VPN

Una Virtual Private Network (VPN) è una rete privata che sfrutta un'infrastruttura pubblica, come Internet, per collegare sedi aziendali, utenti remoti e partner in modo sicuro ed efficiente. L'obiettivo principale delle VPN è estendere la rete locale (LAN) su un'area geografica più ampia, creando una WAN privata senza la necessità di ricorrere a costosi collegamenti dedicati. Rispetto alle reti private tradizionali, che richiedono linee dedicate (come le leased line), le VPN offrono vantaggi significativi, come maggiore flessibilità, rapidità di configurazione e riconfigurazione, scalabilità per crescere insieme alle esigenze aziendali e costi ridotti. Tuttavia, poiché operano su reti pubbliche, le VPN devono affrontare sfide legate alla sicurezza, affidabilità e qualità del servizio (QoS).

2. Tipi di VPN

Le VPN si suddividono principalmente in due categorie, pensate per scopi differenti.

La **Remote-Access VPN** permette ai singoli utenti (ad esempio, dipendenti in smartworking) di connettersi alla rete aziendale da qualsiasi luogo. L'utente installa un client VPN sul proprio dispositivo, che stabilisce una connessione cifrata con un Network Access Server (NAS) o un server AAA (Authentication, Authorization, Accounting). Una volta autenticato, l'utente può accedere alle risorse aziendali come se fosse fisicamente in ufficio. Un esempio pratico è il venditore che accede al database aziendale da un hotel.

La **Site-to-Site VPN**, invece, collega intere sedi aziendali in modo sicuro, creando una rete unificata tra LAN. Può essere un'intranet VPN, quando collega sedi della stessa azienda, o un'extranet VPN, quando collega con partner, fornitori o clienti per condividere dati riservati. In questo caso, i router o firewall delle sedi stabiliscono un tunnel cifrato tra loro, senza necessità di un client VPN sui dispositivi individuali. Un esempio sarebbe un'azienda con uffici a Milano e Roma che condividono file e applicazioni tramite una connessione sicura.

3. Sicurezza nelle VPN

Poiché le VPN viaggiano su Internet, è essenziale che garantiscano riservatezza, integrità e autenticazione. La riservatezza impedisce che i dati vengano letti da estranei, l'integrità assicura che i dati non vengano modificati durante il trasferimento, e l'autenticazione garantisce che solo gli utenti autorizzati possano accedere. Per raggiungere questi obiettivi, le VPN utilizzano tre meccanismi fondamentali. L'**autenticazione** verifica l'identità di chi cerca di accedere alla VPN, tramite username e password, autenticazione a più fattori (MFA) che combina password con un codice temporaneo (come un SMS o un'app Authenticator), oppure certificati digitali usati nei protocolli SSL/TLS. La **cifratura** trasforma i dati in un

formato illeggibile senza la chiave corretta, utilizzando protocolli come IPsec (che usa algoritmi come AES e 3DES) o SSL/TLS (tipicamente utilizzato per le VPN basate su browser). Lo **scambio delle chiavi crittografiche** avviene tramite protocolli come IKE (Internet Key Exchange). Infine, il **tunneling** incapsula i pacchetti di dati in un altro protocollo per nasconderli durante il transito, con modalità di tunneling che possono essere "trasporto" (cifra solo il payload) o "tunnel" (cifra l'intero pacchetto, inclusi l'header IP).

4. Protocolli di Sicurezza Principali

Le VPN si basano su diversi protocolli di sicurezza, ognuno con caratteristiche uniche.

IPsec (IP Security) opera a livello di rete (Layer 3) e protegge tutto il traffico IP, ideale per le connessioni **Site-to-Site**. Include componenti come AH (Authentication Header), che garantisce autenticazione e integrità, ed ESP (Encapsulating Security Payload), che aggiunge cifratura oltre ad autenticazione e integrità.

SSL/TLS (Secure Sockets Layer / Transport Layer Security), invece, opera a livello di sessione (Layer 5) e viene utilizzato principalmente per VPN basate su browser. Offre facilità d'uso, poiché non richiede configurazioni complesse, e consente di accedere alle risorse tramite un semplice browser, sebbene limiti la protezione a solo il traffico TCP, non adatto per UDP o altri protocolli.

BGP/MPLS (Border Gateway Protocol / Multi-Protocol Label Switching) è più utilizzato dai provider per gestire reti VPN su larga scala. Instrada il traffico tramite etichette (labels) invece che indirizzi IP, e isola il traffico di diversi clienti sulla stessa infrastruttura, con vantaggi in termini di efficienza di routing e supporto per QoS, sebbene non offra cifratura (viene spesso combinato con IPsec).

5. Classificazione delle VPN in Base alla Sicurezza

Le VPN possono essere suddivise in tre categorie a seconda del livello di sicurezza e dell'infrastruttura utilizzata.

Le **Trusted VPN** si basano sulla sicurezza garantita dal provider ISP, che assicura che il traffico rimanga isolato (ad esempio, MPLS, ATM). Pur offrendo prestazioni garantite (QoS), non prevedono cifratura, lasciando i dati "nudi" all'interno della rete del provider.

Le **Secure VPN** utilizzano protocolli di cifratura, come IPsec o SSL/TLS, e richiedono autenticazione forte e cifratura end-to-end. Infine, le **Hybrid VPN** combinano gli aspetti di Trusted VPN (per percorsi dedicati) e Secure VPN (per protezione dei dati sensibili), come un’azienda che usa MPLS per collegare le sedi e aggiunge IPsec per proteggere i dati più critici.

6. Confronti e Scenari Pratici

IPsec vs. SSL/TLS

Caratteristica	IPsec	SSL/TLS
Livello	Rete (Layer 3)	Sessione (Layer 5)
Protezione	Tutto il traffico IP	Solo applicazioni TCP (es. HTTPS)
Complessità	Alta (richiede configurazione)	Bassa (accesso via browser)
Casi d'uso	Site-to-Site, client mobili	Accesso remoto via web

MPLS vs. IPsec

MPLS: Ottimo per prestazioni e QoS, ma senza cifratura.

IPsec: Aggiunge sicurezza, ma può introdurre overhead.

Soluzione ideale: Usare MPLS per il backbone e IPsec per i dati sensibili.