



**Universidad Nacional
del Nordeste**

**Facultad de Ciencias Exactas y
Naturales y Agrimensura**

Redes Virtuales Privadas

Teleprocesos y Sistemas Distribuidos

Profesor: David L. la Red Martinez

Alumno: Gerardo Gabriel Brollo

2008

Contenido

1. LOS ENLACES PRIVADOS ANTES DE LA APARICION DE LAS REDES PRIVADAS VIRTUALES

- 1.1. Introducción.
- 1.2. Enlaces Privados.
- 1.3. Tipos de Enlaces Privados.
 - 1.3.1. Enlaces Dedicados.
 - 1.3.1.1. Clear Channel.
 - 1.3.1.2. Frame Relay.
 - 1.3.1.3. ATM (Asynchronous Transfer Mode).
 - 1.3.2. Enlaces Conmutados.
 - 1.3.2.1. Enlaces Conmutados Analógicos.
 - 1.3.2.2. Enlaces Conmutados Digitales – RDSI.

2. REDES PRIVADAS VIRTUALES – VPNs

- 2.1. Introducción.
- 2.2. Que son las Redes Virtuales Privadas – VPN?
- 2.3. ¿Por qué una VPN?
- 2.4. Medios.

3. ARQUITECTURAS VPN

- 3.1. Intranet VPN Lan – to - Lan.
- 3.2. Acceso Remoto VPN.
- 3.3. Extranet VPN.
- 3.4. Modelo de Enrutamiento.
- 3.5. VPN Interna WLAN.

4. IMPLEMENTACIONES VPNs

- 4.1. Sistemas Basados en Hardware.
- 4.2. Sistema Basados en Cortafuegos.
- 4.3. Sistema Basados en Software.

5. TECNOLOGÍAS DE TUNEL Y CIFRADO DE DATOS

- 5.1. PPP (Point-to-Point Protocol).
- 5.2. PPTP (Point-to-Point Tunneling Protocol).
 - 5.2.1. Vulnerabilidad de PPTP.
 - 5.2.2. Túneles.
 - 5.2. L2TP (Layer 2 Tunneling Protocol).
 - 5.2.1. Componentes Básicos de Túneles L2TP.
 - 5.2.1.1. Concentrador de acceso L2TP (LAC).
 - 5.2.1.2. Servidor de Red L2TP (LNS).

5.2.1.3. Túnel.

5.2.2. Topología de L2TP.

5.3. IPSEC.

5.3.1. Componentes de IPSEC.

5.3.1.1. Protocolos de Seguridad.

5.3.1.2. Asociaciones de Seguridad (SAs).

5.3.1.3. Bases de Datos de Seguridad.

5.3.1.3.1. Bases de Datos de Asociaciones de Seguridad (SAD).

5.3.1.3.2. Bases de Datos de Políticas de Seguridad.

6. COMPARATIVA ENTRE DISTINTAS TECNOLOGIAS DE TUNELAMIENTO

7. VPN DINÁMICAS

7.1 Funcionamiento de las D - VPNs.

8. CONCLUSIONES

9. BIBLIOGRAFÍA

1. LOS ENLACES PRIVADOS ANTES DE LA APARICION DE LAS REDES PRIVADAS VIRTUALES

1.1. INTRODUCCIÓN

Desde el principio de los tiempos, la humanidad ha tenido la necesidad de comunicarse. Paralelamente también ha existido la necesidad de hacerlo de manera privada, es decir que el mensaje sólo le llegue a determinados receptores.

En las redes de comunicaciones pasa exactamente lo mismo. En especial el sector corporativo siempre ha requerido la implementación de enlaces privados para transportar de forma segura toda su información confidencial.

1.2. ENLACES PRIVADOS

Los enlaces privados se caracterizan por brindar seguridad en la transmisión de datos de extremo a extremo. Se valen siempre de una red de transmisión (en algunos casos también existe una red de conmutación) para conectar las partes. Estos enlaces pueden ir desde los 9600bps (en el caso de una conexión conmutada usando un modem análogo de 9600bps) hasta el orden de los Gigabps (usando redes ópticas, con equipos de transporte de última generación o multiplexores DWDM).

1.3. TIPOS DE ENLACES PRIVADOS

Las redes de computadores se han valido de los enlaces privados para interconectarse a través de grandes distancias geográficas. Antes de la aparición de las VPN habían existido sólo dos tecnologías de enlaces WAN, los enlaces dedicados, y los enlaces conmutados. Dentro de los enlaces dedicados caben topologías tales como Clear Channel, Frame Relay y ATM. Aunque se sabe que Frame Relay usa conmutación de paquetes y ATM usa conmutación de celdas, en este trabajo se clasifican como enlaces dedicados, porque en últimas para el usuario la conmutación es transparente. Dentro de los enlaces conmutados están los análogos que van desde 2400bit/s hasta los 56 kbit/s y los digitales RDSI de 64 kbit/s y 128 kbit/s.

1.3.1. ENLACES DEDICADOS

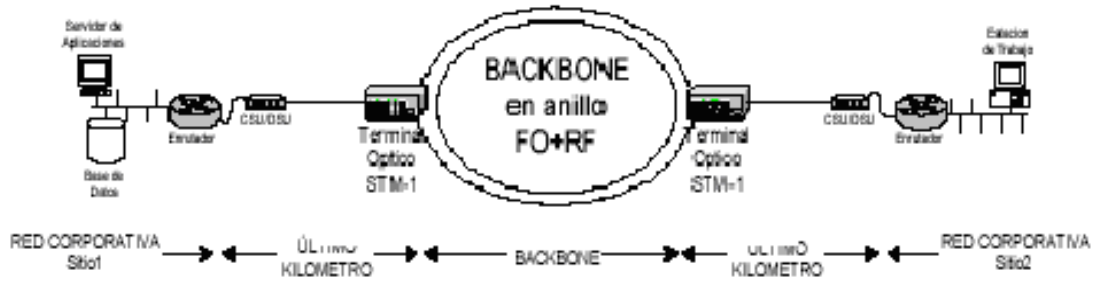
Los enlaces dedicados, como su nombre lo indica, son conexiones permanentes punto-punto, o punto-multipunto, que se valen de una infraestructura de transporte (Capa 1) o de transporte y conmutación (Capa 1 y 2). Los primeros son comúnmente llamados enlaces Clear Channel y los segundos son enlaces Frame Relay o ATM.

1.3.1.1. CLEAR CHANNEL

Son enlaces donde sólo interviene la red de transporte del proveedor de servicios. Para el mercado corporativo comúnmente van desde los 64 kbit/s hasta los 2048 kbit/s. Los enlaces Clear Channel ofrecen un rendimiento efectivo casi del 100% ya que no usan ningún tipo de encapsulación de nivel 2, es decir, no hay presentes cabeceras de ningún tipo. Por lo general, la compañía (o cliente en general) debe tener un puerto disponible DTE que cumpla con las especificaciones técnicas del equipo de comunicaciones entregado por el proveedor. Típicamente la mayoría de los equipos que se usan para recibir los enlaces Clear Channel por parte del cliente

son enrutadores o switches de nivel 3. Y son estos, los que se encargan de manejar los niveles 2 y 3.

Vale la pena aclarar, que los enlaces Clear Channel fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz PCM de los distintos operadores de telefonía locales, nacionales e internacionales. Como era de esperarse, por provenir de una tecnología que no había sido pensada para transmitir datos fue superada rápidamente.



Enlace típico Clear Channel. Esquema detallado

Figura 1.1

La figura 1.1 muestra un esquema detallado de los equipos usados en una topología de transporte de datos Clear Channel. También muestra los límites de la última milla y del backbone que se usa para transporte, estos tramos son generalmente responsabilidad del proveedor del servicio. Los equipos que se muestran pueden variar dependiendo del medio físico a utilizar: cobre, fibra óptica o espectro electromagnético.

1.3.1.2. FRAME RELAY

Frame Relay es un protocolo WAN de alto rendimiento que trabaja en la capa física y de enlace de datos del modelo de referencia OSI. Frame Relay fue diseñado originalmente para trabajar con redes ISDN. Frame Relay es una tecnología de conmutación de paquetes, que permite compartir dinámicamente el medio y por ende el ancho de banda disponible. La longitud de los paquetes es variable para hacer más eficiente y flexible las transferencias de datos. Estos paquetes son conmutados por varios segmentos de la red hasta que llegan hasta el destino final. Todo el acceso al medio en una red de conmutación de paquetes es controlado usando técnicas de multiplexación estadística, por medio de las cuales se minimizan la cantidad de demoras y/o colisiones para acceder al medio.

Ethernet y Token Ring son los protocolos de redes LAN más usados. Todas las ventajas que ofrecen los medios de hoy día, han posibilitado a Frame Relay ofrecer un alto desempeño y una gran eficiencia de transmisión.

Los equipos que se usan en una red Frame Relay se pueden dividir en dos categorías: Equipos Terminales de Datos (DTEs) y Equipos Terminales de Circuitos de Datos (DCEs).

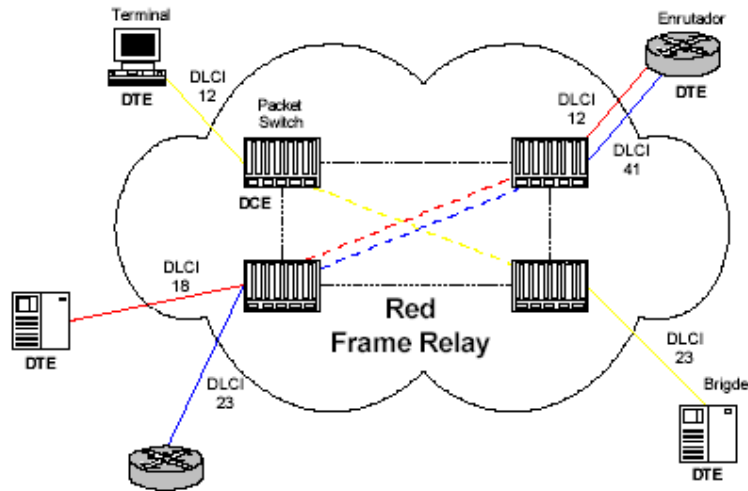


Figura 1.4 Ejemplo de asignación de valores DLCI en una red Frame Relay.

La figura 1.4 ilustra la ubicación de los DTEs y los DCEs en un red Frame Relay. Los DTEs son generalmente considerados equipos terminales de una red específica y típicamente son enrutadores, computadores personales, terminales o bridges. Estos equipos se localizan en las premisas del cliente y en la mayoría de los casos son propiedad de los mismos. Los DCEs son dispositivos normalmente propiedad del carrier. El propósito de los equipos DCEs es proveer o generar señales de reloj y conmutar los paquetes de la red. Por lo general, son llamados packet switches o conmutadores de paquetes.

1.3.1.3. ATM (ASYNCHRONOUS TRANSFER MODE)

El Modo de Transferencia Asíncrono (ATM) es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (ITU-T) para transmitir múltiples tipos de servicios, tales como voz, video y datos usando técnicas de conmutación de celdas pequeñas de tamaño fijo. Las redes ATM son, al igual que las redes Frame Relay, orientadas a conexión.

ATM es una tecnología de multiplexación y de conmutación de celdas que combina los beneficios de una red de conmutación de circuitos (capacidad garantizada, retardos constantes) y de una red de conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente). Permite transmisiones desde unos pocos megabits por segundo hasta cientos de gigabits por segundo.

Su naturaleza asíncrona, hace de ATM una tecnología más eficiente que las síncronas tales como TDM. En TDM a los usuarios se les asigna un timeslot, y ningún otro cliente puede transmitir en ese timeslot así el propietario no esté transmitiendo. Esto hace que la red no sea muy eficiente.

Una red ATM está compuesta de dos tipos de dispositivos: los switches ATM y los terminadores ATM. Un switch ATM es el encargado de recibir las celdas entrantes provenientes de otro switch ATM, leer y actualizar las cabeceras de cada celda y de direccionar la celda hasta que llegue a su destino final. Los terminadores ATM (o sistemas finales) son dispositivos que están provistos de un adaptador de interfaz de red ATM, por lo general están en las premisas del cliente.

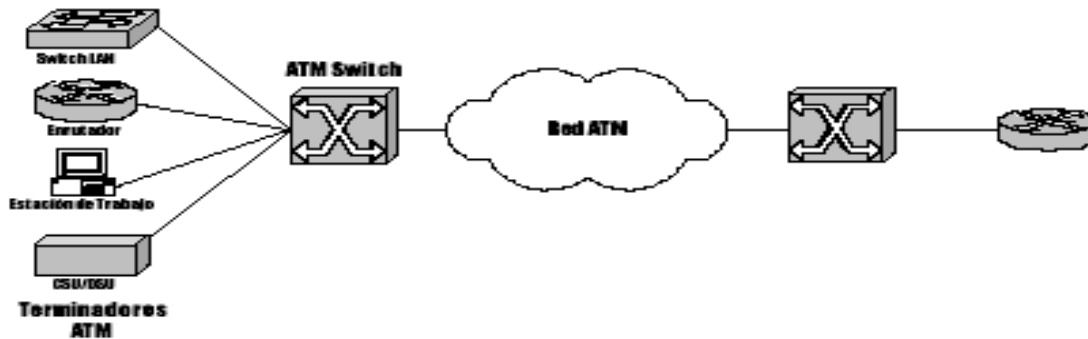


Figura 1.6 Dispositivos que intervienen en una red ATM

Ejemplos de terminadores ATM, como los que aparecen en la figura 1.6 son estaciones de trabajo, enrutadores, switches LAN, video CODECs (coder - decoders). En ATM se distingue dos tipos de interfaces: la UNI (User - Network Interface) que conecta un terminador con un switch ATM y la NNI (Network - Node Interface) que conecta dos switches ATM.

1.3.2. ENLACES CONMUTADOS

Los enlaces conmutados se dividen en dos tipos: los analógicos y los digitales. Los primeros llegan hasta velocidades de 53 kbit/s para el downlink y hasta de 48 kbit/s para el uplink, los segundos transmiten y reciben a 64 kbit/s o 128 kbit/s. Estos últimos son conocidos como enlaces RDSI (o ISDN, en inglés) que son las siglas de Red Digital de Servicios Integrados.

1.3.2.1. ENLACES CONMUTADOS ANALÓGICOS

Fue quizá la primera tecnología de transmisión de datos que usó el hombre para construir redes privadas entre dos sitios remotos. Esto lo hizo aprovechando la Red de Telefonía Pública Conmutada – RTPC (PSTN, en inglés), dicha red ha tenido muchos desarrollos en los últimos 20 años. El servicio tradicional que la RTPC ha prestado ha sido comunicación de voz, y sólo recientemente se empezó a usar para soportar un creciente mercado de transferencia de datos. El rango de frecuencia de la voz humana va desde los 20Hz hasta los 20Khz, pero casi toda la energía espectral se encuentra entre los 300Hz y 3.4Khz, por ende, la ITU ha definido un canal de voz (speech channel) para telefonía en esta banda. En un enlace conmutado de datos, intervienen varios equipos desde el usuario inicial hasta el punto o equipo destino. La figura 1.10 muestra los componentes de un enlace típico de datos sobre la red telefónica pública, se puede notar la necesidad de realizar una conversión A/D y otra D/A. La inercia que resulta de todo este proceso electrónico es la que en últimas limita a 56 kbit/s una comunicación analógica, que incluso puede llegar a 33.6 kbit/s cuando aparece una tercera y cuarta conversión entre la Central Telefónica 2 y el terminador de la llamada.

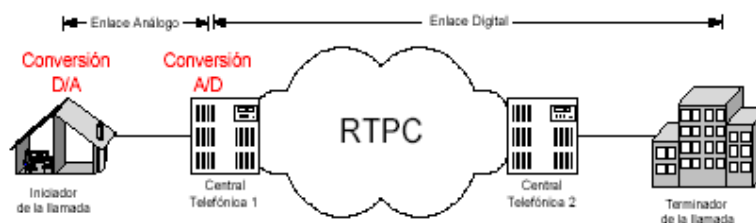
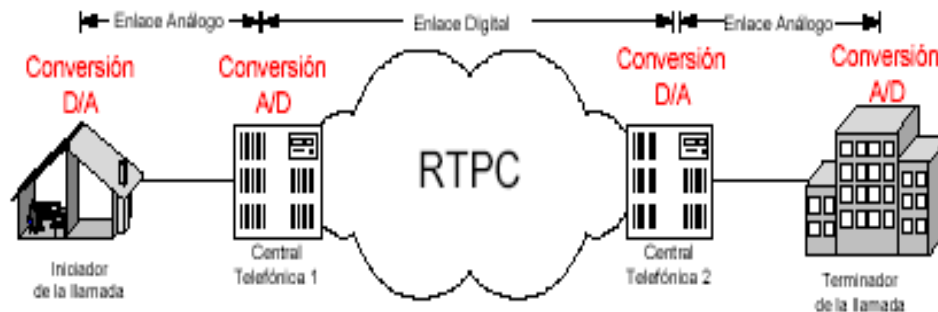


Figura 1.10 Escenario típico de una conexión analógica de datos sobre la RTPC.

Se puede notar que la conexión entre el iniciador de la llamada y la central telefónica es analógica, y se lleva a cabo usando el mismo par de cobre de la línea telefónica, para esto se usa un modem analógico. Mientras que en el lado del sitio remoto la conexión es digital, y para esto se usan enlaces RDSI PRI o BRI. Por lo general los equipos que intervienen en este lado son servidores de acceso remoto (Remote Access Server – RAS). Cuando este enlace es también analógico, entonces se puede notar que en el proceso total de la conexión intervienen cuatro conversiones, dos A/D y dos D/A, esto hace que la velocidad de transmisión y de recepción máximas sean apenas de 33.6 kbit/s. La figura 1.11 ilustra este escenario.



1.3.2.2. ENLACES CONMUTADOS DIGITALES – RDSI

RDSI o Red Digital de Servicios Integrados es un sistema de telefonía digital. Este sistema permite transmitir voz y datos simultáneamente a nivel global usando 100% conectividad digital. En RDSI, la voz y los datos son transportados sobre canales B (del inglés Bearer) que poseen una velocidad de transmisión de datos de 64 kbit/s, aunque algunos switches ISDN limitan esta capacidad a solo 56 kbit/s. Los canales D (o canales de datos) se usan para señalización y tienen velocidades de 16 kbit/s o 64 kbit/s dependiendo del tipo de servicio. Los dos tipos básicos de servicio RDSI son: BRI (del inglés Basic Rate Interface) y PRI (del inglés Primary Rate Interface). Un enlace BRI consiste de dos canales B de 64 kbit/s y un canal D de 16 kbit/s para un total de 144 kbit/s. Este servicio está orientado a brindar capacidad de conexión para usuarios residenciales. Un enlace PRI está orientado a usuarios que requieren un mayor ancho de banda. Para acceder a un servicio BRI, es necesario tener una línea RDSI. Si sólo se desean comunicaciones de voz es necesario tener teléfonos digitales RDSI, y para transmitir datos es necesario contar con un adaptador de Terminal – TA (del inglés Terminal Adapter) o un enrutador RDSI.

A diferencia de las conexiones conmutadas analógicas en una conexión RDSI el camino es 100% digital desde la central hasta el sitio del abonado, por lo cual no existe ningún tipo de conversiones A/D o viceversa, lo que facilita la obtención de velocidades de 64 kbit/s o 128 kbit/s, lo cual se logra convirtiendo los dos canales B de 64 kbit/s o en un canal lógico de 128 kbit/s. Esta característica es usada sólo en transmisión de datos y depende de la facilidad que tenga el equipo terminal de realizar esto. Típicamente esta característica tiene el nombre de Multilink.

2. REDES PRIVADAS VIRTUALES – VPNs

2.1. INTRODUCCIÓN

Es comúnmente aceptado el hecho que las tecnologías de información en Internet han cambiado la forma como las compañías se mantienen comunicadas con sus clientes, socios de negocios, empleados y proveedores. Inicialmente las compañías eran conservadoras con la información

que publicaban en Internet, tal como, productos, disponibilidad de los mismos u otros ítems comerciales. Pero recientemente, con el auge que ha tenido Internet, por el cada vez menor costo que la gente tiene que pagar para acceder a esta gran red y con el significado que esta ha adquirido como el principal medio mundial de comunicación, las redes privadas virtuales han hecho su aparición con más fuerza que nunca y se han ganado un espacio dentro del tan cambiante mundo de las redes de información.

Tradicionalmente, un enlace privado se ha hecho por medio de tecnologías WAN como X.25, Frame Relay, ATM, enlaces Clear Channel o enlaces conmutados (todas estas tecnologías WAN). Ahora con el gran crecimiento de Internet, es posible usar un protocolo como IP, sin importar la tecnología WAN que lo soporte, para disfrutar de los servicios y ventajas que ofrecen las redes privadas. Y mientras que las tradicionales redes privadas se han hecho fuertes en las conexiones LAN – to - LAN, no han sido capaces de atacar el mercado de los usuarios individuales o pequeñas oficinas sucursales, y es aquí principalmente donde han surgido con fuerza las soluciones basadas en VPNs sobre IP, pues su implementación resulta sencilla y bastante económica. Además el hecho que las VPNs se construyan sobre infraestructuras públicas ya creadas ha hecho que las empresas ahorren más del 50% del costo que antes tenían que pagar en llamadas de larga distancia y en equipos físicos de acceso remoto o en alquiler de enlaces privados o dedicados.

2.2. QUÉ SON LAS REDES PRIVADAS VIRTUALES – VPNs

Para poder habilitar redes privadas distribuidas para comunicar de forma segura cada uno de los nodos de una red pública hay una necesidad de evitar que los datos sean interceptados. Una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto.

Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. También hace universales para su transporte los diferentes protocolos LAN entre los que se encuentran IP, IPX, Appletalk y Netbeui, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes virtuales privadas.

La figura 2.1 muestra los distintos escenarios que se pueden manejar con la tecnología de Redes Privadas Virtuales (Dial - Up, Intranet VPN y Extranet VPN). Significativamente, decrece el coste de las comunicaciones porque el acceso a Internet es generalmente local y mucho más barato que las conexiones mediante Acceso Remoto a Servidores.

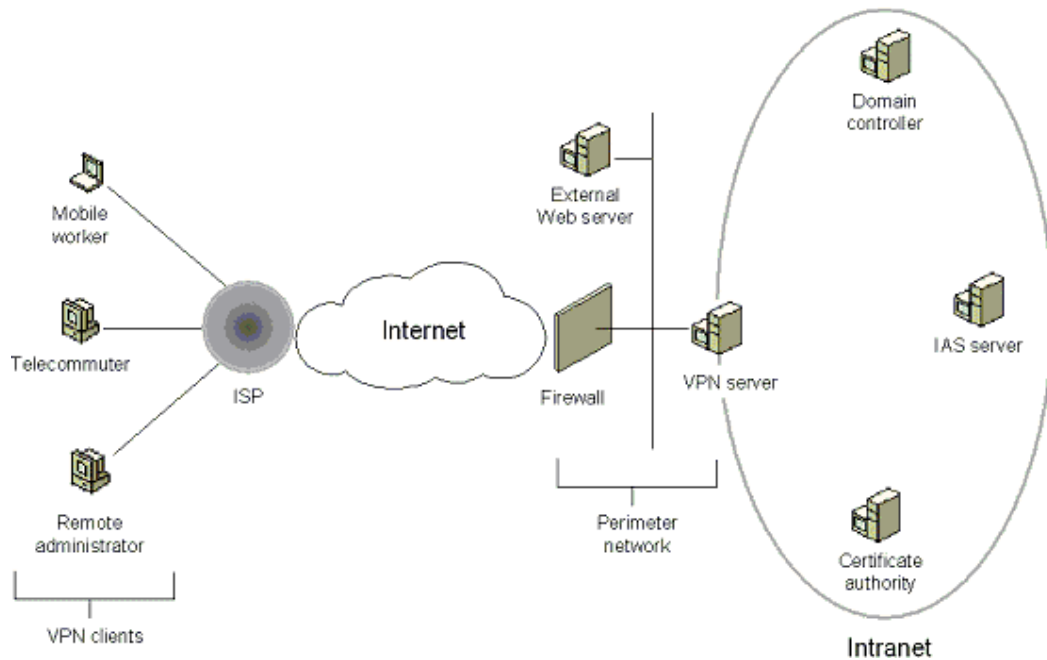


Figura 2.1.

El objetivo final de una VPN es brindarle una conexión al usuario remoto como si este estuviera disfrutando directamente de su red privada y de los beneficios y servicios que dentro de ella dispone, aunque esta conexión se realice sobre una infraestructura pública.

2.3. ¿POR QUÉ VPN?

Las VPN son una salida al costo que puede significar el pagar una conexión de alto costo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red.

Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red.

Las VPNs son una gran solución a distintos problemas, pero sólo en el campo de la economía de los usuarios porque por ejemplo en el caso de que se realice una conexión entre dos sedes de empresas, una en Japón y la otra en Perú, sería muy costoso el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más económica porque sólo se hace uso de Internet que es un conjunto de redes conectadas entre sí.

2.3.1. COSTE

La principal motivación del uso y difusión de esta tecnología es la reducción de los costos de comunicaciones directos, tanto en líneas analógicas (dial-up) como en vínculos WAN dedicados. Los costos se reducen drásticamente en estos casos: En el caso de accesos remotos, llamadas locales a los ISP (Internet Service Provider) en vez de llamadas de larga distancia a los servidores de acceso remoto de la organización. O también mediante servicios de banda ancha.

Otras Ventajas

- **Usuario Móviles:** Una vez que la empresa cuenta con una VPN puede utilizarla para otros servicios sin gastos adicionales, reduciendo así sus costos operativos. Por ej., es muy sencillo

canalizar todas las llamadas telefónicas (locales o larga distancia) entre las sucursales a través de la VPN sin incrementar costos.

- Escalabilidad y Flexibilidad: Es posible integrar nuevos puntos a la VPN a demanda, sólo se debe agregar equipos y contratar conexiones a Internet.
- La disponibilidad, la seguridad, la eficiencia en el manejo del ancho de banda y la amplia cobertura que ha logrado Internet.

2.4. MEDIOS

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

- Autenticación y autorización: ¿Quién está del otro lado?, usuario / equipo y qué nivel de acceso debe tener.
- Integridad: La garantía de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).
- Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de interceptación, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).
- No repudio: Es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.
- Administración de dirección: La solución deberá asignar una dirección al cliente en la red privada y deberá asegurarse que las direcciones privadas se mantengan así.
- Encriptación de datos: Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

3. TECNOLOGÍAS DE TUNELAMIENTO VPN

Existen varios tipos de arquitectura para las VPN, pero en esta ocasión se tratarán sólo algunas de ellas.

3.1. INTRANET VPN LAN – TO - LAN

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

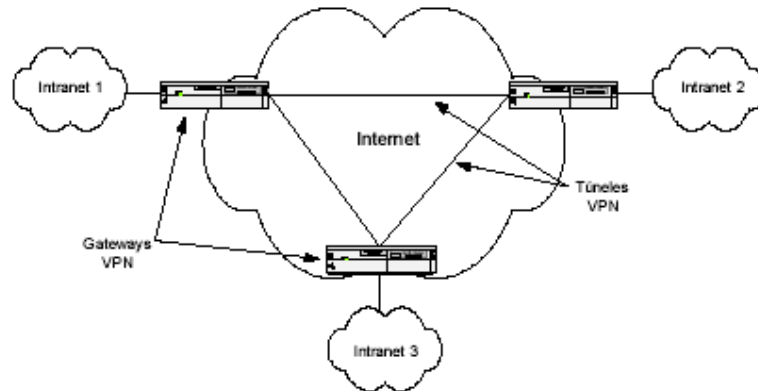


Figura 3.6 Esquema de una solución Intranet VPN (LAN-to-LAN VPN).

Tradicionalmente, para conectar dos o más oficinas remotas de una misma compañía se han necesitado contratar enlaces dedicados Clear Channels o Circuitos Virtuales Permanentes (PVCs) Frame Relay. Las empresas adoptan diferentes topologías de red WAN para interconectar todos sus sitios remotos, entre estas se encuentran: Enlaces punto – a - punto, de estrella, de malla parcial y de malla completa.

En general, cuando se necesita concentrar tráfico en al menos un nodo, es preferible usar tecnologías como Frame Relay pues sólo se necesita un último kilómetro por el cual viajan todos los PVCs contratados con el proveedor de servicio pero económicamente sigue siendo igual de costosa porque las compañías que prestan el servicio de interconexión Frame Relay cobran por PVC activado, así usen la misma solución de último kilómetro.

Si se observa bien, la mayoría de escenarios de enlaces WAN corporativos tienen más de dos nodos interconectados, por tanto habrá al menos un nodo donde existan al menos dos PVCs compartiendo un último kilómetro, esto sería por ejemplo, en la topología de estrella. Si cambiamos a malla completa o parcial, el número de PVCs aumentará considerablemente y con ellos los costos de la solución de transporte de datos. Con una arquitectura Intranet VPN (o LAN – to - LAN VPN) se puede lograr el mismo objetivo de interconectar dos o más sitios de una red corporativa y a un costo mucho menor. La economía se ve reflejada tanto en equipos que se tienen que adquirir o arrendar para el montaje inicial de la topología, como en cargos fijos que se tienen que pagar mes a mes.

3.2. ACCESO REMOTO VPN

Fue la primera aplicación que se le dio a la emergente tecnología de las VPNs. Consiste en usar cualquier RAS que preste servicio de conexión a Internet como punto de acceso a una red corporativa también conectada a Internet por medio de un gateway VPN. Esta solución nació de la necesidad de poder acceder a la red corporativa desde cualquier ubicación, incluso a nivel mundial. Con el Acceso Remoto VPN, los RAS (Remote Access Service) corporativos quedaron olvidados, pues su mantenimiento era costoso y además las conexiones que tenían que hacer los trabajadores de planta externa, como vendedores y personal de soporte técnico, cuando viajaban fuera de la ciudad, y más aun, a otros países eran demasiado costosas. El acceso remoto VPN se vio claramente impulsado por el auge de la Internet que ha hecho que prácticamente en todas partes del mundo se obtenga fácil acceso a la misma.

Con el acceso remoto VPN un trabajador que se haya desplazado a otro país, por ejemplo, y que quiere acceder a la base de datos de su compañía, o al correo interno, o a cualquier otro recurso de su red corporativa, sólo tiene que conectarse a Internet con una simple llamada local a la ISP de la ciudad en la que se encuentre, y ejecutar su cliente de marcación VPN. A partir de la versión Windows 98, Microsoft incluyó un cliente de marcación VPN que funciona con el protocolo

de entunelamiento PPTP.⁷ Todos los gateways VPN vienen con software VPN clientes para ser instalados en los distintos sistemas operativos presentes en el mercado. La figura 3.8 muestra la creación de un túnel conmutado VPN usando un cliente PPTP instalado en el computador del trabajador remoto. Nótese que se realizan dos conexiones, una PPP a la ISP, y una PPTP al gateway VPN de la compañía que se encuentra conectado a Internet. La conexión PPP puede ser analógica o digital RDSI.

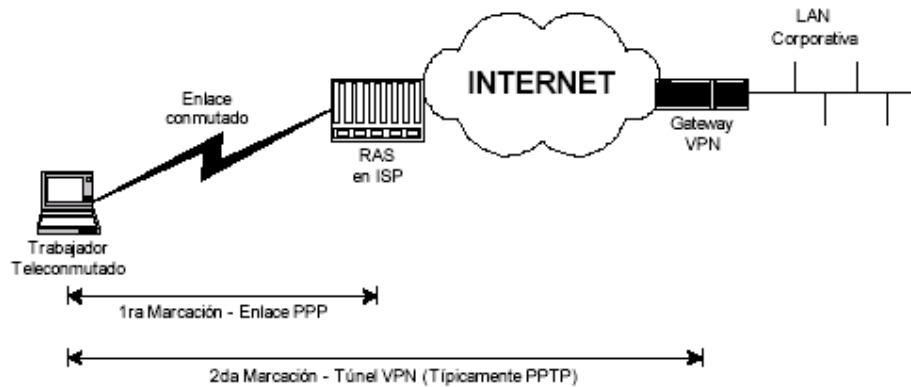


Figura 3.8 Escenario de Acceso remoto VPN.

Otra de las grandes ventajas del acceso remoto VPN sobre el tradicional acceso remoto es poder usar tecnologías de acceso de banda ancha como xDSL y cable módem. Para una empresa sería costoso e inconveniente tener un concentrador xDSL en sus instalaciones para permitirles a sus trabajadores teleconmutados el acceso a su red, mientras que las VPNs usan la infraestructura existente de los proveedores del mercado para acceder a gran velocidad a la red corporativa.

El mejor intento de una empresa por tener su propia infraestructura de acceso tradicional (no VPN) sería montar un RAS con capacidad para recibir conexiones RDSI - BRI, es decir velocidades de 64 kbit/s o 128 kbit/s, además si la llamada la origina un trabajador en otra ciudad o país se tienen que sumar los cargos de esas llamadas.

3.3. EXTRANET VPN

Las empresas necesitan intercambiar información y realizar transacciones no solamente entre sitios de su misma organización sino también con otras compañías. Por ejemplo, una empresa manufacturera quisiera permitirle a los computadores de sus distribuidores acceder a su sistema de control de inventarios. También dicha empresa quisiera poder acceder a la base de datos de sus proveedores y poder ordenar fácil y automáticamente cuando ellos necesiten materia prima.

Hoy en día todas las empresas están haciendo presencia en la Internet y esto hace casi imperativo la comunicación con las otras empresas por este medio.

Ciertamente con una arquitectura de Extranet VPNs cada empresa tiene que controlar muy meticulosamente el acceso a los recursos de su red corporativa y a los datos que van a intercambiar con sus socios de negocios. Implementar una topología Extranet VPN implica incrementar la complejidad de los sistemas de control de acceso y de autenticación. Adicionalmente la tendencia de los mercados hace que un cambio en la topología se pueda realizar fácilmente, para esto una Extranet VPN debe poder adicionar y eliminar dinámicamente acceso seguro a otras compañías. Tal reconfiguración dinámica es difícil cuando se cuenta con circuitos cerrados dedicados.

La presencia de una compañía en Internet y el uso de la arquitectura de Extranet VPN, hace posible crear conexiones dinámicas seguras a otras redes sin necesidad de cambiar la

infraestructura física. Ejemplos de conexiones dinámicas seguras y que son conocidos como Extranet VPNs se muestran en la figura 3.10.

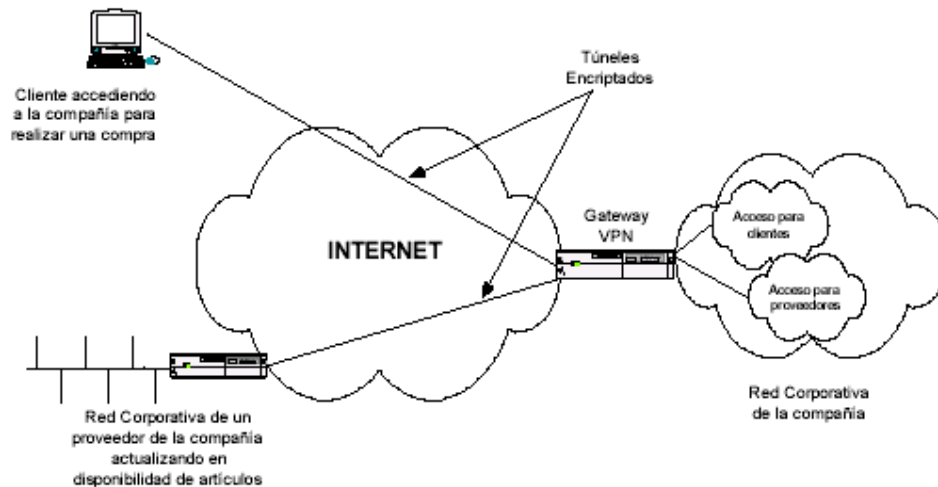


Figura 3.10 Arquitectura Extranet VPN, clasificando el acceso según privilegios de los clientes VPNs remotos

Al igual que en una arquitectura LAN to LAN VPN es necesario un Gateway VPN que se instala en la frontera de la red corporativa. Los túneles son creados a través de Internet entre este gateway y el gateway VPN situado en la red de la otra empresa. De otro modo un cliente VPN en un computador independiente podría acceder a la red corporativa como un cliente usando cualquier acceso remoto.

En la actualidad la mayoría de los gateways VPN pueden establecer múltiples túneles seguros a múltiples empresas. Sin embargo, es importante que una empresa no sea capaz de obtener acceso a la información de otra compañía que está accediendo por medio de Extranet VPNs. Un nivel más de seguridad puede ser adicionado ubicando recursos exclusivos a cada una de las compañías que va a acceder a la red de interés en diferentes servidores.

3.4. MODELOS DE ENTUNELAMIENTO

Internet se construyó desde un principio como un medio inseguro. Muchos de los protocolos utilizados hoy en día para transferir datos de una máquina a otra a través de la red carecen de algún tipo de cifrado o medio de seguridad que evite que nuestras comunicaciones puedan ser interceptadas y espiadas. HTTP, FTP, POP3 y otros muchos protocolos ampliamente usados, utilizan comunicaciones que viajan en claro a través de la red. Esto supone un grave problema, en todas aquellas situaciones en las que queremos transferir entre máquinas información sensible, como pueda ser una cuenta de usuario (nombre de usuario y contraseña), y no tengamos un control absoluto sobre la red, a fin de evitar que alguien pueda interceptar nuestra comunicación por medio de la técnica del hombre en el medio (man in the middle), como es el caso de la Red de redes.

El problema de los protocolos que envían sus datos en claro, es decir, sin cifrarlos, es que cualquier persona que tenga acceso físico a la red en la que se sitúan las máquinas puede ver dichos datos. De este modo, alguien que conecte su máquina a una red y utilice un sniffer recibirá y podrá analizar por tanto todos los paquetes que circulen por dicha red. Si alguno de esos paquetes pertenece a un protocolo que envía sus comunicaciones en claro, y contiene información sensible, dicha información se verá comprometida.

Si por el contrario, se cifran las comunicaciones con un sistema que permita entenderse sólo a las dos máquinas que son partícipes de la comunicación, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos, al no poder descifrar los datos.

Una forma de evitar este problema, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, es usar una técnica llamada tunneling.

Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure SHell), a través de las cuales se realizarán las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de SSH) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar.

3.5. VPN INTERNA WLAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

4. IMPLEMENTACIONES VPNS

4.1. SISTEMAS BASADOS EN HARDWARE

Los sistemas basados en hardware son routers que encriptan. Son seguros y fáciles de usar, simplemente hay que conectarlos. Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido, y de fácil instalación. Algunos de los productos en el mercado son por ejemplo:



ZyWALL USG 2000

Unified Security Gateway Part Number (STD): 91-009-047001B

Es una plataforma de seguridad de altísimo rendimiento para grandes empresas. Incorpora firewall, IDP, filtrado de contenidos, anti-virus, anti-spam y funcionalidades de VPN.



ZyWALL USG 1000

Unified Security Gateway Part Number (STD): 91-009-052001B

Un dispositivo de alto rendimiento con puertos Gigabit Ethernet y funciones firewall/VPN (350/150Mbps) equipado con lo mejor en seguridad orientada tanto a la PYME como a grandes empresas.



ZyWALL USG 300

Unified Security Gateway Part Number (STD): 91-009-034001B

Integra funciones de seguridad de nivel empresarial adaptadas a las PYMES. Con integración de tecnología VPN IPSec y SSL, es la solución ideal para aplicaciones VPN a través de redes distribuidas.



ZyWALL USG 200

Unified Security Gateway Part Number (STD): 91-009-057001B

La seguridad multicapa protege los datos de su empresa y de sus clientes, la propiedad intelectual y los recursos críticos contra amenazas externas e internas.



ZyWALL USG 100

Unified Security Gateway Part Number (STD): 91-009-057001B

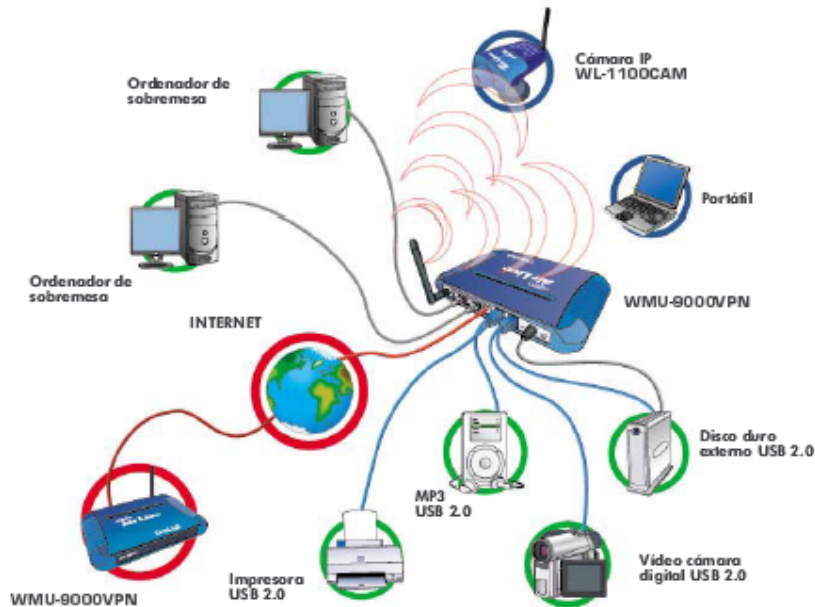
Con integración de tecnología VPN IPSec y SSL, es la solución ideal para aplicaciones VPN a través de redes distribuidas. Mayor conectividad de red con enlaces multi-ISP, tarjetas inalámbricas y 3G



ZyWALL 1050





Dispositivo de Seguridad Part Number (STD): 91-009-057001B

Con tecnología de aceleración por hardware y soporte para hasta 1000 VPNs, el ZyWALL 1050 es un concentrador ideal de VPN en la infraestructura de red.



OvisLink

The Total Networking Solution

	tuxGate® VPN 300 	tuxGate® VPN 1500 	tuxGate® VPN 1600 	tuxGate® VPN 1700 
Número Recomendado de Usuarios (la cantidad máxima de túneles VPN depende del hardware)	Hasta 150 Usuarios	Hasta 150 Usuarios	Hasta 500 Usuarios	Hasta 1.500 Usuarios
Chasis	Servidor de escritorio	Servidor enracable 1U 19"	Servidor enracable 1U 19"	Servidor enracable 1U 19"
Estándares	<ul style="list-style-type: none"> • VIA C3 ≥ 800MHz • 256 MB RAM • 20 GB HDD • Tarjeta RDSI 1x S₀ • 3 x 10/100 Ethernet • 1 x puerto serie (consola) • Fuente de Alimentación 44W AT 	<ul style="list-style-type: none"> • VIA C3 ≥ 800MHz • 256 MB RAM • 20 GB HDD • Tarjeta RDSI 1x S₀ • 5 x 10/100 Ethernet • 1 x puerto serie (consola) • Fuente de Alimentación 180W AT 	<ul style="list-style-type: none"> • 1x Intel XEON ≥ 2,4GHz • 1024 MB RAM • 2x 80 GB HDD ATA Software RAID 1 • 2 x 10/100/1000 Ethernet • 4 x 10/100 Ethernet • 1 x puerto serie (consola) • Fuente de Alimentación 325W 	<ul style="list-style-type: none"> • 1 x Intel XEON ≥ 3,0GHz • 4096 MB RAM • 2x 36 GB HDD SCSI Hardware RAID 1 • 2 x 10/100/1000 Ethernet • 4 x 10/100 Ethernet • 1 x puerto serie (consola) • Fuente de Alimentación 460W
Opciones de Hardware				
Memoria	n.d.	n.d.	Hasta 4 GB	Hasta 8 GB
CPU Dual	n.d.	n.d.	Sí	Sí
NIC	n.d.	n.d.	2x ó 4x 10/100/1000	2x 10/100/1000
RDSI	n.d.	n.d.	Sí (1x S ₀)	Sí (1x S ₀)
Fuente de Alimentación Redundante	n.d.	n.d.	Sí	Sí
Otras Opciones				
Servicio	<ul style="list-style-type: none"> • 12 Meses de Backup y Servicio de Actualización • 12 Meses de ampliación de garantía adicional 	<ul style="list-style-type: none"> • 12 Meses de Backup y Servicio de Actualización • 12 Meses de ampliación de garantía adicional 	<ul style="list-style-type: none"> • 12 Meses de Backup y Servicio de Actualización • 12 Meses de ampliación de garantía adicional 	<ul style="list-style-type: none"> • 12 Meses de Backup y Servicio de Actualización • 12 Meses de ampliación de garantía adicional
Garantía	2 años	2 años	2 años	2 años

4.2. SISTEMAS BASADOS EN CORTAFUEGOS

Estos se implementan con software de cortafuegos (firewall). Tienen las ventajas de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna. También realizan la traducción de direcciones (NAT). Estos satisfacen los requerimientos de autenticación fuerte.

Muchos de los cortafuegos comerciales, aumentan la protección, quitando al núcleo del Sistema Operativo algunos servicios peligrosos que llevan estos de serie, y les provee de medidas de seguridad adicionales, que son mucho más útiles para los servicios de VPN. El rendimiento en este tipo decrece, ya que no se tiene hardware especializado de encriptación.

4.3. SISTEMAS BASADOS EN SOFTWARE

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPNs ofrecen el método más flexible en cuanto al manejo de tráfico. Con este tipo, el tráfico puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en los VPN por hardware, todo el tráfico es enrutado por el túnel. Se puede hacer un enrutamiento inteligente de una manera mucho más fácil.

5. TECNOLOGÍAS DE TÚNELES Y CIFRADO DE DATOS

Para que se establezca un túnel tanto el cliente del túnel como el servidor del túnel deberán utilizar el mismo protocolo de túnel. La tecnología de túnel se puede basar ya sea en el protocolo del túnel de Nivel 2 ó de Nivel 3. Estos niveles corresponden al Modelo de referencia de interconexión de sistemas abiertos (OSI). Los protocolos de nivel 2 corresponden al nivel de Enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP y L2TP y el envío de nivel 2 (L2F) son protocolos de túnel de Nivel 2; ambos encapsulan la carga útil en una trama de Protocolo de punto a punto (PPP) que se enviará a través de la red. Los protocolos de Nivel 3 corresponden al nivel de la red y utilizan paquetes.

IP sobre IP y el modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos de túnel de Nivel 3. Estos protocolos encapsulan los paquetes IP en un encabezado adicional IP antes de enviarlos a través de una red IP.

PROTOCOLO DE PUNTO A PUNTO (PPP)

Debido a que los protocolos de Nivel 2 dependen principalmente de las funciones originalmente especificadas para PPP, vale la pena examinar este protocolo más de cerca. PPP se diseñó para enviar datos a través de conexiones de marcación o de punto a punto dedicadas. PPP encapsula paquetes de IP, IPX y NetBEUI dentro de las tramas del PPP y luego transmite los paquetes encapsulados del PPP a través de un enlace punto a punto. El PPP se utiliza entre un cliente de marcación y un NAS.

Existen cuatro fases distintivas de *negociación* en una sesión de marcación del PPP. Cada una de estas cuatro fases debe completarse de manera exitosa antes de que la conexión del PPP esté lista para transferir los datos del usuario:

Fase 1: Establecer el enlace del PPP: Utiliza el Protocolo de control de enlace (LCP) para establecer, mantener y terminar la conexión física.

Fase 2: Autenticar al usuario: La PC cliente presenta las credenciales del usuario al servidor de acceso remoto. Un esquema seguro de autenticación proporciona protección contra ataques de reproducción y personificación de clientes remotos. Un ataque de reproducción ocurre cuando un tercero monitorea una conexión exitosa y utiliza paquetes capturados para reproducir la

respuesta del cliente remoto, de tal manera que pueda lograr una conexión autenticada. La personificación del cliente remoto ocurre cuando un tercero se apropia de una conexión autenticada. La mayoría de las implementaciones del PPP proporcionan métodos limitados de Autenticación, típicamente el Protocolo de autenticación de contraseña (PAP), el Protocolo de Autenticación de Saludo Challenge (CHAP) y Microsoft Challenge Handshake Authentication Protocol (MSCHAP).

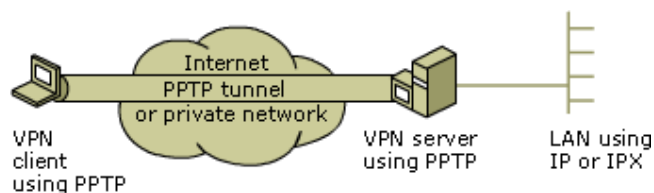
Fase 3: Control de rellamado del PPP: La implementación de Microsoft del PPP incluye una Fase opcional de control de rellamado. Esta fase utiliza el Protocolo de control de rellamado (CBCP) inmediatamente después de la fase de autenticación. Si se configura para rellamado, después de la autenticación, se desconectan tanto el cliente remoto como el NAS.

Fase 4: Invocar los protocolos a nivel de red: Una vez que se hayan terminado las fases previas, PPP invoca los distintos Protocolos de Control de Red (NCPs) que se seleccionaron durante la fase de establecimiento de enlace (Fase1) para configurar los protocolos que utiliza el cliente remoto. Por ejemplo, durante esta fase el Protocolo de Control de IP (IPCP) puede asignar una dirección dinámica a un usuario de marcación.

Fase de transferencia de datos: Una vez que se han terminado las cuatro fases de negociación, PPP empieza a transferir datos hacia y desde los dos iguales. Cada paquete de datos transmitido se envuelve en un encabezado del PPP el cual quita el sistema receptor. Si se seleccionó la compresión de datos en la fase 1 y se negoció en la fase 4, los datos se comprimirán antes de la transmisión. Si se seleccionaron y se negociaron de manera similar la encriptación de datos, los datos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

5.1. PPTP (POINT – TO - POINT TUNNELING PROTOCOL)

Protocolo de túnel de punto a punto (PPTP): El PPTP es un protocolo de Nivel 2 que encapsula las tramas del PPP en datagramas del IP para transmisión sobre una red IP, como la de Internet. El PPTP se documenta en el RFC preliminar, "Protocolo de túnel de punto a punto" (pptp-draft-ietf-ppext-pptp-02.txt). Este proyecto se presentó ante el IETF en junio de 1996 por parte de las compañías miembros del Foro PPTP incluyendo Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics y US Robotics (ahora 3Com). PPTP agrega un nuevo nivel de seguridad mejorada y comunicaciones multiprotocolo a través de Internet. Si se utiliza el nuevo Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol) con métodos de autenticación seguros como los certificados, la transferencia de datos a través de una conexión VPN con PPTP es tan segura como en una LAN de un sitio corporativo.



Protocolo de túnel de punto a punto (PPTP) utiliza una conexión TCP para mantenimiento del túnel y tramas del PPP encapsuladas de Encapsulación de Enrutamiento Genérico (GRE) para datos de túnel (puerto 1723). Se pueden encriptar y/o comprimir las cargas útiles de las tramas del PPP encapsulado. La Figura 5.1. muestra la forma en que se ensambla el paquete del PPTP antes de la transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño de la trama final muestra la encapsulación para un cliente de marcación (controlador de dispositivo PPP).

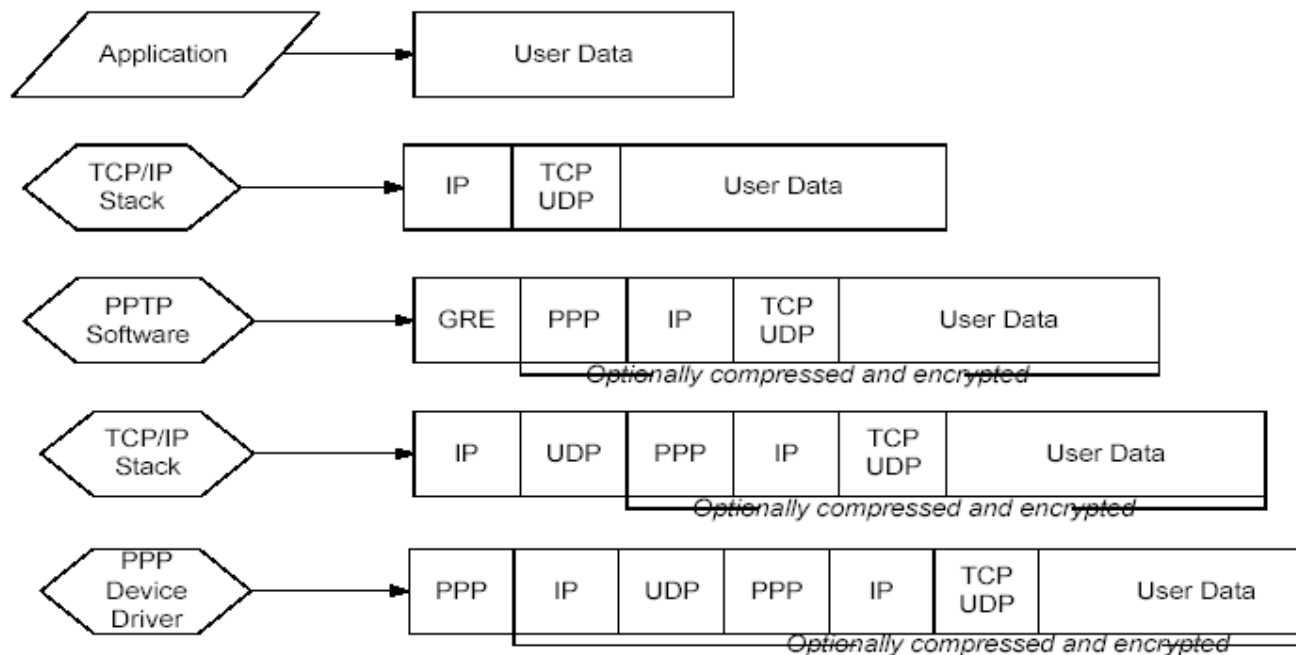


Figura 5.1.

Está especialmente diseñado para las aplicaciones de acceso remoto de VPN, pero también soporta las otras aplicaciones de VPN. PPTP soporta encriptación de datos y la compresión de estos paquetes. Además usa una forma de GRE (General Routing Encapsulation, Protocolo Genérico de Encapsulación). En el entorno de un acceso remoto VPN usando PPTP a través de Internet, los túneles VPN son creados en dos pasos:

1. El cliente PPTP conecta a su ISP usando PPP dial - up (mediante modem tradicional o ISDN).
2. Por medio del dispositivo intermedio ya mencionado, PPTP crea una conexión de control TCP entre el cliente VPN y el servidor VPN para establecer un túnel (PPTP usa el puerto 1723 para estas conexiones).

Por otro lado, PPTP soporta conexiones VPN a través de una LAN, por lo que no es necesario conectar a un ISP. Los túneles son creados directamente. Una vez que el túnel VPN está establecido, PPTP soporta dos tipos de flujo de información:

1. Mensajes de control para manejar y/o eliminar la conexión VPN. Este tipo de mensajes pasan directamente entre el cliente VPN y el servidor.
2. Paquetes de datos que pasan a través del túnel, hacia o desde el cliente VPN.

Volviendo al tema del control de conexión en PPTP, una vez que la conexión TCP está establecida, PPTP utiliza una serie de mensajes de control para mantener la conexión VPN. Algunos de estos mensajes son los siguientes:

1. *StartControlConnectionRequest*: Inicia la configuración de la sesión VPN; puede ser enviado tanto por el cliente como por el servidor.
2. *StartControlConnectionReply*: Enviado en respuesta a (1). Contiene información que indica el éxito o el fracaso de la operación de configuración y del número de versión del protocolo.
3. *StopControlConnectionRequest*: Petición de cerrar la conexión de control.

En cuanto a la seguridad en PPTP, soporta autenticación (usa para ello protocolos basados en PPP, tales como EAP, CHAP y PAP), encriptación y filtrado de paquetes. PPTP depende de la funcionalidad de PPP para autenticar a los usuarios y mantener la conexión remota dial up y para encapsular y encriptar los paquetes IP, IPX o NetBEUI pero se encarga directamente del mantenimiento del túnel VPN y de transmitir los datos a través del túnel. PPTP además tiene algunas características adicionales de seguridad aparte de la que provee PPP. La popularidad de

PPTP se debe en gran parte a Microsoft, ya que los clientes PPTP están disponibles en Windows.

VENTAJAS

Coste y Escalabilidad: Como ya se ha comentado, tienen un bajo coste ya que no hacen uso de líneas dedicadas de larga distancia y sólo se hace necesario una conexión dedicada a un proveedor de servicios. Esta conexión podría ser a través de una línea dedicada de corta distancia (mucho más barata que las de larga distancia) o simplemente una conexión de banda ancha como por ejemplo DSL. Otra forma de reducir costes con VPN se da en la opción de acceso remoto; en este caso y por norma general, el cliente VPN no tiene que hacer una llamada de larga distancia al punto de acceso del proveedor de servicios, con una llamada local bastaría. Por otro lado, el coste es bajo ya que son los proveedores del servicio los que cargan con el coste de acceso y no las compañías. A medida que una compañía crece, si utilizase líneas dedicadas el número de estas se vería incrementado al mismo tiempo (según las necesidades de la compañía) con el consiguiente aumento de los gastos. Con VPN, y utilizando Internet, se solucionaría este problema ya que se usa la red ya disponible pudiendo acceder con ella, además, a puntos donde las líneas dedicadas no podrían llegar.

DESVENTAJAS

Incompatibilidad: Este protocolo suele utilizar más de un estándar para la autenticación y la encriptación, por lo que, por ejemplo, dos clientes PPTP pueden ser incompatibles entre ellos si encriptan los datos de manera diferente.

Vulnerabilidad: La seguridad de PPTP ha sido completamente rota y las instalaciones con PPTP deberían ser retiradas o actualizadas a otra tecnología de VPN. La utilidad ASLEAP puede obtener claves de sesiones PPTP y descifrar el tráfico de la VPN. Los ataques a PPTP no pueden ser detectados por el cliente o el servidor porque el exploit es pasivo. Aunque tengan estos puntos en contra se puede implementar PPTP con EAP-TLS para soportar certificados de seguridad.

ACTUALIZACIÓN DE PPTP

La actualización de PPTP para las plataformas Microsoft viene por parte de L2TP o IPSec. Su adopción es lenta porque PPTP es fácil de configurar, mientras L2TP requiere certificados de clave pública, e IPSec es complejo y poco soportado por plataformas antiguas como Windows 98 y Windows Me.

5.1.2. TÚNELES

PPTP permite a los usuarios y a las ISPs crear varios tipos de túneles, basados en la capacidad del computador del usuario final y en el soporte del ISP para implementar PPTP. Los túneles se pueden dividir en dos clases, voluntarios y permanentes.

Túneles voluntarios son creados por requerimiento de un usuario y para un uso específico. Los *túneles permanentes* son creados automáticamente sin la acción del usuario y no se le permite escoger ningún tipo de privilegio.

En los túneles voluntarios, la configuración del mismo depende del usuario final; cuando se usan túneles de este tipo, el usuario puede simultáneamente acceder a Internet y abrir un túnel seguro hacia el servidor PPTP. En este caso el cliente PPTP reside en el computador del usuario. Los túneles voluntarios proveen más privacidad e integridad de los datos que un túnel permanente.

Túneles permanentes son creados sin el consentimiento del usuario, por lo tanto, son transparentes para el mismo. El cliente PPTP reside en el servidor de acceso remoto del ISP al

que se conectan los usuarios finales. Todo el tráfico originado desde el computador del usuario final es reenviado por el RAS sobre el túnel PPTP. En este caso la conexión del usuario se limita sólo a la utilización del túnel PPTP, no hay acceso a la red pública (Internet) sobre la cual se establece el túnel. Un túnel permanente PPTP permite que múltiples conexiones sean transportadas sobre el mismo túnel.

5.2. L2TP (LAYER 2 TUNNELING PROTOCOL)

L2TP [REF5.4] fue creado como el sucesor de PPTP y L2F. Las dos compañías abanderadas de cada uno de estos protocolos, Microsoft por PPTP y Cisco por L2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 y así lograr su estandarización por parte de la IETF.

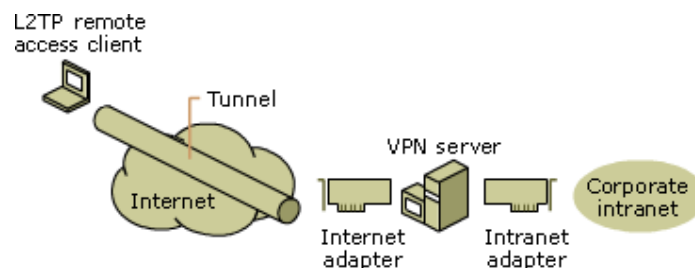
Como PPTP, L2F fue diseñado como un protocolo de entunelamiento usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el entunelamiento de este último no depende de IP y GRE, permitiéndole trabajar con otros medios físicos por ejemplo Frame Relay. Paralelamente al diseño de PPTP, L2F utilizó PPP para autenticación de usuarios accediendo vía telefónica conmutada, pero también incluyó soporte para TACACS+ y Radius. Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión. Hay dos niveles de autenticación del usuario: primero, por el ISP antes de crear el túnel; segundo, cuando la conexión está configurada y la autenticación la realiza el gateway corporativo.

Todas las anteriores características de L2F han sido transportadas a L2TP. Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de Internet a un sitio destino. Sin embargo, como se ha mencionado anteriormente, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo transporte sobre una amplia variedad de medios de empaquetamiento tales como X.25, Frame Relay y ATM.

Dado que L2TP es un protocolo de capa 2, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI.

Puesto que L2TP usa PPTP en enlaces conmutados, incluye mecanismos de autenticación nativos de PPP como PAP y CHAP.

Microsoft incluye L2TP a partir del sistema operativo Windows 2000, ya que las mejoras de L2TP con respecto a PPTP saltan a la vista.



El L2TP sobre las redes IP utiliza UDP y una serie de mensajes del L2TP para el mantenimiento del túnel. El L2TP también utiliza UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel. Se pueden encriptar y/o comprimir las cargas útiles de las tramas PPP encapsuladas. La Figura 5.2 muestra la forma en que se ensambla un paquete L2TP antes de su transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño final de trama muestra la encapsulación para un cliente de marcación (controlador de dispositivos PPP). La encapsulación supone el L2TP sobre IP.

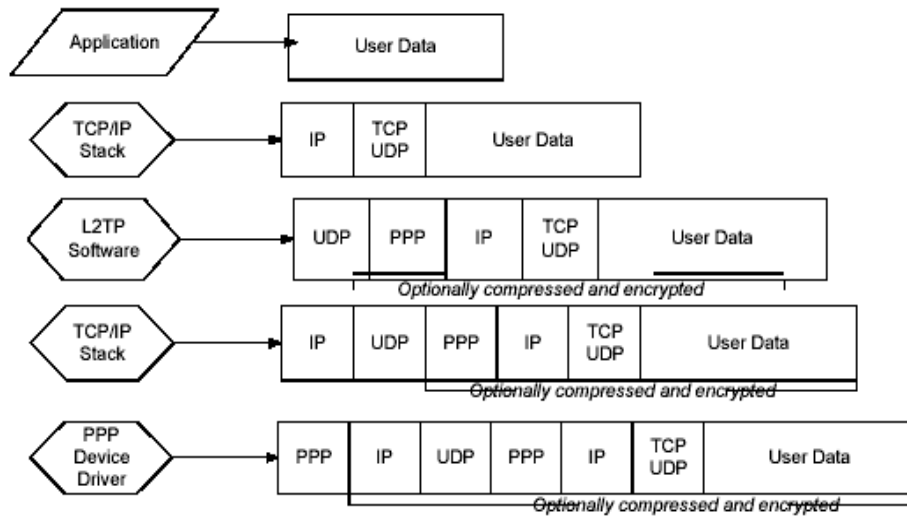


Figura 5.2.

5.2.1. COMPONENTES BÁSICOS DE UN TÚNEL L2TP

5.2.1.1. CONCENTRADOR DE ACCESO L2TP (LAC)

Un LAC es un nodo que se encuentra en un punto extremo de un túnel L2TP. El LAC se encuentra entre un LNS y un sistema remoto y reenvía los paquetes a y desde cada uno. Los paquetes enviados desde el LAC hasta el LNS van tunelizados. En algunas ocasiones el sistema remoto actúa como un LAC, esto se presenta cuando se cuenta con un software cliente LAC.

5.2.1.2. SERVIDOR DE RED L2TP (LNS)

Un LNS es un nodo que se encuentra en un punto extremo de un túnel L2TP y que interactúa con el LAC, o punto final opuesto. El LNS es el punto lógico de terminación de una sesión PPP que está siendo tunelizada desde un sistema remoto por el LAC.

5.2.1.3. TÚNEL

Un Túnel existe entre una pareja LAC-LNS. El túnel consiste de una conexión de control y de ninguna o más sesiones L2TP. El túnel transporta datagramas PPP encapsulados y mensajes de control entre el LAC y el LNS.

5.2.2. TOPOLOGÍA DE L2TP

La figura 5.7 describe un escenario típico L2TP. El objetivo es tunelizar tramas PPTP entre un sistema remoto o un cliente LAC y un LNS localizado en la LAN corporativa.

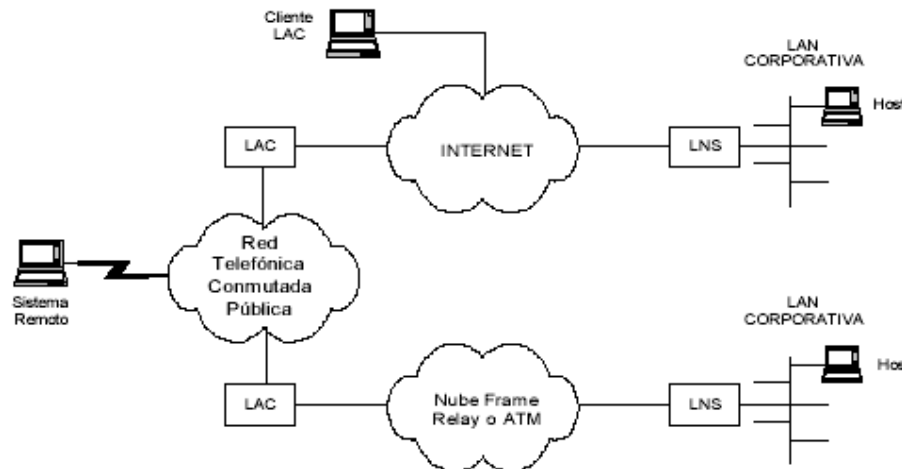


Figura 5.7 Distintos escenarios de túneles L2TP.

El sistema remoto inicia una conexión PPP a través de la red de telefonía pública conmutada a un LAC. El LAC luego tuneliza la conexión PPP a través de Internet o una nube Frame Relay o ATM a un LNS por donde accede a la LAN remota corporativa. La dirección del sistema remoto es dada desde la LAN corporativa por medio de una negociación PPP NCP. La autenticación, autorización y accounting puede ser provista por el dominio de la red corporativa remota como si el usuario estuviera conectado a un servidor de acceso de la red directamente.

5.3. IPSEC

En IPv4 no se desarrollaron mecanismos de seguridad inherentes al protocolo, por tanto, protocolos y procedimientos adicionales a IPv4 fueron necesarios para brindar servicios de seguridad a los datos. IPsec [REF5.5] es un conjunto de protocolos diseñados para proveer seguridad basada en criptografía robusta para IPv4 e IPv6, de hecho IPsec está incluido en IPv6. Entre los servicios de seguridad definidos en IPsec se encuentran, control de acceso, integridad de datos, autenticación del origen de los datos, protección anti - repetición y confidencialidad en los datos. Entre las ventajas de IPsec están la modularidad del protocolo, ya que no depende de un algoritmo criptográfico específico.

5.3.1. COMPONENTES DE IPSEC

IPsec está compuesto por tres componentes básicos: los protocolos de seguridad (AH y ESP), las asociaciones de seguridad (SAs) y las bases de datos de seguridad; cada uno de los cuales, trabaja de la mano con los demás y ninguno le resta importancia al otro.

5.3.1.1. PROTOCOLOS DE SEGURIDAD

IPsec es un conjunto de protocolos que provee varios servicios de seguridad. Esos servicios de seguridad trabajan gracias a dos protocolos, el Authentication Header (AH) [REF5.6] y el Encapsulating Security Payload (ESP) [REF5.7], y también al uso de protocolos y procedimientos para el manejo de llaves criptográficas tales como IKE (Internet Key Exchange Protocol) [REF5.8].

El éxito de una implementación IPsec depende en gran medida de una adecuada elección del protocolo de seguridad y de la forma como se intercambian las llaves criptográficas.

AH es un protocolo que añade una nueva cabecera justo después de la cabecera IP original. AH provee autenticación del origen de los datos e integridad de los mismos, también provee

integridad parcial para prevenir ataques de repetición. Este protocolo es apropiado cuando se requiere autenticación en vez de confidencialidad.

ESP provee confidencialidad para el tráfico IP, al igual que autenticación tal cual como lo hace AH, pero solo uno de estos servicios puede ser proporcionado por ESP al mismo tiempo. IKE es un protocolo que permite a dos entidades IPsec negociar dinámicamente sus servicios de seguridad y sus llaves de cifrado al igual que la autenticación de la sesión misma.

5.3.1.2. ASOCIACIONES DE SEGURIDAD (SAS)

El concepto de Asociación de Seguridad (SA) es clave en IPsec. Una SA define las medidas de seguridad que deberían ser aplicadas a los paquetes IP basados en quién los envía, hacia dónde van y qué tipo de carga útil ellos transportan. El conjunto de servicios de seguridad ofrecidos por una SA dependen de los protocolos de seguridad y del modo en el cual ellos operan definidos por la SA misma. La figura 5.16 muestra los dos modos en los cuales un protocolo de seguridad puede operar: transporte y túnel; la diferencia radica en la manera como cada uno de ellos altera el paquete IP original. El modo de transporte es diseñado para proteger los protocolos de capas superiores tales como TCP y UDP. En modo túnel, el paquete IP original se convierte en la carga útil de un nuevo paquete IP. Esto le permite al paquete IP inicial, "ocultar" su cabecera IP para que sea encriptada, considerando que el paquete IP externo sirve de guía a los datos a través de la red.

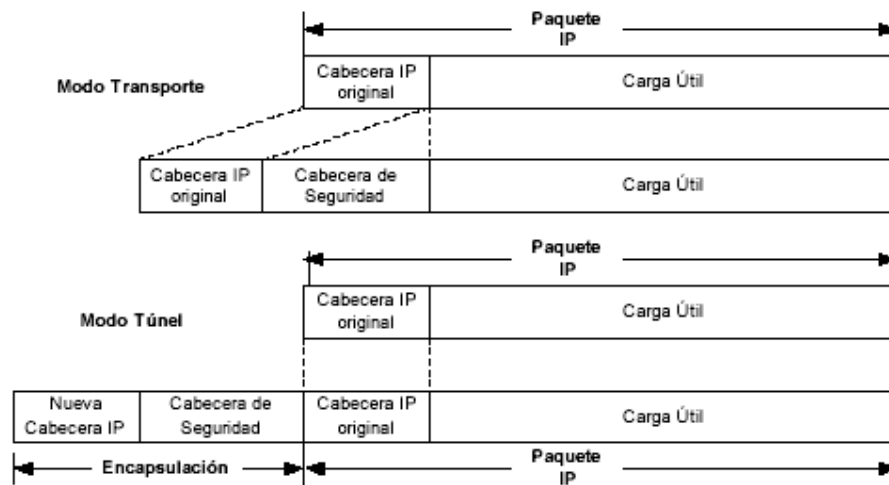


Figura 5.16 Estructura del paquete IP en modo de Transporte y Túnel

Las SAs pueden ser negociadas entre dos entidades IPsec dinámicamente, para lo cual se basan en políticas de seguridad dadas por el administrador del sistema o estáticamente especificadas por el administrador directamente.

Una SA es únicamente identificada por tres parámetros: una dirección IP de destino, un identificador del protocolo de seguridad y un índice del parámetro de seguridad (SPI). La dirección IP de destino es aquella por la cual se identifica el punto final de la SA, el SPI es un número de 32 bits usualmente escogido por el punto final de destino de la SA y que sólo tiene significado local dentro de ese punto destino. El identificador del protocolo de seguridad es un número con el cual se define cada uno de ellos, 51 para AH o 50 para ESP.

Como se nota, la dirección IP del origen no se usa para definir una SA, esto dado que una SA se define entre dos host o gateways para datos enviados en una sola dirección, de aquí que, si dos dispositivos necesitan intercambiar información en ambas direcciones usando IPsec, requerirán de dos SAs, una para cada sentido.

En modo de transporte, la cabecera IP original se mantiene intacta y una cabecera de seguridad es colocada entre la cabecera IP misma y su carga útil. La cabecera IP original es modificada para que el receptor del paquete entienda que antes de la carga útil se encuentra una cabecera de seguridad. En modo túnel, el paquete IP original se convierte en la carga útil de un paquete IP encapsulado. La cabecera IP nueva le indica al receptor del paquete que una cabecera de seguridad se encuentra a continuación de ella.

Varias SAs pueden ser aplicadas en serie para incrementar los servicios de seguridad del tráfico IP. En estas situaciones una SA es encerrada por otra. El protocolo IPSec define dos formas: transporte adyacente y túneles iterados.

En *transporte adyacente* se usan tanto AH como ESP y ellos son aplicados por el mismo host. Es de anotar que trabajar con adyacencias de transporte AH sobre AH o ESP sobre ESP no trae beneficios adicionales. Lo deseable en este caso es aplicar AH después de ESP.

En *túneles iterados*, se puede combina cualquier cantidad de túneles con lo cual se logra proveer de capas anidadas de seguridad. Los puntos finales del túnel pueden estar en la misma o en diferentes locaciones. Por ejemplo, un túnel host – to - host puede ser entunelado por un túnel gateway – to - gateway; y un túnel gateway – to - gateway puede de nuevo ser entunelado por otro túnel gateway – to - gateway.

5.3.1.3. BASES DE DATOS DE SEGURIDAD

IPSec trabaja con dos bases de datos de seguridad, en una se encuentran las políticas de seguridad y en la otra las asociaciones de seguridad, SPD (Security Policy Database) y SAD (Security Association Database) respectivamente. El administrador de políticas define un conjunto de servicios de seguridad para ser aplicados al tráfico IP tanto entrante como saliente. Esas políticas son guardadas en las SPDs y son usadas por las SAs cuando éstas se crean. Todas las SAs son registradas en la SAD.

5.3.1.3.1. BASES DE DATOS DE ASOCIACIONES DE SEGURIDAD (SAD)

La base de datos de asociaciones de seguridad almacenan todos los parámetros concernientes a las SAs, cada una de ellas tiene una entrada en la SAD donde se especifican todos los parámetros necesarios para que IPSec realice el procesamiento de paquetes IP que son gobernados por esa SA. Entre los parámetros que se encuentran en una SAD se tienen:

- El índice de parámetro de seguridad.
- El protocolo a ser usado por la SA (ESP o AH).
- El modo en el cual el protocolo es operado (túnel o transporte).
- Un contador numérico secuencial.
- La dirección IP fuente y destino de la SA.
- El algoritmo de autenticación y la llave de autenticación usadas.
- El algoritmo de cifrado y su llave.
- El tiempo de vida de las llaves de autenticación y de cifrado.
- El tiempo de vida de la SA.

Para el procesamiento de los paquetes IP entrantes una SA apropiada es encontrada en la SAD tal que concuerde con los siguientes tres valores: la dirección IP destino, el tipo de protocolo IPSec y el SPI. La dirección IP de destino y el tipo de protocolo IPSec son obtenidos de la cabecera IP y el SPI se obtiene de la cabecera AH o ESP. Si una SA es encontrada para el paquete IP entrante en mención, éste es procesado de acuerdo a los servicios de seguridad especificados. Luego se aplican al paquete todas las reglas descritas en la SPD para la SA que lo gobierna.

Para el procesamiento de paquetes IP salientes, primero se aplica el procesamiento relacionado con la SPD. Si se encuentra una política para el paquete de salida que especifique que un procesamiento IPSec es necesario, la SAD es buscada para determinar si una asociación de

seguridad ha sido previamente establecida. Si una entrada es encontrada, el paquete es procesado de acuerdo a la SA. Si por lo contrario no se encuentra ninguna entrada para este paquete una nueva SA es negociada y luego guardada en la SAD.

5.3.1.3.2. BASE DE DATOS DE POLÍTICAS DE SEGURIDAD

Una base de datos de políticas de seguridad es una lista ordenada de políticas de seguridad a ser aplicadas a los paquetes IP. Dichas políticas son en general reglas que especifican como los paquetes IP deben ser procesados. La SPD es mantenida por el administrador del dispositivo IPSec.

Una entrada SPD tiene dos componentes: un juego de selectores y una acción. Los selectores clasifican un paquete IP sobre una acción. Un selector es un parámetro y el valor o rango de valores para éste parámetro. Los parámetros generalmente se encuentran dentro de una de éstas dos categorías:

- Aquellos que se encuentran dentro de un paquete IP, tales como, la dirección IP, número de protocolo y números de puertos de capas superiores.
- Aquellos que se derivan de la credencial de autenticación de una entidad de comunicación, tales como, una dirección de correo o un nombre distinguido DN (Distinguished Names) en certificados digitales. Diferentes operadores lógicos como AND, OR y NOT pueden ser aplicados a las políticas para combinar más de un selector.

Cuando un paquete IP contiene valores que concuerdan con los especificados por algún selector de una entrada, la acción que se especifica en dicha entrada es aplicada al paquete. Hay tres opciones: aplicar el servicio de seguridad IPSec, descartar el paquete IP o permitir que el paquete IP omita el procesamiento IPSec.

La figura 5.17 muestra una entrada en una base de datos de políticas de seguridad para un paquete entrante y saliente, claramente se notan las partes que componen un selector como lo son los parámetros y su correspondiente valor; al frente se encuentra la acción que IPSec tomaría si los paquetes IP concuerdan con los valores de los selectores.

Entrantes	Selectores	Acción
	dirección_IP fuente = 10.0.0.92	IPSec (ESP, 3DES, HMAC-SHA-1)
	AND dirección de e-mail fuente = financiera@telesat.com.co	
	nombre_distinguido fuente = Andrés Gómez	IPSec (ESP, 3DES, HMAC-MD5)
	dirección_IP destino = 192.89.0.169	Omitir

Salientes	Selectores	Acción
	dirección_IP destino = 10.0.0.92	IPSec (ESP, 3DES, HMAC-SHA-1)
	nombre_distinguido destino = Andrés Gómez	IPSec (ESP, 3DES, HMAC-MD5)
	dirección_IP fuente = 192.89.0.169	Omitir

Figura 5.17 Ejemplos de entradas en una base de datos de políticas de seguridad

Es posible que un paquete IP concuerde con más de una entrada en la SPD. Por esto, se debe tener en cuenta el orden de las entradas en una SPD, ya que la primera concordancia será la política seleccionada. En adición, una política por defecto debe ser aplicada para el nodo y ésta se aplica cuando el paquete IP no concuerda con ninguna de las entradas de una SPD. Usualmente, esta política por defecto es descartar el paquete IP.

La SPD trata al tráfico saliente y entrante de manera separada, esto es, que se deben aplicar políticas de seguridad distintivas de entrada y de salida por cada interfaz de red. Cuando un paquete IP llega a una interfaz de red, IPSec primero busca en la SAD la apropiada SA, cuando

la encuentra, el sistema inicia los procesos SAD y SPD. Después del procesamiento SPD, el sistema reenvía el paquete al siguiente salto o le aplica procedimientos adicionales tales como las reglas de algún firewall. El procesamiento PSD se realiza primero en paquetes salientes. Si la entrada SPD que concuerda especifica que un procesamiento IPsec es necesario, la SAD es consultada para determinar si una SA ha sido previamente establecida, en caso contrario se negocia una nueva SA para el paquete. Dado que los procesos SPD son realizados tanto para los paquetes IP salientes como entrantes, este procedimiento puede alterar negativamente el desempeño de un dispositivo IPsec. De hecho, el procesamiento SPD es el cuello de botella más representativo en una implementación IPsec.

5.3.2. AUTHENTICATION HEADER (AH)

El protocolo de cabecera de autenticación AH es usado para propósitos de autenticación de la carga útil IP a nivel de paquete por paquete, esto es autenticación de la integridad de los datos y de la fuente de los mismos. Como el término autenticación indica, el protocolo AH se asegura que los datos entregados dentro del paquete IP son auténticos, es decir, que han arribado a su destino sin ninguna modificación. AH también provee de un mecanismo de protección opcional anti - repetición de paquetes IP. Sin embargo, AH no protege la confidencialidad de los datos, es decir, no recurre a ningún tipo de cifrado de los mismos. El protocolo AH define cómo un paquete IP sin protección es convertido en uno nuevo que contiene información adicional y que brinda autenticación. El elemento fundamental usado por AH es una cabecera de autenticación como se muestra en la figura 5.18.

El nuevo paquete IP es formado insertando la cabecera de autenticación, bien sea, después de la nueva cabecera IP o después de la cabecera IP original modificada según sea el modo en el cual trabaje la SA; estos dos modos son: *transporte* y *túnel*.

Cuando la cabecera de autenticación es insertada, la cabecera IP que la precede deberá indicar que la próxima cabecera que se encuentra es la cabecera de autenticación y no la carga útil del paquete original. La cabecera IP realiza esta acción colocando el campo Protocolo en el valor 51 (valor de protocolo para AH).

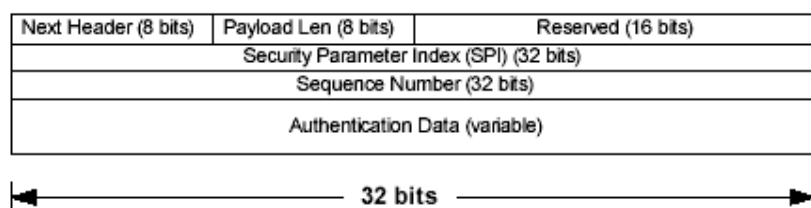


Figura 5.18 Formato de la cabecera de autenticación

La cabecera de autenticación contiene seis campos:

- *Next Header*: El campo Next Header es un campo de ocho bits que identifica el tipo de protocolo de la carga útil del paquete IP original.
- *Payload Len*: El campo Payload Len es un campo de ocho bits que especifica la longitud de la cabecera de autenticación (no confundir con la cabecera original del paquete IP).
- *Reserved*: El campo Reserved se encuentra reservado para uso futuro, actualmente debe ser puesto en 0.
- *Security Parameter Index*: El campo Security Parameter Index es un número arbitrario de 32 bits. Este valor es usado junto con la dirección IP de destino y el tipo de protocolo IPsec (en este caso, AH) únicamente para identificar la SA para este paquete IP. El valor SPI es escogido por el sistema destino cuando la SA es establecida.
- *Sequence Number*: El campo Sequence Number es un campo de 32 bits que mantiene un incremento monótonico de la secuencia de paquetes IPsec. Comienza en 0 cuando la SA

es establecida y se incrementa por cada paquete IP saliente que usa esta SA. Este campo se usa como un mecanismo de protección anti - repetición.

- *Authentication Data*: El campo Authentication Data es un campo de longitud variable que contiene el valor de chequeo de integridad ICV (Integrity Check Value) para este paquete IP. El ICV es calculado con el algoritmo seleccionado por la SA y es usado por el receptor para verificar la integridad del paquete IP entrante. Los algoritmos por defecto requeridos por AH para trabajar son HMAC con MD5 y SHA-1.

Hay que tener en cuenta, que la autenticación no puede ser aplicada sobre la cabecera entera del paquete IP, ya que algunos campos de la cabecera IP original cambian durante el tránsito por Internet. Esos campos son llamados Campos Mutables, y son:

- Type of Service (TOS).
- Fragment Offset.
- Fragmentation Flags.
- Time To Live (TTL).
- Header Checksum.

Para consultar más sobre estos campos de una cabecera de un paquete IP puede verse la RFC2402. Para realizar el proceso de autenticación, el emisor calcula el ICV y lo ubica en el campo Authentication Data. El ICV es un valor hash computado sobre todos los campos que la autenticación incluye. La llave secreta es negociada durante el establecimiento de la SA. La autenticación de un paquete recibido es verificada cuando el receptor calcula el valor hash y lo compara con el ICV del paquete entrante. Si el paquete IP no es autenticado exitosamente entonces es descartado.

6. COMPARATIVA ENTRE DISTINTAS TECNOLOGÍAS DE TUNELAMIENTO

En la Figura 6.1 se puede apreciar un cuadro comparativo entre tecnologías de tunelamiento.

<i>Tecnología</i>	Puntos fuertes	Puntos debiles	En desarrollo
<i>IPSEC</i>	<ul style="list-style-type: none"> • Opera independiente de las aplicaciones de niveles superiores • Subconjunto de IPv6 • Ocultación de direcciones de red sin emplear NAT • Acoplamiento con las técnicas usuarios remotos. 	<ul style="list-style-type: none"> • No proporciona la gestión de usuarios • Interoperabilidad entre los fabricantes. • No estandarizado 	<ul style="list-style-type: none"> • Estandarización de todas las facetas de PKI, incluyendo los protocolos de intercambio de certificados y el formato de éstos. • El IETF está en su desarrollo
<i>PPTP</i>	<ul style="list-style-type: none"> • Soporta tunneling extremo a extremo y entre servidores. • Posibilidad de valor añadido para el acceso remoto. • Proporciona una capacidad multiprotocolo. • Empleo de encriptación RSA RC-4 	<ul style="list-style-type: none"> • No proporciona encriptación de datos para los servidores de acceso remoto • Precisa un servidor NT como terminador del túnel. 	<ul style="list-style-type: none"> • Integración con IPsec
<i>L2TP</i>	<ul style="list-style-type: none"> • Combina L2F y PPTP. • Necesidad de únicamente una red de paquetes para operar bajo X.25 y Frame Relay. 	<ul style="list-style-type: none"> • Aún no implementado 	<ul style="list-style-type: none"> • Estandarización y operación en proceso • Será adoptado por los fabricantes para el acceso remoto una

Figura 6.1. Comparativa entre tecnologías de tunelamiento.

7. CONCEPTOS DE LAS VPN DINÁMICAS

Internet no fue diseñada, originalmente, para el ámbito de los negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios. Entonces, ¿cómo establecer y mantener la confianza en un entorno el cual fue diseñado desde el comienzo para permitir un acceso libre a la información?, es decir, ¿cómo conseguir seguridad en una intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperabilidad y facilidad de uso?.

La respuesta apropiada se encuentra en la utilización de VPNs Dinámicas. A diferencia de una VPN tradicional, una VPN Dinámica proporciona, además de un alto nivel de seguridad a ambos extremos, una flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs Dinámicas pueden ofrecer esta flexibilidad ya que están basadas en una única arquitectura. Además, una VPN Dinámica proporciona más recursos y servicios a una Intranet, para hacer mayor uso de los recursos de la información.

Alguna de las características que se proporciona son las siguientes:

- Proporciona una seguridad importante para la empresa.

alcanzar su objetivo. Una vez atravesado el firewall, la petición circula a lo largo del pasillo Internet hasta alcanzar el destino.

El mensaje recibido debe pasar controles de seguridad: El mensaje se transfiere al servidor. El servidor conoce la identidad del usuario cliente cuando recibe la petición.

Durante la petición, se verifican los derechos de acceso de los usuarios: En una VPN dinámica, el sistema debe poder restringir qué usuarios pueden y no pueden acceder a la misma. El servidor debe determinar si el usuario tiene derechos para realizar la petición de información. Esto lo hace usando mecanismos de control, alojados en el Servidor de Control de Acceso. De este modo, incluso si un usuario presenta un certificado válido, puede ser que se le deniegue el acceso basándose en otros criterios.

La petición de información es devuelta por Internet, previamente asegurada: El servidor de información encripta la información y opcionalmente la certifica. Las claves establecidas durante los pasos de autenticación mutua se usan para encriptar y desencriptar el mensaje. De esta forma, un usuario tiene su documento asegurado.

8. CONCLUSIONES

Las redes VPN proporcionan principalmente dos **ventajas**:

- *Bajo coste de una VPN:* Una forma de reducir coste en las VPN es eliminando la necesidad de largas líneas de coste elevado. Con las VPN, una organización sólo necesita una conexión relativamente pequeña al proveedor del servicio. Otra forma de reducir costes es disminuir la carga de teléfono para accesos remotos. Los clientes VPN sólo necesitan llamar al proveedor del servicio más cercano, que en la mayoría de los casos será una llamada local.
- *Escalabilidad de las VPNs:* Las redes VPN evitan el problema que existía en el pasado al aumentar las redes de una determinada compañía, gracias a Internet. Internet simplemente deriva en accesos distribuidos geográficamente.

Hay dos **aplicaciones** principales para las redes VPN:

- *Teletrabajo:* Es la solución ideal, por su efectividad y sus bajos costes, para aquellas organizaciones que necesiten que sus empleados accedan a la red corporativa, independientemente de su ubicación geográfica.
- *VPN Empresa:* Solución de conectividad entre sucursales de la empresa o entre la empresa y sus socios, proveedores, etc. Gracias a su flexibilidad se adapta al tamaño y necesidades de la organización.

Las redes VPN presentan cuatro **inconvenientes**:

- Las redes VPN requieren un conocimiento en profundidad de la seguridad en las redes públicas y tomar precauciones en su desarrollo.
- Las redes VPN dependen de un área externa a la organización, Internet en particular, y por lo tanto dependen de factores externos al control de la organización.
- Las diferentes tecnologías de VPN podrían no trabajar bien juntas.
- Las redes VPN necesitan diferentes protocolos que los de IP.

Se estima que una solución VPN para una determinada empresa puede reducir sus costes entre un 30% y un 50% comparada con las conexiones punto a punto.

8. BIBLIOGRAFÍA

Documentos

- Microsoft – “Seguridad de red privada virtual de Microsoft” (Documento Estratégico).
<http://www.pdf-search-engine.com/pptp-pdf.html>
- Microsoft – “Windows NT Server”.
<http://www.abcdatos.com/tutoriales/sistemasoperativos/windowsnt20002003.html>
- Fernando Andrés Arevalo Jiménez – “Como Escoger e Implementar una VPN”.
http://www.univalle.edu.co/~telecomunicaciones/trabajos_de_grado/informes/tg_FernandoArevalo.pdf

Páginas Web

<http://www.microsoft.com>

Página Web oficial de Microsoft Corporation. Fuente de información sobre los protocolos PPTP y L2TP sobre computadores instalados con sistemas operativos Windows NT, Windows 2000 Server, Windows XP y Windows 2003 Server.

<http://www.cisco.com>

Página Web oficial de Cisco Systems. Compañía mundial líder en la fabricación de equipos para Internetworking. Dentro de sus productos cuenta con equipos concentradores de túneles L2F, L2TP y IPSec. Desarrolla sistemas operativos (IOS) para sus enrutadores y switches que capacitan a los mismos para crear y terminar túneles.

<http://www.cybercursos.net>

Sitio Web donde se pueden descargar documentos referentes a tecnologías de redes y otras.

<http://www.ovislinkcorp.es>

Sitio Oficial de la empresa Ovislink fabricante de dispositivos de red.

<http://www.wikipedia.org>

Enciclopedia libre de Internet.