# VPN: Virtual Private Network

Connessione realizzata su una **infrastruttura condivisa** in modo tale da poter **offrire funzionalità di rete presenti in reti private**. Es: Sicurezza, Qualità del servizio, affidabilità, indirizzamento  
*(Nella rete normale: il traffico va in giro nella rete e un dispositivo intermedio può leggerlo).*

Immagine che contiene testo, diagramma, schermata

Descrizione generata automaticamenteEsempio di uso: Dal mio pc di casa posso collegarmi al server con indirizzo privato presente al poli.   
 *(senza vpn per accedervi dovrei andare nel mio ufficio del poli)*Esempio: Creazione di tante lan interconnesse tra loro come se appartenessero alla stessa struttura fisica

**Elementi fondamentali:**

* **Tunnel:** incapsula in modo sicuro il traffico mentre è in transito sulla rete condivisa  
   *(non sempre presente)*
* **VPN Gateway:** dispositivo di terminazione sulla rete aziendale   
   (può essere endpoint di un tunnel)

Immagine che contiene testo, diagramma, calligrafia, disegno

Descrizione generata automaticamente**Esempio SENZA vs CON VPN**

**Immagine che contiene testo, calligrafia, disegno, diagramma

Descrizione generata automaticamente**Il primo VPN Gateway crea pacchetto aggiungendo un header con L2, IP e incapsulando il vecchio  
 🡪**TUNNELLING**   
Il secondo VPN Gateway estrae il pacchetto incapsulato e lo inoltra all’host.  
 *Con VPN la rete internet (router compresi) vede solo il pacchetto verde senza accorgersi dell’incapsulamento.*

**MOTIVAZIONI**

* Maggior **sicurezza**.
* **Autenticazione**: riesco a far accedere ai miei servizi solo le persone autenticate, emettere e configurare firewall in maniera più semplice.
* Permettono di abbattere i **costi** interconnettendo le varie sedi usando l’infrastruttura pubblica invece che creare una rete fisica privata.
* **Accesso da** **remoto**: permette connessione da remoto ai servizi attraverso vpn.

**TERMINOLOGIA**

**Autenticazione end-Point**: assicura chi/cosa dichiara di essere sia chi sia  
**Integrità dei dati**: garantisce che i dati non vengano manomessi durante il trasporto  
**Confidenzialità dei dati**: dati non devono essere letti da nessuno tranne che dalla destinazione *(crittografia)*  
**Separazione dei dati**: tunnelling

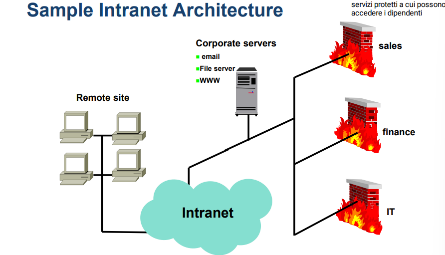
**Vari tipi VPN:**

* **Site-to-site VPN:** *ho due sedi della stessa azienda e le collego tramite tunnel🡪 GW---GW*
  + Immagine che contiene testo, Carattere, schermata, linea

    Descrizione generata automaticamenteConnette reti remote
  + Virtualizza la linea pubblica “affittata”
* **End-to-end VPN*:*** *ho un host che si college ad un altro host in assenza di vpn GW* ***🡪 Host fa da GW*** 
  + Immagine che contiene testo, Carattere, linea, schermata

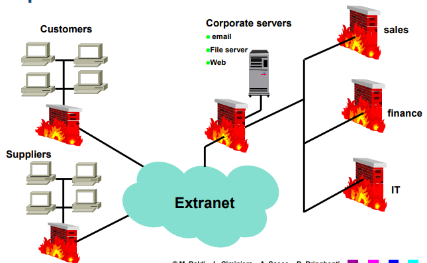
    Descrizione generata automaticamenteConnette host remoti  *H---H*
  + Virtualizza la linea pubblica “affittata”
* **Accesso a VPN o VPN remota o accesso virtuale:** *telelavoro🡪 host collegato a GW🡪 H---GW*
  + Immagine che contiene testo, Carattere, schermata, linea

    Descrizione generata automaticamenteConnette terminale a reti remote
  + Virtualizza accesso a connessione

Scenari VPN:

* **INTRANET VPN:** interconnessione dei diversi siti(luoghi) della mia azienda:

*headquarters(sedi), uffici remoti, telelavoratore, lavoratore in viaggio, varie filiali…*

* + Proteggo servizi 🡪 possono accedere solo i dipendenti
* **EXTRANET VPN:** interconnessione di clienti, fornitori, partner
  + Forniscono controllo sull’accesso di un singolo customer/partner/utente
  + Voglio anche evitare che i supplier accedano ai pc dei dipendenti

🡪devo proteggere anche server e pc dei customer

* + **Problematiche**:
    - * Restringere l’accesso alle sole persone autorizzate 🡪 firewall alle VPN
      * Controllare il traffico 🡪 evitare che il traffico del partner comprometta la rete dell’azienda
      * Range di indirizzi che possano sovrapporsi (Azienda A e azienda B possono aver assegnato gli stessi indirizzi locali ai loro PC) 🡪 gestire

**Tipologie di accesso ad internet:**

* **Immagine che contiene diagramma, testo, linea, schermata

  Descrizione generata automaticamenteCentralizzato:** 
  + raggiungo headquarters usando la rete IP pubblica con un tunnel
  + accesso ad internet tramite gli heaquarters
  + **dunque il pacchetto:**
    - --> parte dal mio pc
    - --> passa per la mia rete aziendale (RouterA =vpnGW)
    - --> va verso la destinazione e verso il servizio che volevo contattare
  + Immagine che contiene testo, diagramma, Piano, mappa

    Descrizione generata automaticamentePRO:
    - Sicurezza: se qualcuno fa sniffing tra routerA e Netflix,

legge IP del router A ma non il mio *perchè il router A*

*estrae il pacchetto nero e modifica ip del pacchetto nero*

*mettendo il suo ip (routerA) come indirizzo ip sorgente.*

*Successivamente* netflix risponde mandando il pacchetto

a router A, router A si ricorda che deve mandarlo al mio router grazie ad una tabella di connessioni attive

* + - Posso accedere ai servizi passando da altre nazioni
  + CONTRO:
    - Più lento
* Immagine che contiene testo, diagramma, Carattere, schermata

  Descrizione generata automaticamente**Distribuito:** usata per collegarsi alla rete aziendale da remoto --> se devo collegarmi a sede principale. *Se il servizio non è nella mia rete aziendale, il mio pacchetto va direttamente a netflix senza passare nella mia rete centrale.*
  + **PRO:** latenza bassa
  + **CONTRO:** perdo sicurezza, non c’è più tunnel

**TOPOLOGIE DELLE VPN** (collegazione tra i siti):

* **HUB and SPOKE**: rendo il mio HeadQuarter HUB --> ogni site/ramo crea un tunnel verso HUB
  + tutto il traffico va prima all'HUB e poi agli altri
  + pochi tunnel
  + hub può diventare collo di bottiglia
* **MESH**: creo dei tunnel tra i vari site --> più tunnel
  + Molti tunnel 🡪 difficile da configurare manualmente
  + Immagine che contiene testo, schermata, diagramma, linea

    Descrizione generata automaticamenteRouting ottimizzato

CONCETTI PER VALUTAZIONE

-deployment model: come deployo

* Overlay Model:
* Peer Model:

-provisioning: chi la fa

-protocol layer: a quale livello dello stack la sto mettendo