che le richiedono. In ambito di virtualizzazioni server, la situazione più comune è la seguente: sulla macchina fisica è installato un **hypervisor**, che crea, gestisce e assegna risorse alle macchine virtuali, su cui viene installato un sistema operativo completo; sono poi queste macchine virtuali a offrire effettivamente i servizi.

3.1.1 Caratteristiche e funzionamento

Gli hypervisor rendono la virtualizzazione possibile attraverso una traduzione delle richieste tra le risorse fisiche e quelle virtuali.

Fondamentalmente, ci sono due tipi di hypervisor: quelli detti **bare-metal**, che vengono eseguiti direttamente sull'hardware fisico e sono spesso installati allo stesso livello del BIOS sulla scheda madre, e quelli detti **in-hosting**, che girano come software standard sul sistema operativo installato sull'hardware fisico (detto host system). Suddividendo le risorse, è possibile assegnarle non più a una sola macchina, ma a molteplici macchine virtuali.

Lo svantaggio degli hypervisor in-hosting è la loro maggiore latenza rispetto agli

hypervisor bare-metal. Ciò è dovuto al fatto che la comunicazione tra hardware e hypervisor non è diretta, ma deve passare attraverso il sistema operativo che lo ospita. Questo tipo di hypervisor è anche detto client hypervisor, essendo più comunemente utilizzato da utenti finali e per il testing di software, scenari in cui la latenza non è particolarmente rilevante.

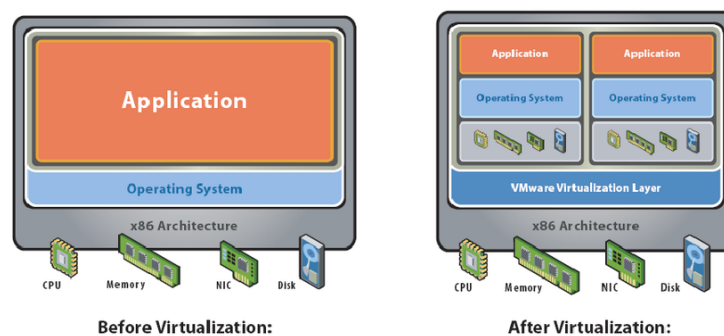


Figura 3.1: Installazione fisica vs Installazione virtuale

3.1.2 VirtualBox

Durante le prime fasi di testing, abbiamo utilizzato Oracle VirtualBox [Ora] sui nostri PC per creare un ambiente di simulazione. VirtualBox è un client hypervisor, open source e disponibile per tutti i sistemi operativi.

3.1.3 VMWare ESXi

Nella fase di realizzazione, abbiamo invece utilizzato un server reale, su cui era installato l'hypervisor VMWare ESXi [vmw]. Una volta allocate le risorse necessarie, abbiamo installato CentOS 7 come sistema operativo sulla macchina virtuale come da requisito. Questa macchina virtuale corrisponde al router/firewall nel diagramma di rete presentato nei capitoli precedenti.

3.1.4 Installazione e configurazione dei servizi VPN

Dopo una fase iniziale di configurazione dei servizi interni ed esterni illustrati nei requisiti, si è passati all'installazione e configurazione dei tre servizi VPN scelti per il

testing.

3.2 Installazione e configurazione di IPsec - tunnel mode

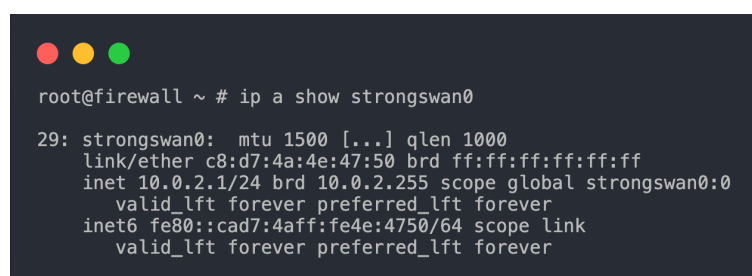
Il primo servizio che è stato installato è IPsec, grazie all'implementazione open source offerta da strongSwan [str].

3.2.1 Aggiunta dell'interfaccia di rete virtuale

Prima di installare strongSwan, è necessario predisporre l'interfaccia di rete virtuale che verrà utilizzata per la creazione del tunnel VPN. Per fare ciò, è necessario abilitare le interfacce virtuali con il comando `modprobe dummy`. A questo punto è possibile aggiungerla e configurarla, assegnandole:

- un nome (e.g.: `strongswan0`)
- un MAC Address qualunque - a patto che sia diverso da tutti quelli presenti nella subnet (e.g.: `C8:D7:4A:4E:47:50`),
- un indirizzo IP con la relativa maschera (e.g.: `10.0.2.1/24`)

e abilitarla. Una volta completato il tutto, visualizziamo il risultato con il seguente comando:



```
root@firewall ~ # ip a show strongswan0
29: strongswan0: mtu 1500 [...] qlen 1000
    link/ether c8:d7:4a:4e:47:50 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.1/24 brd 10.0.2.255 scope global strongswan0:0
        valid_lft forever preferred_lft forever
    inet6 fe80::cad7:4aff:fe4e:4750/64 scope link
        valid_lft forever preferred_lft forever
```

Figura 3.2: Dettagli interfaccia virtuale strongswan0

3.2.2 Installazione di strongSwan

Per installare il daemon di strongSwan è sufficiente lanciare il comando `dnf install strongswan`, che si occuperà di scaricare e installare la versione più recente disponibile.

3.2.3 Configurazione di strongSwan

Per adattare il comportamento del servizio alle proprie esigenze, è necessario modificare il file di configurazione del servizio, che nel caso di strongSwan si trova nella directory `/etc/strongswan/`. Al suo interno, andremo a inserire i parametri adatti. Di particolare rilievo sono i seguenti:

```
conn strongswanVPN      # per la connessione di nome strongswan VPN
    type=tunnel          # IPSec in tunnel mode
    keyexchange=ikev2     # Protocollo per lo scambio chiavi

    # Algoritmi di cifratura consentiti
    ike=aes256-sha256-modp2048,[...],aes256gcm16-prfsha512-ecp384!
    esp=aes256-sha256-modp2048,[...],aes256gcm16-ecp384!

    leftcert=server.crt  # Certificato del server
    rightauth=eap-tls     # Protocollo di autenticazione
    rightdns=8.8.8.8      # DNS Server per il client

    # Range di indirizzi IP assegnabili ai client
    rightsourceip=10.0.2.10-10.0.2.100
```

3.2.4 Creazione del certificato per un client

Una volta terminata la configurazione lato server, è necessario creare un certificato per ogni client che vorrà connettersi alla VPN. È possibile farlo tramite le funzioni della libreria OpenSSL. Essendo in ambiente di testing e non di produzione, non ci si è preoccupati di acquistare un certificato che abbia possibilità di firmare altri certificati; si è scelto infatti di utilizzare sempre OpenSSL per creare una Certificate Authority locale. Questo ha lo svantaggio che i client non hanno modo di verificare presso un ente stabilito (e.g.: Let's Encrypt, o altre CA affermate) la validità del certificato, ma il funzionamento è identico.

3.3 Installazione e configurazione di OpenVPN over TCP

Per il servizio OpenVPN, si è deciso di utilizzare la porta 443 TCP per testare le performance nel caso di reti con firewall stringenti.

3.3.1 Installazione di OpenVPN

L'installazione avviene tramite il comando `dnf install openvpn`, che scarica e installa tutto il necessario per eseguire il servizio. Al file di configurazione di OpenVPN, sono state apportate alcune modifiche. Quelle più rilevanti sono le seguenti:

```
port 1194, proto tcp    # Porta e protocollo da utilizzare

# Dopo l'avvio, si disabilitino i privilegi di root
user nobody, group nobody

# Rende la VPN una sottorete, con prefisso e maschera
topology subnet
server 10.8.0.0 255.255.255.0

push "dhcp-option DNS 8.8.8.8"    # DNS primario per i clients
push "dhcp-option DNS 8.8.4.4"    # DNS secondario per i clients

# Comunica ai client di far passare il loro traffico
#     attraverso il server VPN
push "redirect-gateway def1 bypass-dhcp"

# Nomi dei file della CA, del certificato pubblico del server
#     e della relativa chiave privata
ca ca.crt
cert server_jH2NKwoak6pDEBoQ.crt
key server_jH2NKwoak6pDEBoQ.key
```

```
cipher AES-128-GCM # Algoritmo scelto per la cifratura del canale

tls-version-min 1.2 # Versione minima di TLS
tls-crypt tls-crypt.key
tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
```

3.3.2 Certificati

Per la creazione della Certificate Authority e di tutti i certificati, sono state utilizzate le funzioni della libreria EasyRSA, messa a disposizione sulla repository GitHub di OpenVPN stesso.

3.3.3 Configurazione del profilo VPN per un client

Affinché un client possa connettersi alla VPN, è necessario che egli sia in possesso di un profilo contenente tutti i dettagli tecnici necessari a instaurare una connessione corretta con il server, e il suo certificato personale. In particolare, devono combaciare porta e protocollo utilizzato, gli algoritmi di cifratura, le funzioni di *digest* e i parametri per TLS.

3.4 Installazione e configurazione WireGuard

L'installazione di WireGuard si effettua semplicemente con il comando `dnf install wireguard`, che si generi la chiave del server e che si inserisca all'interno del file di configurazione, insieme all'IP che utilizzerà il server stesso per interfacciarsi con la VPN. In automatico viene creata un'interfaccia di rete virtuale `wg0`, a cui viene assegnato l'IP scelto. Ogni client avrà sempre lo stesso IP, in quanto vengono assegnati nella fase di creazione del profilo di connessione.

3.4.1 Configurazione del profilo VPN per un client

Affinché un client possa connettersi alla VPN, è necessario che nel file di configurazione del server sia presente la chiave pubblica del client, e nel profilo di connessione del client

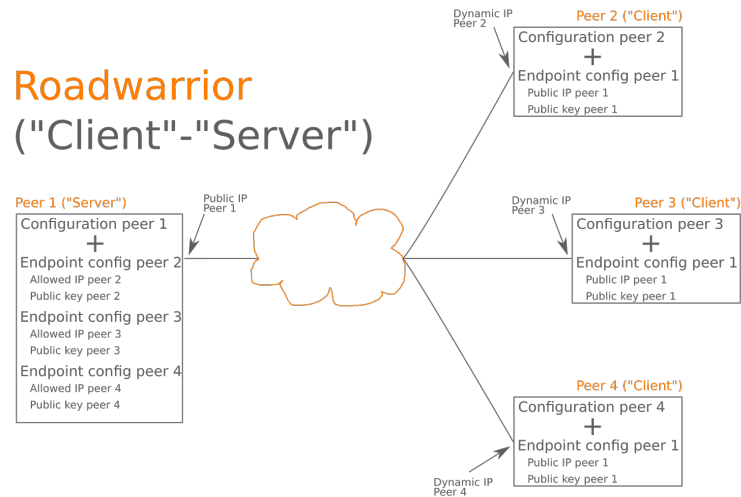


Figura 3.3: Architettura di installazione di WireGuard

sia presente l'IP pubblico del server, la sua chiave pubblica e l'indirizzo IP che il client assumerà.

3.5 Configurazione del Firewall

Nelle policies del firewall, sono state aggiunte delle voci che autorizzano il traffico proveniente dalle interfacce di rete virtuali `strongswan0`, `tun0` e `wg0` a navigare su Internet e a comunicare sulla porta 5201 TCP/UDP con la LAN dei server. Questa sarà la porta utilizzata da un servizio di misura delle performance che sarà in esecuzione sul Web Server, `iperf3`.

Capitolo 4

Testing

4.1 Modalità di esecuzione dei test

In questa sezione si andrà ad analizzare le performance delle tre soluzioni VPN descritte nei capitoli precedenti, al fine di valutare quale di esse offre le prestazioni migliori. Le prestazioni verranno valutate analizzando il throughput, la sua stabilità e la percentuale di packetloss. I software che sono stati utilizzati per effettuare le misurazioni questi dati sono `iPerf3` e `mtr`.

4.1.1 Panoramica di `iPerf3`

`iPerf` è uno strumento open source che permette di misurare le prestazioni di una rete. Per effettuare le misurazioni, `iPerf` crea dei flussi di dati su TCP, UDP o SCTP e invia traffico da un host all'altro; al termine del trasferimento, oltre a un report dettagliato in base al tipo di misurazione richiesta, mostra la larghezza di banda media disponibile. In questo modo, gli utenti possono determinare il throughput effettivamente utilizzabile.

4.1.2 Panoramica di `mtr`

`mtr` è un altro software di misurazione delle performance di una rete, che sostanzialmente unisce i risultati di `traceroute` e `ping`. I test effettuati da `mtr` sono unidirezionali, dunque è opportuno effettuare misurazioni manualmente in entrambe le direzioni, in

```

iperf3 -c firewall.filippovisconti.com -p 64999 -t 10s -i 1
Connecting to host firewall.filippovisconti.com, port 64999
[ 7] local 192.168.1.118 port 59050 connected to 79.61.138.204 port 64999
[ ID] Interval      Transfer    Bitrate
[ 7] 0.00-1.00    sec 7.29 MBytes 61.2 Mbits/sec
[ 7] 1.00-2.00    sec 5.75 MBytes 48.2 Mbits/sec
[ 7] 2.00-3.00    sec 5.64 MBytes 47.3 Mbits/sec
[ 7] 3.00-4.00    sec 5.61 MBytes 47.0 Mbits/sec
[ 7] 4.00-5.00    sec 5.59 MBytes 46.9 Mbits/sec
[ 7] 5.00-6.00    sec 5.57 MBytes 46.7 Mbits/sec
[ 7] 6.00-7.00    sec 5.57 MBytes 46.7 Mbits/sec
[ 7] 7.00-8.00    sec 5.57 MBytes 46.7 Mbits/sec
[ 7] 8.00-9.00    sec 5.57 MBytes 46.8 Mbits/sec
[ 7] 9.00-10.00   sec 5.59 MBytes 46.9 Mbits/sec
- - - - -
[ ID] Interval      Transfer    Bitrate
[ 7] 0.00-10.00   sec 57.7 MBytes 48.4 Mbits/sec
[ 7] 0.00-10.00   sec 56.9 MBytes 47.7 Mbits/sec
iperf Done.

```

Figura 4.1: Esempio di output di iPerf3

quanto i risultati differire in maniera sostanziale. Per avere una misurazione affidabile, è consigliabile far durare il test almeno 10 minuti.

MTR fa affidamento sui pacchetti Time Exceeded dell'Internet Control Message Protocol restituiti dai router, o sui pacchetti Echo Reply, quando il pacchetto raggiunge l'host destinatario.

```

> sudo mtr firewall.filippovisconti.com -s 5000 -c 10 -n -r
Start: 2022-06-28T16:18:24+0200
HOST: Filippos-MBP.lan
  Loss%  Snt  Last  Avg  Best  Wrst  StDev
1. |-- 192.168.1.254      0.0%   10   1.0   1.0   0.7   1.3   0.2
2. |-- 10.103.123.42     0.0%   10   1.8  15.7   1.7  100.5 30.4
3. |-- 10.103.11.38      0.0%   10   3.1   3.9   3.1   6.7   1.2
4. |-- 10.1.170.1        0.0%   10   2.6   2.7   2.4   3.6   0.3
5. |-- 10.254.2.2        0.0%   10   2.2   5.5   2.2  17.9   6.1
6. |-- 89.97.200.190     0.0%   10   2.2   2.6   2.2   2.8   0.2
7. |-- 89.97.200.61      0.0%   10   3.3   3.0   2.4   3.3   0.3
8. |-- 85.36.8.152       0.0%   10   3.2   3.4   3.2   3.6   0.2
9. |-- ???              100.0   10   0.0   0.0   0.0   0.0   0.0
10. |-- ???             100.0   10   0.0   0.0   0.0   0.0   0.0
11. |-- ???             100.0   10   0.0   0.0   0.0   0.0   0.0
12. |-- 79.61.138.204    60.0%   10  12.3  12.1  11.8  12.4   0.3

```

Figura 4.2: Esempio di output di mtr

4.1.2.1 Spiegazione del formato dell'output

Nella prima colonna, si legge un numero e un indirizzo IP: il numero corrisponde alla distanza in *hop* tra l'host da cui parte il test e l'IP indicato alla sua destra. La seconda colonna, **Loss%**, indica la percentuale di pacchetti che quell'IP ha perso. È auspicabile un valore inferiore all'1% per una connessione affidabile. La terza colonna, **Snt**, indica il numero di pacchetti inviati a quell'IP. Le successive 4 colonne indicano il valore

dell'ultimo, del medio, del migliore e del peggiore round-trip-time in millisecondi - ossia il tempo necessario affinché un pacchetto parta dal mittente, raggiunga il destinatario, e torni indietro. L'ultima colonna indica la deviazione standard tra questi ultimi 4 valori. I valori dalla terza colonna in poi forniscono dunque informazioni sulla latenza della rete. È desiderabile il valore più basso possibile. Tuttavia, spesso la latenza dipende da fattori esterni alla rete locale.

Nella misurazione di esempio, è stato richiesto l'invio di 10 pacchetti (`-c 10`) di dimensione 5000 byte (`-s 5000`). Per gli hop 9, 10 e 11, si ha un risultato anomalo: nessun IP restituito e 100% di packetloss. Questo risultato non mostra problemi di connessione, ma indica semplicemente che l'host non ha risposto alle richieste indirizzate a lui (per i motivi più disparati, da un carico di lavoro troppo alto, a un firewall che fa cadere quel tipo di pacchetto), e che però, visto che l'hop 12 risponde correttamente, ha inoltrato correttamente quelle destinate a chi gli succede.

4.1.3 Criteri di valutazione

Per dare una valutazione complessiva alle tre soluzioni testate, si andranno a tenere in considerazione i seguenti parametri: throughput, percentuale di packet loss per un pacchetto di grandi dimensioni e latenza media.

4.1.3.1 Throughput

Il throughput di un canale di comunicazione misura la quantità di dati che può essere trasferita tra mittente e destinatario in una data unità di tempo. In ambito reti, si è soliti utilizzare come unità di tempo il secondo e come quantità di dati il bit, o suoi multipli (Kbit, Mbit, Gbit). La velocità e l'affidabilità di trasmissione dei pacchetti sono parametri fondamentali ed è necessario che siano in grado di soddisfare le necessità dell'azienda proprietaria della rete. Packet loss, latenza e jitter influenzano il throughput di una rete, e più sono elevati, più le performance degradano. Minimizzare tutti questi fattori è un punto cardine della progettazione e ottimizzazione di una rete. La larghezza di banda potrebbe essere confusa con il throughput; è un valore che misura sempre una quantità di bit trasferiti in un'unità di tempo, ma misura il limite massimo teorico, e non quello reale.

È importante sottolineare che una larghezza di banda maggiore non conferisce più velocità, bensì dà soltanto la possibilità di trasferire allo stesso momento una quantità di dati maggiore. Se si hanno problemi di latenza e di perdita dei pacchetti, questi non verranno risolti aumentando la larghezza di banda.

4.1.3.2 Packetloss

Quando un pacchetto non riesce a raggiungere la destinazione prevista, si verifica il fenomeno della perdita di pacchetti, packet loss. Un utente avverte questo problema come interruzioni della rete, perdita di connettività e una velocità di connessione rallentata. Le situazioni in cui si soffre maggiormente questo problema sono tutte quelle in cui è richiesta elaborazione di dati in real-time, dove i ritardi non sono tollerati.

Nel caso di una connessione TCP, la perdita di un pacchetto non comporta perdita di dati, in quanto il protocollo è in grado di chiedere la ritrasmissione del pacchetto perduto; tuttavia, ciò comporta comunque un aumento della latenza e una riduzione del throughput generale.

Un pacchetto potrebbe essere scartato anche se, ad esempio, l'IPv4 header checksum o l'Ethernet frame check sequence indicano che il pacchetto è stato corrotto.

La perdita dei pacchetti viene misurata come la percentuale dei pacchetti che una rete ha effettivamente gestito, rispetto a quanti ne avrebbe in teoria dovuto gestire.

4.1.3.3 Latenza

La latenza di una rete, a volte chiamata anche lag, è un termine che descrive i ritardi di comunicazione attraverso una rete. In particolare, si intende il tempo necessario affinché un pacchetto venga catturato, trasmesso, processato attraverso molteplici apparati, ricevuto dal destinatario e decodificato.

La latenza è generalmente misurata in millisecondi. Minore è la latenza, migliori sono le performance. Una latenza inferiore ai 100ms è considerata accettabile, ma per buone performance si desidera un valore inferiore ai 40ms. Ovviamente, un valore prossimo agli 0ms sarebbe ideale.

4.1.4 Scelta della configurazione di test

Il dispositivo utilizzato per effettuare i test ha una scheda di rete che supporta fino a 1 Gbit/s, ed è collegato a Internet via fibra ottica, che satura il gigabit a disposizione, in modo tale che la macchina per fare i test non sia il collo di bottiglia dell'ambiente.

Per effettuare i test, sono stati scelti i seguenti parametri:

```
iperf3 -c [IP ADDRESS] -p 5201 -t 300s -i 5
```

Si effettuerà un primo test con iperf3 lungo 300 secondi, con report ogni 5 secondi.

```
mtr [IP ADDRESS] -s 5000 -c 1000
```

Con mtr si effettuerà il secondo test, inviando 1000 pacchetti della dimensione di 5000 byte, che comporta una durata del test di oltre 15 minuti.

4.2 Misure senza VPN

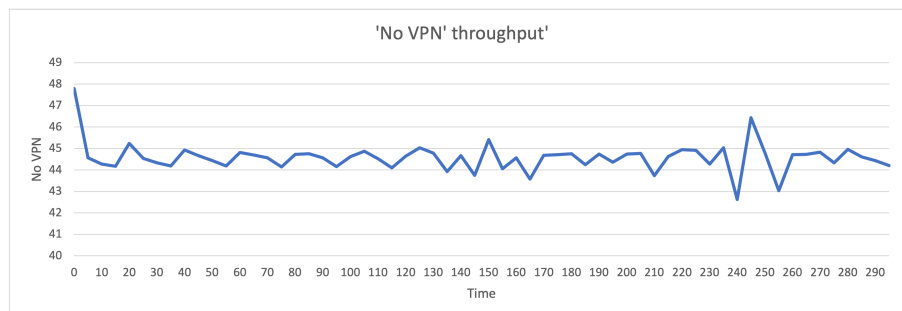


Figura 4.3: Throughput senza VPN su 300 secondi

Nella configurazione base, senza VPN, si può osservare come il throughput sia stabile tra i 44 e i 45 Mbit/s, eccetto per i primi istanti, dovuti a un periodo di assestamento.

In questo grafico invece, si può notare come, fino all'ottavo hop, la latenza sia generalmente bassa e la percentuale di packetloss irrisoria. Gli hop 9, 10 e 11 non rispondono, ma ciò non vuol dire che non funzionino. L'ultimo hop, quello del router di destinazione, ha una percentuale di packetloss molto elevata (più del 50%) e una latenza più elevata, seppur ancora accettabile.

```

> sudo mtr firewall.filippovisconti.com -s 5000 -c 1000 -n -r -w
Password:
Start: 2022-06-29T12:03:33+0200
HOST: Filippos-MacBook-Pro.local Loss% Snt Last Avg Best Wrst StDev
 1|-- 192.168.1.254      0.0% 1000 1.1 0.9 0.6 21.3 0.9
 2|-- 10.103.123.42     0.0% 1000 2.2 3.8 1.1 100.6 7.7
 3|-- 10.103.11.38      0.0% 1000 3.0 3.6 2.5 17.9 1.4
 4|-- 10.1.170.1         0.0% 1000 2.6 2.6 1.8 22.9 1.1
 5|-- 10.254.2.2         0.0% 1000 3.0 3.7 1.5 81.5 4.1
 6|-- 89.97.200.190     0.0% 1000 2.7 2.6 1.8 32.1 1.4
 7|-- 89.97.200.61      0.1% 1000 3.0 3.0 2.2 16.6 1.0
 8|-- 85.36.8.152       0.0% 1000 3.1 3.4 2.5 57.6 3.2
 9|-- ???              100.0 1000 0.0 0.0 0.0 0.0 0.0
10|-- ???              100.0 1000 0.0 0.0 0.0 0.0 0.0
11|-- ???              100.0 1000 0.0 0.0 0.0 0.0 0.0
12|-- 79.61.138.204     53.1% 1000 12.4 27.5 11.4 7144. 329.3

```

Figura 4.4: mtr senza VPN

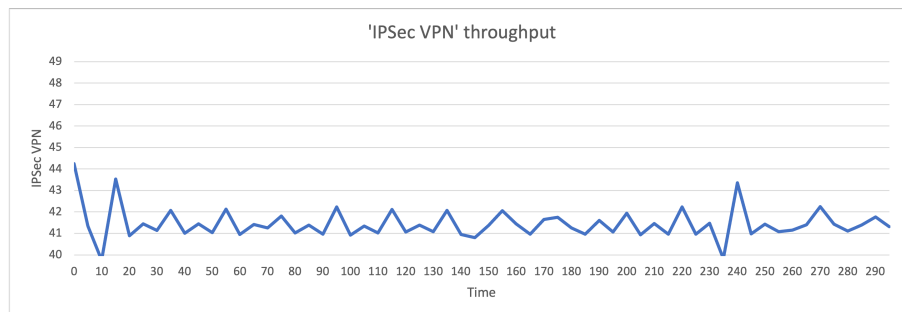


Figura 4.5: IPSec Throughput su 300 secondi

4.3 Misure con IPSec e IKEv2

Ripetendo lo stesso test attraverso un tunnel IPSec, si nota come il throughput sia calato e oscilla tra i 41 e i 42 Mbit/s.

```

> sudo mtr 50.50.50.3 -s 5000 -c 1000 -n -r -w
Password:
Start: 2022-06-29T13:21:20+0200
HOST: Filippos-MacBook-Pro.local Loss% Snt Last Avg Best Wrst StDev
 1|-- 10.222.111.2      0.0% 1000 9.1 8.6 8.0 29.2 1.1
 2|-- 50.50.50.3       0.0% 1000 13.6 13.8 12.7 77.2 2.7

```

Figura 4.6: mtr su IPSec

Il secondo test invece riporta una packetloss a destinazione nulla, ossia nessun pacchetto è stato perso, e una latenza media migliore rispetto a quella del test precedente.

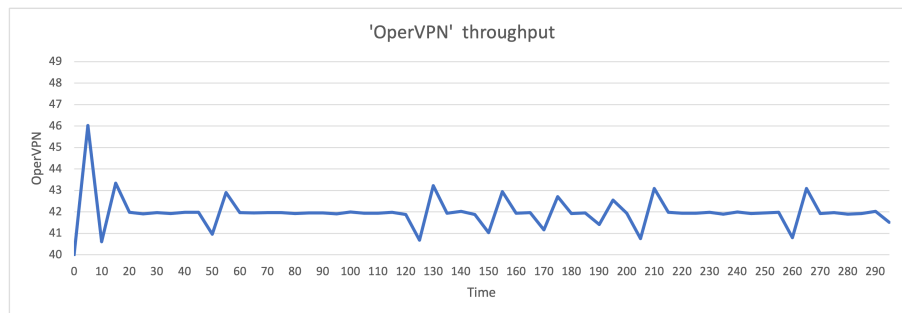


Figura 4.7: OpenVPN Throughput su 300 secondi

4.4 Misure con OpenVPN over TCP

Con OpenVPN, il primo test registra un throughput medio marginalmente più alto di IPSec, anche se con oscillazioni leggermente più ampie.

```
> sudo mtr 50.50.50.3 -s 5000 -c 1000 -n -r -w
Start: 2022-06-29T16:21:37+0200
HOST: Filippou-MBP.lan Loss% Snt Last Avg Best Wrst StDev
1. |-- 10.8.0.1 0.0% 1000 15.6 15.6 14.0 55.6 4.2
2. |-- 50.50.50.3 0.0% 1000 23.7 24.1 22.2 65.4 3.4
```

Figura 4.8: mtr su OpenVPN

Nel secondo test, si ha ugualmente lo 0% di packetloss, ma una latenza media maggiore di 10ms; si tratta comunque di un valore ampiamente accettabile.

4.5 Misure con WireGuard

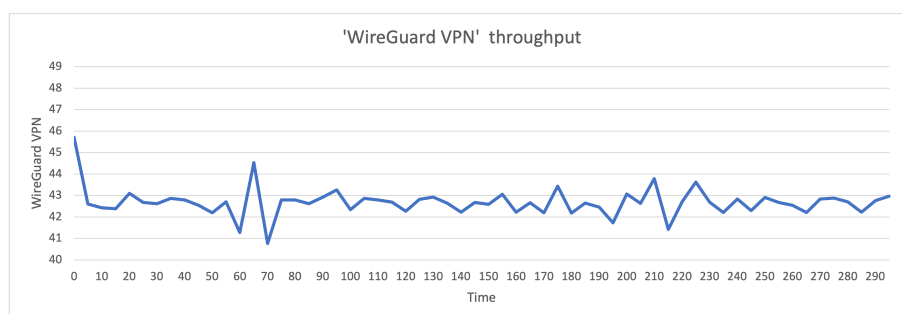


Figura 4.9: WireGuard Throughput su 300 secondi

Utilizzando WireGuard, nel primo test si raggiunge il risultato migliore, con un throughput medio che sfiora i 43 Mbit/s.

```
> sudo mtr 50.50.50.3 -s 5000 -c 1000 -n -r -w
Password:
Start: 2022-06-30T14:23:33+0200
HOST: Filippos-MacBook-Pro.local Loss% Snt Last Avg Best Wrst StDev
1. |-- 10.66.66.1 0.0% 1000 9.6 9.1 8.2 20.9 0.7
2. |-- 50.50.50.3 0.0% 1000 13.6 13.2 12.2 22.8 0.6
```

Figura 4.10: mtr su WireGuard

Nel secondo test, come nelle altre soluzioni VPN, la percentuale di packetloss è a 0, e la latenza è pari a quella ottenuta tramite la soluzione con IPSec, dunque molto buona.

4.6 Analisi delle misure

Questo grafico sovrappone i dati grezzi del primo test, riguardante il throughput medio. Essendo campionato ogni secondo, sono presenti molte oscillazioni che rendono il grafico confuso.

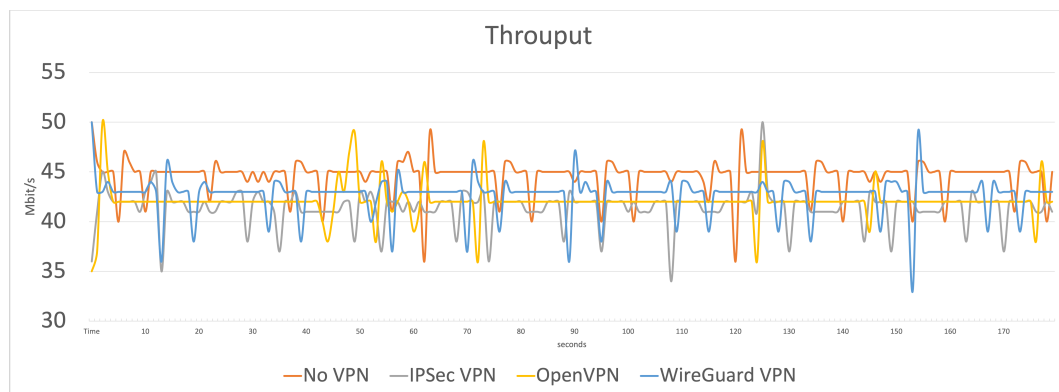


Figura 4.11: Confronto dei throughput grezzi

Campionando invece ogni 5 secondi, si riducono le oscillazioni, che essendo di lieve entità sono poco significative, e diventa chiara la classifica di performance in termini di throughput tra i 4 casi.

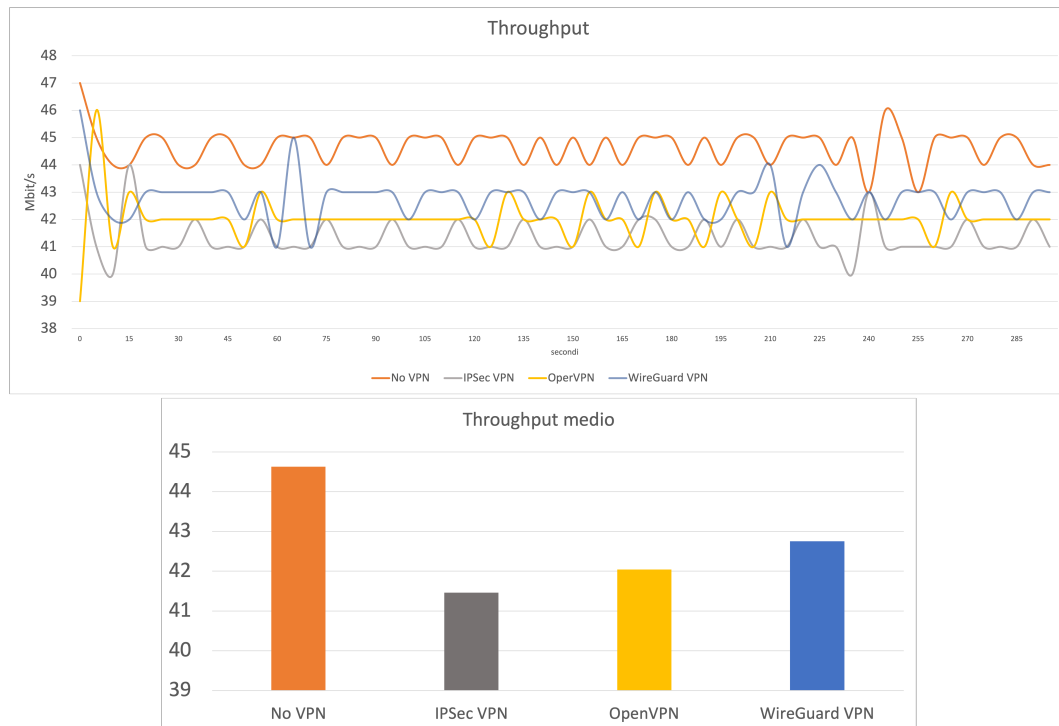


Figura 4.12: Confronto dei throughput raffinati

In questo caso, escluso il caso senza VPN che ovviamente utilizza tutta la banda disponibile per trasferire dati, la soluzione più performante è WireGuard, seguita da OpenVPN e IPsec.

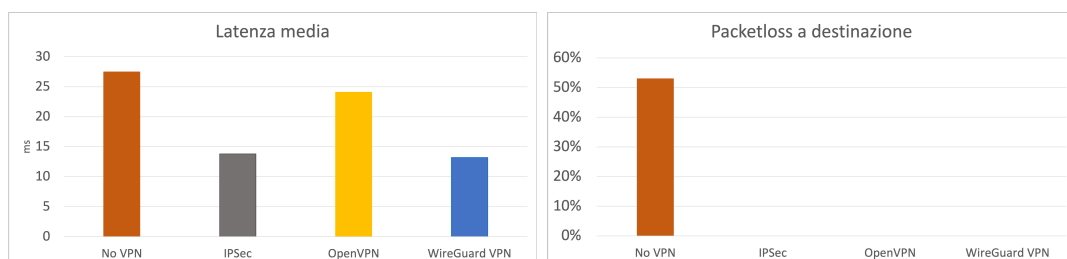


Figura 4.13: Confronto di latenza media e di packetloss

Questo confronto mostra come IPsec e WireGuard abbiano una latenza minore, e tutte e tre le soluzioni portino a 0 la percentuale di packetloss. Ciò comporta una trasmissione dei dati molto più affidabile.

Capitolo 5

Security concerns

5.1 Principali problematiche di sicurezza

Combinare una soluzione VPN sicura con una suddivisione della rete interna in compartimenti isolati sarebbe certamente ideale dal punto di vista della sicurezza. Tuttavia, l'accesso di terze parti alla rete interna di un'organizzazione - siano essi dipendenti, clienti esterni, o altro, aggiunge delle sfide impegnative nel garantire sicurezza. Ad esempio, se il dispositivo di un dipendente o di un cliente viene compromesso, e questa persona aveva instaurato una connessione VPN con l'azienda, coloro che hanno portato a termine l'attacco possono sfruttare il tunnel VPN come ponte per effettuare attività di ricognizione sulla rete interna dell'azienda, nonostante tutte le misure di sicurezza possibilmente implementate dall'azienda stessa.

Tuttavia, implementando una soluzione VPN moderna, è possibile monitorare il traffico, chi lo ha generato, che tipo di traffico è, e come viene usato. Tenere traccia di queste attività tramite il monitoring delle sessioni riduce i rischi, in quanto permette alle organizzazioni di identificare la sorgente del traffico sospetto e terminarlo se ritenuto opportuno.

5.2 Attacchi mirati agli utenti

Il primo step per ridurre i rischi e proteggere i dati sensibili dell'azienda è assicurarsi che tutti i dipendenti, o chiunque altro sia coinvolto nell'uso delle VPN, sappia che la

sicurezza dei dati è una priorità. Per fare questo, è necessario assicurare un'adeguata formazione a tutti loro, che copra tutti i maggiori pericoli, e le misure di difesa, che potrebbero incontrare.

È indiscutibile il fatto che alla base ci deve essere un'infrastruttura adeguata e che i dispositivi utilizzati supportino i più elevati standard di sicurezza. Infatti, i conduttori di un potenziale attacco vanno appositamente alla ricerca di, ad esempio, reti WiFi non protette, o cifrature banali da rompere.

5.2.1 Furto di credenziali

Il furto di credenziali è un tipo di crimine che consiste nel trafugare qualcosa che permette alla vittima di certificare la propria identità - ad esempio, email e password. Una volta rubate le credenziali, colui che le ha rubate avrà gli stessi permessi e gli stessi privilegi della vittima. Permette al ladro di resettare password, impedire alla vittima di accedere ai suoi stessi account, scaricare dati privati, ottenere accesso agli altri computer nella rete della vittima, distruggere backup, e via dicendo.

Gestire questo tipo di furti, e le loro conseguenze, dovrebbe avere altissima priorità per tutte le aziende, ma anche per i singoli utenti.

Esistono dei servizi, quali <https://haveibeenpwned.com>, che permettono agli utenti, inserendo il proprio indirizzo email, di verificare se sono stati coinvolti in un data breach - una divulgazione non autorizzata di dati sensibili in seguito a un attacco a una azienda. Questi servizi, che lo fanno a fin di bene, ottengono questi dati attraverso il dark web, così come lo fanno dei malintenzionati. Sapere di essere stato coinvolto in un furto di credenziali permette di prevenire un uso scorretto di esse, cambiando la password e aggiungendo misure di sicurezza più efficaci, quali ad esempio una One-Time-Password.

Le credenziali possono essere rubate sotto varie forme: hashes, tokens o anche testo in chiaro. Per trarre in inganno gli utenti, i malintenzionati spesso utilizzano la tecnica del phishing o dello spearphishing. Si tratta di soluzioni economiche ed efficienti, perché si fondano sull'interazione umana, sulla manipolazione e sull'inganno, anziché sullo sfruttamento di vulnerabilità software.

Nel caso di furto di credenziali aziendali, i criminali effettuano una ricognizione per capire chi sono le persone che posseggono i privilegi necessari a raggiungere il loro scopo,

e indirizzeranno a loro i tentativi di phishing.

Alcuni modi per prevenire il furto di credenziali sono:

- Autenticazione a più fattori
- Formazione degli utenti su come riconoscere i tentativi di Phishing
- Formazione degli utenti su come impostare password sicure
- Limitare l'utilizzo delle credenziali aziendali ad applicativi sicuri e controllati
- Mantenere aggiornati i sistemi operativi e i software utilizzati
- Effettuare regolarmente valutazioni sulle vulnerabilità
- Utilizzare strumenti di monitoring del traffico

5.2.2 Social Engineering

Con social engineering si intende quell'insieme di tecniche di manipolazione che vanno a sfruttare l'errore umano per ottenere informazioni riservate, accesso a sistemi protetti od oggetti di valore. Sono particolarmente efficaci contro utenti ingenui e/o ignoranti in materia, che non si aspettano un pericolo. Questo tipo di attacco può avvenire online, ma anche di persona o al telefono.

5.2.2.1 Phishing e Spear Phishing

Il phishing è un tipo di truffa facente parte delle tecniche di social engineering che è comunemente camuffata in email o SMS fraudolenti. La truffa consiste nel far raggiungere alla vittima la pagina di login di un sito web, dall'aspetto identica a quella del servizio di cui si vogliono rubare le credenziali, che però, anziché portare correttamente a termine il login, inoltra le credenziali al truffatore. Tra le informazioni nel mirino dei truffatori si ha:

- Username
- Password

- Indirizzo Email
- Residenza
- Numeri di carte di credito
- Data di nascita

Lo Spear Phishing è un caso particolare di phishing in cui il malintenzionato ha studiato la vittima e le sue abitudini. Per aumentare le possibilità di successo, infatti, includerà nel messaggio fraudolento quante più informazioni personalizzate possibili in modo da far abbassare la guardia della vittima.

Nonostante alcuni tentativi di phishing siano effettivamente ben costruiti, la maggior parte è facilmente riconoscibile.

Di seguito, alcune bandiere rosse per identificare un messaggio fraudolento:

- errori ortografici e grammaticali: ad esempio, è difficile che una banca invii un messaggio non curato
- messaggi contenenti richieste di informazioni personali: ad esempio richieste di credenziali per accedere a un servizio
- messaggi estremamente urgenti: ad esempio, un messaggio inaspettato contenente una minaccia di chiudere l'account della vittima
- email contenenti mittenti sospetti: ad esempio, una email proveniente da john@mybankofamerica.com, quando il dominio usuale è @bankofamerica.com

5.3 Attacchi mirati al sistema

Nel mirino dei malintenzionati, non c'è solo l'utente finale. Un altro punto di ingresso possibile si ottiene sfruttando le possibili vulnerabilità non mitigate presenti sui sistemi della vittima, sia essa un utente singolo o un'intera azienda. Infatti, nessun software è privo di bug, ed essi a volte portano a falle di sicurezza, di varie gravità. Nelle situazioni più drammatiche, una falla permette a un utente non autorizzato di eseguire codice arbitrario sul sistema colpito dalla falla.

5.3.1 Versione non aggiornata

Le software house, non appena vengono a conoscenza delle falle di cui sopra, si mettono al lavoro per rilasciare un aggiornamento che chiuda la falla. I tempi di rilascio variano, in base a diversi fattori. È in ogni caso compito dell'amministratore di sistema essere aggiornato sulle vulnerabilità che si presentano e mantenere sempre aggiornati i software in esecuzione, o trovare altri sistemi per mitigare le falle nell'attesa che venga rilasciata una patch ufficiale. Nel caso delle soluzioni VPN in esame, esse hanno una potente arma in loro favore. Essendo tutte e tre open source, il codice è pubblico per la sua interezza e tutti possono ispezionarlo e modificarlo. L'idea di fondo è: più persone esperte lavorano su quel codice, più sarà facile che le vulnerabilità vengano scoperte prima che vengano utilizzate per scopi malevoli. Inoltre, potendo inserire modifiche, la platea di sviluppatori che potenzialmente ha le conoscenze per risolvere la falla si amplia.

5.3.2 Exploit di vulnerabilità zero-day

Una vulnerabilità senza patch è tra i casi più gravi e potenzialmente difficili da gestire. Una vulnerabilità zero-day è proprio questo, una vulnerabilità conosciuta ma senza una patch disponibile.

5.4 Multi-factor authentication

A seguito di un tentativo di phishing riuscito, un malintenzionato è in possesso delle credenziali di accesso di un utente a un servizio. Se il servizio in questione è quello della VPN aziendale, egli ha accesso alla porzione di rete a cui è autorizzato ad accedere l'utente vittima. Per diminuire drasticamente l'efficacia del phishing, uno strumento potente ed efficace è quello dell'autenticazione a più fattori. L'autenticazione a più fattori richiede che, affinché il login abbia successo, vengano inseriti, oltre a email e password, altre "proof of identity", che possono essere un certificato, un'impronta digitale, una smart card, o una password monouso temporanea.

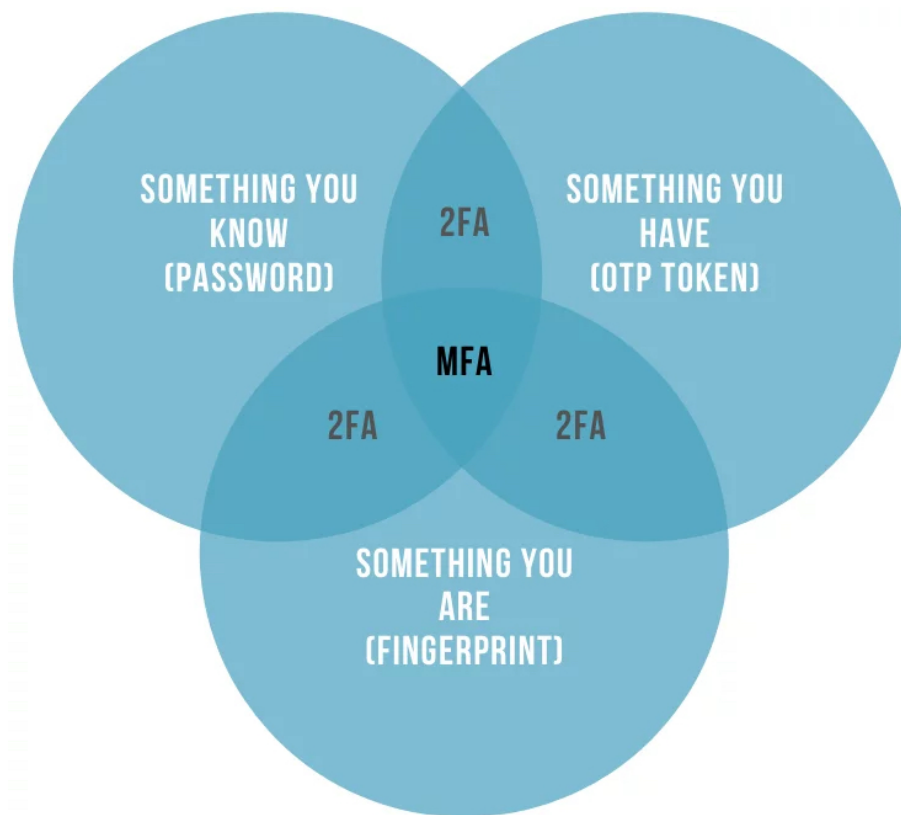


Figura 5.1: MFA

5.4.1 Certificato

I certificati possono essere utilizzati per autenticare sia i server VPN che i client. Generalmente, è sempre richiesto che un client che si vuole connettere sia autorizzato da un certificato.

Essi non contengono informazioni specifiche di una particolare VPN. Sono rilasciati da una Certificate Authority come prova di identità. I gateway che realizzano il tunnel VPN sono configurati in modo tale da accettare la CA che ha firmato il certificato partner come fidata. Tutti i certificati rilasciati da una CA autorizzata sono ritenuti validi, dunque si possono aggiungere e rinnovare senza alcun effetto collaterale sulla VPN. Lo stesso certificato potrebbe, anche se dipende dalla configurazione, essere utilizzato su diversi dispositivi.

I certificati riducono la manutenzione richiesta perché non devono essere cambiati

così frequentemente come le Pre-Shared Keys. Tutti i certificati nascono con una data di scadenza, oltre la quale il certificato non è più valido. Dopo la scadenza, è necessario creare un nuovo certificato.

I certificati per VPN possono essere generati sia da una CA esterna che da una interna, a patto che i gateway siano configurati in modo tale da accettarla come fidata.

Come controindicazione, si ha che tutti i client VPN devono supportare l'algoritmo della CA, altrimenti è impossibile instaurare una comunicazione.

5.4.2 Username e password

L'autenticazione con username e password è il metodo più semplice per identificare e autenticare gli utenti. Se la password immessa dall'utente non corrisponde a quella memorizzata nel sistema, l'accesso è ovviamente negato.

La password non viene mai memorizzata in chiaro, bensì viene memorizzato il suo hash, tramite un algoritmo di hashing scelto. Un algoritmo di hash consiste in una funzione che prende un input e restituisce un output indecifrabile e incomprensibile, da cui è impossibile ricostruire l'input, se non tramite brute-force. Tuttavia, ogni volta che l'algoritmo viene eseguito con uno stesso input, l'output è sempre uguale. Quando l'utente inserisce la password, dunque, viene calcolato l'hash e viene confrontato l'hash calcolato con quello memorizzato sul server.

Gli svantaggi consistono principalmente nel fatto che, se il numero di utenti cresce, la manutenzione diventa particolarmente complessa. Infatti, in quei casi si è soliti ricorrere a soluzioni quali l'autenticazione di Active Directory.

5.4.3 One Time Password

L'autenticazione a due fattori impedisce a malintenzionati di avere accesso ai sistemi della vittima utilizzando le credenziali rubate. Infatti, l'autenticazione con OTP richiede all'utente di validare la propria identificazione inserendo una password monouso temporanea (One-Time-Password). Questa OTP viene mostrata su qualcosa che l'utente possiede (un device apposito o una applicazione sul suo smartphone) noto come *authenticator*.

Conclusioni e sviluppi futuri

Quale è uscito vincitore

Nella fase di testing, si sono valutate le performance di VPN realizzate con IPSec, OpenVPN e WireGuard dal punto di vista del throughput medio, della latenza media e della percentuale di packetloss a destinazione. Dal punto di vista del throughput medio, la soluzione con migliori performance è quella di WireGuard, rispecchiando le affermazioni fatte sulla documentazione ufficiale. Per quel che riguarda la percentuale di packetloss, nonostante siano stati utilizzati pacchetti di grandi dimensioni per fare i test, tutte le soluzioni hanno riportato una perdita di pacchetti nulla, a dimostrazione della loro affidabilità. Sulla latenza media, si vede OpenVPN al secondo posto con uno svantaggio di 10 millisecondi rispetto a IPSec e WireGuard. Ultima nota che si può tenere in considerazione è la necessità di un client software da installare sui dispositivi che devono collegarsi in VPN. IPSec è integrato direttamente in tutti i sistemi operativi, dunque, nel caso si abbiano restrizioni sui software che è possibile installare, rimane l'unica scelta possibile. OpenVPN e WireGuard hanno entrambe bisogno di un client installato, in cui si importa il profilo di configurazione. Da notare è che WireGuard, a partire dalla versione 5.6 del kernel Linux, è parte del kernel stesso.

Come migliorare le misure

Altre informazioni che potrebbero essere interessanti nella valutazione della soluzione VPN da installare potrebbero essere l'overhead per pacchetto aggiunto da ogni soluzione, e di conseguenza anche la Maximum Transmission Unit.

Test di VPN Peer-To-Peer

Nel panorama delle soluzioni VPN disponibili, esiste una ulteriore tipologia che sfrutta la tecnologia Peer-To-Peer, su cui instaura una overlay network virtuale e privata.

Zero Tier

ZeroTier One [Zer] è una soluzione open source che usa alcuni dei più recenti sviluppi nel Software-defined networking per permettere agli utenti di creare reti private virtuali sicure e facilmente gestibili. Offre una console web per la gestione della rete e software da installare sui client. Si tratta di una connessione cifrata Peer-To-Peer. Ciò significa che la comunicazione tra due host non deve passare da un server centrale, bensì può avvenire direttamente, mantenendo un'elevata efficienza e una minima latenza.

ZeroTier è hypervisor di rete distribuito, costruito sopra una rete globale Peer-To-Peer crittograficamente sicura.

L'hypervisor di rete di ZeroTier è un virtualizzatore di reti auto-contenuto che implementa un livello 2 virtuale al di sopra di una rete Peer-To-Peer cifrata globale.

Il protocollo utilizzato da ZeroTier è originale, anche se alcuni suoi aspetti sono simili a VXLAN e IPSec. Consiste in due livelli concettualmente separati ma fortemente accoppiati: VL1 e VL2, che corrispondono ai livelli 1 e 2 del modello OSI. VL1 è formato dal livello di trasporto Peer-To-Peer, il "cavo virtuale"; VL2 è un livello 2 emulato che offre ai sistemi operativi e agli applicativi un mezzo di comunicazione familiare.

Nelle reti tradizionali, il livello 1 del modello OSI rappresenta il cavo fisico virtuale o il canale radio di comunicazione attraverso il quale i dati sono trasmessi. VL1 svolge lo stesso compito, utilizzando cifratura e autenticazione, oltre a un'altra serie di artifici per creare cavi virtuali al bisogno, in maniera dinamica.

Per raggiungere questo scopo, VL1 è organizzato con uno schema simile al DNS. Alla base della rete c'è una collezione di root server sempre attivi, il cui ruolo è simile a quello dei DNS root name server. Sui root server gira lo stesso software degli endpoint, ma la loro posizione è fissa e nota, e hanno performance elevatissime.

PAM vs VPN

Una soluzione alternativa alle VPN per garantire un accesso remoto sicuro a risorse interne è un meccanismo chiamato Privileged Access Management (PAM). Per minimizzare i rischi correlati all'accesso con VPN, è opportuno che ogni client che si colleghi abbia accesso solo ed esclusivamente ai sistemi di cui effettivamente necessitano per portare a termine il loro lavoro con successo. Purtroppo, questo controllo a grana fine non è raggiungibile in maniera efficiente utilizzando soltanto una soluzione VPN. In soccorso arrivano soluzioni per gestire gli accessi privilegiati, quali PAM - privileged access management. PAM permette alle aziende di dare ai dipendenti o ai clienti accesso alla propria rete interna senza una connessione VPN e permette allo staff IT di controllare, monitorare e gestire l'accesso a risorse critiche. Questo consente alle aziende di sapere con precisione quali account sono responsabili di quali attività. Introducendo diversi livelli di privilegi, PAM riduce anche la superficie esposta ad attacchi.

Bibliografia

- [Apa] Apache. <https://httpd.apache.org>.
- [BMM04] U. Blumenthal, F. Maino, and K. McCloghrie. The advanced encryption standard (aes) cipher algorithm in the snmp user-based security model. RFC 3826, RFC Editor, June 2004.
- [Cen] CentOS. <https://www.centos.org>.
- [CSF⁺08] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. RFC 5280, RFC Editor, May 2008. <http://www.rfc-editor.org/rfc/rfc5280.txt>.
- [Dro97] Ralph Droms. Dynamic host configuration protocol. RFC 2131, RFC Editor, March 1997. <http://www.rfc-editor.org/rfc/rfc2131.txt>.
- [Fre00] N. Freed. Behavior of and requirements for internet firewalls. RFC 2979, RFC Editor, October 2000.
- [HPV⁺99] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn. Point-to-point tunneling protocol (pptp). RFC 2637, RFC Editor, July 1999.
- [Kau05] C. Kaufman. Internet key exchange (ikev2) protocol. RFC 4306, RFC Editor, December 2005. <http://www.rfc-editor.org/rfc/rfc4306.txt>.
- [KE10] H. Krawczyk and P. Eronen. Hmac-based extract-and-expand key derivation function (hkdf). RFC 5869, RFC Editor, May 2010. <http://www.rfc-editor.org/rfc/rfc5869.txt>.

- [Ken05a] S. Kent. Ip authentication header. RFC 4302, RFC Editor, December 2005. <http://www.rfc-editor.org/rfc/rfc4302.txt>.
- [Ken05b] S. Kent. Ip encapsulating security payload (esp). RFC 4303, RFC Editor, December 2005. <http://www.rfc-editor.org/rfc/rfc4303.txt>.
- [Lin] Red Hat Enterprise Linux. <https://www.redhat.com/en>.
- [Moc87] P. Mockapetris. Domain names - concepts and facilities. STD 13, RFC Editor, November 1987. <http://www.rfc-editor.org/rfc/rfc1034.txt>.
- [NL15] Y. Nir and A. Langley. Chacha20 and poly1305 for ietf protocols. RFC 7539, RFC Editor, May 2015. <http://www.rfc-editor.org/rfc/rfc7539.txt>.
- [Noi] Noise. <http://noiseprotocol.org/noise.pdf>.
- [Ora] Oracle. <https://www.virtualbox.org>.
- [Pos81] Jon Postel. Internet protocol. STD 5, RFC Editor, September 1981. <http://www.rfc-editor.org/rfc/rfc791.txt>.
- [PR85] J. Postel and J. Reynolds. File transfer protocol. STD 9, RFC Editor, October 1985. <http://www.rfc-editor.org/rfc/rfc959.txt>.
- [SA15] M-J. Saarinen and J-P. Aumasson. The blake2 cryptographic hash and message authentication code (mac). RFC 7693, RFC Editor, November 2015.
- [str] strongSwan. <https://www.strongswan.org>.
- [vmw] vmware. <https://www.vmware.com/it/products/esxi-and-esx.html>.
- [Zer] ZeroTier. <https://www.zerotier.com/>.