UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

Redes Privadas Virtuales

Tesina

QUE PARA OBTENER EL TITULO DE

Licenciado en Matemáticas Aplicadas y Computación

PRESENTA

Abimael Ponce Orduño

Asesor: Ing. Rubén Romero Ruíz

Octubre 2006

Dedicatorias

A mi padre, Moisés, por que siempre lo he admirado, por su trabajo, su dedicación, esfuerzo, paciencia, valores, su sentido del humor y por haberme dado la oportunidad de estudiar.

A mi madre, Magdalena, por su espíritu tan grande, su apoyo incondicional en todo momento y sus sabios consejos, te quiero mamá.

A mis hermanos Moisés, Esther y Yuli, por ser una parte fundamental en mi vida.

A Beatriz, por todos esos momentos felices que compartimos en la escuela y fuera de ella, por todo su apoyo en los momentos difíciles, pero sobre todo por estar conmigo, gracias betita. Te amo.

A todos los integrantes del poderoso equipo de básquetbol “Excalibur”

A mis compañeros: Adriana, Araceli, Beatriz Arroyo, Carlos, Cuca, Israel, Laura, Lola, Omar, Rocío, Yonas.

Agradecimientos

A la máxima casa de estudios la UNAM y en especial a la FES Acatlán por haberme permitido formarme en sus aulas académicamente, humanamente y culturalmente.

A mi asesor Ing. Rubén Romero Ruíz, por todo su apoyo y conocimiento que permitieron que concluyera este trabajo.

Al profesor Fis. Carlos Pedro Curiel García por su tiempo y sus valiosas aportaciones.

Al Lic. Carlos Alberto Rangel Rojas

Al Lic. Juan Torres Lovera

A todos los profesores de la FES Acatlán por su arduo trabajo que desempeñan en las aulas que es el enseñar, gracias profesores.

A mis sinodales:

Ing. Rubén Romero Ruíz

Ing. Juan José Cortés Buenrostro

Ing. José Alfredo López Rodríguez

Fís. Carlos Pedro Curiel García

Lic. Alejandro Roberto Rubio Pérez

CONTENIDO

Capítulo II Redes privadas Virtuales

Capítulo III Tecnología de las Redes privadas Virtuales

Capítulo IV Ejemplo de Implementación

INTRODUCCIÓN

El intercambio de información siempre ha sido importante dentro de una organización para su crecimiento, el uso de Internet para dicho intercambio ha hecho que se simplifiquen las cosas, (se pueden transferir datos, audio, video) ha propiciado el gran auge para el crecimiento de los negocios por Internet, sin embargo, los Hackers, Virus informáticos y de más programas dañinos han hecho que sea desde sus inicios una red pública poco segura.

El objetivo del presente trabajo es describir y analizar las redes privadas virtuales por medio de un comparativo de sus funcionalidades y tecnologías existentes para poder plantearlas como un medio de transmisión de datos seguro, práctico, económico y eficiente.

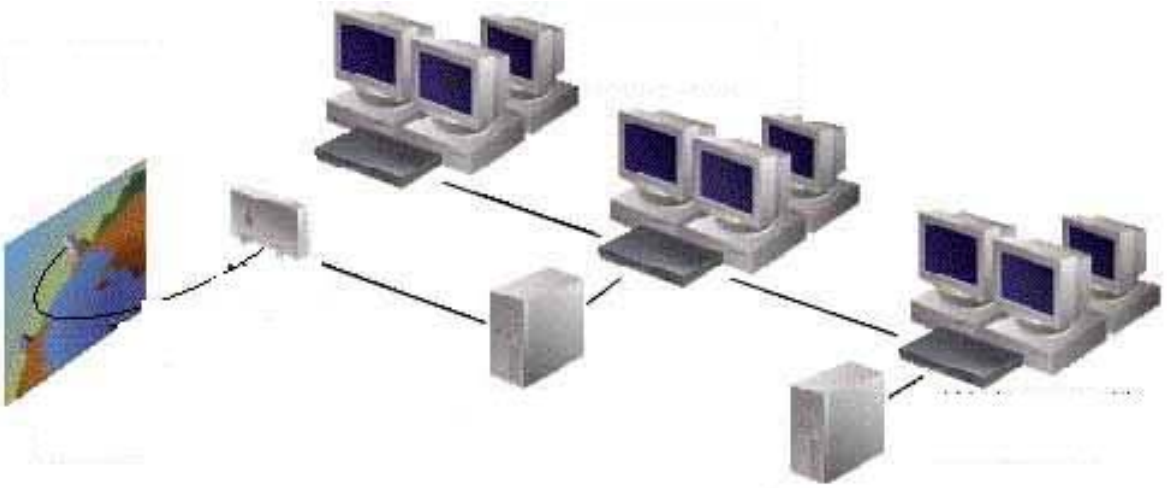
Por lo tanto para poder hablar de redes privadas virtuales, se deben conocer conceptos básicos sobre las redes de computadoras. El tema de redes computacionales es muy extenso, por lo tanto en el capítulo I se da una breve descripción de estas, su protocolo TCP/IP y servicios de conexión para transferencia de datos. Así como el proceso de evolución (Intranets y Extranets) que dan el origen a las redes privadas virtuales.

En el capítulo II se describe el concepto, componentes, los tipos, ventajas y desventajas de las redes privadas virtuales, así como sus principales arquitecturas.

En el capítulo III se analiza las diferentes tecnologías de las redes privadas virtuales, componentes y conceptos así como sus escenarios óptimos para poder aplicarse.

Finalmente en el capítulo IV se realiza un ejemplo de implementación de una red privada virtual, incluyendo los requisitos que debe de cumplir, tales como autenticación, autorización y seguridad.

Antecedentes de las Redes Privadas Virtuales



FES UNAM ACATLAN

1.1 ¿Qué es una red de computadoras?

Podemos definir red de computadoras [1] como un conjunto de computadoras conectadas mediante una o más vías de transmisión, con la finalidad de cumplir un cierto objetivo, que es, generalmente la transferencia e intercambio de información.

Las vías de transmisión para realizar la conexión pueden ser variados como: cable de cobre, fibras ópticas, las microondas, los rayos infrarrojos y los satélites de comunicaciones.

1.2 ¿Por qué utilizar una red de computadoras?

Actualmente en este mundo globalizado implementar una red significa: aumentar la eficiencia y reducir costes. Esto se logra básicamente de tres formas principales que son:

- Compartir Información
- Compartir Hardware y Software
- Centralizar la administración y el soporte

1.2.1 Compartir información

Compartir información es uno de los usos más importantes que se le da a la tecnología de redes, al hacer que la información este disponible para ser compartida, las redes pueden reducir la necesidad de comunicación por escrito, incrementar la eficiencia y hacer prácticamente que cualquier tipo de dato este disponible simultáneamente para cualquier usuario que lo necesite.

[1] Black, Uyless, Redes de computadores: Protocolos, normas e interfaces, Editorial Ra-Ma, Madrid 1995, p.1.

1.2.2 Compartir Hardware y Software

Las redes permiten que varios usuarios puedan compartir simultáneamente periféricos y datos, una impresora es un ejemplo de cómo varios usuarios pueden hacer uso de una impresora disponible en la red.

Las redes pueden usarse para compartir y estandarizar aplicaciones, como procesadores de texto, hojas de cálculo, base de datos, etc. Ya que todos los usuarios de la red utilizan las mismas aplicaciones y las mismas versiones de estas aplicaciones.

1.2.3 Centralizar la administración y el soporte

Al estar los equipos conectados en red es más fácil darles soporte ya que es mucho más eficiente darle soporte a una versión de un sistema operativo o aplicación y configurar todos los equipos del mismo modo que dar soporte a muchos sistemas y configuraciones individuales y diferentes.

1.3 Tipo de redes

Las redes de computadoras se clasifican dependiendo su tamaño y su función, en los siguientes puntos se mencionan las más importantes.

1.3.1 Red de área local

Las redes de área local (LAN, del inglés Local Area Network) son aquellas que están confinadas a un área geográfica limitada puede ser simplemente dos equipos conectados por medio de un cable o compleja con cientos de equipos y periféricos conectados dentro de una empresa. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información.

1.3.2 Redes de área metropolitana

Redes de área Metropolitana (MAN, del inglés Metropolitan Area Network) están conformadas por redes de área local interconectadas entre si restringidas a un área de la dimensión de una ciudad.

1.3.3 Redes de área amplia

Las redes de área amplia (WAN, del inglés Wide Area Network), no tienen limitaciones geográficas, pueden conectar equipos y otros dispositivos situados en diferentes puntos geográficos del planeta. Una WAN esta conformada por varias LAN interconectadas.

Las WAN se comunican por medio de subred de comunicación que son las encargadas de enviar la información de un host (las computadoras personales de un usuario) a otro, generalmente son las compañías telefónicas o proveedores de Internet los que operan la subred de comunicación.

En la mayoría de las WAN, la subred de comunicación consta de dos componentes distintos: líneas de transmisión y elementos de conmutación. Las líneas de transmisión mueven bits entre máquinas. Pueden estar hechas de cable de cobre, fibra óptica o radioenlaces. Los elementos de conmutación son computadoras especializadas que conectan tres o más líneas de transmisión. Cuando los datos llegan a una línea de entrada, el elemento de conmutación debe elegir una línea de salida para reenviarlos. Estas computadoras de conmutación reciben nombres como: conmutadores y ruteadores entre lo más comunes. El conjunto de líneas de comunicación y ruteadores (no de host) y el direccionamiento de red forman la subred.

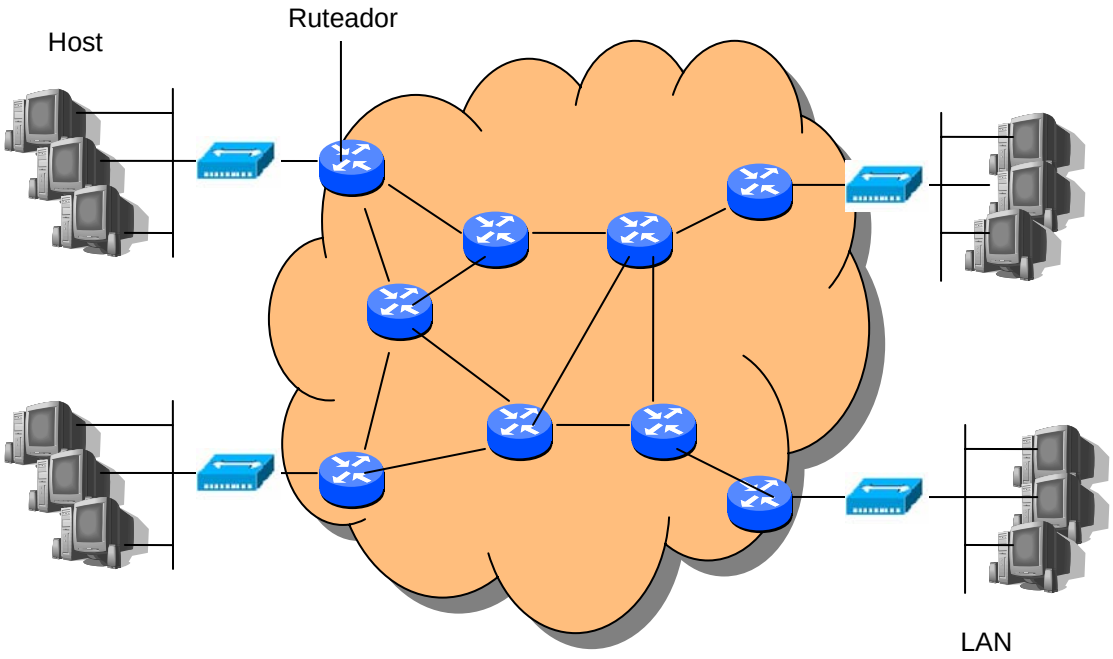


Figura 1.1 Relación entre hosts de LANs y la subred.

En la figura 1.1 se muestra cada host conectado a una LAN en la que existe un ruteador, aunque en algunos casos un host puede estar conectado directamente a un ruteador.

1.4 Internet

Podemos definir Internet como la red interconectada más grande del mundo y de rápido crecimiento en la historia. Internet es un sistema de telecomunicaciones abierto (no hay ningún propietario de Internet, no hay ninguna autoridad centralizada que pueda imponer un precio o unas condiciones diferentes de las estrictamente técnicas), de tecnologías y protocolos, que permite a los usuarios con diferentes tipos de computadoras y sistemas operativos acceder a los millones de sitos de información a través de interfaces gráficas que conocemos como exploradores.

Internet ofrece una amplia gama de servicios atractivos para los usuarios, entre los más importantes se encuentran:

- Correo electrónico
- Servicio de noticias
- El WWW
- Servicios de telefonía
- Nuevas oportunidades de negocios

1.5 Modelos de Referencia

1.5.1 Modelo de referencia OSI

El modelo de referencia de interconexión abierta OSI[2] (Open Systems Interconnection) es un modelo de referencia internacional para enlazar diferentes tipos de computadoras y redes, este conjunto de especificaciones lo divulgó la Organización Internacional de Estándares (ISO, por sus siglas en inglés) para enfrentar los problemas de Incompatibilidad de redes. Es decir el modelo OSI proporciona a los fabricantes un conjunto de estándares que aseguran una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

El modelo OSI esta compuesto por siete niveles, los cuales representan los procesos mediante el cual los datos se empaquetan y se transmiten desde una aplicación emisora, a través de medios físicos como cables(telefónico, coaxial, UTP de categoría 5, fibra óptica) o medios inalámbricos(ondas de radio, microondas, infrarroja, etcétera) hacia la aplicación receptora. Estos niveles se muestran en la figura 1.2

[2] Laudon, Kenneth C., Laudon Jane P., Administración de los Sistemas de Información: Organización y tecnología, Editorial Pearson Education, México 1996, p.352.

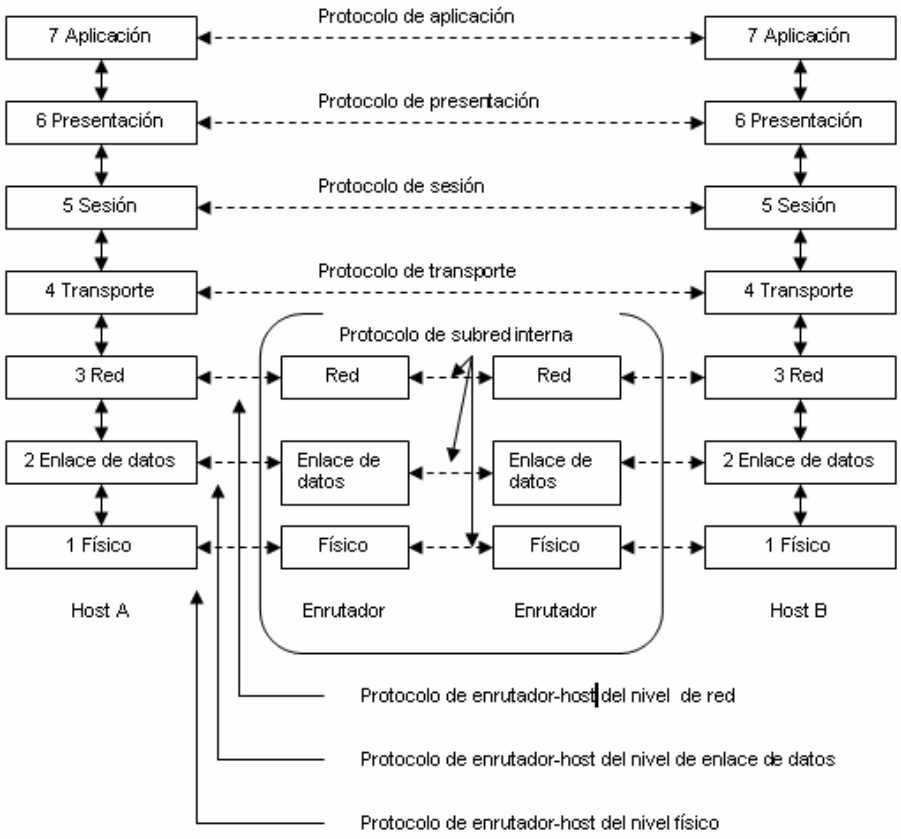


Figura 1.2 El modelo de referencia OSI

1.5.1.1 Nivel de aplicación

El nivel de aplicación es el más alto dentro del modelo de referencia OSI, soporta los procesos de aplicación de los usuarios finales, como software para transferencia de archivos, acceso a base de datos y correo electrónico. Suministra los servicios de red a los procesos de aplicaciones.

Los niveles inferiores soportan las tareas que se realizan en el nivel de aplicación. Estas tareas incluyen el acceso general a la red, el control de flujo y la recuperación de errores.

1.5.1.2 Nivel de presentación

Este nivel garantiza que los datos sean legibles para el sistema receptor, define el formato utilizado para el intercambio de datos. Dentro del equipo emisor, el nivel de presentación traduce los datos del formato enviado por el nivel de aplicación en un formato intermedio, generalmente reconocido. En el equipo receptor, este nivel traduce el formato intermedio en un formato que pueda ser útil para el nivel de aplicación de ese equipo.

Este nivel también es el responsable de la conversión de protocolos, la traducción de los datos, la encriptación de los datos, la modificación o conversión del conjunto de caracteres y la expansión de los comandos básicos.

1.5.1.3 Nivel de sesión

Este nivel permite que los usuarios de máquinas diferentes establezcan *sesiones* entre ellos. Las sesiones ofrecen varios servicio, como el control de diálogo (dar seguimiento a quien le toca transmitir), administración de token (impide que las dos partes traten de realizar la misma operación crítica al mismo tiempo) y sincronización (la adición de puntos de referencia a trasmisiones largas para permitirles continuar desde donde se encontraban después de una caída).

1.5.1.4 Nivel de transporte

La función básica de este nivel es aceptar los datos provenientes de los niveles superiores, dividirlos en unidades más pequeñas si es necesario, pasar estas al nivel de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo. Garantiza que los datos se envíen sin errores, en secuencia, y sin perdida de datos. Esto se realiza mediante el control de flujo, verificación y secuencia de datos.

El nivel de transporte es una verdadera conexión de extremo a extremo, en toda la ruta desde el origen hasta el destino.

1.5.1.5 Nivel de red

Este nivel especifica el encaminamiento por la red y las comunicaciones entre redes. Determina el camino que deben tomar los datos en base a las condiciones de la red, la prioridad de los servicios y otros factores. También gestiona los problemas de tráfico en la red, como la conmutación y encaminamiento de paquetes y el control de la congestión de los datos.

1.5.1.6 Nivel de enlace de datos

Es el responsable de la transferencia de datos desde el nivel de red hasta el nivel físico. Controla los impulsos eléctricos que entran y salen del cable de red. Una de sus funciones principales es ocuparse de la detección de errores de transmisión y proporcionar mecanismos para la recuperación de datos perdidos, duplicados o erróneos.

1.5.1.7 Nivel físico

Este nivel es el más bajo del modelo OSI, transmite el flujo de bits puros no estructurados sobre un medio físico (como el cable de red). Este nivel esta orientado al hardware y se encarga de todos los aspectos de establecimiento y mantenimiento de un enlace físico entre los equipos a comunicar.

Este nivel también define la técnica de transmisión que se utilizará para enviar datos sobre el cable de red. Proporciona codificación de datos y sincronización de bits.

1.5.2 Modelo de referencia TCP/IP

El modelo de referencia TCP/IP es una arquitectura creada para conectar múltiples redes de una manera sólida de acuerdo con sus dos protocolos primarios.

El Protocolo de Control de transferencia (TCP) y el protocolo de Internet (IP) son un conjunto de protocolos o reglas desarrollados para permitir el intercambio de recursos en redes de computadoras.
El TCP/IP se ha convertido en el protocolo estándar, la mayoría de redes permiten TCP/IP como protocolo de interconexión de redes, permite acceder a Internet y a sus recursos.

El modelo de referencia TCP/IP esta compuesto por los siguientes niveles:

- Nivel de aplicación
- Nivel de transporte
- Nivel de Internet
- Nivel acceso a red

Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta.

1.5.2.1 Nivel de aplicación

Este nivel se corresponde con los niveles de sesión, presentación y aplicación del modelo OSI, y conecta las aplicaciones a la red. En este nivel se encuentran los protocolos de nivel de aplicación o de alto orden y los de la colección de TCP/IP se encuentran entre los más utilizados por la industria.
TELNET.- Terminal virtual
FTP.- Transferencia de archivos
SMTP.- Correo electrónico
Con el tiempo se han agregado muchos otros protocolos:
DNS.- (Sistema de Nombres de dominio) para la resolución de nombres de host en sus direcciones de red.
NNTP.- Para transportar los artículos de noticias de USENET
HTTP.- Para las páginas de World Wide Web.

1.5.2.2 Nivel de transporte

El nivel de transporte es el encargado de ofrecer maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo.

Uno de sus protocolos , el protocolo para el control de transmisión (TCP) es un protocolo confiable, orientado a la conexión y es el responsable para la transmisión de datos de un nodo a otro, ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo.

El segundo protocolo de este nivel es el Protocolo de Datagrama de usuario (UDP), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control del flujo TCP y que desean proporcionar el suyo. La relación de IP, TCP y UDP se muestra en la figura 1.3.

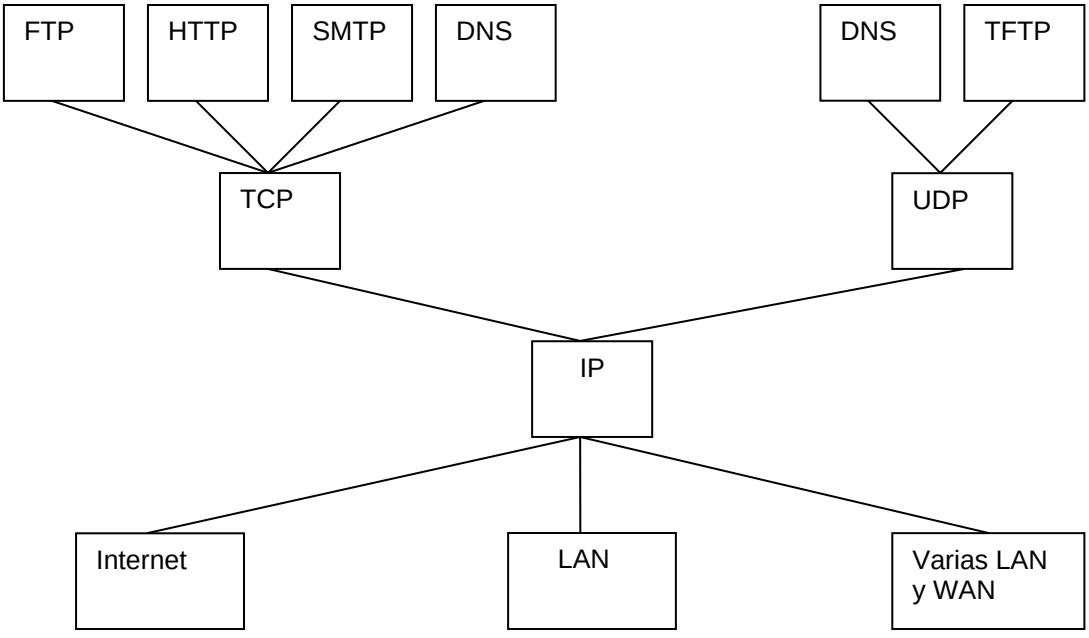


Figura 1.3 Gráfico de protocolo TCP/IP

1.5.2.3Nivel de Internet

Este nivel utiliza varios protocolos para encaminar y entregar los paquetes. Encuentra su correspondencia con el nivel de red del modelo OSI. En el modelo TCP/IP existe solamente un protocolo de red: el protocolo Internet, o IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada. *IP* sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento.

1.5.2.3.1 Protocolo Internet (IP)

El protocolo de Internet (IP) es un protocolo de conmutación de paquetes que realiza direccionamiento y encaminamiento.

El IP ejecuta las siguientes operaciones:

- Define un paquete y un esquema de direccionamiento.
- Transfiere los datos entre la capa Internet y las capas de acceso de red.
- Enruta los paquetes hacia los hosts remotos.

El propósito de este nivel es dividir los segmentos TCP en paquetes y seleccionar la mejor ruta para enviarlos desde cualquier red. Cada paquete IP está compuesto por una dirección de origen y una de destino, un identificador de protocolo, un checksum (un valor calculado) y un tiempo de vida (TTL del inglés time to live).

1.5.2.3.2 Direcciones IP

Las direcciones IP sirven para identificar las computadoras y las redes que están conectadas. La dirección IP no identifica por sí misma a una computadora, si no la conexión de una computadora en su red.

Una dirección IP es una secuencia de unos y ceros de 32 bits. Para que la dirección sea más sencilla, la dirección IP se escribe en formato de cuatro números decimales separados por puntos. Por ejemplo.

La dirección IP 192.168.1.7 sería 11000000.10101000.00000001.00000111 en notación binaria, la notación decimal punteada es más sencilla de comprender que el método binario de unos y ceros.

El formato de la dirección IP es:

Dirección IP = Dirección de red + Dirección de computador

Las direcciones IP se clasifican en grupos llamados clases. Están permitidas cuatro clases:

- Clase A: Se diseño para redes de gran tamaño acepta más de 16 millones de direcciones de host.
- Clase B: Es para redes de tamaño moderado a grande.
- Clase C: Las direcciones de clase C esta diseñada para redes pequeñas y contienen menos de 256 computadoras.
- Clase D: La clase D se reserva para multidifusión en una dirección IP, dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

1.5.2.4 Nivel acceso a red

Este nivel corresponde con el nivel físico y de enlace de datos del modelo OSI, este nivel guarda relación con todos los componentes, tanto físicos como lógicos, necesarios para lograr un enlace físico. Incluye los detalles entre la arquitectura de red y el nivel de Internet.

1.5.3 Envío de datos en una red

Todas las comunicaciones de una red parten de un origen y se envían a un destino, y que la información que se envía a través de una red se denomina datos o paquete de datos. Inicialmente se puede pensar que los datos se envían desde una computadora (Host A) a otra (Host B) como una serie continua de unos y ceros. De hecho, los datos se dividen en paquetes pequeños y manejables, cada uno dividido con la información esencial para ir desde el origen hasta el destino, a todo este proceso se le llama encapsulamiento.

El encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.
Los componentes de un paquete tienen varias propiedades en común. Entre ellas se incluyen:

- Una dirección de origen que identifica al equipo que realiza el envío.
- Los datos que se quieren transmitir.
- Una dirección de destino que identifica al destinatario.
- Instrucciones que indican a los componentes de la red cómo pasar los datos.
- Información que indica al equipo de destino cómo conectar el paquete con el resto de los paquetes para reorganizar el bloque completo de datos.
- Información de comprobación de errores que asegura que los datos lleguen intactos.

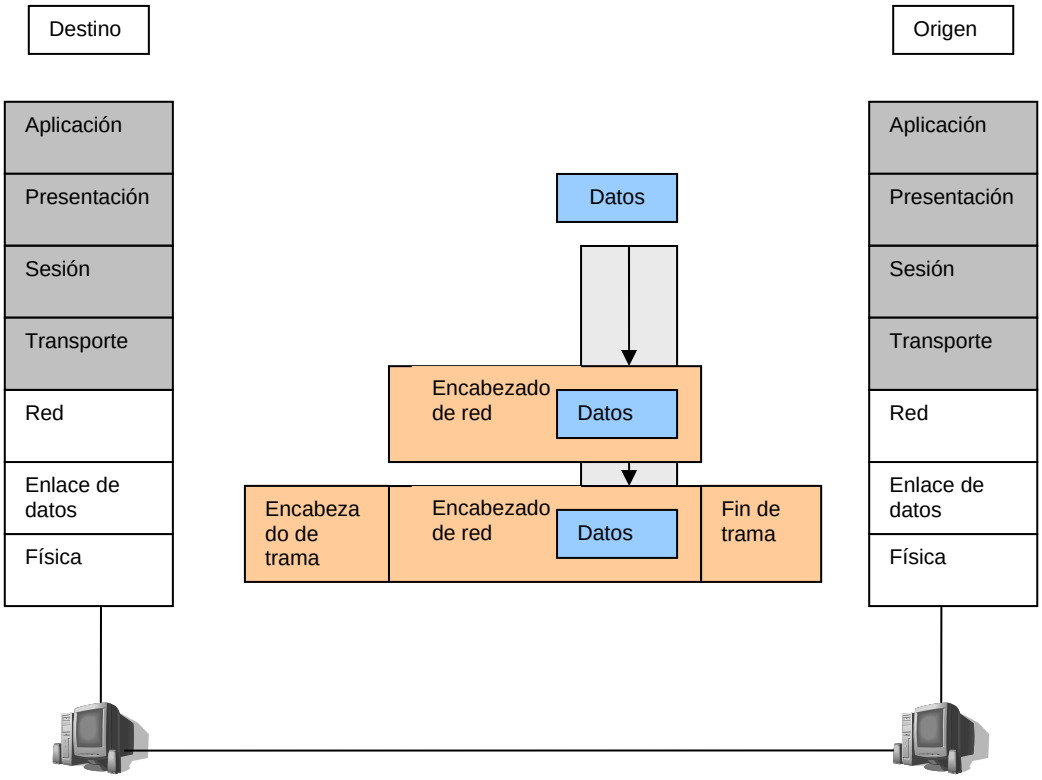


Figura 1.4 Encapsulamiento de datos

En las figuras 1.4 y 1.5 Se puede observar como se produce el encapsulamiento, en donde los datos una vez enviados desde el origen, viajan a través del nivel de aplicación directo hacia los otros niveles, como se puede observar el empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las redes ofrecen sus servicios a los usuarios finales. Las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

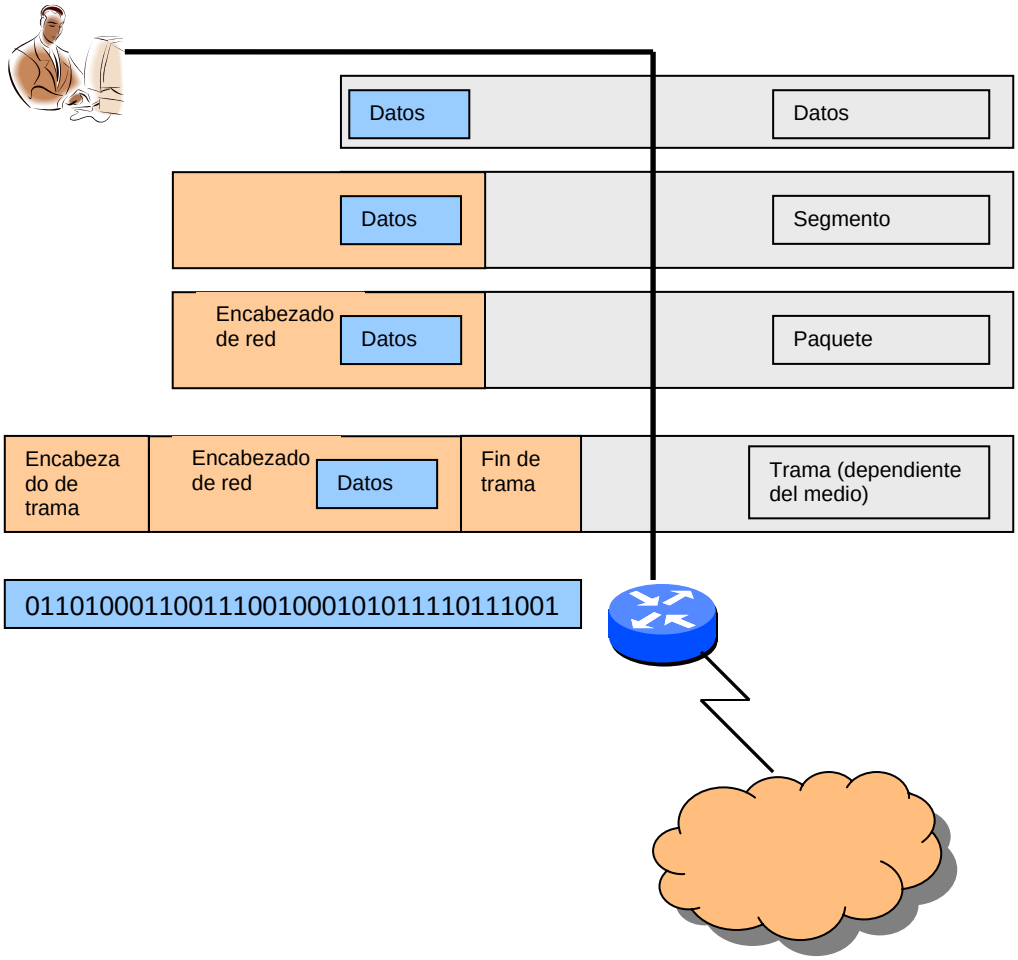
1.- Crear los datos. Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la red.

2.- Empaquetar los datos para ser transportados de extremo a extremo. Los datos se empaquetan para ser transportados por la red. Al utilizar segmentos, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

3.- Anexar (agregar) la dirección de red al encabezado. Los datos se colocan en un paquete o datagrama que contiene el encabezado de red con las direcciones lógicas origen y destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

4.- Anexar (agregar) la dirección local al encabezado de enlace de datos. Cada dispositivo de la red debe poner el paquete dentro de una trama. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

5.-Realizar la conversión a bits para su transmisión. La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio (por lo general un cable). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la red física de redes puede variar a lo largo de la ruta utilizada. Los encabezados y la información final se agregan a medida que los datos se desplazan a través de las capas del modelo OSI.



1.5 Ejemplo de encapsulamiento de datos

1.6 Servicios de conexión para la transmisión de datos

Los servicios orientados a la conexión tienen sus orígenes en el sistema telefónico, vienen del mundo de las compañías telefónicas. Quien llama debe marcar el número de la parte a la que desea llamar y esperar la conexión antes de poder hablar o enviar los datos. Esta configuración de conexión establece una ruta a través del sistema telefónico que se mantiene hasta que se termina la llamada. Todas las palabras o paquetes siguen la misma ruta.

Al establecer una conexión, la subred puede reservar recursos como espacio de búfer y capacidad de procesamiento (CPU) en los ruteadores. Si se intenta establecer una llamada y los recursos disponibles son insuficientes, la llamada

se rechaza y el invocador recibe una señal de ocupado. De manera opuesta, una vez establecida la conexión, ésta da un buen servicio.

Los servicios de conexión nos proporcionan diferentes opciones, cuando deseamos conectar nuestra red a otras que se encuentran ubicadas a cierta distancia geográfica. A continuación se muestran los servicios que se ofrecen para dichas conexiones que van de las sencillas como líneas telefónicas hasta los servicios digitales de alta velocidad.

1.6.1 Línea telefónicas

Existen dos tipos de líneas telefónicas para las comunicaciones vía MODEM:

- Líneas de llamada.- Son la líneas telefónicas habituales. Son lentas, requieren que los usuarios realicen una conexión, para cada comunicación y no son recomendables para la transmisión de grandes cantidades de información.
- Líneas alquiladas (dedicadas).- Estas líneas proporcionan conexiones dedicadas a tiempo completo y no utilizan una serie de conmutadores para realizar la conexión. La calidad de esta línea es a menudo superior a las líneas telefónicas para la transmisión de voz. El rango de velocidad de estas líneas va desde los 56 Kbps hasta por encima de los 45 Mbps.

1.6.2 Redes de conmutación de paquetes

Este tipo de red se origina como consecuencia de las debilidades del sistema de comunicación por red telefónica, debido a que era demasiado fácil inutilizarlo (ya que si se destruía una central telefónica importante, buena parte de las comunicaciones telefónicas quedarían inutilizadas). Así fue como se diseño una nueva tecnología denominada *conmutación de paquetes*, esta tecnología se utiliza para transmitir datos sobre grandes áreas como ciudades, estados o países. Es una tecnología rápida, conveniente y fiable.

Funciona dividiendo toda la información que esta lista para salir de una Terminal en bloques de una determinada longitud llamados paquetes. A cada

paquete se le añade información adicional al comienzo del mismo y, así, se puede mover por la red de forma independiente. Si en un momento dado, alguna ruta o nodo de comunicaciones quedara fuera de servicio, los paquetes se desviarían por otras rutas para llegar a su destino.

1.6.3 X.25

X25 fue la primera red de datos pública, se desplegó en la década de 1970. Para utilizar X.25, una computadora establecía primero una conexión con la computadora remota, es decir, hacía una llamada telefónica. Esta conexión daba un número de conexión para utilizarlo en los paquetes de transferencias de datos.

X.25 es un conjunto de protocolos incorporados en una red de conmutación de paquetes. Esta red utiliza conmutadores, circuitos y ruteadores para proporcionar la mejor ruta para cada transmisión. En una red X.25 un endpoint o nodo es llamado Equipo Terminal de datos (DTE por sus siglas en inglés), este DTE puede ser una tarjeta instalada en una PC o en un servidor que interactúan con un ruteador, o esta puede estar en una unidad sola. Los DTE son conectados a un dispositivo llamado Equipo de circuito de datos (DCE por sus siglas en inglés) que a su vez conecta a los usuarios con el backbone de la red X.25.

Estos componentes se pueden describir como nubes, puesto que cambian rápidamente dependiendo de las necesidades y disponibilidad. En la figura 1.6 se muestra la conmutación de paquete X.25

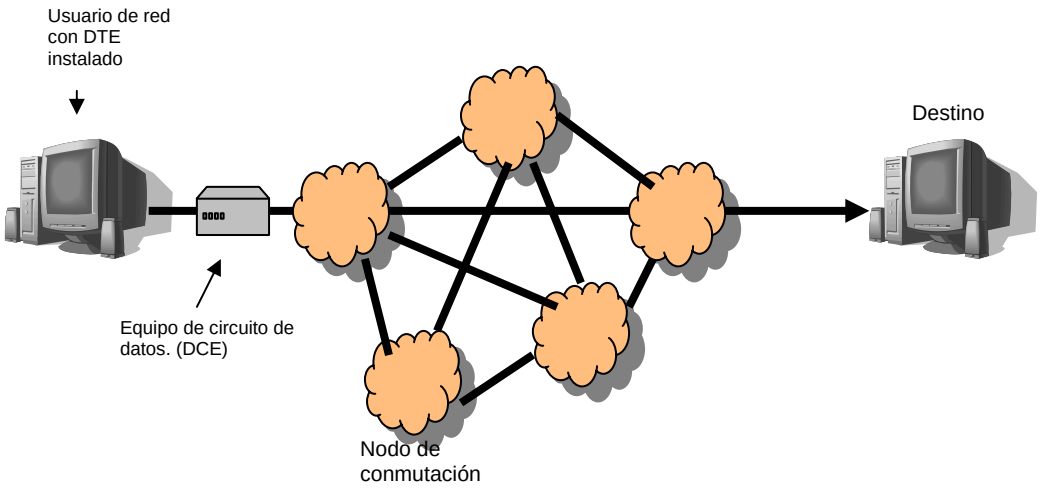


Figura 1.6 La conmutación de paquetes X.25

1.6.4 Circuitos punto a punto

Un circuito punto a punto es un conjunto de medios que hace posible la comunicación entre dos puntos determinados, de forma permanente y sin posibilidad de acceder a la red pública telefónica ni a ningún otro circuito, sin necesidad de realizar algún tipo de marcado para establecer la comunicación.

1.6.5 Frame Relay

En la década de 1980, las redes X.25 fueron reemplazadas ampliamente por un nuevo tipo de red llamada Frame Relay[3] (retransmisión de tramas). Esta es una red orientada a la conexión sin controles de error ni de flujo. Frame Relay es un protocolo de conmutación de paquetes que se fragmentan en unidades de transmisión llamadas *tramas* y se envían en ráfagas de alta velocidad a través de una red digital.

[3] Tanenbaum, Andrew S., Redes de computadoras, Editorial Prentice Hall, México 2003, p.61.

Las redes Frame Relay utilizan de forma más rápida las operaciones básicas de conmutación de paquetes con respecto a otros sistemas de conmutación ya que son sistemas punto a punto que utilizan circuitos virtuales permanentes (PVC), lo que les permite conocer el camino desde el origen hasta el final. Las redes Frame Relay proporcionan a los abonados el ancho de banda a medida que lo necesitan, permitiendo al cliente cualquier tipo de transmisión. Al igual que las redes X.25 Frame Relay utiliza DTE que pueden ser dispositivos individuales o ruteadores y DCE para conectar apropiadamente las redes. Al backbone que es creado con este conjunto de dispositivos se le llama Frame Relay Bearer Service (FRBS) El la figura 1.7 se muestra Frame Relay.

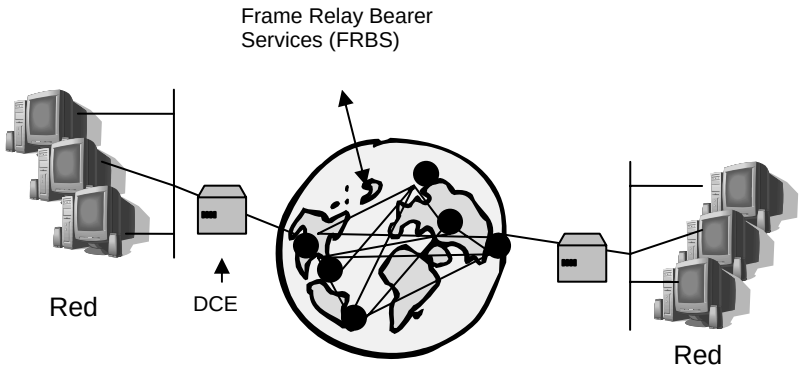


Figura 1.7 Frame Relay utiliza sistema punto a punto

1.6.6 Red Digital de Servicios Integrados (RDSI)

La red digital de servicios integrados (RDSI) supone la digitalización completa, de forma que toda comunicación que se establezca será en forma digital, ofreciendo servicios como transporte de voz, datos e imágenes.

La capacidad de transferencia de información entre el usuario y la RDSI está estructurada en forma de canales de transferencia de información.

Basic Rate RDSI divide su ancho de banda en tres canales de datos. Dos de ellos desplazan los datos a 64 Kbps, mientras el tercero lo hace a 16 Kbps.

Los canales de 64 Kbps se conocen como canales B y estos pueden transportar voz, datos e imágenes. El canal más lento se conoce como canal D y transporta el muestreo de señales y los datos de gestión del enlace.

Primary Rate RDSI utiliza el ancho de banda completo de un enlace T1 proporcionando 23 canales B a 64 Kbps y un canal D a 64 Kbps. El canal D solo se utiliza para el muestreo de señales y gestión de enlace.

1.6.7 Modo de Transferencia Asíncrono (ATM)

El modo de transferencia asíncrono es una implementación de transferencia de datos digitales de alta velocidad para enviar paquetes de tamaño fijo a través de LAN, WAN y MAN de banda amplia o banda base.

ATM es una tecnología orientada a conexión, el envío de datos requiere primero se envíe un paquete para establecer la conexión. Conforme el mensaje de establecimiento sigue su camino a través de la subred, todos los conmutadores que se encuentran en la ruta crean una entrada en sus tablas internas tomando nota de la existencia de la conexión y reservando los recursos que necesite la conexión. Con frecuencia a las conexiones se les conoce como circuitos virtuales, en analogía con los circuitos físicos utilizados en el sistema telefónico.

Una vez establecida la conexión, cada lado puede empezar a transmitir datos. La idea básica en que se fundamenta ATM es transmitir toda la información en paquetes pequeños, de tamaño fijo, llamados “celdas”.

ATM permite:

- Voz
- Datos
- Fax
- Vídeo en tiempo real
- Audio en calidad CD
- Imágenes

1.6.8 Servicio T1

El servicio T1 provee transmisión de datos de alta velocidad sobre líneas digitales, se trata de una transmisión punto a punto que utiliza dos pares de hilo (un par para enviar y otro para recibir) para transmitir una señal en ambos sentidos (full-duplex) a una velocidad de 1,544 Mbp.

El servicio T1 es, quizá, el tipo de línea digital más utilizado por los proveedores de Internet y son las líneas más caras de todos los enlaces WAN. T1 se utiliza para transmitir señales digitales de voz, datos y video.

1.7 Redes Privadas

1.7.1 Definición

Podemos definir a una red privada[4] como una red de área amplia (WANs) que conectan LANs dispersas, por lo general entre una oficina central y oficinas de sucursal o clientes de PC remotos en oficinas caseras o ambos, construida, mantenida y controlada por la organización a la que sirve. Con la finalidad de garantizar un buen desempeño, seguridad y velocidad, en la transmisión de datos. Las redes privadas funcionan bien y son muy seguras. Si las únicas líneas disponibles son las alquiladas, el tráfico no puede fugarse de las ubicaciones de la compañía y los intrusos tienen que intervenir físicamente las líneas para infiltrarse, lo cual no es fácil de hacer.

En la figura 1.8 se muestra una red privada de ejemplo que conecta tres ubicaciones.

1.7.2 Características principales de las redes privadas

- La comunicación de una red privada es en base a una línea de comunicación principal, esta puede ser una línea alquilada o fibra dedicada.

- El acceso remoto a una red privada puede permitirse a través de líneas telefónicas estándares o digitales como las líneas ISDN o DSL(Digital Suscriber Line, línea digital de suscriptor)

- Las redes privadas soportan varios protocolos como retransmisión de tramas, modo de transmisión asincrónica ATM, y TCP/IP.

[4] Leon Clark, David, Guía de Administrador de Redes Privadas Virtuales (RPV), Editorial Mc. Graw Hill, México 2001, p.20.

- Rentar una línea suele ser muy costoso, alquilar una sola línea T1 cuesta miles de dólares mensuales y las líneas T3 son muchas veces más costosas.

- Las redes privadas son costosas en mantenimiento y difíciles de manejar, ya que una vez instaladas es difícil y costoso unir nuevas líneas para ubicar nuevos socios comerciales, proveedores o empresas internacionales.

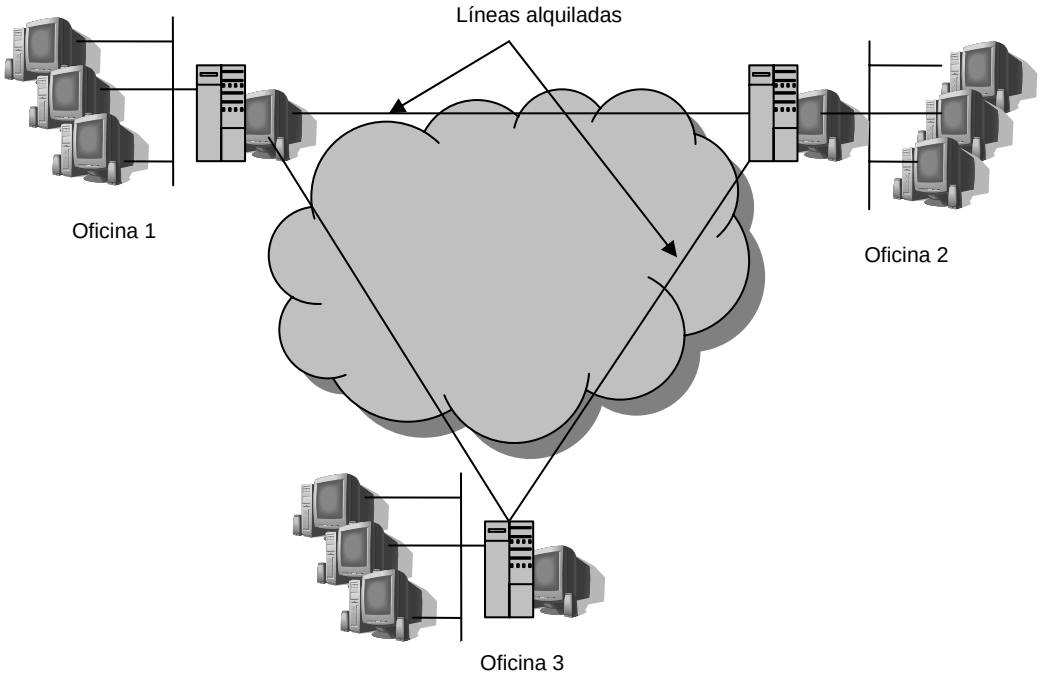


Figura 1.8 Red privada con línea alquilada

1.8 Intranet

Intranet puede definirse como una red privada interconectada que implementa las tecnologías y protocolos de Internet para facilitar la comunicación y acceso a la información, muchas veces restringida a nivel programación como lo son usuarios y contraseñas de acceso o incluso a nivel Hardware como un sistema firewall (cortafuegos) que puede restringir el acceso a la red organizacional. Incorporan tecnología de Internet como exploradores, sitios Web y HTML, de esta forma proporcionan las mismas funciones que Internet, incluyendo el uso de enrutado del protocolo TCP/IP.

Las Intranet son parecidas a los sitios Web y en la mayoría de las grandes empresas donde la distribución de la información se convierte en una tarea de gran relevancia, el uso de las Intranets ofrece grandes ventajas, especialmente si existe necesidad de consultar una base de datos, compartir calendario de funciones, o cualquier otro función que se tenga que resolver en equipo. Si la información cambia con frecuencia, la utilidad de la Intranet aumenta ya que una sola persona puede actualizar la información y todos los de más tendrán acceso inmediato a la información actualizada en sus equipos. Para el uso de la Intranet no se necesita que los usuarios tengan grandes equipos, basta con una computadora sencilla que soporte un navegador Web.

1.8.1 Funciones principales que desempeñan las Intranets

Comunicación y colaboración

- Enviar y recibir mails, faxes, correos de voz
- Foros de discusión y chats.
- Conferencias de audio y video
- Conferencias virtuales de grupo y colaboración de proyectos

Publicaciones Web

Desarrollo y publicación de hipervínculos multimedia como:

- Noticias de la empresa
- Normas y políticas de la empresa
- Catálogo de productos
- Material de entrenamiento
- Directorios telefónicos

Administración y operaciones de la empresa

- Procesamiento de pedidos
- Control de inventarios
- Administración de sistemas de información
- Acceso a base de datos

Administración del Portal de la Intranet

- Administración central de todas las funciones de la empresa incluyendo servidores, clientes, seguridad, directorios y tráfico

- Proporcionar a los usuarios acceso a una variedad de aplicaciones de negocios internas como externas

1.8.2 Ventajas principales de usar Intranets

- Interoperabilidad. Se tiene acceso a todos los servicios de Internet pero restringidos al uso interno de la empresa y a todos los productos de la red.

- Escalabilidad. Se puede dar acceso fácilmente a nuevos usuarios de la empresa a dichos servicios sin molestias para los que ya la están utilizando.

- Seguridad. Se produce una gran mejora en la seguridad de la red local al evitar el acceso a usuarios no autorizados a nuestros servicios de Internet

- Aumento de la efectividad. Si está bien diseñada, permite una mejora de la efectividad al tener acceso de forma sencilla a una serie de servicios que simplifican el trabajo y mejoran el tiempo de acceso a la información.

- Reducción de costos en impresión, distribución y papeleo de normas y políticas, noticias, catálogos de productos, material de entrenamiento y directorios telefónicos de la empresa.

- Fácil de usar, no se requiere entrenamiento especializado.

- Simplificar el control interno de la información y mejorar la comunicación dentro de las organizaciones, ofreciendo ayudas sumamente sencillas, pero poderosas, como las derivadas del uso de hipervínculos.

1.8.3 Desventajas y limitaciones de las Intranets

- Es una tecnología envolvente que requiere actualizaciones y puede ocasionar problemas de incompatibilidad de software.

- Elementos de seguridad pueden ser inadecuados

- Inadecuado desempeño de administración del sistema y un pobre soporte

1.9 Extranet

Podemos definir a una Extranet como una red privada resultante de la interconexión de dos o más intranets que vinculan de modo seguro, organizaciones externas (cliente o red que no son de la compañía), como socios comerciales, clientes preferidos o proveedores, con aplicaciones internas que se ejecutan en su Intranet segura.

El concepto Extranet nace cuando una empresa quiere dar acceso a unas determinadas personas o grupos de personas a una determinada información de su Intranet. Sin hacerla pública, la hace accesible a otras personas que puedan necesitarla o con quien mantienen relaciones comerciales. La vinculación de empresas separadas en una red unificada está revolucionando la manera en que las empresas se comunican, acceden información, colaboran, conducen transacciones de negocio a negocio y realizan negocios en general. El ejemplo más antiguo es el de la banca electrónica donde los bancos nos permiten acceder a su sistema de información para conocer u operar con nuestras cuentas, en la actualidad casi todos los bancos permite este tipo de acceso.

Una Extranet requiere seguridad e intimidad. Por tanto se hace necesaria la administración de una "firewall" en el servidor, la emisión y uso de certificados digitales o medios similares para autentificar al usuario, la encriptación de mensajes y el uso de redes privadas virtuales (virtual private networks, VPNs) que corren de manera transparente en la red pública.

Antes cuando la tecnología de las Redes Privadas Virtuales comenzaba, Extranet y Red Privada Virtual se utilizaban de manera indistinta. En la actualidad Extranet se refiere sobre todo a una Intranet que vincula socios comerciales externos, mientras que red privada virtual se refiere más al método para lograr ese fin.

1.9.1 Funciones principales que desempeñan las Extranets

- Intercambiar grandes volúmenes de datos usando Intercambio Electrónico de Datos (Electronic Data Interchange, EDI)

- Al igual que un centro de reuniones para la gente, una Extranet reduce significativamente las líneas de comunicación entre las diferentes partes, incluyendo a los clientes más importantes, con lo cual aumenta la productividad y se gana tiempo.

- Compartir catálogos exclusivamente con mayoristas o personas dentro de su negocio o ramo.

- Colaborar con otras empresas en esfuerzos conjuntos de desarrollo

- Desarrollar y usar conjuntamente con otras empresas programas de capacitación

- Proporcionar o acceder servicios que ofrece una compañía a otro grupo de empresas, como la aplicación de actividades bancarias en línea administradas por una empresa a nombre de bancos afiliados a ella.

- Compartir noticias de interés común en forma exclusiva con empresas asociadas.

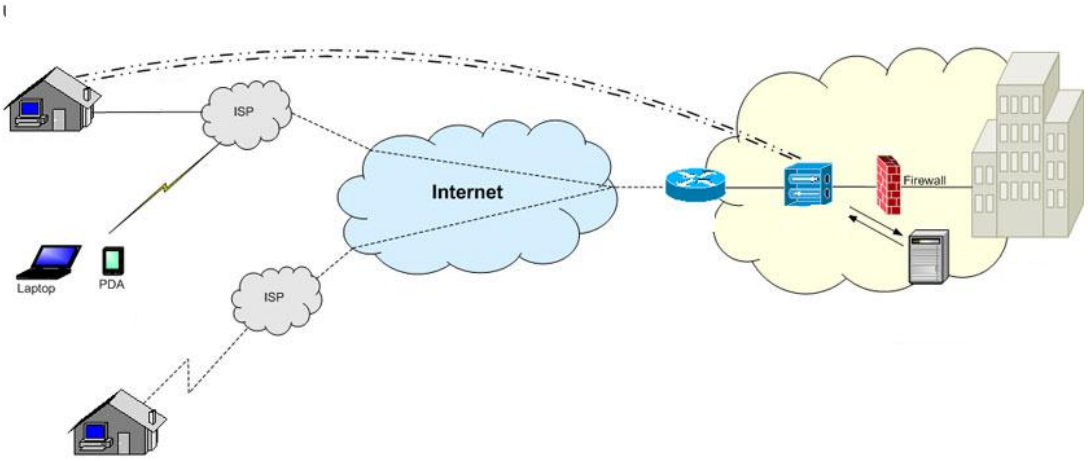
- Una Extranet puede estar equipada con cámaras Web y equipos multimedia para mantener a todos actualizados, por ejemplo, acerca de lo último que ha sucedido con algún proyecto de construcción.

- Permite contactar a personas interesadas, clientes y socios de negocios, de una forma personalizada.

- Emisión de pedidos de determinados productos mediante la asistencia de un formulario Web, seguimiento del estado de los mismos durante todo el proceso de suministro desde la realización del pedido hasta la fase de entrega. La adición de una funcionalidad de pasarela de pago permitiría llegar hasta la facturación electrónica completando así el proceso de negocio.

Cabe señalar que las ventajas y desventajas de una Extranet son prácticamente las mismas de una Intranet.

Redes Privadas Virtuales



FES UNAM ACATLAN

2.1 ¿Qué es una Red Privada Virtual?

Como ya se menciono en el capitulo anterior una Extranet se refiere a una intranet que vincula socios comerciales externos y los métodos que se utilizan para lograr ese fin es lo que se llama: Red Privada Virtual. (VPN, Virtual Private Network)

Por lo tanto una Red Privada Virtual es la tecnología que se utiliza para ofrecer una conectividad y transferencia de datos desde un punto hacia otro de manera segura y fiable, sobre una infraestructura de red pública compartida, como Internet.

El término virtual se refiere a que la tecnología VPN emula la separación de dos protocolos diferentes sobre el mismo canal de transmisión de datos, es decir *la tecnología VPN se implementa sobre el protocolo TCP/IP, sin embargo los datos se abstraen hasta el punto que los VPN en bruto no son compatibles con dicho protocolo. Por lo tanto la separación de protocolos tiene como resultado una red virtua*l[1]

Desde la perspectiva del usuario, la red privada virtual es una conexión punto a punto entre el equipo (el cliente VPN) y el servidor de la organización (el servidor VPN). La infraestructura exacta de la red compartida o pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado.

En lo referente a “Privada” significa que la privacidad deseada de nuestra información se transmita a través de una red o Internet sin sufrir ataques o alteraciones a su destino. Las VPN proporcionan vínculos seguros de transporte de datos, llamados túneles, a través de las líneas públicas de Internet. Los túneles (Tunneling) seguros se establecen entre dos nodos o sitios de Internet mediante las tecnologías de encriptación, autenticación y

[1] Oleg Kolesnikov, Brian Hatch, Guía avanzada redes privadas virtuales con Linux, Pearson Educación, Madrid 2003, p. 5

validación de datos que trabajan en concierto. Permitiendo que solo el destinatario, o la red destinataria, pueden entender la información.

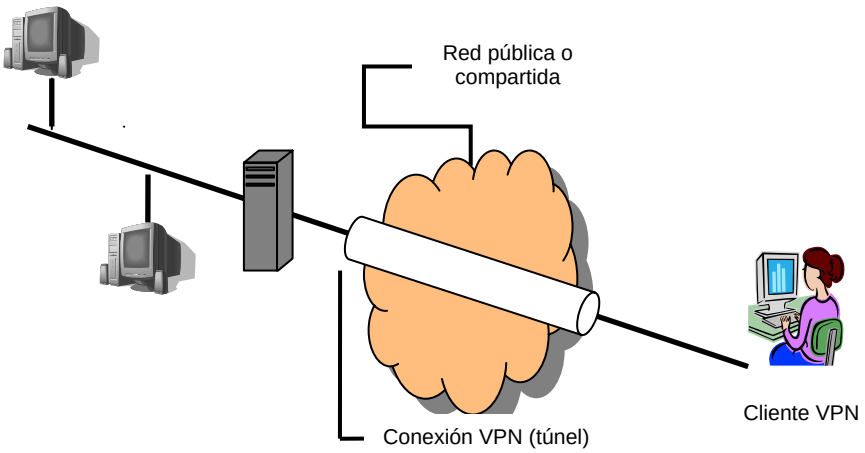


Figura 2.1 Red privada virtual

2.2 Componentes de una Red Privada Virtual

A continuación se describen los diferentes elementos que conforman una VPN los cuales nos permiten que esta pueda ser segura, disponible y fácil de usar para cualquier organización.

2.2.1 Dispositivos para Redes Privadas Virtuales

Un dispositivo VPN es el encargado de aceptar una conexión VPN proveniente de un cliente VPN. Existen dispositivos de hardware y software que establecen la conexión por medio de una técnica llamada entunelamiento (Tunneling).

Los dispositivos basados en Hardware son generalmente ruteadores que encriptan la información, son seguros y fáciles de usar, es hardware dedicado, muy rápido y de fácil instalación. Dentro de las compañías que ofrecen estas

soluciones se encuentran: Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, CheckPoint Software Technologies, etc.

Los dispositivos basados en software esta instalado en una plataforma PC o servidor, el software desempeña todas las funciones de las VPN. El rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general Un ejemplo de esto sería el sistema operativo Windows 2003 Server.

2.2.2 Cliente VPN

Un cliente VPN puede ser un dispositivo o computadora que inicializa una conexión VPN con un servidor VPN. Los dispositivos pueden ser también computadoras portátiles (Laptop), teléfonos celulares, PDAs (Personal Digital Assistant) Asistente personal digital.

2.2.3 Red de tránsito

La red de tránsito es simplemente la red por donde son cruzados nuestros datos encapsulados, generalmente es una red pública como Internet.

Por red pública se entiende un servicio comercial WAN en donde cualquier persona física o jurídica puede contratar servicios a la red y realizar intercambios de información con cualquiera de los equipos terminales de datos conectados a ella y que permitan dicha comunicación. La red de tránsito puede ser Internet o una Intranet privada que utilice el protocolo IP.

2.2.4 Túnel VPN

Esta tecnología se explicará con más detalle en el siguiente capitulo. Básicamente la tecnología Túnel o Tunneling consiste en transferir los datos de una red a otra utilizando técnicas de encriptación y encapsulación.

Los datos que se transferirán (o la carga útil) pueden ser los frames (o paquetes) de otro protocolo. En vez de enviar un frame como es producido por el nodo original, el protocolo al hacer un túnel encapsula el frame en una cabecera adicional. La cabecera adicional proporciona la información de encaminamiento de modo que la carga útil encapsulada pueda atravesar la red intermedia.

Los paquetes encapsulados entonces se encaminan entre los puntos finales del túnel sobre la red interna. La trayectoria lógica a través de la cual los paquetes encapsulados viajan a través de la red interna se llama *túnel*. Una vez que los marcos encapsulados alcancen su destino en la red interna, el frame o paquete es desencapsulado y se envía a su destino final dentro de la red. El hacer un túnel incluye el proceso entero (encapsulación, transmisión, y desencapsulado de paquetes).

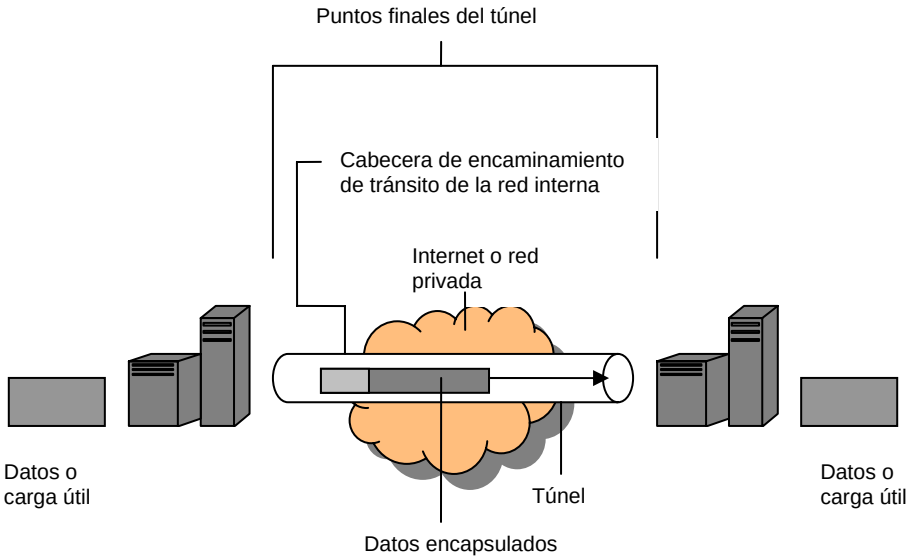


Figura 2.2 Túnel o Tunneling

Las redes privadas virtuales utilizan la encriptación para proteger los datos, los datos se cifran en la transmisión y se descifran en la recepción. Esto da la impresión de que los dos host se comunican directamente, en lugar de tener que enviar los datos de nodo a nodo sin protección durante el trayecto. Por tanto es como canalizar directamente los datos de un lugar a otro.

Esto lo logra por medio de protocolos especializados que administran el túnel y la encriptación, un ejemplo sería Point-to-Point Tunneling Protocol (PPTP).

2.2.5 Autenticación

La autenticación es uno de los elementos más importantes de una VPN en cuestión de seguridad, maneja dos aspectos: *La autenticación establece la identidad del emisor y / receptor de la información. Y la autorización, esta estrechamente vinculada a la autenticación en la mayoría de los requisitos de acceso a recursos de red. La autorización establece aquello que se le permite a uno hacer después de haberse identificado (lo que también se conoce como control de acceso, capacitaciones y permisos).*[2]

Las redes privadas virtuales utilizan procesos de autenticación de datos y usuarios. La autenticación de usuario consiste en verificar si el usuario es válido y garantizarle el acceso a la red mientras a los no válidos se les deniega. La autenticación de datos reafirma que nuestros datos han sido enviados completamente y que no ha sido alterado de ninguna forma.

La autenticación de las redes privadas virtuales utiliza protocolos de autenticación estándar, que normalmente utilizan algoritmos de dispersión. Si cambia cualquier parte del mensaje, incluso un solo bit de todo un mensaje, el resultado del algoritmo cambia. Si la dispersión es diferente de la esperada, el dispositivo de la red privada virtual sencillamente rechaza el paquete.

2.2.5.1 Protocolos de autenticación

Existen diferentes esquemas de autenticación, desde las clásicas contraseñas sencillas hasta los protocolos de autenticación avanzados. En la siguiente tabla 1 se mencionan brevemente los principales protocolos y métodos de autenticación

[2] Merike Kaeo, Diseño de seguridad en redes, Editorial Pearson Educación, Madrid 2003, p.19

Protocolos o Método de Autenticación	**Descripción**
Contraseñas del sistema operativo	Utilizar contraseñas es un medio de protección muy pobre, a pesar de ser un medio de protección muy común por su fácil instalación e implementación y por ser económicas. Pueden presentar fallas de seguridad muy peligrosas, ya que una sola computadora puede tener miles de cuentas protegidas por contraseña, irrumpir en este archivo de contraseñas puede contraer consecuencias devastadoras para la organización.
S/KEY	Es un sistema de contraseñas de un solo uso, utiliza algoritmos de una sola dirección desarrollado por Ron Rivest, con este sistema la contraseña se envía de forma abierta sobre la red, sin embargo una vez utilizada ya no resulta útil para cualquier intruso. La principal ventaja de S/KEY es que protege contra cualquier intrusión sin efectuar una modificación del software de cliente.
RADIUS	RAIDUS (Remote Acces Dial In User Service) Servicio de marcación para autenticación de usuarios remotos, Es un sistema de seguridad que utiliza autenticación, autorización y registro de actividades del usuario mientras accede a los recursos de la red. Utiliza el modelo cliente-servidor, RADIUS autentica los usuarios a través de una serie de comunicaciones entre el cliente y el servidor.
Kerberos V5	Es un protocolo de autenticación confiable, se utiliza con una contraseña o con una tarjeta inteligente para el inicio de sesión interactivo, el proceso de autenticación de Kerberos V5 consiste en emitir vales o credenciales para tener acceso a los servicios de red, estos vales o credenciales contienen datos cifrados, que incluyen una contraseña cifrada para confirmar la identidad del usuario al servicio solicitado.
Certificados Digitales	Los certificados digitales son un método para autenticar dispositivos o usuarios, son estructuras o paquetes de datos que contienen información como, por ejemplo, su nombre o dirección IP, el número de serie del certificado, la fecha de caducidad del mismo y una copia de la clave pública del portador del certificado. Los certificados digitales tienen un alto nivel de seguridad y generalmente se utilizan para transacciones financieras, comercio

	electrónico y otras aplicaciones seguras. Para obtener un certificado digital el cliente debe ir con un "Autoridad Emisora de Certificados (CA) "y comprar uno.
Tarjetas Inteligentes	Una tarjeta inteligente es un dispositivo muy similar a una tarjeta de crédito, contiene un pequeño chip incrustado y soporta distintas aplicaciones. Las tarjetas inteligentes funcionan utilizando algoritmos criptográficos proporcionando un sistema de almacenamiento difícil de manipular para proteger claves privadas y otro tipo de información. Permite que los usuarios tengan acceso a datos personales y empresariales.
Biometría	Una biometría en cuestiones de aplicaciones de cómputo, se emplea como una forma de identificación. *Una técnica biométrica de identificación es la característica o acción de un humano con el único propósito de identificarlo*[3] Es así como se puede identificar a una persona por medio de sus huellas dactilares, registro de voz, reconocimientos de retina, etc. Con un sistema biométrico de identificación, una empresa puede adquirir un factor de autenticación muy poderoso.

Tabla 1 Principales protocolos y métodos de autenticación

[3] Steven Brown, Implementación de redes privadas virtuales, editorial McGraw Hill, México 2001, p.405

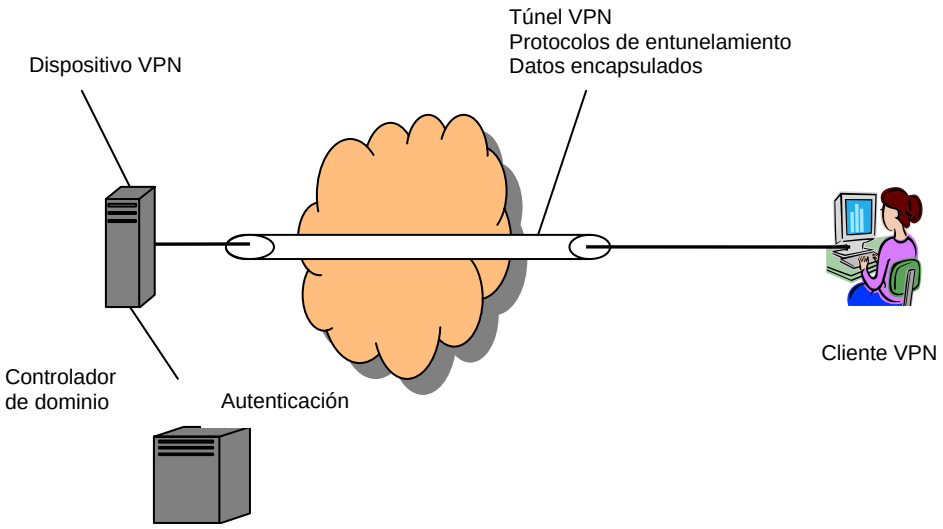


Figura 2.3 Componentes de una VPN

2.3 Proceso de conexión de una Red Privada Virtual

El proceso de conexión de una VPN se describe el los siguientes pasos:

1. Un cliente VPN hace una conexión a un servidor VPN que esta conectado a Internet. El Servidor VPN actúa como pasarela y normalmente esta configurado para proveer un acceso entero a la red por lo que el VPN es agregado.
2. El servidor VPN responde la llamada virtual
3. El servidor VPN autentifica la llamada y autoriza la conexión con el cliente
4. El servidor VPN transfiere la información entre el cliente VPN y la organización.

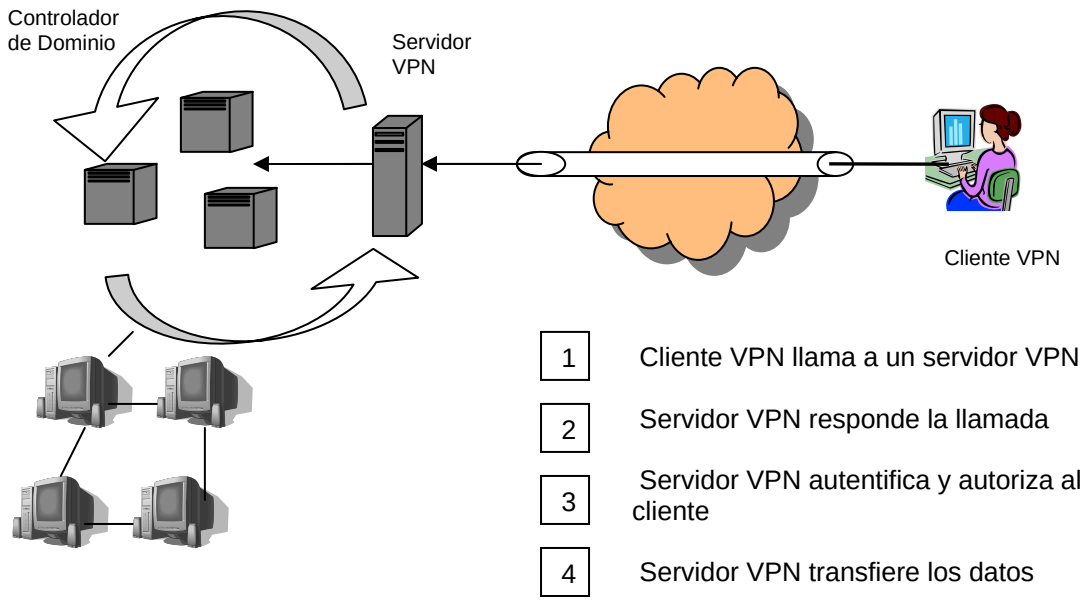


Figura 2.4 Proceso de conexión VPN

2.4 Tipos principales de Redes Privadas Virtuales

Los tipos en donde se pueden implementar las redes privadas virtuales son los siguientes:

2.4.1 Redes Privadas Virtuales de Intranet

Las VPN de Intranet están conformadas por una oficina central y sucursales externas enlazadas a una red interna sobre una infraestructura compartida usando conexiones dedicadas. Gracias a las VPN de Intranet las empresas con sucursales distribuidas en diferentes puntos geográficos pueden comunicarse entre sí como si se formara una gran red.

Normalmente solo se utiliza dentro de la red de la compañía y únicamente acceden los empleados de la misma. Los usuarios de la red que se hallan en cada lado de los lados del túnel pueden comunicarse entre sí, como si se tratara de una sola red. Las VPN de Intranet suponen reducción en costes

frente a la tecnología Frame Relay y líneas dedicadas, ya que generalmente utilizan Internet para reducir distancias, ocasionalmente grandes, entre las sucursales. En la figura 2.5 se muestra un ejemplo de VPN de Intranet.

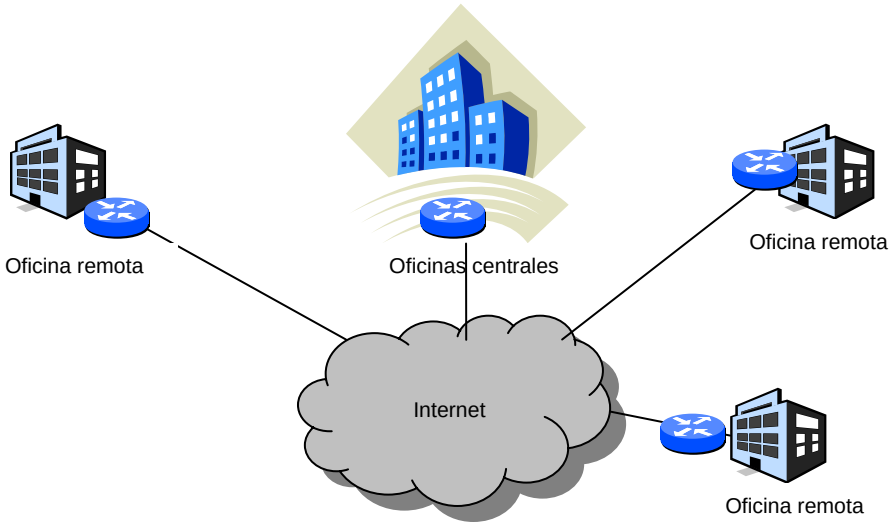


Figura 2.5 VPN de Intranet

2.4.2 Redes Privadas Virtuales de Acceso remoto

Este tipo de VPN nació de la necesidad de poder acceder a la red corporativa desde cualquier ubicación, incluso mundial. Las VPN de acceso proporcionan acceso remoto entre la Intranet o Extranet de una empresa y los usuarios móviles remotos.

Un usuario móvil puede estar ubicado en algún punto geográfico y puede acceder a los recursos de su red corporativa conectándose con cualquier proveedor de servicios de Internet (PSI) a través de una llamada telefónica, un cable, una línea DSL y conectarse a Internet, así puede acceder a los recursos de su red corporativa como son, correo interno, bases de datos, etc.

Las VPN de acceso remoto pueden soportar las necesidades de los usuarios móviles, las extranets cliente a empresa, etcétera. Una VPN de acceso remoto

puede terminarse en dispositivos de extremo final. Un dispositivo de extremo final puede ser un ruteador, firewall o un hub desplegado en el perímetro de una red.

Las VPN de acceso remoto utilizan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscriptor digital (ADSL), IP móvil y de cable para conectar de forma segura usuarios móviles, teletrabajadores y sucursales. En la figura 2.6 se muestra uno de los tipos de acceso más comunes utilizando un PSI para poder acceder a la red.

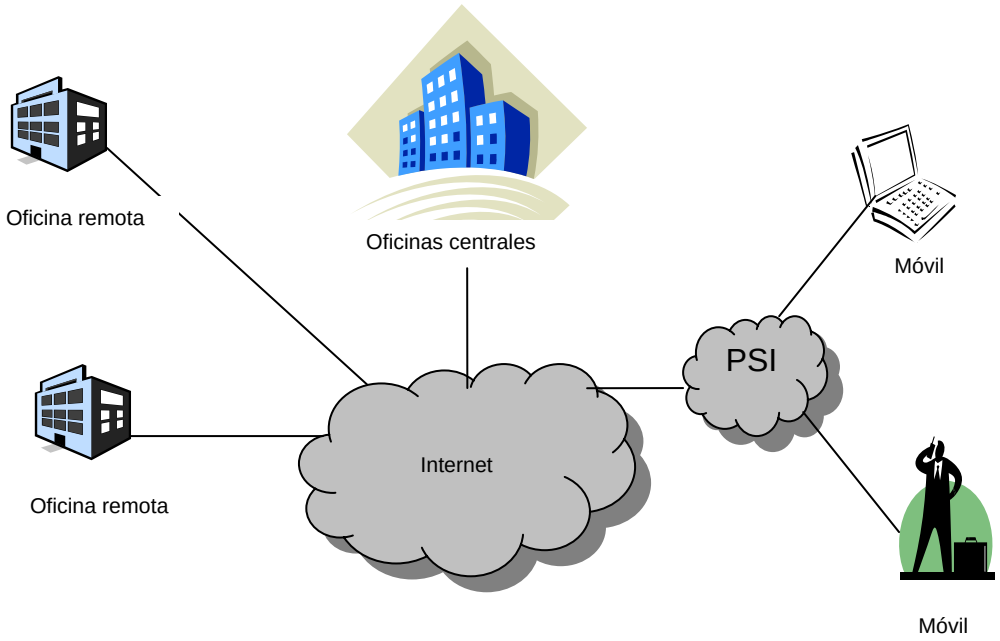


Figura 2.6 VPN de acceso remoto

Las VPN inalámbricas son del tipo de acceso remoto, en donde la conexión se establece desde terminales móviles, como pueden ser laptops, PDA`s, incluso teléfonos celulares. La autenticación se realiza por usuario y contraseña en el cliente VPN instalado en el dispositivo móvil. Para poder crear la VPN, estos usuarios que están en continuo movimiento pueden adquirir acceso a diferentes medios de redes, como pueden ser WLAN 802.11, CDMA2000 1xRTT y conexión de datos inalámbricos GPRS. El problema que puede existir en este tipo de conexiones, es cuando el usuario móvil cambia de locación

geográfica, y por lo tanto la conectividad VPN se interrumpe, si existe alguna aplicación en proceso esta se pone en espera y si existen datos en transmisión estos se pierden. La conectividad se restablece reiniciando los clientes VPN los cuales tienen que renovar la IP por medio de algún mecanismo de asignación de direccionamiento IP dinámico, como por ejemplo un DHCP o por medio de un protocolo de control de IP como el protocolo point-to point protocol (PPP).

2.4.3 Redes Privadas Virtuales de Extranet

Las VPN de Extranet son casi idénticas a las VPN de Intranet con la diferencia que estas están dirigidas a socios externos.

Las VPN de Extranet enlazan clientes exteriores, proveedores, socios o comunidades de interés para una empresa, con el propósito de intercambiar información y realizar transacciones.

Implementar una VPN de Extranet implica incrementar complejidad en lo referente a la autenticación y el acceso, por medio de los túneles VPN y Firewalls, para que las empresas socias puedan acceder de forma segura a ciertos recursos específicos, sin tener por ello acceso a toda la información corporativa confidencial.

La conexión se puede realizar por el protocolo HTTP y navegadores Web actuales, o se puede acordar otros tipos de conexión con servicios y protocolos diferentes, previamente acordados por las partes involucradas. En la figura 2.7 se muestra un ejemplo de VPN de Extranet.

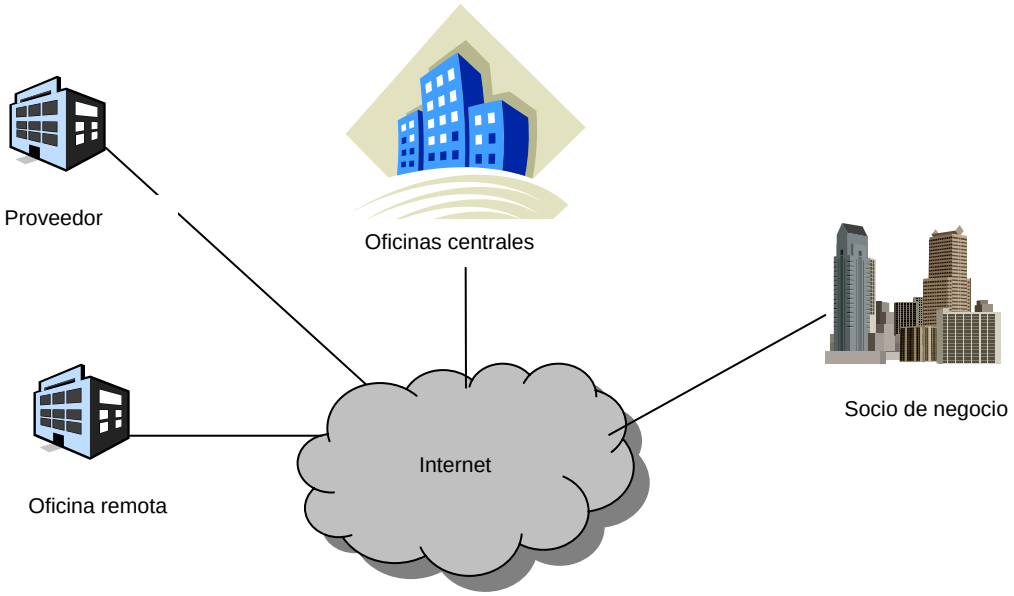


Figura 2.7 VPN de Extranet

2.5 Ventajas de las Redes Privadas Virtuales

Son muchas las ventajas que puede ofrecer una VPN bien planeada, tal vez una de las principales tiene que ver con la utilización de redes públicas como Internet ya que permite que una compañía obtenga ahorros considerables en vez de utilizar una instalación de líneas rentadas.

Pero también existen otras ventajas relacionadas con la administración, seguridad, consolidación y transparencia. A continuación se mencionaran algunas de estas ventajas.

- Una VPN permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder.

- La tecnología VPN es independiente, puede implementarse en diversas plataformas de sistemas operativos como UNIX, Windows, Linux, etc.

- Las VPN cuenta con una diversificación de conexiones, puede utilizarse en líneas rentadas, enlaces Frame Relay, ATM, RDSI, T1 o Wireless.

- Una de las ventajas de las Redes Privadas Virtuales es que por lo general la responsabilidad de su funcionamiento recae sobre el proveedor de servicios, lo cual libera a la empresa de los costos y recursos necesarios para operar y mantener una infraestructura de red, algo de especial valor para empresas que cuentan con configuraciones de red de gran complejidad.

- El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un ordenador en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, etc. a través de un acceso público.

- Las VPN al utilizar Internet como medio de comunicación reducen los costos drásticamente en comparación a las líneas dedicadas o infraestructuras de marcación interna.

- Las VPN ofrecen flexibilidad al poder optar por múltiples tecnologías y proveedores de servicio. Esa independencia posibilita que la red se adapte a los requerimientos del negocio.

- Aumenta la conectividad geográfica. Con el uso de Internet se puede conectar a la LAN de su compañía desde cualquier punto del planeta siempre y cuando exista un proveedor de servicios de Internet (PSI) en esa área.

- Seguridad mejorada. Una VPN ofrece múltiples elementos de seguridad, reduce riesgos como falseamiento IP, la pérdida de confidencialidad y la inyección de paquetes.

- Facilidad de ampliación. Conforme los proveedores de red incrementan el ancho de banda en sus redes, las VPN pueden crecer y aprovechar este ancho de banda.

- Beneficios en el diseño de red. El administrador de red no tiene que lidiar con problemas en el diseño como las de una WAN sobre líneas rentadas, como flujo de tráfico entre departamentos ubicados en distintos puntos geográficos, y creación de conductos adecuados para este tráfico, ni con las cuentas de acceso de usuarios remotos por marcación y cargas adicionales de instalar enlaces redundantes en caso de que falle el enlace de comunicación principal. Con la arquitectura VPN todo el trabajo se reduce, todo lo que se requiere es una conexión a Internet, y el PSI se encarga del transporte.

- Asignación de prioridades de tráfico. Debido a que una VPN ofrece acceso a una Intranet, Extranet o servidores internos de una organización, varios proveedores ofrecen asignación de tráfico a través de sus productos VPN.
- Es posible asignar que tipo de tráfico puede pasar libremente, con el fin de conservar el ancho de banda, mientras que otro tipo de tráfico queda en cola de espera. Esto añade gran flexibilidad a la utilización de tráfico de una compañía mediante su enlace con Internet.

2.6 Desventajas de las Redes Privadas Virtuales

Implementar tecnología VPN implica ciertos costos adicionales por parte de la organización, que se podría considerar como desventaja. Estos costos adicionales están involucrados con los aspectos de implementación, mantenimiento, costo de las licencias y algunos cargos de telecomunicaciones que no se eliminan por completo. A continuación se mencionan los más significativos.

Equipo VPN. La gran variedad de equipos que existen para implementar VPN pueden representar un problema a la hora de la implementación, hay que saber

que tipo de hardware y software se implementará o se añadirá, como puede ser ruteadores, concentradores, servidores, cableado, etc. Todo esto se tiene que multiplicar por el número de sitios que se tienen y se obtendrá un costo aproximado.

Licencias. Las licencias son otro tipo de desventaja que se puede observar en las VPN, este tipo de licencia tiene un costo para el tipo de producto que se requiera y dependen del proveedor. Algunos proveedores cobran por el número de usuarios simultáneos que pasan a través de un dispositivo de red. Mientras que otros añaden una cuota de licencia simple al ruteador, permitiendo conexiones VPN ilimitadas, otras basan sus cuotas de licencias en el número de túneles que se pueden crear.

Administración y Mantenimiento. Si el encargado del mantenimiento y administración de la VPN es su PSI, entonces esto incluye un costo extra por el servicio. Por ejemplo, si surge un problema con el hardware hay que tomar en cuenta el tiempo en que se llevara repararlo y el precio de repararlo. Generalmente los proveedores ofrecen líneas de mantenimiento con precios variables y pueden abarcar los fines de semana, es otro gasto que se incurre con el uso de esta tecnología.

2.7 Principal Arquitectura de las Redes Privadas Virtuales

Las distintas infraestructuras de red y los diferentes requisitos organizacionales exigen diferentes tipos de arquitecturas. En este punto se describen las principales arquitecturas que existen en el mercado de las VPN así como sus principales funciones en cuestiones de seguridad, autorización, acceso a usuarios, la interoperabilidad con la red interna, con los clientes y proveedores externos, para ofrecer una solución a las organizaciones interesadas en implementar la tecnología VPN.

2.7.1 Redes Privadas Virtuales basadas en Firewall

Una de las arquitecturas más importantes es la de las VPN basadas en Firewall o Cortafuego. Las VPN son un proceso muy efectivo para proteger nuestra información que viaja sobre redes públicas como Internet, pero no ofrecen protección para la propia red.

"Un Firewall o cortafuegos es un sistema de seguridad, normalmente una combinación de hardware y software que está destinado a proteger la red de una organización frente a amenazas externas que proceden de otra red, incluyendo Internet."[4]

Hoy en día es difícil encontrar una compañía que utilice Internet sin este sistema de protección, así que una Firewall es el complemento perfecto de una VPN para ofrecer una mayor seguridad en la propia red.

Una ventaja de aprovechar un firewall de una organización que ya los tiene implementados, es que se les puede instalar el software VPN y así se puede lograr un solo punto de entrada a la red. Esta es una de las configuraciones más fáciles y comunes de implementar.

Otra de las configuraciones más comunes que existen es colocar el servidor VPN tras un firewall, como se muestra en la figura 2.8 en donde el firewall está conectado a Internet y el servidor VPN es otro recurso más conectado a una zona desmilitarizada (DMZ). La DMZ es un segmento de una red IP que generalmente contiene recursos disponibles a los usuarios de Internet tales como servidores Web y de FTP. El servidor VPN tiene una interfase hacia la DMZ y una interfase hacia la intranet.

Los paquetes deben llegar al servidor VPN a través del firewall dedicado, protegiéndolo completamente frente a Internet.

Una solución basada en firewall puede ofrecer ventajas como:

[4] Fundamentos de Redes plus, curso oficial de certificación MCSE, varios autores, Editorial McGraw Hill, España 2000, P.400

- Proporciona niveles altos de seguridad y rendimiento
- La VPN está completamente protegida frente a Internet
- Si se ubica el servidor VPN tras un Firewall entonces sólo habrá un equipo que controle todo el acceso a y desde Internet
- Las restricciones de red del tráfico VPN están ubicadas únicamente en el servidor VPN lo que es más fácil crear conjuntos de normas.

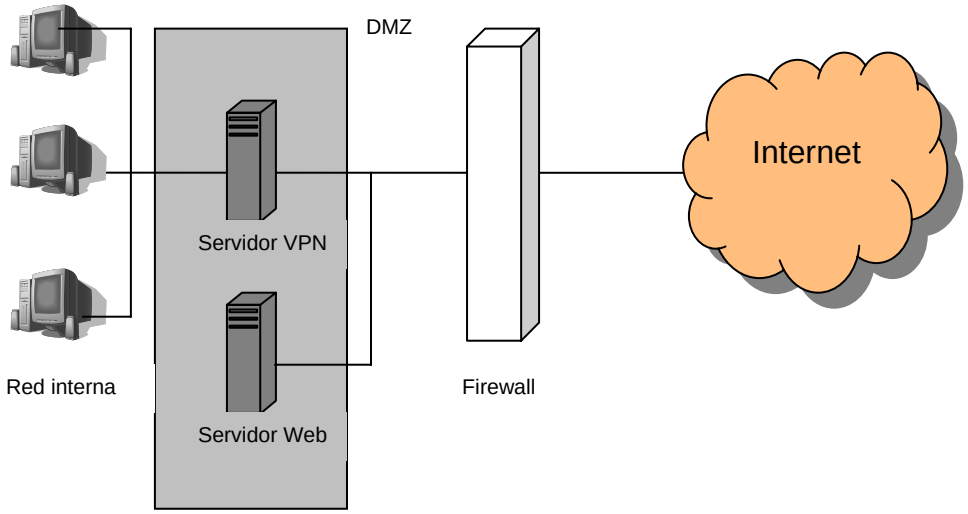


Figura 2.8 VPN sencilla basada en Firewall

Existen diferentes productos de firewall en el mercado, el producto varía desde firewall dedicados hasta “híbridos” (dispositivos con tecnología integrada de firewall y cifrado VPN) y la elección de uno de estos depende de las necesidades de la organización.

2.7.2 Redes Privadas Virtuales basadas en Router

Las VPN basadas en ruteadores es ideal para aquellas organizaciones que hayan invertido en ruteadores y además tienen una gran experiencia en ellos. Al igual que las VPN basadas en firewall existen varios proveedores de esta solución y existen diferentes tipos de VPN basadas en ruteador que manejan los proveedores.

En una, el software se agrega al ruteador para que el sistema de cifrado ocurra, en otra se le instala una tarjeta al ruteador y así se endosa el proceso de cifrado al CPU del ruteador a la tarjeta adicional. En cualquiera de estos dos tipos hay que tener en cuenta el desempeño, ya que al añadirle procesos de cifrado al enrutamiento, se agrega una carga más pesada al ruteador, especialmente si este esta manejando una gran cantidad de rutas o implementando un algoritmo de enrutamiento intensivo.

O existen proveedores que ofrecen ruteadores dedicados con tecnología VPN implementada, así proporcionan una solución de enrutamiento completa. La mayoría de este software ofrece VPN con capacidades de firewall, detección de intrusos y una fácil administración. La mayoría de este tipo de software VPN añade fuerte autenticación de cifrado a través de certificados digitales. En la figura 2.9 se muestra un VPN sencilla basada en ruteador donde los datos se cifran desde el origen hacia el destino

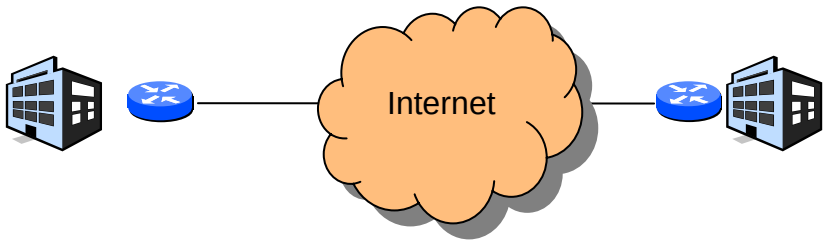


Figura 2.9 VPN sencilla basada en ruteador

Un problema que puede surgir en las VPN basadas en ruteador es la interoperabilidad, hay que tener especial cuidado en el tipo de tecnología que

se implementa en el ruteador, como puede ser PPTP, L2TP, IPSec, etc. Por ejemplo, si se requiere conectarse a otra organización y sus ruteadores están configurados con distinta tecnología a la de su empresa, surge el problema de interoperabilidad y no se podrá establecer la conexión VPN.

2.7.3 Redes Privadas Virtuales basada en acceso remoto

Este tipo de solución o arquitectura es adecuado cuando la compañía tiene muchos usuarios externos que están ubicados en diferentes puntos geográficos. Este tipo de VPN permite a los usuarios estar en continuo movimiento y conectados a su red corporativa usando una red pública disponible como Internet también puede ser, una línea de marcación, una línea ISDN , una red X.25, etc.

Ya sean trabajadores o socios, los clientes VPN tratan de establecer una conexión con la organización empleando dispositivos que puede ser desde una computadora portátil (Laptop) o dispositivos como, asistentes personales digitales (PDA), Teléfonos celulares. Estos dispositivos deben de cumplir con ciertos requerimientos, como: El equipo portátil debe cargar software VPN, tiene que establecer la opción de configuración del software VPN para que indique la dirección IP pública del dispositivo VPN y necesita conseguir la clave del dispositivo VPN.

Este software se ejecuta en los dispositivos de los usuarios remotos, algunos dispositivos ya lo traen instalado y otros se les pueden instalar con los diferentes proveedores que existen para los dispositivos móviles. En el caso de los teléfonos celulares es posible que se tenga que instalar software especial en el servidor de autenticación.

La conexión se realiza por medio de túneles a los servidores internos de la compañía o desde una línea de acceso por marcación como ISDN hacia un servidor de autenticación. El servidor de acceso instalado en la red, ya sea

ruteador, firewall, o un servidor de autenticación dedicado independiente, será el encargado de permitir el acceso a los recursos de la red. Estos dispositivos de acceso remoto reduce la cantidad de costosos equipos de líneas rentadas y de acceso por marcación remota.

2.7.4 Redes Privadas Virtuales proporcionada por un proveedor de servicios de red

Una manera más sencilla de conectar la organización a Internet y obtener los beneficios de una VPN, es contratar estos servicios a un proveedor. Es una manera de reducir costos de infraestructura, operación y mantenimiento. El proveedor será el encargado de proporcionar una solución VPN para la organización.

Al escoger este tipo de solución, se debe de tener especial cuidado en recalcar que tipo de responsabilidades abarca el proveedor, el PSI instalará dispositivos en la red de la organización y se hará responsable de las comunicaciones y buen funcionamiento asociadas a ese dispositivo, pero se debe de tener especial cuidado en cuestiones como:

Control de cambios.- Cualquier cambio de control de acceso que se requiera realizar se debe prever con un tiempo de anticipación para notificarle al proveedor, ya que lleva de 4 hasta 24 horas realizar este proceso de control de cambio.

Utilización de la red.- El PSI es el encargado de manejar la VPN, pero no de instalar capacidades de supervisión de red para la compañía. Se debe de conocer cómo funciona la red, si la compañía empieza a crecer se necesitara más ancho de banda y por consecuencia requerirá más servicios VPN, se deberá estar listo para realizar una actualización.

Seguridad.- Se debe conocer quien tiene el control de la base de datos de usuarios que permitirá crear el túnel VPN hacia la organización, si se encuentra en el dispositivo del proveedor o en algún otro dispositivo, si se encuentra en el

dispositivo del proveedor se debe de conocer el tiempo que se requiere para que una autorización se vuelva efectiva. Esto es importante, por ejemplo, en el caso de un empleado despedido.

En México una de las compañías que ofrece este tipo de solución es la multinacional AT&T, ofrece servicio de administración y mantenimiento con tecnología de dispositivos Cisco para los tres tipos de VPN.

2.7.5 Redes Privadas Virtuales basadas en Software y Hardware

Las VPN basadas en software son prácticamente programas para establecer programas de un host a otro, generalmente utilizan el modelo cliente - servidor. En este tipo de arquitectura el tráfico sale del anfitrión se cifra o encapsula, dependiendo de la VPN instalada, y se enruta a su destino. Lo mismo ocurre para alguien que esta intentando conectarse a la red interna. En este tipo de arquitectura se necesitará contar con una buena administración de claves y llaves públicas, ya que si se utiliza el modelo cliente a servidor, cada estación posiblemente podría tener su propio par de claves privada / pública.
En el caso de las VPN basadas en hardware, son dispositivos independientes a los que se les a agregado algoritmos de tecnología VPN, estos dispositivos son generalmente más rápidos en los procesos de cifrado / descifrado que los dispositivos de software. Los dispositivos actuales contienen procesadores internos dedicados, que manejan la autentificación, el tipo de tecnología y otros tipos de funciones VPN y muchas veces proporcionan un firewall al hardware.

Al igual que en la figura 2.8 un dispositivo VPN se puede ubicar por detrás del firewall de la red interna. Conforme los datos pasan por estos dispositivos, se mantienen intactos o se cifran, dependiendo de la configuración del dispositivo.
Este tipo de dispositivos tienen la ventaja de una fácil administración, generalmente se pueden configurarse y mantenerse con el uso de un explorador Web. Los dispositivos VPN suelen ser más caros que las VPN

basadas en software, debido que un VPN hardware es una opción más realista para las grandes empresas que para las sucursales o pequeñas empresas, debido a la gran variedad de funciones que ofrecen como alto rendimiento, cargas masivas del cliente, redundancia y balanceo de cargas, son únicamente posibles con este tipo de hardware VPN.

III

Tecnología de las Redes Privadas Virtuales

FES UNAM ACATLAN

3.1 Tecnología de las Redes Privadas Virtuales

La tecnología VPN esta basada en la creación de túneles para establecer VPN seguras a través de un medio público como Internet, esto se logra, a través de protocolos que integran técnicas claves de entunelamiento, autenticación y encriptación. Estos protocolos trabajan en el nivel 2 y nivel 3 del modelo OSI. Los protocolos de nivel 2 corresponden al enlace de datos y usan tramas como unidad de intercambio, PPTP y L2TP son protocolos de nivel 2 y ambos encapsulan la información dentro de frames PPP para ser enviados a través de una red pública o Internet. Los protocolos de nivel 3 corresponden al nivel de red y utilizan paquetes de información que son enviados a través de una red IP.

Estos protocolos los podemos dividir en protocolos *estándar* y protocolos de *fuente abierta* o *no estándar*, los protocolos *estándar* son sancionados por una agencia de vigilancia, que por lo general se encarga de las especificaciones de desarrollo y las políticas de desempeño para toda una industria. La organización que se encarga de esto en el caso de los protocolos VPN estándar, es la IETF (Internet Engineering Task Force) La Fuerza de Trabajo de Ingeniería de Internet que a su vez es supervisada por la IAB (Internet Architecture Board) Consejo sobre Arquitectura Internet, y los estándares son publicados en forma de RFC (Request For Comments) Petición de comentarios.

Los protocolos de fuente abierta o no estándar, no necesariamente son sancionados por una organización, ignoran totalmente los estándares de estas agencias, principalmente por cuestiones de diseño, normalmente son protocolos y especificaciones que son populares y fáciles de usar. La desventaja con este tipo de tecnología es la falta de soporte y de documentación.

3.2 Protocolo de Túnel Punto a Punto. PPTP

El protocolo de Túnel Punto a Punto es un protocolo que fue diseñado por varias empresas como: Ascend Communications, Microsoft Corporation, 3Com, Copper Mountain Networks y ECI Telematics, siendo Microsoft a quien se le atribuye el desarrollo por haberlo popularizado, al implementarlo en su sistema operativo Windows NT, y posteriormente a sus demás sistemas operativos.

El protocolo PPTP es un protocolo que se diseño principalmente, para VPNs tipo de acceso remoto, el PPTP permite la transferencia de datos de un cliente remoto a un servidor corporativo privado a través de Internet u otra red pública, implementa concretamente el modelo cliente-servidor y es una combinación del protocolo punto a punto (PPP) y del protocolo TCP / IP.

PPTP combina funciones del PPP como el multiprotocolo, la autenticación de usuarios y la compresión de paquetes de datos, y TCP / IP ofrece capacidad para en rutar esos paquetes por Internet.

El protocolo PPTP especifica una serie de mensajes de control con el fin de establecer, mantener y destruir el túnel PPTP estos mensajes son transmitidos en paquetes de control en el interior de segmentos TCP. PPTP encapsula los paquetes de PPP en datagramas IP utilizando el protocolo TCP para establecer los túneles. Por esta razón, además de establecer túneles de IP, también encapsula los protocolos que no son TCP tales como IPX, NetBEUI y NetBIOS. Estos protocolos proporcionan archivos o directorios compartidos, soporte a periféricos y soporte a hardware, respectivamente, dentro de una LAN, dándole al usuario remoto la impresión de trabajar en un ambiente de una LAN común o en uno de Intranet como si estuvieran conectados localmente.

3.2.1 Redes Privadas Virtuales y PPTP

El típico escenario de una VPN con PPTP involucra tres elementos, un cliente VPN, un servidor de acceso a la red y un servidor PPTP.

Un usuario remoto necesita acceder a la red corporativa, primero necesita conectarse a un servidor de acceso a red (NAS) marcando a su PSI local, un servidor de acceso remoto implementa las siguientes funciones:

- Proporciona una interfaz física nativa a las redes telefónicas conmutadas públicas (PSTN) o RDSI y controlar los adaptadores externos de MODEM o digital.
- Terminación lógica de un protocolo PPP.
- Participar en los protocolos de autenticación PPP.
- Proporcionar la adición y la administración para el protocolo multienlace PPP.
- Terminación lógica de los distintos protocolos de control de red de PPP.
- Realizar el enrutamiento y el punteado multiprotocolo entre las interfaces del NAS.

El protocolo PPTP es el encargado de dividir todas estas funciones entre dos entidades:

- Concentrador de acceso PPTP (PAC). Este dispositivo esta conectado a una o más líneas PSTN o RDSI capaces de funcionar con PPP y de manipular el protocolo PPTP.

- Servidor de red PPTP (PNS). Administra el lado del servidor del protocolo PPTP, es el encargado de la adición de canales, la terminación de los protocolos de control de red, así como del enrutamiento y el punteado multiprotocolo entre las interfaces del NAS.

En la figura 3.1 se muestra una conexión de un cliente a un servidor de acceso a red, donde lo primero que se realiza es una autenticación sencilla previa al envío y recibo de tramas PPP de datos.

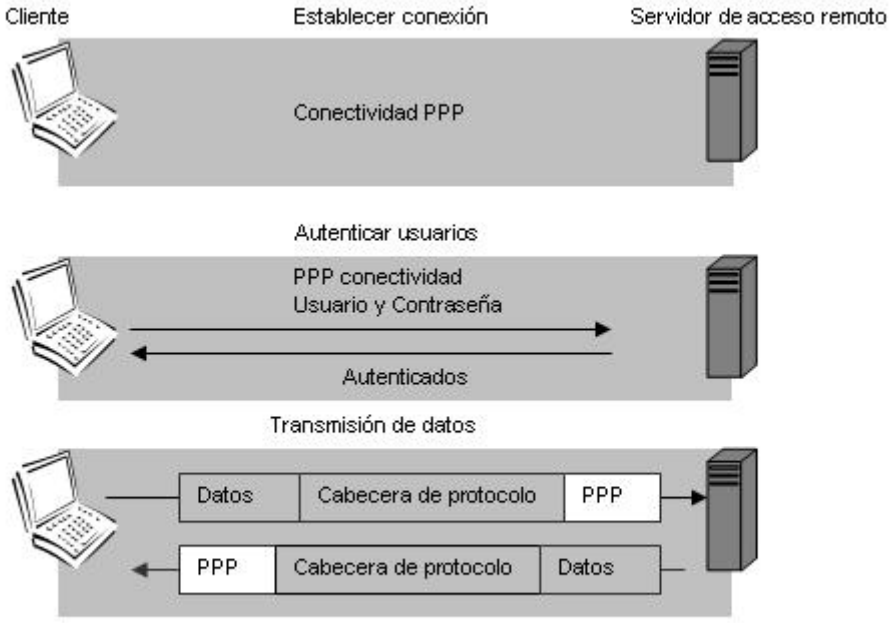


Figura 3.1 Conexión PPP entre un cliente y NAS

Una vez establecida la conexión PPP con el PSI, se realiza un segundo establecimiento de llamada sobre la conexión existente PPP, el protocolo PPTP realiza la conexión entre el cliente PPTP y el servidor PPTP esto es lo que crea la conexión VPN y se refiere como túnel PPTP a través del cual fluyen los paquetes de red. Los mensajes de control son los que establecerán, mantendrán y finalizaran el túnel PPTP. Los mensajes de control se muestran en la siguiente tabla 2.

Tipo de mensaje	**Significado**
PPTP_START_SESSION_REQUEST	Inicia sesión
PPTP_START_SESSION_REOLY	Responde la solicitud
PPTP_ECHO_REQUEST	Mantiene la sesión
PPTP_ECHO_REPLY	Responde para mantener la sesión
PPTP_WAN_ERROR_NOTIFY	Error en la conexión en un enlace PPP
PPTP_SET_LINK_INFO	Configura la conexión entre cliente y servidor PPTP
PPTP_STOP_SESSION_REQUEST	Termina la sesión PPTP
WAN_ERROR_NOTIFY	Errores en la interfaz PPP de la WAN

Tabla 2. Mensajes de control

PPTP toma los paquetes PPP y los encapsula dentro de un encabezado con Encapsulamiento para Enrutamiento Genérico (GRE), PPTP utiliza del protocolo PPP, el Protocolo de autenticación de contraseña (PAP) y el protocolo de de autenticación de intercambio de señales por desafío (CHAP) para proporcionar mecanismos de autenticación.

3.2.2 Los túneles PPTP

Los túneles PPTP son la etapa final de la transmisión, donde los datos del usuario son transmitidos entre el cliente y el servidor PPTP y es cuando el servidor PPTP descifra estos paquetes y los envía a los anfitriones respectivos.

Un túnel viene definido por un par de PNS-PAC. El túnel transporta datagramas PPP entre el PAC y el PNS. PPTP requiere el establecimiento de un túnel para cada par PNS-PAC que se comunique, este túnel se usa para transportar todos los paquetes PPP de sesión de usuario para las sesiones que impliquen un par PNS-PAC determinado. Estos datos de usuario que transporta el protocolo PPTP son transmitidos en datagramas IP y contenidos dentro de paquetes PPP. Estos datagramas IP son creados, usando el protocolo de encapsulamiento para enrutamiento genérico GRE (Generic Routing Encapsulation), la cabecera GRE es usada para encapsular el paquete PPP dentro del datagrama IP.
En la siguiente figura 3.2 se muestra la estructura general de paquetes que se transmite sobre los túneles que hay entre un PAC y un PNS.

Figura 3.2 Estructura de un paquete PPTP

Estos datagramas IP se encaminan sobre Internet o red pública hasta que llegan al servidor PPTP que esta conectado a Internet y a la red corporativa. El servidor PPTP desmonta el datagrama IP en un paquete del PPP usando el protocolo de red de la red corporativa. De tal manera, los protocolos de red de

la red corporativa que son soportados por PPTP son IPX, NetBEUI o TCP/IP. Cuando el servidor PPTP recibe el paquete de la red, la envía a través de la red corporativa a la computadora destino. El servidor PPTP hace esto procesando el paquete PPTP para obtener la información privada del nombre o de la dirección de la computadora de red en el paquete encapsulado PPP.

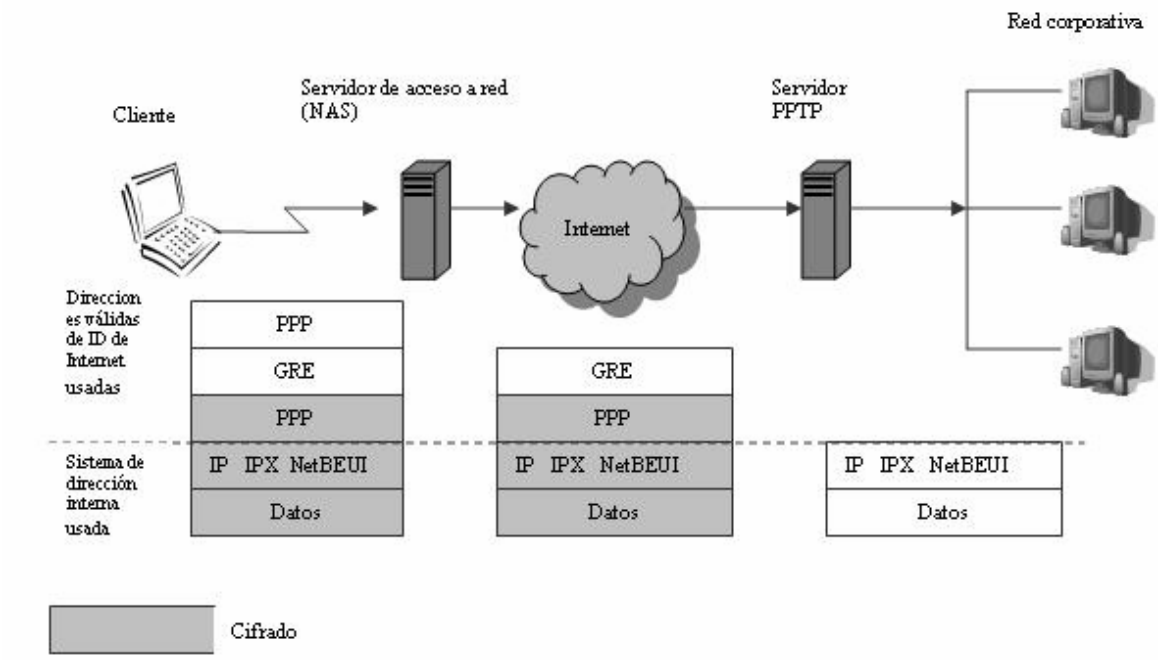


Figura 3.3 Estructura de túnel PPTP

La figura 3.3 ilustra el soporte multiprotocolo construido en PPTP. Un paquete enviado del cliente de PPTP al servidor de PPTP pasa a través del túnel de PPTP a una computadora destinada en la red corporativa.

PPTP soporta dos tipos de túneles, modo obligatorio o permanente y modo voluntario, son determinados por las capacidades del cliente VPN y del soporte para implementar túneles PPTP del servidor de acceso remoto.

El modo obligatorio, utiliza los servicios de un PSI junto con un procesador frontal (FEP) PPTP[1], no se necesita ningún tipo de software PPTP en el cliente ya que este reside en el NAS del PSI, en modo obligatorio los túneles se crean

[1] Los servidores de acceso remoto también son referidos como procesadores frontales (FEP), servidores de petición de marcado (dial-in) o servidores de punto de presencia (POP)

sin consentimiento del usuario y por lo tanto son transparentes para el mismo. El protocolo PPP maneja cualquier problema de comunicación en una conexión por marcación al PSI, si existe algún problema en el equipo portátil puede deberse a la configuración de marcación a la red. La conexión se restringe solo a la utilización del túnel PPTP, por lo tanto no hay acceso a la red pública o Internet sobre la cual se establece el túnel, el túnel obligatorio permite que múltiples conexiones sean transportadas por el mismo túnel. En la figura 3.4 se muestra un túnel obligatorio.

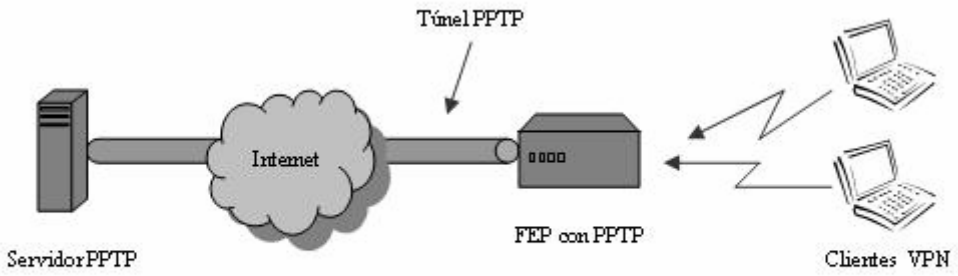


Figura 3.4 Túnel modo obligatorio

En el modo voluntario los clientes establecen una conexión directa con el servidor PPTP en el otro extremo de la red para crear un túnel. En el PPTP de modo voluntario no hay requisitos para el FEP de un PSI. Las conexiones se hacen directamente al servidor PPTP de la red corporativa, el software PPTP reside en la computadora del cliente y puede acceder simultáneamente a Internet y abrir un túnel seguro hacia el servidor PPTP. En la figura 3.5 se muestra un túnel en modo voluntario.

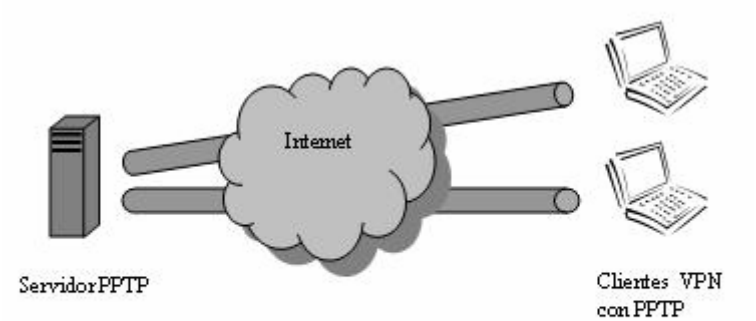


Figura 3.5 Túnel PPTP de modo voluntario

3.3 Protocolo de reenvío de capa dos. L2F

El protocolo de reenvío de capa dos (Cisco Layer Two Forwarding (protocol L2F)) es un protocolo desarrollado por Cisco Systems, su salida al mercado, fue al mismo tiempo que el protocolo PPTP de Microsoft lo que lo opacó e hizo que no fuera popular.

El protocolo L2F es muy parecido al PPTP de Microsoft, es un protocolo que encapsula tramas para transportarlos a nivel de enlace como: Control de enlace de datos de alto nivel (HDLC), PPP, Protocolo Internet de línea serie (SLIP), etc. El usuario hace una conexión PPP o SLIP a un proveedor PSI de marcación, y con el uso de L2F, se conectan a las máquinas de su compañía. Estos túneles se encuentran en los extremos de la conexión de la red pública o Internet, y son ruteadores con software para el establecimiento de túneles L2F.

El protocolo L2F a comparación del protocolo PPTP no depende de IP para entunelar los protocolos de entunelamiento de nivel dos de otros medios de red orientados a paquetes como retransmisión de tramas, X.25 o ATM.

El reenvío de nivel 2 ofrece muchos beneficios, como los siguientes:

- Independencia de protocolo (IPX, SNA)
- Autenticación (PPP, CHAP, TACACS)
- Administración de direcciones (asignadas por destino)
- Túneles dinámicos y seguros
- Independencia de medios, por ejemplo, sobre L2F (ATM, X.25)

3.3.1 Red Privada Virtual con L2F

La figura 3.6 muestra un escenario de ejemplo para L2F.

El usuario remoto inicia una conexión PPP con un PSI, el NAS acepta la conexión y se establece el enlace PPP. El PSI autentica el sistema o usuario final con CHAP o PAP, el NAS inicia el túnel L2F con el gateway del servidor corporativo deseado, donde el gateway del servidor corporativo debe autenticar al usuario remoto y acepta o rechaza el túnel, Si el servidor acepta la conexión, crea una interfaz virtual para PPP, de una forma análoga a como se haría en conexión telefónica directa. Con esta interfaz virtual, las tramas del nivel de enlace pueden pasar por este túnel en ambos sentidos. Las tramas del usuario remoto son recibidas por el NAS, encapsuladas en L2F y reenviadas por el túnel adecuado.

El gateway del servidor corporativo acepta estas tramas, elimina la encapsulación L2F, y las procesa como tramas entrantes normales en relación a la interfaz y protocolo apropiado. El sentido contrario se comporta de manera análoga, el servidor corporativo encapsula el paquete en L2F, y el NAS elimina la encapsulación L2F antes de enviar la interfaz física al usuario remoto. Al llegar a este punto el servidor corporativo intercambia las negociaciones PPP con el usuario remoto.

Figura 3.6 Escenario de ejemplo L2F

Dado que el usuario remoto se ha convertido en otro cliente de acceso telefónico del servidor de acceso del gateway corporativo, la conectividad del cliente podrá ser manipulada utilizando mecanismos tradicionales con respecto a la autorización, la negociación de direcciones, el acceso de protocolos, la contabilidad y el filtrado. Finalmente los datos de extremo a extremo son canalizados entre el usuario remoto y el gateway corporativo.

3.3.2 Operación del protocolo L2F

La encapsulación de paquetes PPP con L2F y la administración de la conexión de L2F son de gran importancia para el buen funcionamiento del protocolo L2F. El NAS del PSI así como el servidor corporativo requieren ser compatibles con el protocolo de encapsulamiento para poder transmitir y recibir con éxito paquetes de SLIP y PPP a través de la red pública o Internet. El túnel se debe iniciar y terminar como necesidad de los identificadores de multiplexión (Multiplex ID) que están dentro del túnel. La terminación del túnel incluye códigos de diagnostico para asistir en diagnósticos de problemas.

Los paquetes PPP pueden ser encapsulados dentro de L2F. El paquete encapsulado es el paquete que será transmitido sobre un enlace físico. El

formato del paquete L2F encapsulado tiene la siguiente forma, mostrado en la figura 3.7.

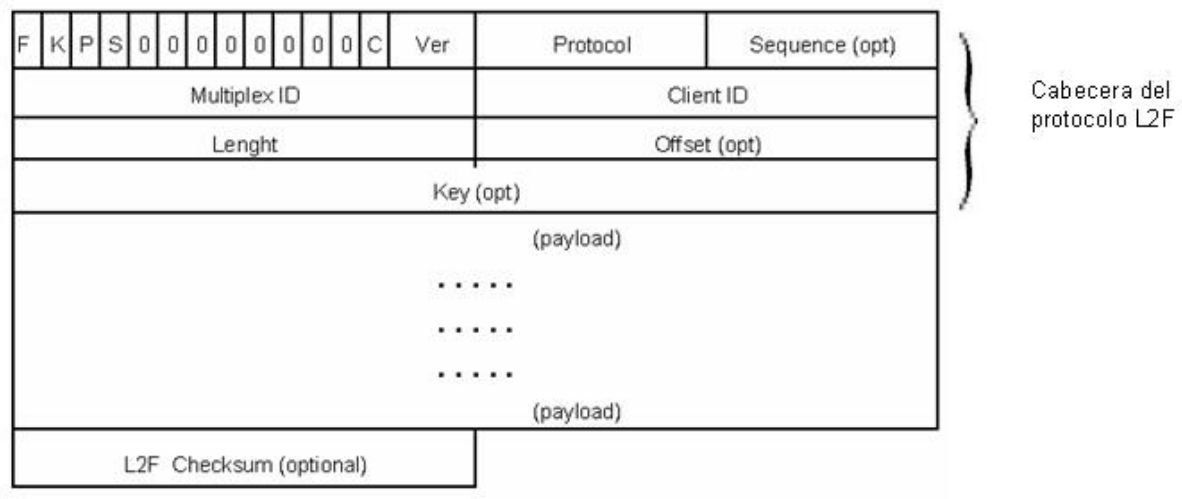


Fig. 3.7 Formato de un paquete entero L2F encapsulado.

El campo Ver (Version) representa la versión principal del software L2F que crea el paquete. Este campo debe contener el valor 001.Si el campo es diferente de 1 entonces se definirá como un paquete inválido.
El campo protocolo, específica el protocolo llevado dentro del paquete L2F. Los valores legales expresados en hexadecimal en la siguiente tabla son:

Valor	Tipo	Descripción
0x00	L2F_ILLEGAL	Ilegal
0x01	L2F_PROTO	Administración de paquetes L2F
0x02	L2F_PPP	Túnel PPP de L2F
0x03	L2F_SLIP	Túnel SLIP de L2F

Si un paquete se recibe con un protocolo L2F_ILLEGAL o de cualquier otro valor desconocido, se tratará como un paquete ilegal.

El campo sequence esta presente si el bit S de la cabecera L2F se fija en 1.Este bit tiene que ser 1 para toda la gestión de paquetes L2F.

Multiplex ID (MID) se utiliza para identificar una conexión particular dentro del túnel. Cada nueva conexión se asigna a un MID dentro del túnel. El MID con valor 0 tiene un significado especial y se utiliza para comunicar el estado del mismo túnel, a diferencia de cualquier otra conexión dentro del mismo túnel, solamente los paquetes L2F_PROTO pueden ser enviados usando un valor 0, otro tipo de paquete enviado con MID 0, se considerará ilegal.

Client ID (CLID) es usado para asistir los puntos finales, en el desmultiplexado de los túneles, cuando la conexión punto a punto carece de una técnica confiable para hacer esto directamente. Usando CLID es posible desmultiplexar túneles múltiples cuyos paquetes llegan sobre la conexión punto a punto, sin requerir semántica específica.

Lenght es el tamaño en octetos del paquete entero, incluye cabecera, todos los campos presentes y la carga útil.

El Checksum esta presente si el bit C esta presente en la bandera de la cabecera. Es aplicado sobre el paquete entero, comenzando con el primer octeto de banderas L2F, a través del último byte de la carga útil de datos

El campo Offset esta presente si el bit F es fijado en la bandera de la cabecera.
Este campo especifica el número de bytes pasados más allá de la cabecera de L2F en la cual se espera que los datos de la carga útil comiencen.

El campo Key es presente si el bit K es fijado en la cabecera L2F. Este campo se basa en la última respuesta de la autenticación del punto durante la creación del túnel. Sirve como llave durante la vida de una sesión para resistir los ataques basados en spoofing. Si se recibe un paquete en el cual Key no empareja el valor previsto, el paquete debe ser desechado silenciosamente.

Si el bit P se fija a 1 en la cabecera L2F, este paquete es un paquete de prioridad. Cuando es posible para una implementación, un paquete recibido con el bit P=1 se debe procesar en preferencia a los paquetes sin procesar previamente recibidos sin el bit P.

3.4 Protocolo para establecimiento de túneles de nivel dos. L2TP

Debido a la similitud de funciones entre los protocolos PPTP de Microsoft y L2F de Cisco, conjuntamente con otros fabricantes, deciden realizar un protocolo estándar único que, da como resultado una combinación de ambos protocolos, y lo denominan Protocolo para establecimiento de nivel dos (Layer Two Tunneling Protocol. LT2P) que es supervisado por la IETF.

El protocolo L2TP, se apoya en el protocolo PPP para establecer conexión por marcación, pero a diferencia de PPTP y al igual que L2F, no dependen de IP para encapsular los protocolos de entunelamiento del nivel dos, permitiéndole trabajar con otros medios físicos, como por ejemplo Frame Relay. L2TP define sus propios protocolos basado en L2F para establecer túneles, permitiendo transporte sobre una amplia variedad de medios orientados a paquetes como retransmisión de tramas, X25 o ATM.

La autenticación de usuarios por vía de acceso telefónico viene proporcionada por los protocolos CHAP, PAP, EAP de PPP e incluye soluciones TACACS y RADIUS, también soporta las tarjetas inteligentes y las contraseñas de un solo uso. Como L2TP es un protocolo de nivel 2, al igual que PPTP soporta otros protocolos que no son IP tales como IPX y NetBEUI.

Los cambios a comparación con los elementos de PPTP son semejantes, el servidor PPTP es remplazado por uno L2TP, y que el FEP PPTP del PSI ha sido remplazado por un concentrador de acceso L2TP. L2TP permite varias conexiones dentro de un túnel y asigna un identificador de llamadas único a cada sesión dentro del túnel.

3.4.1 Red Privada Virtual con L2TP

El escenario de una red privada virtual con L2TP es muy similar al escenario de PPTP, el cliente VPN debe realizar una conexión PPP con un PSI que utiliza PSTN o RDSI, el servidor de acceso remoto NAS debe soportar L2TP y en este caso puede ser un concentrador de acceso L2TP (LAC) o un NAS que actué como LAC.

El concentrador de acceso L2TP tiene como función implementar los medios sobre los cuales funciona L2TP para pasar el tráfico a uno o más servidores de red L2TP. También es el iniciador de las llamadas salientes y el receptor de las llamadas entrantes. El LAC puede entunelar todos los protocolos que sean transportados dentro de PPP

El servidor de red L2TP (LNS), funciona en toda plataforma que soporte PPP. Dado que L2TP se apoya exclusivamente en el único medio sobre el que llegan los túneles L2TP, el LNS puede tener solo una interfaz LAN o WAN pero es capaz de finalizar las llamadas que lleguen en cualquier intervalo completo del LAC de las interfaces PPP como RDSI, PPP sobre ATM, PPP sobre Frame Relay.

Una vez que LAC acepta la conexión y se establece el enlace PPP. L2TP permite que el LAC compruebe la señal de una llamada LNS antes de aceptarla. Esto es útil por que proporciona información acerca de donde se esta realizando la llamada para conectarse el usuario, a esto se le conoce como cadena de información del número marcado (DNIS).

El PSI puede ahora realizar una autenticación parcial del sistema o usuario final, como ya se menciono anteriormente, utiliza protocolos de PPP tales como PAP y CHAP para realizar la autenticación. Antes de que se produzca el túnel entre un concentrador de acceso L2TP y un servidor de red L2TP, se realiza un intercambio de mensajes de control entre ellos. Los mensajes de control, son los medios responsables de funciones, como la configuración, la terminación,

la administración de la sesión y el estado del túnel. Los mensajes de control mantienen las características dentro del túnel como es el control del flujo y determinar la velocidad de transmisión y los parámetros de la memoria intermedia para los paquetes PPP de sesiones individuales. Los mensajes de datos son paquetes PPP sin la información de tramas que están siendo transportadas sobre el túnel. En la figura 3.8 se muestra la relación que existe entre los tramas PPP y los mensajes de control sobre los canales de control y datos de L2TP.

Las tramas PPP son transportadas sobre un canal de datos no fiable, encapsulados primero por una cabecera L2TP y luego por transporte de paquetes como UDP, Frame Relay, ATM, etc. Los mensajes de control son enviados sobre un canal L2TP fiable, el cual transmite paquetes sobre el mismo transporte de paquetes.

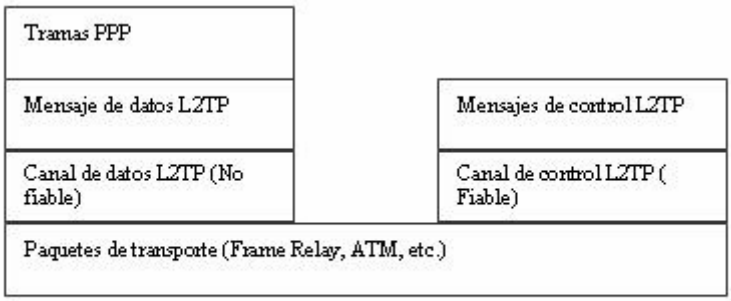


Figura 3.8 Estructura del protocolo L2TP

L2TP al igual que PPTP tiene su propia lista de mensajes de control y se muestra en la siguiente tabla 3.

Tipo de mensaje	**Significado**
Start-Control-Connection-Request (SCCRQ)	Inicia la sesión
Start-Control-Connection-Reply (SCCRP)	Responde la solicitud
Start-Control-Connection-Connected (SCCCN)	Responde la réplica; termina el reconocimiento en el establecimiento del túnel
Stop-Control-Connection-Notification (StopCCN)	Cierra la conexión de control
HelloTunnel (Hello)	Está activo
Outgoing-Call-Request (OCRQ)	LNS informa a LAC que debe establecer una llamada externa
Outgoing-Call-Reply (OCRP)	Respuesta de LAC
Call-Disconnect-Notify (CDN)	Notificación de finalización de sesión

Tabla 3 Mensajes de control L2TP

Una vez que se establece el túnel con el LNS deseado, éste puede ser usado para transportar paquetes PPP de sesión de usuario, en las sesiones que implique un par LNS-LAC determinado. El campo Session ID de la cabecera de L2TP indica la sesión a la que pertenece un determinado paquete PPP.

La cabecera L2TP se muestra en la siguiente figura 3.9 en donde los paquetes L2TP, para el canal de control y el canal de datos, comparten un formato de cabecera en común.

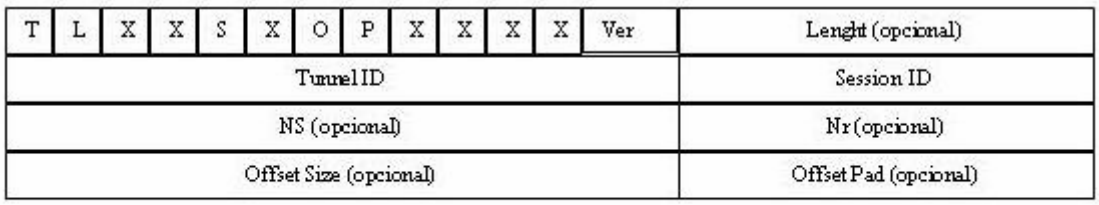


Figura 3.9 Formato de cabecera L2TP

Las especificaciones del formato de cabecera de L2TP es el siguiente:

El bit Type (T) indica el tipo de mensaje. Es 0 para un mensaje de datos y 1 para los mensajes de control.

El bit Lenght (L) si es 1 el campo de longitud esta presente. Este bit se debe de fijar en 1 para los mensajes de control.
Los bits X están reservados para futuras extensiones. Todos los bits reservados se deben fijar en 0 en mensajes de salida e ignorar en mensajes entrantes.

El bit de Sequence (S) si esta fijado en 1 los campos NR y NS están presentes. El bit S se debe fijar en 1 para los mensajes de control.

El bit Offset (O) si es 1, el campo de tamaño Offset está presente. El bit Offset debe ser puesto en 0 para los mensajes de control.

El bit Priority (P) si es 1, este mensaje de datos debe recibir un tratamiento preferencial en las colas locales y en la transmisión. Las peticiones del LCP usadas para el enlace como keepalive, por ejemplo, se deben enviar generalmente con este bit fijado en 1. Si esto se puede ocasionar una demora en los mensajes keepalive, ocasionando una perdida innecesaria del enlace.
Ver debe ser igual a 2 e indica la versión de la cabecera de mensajes de datos L2TP que se está usando. El valor 1 se reserva para permitir la detección de los paquetes L2F. Los paquetes recibidos con un campo desconocido de "Ver" deben ser descartados.
El campo lenght indica la longitud total de los mensajes en octetos.

El campo Túnel ID indica el identificador para la conexión de control. Los túneles L2TP son nombrados por los identificadores que tienen significado local solamente, es decir el mismo túnel será dado por diferentes "Tunnel IDs" por

cada extremo del túnel. El tunnel ID en cada mensaje es la del receptor previsto, no el remitente.

Session ID indica un identificador para una sesión dentro de un túnel. Las sesiones L2TP son nombradas por identificadores que tienen significado local únicamente.

Ns indica el número de secuencia para los mensajes de datos o de control

Nr indica el número de secuencia esperado en el mensaje siguiente de control para ser recibido. En mensajes de datos, Nr es reservado, y si esta presente debe ser ignorado según el bit S.

El campo Offset size, si esta presente, especifica el número de octetos después de la cabecera L2TP en el cual se espera que los datos de la carga útil comiencen.

Los paquetes PPP son multiplexados y desmultiplexados sobre un solo túnel entre un par determinado LNS-LAC. De esta manera es posible que haya múltiples túneles en un determinado par LNS-LAC, la ventaja de tener múltiples túneles, es que a cada uno se le puede asignar una sola sesión de usuario y los medios del túnel pueden tener atributos de servicios de calidad (QoS) específicos dedicados a un usuario concreto. En la figura 3.10 se muestra un escenario de ejemplo L2TP.

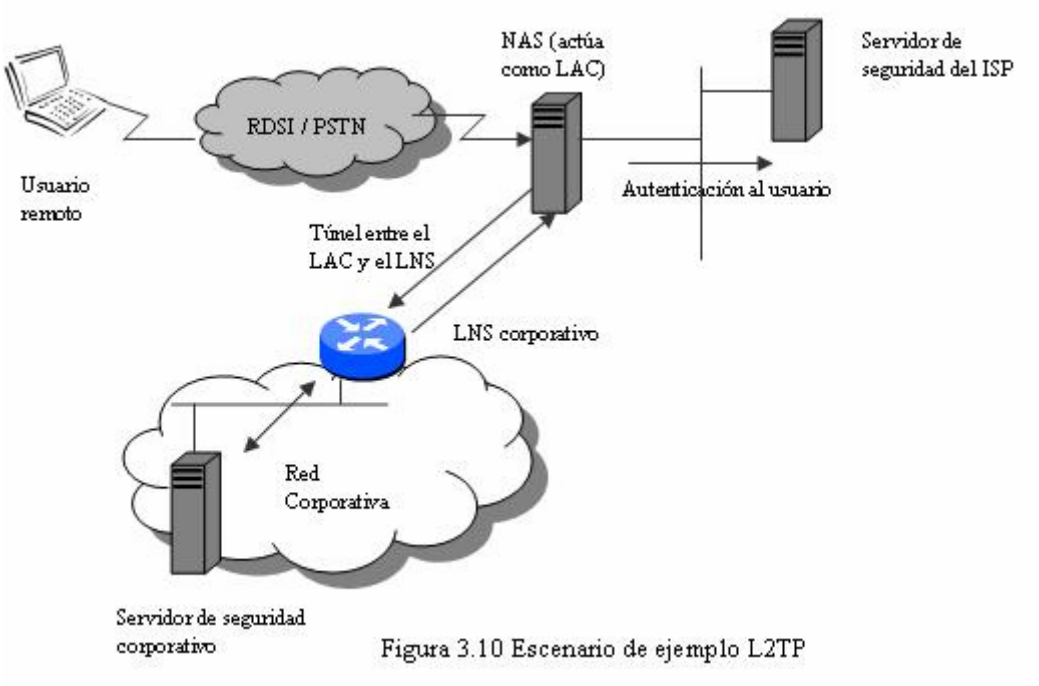


Figura 3.10 Escenario de ejemplo L2TP

3.4.2 Operación del protocolo

Para tunelizar una sesión PPP con L2TP se necesita dos factores, el primero, estableciendo una conexión de control para el túnel y el segundo estableciendo una sesión, según la operación por una petición de una llamada entrante o saliente. El túnel y la conexión correspondiente de control, deben ser establecidos antes de que se inicie una llamada entrante o saliente. Una sesión de L2TP debe establecerse antes de que L2TP pueda empezar a tunelizar tramas PPP. Las sesiones múltiples pueden existir a través de un solo túnel y los túneles múltiples pueden existir entre el mismo LAC y LNS. En la siguiente figura 3.11 se muestra el entunelamiento de PPP con L2TP.

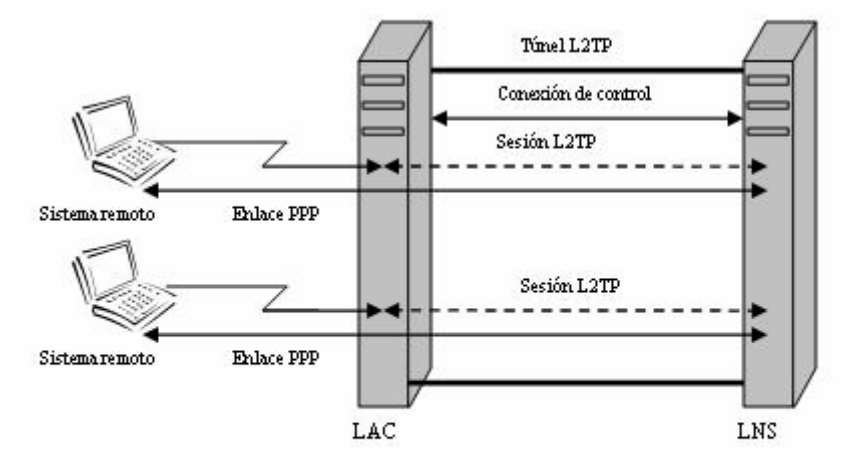


Figura 3.11 Entunelamiento PPP usando L2TP

La conexión de control, es la primera conexión que se lleva a cabo entre un LAC y LNS antes de que las sesiones se puedan subir. El establecimiento de la conexión de control incluye asegurar la identidad de ambos (LAC y LNS) así como la identificación de la versión de L2TP que utilizan. Un intercambio de tres mensajes se utiliza para preparar la conexión de control. La siguiente figura 3.12 muestra un intercambio típico de mensaje[2].

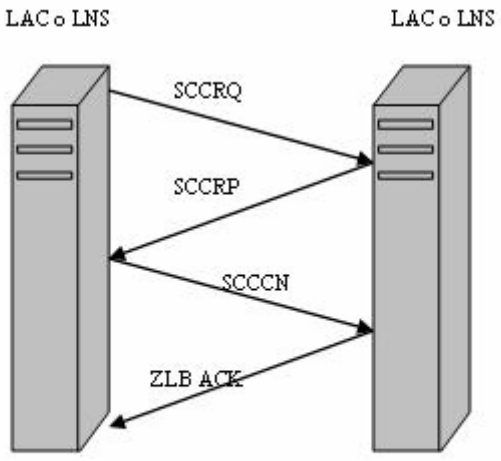


Figura 3.12 Establecimiento de conexión de control.

El mensaje ZLB ACK se envía si no hay otros mensajes en cola de espera para ese par. Para la autenticación L2TP utiliza un sistema simple y opcional

[2] Los mensajes son los que se especifican en la tabla 3

parecido al CHAP, durante el establecimiento de la conexión de control. Después de establecer la conexión de control correctamente, las sesiones individuales pueden ser creadas. Cada sesión corresponde a una sola dirección PPP entre el LAC y el LNS. A diferencia del establecimiento de la conexión de control, el establecimiento de la sesión es direccional con respecto al LAC y LNS. El LAC solicita al LNS aceptar una sesión para una llamada entrante, y el LNS solicita a LAC aceptar una sesión para una llamada saliente.

Una vez que el establecimiento del túnel se ha completado, las tramas PPP del sistema remoto se reciben en el LAC, se encapsulan en L2TP y se remiten sobre el túnel apropiado. El LNS recibe el paquete de L2TP y procesa la trama encapsulada de PPP como si fuera recibido en una interfaz local de PPP.

El remitente de un mensaje asociado con una sesión particular y el túnel coloca el identificador de sesión y de sesión en la cabecera de los campos Session ID y tunnel ID para todos los mensajes de salida. De esta manera las tramas PPP son multiplexeadas y desmultiplexeadas sobre un solo túnel entre un par dado de LAC-LNS. Los túneles múltiples pueden existir entre un par dado de LNS-LAC, y las sesiones múltiples pueden existir dentro de un túnel.

Para terminar la sesión se puede realizar por el LAC o el LNS y se logra enviando un mensaje de control CDN. Después de que la última sesión se ha limpiado, la conexión de control también se puede terminar.

Para finalizar una conexión de control se puede realizar por medio del LAC o de LNS y es logrado enviando un solo mensaje de control StopCCN. EL receptor de un StopCCN debe enviar un ZLB ACK para reconocer el recibo del mensaje y para mantener suficientemente el estado de la conexión de control para aceptar correctamente el excedente de las retransmisiones de StopCCN. En la siguiente figura 3.13 se muestra el intercambio de mensajes de control para terminar la conexión. También una implementación puede terminar un

túnel entero y todas las sesiones sobre el túnel enviando StopCCN. Así no es necesario terminar cada sesión individualmente para poder terminar con el túnel.

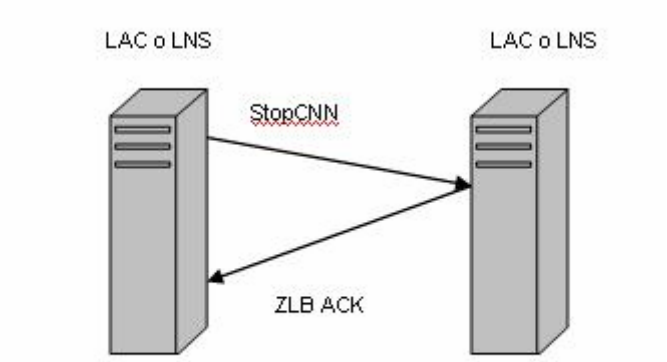


Figura 3.13 Terminando la conexión de control

3.5 Seguridad del protocolo Internet. IPSec

El protocolo de seguridad de Internet IPSec, es un estructura que comprende un conjunto de estándares de protocolos de seguridad y algoritmos, utilizados para proporcionar servicios de seguridad, integridad y autenticación de datos en el nivel de red (IP) y a todos los protocolos superiores basados en IP (TCP, UDP, etc.).

La tecnología IPSec esta basada en tecnología de criptografía moderna, lo que proporciona privacidad y autentificación segura de datos, las redes privadas virtuales, utilizan esta tecnología de autenticación y encriptamiento, como parte de sus medidas de seguridad, ya que proporciona, la confidencialidad de datos enviados y evitando el acceso a usuarios no autorizados en la VPN, entre otras cosas.

IPSec se basa en los siguientes dos protocolos para proporcionar seguridad del tráfico, cada uno de los cuales se implementan mediante cabeceras de extensión que siguen a la cabecera principal de IP y son:

- Cabecera de autenticación (AH). Proporciona protección a todo el datagrama incrustando la cabecera en los datos, también verifica la integridad del datagrama IP.
- Carga de seguridad de encapsulamiento (ESP). Encapsula los datos pero no ofrece protección a las cabeceras externas, ESP encripta la sobrecarga para la confidencialidad de los datos.

IPSec también utiliza estándares de cifrado existentes formando un conjunto de protocolos que proveen varios servicios de seguridad:
Algoritmos de cifrado, tales como:

- Estándar de cifrado de datos (DES)
- Triple DES (3DES)
- Diffie-Hellman(D-H)
- Boletín de mensajes 5 (MD5)
- Algoritmo hash seguro-1 (SHA-1)
- Firmas Rivest, Shamir y Alderman (RSA)
- Dominio de interpretación (DOI)
- Intercambio de clave de Internet (IKE)
- Asociaciones de seguridad (SA)

La forma de como se puede estructurar IPSec se muestra en la siguiente figura 3.14.

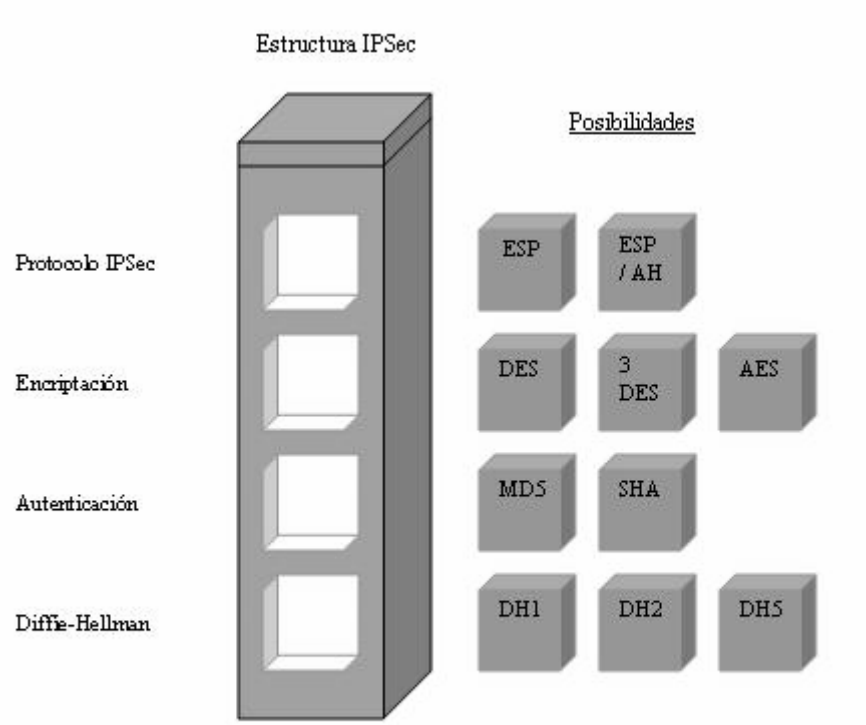


Figura 3.14 Estructura de cómo se puede formar IPSec

3.5.1 Protocolo de autenticación de cabecera. AH

El protocolo AH, es un protocolo que cuando se añade a un datagrama IP, proporciona integridad y autenticación de los datos, además de ofrecer protección contra ataques repetitivos mediante números de secuencia. La integridad garantiza que el datagrama no sea alterado en forma inesperada o maliciosa, y la autentificación, proporciona un medio al receptor para autentificar el origen de los datos. AH proporciona dicha autentificación para toda la cabecera IP que sea posible, así como para los datos de los protocolos de niveles superiores. Sin embargo AH no proporciona protección de la confidencialidad ya que no soporta métodos de encriptamiento, es decir los datos pueden ser vistos por terceros. El protocolo AH es apropiado cuando importar, exportar o usar encriptación esta prohibido por disposiciones de gobiernos locales.

AH puede aplicarse solo o en combinación de ESP, o de una manera anidada a través de un túnel. Los servicios de seguridad pueden ofrecerse a través de un par de host comunicados, o entre un servidor de seguridad y un host.
La cabecera de autenticación que se añade aun datagrama se muestra en la siguiente figura 3.15

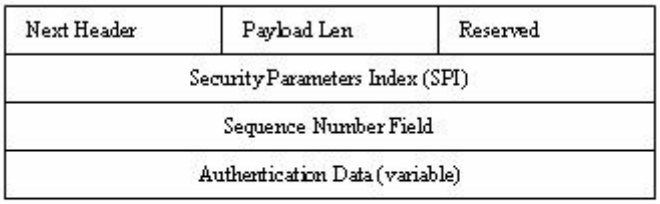


Figura 3.15 Formato de la estructura AH

El campo Next Header. Es un campo de 8 bits, que identifica el tipo de la carga útil después de la cabecera de autenticación.
Payload Lenght. Es un campo que especifica la longitud de la cabecera de autenticación AH.
Reserved. Es un campo de 16 bits reservado para un futuro uso. Tiene que estar fijado en cero.
Security Parameters Index (SPI). El SPI es un valor arbitrario de 32 bits, que en combinación con la dirección IP destino y el protocolo IPSec (AH), únicamente identifica la asociación de seguridad (SA) usada para ese paquete.
Sequence Number. Este campo, contiene un número de secuencia de 64 bits que previene la repetición del paquete. Es obligatorio y siempre esta presente.
Authentication Data. Este es un campo de longitud variable, que contiene el valor de chequeo de integridad (ICV), para este paquete IP. Las especificaciones del algoritmo de autenticación deben especificar la longitud del ICV, las reglas de comparación y los pasos del procesamiento para la validación.

3.5.2 Carga de seguridad de encapsulación. ESP

La cabecera de carga de seguridad de encapsulación, esta diseñada para proporcionar una combinación de servicios de seguridad en IPV4 e IPV6. Este protocolo también puede ser aplicado solo o en combinación de AH. La cabecera ESP es insertada después de la cabecera IP y antes de la cabecera del protocolo de nivel superior (modo transporte) o antes en una cabecera IP encapsulada (modo túnel), estos modos se describen en el siguiente punto.

ESP se emplea para proporcionar confidencialidad, autenticación de datos de origen, integridad sin conexión, servicio anti-repetición y confidencialidad del flujo de tráfico limitado. Este conjunto de servicios ofrecidos depende de las opciones seleccionadas en el momento de establecer la asociación de seguridad (SA) y en el momento de efectuar la implementación. La confidencialidad puede ser seleccionada independientemente de todos los de más servicios. Sin embargo el uso de la confidencialidad sin las características de integridad / autenticación ya sea con ESP o de una manera separada en AH, podría estar expuesto el tráfico a ciertas formas de ataques activos que minaran el servicio de confidencialidad.

La autenticación de los datos de origen y la integridad sin conexión son servicios conjuntos que se ofrecen como opción junto con la confidencialidad. El servicio anti-repetición sólo puede seleccionarse si esta activada la autenticación de datos en origen. La confidencialidad y la autenticación son opcionales, pero al menos una de ellas debe estar seleccionada. En la figura 3.16 se muestra el formato de la cabecera del paquete ESP.

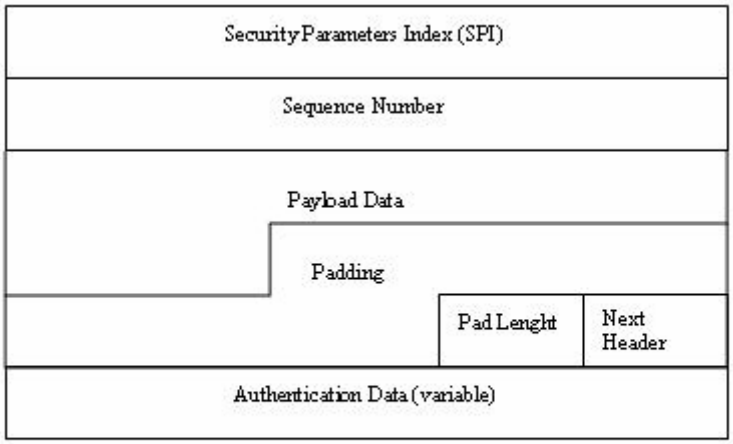


Figura 3.16 Formato de la cabecera ESP

El SPI es un valor arbitrario de 32 bits, que en combinación con la dirección IP destino y el protocolo IPSec (ESP), únicamente identifica la asociación de seguridad (SA) usada para ese paquete.

Sequence Number. Este campo, contiene un incremento monotónico. Es obligatorio y siempre esta presente, previene la repetición del paquete.

Payload Data. Es un campo de longitud variable que contiene los datos descritos por el campo Next Header. Es un campo obligatorio y es un número entero de bytes en longitud. Si el algoritmo usado para encriptar la carga útil requiere los datos criptográficos de la sincronización, entonces estos datos pueden ser llevados explícitamente en el campo pay load.

Padding. Es un campo que apoya los procesos de cifrado, es un campo opcional dentro de la cabecera ESP, pero todas las implementaciones deben soportar la generación y el consumo del campo.

Pad Lenght. Es un campo obligatorio, indica el numero de bytes del pad inmediatamente antes de el. El rango de valores validos es 0-255, donde un valor de cero indica que no hay bytes de rellenos presentes.

Next Header. Es un campo de 8 bits que identifica el tipo de datos contenidos en el campo Payload Data. Este campo es obligatorio.

Authentication Data. Es un campo de longitud variable, que contiene el valor de chequeo de integridad (ICV), computado sobre el paquete ESP menos los datos de autenticación. La longitud del campo es especificada por la función de

la autentificación seleccionada, este campo es opcional y es incluido solamente si el servicio de autenticación ha sido seleccionado por la SA. La especificación del algoritmo de autentificación debe especificar la longitud del ICV, las reglas de la comparación y los pasos de proceso para la validación.

3.5.3 Modos de transporte IPSec

IPSec soporta dos tipos de modos para enrutar nuestros datos de una manera segura a través de redes no fiables, modo túnel y modo de transporte. ESP y AH pueden aplicarse a los paquetes IP en ambos modos.

En el modo transporte cada host final efectúa la encapsulación IPSec de sus propios datos, host-a-host, por lo tanto debe implementase IPSec en los host finales, el punto final de la aplicación, también debe encontrase en el punto final IPSec. En el modo túnel, se hace uso de los gateways los cuales ofrecen los servicios IPSec al resto de host en túneles igual-a-igual. Los gateways IPSec ofrecen protección transparente para el tráfico de otros host a través de la red, los host finales no saben que se esta utilizando IPSec para proteger su tráfico. En la siguiente figura 3.17 se muestra una ruta IPSec protegida en modo túnel y en modo transporte.

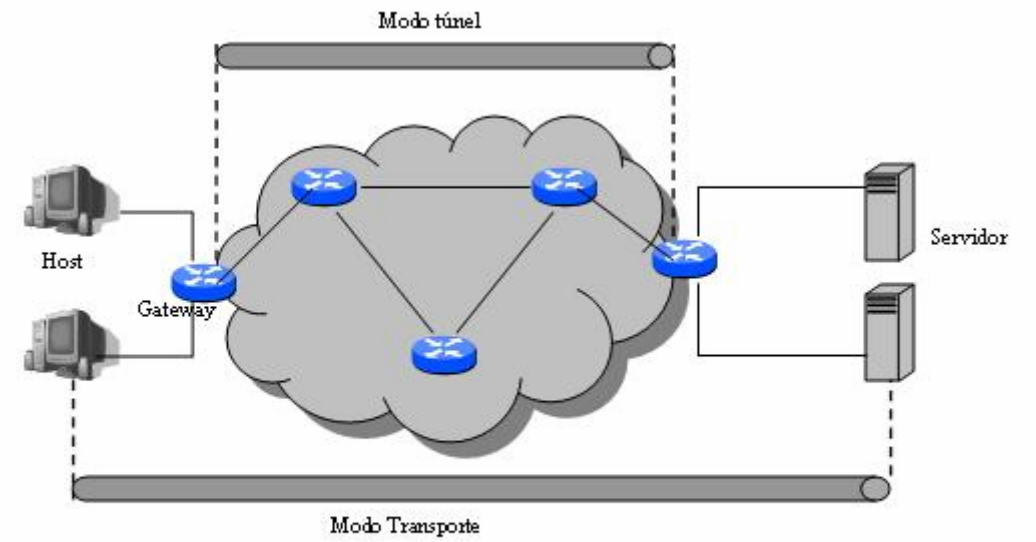


Figura 3.17 Comparación de modos de transporte de IPSec

En el modo transporte, la seguridad solo se aplica al nivel de transporte y a los protocolos superiores, y solo protege la sobrecarga del paquete pero deja la dirección IP original abierta, esta dirección se utiliza para enrutar el paquete a través de Internet.

El modo túnel protege todo el paquete IP original, es decir, todo el paquete es encriptado, la dirección IP externa se utiliza para enrutar el paquete a través de Internet, el paquete encriptado se encapsula en otro paquete IP y la dirección IP externa se utiliza para enrutar el paquete a través de Internet. Las nuevas cabeceras AH, y las cabeceras de túnel opcionales, se incorporan al paquete. En la siguiente figura 3.18 se muestra el modo transporte para AH, la cabecera AH añade 24 bytes a cada paquete, mientras en el modo túnel que se presenta en la figura 3.19, las cabeceras IP y AH añaden 24 bytes a cada paquete.

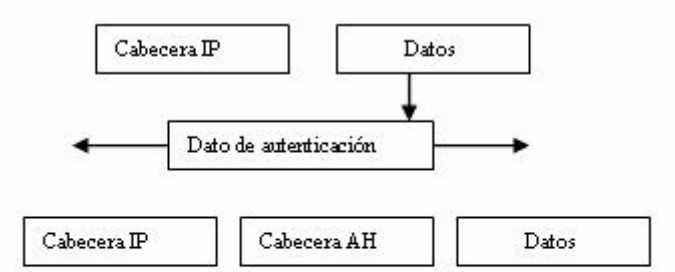


Figura 3.18 Transporte en modo AH

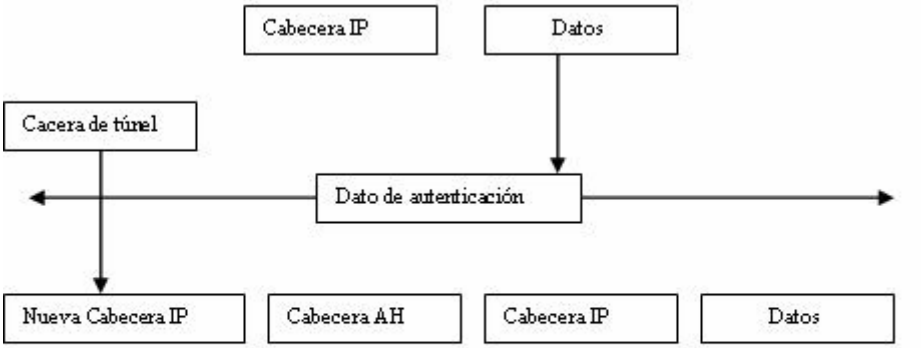


Figura 3.19 Túnel en modo AH

Para el modo transporte con ESP, las nuevas cabeceras ESP, las cabeceras de túnel opcionales y un bloque de información final (trailer) se incorporan al paquete, la cabecera / bloque de información final ESP añade normalmente hasta 37 bytes a cada paquete, mientras que en modo túnel, las cabeceras ESP e IP y el bloque de información final añaden hasta 57 bytes. Si se utiliza AH y ESP en modo túnel, se puede llegar a añadir hasta 101 bytes. En las siguientes figuras 3.20 y 3.21 se muestran los modos transporte y túnel en modo ESP respectivamente.

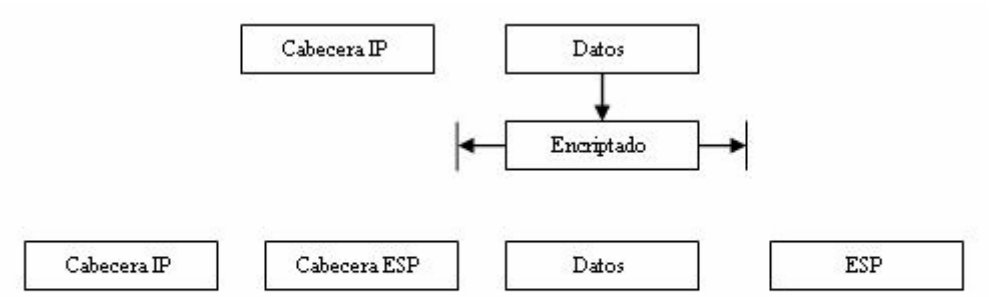


Figura 3.20 Transporte en modo ESP

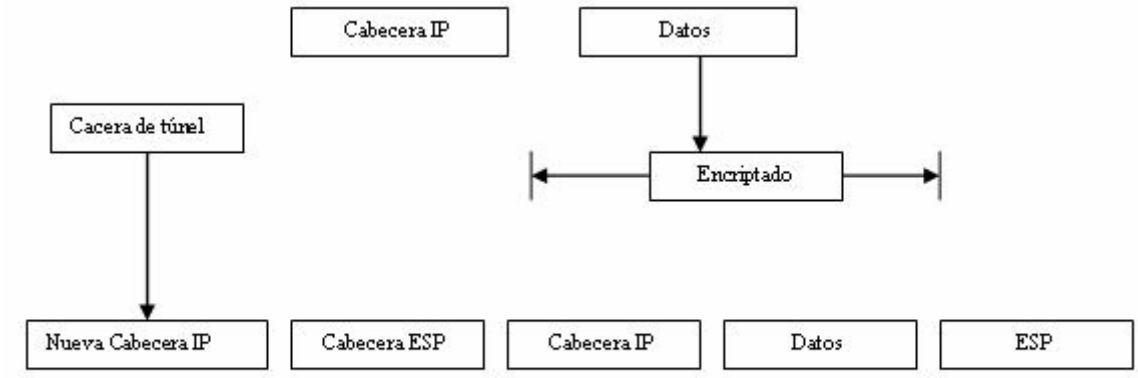


Figura 3.21 Túnel en modo ESP

3.5.4 Asociaciones de seguridad

"Una asociación de seguridad (SA) es una relación entre dos o más entidades que describe como las entidades usarán los servicios de seguridad para comunicarse de forma segura."[3] Por lo tanto IPSec establece que antes de que ocurra cualquier comunicación, se negociará una SA entre los dos nodos o compuertas de la red privada virtual y describen el modo en que esos iguales usarán los servicios de seguridad IPSec, para proteger el tráfico de la red. Aspectos como los servicios a nivel aplicación, autenticación y carga cifrada también se determinan durante esta comunicación de asociación de seguridad.

Las SA son unidireccionales para IPSec, de modo que el igual 1 ofrecerá al igual 2 una norma. Si el igual 2 acepta esta norma, enviará de vuelta al igual 1.

[3] Redes Privadas virtuales de Cisco Secure Pág.26

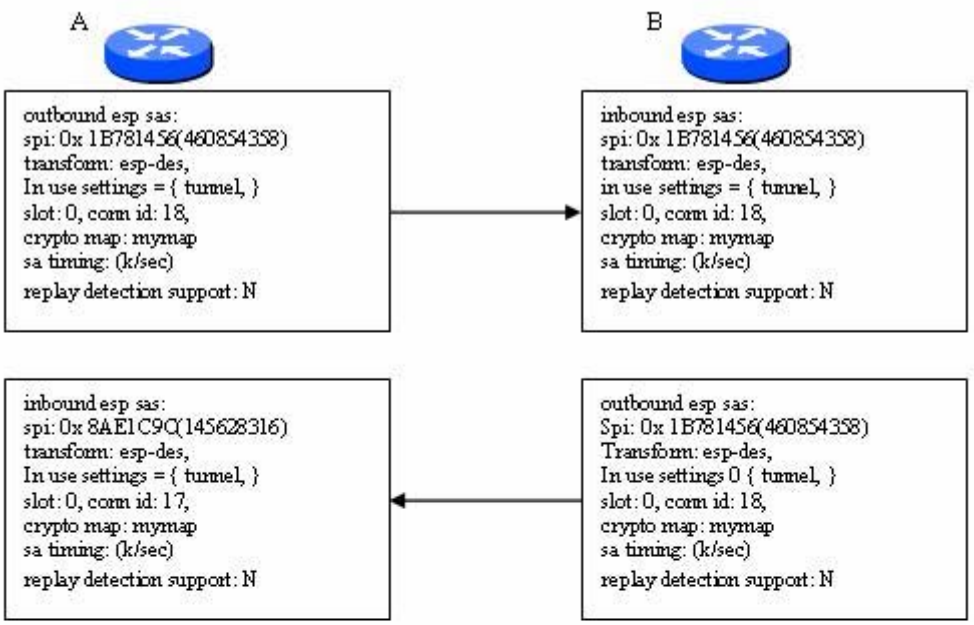
Esto establece dos AS bidireccionales entre los iguales. Por ejemplo, si dos host A y B, se comunican de forma segura utilizando AH y ESP, cada uno de ellos construye SAs separadas, de entrada y salida, para cada protocolo. Los dispositivos VPN almacenan sus SAs activas en una base de datos local llamada SADB (SA database, Base de Datos SA).

Cada SA consta de valores tales como la dirección de destino, un índice de parámetro de seguridad (SPI), las transformaciones IPSec utilizadas para esa sesión, las claves de seguridad y los atributos adicionales. Un ejemplo de estos valores se muestra en la siguiente figura 3.22

Dirección de destino	190.168.2.1
Índice de parámetros de seguridad (SPI)	7A390BC1
Transformación IPSec	AH, HMAC-MD5
Clave	7541CA48F765233689
Atributos AS adicionales (por ejemplo, tiempo de vida)	Un día o 100MB

Figura 3.22 Asociación de seguridad IPSec

Un ejemplo de la utilización de estos parámetros se muestra en la siguiente figura 3.23, donde cada AS de IPSec es unidireccional, y los parámetros AS deben coincidir en cada igual IPSec.



Parámetro	Descripción
outbound esp sas:spi:	Indice de parámetro de seguridad, que coincide con el SPI de salida para esa AS
transform: esp-des	Transformación IPSec
In use settings = {tunnel, }	Modo de transformación IPSec (túnel o transporte)
spot: 0, conn id: 18, crypto map: mymap	Información de motor de cifrado y de mapa de cifrado
sa timing: (k / sec)	Tiempo de vida de la SA en KB y segundos
replay detection support: N	Detección de reproducción on u off

Figura 3.23 Ejemplo de parámetro AS con routers

3.5.5 Intercambio de claves en Internet. IKE

Debido a que IPSec carece de un sistema para administrar claves; la creación, el intercambio y el mantenimiento de estas claves criptográficas no existe en IPSec, sin embargo el protocolo de intercambio de claves de Internet IKE es una norma de un protocolo de administración de claves usado por IPSec que le proporciona características adicionales y flexibilidad, además de hacer que sea más sencillo de configurar.

IKE “Es un protocolo híbrido que implementa los intercambios de clave Oakley y Skemi dentro de la estructura ISAKMP”, estos son protocolos definidos por IKE ofreciendo autenticación, negociación de claves y asociaciones de seguridad a los iguales de IPSec.

ISAKMP (Protocolo de administración de clave de asociación para la seguridad de Internet), es un protocolo que define el proceso y los formatos de los paquetes para configurar, negociar, modificar y eliminar las asociaciones de seguridad. La asociación de seguridad contiene información, como autenticación y el encapsulamiento de carga. ISAKMP define la carga para intercambiar la generación de claves y la autenticación de datos. Sin embargo, no está ligado a ningún algoritmo criptográfico, técnica de generación de claves o mecanismo de seguridad, así que podría estar abierto a un ataque de un intermediario; por lo tanto las firmas digitales son obligatorias.

Oakley es un protocolo para establecer las claves de sesión, soporta el secreto perfecto, el cual utiliza con el protocolo ISAKMP para administrar las asociaciones de seguridad. Oakley es un intercambio de claves genérico con claves de larga duración.

Skemi (Mecanismo de intercambio de claves seguro para Internet) describe un intercambio de claves versátil que proporciona el anonimato, la rentabilidad y la actualización rápida de claves.

IKE proporciona los siguientes beneficios:

- Permite el intercambio de claves de encriptación durante las sesiones IP

- Permite que se actualicen las claves encriptadas durante las sesiones IPSec
- Permite que IPSec proporciones servicios contra repeticiones
- Permite el soporte de la autoridad emisora de certificados
- Permite que los administradores especifiquen un tiempo de vida para la asociación de seguridad IPSec.

En la figura 3.24 se muestra como IPSec utiliza IKE para proteger las negociaciones SA utilizando ruteadores, la configuración del modo IKE permite que un gateway descargue en el cliente una dirección IP y otro tipo de parámetros a nivel red como parte de la negociación IKE. Con este intercambio, el gateway entrega direcciones IP al cliente IKE para que sean utilizadas como una dirección IP interna encapsulada bajo IPSec, todo este proceso ofrece una dirección IP conocida al cliente, la cual puede cotejarse después con una política IPSec.

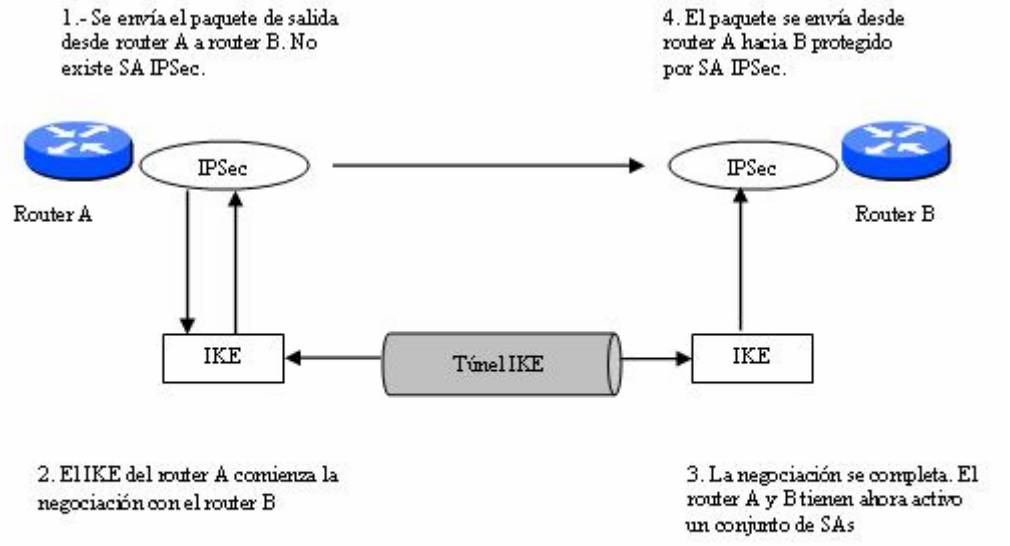


Figura 3.24 IPSec con IKE

A continuación se describen las tecnologías implementadas más importantes que para utilizarse con IKE:

Estándar de cifrado de datos (DES). Es el esquema de cifrado simétrico más común, IKE lo utiliza para encriptar paquetes de datos e implementa el DES-CBC (Cipher Block Chaining) de 56 bits con el estándar explicit IV.

Encriptación 3DES de 168 bits. Es superior al DES, puede utilizar una, dos o tres claves diferentes, sacrifica velocidad a cambio de un algoritmo más seguro. Tanto el algoritmo DES como 3DES son de dominio público y de libre disposición.

Diffie-Hellman (D-H). Es un protocolo que sirve para crear claves de sesión secretas de forma distribuida utilizando algoritmos de cifrado (DES o MD5 por ejemplo), proporciona un mecanismo para que dos partes establezcan una clave secreta compartida que sólo ellas conocen, incluso cuando se comunican a través de un canal inseguro.

Algoritmo Message Digest 5(MD5). Es un algoritmo creado por Ron Rivest en 1991 en los laboratorios RSA, es un algoritmo *hash* utilizado para autenticar paquetes, una función tipo hash es un algoritmo de cifrado unidireccional que toma como entrada un mensaje de longitud arbitraria y produce un mensaje de salida de longitud fija.

Algoritmo hash seguro (SHA). Es un algoritmo desarrollado por el Instituto nacional de estándares y tecnología (NIST), es utilizado para la autenticación de paquetes, toma una cadena y produce un compendio de mensajes de 160 bits. Aun cuando es más lento que otras funciones de transformación de código, se considera más seguro ya que tiene mayor longitud.

Los certificados X.509v3. También se pueden utilizar con IKE, cuando la autenticación precisa de claves públicas, estos certificados permite que la red protegida se escale, proporcionando el equivalente a una tarjeta de identificación digital a cada dispositivo.

3.6 Conmutación multiprotocolo por etiquetas. MPLS

La conmutación multiprotocolo por etiquetas (Multiprotocol Label Switching. MPLS) es un grupo de trabajo perteneciente a la IETF, que consiste en desarrollar una tecnología para acelerar el tráfico de red y hacerlo más sencillo de gestionar, su principal objetivo es crear redes flexibles y escalables con un incremento en el desempeño, decisiones de enrutamiento y conmutación de flujo de tráfico a través de la red, combinando los atributos de las tecnologías de conmutación de nivel 2 y de enrutamiento de nivel 3. Esto incluye, ingeniería de tráfico y soporte de redes privadas virtuales, el cual ofrece calidad de servicio (QoS).

MPLS se denomina multiprotocolo puesto que se puede integrar a cualquier infraestructura existente, tal como, IP, Frame Relay, ATM, etc., el mecanismo de envío de paquetes de información a través de una red es por intercambio de etiquetas, en cuyas unidades de datos (por ejemplo un paquete o una celda) se transporta una etiqueta corta, de longitud fija, que indica a los nodos de conmutación, que hay a lo largo de la ruta, como procesar y enviar los datos.

El estudio de este protocolo es muy largo, por eso en los siguientes puntos, solo se describirán sus aspectos más importantes.

3.6.1 Componentes básicos de MPLS

A continuación se describirán los componentes básicos que componen una red MPLS.

FEC (Forward Equivalent Class, Clase Equivalente de Envío). Es una representación de un grupo de paquetes IP que son enviados de la misma manera, como por ejemplo en el mismo camino, con el mismo tratamiento de envío.

Etiquetas. Es un identificador con un significado local, de longitud fija y corta que sirve para identificar una clase FEC. La etiqueta se pone en un paquete determinado y representa la clase equivalente de envío asignada al paquete, generalmente un paquete es asignado a una clase FEC en base (completamente o parcialmente) a su dirección destino de nivel red, sin embargo, la etiqueta nunca es una codificación de esta. Una etiqueta en su forma simple, identifica el camino que debe de seguir un paquete.

LSR (Label Switch Router). Es un ruteador (router) que soporta la tecnología MPLS, implementa distribución de etiquetas así como procedimientos para enviar paquetes basándose en etiquetas. Su función principal de los procesos de distribución de etiquetas, permitir que un LSR distribuya sus enlaces de etiquetas a otros LSR de la misma red MPLS, se encuentran ubicados en el interior de la red MPLS, el cual debe soportar los protocolos de enrutamiento IP y participa en el establecimiento de los LSP (Label Switched Paths) utilizando el protocolo de señalización adecuado.

LSR de entrada. Es el ruteador que inicia el camino LSP, un camino LSP es una secuencia de ruteadores <R1,….., Rn> donde R1 es el ruteador de entrada del camino LSP.

LSR de salida. Es el último rutedor por donde salen los paquetes de la red MPLS.

LSP (Label Switched Path). Es el camino a través de uno o más LSR a un nivel de jerarquía, seguido por un paquete de una determinada clase.

Paquete etiquetado. Es un paquete en el que se ha codificado una etiqueta, las etiquetas pueden residir en una cabecera encapsulada que existe específicamente para este fin o pueden residir en la cabecera existente de nivel de red o nivel de enlace.

En la figura 3.25 se muestra una red MPLS con sus componentes.

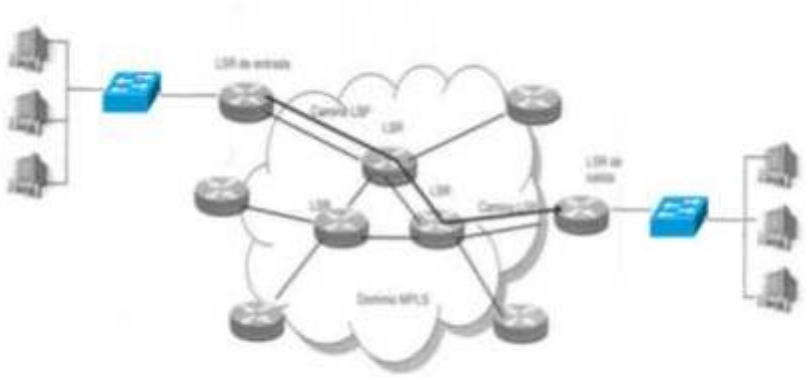


Figura 3.25 Componentes de una red MPLS

3.6.2 MPLS y el enrutamiento tradicional

El envío tradicional de paquetes por la capa de red, como podría ser, el envío de paquetes IP por Internet, se apoya en la información proporcionada por los protocolos de enrutamiento del nivel de red, por ejemplo, primero la ruta más corta o protocolo de gateway fronterizo (BGP), también se apoya en el enrutamiento estático, para tomar una decisión de envío independiente de cada salto (ruteador) dentro de la red.

MPLS modifica el enrutamiento convencional IP, en el enrutamiento tradicional, cada paquete viaja de un ruteador a otro, y cada ruteador toma una decisión independiente del envío de este paquete; es decir cada ruetador analiza la cabecera del paquete y cada ruteador utiliza un algoritmo de encaminamiento a nivel red, para determinar de forma independiente el próximo salto del paquete, a medida que el paquete se desplaza desde su origen a su destino final.

La cabecera del paquete contiene más información de la que se necesita para elegir el próximo salto. Para determinar el próximo salto se puede pensar en la composición de dos funciones. La primera función particiona todo el conjunto de posibles paquetes en un conjunto de clases FEC (Forwarding Equivalence Classes) y la segunda función mapea cada clase FEC. Así las decisiones de envío correspondientes son:

- Los paquetes que son mapeados en la misma clase FEC no se distinguen, todos los paquetes que pertenecen a una misma clase FEC y que viajan desde un nodo determinado seguirán el mismo camino.

- En el envío tradicional IP, generalmente un ruteador considerará que dos paquetes son de la misma clase FEC si hay algún prefijo de dirección X en las tablas de encaminamiento del ruteador de forma que este prefijo X es el encaje más largo para la dirección destino de cada paquete. A medida que el paquete atraviesa la red, a cada salto se vuelve a examinar el paquete y se le asigna una clase FEC.

En MPLS, la asignación de un determinado paquete a una determinada clase FEC, se hace solo una vez, que es cuando el paquete entra a la red. La clase FEC a la cual se asigna el paquete se codifica como un valor corto de longitud fija llamado etiqueta.

Cuando el paquete es enviado al salto siguiente, la etiqueta es enviada con el, así los paquetes son etiquetados antes de ser enviados.

En los saltos siguientes no se analiza la cabecera del nivel de red del paquete, si no que se utiliza como un índice en la tabla que especifica el próximo salto y una nueva etiqueta, así la etiqueta vieja es sustituida por la nueva y el paquete es enviado al salto siguiente. Así el modelo de envío MPLS una vez que un paquete es asignado a una clase FEC, no se hace ningún análisis de su

cabecera en los ruteadores siguientes, todo el envío es dirigido por las etiquetas.

3.6.3 MPLS y Redes Privadas Virtuales

Las Redes Privadas Virtuales basadas en MPLS se definen como "Una comunidad de intereses o como un grupo de usuarios cerrado, todo lo cual estará dictado por la visibilidad del enrutamiento que tendrá el sitio[4]", es decir cada "sitio" es una representación de una VPN en la que solamente pueden entrar los miembros de la misma VPN. Cada VPN tiene su propia tabla de enrutamiento y envío en el ruteador, por lo que a cada cliente o sitio que pertenezca a dicha VPN sólo se le proporcionara al conjunto de rutas que contenga esa tabla.

Para lograr el enrutamiento VPN, MPLS utiliza ruteadores a los cuales asigna una instancia de enrutamiento y reenvío virtual a cada VPN (VRF, Virtual Forwarding and Routing), únicamente los paquetes con esta VRF, puede entregarse a destinos de la VPN ya que se utilizan tablas de enrutamiento y reenvío independientes para cada VPN, la etiqueta que incluye la VRF se añade al paquete basándose en la interfaz física en la que haya llegado el ruteador de extremo del proveedor.

En la figura 3.26 se muestra en ejemplo de una VPN basada en MPLS donde se utiliza una VPN mediante proveedor de servicios de red, los ruteadores del proveedor mantienen las tablas de enrutamiento virtual para cada sucursal conectada a ellos y distribuirán estas tablas a otros ruteadores de extremo en la misma VPN.

[4] Ivan Pepelnjak, Arquitecturas MPLS y VPN, editorial PEARSON EDUCACIÖN, Madrid 2003 P.148

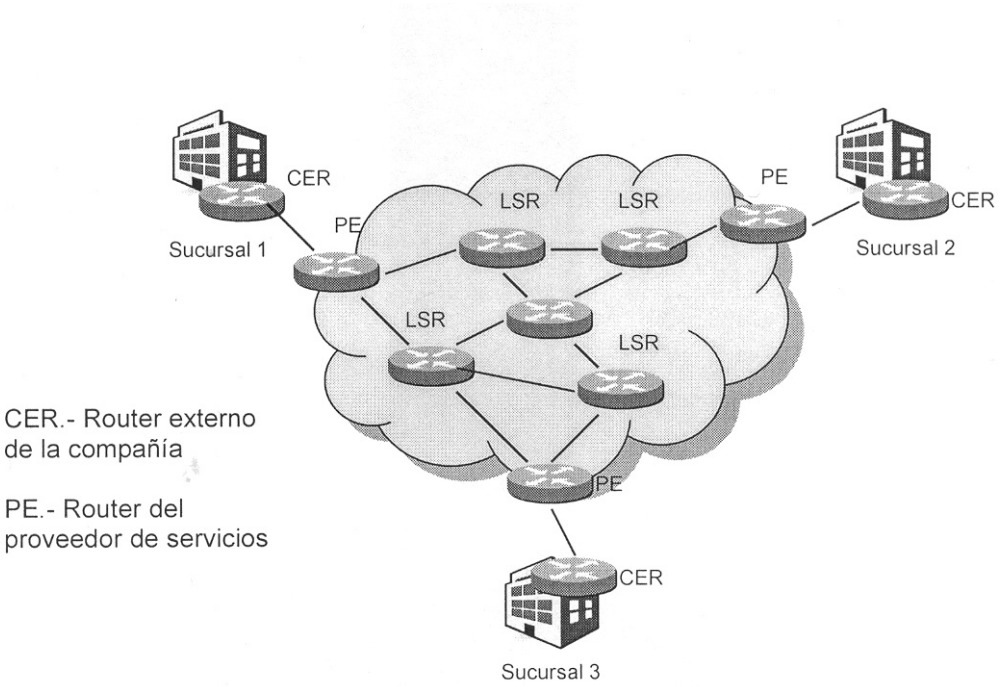


Figura 3.26 Ejemplo de VPN con MPLS

En la figura 3.27 se muestra un ejemplo de una VPN con MPLS con conectividad hacia otros clientes, la situación se vuelve un poco más compleja y se necesita más de una VRF para cada VPN cliente, la información se transporta por túneles y se utiliza el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de ruteado IP.

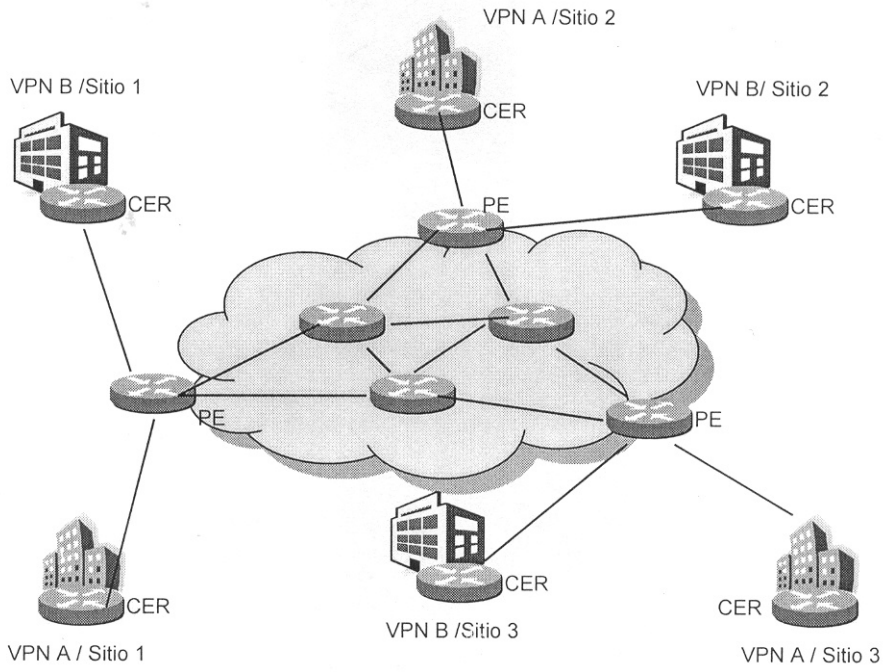


Figura 3.27 Ejemplo de VPN con MPLS con varios sitios

3.6.4 Túneles MPLS

Un túnel MPLS se crea cuando un determinado paquete se quiere entregar de un ruteador A a un ruteador B sin importar que estos ruteadores no sean consecutivos ni el ruteador B sea el último destino del paquete, esto se puede hacer encapsulando el paquete dentro de un paquete de nivel de red cuya dirección destino es la dirección del ruteador B. Así es como se crea un túnel del ruteador A al B, y cualquier paquete manejado de esa forma se dice que es un paquete tunelado.

MPLS acepta tres tipos de túneles:

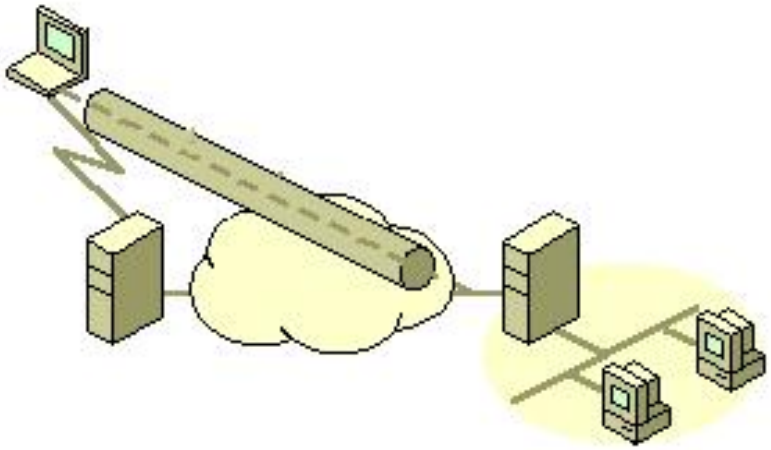
Túnel encaminado salto a salto. Es cuando un paquete tunelado sigue el camino salto a salto, del ruteador A al ruteador B, cuyo extremo de transmisión es el ruteador A y el extremo de recepción es el ruteador B.

Túnel encaminado explícito. Es cuando un paquete tunelado viaja de un ruteador A a un ruteador B por un camino diferente del camino salto a salto. Por ejemplo se puede enviar un paquete a través del túnel encaminado explícito encapsulándolo en un paquete que es encaminado en el origen.

Túnel LSP. Es un túnel implementado como un camino LSP y usa la conmutación de etiquetas más que encapsulación a nivel de red para hacer que un paquete viaje a través del túnel, el túnel es formado por un conjunto de ruteadores <R1…..Rn>, donde R1 es el extremo de transmisión del túnel y el ruteador Rn es el extremo de recepción del túnel, a todo esto se le llama túnel LSP.

El conjunto de paquetes que se envía a través del túnel LSP constituye una clase FEC y cada ruteador LSP asigna una etiqueta a esta clase FEC, el criterio para asignar un paquete a un túnel LSP es un asunto local en el extremo de la transmisión del túnel, y para poner un paquete en un túnel LSP, el extremo de transmisión pone una etiqueta para el túnel en la pila de etiquetas y envía el paquete etiquetado al salto siguiente en el túnel.

IV Ejemplo de Implementación



FES UNAM ACATLAN

4.1 Escenario de ejemplo

En este capítulo se asume que se conoce acerca de la instalación del Windows Server 2003, así mismo como sus funciones que ofrece como: servidor DHCP y servidor de Dominio. Por lo tanto no se explicara su instalación.

El escenario de ejemplo es el siguiente:

Tipo de VPN: VPN de acceso remoto, utilizando Internet como medio de acceso y software, utilizando Windows Server 2003 Enterprise

Tecnología de túnel: Protocolo de túnel punto a punto. PPTP

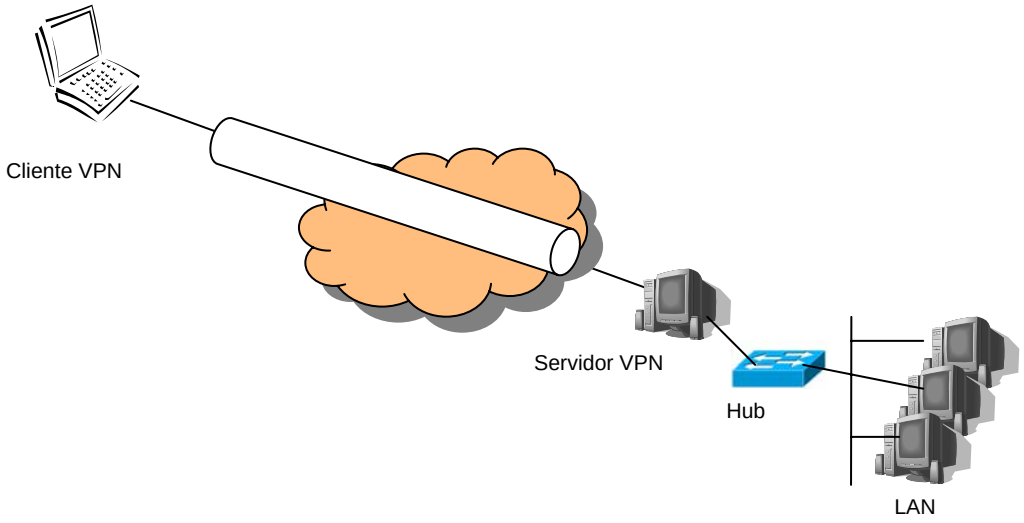


Figura 4.1 Escenario de ejemplo

Equipo utilizado: Maquina genérica Pentium 4 a 2.4 GHZ, 512MB RAM, Disco duro de 80GB, dos tarjetas de red, equipo actuando como servidor VPN, servidor de Dominio y servidor DHCP.

Máquina genérica Celaron a 2.13GHZ, 256 MB en RAM, Disco duro de 40GB con sistema operativo Windows XP, utilizada como cliente VPN

En la figura 4.1 se muestra el escenario de ejemplo de la VPN a implementar, como se puede observar la maquina que esta actuando como servidor, cuenta con dos NIC (Network Interface Connects), es decir tarjetas de red, una configurada para Internet y la otra configurada a la Intranet, esto es esencial para una implementación del servidor VPN en Windows Server 2003.

4.1.1 Configuración del servidor de acceso remoto para una conexión VPN

Dentro de las funciones integradas de Windows Server 2003, trae incorporado un soporte para VPN tanto para servidor como para clientes, que viene incorporado dentro de la consola de “Enrutamiento y Acceso Remoto (RRAS)”, para activarlo y configurarlo, nos dirigimos a “Inicio/ Herramientas Administrativas/ Enrutamiento y Acceso remoto” (Figura 4.2)

Figura 4.2

Ya que se ingresó a la consola de “enrutamiento y acceso remoto”, en su “console tree” (pantalla ubicada del lado izquierdo) muestra los servidores, en este caso muestra el servidor “Server03” que es el nombre de nuestro servidor, con una flechita roja, la cual indica que el servidor no esta configurado. Dándole clic derecho seleccionamos “Configurar y habilitar Enrutamiento y acceso remoto”

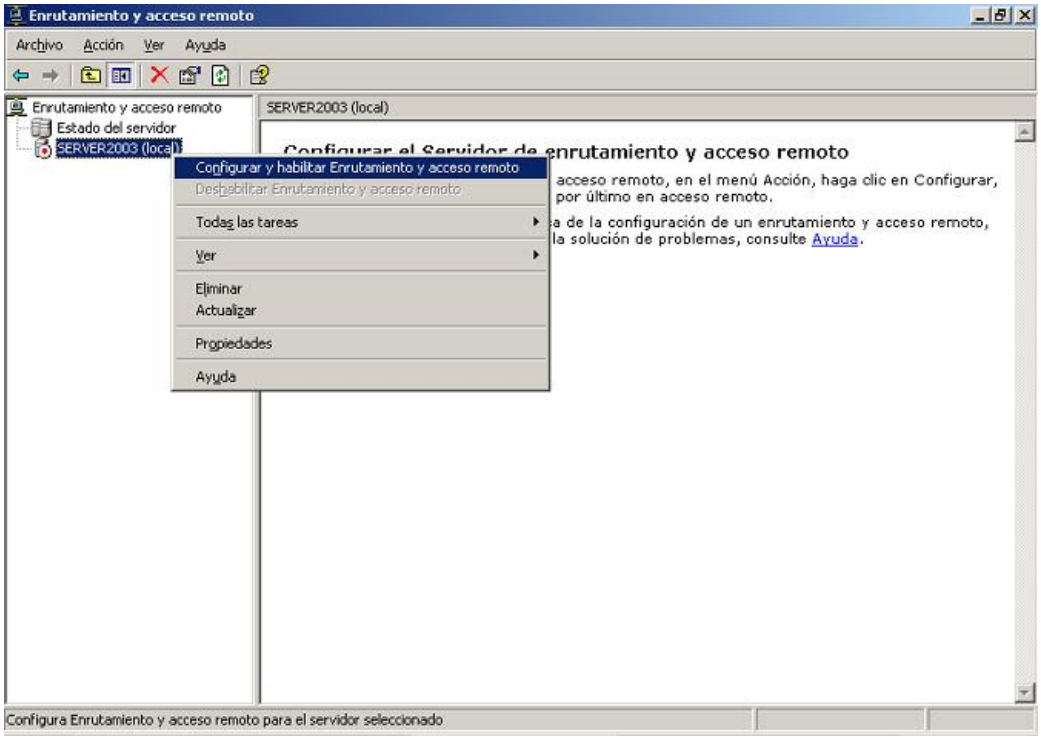


Figura 4.3 Consola de Enrutamiento y acceso remoto

A continuación se abrirá el asistente para la configuración del “Enrutamiento y acceso remoto” y damos clic en siguiente. La pantalla que se muestra a continuación, muestra todas las posibles configuraciones que se pueden realizar, para nuestro ejemplo seleccionamos la primera “Acceso remoto (dial-up o VPN)” y clic en “siguiente”. (Figura 4.4)

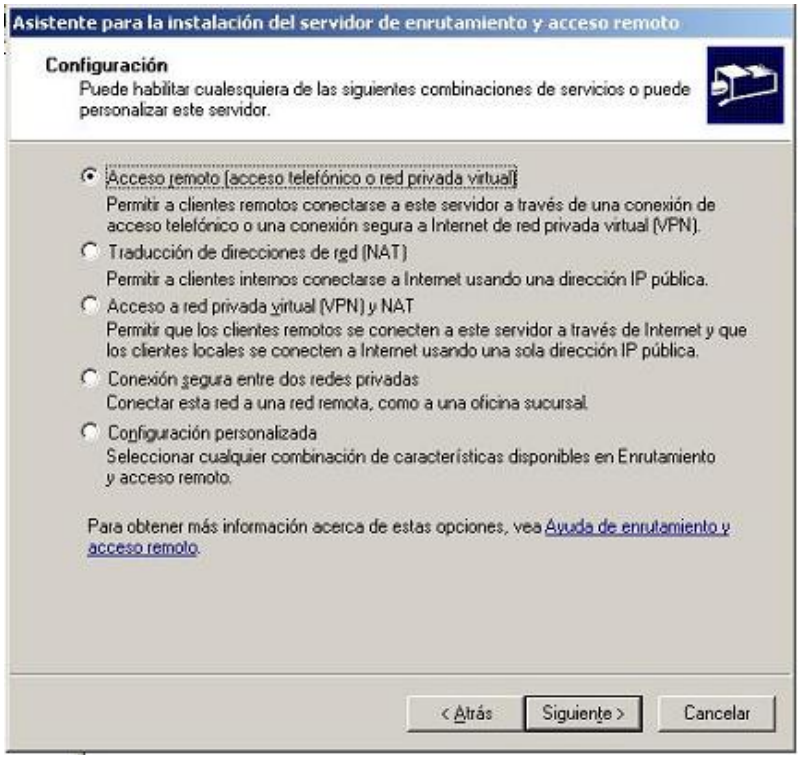


Figura 4.4

En la siguiente pantalla se muestra dos opciones para recibir conexiones de acceso remoto, para nuestro ejemplo verificamos que la opción sea VPN y clic en “siguiente”. (Figura 4.5)

Figura 4.5

En la siguiente pantalla “Conexión VPN”, (Figura 4.6) debemos elegir como se va a conectar nuestro servidor, como lo mencionamos anteriormente la pantalla

muestra las interfaces conectadas en nuestra máquina, seleccionamos la interfaz que conecta a Internet, en este ejemplo es la que se llama “Modem” con la direccion IP 201.128.14.212 que provee el PSI, la cual nos servirá para recibir conexiones de los clientes VPN desde Internet. Cualquier otra conexión que no se elija será configurada como una conexión a la LAN, en este ejemplo “red local”.

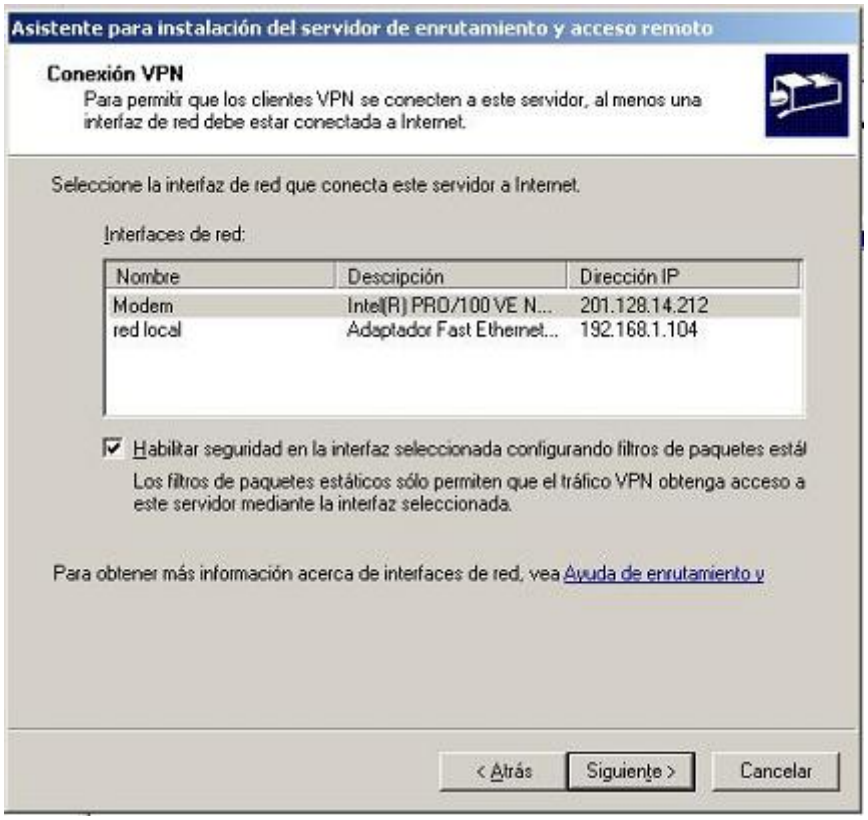


Figura 4.6

La siguiente pantalla “Asignación de direcciones IP” (Figura 4.7), es la manera en el que el servidor VPN va asignar direcciones IP a los clientes de acceso remoto, como se puede observar en la figura, existen dos maneras, mediante direcciones que el servidor VPN obtiene de un servidor DHCP o mediante direcciones de un intervalo de direcciones especificado que se configure en el servidor VPN. Para nuestro ejemplo seleccionamos la primera opción “Automáticamente” y clic en siguiente.

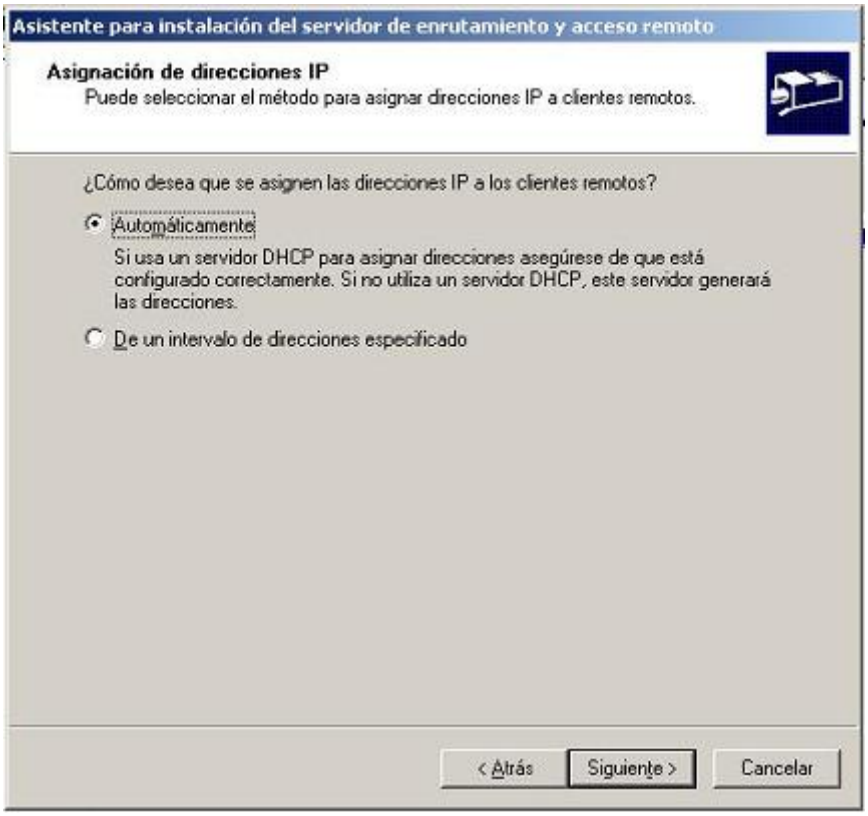


Figura 4.7

En la pantalla de “Administrar servidores de acceso múltiples” la opción “No usar enrutamiento y acceso remoto para autenticar las solicitudes de conexión” es seleccionada automáticamente. Esta selección configura el servidor VPN para autenticar peticiones de conexiones locales usando la autenticación de Windows, cuentas de Windows y reglas de acceso remoto almacenadas localmente.

La otra opción se utilizaría, si se quiere usar un servidor de autenticación RADIUS, esta opción es recomendable cuando se dispone de más de un servidor de acceso remoto, en vez de administrar de forma independiente las directivas de acceso remoto de todos los servidores de acceso remoto, puede configurar un único servidor con el Servicio de autenticación de Internet (IAS, Internet Authentication Service) como servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS, Remote Authentication Dial-In User Service) y configurar los servidores de acceso remoto como clientes RADIUS. El servidor IAS proporciona autenticación, autorización,

administración de cuentas y auditorias de acceso remoto centralizado. Para nuestro ejemplo seleccionamos la primera opción y clic en siguiente. (Figura 4.8)

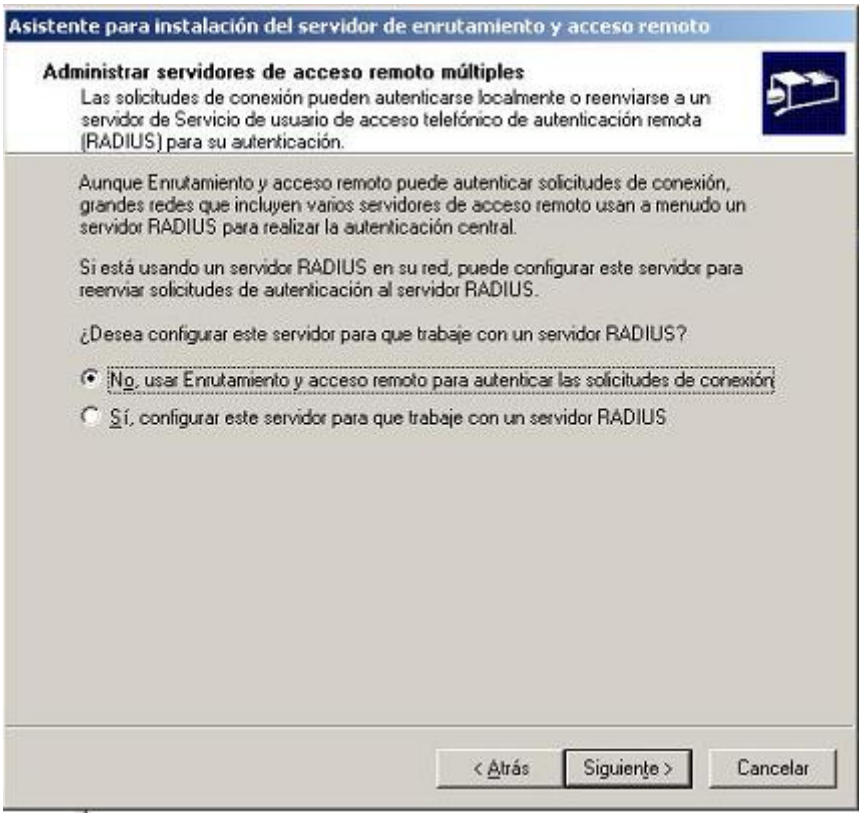


Figura 4.8

La última pantalla del asistente (Figura 4.9), nos indica que la instalación del “Enrutamiento y acceso remoto” ha finalizado, aparece un resumen de la información de la cual hay que verificar que: Los clientes VPN estén conectados en la interfaz pública correcta, los clientes VPN tienen asignados direcciones IP correctas para la interfaz de red y las conexiones de cliente son aceptadas y autenticadas para usar reglas de acceso remoto para el servidor VPN. Si la información es correcta damos clic en finalizar.

Figura 4.9 Finalización de la configuración del servidor VPN

4.1.2 Configuración del número de puertos disponibles en el servidor

Por default el asistente de instalación del servidor de enrutamiento y acceso remoto configura 128 puertos PPTP y 128 puertos L2TP, permitiendo 128 conexiones simultáneas de PPTP y 128 conexiones simultáneas de L2TP. Dependiendo de las necesidades que se tengan, si se requiere reducir o aumentar el número de conexiones, en Windows Server 2003 Standard Edition se puede crear hasta 1.000 puertos del Protocolo de túnel punto a punto PPTP y hasta 1.000 puertos del Protocolo de túnel de capa 2 L2TP. Windows Server 2003 Standard Edition, puede aceptar hasta 1.000 conexiones VPN simultáneas. Si se conectan 1.000 clientes VPN, se denegarán los intentos de conexión posteriores hasta que el número de conexiones sea inferior a 1.000.

Para configurar los puertos se realiza desde la consola de enrutamiento y acceso remoto, en la “Console tree” damos clic con botón derecho sobre “Puertos” y seleccionamos “Propiedades” (Figura 4.10)

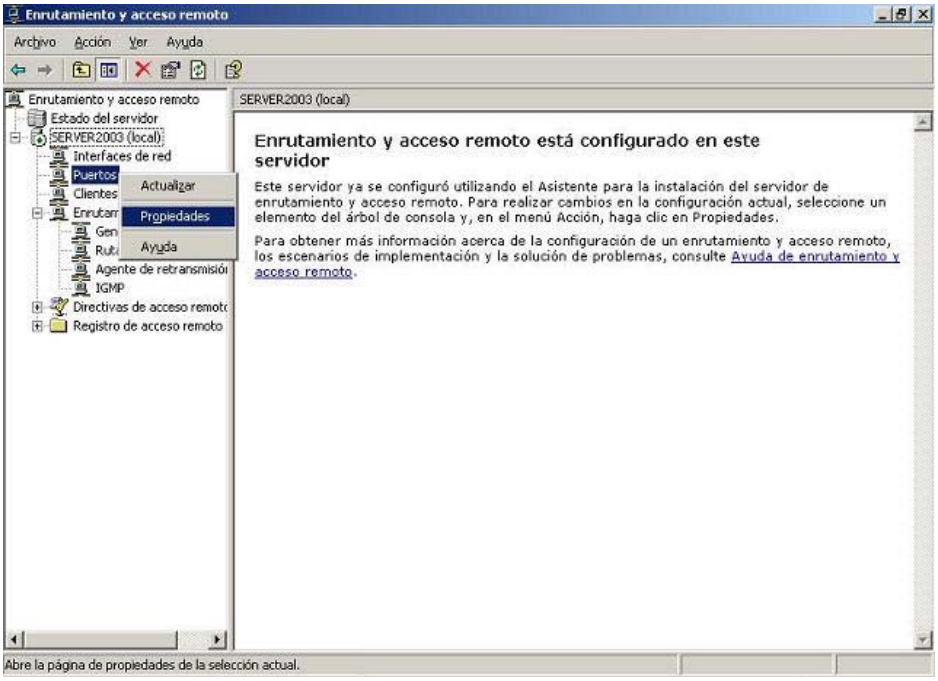


Figura 4.10

La ventana que se muestra (Figura 4.11), “Propiedades de los puertos” muestra información sobre los tipos de puertos habilitados así como la cantidad de cada uno de ellos. Se selecciona el puerto apropiado, en este caso seleccionamos PPTP y clic en “configurar”.

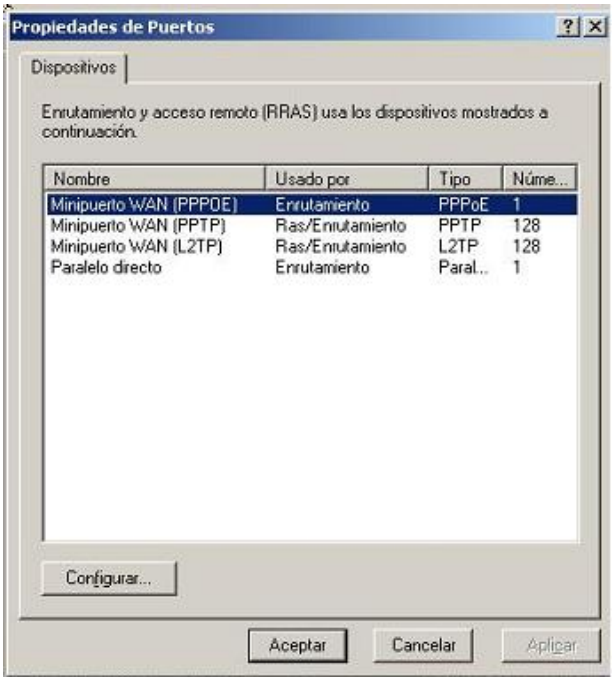


Figura 4.11 Propiedades de los puertos

La pantalla que se muestra (Figura 4.12), podemos configurar el máximo de puertos para nuestro protocolo, para el ejemplo seleccionamos cinco, los “check box” que se muestran: “Conexiones de acceso remoto (solamente)” sirven para configurar nuestro servidor para aceptar solo conexiones de entrada desde nuestra tarjeta de red configurada para la Internet y la otra opción acepta conexiones de entrada y salida y sirve para configurar conexiones de acceso remoto por marcado (dial-up), las dejamos como están y clic en “OK”. Los cambios en la configuración de los puertos se realizan.

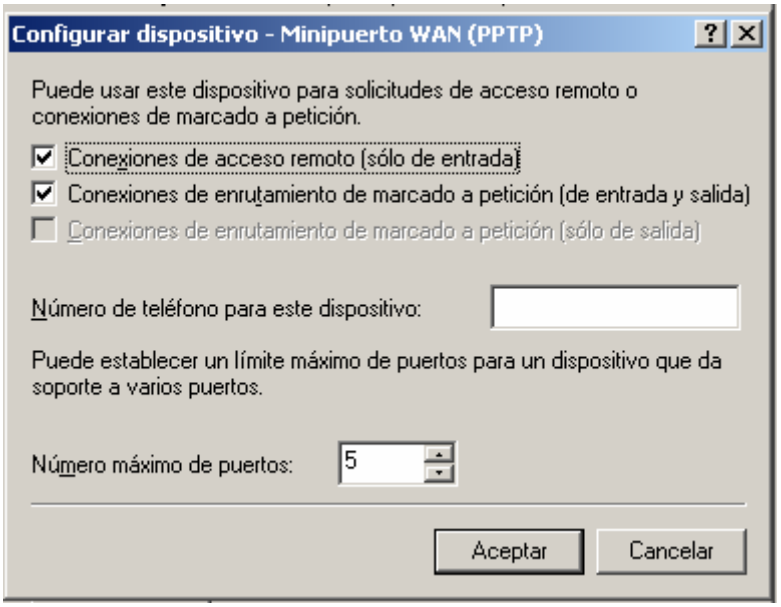


Figura 4.12

Repetimos los mismos pasos para configurar los puertos L2TP, como en nuestro ejemplo no los vamos a utilizar, lo configuramos a cero y aceptamos los cambios. La pantalla final con los nuevos cambios se muestra en la Figura 4.13

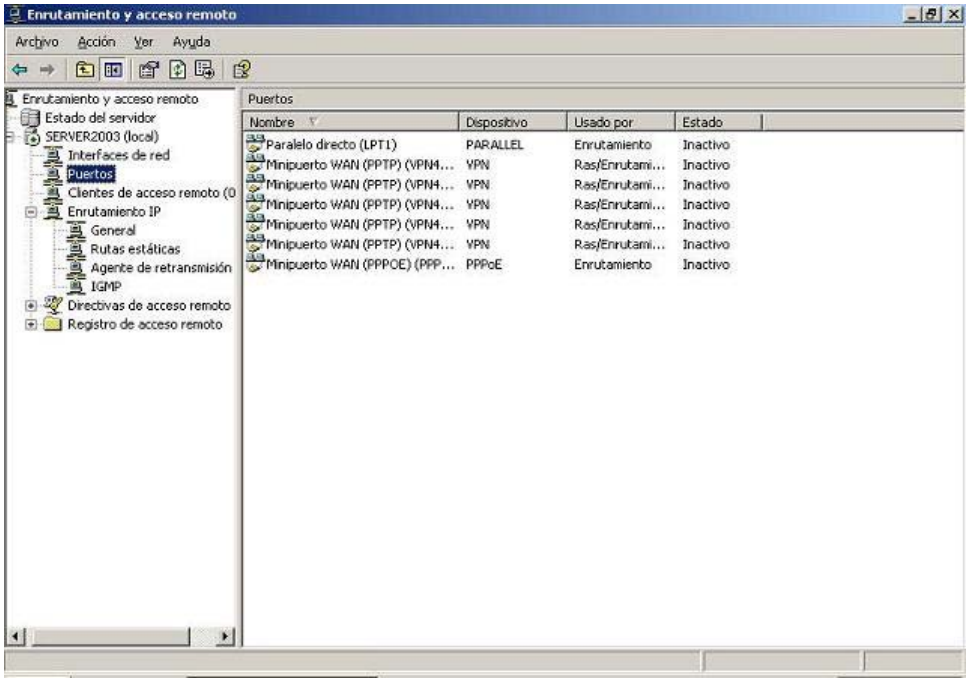


Figura 4.13

4.1.3 Configuración de directivas de acceso remoto

Las directivas de acceso remoto en Windows Server 2003 son reglas de seguridad, que definen cómo se autorizan o se rechazan las conexiones. Estas políticas de acceso se configuran para grupos de usuarios o usuarios individuales, para configurar estas reglas de seguridad, se realiza desde la consola de “Enrutamiento y acceso remoto”, cuando configuramos el servidor VPN por “default” Windows Server 2003 crea automáticamente dos reglas, para el ejemplo se eliminaran y se creara una nueva (Figura 4.14)

Desde la “console tree” nos situamos sobre “Políticas de acceso remoto” y del lado derecho de la pantalla con botón derecho sobre cada una de las reglas que crea Windows, se procede a borrarlas y creamos las nuevas con botón derecho sobre “Políticas de acceso remoto” y seleccionamos “Nueva política de acceso remoto”

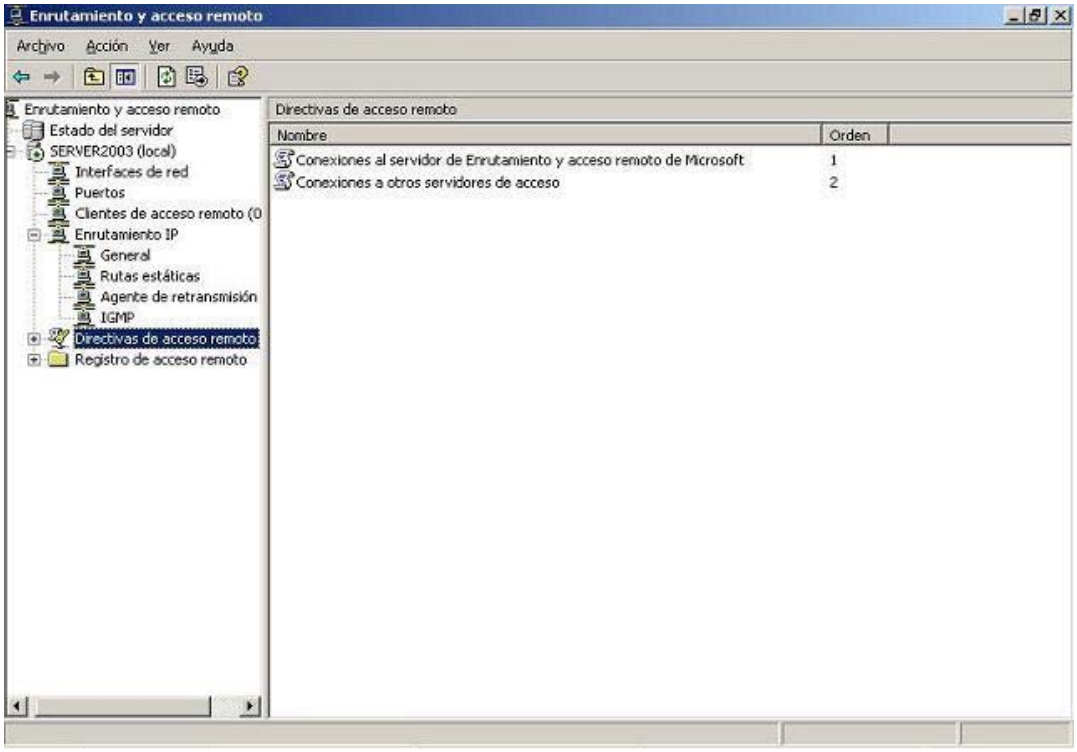


Figura 4.14 Directivas de seguridad

La pantalla que se muestra permite crear la nueva regla por medio de un asistente, también permite escribir el nombre que identificará la nueva regla, para este ejemplo se puso, “Directivas de acceso a la VPN “. Se da clic en siguiente. (Figura 4.15)

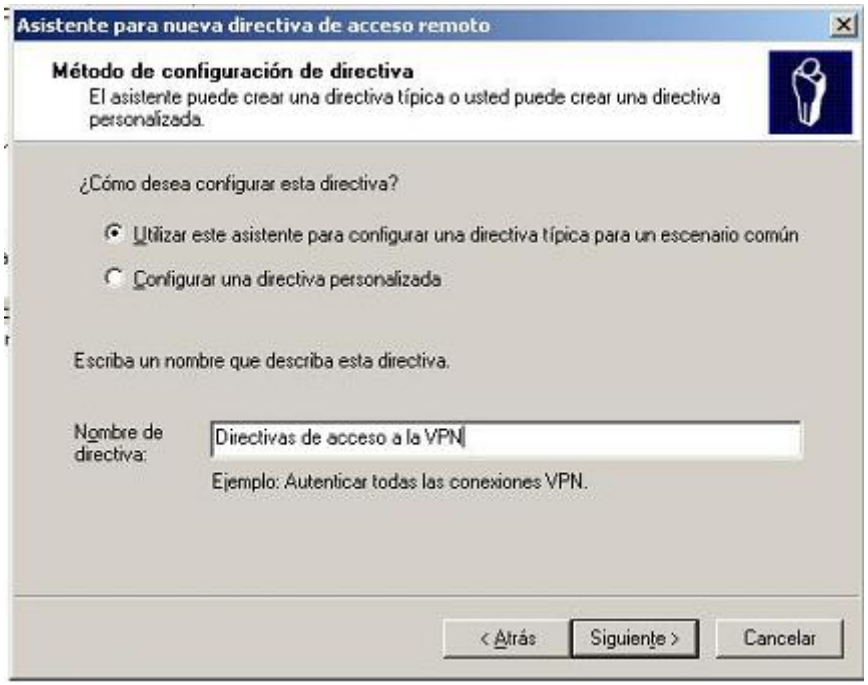


Figura 4.15

La pantalla siguiente (Figura 4.16), muestra los posibles métodos de acceso a los cuales se les puede crear directivas, para nuestro ejemplo seleccionamos la primera “VPN” y clic en siguiente.

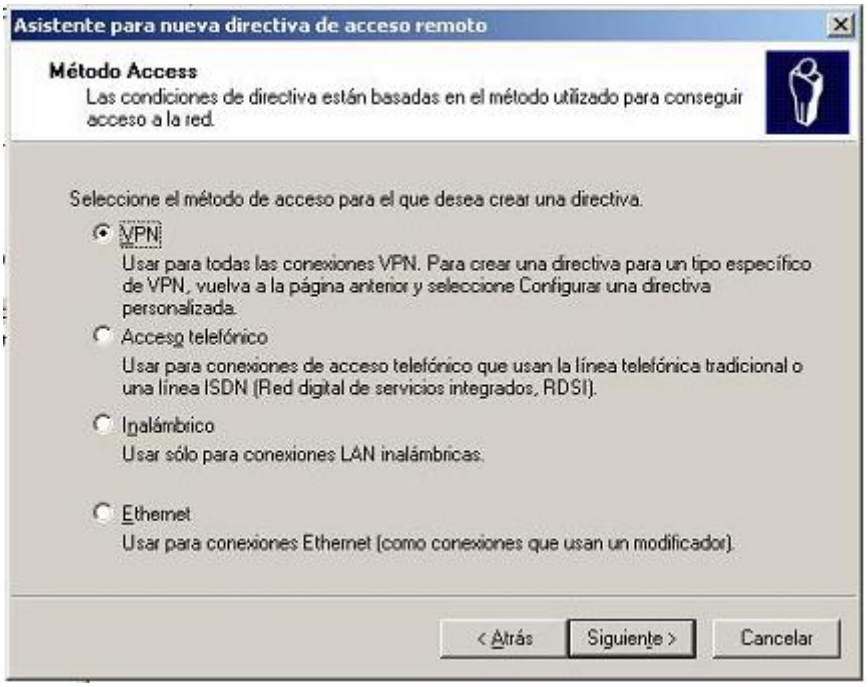


Figura 4.16

En la pantalla de “Usuario o Grupos de acceso” (Figura 4.17), es la pantalla que configurará al usuario o grupos de usuarios que tendrán derecho de conectarse al servidor, para este ejemplo se creó una grupo llamado “Usuarios VPN “se da clic en “Agregar” y se escribe la ruta correcta del grupo, y se da clic en siguiente

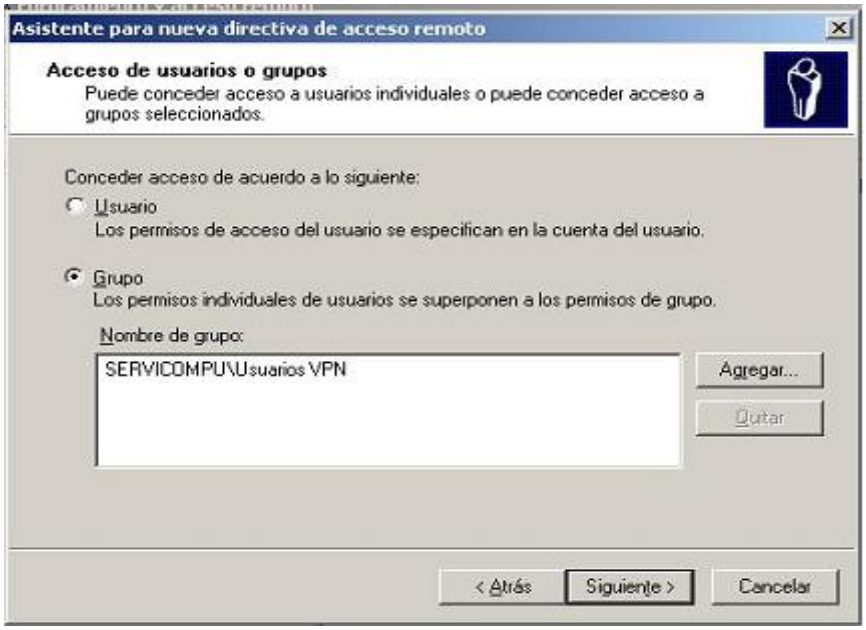


Figura 4.17

La siguiente pantalla “Métodos de autenticación” (Figura 4.18), nos muestra tres posibles opciones con la que se autenticaran a los clientes VPN.

“Protected EAP (PEAP)”:- si queremos utilizar certificado digitales para la autenticación.

“Microsoft Encrypted Authentication version 2 (MS-CHAPv2).- Es la opción que viene por default , es un protocolo de autenticación de usuarios basado en contraseñas creado por Microsoft.

“Microsoft Encrypted Authentication (MS-CHAP)”. - Esta opción se selecciona si existen clientes que no soportan MS-CHAPv2

Para nuestro ejemplo seleccionamos la que viene por default y damos cilc en siguiente.

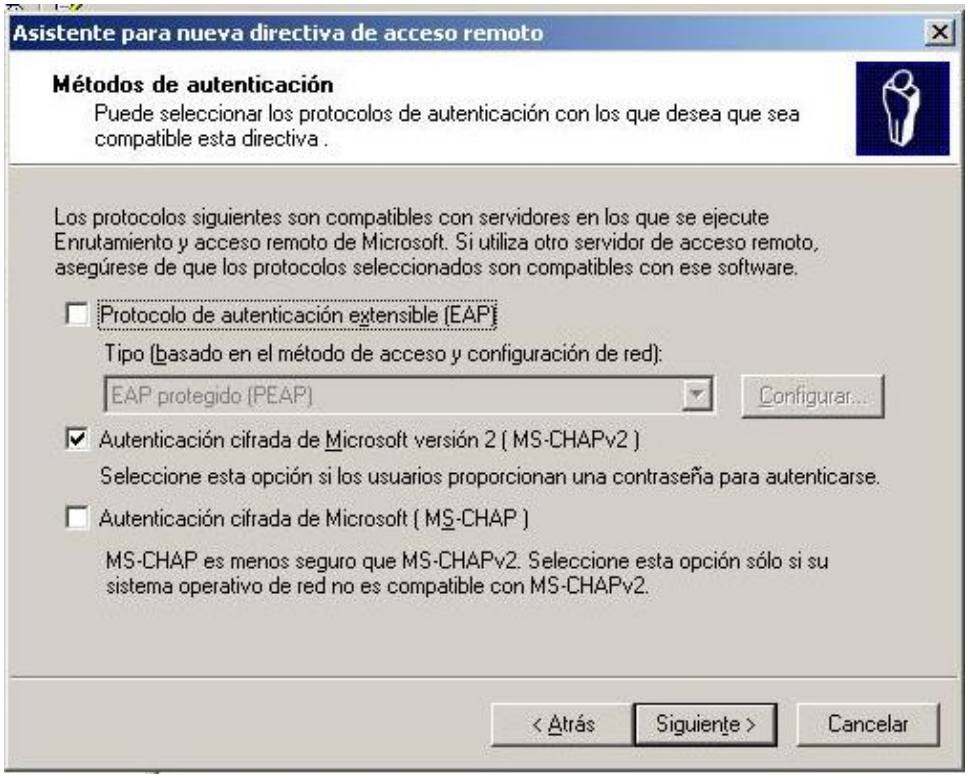


Figura 4.18

La última pantalla (Figura 4.19), nos muestra el nivel de encriptamiento que se utilizará para proteger nuestra información:

Encriptación básica (IPSec 56-bit DES or MPPE 40-bits)

Encriptación fuerte (IPSec 56-bit DES or MPPE 56-bits

Encriptación mas fuerte (IPSec Triple DES or MPPE 128-bit)

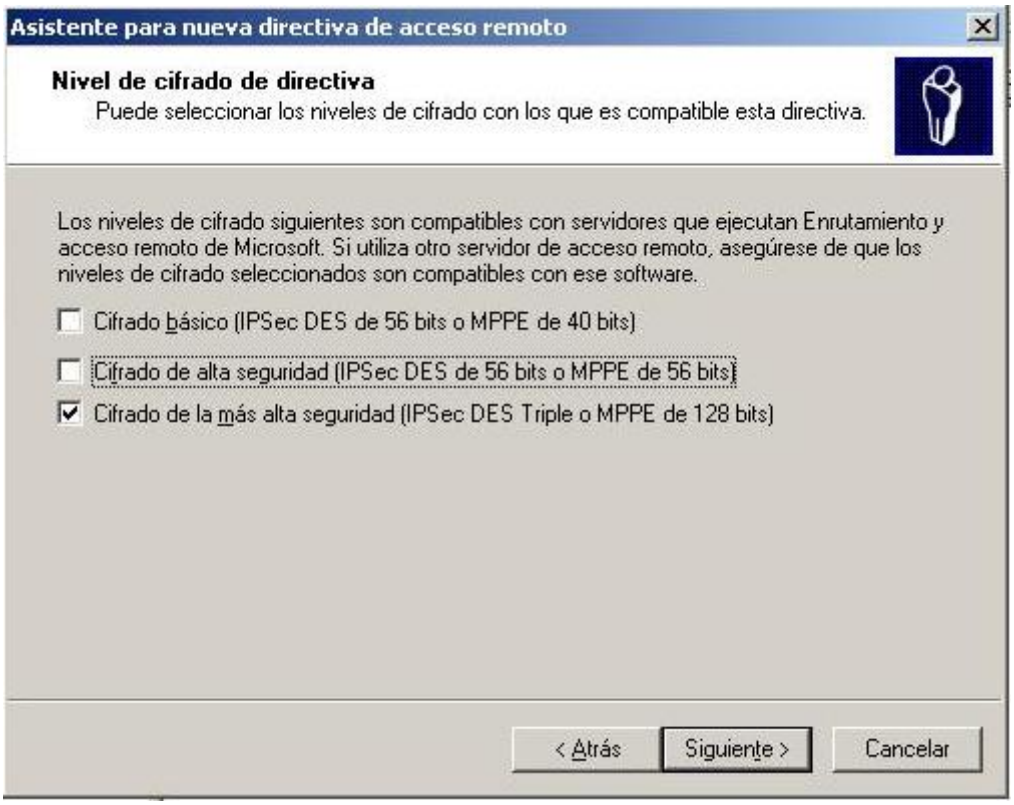


Figura 4.19

Para nuestro ejemplo seleccionamos la mas fuerte y damos clic en siguiente, en la ultima pantalla del asistente damos clic en finalizar y así se ha creado la nueva directiva.

4.1.4 Configurar cuenta de usuarios para acceso a la red

Para poder permitir que nuestros usuarios se conecten al servidor VPN, hay que darles los permisos correspondientes. Para poder configurar permisos de acceso remoto para un usuario, siendo que para el ejemplo de implementación el servidor de acceso remoto forma parte de un dominio de Windows Server 2003, se realiza desde la consola de “Usuarios y equipos de Active Directory”, en la “Console tree” damos clic en “usuarios” y en el panel de la derecha seleccionamos el usuario al que se quiere otorgar los permisos, con clic derecho seleccionamos “Propiedades” (Figura 4.20)

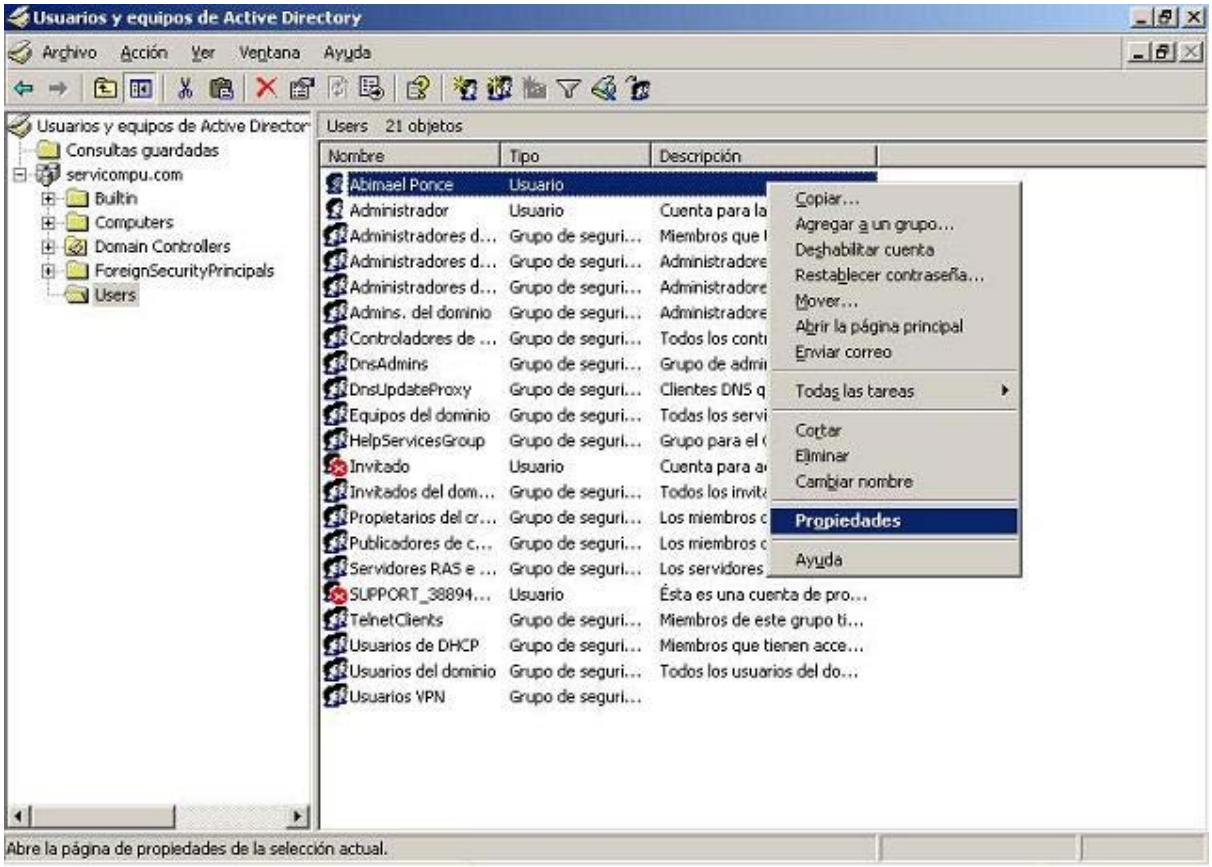


Figura 4.20

La pantalla que se abre muestra las propiedades de la cuenta “Abimael Ponce” se da clic en la “pestaña Marcado” y en la opción de “Permiso de acceso remoto (acceso telefónico o red privada virtual)” se selecciona “Permitir acceso” (Figura 4.21)

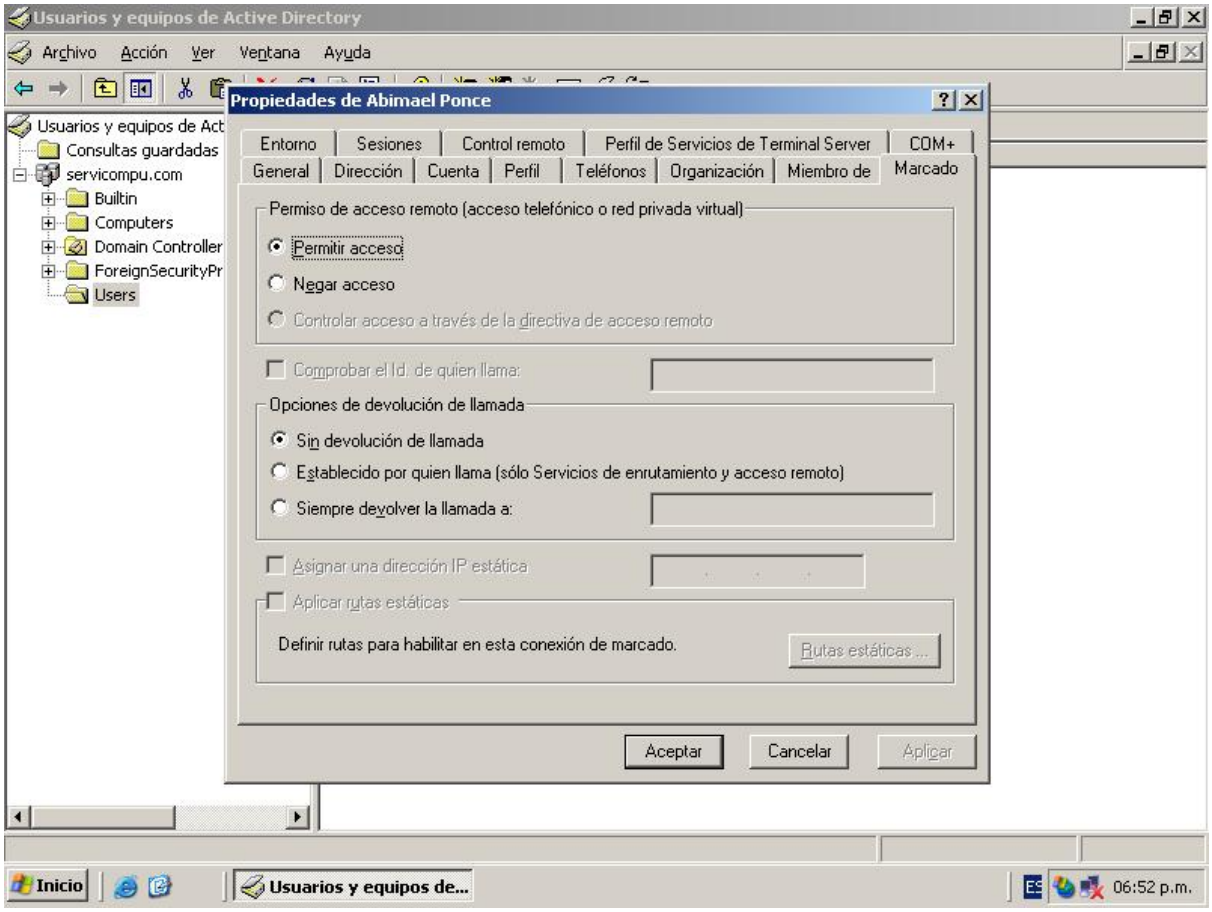


Figura 4.21

La opción “Negar acceso” permite denegar el acceso al usuario, incluso si tiene configurado los permisos a través de las directivas del servidor VPN. Las otras opciones que se observan en la pantalla “Opciones de devolución de llamada” se utilizan cuando se tiene configurado las opciones de “Marcado (dial-up)”, permitiendo devolver llamadas a un cliente que se este conectando por “marcación (dial-up)”. La opción “Asignar una dirección IP estática” permite otorgar la misma dirección IP a un cliente VPN.

Se da clic en “Aceptar” y Finalmente se ha autorizado al usuario para poder establecer conexión al servidor VPN.

4.1.5 Configuración de archivos de registros

Utilizar el evento de registros (logs) es útil para llevar un seguimiento de la actividad que existe en el servidor, se puede utilizar para grabar errores del servidor, warnings y otra información detallada en el registro del evento en el sistema. Para habilitar este evento, y configurar el nivel de sucesos de registros, se realiza desde la pestaña “Inicio de sesión” (Figura 4.22), que aparece en las propiedades del servidor de acceso remoto.

En la pestaña “Inicio de sesión”, se podrá seleccionar una de las tres siguientes opciones:
Solo registrar errores
Registrar errores y advertencias
Registrar todos lo sucesos
No registrar ningún suceso

El nombre indica por si mismo la función que realiza, para nuestro ejemplo seleccionamos “Registrar todos lo sucesos” Si es aplicable, se selecciona “Registrar información adicional de enrutamiento y acceso remoto”, esta opción registra los eventos durante el proceso de establecer una conexión PPP.

Figura 4.22

Para configurar los sucesos que se quiere “registrar” seleccionamos “Registro de acceso remoto” de la “console tree” con clic derecho seleccionamos “archivos locales” y la pantalla que abre “propiedades de archivo local” muestra dos pestañas, en “Configuración” seleccionamos las tres opciones, para tener un buen seguimiento del servidor, la otra pestaña “Archivo de registro” (Figura 4.23), permite especificar la ruta y el formato del archivo donde va ser guardada la información, Windows Server 2003 tiene dos opciones configuradas: Archivo Local Y Servidor SQL.

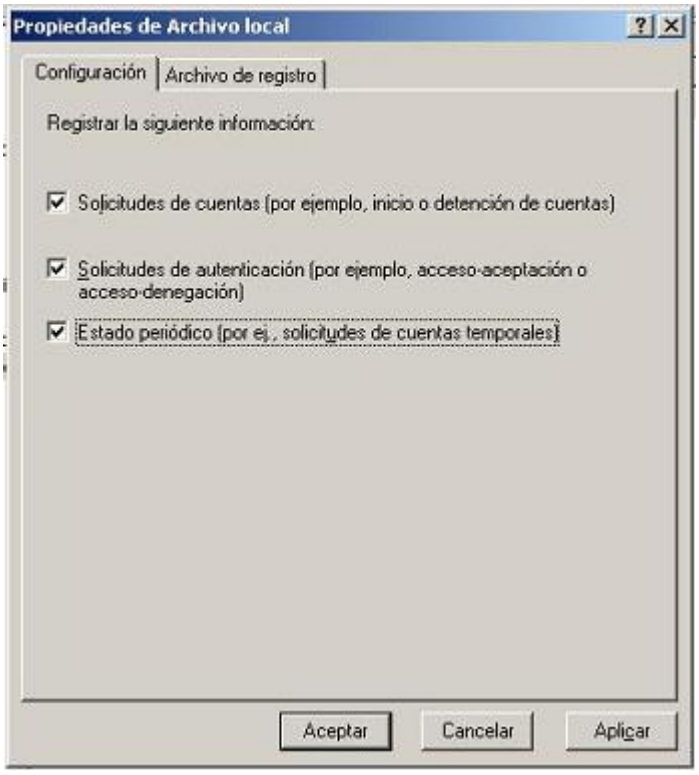


Figura 4.23

“Archivo local” viene con una configuración preestablecida para registrar los sucesos en un archivo normal dentro del disco duro: D:\WINDOWS\system32\LogFiles. Sí se cuenta con un servidor SQL, se puede configurar para enviar la información “registrada” a una Base de datos. Finalmente se da clic en “Aceptar” y se tiene configurado los archivos de registro.

4.1.6 Configuración del cliente de acceso remoto para una conexión VPN

Windows XP y Windows 2000 traen incorporado un asistente compatible con Windows Server 2003 para crear conexiones a una VPN, para Windows anteriores como Windows NT o Windows 98, se puede bajar el software de su página oficial. Para este ejemplo se utilizará Windows XP para crear la conexión a la VPN.

Para crear la conexión en el equipo remoto, que cuenta con Windows XP, se realiza desde el Panel de control / Conexiones de red, dentro de la consola de conexiones de red, se da clic en crear “conexión nueva” (Figura 4.24) y en seguida aparecerá el asistente para la conexión y damos clic en “Siguiente”.

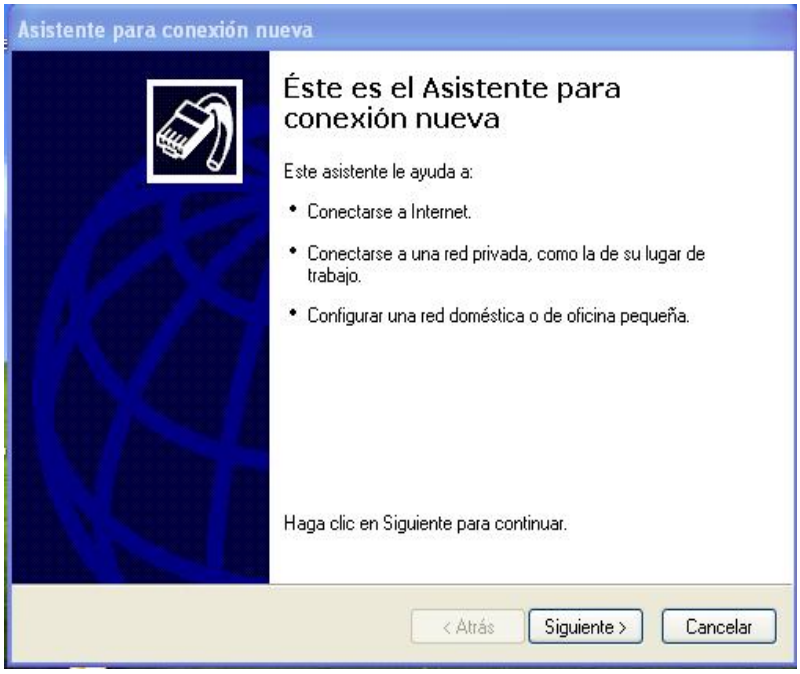


Figura 4.24

En la pantalla que aparece “Tipo de conexión” se elige la segunda opción “Conectarse a la red de mi lugar de trabajo” (Figura 4.25)

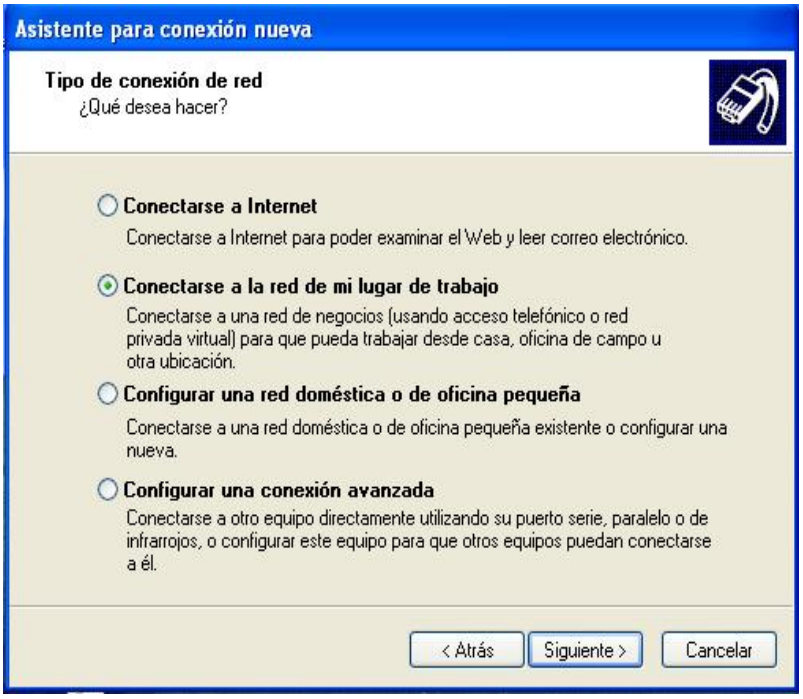


Figura 4.25

En la siguiente pantalla (Figura 4.26) se elige “Conexión de red privada virtual” ya que es la forma en la que se quiere conectar.

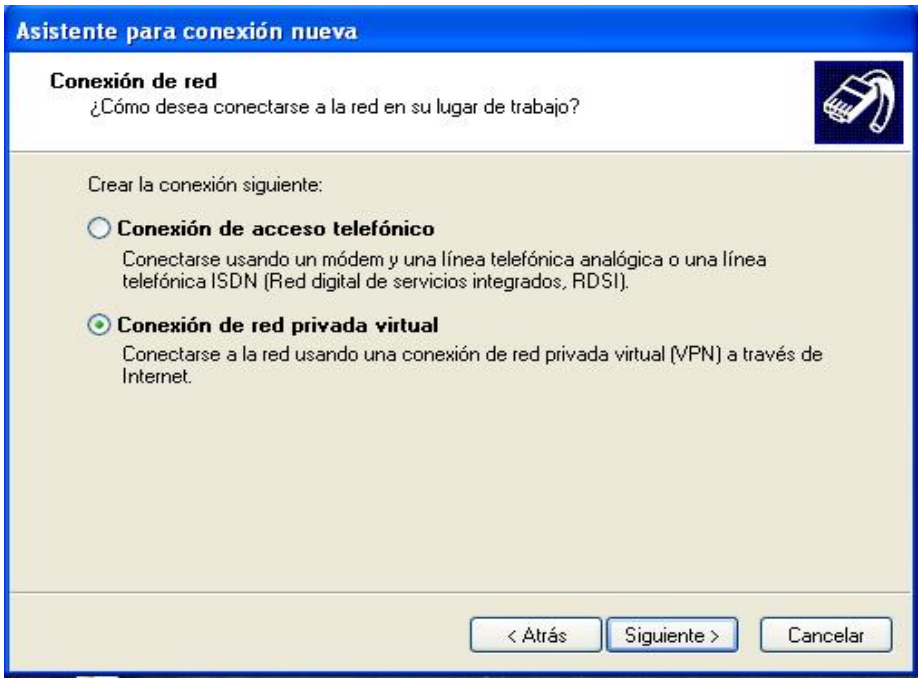


Figura 4.26

La pantalla siguiente (Figura 4.27), es para especificar un nombre a la conexión que se esta creando. Para nuestro ejemplo es “Server03”

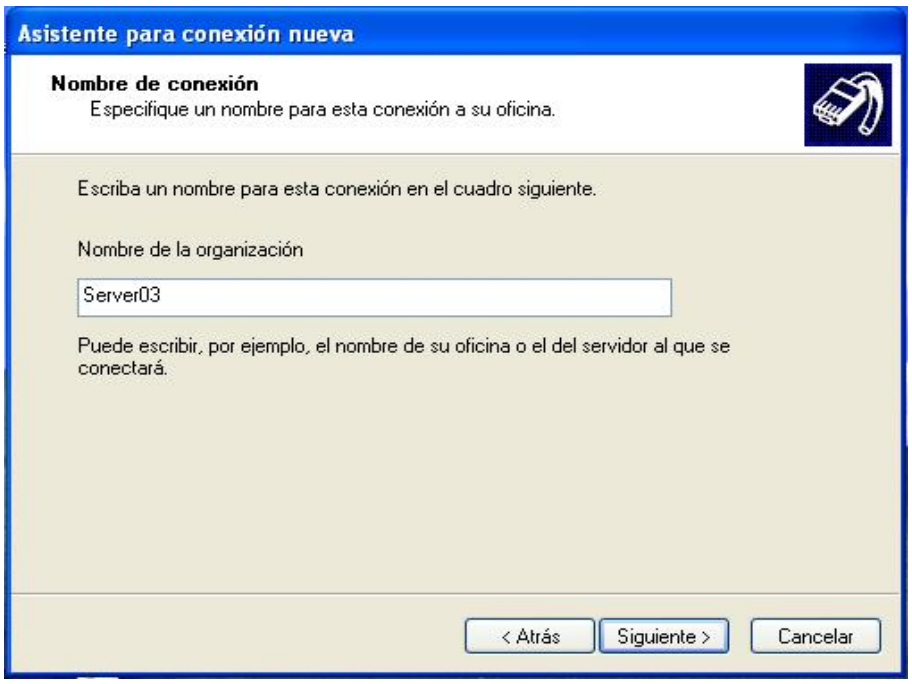


Figura 4.27

La siguiente pantalla “Selección de servidor VPN” (Figura 4.28), es clave para el buen funcionamiento de la conexión al servidor VPN, en esta pantalla se debe escribir el nombre DNS o la dirección IP de la salida de Internet que se configuró anteriormente. Se da clic en “Siguiente”

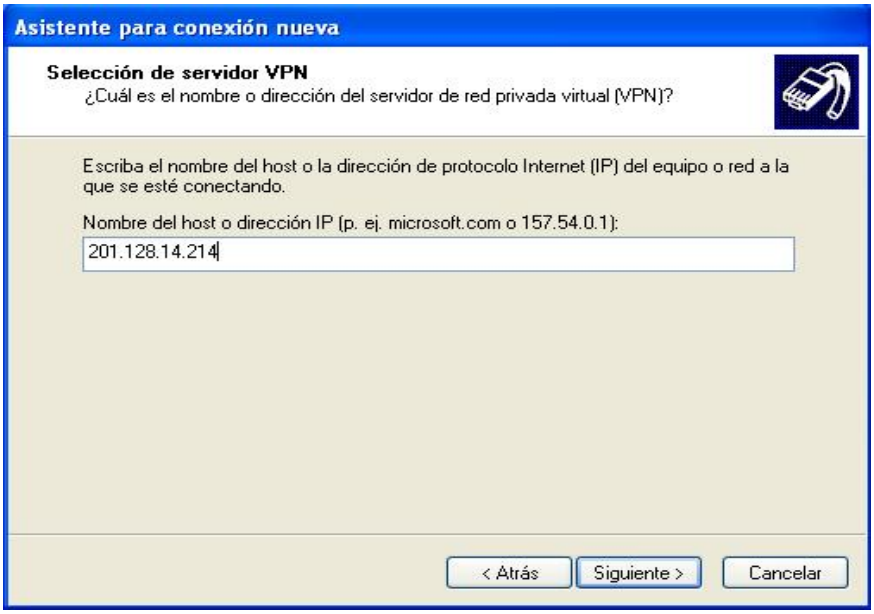


Figura 4.28

Y finalmente se ha creado la nueva conexión. (Figura 4.29)

Figura 4.29

Después de finalizar, aparecerá una nueva conexión llamada “Server03”, se da doble clic y aparece el cliente VPN que permitirá establecer la conexión. En donde se debe escribir el nombre de usuario y contraseña para poder acceder (Figura 4.30)

Figura 4.30

Si el usuario y contraseña son correctos, la conexión se establecerá y aparecerán pantallas como las siguientes (Figura 4.31 y Figura 4.32)

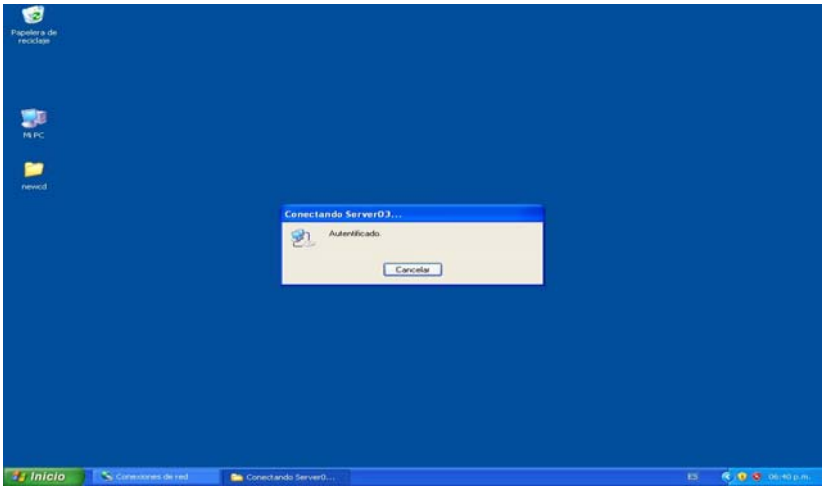


Figura 4.31

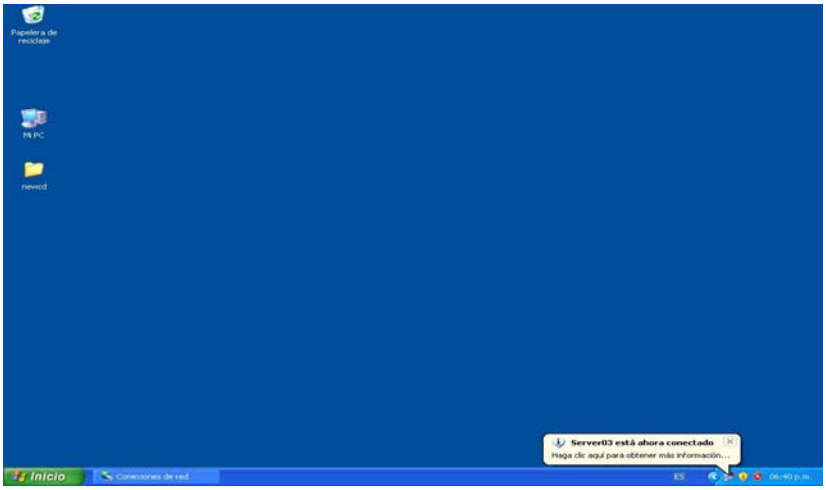


Figura 4.32

Desde la consola de “Enrutamiento y Acceso remoto” en el nodo de” acceso remoto” de la “console tree” se puede observar una conexión y el usuario conectados (Figura 4.33)

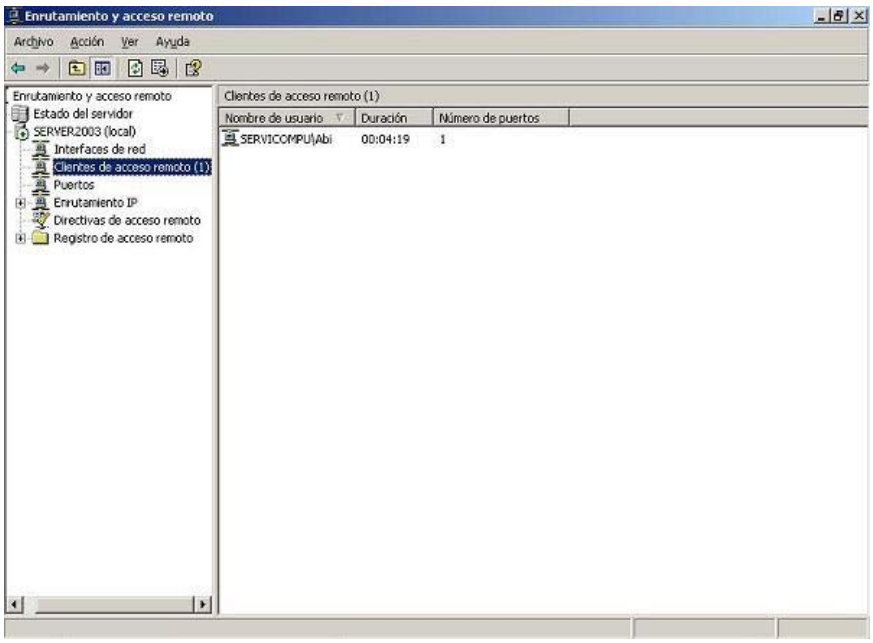


Figura 4.33

Finalmente se ha creado la conexión de acceso remoto a un servidor VPN.

Como se menciono en el capitulo II una VPN debe cumplir con ciertas elementos como autenticación, autorización y sobre todo seguridad en los

datos. En este ejemplo de implementación de VPN se configuró cada uno de los elementos mencionados.

4.2 Mantenimiento de una Red Privada Virtual

El mantenimiento de una Red privada Virtual, prácticamente recae sobre la infraestructura de soporte que la compone, por ejemplo, cuando se implementa una VPN, se establecen túneles, se crean base de datos de acceso para los usuarios y se instalan esquemas de cifrado y de administración de claves, se puede instalar servidores de autenticación de usuarios como RADIUS. Prácticamente los requisitos de mantenimiento recaen en esa infraestructura, como la autenticación de datos y usuarios, la seguridad, la administración de claves, etc.

En cuanto a los dispositivos, no son tanto problema, ya que con la tecnología actual y en constante desarrollo, el tiempo de vida de un dispositivo es de años. En la figura 4.34 muestra algunos de los requisitos de mantenimiento de una red privada virtual.

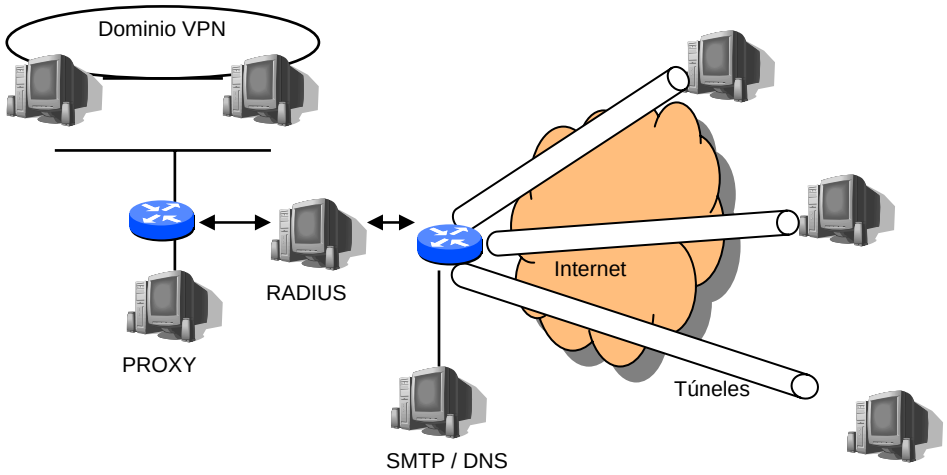


Figura 4.34 Requisitos de mantenimiento

La actualización de software es importante cuando se ha optado por una VPN basada en sistemas operativos. Es sabido que todos los sistemas operativos presentan problemas en cuestión de seguridad, en este caso hay que estar al tanto en sus páginas Web de soporte, sobre las actualizaciones y parches de seguridad. Muchos dispositivos también hacen uso de software por ejemplo, las firewall con VPN, en estos casos también es importante mantener su software actualizado.

La administración de claves es otro factor importante dentro de la tecnología de una VPN, si llegase a fallar el servidor de claves, ninguna comunicación con la VPN se efectuará y tal vez se tenga que utilizar alguna clave vieja. Por lo que hay que tener un especial cuidado en esto, la administración de claves abarcan el proceso de asegurar, generar, distribuir y almacenar claves, por lo que se requiere mantener una supervisión constante para garantizar su protección.

La buena configuración y mantenimiento de los registros también es muy importante en cuestión de seguridad de la VPN, como ya se había mencionado, con los registros se puede saber, por que dirección IP entraron y que servidor fue el que intentaron atacar. Aun si se ha falsificado la dirección IP, se puede decir de cual PSI vienen y al menos el PSI intentará ayudar.

Generalmente mucho de los problemas que involucran a las VPN no son precisamente problemas de la VPN, si no que tienen que ver con problemas de enrutamiento, de traducciones de direcciones de red, de instalación y configuración. Solo pequeños problemas son los que pertenecen a la VPN, por ejemplo las claves de cifrado que no se encuentren sincronizadas.

Conclusiones Generales

Conclusiones Generales

Como se menciono en el capítulo I, la finalidad de una red de computadoras, Intranets y Extranets dentro de una organización es la de aumentar la eficiencia y reducir costes, esto se logra básicamente compartiendo información, recursos y servicios.

El uso de las redes de computadoras y de Internet para los negocios y para la transferencia de datos aumenta considerablemente cada año en las organizaciones, su uso ha cambiado la forma de comunicar a la gente, acortando distancias geográficas, por ejemplo, se puede enviar información en un correo electrónico de México hasta España en cuestión de minutos, se puede establecer una videoconferencia entre varias instituciones ubicadas en distintos puntos geográficos, etcétera.

Sin embargo, casi a la par, el aumento de hackers, crackers, virus y programas dañinos ha ocasionado que las redes de computadoras y la Internet sean su blanco de ataques.

Por lo tanto al término de este trabajo se ha podido observar que la integración de redes privadas virtuales en las organizaciones es benéfica en muchos sentidos.

La seguridad y la accesibilidad es uno de los principales beneficios, el poder dejar de usar líneas alquiladas que representa una fuerte inversión económica y poder usar una red pública como Internet, para la transmisión de datos, es una gran ventaja; conectarse a una red desde cualquier punto geográfico y tener acceso a sus recursos de una manera segura ha ocasionado que las soluciones VPN tengan el éxito asegurado.

Los deseos de las organizaciones para proteger su información, ha ocasionado que las soluciones VPN estén en constante desarrollo, realizando mejoras en los protocolos PPTP, L2TP, IPSec, MPLS, entre otros, en técnicas de autenticación y en dispositivos dedicados, ocasiona que los proveedores se vean forzados a competir entre ellos para ofrecer la mejor solución, y por lo tanto un abaratamiento en sus precios, siendo beneficiados los consumidores. En la siguiente tabla 1 se muestra algunos proveedores importantes de los cientos que existen en el desarrollo de tecnología VPN.

Compañía	**Solución VPN**	**Solución Firewall**	**Plataforma**
CISCO	VPN de CISCO	Firewall PIX de Cisco Secure	Routers optimizados de VPN con interfaces familiares de Windows 95 o Windows NT
Symantec	Symantec Enterprise VPN 7.0	Symantec Enterprise Firewall	Servidores: Windows NT,2000,2003 Solaris7 y 8 Clientes: Windows 95, 98, 2000 y XP
CyberGuard	SnapGear	SnapGear	Dispositivo VPN dedicado Clientes: Windows XP,2000 Sun solaris
Check Point	VPN-1 Pro	Firewall-1	Servidores: Windows 2003 SP1, Windows2000, XP, 98. Solaris 8 y 9. Mac OS, Nokia IPSO 3.9/4.0 Clientes: Windows2003,2000,XP,98 Mac OS Hand-Held PC200
US.Robotics	USR8200 Firewall / VPN	USR8200 Firewall / VPN	Dispositivo VPN dedicado, soporta clientes Windows 95,98, 2000,XP Cualquier versión Linux, Solaris y Mac OS
Stonesoft	StoneGate	StoneGate	Solución de software para servidores LX50 de Sun Microsystems
Nortel Networks	Routers VPN serie 200/600/1000/5000		Dispositivo VPN dedicado, soporta clientes: Windows 95,98,2000 y XP, Windows Mobile(Pocket PC) IBM-AIX, SUN-Solaris, HP-UX, Linux.
Novell	Novell Border Manager 3.8	Novell Border Manager 3.8	Servidor: NetWare Clientes: Windows 2000, 98 y XP
Juniper Networks	SSL VPN	Juniper Networks Firewall / IPSec	Dispositivo VPN dedicado
WatchGuard	WatchGuard Firebox	WatchGuard Firebox	Dispositivo VPN / Firewall Clientes: Cualquier versión de Windows

Tabla 1 Algunas compañías encargadas de desarrollar tecnología VPN

La implementación de una VPN siempre dependerá de las necesidades de la empresa, el uso efectivo de la tecnología VPN y la elección de los mismos requiere de un claro entendimiento de los objetivos de seguridad de la organización o de los usuarios que quieran implementarla. No es necesario invertir en grandes cantidades de dispositivos con lo último en tecnología VPN, o pagar a una compañía PSI para que la administre, como se pudo observar en el capítulo IV, se implemento una VPN sencilla basada en software, pero eso no implica, que es menos segura, ya que se configuró los requisitos primordiales en una VPN tales como: seguridad a nivel VPN, políticas de acceso y conexión, seguimiento de registros así como permisos de usuarios.

El único impedimento que puede existir en el desarrollo de las redes privadas virtuales es de tipo gubernamental, ya que en algunos países como el de Estados Unidos de América el uso de cifrado esta restringido a DES de 128 bits, ocasionando estancamiento en el desarrollo de nuevos dispositivos que soporten, por ejemplo, cifrado de 256 bits o superiores, argumentando cuestiones de “seguridad nacional”, presionando a los fabricantes para que construyan productos de cifrado que contengan puertas traseras en sus productos, para poder intervenir cualquier tipo de transmisión que consideren “sospechosa”, e imponiendo grandes penas a las compañías que violen dicho cifrado; en México todavía no existe una legislación en cuanto al cifrado.

No obstante se puede considerar a las redes privadas virtuales como una solución que seguirá creciendo y evolucionando, son cada vez más compañías las que están migrando a este tipo de solución, por ser consideradas una herramienta que permite la transferencia de datos, en ocasiones con calidad de servicio (QoS) sobre redes públicas como Internet de una manera segura, practica, económica y eficiente.

En mi opinión las materias de Sistemas de información y Redes computacionales fueron primordiales para que me naciera el interés sobre los sistemas de información y las redes computacionales, y de ahí enfocarme hacia lo que es la seguridad en redes, considerando el auge y la importancia que están tomando estos temas en la vida real y sobre todo en un país tan grande como México, a estas materias se les debería dar más apoyo para que surjan especialistas en cuestiones de redes, sistemas y seguridad, este apoyo prácticamente consistiría en laboratorios para realizar practicas un tanto reales que en un futuro sirvan al alumno para poder enfrentar situaciones reales, en cuestión de materias, se tendría que agregar algunas materias tales como “seguridad de redes” que sirvan para complementar la formación del alumno.

Bibliografía

BIBLIOGRAFIA

📖 Leon Clark, David. **Guía para el Administrador de Redes Privadas Virtuales (RPV)**, Editorial Mc Graw Hill, México 2001, 321p.

📖 Kolesnikov, Oleg, Hatch, Brian. **Redes Privadas Virtuales con Linux,** Editorial Prentice Hall, España 2003, 414p.

📖 Brown, Steven. **Implementación de Redes Privadas Virtuales- RPV**, Editorial Mc Graw Hill, México 2001.

📖 Manson, G. Andrew. **Redes Privadas Virtuales de Cisco Secure**, Editorial Pearson Education, Madrid 2002, 400p.

📖 Black, Uyless. **Redes de Computadores: Protocolos, normas e interfaces**, Editorial Ra-Ma, España 1995. 585p.

📖 Microsoft Corporation. **Microsoft Fundamentos de redes Plus. Curso oficial de certificación de MCSE,** Editorial Mc Graw Hill, Madrid 2000, 646p.

📖 Gallo, Michael A., Hancock, William M. **Comunicación entre computadoras y tecnología de redes**, Editorial THOMSON, México 2002, 632p.

📖 Tanenbaum, Andrew S. **Redes de computadoras**, Editorial PEARSON EDUCACION, México 2003, 912p.

📖 Evans, Tim **Construya su propia Intranet, Guía práctica para configurar una Web interna**, Editorial Prentice Hall Hispanoamericana, México 1996, 668p.

📖 Microsoft Official Course, **Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure: Network Services**, Microsoft Corporation 2003.

📖 Cisco Systems, Inc. **Academia de Networking de Cisco Systems: Fundamentos de seguridad de redes. Especialista en Firewall Cisco**, Editorial PEARSON EDUCATION, Madrid 2005, 832p.

Otras fuentes de Información

Microsoft Windows Server 2003 TechCenter. **"Acceso Remoto"** [en línea]. Microsoft TechNet 21 de enero 2005. <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/94ff4edf-ddc7-411a-a125-36ece8ad3053.mspx?mfr=true > [Consulta: septiembre 2005].

Uri Goren. **"Virtual Private Networks"**. [en línea]. RAD data communication. <http://www2.rad.com/networks/2004/vpn/main.htm> [Consulta: septiembre 2005].

CISCO Systems **"VPN Services"** [en línea]. <://www.cisco.co/en/us/netsol/ns341/ns121/ns193/networking_solutions_solution.htl> [Consulta:Marzo 2006].

Lloyd, B.; Simpson, W., ed. **PPP Authentication Protocols** [Lugar de publicación desconocido]: Internet Engineering Task Force, Octubre 1992. Request for comments: 1334. [26 pp.] Disponible en Internet en: http://www.ietf.org/rfc/rfc1334.txt?number=1334

Simpson, W., ed. **The Point-to-Point Protocol (PPP)** [Lugar de publicación desconocido]: Internet Engineering Task Force, Julio 1994. Request for comments: 1661. [52pp] Disponible en Internet en: http://www.ietf.org/rfc/rfc1661.txt?number=1661

Hamzeh, K.; Pall, G.; Verthein, W.; Taarud, J.; Little, W.; Zorn, G., ed. **Point-to-Point Tunneling Protocol (PPTP)** [Lugar de publicación desconocido]: Internet Engineering Task Force, Julio 1999. Request for comments: 2637. [57pp] Disponible en Internet en http://www.ietf.org/rfc/rfc2637.txt?number=2637

Townnsley, W.; Valencia, A.; Rubens, A.; Pall, G.; Zorn, G; Palter, B., ed. **Layer TwoTunneling Protocol "L2TP"** [Lugar de publicación desconocido]: Internet Engineering Task Force, Agosto 1999. Request for comments: 2661. [80 pp.] Disponible en Internet en: http://www.ietf.org/rfc/rfc2661.txt?number=2661

Valencia, A.; Littlewood, M.; Kolar, T., ed. **Cisco Layer Two Forwarding (Protocol) "L2F"** [Lugar de publicación desconocido]: Internet Engineering Task Force, Mayo 1998. Request for comments: 2341. [29pp] Disponible en Internet en: http://www.ietf.org/rfc/rfc2341.txt?number=2341

Lau, J.; Townsley, M.; Goyret, I., ed. **Layer Two Tunneling Protocol – Version 3 (L2TPv3)** [Lugar de publicación desconocido]: Internet Engineering Task Force, Marzo 2005. Request for comments: 3931. [94pp] Disponible en Internet en: http://www.ietf.org/rfc/rfc3931.txt?number=3931

Kent, S.; Atkinson, R., ed. **Security Architecture for the Internet Protocol** [Lugar de publicación desconocido]: Internet Engineering Task Force, Noviembre 1998. Request for comments: 2401. [66pp] Disponible en Internet en: http://www.ietf.org/rfc/rfc2401.txt?number=2401

Kent, S.; Atkinson, R., ed. **IP Authentication Header** [Lugar de publicación desconocido]: Internet Engineering Task Force, Noviembre 1998. Request for comments: 2402. [22pp] Disponible en Internet en: http://www.ietf.org/rfc/rfc2402.txt?number=2402

Kent, S.; Atkinson, R., ed. **IP Encapsulating Security Payload (ESP)** [Lugar de publicación desconocido]: Internet Engineering Task Force, Noviembre 1998. Request for comments: 2406. [22pp] Disponible en Internet en: http://www.ietf.org/rfc/rfc2406.txt?number=2406

Harkins, D.; Carrel, D.; ed. **The Internet Key Exchange (IKE)** [Lugar de publicación desconocido]: Internet Engineering Task Force, Noviembre 1998. Request for comments: 2409 [41pp] Disponible en Internet en: http://www.ietf.org/rfc/rfc2409.txt?number=2409

Rosen, E.; Viswanathan, A.; Callon, R.; ed. **MultiProtocol label Switching Architecture** [Lugar de publicación desconocido]: Internet Engineering Task Force, Enero 2001. Request for comments: 3031. [61pp] Disponible en Internet en: http://www.ietf.org/rfc/rfc3031.txt?number=3031

Glosario

GLOSARIO

Autenticación.- Proceso de identificar positivamente la identidad del emisor.

Calidad de servicio (QoS).- Nivel de prestaciones de un servicio, basado en parámetros tales como velocidad de respuesta, nivel de retardo, rendimiento, horario, etcétera.

Cifrado.- Es el proceso de codificar un paquete de datos mediante técnicas criptográficas.

CDMA2000 1xRTT.- es una familia de estándares en telecomunicaciones móviles de tercera generación (3G) que utilizan CDMA, un esquema de acceso múltiple para redes digitales, para enviar voz, datos, y señalización entre teléfonos celulares y estaciones base.

Conmutador.- Dispositivo empleado para cambiar el paso de la corriente eléctrica entre distintos conductores.

Cracker.- Al igual que hacker es una palabra que se utiliza para designar a una persona con amplio conocimiento, pero a diferencia del hacker sus intrusiones a los sistemas, son con finalidad destructiva.

Datagrama.- Paquete de datos autónomo con información suficiente como para ser dirigido desde la fuente al destino con independencia del camino recorrido a través de una red.

DES.- (Data Encryption Standard) Estándar de cifrado de datos, se utiliza para cifrar y descifrar los datos de los paquetes. DES utiliza una clave de 56 bits para garantizar un cifrado de alto rendimiento.

DHCP.- (Dynamic Host Configuration Protocol) Protocolo Dinámico de configuración de Hosts, protocolo para la configuración TCP/IP automática que proporciona un reserva y gestión estática y dinámica de direcciones.

DNS.- (Domain Name System) Sistema de Nombres de Dominio, Esquema de traducción a direcciones IP de cadenas de palabras que identifican usuarios y localizaciones. Los servidores de nombres se encargan de establecer esta correspondencia, traduciendo un nombre alfabético común en su dirección IP numérica. Un servidor DNS permite a los usuarios localizar ordenadores en Internet por su nombre en lugar de por su dirección IP, manteniendo una base de datos de nombres de host y direcciones IP

Encapsulamiento.- Para que se puedan producir comunicaciones confiables a través de una red, los datos que se deben enviar se deben colocar en paquetes que se puedan administrar y rastrear. Esto se realiza a través del proceso de encapsulamiento.

Encriptación.- Es el proceso mediante el cual cierta información es cifrada de forma que el resultado sea ilegible a menos que se conozca los datos necesarios para su interpretación.

Extranet.- Red privada resultante de la interconexión de dos o más Intranets que vinculan de modo seguro organizaciones externas.

FEP.- Un procesador frontal o FEP, es un dispositivo encargado de interconectar un usuario con el sistema que atenderá el requerimiento,

Firewall.- Sistema de seguridad que puede ser hardware o software que protege nuestra red corporativa de intrusiones externas que pueden ser otra red, incluyendo la Internet.

Hacker.- Palabra que se utiliza para referirse a una persona experta en una o más ramas técnicas relacionadas con la tecnología de la información y las telecomunicaciones (redes, sistemas operativos, programación, etcétera). Su elevado conocimiento hace que tomen como reto la intrusión a sistemas con la finalidad de probar sus conocimientos y habilidades.

Host.- Son las máquinas personales de los clientes, diseñadas para programas de aplicaciones del usuario o cliente.

IAB.- (Internet Architecture Board) Consejo sobre arquitectura de Internet, órgano de la Internet Society (ISOC) que determina las necesidades técnicas a medio y largo plazo, y toma las decisiones sobre la orientación tecnológica de Internet. La IAB aprueba las recomendaciones y estándares de Internet a través de una serie de documentos denominados RFC.

IETF.- (Internet Engineering Task Force) La Fuerza de Trabajo de Ingeniería de Internet, agencia de vigilancia, que por lo general se encarga de las especificaciones de desarrollo y las políticas de desempeño de protocolos y su integración a la Internet.

Internet.- Red interconectada más grande del mundo, es un sistema de telecomunicaciones abierto, de tecnologías y protocolos, que permite a los usuarios con diferentes tipos de computadoras y sistemas operativos acceder a los millones de sitos de información a través de interfaces gráficas que conocemos como exploradores.

Intranet.- Red privada interconectada que utiliza las tecnologías y protocolos de Internet como exploradores, sitios Web y HTML.

LAN.- (Local Area Network) Red de área local, es una red confinada a un área geográfica limitada, como ejemplo, el interior de un edificio.

TCP/IP.- Conjunto de protocolos de Internet que proporciona comunicaciones en un conjunto heterogéneo, proporciona un protocolo de red encaminable y un acceso a Internet y sus recursos.

Paquete.- Es el termino que se utiliza para referirse a las unidades de datos de la capa de red, es una agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario.

Periférico.- Dispositivo de una computadora que potencia la capacidad de esta y permite la entrada y/o salida de datos.

Protocolo.- Reglas y procedimientos que rigen la forma en la que los dispositivos de una red intercambian información.

Protocolo punto a punto (PPP).- Protocolo que permite establecer el protocolo TCP/IP en líneas telefónicas de marcación serial y en líneas dedicadas como ISDN.

Proveedor de servicios Internet (PSI).- Compañía comercial que proporciona acceso a Internet.

Red.- Conjunto de computadoras interconectadas entre si con la finalidad de intercambiar información.

Router.- (ruteador o encaminador) Dispositivo de hardware o software para la interconexión de redes. Los ruteadores funcionan a nivel de red en el modelo de referencia OSI, así que un ruteador puede conmutar y encaminar paquetes por varias redes, también determinan el mejor camino para enviar datos.

Segmento.- unidad única de información de capa de transporte, dentro de las especificaciones TCP, también se usan para describir agrupamientos de información lógica en diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Servidor de acceso remoto (RAS).- Dispositivo que permite a los usuarios móviles o remotos que utilizan vínculos de comunicaciones de acceso telefónico tener acceso a las redes corporativas, como si estuvieran conectados directamente.

Subred de comunicación.- Conjunto de ruteadores, líneas de comunicación y direccionamiento de redes que mueven paquetes de datos del host de origen al destino.

Trama.- Agrupación lógica de información enviada como unidad de capa de enlace de datos en un medio de transmisión. Generalmente se refiere al encabezado y a la información final, utilizados para la sincronización y el control de errores, que rodean los datos de usuario contenidos en la unidad.

Virus informático.- Programa de computadora, diseñado para modificar otros programas para incluir copias de si mismo, los daños que pueden ocasionar estos virus son perdida de información, robo de información y cortes en los sistemas.

WAN.- (Wide Area Network) Red de área amplia. Es una red que no tiene limitaciones geográficas, se pueden conectar a equipos o dispositivos ubicados en distintos puntos geográficos.