

Per realizzare in sicurezza una interconnessione tra reti locali, di un'unica organizzazione, geograficamente distanti attraverso il mondo Internet è essenziale mantenere il grado di riservatezza garantito dall'uso di una singola rete privata; la necessità di salvaguardare tali caratteristiche su una rete "non privata" gestita da un'ISP (Internet Service Provider) richiede soluzioni in grado di virtualizzarne il concetto.

Una rete in cui la riservatezza dei dati e l'accesso alle risorse sono ottenute non fisicamente ma mediante l'uso di protocolli e meccanismi condivisi da tutti i partecipanti viene denominata "**VPN (Virtual Private Network)**". Le VPN vengono classificate:

- **VPN a livello collegamento dati:** virtual circuit (VC) messi a disposizione da tecnologie come ATM e Frame Relay; le funzioni crittografiche sono spesso generalmente proprietarie.
- **VPN a livello rete IP-based:** il sistema crittografico è definito dall'architettura IPSEC, ma possono essere adottate anche soluzioni proprietarie veicolate tramite altri protocolli di "tunneling". Ogni tunnel viene trattato dal gateway come un'interfaccia virtuale punto-punto alla quale possono essere associate le route per più subnet IP private.
- **VPN a livello trasporto e applicazione:** associazione client / server sicure grazie a specifiche funzioni crittografiche introdotte a livello trasporto o applicazione (SSH, TLS).

Esistono diverse soluzioni per l'incapsulamento ed il **tunneling** di pacchetti IP privati su una rete TCP/IP; oltre ai protocolli che compongono IPSEC (AH ed ESP), le alternative per realizzare una rete VPN sono:

- **Tunnel GRE**
- **Tunnel PPTP**

Protocollo	Vantaggi	Svantaggi
PPTP	Nativo su windows da 98 a XP; Nativo sui palmari con windows CE	Medio/basso livello sicurezza; Di difficile impiego dietro a NAT
L2TP	Più versatile di PPTP; Nativo su windows 2000 ed XP; Disponibile come patch su windows 98/ME	Medio/basso livello sicurezza; Di difficile impiego dietro a NAT; Sarà supportato solo a partire da windows CE 2003
IPSec	Massimo livello sicurezza; Nativo su windows 2000 ed XP; Disponibile come patch su windows 98/ME	Richiede client proprietari per essere usato in modalità accesso remoto
L2TP/IPSec	Massimo livello sicurezza; Nativo su windows 2000 ed XP; Disponibile come patch su windows 98/ME; Può essere impiegato dietro NAT (nativo su windows XP tramite patch su windows 98).	Richiede una infrastruttura PKI; Maggiore impiego di risorse sui concentratori; Sarà supportato solo a partire da windows CE 2003.