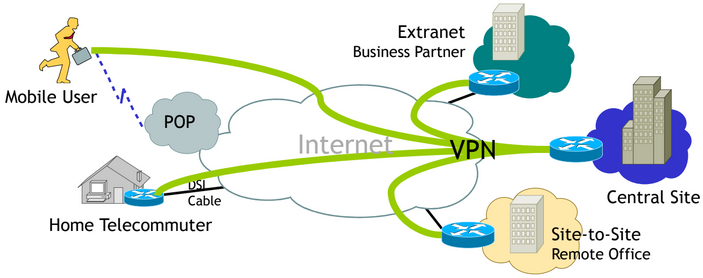
VPN

Red privada virtual.

Utilizando una red pública, armamos una red privada sobre ella.

Permite conectar dos puntos como si formaran una red privada, pero en realidad están atravesando la red de un proveedor.

# Variantes VPN

Generalmente una VPN refiere a un túnel IPSec sobre internet. Existen dos variantes:

* Remote access: permite al dispositivo (mobile user) operar como si estuviera directamente conectado a la red destino (central site).
* Site-to-site o LAN-to-LAN: si quiero comunicar dos redes (oficina central y sucursal, ambas con acceso a internet), mediante los routers configuro un túnel para que esas dos redes se comuniquen como si estuviesen directamente conectadas con un servicio privado de transmisión de datos. De esta manera logro la comunicación entre dos redes, a través de internet, de manera segura.

## Variantes de protocolos para tunneling

* PPTP:Desarrollado por MS, no provee encriptación (capa 2).
* L2TP: Desarrollado por Cisco y MS, mejora el PPTP incluyendo encripción a través de IPSec (ESP) (capa 2).
* **IPSec: Considerado el estándar actual (capa 3).**
* SSL: No requiere cliente de software (capa 4).

# IPSec (estándar actual de VPN)

Es una suite de protocolos destinados a proveer seguridad a nivel de red.

Dos protocolos:

* AH protocol: cabecera de autentificación.
* ESP protocol: Encrypted Security Payload.

## Modos de operación

Dos modos de operación:

* Modo transporte.
* Modo túnel.

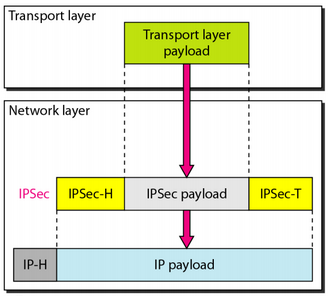
Dichos modos no afectan a la codificación de paquetes. **Los paquetes están protegidos por AH, ESP, o ambos en cada modo**.

Los modos aplican la directiva de un modo distinto cuando el paquete interior es un paquete IP, como en el caso siguiente:

* **En modo transporte**, el encabezado exterior determina la directiva IPsec que protege el paquete IP interior.
* **En modo túnel**, el paquete IP interior determina la directiva IPsec que protege su contenido.

### Modo transporte

La cabecera AH o ESP es insertada entre el área de datos y la cabecera IP, de tal forma que se mantienen las direcciones IP originales.

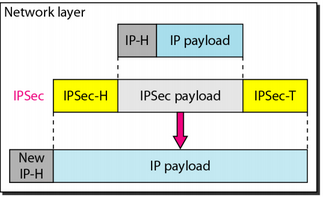
El contenido encapsulado en un datagrama AH o ESP proviene directamente de la capa de transporte. Por tanto, la cabecera IPSec se insertará a continuación de la cabecera IP y justo antes de los datos aportados por la capa de transporte. De esta forma, **sólo la carga útil es cifrada y autenticada.**

El modo transporte asegura la comunicación extremo a extremo pero **los extremos deben saber de la existencia del protocolo IPsec para poder entenderse**.

Es decir, encripta hasta el protocolo de transporte TCP pero **las direcciones host origen y destino son conocidas por todos** (la cabecera de IP no se encripta).

### Modo túnel

En el modo túnel, **el paquete IP entero (cabecera + datos) es cifrado y autenticado**. Este paquete **será encapsulado en un nuevo paquete IP**, por tanto, **la dirección IP cambiará por la del último paquete IP**. Por tanto, al paquete original se le añade una cabecera AH o ESP y a continuación se le añade la cabecera IP que servirá para encaminar el paquete a través de la red.

El modo túnel normalmente es usado para comunicar redes con redes, pero también se puede usar (y de hecho se usa), para comunicar ordenadores con redes y ordenadores con ordenadores. Este modo de funcionamiento **facilita que los nodos puedan ocultar su identidad de otros nodos que se estén comunicando.**

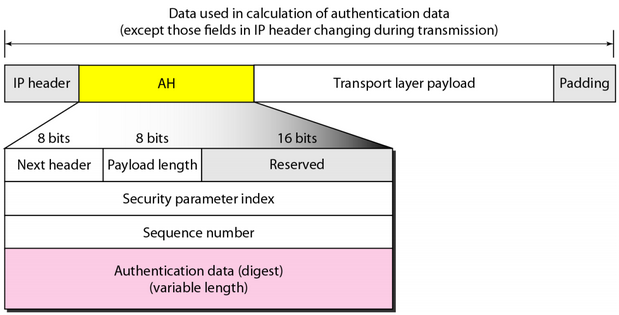
A diferencia del modo transporte**,** aquí se crea **un túnel entre los routers.** Cuando le llega el paquete del host al router, este ultimo al ver que el destino está al otro lado del router, encripta el paquete completo y le pone la **cabecera IP de dirección origen ese router y destino el otro router** (a diferencia de transporte que son la de los hosts). **En esa cabecera que agrega el router, el campo protocolo dice 50 (refiere a IPSec)**, por lo que el **router destino lo va a reconocer y lo va a desencriptar.**

## Protocolos

### AH (Authentication Header)

Encabezado de autenticación.

* Provee: autenticidad del origen e integridad de los datos (garantiza que no fue modificado)
* No provee: privacidad (no está encriptado el contenido de AH).

Estructura en transporte pero es ídem en túnel:

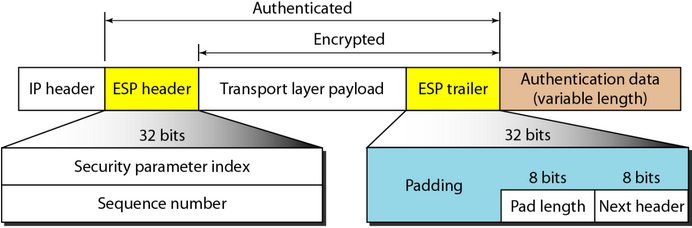
### ESP (Encapsulating Security Payload)

Carga de seguridad encapsulada.

* Provee autenticidad del origen, integridad de los datos **y privacidad**.

Mientras que el AH evita la manipulación de un paquete, el ESP garantiza que la información dentro del paquete esté encriptada y no pueda leerse. Se utilizan un encabezado ESP, un tráiler y un bloque de autenticación para cifrar la carga útil completa de un paquete.

Estructura en transporte pero es idem en túnel:



# Implementación

|  |  |
| --- | --- |
| Fase 1: IKE Policy | Fase 2: IPsec Policy |
| crypto isakmp policy 1  authentication pre-share  hash sha  encryption 3des  crypto isakmp key clave\_privada address 10.10.10.1 | crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac  access-list 102 permit ip X.X.X.X 0.0.0.255 Y.Y.Y.Y 0.0.0.255  crypto map IPSEC 20 ipsec-isakmp  set peer 10.10.10.1  match address 102  set transform-set ESP-3DES-SHA  interface serial 0  crypto map IPSEC |