VPN

Le VPN (Virtual Private Network) sono delle reti virtuali per la connessione di client ad una rete privata attraverso l'uso di Internet. Infatti senza di esse si sarebbe costretti a progettare delle WAN che connettono più LAN interne. Tale processo risulta, però sia costoso che poco sicuro.
Sono necessari per l'invio e ricezione del pacchetto sulla VPN dei particolari router VPN.

Le VPN forniscono numerosi vantaggi, ed è questo il motivo per cui sono utilizzate da molte aziende:

1. Economiche
2. Scalabili
3. Sicure
4. Permettono di lavorare esternamente all'azienda
5. Sono indipendenti dalla struttura fisica della rete

A seconda delle esigenze le VPN si possono classificare per tipologia di accesso:

- **Ad accesso remoto:** sono le VPN più utilizzate con le quali un dipendente può lavorare fuori sede avendo accesso alla rete Intranet dell'azienda.
  Dal punto di vista strutturale è una semplice connessione Point To Point
- **Da sito a sito:** connette due frazioni di una linea privata

Le VPN sono fondate sul processo di tunneling, ossia l'apertura di una connessione con un server privato e l'invio dei dati tramite Internet.
Le VPN in base al tipo di tunneling per cui sono progettate sono divise in tre gruppi:

1. **Trusted:** I pacchetti vengono assicurati su un percorso prestabilito (ossia vengono definiti tutti i router che il pacchetto deve transitare). E' meno costosa, ma priva di sicurezza, in quanto sensibile al rintracciamento e sniffing dei pacchetti.
   Nessuno tranne l'amministratore del server può modificare la gestione della VPN, nè modificare i dati in entrata e uscita, ma limitano la VPN all'utilizzo di un IP statico.
2. **Secure:** i pacchetti vengono crittografati ed inviati su dei canali sicuri, ma il percorso non viene assicurato.
   La crittografia può essere a chiave simmetrica o asimmetrica.
3. **Hybrid:** vengono combinate le tecnologie Trusted e Secure, ossia viene assicurato il percorso e la criptazione.

Nella VPN circolano solitamente dati sensibili, perciò è strettamente necessario proteggerla da attacchi hacker, sniffing, DOS e DDOS.
La struttura di sicurezza della VPN si compone quindi di:

- Firewall
- AAA (Authentication Autorization, Account) Server
- Algoritmi di crittografia
- Protocolli di crittografia (IPsec)

L'**AAA Server** è un particolare tipo di server (la maggior parte delle volte è una funzionalità del server centrale) che si occupa di fornire i certiicati assicurandosi:

- Chi è l'utente?
- Che permessi ha?
- Cosa deve fare?

Tunneling
E' un tunnel concettuale sicuro nel quale transitano i pacchetti nella connessione client-server.
Il processo di tunneling avviene prima della spedizione del pacchetto da parte del router e consiste nell' effettuare un incapsulamento multiprotocollo dei dati, ossia rendere i dati indipendenti dai protocolli della rete, li imbusta in un nuovo header IP dal protocollo di tunneling.
Le reti VPN contengono enormi quantità di dati sensibili i quali però vengono protetti attraverso i sistemi di autenticazione e crittografia.

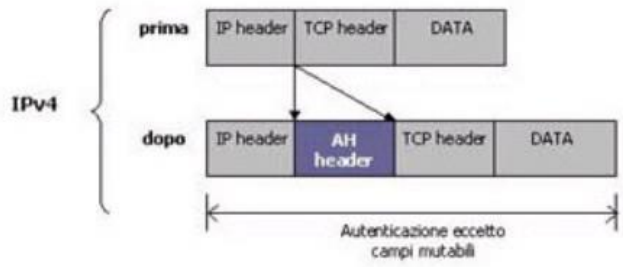
I sistemi di autenticazione si fondano su determinati schemi di autenticazione che garantiscono protezioni piùo meno elevate:

- AH - Authentication Header
- EAP - Extensible Authentication Protocol
- PAP Password Authentication Protocol

AH - Authentication Header
Protoccolo che fornisce l'autenticazione della sorgente e l'integrità dei dati ma non la segretezza. Quando un determinato host sorgente vuole inviare uno o più datagram utilizzando IPSec, prima stabilisce una SA con la destinazione, dopo di che può iniziare a spedire effettivamente i datagram sicuri verso di essa

AH (Modalità Trasporto)

In questa modalità i datagram IPsec comprendono l'intestazione AH, che è inserita fra i dati del datagram IP originale (per esempio un segmento TCP) e l'intestazione IP, come mostrato in figura. L'header del pacchetto originale subisce una modifica nel

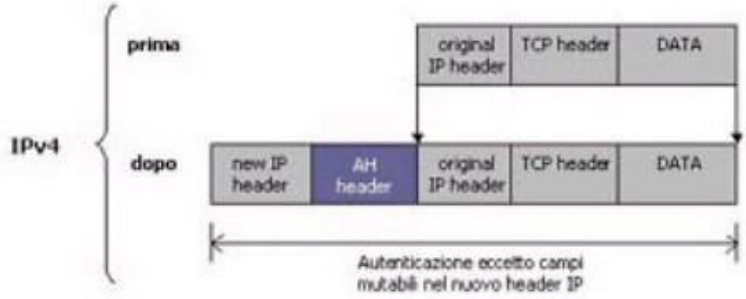


campo next protocol nel quale viene inserito il valore 51 per indicare che il datagram sta incapsulando un'intestazione AH. Quando l'host di destinazione riceve il datagram

IP, esso si accorge del valore 51 presente nel campo protocollo ed elabora il datagram usando il protocollo AH. I router intermedi elaborano i datagram come hanno sempre fatto: esaminano l'indirizzo IP di destinazione e instradano i datagram in funzione di questo indirizzo

AH (Modalità Tunnel)

La modalità Tunnel invece, prevede la creazione, da parte del mittente, di un pacchetto IP ausiliario utilizzato per ospitare l'originario datagram IP. Quest'ultimo viene messo in sicurezza mediante incapsulamento in un pacchetto AH.



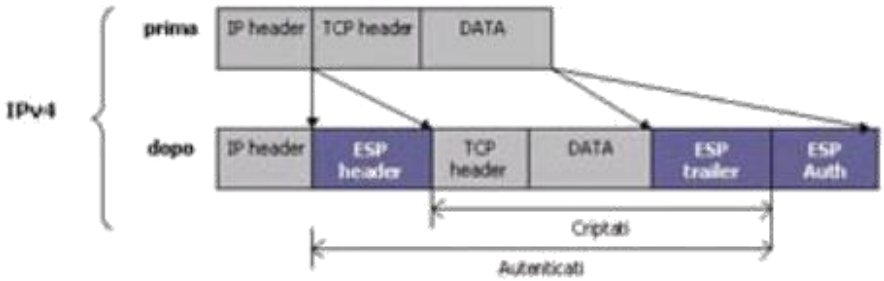
Il traffico VPN deve anche essere **crittografato** in modo che non possa essere leggibile dall'esterno, i protocolli di crittografia più comuni sono:

- AES - Advanced Encryption Standard
- DES - Data Encryption Standard
- ESP - Encapsulated Security Payload
- RC4/5 - Rivest Cypher 4/5
- MD5 - Message Digest 5
- SHA - Secure Hash Algorithm
- RSA - Rivest Shamir Adleman

ESP(Encapsulating Security Payload)
Il protocollo ESP fornisce la segretezza a livello dello strato della rete, ma può fornire anche autenticazione dell'host così come AH.
Nel caso di modalità trasporto, così come avveniva per AH, è necessario indicare il valore 50 nel campo "next header" del datagram IP originario, per indicare che il datagram contiene un pacchetto ESP.

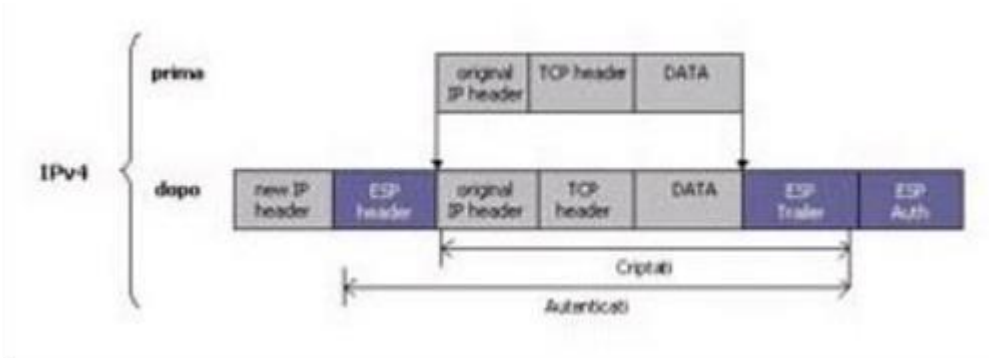
ESP (Modalità Trasporto)

ESP in modalità trasporto può essere applicato solo a comunicazioni host-to-host e vengono protetti solo i dati relativi ai protocolli superiori, non l'header IP del pacchetto stesso. In modalità di trasporto, ESP è inserito dopo l'header IP e prima dei protocolli di livello superiore (TCP, UDP, ICMP, ...) e di qualsiasi altro header IPsec precedentemente inserito



ESP (Modalità Tunnel)

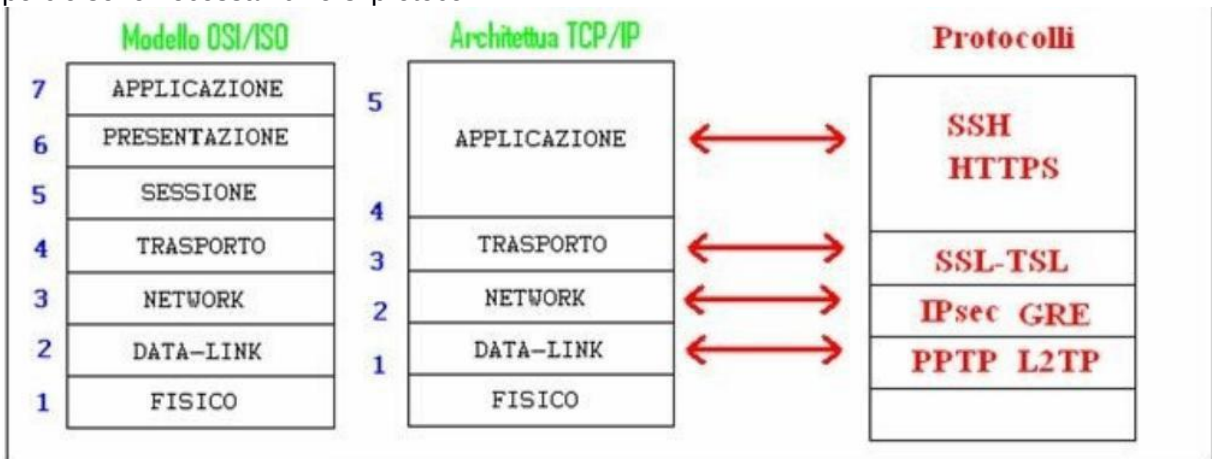
Nella modalità Tunnel invece, il datagram sicuro è creato circondando l'intero datagram IP originale con i campi intestazioni e trailer del pacchetto ESP, e quindi inserendo il tutto, questa volta, in un nuovo pacchetto IP.



Passaggi di autenticazione

1. Il client VPN contatta il Server.
2. Il Server se presente notifica la sua presenza.
3. Il client si presenta e richiede di essere autenticato (ovvero il client richiede al server di identificarlo).
4. Il server esegue la procedura di autenticazione e autorizzazione (ovvero il server verifica che il tentativo di connessione tra client e server sia permesso dopo il processo di autenticazione sia riuscito).
5. Il server risponde alla richiesta di autenticazione.
6. Il Client può comunicare con la rete (o il singolo client) se autorizzato.
7. Inizia la comunicazione tra le due entità.

Il processo di tunneling può avvenire in un qualsiasi strato del modello OSI tranne quello fisico, a seconda delle necessità di crittazione e di complessità richiesta dei dati perciò sono necessari diversi protocolli.

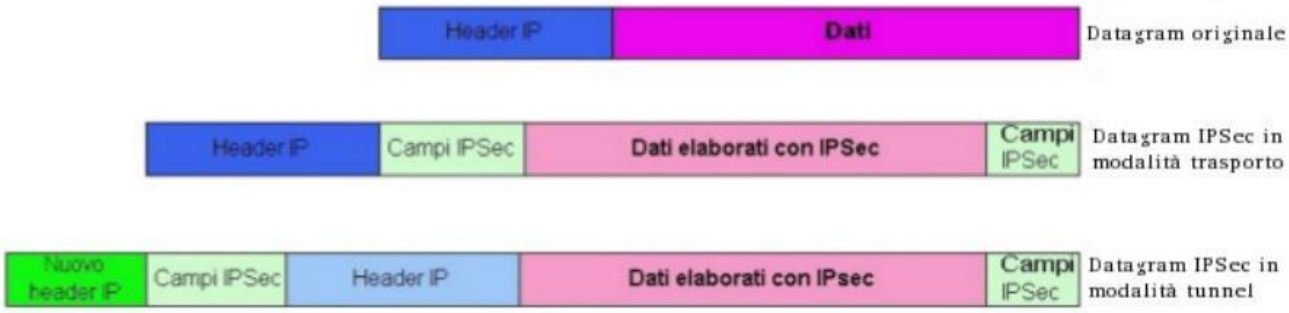


IPsec

Il protocollo IPsec è situato al livello 2 dello stack TCP ed è il più sicuro e diffuso nel suo ambito.

Sfruttando le caratteristiche dello strato Network(Livello Network) e l'imbustamento dei pacchetti esso riunisce il protocollo di autenticazione AH e ESP. Esistono due modalità IPsec:

- Trasporto: usata solo nelle comunicazioni end to end
- Tunnel



Prima di inviari datagram "sicuri sul canale, l'host sorgente e quello destinazione si devono prima scambiare l'handshake creando una connessione logica sullo strato della rete.
Questo canale logico è detto **Associazione di Sicurezza SA** (Security Association).
La connessione logica definita da un SA è una connessione simplex, cioè unidirezionale

Una SA è unicamente identificata da:

- Un identificatore del protocollo di sicurezza (AH o ESP)
- L'indirizzo IP destinazione per una connessione simplex;
- Un identificatore a 32 bit della connessione, detto indice dei parametri di sicurezza (**SPI**, Security Parameter Index).

Per un buon funzionamento di IPSec, è necessario uno schema SA automatico per la gestione delle chiavi. Per fare questo ci sono due protocolli principalmente utilizzati:

- il protocollo Internet per la gestione delle associazioni per la sicurezza e delle chiavi **ISAKMP** (Internet Security Association & Key Management Protocol) il quale definisce le procedure per stabilire e interrompere le SA. ISAKMP prevede due fasi per contrattazione: 1) end-points della comunicazione si autenticano e si accordano su un insieme di funzioni crittografiche per lo scambio dei dati; 2)avviene lo scambio vero e proprio delle SA;

- il protocollo Internet per lo scambio delle chiavi **IKE** (Intenet Key Exchange) RFC 2409

Altri Protocolli

SSL/TLS (Secure Socket Layer/Transport Layer Security)

Un altro protocollo utilizzato oltre all'IPsec è il SSL. E' un protocollo di crittazione. In breve le operazione eseguite sono:

- Apertura connessione

- Frammentaziione messaggio in pacchetti
- Compressione
- Applicazione Message Authentication Code
- Crittografia
- Trasmissione

Con il SSL possono essere utilizzate le cifrature sia a chiave simmetrica che asimmetrica(a chiave pubblica, RSA, per l'autenticazione). Vengono utilizzate chiavi di cifratura simmetrica fino a 4096 bit

PPTP

Livello 2
Ha buone performance a livello di velocità di esecuzione e facile da configurare
Difficilmente instradabile da un firewall perché fa uso di due sessioni distinte di rete
Assicura autenticazione e criptazione dei dati