UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

"ESTUDIO DE LAS TECNOLOGÍAS WINDOWS NT Y GNU/LINUX PARA LA CREACIÓN DE REDES VIRTUALES DE TRABAJO SEGURAS, BAJO INFRAESTRUCTURA PÚBLICA (INTERNET)"

T E S I S

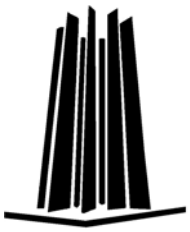
QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

MOISÉS GARCÍA HERNÁNDEZ

ASESOR DE TESIS:
M. EN C. JESÚS HERNÁNDEZ CABRERA



MÉXICO, 2007.

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Dedicatoria

Por el profundo amor y cariño que siempre guardare y que a pesar de las adversidades los tendré muy presentes, son y serán siempre base primordial de mi formación, con todo amor para mi madre Felipa Hernández García y para mi padre Cipriano García Crispín, por su tolerancia, confianza, sacrificio y dedicación, gracias.

A mi esposa Efigenia Cortes Hernández por su apoyo, comprensión, cariño y amor, por que siempre confió en mí para alcanzar esta meta, por ser madre de mis pequeños Moisés David García Cortes, ángel de mi corazón y Andrea Joscelyn García Cortes, reina de mi vida, a ustedes y por ustedes.

Gracias a mis padres por que siempre estuvieron presentes con su apoyo y cariño en mi formación como profesional, siempre los llevare en mi corazón.

Gracias a mi esposa por su amor y confianza, por darme su tiempo en la realización de este trabajo.

Gracias hijos Moisés y Andrea, por existir y ser luz en mi camino, y alegría de mi corazón.

Gracias a mis hermanos Joaquín, Jorge, Miriam y Julián Alejandro, por que siempre me dieron una palabra de aliento y comprensión para continuar en este camino.

Gracias a mis abuelos paternos Julián y Trinidad, maternos Victoria† y Carlos, por enseñarme lo que es la humildad y nunca olvidarme de mis raíces.

Gracias a mis cuñados Moises Alba y Mónica Hernández, por su apoyo.

Gracias a mis sobrinos por ser parte de las alegrías de la familia, pequeños traviesos.

Gracias a cada una de esas personas que nunca dejaron de confiar en mí y que siempre me apoyaron aun en los peores momentos de mi vida.

Gracias a mis amigos de trabajo por que siempre estuvieron ahí y me brindaron su apoyo.

Gracias amigo y hermano M. en C. Jesús Hernández Cabrera, por que confiaste en mí y me diste la oportunidad de continuar con este trabajo de titulación, por tu esfuerzo y dedicación.

Gracias a mis revisores de tesis, Ing. José Manuel Quintero C., Ing. Arturo Ocampo A., M. en I. Arcelía Bernal D., M. en C. Felipe de Jesús Gutiérrez L. por su profesionalismo y su tiempo.

Gracias M. en C. Marcelo Pérez Medel, Jefe de la Carrera Ingeniería en Computación por su dedicación, apoyo y profesionalismo en su trabajo.

Gracias Universidad Nacional Autónoma de México, por dejarme ser parte de tu comunidad, por formarme como profesional y por ser mi Alma Mater.

ÍNDICE

II.- AMBIENTES DE TRABAJO VIRTUAL VPN BAJO LA PLATAFORMA WINDOWS NT

III.- AMBIENTE DE TRABAJO VIRTUAL VPN BAJO LA PLATAFORMA GNU/LINUX

INTRODUCCIÓN

Hoy en día las redes informáticas se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes informáticas reducen en tiempo y costos, los gasto de las empresas o corporaciones, eso ha significado una gran ventaja sobre todo para aquellas que cuentan con oficinas o usuarios remotos a varios kilómetros de distancia, pero también es cierto que estas redes han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad en las redes es de suma importancia, de ahí el origen de este trabajo de tesis cuyo principal objetivo es profundizar más en el tema de las Redes Privadas Virtuales (VPN), conocer las opciones y herramientas que nos ofrece esta nueva manera de crear una red privada sobre una infraestructura pública ya establecida como lo es Internet, además que nos brinde mayor seguridad en la transmisión de nuestra información, facilidad de uso y manejo, bajo costo de implementación, cuidado en la integridad de la información y compatibilidad en la creación de nuestra VPN.

La presente tesis busca solucionar estos problemas enfocándose en la solución de uno solo en concreto: que es la necesidad que existe en el Laboratorio de Cómputo y de la creación de una VPN, cumpliendo con los objetivos que anteriormente mencionamos.

Para iniciar con este proyecto se analizaron los requerimientos que existen en el Laboratorio de Cómputo del Centro Tecnológico de Aragón, principalmente permitir trabajar a los desarrolladores en los proyectos que ahí se realizan a través de Internet y en ubicaciones geográficamente diferentes al Laboratorio, dicho proceso lleva a la utilización de la red pública como lo es Internet, como un medio de comunicación existente y de bajo costo, eliminando así la necesidad de tener que generar un contrato costoso de líneas dedicadas y dirigidas a dicho laboratorio.

También se estudiaron y analizaron dos de los sistemas operativos más conocidos en el ámbito informático para la implementación de una VPN como son: Microsoft Windows NT en su versión Server 2000 y GNU/Linux en su distribución Ubuntu basado en Debian, dichos sistemas fueron implementados para su estudio y su análisis trabajando con las herramientas que nos ofrece para la creación de Redes Privadas Virtuales.

Continuando con los requerimientos solicitados por el Laboratorio de Cómputo, una de las principales problemáticas y preocupaciones es la seguridad de los datos que viajan a través de la red Internet, siendo éste uno de los aspectos más importantes de este proyecto. Se analizaron los protocolos de túnel, los protocolos de cifrado y los métodos de autenticación que conllevan las Redes Privadas Virtuales, otra de las opciones que se pueden manejar son los dispositivos electrónicos de uso especifico para VPN, como por ejemplo: una Plataforma de Multiservicio de Acceso VPN 3600 de Cisco Systems o un Concentrador Cisco VPN 3000, el cual nos brinda seguridad en la transmisión de los datos pero que su costo es muy alto.

Los conceptos relacionados con las VPN y la descripción de los protocolos como sistemas de seguridad se analizaron para su estudio en el capítulo 1, en él encontraremos los conceptos necesarios y una descripción de los diferentes tipos de VPN. También describimos los elementos que la componen, sus propiedades, así como el manejo de Protocolos de Autenticación y Cifrado que conlleva estas redes al establecer una comunicación de forma segura.

En el capítulo 2 analizamos el sistema operativos Windows NT 2000 Server como una de las principales plataformas en el manejo de VPN, y las herramientas que este nos ofrece para la seguridad de nuestro servidor de usuarios y archivos, así como la seguridad en la implementación de nuestra red privada.

En el capítulo 3 analizamos otra de las plataformas como sistema operativo de Software Libre GNU/Linux para la implementación de la VPN como otra opción y que nos brinda herramientas importantes de seguridad como lo es su núcleo basado en UNIX.

En el capítulo 4 implementamos lo que son nuestras VPN en ambos sistemas operativos para el análisis de trabajo y funcionalidad, obteniendo resultados para una toma de decisión en el manejo de una de las dos plataformas que más se adecué a las necesidades del Laboratorio de Cómputo, para así obtener por ultimo la decisión final de tecnología a emplear.

Finalmente se expone la evaluación y conclusiones de este trabajo considerando las pruebas realizadas al implementar nuestra VPN, obteniendo los resultados deseados y la decisión correcta en la elección de nuestros elementos para la creación de dicha VPN.

OBJETIVO GENERAL

- Analizar la tecnología VPN e implementar a través de Windows NT y GNU/LINUX un ambiente de trabajo virtual de acceso remoto (VPN) que permita a los usuarios del Laboratorio de Cómputo trabajar remotamente en los proyectos que ahí se realizan, implementándolo sobre la red de infraestructura pública (INTERNET), esto con el fin de ahorrar tiempo en los avances de los proyectos, costos en infraestructura, seguridad en los datos, confiabilidad y expansión de nuestra red LAN.

OBJETIVOS ESPECÍFICOS

- Definir los conceptos básicos sobre la Redes Privadas Virtuales VPN y determinar las ventajas que tienen sobre otras tecnologías de acceso remoto.

- Conocer las tecnologías de sistemas operativos NT y GNU/LINUX, para el desarrollo de VPN´s: sus conceptos y configuración.

- Realizar las pruebas para determinar que tecnología en sistemas operativos nos ofrece un mejor manejo de las VPN.

- Aplicar conforme a los requerimientos solicitados en el laboratorio de cómputo la mejor plataforma en sistema operativo y VPN, que ayude a cubrir las necesidades en cuanto a costo, seguridad, confiabilidad y expansión en la Red LAN.

- Evaluar los resultados del proyecto VPN implementado en el laboratorio de cómputo.

CAPÍTULO I

REDES PRIVADAS VIRTUALES (VPN's)

- Definir los conceptos básicos de las Redes Privadas Virtuales VPN y determinar las ventajas que tienen sobre otras tecnologías de acceso remoto.

I. ANTECEDENTES.

En los últimos años, las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de las famosas Redes Privadas Virtuales (VPN) y su infraestructura a bajo costo.

I.1 DEFINICIÓN DE UNA VPN.

Una red privada virtual (VPN) es la extensión de una red LAN que utiliza un canal de comunicación público como lo es Internet, mediante técnicas de cifrado, encapsulamiento y autenticación, se protegen los datos que viajaran a través de un túnel que pasara por ese medio de comunicación y solo se vera como una red LAN única y privada combinada con infraestructura pública. Ver Figura 1.1.

Para emular un vínculo punto a punto, los datos se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red compartida o pública hasta alcanzar su destino. Para emular un vínculo privado, los datos se cifran para asegurar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar si

no se dispone de las claves de cifrado. El vínculo en el que se encapsulan y cifran los datos privados es una conexión de red privada virtual (VPN).

Una Red Privada Virtual se extiende, mediante un proceso de encapsulación y en su caso de cifrados, de los paquetes de datos a distintos puntos remotos mediante el uso de una infraestructura pública de transporte. Los paquetes de datos de la red privada viajan por medio de un “túnel” definido en la red pública.

La red privada basada en Internet recibe el calificativo de virtual dado que para una organización o compañía la red se muestra como una red privada dedicada y con uso exclusivo de toda la infraestructura intermedia, aunque realmente todo esto se aleje de la realidad. El tráfico de una red VPN y el tráfico propio de Internet atraviesan la infraestructura de ésta en una base paquete-a-paquete. Dado que todos los usuarios perciben únicamente su propio trafico, la red da la apariencia de estar físicamente dentro de una red LAN.

Técnicamente, cualquier red privada puede ser considerada como virtual dado que emplea una red telefónica conmutada de carácter público para sus comunicaciones, No obstante, y dado que el punto de vista, está basado en la semántica y no en las características o requisitos de la red, los conceptos de red privada basada en red telefónica conmutada y red privada virtual basada en Internet son diferentes.

Los únicos requisitos para redes privadas virtuales basadas en Internet se presentan en cuatro áreas claves: compatibilidad, interoperabilidad, disponibilidad y seguridad.

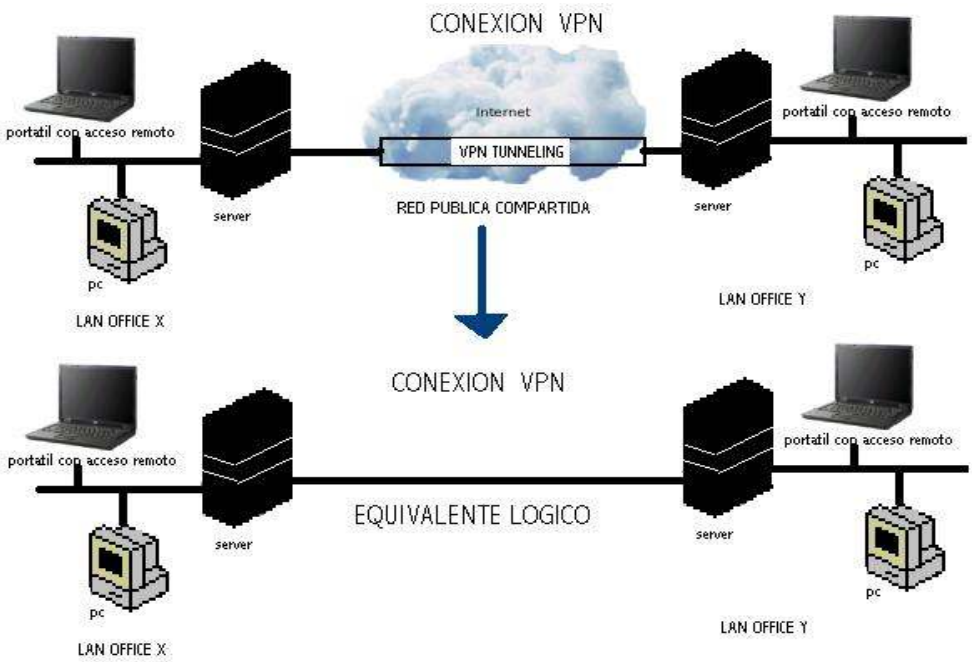


Figura 1.1 Equivalente lógico de una conexión VPN.

Los usuarios que trabajan en casa o que están de viaje pueden usar conexiones VPN para establecer una conexión de acceso remoto al servidor de una organización mediante la infraestructura que proporciona una red pública como Internet. Desde la perspectiva del usuario, la red privada virtual es una conexión punto a punto entre el equipo (el cliente VPN) y el servidor de la organización (el servidor VPN). La infraestructura exacta de la red compartida o pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado.

Las organizaciones también pueden utilizar conexiones VPN para establecer conexiones enrutadas con oficinas alejadas geográficamente o con otras organizaciones a través de una red pública como Internet al mismo tiempo que realizan comunicaciones seguras. Una conexión VPN enrutada a través de Internet funciona lógicamente como un vínculo de WAN dedicado.

Gracias al acceso remoto y a las conexiones enrutadas, una organización puede utilizar conexiones VPN para realizar conexiones a larga distancia, o líneas concedidas para conexiones locales o con un Proveedor de servicios Internet (ISP).

I.2 ELEMENTOS DE UNA CONEXIÓN VPN.

Uno de los elementos principales que nos ayudan a realizar una conexión VPN es el Sistema Operativo de nuestro equipo de cómputo, existen hoy en día dos plataformas esenciales con lo cual es posible realizar nuestra conexión VPN y que son las más utilizadas por los usuarios de cómputo, Microsoft Windows y GNU/LINUX considerado como Software Libre.

Un Sistema Operativo es el conjunto de programas o software destinado a permitir la comunicación del usuario con un ordenador y gestionar sus recursos de manera cómoda y eficiente. Dicho sistema administrara tanto el Hardware como el propio Software que se encuentre instalado en ese momento.

Dentro de lo que es el Sistema Operativo podemos encontrar varias herramientas que son de utilidad para poder crear nuestro acceso remoto VPN entre los que se encuentran las conexiones de red y el acceso telefónico, las herramientas de administración de accesos y usuarios en Windows NT, monitoreo de red y algunos comandos de verificación de la conexión.

Las conexiones de red y de acceso telefónico permiten a su equipo conectarse a Internet, a una red o a otro equipo. Con Conexiones de red y de acceso telefónico, puede tener acceso a recursos y funciones de redes, ya sea que se encuentre físicamente en la ubicación de la red o en una ubicación remota.

Las conexiones se crean, configuran, almacenan y supervisan desde el sistema operativo y dentro del apartado de red y conexiones telefónicas.

Un cliente de acceso remoto (el equipo de un usuario) realiza una conexión VPN de acceso remoto que conecta a una red privada. El servidor VPN proporciona acceso a los recursos del servidor VPN o a toda la red a la que está conectado el servidor VPN. Los paquetes enviados desde el cliente remoto a través de la conexión VPN se originan en el equipo cliente de acceso remoto.

El cliente de acceso remoto (el cliente VPN) se autentica ante el servidor de acceso remoto (el servidor VPN) y, para realizar la autenticación mutua, el servidor se autentica ante el cliente.

Los equipos que ejecutan la plataforma Windows de Microsoft pueden crear conexiones VPN de acceso remoto a un servidor VPN que ejecuta de igual manera Windows para servidores. Los clientes VPN también pueden ser un cliente de Protocolo de Túnel Punto a Punto (PTPP) o un cliente de Protocolo de Túnel de Capa 2 (L2TP) con IPSec que no sean de Microsoft y que puedan estar instalados también el la plataforma de GNU/LINUX o algún otro sistema operativo.

Todas las conexiones de red y de acceso telefónico contienen un conjunto de características que se pueden utilizar para crear un vínculo entre su equipo y otro equipo de la red. Las conexiones salientes se ponen en contacto con un servidor de acceso remoto mediante un método de acceso configurado (LAN, MODEM, Línea ISDN (RDSI), Infrarrojos, Microondas, etc.) para establecer la conexión con la red. A la inversa, una conexión entrante habilita a un equipo que ejecuta Windows NT o GNU/LINUX independiente para que otros equipos se pongan en contacto con él. Es decir, su PC puede funcionar como servidor de acceso remoto. Ya esté conectado de forma local (LAN), remota (acceso telefónico, ISDN (RDSI), etc.) o ambas, se puede configurar cualquier conexión de forma que pueda ejecutar cualquier función de red necesaria. Por ejemplo, puede imprimir en

impresoras de la red, tener acceso a unidades y archivos, examinar otras redes o tener acceso a Internet.

Como todos los servicios y los métodos de comunicación están configurados en la propia conexión, no necesita utilizar herramientas de administración externas para configurar las conexiones (a excepción de los sistemas operativos para servidores). Por ejemplo, la configuración de una conexión de acceso telefónico incluye características utilizadas antes, durante y después de la conexión. Entre ellas se encuentran el Módem con el que marca, el tipo de cifrado de contraseñas que desea utilizar al conectar y los protocolos de red que va a utilizar después de conectar. El estado de la conexión, que incluye la duración y la velocidad de la conexión, se puede ver desde la misma conexión; no hay que utilizar una herramienta de supervisión externa.

I.2.1 Túneles y Protocolos.

-Aspectos Básicos.

El método de túneles es una forma de crear una red privada y es uno de los elementos principales que componen la estructura de una VPN. 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.

El enrutamiento punto a punto o tunneling, es un método que permite enviar datos a una red utilizando una red intermedia. Los datos que se transfieren se denominan carga y los dos extremos del túnel se denominan extremos finales del túnel o del canal. El paquete que se envía se encapsula utilizando la cabecera del protocolo de enrutamiento punto a punto. Los enrutadores de las redes

intermedias utilizan la cabecera del protocolo de enrutamiento punto a punto para enrutar el paquete al punto de destino final del túnel.

Los enrutadores de la red intermedia no saben que están enrutando un paquete de protocolo de enrutamiento punto a punto. Éstos tratan el paquete como uno más en la red. El paquete se origina en uno de los extremos del túnel y alcanza el otro extremo. En el extremo final del túnel, las cabeceras de los paquetes son extraídas y el paquete es enrutado a continuación a su destino final.

Hay que observar que este sistema de túnel incluye todo este proceso (encapsulación, transmisión y desencapsulamiento de paquetes).

Aunque la red de transito puede ser cualquier red, Internet es la solución más económica y la más utilizada como red de transito.

Existen muchos otros ejemplos de túneles que pueden realizarse sobre intranets corporativas. Y aunque la Internet proporciona una de las intranets más penetrantes y económicas, las referencias a Internet en este trabajo se pueden remplazar por cualquier otra intranet pública que actué como de tránsito.

Las tecnologías de túnel existen desde hace tiempo; algunos ejemplos de esa tecnología incluyen:

- Túneles SNA (System Networks Arquitecture) sobre intranets IP. Cuando se envía trafico de la arquitectura de la red el sistema SNA a través de una intranet IP corporativa, la trama SNA se encapsula en un encabezado UPN (User Principal Name) e IP.

- Túneles IPX para Novell NetWare sobre intranets IP. Cuando un paquete IPX se envía a un servidor NetWare o ruteador IPX, el servidor o ruteador envuelve el paquete IPX un encabezado UDP e IP, y luego lo envía a través de una intranet IP.

El ruteador IP a IPX de destino elimina el encabezado UDP e IP, y transmite el paquete al destino IPX

Además, se han introducido en los últimos años nuevas tecnologías de sistema de túneles, misma que son el enfoque principal de esta sección y que posteriormente se verán en función al sistema operativo o plataforma que se este manejando y que incluyen:

- Protocolo de Túnel Punto a Punto. Permite que se cifre el tráfico IP, IPX o NetBEUI, y luego se encapsule en un encabezado IP para enviarse a través de una red IP o una red pública IP, como Internet.
- Protocolos de Túnel Nivel 2. Permite que se cifre el tráfico IP, IPX o NetBEUI, y luego se envié sobre cualquier medio que de soporte a la entrega de datagramas punto a punto, como IPX, X.25, Frame Relay o ATM.
- Modo de Túnel de Seguridad IP. Deja que se cifre las cargas útiles IP y luego se encapsulen en un encabezado IP, para enviarse a través de una red corporativa o una red pública IP como Internet.

-Protocolos de túnel.

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

Un protocolo es un conjunto de reglas que gobierna el formato y el significado de las tramas, paquetes o mensajes que se intercambian entre capas homólogas.

La tecnología de túnel se puede basar en el protocolo del túnel de nivel 2 o de nivel 3; estos niveles corresponden al modelo de referencia de interconexión de sistemas abiertos.

Los protocolos de nivel 2 corresponden al nivel de enlaces de datos, y utilizan tramas como su unidad de intercambio. PPTP Y L2TP y el envió 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 enviara 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 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.

-Como funcionan los túneles.

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

I.2.1.1 Protocolo de Túnel Punto a Punto (PPTP).

El Protocolo de Túnel Punto a Punto (PPTP, Point-to-Point Tunneling Protocol) se admitió por primera vez en Windows NT 4.0 y Windows 98. PPTP es una extensión del Protocolo Punto a Punto (PPP) y aprovecha las ventajas de los mecanismos de autenticación, compresión y cifrado de PPP. La compatibilidad de cliente con PPTP está integrada en el cliente de acceso remoto de Windows XP.

La compatibilidad de servidor VPN con PPTP está integrada en los miembros de la familia Windows de Microsoft. PPTP se instala con el protocolo TCP/IP. En función de las opciones disponibles al ejecutar el asistente para la instalación del servidor de enrutamiento y acceso remoto, PPTP se configura para 5 ó 128 puertos PPTP.

PPTP y el Cifrado Punto a Punto de Microsoft (MPPE, Microsoft Point-to-Point Encryption) proporcionan los principales servicios VPN de encapsulación y cifrado de datos privados.

-Encapsulación.

Las tramas PPP (que consisten en un datagrama IP, IPX o Appletalk) se empaquetan con un encabezado de Encapsulación de Enrutamiento Genérico (GRE, Generic Routing Encapsulation) y un encabezado IP. En el encabezado IP están las direcciones IP de origen y de destino que corresponden al cliente VPN y al servidor VPN.

En la figura 1.2 se muestra la encapsulación PPTP para una trama PPP.

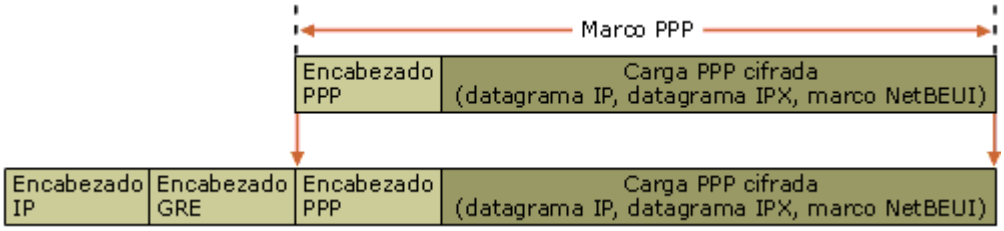


Figura 1.2 Encapsulación PPTP para una trama PPP.

-Cifrado.

La trama PPP se encripta con el Cifrado Punto a Punto de Microsoft (MPPE, *Microsoft Point-to-Point Encryption*) mediante claves de cifrado generadas en los procesos de autenticación MS-CHAP, MS-CHAP v2 o EAP-TLS. Los clientes de red privada virtual deben utilizar el protocolo de autenticación MS-CHAP, MS-CHAP v2 o EAP-TLS para poder cifrar las cargas de las tramas PPP. PPTP aprovecha el cifrado PPP subyacente y encapsula una trama PPP cifrada anteriormente.

Es posible utilizar una conexión PPTP no cifrada en la que la trama PPP se envíe como texto sin formato. Sin embargo, este tipo de conexión PPTP sin cifrado no se recomienda en conexiones VPN a través de Internet, ya que las comunicaciones de este tipo no son seguras.

I.2.1.2 Protocolo de Túnel de Nivel 2 (L2TP).

El Protocolo de Túnel de Nivel 2 (L2TP, Layer Two Tunneling Protocol) es un protocolo basado en RFC (Request For Comments) y estándar del sector que se admitió por primera vez en los sistemas operativos de cliente y de servidor Windows. A diferencia de PPTP, el protocolo L2TP en los servidores que ejecutan Windows Server 2003 no utiliza el Cifrado Punto a Punto de Microsoft (MPPE) para cifrar datagramas de Protocolo Punto a Punto (PPP). L2TP utiliza la Seguridad de Protocolos Internet (IPSec) para los servicios de cifrado. La combinación de L2TP e IPSec se conoce como L2TP/IPSec. L2TP/IPSec proporciona los servicios de red privada virtual (VPN) principales de encapsulación y cifrado de datos privados.

L2TP e IPSec deben ser compatibles con el cliente VPN y el servidor VPN. La compatibilidad de cliente con L2TP está integrada en el cliente de acceso remoto de Windows y la compatibilidad de servidor VPN con L2TP está integrada en los miembros de la familia Windows Server.

L2TP se instala con el protocolo TCP/IP. En función de las opciones disponibles al ejecutar el asistente para la instalación del servidor de enrutamiento y acceso remoto, L2TP se configura para 5 ó 128 puertos L2TP.

-Encapsulación.

La encapsulación de paquetes L2TP/IPSec consta de dos niveles:

1. Encapsulación L2TP. Las tramas PPP (que consisten en un datagrama IP o un datagrama IPX) se empaquetan con un encabezado L2TP y un encabezado UDP.

2. Encapsulación IPSec. El mensaje L2TP resultante se empaqueta a continuación con un encabezado y un finalizador de Carga de Seguridad de Encapsulación (ESP, Encapsulating Security Payload) de IPSec, un finalizador de autenticación IPSec que proporciona autenticación e integridad de mensajes y un encabezado IP final. El encabezado IP contiene las direcciones IP de origen y de destino que corresponden al cliente VPN y al servidor VPN.

La Figura 1.3 muestra la encapsulación L2TP e IPSec para un datagrama PPP.

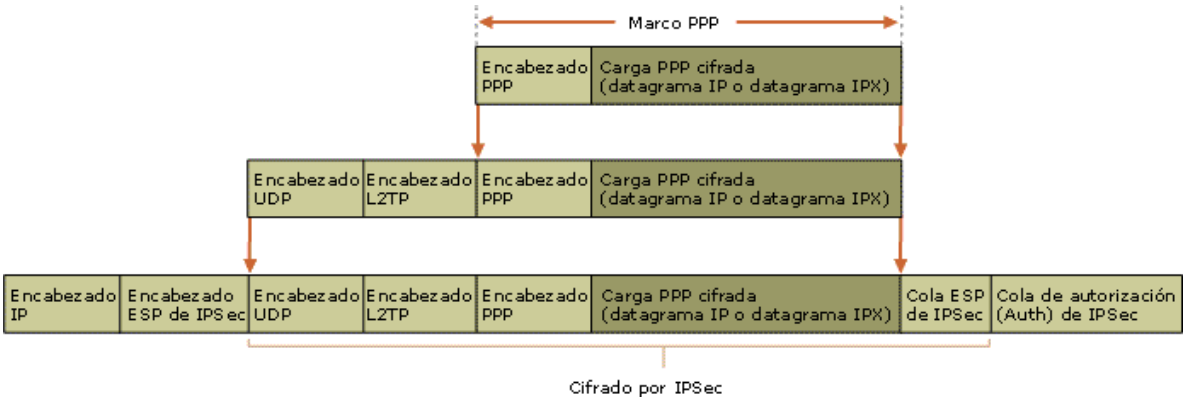


Figura 1.3 Encapsulación L2TP e IPsec para un datagrama PPP.

I.2.1.3 Protocolo Punto a Punto (PPP).

El protocolo PPP proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos "pares".

Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Tiene tres componentes:

1. Un mecanismo de enmarcado para encapsular datagramas multiprotocolo y manejar la detección de errores.

2. Un Protocolo de Control de Enlace (LCP, Link Control Protocol) para establecer, configurar y probar la conexión de datos.

3. Una familia de Protocolos de Control de Red (NCP, Network Control Protocols) para establecer y configurar los distintos protocolos de nivel de red.

La encapsulación PPP provee multiplexamiento de diferentes protocolos de la capa de red sobre el mismo enlace. Ha sido diseñada cuidadosamente para mantener compatibilidad con el hardware mayormente usado.

Sólo son necesarios 8 bytes adicionales para formar la encapsulación cuando se usa dentro del entramado por defecto. En ambientes con escaso ancho de banda, la encapsulación y el entramado pueden requerir menos bytes.

Para establecer comunicaciones sobre un enlace punto a punto cada extremo del mismo debe enviar primero paquetes LCP para configurar y testear el enlace de datos. Después de que éste ha sido establecido, el "par" debe ser autentificado. Entonces, PPP debe enviar paquetes NCP para elegir y configurar uno o más protocolos de red. Una vez que han sido configurados cada uno de los protocolos de la capa de red elegidos, los datagramas de cada protocolo de capa de red pueden ser enviados a través del enlace. El enlace permanecerá configurado para la comunicación hasta que una serie de paquetes NCP o LCP cierren la conexión, o hasta que ocurra un evento externo (por ej., que un timer de inactividad expire o que se produzca una intervención del administrador de la red).

El Protocolo de Control de Enlace (LCP) es usado para acordar automáticamente las opciones del formato de encapsulación, los límites de manipulación de tamaño de paquete, detectar un enlace con ciclos, otros errores comunes por mala configuración, y terminar el enlace. Otras facilidades opcionales provistas son: autenticación de la identidad de los "pares" del enlace, y determinación de cuándo el enlace está funcionando apropiadamente y cuándo está fallando.

I.2.2 Componentes de las Redes Privadas Virtuales.

Una conexión de red privada virtual (VPN) consta de los siguientes componentes:

- Servidor VPN, un equipo que acepta conexiones VPN de clientes VPN. Este servidor proporciona a los usuarios tener acceso a los recursos de una red privada por medio de una conexión de acceso telefónico o una conexión VPN. También en este servidor se proporciona la seguridad y administración para el acceso a la red mediante directivas de seguridad y asignación de IP a cada cliente VPN.
- Cliente VPN, un equipo que inicia una conexión VPN a un servidor VPN. Un cliente VPN puede ser un equipo individual o un enrutador. En este también se encuentran los protocolos utilizados para la VPN como son el PPTP y el L2TP para túneles y de seguridad IP (IPsec). Con esto el cliente se convierte en un nodo remoto de la red privada.
- Túnel. La parte de la conexión en la que se encapsulan los datos mediante los protocolos PPP, PPTP y L2TP para asegurar la confidencialidad de la información a través de la red pública Internet.
- Conexión VPN. La parte de la conexión en la que se cifran los datos. En las conexiones VPN seguras, los datos se cifran y encapsulan en la misma parte de la conexión mediante los protocolos de cifrado y autenticación.

- Protocolos de túnel. Los protocolos utilizados para administrar túneles y encapsular datos privados. Los datos que se envían por el túnel también deben estar cifrados para constituir una conexión VPN. La familia Windows de Microsoft incluye los protocolos de túnel PPTP y L2TP y en Linux su configuración debe de ser manual para el uso de los mismos.
- Datos en túnel. Los datos que normalmente se envían a través de un vínculo punto a punto privado y que llegan a otro nodo de la red privada.
- Conjunto de redes públicas o privadas de tránsito como es la red de Internet que sirve como medio de comunicación entre dos redes ubicadas en diferentes áreas geográficas y que igualmente puede ser una red interna que asegura la confidencialidad entre departamentos de una corporación utilizando una VPN interna.

En la plataforma Windows NT o GNU/LINUX, el conjunto de redes públicas o privadas de tránsito siempre es un conjunto de redes IP. El conjunto de redes públicas o privadas de tránsito puede ser Internet o una intranet privada basada en IP.

La Figura 1.4 y 1.5 muestran los componentes y elementos de una red privada virtual.

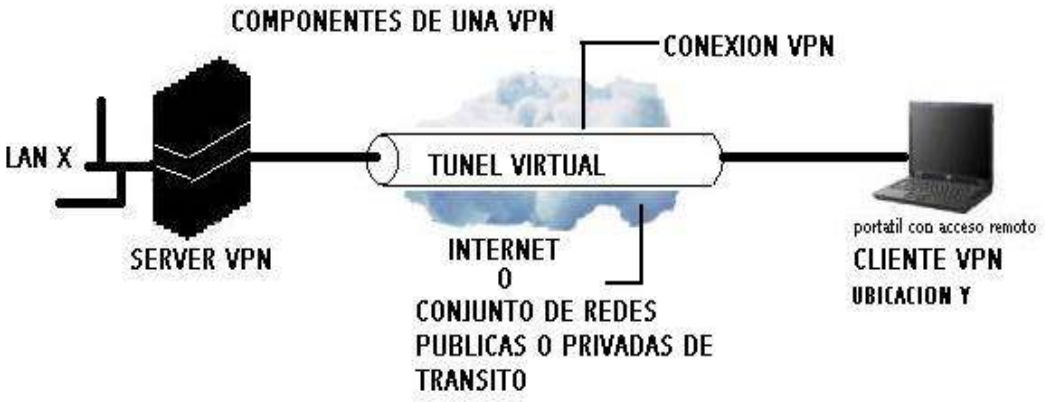


Figura 1.4 Componentes de una Red Privada Virtual.

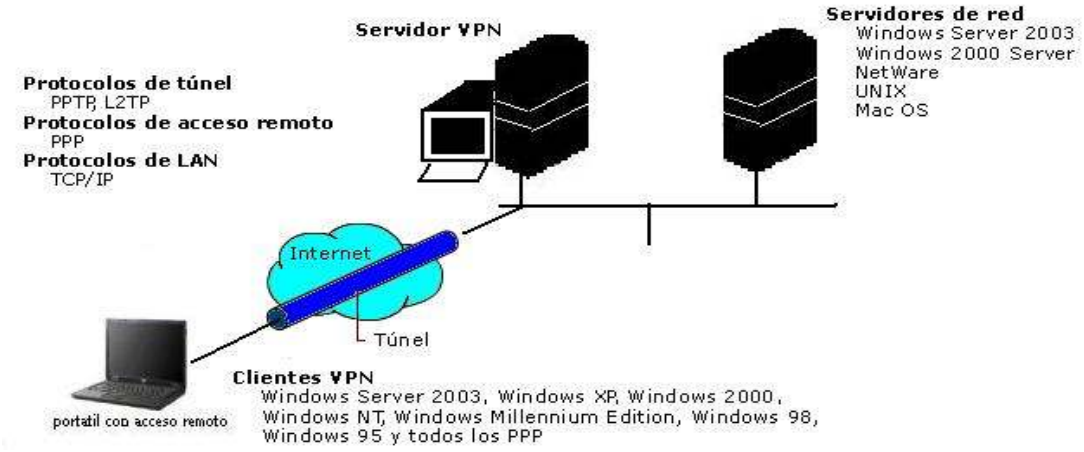


Figura 1.5 Elementos de una Red Privada Virtual.

I.2.3 Hardware.

En cuanto al Hardware los requisitos para las conexiones de red y de acceso telefónico dependiendo de la configuración puede ser el siguiente:

- Tarjeta adaptadora de red con un controlador certificado para Especificación de Interfaz de Controlador de Red (NDIS, *Network Driver Interface Specification*), para la conectividad de LAN.
- Uno o varios Módems compatibles y un puerto COM disponible.
- Módem o adaptador ISDN (RDSI) (si va a utilizar una línea ISDN (RDSI)).
- Adaptador DSL.
- Tarjeta o PAD X.25 (si va a utilizar X.25).
- Línea telefónica analógica.
- Si el equipo está configurado para aceptar conexiones entrantes, un adaptador de múltiples puertos puede aumentar el rendimiento cuando haya varias conexiones.

I.3 Conexiones y tipos de VPN.

-Redes de acceso telefónico externas.

El hardware de comunicaciones disponible para satisfacer las necesidades de acceso telefónico puede ser complicado y no estar bien integrado. En una organización grande, poner en marcha un servidor de acceso remoto requiere Módems, controladores serie y muchos cables. Además, muchas soluciones no proporcionan una única manera integrada de utilizar con eficiencia las líneas de acceso telefónico V.34 e ISDN (RDSI).

A muchas compañías les gustaría contratar acceso telefónico externo a sus redes de red troncal de una forma asequible, sin problemas, independiente del protocolo y segura que no requiera cambios en las direcciones de la red existente. La compatibilidad con redes WAN virtuales a través de conexiones de red privada virtual (VPN) es una forma de que un Proveedor de Servicios Internet (ISP) pueda satisfacer las necesidades de las compañías. De esta manera, la compañía externa mantiene y administra los Módems y las líneas de acceso remoto, y el administrador del sistema sólo necesita ocuparse de administrar los usuarios y los requisitos de autenticación.

Este tipo de solución aprovecha las probadas tecnologías PPP de autenticación, cifrado y compresión.

En la Figura 1.6 se muestra un ejemplo de red externa.

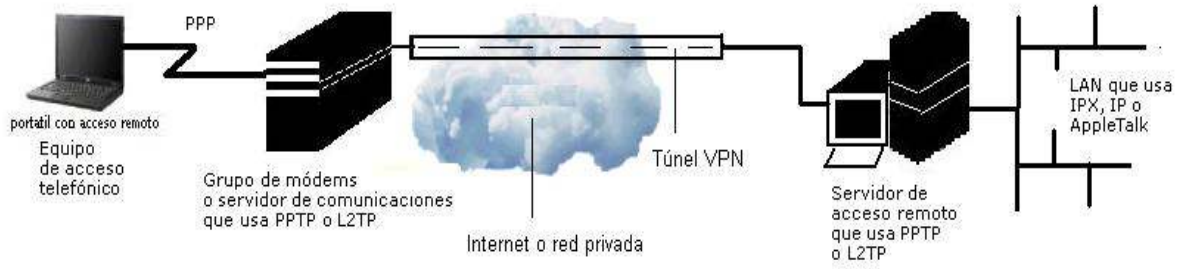


Figura 1.6 Red Externa.

La conexión no necesita tener un controlador PPTP; el cliente solamente realiza una conexión PPP al grupo de Módems o al servidor de comunicaciones. El servidor de comunicaciones o el grupo de Módems tienen que implementar PPTP para la comunicación con el servidor de acceso remoto.

Crear una conexión de red privada virtual (VPN) es muy similar a establecer una conexión punto a punto mediante conexiones de acceso telefónico y enrutamiento de marcado a petición. Hay dos tipos de conexiones VPN:

- Conexión VPN de acceso remoto
- Conexión VPN de enrutador a enrutador

I.3.1 Conexiones VPN de acceso remoto.

Un cliente de acceso remoto (el equipo de un usuario) realiza una conexión VPN de acceso remoto que conecta a una red privada. El servidor VPN proporciona acceso a los recursos del servidor VPN o a toda la red a la que está conectado el servidor VPN. Los paquetes enviados desde el cliente remoto a través de la conexión VPN se originan en el equipo cliente de acceso remoto.

El cliente de acceso remoto (el cliente VPN) se autentica ante el servidor de acceso remoto (el servidor VPN) y, para realizar la autenticación mutua, el servidor se autentica ante el cliente.

Los equipos que ejecutan la plataforma Windows de Microsoft pueden crear conexiones VPN de acceso remoto a un servidor VPN que ejecuta igualmente una plataforma de Windows para servidores. Los clientes VPN también pueden ser un cliente de Protocolo de Túnel Punto a Punto (PTPP) o un cliente de Protocolo de Túnel de Capa 2 (L2TP) con IPSec que no sean de Microsoft como lo es Linux.

I.3.2 Conexiones VPN de ruteador a ruteador.

Un enrutador realiza una conexión VPN de enrutador a enrutador que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN. En una conexión VPN de enrutador a enrutador, los paquetes enviados desde uno de los enrutadores a través de la conexión VPN normalmente no se originan en los enrutadores.

El enrutador de llamada (el cliente VPN) se autentica ante el enrutador de respuesta (el servidor VPN) y, para realizar la autenticación mutua, el enrutador de respuesta se autentica ante el enrutador de llamada.

Los equipos que ejecutan la plataforma de Windows NT de Microsoft con los servicios de enrutamiento y acceso remoto (RAS) pueden crear conexiones VPN de enrutador a enrutador. Los clientes VPN también pueden ser un cliente de Protocolo de Túnel Punto a Punto (PPTP) o un cliente de Protocolo de Túnel de Capa 2 (L2TP) con IPSec que no sean de Microsoft como lo es Linux en su versión para servidores.

I.3.3 Conexión VPN de acceso telefónico de enrutador a enrutador.

Las conexiones de red privada virtual de enrutador a enrutador suelen utilizarse para conectar oficinas remotas cuando ambos enrutadores están conectados a Internet a través de vínculos WAN permanentes, como T1 o Frame Relay. En esta configuración, la conexión VPN siempre está disponible. Sin embargo, cuando no es posible o práctico utilizar un vínculo WAN permanente, se puede configurar una conexión VPN de acceso telefónico de enrutador a enrutador.

En la Figura 1.7 se muestra una conexión VPN de acceso telefónico de enrutador a enrutador.

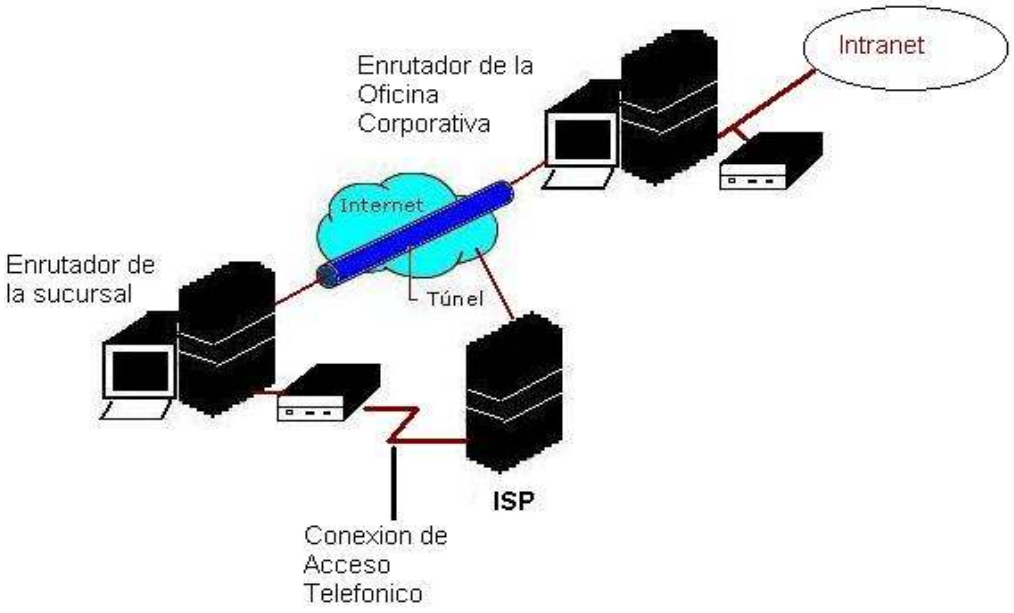


Figura 1.7 Conexión VPN de acceso telefónico de enrutador a enrutador.

Las conexiones VPN de acceso telefónico de enrutador a enrutador constan de dos interfaces de marcado a petición y dos rutas estáticas configuradas en el cliente VPN (el enrutador que realiza la llamada):

- Una interfaz de marcado a petición para marcar a un Proveedor de Servicios Internet (ISP, Internet Service Provider) local.
- Una interfaz de marcado a petición para la conexión VPN de enrutador a enrutador
- Una ruta de host estática para establecer una conexión dinámica con Internet.
- Una ruta estática para llegar a las ubicaciones de la oficina central

Las conexiones VPN de acceso telefónico de enrutador a enrutador se establecen automáticamente al enrutar las transmisiones a una ubicación específica. Por ejemplo, en la configuración de una sucursal, cuando se recibe un paquete que se va a enrutar a la oficina central, el enrutador de la sucursal utiliza un vínculo de acceso telefónico para conectar con el Proveedor de Servicios Internet (ISP) local y, a continuación, crea una conexión VPN de enrutador a enrutador con el enrutador de la oficina central que se encuentra en Internet.

I.3.4 Conexiones VPN Internet e intranet.

Puede utilizar conexiones de red privada virtual (VPN) cuando necesite una conexión punto a punto segura para conectar usuarios o redes. Las conexiones VPN típicas se basan en Internet o en una intranet.

I.3.4.1 Conexiones VPN sobre Internet.

Mediante una conexión de red privada virtual (VPN) basada en Internet, puede ahorrar los gastos de llamadas telefónicas de larga distancia y a números de costos por minuto, y aprovechar la disponibilidad de Internet.

En lugar de realizar una llamada de larga distancia o a un número de costos por minuto para conectar con un servidor de acceso a la red (NAS, Network Access Server) de la compañía o externo, los clientes de acceso remoto pueden llamar a un ISP local.

Mediante la conexión física establecida con el ISP local, el cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor VPN de la organización. Una vez creada la conexión VPN, el cliente de acceso remoto puede tener acceso a los recursos de la Intranet privada.

La Figura 1.8 muestra el acceso remoto de un cliente VPN marcando un ISP.

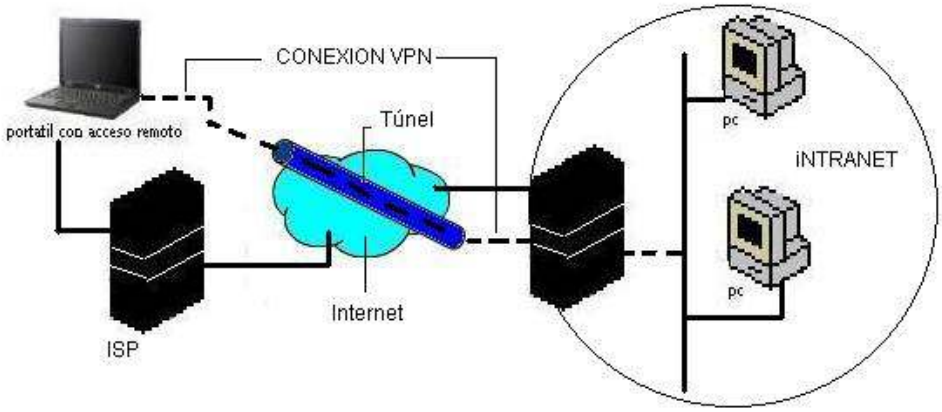


Figura 1.8 Acceso remoto a través de Internet.

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

La Figura 1.9 muestra la conexión de redes LAN por medio de una VPN y a través de Internet.

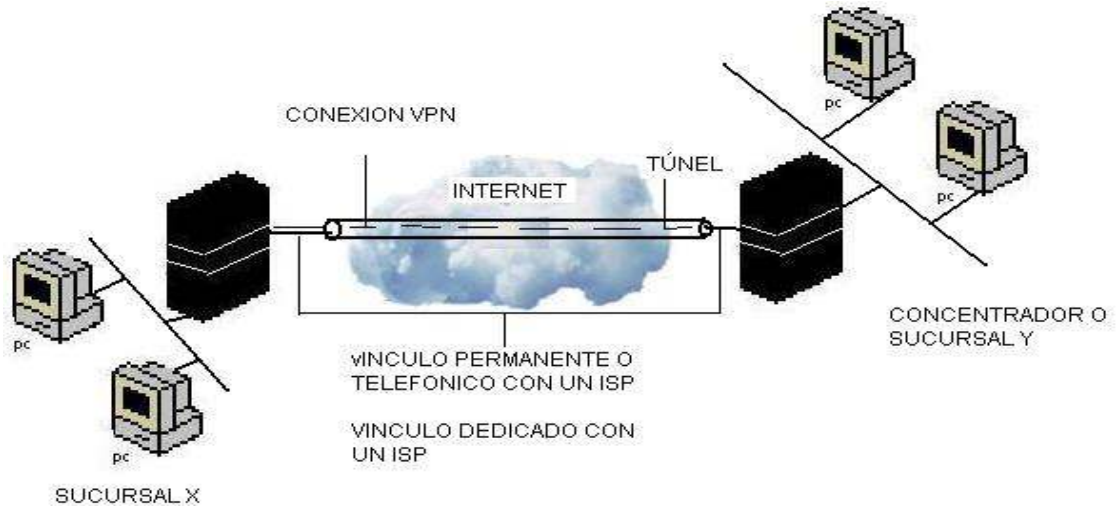


Figura 1.9 Conexiones de redes LAN sobre Internet utilizando una VPN.

-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.

-Usar vínculos WAN de acceso telefónico.

En lugar de realizar una llamada de larga distancia o marcar un número de pago por minuto para conectar con un NAS (Network Attached Storage) 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 factible 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.

I.3.4.2 Conexiones VPN basadas en intranets.

Las conexiones de red privada virtual (VPN) basadas en Intranet aprovechan la conectividad IP en la Intranet de una organización.

-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 derechos para establecer una conexión VPN, la red del departamento está oculta a la vista.

La Figura 1.10 muestra el acceso remoto a un servidor VPN a través de una Intranet como se menciono en el párrafo anterior.

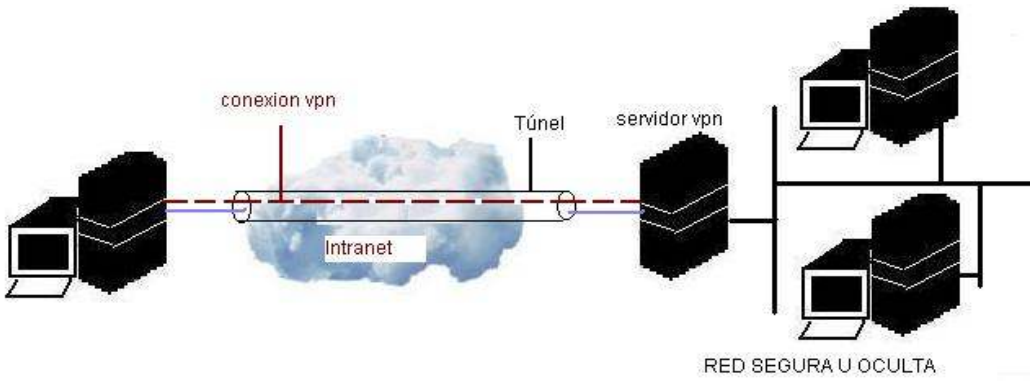


Figura 1.10 Acceso remoto a través una Intranet.

-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 enrutadores 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 Figura 1.11 muestra la conexión de dos redes LAN internas a través de una VPN sobre una Intranet.

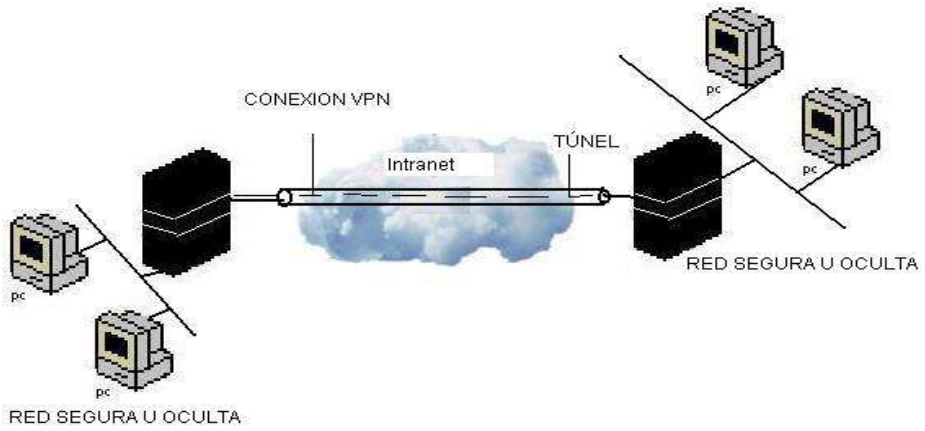


Figura 1.11 Conexión de dos redes LAN en una Intranet por medio de una VPN.

I.3.4.3 Acceso remoto VPN externo.

En este tema se describe el uso de IAS (Servicio de Autenticación de Internet) por parte de un proveedor de servicios externo y una organización para el acceso remoto externo basado en VPN. El proveedor de servicio externo ofrece Puntos de Presencia (POP, Points of Presence) universales, a los que pueden llamar los empleados de una organización. Después de realizarse esta llamada, el equipo del empleado establece una conexión VPN de Protocolo de Túnel Punto a Punto (PPTP, Point-to-Point Tunneling Protocol) con uno de los servidores VPN de la organización.

En esta configuración de ejemplo la organización tiene una ubicación central de gran tamaño con usuarios remotos. Cada usuario necesita acceso seguro a la red de la organización. La organización ha determinado que sale más rentable proporcionar acceso remoto VPN mediante contratación externa que implementar y mantener su propia infraestructura de acceso remoto telefónico.

Los requisitos de cifrado y autenticación para la conexión a Internet son menos rigurosos que los de la conexión VPN. Por ejemplo, la conexión a Internet utiliza el protocolo CHAP sin cifrado, mientras que la conexión VPN utiliza tarjetas inteligentes y el Protocolo de Autenticación Extensible-Seguridad de Nivel de Transporte (EAP-TLS, Extensible Authentication Protocol-Transport Level Security) con cifrado de 128 bits.

En la Figura 1.12 se muestra la configuración VPN externa.

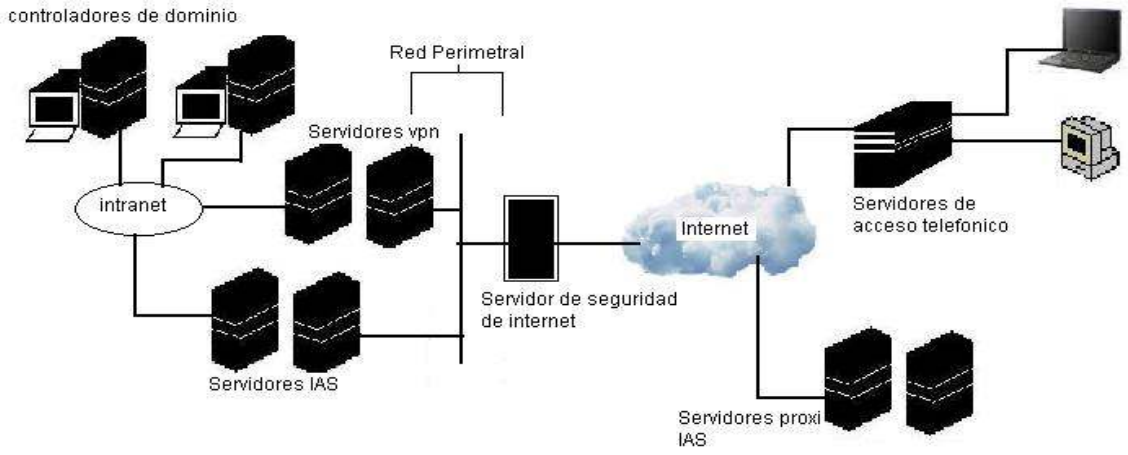


Figura 1.12 VPN externa.

I.4 PROPIEDADES DE UNA VPN.

Las conexiones de red privada virtual (VPN) que utilizan PPTP y L2TP/IPSec tienen las siguientes propiedades:

- ENCAPSULACIÓN
- AUTENTICACIÓN
- CIFRADO DE DATOS

I.4.1 Encapsulación.

En la tecnología VPN, los datos privados se encapsulan con un encabezado que proporciona información de enrutamiento, lo que permite que los datos atraviesen los conjuntos de redes públicas y privadas de tránsito.

I.4.2 Autenticación.

La autenticación en las conexiones VPN toma tres formas diferentes:

- Autenticación en el nivel de usuario mediante la autenticación PPP. Para establecer la conexión VPN, el servidor VPN autentica al cliente VPN que intenta realizar la conexión mediante un método de autenticación en el nivel de usuario del Protocolo Punto a Punto (PPP) y comprueba que el cliente VPN tiene la autorización correspondiente. Si se utiliza la autenticación mutua, el cliente VPN también autentica al servidor VPN, lo que proporciona protección contra equipos enmascarados como servidores VPN.
- Autenticación en el nivel de equipo mediante IKE Para establecer una asociación de seguridad IPSec, el cliente VPN y el servidor VPN utilizan el Protocolo de Intercambio de Claves de Internet (IKE, Internet Key Exchange) para intercambiar certificados de equipo o una clave previamente compartida. En ambos casos, el cliente y el servidor VPN se autentican mutuamente en el nivel de equipo. La autenticación mediante certificados de usuario es muy recomendable, ya que se trata de un método de autenticación mucho más seguro. La autenticación en el nivel de equipo sólo se lleva a cabo para conexiones L2TP/IPSec.
- Autenticación del origen de los datos e integridad de los datos. Para comprobar que los datos enviados en la conexión VPN se originaron en el otro extremo de la conexión y que no se modificaron en el tránsito, los datos contienen una suma de comprobación criptográfica basada en una clave de cifrado que sólo conocen el que realiza el envío y el que lo recibe. La autenticación del origen de los datos y la integridad de los datos sólo está disponible en conexiones L2TP/IPSec.

I.4.3 Cifrado de datos.

Para asegurar la confidencialidad de los datos a medida que atraviesan el conjunto de redes públicas y privadas de tránsito, el que realiza el envío cifra los datos y el que lo recibe los descifra. Los procesos de cifrado y descifrado dependen de que el que realiza el envío y el que lo recibe utilicen una clave de cifrado común.

Los paquetes interceptados que se envían en la conexión VPN a través del conjunto de redes públicas y privadas son ininteligibles para todo aquél que no disponga de la clave de cifrado común. La longitud de la clave de cifrado es un parámetro de seguridad importante. Se pueden utilizar técnicas de computación para averiguar la clave de cifrado. Sin embargo, estas técnicas requieren más capacidad y tiempo de computación a medida que las claves de cifrado son más grandes. Por lo tanto, es importante utilizar el tamaño de clave más grande posible para asegurar la confidencialidad de los datos.

I.5 PROTOCOLOS DE AUTENTICACION Y CIFRADO.

Como se había mencionado anteriormente las VPNs 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.

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 cifrado 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 cifrado y autentificación y que se describirán en este capítulo a través de lo que son los protocolos de autenticación y cifrado de los datos.

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 cifrados.

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al “logeo” 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 entrometido 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), RSA y EAP.

I.5.1 Protocolo de autenticación CHAP.

El Protocolo de Autenticación Handshake de Microsoft (MS-CHAP) es un mecanismo de autenticación que se utiliza para validar las credenciales del usuario contra los dominios Windows NT, mientras que las claves de sesión resultantes se utilizan para cifrar los datos del usuario, como se describe a continuación en Análisis de MPPE.

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 “Desafió-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 “Desafió-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.

I.5.2 Protocolo de autenticación MS-CHAPv2.

La plataforma de Windows 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 Datos. 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 computadoras que corren la plataforma de Windows. Para computadoras con Windows 95, MS-CHAP v2 esta solo soportado para conexiones VPN, y no para conexiones dial-up.

La versión 2 MS-CHAP incluye una función de una salida de la contraseña del usuario, un reto generado por el servidor y el cliente, además de datos adicionales en el mensaje satisfactorio de la versión 2 MS-CHAP. El cliente de la versión 2 MS-CHAP se desconecta si no puede autentificar el servidor.

Cuando el servidor de acceso de red recibe una solicitud de autenticación MS-CHAP versión 2, por parte de un cliente remoto, éste envía un reto, el cual consiste en una ID de sesión y una cadena de retos arbitrarios, para el cliente remoto. El cliente remoto debe confirmar el nombre del usuario, el hash de la cadena de retos, la ID de sesión y la contraseña hashed. Este diseño, el cual manipula un hash del hash de contraseña, proporciona un nivel adicional de seguridad ya que permite que el servidor almacene contraseñas hashed en lugar de contraseñas de texto.

La versión 2 MS-CHAP también proporciona códigos de error adicionales incluyendo un código expirado de contraseña, mensajes cifrados adicionales de cliente-servidor permiten a los usuarios cambiar sus contraseñas. En la implementación de la versión 2 de MS-CHAP de Microsoft, tanto el cliente como el servidor generan una clave inicial de manera independiente para el cifrado de datos subsecuentes por MPPE.

Anteriormente, las VPNs PPTP de Microsoft podían ser configuradas para aceptar protocolos de autenticación menos demandantes. Para mejorar la seguridad durante la autenticación, Microsoft PPTP ahora utiliza únicamente MS-CHAP.

I.5.3 Protocolo de Autenticación RSA.

El algoritmo de cifrado RSA, es el criptosistema de clave pública más extendida. Su nombre proviene de sus creadores Rivest, Shamir, y Aldemar, quienes lo desarrollaron en 1978.

Este sistema usa dos claves y cualquiera de las dos puede ser pública o privada. Las dos claves se generan matemáticamente basándose en parte en la combinación de grandes números con factores primos.

Dado que las claves se generan a partir del producto de dos números primos, la única forma de atacarla sería factorizándolas en dichos números primos. Lo cual es demasiado costoso y complicado, ya que los números producto de dos primos, son de los más difíciles de factorizar.

Todo usuario de dicho sistema hace pública una clave de cifrado y oculta una clave de descifrado. Una llave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes. Cuando se envía un mensaje, el emisor busca la clave pública de cifrado del receptor y una vez que dicho mensaje llega al receptor, éste se ocupa de descifrarlo usando su clave oculta. Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado. La seguridad de este algoritmo radica en que no hay maneras rápidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales. La computación cuántica podría proveer una solución a este problema de factorización.

La generación de llaves en RSA se lleva a cabo de la manera siguiente:

1.-Seleccione dos números primos p y q.
2.-Calcule el producto: n = pq.
3.-Calcule Phi(n) = (p - 1)(q - 1).
4.-Seleccione un entero e tal que el MCD(Phi(n),e) = 1 y 1<e<Phi(n).
5.-Calcule d = e^-1 mod Phi(n).
6.-La clave privada será d y la clave pública será e. *Adicionalmente el parámetro n debe hacerse público.

Un usuario elige dos números primos p y q de 200 dígitos aproximadamente.

Sea $n = p \cdot q$

Buscamos e tal que sea primo con:

$$\Phi(n) = (p - 1) \cdot (q - 1)$$

Como *e* y Φ(n) son primos entre sí, entonces existe *d* tal que:

$$e \cdot d \equiv 1 \bmod \Phi(n) = n+1 - p - q$$

d se puede calcular mediante el algoritmo de Euclides.

Clave Pública: (e,n).

Clave Privada: (d,n).

Los datos que han de mantenerse privados son:

- *p y q.*
- Φ *(n).*
- *d.*

Cualquiera que conozca estos datos podrá descifrar los mensajes del propietario de la clave.

Además de estos datos hemos de fijar la longitud de bloque:

- Longitud del bloque que vamos a cifrar.
- Longitud del bloque cifrado.

Ejemplo

Elegimos dos primos *p = 281 y q = 167*.

n = 281 · 167 = 46,927

Φ (n) = (280 - 1) · (167- 1) = 46,480

Buscamos e y d tales que:

$$e \cdot d \equiv 1 \bmod \Phi(46{,}927)$$

Por ejemplo:

e = 39,423

d = 26,767

Las claves serán:

Clave Pública: (39,423, 46.927).

Clave Privada: (26,767, 46,927).

Supongamos que vamos a cifrar bloques de dos letras en bloques de tres letras, y que queremos cifrar “HOLA” utilizando un alfabeto de 36 símbolos.

El procedimiento es el siguiente:

1. Asignamos a cada letra un número según un alfabeto:

HOLA = (17, 24, 21, 10)

2. Bloques a cifrar: (17,24) y (21,10).

3. Expresamos ambos bloques como un número en base 36:

(17, 24) = 17 · 36º +24 · 36 = 881

(21,10) = 21 · 36º +10 · 36 = 381

4. Elevamos estos números a ***e*** módulo 46,927:

$$881^{39,423} \equiv 45,840 \bmod 46,927$$

$$381^{39,423} \equiv 26,074 \bmod 46,927$$

5. Expresamos estos números en base 36, teniendo en cuenta que vamos a tener tres componentes:

45,840 = 12 · 360 +13 · 36+35 · 362 = (12,13, 35)

26,074 = 10 · 360 +4 · 36+20 · 362 = (10, 4, 20)

6. Según el alfabeto considerado a cada número le asignamos una letra:

(12, 13, 35) ➔CDZ
(10, 4, 20) ➔ A4K

Luego el mensaje cifrado es "CDZA4K".

Para descifrar habría que hacer el mismo proceso, pero partiendo de bloques de tres letras y terminando en bloques de dos letras y elevando a ***e*** en lugar de ***d***.

-Seguridad RSA.

Como las claves públicas son públicas, cualquiera puede cifrar un texto a partir de un texto plano e intentar averiguar la clave privada.

Supongamos que ciframos el texto "HOLA", durante el proceso de descifrado tendremos:

$$45{,}840^{d} \equiv 881 \bmod 46{,}927$$
$$26{,}074^{d} \equiv 381 \bmod 46{,}927$$

o lo que es lo mismo:

$$d = \log_{45{,}840} 881 \bmod 46{,}927$$
$$d = \log_{26{,}074} 381 \bmod 46{,}927$$

d no es conocido ya que forma parte de la clave privada, para romper este criptosistema lo podemos intentar de varias formas:

1. A fuerza bruta. . .
2. Mediante un ataque de intermediario.
3. Intentando resolver cualquiera de los dos logaritmos discretos anteriores . . .
4. Resolviendo:

$$e \cdot d \equiv 1 \bmod \Phi(46{,}927)$$

Lo cual equivale a conocer Φ (46,927), que a su vez equivale a conocer la factorización en números primos de 46,927.

Lo cual es un problema con el mismo grado de complejidad que el logaritmo discreto (problema de tipo exponencial) para números lo suficientemente grandes.

I.5.4 Protocolo de Autenticación EAP.

El Protocolo de Autenticación Ampliable (EAP) es una extensión de PPP, que proporciona un mecanismo de soporte estándar para los esquemas de autenticación como las tarjetas token, Kerberos, Clave pública y clave/S, y está totalmente soportado tanto en Windows NT Dial-Up Server como en Dial-Up Networking Client. EAP es un componente de tecnología crítica para las VPNs seguras, protegiéndolas de la fuerza bruta de un ataque de diccionario o de que las contraseñas sean adivinadas.

EAP permite que los módulos de autenticación de terceros interactúen con la implementación de una VPN de Servicio de Acceso Remoto (RAS) Microsoft Windows NT. La disponibilidad de EAP en Windows NT es una respuesta a la creciente demanda para aumentar la autenticación RAS con dispositivos de seguridad de terceros.

EAP es una extensión propuesta por IETF[1] para PPP que permite que los mecanismos arbitrarios de autenticación se empleen para la validación de una conexión PPP. EAP se diseñó para permitir la adición dinámica de módulos de conexión de autenticación tanto del lado del cliente como del servidor en una conexión. Esto permite que los proveedores suministren un nuevo esquema de autenticación en cualquier momento. EAP proporciona la máxima flexibilidad en variedad y singularidad de autenticación. Se planea que EAP se pondrá en marcha en Microsoft Windows 2000.

[1] El **IETF** (**I**nternet **E**ngineering **T**ask **F**orce, en castellano Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en EE.UU. en 1986.

I.5.5 Protocolo de Autenticación AH en IPSEC.

La Cabecera de Autenticación proporciona autenticación e integridad a los datagramas pasados entre dos sistemas.

Esto se logra aplicando una función tipo hash unidireccional con clave al datagrama para crear un boletín de mensajes. SI alguna parte del datagrama es modificada durante el tránsito, será detectada por el receptor cuando realice la misma función tipo hash unidireccional sobre el datagrama y compare el valor del boletín de mensajes que el emisor ha proporcionado. La operación hash unidireccional también implica el uso de un secreto compartido entre los dos sistemas, lo que significa que la autenticidad puede ser garantizada.

La AH puede también reforzar la protección antireproducción al requerir que un host receptor defina el bit de reproducción en la cabecera para indicar que el paquete ha sido visto. Sin esta protección, un atacante podría ser capaz de reenviar el mismo paquete muchas veces.

La función AH se aplica a todo el datagrama, exceptuando aquellos campos de la cabecera de IP mutables que cambien en tránsito, como por ejemplo, los campos Tiempo de Vida (TTL) que son modificaos por los routers a lo largo de la ruta de transmisión.

La AH funciona de la siguiente manera:

Paso 1. Se aplica la función tipo hash a la cabecera de IP y la sobre carga de datos.

Paso 2 La función tipo hash se utiliza para construir una nueva cabecera AH, que se añade al paquete original.

Paso 3. El nuevo paquete se transmite al vecino IPSec.

Paso 4. El IPSec aplica una función tipo hash a la cabecera IP y la sobrecarga de datos, extrae el resultado de las dos funciones hash. Los resultados de las funciones tipo hash debe coincidir con exactitud. Incluso si un bit es cambiado en el paquete transmitido, la salida de la función tipo hash en el paquete recibido cambiará y la cabecera AH no coincidirá.

AH proporciona autenticación en el encabezado IP en la medida de lo posible, al igual que en los datos de protocolos de nivel superior. Sin embargo, algunos campos de los encabezados IP pueden cambiar el trayecto y los valores de estos campos, cuando el paquete llegue al receptor, podrían no ser predecibles por el emisor. Los valores de tales campos no pueden protegerse con AH. Por lo tanto, la protección que AH proporciona al encabezado IP se degrada en cierta forma.

AH puede utilizarse en los modos de túnel y transporte. En el modo de transporte, se inserta después del encabezado IP original y protege a los protocolos de nivel superior. En el modo de túnel, se inserta antes del encabezado original y se introduce un nuevo encabezado IP. Además, AH se diseño para IPv6; en este protocolo AH se considera una carga de extremo a extremo y, de acuerdo con el RFC-2402, aparecerá después del encabezado de enrutamiento. Ver figura 1.13.

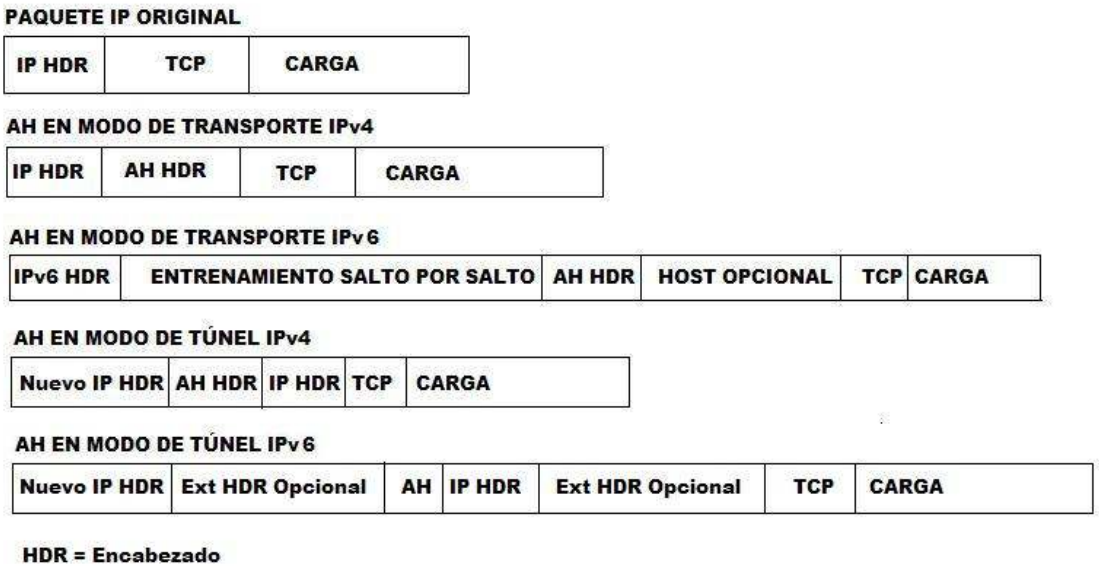


Figura 1.13. Muestra de varios modos para AH.

I.5.6 Protocolo de Autenticación PAP.

Password Authentication 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.

Todas las VPNs tienen algún tipo de tecnología de cifrado, que esencialmente empaqueta los datos en un paquete seguro. El cifrado es considerado tan esencial como la autenticación, ya que protege los datos transportados sin ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de cifrado que se usan en las VPN: cifrado de clave secreta, o privada, y cifrado de clave pública.

El cifrado es el proceso de codificación de datos que sirve para prevenir el acceso no autorizado, especialmente durante la transmisión. El Cifrado se lleva acabo utilizando un algoritmo especial junto con uno confidencial (también conocido como clave) para transformar datos, como puede ser una contraseña, de manera tal que los datos no puedan ser entendidos por ninguna persona que no conozca la clave correcta. La contraseña hashed sólo puede ser descifrada por una computadora que tenga la misma clave como si dos niños tuvieran los anillos decodificadores, pero utilizando algoritmos que harían casi imposible romper el cifrado, especialmente en claves de más de 128 bits.

La seguridad VPN se mejora con el uso de cifrados para proteger contraseñas además del contenido de paquetes de datos. Las claves que se utilizan para cifrar datos se derivan de las credenciales del usuario y no se transfieren por cable. Cuando se termina la autenticación, se verifica la identidad del usuario, y se utiliza la clave de autenticación para el descifrado.

Tanto los protocolos de cifrado y compresión opcionales inherentes PPTP y L2TP como la seguridad adicional de cifrado, pueden agregarse implementando el protocolo IPSec, ya que la implementación Microsoft de L2TP está permitida para el cifrado IPSec. Se pueden utilizar varias tecnologías de cifrado para proporcionar seguridad de datos con las VPNs.

I.5.7 Cifrado de clave secreta o simétrica.

El cifrado simétrico o de clave privada (también conocida como cifrado convencional) se basa en una clave secreta que se comparte por dos partes que están en comunicación. La parte que envía, utiliza la misma clave secreta como parte de la operación matemática para cifrar el texto sencillo a ciphertext. La parte que recibe, utiliza la misma clave secreta para descifrar ciphertext a texto sencillo.

Algunos ejemplos de los esquemas de cifrado simétrico son: el algoritmo RAS RC4 (que sienta las bases para el cifrado de punto a punto de Microsoft), Estándar de Encriptación de Datos (DES), el Algoritmo Internacional de Encriptación de Datos (IDEA) y la Tecnología de Encriptación Skipjack propuesta por el gobierno de los Estados Unidos para utilizarse en el chip Clipper.

I.5.8 Cifrado de clave pública o asimétrica.

El cifrado asimétrico o de clave pública utiliza dos claves diferentes para cada usuario: una es la clave privada que sólo conoce el usuario. La otra es la clave pública correspondiente que puede acceder cualquier persona. Las claves privadas y públicas están relacionadas matemáticamente por el algoritmo de cifrado. Una clave se utiliza para el cifrado, y la otra para el descifrado, dependiendo de la naturaleza del servicio de comunicación que se esté implementando. Asimismo, las tecnologías de cifrado de clave pública permiten que se coloquen firmas digitales en los mensajes; una firma digital utiliza la clave privada del emisor para cifrar una parte del mensaje. Cuando se recibe el mensaje, el receptor utiliza la clave pública del emisor para descifrar la firma digital y verificar la identidad del emisor.

Con el cifrado simétrico, tanto el emisor como el receptor tienen una clave secreta compartida. La distribución de la clave secreta debe ocurrir antes que cualquier comunicación cifrada (con protección adecuada). Sin embargo, con el cifrado asimétrico, el emisor utiliza una clave privada para cifrar o firmar digitalmente los mensajes, mientras que el receptor utiliza una clave pública para descifrar estos mensajes. La clave pública puede distribuirse libremente a cualquiera que necesite recibir los mensajes cifrados o firmados digitalmente. El emisor necesita proteger cuidadosamente sólo la clave privada.

En las VPNs, el cifrado debe ser realizado en tiempo real. Por eso, los flujos cifrados a través de una red son encriptados utilizando cifrados de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para el cifrado dentro de las VPNs es IPSec, que consiste en un conjunto de propuestas del IETF que delinean un protocolo IP seguro para IPv4 e IPv6. IPSec provee cifrados a nivel de IP.

Además de este, también existen otros protocolos de cifrado que se describirán en los párrafos siguientes de este capítulo, como son: MPPE, ESP, IPSEC.

I.5.9 Protocolo de cifrado IPSEC.

IPSec es el nuevo marco de seguridad IP, definido con el advenimiento del IPv6. Aunque IPv6 está muy poco difundido en este momento, la tecnología marco IPSec se está utilizando ya, lo que asegura, entre otras cosas, la interoperatividad de los sistemas de diversos fabricantes. Al menos en teoría. IPSec integra confidencialidad, integridad y autentificación en un mismo marco interoperante.

La Seguridad de Protocolo de Internet (IPSec) fue diseñada por IETF como un mecanismo de extremo a extremo para reforzar la seguridad de datos en comunicaciones basadas en IP. IPSec ha sido desarrollada y analizada por algunos expertos en seguridad de red durante varios años. Es un esquema que autentifica y cifra individualmente paquetes IP, se cree que es sumamente segura. Sin embargo, IPSec fue diseñada en un principio para brindar protección a cada máquina (en particular, para proteger el tráfico entre los encaminadores de Internet). Actualmente, IPSec más o menos asume que cada Host tiene una dirección estática IP.

Se ha definido IPSec en una serie de petición de comentarios (RFCs) notablemente RFCs 1825, 1826, y 1827, los cuales definen la arquitectura general, un iniciador de autenticación para verificar la integridad de datos y una carga de pago de seguridad de encapsulamiento para cifrado e integridad de datos.

El enfoque principal de IPSec connota en proporcionar seguridad a nivel de red para IP. IPSec se integra con la seguridad inherente del sistema operativo Windows NT Server para proporcionar una plataforma ideal que proteja las comunicaciones de Internet e intranet.

IPSec habilita la conexión por túnel de servidor a servidor, tales como la que existe entre los encaminadores, en lugar de que se usen para la conexión por túnel de servidor de cliente. Por lo tanto, lo complementa en lugar de superponer la funcionalidad proporcionada por PPTP y L2TP. Por lo tanto la flexibilidad de los protocolos VPN nivel 2 (PPT/L2TP) pueden combinarse de manera avanzada con la seguridad proporcionada por IPSec.

Además de su definición de los mecanismos de cifrado para tráfico IP, IPSec define el formato de paquete IP sobre un modo de túnel IP, generalmente llamado modo túnel IPSec. Un túnel IPSec consiste en un servidor de túnel y en un cliente de túnel, los cuales se configuran para usar la conexión por túnel IPSec y un mecanismo de cifrado negociado.

El modo de túnel IPSec utiliza el método de seguridad negociada (si hay alguno) con el propósito de encapsular y cifrar paquetes completos de IP para transferencia segura a través de Internet IP público o privado. La carga de pago cifrada se encapsula otra vez con un iniciador IP de texto sencillo, y se envía entre redes para entregarse al servidor de túnel. Cuando el datagrama lo recibe, el servidor de túnel procesa y descarta el iniciador IP de texto sencillo, y descifra sus

contenidos para retirar el paquete original IP de carga de pago. El paquete IP de carga de pago se procesa normalmente y se encamina a su red objetiva.

El modo de túnel de IPSec soporta sólo el tráfico IP, y funciona desde el inicio de la pila IP. Por lo tanto las aplicaciones y protocolo de más alto nivel heredan su comportamiento. Se controla por medio de una política de seguridad o una serie de reglas de adaptación de filtro, el cual establece los mecanismos de cifrado y conexión por túnel disponibles en orden de preferencia al igual que los métodos de autenticación. Tan pronto como hay tráfico, las dos máquinas desempeñan la autenticación mutua, y después negocian los métodos de cifrado que se utilizarán. Después, se cifra todo el tráfico usando el mecanismo negociado de cifrado y luego se envuelve en un iniciador de túnel.

I.5.9.1 Autenticación IPSec.

IPSec utiliza un encabezado de autenticación y un número de secuencia para proporcionar autenticación de fuente e integridad sin cifrado. IPSec utiliza la carga de pago de seguridad encapsulada (ESP) para proporcionar integridad y autenticación además del cifrado. Con la seguridad IP, sólo el emisor y el receptor conocen la clave de seguridad. Si los datos de autenticación son validos, el receptor sabe que la comunicación vino del emisor y que no fue cambiada en tránsito.

I.5.10 Protocolo de Encapsulamiento ESP.

La Sobrecarga de Seguridad del Encapsulamiento (ESP) es un protocolo de seguridad usado para proporcionar confidencialidad (cifrado), autenticación del origen de los datos, integridad, servicio antireproduccion opcional y confidencialidad del flujo de tráfico limitado anulando el análisis del flujo de trafico.

ESP proporciona confidencialidad realizando un cifrado en la capa del paquete IP. Soporta varios algoritmos de cifrado simétrico. El algoritmo predeterminado para IPsec es DES de 56 Bits. Este código debe ser implementado para garantizar la interoperabilidad entre los productos IPSec.

Como en AH, ESP puede emplearse en dos modos, de transporte y de túnel, tanto para IPv4 como para IPv6.

La confidencialidad puede ser independiente de todos los otros servicios. Sin embargo, el uso de la confidencialidad sin integridad / autenticación puede someterse al tráfico a ciertas formas de ataques activos que podrían destruir el servicio de confidencialidad.

Al igual que en AH, ESP en modo de transporte protege a los protocolos de niveles superiores y la figura 1.14 ilustra distintos modos de ESP.

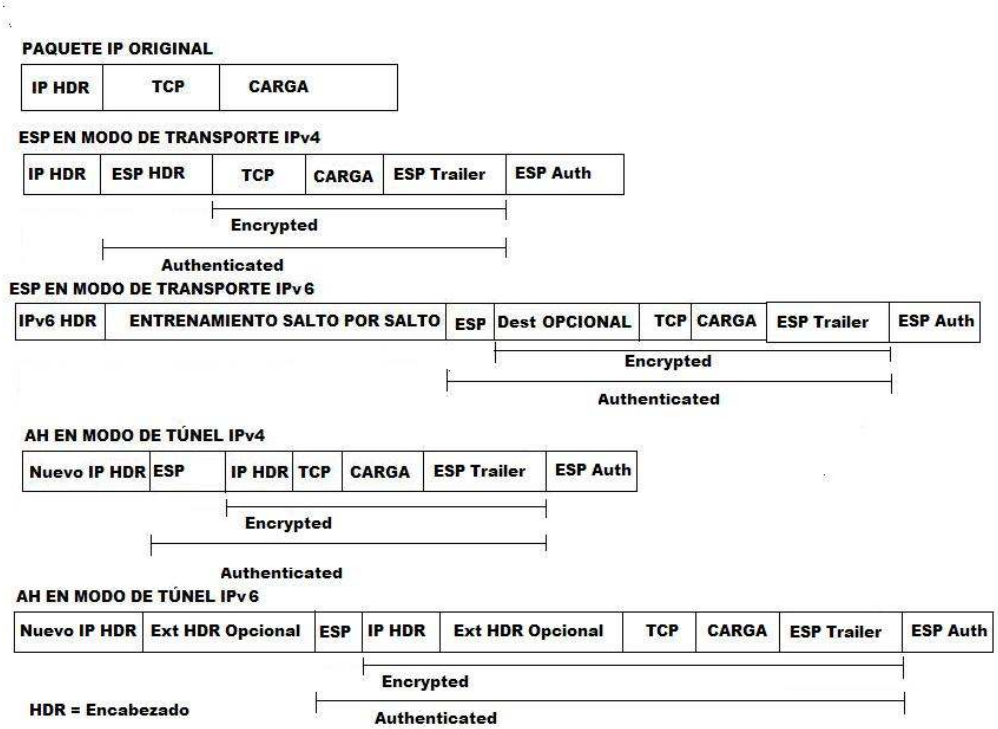


Figura 1.14. Modos de ESP.

I.5.11 Protocolo de Cifrado MPPE.

Microsoft Point to Point Encryption (MPPE) es una forma de presentar paquetes PPP encriptados[2]. MPPE 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 and 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.

I.5.12 Protocolo de Encriptación 3DES (Triple Data Encryption Standard).

D.E.S. (Data Encryption Standard o estándar de encriptación de datos) es, probablemente, el algoritmo simétrico mas utilizado en el mundo.

Fue desarrollado por IBM en los 70 por encargo del NBS (National Bureau of Standards) hoy conocido como NIST (National Institute of Standards and Technology). En 1977 fue modificado y adoptado como estándar para cifrado de datos no clasificados por el gobierno de los EE.UU. Originalmente era conocido como Lucifer, trabajaba sobre bloques de 128 bits y tenia una clave de 128 bits. Únicamente utilizaba operaciones booleanas y era fácil de implementar tanto en hardware como en software. Las modificaciones que introdujo el NBS fueron básicamente reducir la longitud tanto de la clave como de los bloques a 64 bits.

[2] Se maneja la palabra Encriptación como tecnicismo del idioma ingles para el área de computación, aunque la palabra correcta es cifrado, encriptación no existe dentro del lenguaje español.

Este algoritmo simétrico cifra bloques de 64 bits de longitud con una clave de 64 bits de longitud. Dentro de la clave el último bit de cada byte es de paridad, con lo cual tenemos que la clave en realidad es de 56 bits, esto hace que haya 256 posibles claves para este algoritmo.

Este algoritmo utiliza un “dispositivo” denominado SBB (Standard Building Block o constructor estándar de bloques), el cual requiere como entrada un bloque de 64 bits y una clave de 48 bits, produciendo una salida de 64 bits. El DES requiere 16 dispositivos SBB.

Tenemos una clave original, K, de 64 bits, 56 en realidad. De ella se extraen 16 subclaves Ki de 48 bits de longitud. El algoritmo es el siguiente:

1. Se aplica una permutación original, IP, a cada bloque de 64 bits. Produciendo una salida Bj de 64 bits.

2. Pasamos Bj con la subclave K1 por el primer SBB, la salida la pasamos por el segundo SBB con la subclave K2 y así con los 16 SBB.

3. A la salida del ultimo SBB le aplicamos la permutación IP¡1. De donde obtenemos el texto cifrado.

Para descifrar tomamos como entrada el texto cifrado y aplicamos las subclaves Ki en orden inverso, es decir en el primer SBB utilizamos K16, en el segundo K15 . . . y en el ultimo SBB utilizamos K1. Ver figura 1.15.

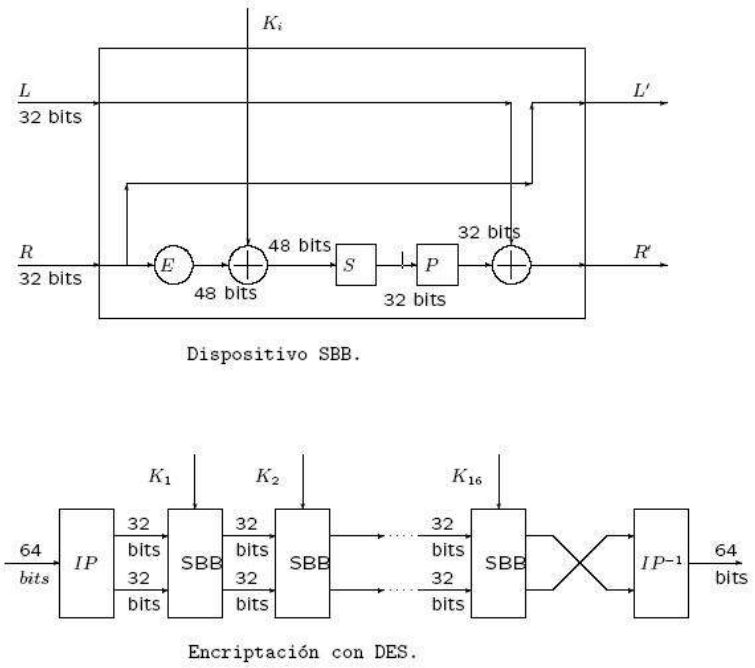


Figura 1.15 Diagrama del protocolo 3DES.

-DES Múltiple.

Consiste en aplicar el algoritmo DES, con diferentes claves, varias veces. Este método aumenta la seguridad ya que el DES no posee estructura de grupo.

Dentro de esta familia el más utilizado es el Triple-DES (3DES). Elegimos dos claves *K*1 y *K*2, el procedimiento es el siguiente:

***C* = *EK*1(*DK*2(*EK*1(*M*)))**

La clave en este caso tendría 112 bits.

I.5.13 Protocolo de Encriptación RC4 de RSA en PPTP.

Es un algoritmo de Cifrador de flujo (no de bloques), creado en 1987 por Ronald Rivest (la R de RSA - Secreto Comercial de RSA Data Security). Fue publicado el 13 de Septiembre de 1994 usando remailers anónimos en un grupo de news: sci.crypt. Es usado por diversos programas comerciales como Netscape y Lotus Notes.

Funciona a partir de una clave de 1 a 256 bytes (8 a1024 bits), inicializando una tabla de estados. Esta tabla se usa para generar una lista de bytes pseudo-aleatorios, los cuales se combinan mediante la función XOR con el texto en claro; el resultado es el texto cifrado.

I.5.14 Técnica de encapsulamiento en el protocolo PPTP.

Está basado en el protocolo GRE (Generic Routing Encapsulation) que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un Header (Encabezado) de envío, un header IP, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcado para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, Frame Relay, PPP. El header IP contiene información relativa al paquete IP, como son, 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 concernientes a la conexión entre el cliente y servidor.

Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La figura 1.16 ilustra las capas del encapsulamiento PPTP.

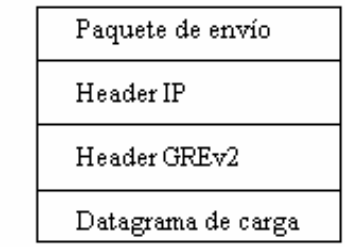


Figura 1.16 Capas de Encapsulamiento PPTP y GRE.

I.5.15 IKE. Internet Key Exchange.

Permite autentificar a los nodos participantes. Es el método estándar establecido por el IETF para las relaciones de seguridad y de intercambio de claves. Entre sus ventajas está el control centralizado de las relaciones de seguridad (reduciendo el tiempo de conexión), y la generación y la supervisión de las claves secretas usadas para asegurar la información.

I.6 SEGURIDAD DE REDES PRIVADAS VIRTUALES.

La seguridad de las VPN también se basa en los siguientes puntos como apoyo a las diferentes propiedades que tienen estas con los protocolos de autenticación y cifrado dentro de cada equipo de cómputo y administración de la red.

- Autorización para el acceso a aplicaciones y servidores
- Cifrado y descifrado de los datos a través de llaves de seguridad
- Niveles de acceso a las VPN
- Interoperabilidad entre diferentes plataformas, sistemas operativos, topologías de redes, tipo de transporte y protocolos.

I.6.1 Firewalls.

Los cortafuegos son mecanismos gracias a los cuales una red privada se encuentra protegida contra accesos no autorizados procedentes de Internet. La gran cantidad de servicios de red que un sistema ofrece al resto de equipos y el hecho de que no existan mecanismos de protección contra todos estos servicios, provoca que sea virtualmente imposible proteger una red privada tomando medidas de seguridad en base a los equipos. En este punto es donde surge el concepto de cortafuegos, el cual separa la red interna de Internet, monitorizando y filtrando todas las conexiones de Internet a la red privada y viceversa en un único punto que será considerado como el punto fuerte de defensa.

Los cortafuegos monitorizan y filtran todo el tráfico, tanto entrante como saliente. En principio existen tres técnicas de filtrado y monitorización del tráfico: filtrado a nivel IP, filtrado a nivel de conexión, y filtrado a nivel de aplicación (Proxy).

El principio básico del filtrado a nivel IP reside en el análisis de la información presente en las cabeceras de los paquetes IP. Entre estos campos hay que destacar las direcciones IP fuente y destino, el puerto destino y el tipo de paquete transportado. En este caso, la implementación puede llevarse a cabo por medio del router existente en la conexión a Internet y sus listas de acceso, evitando la necesidad de tener que adquirir una estación con un sistema operativo en particular. Sin embargo, no todo son ventajas presentando importantes inconvenientes. Primero, la autenticación está basada en las direcciones IP. Este método posee una baja fiabilidad por lo cual no resulta el más adecuado en aquellos casos en los cuales el cortafuegos debe soportar autenticaciones de clientes externos. Además, no permite la monitorización de los datos de niveles superiores intercambiados entre el cliente y el servidor. Por último, las direcciones IP son visibles desde Internet por lo que deben ser los clientes internos los que se encarguen de resolver los nombres y direcciones IP de Internet y viceversa.

La base principal de los cortafuegos con filtrado a nivel de aplicación (Proxy) reside en el bloqueo de la totalidad del tráfico a nivel IP entre la red interna e Internet. Los clientes internos establecen una conexión con el cortafuegos y a partir de ese momento dialogan con un servidor (Proxy) presente en éste en lugar de hacerlo directamente con el servidor de Internet. El Proxy actúa como intermediario de la comunicación, comprobando los permisos de los clientes y en su caso, realizando la conexión al servidor remoto en Internet. En principio, este tipo de cortafuegos ofrece el nivel más alto de seguridad. No es necesario preocuparse por los huecos de seguridad en el protocolo IP dado que todo el tráfico a este nivel es bloqueado. Además, al trabajar a nivel de aplicación los proxies permiten la monitorización de los datos al igual que otros muchos servicios, extendiendo las capacidades de registro.

En este caso, los clientes no precisan la resolución de nombres y direcciones dado que los servidores externos se encuentran representados por el cortafuego. En el otro sentido, el cortafuego permite la ocultación interna de la red siendo únicamente visible su interfaz por lo que tampoco es necesaria la resolución de nombres de los clientes internos. Por último, permite la posibilidad de ejecutar software que realice conexiones con diferentes redes privadas en Internet. Para ello, es necesario el establecimiento de líneas virtuales por las cuales los datos intercambiados viajen encriptados y autenticados (por ejemplo empleando IPSec). No obstante, no todo son ventajas. Así, por el momento no es posible disponer de un Proxy genérico que sea capaz de soportar todos los servicios, sino que cada servicio dispone de su Proxy (http-proxy, ftp-proxy, etc). Además, los proxies no son mecanismos transparentes dado que las aplicaciones deben configurarse para que establezcan su conexión al cortafuego en lugar de a los servidores externos.

Por último y a diferencia de las dos técnicas anteriores, el principio básico de los cortafuegos con filtrado a nivel de conexión no reside en el tratamiento sobre los datagramas IP, sino en el control de la conexión entre un cliente y un servidor. Su principal problema reside en la imposibilidad de realizar una autenticación fuerte dado que ésta es llevada a cabo empleando únicamente el nombre de usuario (protocolo SOCKS). En este tipo de filtrado no existe la posibilidad de realizar una monitorización de los datos intercambiados entre el cliente y el servidor: una vez establecida la conexión, el cortafuego actúa de una manera transparente. El hecho de que no sea capaz de implementar una mecanismo de autenticación fuerte unido a la no monitorización del protocolo cliente / servidor supone la principal diferencia con los cortafuegos de tipo Proxy.

En la práctica, los cortafuegos son combinaciones entre las técnicas de filtrado a nivel IP, a nivel de aplicación y a nivel de conexión. La determinación de estas técnicas dependerá del nivel de la flexibilidad, transparencia, y seguridad requerido.

Como se vio en este capítulo los conceptos manejados en este apartado son de suma importancia para poder entender el funcionamiento de una VPN y que nos sirven para continuar con los capítulos siguientes en los cuales retomaremos conceptos importantes que complementan la VPN en un sistema operativo en especifico y en el cual desarrollaremos las pruebas necesarias para su implementación.

CAPÍTULO II

AMBIENTES DE TRABAJO VIRTUAL VPN BAJO LA PLATAFORMA WINDOWS NT.

- Conocer la tecnología NT y su desarrollo para las VPN.

2.1 Antecedentes de NT.

Un tema muy importante para desarrollar e implementar una VPN es el sistema operativo con el que se va a trabajar. Microsoft, empresa dedicada al desarrollo de software crea un sistema operativo llamado Windows NT.

Windows NT es un sistema operativo para servidores, ampliable e independiente. Puede ejecutarse en sistemas basados en procesadores Intel x86, RISC y DEC Alpha, ofreciendo al usuario mayor libertad a la hora de elegir sus sistemas informáticos.

Este sistema operativo fue diseñado para uso en servidores de red de área local (LAN). Ofrece la potencia, la manejabilidad y la capacidad de ampliación de NT en una plataforma de servidor e incluye características, como la administración centralizada de la seguridad y tolerancia a fallos más avanzada, que hace de él un sistema operativo idóneo para servidores de red.

La tecnología de Windows NT continua apegándose íntegramente a Internet y a su protocolo de red TCP/IP. Este sistema operativo, en términos de redes, es un modelo hibrido montado sobre el modelo de red cliente/servidor de la década de 1990 y el modelo de cómputo distribuido propio de Internet con lo que la gente del siglo XXI se encontrará. Windows NT en sus diferentes versiones da soporte a clientes potentes como estaciones de trabajo y PC´s, clientes menores, demandas como terminales basadas en Windows y clientes que ejecutan otros sistemas operativos como MacOS y Unix. En áreas de trabajo, como empresas, la computación no solo seria distribuida, sino también heterogénea.

Microsoft ha continuado con su mejora a la pila de Windows IP[3], y le agrego características como IPsec (Seguridad de Protocolo de Internet), la cual es una norma para transacciones seguras en Internet; L2PT (Segunda Capa del Protocolo de Túnel) y PPTP (Protocolo de Túnel de Punto a Punto), mismas que permiten el uso de servicios para VPN (Redes Privadas Virtuales), y los servicios de telefonía IP para voz sobre redes de datos. Aquí existe un intento real de llevar los beneficios de la comunicación por la Internet de bajo costo y valor como EDI (Intercambio de Documentos Electrónicos). Windows NT también continúa su expansión de los servicios generados dentro del enrutamiento y RAS (Servicios de Accesos Remoto) que permite que este sistema operativo juegue el papel de un sofisticado dispositivo de conmutación real.

La generación de un sistema operativo que incorpore servicios de Internet implica anticiparse y presuponer que en algún momento futuro la mayor parte de las personas tendrá acceso a sistemas interconectados.

2.2 Arquitectura de NT.

NT ofrece arquitectura de 32 bits, dirigido a estaciones de trabajo, servidores de red y ordenadores con múltiples procesadores y se pueden ejecutar el 70% de los programas diseñados para la tecnología de Windows.

Windows 2000 se ha construido sobre la base de Windows NT, el sistema operativo desarrollado por Microsoft a principios de 1990. Este sistema operativo fue diseñado en torno a un pequeño núcleo (kernel) que proporciona las principales características de procesamiento e interacciones con el hardware. El núcleo y la capa de abstracción del hardware (HAL) fueron escritos con el fin de que la HAL pudiera ser fácilmente vuelta a compilar para diferentes microprocesadores, y el núcleo permaneciera igual, con lo que se

[3] La pila de Windows IP es el conjunto de protocolos utilizables en Internet y sus diferentes funciones agregados en el sistema operativo de Microsoft Windows y sus versiones.

lograría un sistema operativo portable entre diversas plataformas. Las versiones del sistema operativo de Windows NT se generaron para las arquitecturas x86 de Intel, Alpha de Digital Computer, PPC de Motorota y el procesador MIPS.

Uno de los objetivos fundamentales de diseño fue el tener un núcleo tan pequeño como fuera posible, en el que estuvieran integrados módulos que dieran respuesta a aquellas llamadas al sistema que necesariamente se tuvieran que ejecutar en modo privilegiado (también llamado modo kernel, modo núcleo y modo supervisor). El resto de las llamadas se expulsarían del núcleo hacia otras entidades que se ejecutarían en modo no privilegiado (modo usuario), y de esta manera el núcleo resultaría una base compacta, robusta y estable. Por eso se dice que Windows NT es un sistema operativo basado en micro-kernel.

La arquitectura Interna de Windows NT consta de un conjunto de módulos, cualquiera de los cuales puede ser utilizado y mejorado internamente sin requerir de un gran reacondicionamiento de todo el sistema operativo. Aunque el código fuente de Windows no se pone a disposición del público en general. Microsoft ha presentado una descripción de las llamadas al sistema requeridas por varios de los módulos a través de un conjunto estándar de Interfaces para la Programación de Aplicaciones (API). La figura 2.1 es un esquema que le muestra los diversos módulos de los que se compone la arquitectura de Windows NT.

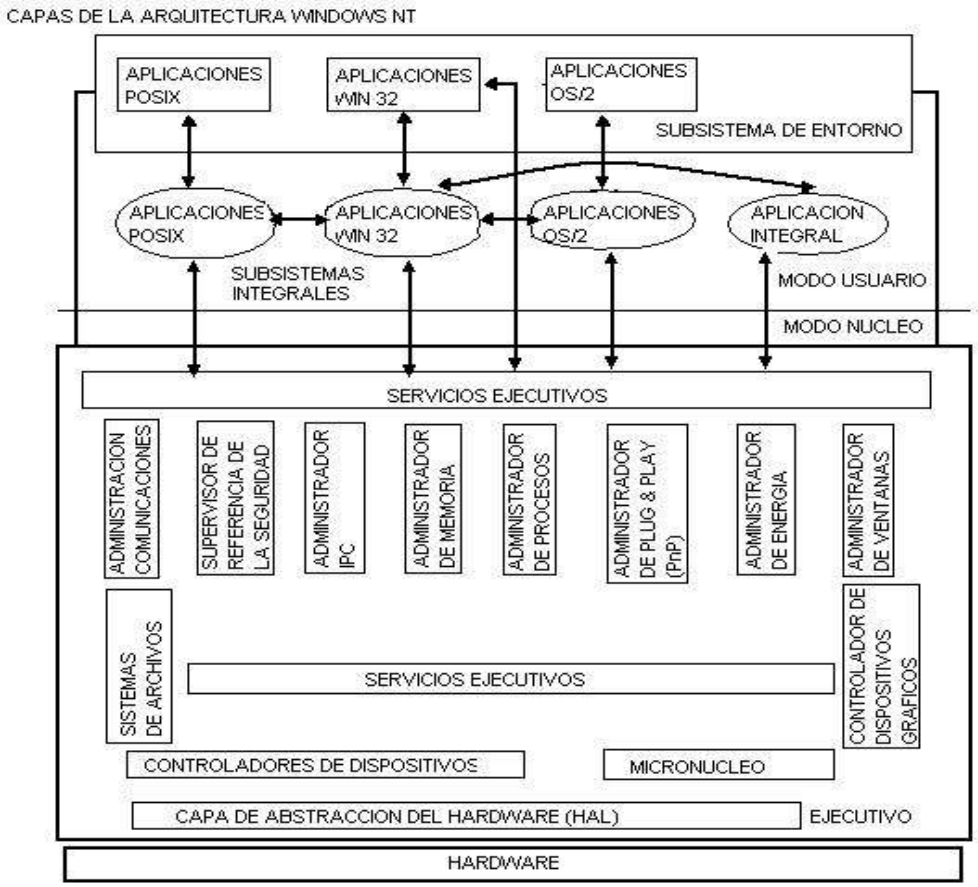


Figura 2.1 Arquitectura de Windows NT.

Al diseñar un pequeño núcleo (la parte del sistema operativo que controla a la CPU) rodeado por un conjunto de módulos interactivos, el sistema operativo NT aísla los más importantes procesos de la CPU y de comunicación con el hardware que son iniciados por las aplicaciones. A su vez, cada aplicación se ejecuta en su propio espacio protegido de memoria, lo que significa que Windows NT tiene la capacidad de ejecutar diversas aplicaciones y resistir muchos errores generados por ellas sin colapsarse. Por ello, Windows NT es mucho más confiable que otras versiones de Windows y otros sistemas operativos.

2.3 Características.

Las principales características que ofrece NT para las redes y acceso VPN son las siguientes:

- Mayor seguridad debido al cifrado de 128 bits de forma que no puedan ser leídos por otras personas.
- El directorio Activo o Active Directory, la nueva organización administrativa, que contiene la información de todos los elementos que forma parte de la red de la empresa y usuarios.
- Soporta 5 subsistemas: windows 32 bits, windows 16 bits, DOS, POSIX y OS/2.
- Funciona como cliente-servidor en una ambiente de red.
- Soporte sistemas de multiproceso.
- Provee datos, aplicaciones y protección del sistema contra accesos inadvertidos.
- Permite a los usuarios un acceso seguro a más información sin comprometer la seguridad del sistema.
- Relaciona nuevos rasgos punto a punto con el protocolo PPTP y TCP/IP.
- Ofrece múltiples conexiones de acceso telefónico y redes.

NT es un sistema operativo que ayuda a organizar la forma de trabajar a diario con la PC su diseño fue pensado para las compañías grandes por lo tanto realiza muy bien las tareas tales como la protección por contraseñas.

En grandes entornos de redes NT ofrece soporte a los siguientes entornos de computación:

- Servidor de base de datos
- Servidor de mensajería
- Servidor de archivos e impresión
- Servidor de comunicaciones
- Servidor Web

Soporte a múltiples plataformas como son:

- Procesadores intel x86
- PowerPC
- Mips
- Dec Alpha AXP
- Computadoras con simple o múltiple procesador

2.4 Conexiones de red y de acceso telefónico.

El crecimiento en la evolución de Windows NT nos ha puesto de manifiesto varios cambios en su funcionalidad. A parte de las conexiones nativas a la red y la conexión telefónica con un servidor de acceso remoto, NT había sido mejorado con herramientas como el RRAS (Servidor de enrutamiento y acceso remoto) el cual ahora esta integrado a la plataforma de Windows 2000.

RRAS permite utilizar el servidor como una plataforma de enrutamiento basada en software con el uso de adaptadores de red estándar como la interfaz de enrutamiento. Al utilizar los protocolo para el enrutamiento de información junto con la instalación de Bag Networks del protocolo OSPF (Abrir la ruta de acceso más corta primero), podrá convertir a su servidor de Windows NT en un enrutador eficiente para redes pequeñas**.**

Esto puede hacerse sin el costo de enrutadores de hardware más costosos cuando no haya mayor volumen de necesidades de enrutamiento.

La conexión de acceso telefónica ha sido, en general, un punto fuerte de NT y así aparece con Windows 2000. Ahora se reconoce una mayor cantidad de modos, se utiliza mayores posibilidades de conexión y se sustentan tarjetas WAN (para redes de área amplia), como Frame Relay y dispositivos ISDN directamente conectadas al servidor.

En la actualidad hay cinco tipos de conexiones disponibles en Windows NT, algunas de ellas ya existían en las versiones anteriores pero en esta versión se han mejorado:

1. Acceso telefónico a red privada, este se hace conectado la red a la que se llama, no tiene acceso a Internet, pero alguna otra red permite su acceso. A su vez, las dos redes podrían ser por completo privadas como para llevar algún tipo de comercio entre si.
2. Acceso telefónico a Internet, como lo hace al navegar en la Web con una conexión PPP (Protocolo Punto a Punto).
3. Conectar a una red privada a través de Internet. Las VPN (Redes Privadas Virtuales) se utilizan para forjar un “Túnel” a través de Internet al encapsular el flujo de datos con algún tipo de protección, lo que evita que otras personas puedan ver los datos. Las VPN son tan seguras como la opción 1 si se maneja adecuadamente.
4. Aceptar conexiones entrantes. Esta es la misma que la herramienta RAS de Windows NT.
5. Conectar directamente con otro equipo. Este tipo de conexión funcionaba con Windows NT 4 pero era difícil de configurar y establecer. Windows 2000 ha facilitado el proceso y permite utilizar puertos seriales, paralelos y los nuevos (aunque lento) puertos infrarrojos que se encuentran en las nuevas placas base.

2.5 Servicios de NT para acceso remoto.

La tecnología NT maneja y gestiona los accesos a la red mediante varios procedimientos de los cuales son controlados a través de su sección de acceso telefónico a redes y conexiones de red, opción que permite a un equipo conectarse a Internet, a una red o a otro equipo con la finalidad de tener acceso a los recursos y funciones de red ya se encuentre físicamente en la ubicación de la red o en una ubicación remota.

Todas las conexiones contienen un conjunto de características que se pueden utilizar para crear un vínculo entre su equipo y otro equipo en la red. Las conexiones salientes se ponen en contacto con un servidor de acceso remoto mediante un método de acceso configurado [LAN, MODEM, Línea ISDN (RDSI), etc.] para establecer la conexión con la red. A la inversa, una conexión entrante habilita a un equipo que ejecuta Windows con tecnología NT independiente para que otros equipos se pongan en contacto con él. Ya esté conectado en forma local (LAN), remota [acceso telefónico, ISDN (RDSI), etc.] o ambas, se pueden configurar cualquier conexión de forma que pueda ejecutar cualquier función de red necesaria. Por ejemplo, puede imprimir, tener acceso a unidades y archivos, examinar otras redes o tener acceso a Internet.

En toda conexión remota existen dos elementos: **el servidor**, que es el equipo encargado de proporcionar una serie de recursos, y **los clientes**, demandantes de recursos. El funcionamiento es siempre el mismo: existen unos equipos que disponen de una serie de recursos de la red que quieren hacer disponibles a otras computadoras. Para ellos a una de esas computadoras se le instala el servicio a utilizar como por ejemplo: el RAS para que permita a los clientes conectarse de manera remota y acceder a dichos recursos o el Servidor VPN que permite a los usuario establecer una comunicación privada a través de un túnel por la red de redes, Internet. El servidor VPN instalado será el encargado de comprobar que son usuarios autorizados y en caso afirmativo el cliente tendrá acceso a todos los recursos de manera similar al de cualquier

computadora que pertenezca físicamente a la red y desde cualquier parte de Internet como usuario remoto.

Conectarse a la red mediante un túnel a través de Internet: Utilizar está opción para conectar su equipo a una red privada virtual VPN mediante un MODEM es una de las opciones que más se utiliza con esta tecnología NT ya que abarca vínculos encapsulados, cifrados y autenticación en redes públicas y compartidas para los datos. Las conexiones VPN pueden proporcionar acceso remoto y conexiones enrutadas a redes privadas a través de Internet. Con el protocolo de túnel punto a punto (PPTP) o el protocolo de túnel de nivel dos (L2TP), que se instalan automáticamente con la tecnología NT, puede tener acceso de forma segura a los recursos de una red al conectar con un servidor de acceso remoto que ejecute NT a través de Internet u otra Red.

Con la tecnología NT y las Redes privadas virtuales se estudiaran las ventajas y desventajas que están representan para los usuarios móviles y la capacidad que estas tienen para manejar la seguridad en los datos.

Los usuarios que trabajan en casa o que están de viaje pueden usar conexiones VPN para establecer una conexión de acceso remoto al servidor de una organización mediante la infraestructura que proporciona una red pública como Internet. Para el usuario, la red privada virtual es una conexión punto a punto entre su equipo (el cliente VPN) y el servidor de la organización (el servidor VPN).

Los clientes VPN de Microsoft pueden utilizar los protocolos de autenticación de la forma descrita en la tabla siguiente:

Cliente VPN	Protocolo de Autenticación de Acceso Remoto compatibles
Windows 2000	MS-CHAP, CHAP, SPAP, PAP, MS-CHAP v2 y EAP.
Windows NT 4.0	MS-CHAP, CHAP, SPAP, PAP, MS-CHAP v2.
Windows 98	MS-CHAP, CHAP, SPAP, PAP, MS-CHAP v2.
Windows 95	MS-CHAP, CHAP, SPAP, PAP, MS-CHAP v2.

2.6 Configuración de un servidor VPN.

-Configuración previa.

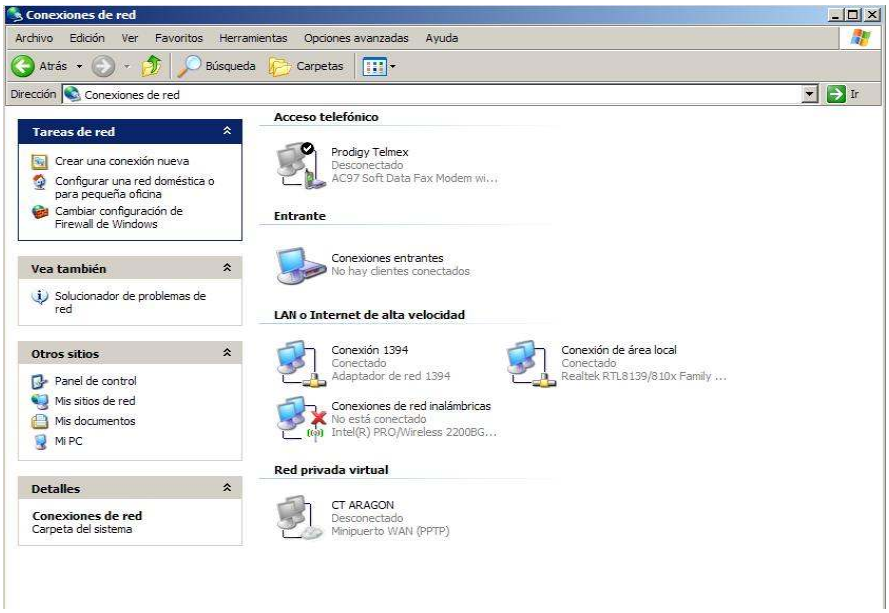
Antes de configurar el servidor como servidor VPN de acceso remoto, debe comprobar lo siguiente:

- El sistema operativo está configurado correctamente. En la familia de Windows NT, la VPN de acceso remoto depende de la configuración adecuada del sistema operativo y sus servicios. Si tiene una nueva instalación Windows NT, puede utilizar la configuración predeterminada del servicio. No se requiere ninguna otra acción.

- El servidor está configurado correctamente para ofrecer una seguridad óptima que cubre las necesidades de la red. Puesto que el servidor VPN de acceso remoto conectará la red privada, Internet y los clientes remotos, debe asegurarse de que es seguro. La seguridad de la red privada depende de la del servidor VPN de acceso remoto.
- Este equipo dispone de dos interfaces de red, una con conexión a Internet y otra con conexión a la red privada. La conexión a Internet debe ser una conexión dedicada con suficiente ancho de banda para que los usuarios de VPN puedan conectarse a la red privada y los usuarios de la red privada conectarse a Internet. La conexión de equipos a la red privada se debe realizar mediante un dispositivo de hardware, por ejemplo, un adaptador de red.
- Se han instalado todos los protocolos de red necesarios para las interfaces de red.
- Firewall de Windows está deshabilitado en el servidor que desea configurar para el acceso remoto o VPN. Configurará la característica Servidor de seguridad básico de Enrutamiento y acceso remoto durante la instalación, que sustituirá a Firewall de Windows.
- Conexión compartida a Internet está deshabilitado en el servidor que desea configurar para el acceso remoto o VPN. Conexión compartida a Internet no es compatible con Enrutamiento y acceso remoto.

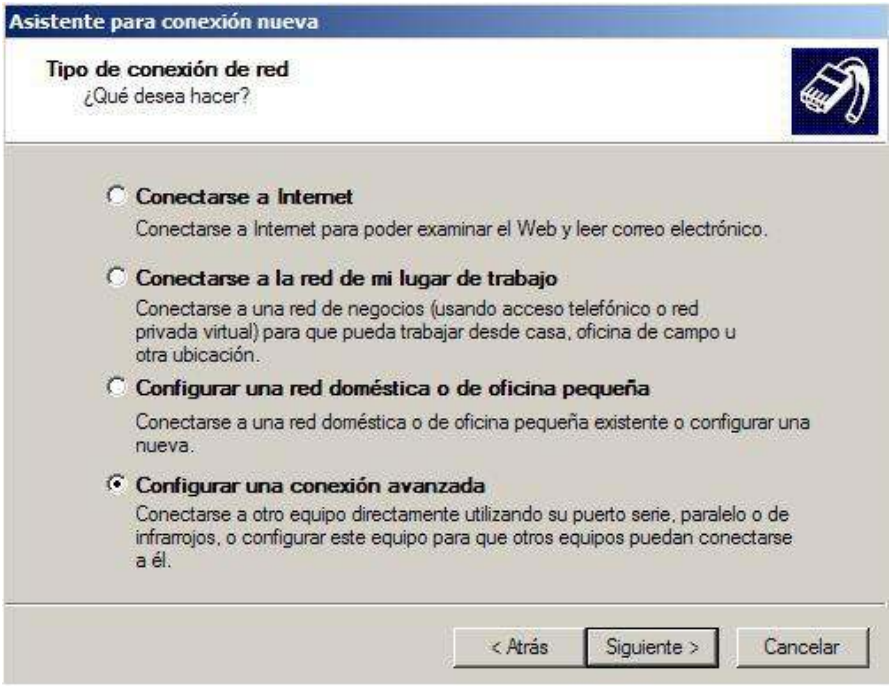
-Configuración paso a paso.

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

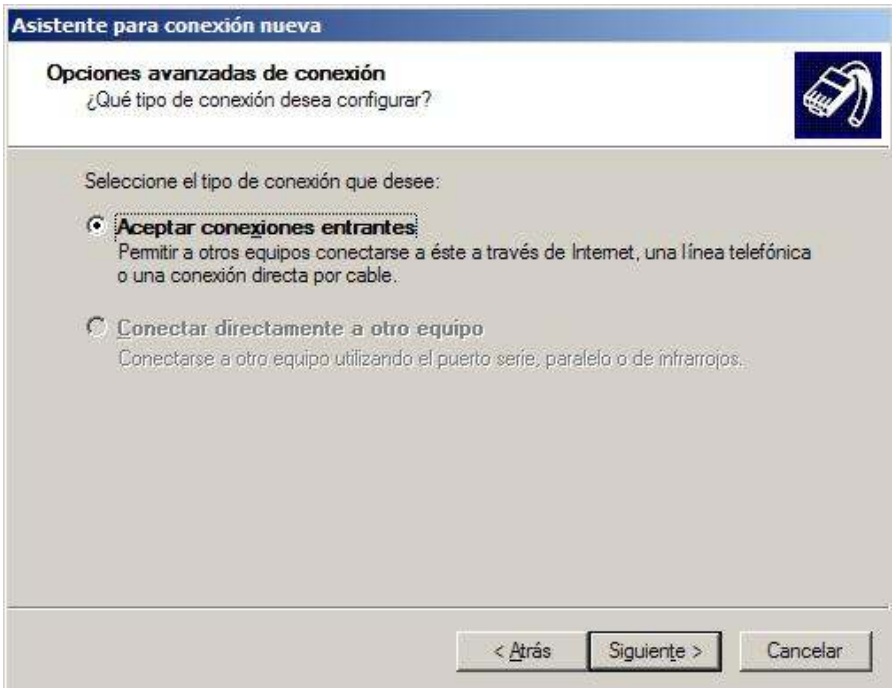


Ahora estamos en el "Asistente para conexión nueva". Pulsamos en el botón "Siguiente" para continuar.

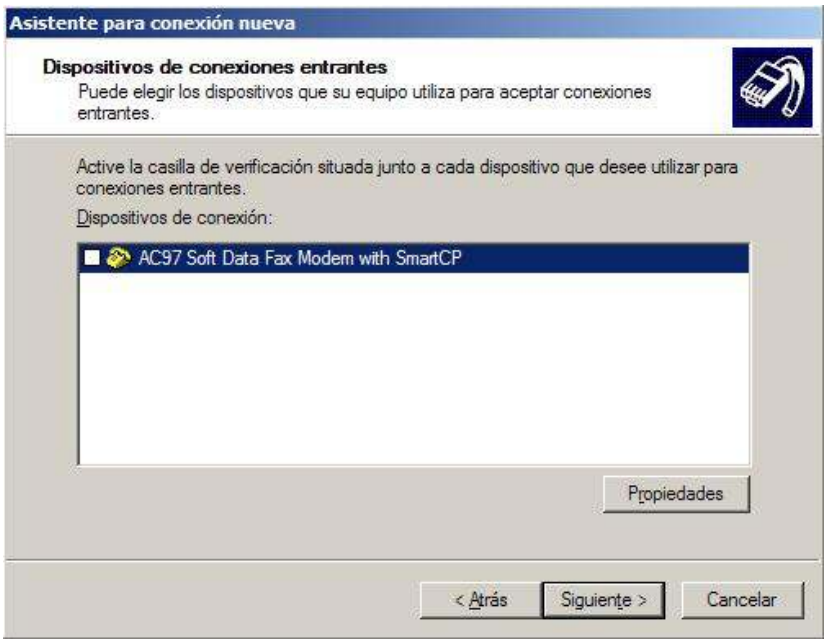
Entre las opciones disponibles seleccionamos "Configurar una conexión avanzada", y pulsamos en "Siguiente".



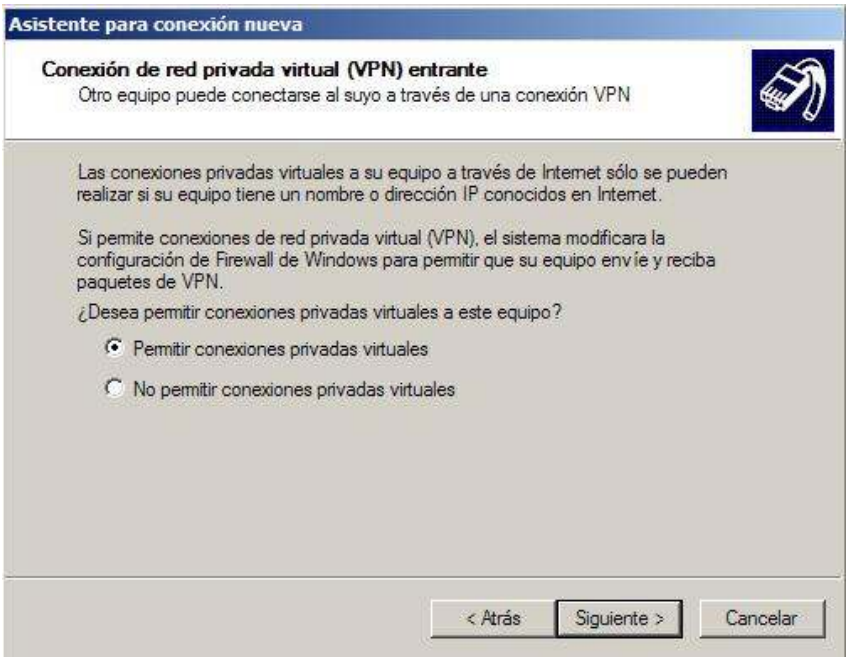
Ahora seleccionamos "Aceptar conexiones entrantes" y pulsamos "Siguiente" para continuar.



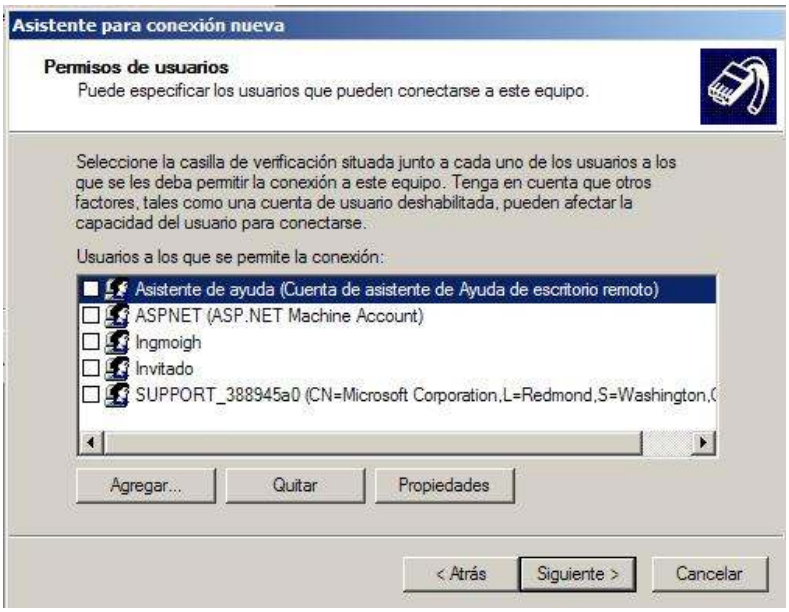
En la pantalla "Dispositivos de conexiones entrantes" no seleccionamos ninguno, pues no queremos que se conecten a este equipo haciendo una llamada o usando el puerto paralelo. Pulsamos en "Siguiente".



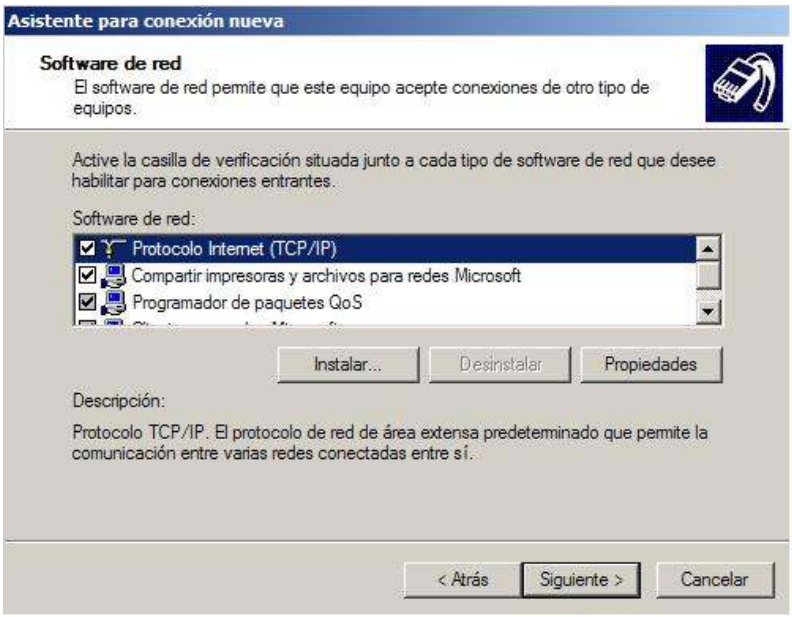
En la pantalla "Conexión de red privada virtual (VPN) entrante" debemos seleccionar "Permitir conexiones virtuales privadas". Pulsamos en "Siguiente".



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".



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.



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 IPs de los clientes o establecer un intervalo de IPs, o incluso permitir que los clientes especifiquen su IP.

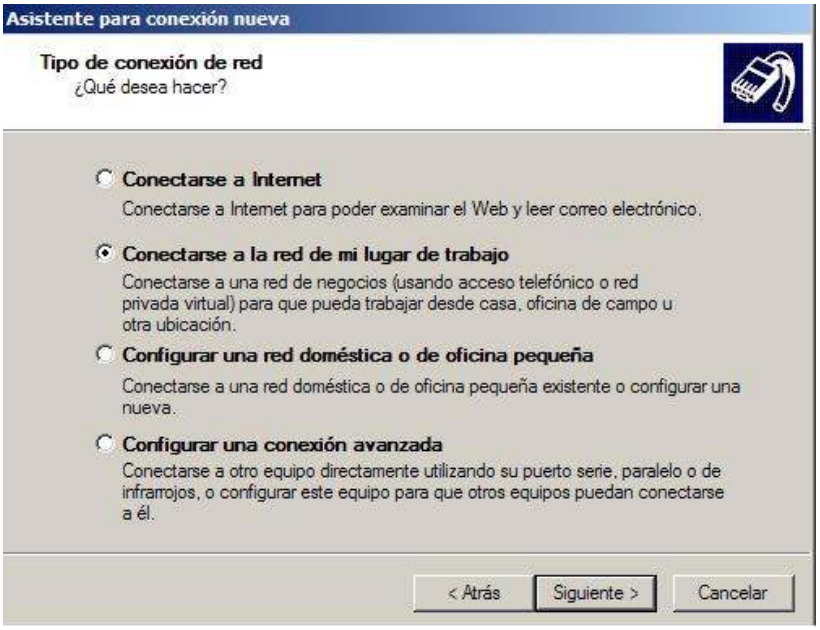
Guardamos la configuración de TCP/IP y pulsamos en el botón siguiente del asistente y ya habremos terminado. En este momento tendremos una nueva conexión en la carpeta de Conexiones de red. Seleccionando la nueva conexión podremos ver el estado de ésta, los clientes conectados, cambiar las opciones de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

Ahora ya tenemos configurado el servidor VPN y ya está listo para aceptar clientes VPN.

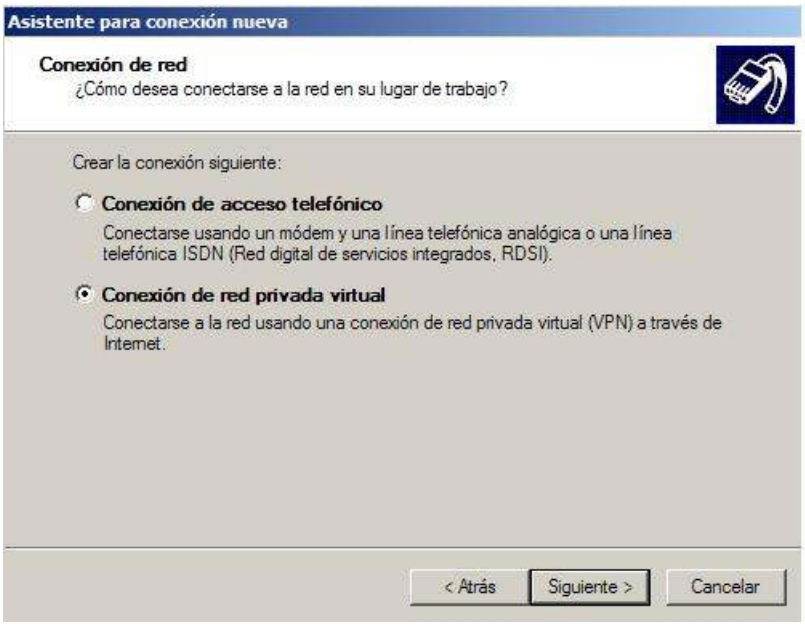
A continuación configuraremos una conexión VPN para que se conecte al servidor.

2.7 Configuración de un cliente VPN.

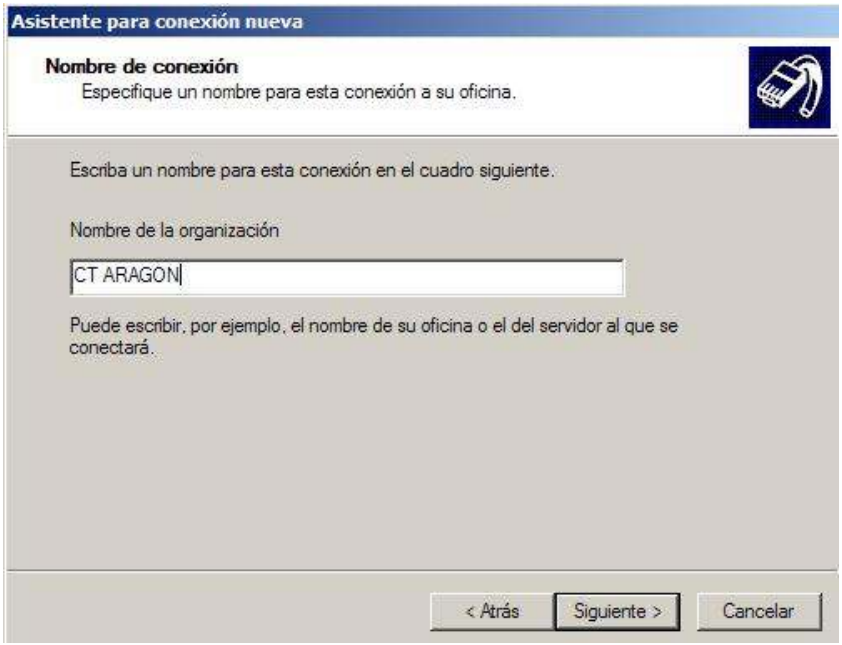
Abrimos la carpeta de "Conexiones de red" y en el menú Archivo seleccionamos "Nueva conexión". En el asistente para conexión nueva seleccionamos "Conectarse a la red de mi lugar de trabajo", y pulsamos siguiente.



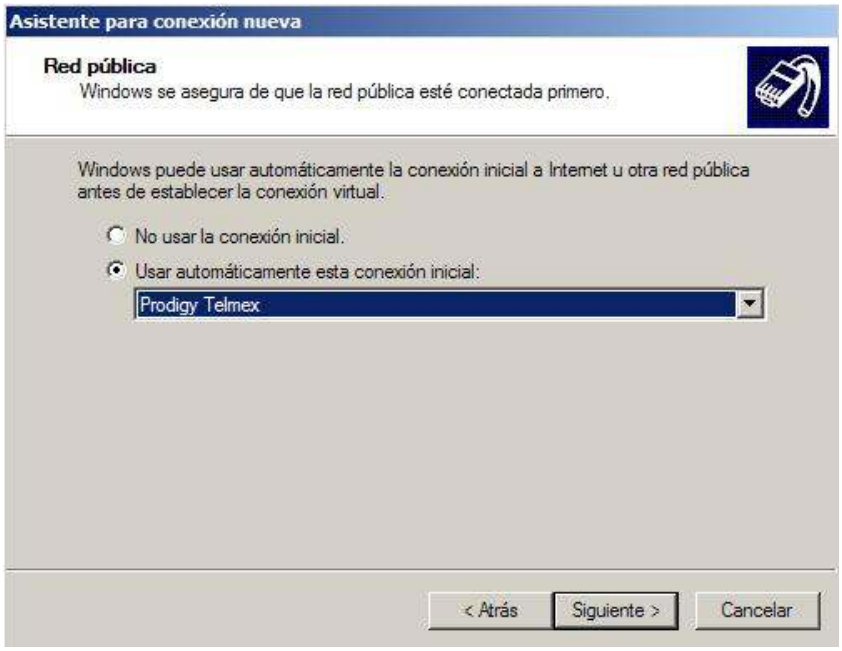
Seleccionamos "Conexión de red privada virtual", y pulsamos siguiente.



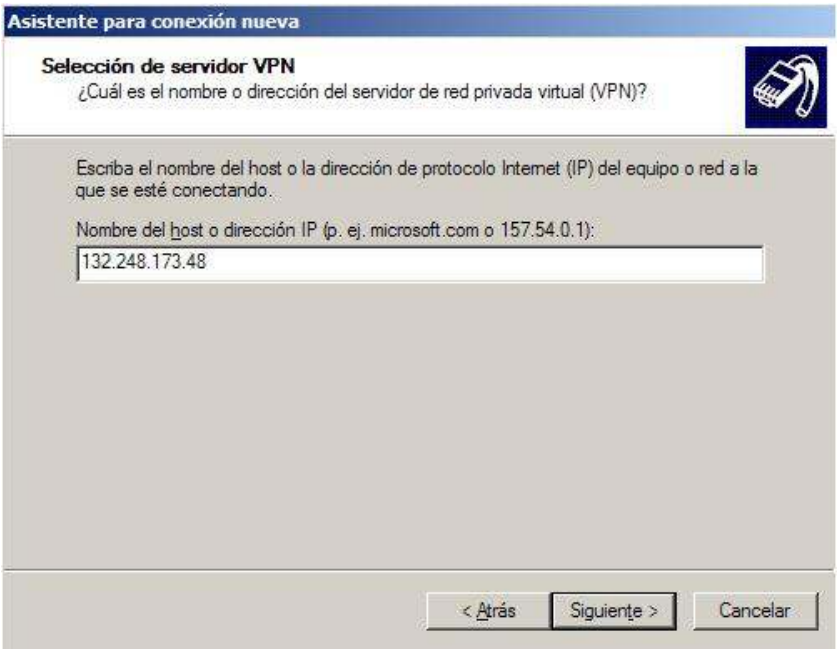
En la siguiente ventana indicaremos el nombre de nuestro servidor a donde iniciaremos la conexión VPN en este caso el Centro Tecnológico Aragón.



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.

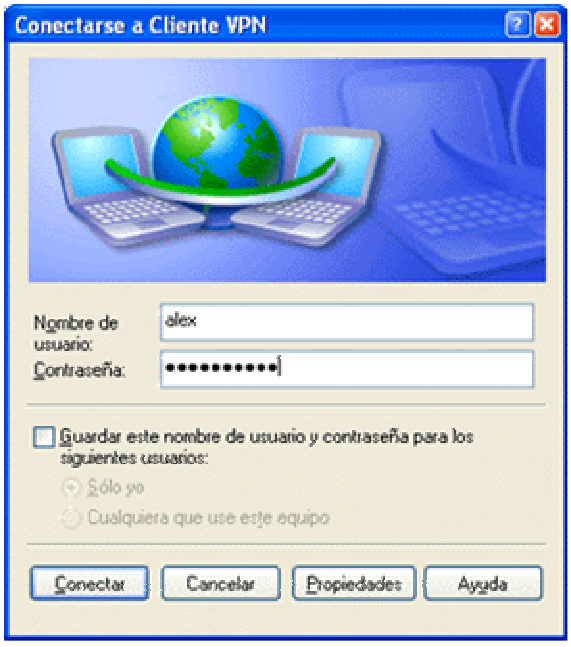


En la figura que se muestra a continuación colocaremos la dirección IP fija que tendrá nuestro servidor VPN para realizar el acceso remoto y poder así ubicar fácilmente nuestro servidor.



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 MODEM o Cable la IP puede cambiar (IPs 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 trabajara lenta por el ancho de banda que ofrece esta tecnología. 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 10.0.0.1 pondremos \\10.0.0.1 en la barra de direcciones del Explorador de Windows y de esta forma ya tendremos acceso a los ficheros e impresoras de la máquina indicada.

Para usar otros recursos, como servidores de base de datos, etc. Simplemente usamos la IP en la VPN de la máquina destino.

2.8 Seguridad

Lo que se refiere a seguridad este sistema operativo incorpora funciones de control de acceso discrecional que permite asignar permisos a archivos individuales. El concepto de derechos de usuario le ofrece un sistema de control discrecional de las funciones básicas del sistema operativo como establecer la hora y cerrar la computadora.

También centraliza las cuentas de usuario de red y otro tipo de información de seguridad, facilitando el uso y la administración de la red. Con una administración centralizada de la seguridad solo es necesario administrar una cuenta por cada usuario. Dicha cuenta permite al usuario acceder a todos los recursos de la red.

La seguridad en Windows NT es una combinación de técnicas que aseguran un nivel de protección consistente contra los accesos no deseados. Para implementar la seguridad, tendremos que proteger la red, el sistema operativo y los datos. Para eso, disponemos de la autentificación de acceso propia de Windows NT, seguridad a nivel de objeto y derechos de usuarios.

La seguridad puede ser clasificada en tres diferentes áreas funcionales: seguridad a nivel de red, seguridad del sistema operativo y cifrado de datos.

- La Seguridad de red ofrece autentificación (verificando que el servidor de datos y que el receptor de los mismos son correctos) y verificando la integridad de la información (de forma que los datos enviados y los recibidos sean los mismos). Conseguir este nivel de seguridad a nivel de red significa haber implementado un protocolo de red, como NetBEUI[4] o TCP/IP, ajustado a las necesidades de la red.

Esos protocolos ofrecen varios niveles de seguridad, rendimiento (conseguidos reduciendo al mínimo la carga derivada de la seguridad), flexibilidad, y disponibilidad sobre múltiples plataformas.

- La seguridad a nivel de sistema operativo debe estar integrada con él mismo desde un buen principio. Si esas funciones básicas de seguridad no han sido implementadas al propio sistema operativo desde un principio, implementarlas con posterioridad será casi imposible. Por ejemplo, Microsoft no fue capaz de implementar una seguridad seria a sus versiones de 16 bits de Windows tras su fase de desarrollo. Fue necesario un nuevo sistema operativo de 32 bits, y un nuevo modelo de programación (la API Win32) para poder hacerlo. Windows NT dispone de unas robustas funciones de seguridad que controla el acceso de los usuarios a los objetos como archivos, directorios, registro de sistema e impresoras.

[4] NetBEUI es un protocolo de nivel de red sencillo utilizado en las primeras redes de Microsoft y en versiones como Windows 95.

- También incluye un sistema de auditoría que permite a los administradores rastrear los accesos a los archivos u a otros objetos, reintentos de inicio de sesión, apagados y encendidos del sistema, etc. En cambio, Windows 95 dispone únicamente de un rudimentario sistema de seguridad en el inicio de sesión, y no dispone de seguridad a nivel de objetos.
- Cifrado de datos. Puede operar de distintas formas. Muchas aplicaciones disponen de cifrado por sí mismas. Algunos protocolos, como SSMTP (Secure Simple Mail Transfer Protocol) soportan cifrado automático. Incluso Microsoft ha añadido un sistema de cifrado básico, CAPI (Cryptography API) a la API Win32.

CAPI consiste en un juego de funciones que permiten a las aplicaciones y a los desarrolladores de sistemas de software acceder de forma independiente a los servicios de criptografía. NT dispone de un servicio básico de criptografía que nos permite codificar los datos facilitando así el almacenamiento seguro y una transmisión segura combinando claves públicas y privadas.

2.9 Ventajas

- Los sistemas operativos de Microsoft proporcionan comunicaciones económicas, seguras y fáciles que habilitan los negocios sin límites. Una de las funciones de una plataforma de comunicaciones basada en Windows es el soporte de Red Privada Virtual (VPN).
- Las VPN se han hecho populares debido a que ofrecen ahorros operacionales. Al tiempo que mantienen la seguridad relacionada con la infraestructura de red privada. La seguridad se mantiene debido a que VPN utiliza un túnel seguro, con lo que permite que sólo los usuarios autentificados accedan a la Intranet corporativa. Las soluciones VPN de Microsoft ofrecen cifrado de datos de 128 bits.

- Microsoft ha sido pionero en la integración de soluciones VPN y sigue trabajando con los socios industriales y con la Fuerza de Ingeniería de Tareas (IEFT) de Internet para impulsar la tecnología y seguridad de redes privadas virtuales.
- Las VPN de Microsoft cubren un espectro de necesidades de seguridad. El protocolo de Túnel (PPTP), el cual esta disponible para los sistemas operativos de Windows, fue diseñado para proporcionas los costos totales de propiedad más bajos. PPTP se ejecuta bien en una amplia variedad de hardware, soporta la autenticación de contraseñas, y no requiere la implementación de una infraestructura certificada, aunque el soporte certificado estará disponible en la configuración de tiempo de Windows en su versión 2000.
- Las implementaciones de Protocolo de túnel de nivel 2 (L2TP) y seguridad protocolo Internet (IPSEC) de Microsoft, las cuales estarán disponibles en la plataforma de Windows 2000, están diseñadas para proporcionas la mayor seguridad posible. En consecuencia, estas soluciones VPN requieren la implementación de una infraestructura de clave pública, y requiere de un procesador de clase Pentium.
- La solidez de la seguridad de las soluciones VPN Microsoft permite que las organizaciones aprovechen al máximo la conveniencia y ahorros en los costos de conexión por túnel a través de redes públicas, sin permitir el acceso no autorizado.

2.10 Sistema de Administración de Usuarios

La administración de VPN se puede llevar a cabo mediante Active Directory (Directorio Activo) de Windows 2000 Server, el administrador de sistema puede configurar parámetros de usuarios para la Red Privada Virtual, que refuerce notablemente las medidas de seguridad; por ejemplo, los niveles requeridos de cifrado de datos y contraseñas, y la autenticación, estos requisitos se pueden aplicar a usuarios individuales o a un grupo (o perfil) de usuarios similares. Por ejemplo, el administrador de sistema puede configurar el marcado de acceso remoto para definir un perfil de grupo, todos los usuarios asignados a ese perfil de deberán autenticarse mediante el Protocolo de Autenticación Extensible (EAP) y cifrar sus datos mediante el cifrado de datos de alto nivel (128 bits). Al asignar un usuario el perfil de grupo, estas medidas de seguridad se exigirán automáticamente cuando cualquier usuario con ese perfil de grupo se conecte al servidor de acceso remoto.

El estudio y análisis de este sistema operativo es importantes ya que demuestra que es una plataforma comercial y muy utilizada en la infraestructura de las redes de cómputo de las corporaciones, tomando en cuenta esto el desarrollo de las VPN en este sistema operativo va aumentando cada día, mejorando su estructura de programación y funcionalidad en esta plataforma, a comparación de otros sistemas operativos, éste se maneja en mayor medida por los administradores de sistemas y como veremos en el siguiente capítulo existe otra alternativa de VPN en un sistema operativo que aunque no es comercial si es muy utilizado, por varias corporaciones que requieren una disminución de costos en sus sistemas y sus licencias del producto.

CAPÍTULO III

AMBIENTE DE TRABAJO VIRTUAL VPN BAJO LA PLATAFORMA GNU/LINUX.

- Conocer la tecnología GNU/LINUX y su desarrollo en las VPN.

3.1 GNU/LINUX.

El sistema operativo Linux cuenta con una implementación de servicios de red basada en el núcleo (kernel), escrita casi por completo partiendo de cero, desde su creación. Su rendimiento en los núcleos recientes lo convierten en una alternativa valida incluso con los mejores sistemas operativos del mercado para estos servicios en redes. Dentro de Linux la mayoría de las distribuciones vienen por defecto con el soporte de red activado, por lo cual no es necesario recompilar el núcleo, a menos que el soporte con tarjetas de marcas no muy comunes hagan necesaria esta recompilación.

El sistema lo forma el núcleo llamado Kernel más un gran número de programas/biblioteca que hacen posible su utilización. Muchos de estos programas y bibliotecas han sido posibles gracias al proyecto GNU (General Public License), por esto mismo, muchos llaman a Linux, GNU/Linux, para resaltar que el sistema lo forma tanto el núcleo como gran parte del software producido por el proyecto GNU.

Linux es a partir de la versión original un clon del sistema operativo Unix y que fue escrito desde cero por Linus Torvalds. Una de las cosas interesantes de Linux es que el desarrollo ocurre simultáneamente alrededor del mundo. Mucha gente contribuye a el desarrollo de este sistema operativo considerado GNU o GPL y que esta diseñada para evitar que alguna persona restrinja la distribución del software.

3.2 Antecedentes.

En algún momento se pensó que Linux podría ser una herramienta importante para la solución de redes LAN y de Acceso remoto y que muy pronto cambiara el rumbo de las redes, con la creación del desarrollo de los primeros controladores de dispositivos para la implementación del protocolo SLIP (Serial Line Internet Protocol) en Linux se empezaron a crear las primeras conexiones de Internet y de ahí surgió la idea de todas las posibilidades que podrían hacerse realidad si Linux tuviera un soporte total de red y creciera el número de usuarios usando y experimentando de forma activa el software de red que existía.

El sistema operativo GNU/Linux permite establecer Redes Privadas Virtuales siguiendo todos los estándares de la industria, entre ellos, la tecnología más implantada es IPSec que goza de varias implementaciones muy potentes en GNU/ Linux.

Linux es un sistema operativo más barato que los otros sistemas operativos y con frecuencia es menos problemático que algunos sistemas comerciales esto por las características que a continuación se detallan en este capitulo.

3.3 Arquitectura GNU/Linux.

Muchas distribuciones de GNU/Linux vienen con discos de arranque que funcionan con el hardware para PC más común. Normalmente, el núcleo suministrado es altamente modulable e incluye casi cualquier controlador que pueda necesitar.

Las arquitecturas en las que en un principio se puede utilizar Linux son Intel 386, 486, Pentium, Pentium Pro, Pentium II/III/IV, Amd 5x86, Cyrix y Motorota 68020, IBM s/390, DEC Alpha, MIPS, Power Pc y UltraSparc. Además no es difícil encontrar nuevos proyectos portando Linux a nuevas arquitecturas.

3.4 Características.

En Linux el fragmento común de código de todas las versiones o distribuciones[5] es el kernel o núcleo del sistema operativo. Si bien este kernel se puede modificar para incluir el soporte para las utilidades que desee incorporar, cualquier kernel de Linux ofrece las siguientes características:

- Multiusuario. No solo puede tener muchas cuentas de usuario disponibles en un sistema Linux, sino que también se puede tener múltiples usuarios conectados y trabajando en el mismo sistema al mismo tiempo. Los usuarios pueden tener sus propios entornos dispuestos como ellos deseen, su propio directorio de inicio para poder almacenar sus archivos, así como su propia interfaz de escritorio.

- Multitarea. En Linux es posible tener muchos programas ejecutándose al mismo tiempo o que implica que no solo puede tener muchos programas funcionando al mismo tiempo, si no que también Linux puede ejecutar programas en segundo plano. Muchos de estos procesos del sistema hacen que Linux pueda funcionar como servido, ya que estos procesos en segundo plano escuchan las peticiones de la red para acceder al sistema. Estos procesos en segundo plano se denominan DAEMONS (Demonios).

[5] Una distribución Linux es un conjunto de aplicaciones reunidas que permiten mejoras para instalar fácilmente un sistema Linux, se destacan por sus herramientas para configuración y sistemas de paquetes de software a instalar.

- Conectividad a la red. Para conectar el sistema Linux a una red, Linux ofrece soporte para una serie de tarjetas de red, módems y dispositivos serial para una Red de Área Local (LAN). Además de los protocolos de Lan, como los protocolos ethernet y token ring, se pueden incorporar todos los protocolos de red de nivel superior más populares. El más conocido de estos protocolos es el TCP/IP.

- Servidores de Red. Lo que Linux hace mejor es ofrecer servicios de red a los ordenadores clientes de LAN o para todo Internet. Se puede tener acceso a una gran variedad de paquetes de software que le permiten usar Linux como servidor Web, de impresión, servidor de archivos, ftp, servidor de correo o servidor de grupo de trabajo.

3.5 Protocolos en Linux para VPN.

GNU/Linux ofrece todo lo necesario para trabajar en red con TCP/IP (el protocolo de Internet). Desde manejadores para las tarjetas de red más populares, PPP (que permite acceder a una red TCP/IP utilizando un módem y la línea telefónica), PPPoE (acceso TCP/IP mediante ADSL), PPTP Protocolo de Túnel Punto a Punto (PoPToP). Y también existen gran cantidad de aplicaciones relacionadas con Internet, como navegadores, clientes de correo, clientes de mensajería instantánea, etc.

3.5.1 PPP en Linux.

Diseñado como una extensión del PPP, PPTP encapsula paquetes PPP dentro de datagramas IP para la transmisión a través de Internet u otras redes públicas basadas en TCP/IP.

PoPToP es la solución para servidores PPTP bajo GNU/Linux. PoPToP permite a servidores Linux funcionar correctamente en entornos PPTP VPN. La versión actual soporta clientes PPTP Windows 95/98/NT/2000 y clientes PPTP Linux. PoPToP es software libre GNU.

Requerimientos del sistema

- Una distribución de GNU/Linux actual (RedHat, Debian, etc.) con un kernel reciente, aunque funciona con kernel 2.0.x y 2.2.x, la mejor opción el uso de un kernel 2.4.x.
- PPP 2.3.8, aunque muchas distribuciones actuales ya llevan 2.4.x, y aparte necesitaremos el parche para el ppp de MSCHAPv2/MPPE para la autenticación y encriptación compatible con los clientes de Microsoft.
- Parche MPPE para el kernel, soportados como ya he dicho anteriormente, 2.0.x, 2.2.x y 2.4.x.
- Servidor PPTP para GNU/Linux, PoPToP.

3.6 Conexiones VPN sobre GNU/Linux.

Linux nos ofrece diversas soluciones para aplicar VPN e intercomunicar dispositivos en la red que manejan IPsec. Algunos de estos productos pueden ser:

- **Freeswan**
- **CIPE**
- **VPND**
- **OPENVPN**

3.6.1 Implementación de VPN's con IPSec y FreeS/WAN.

FreeS/WAN es una implementación *libre* distribuida bajo licencia GPL del protocolo IPsec para sistemas operativos GNU/Linux. IPsec proporciona servicios de cifrado y autentificación en red a nivel IP, protegiendo de esta forma *todo* el tráfico IP entre los dos equipos que hayan establecido una sesión IPsec, en lugar de cifrar sólo el tráfico de un determinado protocolo como es el caso con los servidores seguros tipo SSH, HTTPS, etc. De esta forma se consigue un nivel de seguridad mucho mayor entre los dos hosts que intervienen en la conversación.

El protocolo IPsec (y, por lo tanto, FreeS/WAN) se puede utilizar en cualquier equipo en una red IP, ya sea su papel el de cliente, servidor, router, etc. El caso más común que nos podremos encontrar es el de un router de una red corporativa que se conecta a través de Internet (una red insegura) utilizando IPsec al router de la red corporativa de otra sede de la misma empresa, estableciendo así una VPN (Virtual Private Network, *Red Privada Virtual*) entre ambas sedes. FreeS/WAN es la solución perfecta en el caso de que el router que realiza la conexión IPsec sea un PC con Linux.

FreeS/WAN provee hoy por hoy del protocolo IPsec a la implementación IPv4 (la actual versión de IP) del núcleo de Linux, y ya se está trabajando en la integración de FreeS/WAN en la pila IPv6 de Linux, por lo que con toda probabilidad será la implementación oficial del estándar IPsec para Linux.

FreeS/WAN se compone de varias partes, que entre todas colaboran para implementar todos los protocolos de IPsec:

- KLIPS (Kernel IPsec, *IPsec en el Núcleo*), una serie de rutinas en el núcleo del sistema operativo Linux que implementan los protocolos AH y ESP, y todas las funcionalidades necesarias para manejar estos tipos de paquetes en la red.
- Pluto (*demonio IKE*[6]), un servicio que se ejecuta ya fuera del kernel, en espacio de usuario, que gestiona la totalidad del protocolo IKE.
- Varios scripts y utilidades en espacio de usuario, para configurar y gestionar IPsec.

3.6.2 VPND en Linux.

La red privada virtual demonio VPND es un *demonio* que conecta dos redes en el nivel de red a través de TCP/IP o una línea (virtual) arrendada ligada a una interfaz serial. Todos los datos transferidos entre las dos redes se cifran usando el algoritmo Blowfish[7] (no patentado y gratuito).

VPND no se propuso como reemplazo del software de seguridad en las comunicaciones existente como ssh o facilidades de *tunneling* del sistema operativo. Sin embargo, se propuso como un medio para asegurar la interconexión transparente de redes a través de canales potencialmente inseguros como lo es Internet.

[6] IKE Internet Key Exchange es un protocolo que permite autentificar dos nodos en una red. Véase Capitulo 1 apartado 1.5.15 Protocolo IKE.
[7] En criptografía, **Blowfish** es un codificador de bloques simétricos.

La figura 3.1 muestra básicamente como trabaja la VPND (en lugar del socket TCP, VPND puede usar un dispositivo serial):

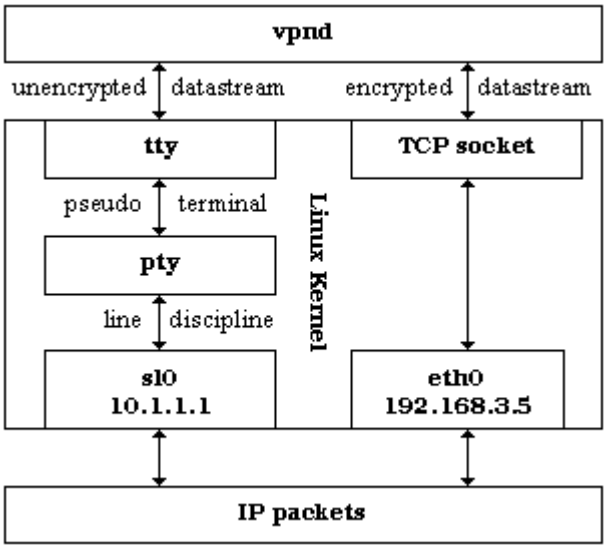


Figura 3.1 Estructura del VPND.

La VPND adquiere una pseudo Terminal (un dispositivo par pty/tty) y enlaza una disciplina de línea SLIP a ella. El efecto de esto es que la VPND ahora tiene su propia interfaz de red, una interfaz SLIP llamada slx donde x es algún número de la terminal que obtuvo al conectarse. Todos los paquetes IP enviados a esta interfaz se leen como un *datastream* por la VPND y el datastream escrito por la VPND reaparece como paquetes IP en esta interfaz.

A continuación, VPND cifra el datastream leído y lo envía a través de una conexión TCP o sobre una línea serial a su par VPND. El datastream recibido por VPND de su par es descifrado y luego escrito en la pseudo Terminal.

Como una VPND no reconoce el datastream de la pseudo Terminal, todos los paquetes escritos por el kernel a la interfaz SLIP son transportados.

Así la red de túneles VPND trafica entre dos sistemas como un demonio de nivel de usuario.

3.6.2.1 Seguridad con VPND.

VPND usa la clave maestra compartida solo para la instalación de un buffer de limpieza (*whitening*) y el cambio de la clave de la primera sesión cuando se establece la conexión TCP o línea serial. Las claves de sesión constan de datos aleatorios. Como puede verse, la clave maestra sólo se usa para transferir datos aleatorios. Así es imposible recuperar la clave maestra espiando el tráfico de red. La clave maestra compartida entre dos pares VPND es una diferencia principal para muchos otros paquetes de software como ssh. Hay, sin embargo, una ventaja mayor: VPND no requiere ninguno de los algoritmos de clave pública / privada patentados como RSA. El algoritmo Blowfish es el mas utilizado en este caso por ser un codificador eficiente y su único defectos es que no está patentado.

La longitud de clave por defecto y máxima de 576 bits es más que suficiente. Se tiene que recordar que esta es la longitud de clave de una cifra simétrica. Para estas cifras una longitud de clave de 128 bits se considera normalmente como muy segura. Así, la longitud de clave máxima debería ser suficiente para cubrir el incremento del poder de cómputo de los próximos años.

3.6.3 VPN con CIPE (Encapsulación del Criptograma IP).

Este es un proyecto prolongado para construir enrutadores IP cifrados. Está diseñado para paso de paquetes cifrados entre enrutadores previamente organizados en la forma de paquetes UDP. Esto no es tan flexible como el IPSec pero es suficiente para el propósito original: conectando subredes firmemente sobre un tránsito inseguro de redes.

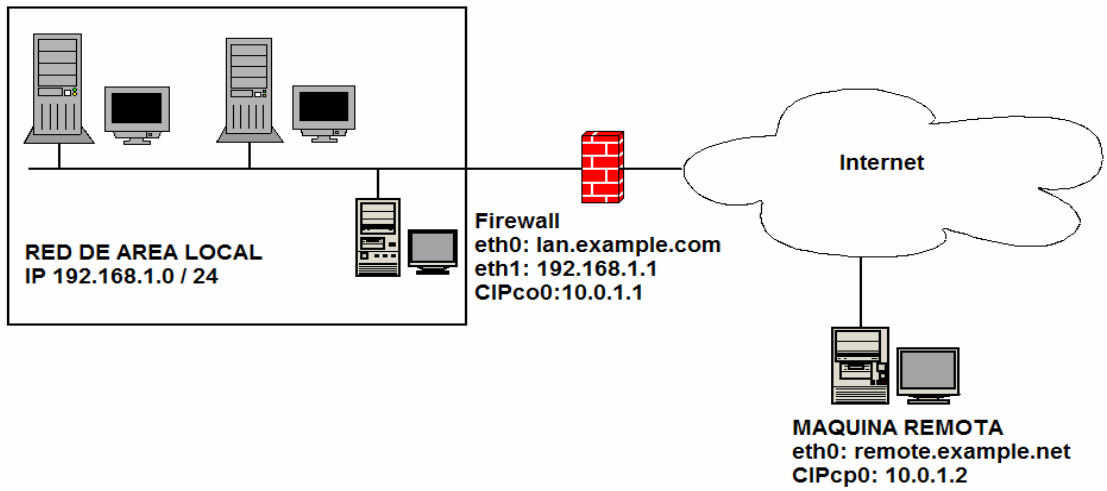


Figura 3.2. Una red y un cliente remoto conectados por CIPE.

En la figura 3.2 muestra una red ejecutando CIPE en un cortafuegos (firewall) y una máquina cliente remota actuando como el nodo CIPE. La conexión CIPE actúa como un túnel a través del cual todos los datos relacionados a la Intranet son enrutados entre los nodos remotos. Todos los datos son cifrados usando llaves de 128-bits generadas dinámicamente y pueden ser comprimidas para las transferencias de grandes archivos o para enviar por un túnel las aplicaciones X

hasta un host remoto. CIPE puede ser configurado para establecer comunicación entre dos o más máquinas Linux con CIPE y tiene los controladores de red para sistemas operativos basados en Win32.

La única implementación disponible por ahora es un controlador de Kernel para Linux. Otra implementación, un controlador de nivel de usuario (*user-level*) para Linux y sistemas BSD fue implementado a medias como un test-bed pero fue abandonado. Estas implementaciones están disponibles gratuitamente bajo el GNU GPL o condiciones menos restrictivas.

CIPE es una descripción de un protocolo para una encriptación IP ultraliviana. La meta principal de este software es proporcionar facilidades para asegurar la interconexión a través de un paquete sobre una red insegura tal como lo es Internet.

3.6.3.1 Generalidades.

Este protocolo fue diseñado para ser simple y eficiente y para trabajar con facilidades en comunicaciones existentes, especialmente para encapsulamiento de paquetes UDP. La compatibilidad con protocolos existentes tales como el IPSEC RECs no fueron concernientes. Las primeras implementaciones de prueba fueron hechas sobre el nivel de usuario, mientras que últimamente se publicó una que consiste en un modulo kernel y un programa de nivel de usuario.

El modelo CIPE asume un enlace fijo entre dos pares con intercambio de datagramas. La forma más común de implementarlo en enviando mensajes UDP entre ellos (otra forma podría ser encapsulamiento por medio de PPP).

El protocolo CIPE consta de dos partes: encriptación y suma de verificación de los paquetes de datos e intercambio de claves dinámico.

3.6.3.2 Cifrado de paquetes.

Cada datagrama IP se toma como un todo, incluyendo la cabecera. Se rellena al final con cero a siete octetos aleatorios tal que la longitud total en octetos es congruente a tres módulo ocho. Al paquete rellenado se le adiciona un octeto del valor P y el CRC-32 al paquete construido hasta el momento e incluyendo P. Esto hace que la longitud del paquete completo sea un múltiplo de ocho octetos.

El valor P se da así: los bits 6, 5, 4 indican la longitud del relleno entre el final del paquete original y P. Los bits 2 y 1 son un tipo de código e indican la clase de paquete. Los bits sobrantes 7, 3 y 0 están reservados y deben ser cero.

Los tipos de código son:
00 - dato
01 - intercambio de clave
10 - reservado
11 - reservado

Consideraciones de seguridad.

Los paquetes que se transmiten no llevan ninguna información relativa al datagrama IP original aparte de su longitud, rellenada a un múltiplo de ocho. Esto debería guardar efectivamente contra la mayoría de los aspectos de análisis de tráfico.

3.6.4 OpenVPN Linux.

OpenVPN es un Proyecto Open Source y se encuentra bajo la licencia GPL. Licencias Comerciales también se encuentran disponibles para compañías que deseen redistribuir OpenVPN con sus propios programas o Aplicaciones.

OpenVPN es una solución completa SSL[8] VPN la cual puede organizar un amplio rango de configuraciones, incluido acceso remoto, sitio-a-sitio VPN's, seguridad WiFi, y soluciones de escala remota empresariales, balanceando la carga, previendo la saturación, y teniendo buenos accesos garantizados.

OpenVPN es un demonio utilizado para crear redes privadas virtuales. Esto significa que es capaz de enlazar dos computadoras de forma que parezca que están en la misma LAN Además, esta conexión entre los dos nodos puede ir cifrada utilizando OpenSSL, lo que se convierte en una herramienta idónea para ser utilizada en redes wireless de forma segura.

La primera ventaja de OpenVPN es que se encuentra bajo la licencia GPL, es decir, es software libre. Puede utilizar tanto TCP como UDP para comunicar los dos nodos extremo, recomiendan el uso de UDP por cuestiones de congestión de la red. En un principio no se entendía esto ya que UDP no tiene control de errores y por tanto se podrían perder paquetes, por eso se decide por utilizar TCP. Openvpn vendría a representar una capa inferior y las capas superiores utilizarían TCP, es decir, es posible usar openvpn con UDP ya que el control de errores se hará a un nivel superior, por ejemplo cuando conectemos a una Web. Es lo mismo que la propia Internet, el medio físico no te garantiza que el paquete vaya a llegar correctamente y tienes que poner controles en capas superiores. Aquí el medio físico vendría a ser UDP.

[8] SSL Secure Socket Layer.

OpenVPN implementa en la capa 2 y 3 del Modelo OSI de Seguridad de Red extendiéndose así a los estándares de la industria el protocolo SSL/TLS, soporta la autentificación flexible del cliente, métodos basados en certificados, tarjetas inteligentes, y/o autentificación, y permite al usuario o grupo especifico controlar las políticas usando reglas de firewall aplicadas hacia la VPN la interfase Virtual. OpenVPN no es un Proxy de Aplicación en Web y no funciona a través de un Navegador Web.

OpenVPN opera bajo las siguientes plataformas:

Linux, Windows 2000/XP y superior, OpenBSD, FreeBSD, NetBSD, Mac OS X, y Solaris.

3.6.4.1 Características de OpenVpn.

- Hacer un túnel por cualquier subred IP o por un adaptador virtual de Ethernet o sobre un solo puerto del UDP o TCP.
- Configurar y hacerlo redimensionable, tener una Carga – Balanceada en el servidor VPN usando unas o más máquinas que pueden manejar millares de conexiones dinámicas de clientes entrantes de VPN.
- Utilizar todo el cifrado, autentificación, y características de la certificación de la biblioteca de OpenSSL para proteger del tráfico tu red privada así como el tráfico de Internet.
- Utilizar cualquier cifra, tamaño de la llave, o resumen de HMAC (para la verificación de la integridad del Datagrama) apoyado por la biblioteca de OpenSSL.
- Escoger entre una llave-estática basada en un cifrado convencional o un certificado- basado en un cifrado de llave publica.
- Utilizar las llaves estáticas, llaves pre-compartidas o TLS-basadas en el intercambio dinámico de llaves.

- Utilizar en tiempo real la compresión adaptable y controlar el desempeño de la red en base a la utilización del ancho de banda.
- Hacer un túnel en las redes públicas que son puntos finales y que son dinámicas tal como DHCP o Clientes de acceso dial-in.
- Las Redes de túnel a través de una conexión- de Inspección minuciosa a través de firewalls sin tener que explicar reglas explicitas del firewall.
- Redes de Túnel sobre NAT,
- Crear puentes seguros usando los dispositivos virtuales, y el control de la OpenVPN usando una interfaz GUI en Windows o en Mac OS X.

3.6.4.2 Ventajas de OpenVpn.

- OpenVPN las principales virtudes que incluye es la multiplataforma llevándola a través de la mayor parte del universo que la computación ha conocido, excelente estabilidad, escalabilidad hacia cientos de miles de clientes, relativamente de instalación fácil, y de ayuda para las direcciones dinámicas de IP y NAT.
- OpenVPN proporciona un marco ampliable de VPN el cual ha sido diseñado para su fácil adaptación de un sitio especifico, por ejemplo el abastecimiento de la capacidad para distribuir un paquete modificado de requisitos particulares en la instalación a los clientes, o los métodos alternativos de soporte de la autentificación vía OpenVPN con un modulo.
- OpenVPN ofrece un interfaz de manejo la cual puede ser utilizada remotamente o manejada centralmente el uso de demonio de OpenVPN. El manejo de la interfase puede ser también utilizada para el desarrollo de una interfaz GUI o Una aplicación Web de principio y fin desarrollada para OpenVPN.
- En Windows, OpenVPN puede leer certificados y llaves primarias desde tarjetas inteligentes el cual es soportado desde una API cifrada en Windows.

- OpenVPN usa un modelo de seguridad diseñado para proteger contra ataques pasivos y activos. El modelo de la seguridad de OpenVPN se basa en usar SSL/TLS para la autentificación de la sesión y el protocolo de IPSec para asegurar el transporte del túnel sobre el UDP. OpenVPN soporta el X509 PKI (Llave de Infraestructura pública) para la autentificación de la sesión, El protocolo TLS para intercambio de llaves, El OpenSSL cifra- independientemente de la interfase EVP para los datos del túnel que cifran, y el algoritmo HMAC-SHA1 para los datos de autenticidad del túnel.
- OpenVPN corre para Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X, y Windows 2000/XP. Porque OpenVPN se escribe como espacio-usuario un demonio en vez de un módulo de kernel como una modificación compleja a la capa del IP.
- OpenVPN es fácil de utilizarse. En general, un túnel puede ser creado y configurado con un solo comando (y sin ningún archivo requerido en la configuración).
- OpenVPN ha sido rigurosamente diseñado y probado para operar en un ambiente robusto y en redes no confiables. Una de las metas más importantes en el diseño de una OpenVPN debería de ser sensible, en términos de operación normal y de recuperación de errores, como la capa subyacente del IP haciendo un túnel por encima. Eso significa que la Capa de IP deja de funcionar por 5 minutos, Cuando regresa, el tráfico del túnel se reanudara inmediatamente aunque la interrupción que interfirió con un intercambio dinámico de llave que fue programado durante ese tiempo.
- OpenVPN ha sido desarrollado con un poderoso diseño modular. Todo el cifrado es dirigido por la biblioteca de OpenSSL, y toda la funcionalidad de los túneles del IP se proporciona a través del adaptador virtual de la red TUN[9]/TAP[10].

[9] TUN es un dispositivo Punto a Punto virtual y trabaja con tramas IP.
[10] TAP es un dispositivo Ethernet virtual y trabaja con tramas Ethernet.

- Los beneficios de la modularidad se pueden ver en la manera que OpenVPN puede ser dinámicamente ligado con la nueva versión de librería de OpenSSL Y tener inmediatamente acceso a cualquier funcionalidad proporcionada por la nueva versión. Cuando OpenVPN se construye con la ultima versión de OpenSSL (0.9.7), Donde automáticamente tiene el acceso a nuevos cifras tales como AES-256 (Estándar Avanzado de Cifrado llave de 256 bits) y la capacidad del motor de cifrado de OpenSSL que permite la utilización para un propósito especial de los aceleradores de hardware para optimizar el cifrado, descifrado, y el rendimiento de la autentificación.

De la misma forma, OpenVPN trabaja en el espacio-Usuario diseñado, permite llegar directo a cualquier sistema operativo que incluya Adaptador de Red virtual TUN/TAP.

OpenVPN es rápido. Corriendo Redhat 7.2 en una maquina Pentium II 266mhz, Usando TLS-based en la sesión de autentificación, El cifrado de bloques **Blowfish**, la Autentificación **SHA1** de datos por túnel, y haciendo un túnel una sesión del ftp larga, archivos precomprimidos, OpenVPN archiva envía y recibe una transferencia de 1.455 megabytes por segundo tiempo de CPU (combinado el tiempo de usuario y kernel).

Mientras, OpenVPN proporciona varias opciones para controlar los parámetros de la seguridad del túnel de la VPN , También proporciona opciones para proteger la seguridad en el mismo Server , tal como **-- chroot** para restringir los archivos de sistema que el demonio tiene acceso en la OpenVPN , **--user** y **--group** para quitar los privilegios del demonio después de la inicialización, y **--mlock** para asegurarse que el material clave y los datos de el túnel nunca se pagina al disco donde puede ser que sea recuperado más adelante.

TLS es la última evolución de la familia de protocolos de SSL desarrollados originalmente por Netscape para la seguridad de sus navegadores. Los predecesores de TLS y SSL han sido extensamente difundidos por varios años para su uso por Internet y han sido extensivamente analizados para buscar sus debilidades. Alternadamente, este análisis ha conducido a una consolidación subsiguiente del protocolo, ya que hoy, SSL/TLS está considerado como uno de los protocolos mas seguros y fuertes que se puedan encontrar. Como tal, creemos que TLS es una opción excelente para el mecanismo de la autentificación y del intercambio de la llave de un producto de VPN.

Hay tres familias importantes de VPN que hoy en día se utilizan ampliamente: SSL, IPSec, y PPTP. OpenVPN es una SSL VPN y como tal no es compatible con IPSec, L2TP, o PPTP.

El protocolo IPSec esta diseñado para ser implementado como una modificación de IP ampliado en el espacio del kernel, por lo tanto cada sistema operativo requiere su propia puesta en práctica independientemente de IPSec.

Por el contrario, la puesta en práctica del usuario-espacio de OpenVPN permite la compatibilidad a través de sistemas operativos y arquitecturas de procesadores, la operación amistosa del funcionamiento Firewall y NAT-, Soporte de direcciones dinámicas, y soporte de múltiples protocolos incluyendo el protocolo de puenteo.

Hay ventajas y desventajas en los dos acercamientos. La principal ventaja de OpenVPN son la compatibilidad, fácil configuración, y compatibilidad con las direcciones dinámicas de NAT. La curva de aprendizaje para la instalación y uso de una OpenVPN está en parte relacionado con el otro software seguridad del demonio tal como SSH.

OpenVPN es compatible con cerificados de SSL/TLS, RSA y X509 PKI, NAT, DHCP, y TUN/TAP y dispositivos virtuales.

OpenVPN no es compatible con IPSec, IKE, PPTP, o L2TP.

3.6.4.3 Instalación y configuración de OpenVPN.

La instalación del paquete OpenVPN lo hemos de instalar tanto al cliente como en el servidor.

Debemos asegurarnos que tenemos el controlador tun/tap instalado en el kernel, aunque si tenemos un kernel 2.4.27 o superior, casi seguro que lo tenemos, pero vamos a comprobar si estamos en lo cierto con el comando modprobe -l | grep 'tun/tap' o con lsmod.

- Fichero de configuración del servidor.

Está en /etc/openvpn y lo hemos llamado tunel.conf y es así:

```
Vim /etc/openvpn/tunel.conf
status openvpn-status.log
log openvpn.log
verb 6
server 10.0.0.0 255.255.255.0 "esta es la red de IP`s virtuales"
ifconfig-pool-persist ipp.txt
dh /etc/openvpn/dh1024.pem
client-config-dir /etc/openvpn/cld
ca /etc/openvpn/keys/mi-ca.crt
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key
dev tun
comp-lzo
port 50000
ifconfig 10.0.0.10 10.0.0.83
route 10.0.0.1 255.255.255.0 "red del servidor"
push "route 10.0.0.5 255.255.255.0″ "red del cliente"
```

- Instalación de openssl para generar certificados.

apt-get install openssl

Nuestro fichero quedo de la siguiente manera:

```
HOME = .
RANDFILE = $ENV::HOME/.rnd
oid_section = new_oids

 [ca]
default_ca = CA_default # The default ca section

 [CA_default]
dir = ./demoCA # Where everything is kept
certs = $dir/certs # Where the issued certs are kept
crl_dir = $dir/crl # Where the issued crl are kept
database = $dir/index.txt # database index file.
new_certs_dir = $dir/newcerts # default place for new certs.
certificate = $dir/cacert.pem # The CA certificate
serial = $dir/serial # The current serial number
crl = $dir/crl.pem # The current CRL
private_key = $dir/private/cakey.pem# The private key
RANDFILE = $dir/private/.rand # private random number file
x509_extensions = usr_cert # The extentions to add to the cert
name_opt = ca_default # Subject Name options
cert_opt = ca_default # Certificate field options
default_days = 3650 # duracion para 10 años
default_crl_days= 30 # how long before next CRL
default_md = md5 # which md to use.
preserve = no # keep passed DN ordering
# For the CA policy
[ policy_match ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
[ policy_anything ]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
```

```
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
 [ req ]
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
x509_extensions = v3_ca # The extentions to add to the self signed cert
string_mask = nombstr
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = ES #pais
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = LasPalmas #Provincia
localityName = Locality Name (eg, city)
localityName_default = GALDAR #Localidad
0.organizationName = Organization Name (eg, company)
0.organizationName_default = Excmo. CentroTecnologico #nombre de tu
organizacion
organizationalUnitName = Organizational Unit Name (eg, section)
#organizationalUnitName_default = Dpto. NNTT #nombre de la unidad
organizativa
commonName = Common Name (eg, YOUR name)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 64
emailAddress_default = tu email
[ req_attributes ]
challengePassword = A challenge password
challengePassword_min = 4
challengePassword_max = 20
unstructuredName = An optional company name
[ usr_cert ]
basicConstraints=CA:FALSE
# This is OK for an SSL server.
# nsCertType = server
nsComment = “OpenSSL Generated Certificate”
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
[ v3_req ]
```

```
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
[ v3_ca ]
# Extensions for a typical CA
# PKIX recommendation.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = CA:true
[ crl_ext ]
authorityKeyIdentifier=keyid:always,issuer:always
```

Con esto ya inicia la función del fichero de configuración

Bien, ahora con un script que se colocara como ct aragon vamos a generar todos los certificados.

```
#!/bin/sh
# Para asegurarnos que partimos de un directorio “Limpio”
d=./keys
if test $d; then
rm -rf $d
fi
mkdir $d
chmod go-rwx $d
touch $d/index.txt
echo “01″ > $d/serial
# Generar Certificado de Entidad Certificadora (CA)
openssl req -nodes -new -x509 -keyout mi-ca.key -out mi-ca.crt -days 3650
echo “Generado Certificado (CA)”
chmod 0600 mi-ca.key
# Generar Certificado del Servidor (server)
echo “A Generar Certificado del Servidor”
openssl req -nodes -new -keyout server.key -out server.csr
echo “Certificado del Servidor generado”
chmod 0600 server.key
# Firmar Certificado del Servidor
echo “Firmando el Certificado del Servidor”
openssl ca -out server.crt -in server.csr -outdir $d -cert mi-ca.crt -keyfile mi-ca.key -
config mi-openssl.cnf
# Generar Certificado del primer cliente (client1)
echo “A Generar certificado del primer cliente”
openssl req -nodes -new -keyout client.key -out client.csr
echo “Certificado del Primer Cliente generado”
chmod 0600 client.key
```

```
# Firmar Certificado del primer cliente
echo “Firmando el Certificado del Primer Cliente”
openssl ca -out client.crt -in client.csr -outdir $d -cert mi-ca.crt -keyfile mi-ca.key -
config mi-openssl.cnf
# Er’ fichero Diffie Hellman
echo “Creando fichero Diffie Hellman”
openssl dhparam -out dh1024.pem 1024
echo “Fichero DH Generado.”
chmod 0600 dh1024.pem
# Coloca los ficheros dentro del directorio $d
echo “Reubicando los archivos en $d”
mv mi-ca.* $d
mv server.* $d
mv client.* $d
mv dh1024.* $d
```

Con esto ya tenemos todos los certificados hechos, tanto para el cliente como para el servidor.

- El cliente.

Hemos de instalar como se menciono anteriormente el paquete openvpn y también el paquete openssl.

El fichero de configuración del cliente también se llamara tunel.conf y su localización es la misma que la del servidor.

```
Vim /etc/openvpn/tunel.conf
client
remote 192.168.111.2”ip publica del server”
ca /etc/openvpn/keys/mi-ca.crt
cert /etc/openvpn/keys/client.crt
key /etc/openvpn/keys/client.key
dev tun
comp-lzo
user nobody
group nogroup
port 50000
```

Por último y para terminar lo que es la parte de configuración hemos de copiar en el directorio /etc/openvpn/keys/ del cliente los certificados generados anterior mente con el script de ct aragon, concretamente hemos de pasarle los siguientes:

mi-ca.crt, client.key y el client.crt

Ahora solo nos queda arrancar la VPN, pero si queremos que se arranque siempre que encendamos la maquina vamos a hacer un pequeño script, que pondremos en el arranque.

ArrancandoVpn.sh
#!/bin/sh
openvpn –daemon –verb 0 –config
/etc/openvpn/tunel.conf
#fin del script

Ahora le damos permisos de ejecucion chmod 755 ArrancandoVpn.sh y lo metemos en el arranque con update-rc.d ArrancandoVpn.sh defaults , esto lo que hará será ponerlo en cada uno de los rc´s.

Bien solo nos queda arrancar la VPN y lo podemos hacer de dos formas:

a)openvpn –verb 6 –config /etc/openvpn/tunel.conf
b)/etc/init.d/openvpn restart.

3.7 SSH y las VPN en Linux.

Estas tres familias de protocolos (SSH: Secure Shell. SSL: Secure Socket Layer. TLS: Transport Layer Security) funcionan con el mismo principio básico que las Redes Privadas Virtuales: El primer intercambio de información entre cliente y servidor es el envío de las llaves públicas de ambos. De esta manera, se puede entablar una sesión con comunicación segura. Acto seguido, una de las partes (o entre ambas) crean aleatoriamente una llave secreta, que será utilizada únicamente durante la sesión en cuestión, y será descartada inmediatamente al

terminar ésta. De ahí en adelante, la sesión se maneja cifrándola únicamente con un algoritmo de llave simétrica.

SSH es principalmente utilizado para el acceso remoto a computadoras **Unix**, aunque también es utilizado para realizar transferencias de archivos.

SSL es una *envoltura* que se puede aplicar a prácticamente cualquier protocolo TCP, encargándose de mantener una comunicación segura entre dos hosts sin importarle qué tipo de datos está enviando. Las versiones seguras de http, pop3, imap, smtp y otros varios servicios viajan sobre túneles SSL.

TLS busca integrar un esquema tipo SSL al sistema operativo - SSL hace únicamente túneles, redireccionando la entrada y salida procesadas de un puerto seguro a un puerto inseguro. TLS busca hacer esto a nivel de la capa TCP/IP, para que este tuneleo sea realmente transparente a las aplicaciones.

SSH (*Secure Shell*) es un programa de login remoto que permite una transmisión segura de cualquier tipo de datos: passwords, sesión de login, ficheros, sesión X remota, comandos de administración, etc. Su seguridad estriba en el uso de criptografía fuerte de manera que toda la comunicación es cifrada y autentificada de forma transparente para el usuario. Es un claro y sencillo sustituto de los típicos comandos "r" de BSD (rlogin, rsh, rcp), telnet, ftp e incluso de cualquier conexión TCP.

Entre las mejoras que se pueden apreciar en el uso de SSH se encuentra una autenticación más robusta de usuarios y hosts, que la tradicionalmente ofrecida basada en direcciones IP y nombres de máquinas. Una privacidad mayor para el usuario debido al uso de canales de encriptación.

Así, el ssh establece un entorno protegido contra ataques típicos como: Ip Spoofing, Ip source routing, DNS spoofing, Sniffing, X11 Server Spoofing, etc.

SSH permite autentificar a un usuario utilizando su password Unix ordinario. La única (e importante) diferencia es que el password no viaja nunca en claro por la red. Si utilizamos SSH para sustituir a telnet, rlogin o ftp evitaremos el peligro de que nuestro password sea capturado por posibles "sniffers" en la red.

3.7.1 Ventajas VPN sobre SSH.

Como se mencionaron anteriormente las ventajas de las VPN, ahora se mostraran las ventajas del protocolo SSH y se observara cual de las dos aplicaciones se adecua a nuestras necesidades según el proyecto a implementar en cada caso para una mejor seguridad en nuestra conexión de acceso remoto y la integridad de nuestra información.

Redes Privadas Virtuales (VPN)

- Las VPN se apoyan en Internet como infraestructura
- Bajos costos de mantenimiento y configuración
- Son escalables
- Rápido y sencillo para los usuarios en cuando a manejabilidad
- Conexión de forma segura 128 bits
- Expansión de redes LAN de forma segura vía Internet
- Ingreso a toda la red LAN corporativa
- Seguridad en las direcciones IP
- Optimización del trafico de datos para el cliente

Secure Shell (SSH)

- Trabaja por lo general sobre sistemas Unix, aunque existen aplicaciones para usarse bajo la plataforma Windows de Microsoft
- Proporciona conexión segura entre dos sistemas
- Encriptación altamente segura difícil de descifrar 128 bits
- Utiliza una interfaz grafica X11 lanzada desde el interprete de comandos
- Solo para usuarios avanzados
- Remplaza programas para transferir archivos como ftp y rcp y otras aplicaciones como telnet o rsh
- Utiliza Internet como infraestructura
- Conexión remota cliente-servidor (uno a uno)
- Ssh cifra la sesión de conexión, difícil de obtener contraseñas

3.8 Sistema de administración de usuarios VPN en Linux.

Bajo GNU/Linux, para que los usuarios puedan identificarse en el sistema, deben presentarse (login) mediante un proceso que consta de dos pasos: Introducir el nombre de usuario (login), y una contraseña (password), la cual es su llave personal secreta para entrar en la cuenta.

En los sistemas Unix tradicionales, el administrador del sistema asignará el nombre de usuario y una contraseña inicial en el momento de crear la cuenta de usuario. Además, cada sistema tiene un nombre (hostname) asignado, que le da nombre a la máquina. El nombre del sistema es usado para identificar computadoras en una red, pero incluso aunque la máquina no esté en red, debería tener su nombre.

Una vez que hemos introducido correctamente el nombre de usuario y la contraseña, estamos presentados en el sistema y listo para iniciar una sesión interactiva y comenzar a trabajar, según los derechos de acceso que nos brinde nuestra cuenta.

Existen distintas distribuciones de GNU/Linux, orientadas a distinto tipo de usuarios o de sistemas, con herramientas de administración diferentes, o con distintas políticas.

El control de los *usuarios* y *grupos* es un elemento clave en la administración de sistemas de Linux.

Los *Usuarios* pueden ser gente real, es decir, cuentas ligadas a un usuario físico en particular o cuentas que existen para ser usadas por aplicaciones específicas.

Los *Grupos* son expresiones lógicas de organización, reuniendo usuarios para un propósito común. Los usuarios dentro de un mismo grupo pueden leer, escribir o ejecutar archivos que pertenecen a ese grupo.

Cada usuario y grupo tiene un número de identificación único llamado *identificador de usuario* (*UID*) y un *identificador de grupo* (*GID*) respectivamente.

Una de las tareas más importantes de cualquier administrador del sistema, es la de administrar adecuadamente usuarios y grupos, así como asignar y revocar permisos.

La razón principal para las cuentas de usuario es verificar la identidad de cada individuo utilizando un computador. Una razón secundaria (pero aún importante) es la de permitir la utilización personalizada de recursos y privilegios de acceso.

Los recursos incluyen archivos, directorios y dispositivos. El control de acceso a estos dispositivos forma una gran parte de la rutina diaria de un administrador de sistemas; a menudo el acceso a un recurso es controlado por grupos. Los grupos son construcciones lógicas que se pueden utilizar para enlazar a usuarios para un propósito común. Por ejemplo, si una organización tiene varios administradores de sistemas, todos ellos se pueden colocar en un grupo administrador de sistema.

Luego se le pueden dar permisos al grupo para acceder a recursos claves del sistema. De esta forma, los grupos pueden ser una herramienta poderosa para la administración de recursos y acceso.

3.9 Seguridad Blowfish.

En criptografía, Blowfish es un codificador de bloques simétricos, diseñado en 1993 e incluido en un gran número de conjuntos de codificadores y productos de cifrado.

Blowfish se diseño como un algoritmo de uso general, intentando reemplazar al antiguo DES y libre de problemas asociados con otros algoritmos. Al mismo tiempo, muchos otros diseños eran propietarios, patentados o los guardaba el gobierno. Su creador Schneier declaro “Blowfish no tiene patente, y así se quedará en los demás continentes. El algoritmo está a disposición de dominio público, y puede ser usado libremente por cualquiera”.

El Algoritmo.

Blowfish usa bloques de 64 bits y llaves que van desde los 32 bits hasta 448 bits. Es un codificador de 16 rondas Feistel y usa llaves que dependen de las Cajas-S. Tiene una estructura similar a CAST-128, el cual usa Cajas-S fijas.

El diagrama de la figura 3.3 muestra la acción de Blowfish. Cada línea representa 32 bits. El algoritmo guarda 2 arreglos de subllaves: El arreglo P de 18 entradas y 4 cajas-S de 256 entradas. Una entrada del arreglo P es usada cada ronda, después de la ronda final, a cada mitad del bloque de datos se le aplica un XOR con uno de las 2 entradas del arreglo P que no han sido utilizadas.

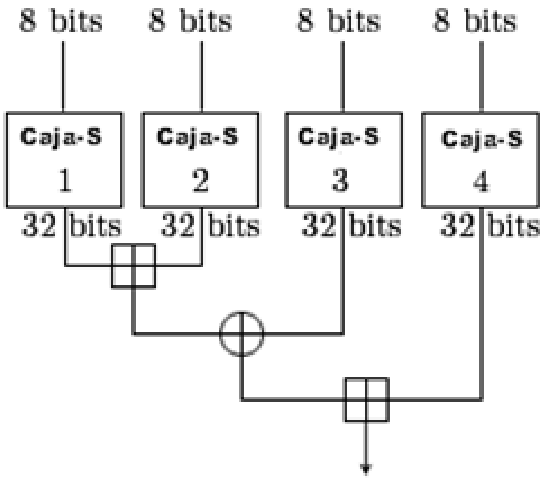


Figura 3.3 Algoritmo y funcionamiento de Blowfish.

La función divide las entradas de 32 bits en 4 bloques de 8 bits, y usa los bloques como entradas para las cajas-S. Las salidas deben estar en módulo 2^{32} y se les aplica un XOR para producir la salida final de 32 bits.

Debido a que Blowfish esta en la red Feistel, puede ser invertido aplicando un XOR entre P_{17} y P_{18} al bloque texto codificado, y así sucesivamente se usan las P-entradas en orden reversivo.

La generación de llaves comienza inicializando los P-arreglos y las cajas-S con los valores derivados de los dígitos hexadecimales de pi, los cuales no contienen patrones obvios. A la llave secreta se le aplica un XOR con las P-entradas en orden (ciclando la llave si es necesario). Un bloque de 64 bits de puros ceros es

cifrado con el algoritmo como se indica. El texto codificado resultante reemplaza a P_1 y P_2. Entonces el texto codificado es cifrado de nuevo con la nuevas subllaves, P_3 y P_4 son reemplazados por el nuevo texto codificado.

Esto continúa, reemplazando todas las entradas del P-arreglo y todas las entradas de las cajas-S. En total, el algoritmo de cifrado Blowfish correrá 521 veces para generar todas las subllaves, cerca de 4KB de datos son procesados.

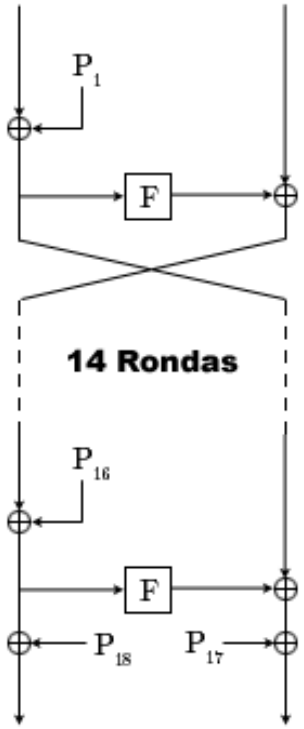


Figura 3.4 Diagrama para la creación de llaves de seguridad en el Algoritmo Blowfish.

A comparación de las VPN en el sistema operativo Windows NT, esta otra alternativa en el sistema operativo GNU/Linux es una opción más de estudio que realizamos para poder tomar en cuenta las opciones de seguridad y fiabilidad para un análisis de lo que será la implementación y desarrollo de nuestro problema. Como se verá en el capítulo siguiente, tomando en cuenta los capítulos anteriores se manejaran todos los conceptos y procesos de las VPN para continuar con nuestro proyecto y manejar la mejor opción a implementar en el Laboratorio de Cómputo.

CAPÍTULO IV

IMPLEMENTACIÓN DE UN AMBIENTE VIRTUAL REMOTO DE TRABAJO (VPN) PARA EL LABORATORIO DE CÓMPUTO DEL CENTRO TECNOLÓGICO ARAGÓN.

- Implementar conforme a los requerimientos solicitados en el Laboratorio de Cómputo la mejor plataforma en sistema operativo y VPN, que ayude a cubrir las necesidades de acceso remoto a la red LAN para sus aplicaciones y proyectos que ahí se realizan.

En la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México se encuentra ubicado el Centro Tecnológico, en donde se realizan proyectos de investigación para la Universidad, Empresas Privadas y Públicas, con lo cual se abre la posibilidad a la extensión universitaria para desarrollarse en el ámbito laboral y profesional, en dicho Centro se encuentra el Laboratorio de Computo área de desarrollo de proyectos informáticos y de sistemas.

4.1 Planteamiento del Problema.

El laboratorio de cómputo cuenta con información de suma relevancia ya que ahí se desarrollan proyectos de gran nivel, en la cual se maneja información con datos reales por ejemplo: los datos del programa de verificación vehicular proyecto elaborado para la Secretaría del Medio Ambiente del Estado de México y en el cual se contemplan datos reales para las pruebas de dicho proyecto y que deben ser resguardados por la seguridad informática que hoy en día existe, como por ejemplo: Firewall, Sistemas Integrales de antivirus, Antispyware, Sistemas de seguridad en Hardware, etc. Y muy principalmente se requiere que esa información sea totalmente segura cuando es transmitida a través de la red Internet, siendo éste un medio de bajo costo que requiere ser utilizado para dicha transmisión de datos, por lo cual la preocupación en la integridad de esta información al viajar por Internet debe de ser la más segura.

Para cubrir esta necesidad se requiere de una infraestructura adicional que sirva como apoyo a sus proyectos de trabajo e investigación desde otros lugares de trabajo físicos, geográficamente hablando, y que le den continuidad, seguridad e integridad a la información con la que se trabaja, todo esto aprovechando la tecnología que hoy existe, como lo es la red de Internet, y los sistemas operativos que hoy en día cuentan con herramientas importantes para la creación de enlaces remotos y conectividad de redes para su ampliación.

Tomando en cuenta la investigación de las Redes Privadas Virtuales por su bajo costo confiabilidad, integridad e implementación en los Sistemas Operativos desarrollaremos el proyecto en el Laboratorio de Cómputo para analizar su funcionamiento, además de la seguridad que va a manejarse para el usuario y su acceso remoto a una red geográficamente ubicada en otro sitio se implementara dicho proyecto para su evaluación.

4.2 Puntos a considerar para la creación de la VPN.

1. Seguridad en los datos
2. Confiabilidad en la transmisión de los mismos.
3. Autentificación, seguridad y permisos de los usuarios.
4. Tiempos de conexión a la red.
5. Velocidad en la Transmisión de los datos.
6. Costos de Infraestructura.
7. Administración de la VPN en la Red LAN.
8. Compartir Carpetas, Impresoras y recursos generales de la Red de forma segura.
9. Crecimiento a futuro de nuestra red LAN.

En este capítulo implementaremos el funcionamiento de las VPN en el sistema operativo Windows 2000 Server y GNU/Linux. Para esto se utilizará todo lo visto en los capítulos anteriores sobre las Redes Privadas Virtuales y se manejaran las etapas de configuración de servidor y cliente en ambos sistemas operativos. En los módulos de configuración de Linux se manejará la configuración del servidor OpenVPN y como cliente la aplicación PPTPClient, la información está brevemente detallada ya que la implementación de una VPN en Linux en sus diferentes distribuciones van cambiando por el desarrollo que se tiene de este proyecto en esta plataforma en forma constante.

4.3 Estructura de la red interna.

Para la creación de la Red Privada Virtual en el Laboratorio de Cómputo del Centro Tecnológico Aragón, se presenta lo siguiente:

- La infraestructura de la red se compone de aproximadamente 14 máquinas con tecnología de Red LAN Fast Ethernet 10/100 Mbps.
- Los sistemas operativos son variados, ya que es un área donde se investiga todo lo relacionado a la Ingeniería en Computación.
- Cuenta con conexión a Internet a través de la infraestructura de Red de la Universidad Nacional Autónoma de México.
- La conexión principal a la red LAN será a través de un sistema operativo de la tecnología NT y GNU/Linux.

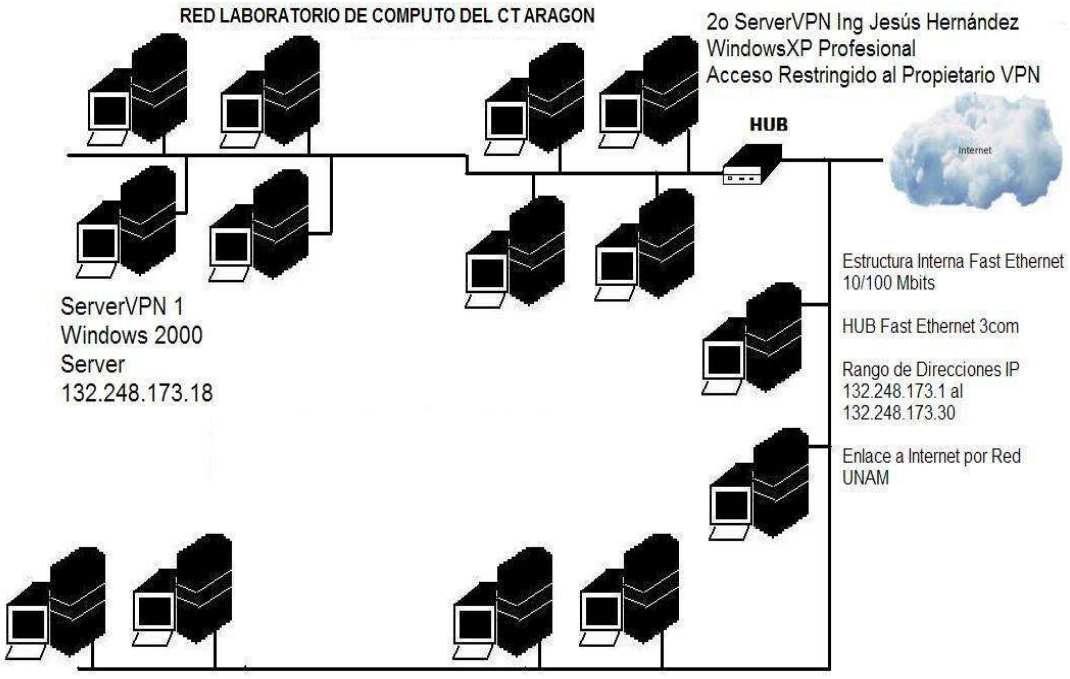


Figura 4.1 Diagrama de la Red del Laboratorio de Cómputo del CT Aragón.

4.4 Implementación de una VPN en el ambiente Windows NT 2000.

Especificaciones del Servidor en Windows NT 2000.
El equipo o nodo asignado para la configuración de nuestro servidor VPN cuenta con las siguientes características:

- Equipo de Computo Personal (PC) con Procesador Intel P4 2.8 Ghz.
- Capacidad en Memoria Ram 256 MB.
- Disco Duro con capacidad de 80 GB.
- Tarjeta de Red Fast Ethernet 10/100 Mbits Intel.
- Sistema Operativo Microsoft Windows NT 2000 Server.

4.4.1 Configuración del Servidor VPN en Windows NT.

El adaptador de red utilizado para conectar al segmento de la intranet (Tarjeta de Red) y el adaptador HUB utilizado para conectar a Internet se han instalado de acuerdo con las instrucciones del fabricante. Una vez que se han instalado los controladores y están en funcionamiento, ambos adaptadores aparecen como conexiones de área local en la carpeta Conexiones de red y de acceso telefónico. Ver figura 4.2. Conexiones de red.

Figura 4.2 Conexiones de red.

La configuración del equipo inicia desde el nombre de nuestro servidor y la configuración del grupo de trabajo para este caso será asignado de la siguiente manera:

En mi PC ingresamos a las propiedades del sistema y colocaremos la información solicitada para la identificación de nuestro equipo en la red. Fig. 4.3.

- Descripción de equipo: ServerVPN.
- Nombre completo del equipo: UNAMVPN.
- Grupo de Trabajo: CT ARAGON

Figura 4.3 Identificación del equipo en la red.

4.4.2 Configurar TCP/IP en los adaptadores LAN.

Continuamos con la configuración de nuestra Tarjeta de Red y la dirección IP asignada a este servidor al igual que los protocolos adicionales y servicios para que nuestro equipo sea compatible con nuestra red principal y tengamos los recursos necesarios para trabajar, quedando de la siguiente manera:

- Tarjeta de Red Intel Fast Ethernet 10/100 Mbps.
- Dirección IP **10.0.0.1**
- Protocolo TCP/IP.
- Compartir impresoras y archivos para redes Microsoft.
- Programador de Paquetes QoS.
- Clientes para redes Microsoft.

Esta información queda registrada como se muestra en la figura 4.4 de las Propiedades de Conexión de Red.

Figura 4.4 Configuración TCP/IP y componentes adicionales de la Red.

Si nuestra red principal contará con la configuración del protocolo IPX/SPX/NetBEUI, éste se seleccionará en la configuración de servicios y propiedades de conexiones entrantes y así poder transferir archivos compatibles con este protocolo.

4.4.3 Instalar el Servicio de enrutamiento y acceso remoto.

Se ejecuta el Asistente para configuración de enrutamiento y acceso remoto. En el asistente, se ha habilita el enrutamiento LAN y WAN, se habilitan todos los puertos para enrutamiento y acceso remoto, y se ha habilitado el cifrado IPSec en las conexiones L2TP.

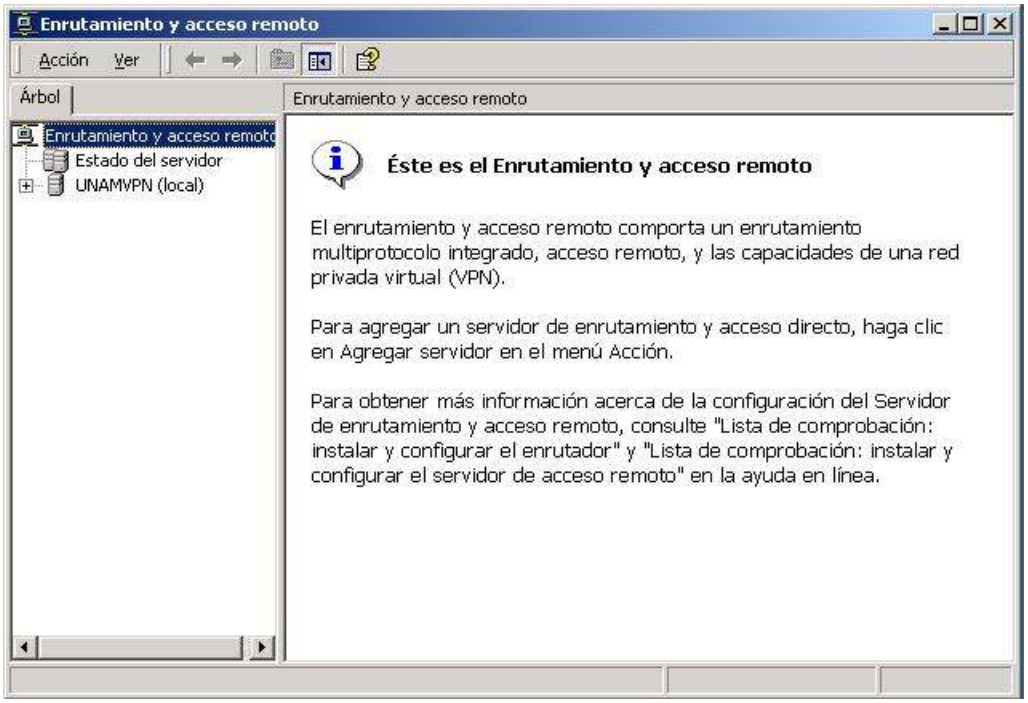


Figura 4.5 Asistente de configuración de enrutamiento y acceso remoto.

En el asistente, como se muestra en la figura 4.5, se ha configurado un grupo de direcciones IP estáticas con la dirección IP inicial **10.0.0.1** y la dirección IP final **10.0.0.30** Así se crea un grupo de direcciones estáticas para 29 clientes VPN.

De forma predeterminada, sólo hay cinco puertos L2TP y cinco puertos PPTP habilitados para conexiones VPN en la configuración de acceso remoto, pero se puede aumentar dependiendo los requerimientos del Laboratorio de Computo. Ver figura 4.6. Puertos VPN, PPTP y L2TP.

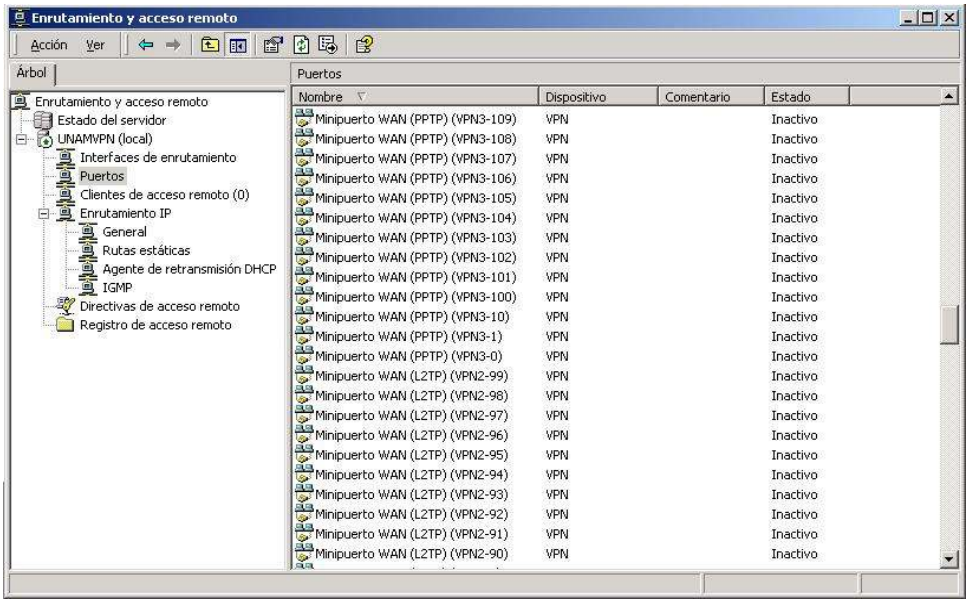


Figura 4.6 Puertos habilitados VPN (PPTP Y L2TP).

La configuración de nuestro servidor VPN se realizará como se indicó en el capítulo 2, creando la CONEXIÓN ENTRANTE que permitirá el acceso a nuestros usuarios. La figura 4.7 muestra la conexión entrante realizada.

Figura 4.7 Conexión Entrante como Acceso al servidor VPN.

4.4.4 Administración de usuarios y control de acceso.

Para facilitar la transición desde un entorno Windows, la administración de la red del Laboratorio de Cómputo decide implementar un modelo administrativo de acceso por usuario para un mejor control. El acceso remoto se controla mediante la configuración de los permisos de marcado de las cuentas de usuario individuales como **Permitir acceso** o **Denegar acceso**. Se utilizan directivas de acceso remoto para aplicar diferentes configuraciones de conexión VPN basadas en la pertenencia a grupos y se ha eliminado la directiva predeterminada de acceso remoto **Permitir el acceso si está habilitado el permiso de acceso telefónico**.

La administración de los usuarios se realizará a través de las herramientas de administración de Windows 2000 Server en la cual se asignará un grupo de trabajo o perfil y cada usuario tendrá asignado los permisos necesarios y requeridos para el acceso a nuestra red y maneja la mayor seguridad sin quitarles privilegios para el uso compartido de las carpetas y servicios que la red pueda ofrecer.

Active Directory es el servicio de directorio utilizado en Windows 2000 Server y constituye el fundamento de las redes distribuidas de Windows 2000.

Las cuentas de usuario y de equipo de Active Directory representan una entidad física como una persona o un equipo. Las cuentas de usuario y de equipo (así como los grupos) se denominan principales de seguridad. Los principales de seguridad son objetos de directorio a los que se asignan automáticamente identificadores de seguridad. Los objetos con identificadores de seguridad pueden iniciar sesiones en la red y tener acceso a los recursos del dominio. Una cuenta de usuario o de equipo se utiliza para:

- Autenticar la identidad del usuario o equipo.
- Autorizar o denegar el acceso a los recursos del dominio.
- Administrar otros principales de seguridad.
- Auditar las acciones realizadas con la cuenta de usuario o de equipo.

4.4.5 Configuración de la conexión de Red Privada Virtual cliente.

Al iniciar nuestra conexión de acceso a la VPN como cliente, lo primero que tenemos que definir es la conexión al servicio ISP que nos proporcione acceso a la red pública de Internet, obviamente de la manera más económica con llamada local o con un servicio disponible localmente en la zona, puede ser este a través de una conexión Dial Up o a través de ADSL, en este caso la zona nos ofrece un servicio de la Compañía Telmex (Teléfonos de México) en las dos modalidades antes mencionadas.

El establecer esta comunicación sirve como anteriormente se mencionó en este proyecto para utilizar la infraestructura pública de Internet como medio de comunicación a nuestra red LAN de trabajo, manejando la seguridad por medio de los túneles que se inician una vez realizando la conexión de nuestra VPN como cliente.

Por tal motivo iniciaremos configurando nuestra conexión a nuestro ISP local de la siguiente manera en la modalidad Dial Up:

- Abra Conexiones de red y de acceso telefónico. Haga doble clic en **Realizar conexión nueva** y, a continuación, haga clic en **Siguiente**.
- Haga clic en **Conectarse a Internet**, a continuación, haga clic en **Siguiente**.
- Haga clic en **Conectar usando un MODEM de acceso telefónico**, a continuación, haga clic en **Siguiente**.
- Se ingresa el Nombre del ISP en este caso **Telmex,** a continuación, haga clic en **Siguiente**.
- Ingresamos el número de teléfono local, **53289928,** a continuación, haga clic en **Siguiente**.
- Ingresamos nuestro Nombre de usuario y Contraseña asignados por nuestro ISP Telmex para tener acceso a la red Internet y finalizamos nuestra conexión de acceso telefónico Telmex.

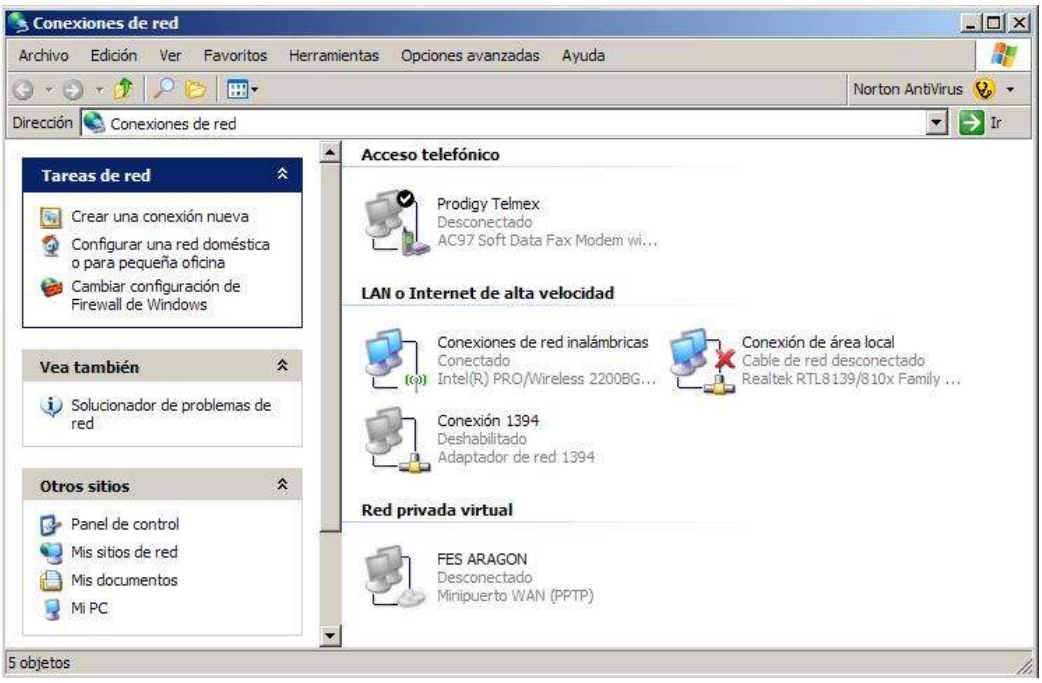


Figura 4.8 Configuración del acceso a Internet Telmex.

Como se menciono en el capitulo 2 la configuración del cliente VPN en Windows XP o Windows 2000 Profesional será de la siguiente manera:

1. Abra Conexiones de red y de acceso telefónico
2. Haga doble clic en **Realizar conexión nueva** y, a continuación, haga clic en **Siguiente**.
3. Haga clic en **Conectar a una red privada a través de Internet**, a continuación, haga clic en **Siguiente**.
4. Si ya ha establecido una conexión de acceso telefónico, se realizara la siguiente acción:

    - Se establecerá una conexión con el ISP o con otra red antes de establecer el túnel con el equipo o red de destino, para eso hacemos clic en **Usar automáticamente esta conexión inicial**, en una de las conexiones de la lista y, después, en **Siguiente**.

5. Escriba el nombre de host o la dirección IP del equipo o la red con la que va a conectar y, a continuación, haga clic en **Siguiente**.

6. Como este equipo va estar en función de un Cliente VPN no se desea compartir ningún otro acceso o recurso sobre esta conexión por lo cual la casilla de verificación **Habilitar Conexión compartida a Internet para esta conexión** estará deshabilitada y a continuación, haga clic en **Siguiente**.

7. Escriba el nombre de la conexión y, después, haga clic en **Finalizar**.

Esta configuración se puede ver en la figura anterior en la que se muestran las dos conexiones una dial up y la otra de acceso VPN cliente dirigida a FES ARAGON. Esto es todo lo que conlleva la configuración de un cliente VPN, por lo que a continuación pasaremos a realizar las configuraciones de los recursos de la red en el Servidor VPN para que estén disponibles al ingresar nuestros clientes a dicho servidor.

4.4.6 Compartir Recursos en el Servidor VPN.

A través de las conexiones VPN, se pueden compartir carpetas y archivos que ayuden al trabajo remoto y que esta información pueda viajar totalmente seguro por Internet, y este recurso puede ser manejado de la siguiente manera una vez establecida la conexión VPN como se muestra a continuación:

Para cambiar los permisos de una carpeta compartida

1. Abra Carpetas compartidas.
2. En el árbol de la consola, haga clic en **Recursos compartidos**.
3. Haga clic con el botón secundario del *mouse* (ratón) en la carpeta compartida en la que desee establecer permisos y, después, haga clic en **Propiedades**.
4. En la ficha **Seguridad**, haga clic en el nombre del usuario o el grupo cuyos permisos desee cambiar.
5. En **Permisos**, haga clic en **Permitir** o en **Denegar** para cada uno de los permisos.

Consideraciones al compartir carpetas:

- Al asignar permisos suele ser más fácil asignar permisos a grupos y, después, agregar usuarios a los grupos en vez de asignar permisos idénticos a varios usuarios individuales.

- Para este proyecto se crearan dos grupos llamados de la siguiente manera: Becarios y ProyectManager. Estos grupos tendrán sus privilegios para el acceso a la red principal y cada usuario tendrá asignada su propia contraseña que los identificara en la red al autenticarse en el sistema VPN.

- Los permisos para una carpeta compartida sólo están vigentes cuando se tiene acceso a la carpeta a través de la red.

- Los permisos para una carpeta de un volumen NTFS se agregan a los permisos de acceso de NTFS establecidos en la carpeta. Los permisos de carpetas compartidas especifican el máximo acceso permitido a través de la red.

Con Carpetas compartidas, se pueden realizar las tareas siguientes:

- Crear, ver y establecer permisos para recursos compartidos, incluidos los de equipos donde se ejecute Windows NT 4.0.
- Ver una lista de todos los usuarios conectados al equipo a través de una red y desconectar alguno o todos.
- Ver una lista de los archivos abiertos por usuarios remotos y cerrar alguno de ellos o todos.

Carpetas compartidas proporciona información, ordenada en columnas, acerca de todos los recursos compartidos, sesiones y archivos abiertos en el equipo local. Los encabezados de columna se definen a continuación.

Recursos compartidos proporciona la información siguiente acerca de los recursos compartidos disponibles en el equipo:

- Carpeta compartida
- Ruta de acceso compartida
- Tipo
- Nº de sesiones comentario

La figura 4.9 muestra el detallado de la información en el administrador de equipos.

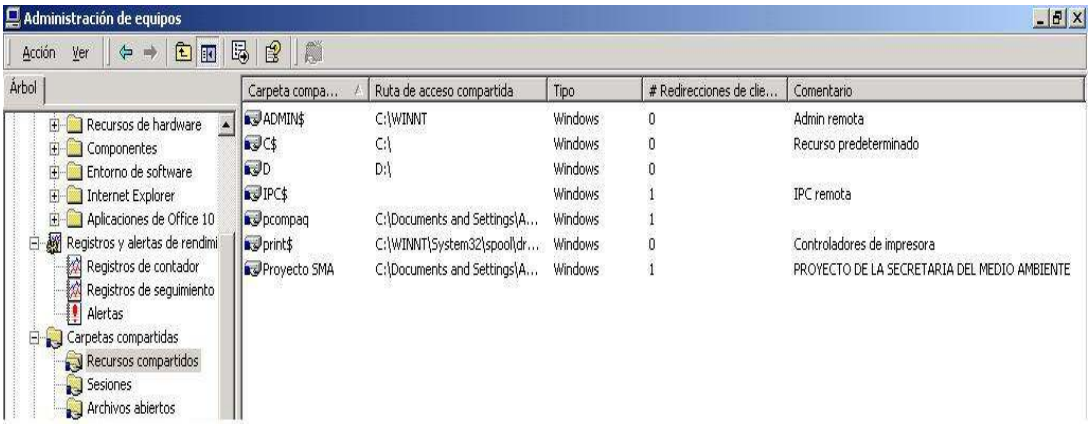


Figura 4.9 Recursos compartidos.

Sesiones proporciona la información siguiente acerca de todos los usuarios de red conectados al equipo:

- Usuario
- Equipo (o PC)
- Tipo
- Archivos abiertos
- Tiempo conectado
- Tiempo de inactividad
- Invitado

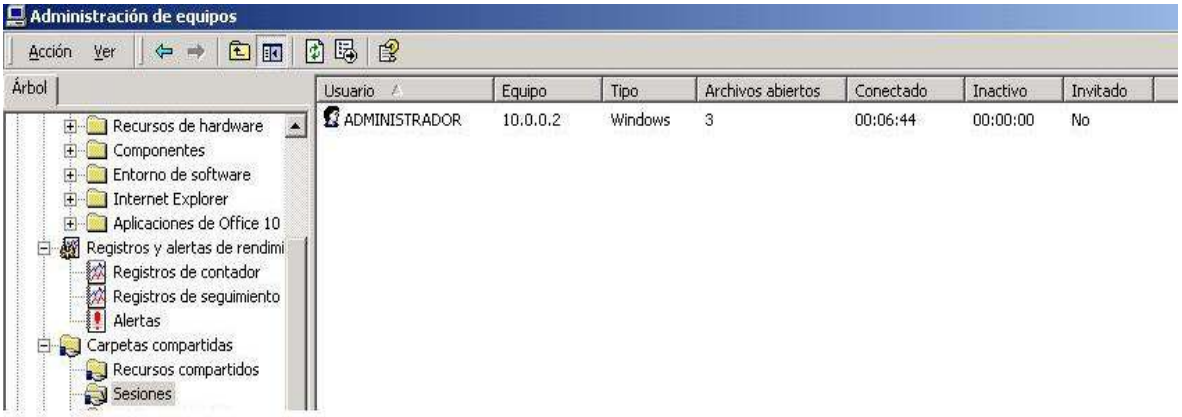


Figura 4.10 Sesiones de los usuarios.

Archivos abiertos proporciona la información siguiente acerca de todos los archivos abiertos en el equipo:

- Archivo abierto
- Abierto por
- Tipo
- Nº de bloqueos
- Modo de apertura

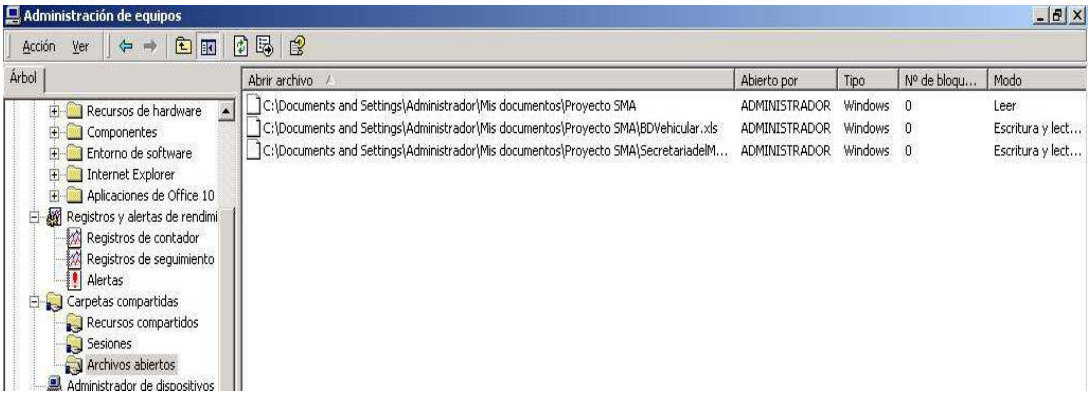


Figura 4.11 Archivos abiertos.

4.4.7 Tipos de permisos de acceso para recursos compartidos

Los siguientes tipos de permisos de acceso se pueden aplicar a las carpetas compartidas.

El permiso de lectura permite:

- Ver los nombres de archivos y subcarpetas.
- Desplazarse por las subcarpetas.
- Ver los datos de los archivos.
- Ejecutar archivos de programa.

El permiso de cambio proporciona todos los permisos de lectura, así como:

- Agregar archivos y subcarpetas.
- Cambiar datos en archivos.
- Eliminar subcarpetas y archivos.

Es el permiso que se aplica de forma predeterminada a los recursos compartidos que se crean. Proporciona todos los permisos de lectura y cambio, así como:

- Cambiar permisos (sólo en archivos y carpetas NTFS).
- Tomar posesión (sólo en archivos y carpetas NTFS).

4.4.8 Compartir la impresora como recurso de Red.

1. Abra Impresoras.
2. Haga clic con el botón secundario del *mouse* (ratón) en la impresora que desee compartir y, después, haga clic en **Compartir**.
3. En la ficha **Compartir**, haga clic en **Compartida como** y, después, escriba un nombre para la impresora compartida.

Si comparte la impresora con usuarios que utilizan diferentes componentes de hardware o sistemas operativos, haga clic en **Controladores adicionales**. Haga clic en el entorno y el sistema operativo para los demás equipos y, después, haga clic en **Aceptar** para instalar los controladores adicionales.

Como se muestra en ese apartado todo lo relacionado a los recursos de la red LAN se pueden compartir a través de una VPN y continuar con esos permisos de acceso a los recursos siempre y cuando el administrador pueda proporcionar dichos recursos a los usuarios permitidos por individual o por grupo, con esto vemos que la flexibilidad del sistema operativo Windows NT en cuanto a trabajo en red se refiere puede ser totalmente confiable y seguro.

4.4.9 Pruebas de conexión.

Aceptar un intento de conexión

Cuando un usuario intenta una conexión, el intento de conexión se acepta o se rechaza en función de la lógica siguiente:

1. Se comprueba la primera directiva de la lista ordenada de directivas de acceso remoto. Si no hay directivas, se rechaza el intento de conexión.
2. Si todas las condiciones de la directiva coinciden con el intento de conexión, se comprueba la configuración del permiso de acceso remoto del usuario que intenta la conexión.
    - Si está activada la directiva **Denegar acceso**, se rechaza el intento de conexión.
    - Si está activada la directiva **Permitir acceso**, se aplican las propiedades de la cuenta de usuario y las propiedades del perfil.

- Si el intento de conexión no coincide con la configuración de las propiedades de la cuenta de usuario y las propiedades del perfil, se rechaza el intento de conexión.
- Si el intento de conexión coincide con la configuración de las propiedades de la cuenta de usuario y las propiedades del perfil, se acepta el intento de conexión.
- Si el permiso de acceso remoto no está establecido en **Permitir acceso** o **Denegar acceso**, el permiso de acceso remoto debe establecerse en **Controlar acceso a través de la directiva de acceso remoto**. Por tanto, debe comprobar la configuración del permiso de acceso remoto de la directiva.
- Si está activada la directiva **Conceder permiso de acceso remoto**, se aplican las propiedades de la cuenta de usuario y las propiedades del perfil.

En la figura 4.12 se muestra a través de un diagrama de flujo el manejo lógico de las directivas de acceso remoto.

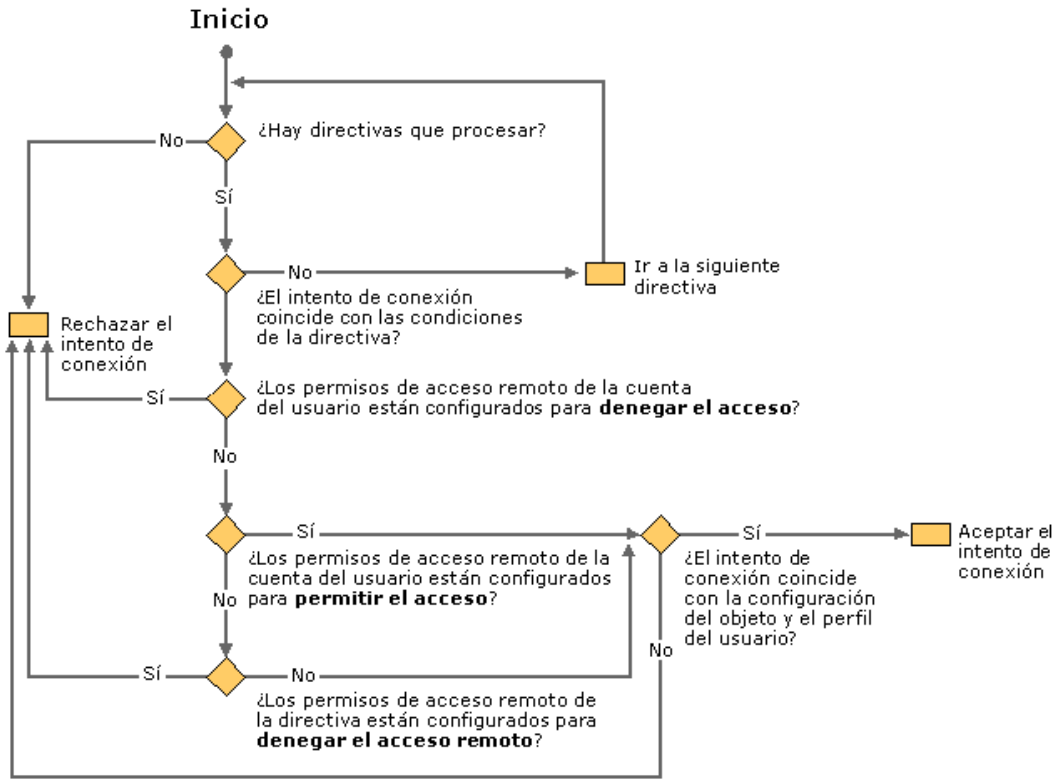


Figura 4.12. La ilustración siguiente muestra la lógica de las directivas de acceso remoto.

4.4.10 Exigir que los clientes VPN utilicen cifrado de alto nivel.

En este caso, el administrador de la red utiliza el modelo administrativo de acceso por usuario. Para los usuarios a los que se permite el acceso remoto, el permiso de acceso remoto está establecido como **Permitir acceso**. Para los usuarios a los que no se permite el acceso remoto, el permiso de acceso remoto está establecido como **Denegar acceso**.

El administrador de la red desea que todos los clientes de Red Privada Virtual (VPN, *Virtual Private Network*) utilicen cifrado de alto nivel. Para las conexiones PPTP, debe utilizarse el cifrado punto a punto de Microsoft (MPPE, *Microsoft Point-to-Point Encryption*) de 128 bits. Para las conexiones L2TP sobre IPSec, debe utilizarse el Estándar de cifrado de datos triple (3DES, *Triple Data*

Encryption Standard). Los clientes de acceso telefónico a redes pueden utilizar la configuración predeterminada para el cifrado. La figura 4.13 muestra el detalle de las propiedades de la conexión VPN y el tipo de autenticación utilizado junto con el protocolo de cifrado de datos.

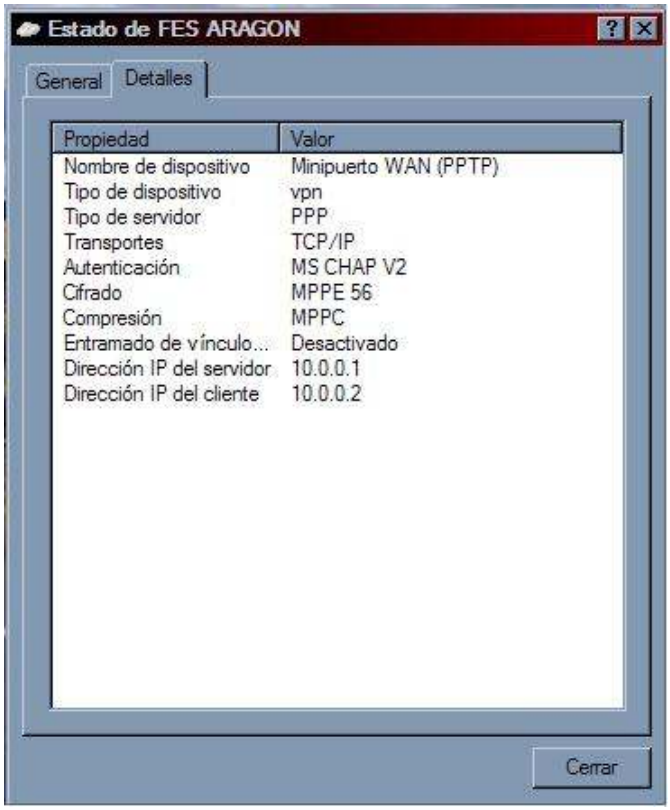


Figura 4.13 Detalles de conexión VPN.

En este caso, se necesitan dos directivas:

- Una directiva que exige que las conexiones VPN utilicen cifrado de alto nivel.
- Una directiva que acepta intentos de conexión de todos los demás usuarios en cualquier momento del día (la directiva predeterminada denominada **Permitir el acceso si está habilitado el permiso de acceso telefónico**).

Para implementar este caso de acceso remoto, el administrador completa los pasos siguientes:

1. Comprobar que existe la directiva predeterminada denominada **Permitir el acceso si está habilitado el permiso de acceso telefónico**.
2. Crear una nueva directiva denominada **Los clientes VPN deben usar cifrado de alto nivel**.
3. Agregar la condición **Tipo-Puerto-NAS** a la nueva directiva y, a continuación, agregar **Virtual (VPN)**.
4. Comprobar que la opción **Conceder permiso de acceso remoto** está activada en la nueva directiva.
5. Modificar el perfil en la nueva directiva. En la ficha **Autenticación**, active sólo las casillas de verificación **Autenticación cifrada de Microsoft (MS-CHAP)** y **Autenticación cifrada de Microsoft versión 2 (MS-CHAP v2)**.
6. En la ficha **Cifrado**, desactive todas las opciones excepto **Muy fuerte**.

7. Mover la nueva directiva de forma que sea la primera directiva que se evalúe.

- Como se utiliza el modelo administrativo de acceso por usuario, la configuración de permisos de acceso remoto en la cuenta de usuario suplanta a la de la directiva. No obstante, para preparar una eventual transición a un modelo administrativo de acceso por directiva, el administrador de la red establece el permiso de acceso remoto en **Conceder permiso de acceso remoto**.

Cuando un usuario marca, se utiliza la siguiente lógica para aceptar o rechazar el intento de conexión (siempre y cuando se haya establecido la configuración predeterminada en las propiedades de acceso telefónico de la cuenta de usuario):

1. Se comprueba la primera directiva denominada **Los clientes VPN deben usar cifrado de alto nivel**.
2. Si el tipo de conexión es una conexión VPN, se evalúa la configuración de **Permiso de acceso remoto (acceso telefónico o red privada virtual)** en la cuenta de usuario.
    - Si está activada la opción **Denegar acceso**, se rechaza el intento de conexión.
    - Si está activada la opción **Permitir acceso**, la configuración del perfil se aplica a la conexión.
    - Si el intento de conexión está usando cifrado MPPE de 128 bits o cifrado 3DES IPSec, se acepta la conexión.
    - Si el intento de conexión no está usando cifrado MPPE de 128 bits o cifrado 3DES IPSec, se rechaza la conexión.

1. Si el intento de conexión no es una conexión VPN, se comprueba la siguiente directiva de acceso remoto denominada **Permitir el acceso si está habilitado el permiso de acceso telefónico**.

   Como el usuario tiene acceso telefónico cualquier día a cualquier hora, se evalúa la configuración de Permiso de acceso remoto (acceso telefónico o red privada virtual) en la cuenta de usuario.

   - Si está activada la opción **Denegar acceso**, se rechaza el intento de conexión.
   - Si está activada la opción **Permitir acceso**, se acepta la conexión de acuerdo con la configuración predeterminada de las propiedades de la cuenta de usuario y del perfil.

También debe tomarse en cuenta que la tasa de transferencia en una conexión VPN va a depender de la conexión que tengamos a Internet, ya sea por Dial Up, ADSL, ethernet (otra red LAN) o T1.

4.5 Implementación de una VPN en el ambiente Linux.

El servidor a utilizar para la implementación de nuestro sistema operativo VPN en Linux contendrá las mismas características que se utilizaron en el Sistema Operativo de Microsoft Windows NT 2000 Server, para así poder evaluar el rendimiento de la VPN con ambos sistemas.

El sistema operativo elegido es la distribución Ubuntu basado en Debian. Este Sistema Operativo se esta volviendo más popular y utilizado por su facilidad de acceso, uso e instalación, una de las ventajas principales es que reconoce la mayoría de los dispositivos electrónicos, como son: las tarjetas de red alámbricas y las tarjetas de red inalámbricas, principalmente, esto es una ventaja ya que son los dispositivos mas utilizados dentro de este proyecto de Redes Privadas Virtuales.

La configuración del equipo en cuanto a nombre, identificación de la red, direcciones IP, todo se mantendrá de la misma manera como se configuró el servidor de Windows NT 2000 Server, como se menciono anteriormente esto nos va ayudar a evaluar el rendimiento de nuestros sistemas operativos al implementar y trabajar con nuestras VPN.

4.5.1 Administración de usuarios y control de acceso en Linux.

El sistema de administración de usuarios para la distribución Debian de Ubuntu es localizada en las opciones de **administración** del **sistema** y tiene por nombre **usuarios y grupos,** en esta parte se pueden asignar los grupos y usuarios específicos para ingresar al sistema y tener el acceso remoto a través de nuestra VPN por medio de Linux. La ilustración 4.14 muestra la información que se requiere para tener nuestros usuarios dados de alta.

Figura 4.14 Registro de usuarios.

Dentro de cada usuario podemos asignar los privilegios de trabajo dentro del sistema, como son el acceso a dispositivos, Administración del sistema, conexión a Internet a través de un MODEM, monitor del registro del sistema, etc. Como se muestra en la figura 4.15.

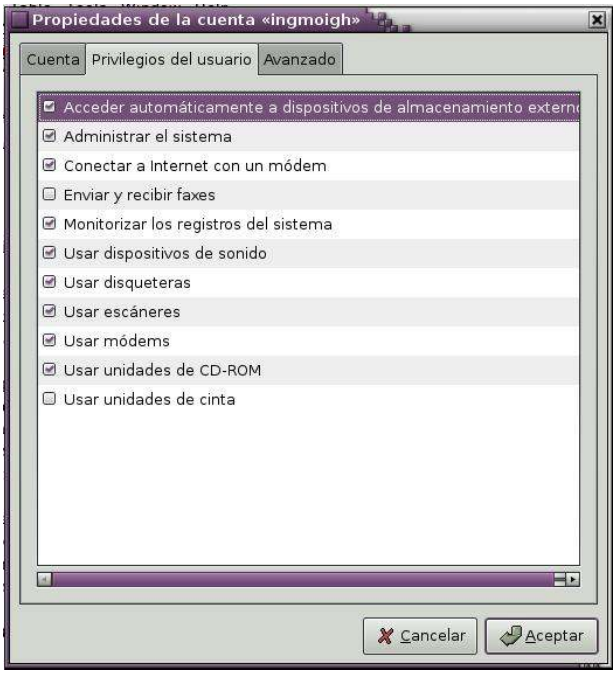


Figura 4.15 Privilegios de usuarios.

Las propiedades de cada usuario están asignados por una configuración básica, como es, El nombre de usuario, Nombre real y Contraseñas, entre otra información opcional que se puede manejar en esa ficha.

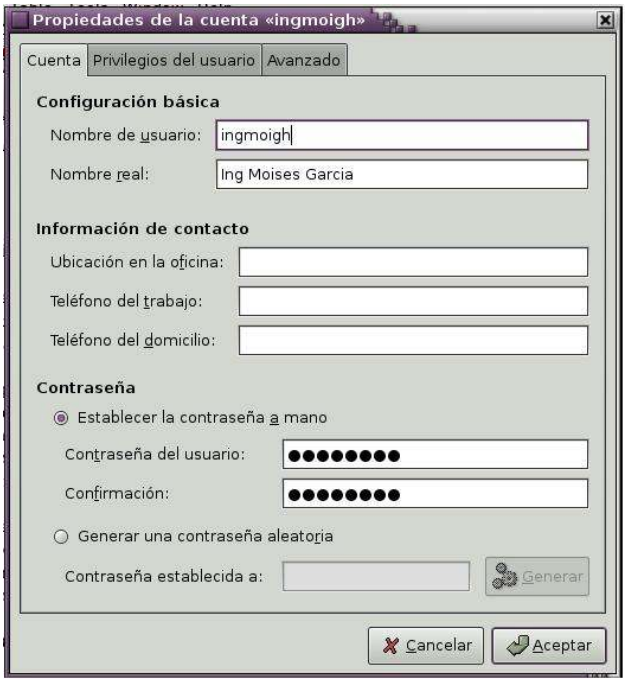


Figura 4.16 Información de la cuenta de usuario.

También podemos encontrar la configuración de avanzado donde podemos asignar el Directorio inicial para cada usuario, permitiendo así una partición del disco duro para trabajos, documentos y demás recursos a utilizar, se le asignara su interprete de comandos, el grupo principal al que pertenece dicho usuario y un identificador asignado por el sistema.

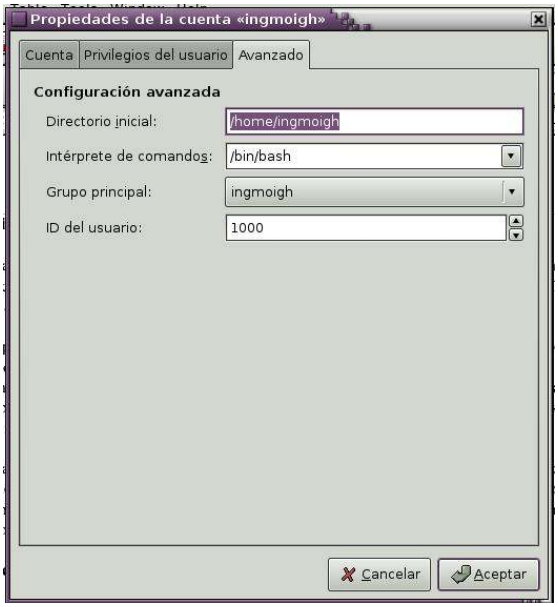


Figura 4.17 Configuración avanzada de los usuarios.

4.5.2 Configuración PPTP Cliente en Linux.

Esta es la parte de configuración de nuestro cliente PPTP para nuestra VPN, para poder configurar nuestro servidor en el sistema operativo Linux tomaremos en cuenta el apartado 3.6.4.3 Instalación y configuración de OpenVPN Servidor en Linux de nuestro capitulo 3, dado que la configuración de nuestro servidor VPN cuenta con las características y los protocolos de conexión por túnel, el acceso a nuestro servidor no genera ningún conflicto, por así mencionarlo los dos se configuración con el protocolo de túnel PPTP y el método de cifrado MPPE, si se requiere manejar un túnel a través del sistema operativo de Windows, este también nos ofrece el acceso por medio de estos protocolos compatibles sin generar algun conflicto en la conexión.

En el capítulo 3 se mencionó que el sistema OpenVPN también puede ser configurado para cliente PPTP y las características de configuración son las mismas manejadas en la aplicación PPTP configurada en este capitulo por lo que no causa ningún problema el utilizar uno u otro.

La configuración de nuestro cliente VPN estará dado por la siguiente información que a continuación se presenta siendo esta la configuración pptpconfig, este programa se maneja como una aplicación desarrollada en el ambiente Linux, el cual nos muestra los parámetros necesario para crear nuestro túnel. Paso a paso iremos describiendo la información que nos pide dicha aplicación para iniciar una VPN cliente y que estará dirigida a nuestro servidor VPN principal.

La figura 4.18 muestra la configuración del servidor VPN a donde dirigiremos nuestro túnel, los datos principales de configuración esta dada por los siguientes datos:

- Name: Nombre de la conexión VPN Cliente, en este caso el nombre a colocar es CT ARAGON.
- Server: El nombre del servidor o dirección IP para crear el túnel a través del protocolo PPTP.
- Domain: Nombre del Dominio de Autentificación del Servidor VPN.
- Username: Nombre de usuario del cliente registrado en el servidor VPN.
- Password: Contraseña del usuario cliente registrado en el servidor VPN.

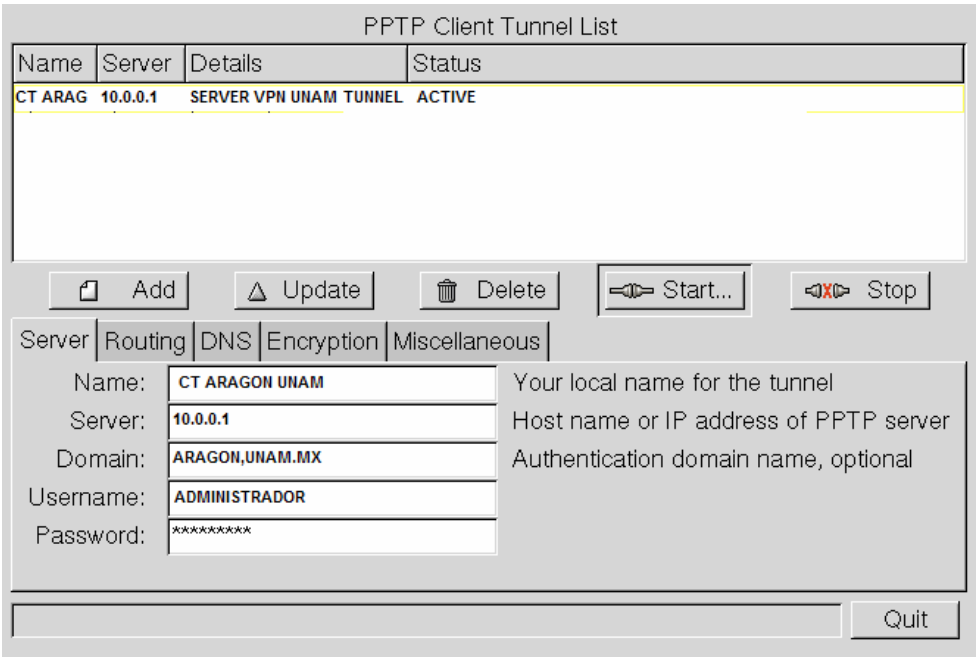


Figura 4.18. Configuración Cliente a Servidor VPN.

En la figura 4.19 se muestra la configuración del tipo de enrutamiento para considerar el manejo del protocolo de túnel, es decir, un túnel de LAN a LAN, un túnel de Cliente a LAN, o un enrutamiento por túnel completamente. Esto dependerá del administrador de la red y del manejo de su configuración para encaminar su red a alguna configuración en específico. La implementación de nuestro sistema operativo maneja la configuración cliente a LAN a través de nuestro protocolo PPTP, por lo cual se considero esta configuración en nuestra implementación para nuestro cliente y nuestro proyecto.

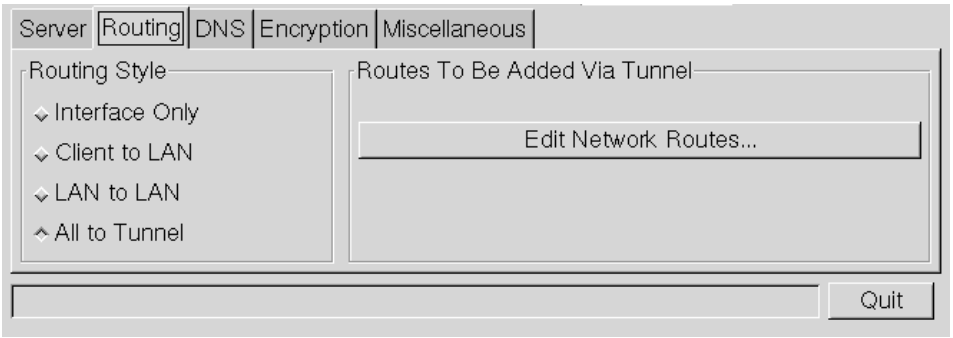


Figura 4.19 Configuración de enrutamiento de Túnel de Red.

Una de las partes esenciales de la configuración de nuestro túnel con esta aplicación es el requerimiento del tipo de cifrado de datos que se manejara en nuestra VPN, el sistema operativo Linux en su distribución de Ubuntu cuenta con el paquete ya instalado MPPE, por lo consiguiente en el apartado de Cifrado (Encryption) vamos a seleccionar esta opción como se muestra en la figura siguiente:

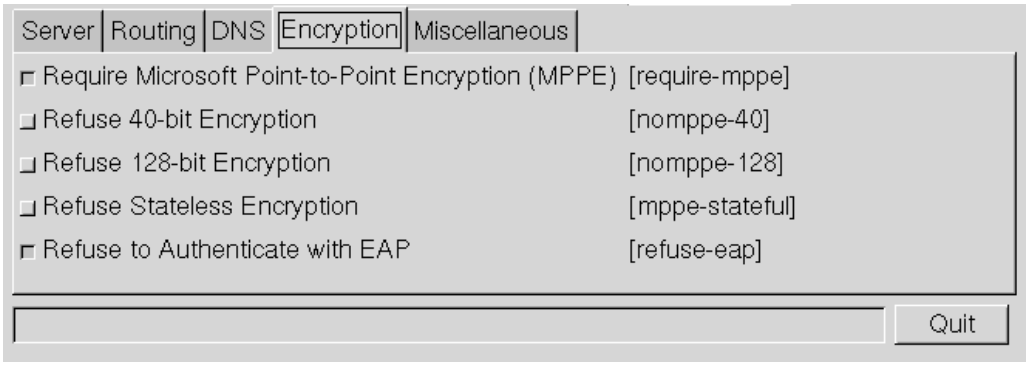


Figura 4.20 Configuración de Cifrado de datos.

La configuración de nuestro cliente PPTP está lista para iniciar con el túnel para nuestra Red Privada Virtual, tomaremos en cuenta una de las pestañas que aparecen en nuestra aplicación llamada miscelánea en el cual podemos corregir algunos datos de configuración en caso de que nuestra conexión presente algunas fallas, estos datos pueden ser corrección de errores en nuestra conexión, actualizaciones de nuestra aplicación o Intentar de nuevo la conexión. Ver Figura 4.21.

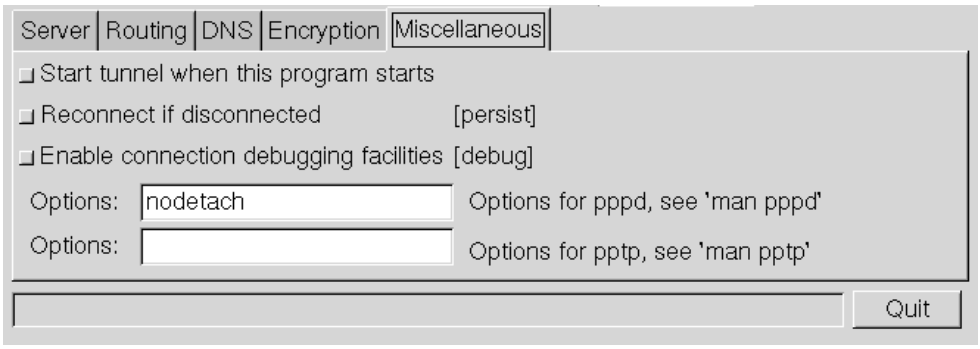


Figura 4.21 Configuración para corrección de errores.

4.5.3 Pruebas de conexión.

En esta parte las pruebas de conexión estarán dadas por el comando Ping que verifica el estatus de nuestro túnel y el tiempo de vida de nuestro paquete TTL a través del mismo, este comando puede ser utilizado en una Terminal de nuestro sistema operativo o a través de la aplicación de configuración PPTP cliente y las pruebas quedaran de la siguiente manera como se muestra en la figura 4.22:

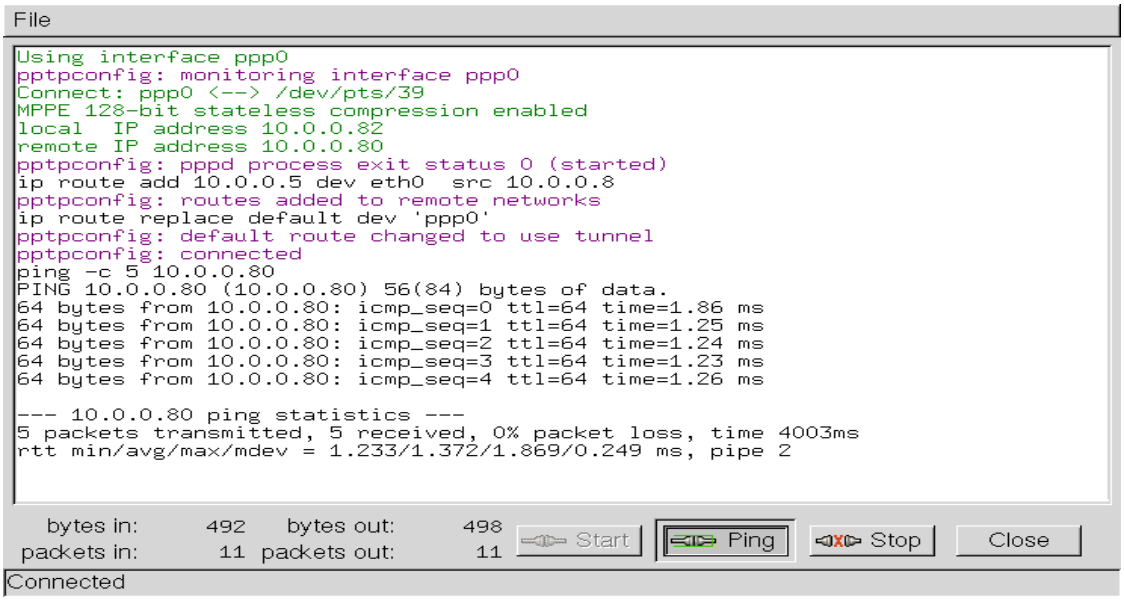


Figura 4.22 Prueba de conexión por Ping.

En el caso de esta implementación nuestra VPN decidimos que todo el tráfico de la red debe ir vía túnel VPN esto lo tomamos en cuenta ya que la aplicación nos permite encaminar nuestra información a través del túnel o no, como se mencionó en el apartado de la configuración del router de la aplicación PPTP Cliente.

Evaluación de los sistemas operativos en VPN.

La comparación de trabajo VPN en cada sistema operativo viene dada más que nada por las opciones de configuración que nos presentan al realizarla, por ejemplo, Windows NT nos ofrece mayores herramientas de administración de acceso remoto, administración de Archivos , Administración de usuarios, Administración de Puertos VPN, una disposición variada de protocolos implementados para estas redes de túnel como son PPTP, LP2T, sistemas variados de protocolos de autentificación y cifrado de datos, seguridad adicional y un sin fin de componentes que en este proyecto se describen para el manejo de VPN´s, por lo consiguiente el sistema operativo de Microsoft Windows NT es el más completo para el manejo de VPN. La única desventaja y que no hay que pasar por alto es el costo de la licencia para su uso.

En comparación con el sistema operativo Linux, debemos empezar diciendo que el costo de su licencia es cero, ya que este sistema se maneja bajo la filosofía de licencia libre, su conjunto de módulos en cuanto administración de usuarios y archivos es fiable por la seguridad que implementa y por que esta basado bajo una de las plataformas más seguras como es el sistema operativo UNIX, en cuando a la implementación de la VPN la configuración debe llevarse mediante paquetes que deben ser instalación, configurados y compilados para su uso, sin estos los módulos de los protocolos PPTP no pueden ser usados y como se había mencionado anteriormente el desarrollo de las VPN en Linux cambia constantemente por los nuevos desarrolladores de la comunidad Linux, en sus diferentes distribuciones, por lo que es difícil poder manejar un configuración en especifico para hacer uso de una VPN.

CONCLUSIONES.

Con esta parte concluimos que el Sistema Operativo Windows NT 2000 Server nos ofrece seguridad, confiabilidad, facilidad y un buen manejo de las conexión VPN, ya que sus directivas de seguridad son de las más avanzadas por el manejo de los protocolos de cifrado y el manejo de usuarios a través de sus herramientas de administración del propio sistema operativo, los resultados de las conexión fueron exitosas sin tener algún contratiempo al ingresar a nuestro servidor VPN.

Por otra parte podemos decir que la conexión VPN cumplió con su objetivo que es el compartir los recursos de la red principal y extender la red a lugares geográficamente ubicados en otro lugar. Siendo esto un estudio para un fin que es la de continuar con los proyectos en el Laboratorio de Cómputo, podemos indicar que las VPN pueden tener otras funciones u objetivos como son: el manejo de programas especiales con una conexión VPN para usuarios y clientes remotos ya programados en dichos sistemas, enlaces directos a aplicaciones como por ejemplo: sistemas de pedidos farmacéuticos, sistemas de nomina de alguna corporación, manejo de bases de datos, etc.

Al realizar la implementación de la VPN tanto cliente como servidor en el ambiente Linux, nos encontramos con algunos detalles de configuración que nos impidió llevar a cabo en el tiempo determinado la configuración del mismo por falta de algunos paquetes que se requieren adicionales a la configuración de la VPN en dicho sistema.

Aunque este problema puede solucionarse descargando dichos paquetes de Internet, la configuración tendrá que ser por medio de una persona con experiencia en el manejo y configuración de el sistema operativo Linux, lo cual podemos concluir que para poder llevar a cabo el manejo de una VPN Linux, el sistema debe contener todos los requerimientos necesarios, por lo consiguiente al no tenerlos se complica la instalación y configuración del mismo y esto hace

que se atrase su manejo en una red LAN o en algunas aplicaciones en ese momento requeridas, la configuración no es tan sencilla por lo que complica la tardanza en su instalación y no cumple con uno de los objetivos que es la facilidad, se requiere tiempo de configuración, la parte del costo es lo que cumple ya que este sistema es de licencia libre, la integridad de los datos y seguridad en la transmisión de la información cumple con los objetivos de este tema por lo que podría terminar concluyendo que el sistema es totalmente fiable, siempre y cuando sea manejado por personal capacitado y con experiencia en la administración del Sistema Operativo Linux.

BIBLIOGRAFÍA

[1] Andrew G. Mason, Redes Privadas Virtuales de Cisco Secure, primera edición, Pearson Educación, 2002.

[2] Steve Brown, Implementación de Redes Privadas Virtuales, primera edición, McGraw Hill Interamericana, 2001.

[3] Christopher Wegus, RedHat Linux 7, segunda edición, Ediciones Anaya, 2001.

[4] Thomas Schenk et Al, Administración de RedHat Linux, segunda edición, Prentice Hall, 2001.

[5] Javier González Cotera, Seguridad Profesional en Windows NT, segunda Edición, Alfaomega-Rama, 2000.

[6] Barrie Sosinsky, Jeremy Moskowitz, Aprendiendo Microsoft Windows 2000 Server en 24 horas, primera Edición, Pearson Educación, 2000.

[7] Cesar Pérez López, Domine Microsoft Windows Xp Professional, primera Edición, Alfaomega, 2002.

[8] Cesar Pérez López, Domine Microsoft Windows 2000 Professional, primera Edición, Alfaomega, 2001.

[9] Michael D. Bauer, Seguridad en servidores Linux, primera edición, Anaya Multimedia, 2005.

[10] Sebastián Sánchez Prieto, Unix y Linux: guía práctica, tercera edición, Alfaomega, 2005.

[11] David León Clark, Guía para el administrador de redes privadas virtuales RPV, primera edición, McGraw Hill, 2001.

REFERENCIAS A PÁGINAS DE INTERNET.

[R1] https://www.microsoft.com/windows2000/es
Documentación de Microsoft Windows 2000 Advanced Server.

[R2] http://quozl.netrek.org/pptp/pptpconfig/pptpconfig.phtml
Software PPTPclient para la creación de túneles cliente.

[R3] http://openvpn.net/
Proyecto de OPENVPN en Linux.

[R4] http://www.freeswan.org/
Proyecto de VPN Frees/wan en Linux.

[R5] http://pptpclient.sourceforge.net/
Aplicaciones del Protocolo PPTP para las distribuciones Linux.

[R6] http://www.gnu.org/
Pagina del proyecto GNU.

[R7] http://www.opensource.org/licenses
Página de la Licencia Pública General de Linux.

[R8] http://www.poptop.org/
Proyecto del Protocolo PPTP para Servidores Linux.

[R9] http://www.microsoft.com/technet/itsolutions/network/ipsec/default.mspx
Información del Protocolo IPSec.

[R10] http://www.ipsec-howto.org/spanish/x161.html
Documentación de IPSec.

[R11] http://www.kriptopolis.org
Documentación y algoritmos de Criptografía y Cifrado de datos.

[R12] http://www.networksorcery.com/
Pagina de RFC de algoritmos de cifrado, autenticación y túneles utilizados en VPN.

[R13] http://www.ubuntu-es.org/
Pagina de la Comunidad de Ubuntu Linux