VPN – Virtual Private Network

Esistono sia reti private vere e proprie che collegano più sedi in una rete aziendale tramite canali dedicati, sia reti private virtuali. I vantaggi delle reti private sono:

- Larghezza di banda sempre disponibile;
- Nessun problema di accesso;
- Nessuna congestione del traffico;
- Sicurezza e prestazioni ottimali;

Abbiamo anche numerosi svantaggi:

- Alti costi ricorrenti di gestione;
- Lunghi tempi di configurazione;
- Mancanza di scalabilità;
- Rischio di blocco del canale in caso di guasto;

Per ovviare a questi problemi si ricorre alle reti private virtuali. Una VPN (Virtual Private Network) è una rete privata creata all'interno di un'infrastruttura di rete pubblica come Internet. Il rischio di blocco della rete è minimo grazie all'alto grado di ridondanza offerto dalla rete pubblica. Purtroppo vi sono anche delle problematiche, le principali sono 3:

- variabilità di tempo di trasferimento;
- controllo degli accessi;
- sicurezza delle trasmissioni;

Il primo problema viene affrontato tramite l'utilizzo delle WAN, il secondo e il terzo grazie ai fattori di autenticazione, cifratura e tunneling. Esistono due tipi di VPN in commercio, le Remote-access VPN e le Site-to-site VPN.

Remote-Access VPN

Una remote-access VPN consente ai singoli utenti di stabilire connessioni sicure con la LAN aziendale remota, vi sono due componenti indispensabili per la sua realizzazione, il Server NAS (Network Access Server) è il primo, esso può essere o un server dedicato o un'applicazione software in esecuzione su un server condiviso. Attraverso esso l'utente si connette a Internet e può utilizzare una VPN, richiede all'utente di fornire le credenziali per accedere alla VPN e per autenticare queste ultime il NAS utilizza il proprio processo di autenticazione o si avvale di un server di autenticazione separato in esecuzione sulla rete, come il RADIUS AAA Server (AAA sta per i servizi: Authentication, Authorization, Accounting).
L'altro componente di un accesso remoto VPN è un software VPN client, inoltre è necessario un firewall che faccia da barriera tra la rete privata e Internet. In genere le aziende esperte decidono di implementare e gestire in proprio la VPN ad accesso remoto, anche se le aziende possono decidere di esternalizzare (outsourcing) i propri servizi VPN tramite il provider dei servizi enterprise. Tirando le somme una Remote-access VPN è adatta per i singoli dipendenti/utenti o per aziende con filiali costituite da piccoli uffici.

Site-to-Site VPN

Una Site-to-site VPN permette di stabilire connessioni sicure attraverso una rete pubblica, anche ad aziende con tante soldi, ognuna con la sua LAN, ne esistono due tipi:

- Intranet-based, se si desidera unire le reti delle sedi remote in un'unica rete privata;
- Extranet-based, se si desidera unire in un ambiente sicuro le LAN di aziende diverse, in modo da condividere risorse senza l'accesso preventivo alla propria intranet;

Anche se gli scopi della Site-to-site VPN sono diversi da quelli della Remote-access VPN, è possibile utilizzare parte dello stesso software e gli stessi dispositivi, in genere la Site-to-site dovrebbe eliminare la necessità di eseguire il software VPN client come se l'host fosse una Remote-access VPN.

La Sicurezza delle Reti

Ovviamente le VPN devono affrontare seri problemi nell'ambito sia della sicurezza dei dati che della riservatezza delle trasmissioni. In questo campo i fattori su cui bisogna concentrare la nostra attenzione sono 3:

Autenticazione dell'Identità = il processo con cui il sistema informatico, un applicativo o un utente verifica l'identità di un altro sistema che vuole comunicare attraverso una connessione per poi concedergli l'autorizzazione ad usufruire dei relativi servizi associati. Bisogna autenticarsi prima di connettersi alla VPN, questa procedura è nota come MultiFactor Authentication, per esempio dopo il login viene chiesto di inserire un codice generato tramite una chiave elettronica. Ad oggi questa pratica è però superata dall'uso di applicazioni che associano alla generazione di una sequenza di caratteri da usare una volta sola. L'amministratore deve definire delle apposite autorizzazioni per

ciascun utente per l'accesso ai servizi della rete, la maggior parte delle VPN garantisce anche l'integrità, l'autenticità dei dati e prevede dei meccanismi di accounting. Con accounting si intendono tutte le azioni volte a misurare e documentare le risorse concesse a un utente durante un accesso, ciò può includere la durata della sessione di lavoro, o il quantitativo di traffico di dati in una sessione di lavoro. Le informazioni ottenute dalla trascrizione possono poi essere usate per un controllo per le autorizzazioni.

Cifratura = le VPN utilizzano diversi algoritmi di crittografia come il 3DES, CAST o IDEA per cifrare il traffico di rete. Nello specifico nelle VPN viene utilizzato il protocollo Internet Key Exchange (IKE), che implementa lo scambio delle chiavi per cifrare i pacchetti, esso automatizza la gestione delle chiavi.

Tunneling = i protocolli di tunneling aggiungono un livello di sicurezza al fine di proteggere ogni pacchetto nel suo viaggio su Internet, le VPN possono essere protette sia in modalità trasporto che in modalità tunneling. In caso di modalità trasporto hanno un ruolo importante i software impiegati. Nel caso di modalità tunneling hanno un ruolo fondamentale gli apparati router e firewall. In questa modalità l'intero pacchetto viene posto all'interno di un altro pacchetto passeggero che andrà su Internet, proteggendo il contenuto dalla vista del pubblico e facendo viaggiare il pacchetto passeggero all'interno di un tunnel virtuale. Tale stratificazione dei pacchetti viene definita incapsulamento, gli host alle estremità del tunnel possono incapsulare i pacchetti in uscita e riaprire i pacchetti in entrata.

I principali protocolli usati per garantire la sicurezza della rete sono :

- IPsec;
- SSLTLS;
- BGP/MPLS (Border Gateway Protocol / Transport Layer Security);

IPsec

L'IPsec è la scelta più frequente per realizzare sia le Site-to-site VPN con topologia a maglia completa che le Remote-access VPN con topologia a stella. Questo non è un singolo protocollo, ma piuttosto un'intera infrastruttura di sicurezza a livello Network composta da 3 protocolli:

- Authentication Header (AH): garantisce l'autenticazione e l'integrità del messaggio, ma non offre confidenzialità. Viene definito nell'RFC 4302;
- Encapsulating Security Payload (ESP): fornisce autenticazione, confidenzialità e integrità del messaggio. Viene definito nell'RFC4303;
- Internet Key Exchange (IKE): implementa lo scambio delle chiavi per il flusso crittografico. Viene definito nell'RFC 7296;

IPsec utilizza il protocollo **ESP** per l'invio sicuro dei datagrammi, poiché fornisce confidenzialità rispetto ad **AH**. In **IPv4**, AH ed ESP sono header di protocollo, mentre in **IPv6** sono extension header. Il protocollo **IKE**, invece, opera a livello Application sia in IPv4 che in IPv6. IPsec può funzionare in due modalità:

- **Trasporto**: aggiunge gli header AH/ESP tra l'header IP e il protocollo di trasporto (TCP/UDP);
- **Tunnel**: incapsula completamente il pacchetto IP originario;

Per garantire la sicurezza, due host stabiliscono una **Security Association (SA)** tramite **IKE**. Poiché le SA sono unidirezionali, ne servono due per una comunicazione bidirezionale. Le SA attive sono memorizzate nel **SAD (SA Database)**, mentre le politiche di sicurezza sono nel **SPD (Security Policy Database)**. L'elaborazione dei pacchetti distingue il **traffico in uscita (outbound)** da quello **in entrata (inbound)**:

- **Outbound**: si verifica lo SPD, si associa il pacchetto a una SA esistente (o si crea con IKE), si applica IPsec e si inoltra;
- **Inbound**: si ricompone il datagramma IP (se frammentato), si identifica il pacchetto tramite il campo protocollo e il valore **SPI**, si eseguono le operazioni IPsec, si controlla lo SPD e si inoltra il pacchetto alla destinazione o al livello superiore;

Ora andiamo a dare uno sguardo più specifico ai 3 protocolli principali dell'IPsec:

- AH: fornisce servizi di autenticazione, integrità e protezione da attacchi di tipo replay, in cui un intruso immette nella rete un pacchetto autentico precedentemente intercettato. Il campo più interessante dell'AH è Security Parameters Index SPI, che contiene un valore numerico che insieme all'indirizzo IP di destinazione e il protocollo, identifica l'SA utilizzata;
- ESP: fornisce servizi di confidenzialità, autenticazione, integrità e protezione da attacchi di tipo replay. È possibile utilizzare solo alcuni servizi o tutti i servizi insieme. Per quanto riguarda la confidenzialità differisce dall'AH in quanto essa non copre l'header esterno. ESP aggiunge anche un campo Authentication che contiene i dati usati per autenticare il pacchetto;
- IKE: realizza un collegamento peer-to-peer in due fasi, in primis i due host creano una Security Association per IKE stesso, ovvero un canale sicuro per la condivisione dei messaggi. In secundis, utilizzano l'SA appena creata per negoziare Security Association per altri protocolli (IPsec SA);

SSL/TLS

Una valida alternativa all'IPsec è rappresentata dai protocolli SSL/TLS (Security Sockets Layer/Transport Layer security). Le differenze tra SSL e TLS sono minime, in genere vengono implementati entrambi rendendoli interoperabili, Il TSL è un protocollo del livello Session ed è uno standard IETF e deriva dal SSL.

Il protocollo SSL/TLS è composto da due livelli:

- Record Protocol, che opera subito sopra un protocollo di livello Transport (come TCP) ed è utilizzato per incapsulare protocolli di livello superiore;
- Handshake Protocol, che rappresenta il livello superiore e si occupa della fase di negoziazione in cui si autentica l'interlocutore e si stabilisce la crittografia comune;

Per realizzare un SSL/TSL bisogna utilizzare tale protocollo al posto di IKE nell'IPsec, per la fase di autenticazione degli estremi del tunnel e la creazione delle chiavi. Per definizione, SSL/TLS è un semplice protocollo Client/Server che ha lo scopo di autenticare il server da parte del client e, opzionalmente, anche il client da parte del server, e di creare un canale cifrato sicuro per la comunicazione tra i due.

L'autenticazione si basa su **certificati digitali** firmati da una **Certification Authority (CA)**. Il server invia il proprio certificato al client, che ne verifica la validità controllando la firma digitale. Se valida, il server viene autenticato, altrimenti la connessione fallisce. I passaggi per una connessione sicura sono:

- **Client → Server**: invia la richiesta di connessione con gli algoritmi di crittografia supportati e un valore random per la pre-master key;
- **Server → Client**: invia il certificato digitale, la scelta degli algoritmi e il proprio valore random;
- **Client → Server**: verifica il certificato, invia il proprio certificato e la pre-master key cifrata con la chiave pubblica del server, poi richiede il passaggio alla comunicazione cifrata;
- **Server → Client**: conferma l'avvenuta autenticazione e avvia la comunicazione cifrata;

Mettendo a confronto i due protocolli, IPsec e SSL/TLS:

- **IPsec** è un'**architettura complessa** con più protocolli, mentre **SSL/TLS** è un **protocollo definito tramite RFC**;
- **IPsec** offre più metodi di autenticazione, ma **SSL/TLS** si basa solo sui certificati digitali;
- **SSL/TLS** può autenticare solo il server senza il client, mentre **IPsec** richiede autenticazione reciproca;
- **SSL/TLS opera a livello Session**, proteggendo i dati fino alla consegna. **IPsec opera a livello Network**, proteggendo tutto il traffico IP ma non i dati dopo l'arrivo all'host;
- **SSL/TLS funziona solo con TCP**, mentre IPsec protegge tutti i protocolli sopra IP (TCP, UDP, ICMP);

Classificazione della VPN in Base alla Sicurezza

In base ai protocolli che utilizzano e al grado di sicurezza che garantiscono, possiamo classificare le VPN in 3 categorie:

Trusted VPN = Nelle trusted VPN la riservatezza dei dati trasmessi attraverso Internet è controllata da un ISP. Queste non utilizzano i protocolli che permettono la cifratura e il tunneling dei dati trasmessi, l'ISP assicura una qualità del servizio utilizzando e controllando i percorsi dedicati, garantendo che nessun altro possa usufruire del canale assegnato alla VPN. I protocolli e le tecnologie utilizzate dalle Trusted VPN sono:

- Layer 2: trasporto di rete ATM e trasporto del layer 2 su tecnologia MPLS;
- Layer 3: MPLS con distribuzione limitata dalle informazioni del percorso attraverso il BGP;

Secure VPN = Le secure VPN utilizzano i protocolli che consentono la cifratura e il tunneling. Per essere definita secure VPN, una VPN deve garantire:

- la presenza di un sistema di comunicazione;
- che i dati viaggino criptati;
- che il livello di cifratura dei dati sia elevato e modificabile nel tempo;

I protocolli e le tecnologie utilizzate dalle secure VPN sono le seguenti:

- IPsec;
- SSL/TSL;
- PPTP (point-to-point Tunneling Protocol);
- SOCKS Protocol;
- L2TP (Layer 2 Tunneling Protocol);
- L2TPv3;
- MPLS (Multiprotocol Label Switching);

Hybrid VPN = Le Hybrid VPN rappresentano il tentativo di unire le caratteristiche delle Trusted VPN e delle Secure VPN, infatti le Secure VPN assicurano la cifratura dei dati ma non assicurano i percorsi, mentre le Trusted VPN assicurano le proprietà dei percorsi ma non garantiscono un alto livello di sicurezza. In merito ai protocolli usati nelle Hybrid VPN, si può affermare che ogni tecnologia supportata dalla Secure VPN si muove attraverso ogni tecnologia supportata dalla Trusted VPN.