

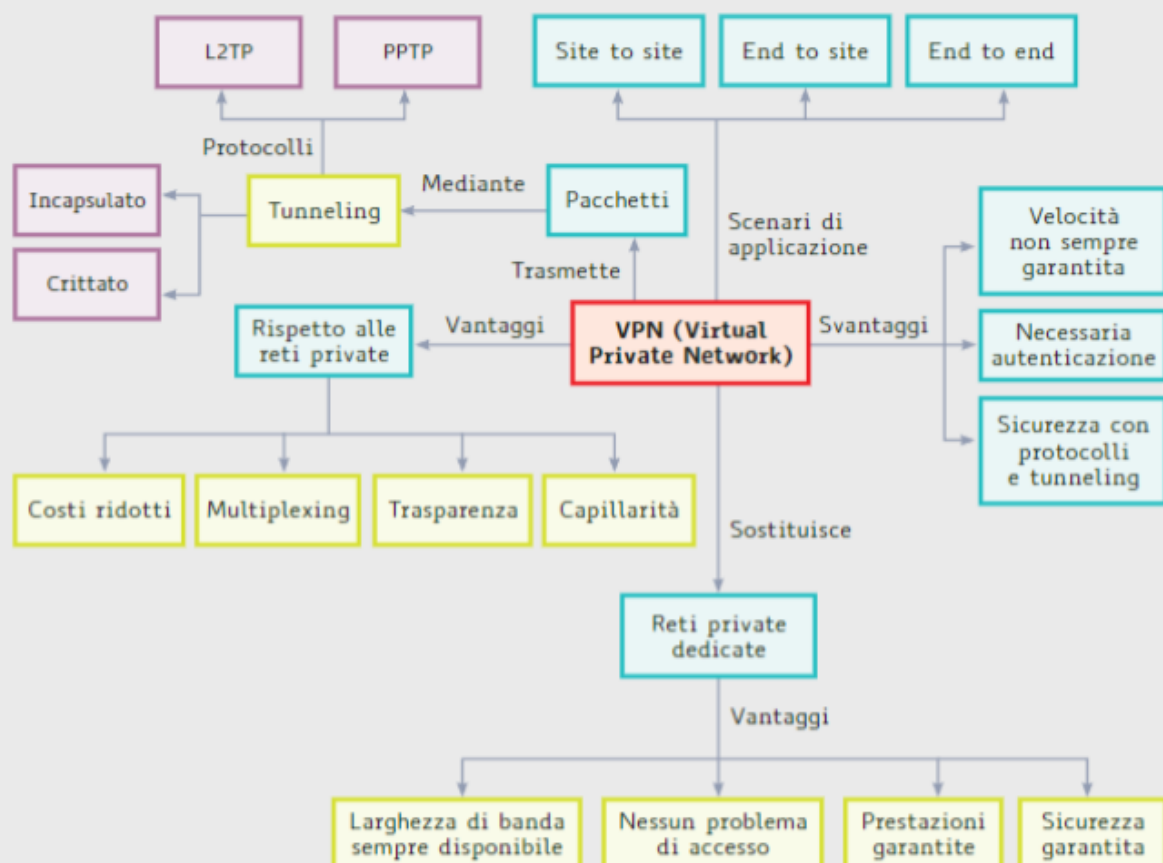
LEZIONE 3

3 Reti private virtuali (VPN)

IN QUESTA LEZIONE IMPAREREMO...

- riconoscere il campo di utilizzo di una VPN
- a riconoscere le differenze tra VPN e Proxy
- a individuare le caratteristiche delle VPN

MAPPA CONCETTUALE



Virtual Private Network

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.



Per poter applicare una rete privata virtuale è necessario che all'interno della stessa VPN l'indirizzamento sia unico, cioè i nodi appartengano alla stessa rete.

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.

Differenze tra reti private dedicate e VPN

Le reti **private dedicate**, che potremmo definire reti private "vere e proprie", collegano più siti di una rete aziendale attraverso canali dedicati, a uso esclusivo, pagandone l'affitto al proprietario o gestore. Possiedono alcuni vantaggi tra i quali citiamo:

- larghezza di banda sempre disponibile;
- nessun problema di accesso;
- prestazioni garantite;
- sicurezza garantita.



Le reti **private dedicate** sono ottimizzate per ottenere le migliori prestazioni possibili, ma non per garantire l'efficienza della rete, e possiedono un rapporto costi/benefici non sempre elevato.

Inoltre le reti private "vere e proprie" possiedono elevati costi per l'installazione e la manutenzione, oltre a tempi lunghi per configurazione e riconfigurazione, in quanto non sono scalabili e incorrono spesso in rischi tra i quali il blocco della rete in caso di grave guasto su un canale.

Le **reti private virtuali (VPN)** invece sono configurabili e riconfigurabili facilmente, inoltre sono scalabili e offrono un valido rapporto tra costi e funzionalità. Inoltre utilizzando come mezzo di trasmissione la rete pubblica, abbiamo un alto grado di ridondanza che è una garanzia contro il rischio di blocco della rete, che è praticamente zero. In sintesi, le **VPN**, rispetto alle reti private dedicate, possiedono i seguenti vantaggi:


- costi ridotti, in quanto vi è una sola infrastruttura da gestire;
- multiplexing dei canali logici;
- trasparenza, in quanto il gestore della rete pubblica potrebbe anche non essere a conoscenza della VPN;
- capillarità con supporto per sedi remote e utenti mobili.



Tuttavia la natura stessa della VPN, che la rende condivisa, implica tre problematiche, legate a:

- velocità di trasmissione non sempre garantita, dovuta al traffico della rete pubblica, alla latenza e alla perdita di pacchetti;
- autenticazione necessaria per controllo degli accessi;
- sicurezza delle trasmissioni con protocolli e tecniche di cifratura e tunneling.

Tunneling

Il **tunneling**  rappresenta il processo di trasmissione di informazioni riservate attraverso una rete pubblica in modo tale che i nodi che appartengono alla rete pubblica siano inconsapevoli del fatto che il processo di trasmissione faccia parte della rete privata. I dati vengono suddivisi in sezioni di dimensioni ridotte, chiamate pacchetti, che vengono trasmessi nel tunnel fino a destinazione. Durante il tragitto nel tunnel i pacchetti vengono **crittati** e **incapsulati**. I dati della rete privata e il protocollo sono anch'essi incapsulati in unità di trasmissione di rete pubblica. Ovviamente il ricevente deve effettuare una decapsulazione e decrittazione per ri-ottenere i dati originali. Gli strati di **tunneling VPN** possono essere creati ai seguenti livelli dell'interconnessione:

Livello 2: strato di collegamento dati

I protocolli VPN che operano in questo livello sono il protocollo di **tunneling** punto a punto e il protocollo di tunneling del livello 2.

Livello 3: livello di rete

IPSec può operare come protocollo VPN a livello di rete del modello di riferimento OSI.

I **protocolli** coinvolti nel processo di **tunneling** sono invece i seguenti:

– Protocollo PPTP (Point to Point Tunneling Protocol)

In questo protocollo i dati vengono mantenuti al sicuro anche se comunicati su reti pubbliche. Gli utenti autorizzati possono accedere a una rete privata che viene chiamata rete privata virtuale o **VPN** fornita da un provider di servizi Internet o **ISP**. Si tratta di una rete privata in senso virtuale perché è creata in un ambiente che viene incanalato. Questo protocollo permette alle aziende di estendere la propria rete aziendale attraverso un canale privato su Internet pubblico.

– Protocollo L2TP

Questo protocollo prevede la combinazione dell'utilizzo del **PPTP** e dell'inoltro a livello 2 ed è usato per supportare le **VPN** come parte di servizi **ISP**. In sé non fornisce crittografia e riservatezza di per sé stessa ma utilizza un protocollo di crittografia che passa all'interno del tunnel.

Scenari di applicazione di una VPN

Esistono principalmente tre scenari di applicazione delle **VPN** (reti **private virtuali** ):

- collegamento di due o più sedi aziendali attraverso una rete aperta (**site to site**);
- accesso alla rete aziendale da casa o da mobile (**end to site**);
- accesso remoto da un computer a un altro (**end to end**).



Tunneling

Il **tunneling** è un protocollo di comunicazione che permette lo spostamento di dati da una rete a un'altra. Consente di inviare comunicazioni private attraverso una rete pubblica, questo processo è chiamato **incapsulamento**. In questo processo di incapsulamento, i pacchetti di dati appaiono come se fossero di natura pubblica per una rete pubblica quando in realtà sono considerati pacchetti di dati privati. Questo permette loro di passare inosservati.



Private virtuali

Per **rete privata** si intende una rete che può anche non rispettare le regole delle reti pubbliche in termini di indirizzi IP e di routing, è isolata da sorgenti esterne e gli accessi sono esplicitamente configurati, garantendo privacy e autenticazione nelle comunicazioni. Per **rete virtuale** si intende una rete che possiede caratteristiche "reali" ed è formata da un sottoinsieme (**subset**) di nodi chiamati **overlay network**, cioè rete costruita sopra a un'altra. L'utente in tal modo non si accorge dell'esistenza dell'infrastruttura fisica: tipico esempio il **tunneling** dove avviene l'incapsulamento di un protocollo in un altro.



Rispetto ai **proxy**, che scambiano dati con la rete pubblica semplicemente **cambiando** l'indirizzo IP, le **VPN** **crittano** anche i dati, in modo che se intercettati non siano utilizzabili.

VPN site to site

Questo tipo di VPN, chiamato anche **VPN lan to lan**, si applica quando vi è la necessità di collegare più reti locali attraverso un **canale** di trasmissione **pubblico** su di una rete di comunicazione virtuale. Questa situazione potrebbe per esempio verificarsi quando vi è l'esigenza di stabilire un collegamento tra diverse aree aziendali, sedi distaccate o succursali.



In alternativa alla VPN in questo caso si potrebbe utilizzare una rete **CN** (**corporate network**) che sfrutta una connessione privata e fissa, generalmente da affittare a pagamento. Il collegamento tramite **VPN** invece, utilizzando la rete pubblica, comporta esclusivamente i costi di connessione Internet.

La struttura di una VPN **site to site** richiede la presenza di un **router VPN** per ciascuna sede, che rappresenta il **tunnel** VPN tra le reti locali.

VPN end to site

Le VPN **end to site**, chiamate anche VPN ad accesso remoto, trovano applicazione quando la rete aziendale deve essere accessibile da remoto o da casa. Il **tunnel** VPN tra la rete aziendale e il terminale dell'utente che si collega viene realizzato da un **client VPN**, e il canale è rappresentato dalla rete pubblica (Internet). Questo permette agli utenti remoti di accedere alla rete aziendale e quindi a server, grazie a una connessione Internet con semplice autenticazione.

VPN end to end

Quando l'accesso remoto non avviene su di una rete locale, ma solo da una postazione all'altra, tipicamente rappresentata da un computer, si parla di VPN **end to end**. Lo scenario di applicazione per questo tipo di connessione è il protocollo **remote desktop**, nel quale le applicazioni eseguite su di un computer vengono visualizzate e gestite da un altro dispositivo di elaborazione (computer). Il canale di trasmissione può essere Internet oppure una rete aziendale locale. In una rete aziendale, una VPN **remote desktop**, viene utilizzata quando per esempio un impiegato vuole accedere da casa al suo computer direttamente sulla postazione presente sul posto di lavoro.

VPN e sicurezza

Possiamo classificare le reti private virtuali in tre categorie, in base al grado di sicurezza offerto:

– Trusted VPN

Vengono anche chiamate **VPN di fiducia**, dove la sicurezza è affidata al **provider** (**ISP**) della rete pubblica. Essendo demandato il controllo sulla sicurezza all'**ISP**, le **Trusted VPN** assicurano le proprietà dei percorsi ma non garantiscono un alto livello di sicurezza.

– Secure VPN

I protocolli di cifratura e di tunneling utilizzati sono **IPsec** e **TLS/SSL**, che assicurano la cifratura dei dati ma non garantiscono le proprietà dei percorsi. Vengono attualmente adottati dai principali tipi di rete VPN in commercio, essendo la richiesta di riservatezza la caratteristica prioritaria nelle reti di questo tipo. In generale dal punto di vista della sicurezza le secure VPN sommano le caratteristiche delle reti

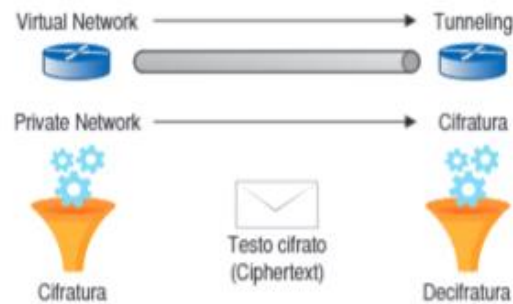


IPsec

Le fasi di comunicazione sicura con **IPsec** sono le seguenti:

- **connessione**: i due nodi della VPN si mettono in contatto tra di loro: il firewall del nodo 1 contatta il firewall del nodo 2 per stabilire una connessione **IPsec**;
- **encapsulation**: i pacchetti vengono crittografati per essere resi sicuri;
- **tunneling**: i pacchetti crittografati viaggiano su Internet per raggiungere l'altro capo della VPN;
- **check out**: durante il tragitto la VPN viene monitorata per assicurarne la sicurezza;
- **destinazione**: il pacchetto giunge a destinazione e viene decrittato.

private (**cifratura**) e di quelle virtuali (**tunneling**), garantendo appunto entrambe le caratteristiche (cifratura + tunneling).



– Hybrid VPN

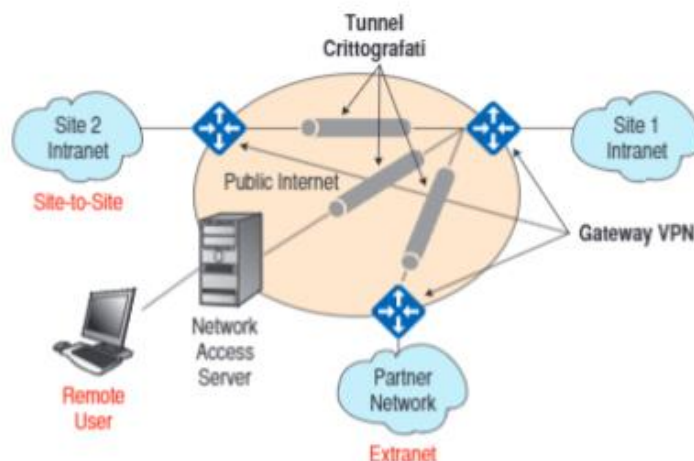
Si tratta di un tentativo di unire le caratteristiche di entrambe le reti VPN, come progetto di una rete virtuale sicura (**Secure VPN**) come sottoinsieme di una **Trusted VPN**.

Categorie d'uso delle VPN

Possiamo suddividere le **VPN** in tre principali **categorie d'uso**.

- **Remote access** (per lavoro remoto, piccoli uffici)
- **Intranet** (per sedi diverse della stessa organizzazione/società con traffico sostenuto e costante)
- **Extranet** (per organizzazione/società diverse con politiche di accesso)

Vediamo le operazioni che deve effettuare il gateway nei tre casi.



1. Remote access.


Una rete VPN di tipo **remote access**, chiamata anche **VPDN** (**Virtual Private Dial-up Network**), permette a un utente di connettersi da una postazione remota alla rete privata. Deve possedere due componenti indispensabili:

- **NAS** (**Network Access Server**): si tratta di un server di accesso alla rete che fornisce agli utenti un software di connessione che si collega alla VPN chiamando un numero gratuito. L'utente si deve autenticare con le proprie credenziali. In alternativa il NAS si può anche avvalere di un server **AAA**, cioè un server di autenticazione separato sulla rete.

- **software VPN client**: consente di connettersi alla VPN usando il proprio computer, in questo caso gli utenti necessitano di un software che stabilisce e mantiene la connessione. Per la sicurezza è necessario tuttavia dotare il sistema di un firewall, collocandolo tra la rete privata e Internet.



Nel caso del **remote access** il **gateway VPN** deve implementare l'allocazione dinamica di indirizzi (**DHCP**) ed effettuare:

- la crittografia di tutto il traffico con algoritmo **3-DES** a cifratura simmetrica con chiave unica;
- la generazione dinamica delle chiavi;
- il **tunneling ESP (Encapsulation Security Payload)** e **IKE** .
- la gestione del **Firewall**;
- la gestione di autenticazioni multiple con **RADIUS** e **certificati digitali**.

Deve inoltre consentire:

- l'accesso differenziato sulla base di identità e policy;
- l'accesso simultaneo da Internet e da intranet.



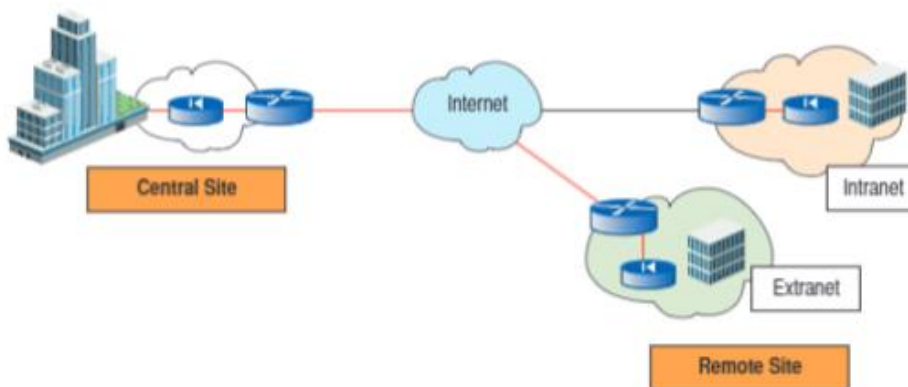
IKE

Il meccanismo di scambio delle chiavi per cifratura viene chiamato **IKE (Internet Key Exchange)**, ed è basato sull'**ISA-KMP (Internet Security Association and Key Management Protocol)**. Gli scopi di IKE sono principalmente:

- autenticare i due interlocutori;
- stabilire i protocolli e le chiavi segrete da utilizzare per trasferire i dati.

2. 3. Intranet ed extranet

Nelle categorie d'uso **intranet** ed **extranet**, abbiamo una **VPN di tipo site to site**, dove la società/organizzazione consente l'accesso remoto in larga scala. Estende la rete aziendale realizzando il concetto di **WAN** come insieme di **LAN**.



Nella categoria **intranet**, cioè Intra-aziendale, la comunicazione avviene esclusivamente tra i siti della stessa società/organizzazione, secondo il modello VPN **site to site**.

Nella categoria **extranet**, cioè inter-aziendale, la comunicazione avviene tra società/organizzazioni che hanno interessi comuni, sempre secondo il modello VPN **site to site**, con il problema tuttavia dell'univocità degli indirizzi.

Nel caso di **intranet** il **gateway VPN** deve effettuare:

- la crittografia di tutto il traffico con algoritmo **3-DES** a cifratura simmetrica con chiave unica;
- la generazione dinamica delle chiavi;
- fare comunicare le sottoreti tra loro tramite le **VPN** con incapsulamento per nascondere indirizzi privati, utilizzando **IPsec** in **Tunnel Mode** e aggregando il traffico;
- la gestione di **certificati digitali** per l'autenticazione reciproca tra ogni coppia di gateway con algoritmo **IKE** (scambio chiavi).

Nel caso di **extranet** il **gateway VPN** deve effettuare:

- la crittografia di tutto il traffico con algoritmo **3-DES** a cifratura simmetrica con chiave unica;
- la generazione dinamica delle chiavi;
- il **tunneling ESP** (**Encapsulation Security Payload**) e **IKE**.

La rete extranet può accedere solo a un sottoinsieme limitato di server interni mediante:

- filtri di accesso;
- **SPD** (**Security Policy Database**);
- più tunnel con la stessa extranet;
- autenticazione forte;
- certificati digitali.