VPN - Virtual Private Network

Cos’è la VPN e come funziona?

La VPN è una connessione sicura fra sedi aziendali, o fra utente remoto e rete aziendale.

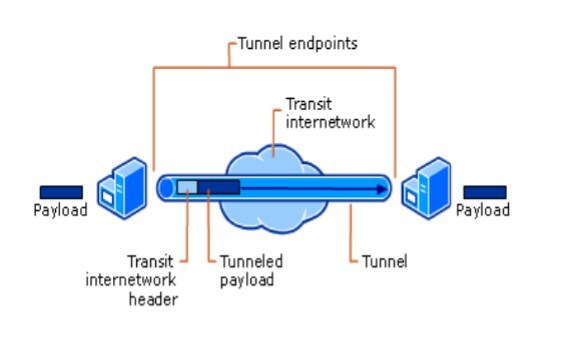
Globalizzazione, decentramento, lavoro da casa, partnership tra aziende sono alcuni dei fattori che hanno determinato un forte incremento della richiesta di connettività.

Le soluzioni tradizionali, come l'affitto di linee dedicate e il collegamento diretto via modem (dial-up) alle reti aziendali, erano molto costose così sono nate le reti private virtuali o VPN, con lo scopo di realizzare connessioni private attraverso una rete pubblica, o più precisamente Internet.

Questo ha portato un enorme risparmio in canoni e attrezzature. Internet però è il più insicuro degli ambienti di comunicazione, quindi sono state sviluppate diverse tecnologie per rendere sicure le connessioni attraverso la rete.

La maggior parte delle VPN infatti è realizzata attraverso il tunneling in combinazione con funzioni di autenticazione e cifratura.

Tunneling

Tunneling è il concetto di creare un tunnel, attraverso una rete pubblica insicura, come Internet, dentro il quale convogliare il traffico privato, al riparo da intercettazioni e manomissioni.

Sia pure con molte varianti e complicazioni, di base il tunneling è realizzato prendendo ogni pacchetto di dati e inserendolo dentro un altro pacchetto (il tunnel) è possibile creare una forma una corazza protettiva, nascondendo così tutto o parte del pacchetto originario tramite cifratura.

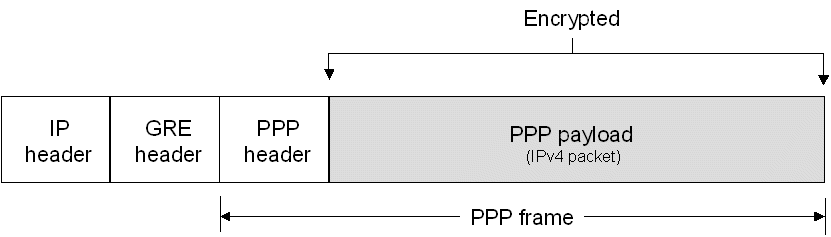
Utilizzo

I due impieghi principali di una VPN sono per collegare due sedi di un'azienda (connessione site-to-site) o per collegare un utente remoto alla rete aziendale (connessione remote access). Il primo caso si estende alla connessione tra aziende partner, per esempio per avere accesso permanente a informazioni tecniche, scorte, listini, contabilità.

In generale, un dispositivo VPN (hardware o software) funge da server e un altro funge da client e stabilisce la connessione con il server. I principali protocolli VPN utilizzati sono PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) e IPSec (Internet Protocol Security).

Oggi IPSec è la tecnologia più sicura per realizzare una VPN. PPTP è stato sviluppato da Microsoft e da altri produttori nel '96; non è uno standard e nel corso degli anni ha dimostrato di essere ampiamente insicuro. Non è quindi adatto per connessioni permanenti, ma si presta per connessioni occasionali.

Protocolli principali per le Virtual Private Network

PPTP

Il protocollo PPTP è nato come estensione del Point-to-Point Protocol (PPP), il protocollo più usato per collegarsi a un Internet Service Provider (ISP) via modem e una normale linea telefonica.

Un frame (pacchetto) PPP è formato dal pacchetto IP con l'aggiunta dell'intestazione PPP. Ora, per inserire il frame PPP dentro il tunnel protettivo, si prende il pacchetto PPP, se ne cifra la parte dati con il protocollo MPPE di Microsoft (la cifratura non fa parte del PPTP ma è normalmente eseguita) e si aggiungono due intestazioni: quella GRE (Generic Routing Encapsulation) e una nuova intestazione IP per inoltrare il pacchetto verso la destinazione.

Questa azione di inserire un pacchetto dentro un altro si chiama incapsulazione (da cui il nome del protocollo GRE). Ora al pacchetto IP (strato 3, Rete, del modello OSI) basta aggiungere l'intestazione propria del mezzo di connessione (strato 2, Data Link, per esempio Ethernet o wireless) e passare il frame allo strato fisico (cavo, onde radio, ecc) per la trasmissione verso il destinatario.

L2TP

Il protocollo L2TP, a differenza del protocollo [PPTP](https://it.wikipedia.org/wiki/PPTP), non dipende dalle tecnologie di crittografia specifiche di ciascun fornitore, per l'autenticazione dell'utente. Il funzionamento avviene al livello 2 della [pila ISO/OSI](https://it.wikipedia.org/wiki/Pila_ISO/OSI), ma di fatto è un protocollo che agisce al livello 5. Utilizza ufficialmente la porta [UDP](https://it.wikipedia.org/wiki/User_Datagram_Protocol) 1701. In realtà L2TP non fornisce alcuna sicurezza di per sé e deve essere usato insieme ad altri protocolli di autenticazione e criptazione. In genere si usa [IPsec](https://it.wikipedia.org/wiki/IPsec" \o "IPsec) che fornisce sia l'autenticazione che la criptazione. La combinazione di questi protocolli è nota come L2TP/[IPsec](https://it.wikipedia.org/wiki/IPsec" \o "IPsec).

Gli estremi di una connessione L2TP sono chiamati LNS (L2TP Network Server) e LAC (L2TP Access Concentrator). LNS è il [server](https://it.wikipedia.org/wiki/Server) che attende le connessioni, il LAC inizia la connessione. Una volta stabilita la connessione, il traffico potrà passare bidirezionalmente al suo interno, come in una galleria. A questo punto è possibile far transitare dei protocolli più evoluti all'interno del tunnel che abbiamo creato. In genere per fare questo si usa il protocollo [PPP](https://it.wikipedia.org/wiki/Point-to-Point_Protocol). L2TP permette di instradare più [VPN](https://it.wikipedia.org/wiki/Virtual_Private_Network) all'interno dello stesso tunnel.

IPSec

IPsec è stato progettato per rendere sicure sia comunicazioni portal-to-portal sia comunicazioni  end-to-end. Nella prima configurazione il traffico viene reso "sicuro" a diversi computer (in alcuni casi ad un'intera [LAN](https://it.wikipedia.org/wiki/LAN)); nella seconda solo i peer che stabiliscono la connessione scambiano pacchetti protetti. Tuttavia l'uso predominante di IPsec è la creazione di VPN ([virtual private network](https://it.wikipedia.org/wiki/Virtual_private_network" \o "Virtual private network)); per conseguire tale scopo possono essere utilizzati entrambi i metodi prima esposti. IPsec è una collezione di [protocolli](https://it.wikipedia.org/wiki/Protocollo_di_rete) formata da:

* Protocolli che implementano lo scambio delle chiavi per realizzare il flusso crittografato.
* Protocolli che forniscono la cifratura del flusso di dati.

Tipi di VPN (Remote Access/Site-to-Site)

Remote Access

Una Remote Access VPN permette di stabilire connessioni sicure alla LAN aziendale remota. Gli utenti possono accedere direttamente alle risorse della rete protetta come se fossero direttamente collegati alla rete stessa. Per realizzare un accesso di tipo remoto c’è bisogno di un server di accesso alla rete ovvero un NAS (Network Access Server).

Può essere sia un server dedicato o un applicazione software su un server condiviso. Il NAS chiede all’ utente di inserire credenziali valide per accedere alla VPN e o si avvale del proprio processo di autenticazione o si avvale di un serve AAA cioè un server che si occupa di confermare chi sei (Authentication), identifica ciò che ti è permesso vedere (Authorization) e tiene traccia di ciò che fai (Accounting).

Oltre al NAS c’è anche bisogno di un software VPN client che permette il collegamento vero e proprio con la rete.

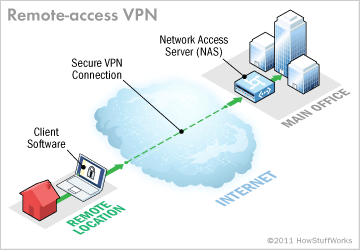
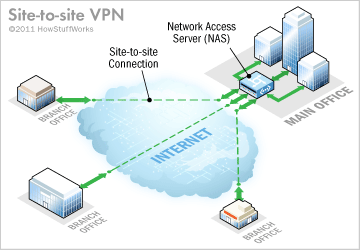
Site-to-Site

La VPN site-to-site è un tipo di connessione VPN creata tra due ubicazioni separate.

Offre la possibilità di connettere posizioni o reti geograficamente separate, di solito tramite la connessione Internet pubblica o una connessione WAN.

Le VPN site-to-site creano in una connessione diretta, non condivisa e sicura tra due endpoint e possono essere basate su Intranet o Extranet. La VPN site-to-site basata su Intranet viene creata tra le reti di proprietà di un'organizzazione, mentre la VPN site-to-site basata su extranet viene utilizzata per la connessione con reti di partner esterni o una rete intranet.

La connessione in una VPN site-to-site è generalmente abilitata tramite un dispositivo gateway VPN.



Tipi di VPN in base ai protocolli e al grado di sicurezza che offrono

Trusted VPN

La garanzia che offre la rete Trusted VPN è la sicurezza che nessun terzo non autorizzato possa usufruire del circuito del cliente. Questo implica che il cliente abbia un proprio [indirizzo IP](https://it.wikipedia.org/wiki/Indirizzo_IP) e una propria politica di sicurezza.

Il circuito viaggia attraverso uno o più "interruttori" di comunicazione che possono essere compromessi da chi vuole disturbare il [traffico](https://it.wikipedia.org/wiki/Traffico_(telecomunicazioni)) della rete. Il cliente di una VPN si aspetta quindi che il fornitore (*provider*) della VPN mantenga l'integrità del circuito in modo da impedire l'accesso di intrusi.

Le aziende che utilizzano una Trusted VPN vogliono avere la sicurezza che i loro dati si muovano attraverso una serie di percorsi che hanno proprietà specifiche e che sono controllati da un ISP ([Internet Service Provider](https://it.wikipedia.org/wiki/Internet_Service_Provider)). Il cliente ha quindi fiducia che i percorsi attraverso i quali questi dati si muovono siano mantenuti sicuri secondo i criteri di un precedente accordo, anche se generalmente il cliente non conosce quali siano i percorsi utilizzati dal fornitore della VPN Trusted.

Più recentemente i fornitori di servizio hanno cominciato a offrire un nuovo tipo di Trusted VPN, questa volta usando Internet invece della [rete telefonica](https://it.wikipedia.org/wiki/Rete_telefonica) come substrato di comunicazione. Queste nuove Trusted VPN non offrono sicurezza, ma danno ai clienti un modo di creare facilmente segmenti di rete su vasta scala ([WAN](https://it.wikipedia.org/wiki/Wide_Area_Network)). I segmenti Trusted VPN possono essere inoltre controllati da un posto unico e spesso con una [qualità di servizio](https://it.wikipedia.org/wiki/Qualit%C3%A0_di_servizio) garantita (QoS - *quality of service*) dal provider.

Secure VPN

I fornitori di connettività hanno cominciato a creare protocolli che permettessero la cifratura dei dati da parte della rete o da parte del [computer](https://it.wikipedia.org/wiki/Computer) di provenienza, in modo da essere trasportati in Internet come qualsiasi altro dato, per poi essere decifrati all'arrivo nella rete dell'azienda o nel computer ricevente.

Questo traffico cifrato agisce come un "[tunnel](https://it.wikipedia.org/wiki/Tunneling)" tra due reti: anche se un intruso cercasse di leggere i dati non potrebbe decifrarne il contenuto né modificarli, dato che eventuali modifiche sarebbero immediatamente rilevate dal ricevente e quindi respinte. Le reti costruite utilizzando la cifratura dei dati sono chiamate Secure VPN.

Il motivo principale per cui le società usano una Secure VPN è che possono trasmettere informazioni delicate su Internet senza temere che vengano intercettate.

Le Secure VPN sono particolarmente utili per permettere accessi remoti da parte di utenti connessi a Internet da zone non controllate dall'[amministratore di rete](https://it.wikipedia.org/wiki/Amministratore_di_rete).

Hybrid VPN

Sono un ibrido tra le due precedenti tipologie, ne offre i vantaggi di entrambe in quanto:

* le Secure VPN danno sicurezza, ma non assicurano i percorsi;
* le Trusted VPN assicurano le proprietà dei percorsi come QoS, ma non la sicurezza da intrusioni.

A causa di questi punti di forza e di debolezza sono state introdotte le Hybrid VPN. Gli scenari di utilizzazione sono tuttavia ancora in evoluzione. Una situazione tipica per il dispiegamento di una Hybrid VPN è quando un'azienda ha già una Trusted VPN e desidera sicurezza su una parte della VPN.

Perché avere una VPN? Pro & Contro

### Pro: la sicurezza

Spesso navighiamo e **distribuiamo i nostri dati in giro per la rete**, una VPN dovrebbe per costruzione **criptare completamente il vostro traffico di rete** prima di trasmetterlo in sicurezza via Internet. Questo è il motivo per cui le aziende utilizzano spesso delle VPN per permettere ai propri dipendenti l’accesso ai dati delle compagnia.

### Evitare blocchi e restrizioni regionali

Visto che le VPN instradano il vostro traffico attraverso una rete, ovviamente sembrerà che tutti  i componenti della rete privata siano connessi ad Internet dallo stesso luogo, che sarà di solito **molto diverso dalla vostra posizione**. E’ quindi la soluzione più semplice per aggirare le**restrizioni geografiche**, alcuni siti come Netflix hanno sempre limitato l’accesso ad alcuni mercati, e moltissimi utenti hanno aggirato il blocco. Di recente anche il governo cinese ha cercato di bloccare e regolamentare le VPN visto che erano il modo preferito dei cittadini del gigante asiatico per **eludere la censura** imposta dal governo.

### Facilità di scambio file fra PC in rete

### Essendo per architettura simile a una rete locale, una VPN si comporta esattamente alla stessa maniera. Quindi ogni client connesso, ha accesso ai dati della rete locale come se fosse nello stesso edificio. Questo è molto importante per le aziende sopratutto multinazionali che possono così fornire in sicurezza l’accesso ai dati sensibili ai dipendenti lontani.

### Contro: la velocità

Noi tutti apprezziamo le VPN perché criptano tutto il nostro traffico, ciò è anche la loro debolezza. Un maggiore livello di codifica in genere implica un maggiore utilizzo di risorse hardware e quindi in genere maggiori**tempi di attesa per l’invio e la ricezione delle informazioni**. Tutto ciò rallenta inevitabilmente la connessione, tanto che gran parte delle VPN è abbastanza lento.

Complessità della rete Più un servizio VPN è serio più di solito la rete su cui si basa è complessa. Ciò di solito è fatto con l’intento di assicurare una rete più robusta e resistente agli attacchi. Purtroppo però una maggiore complessità non è sempre un vantaggio, in quanto rende più opachi e meno trasparenti tutti i nodi che i vostri dati attraversano.

Linkopedia

Video Spiegazione VPN

<https://www.youtube.com/watch?v=AjzomZt1EZY>

FINE, Grazie per l’attenzione !!!