CARACTERÍSTICAS DE UNA VPN

Cifrado de datos — Ocultamiento de IP

Acceso a redes restringidas — Protección contra ciber ataques

NIVELES DE SEGURIDAD EN UNA CONEXIÓN DE RED

CIFRADO DE DATOS

Se cifran los datos transmitidos para evitar el acceso no autorizado con técnicas como por ejemplo el sniffing en ataques man in the middle.

FIREWALLS Y SEGURIDAD PERIMETRAL

Las VPN suelen incorporar firewalls y otros mecanismos de seguridad perimetral para proteger las redes locales de las amenazas externas.

SEGURIDAD EN EL NIVEL DE ENLACE (Protocolo L2TP)

Puesto que la capa de enlace es la segunda, su seguridad está muy próxima al adaptador de red. Por tanto, los métodos para asegurar la info serán transparentes a los protocolos de alto nivel y a las aplicaciones de los usuarios.

SEGURIDAD EN EL NIVEL DE RED (Protocolo IPsec)

En el protocolo IP se produce el transporte de paquetes, los datos originales se encapsulan en paquetes IP que posteriormente son asegurados mediante el protocolo IPsec. De este modo, las aplicaciones son transparentes al método de seguridad elegido

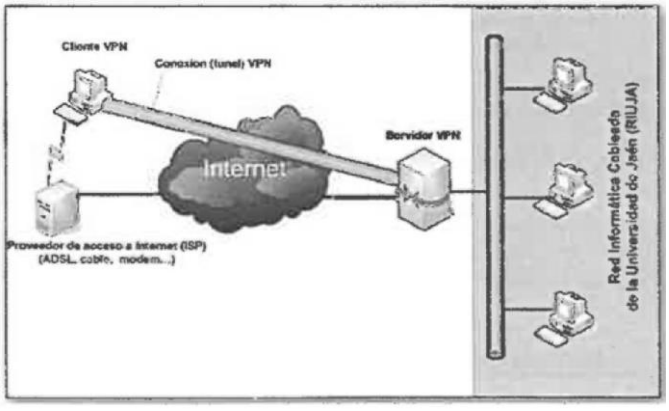
SEGURIDAD EN EL NIVEL DE APLICACIÓN (Protocolos https, smtps...)

En este caso la seguridad no es transparente a las aplicaciones puesto que estas deben ser reprogramadas para sustituir protocolos inseguros y que empiecen a utilizar las versiones seguras como http -> https o smtp -> smtps.

ARQUITECTURAS BÁSICAS DE VPN

LA TÉCNICA DE TUNELIZACIÓN

Consiste en encapsular un protocolo de red PDU sobre otro de nivel inferior denominado (protocolo de red encapsulador). De esta forma, se crea un túnel seguro para la transmisión de datos desde un extremo al otro a través de redes públicas.



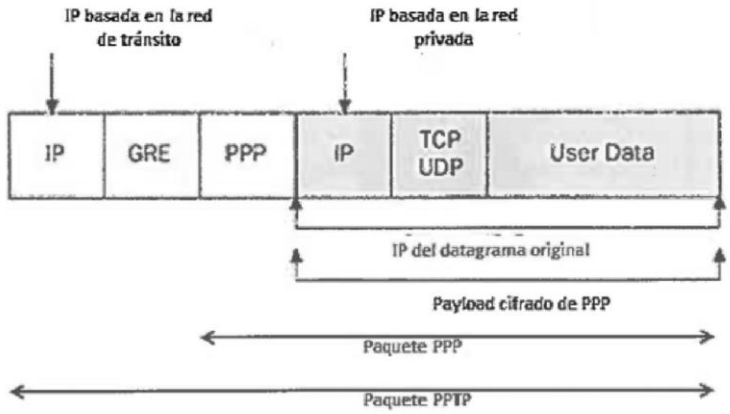


Figura 6.2. Encapsulamiento PPP y PPTP para la tunelización de datagramas IP.

El protocolo encapsulador desconoce los datos encapsulados

La tunelización evita ataques de tipo man in the middle

Campo PPP, que lleva el control de autenticación y cifrado propio del protocolo PPP (Point to Point Protocol).

Campo GRE, que lleva información sobre el túnel que establece PPTP.

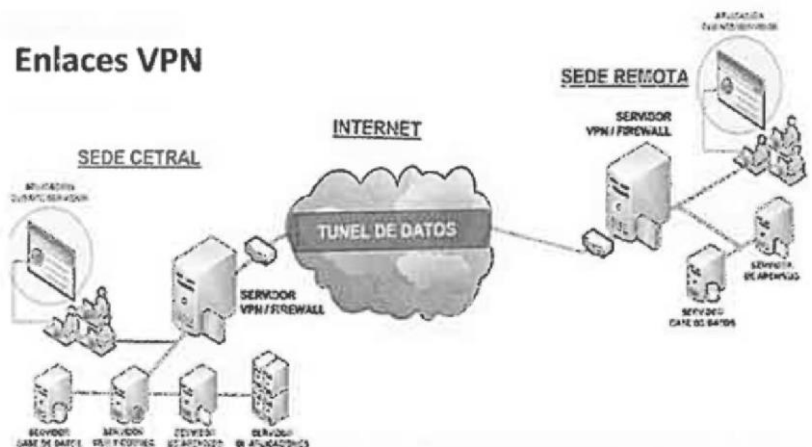
Campo IP, que especifica las direcciones IP de todo el paquete completo en la red de tránsito según las especificaciones de PPTP.

El paquete viaja por la red con la IP del paquete encapsulador (nunca el del encapsulado). Una vez que el paquete completo ha llegado al destino, el otro extremo del túnel extrae el paquete encapsulado, descifrándolo y poniéndolo en la red local de destino cuyas direcciones IP serán compatibles con las que tiene el paquete encapsulado.

ACCESO PUNTO A PUNTO

Este tipo de VPN el túnel se establece entre dos redes locales, por lo que cada red local debe tener su propio servidor VPN.

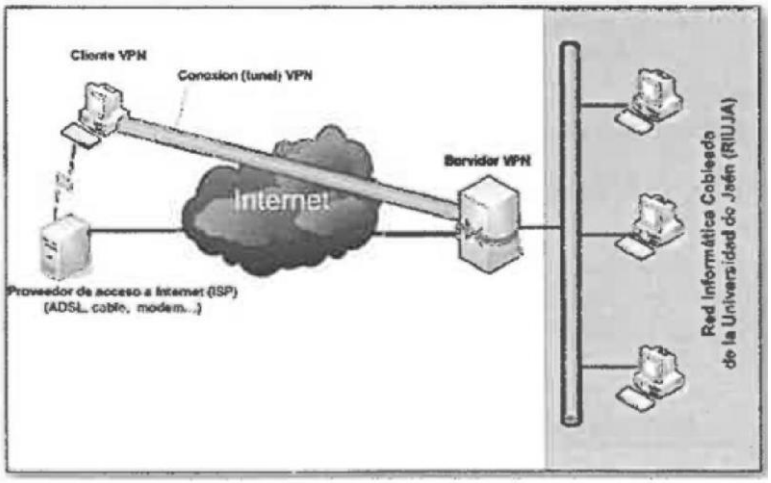
Los clientes de cada red podrán conectarse con el resto de clientes de la otra red como si estuvieran en la misma red local.



ACCESO REMOTO

Este tipo de VPN permite a los usuarios conectarse de forma segura a una red privada desde ubicaciones remotas a través de Internet, como desde sus hogares o sitios de teletrabajo. Se conectan al servidor VPN remoto que le proporciona el acceso a una red local.

Para la creación del túnel el usuario debe autenticarse en el servidor remoto. Solo aquellos usuarios con permiso podrán establecer el túnel.



VPN SOBRE LAN

Este tipo de VPN es muy eficaz para asegurar conexiones dentro de las redes locales. El esquema es semejante al del acceso remoto, pero sustituyendo Internet por la red local, impidiendo escuchas o suplantaciones dentro de la propia LAN. Se usa para aislar servidores o conjunto de ellos dentro de la LAN.

IMPLEMENTACIÓN DE UNA VPN

Las VPN pueden funcionar por software o por hardware que tienen mejor rendimiento y son más fáciles de configurar pero menos flexibles

Ell protocolo más utilizado es IPsec, aunque también se utilizan PPTP, LF2, L2TP, SSL/TLS, SSH, etc.

DIAL UP NETWOKING

El Dial-Up Networking (conexión mediante marcado) Tecnología obsoleta que permitía conexiones a internet o a una red atraves de la línea telefónica

RAS (Remote Access Server) es el software servidor de dial-up de Microsoft hasta Windows 2000. Posteriormente, se unió a un paquete mas amplio llamado RRAS (Routing and Remote Access Service).

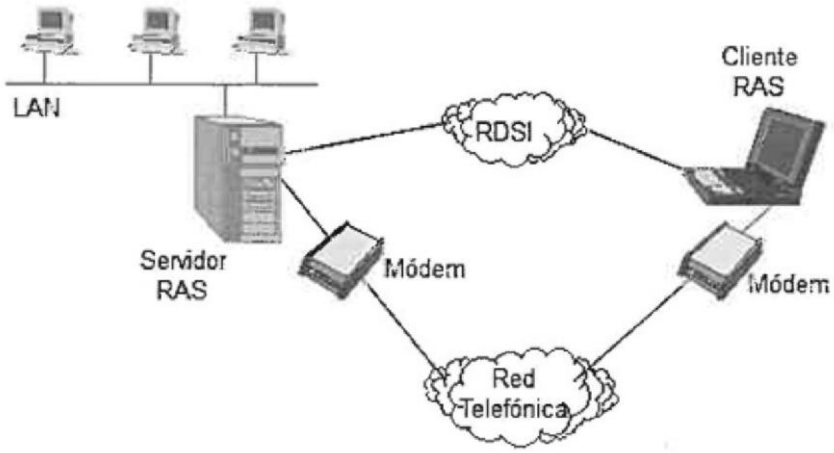


Figura 6.5. Conexiones posibles entre un cliente RAS y un servidor RAS.

PROTOCOLOS DE ACCESO REMOTO SLIP Y PPP

Son dos protocolos que conectan un cliente y un servidor mediante una conexión serie (módem o clable serie, normalmente).

Encapsulan los protocolos de alto nivel TCP e IP en tramas de datos de bajo nivel para transmitirlas

SLIP (Serial Line Internet Protocol)

- Anterior, más simple, solo transporta paquetes IP

- La IP del cliente y servidor hay que configurarla de manera estática

- NO cifra, NO comprime y NO corrige errores

- Sólo soporta transmisiones asíncronas

PPP (Point-to-Point Protocol)

- Más moderna, también transporta paquetes de otras capas.

- La IP del cliente y servidor se puede asignar automáticamente con DHCP

- SI cifra SI comprime SI corrige errores

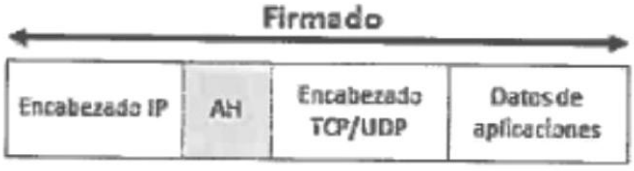
- Soporta transmisiones síncronas y asíncronas

	SLIP (Serial Line Internet Protocol)	PPP (Point-to-Point Protocol)
ANTIGÜEDAD	MAS ANTIGUO	MAS NUEVO
SOPORTA CIFRADO	NO	SI
SOPORTA COMPRESIÓN	NO	SI
CORRIGE ERRORES	NO	SI
TRANSMISIONES SÍNCRONAS	NO	SI
TRANSMISIONES ASÍNCRONAS	SI	SI
CONFIGURACIÓN DE IP	MANUAL (ESTÁTICA)	AUTOMÁTICA (DHCP)
TRANSPORTA PAQUETES IP	SI	SI
TRASN. PAQ DE OTRAS CAPAS	NO	SI

PROTOCOLO IPSEC (dos modos: transporte y tunel)

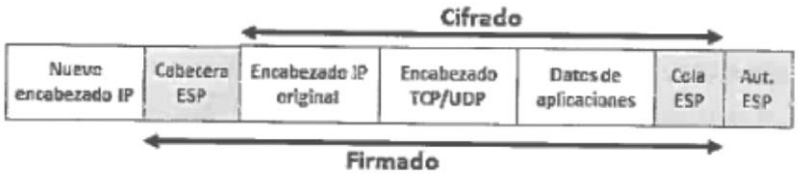
En modo transporte, IPsec solo encapsula los datos del datagrama IP, conservando la cabecera IP original del datagrama.

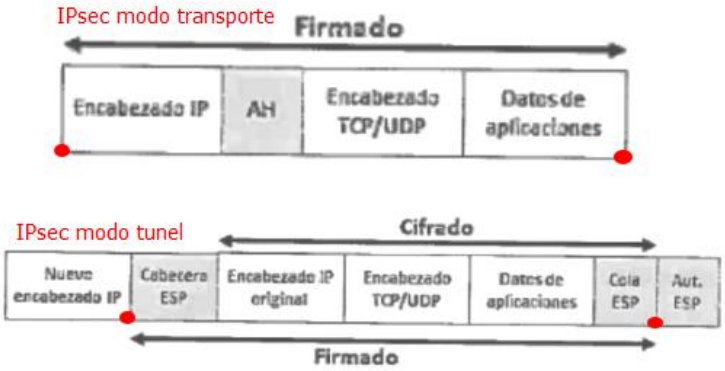
El cifrado es de extremo a extremo (host origen a host destino) por lo que todos los nodos de las redes que se conectan deben implementar tecnología IPsec



En modo túnel, el datagrama IP es encapsulado completamente dentro de IPsec, por lo que se requiere una nueva cabecera IP para poder enviar el datagrama por la red.

El cifrado es de router frontera a router frontera implementando una VPN de tipo punto a punto





PROTOCOLOS DE AUTENTICACIÓN EN LA RED

PAP (Password Authentication Protocol)

Protocolo de autenticación inseguro ya que envía el usuario y contraseña sin cifrar, alguien podría conseguir esa información capturando la trama PPP

CHAP (Challenge Handshake Authentication Protocol)

Protocolo de autenticación por desafio mutuo. En CHAP el cliente envía una petición de acceso con un hash de la contraseña (no la contraseña, que nunca viaja por la red). Entonces el servidor manda al cliente un desafío. El cliente utiliza un algoritmo hash (MDS) para calcular un resultado con su contraseña y el desafío, y lo envía al servidor. El servidor hace el mismo cálculo con la contraseña que él posee y compara el resultado con el recibido por el cliente. Solo si son iguales se permite el acceso.

EAP (Extensible Authentication Protocol)

Protocolo de autenticación extensible. EAP admite diversos modos de autenticación. Es más una arquitectura que un único protocolo. Puede utilizar tanto certificados digitales como tokens e incluso parejas usuario/contraseña. Es muy usado en redes inalámbricas y en conexiones punto a punto.

KERBEROS

Creado por el MIT (Instituto Tecnológico de Massachusetts) y estandarizado en la RFC 4120. Cliente y servidor se autentican recíprocamente. Utiliza cifrado AES (RFC 3962). Cada servidor, usuario o servicio dispone de una clave que se registra en una base de datos unificada en el servidor Kerberos.

El servidor Kerberos rula en Windows y Linux proporcionando tickets de sesión al usuario y al servidor para que puedan autenticarse en los servicios de red,