UNIVERSIDAD DEL AZUAY

FACULTAD DE ADMINISTRACION

ESCUELA DE INGENIERIA DE SISTEMAS

TEMA:

"CONFIGURACIÓN DE UNA RED PRIVADA VIRTUAL (VPN) PARA LA TRASMISIÓN DE DATOS DE UNA PC CLIENTE (WINDOWS XP) CON UN SERVIDOR LINUX"

Monografía previa a la obtención del

Título de Ingeniero de Sistemas

AUTORES:

Mónica Cedillo Durán

Antonio Molina Minchalo

DIRECTOR:

Ing. Pablo Esquivel

Cuenca – Ecuador

2006

Las ideas, hechos y contenidos de esta monografía son de exclusiva responsabilidad de los autores.

Mónica Cedillo
CI: 0103981676

Antonio Molina M
CI: 0103666962

DEDICATORIA

Este trabajo de Graduación está dedicado a Dios que nos ha guiado por sus sendas durante esta etapa de nuestras vidas, a nuestros Padres, por todo el esfuerzo y sacrificio que nos han entregado para prepararnos como buenos profesionales y a nuestros Hermanos por el apoyo e incentivo que nos han brindado en estos años.

AGRADECIMIENTO

Un agradecimiento especial a la Universidad del Azuay, por brindarnos la oportunidad de realizar nuestros estudios de Ingeniería, a nuestros profesores por compartirnos sus conocimientos, en particular al Ing. Pablo Esquivel por el apoyo brindado en la realización de esta monografía.

Indice de Contenidos

CAPITULO IV

PROTOCOLOS Y TUNEL VPN

RESUMEN

El siguiente trabajo trata de las Redes Privadas Virtuales conocidas como VPN (Virtual Private Network).

Una VPN es una extensión de una red local y privada de computadoras, que puede utilizar Internet como medio de comunicación.

Este método permite enlazar dos o más redes simulando una única red privada, permitiendo la comunicación entre computadoras como si fuera punto a punto.

Un usuario remoto se puede conectar individualmente a una red privada utilizando una conexión VPN, y de esta manera utilizar aplicaciones, enviar datos, etc. de forma segura. Las VPN's crean una especie de túnel en Internet, entre dos puntos para la transmisión de datos, por medio de un proceso de encapsulación y encriptación, con lo que la información se transmite en forma segura y ésta se vuelve ilegible para quien intercepte estos paquetes.

En este documento se dará una descripción general de las VPN's y su funcionamiento, se concluirá con un trabajo práctico que consiste en la implementación de un túnel VPN entre una PC personal y una red privada con un Servidor Linux.

ABSTRACT

The next project is about the Virtual Private Network, known as VPN.

A VPN is an extension of a local network and private of computers which can use internet as a media of communication.

This method allows linking two or more reds simulating a unique private red allowing the communication between computers as if it were point by point.

A remote user can individually get connected to a private network using a connection VPN to use applications, send data, etc. in a safety way.

The VPN's form a kind of tunnel in Internet, between two points for the transition of data through a process of encapsulation and encryption that transmit information safely, and it is illegible for who intercept these packages.

In this document will be given a general description of the VPN's and its functioning and will conclude with a practice work that consist in the creation of a tunnel VPN between a personal PC and a private network with a Linux Server.

CAPITULO I

INTRODUCCION A LAS VPN

1.1 Introducción

Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de email, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

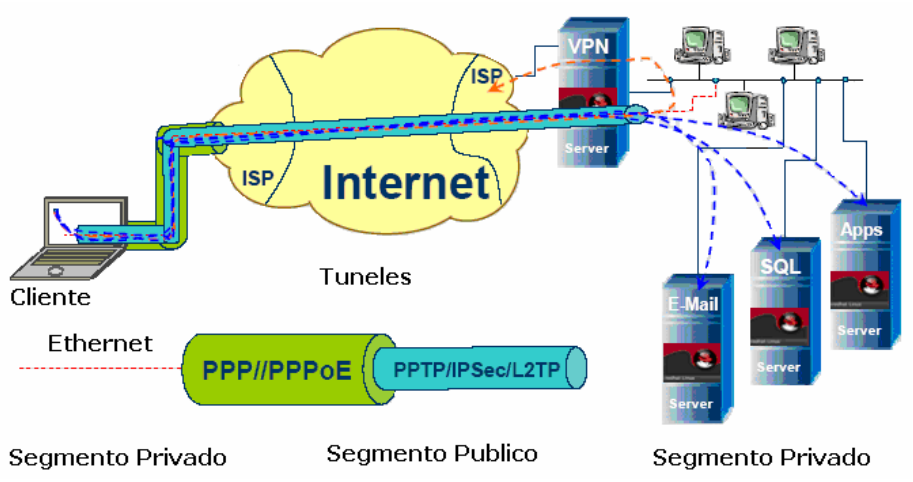
A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad.

Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante RAS, este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.

El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un abono mensual más una tarifa por el uso, en el que se tienen en cuenta la duración de las llamadas y la distancia hacia donde se las hace. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas, y, además, tiene sucursales en otros países, los costos telefónicos pueden llegar a ser prohibitivos. Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan.

Las VPN's son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

1.2 Concepto de VPN



Una VPN es una red virtual que se crea "dentro" de otra red, como por ejemplo Internet. Generalmente las redes privadas se crean en redes públicas, en las que se quiere crear un entorno confidencial y privado. La VPN nos permitirá trabajar como si estuviésemos en la red local, es totalmente transparente para el usuario.

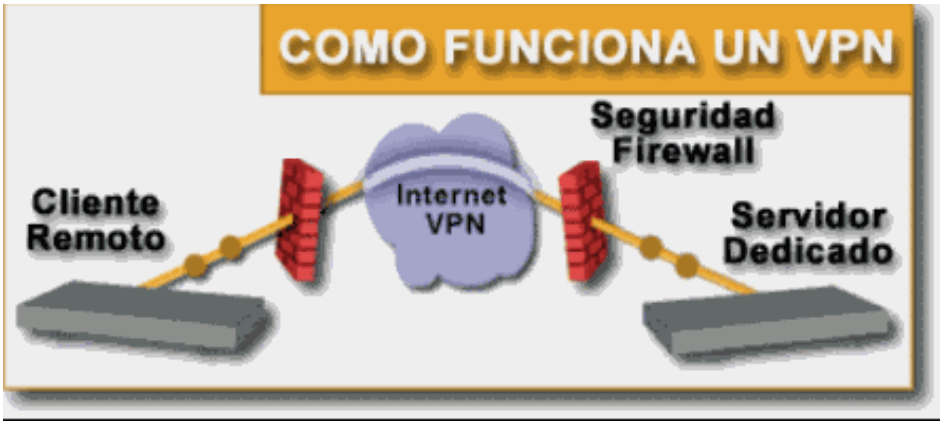
Se extiende, mediante un proceso de encapsulación y encriptación de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte, de forma que sólo el emisor y el receptor son capaces de leerlos. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su ordenador remoto las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet publico.

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

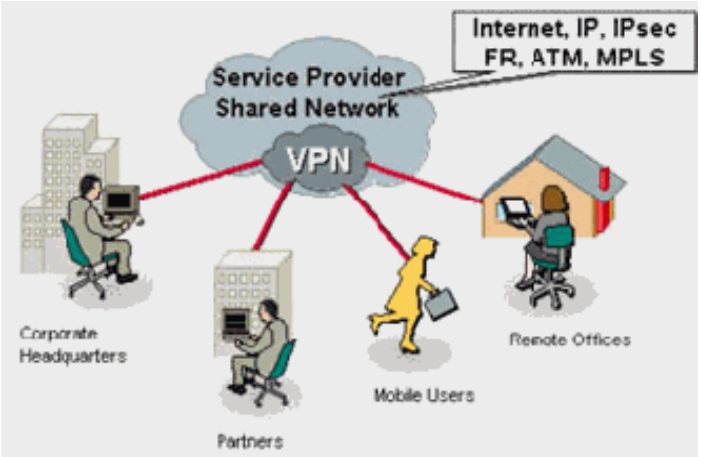
- Autenticación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: La garantía de que los datos enviados no han sido alterados.
- Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son 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.

1.3 Como Funciona una VPN



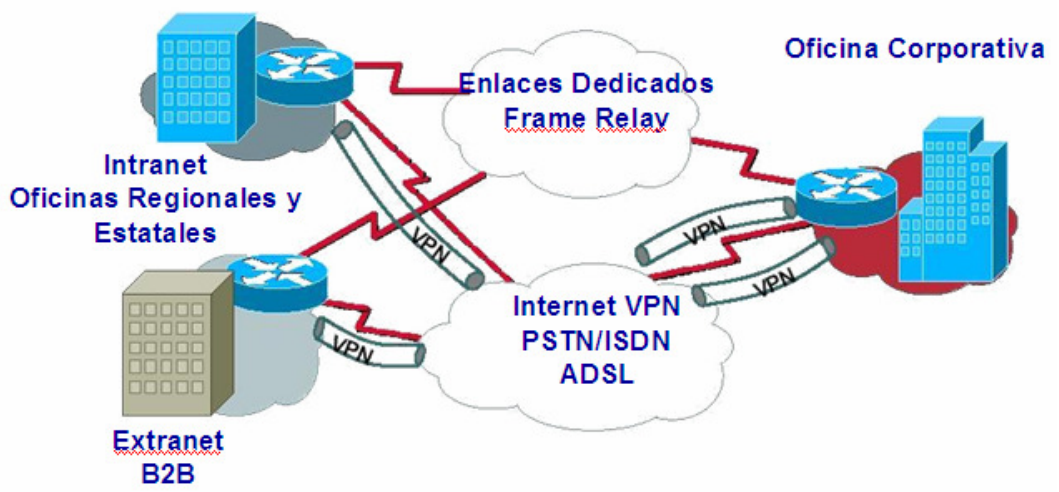
En la figura anterior se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de Internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado, lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, Ipsec, Frame Relay, ATM como lo muestra la figura siguiente.



1.4 Por que usar una VPN

Las redes privadas virtuales surgen como una alternativa a los servicios de comunicaciones tradicionales de red amplia (WAN) de enlaces dedicados.



Este tipo de comunicaciones presentan múltiples ventajas y beneficios para los usuarios:

Bajo costo

La principal motivación del uso y difusión de esta tecnología es la reducción de los costos de comunicaciones directos, tanto en líneas *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.
- En el caso de conexiones punto a punto, utilizando servicios de banda ancha para acceder a Internet, y desde Internet llegar al servidor VPN de la organización. Todo esto a un costo sensiblemente inferior al de los vínculos WAN dedicados.

Flexibilidad

Se puede optar por múltiples tecnologías o proveedores de servicio. Esa independencia posibilita que la red se adapte a los requerimientos de los negocios, y se puede elegir el medio de acceso más adecuado. Por ejemplo, si se trata de una pequeña oficina remota, se puede utilizar acceso discado, ISDN, xDSL o cable módem.

Implementación rápida

El tiempo de implementación de un *"backbone"* de WAN para una empresa es muy alto frente a la implementación de una red privada virtual sobre un *"backbone"* ya existente de un proveedor de servicio. Más aún, la flexibilidad de esta arquitectura permite implementar nuevos servicios de manera muy rápida, que concuerdan con los tiempos del negocio de la empresa.

Escalabilidad

El desarrollo masivo de redes como Internet permite que la empresa tenga puntos de presencia en todo tipo de lugares. Por otro lado, la independencia con respecto a la tecnología de acceso posibilita escalar el ancho de banda de la red de acuerdo con el requerimiento del usuario. Además, la escalabilidad de la red no incide en la operatoria y gestión de ésta, dado que la infraestructura de la WAN es responsabilidad del proveedor del servicio.

Módem

Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

Línea Privada

Se tendría que tender cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo se necesita enlazar una oficina central con una sucursal que se encuentra a 100 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

Seguridad

Se tiene la posibilidad de que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

Ancho de banda

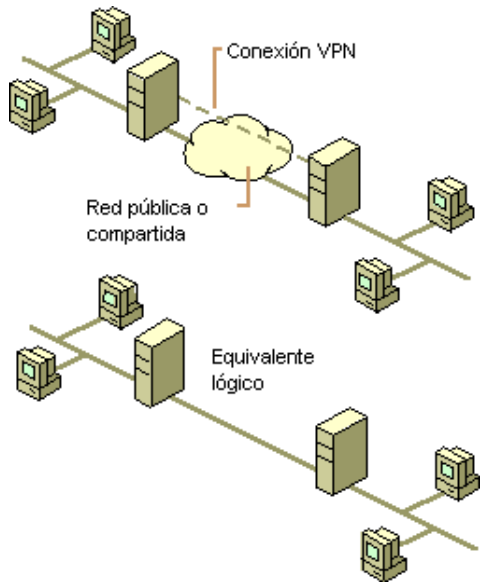
Podemos encontrar otra motivación en el deseo de mejorar el ancho de banda utilizado en conexiones *dial-up*. Las conexiones VPN de banda ancha mejoran notablemente la capacidad del vínculo**.**

CAPITULO II

GENERALIDADES DE LAS VPN'S

2.1 Estructura de una VPN

Una *Virtual Private Network* (VPN) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura siguiente, la idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.



Las VPN's también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e

integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación.

La tecnología de túneles *("Tunneling"*) es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autenticación son esenciales en las VPN's, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPN's es conceptualmente parecido al logueo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Ejemplos de sistemas de autenticación son *Challenge Handshake Authentication Protocol (CHAP) y RSA.*

Todas las VPN's tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos

de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPN's, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPN's es IPSec, que consiste en un conjunto de propuestas del IETF que delinean un protocolo IP seguro para IPv4 y IPv6. IPSec provee encriptación a nivel de IP.

El método de túneles, como fue descrita anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran *Point-to-Point Tunneling Protocol* (PPTP), *Layer-2 Fowarding Protocol* (L2FP) y el modo túnel de IPSec.

2.2 Características de una VPN

Las VPN consisten en hardware y software, y además requieren otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que la red sea segura, este disponible y sea fácil de mantener. Son necesarios ya sea que un PSI proporcione la VPN o que usted haya decidido instalar una por si mismo.

Disponibilidad: Se aplica tanto al tiempo de actualización como al de acceso.

Control: Suministra capacitación, experiencia, supervisión meticulosa y funciones de alerta que ofrece algunos proveedores de servicios administrados. Una consideración significativa es que sin importar que tan grande sea la organización, es probable que solo cuente con una VPN; puede tener otros puntos de acceso pero seguirá siendo una VPN corporativa.

Compatibilidad: Para utilizar tecnología VPN e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el IP nativo de Internet.

Seguridad: Es lo mas importante en una VPN, desde el proceso de cifrado que implementa y los servicios de autenticación que usted elige hasta las firmas digitales y las autoridades emisoras de certificados que utilizan. Abarca el software que implementa los algoritmos de cifrado en el dispositivo de la VPN.

Confiabilidad: Cuando una compañía decide instalar el producto VPN de un PSI, está a merced de este.

Autenticación de datos y usuarios:

Datos: Reafirma que el mensaje a sido enviado completamente y que no ha sido alterado de ninguna forma.

Usuarios: Es el proceso que permite que el usuario acceda a la red.

Sobrecarga de tráfico: En todo tipo de tecnologías existen sacrificios: velocidad contra desempeño, seguridad contra flexibilidad. Las VPN caben en la misma categoría cuando se hablan de tamaño de paquetes cifrados las sobre carga esta en

juego, ya que si mandamos varios paquetes se incrementa el tamaño de estos y por lo tanto se afecta la utilización del ancho de banda.

Sin repudio: Es el proceso de identificar positivamente al emisor de tal manera que no pueda negarlo.

Velocidad*:* La velocidad es un criterio crucial al momento de escoger una VPN. Para grandes empresas las soluciones de VPN alcanzan velocidades mayores a 2G bit/sec. El componente crítico de la velocidad es la capacidad de la tecnología para escalar sobre una línea de productos.

La seguridad y reducción del costo: Las VPN's son una solución comercial porque ellas proporcionan seguridad punto a punto para altas velocidades en el cable con una reducción del costo comparada a una red privada. Proporcionan una fuerte seguridad para los usuarios y gerentes, sitios del negocio electrónico y aplicaciones, oficinas de la rama y usuarios móviles o remotos.

Facilidad de Administración: Las capacidades avanzadas del administrador de red reducen la necesidad de hardware adicional así como proporciona una aplicación detallada informando y reconociendo la alerta del incidente. VPN's ofrecen total solución de manejo que les proporciona redes profesionales con facilidad, para una global integración de acceso a tareas, el sitio y manejo de la unidad. Un simple punto de control se requiere para supervisar y provisionar la red entera.

2.3 Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

Identificación de usuario: La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

Administración de direcciones: La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos: Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves: La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples: La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX) entre otros.

2.4 Seguridad

¿Porque es importante la seguridad cuando se implementa una VPN?

- Solo a las partes autorizadas se les permite el acceso a las aplicaciones y servidores corporativos, ya que se permite que las personas entren y salgan de Internet o de otras redes públicas y también se les ofrece acceso a los servidores.
- Cualquiera que pase a través de flujo de datos cifrados de la VPN no debe estar capacitado para descifrar el mensaje.
- Los datos deben permanecer intocables al 100%.
- Se debe tener facilidad de administración, la configuración debe ser directa y el mantenimiento y actualización deben estar asegurados.

Un punto fundamental es el particionamiento de las redes públicas o de uso compartido para implementar las VPN's. Esto se logra mediante el uso de túneles que no son ni más ni menos que técnicas de encapsulado del tráfico**.** Las técnicas que se utilizan son: GRE, que permite que cualquier protocolo sea transportado entre dos puntos de la red encapsulado en otro protocolo, típicamente IP; L2TP que permite el armado de túneles para las sesiones PPP remotas, y por último IPSec para la generación de túneles con autenticación y encriptado de datos.

2.4.1 Calidad de servicio

La calidad de servicio permite la asignación eficiente de los recursos de la red pública a las distintas VPN's para que obtengan una performance predecible. A su vez, las VPN's asignarán distintas políticas de calidad de servicio a sus usuarios, aplicaciones o servicios. Las componentes tecnológicas básicas son:

Clasificación de Paquetes: asignación de prioridades a los paquetes basados en la política corporativa. Se pueden definir hasta siete clases de prioridades utilizando el campo de *IP precedence* dentro del encabezado del paquete IP.

Committed Access Rate (CAR): garantiza un ancho de banda mínimo para aplicaciones o usuarios basándose en la política corporativa.

Weighted Fair Queuing (WFQ): determina la velocidad de salida de los paquetes en base a la prioridad asignada a éstos, mediante el encolado de los paquetes.

Weighted Random Early Detection (WRED): complementa las funciones de TCP en la prevención y manejo de la congestión de la red, mediante el descarte de paquetes de baja prioridad.

Generic Traffic Shaping (GTS): reduce la velocidad de salida de los paquetes con el fin de reducir posibles congestiones de la red que tengan como consecuencia el descarte de paquetes.

2.5 Ventajas y Desventajas

2.5.1 Ventajas de VPN's

La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. 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. Al mismo tiempo,

todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizaran usando los recursos y conexiones que tenga la red privada.

Dentro de las ventajas más significativas podremos mencionar:

El Costo Bajo de una VPN: Una razón de que una VPN baje el coste es la eliminación de la necesidad por las líneas arrendadas a largas distancias caras. Con VPN's, una organización necesita sólo una conexión especializada relativamente corta al proveedor de servicio. Esta conexión podría ser una línea arrendada local o podría ser una conexión de banda ancha local como servicio de DSL.

Otra manera que las VPN's reducen el costo es disminuyendo la necesidad por cargos del teléfono, largas distancias para acceso remoto. Los clientes de VPN sólo necesitan que llamen al punto de acceso del proveedor de servicio más cercano. En algunos casos esto puede requerir una llamada de larga distancia, pero en muchos casos será una llamada local.

Escalabilidad y VPN's: El costo de una organización de líneas arrendadas tradicionales puede ser al principio razonable pero puede aumentar exponencialmente como la organización que crece. Una compañía con dos oficinas de la rama, por ejemplo, puede desplegar simplemente una línea dedicada para conectar las dos situaciones. Si una tercera oficina de la rama necesita online, sólo dos líneas adicionales se exigirán conectar esa situación directamente a las otras dos.

Sin embargo, cuando una organización crece y más compañías deben agregarse a la red, el número de líneas arrendadas requieren aumentos dramáticamente. Cuatro oficinas de la rama requieren seis líneas para la conectividad, cinco oficinas requieren diez líneas, y así sucesivamente. Matemáticamente llaman a este fenómeno como "la explosión de la combinación," y en una tradicional WAN esta explosión limita la flexibilidad por crecimiento. VPN's que utiliza el Internet evita este problema simplemente ya usando el acceso geográficamente-distribuido disponible.

Comparado a las líneas arrendadas, VPN's basado en Internet ofrecen el alcance global mayor, dado que esos puntos de acceso de Internet son accesibles en muchos lugares donde las líneas especializadas no están disponibles.

Entre otras ventajas que ofrecen las VPN's se pueden citar:

- La integridad, confidencialidad y seguridad de los datos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

2.5.2 Desventajas de VPN's

Entre los inconvenientes podemos citar:

- Una mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos.

- Se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP).

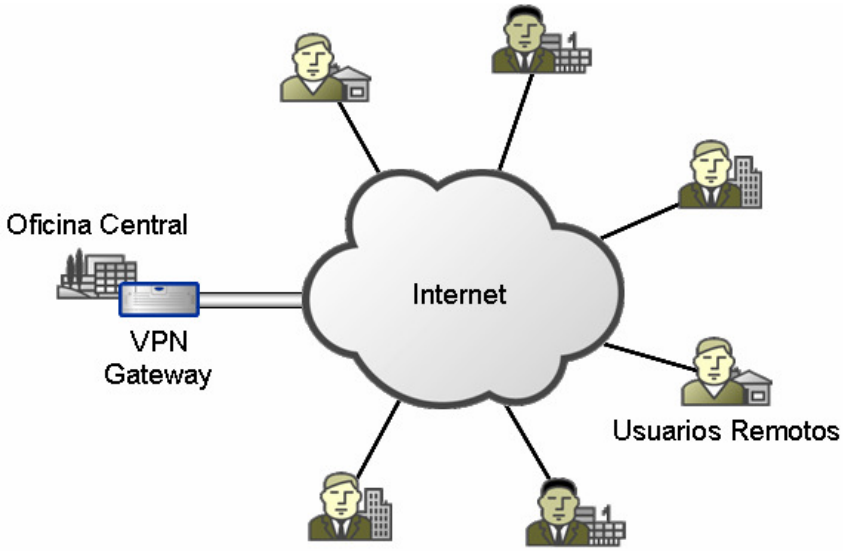
- Requieren una comprensión en profundidad de seguridad de la red pública.

- Los diferentes proveedores de tecnologías VPN no pueden trabajar bien juntos debido a las normas no estandarizadas.

CAPITULO III

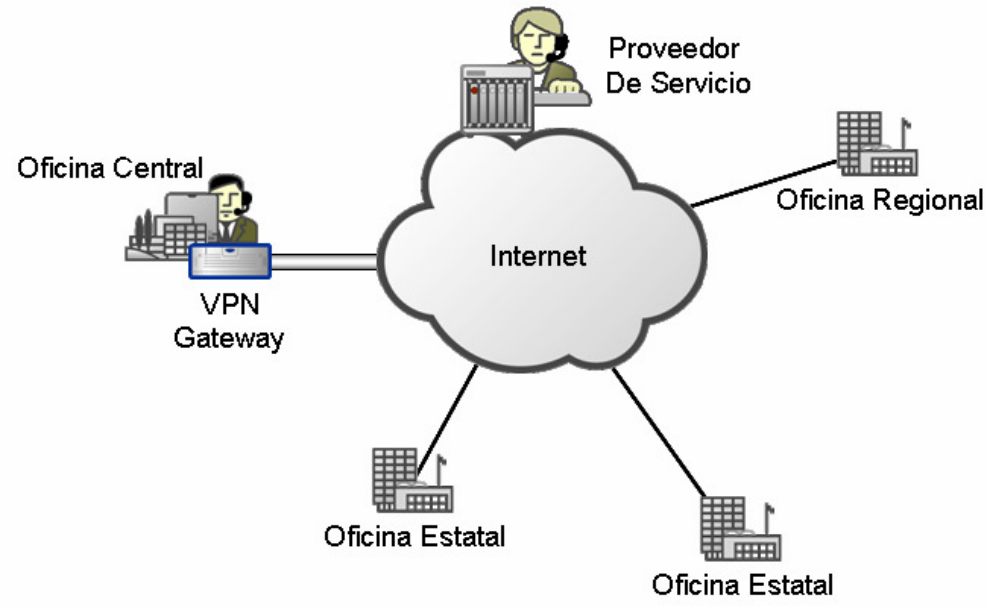
TIPOS DE VPN

3.1 VPN de acceso remoto



Éste es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hotel, aviones, etc.) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura *dial-up* (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos módems.

3.2 VPN punto a punto



Este esquema se utiliza para conectar oficinas remotas con la sede central de 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.

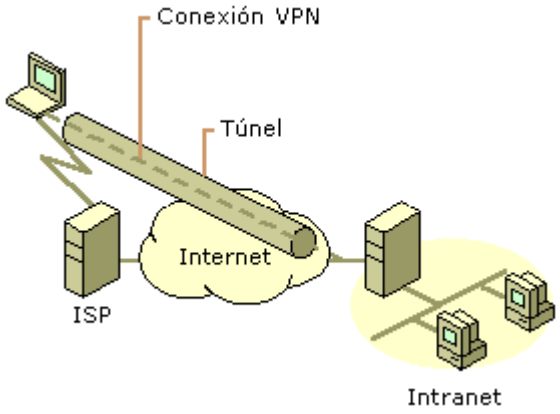
3.3 VPN interna

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 muy 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.

3.4 Redes privadas virtuales basadas en Internet

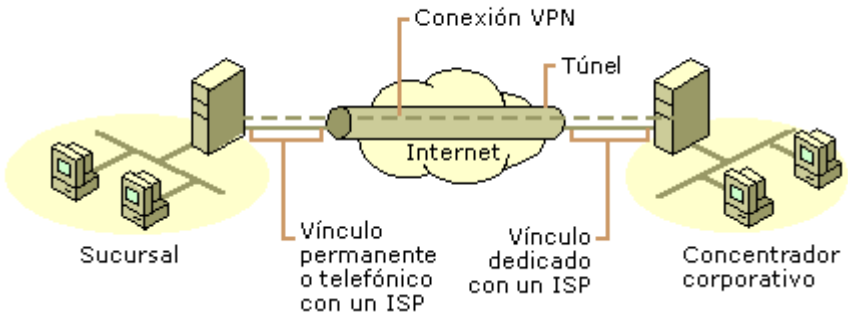
La ilustración siguiente muestra el acceso remoto a través de Internet.



3.4.1 Conectar redes a través de Internet

Cuando las redes están conectadas a través de Internet, un enrutador reenvía paquetes a otro enrutador a través de una conexión VPN. Para los enrutadores, la red privada virtual funciona como un vínculo de la capa de vínculo de datos.

La ilustración siguiente muestra la conexión de redes a través de Internet.



3.4.2 Usar vínculos WAN dedicados

En lugar de utilizar un vínculo WAN dedicado de larga distancia y caro entre las distintas oficinas de la compañía, los enrutadores de las oficinas se conectan a Internet mediante vínculos WAN dedicados locales con un ISP local. Así, cualquiera de los enrutadores inicia una conexión VPN de enrutador a enrutador a través de

Internet. Una vez conectados, los enrutadores pueden reenviarse entre sí transmisiones de protocolos enrutadas o directas mediante la conexión VPN.

3.4.3 Usar vínculos WAN de acceso telefónico

En lugar de realizar una llamada de larga distancia para conectar con un NAS de la compañía o externo, el enrutador de una oficina puede llamar a un ISP local. Mediante la conexión establecida con el ISP local, el enrutador de la sucursal inicia una conexión VPN de enrutador a enrutador con el enrutador de la oficina central a través de Internet. El enrutador de la oficina central actúa como un servidor VPN y debe estar conectado a un ISP local mediante un vínculo WAN dedicado.

Es posible mantener conectadas ambas oficinas a Internet mediante un vínculo WAN de acceso telefónico. Sin embargo, esto sólo es posible si el ISP admite el enrutamiento a clientes mediante marcado a petición; es decir, el ISP llama al enrutador del cliente cuando hay que entregar un datagrama IP al cliente. Muchos ISP no admiten el enrutamiento de marcado a petición para clientes.

3.5 Redes privadas virtuales basadas en intranet

Las conexiones de red privada virtual basadas en intranet aprovechan la conectividad IP en la intranet de una organización.

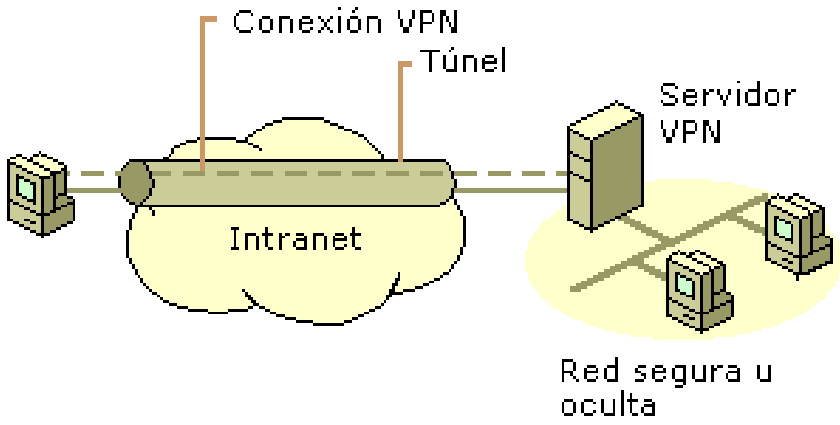
3.5.1 Acceso remoto a través de una intranet

En las intranets de algunas organizaciones, los datos de un departamento, por ejemplo, el departamento de recursos humanos, son tan confidenciales que la red del departamento está físicamente desconectada de la intranet del resto de la organización. Aunque así se protegen los datos del departamento, se crea un problema de acceso a la información por parte de aquellos usuarios que no están físicamente conectados a la red independiente.

Mediante una conexión VPN, la red del departamento está físicamente conectada a la intranet de la organización pero se mantiene separada gracias a un servidor VPN. El servidor VPN no proporciona una conexión enrutada directa entre la intranet de la organización y la red del departamento. Los usuarios de la intranet de la organización

que disponen de los permisos apropiados pueden establecer una conexión VPN de acceso remoto con el servidor VPN y tener acceso a los recursos protegidos de la red confidencial del departamento. Adicionalmente, para mantener la confidencialidad de los datos, se cifran todas las comunicaciones realizadas a través de la conexión VPN. Para aquellos usuarios que no tienen permisos para establecer una conexión VPN, la red del departamento está oculta a la vista.

La ilustración siguiente muestra el acceso remoto a través de una intranet.

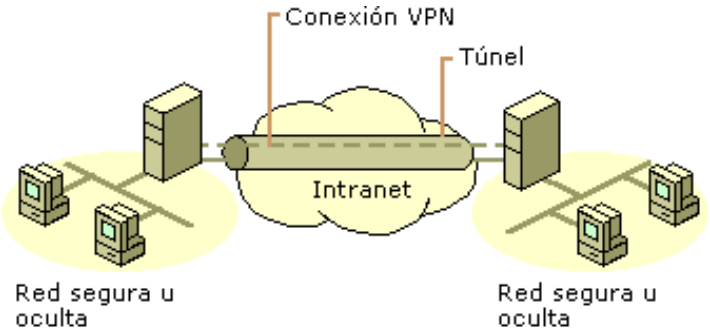


3.5.2 Conectar redes a través de una intranet

También puede conectar dos redes a través de una intranet mediante una conexión VPN de enrutador a enrutador. Las organizaciones que tienen departamentos en diferentes ubicaciones, cuyos datos son altamente confidenciales, pueden utilizar una conexión VPN de enrutador a enrutador para comunicarse entre sí. Por ejemplo, el departamento financiero podría necesitar comunicarse con el departamento de recursos humanos para intercambiar información acerca de las nóminas.

El departamento financiero y el departamento de recursos humanos están conectados a la intranet común con equipos que pueden actuar como clientes VPN o servidores VPN. Una vez establecida la conexión VPN, los usuarios de los equipos de ambas redes pueden intercambiar datos confidenciales a través de la intranet corporativa.

La ilustración siguiente muestra la conexión de redes a través de una intranet.



CAPITULO IV

PROTOCOLOS Y TUNEL VPN

4.1 Protocolos utilizados

A nivel del Túnel VPN:

– PPTP – Point2Point Tunneling Protocol (RFC2631)
– GRE – Generic Routing Encapsulation (RFC2784)
– IPSec – IP Security Protocol (RFC1825)
– SSL/TLS - Secure Sockets Layer y Transport Layer Security (RFC2246)
– L2TP – Layer 2 Tunneling Protocol (RFC2661)
– L2F - Layer 2 Forwarding (Obsoleto por L2TP, RFC2341)
– IPIP - IP-in-IP (Utilizado en Redes Móviles-IP, RFC2003)

A nivel de Cifrado de datos de Usuario VPN:

– MPPE – Microsoft Point2Point Encryption (RFC3078)

A nivel de Autentificación:

– PAP
– CHAP
– MSCHAP / MSCHAPv2

4.1.1 PPTP

Protocolo de *Tuneling* Punto a Punto (*Point-to-Point Tunneling Protocol*) desarrollado por ingenieros de *Ascend Communications*, U.S. *Robotics*, 3Com *Corporation*, Microsoft, y ECI *Telematics* para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

PPTP encapsula data gramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet. Diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un módem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

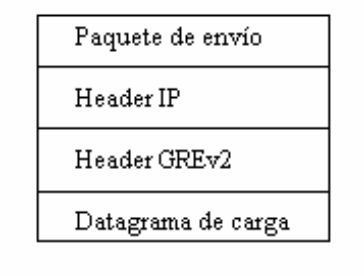
- El usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS (el usuario remoto establece una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS).

- El usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente (el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP).

Establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para los medios a través de los cuales el paquete viaja (Ethernet, frame relay, PPP). El header IP contiene información relativa al paquete IP, como direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP relativos a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado.

La siguiente figura ilustra las capas del encapsulamiento PPTP.



Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, estándar en el que se intercambia un "secreto" y se comprueba que ambos extremos de la conexión posean el mismo. MS-CHAP es un estándar propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Protocolo de Autenticación de Password), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

4.1.2 IPSec

Intenta remediar algunas falencias de IP, como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Protocolo de Autenticación (AH) y Carga útil Encapsulada con Seguridad (ESP).

Confidencialidad: Los datos transferidos sean sólo entendidos por los participantes de la sesión.

Integridad: Los datos no sean modificados en el trayecto de la comunicación.

Autenticidad: La validación de remitente de los datos.

Protección a repeticiones: Una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH brinda autenticación, integridad y protección a repeticiones pero no así confidencialidad. AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header. El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

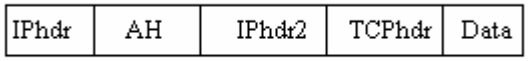
Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

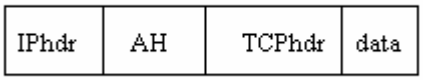
- El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Asociaciones de Seguridad (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un único punto a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP.

Un ejemplo de paquete AH en modo túnel es:



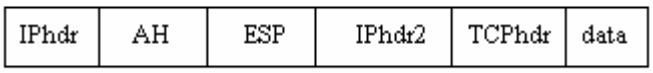
Un ejemplo de paquete AH en modo transporte es:



Como ESP no puede autentificar el header IP más exterior, es muy útil combinar un header AH y ESP para obtener lo siguiente:

Este tipo de paquete se denomina *Transport Adjacency*.

La versión de entunelamiento sería:



4.1.3 Secure Sockets Layer (SSL) y Transport Layer Security (TLS)

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, solo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene

sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes.

SSL supone una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Encriptación del tráfico basado en cifrado simétrico

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);
- Con funciones hash: MD5 o de la familia SHA.

Como funciona SSL

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, encriptado y empaquetado con un código de autenticación del mensaje (MAC). Cada registro tiene un campo de *content_type* que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo *handshake*, que tiene el *content_type* 22.

El cliente envía y recibe varias estructuras *handshake*:

- Envía un mensaje *ClientHello* especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde.
- Después, recibe un registro *ServerHello*, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.
- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.
- El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autenticada.
- Cliente y servidor negocian una clave secreta común llamada *master secret*, posiblemente usando el resultado de un intercambio Diffie-Hellman, o simplemente encriptando una clave secreta con una clave pública que es desencriptada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este *master secret* (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una *función pseudo aleatoria* cuidadosamente elegida.

TLS/SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC).
- Protección contra varios ataques conocidos (incluidos ataques man in the middle attack), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.
- El mensaje que finaliza el protocolo *handshake* (*Finished*) envía un *hash* de todos los datos intercambiados y vistos por ambas partes.

- La función pseudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

Aplicaciones

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.

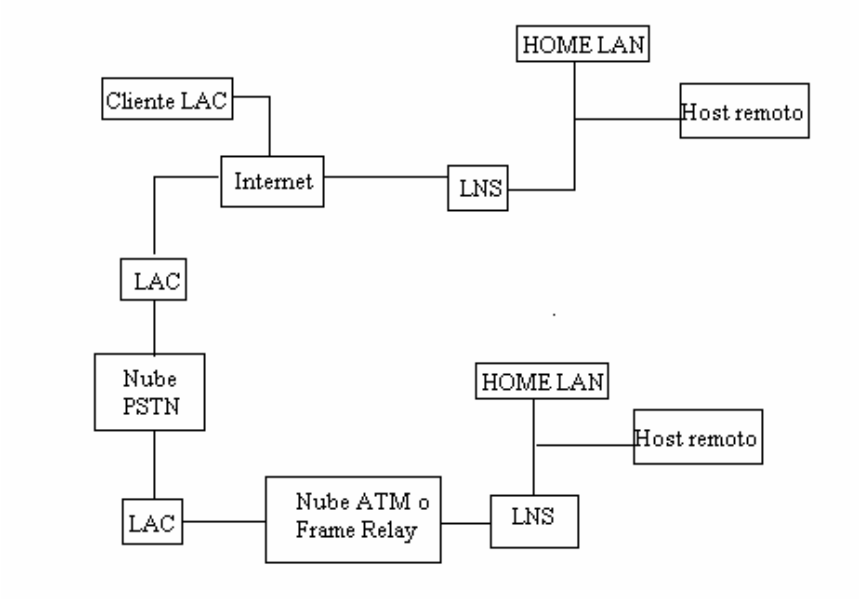
Aunque un número creciente de productos clientes y servidores pueden proporcionar SSL de forma nativa, muchos aún no lo permiten. En estos casos, un usuario podría querer usar una aplicación SSL independiente como *Stunnel* para proporcionar encriptación. No obstante, el *Internet Engineering Task Force* recomendó en 1997 que los protocolos de aplicación ofrecieran un forma de actualizar a TLS a partir de una conexión sin encriptación (plaintext), en vez de usar un puerto diferente para encriptar las comunicaciones, esto evitaría el uso de envolturas (wrappers) como Stunnel.

SSL también puede ser usado para tunelar una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

4.1.4 L2TP

Protocolo de *Tunneling* de Capa dos (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea transparente a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura:



Un Concentrador de Acceso L2TP (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

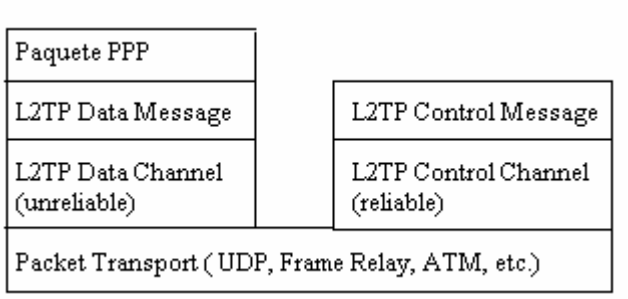
Un Servidor de Red de L2TP (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el

envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

La siguiente figura muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.



Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Es necesario que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al emplearse UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo los de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único que es usado como autenticado como autenticador.

La seguridad del paquete L2TP, requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

4.1.5 L2F – Layer 2 Forwarding

Este sistema es el precursor del L2TP, y es utilizado en los Routers CISCO, pero los trabajos en el L2TP lo han dejado obsoleto. Resulta útil, no obstante, si tenemos Routers Cisco a nuestra disposición. Como L2TP, encapsula tramas PPP sobre medios arbitrarios.

4.1.6 IPIP – IP in IP

IPIP define un encapsulado mínimo de los datagramas IP ya que, esencialmente, sólo se les añade una cabecera al principio. Este sistema es utilizado en redes "mobile-IP", para independizar las direcciones IP de la topología física de la red en un momento dado. No define ningún mecanismo de cifrado o autentificación.

4.1.7 MPPE – Microsoft Point to Point Encryption

MPPE es una forma de presentar paquetes PPP encriptados. Usa los algoritmos RSA RC4 para proveer los datos confidenciales. El largo de la “llave” de cifrado puede ser negociado, MPPE actualmente soporta 40-bit (Win98/ME), 56-bit y 128-bit (WinXP/2000).

Los cifrados en MPPE pueden ser establecidos al inicio de la sesión como también modificados durante el tráfico, paquete a paquete.

4.1.8 PAP – Password Authentification Protocol

PAP es un protocolo de autentificación simple, en el cual el “User Name & Password” es enviado al Server de Acceso Remoto en formato de Texto Plano (Sin

Encriptar/Cifrar). El uso de este protocolo es muy poco recomendable, ya que las password son fácilmente reconocibles desde los paquetes PPP enviados en el proceso de autentificación.

4.1.9 CHAP/MS-CHAP – Challenge Handshake Authentication Protocol

Microsoft creo MS-CHAP para autenticar estaciones de trabajo remotas de Windows, proporcionando esta funcionalidad con la cual los usuarios LAN ya están familiarizados. Tal como CHAP, MS-CHAP usa un mecanismo de "Desafío-Respuesta" con el objetivo de mantener las Passwords en el background durante el proceso de autentificación.

MS-CHAP usa el Algoritmo Hashing "Message Digest 4 (MD4)" y el Algoritmo de Encriptación de Datos DES (Data Encryption Standard) para generar el "Desafío-Respuesta", además de proveer el mecanismo de reporte de conexiones con error y cambio de passwords de usuarios. Por su puesto a diferencia de CHAP, los paquetes de respuesta de MS-CHAP están específicamente diseñados para trabajar con productos de Networking Microsoft, Windows 95/98/ME/NT/2000/XP.

4.1.10 MS-CHAPv2

Windows XP soporta *Microsoft Challenge Handshake Authentication Protocol* versión 2 (MS-CHAP v2). MS-CHAP v2 provee autentificación Dual/Mutua, generando poderosas claves de inicio para Microsoft MPPE (Microsoft Point-to-Point Encryption), y claves diferentes para la Tx/Rx de Data. Para minimizar el riesgo en el cambio de Passwords, el soporte para el antiguo procedimiento MSCHAP no esta soportado.

Dado que MS-CHAPv2 es mucho mas seguro que MS-CHAP, es ofrecido como opción de conexión en primera instancia, para todas las conexiones. MS-CHAP v2 esta soportado por computadores que corren Windows 98/ME/NT/2000/XP. Para computadores con Windows 95, MS-CHAP v2 esta solo soportado para conexiones VPN, y no para conexiones dial-up.

4.2 Túnel de VPN

Un túnel VPN funciona mediante la encapsulación de datos dentro de paquetes IP para transportar información que no cumple de ninguna forma con los estándares de direccionamiento en Internet. Posteriormente, estos paquetes encapsulados se transportan entre una red, o cliente único, y otra red sobre una red intermedia. A todo este proceso de encapsulación y transmisión de paquetes se le conoce como conexión por túnel, y a la conexión lógica por la que los paquetes viajan se le llama túnel. Un túnel es una conexión a través del Internet u otra red intermediaria. El resultado es que los usuarios remotos se convierten en nodos virtuales en la red a la que han sido conectados por túnel.

Desde la perspectiva del usuario, la naturaleza de la red física que ha sido conectada por túnel es irrelevante ya que aparece como si la información haya sido enviada sobre una red privada dedicada.

La comunicación a través de Internet requiere que, tanto la encapsulación como la encriptación de flujo de datos, sea viable. PPTP y L2TP proporcionan servicios de encapsulación, a fin de facilitar las comunicaciones de protocolos múltiples mediante Internet. La encapsulación permite que los paquetes de datos no basados en IP se comuniquen a través de Internet basada en IP desde un cliente remoto a una LAN corporativa privada, la cual permite que las redes no basadas en IP aprovechen al máximo el Internet.

4.2.1 Protocolos de túneles

Para que se establezca un túnel, tanto el cliente de éste como el servidor deberán utilizar el mismo protocolo de túnel.

La tecnología de túnel se puede basar en el protocolo del túnel de Nivel 2 o e 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; éstos encapsulan los paquetes IP en un encabezado adicional antes de enviarlos a través de una red IP.

4.2.2 Como funcionan los túneles

Para las tecnologías de túnel de Nivel 2 como PPTP y L2TP, un túnel es similar a una sesión; los dos puntos finales deben estar de acuerdo respecto al túnel, y negociar las variables de la configuración, como asignación de dirección o los parámetros de encriptación o de compresión.

En la mayor parte de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas; se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar al mismo.

Por lo general, las tecnologías del túnel de Nivel 3 suponen que se han manejado fuera de banda todos los temas relacionados con la configuración, normalmente a través de procesos manuales; sin embargo, quizá no exista una fase de mantenimiento de túnel. Para los protocolos de Nivel 2 (PPTP y L2TP) se debe crear, mantener y luego concluir un túnel.

Cuando se establece el túnel, es posible enviar los datos a través del mismo. El cliente o el servidor utilizan un protocolo de transferencia de datos del túnel a fin de preparar los datos para su transferencia.

Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor, primero adjunta un encabezado de protocolo de transferencia de datos de túnel a la carga útil. Luego, el cliente envía la carga útil encapsulada resultante a través de la red, la que

lo enruta al servidor del túnel. Este último acepta los paquetes, elimina el encabezado del protocolo de transferencia de datos del túnel y envía la carga útil a la red objetivo. La información que se envía entre el servidor del túnel y el cliente del túnel se comporta de manera similar.

4.2.3 Tipos de túnel

Se pueden crear túneles en diferentes formas:

4.2.3.1 Túneles voluntarios

Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente de éste.

4.2.3.2 Túneles obligatorios

Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con uno de éstos, la computadora del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del mismo.

4.3 Implementaciones de las VPN's

Todas las opciones disponibles en la actualidad caen en tres categorías básicas: soluciones de hardware, soluciones basadas en firewall y aplicaciones VPN por software.

- Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, etc.

- En el caso basado en firewall, se obtiene un nivel de seguridad alto por la protección que brinda el firewall, pero se pierde en rendimiento. Muchas veces se ofrece hardware adicional para procesar la carga VPN. Por ejemplo: Checkpoint NG, Cisco Pix.

- Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, Linux y los Unix en general. Por ejemplo productos de código abierto (Open Source) como OpenSSH, OpenVPN y FreeS/Wan.

4.4 El futuro de VPN

El éxito de VPN's en el futuro depende principalmente de la dinámica de la industria. El valor de VPN's se queda en el potencial de los negocios que ahorran dinero. Si el costo de llamadas telefónicas a largas distancias y las líneas arrendadas continuaran cayéndose, menos compañías podrán sentir la necesidad de cambiar a VPN's para acceso remoto. Por el contrario, si las normas de VPN solidifican e ínter-operan los productos del vendedor totalmente con otro, la apelación de VPN's debe aumentar.

El éxito de las VPN's también depende de la habilidad de intranets y extranets de dar sus promesas. Las compañías han tenido dificultad que mide las economías del costo de sus redes privadas, pero si puede demostrarse que éstos proporcionan valor significante, el uso de tecnología de VPN puede también aumentar internamente.

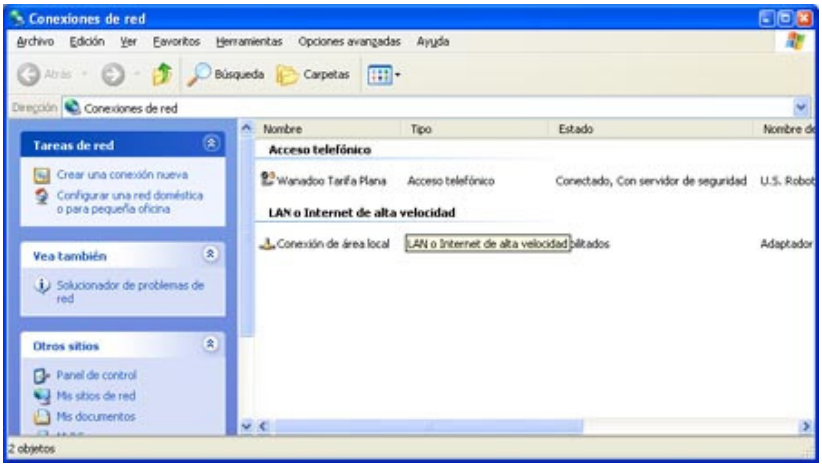
CAPITULO V

CONFIGURACION DE LA VPN

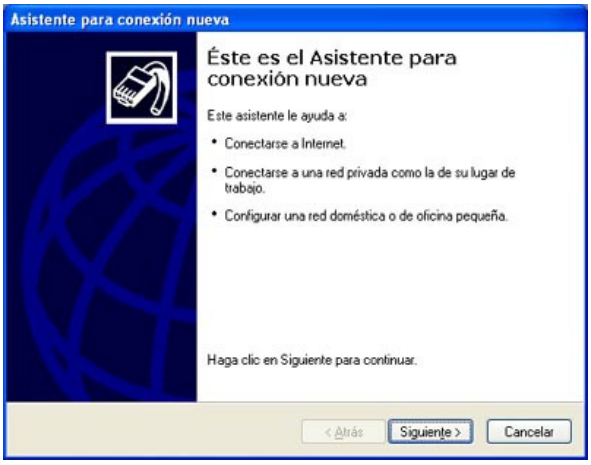
5.1 Configuración de una VPN bajo Windows

5.1.1 Configuración Servidor VPN

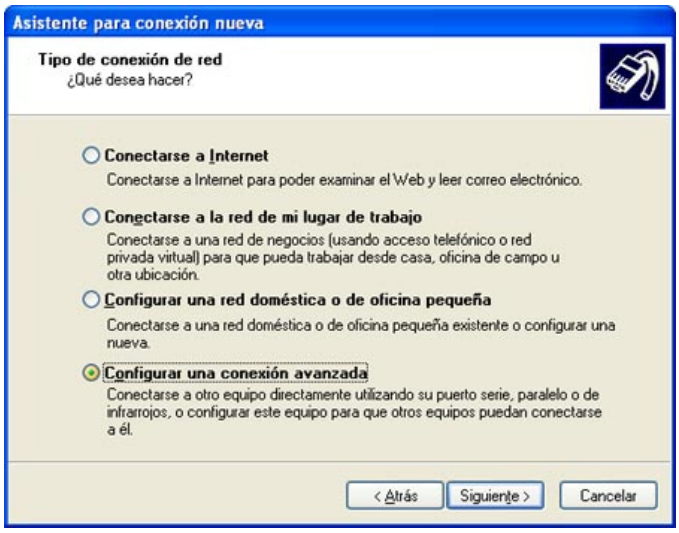
- Vamos al Panel de control, y abrimos la carpeta de "Conexiones de red" y en el menú Archivo seleccionamos "Nueva conexión".



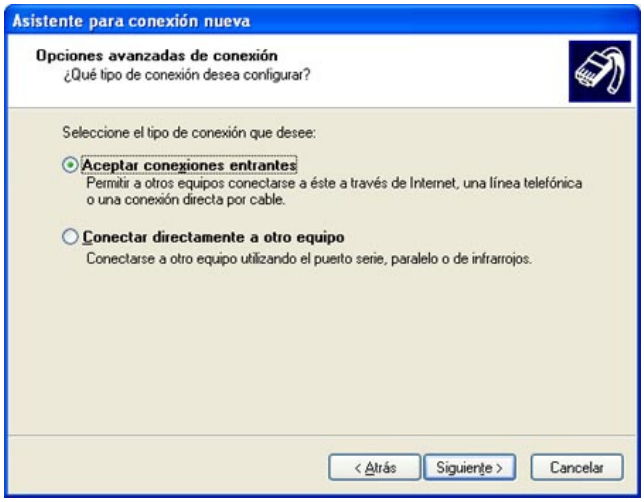
- Ahora estamos en el "Asistente para conexión nueva". Pulsamos en el botón "Siguiente" para continuar.



- Entre las opciones disponibles seleccionamos "Configurar una conexión avanzada", y pulsamos en "Siguiente".

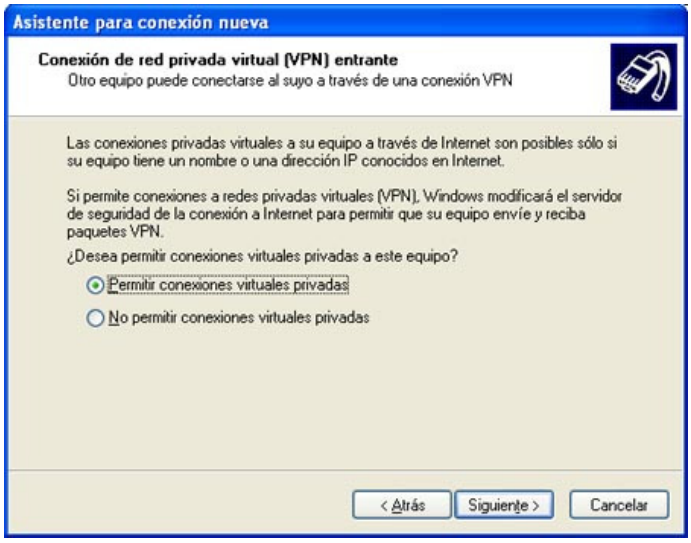


- Ahora seleccionamos "Aceptar conexiones entrantes" y pulsamos "Siguiente" para continuar.



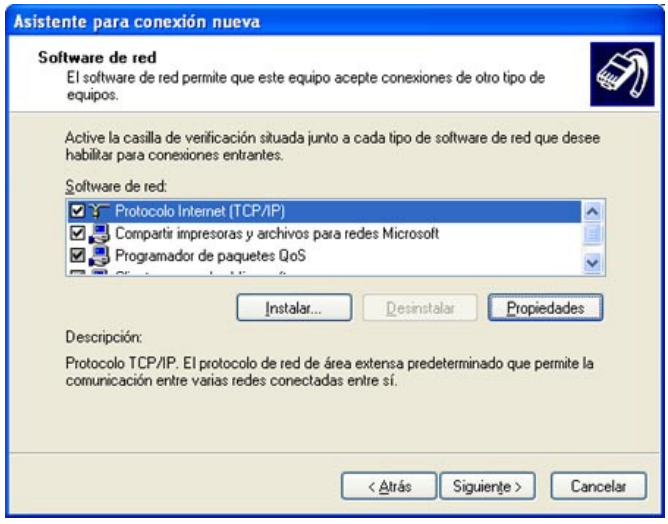
- En la pantalla "Dispositivos de conexiones entrantes" no seleccionamos ninguno, pues no queremos que se conecten a este equipo haciendo una llamada o usando el puerto paralelo. Pulsamos en "Siguiente".

- En la pantalla "Conexión de red privada virtual (VPN) entrante" debemos seleccionar "Permitir conexiones virtuales privadas". Pulsamos en "Siguiente".

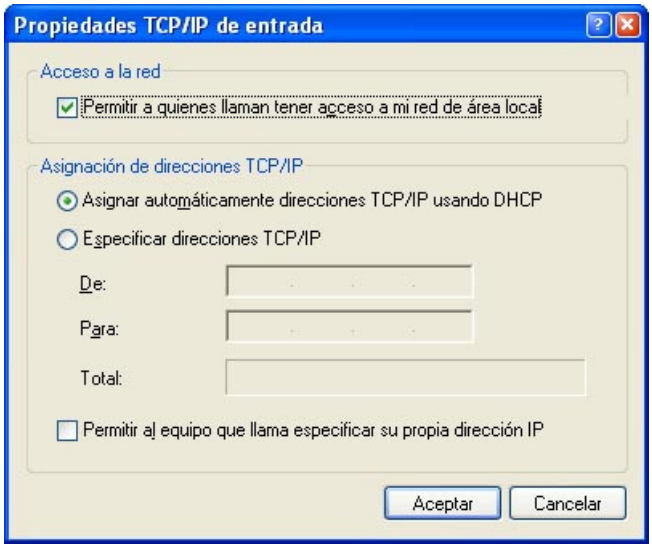


- En la pantalla "Permisos de usuarios" seleccionamos los usuarios que podrán conectarse a nuestro equipo usando la VPN. Desde esta misma pantalla podremos crear nuevos usuarios. Pulsamos en "Siguiente".

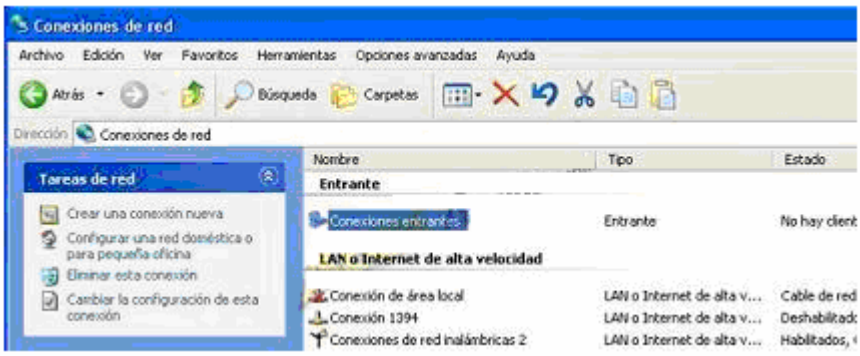
- Ahora debemos seleccionar los protocolos que habilitaremos en la VPN. Como queremos compartir ficheros e impresoras marcaremos "Protocolo Internet (TCP/IP)", "Compartir impresoras y archivos para redes Microsoft". Podremos agregar los protocolos que queramos usando el botón Instalar. Seleccionamos el protocolo "Protocolo Internet (TCP/IP)" y pulsamos en el botón Propiedades para proceder a configurarlo.



- Ahora podemos configurar las propiedades del protocolo TCP/IP. Si queremos que los clientes que se conectan a nosotros puedan acceder a la red local en la que tenemos nuestro servidor deberemos activar la primera casilla. Además podemos dejar que el servidor asigne las IP's de los clientes o establecer un intervalo de IP's, o incluso permitir que los clientes especifiquen su IP.



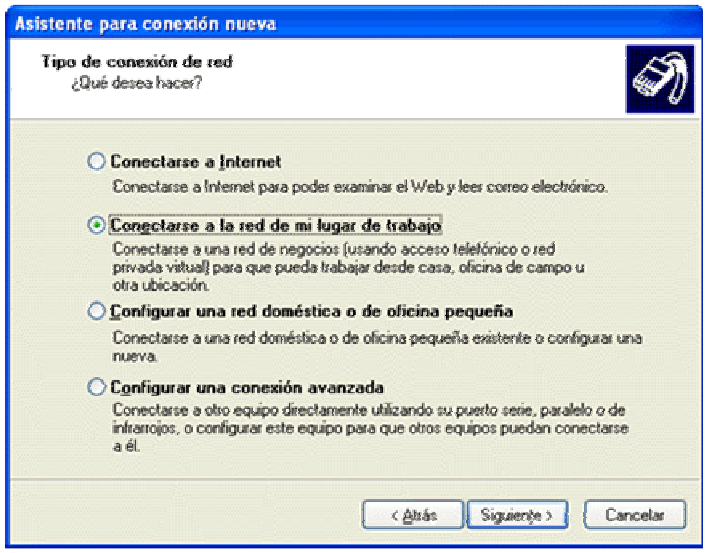
Guardamos la configuración de TCP/IP y pulsamos en el botón siguiente del asistente y ya habremos terminado. En este momento tendremos una nueva conexión en la carpeta de Conexiones de red llamada **Conexiones entrantes**. Seleccionando la nueva conexión podremos ver el estado de ésta, los clientes conectados, cambiar las opciones de configuración, etc.



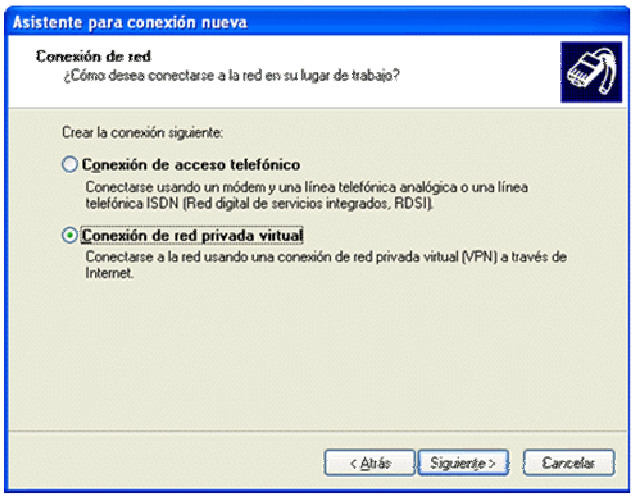
Ahora ya tenemos configurado el servidor VPN y ya está listo para aceptar clientes VPN. A continuación configuraremos una conexión VPN para que se conecte al servidor.

5.1.2 Configuración Cliente VPN

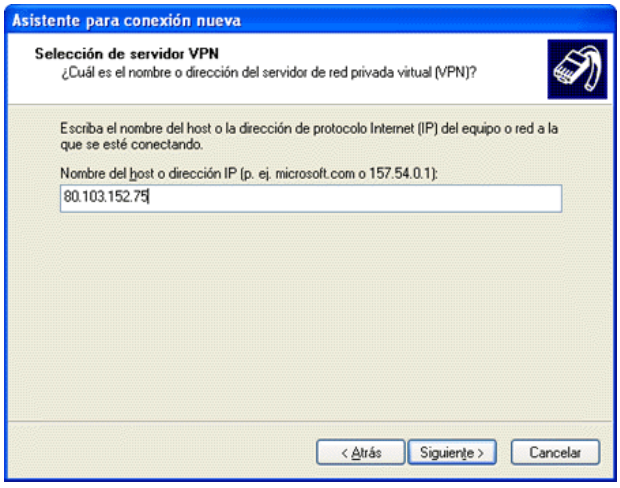
- Abrimos la carpeta de "Conexiones de red" y en el menú Archivo seleccionamos "Nueva conexión". En el asistente para conexión nueva seleccionamos "Conectarse a la red de mi lugar de trabajo", y pulsamos siguiente.



- Seleccionamos "Conexión de red privada virtual", y pulsamos siguiente.



En la siguiente ventana, marcaremos la opción "no usar conexión inicial" a menos que queramos que con la VPN se utilice otra de nuestras conexiones a Internet, si indicamos que al activar esta conexión se active antes otra conexión, por ejemplo una conexión telefónica, se conectará primero a Internet y luego se establecerá la VPN. Si disponemos de cable o ADSL no es necesario activar ninguna de estas conexiones. Tampoco lo es si estamos conectados a Internet cuando activamos la conexión VPN o no queremos que ésta marque ninguna conexión. Por último indicamos la dirección IP del servidor VPN, esta es la dirección IP pública, es decir, la que tiene en Internet en el momento de establecer la conexión entre los clientes y el servidor.



- Al finalizar el asistente ya tendremos la conexión lista para activarse. Ahora debemos indicar el usuario y las password que hemos activado en el servidor y ya podremos conectarnos con el servidor. Si el servidor VPN se conecta a Internet usando un módem o Cable la IP puede cambiar (IP's dinámicas) por lo que será necesario indicarle la IP que tiene en cada momento.

Ya tenemos la conexión VPN lista para funcionar. Si trabajamos con conexiones lentas (módem o similar) la VPN también irá lenta. Es recomendable disponer de conexiones de banda ancha para sacarle todo el rendimiento a este tipo de conexiones.

Para realizar las comunicaciones usando la VPN deberemos usar las IP's de la VPN. Es decir, además de la IP de Internet que tiene el servidor y los clientes se han generado otras IP's internas de la VPN, pues esas deberemos usar para comunicarnos

con los equipos de la VPN, estas se obtendrán como las habituales, pero en el icono de la nueva conexión que aparece en la barra de notificación (junto al reloj).

En conexiones lentas, el Explorador de Windows no será capaz de mostrar los otros equipos de la red, o le llevará mucho tiempo, en ese caso, podremos acceder a ellos escribiendo en la barra de direcciones del Explorador de Windows "\\ip_en_la_VPN" o "\\nombre_maquina" de la máquina a la que queremos acceder, por ejemplo, si la IP (en la VPN) de la otra máquina es 169.254.3.117 pondremos \\169.254.3.117 en la barra de direcciones del Explorador de Windows. Para usar otros recursos, como servidores de base de datos, etc. simplemente usamos la IP en la VPN de la máquina destino.

5.2 Configuración de una VPN bajo LINUX

Para esta configuración usaremos OpenVPN, el cual es una solución de conectividad basada en software: SSL (*Secure Sockets Layer*) VPN *Virtual Private Network* (Red Privada Virtual), OpenVPN ofrece conectividad punto-a-punto con validación, para host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas entre otras. Está publicado bajo licencia de código-libre (OpenSource).

En el siguiente capítulo se dará una descripción detallada de la instalación y la configuración de OpenVPN para la posterior implementación del túnel VPN

CAPITULO VI

APLICACION PRÁCTICA DE UNA VPN

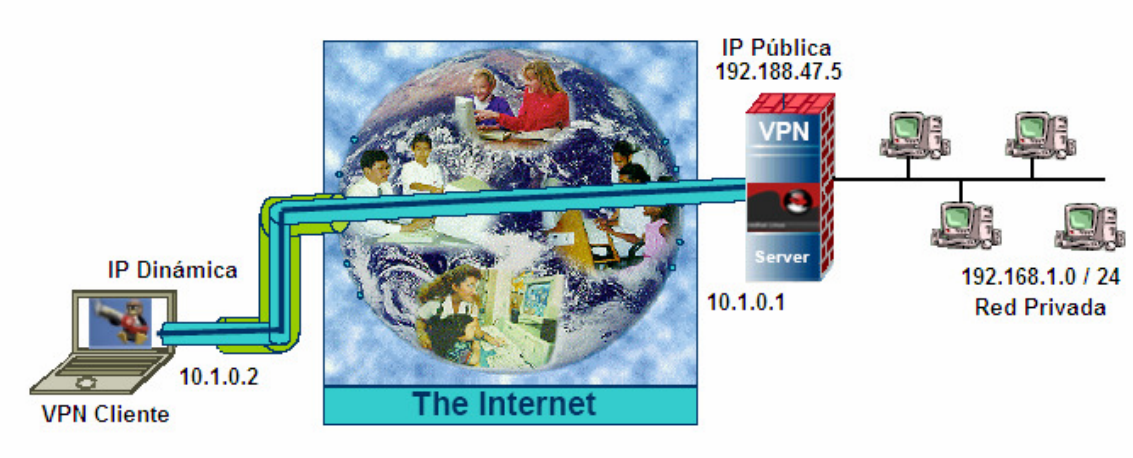


Figura 6.1 – Esquema para la configuración de la VPN

Se tratará de describir la configuración de un sistema completo de una VPN utilizando una computadora con sistema operativo Linux Centos 4.2 el que servirá como servidor VPN, y una computadora personal con Windows XP el que será el cliente VPN (Fig. 6.1).

En nuestro ejemplo, tanto las redes privadas del cliente como la del servidor se unen a Internet por medio de dos puertas de enlace, teniendo el servidor una dirección IP pública y el PC cliente una dirección IP dinámica. La máquina que actúa como Servidor VPN será la puerta de enlace y tendrá dos interfaces de red, una conectada a la red privada y la otra conectada a Internet. Las puertas de enlace dan soporte a los servicios NAT y VPN para las máquinas de las redes privadas. Tanto la configuración del Cliente como la del Servidor son casi simétricas exceptuando que el Servidor tiene una dirección IP fija mientras que la del Cliente tiene una dirección IP dinámica (DHCP).

Parámetros de configuración para la red del Cliente y del Servidor

	Cliente	**Servidor**
Subred ethernet local (Dirección privada)	No se usará subred	192.168.1.0/24
Extremo del túnel (Dirección privada)	10.1.0.2	10.1.0.1
Puerta de enlace OpenVPN (Dirección pública)	cliente DHCP, no necesita ser especificada	192.188.47.5

6.1 Configuración del Servidor VPN bajo Linux Centos 4.2

Para configurar la VPN se utilizara el software OpenVPN.

Instalando OpenVPN

Si no se dispone de la biblioteca OpenSSL debe descargarla e instalarla. Si se utiliza un Linux 2.2 o anterior se debe descargar el controlador TUN/TAP. Los usuarios de Linux 2.4.7 o superior deberían tener el controlador TUN/TAP ya incluido en el kernel.

Descargar ahora la última versión de OpenVPN, se puede utilizar el siguiente enlace: http://prdownloads.sourceforge.net/openvpn/openvpn-1.6.0.tar.gz

Instalar el paquete tar

Descomprimir el paquete:
gzip -dc openvpn-1.6.0.tar.gz | tar xvf

Compilar OpenVPN:

cd openvpn-1.6.0
./configure
make
make install

El comando
./configure --help
muestra todas las opciones de configuración.

Configuración del controlador TUN/TAP

Pasos de configuración a realizar una única vez
Si se esta usando Linux 2.4.7 o superior, es probable que el controlador TUN/TAP este ya incluido en el kernel. Se puede confirmar con el comando:

locate if_tun.h

Esto debe mostrar un fichero como /usr/include/linux/if_tun.h.

Para Linux 2.4.7 o superior (nuestro caso), se usa el siguiente comando para crear el nodo del dispositivo TUN/TAP:
mknod /dev/net/tun c 10 200

Si se está usando Linux 2.2 se debe descargar la versión 1.1 del modulo del kernel TUN/TAP y seguir las instrucciones de instalación.

Pasos de configuración a realizar cada vez que se arranque

En Linux antes de usar OpenVPN, o cualquier otro programa que utilice dispositivos TUN/TAP, se debe cargar el modulo del kernel TUN/TAP:

modprobe tun

Habilitar IP forwarding:

echo 1 > /proc/sys/net/ipv4/ip_forward

Construir una clave estática pre-compartida

Generar una clave estática con el siguiente comando:

openvpn --genkey --secret static.key
La clave estática está formateada en ascii y tiene un aspecto como éste:

```
-----BEGIN OpenVPN Static key V1-----
e5e4d6af39289d53
171ecc237a8f996a
97743d146661405e
c724d5913c550a0c
30a48e52dfbeceb6
e2e7bd4a8357df78
4609fe35bbe99c32
bdf974952ade8fb9
71c204aaf4f256ba
eeda7aed4822ff98
fd66da2efa9bf8c5
e70996353e0f96a9
c94c9f9afb17637b
283da25cc99b37bf
6f7e15b38aedc3e8
e6adb40fca5c5463
-----END OpenVPN Static key V1-----
```

Un fichero de clave estática OpenVPN contiene suficiente entropía como para almacenar tanto una clave cifradora de 512 bits como una clave HMAC de 512 bits para autenticación.

Copiar static.key al otro extremo por medio de un medio seguro.

Fichero de configuración usando una clave estática pre-compartida

Se va a usar un fichero de configuración de OpenVPN. OpenVPN permite pasar opciones en la línea de comandos o en uno o más ficheros de configuración. Las

opciones de los ficheros de configuración pueden omitir los caracteres iniciales "--" necesarios para las opciones de la línea de comandos.

/Openvpn1.6.0/sample-config-files/servidor.conf

```
# Fichero de configuración de OpenVPN para
# el servidor usando una clave estática pre-compartida.
# '#' o ';' pueden usarse para delimitar comentarios.

# Usar un dispositivo tun dinámico.
# OpenVPN también soporta dispositivos ethernet
# virtuales "tap".
dev tun

# 10.1.0.1 es nuestro extremo local VPN (Servidor).
# 10.1.0.2 es nuestro extremo remoto VPN (Cliente).
ifconfig 10.1.0.1 10.1.0.2

# Script que establecerá las rutas de la subred
# cuando la VPN esté activa.
up ./office.up

# Nuestra clave estática pre-compartida
secret static.key

# OpenVPN utiliza el puerto 1194 UDP por defecto.
# lport o rport pueden usarse
# para denotar diferentes puertos
# para local y remoto.
port 5000
```

```
# Detección mas fiable cuando el sistema
# pierde su conexión.  Por ejemplo, conexiones telefónicas o portátiles que
# se desplazan a otros sitios.
ping 15
ping-restart 45
ping-timer-rem
persist-tun
persist-key

# Nivel de información.
# 0 -- callado excepto en errores fatales.
# 1 -- casi callado, pero mostrar errores no-fatales de red.
# 3 -- información media, para funcionar normalmente.
# 9 -- mucha información, útil para resolución de problemas
verb 3
```

/Openvpn1.6.0/sample-config-files/office.up

```
#!/bin/bash
route add -net 192.168.1.0  netmask 255.255.255.0 gw $5
```

6.2 Configuración del Cliente VPN bajo Windows XP

Para la configuración del cliente VPN en Windows usamos el mismo software OpenVpn con la versión ejecutable para Windows XP: openvpn-2.0.5-install.exe.

Una vez instalado el programa se va a Inicio/Programas/OpenVpn/Add a new Tap-Win32 virtual ethernet Adapter.

Luego de esto OpenVpn esta listo para ser activado con cualquier archivo de configuración .ovpn.

Fichero de configuración para el Cliente VPN usando una clave estática pre-compartida

Se va a usar un fichero de configuración de OpenVPN llamado cliente.ovpn. El archivo static.key que fue creado en el Servidor VPN el cual es la clave estática debe ser colocado en la misma carpeta de cliente.ovpn.

C:/Archivos de Programas/OpenVpn/config/cliente.ovpn

```
# Fichero de configuración de OpenVPN para
# Cliente usando una clave estática pre-compartida.
# '#' o ';' pueden usarse para delimitar comentarios.

# Usar un dispositivo tun dinámico.
# OpenVPN también soporta dispositivos ethernet
# virtuales "tap".
dev tun

# Nuestro extremo OpenVPN es la puerta de enlace del Servidor.
remote 192.188.47.5

# 10.1.0.2 es nuestro extremo local VPN (Cliente).
# 10.1.0.1 es nuestro extremo remoto VPN (Servidor).
ifconfig 10.1.0.2 10.1.0.1

# Clave estática pre-compartida
secret static.key

# Puerto que OpenVPN va a utilizar.
# lport o rport pueden usarse
# para denotar diferentes puertos
# para local y remoto.
port 5000
```

```
# Establecerá las rutas de la subred remota
# cuando la VPN esté activa.
route 192.168.1.0 255.255.255.0

# Detección mas fiable cuando el sistema
# pierde su conexión.  Por ejemplo, conexiones telefónicas o portátiles que
# se desplazan a otros sitios.
ping 15
ping-restart 45
ping-timer-rem
persist-tun
persist-key

# Nivel de información.
# 0 -- callado excepto en errores fatales.
# 1 -- casi callado, pero mostrar errores no-fatales de red.
# 3 -- información media, para funcionar normalmente.
# 9 -- mucha información, útil para resolución de problemas
verb 3
```

6.3 Arrancar la VPN en modo clave estática

En el Servidor, arrancar la VPN con el comando:
openvpn --config servidor.conf

Con el Cliente, arrancar la VPN con el comando:
openvpn --config cliente.ovpn

6.4 Pruebas de Funcionamiento de la Red Privada Virtual

Para las siguientes prácticas nos basaremos en la configuración de las redes indicada en la figura 6.1.

Con el Cliente, compruebe la VPN realizando un ping al Servidor a través del túnel: ping 10.1.0.1

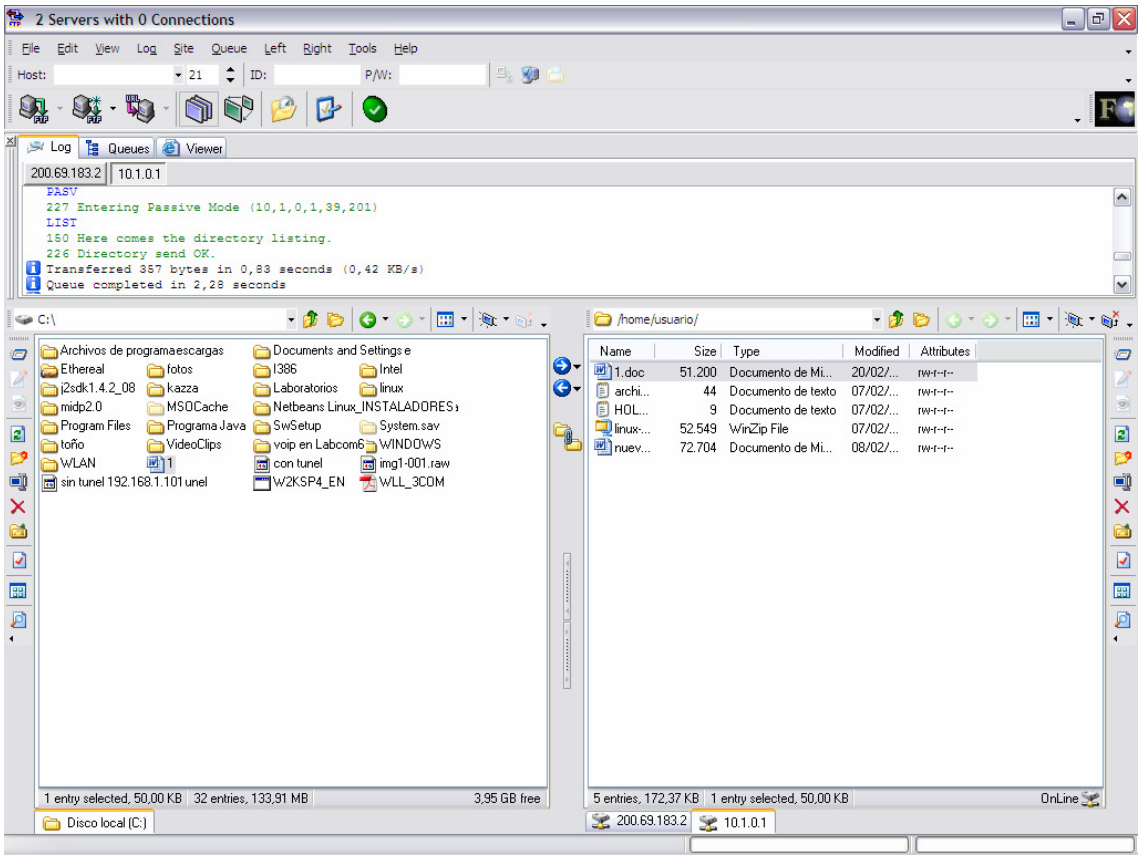
En el Servidor, compruebe la VPN realizando un ping al Cliente a través del túnel: ping 10.1.0.2

Si estas pruebas fallan, se puede re-editar los ficheros de configuración y poner el nivel de información a 9, lo cual producirá información de depuración mucho más detallada.

Si estas pruebas tienen éxito, ahora se puede realizar un ping a través del túnel usando máquinas en la red privada que no sean las puertas de enlace, para probar el ruteado de paquetes. Básicamente la PC que es Cliente VPN podrá acceder a cualquier máquina en la subred 192.168.1.0 y viceversa.

Transmisión de información entre los dos puntos

Para realizar la transmisión de la información entre los dos puntos de la VPN utilizaremos el Protocolo FTP para lo que se empleará el software AceFTP pro 3 en Windows y gFTP en Linux.

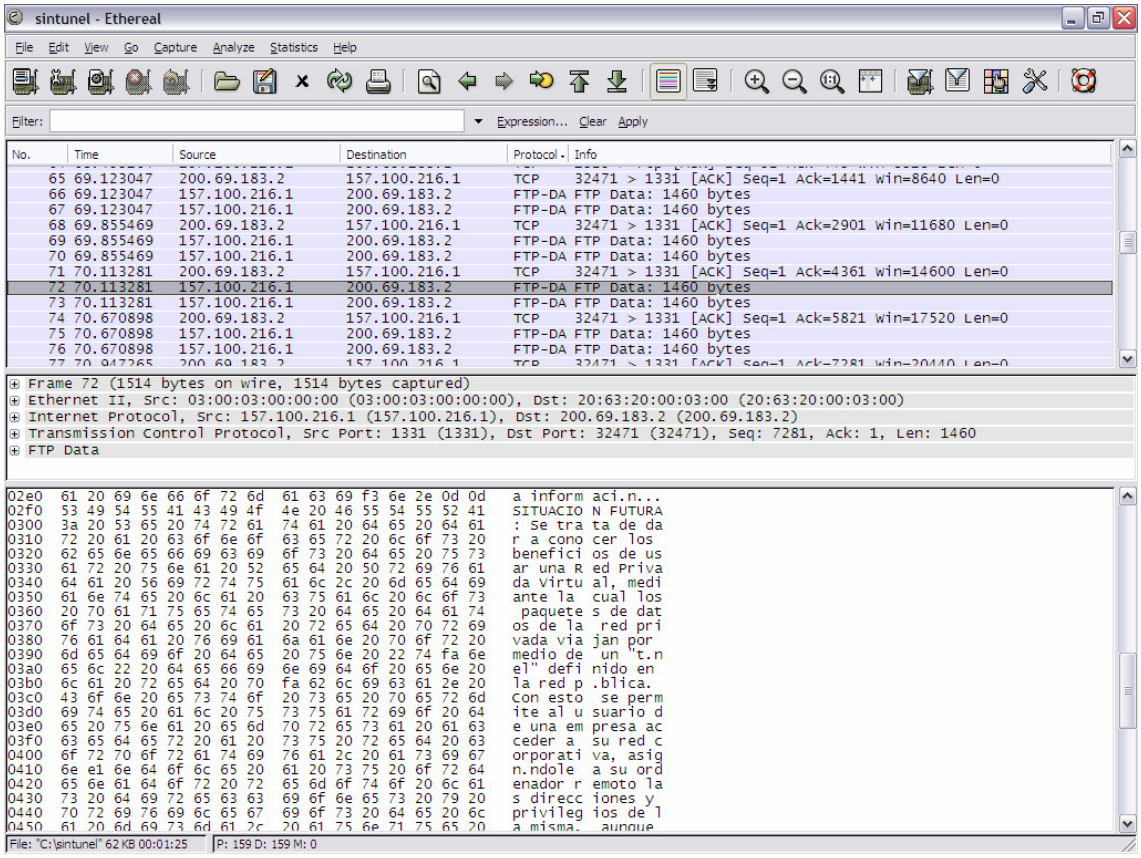


También se utilizará un software (Ethereal) que nos permitirá capturar la información que se está transmitiendo por la Red para poder comprobar que los datos enviados por medio del túnel viajan encriptados y no pueden ser interpretados por intrusos en la red.

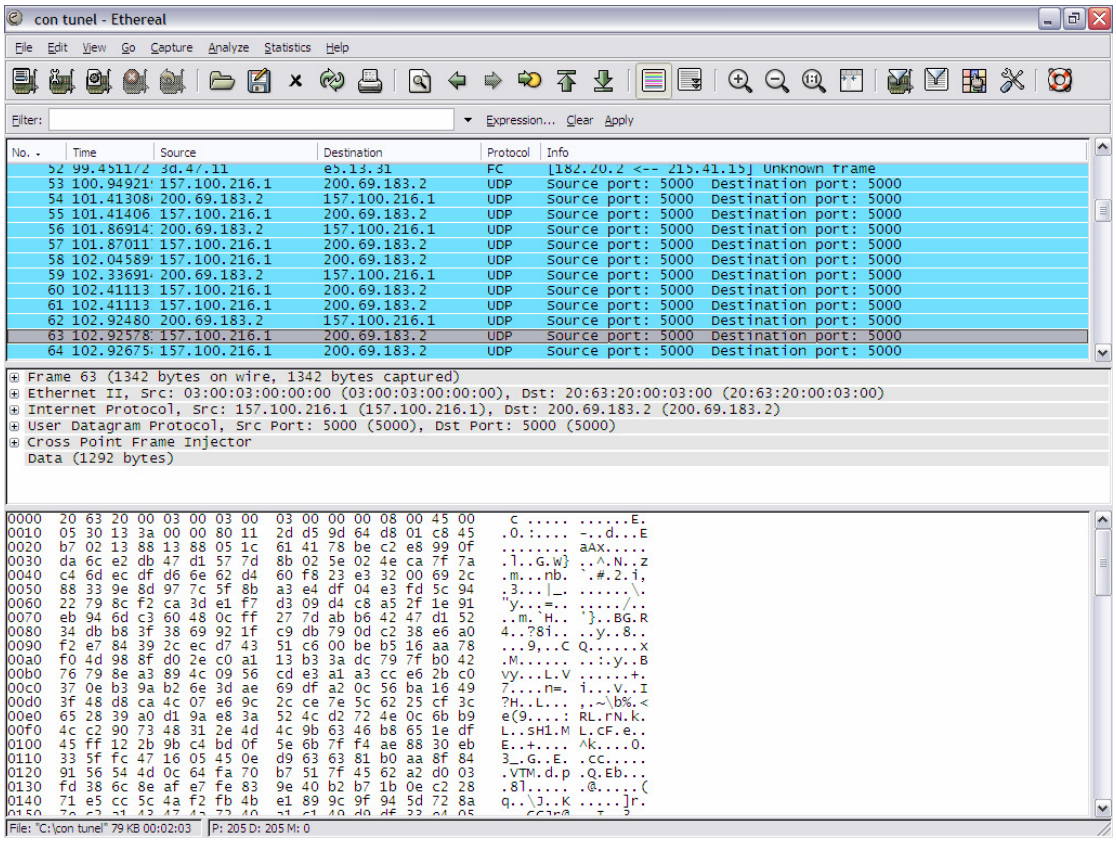
Caso Práctico 1

Se establecerán dos conexiones entre el Cliente VPN con Windows XP y el Servidor VPN con Linux. Una conexión se realizara por medio del túnel con la dirección privada de la VPN 10.1.0.1. y la otra conexión se realizara a la dirección publica del servidor en Internet 192.188.47.5. Se capturara la información trasmitida en ambos casos.

Captura sin utilizar el túnel



Captura utilizando el túnel



Como se puede observar en la conexión con el túnel los datos son incomprensibles y no se puede descifrar su contenido ya que la información esta encriptada y viaja bajo el protocolo UDP, en cambio en el caso que no se usa el túnel VPN los datos se pueden leer claramente, la información es accesible a cualquier intruso y utiliza el protocolo FTP-DATA.

Caso práctico 2

Se establecerán dos conexiones entre el Cliente VPN con Windows XP y una computadora de la red privada 192.168.1.0 / 24, como se observa en el esquema anterior.

En este caso si hacemos un ping de un extremo al otro podemos verificar que existe conexión entre los dos puntos, cuya conexión puede existir solamente cuando la VPN este activa ya que en caso contrario no tendrían forma de conectarse.

De esta manera también se puede realizar cualquier tipo de transmisión de datos entre estos dos puntos, pudiendo así mismo utilizar un cliente y un servidor FTP para la transmisión de archivos. Teniendo en cuenta que la información siempre viajara por el túnel creado entre el cliente VPN y el servidor VPN, y este a su vez distribuirá la información por su subred hasta alcanzar al host requerido.

CAPITULO VII

CONCLUSIONES Y RECOMENDACIONES

7. 1 CONCLUSIONES

Como pudimos observar durante el desarrollo del presente trabajo, una red privada virtual conecta los componentes de una red con otra y opera a través de una red pública, que bien ésta puede ser Internet. Aparentemente las VPN parecen tener el mismo segmento de LAN, pero en realidad están a varias redes de distancia.

Las VPN son de gran utilidad para los usuarios, porque les proporciona acceso remoto a recursos corporativos sobre Internet público y mantiene al mismo tiempo la privacidad de su información incluyendo la integridad de los datos al viajar a través de Internet. Además de que les brinda la certeza de que están trabajando en un canal seguro.

Así toda la información que esté navegando, estará segura de cualquier ataque en la red, por navegadores, curiosos o inexpertos y principalmente de los hackers. Y además el acceso a este tipo de redes será exclusiva para las personas o grupos que estén suscritos a una VPN.

Las Redes Virtuales Privadas son una opción más para que las grandes y pequeñas empresas se mantengan a salvo de cualquier intento de ataque en contra de esa información tan valiosa. Asimismo pueden auxiliarse de la amplia tecnología de vanguardia en cuanto a software y hardware se refiere.

Debemos tomar conciencia de que la tecnología de vanguardia muchas veces se aplica para mal (para violar información privada); pero que en muchas otras ocasiones ésta misma se encuentra en buenas manos y nos permite comunicar rápidamente y sobre todo ser transmitida de una forma segura y confiable.

7.2. RECOMENDACIONES

Recomendamos utilizar las Redes Virtuales Privadas ya que ofrecen posibilidades de expansión a los empresarios, por lo que de muchas redes pequeñas se puede "visualizar" una red muy grande lo cual proporciona mayor cobertura, además de ser un medio de comunicación realmente seguro y que facilita que la información sea actualizada, oportuna y recalcamos son un medio seguro.

GLOSARIO

IP Protocolo de Internet (Internet Protocol)

WAN Red de área Extensa (Wide Area Network)

ISP Proveedor de servicio de Internet (Internet Service Provider)

LAN Red de área local (Local Area Network)

CHAP Protocolo de Autenticación (Challenge Handshake Authentication Protocol)

RSA Sistema criptográfico con clave pública

IPSec Protocolo IP de Seguridad (IP Security Protocol)

L2TP Protocolo d Tunneling de capa dos (Layer 2 Tunneling Protocol)

ADSL Línea de Abonado Digital Asimétrica (Asimetric Digital Subscriber Line)

PPTP Protocolo de *Tunneling* punto a punto (Protocol Tunneling point to point)

GRE Encapsulación de la Ruta Genérica (Generic Routing Encapsulation)

SSL/TLS Secure Sockets Layer y Transport Layer Security

L2F *Forwarding* de capa dos (Layer 2 Forwarding)

IPIP IP en IP (IP-in-IP)

MPPE Encriptación Punto a Punto Microsoft (Microsoft Point2Point Encryption)

PAP Protocolo de Autentificacion de Password (Protocol Autentification Password)

RAS Servidor de Acceso Remoto (Remote Access Server)

AH Protocolo de Autenticación (Authentication Protocol)

ESP Carga útil de Seguridad encapsulada (Encapsulated Security Payload)

SA Asociaciones de Seguridad (Security Associations)

PKI Infraestructura de claves públicas (Publics Keys Infrastructure)

IDEA Algoritmo de Encriptación de Datos Internacional (International Data Encryption Algorithm)

DES Estándar de Encriptación de Datos (Data Encryption Standard)

AES Estándar Avanzado de Encriptación (Advanced Encryption Standard)

LAC Concentrador de Acceso L2TP (L2TP Access concentrador)

LNS Servidor de red L2TP (L2TP Network Server)

NAT Traducción a direcciones de red (Network Address Translation)

DHCP Protocolo de configuración de Host Dinámicos (Dinamic Host Configuration Protocol)

PPP Protocolo Punto a Punto (Point to Point Protocol)

HTTP Protocolo de transferencia de Hipertexto (Hypertext Transfer Protocol)

UDP Protocolo de datagrama del usuario (User Datagram Protocol).

TCP Protocolo de Control de Transmisión (Transmision Control Protocol).

FR Frame Relay.

ISDN Red digital de Servicios Integrados (Integrated Services Digital Network)

CAR Committed Access Rate

WFQ Weighted Fair Queuing

WRED Weighted Random Early Detection

GTS Generic Traffic Shaping

WiFi Wireless Fidelity

NAS Almacenamiento ligado a la red (Network-Attached Storage).

BIBLIOGRAFIA

- Articulo de Robert Bova. Disponible en la web: <http://intranetjournal.com/articles/200110/vpn_10_03_01a.html> [ref. de 13 de diciembre del 2005].

- Rincón del programador. Disponible en la web: <http://www.elrincondelprogramador.com/?pag=articulos/leer.asp&id=55> [ref. de 13 de diciembre del 2005].

- Enciclopedia Wikipedia. Disponible en la web: <http://es.wikipedia.org/wiki/Redes_Privadas_Virtuales> [ref. de 13 de diciembre del 2005].

- Organización OpenVPN. Disponible en la web: <http://openvpn.sourceforge.net/> [ref. de 13 de diciembre del 2005].

- Articulo de Tina Bird. Disponible en la web: <http://vpn.shmoo.com/> [ref. de 13 de diciembre del 2005].

- Articulo de Computer Consultants. Disponible en la web: <http://www.caconsultant.com/Article/VPN/demand_of_the_changing_world> [ref. de 13 de diciembre del 2005].<

- Manejo de las VPN bajo Windows. Disponible en la web: <http://www.microsoft.com/latam/technet/articulos/20008/art04/default.asp> [ref. de 13 de diciembre del 2005].

- Organización Linuca. Disponible en la web: <http://linuca.org/> [ref. de 13 de diciembre del 2005].

- Software OpenVpn. Disponible en la web: <http://www.openvpn.net/> [ref. de 6 de enero del 2006].