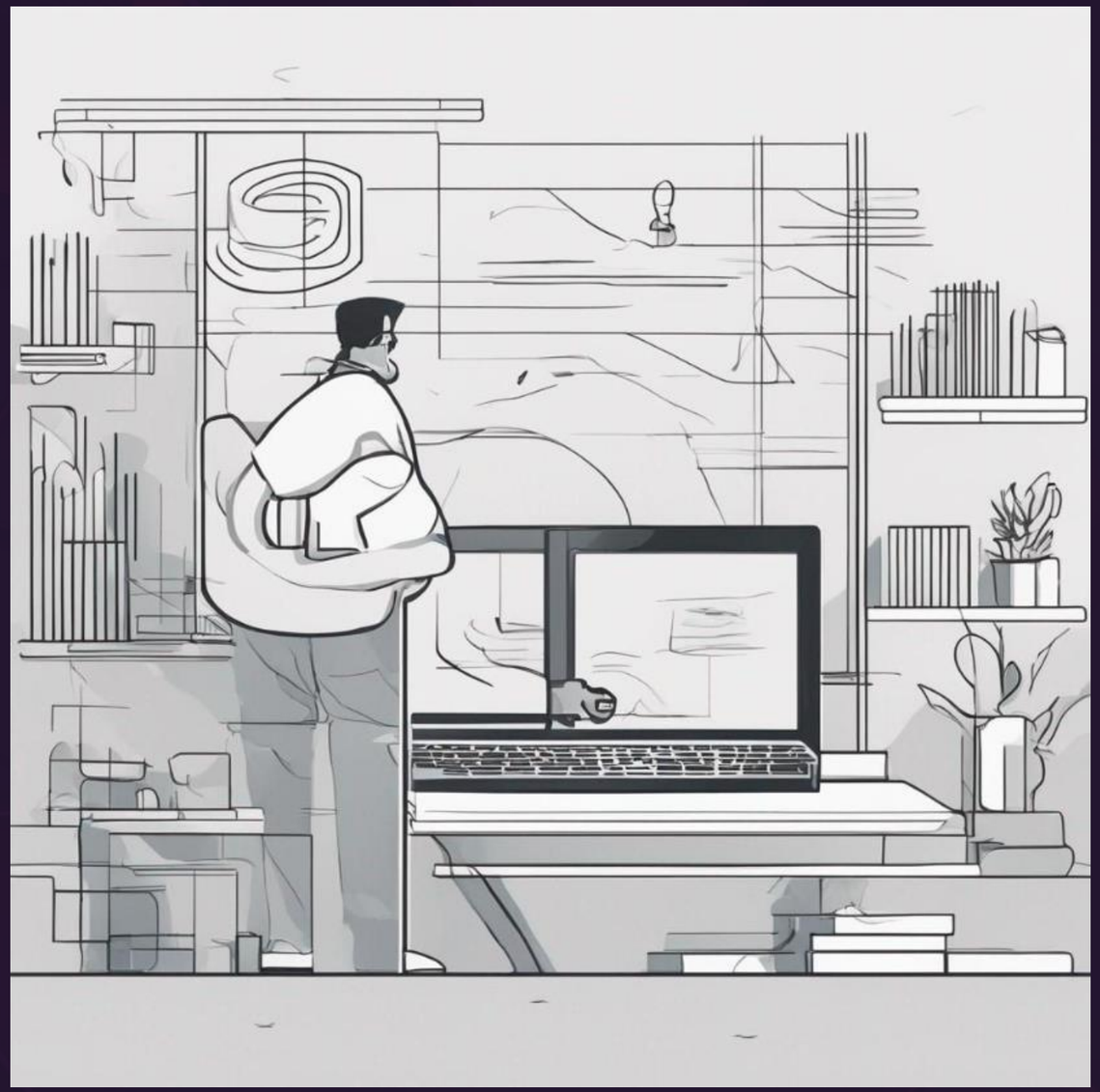
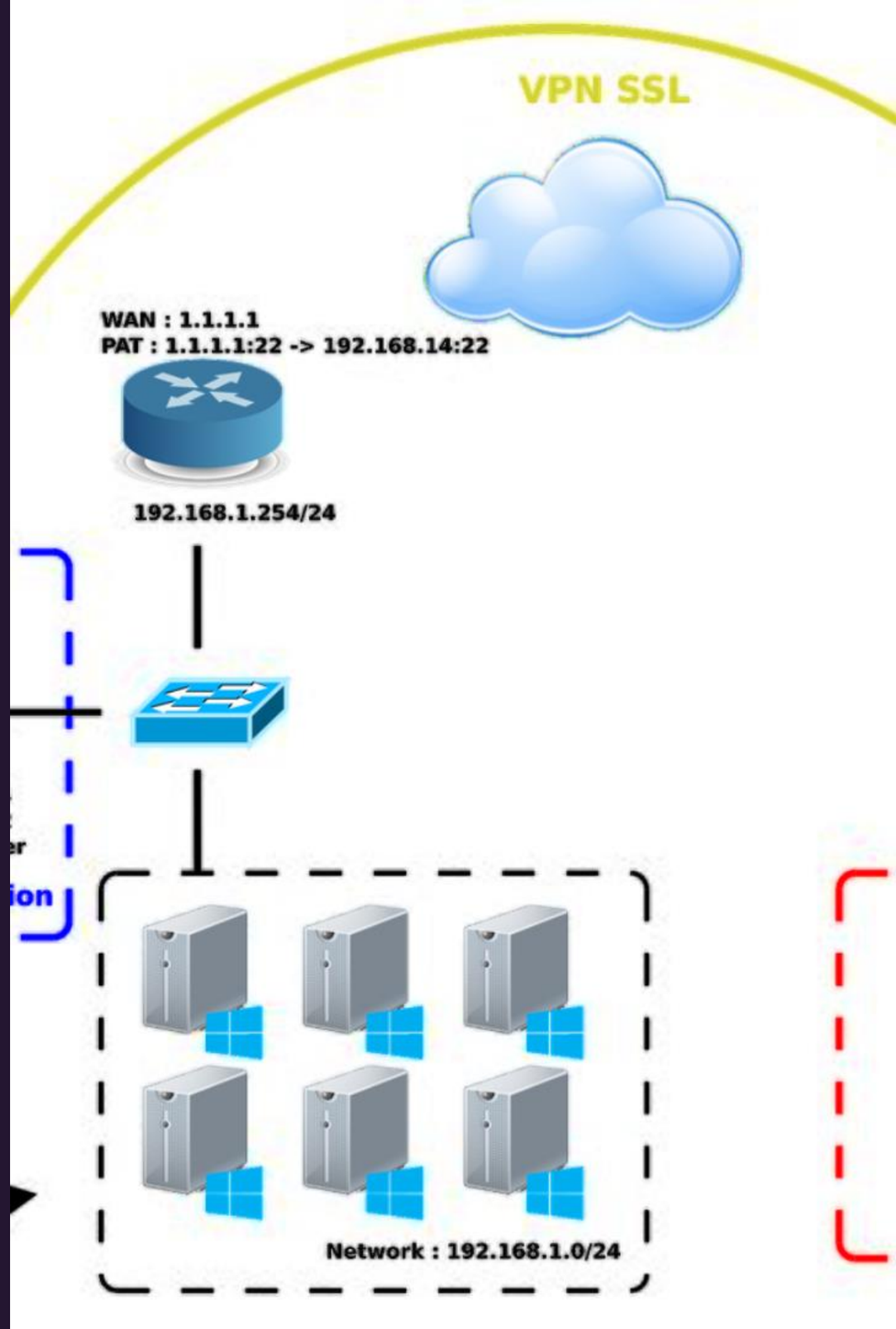
UT6. Acceso remoto con VPN



¿Qué es una VPN?

Una VPN, o Red Privada Virtual, es una tecnología de red que permite a los usuarios enviar y recibir datos de manera segura a través de una red pública, como Internet. Utiliza cifrado para garantizar la privacidad y la seguridad de la información transmitida a través de la red.

NM **by Nicolás Muro Martín**



6.1 Características de una VPN

Una VPN ofrece varias características importantes para garantizar la seguridad y la privacidad en línea. Estas incluyen el cifrado de datos, el ocultamiento de la dirección IP, el acceso a redes restringidas y la protección contra ataques cibernéticos.

6.1 Características de una VPN

En el acceso a un servicio por el sistema tradicional, cliente y servidor se conectan a Internet como punto de encuentro y las peticiones y respuestas se encaminarán a través de Internet y sus enrutadores como en cualquier otra red TCP/IP sin cifrar y con el riesgo de.que el tráfico sea capturado y suplantado, es decir, se utiliza una conexión no segura (Figura 6.1, arriba). Si en este tipo de conexión necesitamos seguridad será necesario que esta sea provista por algún protocolo de nivel superior, por ejemplo, https. No siempre se puede garantizar la existencia de este protocolo seguro de nivel superior, por ello es necesario encontrar otra solución que asegure las conexiones de equipos en redes públicas inseguras con independencia de los protocolos de nivel de aplicación.

6.1 Características de una VPN

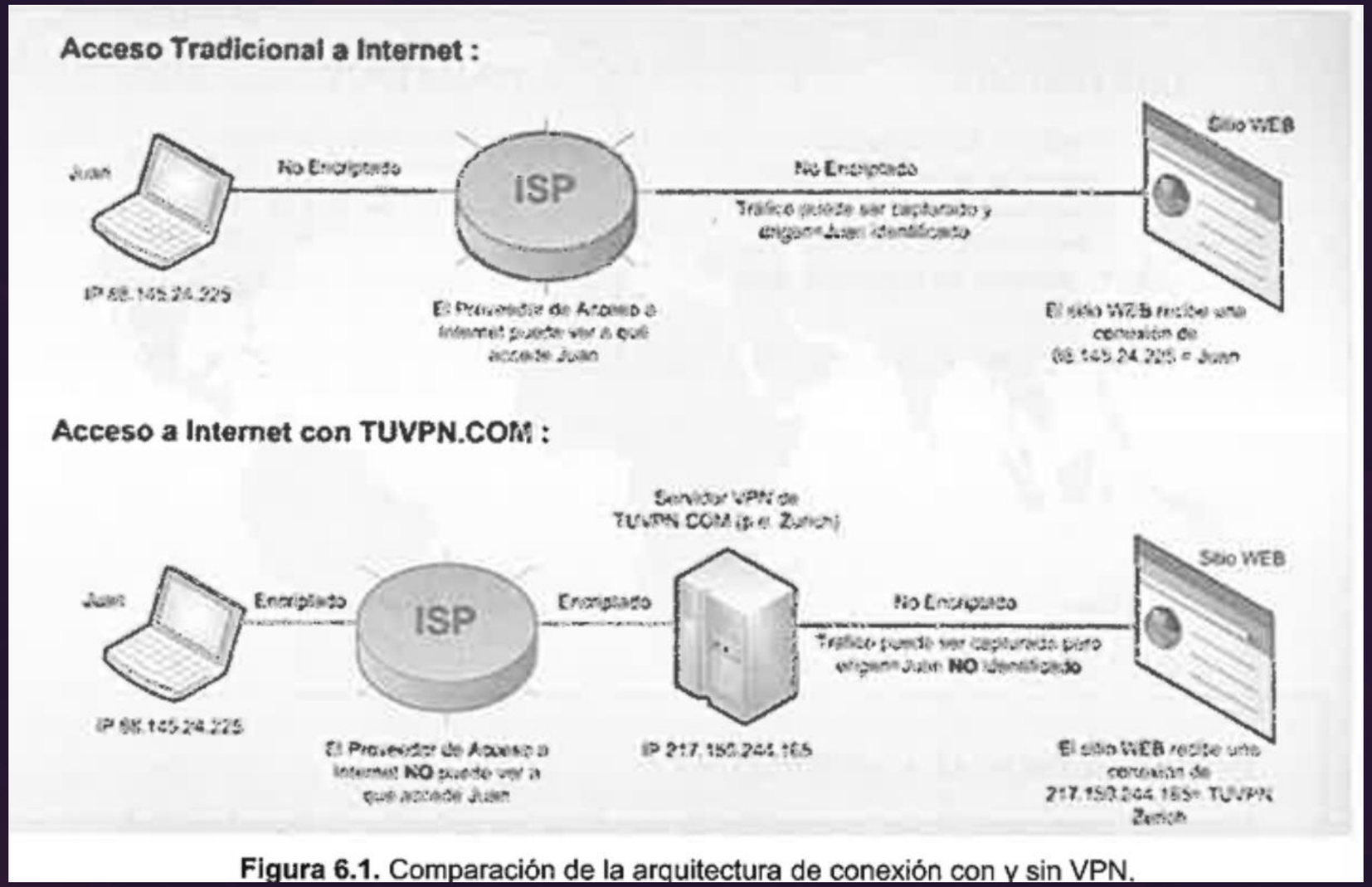
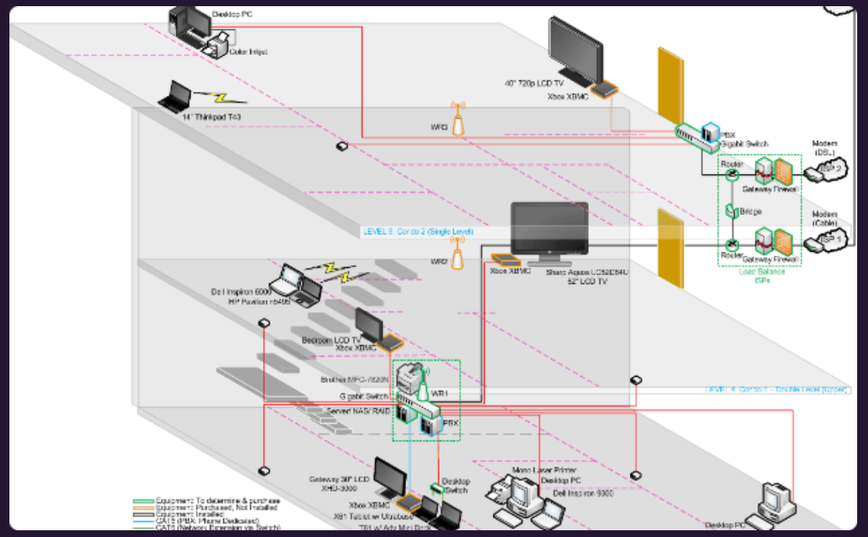
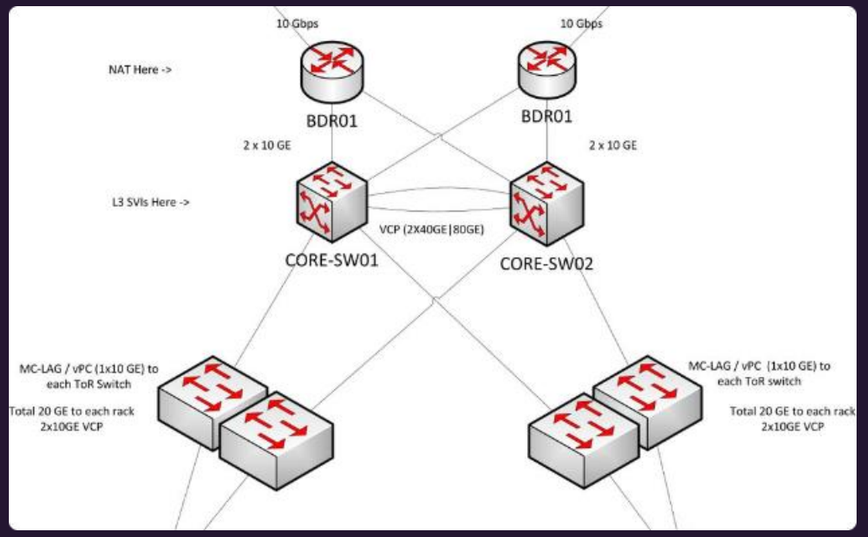


Figura 6.1. Comparación de la arquitectura de conexión con y sin VPN.

6.1.1 Niveles de seguridad en una conexión de red





Cifrado de Datos

Una VPN garantiza un alto nivel de seguridad mediante el cifrado de los datos transmitidos. Esto evita el acceso no autorizado a la información confidencial, protegiendo la privacidad de los usuarios.

Firewalls y Seguridad Perimetral

Las VPNs suelen incorporar firewalls y mecanismos de seguridad perimetral para proteger las redes locales y los dispositivos de los usuarios contra amenazas externas y ataques cibernéticos.

6.1.1 Niveles de seguridad en una conexión de red

Seguridad en el nivel de enlace

Puesto que la capa de enlace es el de más bajo nivel (solo por encima del físico) su seguridad está muy próxima al adaptador de red. Por tanto, si se consigue algún método para asegurar este nivel, su implementación será transparente a los protocolos de alto nivel y, en concreto, a las aplicaciones de los usuarios. Un ejemplo de protocolo de seguridad en este nivel es L2TP, al que nos referiremos más adelante.

6.1.1 Niveles de seguridad en una conexión de red

Seguridad en el nivel de red

Se trata de asegurar el protocolo IP que es el protocolo que produce el transporte de paquetes. Este es el tipo de seguridad que se consigue con IPsec. Para que una aplicación pueda asegurar sus conexiones deberá encapsular los datos a enviar en paquetes IP que serán asegurados mediante IPsec, haciendo también las aplicaciones transparentes al método de seguridad elegido.

6.1.1 Niveles de seguridad en una conexión de red

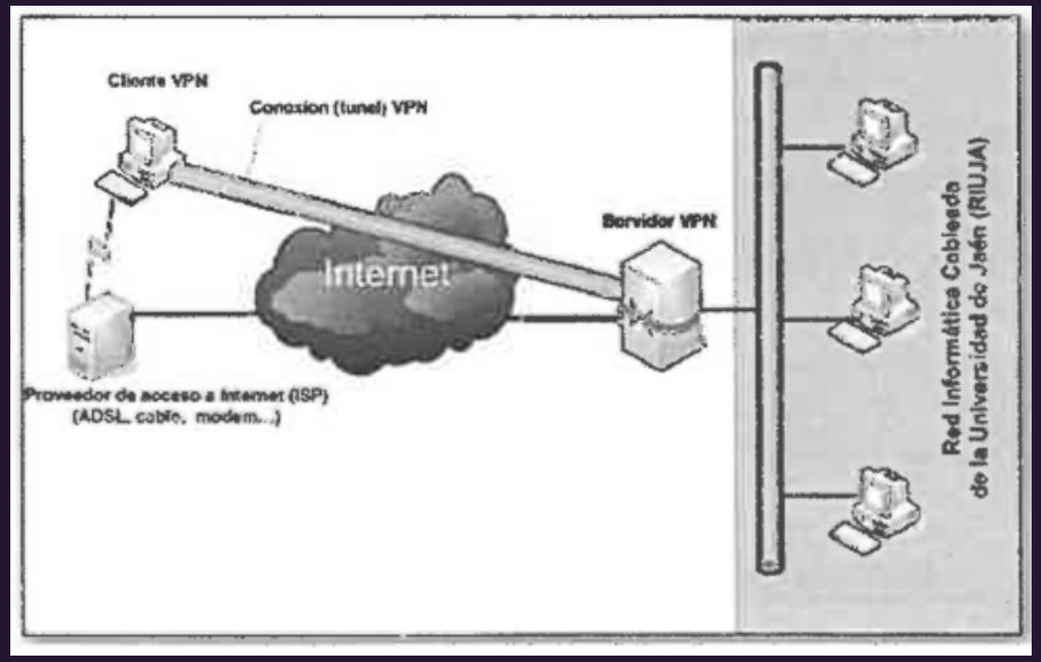
Seguridad en el nivel de aplicación

En este caso se trata de sustituir el protocolo inseguro por otro más seguro pero funcionalmente equivalente. Así, sustituiríamos las conexiones http por conexiones https, smtp por smtps, etc. En este caso la seguridad no es transparente a las aplicaciones puesto que estas deben ser reprogramadas para que puedan utilizar las versiones seguras de protocolos de comunicación.

6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

Consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de ordenadores, que se implementa incluyendo una PDU (Protocol Data Unit) determinada dentro de otra PDU de nivel inferior con el objetivo de transmitirla entre los extremos del túnel sin que sea necesaria una inspección intermedia de los valores de control del protocolo encapsulado, que pasará totalmente desapercibido al protocolo encapsulador. Obviamente, una tunelización evita ataques del tipo Man-In-The-Middle.



6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

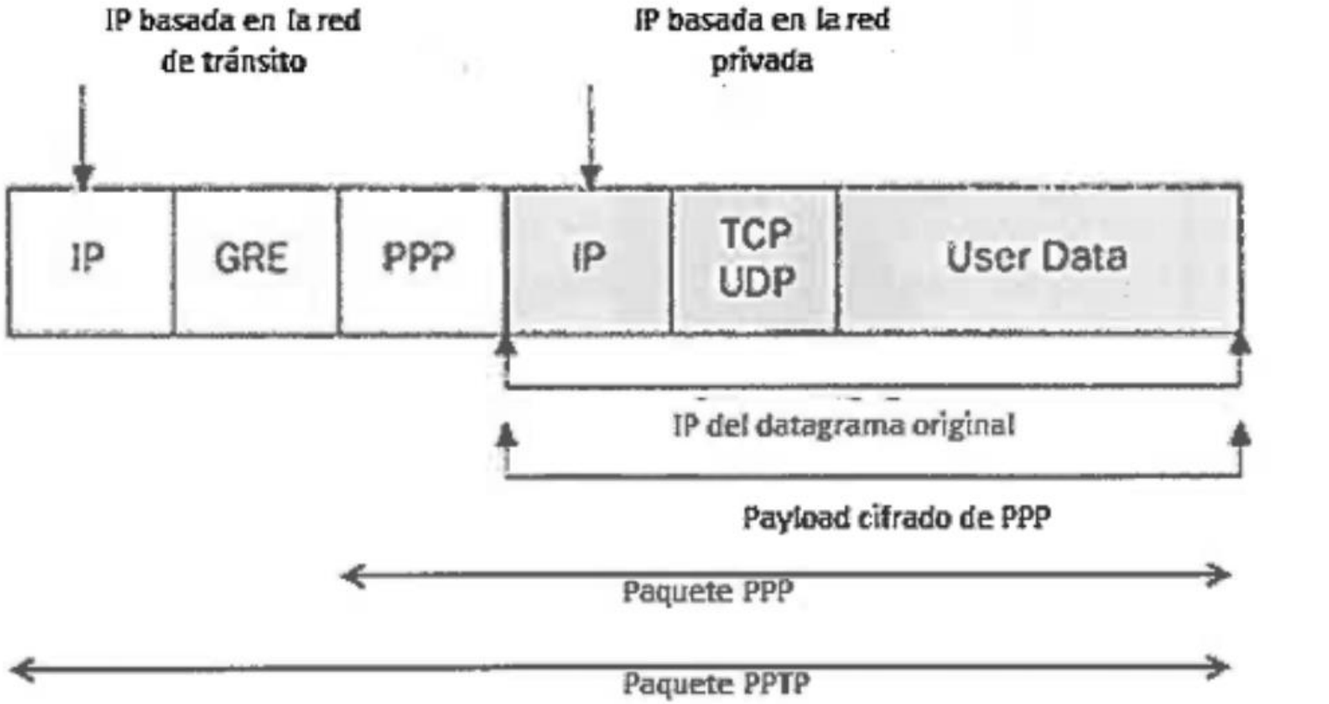


Figura 6.2. Encapsulamiento PPP y PPTP para la tunelización de datagramas IP.

6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

En la Figura 6.2 podemos ver la estructura de un paquete PPTP (Point to Point Tunneling Protocol), propio de túneles VPN. Este paquete contiene otro de tipo PPP que lleva su propia cabecera y que además cifra su carga. Esta carga es un datagrama IP. Como se ve el datagrama original tiene su campo de especificación de direcciones IP (propias de la red origen y destino, pero no de la red de tránsito), la información de nivel de transporte (TCP, UDP) y los datos de usuario que proceden de la capa de aplicación. Se trata de encapsular este paquete dentro de otro en el que añadimos tres cabeceras:

6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

• 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.

6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

La información de enrutado en la red de tránsito se hace de acuerdo 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.

6.1.2 Arquitecturas básicas de VPN

Acceso Remoto

Acceso Punto a Punto

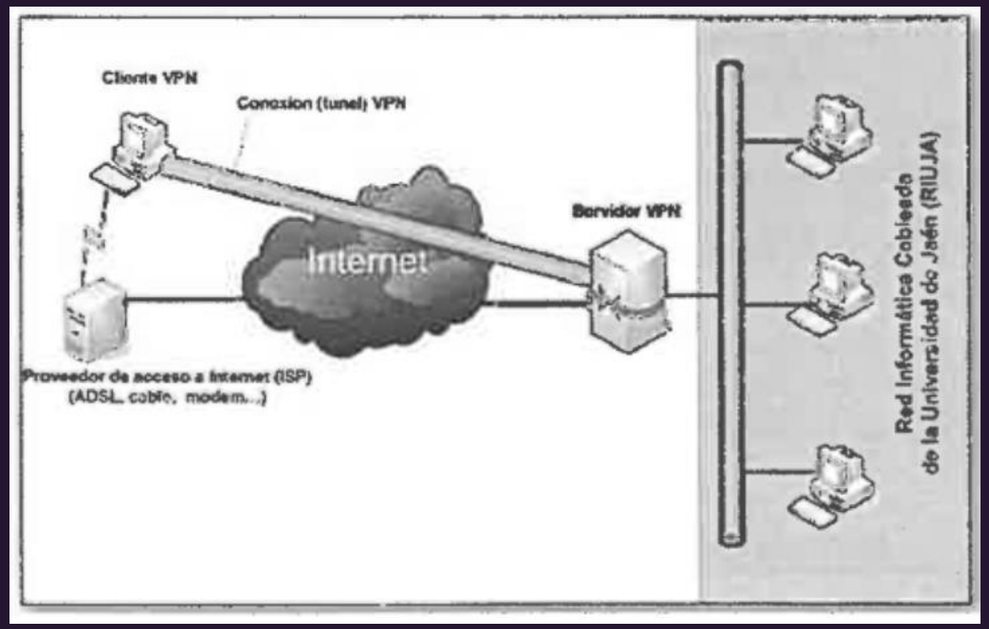
VPN sobre Lan

6.1.2 Arquitecturas básicas de VPN

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.



6.1.2 Arquitecturas básicas de VPN

Acceso Punto a Punto

Este tipo de VPN el tunel 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.

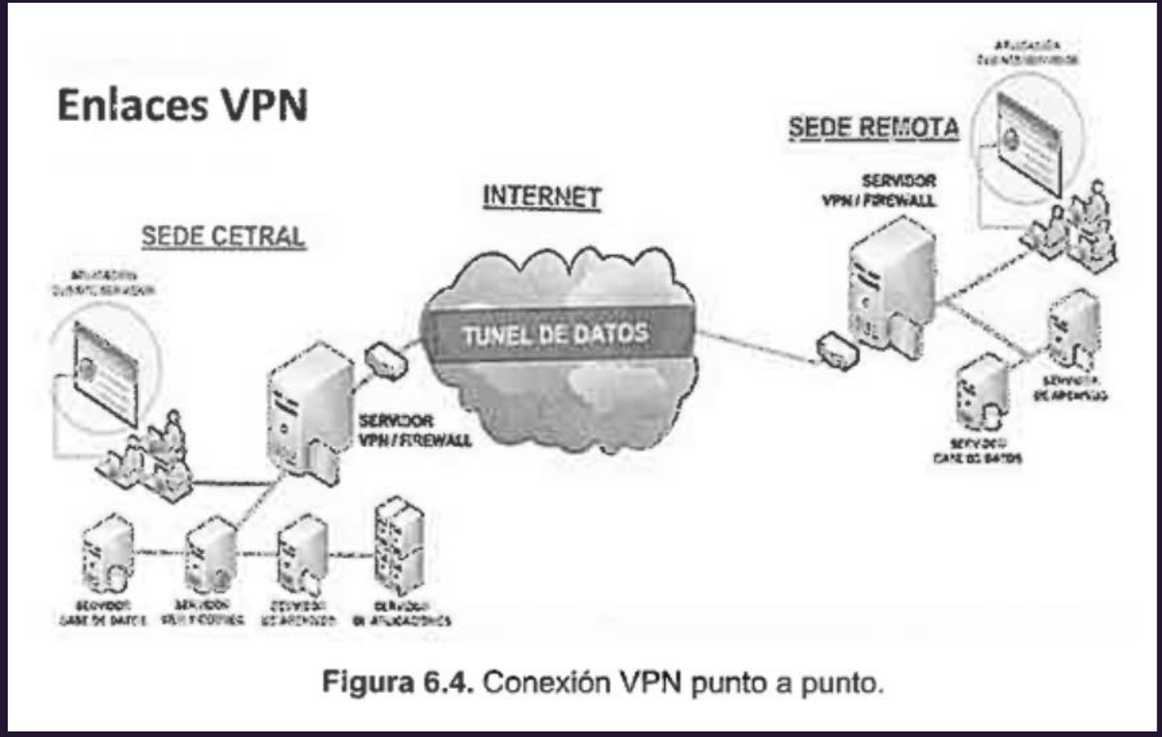


Figura 6.4. Conexión VPN punto a punto.

6.1.2 Arquitecturas básicas de VPN

VPN sobre LAN

Este tipo de VPN es muy eficaz para asegurar conexines 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 suele utilizar para aislar servidores o conjunto de ellos dentro de la LAN.

6.1.3 Implementación de una VPN

Requisitos básicos para establecer una VPN

- Una conexión a Internet o a la red local.
- Dos direcciones IP para cada extremo del tunel. Si la red de tránsito es Internet, las dos direcciones IP deberían ser públicas.

6.1.3 Implementación de una VPN

El protocolo más utilizado es IPsec, pero también se pueden utilizar PPTP, LF2, L2TP, SSL/TLS, SSH, etc.

Las soluciones VPN se pueden implementar pos hardware o por software. Las soluciones hardware tienen mayor rendimiento y son más fáciles de configurar, sin embargo, tienen menos flexibilidad que las de software.

6.2 Protocolos y técnicas específicas de VPN

6.2.1 Dial-up networking

El Dial-Up Networking (conexión mediante marcado) es una antigua tecnología que permitía a los usuarios conectarse a Internet o a una red utilizando una línea telefónica estándar.

RAS (Remote Access Server) es el software servidor de dial-up que Microsoft proveía en sus sistemas operativoshasta su versión Windows 2000. Posteriormente, RAS pasó a ser parte de un paquete software más amplio denominado RRAS (Routing and Remote Access Service).

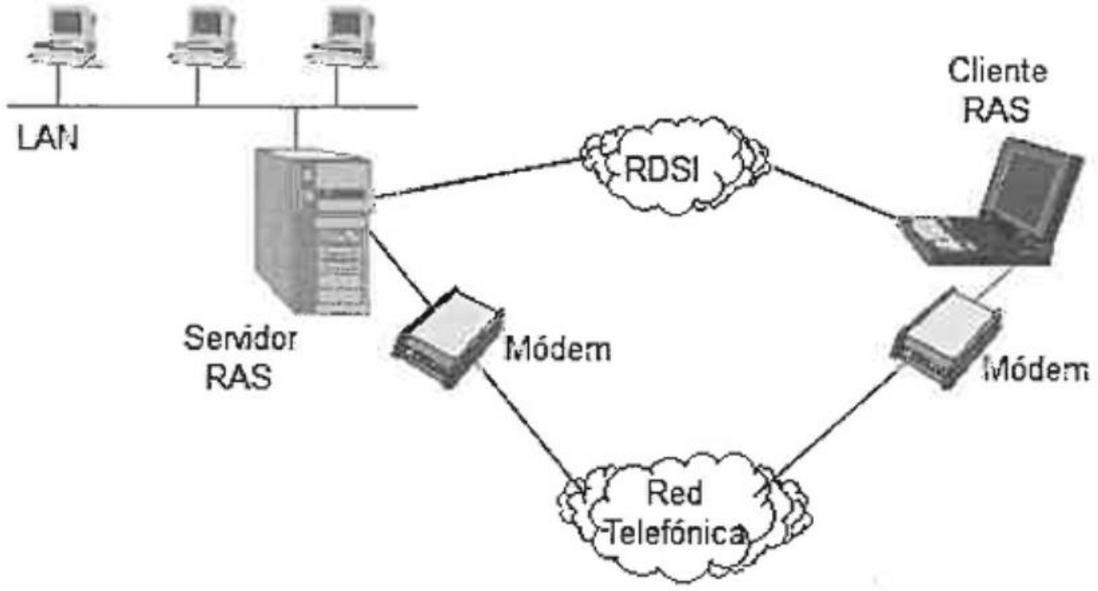


Figura 6.5. Conexiones posibles entre un cliente RAS y un servidor RAS.

6.2.2 Protocolos de acceso remoto

El Dial-Up Networking (conexión mediante marcado) es una antigua tecnología que permitía a los usuarios conectarse a Internet o a una red utilizando una línea telefónica estándar.

RAS (Remote Access Server) es el software servidor de dial-up que Microsoft proveía en sus sistemas operativoshasta su versión Windows 2000. Posteriormente, RAS pasó a ser parte de un paquete software más amplio denominado RRAS (Routing and Remote Access Service).

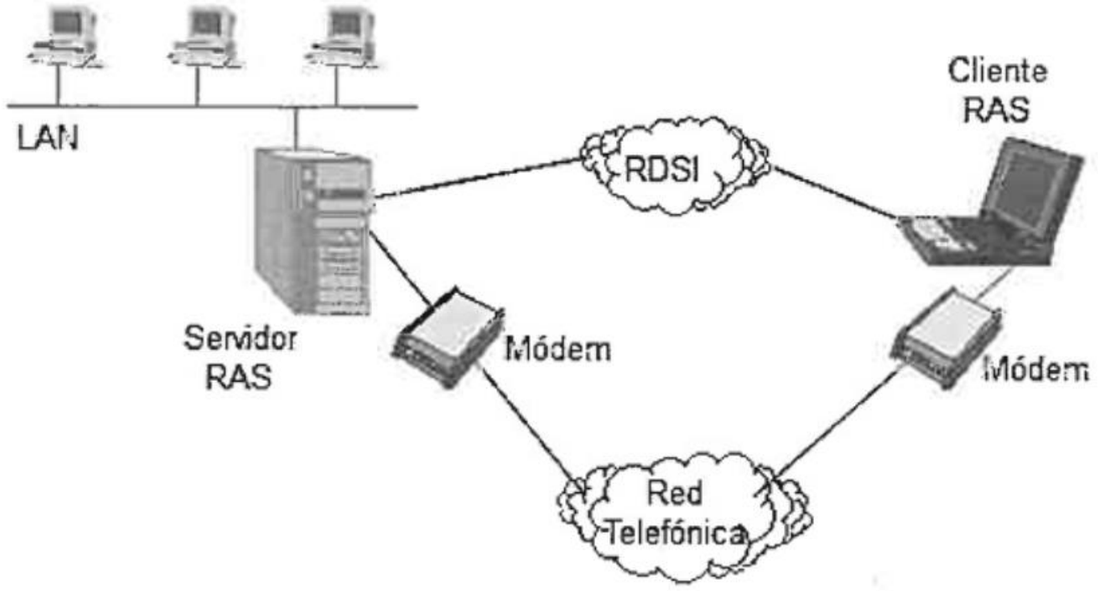


Figura 6.5. Conexiones posibles entre un cliente RAS y un servidor RAS.

6.2.3 Protocolos de acceso remoto

SLIP y PPP

SLIP (Serial Line Internet Protocol) y PPP (Point-to-Point Protocol) son dos protocolos que permiten a un cliente conectarse a un servidor utilizando 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 ser transmitido por las líneas serie.

6.2.3 Protocolos de acceso remoto

SLIP

-Anterior y más simple

-Sólo puede transportar paquetes IP

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

- No hace corrección de errores ni compresión

- No soporta cifrado

- Sólo soporta transmisiones asíncronas

PPP

-Posterior

- Puede transportar paquetes de otras capas de red.

- La IP del cliente y servidor se puede asignarautomáticamente con técnicas de DHCP

- Sí hace corrección de errores y compresión

- Soporta cifrado

- Soporta tato transmisiones síncronas como asíncronas

6.2.3 Protocolos de acceso remoto

PPPoE

PPP over Ethernet es el estándar que permite conectar estaciones utilizando PPP sobre Ethernet.

En la creación de túneles, PPP se suele utilizar con un protocolo de tunelización denominado GRE, pero también puede utilizarse L2TP.

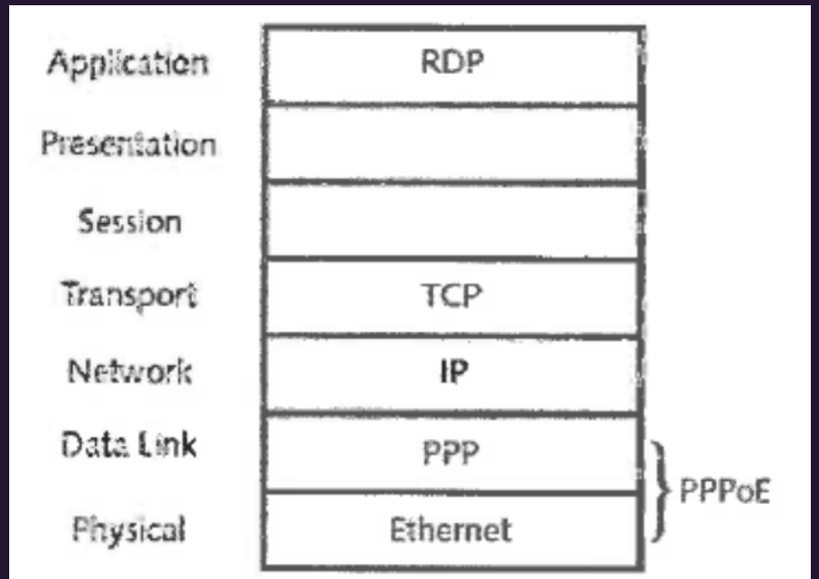


Figura 6.6. Pila de protocolos para el acceso remoto.

6.2.3 Protocolos de acceso remoto

PPPoE

En la Figura 6.6 se puede ver la arquitectura de protocolos utilizados para realizar una conexión RDP y abrir una sesión de escritorio remoto en un servidor. RDP seria le protocolo de la capa de aplicación que se encapsula sobre TCP e IP. Por debajo, para asegurar la conexión, en vez de crear una trama Ethernet se crea una trama PPPoE que encapsula a su vez un protocolo PPP, que proporciona el cifrado y autenticado, para finalmente construir una trama Ethernet

6.2.4 Protocolos de tunelización PPTP y L2TP

PPTP

PPTP (Point-to-Point Tunneling Protocol) es un protocolo desarrollado por Microsoft que expande las características de PPP que le encapsula para que cualquier tipo de datos PPP puedan atravesar Internet como una transmisión IP habitual. Soporta eneriptación. autenticación y servicios de acceso, que son provistos por RRAS en las versiones servidoras de Windows. Los clientes pueden llamar directamente al servidor RRAS o bien a su ISP primero y luego hacer una conexión de tipo VPN.

6.2.4 Protocolos de tunelización PPTP y L2TP

L2TP

L2TP (Layer 2 Tunneling Protocol) está desarrollado por Cisco y estandarizado por la IETF como heredero de PPTP Y L2F (de Cisco). Encapsula datos como PPP, pero a diferencia de él está aceptado por multitud de fabricantes. Pm? y L2TP no solo se utilizan en la creación de túneles VPN, sino que también son utilizados en las redes por sus capacidades de encriptación de datos.

6.2.5 Protocolo IPsec

IPsec

Es una extensión dcl protocolo IP que permiten asegurar las comunicaciones sobre IP, autenticando y. si se desea, cifrando los paquetes IP de una comunicación. IPsec trabaja en la capa de red y por ello puede ser utilizado por cualquier aplicación sin necesidad de realizar ninguna modificación en la configuración de la misma.

IPsec puede utilizar uno de dos protocolos, Authentication Header (AH) o Encapsulationg Security Payload (ESP). Además IPsec tiene que utilizar ISAKMP (Internet Security Association and Key Management Protocol), un protocolo de gestión de claves de cifrado.

6.2.5 Protocolo IPsec

IPsec

• AH proporciona integridad, autenticación y no repudio de todo el paquete enviado, incluyendo la cabecera IP.

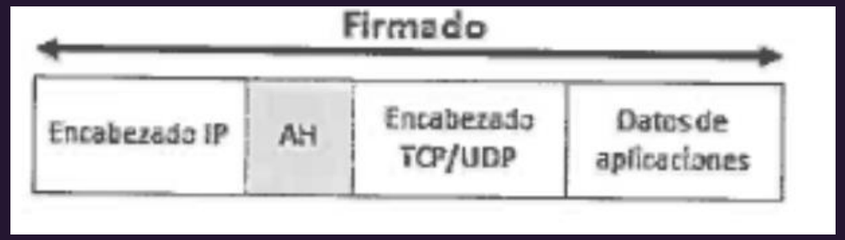
• ESP añade a lo anterior el cifrado de toda la información que se envía, pero no incluye en sus cálculos los datos de la cabecera IP.

6.2.5 Protocolo IPsec

IPsec

IPsec puede funcionar en dos modos distintos, modo transporte y modo túnel.

• En modo transporte, IPsec solo encapsula los datos del datagrama IP, conservando la cabecera IP original del datagrama. En este caso, el cifrado se realiza de extremo a extremo, es decir, desde el host de origen al host de destino. Para implantar esta solución es necesario que todos los nodos de las redes origen y destino implementen la tecnología IPsec.



6.2.5 Protocolo IPsec

IPsec

• En nodo 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. En este caso el cifrado se implementa exclusivamente entre los routers de fontera en cada una de las redes origen y destino, implementando una VPN de tipo punto a punto.

6.2.5 Protocolo IPsec

IPsec

- La ventaja que tiene el modo túnel frente al modo transporte es que no requiere que todos los nodos implementen IPsec.
- El inconveniente del modo túnel es que, al no ser extremo a extremo, es menos seguro puesto que se pueden producir escuchas y suplantaciones en las redes locales origen y destino.
- El modo túnel es más apropiado para proteger el datagrama IP completo y proporcionar una comunicación entre gateways.
- El modo transporte es más apropiado para proteger intranets y las comunicaciones de host a host, pero lleva una mayor carga administrativa.

6.2.5 Protocolo IPsec

Ejemplo encapsulamiento en una VPN

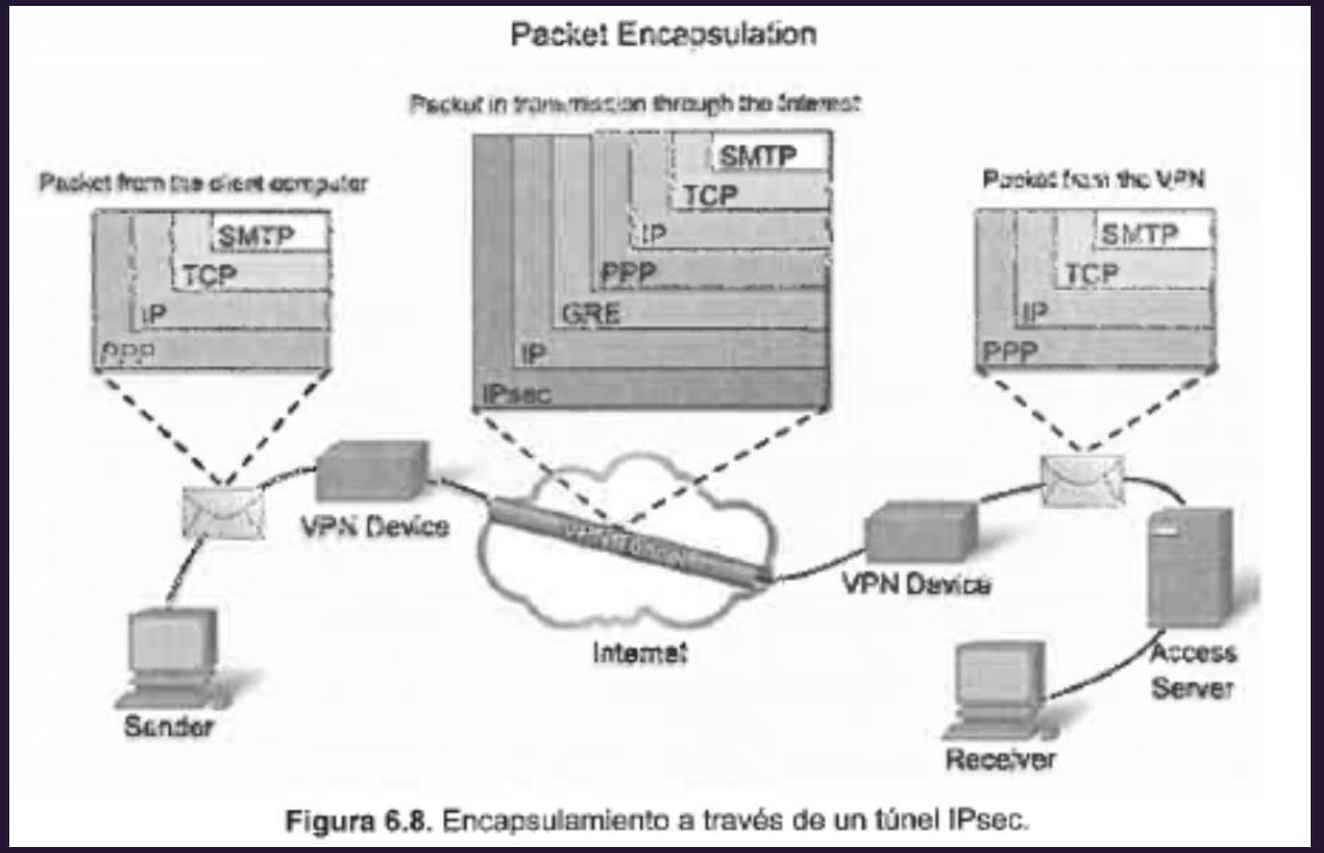


Figura 6.8. Encapsulamiento a través de un túnel IPsec.

6.2.5 Protocolo IPsec

Ejemplo encapsulamiento en una VPN

En origen, el mensaje de correo electrónico es enviado al servidor de correo mediante el protocolo SMTP (nivel de aplicación). Este mensaje será encapsulado sobre TCP en el que se añadirá la información de control (puerto 25, que es el que corresponde con SMTP). A su vez se encapsulará sobre un datagrama IP que será encapsulado sobre PPP para proporcionar el acceso al dispositivo VPN en origen que es el primer extremo del túnel.

Una vez en el túnel habrá que encapsular el paquete PPP para que pueda ser transportado por un túnel IPSec, por lo que habrá que añadirle las cabeceras GRE (gestión del túnel), un nuevo sistema de direccionamiento IP compatible con las IP del túnel en Internet y, por último IPsec en alguno de sus modos (transporte o túnel).

El paquete será transmitido por el túnel utilizando el sistema de direccionamiento IP externo y a la llegada al dispositivo VPN de salida, éste lo desencapsulará para recuperar el paquete PPP de origen quien realizará las operaciones inversas hasta extraer el contenido SMTP y lo depositará en el buzón del destinatario del correo.

6.3 Autenticación de usuarios y sitemas

6.3.1 Protocolos de autenticación en la red

PAP (Password Authentication Protocol)

Protocolo de autenticación de contraseña. En PAP las credenciales del usuario, representadas por el nombre de usuario y su contraseña, se envían por la red sin cifrar, por lo que es un método de autenticación inseguro. Una captura de la trama PPP permitiría un examen libre de la contraseña

6.3.1 Protocolos de autenticación en la red

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.

6.3.1 Protocolos de autenticación en la red

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 utilizado en la autenticación sobre redes inalámbricas y en conexiones punto a punto.

6.3.1 Protocolos de autenticación en la red

EAP-TLS (EAP Transpon Layer Security)

Es una extensión de EAP que permite que EAP interaccione con un servidor RADIUS que proporciona la autenticación de credenciales y las claves de cifrado haciendo de EAP uno de los protocolos más seguros y muy habitual en dispositivos inalámbricos corporativos. También admite la gestión del cifrado y autenticación mediante certificación digital.

6.3.1 Protocolos de autenticación en la red

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. Cliente y servidor confían en el servidor Kerberos, quien les proporciona tickets de sesión que posteriormente serán utilizados para autenticarse frente a los servicios de red. Tanto los sistemas Windows como los GNU/Linux pueden usar Kerberos.

6.3.2 Servidores RADIUS

RADIUS (Remote Authentication Dial-In User Service) es un servicio y un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. El estándar RADIUS está publicado en los RFC números 2138 y 2139 y se le ha dotado de una arquitectura extensible, de modo que aunque el estándar alberga una mayoría de características comunes a todos los fabricantes, permite que cada implementación utilice sus propios dialectos que los hacen característicos. Esta es la razón por la que ocasionalmente el administrador se encuentre con algunas incompatibilidades de unos fabricantes a otros.

6.3.2 Servidores RADIUS

Básicamente las funciones que provee un servidor RADIUS son tres que suelen abreviarse como las tres A (AAA):

1. Autenticación (authentication), que valida las cuentas de los usuarios.
2. Autorización (authorization), que permite o deniega una operación al usuario autenticado.
3. Contabilidad o registro (accounting o loggin), que registra la actividad del servicio.

6.3.2 Servidores RADIUS

Figura 6.9. Elementos de configuración de una instalación RADIUS.

Cuando un cliente necesita ganar el acceso a una red por ejemplo, mediante módem, ADSL, Ethernet o Wi-Fi, envía sus credenciales para que sean validadas en la red.

Esta información se transfiere a un dispositivo denominado Network Access Server (NAS) o authenticator sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS.

El NAS puede ser el puerto del conmutador de conexión que permitirá o denegará el acceso a la red una vez que se valide la autenticación.

El usuario típicamente utilizará como credenciales un nombre de usuario y una contraseña aunque se pueden configurar otros métodos de autenticación.

El servidor RADIUS comprueba las credenciales utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso a la red a través del NAS y le asigna los recursos de red necesarios para realizar la conexión, tales como una dirección IP u otros parámetros como la configuración de L2TP, etc.

6.4 Control de acceso por puertos

IEEE 802.1X es una norma del IEEE que estandariza el control de acceso a red basado en puertos corno parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o denegando el acceso por ese puerto si la autenticación falla.

802.1X está disponible en la mayor parte de los conmutadores de red no domésticos y puede configurarse para autenticar nodos que están equipados con software suplicante (el cliente de acceso). El filtrado de la conexión de acceso se realiza en la el nivel de enlace de datos.

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos corno complemento de seguridad a las técnicas de cifrado específicas para Wi-Fi.

6.4 Control de acceso por puertos

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos corno complemento de seguridad a las técnicas de cifrado específicas para Wi-Fi.

Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación del cliente o, con mayor precisión, una autenticación recíproca entre cliente y punto de acceso de gran fortaleza utilizando protocolos seguros como EAP-TLS.

6.4 Control de acceso por puertos

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos corno complemento de seguridad a las técnicas de cifrado específicas para Wi-Fi.

La arquitectura de un escenario IEEE 802.1X tiene tres capas:

• **Supplicant**. Es el cliente que quiere conectarse a la red.

• **Authenticator**. Es el dispositivo que posee los puertos de conexión y que permitirá o denegará las conexiones.

• **Autbentication server**. Es quien autentica a los usuarios informando al authenticator sobre si debe o no permitir la conexión solicitada por el supplicant o suministrando otro tipo de valores como la VLAN a la que debe conectarle.

Nonnalmente el servidor de autenticación es un servidor RADIUS que puede emplear una amplia variedad de protocolos de autenticación: Usuario y contraseña (con o sin cifrado), certificados digitales, tokens, etc.

6.4 Control de acceso por puertos

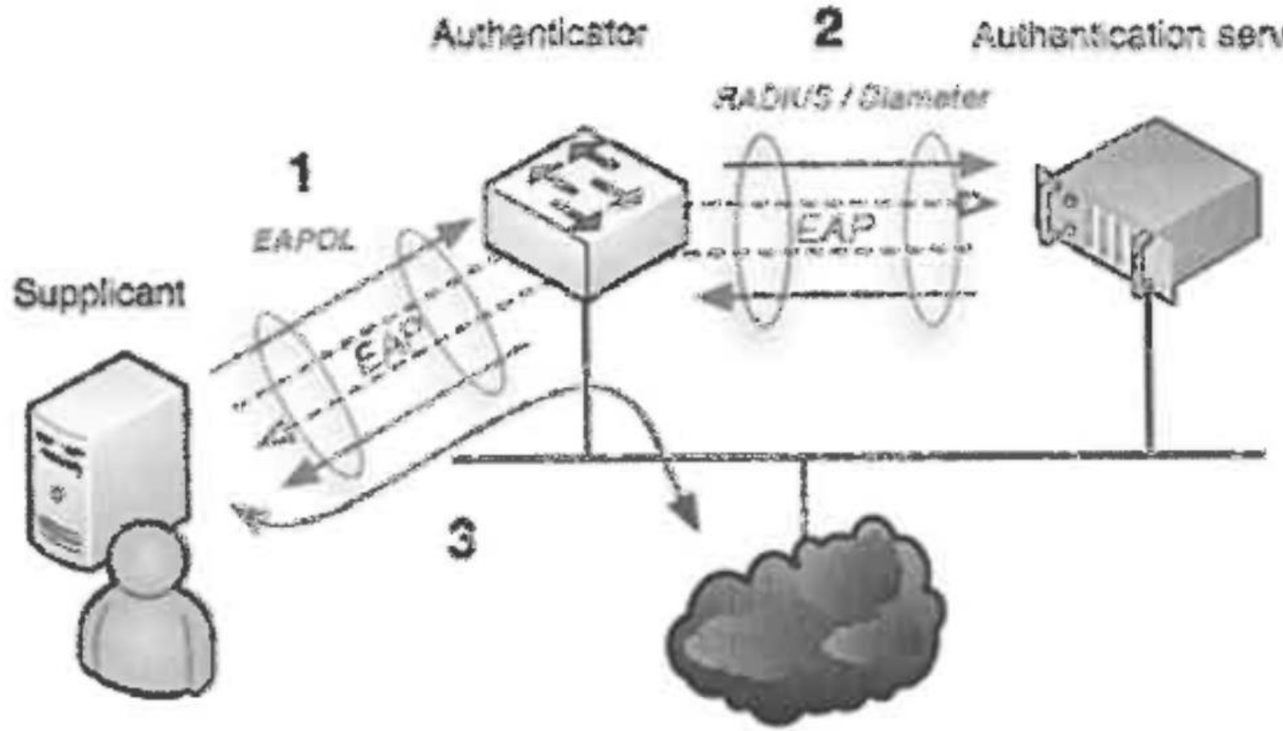


Figura 6.21. Arquitectura de tres capas en IEEE 802.1X.