

VPN - Virtual Private Network

Rete privata virtuale

Il termine **VPN** (**Virtual Private Network**), cioè **rete privata virtuale**, nasce alla fine degli anni 90 e si pone come evoluzione delle **linee dedicate** tra diverse sedi aziendali. Nel passato infatti, i collegamenti tra sedi remote di una stessa società, e quindi tra reti LAN remote, avvenivano solo se era presente una linea di comunicazione fisica dedicata, come per esempio via cavo oppure tramite ponte radio.



Sempre più aziende utilizzano le reti pubbliche come mezzo per garantire il lavoro da remoto ai propri dipendenti, collegando anche sedi diverse tra di loro con la propria infrastruttura informatica. Le VPN nascono quindi con l'esigenza di trasmettere dati in maniera sicura attraverso reti pubbliche. Una rete VPN è una rete privata costruita entro un'infrastruttura di rete pubblica, per esempio Internet permette a computer ubicati in sedi fisiche diverse di stabilire un collegamento tramite una rete non dedicata.

La **VPN** (**Virtual Private Network**) è, quindi, una rete privata che utilizza le reti pubbliche, ad esempio Internet, come infrastruttura di trasporto. Lo scopo delle VPN è quello di fornire alle aziende, le stesse caratteristiche delle linee private ma a costi inferiori sfruttando le reti pubbliche. Il termine VPN non indica un marchio o uno standard ma è un termine che definisce l'idea.

La VPN presenta diversi vantaggi:

- È possibile collegarsi dall'esterno alla rete privata del proprio ufficio o della propria azienda;
- Utilizzano sistemi di autenticazione in modo da garantire l'accesso solo ad utenti autorizzati;
- Gestione dei privilegi per le diverse categorie di utenti;
- Utilizzano sistemi di crittografia a chiave simmetrica (efficienza).

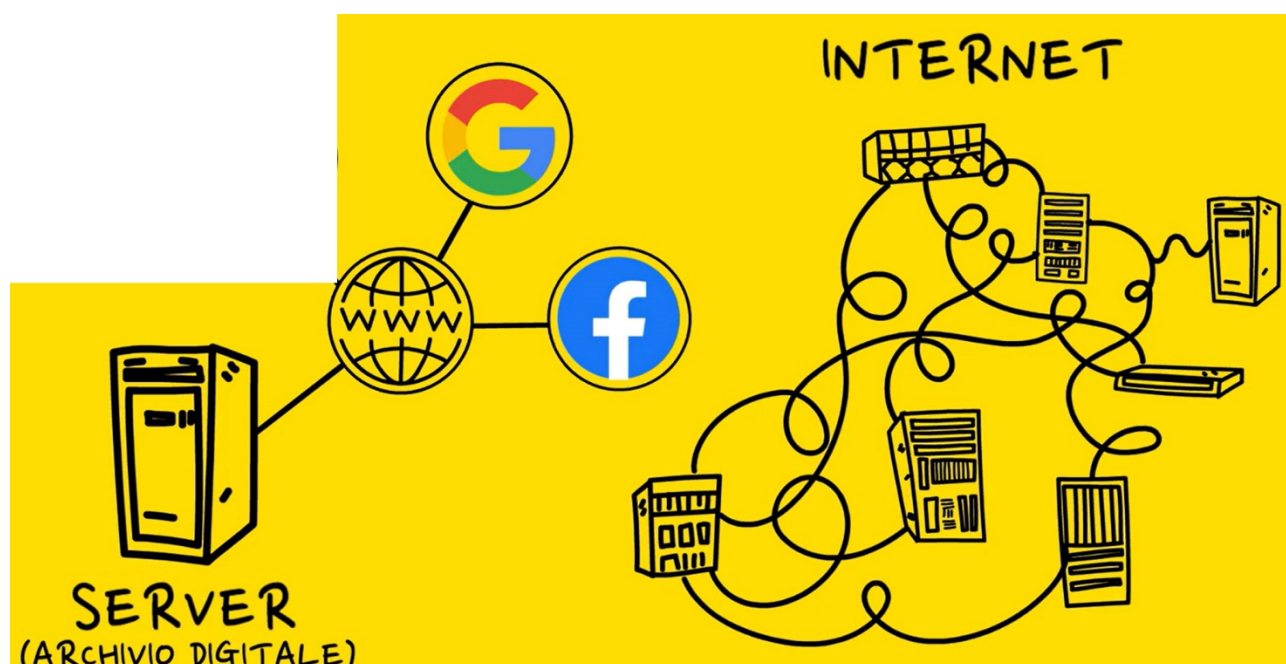
VPN:

COME FUNZIONA?

A CHE COSA SERVE?

SERVE DAVVERO?

Consideriamo un **SERVER**, quindi un PC che funge da archivio digitale, all'interno del quale vengono salvati dati di ogni tipo, per esempio tutti i dati del WWW vengono salvati su Server, dislocati in tutto il mondo da piccolissimi ad enormi e sono tutti collegati da un'intricata rete di cavi che permette ai server di comunicare tra di loro, questa intricata rete di cavi è la rete **INTERNET**.



Quando visitiamo un sito Web, il device che usiamo per collegarci ad Internet, entra in comunicazione con il Server, dove sono stati salvati i dati del sito in

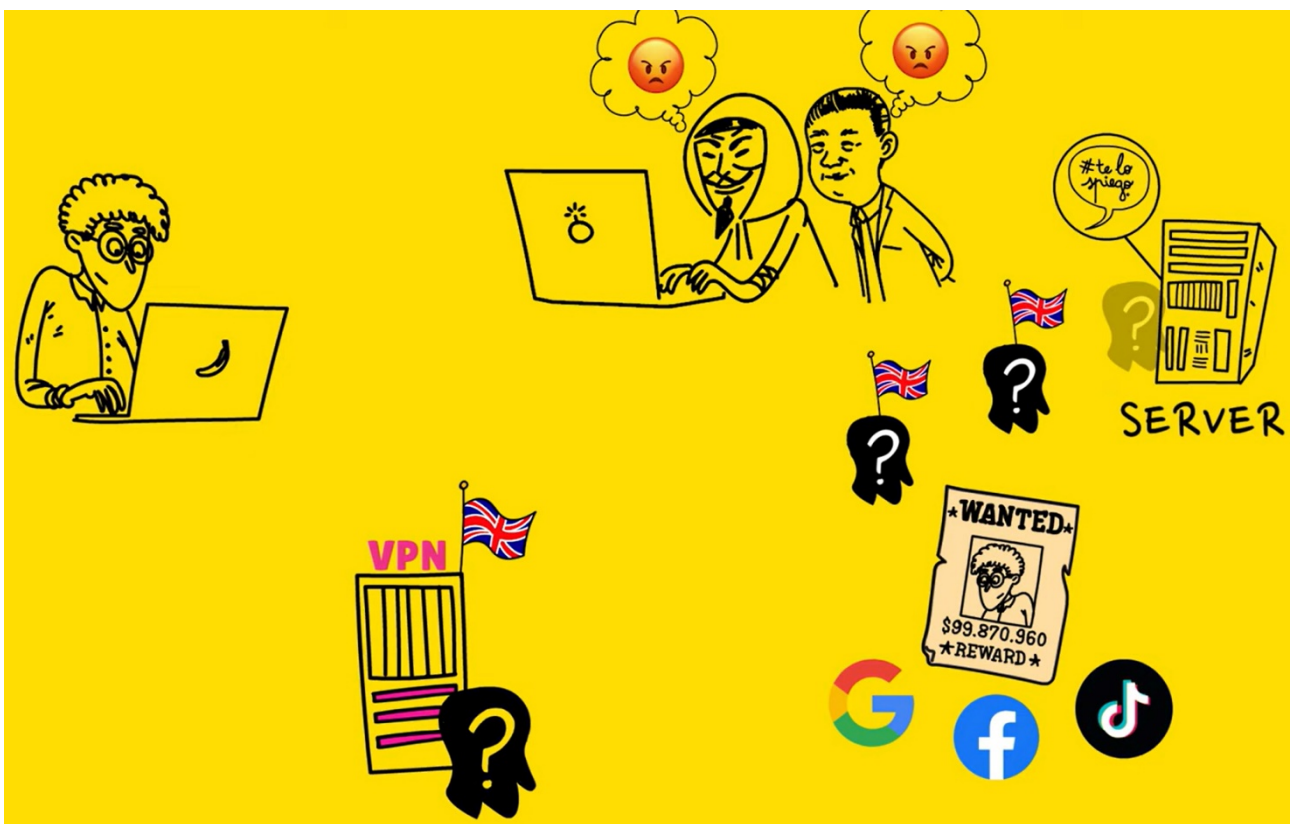
questione ed inizia a scambiare dati con esso ed il nostro browser traduce questi dati, permettendoci di visualizzarli sullo schermo e di interagire con essi e fin qui non ci sono problemi, tranne il fatto che mentre questi dati viaggiano tra il nostro computer ed il server e viceversa, sono vulnerabili e potrebbero essere intercettati e manipolati da pirati informatici e male intenzionati di ogni genere; per evitare questo problema, in genere, la maggior parte dei siti internet di oggi adotta il protocollo di sicurezza HTTPS, che protegge le comunicazioni tra Server ed utente, crittografando i dati, ma per diverse ragioni questo spesso non è sufficiente.



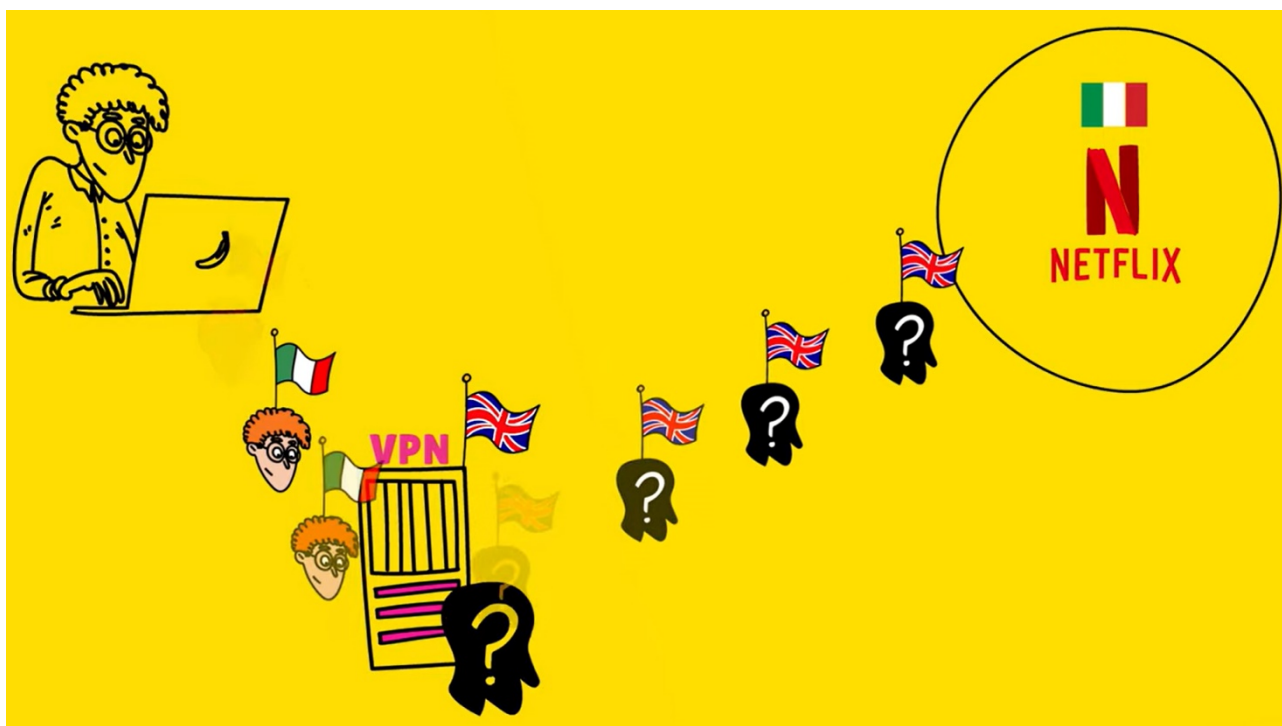
L'HTTPS non protegge dall'enorme arsenale di strumenti a disposizione di hacker e cyber criminali come malware, finte reti Wifi, etc., attraverso cui è facile intercettare dati e password. In generale, qualsiasi attività che svolgiamo online, consente di risalire, più o meno facilmente, alla nostra identità e/o all'indirizzo IP e rilevare quindi la nostra posizione geografica ed altri dettagli a chiunque voglia tracciarli, cosa fatta di frequente da molti siti internet e dai social network; le ricerche che facciamo online hanno un grande valore di mercato, da esse infatti si ricava un preciso profilo: chi siamo, i nostri gusti, interessi, cosa ci piace; informazioni estremamente preziose per le aziende interessate a vendere i loro prodotti, facendo quindi pubblicità mirata o per i governi che vogliono controllare i propri cittadini in modo poco democratico o per qualsiasi altro tipo male intenzionato; inoltre il nostro fornitore di servizi internet, come Vodafone, TIM, fastweb, etc., può vedere tutta la nostra attività online, comprese le pagine web che visitiamo e le informazioni che inviamo e riceviamo che potrebbe registrare, conservare, analizzare o addirittura venderle; uno strumento utile per prevenire questi rischi è la:

Rete Privata Virtuale o VPN

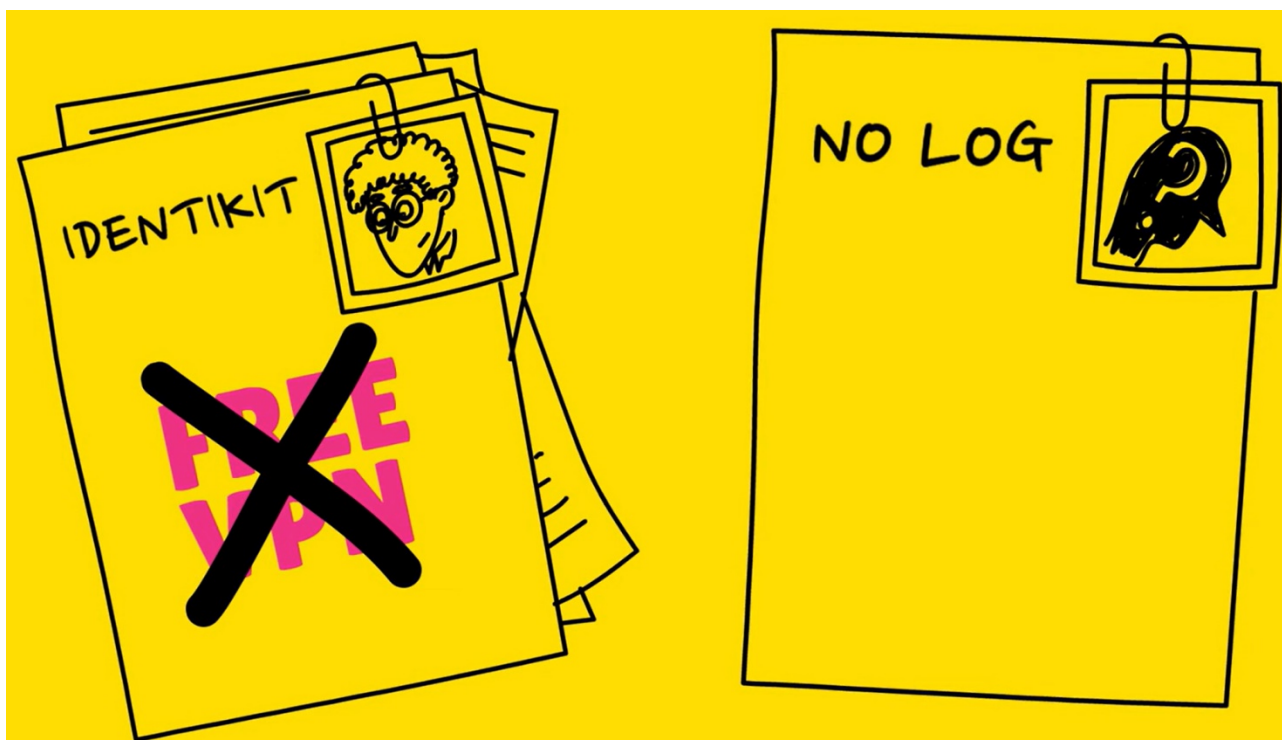
Una VPN in pratica è una specie di percorso alternativo per i nostri dati molto più protetto e sicuro rispetto alla normale rete internet; quando attiviamo una VPN sul nostro computer o telefono il dispositivo si connette direttamente su uno dei server del fornitore del servizio VPN che abbiamo scelto, server che si può trovare in un'altra città o addirittura in un altro stato, molti fornitori di servizi VPN hanno server in quasi tutte le nazioni del pianeta e da quel momento in poi sarà questo server a comunicare con il resto del web tramite internet facendo da filtro, inoltre i dati che verranno scambiati con il server per cui anche se qualcuno dovesse intercettarli, non potrebbe leggerli senza la chiave segreta per decodificarli, in questo modo la nostra identità rimarrà nascosta, i nostri dati rimarranno sicuri e sembrerà che stiamo navigando dal paese in cui si trova il server VPN.



Il fatto di poter scegliere la localizzazione del server offre un altro vantaggio, ossia quello di poter accedere a contenuti online limitati geograficamente, come alcuni video, articoli di notizie o librerie di streaming.



Una VPN affidabile, quindi, ci protegge dal tracciamento online, dalle minacce informatiche, l'importante è scegliere un servizio sicuro ed affidabile se al contrario si utilizza una VPN free, spesso le aziende che offrono questo servizio gratuitamente, raccolgono e vedono i dati dei loro clienti, quindi bisogna scegliere un fornitore di tale servizio che adotti una rigorosa politica di "NO LOG", ovvero che non registra le nostre attività online e che abbia un'ottima reputazione online.



Attualmente esistono tre tipi di VPN: Trusted VPN, Secure VPN, Hybrid VPN.

TRUSTED VPN

Con la Trusted VPN il provider garantisce che nessun terzo non autorizzato possa utilizzare il percorso del cliente. Questo implica che quest'ultimo abbia un proprio indirizzo IP e una propria politica di sicurezza.

Il percorso passa attraverso dei nodi di comunicazione che possono essere compromessi da terzi non autorizzati. Il provider deve garantire l'esclusività e l'integrità del percorso.

Le aziende che utilizzano una Trusted VPN vogliono la sicurezza che i loro dati si muovano attraverso una serie di percorsi con proprietà specifiche (basate sull'esigenza del cliente e precedentemente accordati) e controllati dall'ISP.

I requisiti minimi di una Trusted VPN:

- Nessuno all'infuori dell'ISP può influire sulla creazione o la modifica del percorso della VPN;
- Nessuno all'infuori dell'ISP può modificare i dati in entrata o quelli eliminati dal percorso della VPN;
- Il percorso e l'indirizzo usati devono essere stabiliti prima che la VPN venga creata.

SECURE VPN

Con la Secure VPN sono stati creati ed implementati dei protocolli per la cifratura dei dati in entrata e in uscita dalla rete. Il cliente che richiede questo tipo di VPN desidera trasmettere informazioni sensibili su Internet senza temere che vengano intercettate. Tutte le informazioni in viaggio sono quindi cifrate ad un tale livello che, se anche venisse intercettato il traffico, questo non sarebbe leggibile neanche con un computer ad alte prestazioni. La Secure VPN garantisce quindi la segretezza e l'integrità delle informazioni con una maggiore efficienza in quanto basata su crittografia a base simmetrica (gestione con ISP).

I requisiti minimi di una Secure VPN:

- Tutto il traffico sulla VPN deve essere cifrato e autenticato;
- Le proprietà sulla sicurezza della VPN devono essere concordate da tutte le parti della VPN;
- Nessuno al di fuori della VPN può compromettere la sicurezza delle informazioni e della VPN stessa.

HYBRID VPN

La Hybrid VPN unisce i vantaggi della Trusted VPN a quelli della Secure VPN.

Una **Hybrid VPN** è una combinazione di più tecnologie di VPN, che unisce i vantaggi di diverse soluzioni per soddisfare le esigenze specifiche di un'organizzazione. Questo tipo di VPN utilizza sia connessioni **Trusted VPN** (basate su infrastrutture private) sia connessioni **Secure VPN** per fornire un mix di sicurezza, flessibilità e scalabilità.

È chiaro infatti che quest'ultime hanno proprietà molto differenti:

Secure VPN: offre sicurezza, ma non assicura i percorsi.

Trusted VPN: assicura l'esclusività dei percorsi ma non la sicurezza da intrusioni.

La Hybrid VPN viene richiesta dalle aziende quando si desidera aggiungere sicurezza su parti di Trusted VPN.

I requisiti minimi di una Hybrid VPN:

- L'amministratore deve essere in grado di sapere con certezza se il traffico è o meno parte della Secure VPN.

Esempio pratico di Hybrid VPN:

Un'azienda con:

- **Tre sedi principali:** utilizzano una connessione (Trusted VPN) per garantire prestazioni elevate e sicurezza.
- **Dipendenti remoti o filiali minori:** accedono alla rete aziendale (Secure VPN) usando connessioni Internet.

Questo approccio garantisce che:

- I dati tra le sedi principali viaggino in un canale privato e affidabile.
- I lavoratori remoti abbiano accesso sicuro ai sistemi aziendali senza dover utilizzare infrastrutture costose.

Quando si usa una Hybrid VPN?

- In aziende con molteplici sedi e lavoratori remoti.
- Quando si richiede un bilanciamento tra performance e costi.
- Per garantire un'infrastruttura flessibile che supporti crescita e continuità operativa.

VPN, punti chiave:

1. Cos'è una VPN (Virtual Private Network)

- La VPN è una rete privata che utilizza una rete pubblica (solitamente Internet) per creare connessioni sicure e criptate tra dispositivi o reti remote.
- È spesso usata per garantire la privacy e la sicurezza, specialmente quando si accede a informazioni sensibili.

2. Come funziona una VPN

- La VPN crea un "tunnel" criptato tra il dispositivo dell'utente e il server VPN.
- Quando i dati attraversano Internet, rimangono protetti e riservati perché vengono criptati.

3. Tipi di VPN

- **VPN di accesso remoto:** permette a un utente di accedere a una rete privata da una posizione remota.
- **VPN site-to-site:** collega due reti diverse, come nel caso di uffici in sedi diverse.

4. Protocolli VPN

- Breve panoramica sui protocolli più comuni come PPTP, L2TP, IPsec e OpenVPN, e le loro caratteristiche principali.

5. Applicazioni pratiche

- Accesso a risorse aziendali, protezione della privacy su reti pubbliche, accesso a contenuti geograficamente limitati.

Approfondimento un argomento 1

Cos'è una VPN (Virtual Private Network)

La VPN, o rete privata virtuale, è un servizio che permette di creare una connessione sicura e criptata tra il dispositivo di un utente (come un PC o uno

smartphone) e una rete privata, passando attraverso una rete pubblica come Internet. **L'obiettivo principale di una VPN** è proteggere la privacy dell'utente e garantire la riservatezza dei dati trasmessi online.

Perché si chiama "Virtual Private Network"?

- **Virtual:** Non esiste una connessione fisica diretta tra i dispositivi collegati tramite VPN; viene creata una connessione "virtuale" attraverso Internet.
- **Private:** I dati trasmessi sono privati e protetti tramite crittografia, in modo che solo l'utente e il server VPN possano leggere e interpretare queste informazioni.
- **Network:** La VPN consente a diversi dispositivi di connettersi alla stessa rete virtuale sicura, come se fossero all'interno di una rete locale (LAN).

Funzionamento di una VPN

1. **Connessione dell'utente a un server VPN:** Quando si utilizza una VPN, il dispositivo dell'utente si connette a un server VPN posizionato in una località a scelta dell'utente (spesso in un'altra città o nazione).
2. **Crittografia del traffico:** Tutte le informazioni trasmesse dal dispositivo dell'utente vengono crittate dal software della VPN prima di essere inviate a Internet.
3. **Instradamento:** I dati viaggiano attraverso il server VPN e solo allora vengono inviati alla destinazione finale. Agendo come intermediario, il server VPN nasconde l'indirizzo IP reale dell'utente e utilizza il proprio.

Utilizzi Comuni delle VPN

1. **Sicurezza sui Wi-Fi pubblici:** Le VPN sono usate frequentemente per proteggere i dati quando si accede a Internet da Wi-Fi pubblici non protetti, come quelli di caffetterie o aeroporti.
2. **Privacy:** Nascondendo l'indirizzo IP e crittando i dati, le VPN impediscono a provider Internet e altri osservatori di tracciare l'attività online degli utenti.
3. **Accesso a risorse aziendali:** Le aziende utilizzano le VPN per permettere ai dipendenti di accedere in modo sicuro alla rete aziendale da remoto, mantenendo i dati riservati anche quando l'accesso avviene da reti esterne.
4. **Accesso a contenuti limitati geograficamente:** Alcuni contenuti online, come servizi di streaming, limitano l'accesso a determinate regioni. Con una VPN, l'utente può connettersi tramite server in altre località e bypassare queste restrizioni.

Vuoi includere esempi pratici di connessione VPN o altri dettagli tecnici?

Esempio pratico argomento 1.

Un esempio pratico per spiegare il concetto di VPN è il seguente:

Immaginiamo un dipendente di un'azienda, Maria, che lavora da casa. L'azienda di Maria ha una rete aziendale sicura, con accesso riservato a documenti sensibili e sistemi interni. Per mantenere questi dati al sicuro, l'azienda ha configurato una VPN.

Scenario:

1. **Connessione da casa:** Maria accende il computer e si collega alla sua rete domestica. Senza la VPN, il collegamento da casa a Internet sarebbe esposto a rischi di intercettazione, specialmente durante il trasferimento di dati sensibili.
2. **Avvio della VPN:** Maria apre il software VPN aziendale, inserisce le sue credenziali (nome utente e password) e si autentica. La VPN crea un "tunnel" sicuro tra il suo computer e i server dell'azienda.
3. **Accesso sicuro:** Ora, tutti i dati che Maria invia o riceve dall'azienda viaggiano in questo tunnel cifrato, rendendoli illeggibili a chiunque tenti di intercettarli lungo il percorso.
4. **Protezione:** Anche se Maria sta utilizzando una rete Wi-Fi domestica o pubblica (come quella di un bar), la VPN garantisce che le informazioni aziendali restino protette e sicure.

Esempio con Diagramma

Posso creare un'immagine per visualizzare il flusso del tunnel VPN, che rappresenti il percorso dei dati cifrati tra il dispositivo dell'utente e la rete aziendale, passando per Internet in sicurezza. Vuoi che lo faccia?



Per introdurre in modo dettagliato le VPN, iniziamo con il concetto e le caratteristiche principali:

1. **Cos'è una VPN (Virtual Private Network):**
 - **Definizione:** Una VPN, o Rete Privata Virtuale, permette di creare una connessione sicura su una rete non sicura, come Internet. In pratica, la VPN crea un "tunnel" cifrato tra due punti di connessione (ad esempio, un utente e un server aziendale) che permette il passaggio dei dati in modo protetto.
 - **Scopo:** Le VPN sono utilizzate per garantire privacy e sicurezza quando ci si collega a una rete pubblica, come il Wi-Fi di un bar o di un aeroporto, evitando che i dati trasmessi siano intercettati da terzi.
 - **Utilizzo:** Sono particolarmente comuni in ambienti aziendali, dove i dipendenti devono accedere a risorse interne della rete aziendale da remoto.
2. **Tecnologie e Protocolli Usati in una VPN:**

- **Protocollo di tunneling:** La VPN utilizza un protocollo di tunneling che "incapsula" i dati inviati, come **IPsec** o **OpenVPN**, permettendo una trasmissione sicura attraverso Internet.
- **Autenticazione e Cifratura:** La VPN autentica gli utenti per assicurarsi che siano autorizzati a connettersi e utilizza la crittografia per proteggere i dati trasmessi.

Posso approfondire ulteriormente, ad esempio, sui protocolli VPN o sui vari tipi di VPN (come VPN site-to-site e VPN client-to-site) per rendere la lezione completa.

Approfondimento un argomento 2

L'argomento 2 riguarda il funzionamento della VPN e come riesce a garantire una connessione sicura e privata attraverso la crittografia dei dati.

Dettagli sul funzionamento della VPN

1. **Tunnel VPN (Virtual Private Network Tunnel):** Quando un utente si connette a una VPN, i suoi dati vengono instradati attraverso un "tunnel virtuale". Questo tunnel crea una connessione sicura tra il dispositivo dell'utente e il server VPN, come se si trovassero sulla stessa rete locale. Durante questo percorso, il traffico passa da un punto all'altro attraverso Internet, ma resta protetto e cifrato.
2. **Cifratura dei Dati:** La cifratura è il processo principale che garantisce la riservatezza della VPN. Tutti i dati trasmessi dal dispositivo al server VPN vengono criptati, utilizzando algoritmi come AES-256, una crittografia avanzata utilizzata anche in ambito militare. In questo modo, se qualcuno dovesse intercettare i dati lungo il percorso, non potrebbe leggerli senza la chiave di decrittazione.
3. **Autenticazione:** Per accedere alla VPN, gli utenti devono autenticarsi, solitamente tramite username e password. In contesti aziendali, si può richiedere anche un'autenticazione a due fattori (2FA) per maggiore sicurezza, riducendo il rischio di accessi non autorizzati.
4. **Protocolli di Tunneling:** La VPN utilizza protocolli di tunneling che assicurano l'integrità e la sicurezza della connessione. I protocolli principali sono:
 - **OpenVPN:** Conosciuto per la sua sicurezza e adattabilità, è un protocollo molto utilizzato per le connessioni VPN.
 - **IPsec (Internet Protocol Security):** Si utilizza spesso per garantire sicurezza a livello IP, particolarmente diffuso nelle VPN aziendali.
 - **L2TP (Layer 2 Tunneling Protocol):** Spesso combinato con IPsec per una maggiore sicurezza.
5. **Server VPN:** Dopo essere crittografati e inviati attraverso il tunnel, i dati raggiungono il server VPN. Questo server funge da intermediario e li inoltra verso il loro destinatario finale, modificando l'indirizzo IP visibile con quello del server, nascondendo così l'identità e la posizione dell'utente.

Esempio Pratico

Immagina un dipendente che lavora da casa e si connette alla rete aziendale tramite VPN:

- **Connessione:** Accede alla VPN, fornendo le proprie credenziali.
- **Tunnel:** Una volta connesso, i suoi dati vengono inviati attraverso il tunnel crittografato.
- **Autenticazione e Sicurezza:** I dati cifrati arrivano al server aziendale, che li autentica e consente l'accesso alle risorse aziendali.

Il dipendente può così navigare e accedere ai documenti aziendali come se fosse in ufficio, ma con una connessione sicura e protetta.



Ecco l'immagine che illustra l'esempio pratico del collegamento VPN di un lavoratore remoto alla rete aziendale.

Approfondimento un argomento 3

Protocolli VPN: PPTP, L2TP, IPSec, OpenVPN e WireGuard

I protocolli VPN definiscono il modo in cui i dati vengono trasmessi in modo sicuro attraverso una rete. Ognuno di essi ha caratteristiche, vantaggi e svantaggi diversi. Vediamo i principali protocolli VPN:

1. PPTP (Point-to-Point Tunneling Protocol):

- **Caratteristiche principali:**
 - È uno dei protocolli VPN più vecchi.
 - Usa l'autenticazione basata su PPP (Point-to-Point Protocol) per creare il tunnel.
 - Supporta una crittografia a basso livello (128-bit).
 - **Vantaggi:**
 - Facile da configurare.
 - Compatibile con molti dispositivi e sistemi operativi.
 - **Svantaggi:**
 - Considerato non sicuro per standard moderni.
 - Vulnerabile ad attacchi di forza bruta e decrittazione.
-

2. L2TP (Layer 2 Tunneling Protocol):

- **Caratteristiche principali:**
 - Non fornisce la crittografia da solo, viene spesso usato insieme a IPSec.
 - Crea un tunnel sicuro per i dati.
 - **Vantaggi:**
 - Maggiore sicurezza rispetto a PPTP (quando abbinato a IPSec).
 - Compatibile con molti dispositivi.
 - **Svantaggi:**
 - Richiede più risorse di calcolo per l'uso combinato con IPSec.
 - Può essere bloccato da firewall che bloccano il protocollo UDP.
-

3. IPSec (Internet Protocol Security):

- **Caratteristiche principali:**
 - Garantisce la sicurezza a livello IP.
 - Utilizza algoritmi di crittografia avanzati (es. AES).
 - Può essere usato in due modalità: Transport Mode (solo i dati sono crittografati) o Tunnel Mode (intero pacchetto IP crittografato).
 - **Vantaggi:**
 - Altamente sicuro e flessibile.
 - Adatto per connessioni site-to-site.
 - **Svantaggi:**
 - Complesso da configurare.
 - Richiede hardware compatibile.
-

4. OpenVPN:

- **Caratteristiche principali:**
 - Basato su SSL/TLS per la crittografia.
 - Open source, quindi è altamente configurabile e trasparente.
 - Supporta sia UDP che TCP.
 - **Vantaggi:**
 - Altissima sicurezza.
 - Difficile da bloccare da firewall.
 - Ampia compatibilità con dispositivi e piattaforme.
 - **Svantaggi:**
 - Configurazione iniziale complessa.
 - Richiede risorse di calcolo elevate rispetto a protocolli più semplici.
-

5. WireGuard:

- **Caratteristiche principali:**
 - Protocollo VPN moderno e leggero.
 - Utilizza algoritmi crittografici avanzati (es. Curve25519).
 - Architettura semplice con solo 4.000 righe di codice, rispetto alle decine di migliaia di OpenVPN e IPSec.
- **Vantaggi:**

- Prestazioni elevate.
 - Facilità di configurazione.
 - Sicurezza eccellente grazie a un design minimalista e auditabile.
- **Svantaggi:**
 - Meno compatibile con sistemi legacy.
 - Relativamente nuovo, quindi meno maturo rispetto ad altri protocolli.

Comparazione dei protocolli

Protocollo	Sicurezza	Velocità	Facilità di configurazione	Compatibilità
PPTP	Bassa	Alta	Molto facile	Ampia
L2TP/IPSec	Alta	Media	Moderata	Ampia
IPSec	Molto alta	Media	Complessa	Moderata
OpenVPN	Molto alta	Media	Complessa	Ampia
WireGuard	Molto alta	Molto alta	Facile	Limitata

Utilizzo pratico dei protocolli

- **PPTP:** per accessi VPN casalinghi dove la sicurezza non è critica.
- **L2TP/IPSec:** per VPN aziendali con un livello di sicurezza moderato.
- **IPSec:** per connessioni VPN site-to-site tra filiali aziendali.
- **OpenVPN:** per VPN personali o aziendali dove la sicurezza è fondamentale.
- **WireGuard:** per VPN moderne e ad alte prestazioni, come connessioni mobili.

Esempio pratico: Configurazione di una VPN usando OpenVPN e WireGuard

Scenario:

- Una piccola azienda ha due uffici, uno a Milano e uno a Roma. Entrambi gli uffici devono comunicare in modo sicuro attraverso una VPN.
- Scopo: Configurare due protocolli VPN (OpenVPN e WireGuard) per garantire comunicazioni sicure tra i dispositivi dei due uffici.

Configurazione con OpenVPN

Passaggi:

1. **Server VPN a Milano:**
 - Installare OpenVPN sul server (es. Ubuntu):

```
bash
```



```
Copia codice
sudo apt-get update
sudo apt-get install openvpn
```

- o **Generare le chiavi e i certificati SSL/TLS:**

```
bash
Copia codice
./easyrsa init-pki
./easyrsa build-ca
./easyrsa gen-req server nopass
./easyrsa sign-req server server
```

- o **Configurare il file del server /etc/openvpn/server.conf:**

```
plaintext
Copia codice
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
```

- o **Avviare il server OpenVPN:**

```
bash
Copia codice
sudo systemctl start openvpn@server
```

2. Client VPN a Roma:

- o Installare OpenVPN sul dispositivo client.
- o Copiare i file di configurazione e certificati dal server al client.
- o Connettere il client al server:

```
bash
Copia codice
sudo openvpn --config client.ovpn
```

Configurazione con WireGuard

Passaggi:

1. Server VPN a Milano:

- o Installare WireGuard:

```
bash
Copia codice
sudo apt-get install wireguard
```

- o **Generare chiavi pubbliche e private:**

```
bash
Copia codice
```

```
wg genkey | tee privatekey | wg pubkey > publickey
```

- Configurare il file /etc/wireguard/wg0.conf:

```
plaintext
Copia codice
[Interface]
PrivateKey = <chiave_privata_server>
Address = 10.0.0.1/24
ListenPort = 51820

[Peer]
PublicKey = <chiave_pubblica_client>
AllowedIPs = 10.0.0.2/32
```

- Avviare WireGuard:

```
bash
Copia codice
sudo wg-quick up wg0
```

2. Client VPN a Roma:

- Installare WireGuard.
- Configurare il file /etc/wireguard/wg0.conf:

```
plaintext
Copia codice
[Interface]
PrivateKey = <chiave_privata_client>
Address = 10.0.0.2/24

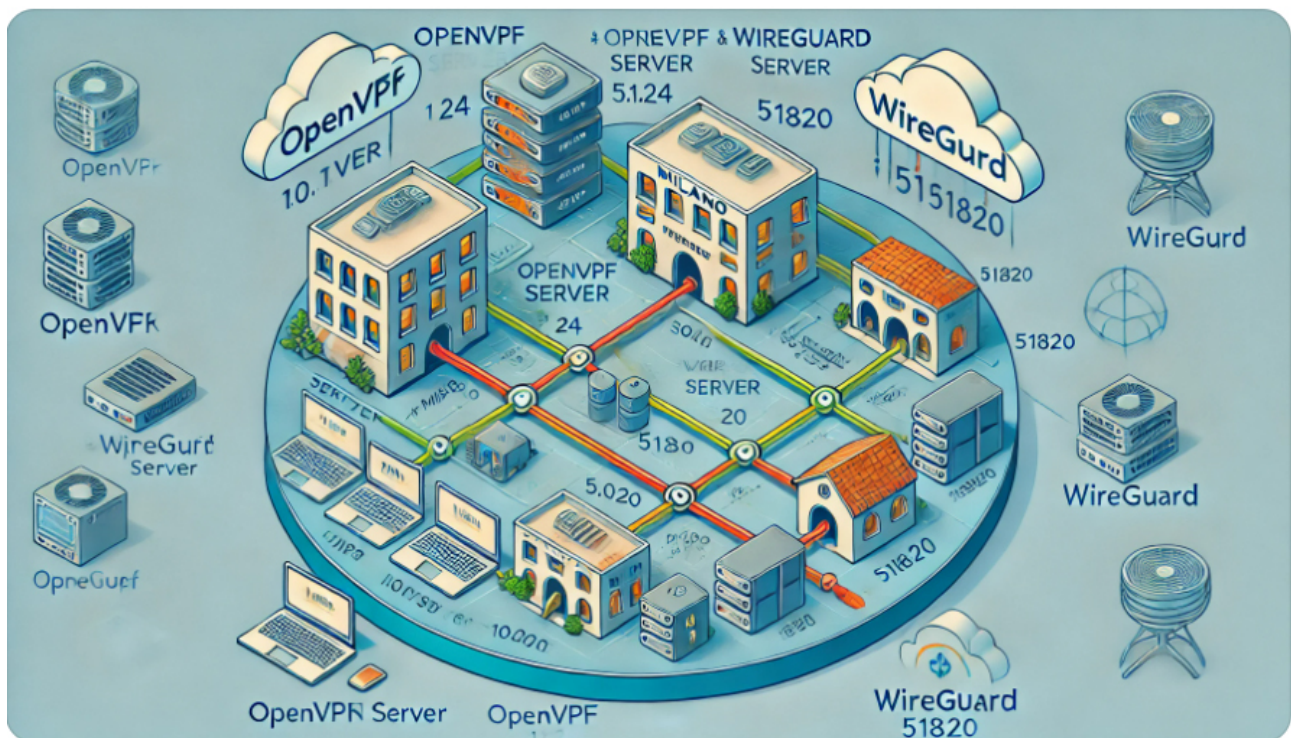
[Peer]
PublicKey = <chiave_pubblica_server>
Endpoint = <IP_del_server>:51820
AllowedIPs = 0.0.0.0/0
```

- Avviare WireGuard:

```
bash
Copia codice
sudo wg-quick up wg0
```

Schema dell'esempio

- **OpenVPN:**
 - Milano e Roma si connettono tramite un server centrale usando chiavi SSL/TLS.
 - Usa la porta **1194 UDP**.
- **WireGuard:**
 - Comunicazione diretta tra Milano e Roma con chiavi pubbliche e private.
 - Usa la porta **51820 UDP**.



Configurazione VPN tra due uffici utilizzando OpenVPN e WireGuard

Approfondimento argomento 4

Sicurezza nella VPN: crittografia, autenticazione e integrità dei dati

Approfondimento

La sicurezza è il cuore di ogni VPN. Una VPN garantisce che i dati trasmessi tra i dispositivi siano protetti da intercettazioni e manipolazioni, utilizzando tre pilastri principali:

1. Crittografia

La crittografia assicura che i dati trasmessi siano leggibili solo da chi possiede la chiave corretta. Ecco come funziona:

- **Simmetrica:** Una chiave unica è condivisa tra il mittente e il destinatario. Es.: AES (Advanced Encryption Standard).
- **Asimmetrica:** Una coppia di chiavi pubblica e privata. La chiave pubblica cifra i dati, e la chiave privata li decifra. Es.: RSA.

Esempio:

- Se un dipendente invia un'email attraverso una VPN, i dati vengono cifrati con AES a 256-bit. Anche se qualcuno intercetta i dati, non può leggerli senza la chiave.

2. Autenticazione

Garantisce che solo utenti autorizzati possano accedere alla rete VPN. Ci sono diversi metodi:

- **Certificati digitali:** Rilasciati da una certificazione, attestano l'identità di un utente o dispositivo.
- **Autenticazione basata su password:** Metodo semplice ma meno sicuro.
- **Autenticazione a due fattori (2FA):** Combina password e un secondo elemento (es. token o app).

Esempio:

- Un'azienda utilizza 2FA per la sua VPN: l'utente accede con una password e un codice generato dal proprio telefono.

3. Integrità dei dati

Questa tecnica garantisce che i dati non siano stati modificati durante il transito. Si basa su:

- **Hashing:** Utilizzo di funzioni di hash crittografico (es. SHA-256) per generare un'impronta digitale del messaggio. Se il messaggio cambia, cambia anche l'impronta.
- **Protocollo IPsec:** Include algoritmi per verificare l'integrità.

Esempio:

- Se un file viene trasmesso tramite VPN e un attacco MITM (Man-In-The-Middle) lo modifica, l'algoritmo di hash segnala che i dati sono corrotti.

Conclusione

Grazie alla crittografia, all'autenticazione e al controllo di integrità, una VPN assicura che i dati siano privati, inviati da fonti affidabili e integri. Questi strumenti sono fondamentali per proteggere sia gli utenti domestici sia le aziende.

Esempio pratico: Sicurezza in una VPN aziendale

Un'azienda utilizza una VPN per consentire ai dipendenti di accedere al server aziendale da remoto. Per garantire la sicurezza:

1. **Crittografia:**
 - Quando un dipendente invia dati, ad esempio un report aziendale, il client VPN cifra i dati con AES a 256-bit. Anche se i dati vengono intercettati da un hacker, non possono essere decifrati senza la chiave di crittografia.
2. **Autenticazione:**
 - Il dipendente accede alla VPN utilizzando un sistema di autenticazione a due fattori (2FA): inserisce la password del proprio account e un codice temporaneo ricevuto sull'app di autenticazione del telefono. Solo dopo entrambe le verifiche può accedere alla rete aziendale.
3. **Integrità dei dati:**

- Quando il report arriva al server aziendale, il sistema verifica l'hash crittografico dei dati. Se il report è stato modificato durante il trasferimento, l'hash non corrisponderà, e il server rifiuterà il file.

Scenario Rappresentato

1. Il dipendente si connette alla VPN dal proprio laptop.
2. La connessione è crittografata con AES.
3. L'autenticazione avviene tramite 2FA.
4. I dati vengono inviati al server aziendale e verificati per garantire l'integrità.



Funzionamento della VPN in un contesto aziendale:

crittografia, autenticazione a due fattori e verifica dell'integrità dei dati

TIPI DI VPN

Trusted VPN – Secure VPN – Hybrid VPN

Una **Trusted VPN** (Virtual Private Network fidata) si basa sull'utilizzo di reti fornite da un operatore o un provider di servizi di telecomunicazione che garantisce l'affidabilità e la sicurezza del canale di comunicazione, anziché implementare una crittografia end-to-end come nelle Secure VPN. Questo approccio si appoggia alla fiducia nei dispositivi, nella rete e nel provider che gestisce il traffico.

Caratteristiche principali di una Trusted VPN:

1. **Uso di protocolli standard:**
 - o La sicurezza è garantita dall'infrastruttura del provider di rete, non da crittografia aggiuntiva. Il provider può implementare protocolli come MPLS (Multiprotocol Label Switching) per separare il traffico delle diverse organizzazioni.
2. **Meno overhead di crittografia:**
 - o Poiché i dati non vengono cifrati a livello dell'utente finale, non ci sono ritardi dovuti all'elaborazione crittografica.
3. **Gestione centralizzata:**
 - o Il provider della rete è responsabile della configurazione e della manutenzione delle connessioni VPN.
4. **Sicurezza basata su segmentazione:**
 - o Il traffico di una Trusted VPN è isolato rispetto ad altri flussi, evitando interferenze o accessi non autorizzati.
5. **Utilizzo tipico:**
 - o Molto utilizzate in ambiti aziendali con più filiali, dove la connessione è garantita dal provider per trasferimenti interni.

Limiti di una Trusted VPN:

- **Dipendenza dal provider:** Il livello di sicurezza è legato alla fiducia nel provider, che potrebbe rappresentare un rischio se compromesso.
- **Mancanza di crittografia a livello utente:** I dati, se intercettati fuori dalla rete controllata, potrebbero non essere protetti.
- **Costo elevato:** Spesso i provider applicano costi superiori rispetto alle Secure VPN che sfruttano Internet pubblico.

Differenze con una Secure VPN:

Caratteristica	Trusted VPN	Secure VPN
Sicurezza	Basata sull'isolamento della rete	Basata sulla crittografia
Configurazione	Gestita dal provider	Gestita dall'utente/azienda
Prestazioni	Generalmente più rapide	Leggermente più lente per crittografia
Rischio di intercettazione	Legato alla rete del provider	Protetto da crittografia

Esempio pratico:

Immagina un'azienda con due sedi (Roma e Milano). La Trusted VPN, offerta dal provider tramite MPLS, garantisce che le comunicazioni tra le due sedi viaggino in un canale dedicato e isolato dal resto del traffico pubblico.



Trusted VPN basata su una linea dedicata MPLS tra due uffici aziendali, con una connessione sicura e isolata tramite un provider di servizi Internet (ISP)