I protocolli di sicurezza usati nelle VPN

Indice

By Bl4ckD0t

1) IPsec

IPSec, abbreviativo di **IP security**, non è un vero e proprio protocollo, ma un'**architettura di protocolli** a livello **Network**. E' la scelta più usata nelle VPN poiché permette di garantire la sicurezza in tutte le tipologie di rete virtuale privata, e supporta anche la modalità **IPv6**.
IPsec è composto principalmente da 3 protocolli:

a. **Authentication Header** (**AH**): garantisce l'autenticazione e l'integrità, ma **non** la confidenzialità.
b. **Encapsulating Security Payload** (**ESP**): fornisce integrità, confidenzialità e autenticazione.
c. **Internet Key Exchange** (**IKE**): permette lo scambio delle chiavi per avviare la comunicazione cifrata.

Il singolo funzionamento dei protocolli lo vedremo poco più avanti.

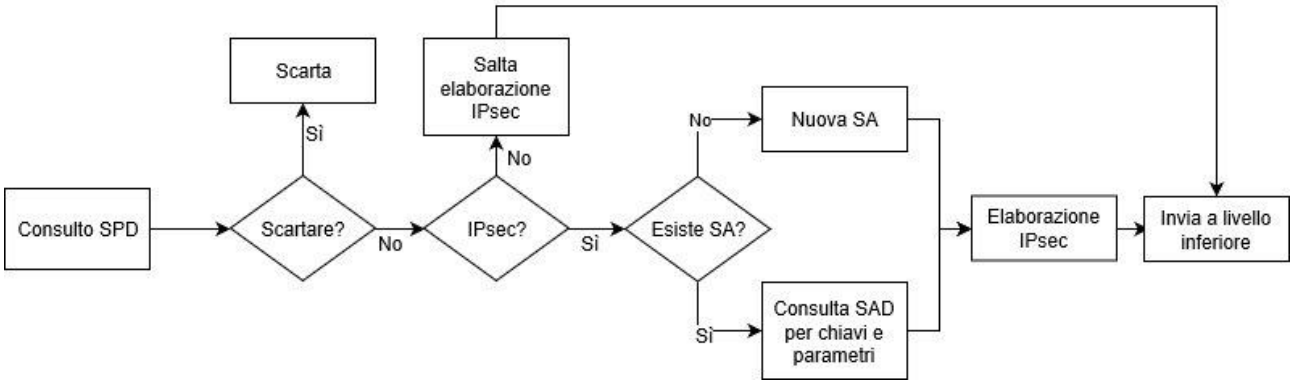
AH ed ESP **non possono** essere usati **contemporaneamente**, ma si deve scegliere tra uno o l'altro.

Entrambi in IPv6 sono **extension header**, mentre IKE sia in IPv4 che IPv6 è un **protocollo** di livello **Application**.
AH ed **ESP** non si preoccupano dello scambio delle chiavi, hanno **bisogno** di **lavorare abbinati a IKE**, che **crea** le **Security Association** (**AS**), cioè coppie di interlocutori, con specifiche regole per la criptazione e meccanismi di sicurezza.
Una SA può essere abbinata solo a **uno tra AH o ESP**, e ha un "periodo di vita", che può essere specificato in termini temporali oppure in dati trasferiti.
Sia AH che ESP possono essere utilizzati in due modalità applicative: **trasporto** o **tunneling**.

Come detto poco fa, un concetto fondamentale in IPsec è quello delle **SA**. Queste non sono altro che **associazioni di due parti che comunicano con IPsec**. Le SA sono **unidirezionali**, quindi occorrono due associazioni per creare una comunicazione, e ogni dispositivo per conoscere le SA ad egli associate dispone di un apposito Database, chiamato **SAD** (**Security Association Database**), nel quale sono elencati tutti gli abbinamenti con le altre parti.
Oltre SAD è fondamentale sapere che esiste anche un altro DB, chiamato **SPD** (**Security Policy Database**), contenente tutte le politiche di sicurezza per ogni SA, che in ricezione di un pacchetto fungono da filtro per sapere se leggerlo o scartarlo.

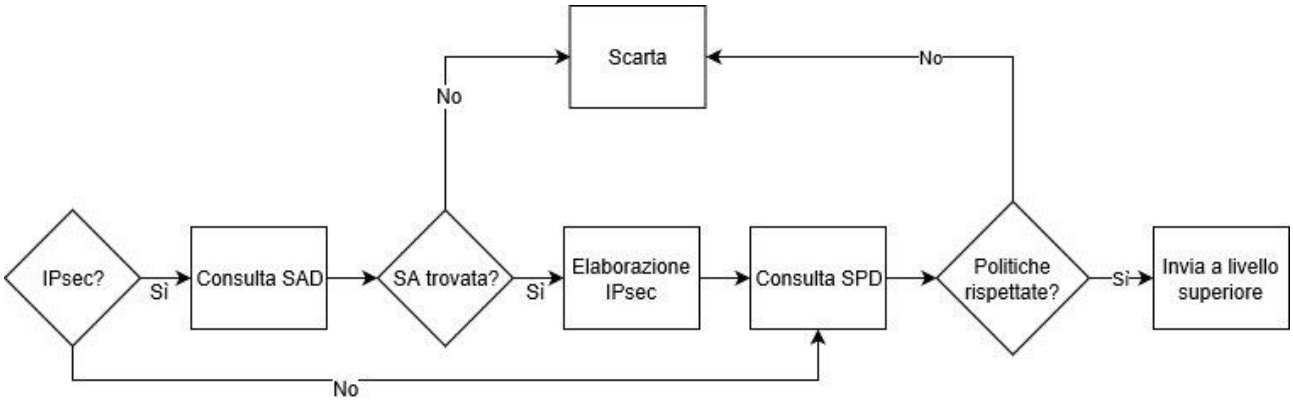
Una macchina che implementa IPsec applica le proprie **policy di sicurezza** a **tutto il traffico**, sia in **entrata** che in **uscita**, senza distinzioni.
Per il traffico in **uscita** il meccanismo è il seguente:

- Si controlla per il pacchetto se è presente una regola nell'SPD ed eventualmente si scarta il pacchetto
- Si controlla se il pacchetto necessiti di IPsec o meno
    - In caso sia previsto IPsec, si cerca nel SAD un'associazione valida, in alternativa se ne crea una con IKE
    - Si elabora il pacchetto (cifratura e tunneling)
- Invio del pacchetto al livello inferiore



Per il traffico in **entrata** invece il meccanismo implementato è come segue:

- Si ricompone il datagram IP e si verifica se il pacchetto necessiti o meno di un' elaborazioneIPsec (guardando se siano presenti header AH/ESP)
    - Se è un pacchetto da elaborare, si identifica la SA associata grazie al campo SPI, altrimenti si scarta
    - Si applica l'elaborazione richiesta
- Si controllano le regole nell'SPD e si decide se inoltrare il pacchetto oppure scartarlo



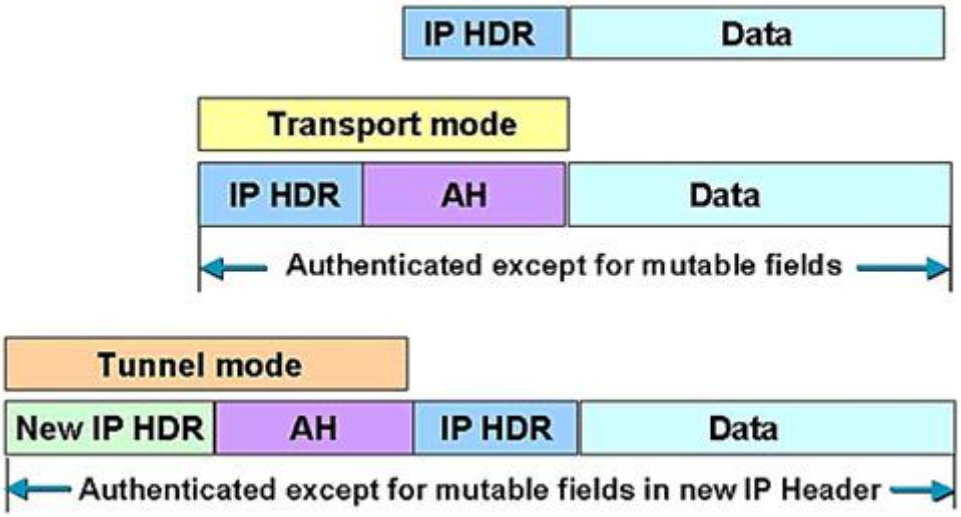
Le SA possono essere combinate tra loro, quindi un host può avere più associazioni differenti. E' consentito applicare sia AH che ESP a patto che venga prima applicato il secondo e poi il primo, e solamente una volta (quindi non si può fare ESP + AH + ESP). Si possono però applicare quanti tunnel si vogliono.

a. AH (AuthenticationHeader)

Il protocollo AH fornisce servizi di **autenticazione**, **integrità** e **protezione** da **attacchi** di tipo **Replay**. Il protocollo autentica **l'intero pacchetto IP** ad **eccezione** dei **campi variabili**.

Importante è il campo **SPI** (**Security Parameters Index**), contenente un valore numerico che abbinato **all'IP destinatario** e al **protocollo usato** (in questo caso AH) **identifica la Security Association**. Questo numero è stabilito dal destinatario quando la SA viene negoziata.

A differenza della modalità trasporto, la modalità **tunnel** incapsula **l'intero header** e **tutto** il **pacchetto** in un **nuovo pacchetto**, autenticando così ogni singolo campo.

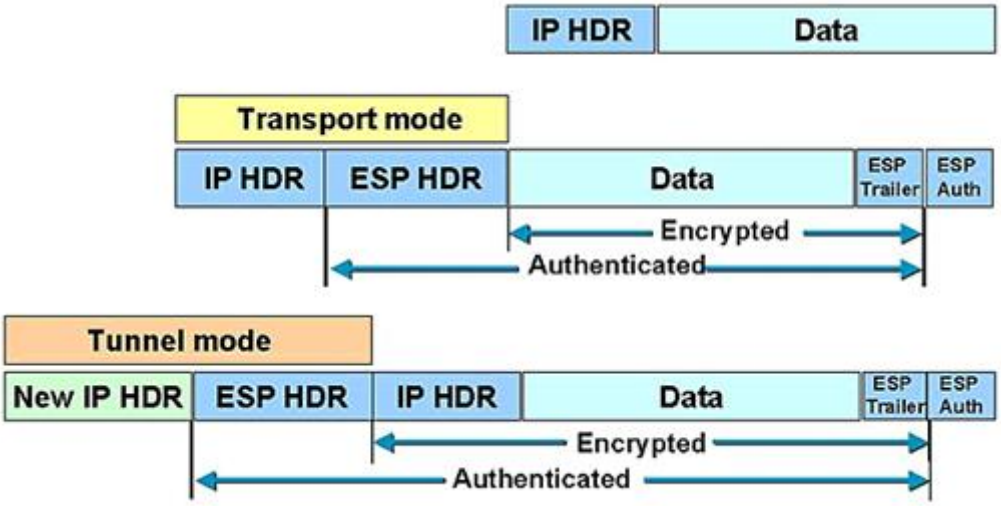


b. ESP (Encapsulating Security Payload)

ESP si differenzia da AH perché oltre a fornire servizi di **integrità**, **autenticazione** e **protezione anti-replay**, fornisce anche servizi di **confidenzialità**, e tali servizi si possono **interscambiare** o utilizzare tutti quanti **contemporaneamente**.

L'autenticazione rispetto ad AH è leggermente differente, perché **non copre l'header IP esterno**.
ESP inoltre aggiunge un **header** e un **trailer** poiché incapsula tutti i dati protetti. Aggiunge infine un campo **Auth** contenente i dati usati per autenticare il pacchetto.

Così come AH, anche ESP dispone del campo **SPI**, con le medesime funzionalità e logiche. L'unica differenza è che usa il protocollo ESP anziché AH.

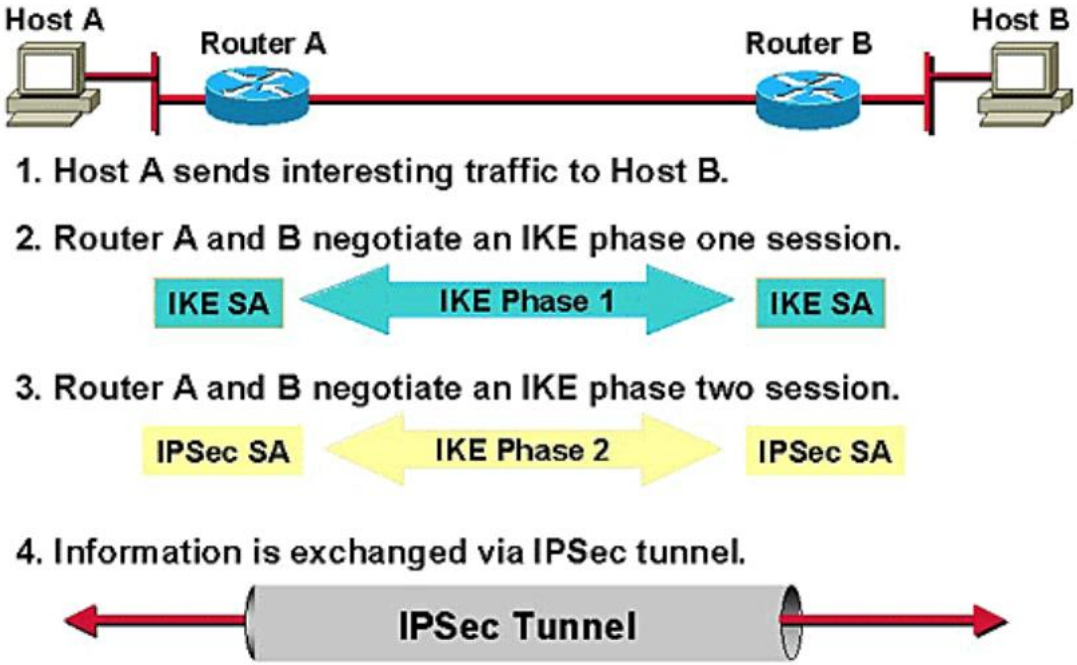


c. IKE (Internet Key Exchange)

Il protocollo IKE è colui che si occupa di **gestire le SA e crearle**.

E' un protocollo **Peer-to-peer** diviso in due fasi:

1. I due nodi **creano** un' **AS** per **IKE** stesso (canale sicuro dove scambiare i dati e gli accordi di IKE).
2. **Utilizzano** la **SA** appena creata per negoziare Security Association per **altri protocolli.**



2) SSL/TLS

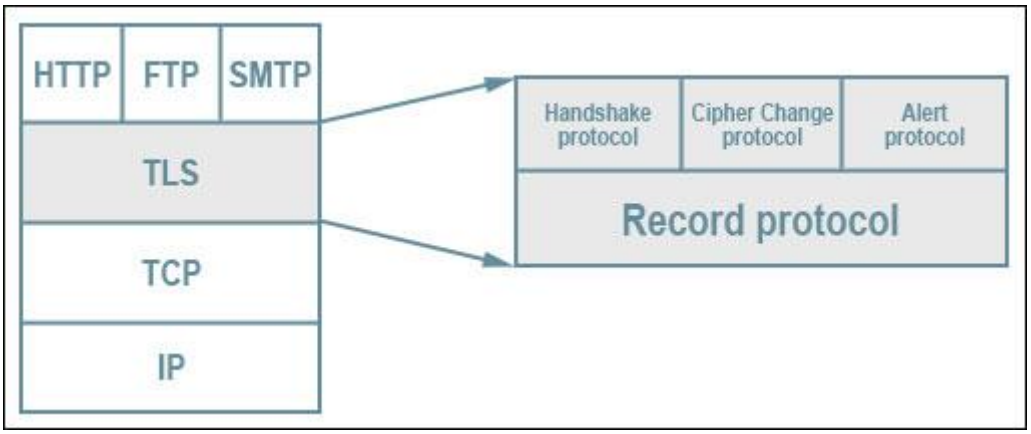
SSL e **TLS**, rispettivamente **Secure Sockets Layer** e **Transport Layer Security**, sono due protocolli molto validi per sostituire IPsec.

I due protocolli (SSL e TLS) hanno differenze davvero minimali, ma nonostante ciò questi due **non sono compatibili**. Vengono quindi implementati entrambi e resi **interoperabili** tramite particolari meccanismi di gestione.

TLS è un protocollo a livello **Sessione**, opera quindi sopra il livello trasporto (per intenderci TCP e UDP) e deriva dal suo predecessore SSL.

Entrambi sono in verità composti da due livelli, che si dividono differenti compiti:

- Il **record protocol**: che ha il compito di **incapsulare** tutto ciò che sta ai livelli superiori, compreso l'handshake protocol.
- L'**handshake protocol**: ha il compito di **negoziare** le **chiavi**, **autenticare** e stabilire algoritmi e **chiavi crittografiche** comuni.

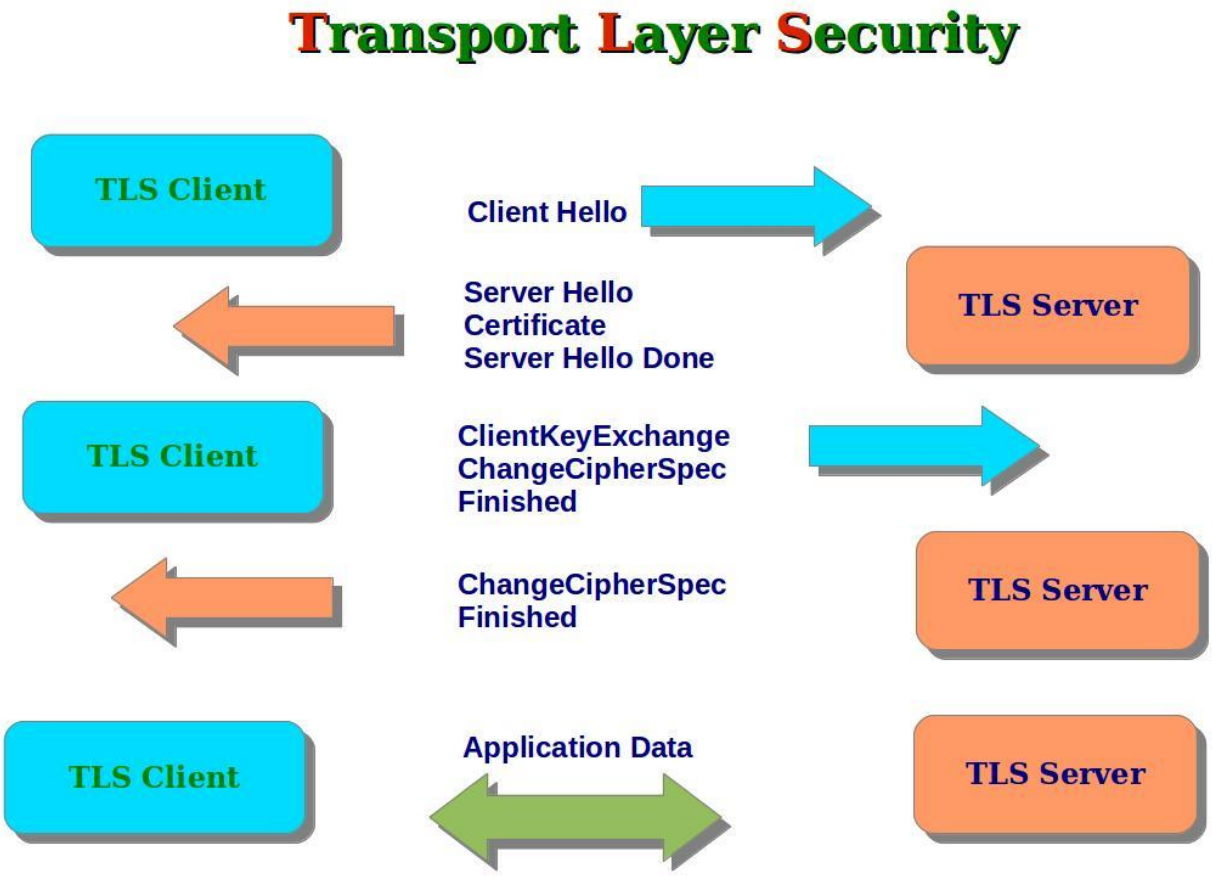


SSL e TLS garantiscono **autenticazione**, **integrità** e **cifratura**, ma solo su reti **TCP/IP**. Una VPN basata su questi protocolli non avrà più bisogno di IKE per lo scambio delle chiavi, poiché SSL/TLS sono semplici protocolli **Client/Server** con lo scopo di autenticare il Server, eventualmente il Client e creare un canale di comunicazione sicuro e cifrato tra i due host.
L'autenticazione è basata sui **Certificati Digitali**, riconosciuti da una **Certification Authority(CA)**.

Il funzionamento dei due protocolli è ilo seguente (**4/3-way handshake**):
NB: Deve essere sempre il client a iniziare la comunicazione per autenticare a sé il Server

1) **Client** → Server: il client invia al server la **richiesta di connessione**, includendo la **lista degli algoritmi** supportati e un **valore random** con cui si creerà la **Pre-masterkey**, utilizzata poi per generare la chiave privata di crittografia.
2) Client ← **Server**: il server invia al client il **proprio certificato**, la **scelta degli algoritmi**, il **valore casuale** per la Pre-master key e la **richiesta del certificato del client**.
3) **Client** → Server: il client **verifica il certificato** del server e se tutto è regolare invia il proprio più la **pre-master key cifrata con la chiave pubblica del server**. Accoda inoltre la **richiesta di passare ad una comunicazione cifrata**.

4) Client ← **Server**: il server conferma al client di aver accettato il proprio certificato **e passa alla comunicazione cifrata**.



a) Confronto tra IPsec e SSL/TLS

IPsec	SSL/TLS
Architettura complessa (3 protocolli + 2 DB)	Singoli protocolli (dettati da una RFC)
Peer-to-peer (IKE)	Client/Server
Livello Network	Livello Session
Canale tra due macchine	Canale tra due applicazioni
Può proteggere tutto il traffico	Può proteggere solo il traffico TCP
Protegge tutto ciò che segue l'header	Protegge i dati a livello Application
Impatto maggiore sul OS	Impatto maggiore sulle applicazioni

1) BGP/MPLS

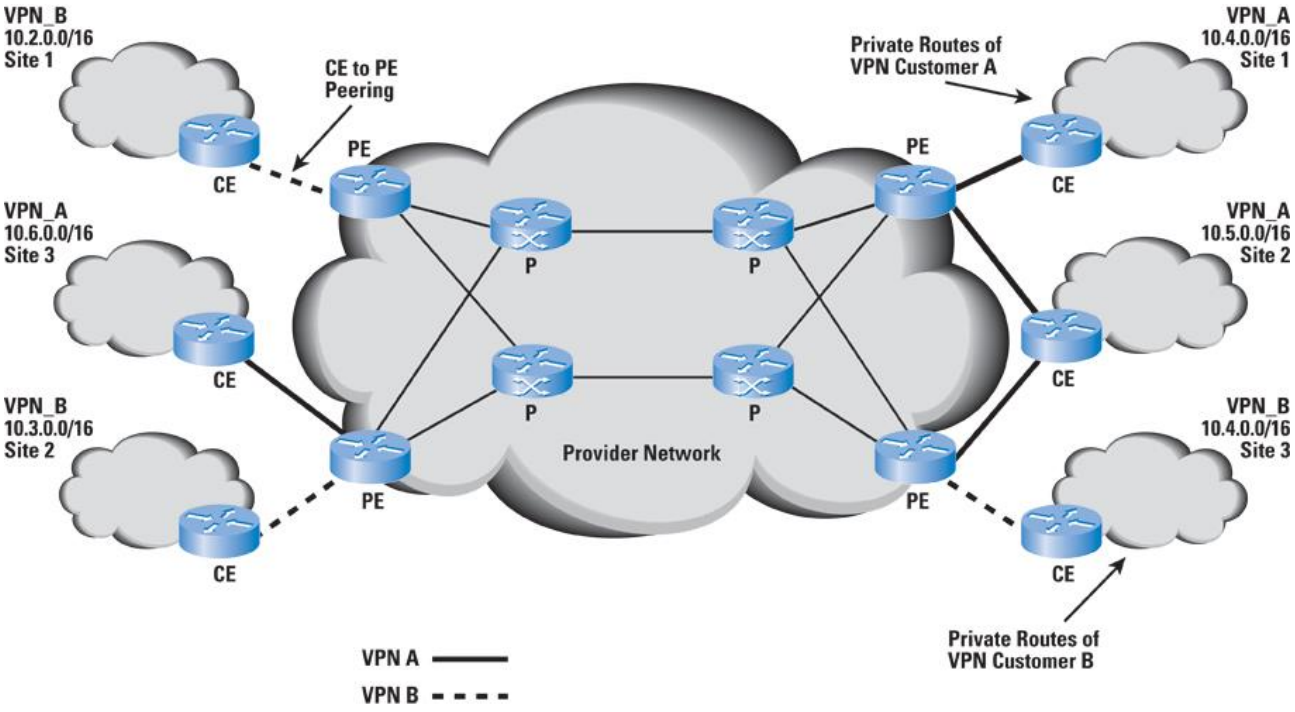
BGP (**Border Gateway Protocol**) e **MPLS** (**Multi-Protocol Label Switching**) sono due protocolli implementabili nelle VPN.

Il primo è un protocollo di tipo **Path Vector**, che elenca tutti gli **Autonomous System** da attraversare per raggiungere la destinazione stabilita, il secondo invece è un protocollo che permette di utilizzare delle **label al posto degli indirizzi IP** per muovere i pacchetti attraverso il proprio dominio. Per individuare il next-hop vengono usate delle apposite tabelle, dette **forwarding table**.

In tal modo viene garantita la separazione del traffico tra i diversi utilizzatori dei servizi, anche se il traffico utilizza lo stesso core di rete.

Gli elementi costitutivi di una VPN che usi questi protocolli sono i seguenti:

- **Customer Edge** (**CE**): è il **router** del sito aziendale, o comunque **dell'utilizzatore**. Ha funzionalità di routing classiche e il suo unico peer è il Provider Edge con cui dialoga tramite il protocollo BGP
- **Provider Edge** (**PE**): è il **router d'accesso alla rete** dell'ISP cui sono collegati uno o più CE. I PE sostanzialmente sono le entrate e uscite all'ISP.
- **Provider Core Router** (**PCR** o solo più semplicemente **P**): sono la **backbone** MPLS dell'ISP



Per trasferire pacchetti tra due host di una VPN, il PE **incapsula** (tunneling) i pacchetti provenienti dal CE mittente e li inoltra nella rete MPLS verso il PE abbinato al CE destinatario. L'ultimo PE instraderà su rete IP.

Siccome però un PE può gestire differenti VPN, affinché non vi siano problemi di indirizzamento IP e route su VPN sbagliate, si adottano le **VRF** (**VPN Routing and Forwarding**), cioè particolari tabelle di cui ogni PE è dotato, le quali indicano una specifica VPN e aiutano il PE nell'instradamento e gestione del traffico tra le diverse VPN. Inoltre il PE possiede anche le **GFT** (**Global Forwarding Table**), tabelle che consentono al PE di indirizzare i pacchetti verso un altro PE, utilizzando però come dati disponibili due label anziché due IP:

- La **prima lable** (**esterna**) che indica il **next hop**
- La **seconda** (**interna**) che identifica il **nodo d'uscita**

a) Confronto fra BGP/MPLS e IPsec

Il confronto in realtà è un paragone che non regge, poiché i due protocolli sono nati per **scopi differenti**.

Il primo è nato per garantire una particolare **efficienza nell'instradamento dei pacchetti e nella loro gestione**, il secondo invece per garantire una **totale sicurezza dei dati**. Le due tecnologie non sono quindi concorrenti, ma complementari. Le VPN MPLS-based non potranno mai diventare un nuovo standard in fatto di sicurezza, ma piano piano potranno sostituire le vecchie tecniche, come le Frame Relay e ATM. Inoltre MPLS non può vivere autonomamente come IPsec, ma necessita di un ISP che ne metta a disposizione l'infrastruttura.