VPN (Virtual Private Network)

Una VPN è una rete privata creata all'interno di un'infrastruttura di rete pubblica (Internet) Per un'azienda con diverse sedi dislocate può essere utile trattare tutte come un'unica rete LAN, la VPN permette di effettuare ciò andando a creare una sorta di WAN privata. Inoltre, può essere utile anche per chi lavora in teleworking o smartworking.

Le reti private vere e proprie collegano + sedi con canali dedicati (pagando gestori)

Vantaggi:

- Larghezza di banda sempre disponibile
- Nessun problema di accesso
- Nessuna congestione del traffico
- Prestazioni garantite
- Sicurezza garantita

Svantaggi:

- Alti costi di installazione
- Costi ricorrenti di manutenzione
- Tempi lunghi per la configurazione
- Mancanza di scalabilità
- Rischio di blocco del canale in caso di guasto (non c'è ridondanza)

Dal momento che la VPN viene creata sulla rete pubblica bisogna fare attenzione a:

- Variabilità del tempo di trasmissione (traffico, congestione, latenza)
- Controllo degli accessi (autenticazione)
- Sicurezza delle trasmissioni (cifratura e tunneling)

Tipi di VPN:

- **Remote-access VPN:** emula il desktop del computer dell'ufficio (homeworking)
- **Site-to-site VPN:** amplia le risorse di rete a filiali, uffici domestici e partner

Remote-access VPN:

- Consente ai singoli utenti di stabilire connessioni sicure con la LAN aziendale
- Realizzata con un server di accesso alla rete (**NAS**) e un software **VPN Client**
- Utilizzata per aziende con piccoli uffici o per i singoli dipendenti/utenti

Un **NAS** (Network Access Server o Nazz) è un server di accesso alla rete che richiede all'utente di inserire credenziali per connettersi. Può essere un server dedicato o un'applicazione software in esecuzione su un server. Il NAS utilizza il proprio processo di autenticazione o si avvale di un server AAA (Autenticazione/Autorizzazione/Accounting).

Un **VPN client** e un firewall che fornisce da barriera tra la LAN privata e Internet

Site-to-site VPN:

Permette di stabilire connessioni sicure su una rete pubblica ad aziende con tante sedi

Può essere **realizzata come:**

- **Intranet-based:** permette ad una società di unire reti di sede remoti in un'unica rete privata
- **Extranet-based:** per le società con rapporti stretti fra loro, permette di lavorare insieme in ambiente sicuro senza l'accesso preventivo alla propria rete

La sicurezza nelle VPN:

- **Autenticazione**
- **Cifratura**
- **Tunneling**

Autenticazione dell'identità:

Processo con cui un sistema informatico o un utente verifica la corretta identità di un altro sistema informatico che vuole comunicare attraverso una connessione, per poi concedergli l'autorizzazione a usufruire dei relativi servizi associati.

Questa procedura di autenticazione è detta **MultiFactor Authentication (MFA)**, per esempio dopo aver effettuato il login con username e password viene richiesto di immettere un codice generato con una chiave elettronica **(key fob)** che cambia ogni volta.

Al giorno d'oggi si utilizzano:

- **OTP (One-Time Password)**
- **Impronte digitali**
- **QR Code**

I protocolli per la sicurezza nelle VPN garantiscono anche **integrità** e **autenticità** dei dati (i pacchetti ricevuti non sono stati modificati e provengano da fonte certa). Per controllare che non siano state effettuate azioni indesiderate e non autorizzate, occorre prevedere **meccanismi di accounting** (azioni x documentare le risorse concesse a un utente durante un accesso come la durata della sessione di lavoro, il quantitativo dei dati (inviati e ricevuti) in una sessione).

Per cifrare il traffico utilizza diversi algoritmi di crittografia (3-DES, CAST, IDEA). Sia l'algoritmo da usare sia le chiavi segrete devono essere concordati e scambiati tra mittente e destinatario attraverso protocolli di sicurezza. Nel caso delle reti VPN, viene soprattutto utilizzato il protocollo **Internet Key Exchange (IKE)**, il cui compito principale è proprio implementare lo scambio delle chiavi per cifrare i pacchetti.

Lo scopo dei protocolli di tunneling è aggiungere un livello di sicurezza con l'incapsulamento al fine di proteggere ogni pacchetto nel suo viaggio su Internet.

Le VPN possono essere protette:

- In modalità trasporto → software impiegati
- In modalità tunnel (tunneling) → apparati (router e firewall)

I protocolli usati per il tunneling sono:

- IPsec (IP security)
- SSL/TLS (Secure Socket Layer / Transport Layer Security)

- BGP / MPLS (Border Gateway Protocol / Multiprotocol Label Switching)
- PPTP (Point-to-Point Tunnelling Protocol)
- IEEE 802.1Q (Ethernet VLANs)
- SSH (Secure SHell)
- GRE (Generic Routing Encapsulation)
- L2TP (Layer 2 Tunneling Protocol)

I protocolli per la sicurezza nelle VPN:

- IPsec
- SSL/TLS

IPsec non è un singolo protocollo, ma una architettura di sicurezza a livello network, composta da vari protocolli e da altri elementi.

I protocolli principali che lo costituiscono sono:

- **Authentication Header (AH):** garantisce autenticazione e integrità del messaggio ma non offre confidenzialità;
- **Encapsulating Security Payload (ESP):** fornisce autenticazione, confidenzialità e integrità del messaggio;
- **Internet Key Exchange (IKE):** implementa lo scambio delle chiavi per realizzare il flusso crittografato.

Nel momento in cui 2 host devono inviarsi dei dati, usando **AH o ESP**, è necessario instaurare prima una connessione logica, detta **Security Association** (SA) → per stabilirla viene usato **IKE**.

IKE è un protocollo a livello Application che usa UDP ma implementa un servizio affidabile, infatti, quando invia una richiesta per attivare una SA, la ritrasmette se non riceve risposta. In generale, le chiavi associate alle SA devono essere usate per un tempo limitato e per proteggere una quantità limitata di dati. Nel caso servisse trasferire altri dati, si instaura una nuova SA.

VPN Site-to-site con tunnelling IPsec

Le SA sono unidirezionali, per cui sono necessarie 2 SA per permettere a 2 host di comunicare tra di loro.

SAD (Security Association Database) → contiene tutte le Security Association attive su un host (o su un security gateway)

SPD (Security Policy Database) → contiene le politiche di sicurezza (tramite queste il sistema decide se un pacchetto deve essere scartato, lasciato passare in chiaro oppure elaborato tramite IPsec)

Il protocollo 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.

Protocolli per la sicurezza nelle VPN (AH):

- **Next header:** contiene l'ID del protocollo dell'header successivo (TCP, UDP, ICMP)
- **Payload length:** contiene la lunghezza dell'header AH
- **Reserved:** riservato per usi futuri, deve essere posto a zero.
- **Security Parameters Index (SPI):** contiene un numero che con l'IP di destinazione ed il protocollo (AH) identifica la SA utilizzata stabilito quando negoziata
- **Sequence number:** specifica il numero di sequenza del pacchetto all'interno della SA, per prevenire i replay attack. Il destinatario gestisce i numeri di sequenza tramite un meccanismo a finestra.
- **Authentication data:** contiene l'**Integrity Check Value (ICV)** del pacchetto. La lunghezza di questo campo è variabile ma deve essere un multiplo di 32 bit, per cui è possibile inserire un padding.

Protocolli per la sicurezza nelle VPN (ESP):

- **Next header:** contiene l'ID del protocollo dell'header successivo (TCP, UDP, ICMP) (se si utilizza il servizio di riservatezza, questo campo è cifrato)
- **Security Parameters Index (SPI):** contiene un numero che con l'IP di destinazione ed il protocollo (AH) identifica la SA utilizzata stabilito quando negoziata
- **Sequence number:** specifica il numero di sequenza del pacchetto all'interno della SA, per prevenire i replay attack. Il destinatario gestisce i numeri di sequenza tramite un meccanismo a finestra.
- **Payload data:** contiene il payload del pacchetto IP originale (modalità trasporto) oppure l'intero pacchetto IP originale (modalità tunnel), cifrato se si utilizza il servizio di riservatezza. Nel caso l'algoritmo di cifratura utilizzato necessiti di **Initialization Vector (IV)** (inserito all'inizio del payload).
- **Padding:** può essere necessario per
    - L'algoritmo di cifratura richiede un dimensione del testo multipla di tot
    - Assicurare il corretto allineamento dei campi successivi
    - Limitare gli effetti dell'analisi del traffico basata sulla dimensione
- **Pad length:** contiene la lunghezza del padding
- **Authentication data:** contiene il valore di controllo integrità **(ICV)** calcolato sull'intero pacchetto ESP escluso questo campo. È presente solo se si utilizza il servizio di autenticazione/integrità

Fornisce servizi di confidenzialità autenticazione, integrità e protezione da attacchi di tipo replay.

- A differenza di AH, l'autenticazione non copre l'header IP esterno
- Anche l'ESP presuppone che esista già una SA tra i due nodi

Protocolli per la sicurezza nelle VPN (IKE):

Realizza un collegamento peer-to-peer in due fasi:

- **1° fase** → i 2 host creano una SA per l'IKE stesso **(IKE SA)**, ovvero un canale sicuro da utilizzare per i messaggi di IKE.
- **2° fase** → utilizzano la SA appena creata per negoziare altre SA per altri protocolli (IPsec SA)

Protocolli per la sicurezza nelle VPN (SSL/TLS):

Le differenze da IKE sono poche e marginali, tuttavia sono non compatibili. In generale, vengono implementati entrambi e viene garantita l'interoperabilità.

TLS è un protocollo di livello Session dello stack ISO/OSI. Opera quindi al di sopra del protocollo di livello Transport. È uno standard IETF e deriva dal protocollo SSL. SSL è stato originariamente proposto da Netscape Communications, ma è un protocollo open

Composto da 2 livelli:

- **Record Protocol:** opera sopra un protocollo di liv. Transport (come TCP), è utilizzato per incapsulare protocolli di livello superiore
- **Handshake Protocol:** si occupa della fase di negoziazione in cui si autentica l'interlocutore e si stabilisce la crittografia comune

La realizzazione di una **VPN SSL/TLS-based** passa innanzitutto attraverso l'uso di **SSL/TLS** per l'**autenticazione** degli estremi del tunnel e la creazione delle **chiavi**.

SSL/TSL è un protocollo Client/Server che ha lo scopo di autenticare il server da parte del client (+ viceversa opzionale), e di creare un canale cifrato di comunicazione tra i 2.

L'autenticazione è basata sui certificati digitali riconosciuti da una **Certification Authority**. Il server invia il proprio certificato al client che ne verifica la validità (confronta la firma digitale con quella a lui nota). Se è valida → accetta il certificato e autentica il server. Analogamente il server può chiedere il certificato al client per verificarne la validità.

1) **Client → Server** il client invia al server:
- La richiesta di connessione
- La lista degli algoritmi di crittografia supportati
- Un valore random necessario a creare la pre-master-key
  (a sua volta servirà a generare la chiave privata di crittografia comune a entrambi)

2) **Server → Client** il server invia al client:
- Il proprio certificato digitale
- La scelta dell'algoritmo di crittografia
- Il proprio valore casuale per la pre-master-key
- La richiesta del certificato del client

3) **Client → Server** il client verifica il certificato del server
   - Se negativo → il protocollo fallisce
   - Se positivo → invia al server:
     - Il proprio certificato digitale
     - La pre-master-key cifrata con la chiave pubblica del server.

   Infine, il client accoda la richiesta di passare a comunicazioni cifrate

4) **Server → Client:** il server conferma al client di aver accettato il suo certificato digitale e passa alla fase di comunicazioni cifrate.

Dopo il punto 3 sia il client che il server hanno tutte le informazioni necessarie per calcolare la chiave, comune ad entrambi, e gli algoritmi a cui applicarla

SSL/TLS è adatto a proteggere la comunicazione tra due applicazioni (autentica l'applicazione o l'utente), **IPsec** può facilmente rendere sicuro il traffico tra host o tra intere sottoreti (autentica la macchina).

Principali differenze tra i due protocolli.

IPsec	SSL/TLS
Architettura complessa.	Singoli protocolli.
Peer-to-peer (IKE).	Client/Server.
Livello Network.	Livello Session.
Canale tra due macchine.	Canale tra due applicazioni.
Protezione di tutto il traffico IP.	Protezione solo del traffico TCP.
Protezione di tutto ciò che segue l'header IP.	Protezione dei dati del livello Application.
Impatto maggiore sul sistema operativo.	Impatto maggiore sulle applicazioni.

Le **reti** possono essere **classificate** per protocolli e grado di sicurezza **in 3 categorie:**

- **Trusted VPN**
- **Secure VPN**
- **Hybrid VPN**

Trusted VPN: (percorsi controllati)

- Riservatezza dei dati trasmessi controllata da un Internet Service Provider (ISP)
- Non utilizzano i protocolli che permettono la cifratura ed il conseguente tunneling
- L'ISP assicura una qualità del servizio (QoS) (controllo di percorsi dedicati)
- L'azienda che si rivolge all'ISP ha fiducia che i percorsi siano mantenuti sicuri

Secure VPN: (cifratura dei dati)

- Utilizzano protocolli che consentono la cifratura e il tunneling
- Per essere definita tale, una VPN deve garantire:
    - Sistema di autenticazione
    - Dati viaggiano criptati
    - Il livello di cifratura dei dati è elevato e modificabile nel tempo

Hybrid VPN: Tentativo di unire le caratteristiche delle Trusted VPN e delle Secure VPN