UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

Tesis previa la obtención del título de Ingeniero en Sistemas Computacionales

Tema: Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de enlace.

AUTOR: **Cosme MacArthur Ortega B.**

DIRECTOR DE TESIS: **Ing. Msc. Rodrigo Naranjo**

Ibarra, Enero del 2003

CERTIFICACIÓN.

Certifico que el desarrollo de la presente tesis fue realizada en su totalidad por el Egresado Cosme MacArthur Ortega Bustamante bajo mi dirección.

_____

Ing. Msc. Rodrigo Naranjo
DIRECTOR DE TESIS

TESIS DE GRADO

Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de enlace.

Agradecimiento

Al Ing. Rodrigo Naranjo, Director de Tesis, por el aporte brindado con sus valiosos conocimientos, cometarios y recomendaciones, para la correcta elaboración de la presente investigación.

A todos los Docentes, Trabajadores y Estudiantes de la Facultad de Ingeniería en Ciencias Aplicadas, por su colaboración en la realización del presente trabajo.

Al Ing. Irving Reascos, compañero de trabajo quien ha colaborado con sus conocimiento y experiencia en el área de Redes.

Dedicatoria

La presente investigación la dedico a mis padres que han dedicado todo su esfuerzo, sacrificio y han sabido conducirme por el camino correcto para la finalización de mis estudios.

Cosme M. Ortega B.

Introducción

La presente investigación tiene como finalidad dar a conocer una nueva tecnología que aún se encuentra en evolución, tecnología que nos permitirá conectar redes distantes geográficamente, de manera segura y a bajos costos, utilizando redes públicas como medio de enlace o transmisión.

Esta tecnología se denomina Redes Privadas Virtuales (VPN en ingles Virtual Private Network). En la actualidad este término (VPN), ya es muy común dentro de las telecomunicaciones, existiendo empresas a nivel mundial que se dedican exclusivamente a la investigación y prestación de servicios de esta tecnología.

Esta investigación nos presenta los aspectos más importantes referentes a VPN´s, empezando por una breve introducción a las Redes Privadas Virtuales, donde analizaremos conceptos sobre VPN, además estudiaremos los diferentes elementos que se necesitan para implementar un sistema de Red Privada Virtual, se revisará los tipos de implementaciones comunes, los requisitos, y sus beneficios de esta tecnología.

En las Redes Privadas Virtuales, utilizaremos protocolos que pertenecen a la pila de protocolos del TCP/IP, por lo que hemos creído necesario hacer un estudio del protocolo TCP/IP, en su formato de 4 capas que corresponde a la capa de interfaz de red, capa de Internet, capa de transporte y capa de aplicación.

Analizaremos los diferentes protocolos de túnel que se pueden utilizar para la implementación de VPN, entre los que tenemos PPTP (Point to Point Tunneling Protocol), el protocolo L2F (Layer Two Forwarding) y el protocolo L2TP (Layer Two Tunneling Protocol) protocolo que reemplazo al L2F, además estudiaremos el protocolo PPP y el IPSec, protocolos muy utilizados en varios tipos de redes.

Las Redes Privadas Virtuales poseen diferentes arquitecturas que deben ajustarse a los requerimientos de las empresas, es por esto que se ha visto la necesidad de estudiar cada una de las arquitecturas entre las que tenemos VPN proporcionada por un proveedor de servicios de Red (ISP), VPN basada en cortafuegos, VPN

basada en caja negra, VPN basada en Enrutador, VPN basada en acceso remoto, VPN basada con herramientas proxy, VPN basada en software. Arquitecturas que el lector deberá escoger de acuerdo a su necesidad.

Una vez estudiadas las arquitecturas he creído conveniente estudiar las diferentes topologías de Redes Privadas Virtuales que se pueden obtener, para tener claro en donde se debe instalar su VPN dentro de su topología de su red. Entre las topologías más comunes tenemos Topología de Cortafuego/VPN a Cliente, Topología de VPN/LAN a LAN, Topología de VPN/Cortafuego a Intranet/Extranet, Topología de VPN/Tramas o ATM, Topología de VPN de hardware (Caja Negra), Topología de VPN/NAT, Túneles de VPN anidados.

Como veremos en el transcurso del desarrollo de esta investigación los términos de VPN y de Seguridad, van de la mano, por lo que hemos dedicados un capitulo de la investigación al tratamiento de las seguridades en VPN, en la que estudiaremos los posibles ataques que se pueden dar a una VPN, la manera de cómo identificar los ataques, la importancia de la seguridad en las Redes Privadas Virtuales, los diferentes requisitos de seguridad en las Redes Privadas Virtuales.

En la parte final, presentamos una metodología para la implementación de Redes Privadas Virtuales con Internet como red de enlace, metodología que sugiere al lector una serie de pasos y aspectos que se deben tomar en cuenta para una mejor implementación de una Red Privada Virtual.

Y por último presentamos la instalación y configuración de una red privada virtual con Windows2000 Server el cual tendrá la función de servidor VPN y Windows98se que será el cliente de la VPN.

Esperando que la presente investigación sirva para afianzar en los lectores los conocimientos referentes a redes y VPN´s, despertar en ellos la curiosidad por esta nueva tecnología que poco a poco va creciendo y posesionándose en el mercado de las telecomunicaciones, y motivar la investigación de este interesante tema.

EL AUTOR.

INDICE

Portada i
Agradecimiento ii
Dedicatoria iii
Introducción iv
Indice vi

CAPITULO 1.
Introducción a las Redes Privadas Virtuales 1
1.1.- Elementos de una conexión VPN 5
1.2.- Implementaciones comunes de una VPN 6
1.2.1.- Intranet 7
1.2.2.- Acceso remoto 7
1.2.3.- Extranet 8
1.2.4.- VPN Interna 9
1.3.- Requisitos de una Red Privada Virtual 10
1.4.- Beneficios de las Redes Privadas Virtuales 13

CAPITULO 2.
Protocolos TCP/IP 16
2.1.- Introducción 17
2.2.- Arquitectura de TCP/IP 18
2.3.- Capa de Interfaz de Red 19
2.4.- Capa de Internet 23
2.4.1.- IP (Internet Protocol) 23
2.4.2.- Fragmentación y ensamblado 33
2.4.3.- Internet Control Message Protocol (ICMP) 33
2.4.4.- Protocolo de Manejo de Grupos de Internet (IGMP) 35
2.5.- Capa de Transporte 36
2.5.1.- Protocolo de Datagrama de Usuarios (UDP) 37
2.5.2.- Protocolo de Control de Transmisión TCP 39
2.5.2.1.- Interfaces TCP 41
2.5.2.2.- Control de Flujo 42
2.6.- Capa de Aplicación 43

CAPITULO 3.
Protocolos de Túnel **46**
3.1.- Introducción 47
3.2.- Protocolos de Túnel 49
3.2.1.- Protocolo Punto a Punto (PPP) 52
3.2.2.- Protocolo de Túnel Punto a Punto (PPTP) 56
3.2.3.- Transmisión de Nivel 2 (L2F) 60
3.2.4.- Protocolo de Túnel de nivel 2 (L2TP) 61
3.2.5.- Protocolo de Internet Seguro (IPsec) 65
3.3.- Tipos de Túnel 67
3.3.1.- Túneles Voluntarios 68
3.3.2.- Túneles Obligatorios 69

CAPITULO 4.
Arquitectura de Red Privada Virtual **71**
4.1.- VPN proporcionada por un proveedor de servicios de Red (ISP) 73
4.2.- VPN basada en cortafuegos 76
4.3.- VPN basada en caja negra 77
4.4.- VPN basada en Enrutador 79
4.5.- VPN basada en acceso remoto 80
4.6.- VPN basada con herramientas proxy 81
4.7.- VPN basada en software 82

CAPITULO 5.
Topologías de Red Privada Virtual **84**
5.1.- Topología de Cortafuego/VPN a Cliente 86
5.2.- Topología de VPN/LAN a LAN 88
5.3.- Topología de VPN/Cortafuego a Intranet/Extranet 90
5.4.- Topología de VPN/Tramas o ATM 92
5.5.- Topología de VPN de hardware (Caja Negra) 94
5.6.- Topología de VPN/NAT 97
5.7.- Túneles de VPN anidados 98

CAPITULO 6.

Seguridades de Red Privada Virtual **100**
6.1.- Ataques a la red privada virtual. 104
6.1.1.- Ataques a los algoritmos criptográficos. 105
6.1.2.- Ataques al generador de números aleatorios. 108
6.1.3.- Ataques a la recuperación de claves. 109
6.1.4.- Ataques al Protocolo de Seguridad de Internet (IPSec). 110
6.1.5.- Ataques al protocolo PPTP. 111
6.1.6.- Ataques a la autoridad emisora de certificados. 113
6.1.7.- Ataques a radius. 113
6.1.8.- Ataques a kerberos. 114
6.1.9.- Ataques a pretty good privacy (PGP). 114
6.1.10.- Ataques de negación de servicio. 115
6.1.11.- Ataques de Autentificación. 117
6.2.- Como identificar los ataques. 119
6.3.- Importancia de la Seguridad en las VPN. 120
6.4.- Requisitos de seguridad en las Redes Privadas Virtuales. 121
6.4.1.- Criptografía. 122
6.4.1.1.- Algoritmos Simétricos. 123
6.4.1.1.1.- Cifras de bloque. 124
6.4.1.1.2.- Cifras de flujo. 126
6.4.1.2.- Algoritmos Asimétricos. 126
6.4.1.2.1.- Algoritmo Diffie-Hellman. 127
6.4.1.2.2.- Algoritmo RSA. 128
6.4.1.3.- Algoritmo Híbrido (PGP). 128
6.4.1.4.- Otros Cifrados. 129
6.4.2.- Certificados Digitales. 130
6.4.3.- Autenticación. 131
6.4.3.1.- Contraseñas del Sistema Operativo. 131
6.4.3.2.- S/KEY. 132
6.4.3.3.- RADIUS. 133
6.4.3.4.- KERBEROS. 133
6.4.3.5.- LDAP. 134
6.4.3.6.- EAP. 134
6.4.3.7.- ISAKMP/Oakley 135
6.4.4.- Sin Repudio. 135
6.4.5.- Cifrado Punto a Punto. 135
6.4.6.- Administración de seguridad centralizada. 136

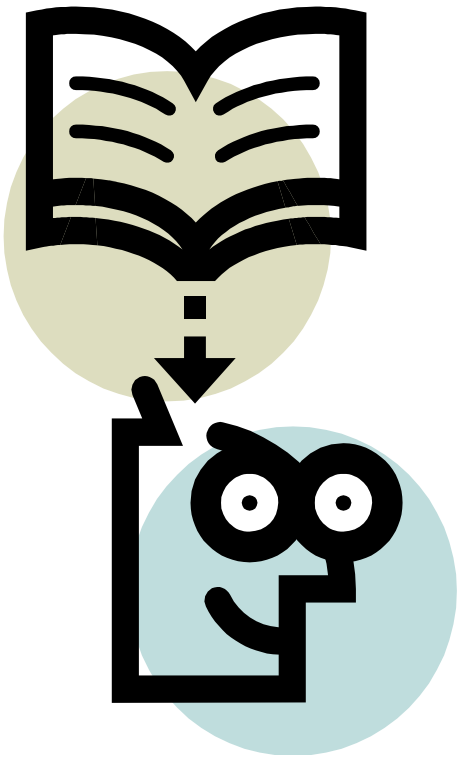
6.4.7.- Procedimientos de respaldo/restauración. 137
6.4.7.1.- Planes de contingencia. 138
6.5.- Sistemas Operativos. 139
6.5.1.- Niveles de Seguridad C2, B1 (Orange book). 139

CAPITULO 7.
Metodología para la implementación de una VPN. 142
7.1. Formación de un Equipo Ejecutor 144
7.2. Fijación del Alcance 145
7.3 Estudio y Análisis 146
7.4. Elección de la Plataforma 147
7.5. Propuestas de Soluciones. (Diseño) 148
7.6. Seguridades. 149
7.6.1. Fijación de Objetivos 149
7.6.2. Relación Costos vs. Riesgos. 149
7.7. Plan de Contingencia. 150
7.8. Costos. 151
7.8.1. Hardware 151
7.8.2. Software 152
7.8.3. Capacitación 152
7.8.4. Contratación de Servicios 152
7.9. Implementación 153
7.10. Mantenimiento 153
7.10.1. El Mantenimiento preventivo 153
7.10.2. El mantenimiento correctivo 154
7.10.3. La Actualización 154
7.10.4. La Renovación 154
7.11. Medición de Resultados. 155

COMPROBACION DE HIPOTESIS 156
CONCLUSIONES 157
RECOMENDACIONES 159
BIBLIOGRAFIA 161
ANEXOS 168
Instalación y configuración del Servidor VPN en Windows 2000 Server. 169

Instalación y configuración del Cliente VPN con Windows XP Profesional. 210
Instalación y Configuración del Cliente VPN con Windows 98se. 220
Referencias Bibliográficas 226

CAPITULO I



INTRODUCCIÓN A LAS REDES PRIVADAS VIRTUALES

1.1.- Elementos de una conexión VPN
1.2.- Implementaciones comunes de una VPN
1.3.- Requisitos de una Red Privada Virtual
1.4.- Beneficios de las Redes Privadas Virtuales

La gran escalabilidad de las empresas y la forma actual de negociación a nivel mundial se basa en la información que estas puedan poseer y manipular, convirtiéndose en un factor vital para estas, el uso de redes de computadores que deben cumplir con atributos como seguridad, confiabilidad, y bajos costos, atributos fáciles de conseguir en una red privada, a la cual ningún agente externo a la red puede ingresar.

En la actualidad es más común escuchar de empresas en las que es necesario tener oficinas muy distantes del lugar geográfico en donde se encuentra la matriz de la empresa, esto nos hace pensar en la forma de conectividad entre estas oficinas y la matriz. La conectividad la podemos obtener de varias formas con costos y tiempos de respuesta muy altos, y algo muy importante la mínima seguridad que estas poseen.

La introducción del término y la tecnología de Redes Privadas Virtuales (en Inglés VPN Virtual Private Network), han evolucionado durante los últimos 5 años (1997), ya que es una tecnología que nació paralelamente con el origen del TPC/IP, en la década de los 70.

Una red VPN es una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas (una red publica y compartida más común es Internet). Con una VPN se puede enviar datos entre dos computadoras a través de redes públicas o compartidas de una manera que emula las propiedades de un enlace punto a punto privado.

Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas:

- ✓ Deben ser capaces de transportar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública.
- ✓ La solución debe agregar encriptación, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado.

- ✓ La solución debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de modo que un adversario no pueda acceder a los recursos del sistema.

Para emular un enlace punto a punto, los datos son encapsulados o envueltos, con una cabecera que proporciona la información de enrutamiento que le permite atravesar la red pública o compartida para llegar a su destino. Para emular un enlace privado, los datos enviados son encriptados para tener confidenciabilidad. Los paquetes que son interceptados en la red pública o compartida son indescifrables. El enlace en el cual los datos son encapsulados y encriptados se conoce como una conexión de red privada virtual (VPN) [WWW05].

La figura 1.1 ilustra el concepto lógico de una VPN.

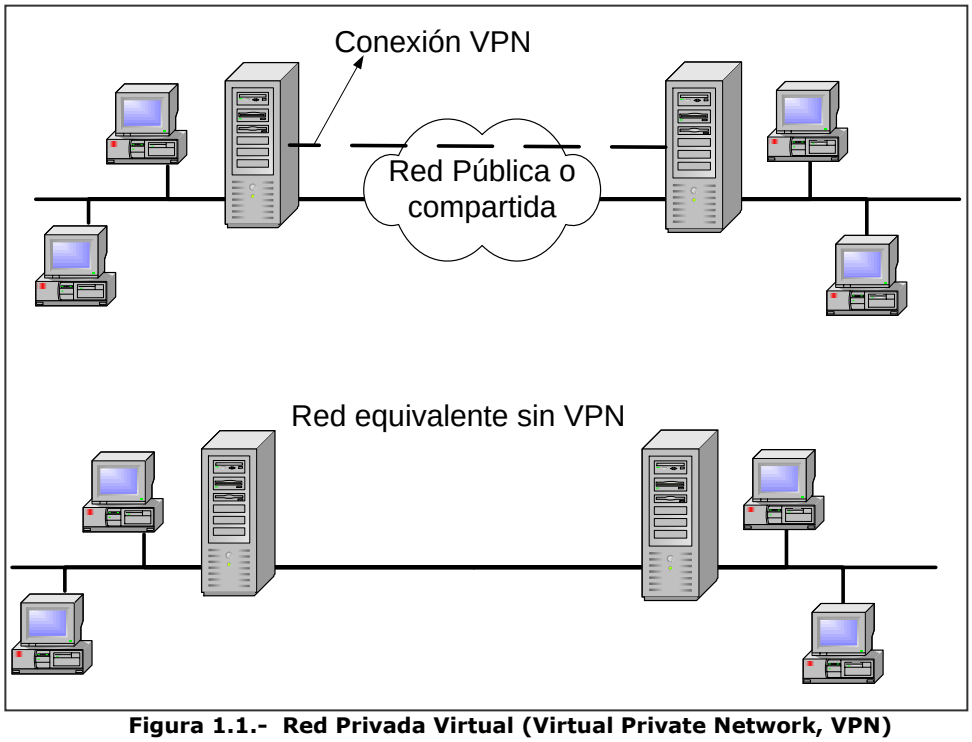


Figura 1.1.- Red Privada Virtual (Virtual Private Network, VPN)

Con las conexiones VPN los usuarios que trabajan en casa o de manera móvil pueden tener una conexión de acceso remoto a un servidor de la organización

utilizando la infraestructura proporcionada por una red pública como Internet. Desde el punto de vista del usuario, la VPN es una conexión punto a punto entre la computadora (cliente VPN), y el servidor de la organización (servidor VPN). La infraestructura exacta de la red pública o compartida es irrelevante porque desde el punto de vista lógico parece como si los datos fueran enviados por un enlace privado dedicado.

Con las conexiones VPN las organizaciones también pueden tener conexiones enrutadas (routed connections) con sus oficinas geográficamente separadas o con otras organizaciones por una red como Internet, manteniendo a la vez una comunicación segura. Una conexión VPN enrutada a través de Internet opera desde el punto de vista lógico como un enlace WAN dedicado.

Con las conexiones VPN, tanto en las conexiones de acceso remoto como las conexiones enrutadas, una organización puede cambiar de líneas rentadas (leased lines) o accesos telefónicos (dial-up) de larga distancia a accesos telefónicos locales o líneas rentadas con un proveedor de servicio de Internet (Internet Service Provider, ISP).

De acuerdo a estos preámbulos se define a una red privada virtual:

> Un intercambio de información entre dos puntos de una forma segura a través de una red insegura y pública

1.1.- Elementos de una conexión VPN.

La tabla 1.1 y la figura 1.2 muestran los elementos de una conexión VPN, los cuales se describen[WWW05].

Elemento	Detalle
Servidor VPN	Administra clientes VPN
Cliente VPN	Cliente Remotos
Túnel	Encapsulamiento de los datos
Conexión VPN	Encriptación de datos
Protocolos de Túnel	Administracíon de túneles
Datos de Túnel	Datos que se transmiten
Red de Tánsito	Red pública de enlace

Tabla 1.1.- Elementos de una conexión VPN

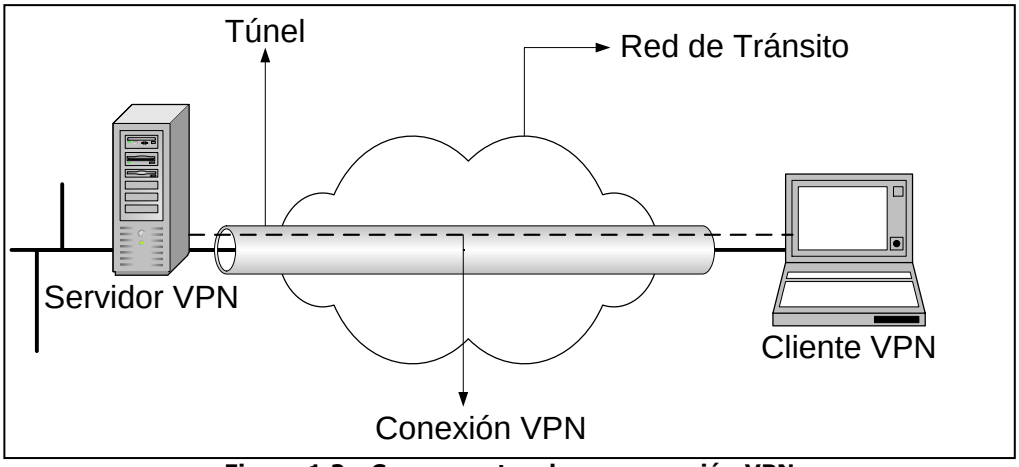


Figura 1.2.- Componentes de una conexión VPN

Servidor VPN.- Computadora que acepta conexiones VPN de clientes VPN. Encargado de administrar todos los clientes VPN y proporcionar la seguridad de la red.

Cliente VPN.- Computadora que inicia una conexión VPN con un servidor VPN.

Túnel.- Porción de la conexión en la que los datos son encapsulados.

Conexión VPN.- Porción de la conexión en la cual los datos son encriptados. Para conexiones VPN seguras, los datos son encriptados y encapsulados en la misma porción de la conexión.

Nota: Es posible crear un túnel y enviar los datos a través del túnel sin encriptación. Esta no es una conexión VPN porque los datos privados viajan a través de la red pública o compartida en una forma no encriptada y fácilmente visible e insegura.

Protocolos de túnel.- Se utilizan para administrar los túneles y encapsular los datos privados. Existen varios protocolos de túnel que se estudiarán más adelante.

Datos del túnel.- Datos que son generalmente enviados a través de un enlace punto a punto.

Red de tránsito.- Red pública o compartida que permite el tránsito de los datos encapsulados. La red de tránsito puede ser Internet o una intranet privada.

1.2.- Implementaciones comunes de una VPN.

Entre las implementaciones más comunes se tiene 4 maneras claramente identificadas [LIB02]:

TIPO	DETALLE
VPN de Intranet	Creación de conexión entre las oficinas centrales y las oficinas remotas.
VPN de Acceso Remoto	Creación de conexión entre las oficinas centrales y los usuarios móviles remotos.
VPN de Extranet	Creación de conexión entre la empresa y sus socios comerciales.
VPN Interna	Creación de conexión dentro de una LAN

Tabla 1.2.- Implementaciones comunes de una VPN

1.2.1.- VPN de Intranet.

Este tipo de implementación esta dada por la creación de una conexión entre las oficinas centrales corporativas y las oficinas remotas que se encuentran en el exterior. A comparación con una Intranet típica el acceso viene desde el exterior a la red y no desde el interior. La siguiente figura ilustra una Red privada Virtual de Intranet.

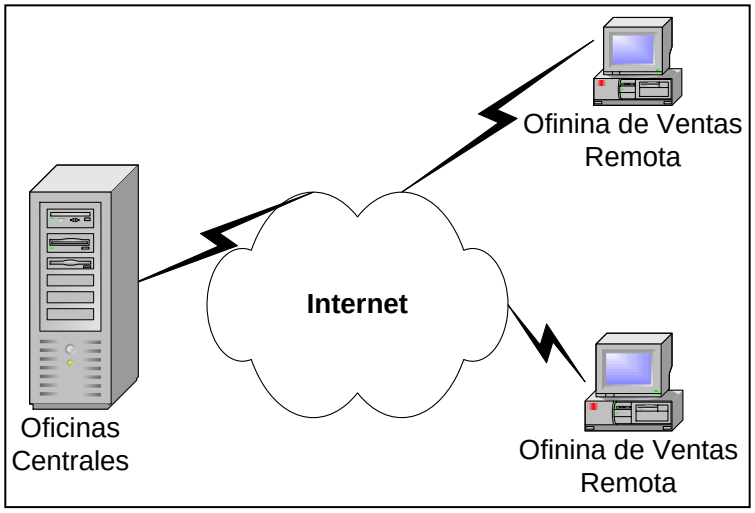


Figura 1.3.- VPN de Intranet

1.2.2.- VPN de Acceso Remoto.

Una red privada virtual de acceso remoto se crea entre las oficinas centrales corporativas y los usuarios móviles remotos a través de un ISP. Como se puede observar en la siguiente figura, el usuario móvil levanta una conexión telefónica con un ISP y crea un túnel de conexión hacia las oficinas centrales corporativas.

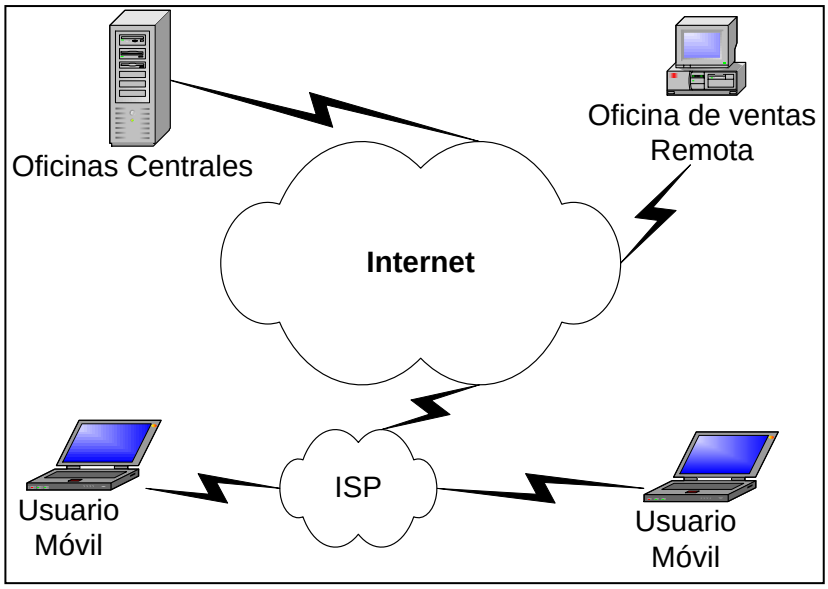


Figura 1.4.- VPN de Acceso Remoto

1.2.3.- VPN de Extranet.

Una red privada virtual de Extranet se crea entre la empresa y sus socios comerciales (clientes, proveedores), mediante el protocolo HTTP, que es el común de los navegadores de Web, o mediante otro servicio y protocolo ya establecido entre las dos partes involucradas. Esta implementación tiene mayor impacto en todo lo referente al comercio electrónico brindando seguridad y eficacia para las empresas y sus socios comerciales. La figura 1.5 ilustra una red privada virtual de extranet.

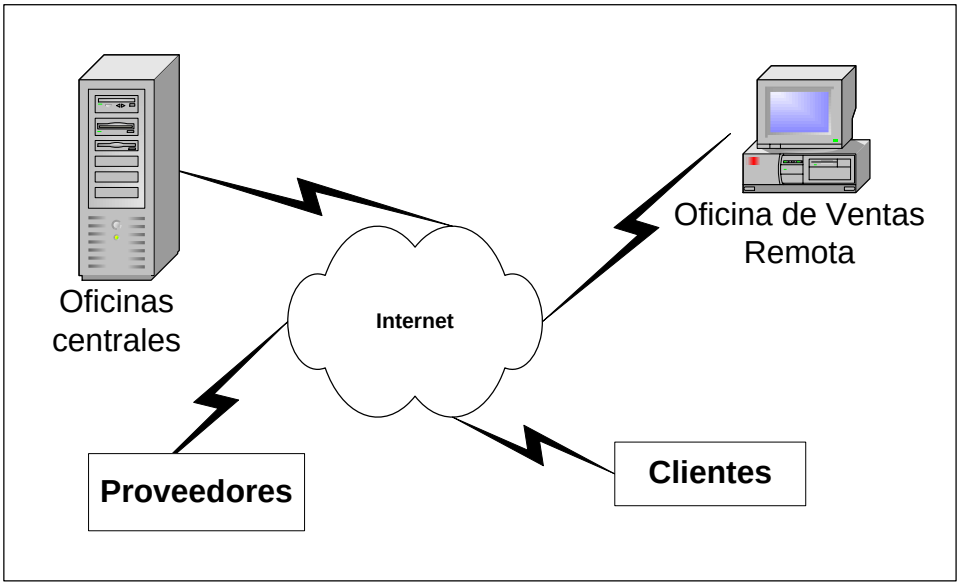


Figura 1.5.- VPN de Extranet

1.2.4.- VPN Interna.

Una red privada virtual interna, es una implementación que no tiene un uso frecuente en el entrono de las redes. Este tipo de implementación se crea en una LAN, siempre que se considere necesario transferir información con mucha privacidad entre departamentos de una empresa.

Esta red privada virtual interna es necesaria implementarla cuando se cree que se pueden tener ataques informáticos realizados por los mismos empleados de la empresa. La figura 1.6 ilustra una configuración típica de red privada virtual interna.

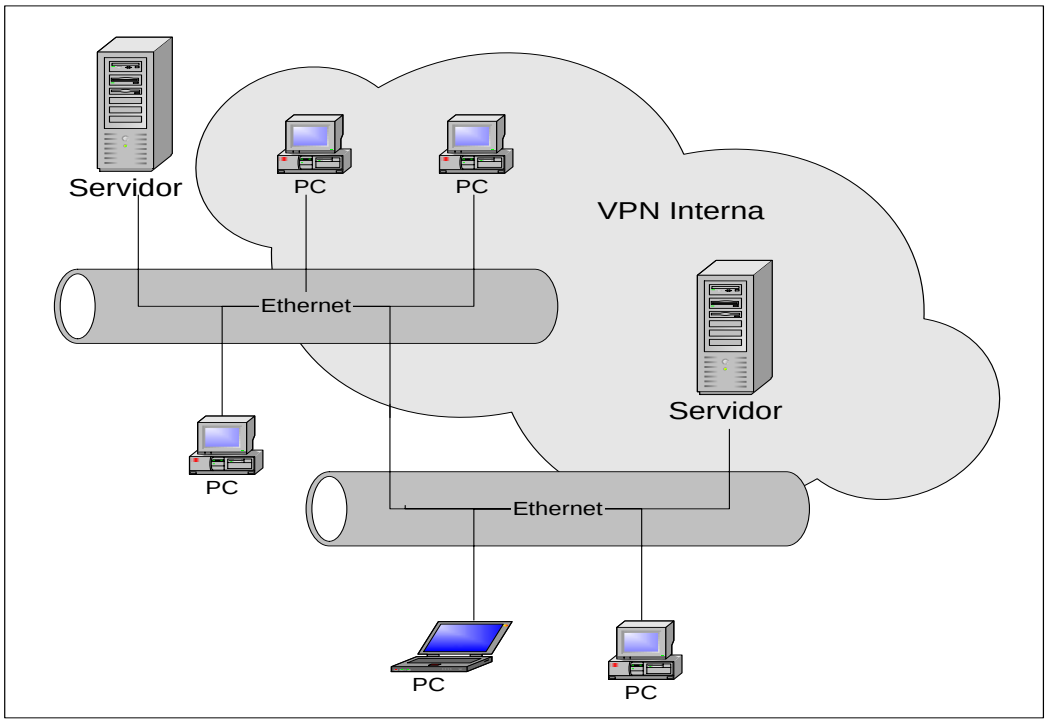


Figura 1.6.- VPN Interna

1.3.- Requisitos de una Red Privada Virtual.

Para garantizar que una red privada virtual sea segura, este disponible y sea fácil de mantener es necesario cumplir con ciertos requisitos esenciales que una empresa debe tomar en cuenta antes de implementar una Red Privada Virtual [LIB02].

Estos requisitos son los siguientes:

- ✓ Disponibilidad
- ✓ Control
- ✓ Compatibilidad
- ✓ Seguridad
- ✓ Interoperabilidad
- ✓ Confiabilidad
- ✓ Autenticación de datos y usuarios

- ✓ Sobrecarga de tráfico
- ✓ Mantenimiento
- ✓ Sin repudio

Disponibilidad.- La disponibilidad se aplica tanto al tiempo de actualización como al de acceso. No basta que el usuario tenga autorización para acceder a los servidores corporativos, si no puede conectarse debido a problemas de la red, por tanto se debe asegurar la disponibilidad en la parte física de la red.

Control.- El control debe ser implementado por el supervisor o administrador de la Red Privada Virtual, sea este interno o externo dependiendo de la como se realizó la implementación de VPN.

Debemos tomar en cuenta que por muy grande que sea la organización es posible tener una solo VPN, lo que facilitará al administrador de la VPN el control sobre la misma.

Compatibilidad.- Debido que al utilizar tecnologías de VPN y de internet estas se basan en protocolo IP, por lo que la arquitectura interna del protocolo de red de la compañía debe ser compatible con el protocolo IP.

Seguridad.- Hablar de seguridad y de red privada virtual, hasta cierto punto se podría decir que son sinónimos. La seguridad en una VPN abarca todo, desde el proceso de cifrado que se implementa hasta los servicios de autenticación de usuarios.

Es necesario que se tenga muy en cuenta este término de seguridad, ya que se puede afirmar que una VPN sin seguridad no es una VPN.

Interoperabilidad.- La interoperabilidad de una red privada virtual, es muy importante para la transparencia en la conexión entre las partes involucradas.

Confiabilidad.- La confiabilidad es uno de los requisitos importantes que debe poseer en una Red Privada Virtual, pero esta confiabilidad se ve afectada en gran porcentaje en la VPN de Acceso Remoto en las que se sujeta a la confiabilidad que se tiene por parte del ISP, ya que si el servicio del ISP se interrumpe la

conexión también y nosotros no se podrá hacer nada hasta que el ISP nuevamente brinde su servicio a los clientes.

Autenticación de Datos y Usuarios.- La autenticación de datos y de usuarios es sumamente importante dentro de cualquier configuración de Red privada Virtual.

La autenticación de datos afirma que los datos han sido entregados a su destinatario totalmente sin alteraciones de ninguna manera.

La autenticación de usuarios es el proceso en el que se controla que solos los usuarios admitidos tengan acceso a la red y no sufrir ataques por usuarios externos y maliciosos.

Sobrecarga de tráfico.- La sobrecarga de tráfico es un problema de cualquier tipo de tecnología de redes, y por ende también es un problema inevitable, especialmente si tenemos una red privada virtual a través de un ISP. Tomando en cuenta que un paquete enviado en una VPN es encriptado y encapsulado lo que aumenta de manera significativa la sobrecarga de tráfico en la red.

Mantenimiento.- El mantenimiento, aspecto del que no se puede olvidar. Si la red privada virtual es implementada con los propios recursos de la empresa es necesario considerar que el mantenimiento debe estar soportado por el propio personal del departamento de sistemas, el cuál debe estar capacitado para este fin. De no poseer el personal capacitado es preferible contratar servicio externos que se encarguen de la implementación y mantenimiento de la red privada virtual de mi empresa.

Sin repudio.- Consiste en el proceso de identificar correctamente al emisor, con la finalidad de tener claro desde donde proviene la solicitud. Si se considera que una VPN me va a servir para contactarme con mis clientes es necesario que este bien identificado de donde proviene el pedido. Para poder realizar cualquier transacción comercial (comercio electrónico) por internet es necesario que esta transacción sea un proceso sin repudio. No podemos dar cuenta que nuevamente se esta hablando de seguridad, una de las características fundamentales en una VPN.

1.4.- Beneficios de las Redes Privadas Virtuales.

El simple hecho de hablar de redes privadas virtuales, como se indicó anteriormente, viene a la mente el término de seguridad, así como también el bajo costo que esta tecnología necesita para implementarla y además su facilidad de uso [WWW05].

En resumen se puede decir que la implementación de una red privada virtual nos hace pensar en tres aspectos fundamentales y beneficiosos para nuestra empresa que son:

- ✓ Seguridad
- ✓ Bajos costos
- ✓ Facilidad de uso

Los costos de implementación de las redes privadas virtuales tiene que ver más con la capacitación del personal de sistemas para la implementación y mantenimiento de la red privada virtual asi como costos de contratación de servicios de un ISP.

Pero todo esto no debe ser tomado como una desventaja de esta tecnología, sino debe tomarse como una inversión para futuros ahorros que se obtendrán.

A continuación se describe algunos de los beneficios que se tiene en la implementación de redes privadas virtuales:

Ahorro en costos.- el ahorro en costos de las redes privadas virtuales esta asociado con diferentes factores que influyen en el paso de una tecnología anterior a una tecnología de redes privadas virtuales.

La eliminación de líneas rentadas, al igual que las líneas por marcación son dos factores fundamentales que permitirán el ahorro en la implementación de una VPN, tomando en cuenta que al eliminar este tipo de comunicación también se elimina los costos de los demás dispositivos involucrados como puede ser equipos pbx, equipos de acceso remoto. También se eliminarán costos de

instalación y configuración de dichos equipos de acceso remoto, entre otros costos.

Diseño de la red.- Uno de los principales beneficios de las redes privadas virtuales se basan en el diseño de estas. Para aclarar de mejor manera estos beneficios observemos el siguiente ejemplo.

En la figura 1.7 se puede observar el diseño de una WAN, en la que es necesario que se tenga en cuenta que al diseñar esta WAN con enlaces de líneas rentadas y de marcación, debe existir un gran esfuerzo por el personal de implementación de la WAN para saber que tráfico se va a tener para saber el tipo de líneas que se debe adquirir y en que porcentajes. Además deberán tener en cuenta los problemas que aparecen al usar líneas ya sea rentadas y de marcación en grandes distancias [LIB02].

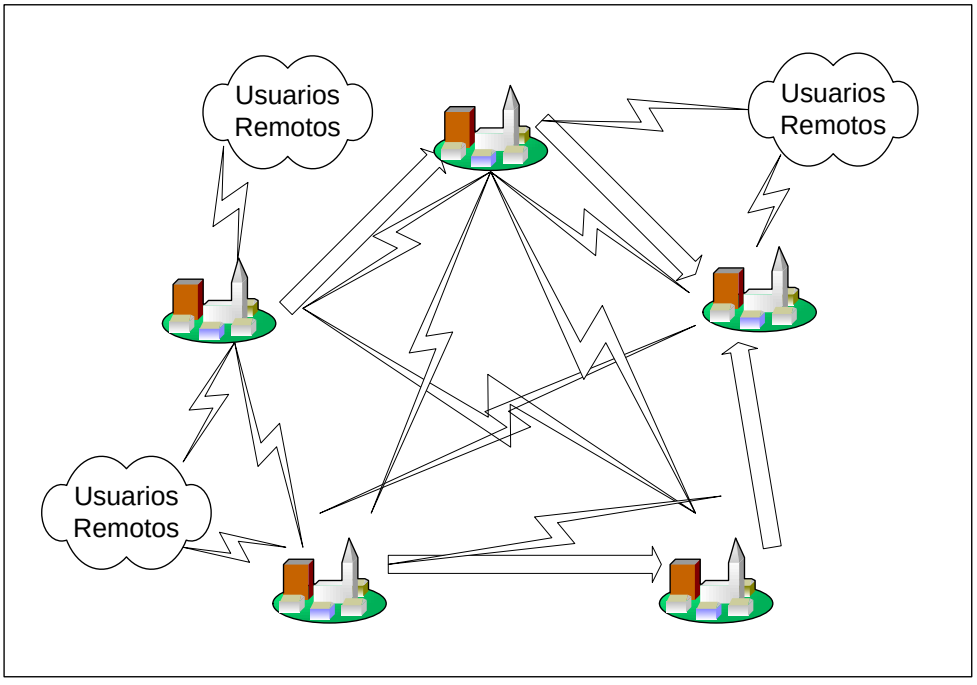


Figura 1.7.- WAN con líneas rentadas y de marcación

En cambio en la figura 1.8 se muestra la misma red WAN con la arquitectura de redes privadas virtuales a través de un ISP. Se puede observar que el diseño se simplifica enormemente y todo lo que corresponde al tráfico de información se

encarga el Internet, haciendo más fácil la conectividad y la escalabilidad de la red.

Este es uno de los principales beneficios en el diseño de redes WAN con arquitectura VPN. Es por eso que esta tecnología cada vez tiene más adeptos a nivel mundial.

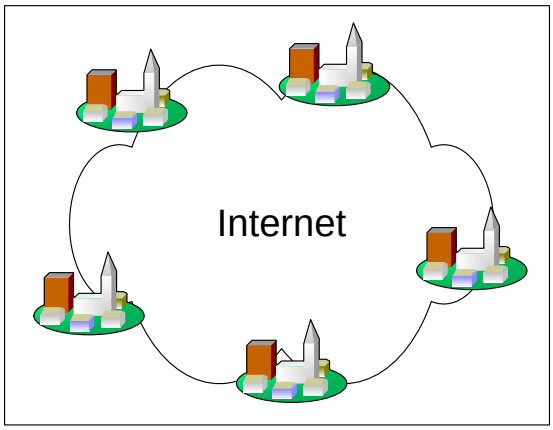


Figura 1.8.- WAN con internet como enlace.

Beneficios para el usuario final.- El usuario final se ve muy beneficiado ya sea un usuario que pertenezca a la propia empresa o un cliente.

En la actualidad las empresas deben llegar al cliente, sin importar donde se encuentre éste, es por eso que se hace necesario que el cliente tenga acceso a los servicios y ya no se lo haga con comunicaciones telefónicas de larga distancia que son muy costosas, sino a través de un ISP local con un enlace más eficiente y menos costoso y además un enlace que va a estar disponible las 24:00h al día los 365 días del año.

El mismo beneficio tendrán los usuarios remotos, facilitándoles el acceso a la información de la empresa en el momento que lo deseen, independiente del lugar en el que se encuentren.

CAPITULO II

PROTOCOLOS TCP/IP

2.1.- Introducción
2.2.- Arquitectura de TCP/IP
2.3.- Capa de Interfaz de Red
2.4.- Capa de Internet
2.5.- Capa de Transporte
2.6.- Capa de Aplicación

2.1.- Introducción.

TCP/IP (Transmisión Control Protocol / Internet Protocol) es un grupo de protocolos estándares de la industria diseñados para redes. Se ha convertido en el protocolo más popular debido a que es utilizado por Internet y esta muy extendido en los sistemas operativos.

TCP/IP se ha convertido en el conjunto de protocolos de red disponible más adaptable por el medio del cual se puede trabajar casi en cualquier medio de Red, Hardware y Sistema Operativo existente, desde una pequeña LAN de grupo de trabajo, hasta la conexión de millones de sistemas que componen la propia Internet.

Historia de TCP/IP.

En 1969, la Agencia de proyectos de investigación avanzada sobre defensa (DARPA) subvencionó un experimento en el que se enlazaron tres computadoras. El objetivo de este proyecto era el de proporcionar una tecnología fiable de trabajo en red que pudiera recuperarse frente a problemas y errores.

Originalmente se enlazaron tres sistemas entre sí con líneas alquiladas a la compañía telefónica y éstos utilizaban un protocolo llamado NCP (Protocolo de Control de Red, Network Control Protocol)

En 1973, la DARPA inició un programa de investigación de tecnologías de comunicación entre redes de diferentes características. El proyecto se basaba en la transmisión de paquetes de información, y tenia por objetivo la interconexión de redes. De este proyecto surgieron dos redes: Una de investigación, ARPANET, y una de uso exclusivamente militar, MILNET.

Para comunicar las redes, se desarrollaron varios protocolos: El protocolo de Internet y los protocolos de control de transmisión. Posteriormente estos protocolos se englobaron en el conjunto de protocolos, los cuales dan lugar al modelo TCP/IP.

En 1980, se incluyo en el UNIX 4.2 de BERKELEY, y fue el protocolo militar estándar en 1983. Con el nacimiento en 1983 de INTERNET, este protocolo se populariza bastante, y su destino va unido al de Internet. ARPANET dejo de funcionar oficialmente en 1990[WWW01].

Algunos de los motivos de su popularidad son:

- ✓ Independencia del fabricante
- ✓ Soporta múltiples tecnologías
- ✓ Puede funcionar en maquinas de cualquier tamaño
- ✓ Estándar de EEUU desde 1983
- ✓ Su destino está ligado a Internet

La arquitectura de un sistema en TCP/IP tiene una serie de metas:

- ✓ La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura del ordenador
- ✓ Conectividad Universal a través de la red
- ✓ Reconocimientos de extremo a extremo
- ✓ Protocolos estandarizados

2.2.- Arquitectura de TCP/IP.

El modelo ISO/OSI (Organización de Estándares Internacionales para la Interconexión de Sistemas Abiertos) utiliza siete capas para organizar una red dentro de módulos funcionales y bien definidos.

Los diseñadores de redes utilizan las descripciones del modelo de estas capas para construir redes reales. En una red por capas, cada módulo (o capa) proporciona funcionalidad específica o servicios a sus capas adyacentes. Además cada capa esta protegida por otras capas arriba de ellas para detalles de implementación de nivel más bajo. Cada capa hace una interfaz sólo con la siguiente capa en la red.

La arquitectura de Internet esta basada en capas. Esto hace más fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura.

Los protocolos TCP/IP mapean un modelo conceptual de cuatro capas conocido como el modelo DARPA, denominado así por la agencia del gobierno de los Estados Unidos que inicialmente desarrolló TCP/IP. Las cuatro capas en el modelo DARPA corresponden a una o más capas del modelo de siete capas de Interconexiones de Sistemas Abiertos (Open Systems Interconnection, OSI). Figura 2.1 [WWW02]

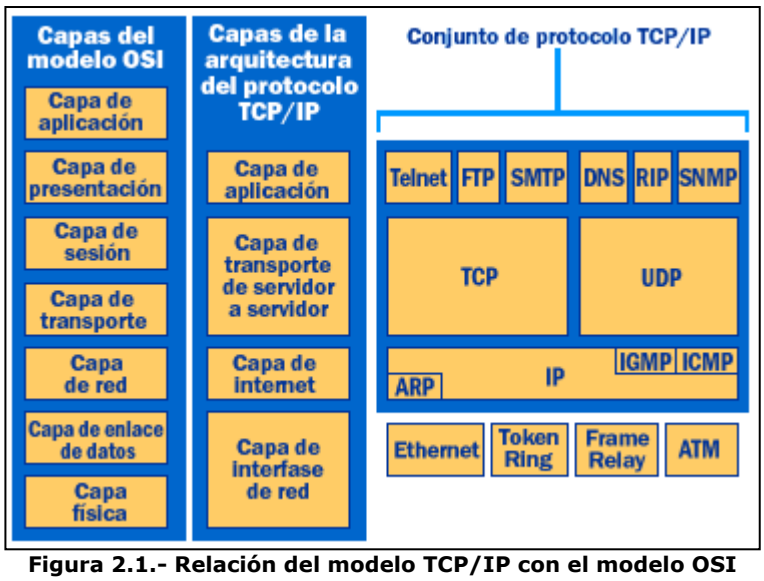


Figura 2.1.- Relación del modelo TCP/IP con el modelo OSI

2.3.- Capa de Interfaz de red.

La capa de interfaz de red (también llamada la capa de acceso a la red) es responsable de colocar los paquetes TCP/IP en el medio de la red y de recibir los paquetes TCP/IP del medio de la red.

El TCP/IP fue diseñado para ser independiente del método de acceso a la red, del formato del cuadro (frame) y del medio. De este modo, el TCP/IP puede ser utilizado para conectar diferentes tipos de red. Esto incluye tecnologías de LAN,

tales como Ethernet o Token Ring y tecnologías de WAN tales como X.25 o Frame Relay. La independencia de cualquier tecnología de red específica le da al TCP/IP la habilidad de ser adaptado a las nuevas tecnologías tales como Asynchronous Transfer Mode (ATM).

La capa de interfaz de red comprende a las capas de enlace de datos y física del modelo OSI. Note que la capa de Internet no aprovecha los servicios de secuenciación y la confirmación que pudieran estar presentes en la capa de enlace de datos. Se asume una capa de interfaz de red no confiable, y la comunicación confiable es responsabilidad de la capa de transporte, a través del establecimiento de la sesión y la confirmación de paquetes.

La capa física en una red TCP/IP es idéntica a la capa física del modelo ISO/OSI, la cual incluye el medio de transmisión que transporta los datos por la red. Este medio es casi siempre algún tipo de cable coaxial, par trenzado o fibra óptica. El modelo TCP/IP no considera oficialmente el medio hardware como componente específico en su diseño. TCP/IP tiende a agrupar la interfaz hardware con el nivel de interfaz de red.

Independientemente del medio hardware que se utilice, se necesitará una tarjeta de interfaz de red específica. Estos dispositivos de interfaz de red son específicos del medio hardware por el que se transmiten las señales. Cada uno de estos servicios necesita un componente software llamado controlador de dispositivo. En la mayoría de los sistemas operativos de red, el controlador de dispositivo debe incluirse con el sistema operativo de base o proporcionarlo el fabricante del hardware.

La capa de enlace incluye una interfaz de hardware y dos módulos de protocolos: El Protocolo de Resolución de Direcciones (ARP) y el Protocolo de Resolución de Direcciones Inverso (RARP).

Las direcciones Ethernet (a nivel físico) son de seis bytes de longitud, mientras las direcciones IP son de cuatro bytes. Todos los datos transmitidos a través de la red mediante tecnología Ethernet deben utilizar tramas de datos Ethernet; las tarjetas de interfaz Ethernet observan las tramas en la red en busca de sus

propias direcciones Ethernet. Las tarjetas de interfaz no saben ni se preocupan por la dirección IP.

En otras palabras, los protocolos de TCP/IP sólo funcionan con direcciones IP; las tramas Ethernet con direcciones Ethernet. Estos diferentes tipos de direcciones representan un problema de comunicación en la red. Los protocolos de Resolución de Direcciones y de Resolución de Direcciones Inverso solucionan este problema analizando las direcciones: traducen las direcciones IP a direcciones de la capa de enlace y viceversa.

Protocolo resolución de direcciones (ARP)

El encaminamiento en el entorno de la red local utiliza el protocolo ARP que relaciona el nivel de red IP con los niveles inferiores. El protocolo ARP se usa para traducir las direcciones IP (lógicas) en direcciones de la red local (físicas).

El proceso ARP.

El IP envía información al ARP. El ARP recibe el paquete IP, la dirección IP de redireccionamiento, y la interfaz a ser utilizada para redireccionar el paquete. Independientemente de si se ejecuta una entrega directa o indirecta, el ARP ejecuta los siguientes procesos tal como se visualiza en la figura 2.2.

- ✓ Basado en la interfaz y en la dirección IP de redireccionamiento, el ARP consulta el caché ARP apropiado buscando un elemento para la dirección IP de redireccionamiento. Si se encuentra un elemento, el ARP salta hasta el último paso.
- ✓ Si no se encuentra una coincidencia, el ARP construye un cuadro ARP de petición conteniendo la dirección MAC de la interfaz que envía la petición ARP y la dirección IP de redireccionamiento. El ARP entonces transmite la petición ARP enviando un mensaje a toda la red utilizando una dirección de "difusión".
- ✓ Todos los servidores reciben el cuadro transmitido y la petición ARP es procesada. Si la dirección IP del servidor que recibe coincide con la dirección IP solicitada (la dirección IP de redireccionamiento), su

caché ARP es actualizado con la dirección de quién envía la petición ARP. Si la dirección IP del servidor que recibe no coincide con la dirección IP solicitada, la petición ARP es descartada silenciosamente.

- ✓ Se formula una respuesta ARP conteniendo la dirección MAC solicitada y es enviada directamente a quien envió la solicitud ARP.
- ✓ Cuando la respuesta ARP es recibida por quien envió la solicitud ARP, actualiza su caché ARP con la dirección. Entre la petición ARP y la respuesta ARP, ambos servidores ahora tienen las direcciones del otro en sus cachés ARP.
- ✓ El paquete IP es enviado a la dirección MAC del servidor de redireccionamiento al indicarle que convierta la dirección MAC

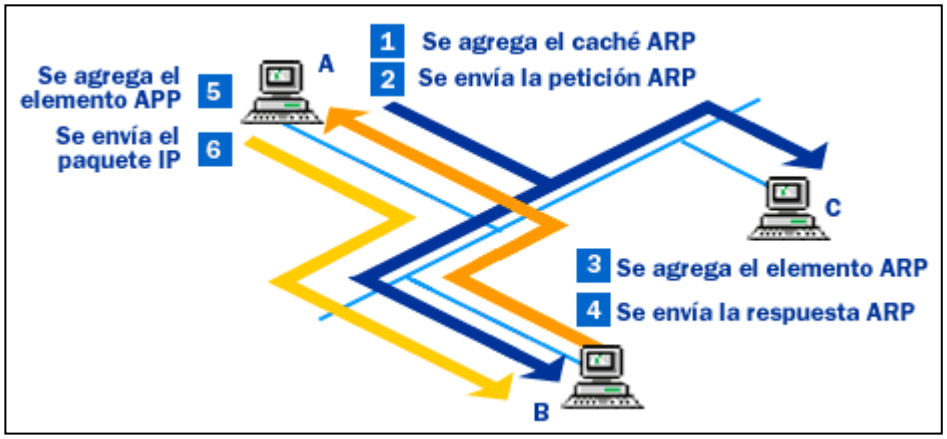


Figura 2.2.- El Proceso ARP

Las implementaciones del protocolo ARP incorporan Buffers con las tablas de correspondencia entre direcciones IP y direcciones físicas de la red, de forma que se reduce el número de consultas que se deben realizar [WWW02].

Protocolo de Resolución de Direcciones Reversa (RARP)

El protocolo RARP (Reverse Address Resolution Protocol) es el encargado de asignar una dirección física a una dirección lógica (IP).

Los desarrolladores de TCP/IP diseñaron RARP para que lo usaran computadoras sin disco duro. Por ejemplo, una estación de trabajo sin disco puede leer la

dirección de su capa de enlace de su tarjeta de interfaz de red y solicitar a otro sistema que le cargue el sistema operativo [LIB01].

2.4.- Capa de Internet.

La capa de Internet es el corazón de cualquier red basada en el protocolo TCP/IP. La capa de Internet en el modelo TCP/IP es análoga a la capa de red en el modelo ISO/OSI.

Esta capa incluye el protocolo Internet (IP), el protocolo de control de mensajes de Internet (ICMP, Internet Control Message Protocol) y el protocolo de manejo de grupos de Internet (IGMP; Internet Group Management Protocol). IP hace casi todo el trabajo dentro de la capa de Internet. ICMP e IGMP son protocolos de apoyo para IP, pues lo ayudan a manejar los mensajes especiales de la red, como los de error y de transmisiones múltiples (mensajes enviados a dos o más sistemas).

Además la capa de Internet controla la comunicación entre un equipo y otro. Conforma los paquetes IP que serán enviados por la capa inferior, desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación.

2.4.1.- IP (Internet Protocol).

El protocolo de Internet (Internet Protocol, IP) es un protocolo enrutable responsable del direccionamiento IP, de la fragmentación y ensamble de los paquetes y su unidad básica de transferencia de datos es el datagrama.

El IP es un protocolo de datagramas no confiable, sin conexión y principalmente responsable del direccionamiento y enrutamiento de los paquetes entre servidores. Sin conexión significa que una sesión no se establece antes de intercambiar los datos. No confiable significa que la entrega no está garantizada. El IP siempre hace un mejor esfuerzo para intentar entregar un paquete. Un

paquete IP podría perderse, entregarse fuera de secuencia, duplicado o retrasado. El IP no intenta recuperarse de este tipo de errores. La confirmación de la entrega de los paquetes y la recuperación de paquetes perdidos es responsabilidad de un protocolo de alguna capa superior, tal como el TCP.

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta, o fragmentados intencionadamente para permitir que un nodo con un buffer limitado pueda coger todo el datagrama. Es la responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la máquina origen (esto lo hace el protocolo ICMP).

El protocolo IP también define cual será la ruta inicial por la que serán mandados los datos.

Cuando los datagramas viajan de unos equipos a otros, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (Maximum Transmission Unit), y ninguna red puede transmitir un paquete de tamaño mayor a esta MTU. El datagrama consiste en una cabecera y datos [RFC791].

Direcciones IP

Cada nodo TCP/IP está identificado por una dirección IP lógica. La dirección IP es una dirección de la capa de red y no tiene dependencia sobre la dirección de la capa de enlace de datos (tal como una dirección MAC de una tarjeta de interfaz de red). Una dirección IP única es necesaria para cada servidor y componente de red que se comunique usando TCP/IP.

Las direcciones IP hacen que el envío de datos entre ordenadores se haga de forma eficaz, de un modo similar al que se utilizan los números de teléfono.

Las direcciones IP tienen 32 bits, formados por cuatro campos de 8 bits separados por puntos. Cada campo puede tener un valor comprendido entre 0 y 255. Esta compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host, la cual debe ser única.

La comunidad de Internet originalmente definió cinco clases de direcciones para acomodar redes de diferentes tamaños. La clase de direcciones define cuales bits son usados para el identificador de red y cuales bits son usados para el identificador de servidor. También define el número posible de redes y el número de servidores por red [LIB01].

- ✓ La clase A contiene 7 bits para direcciones de red (bit de orden alto siempre es igual a cero), con lo que permite tener hasta 128 redes. Los 24 bits restantes representan el identificador del host, lo cual permite tener 16.777.216 ordenadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0. y 127.255.255.255. y la mascara de subred será 255.0.0.0. La figura 2.3 ilustra la estructura de las direcciones de clase A.

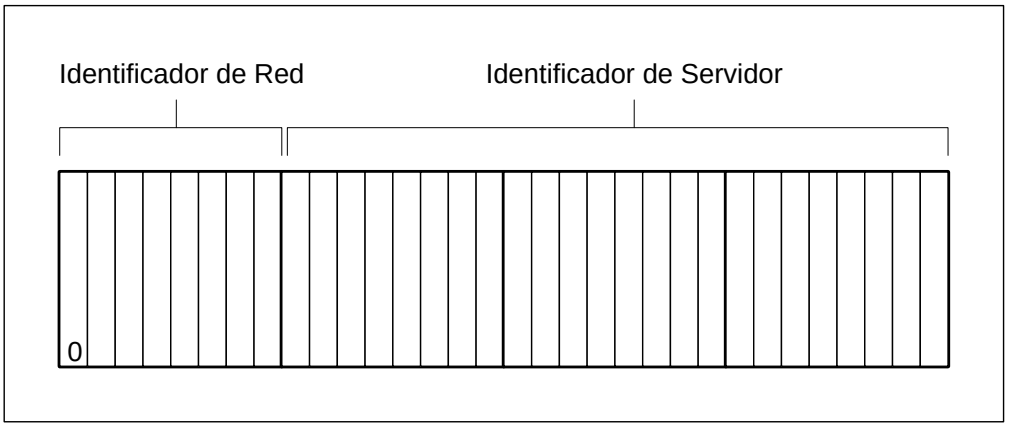


Figura 2.3.- Formato de Dirección IP Clase A

- ✓ La clase B contiene 14 bits para direcciones de red (los dos bits de orden más alto en una dirección de clase B son siempre iguales al binario 10) y 16 bits para direcciones de hosts. El número máximo de redes es 16.536 redes, con 65.536 ordenadores por red. Las direcciones estarán comprendidas entre 128.0.0.0. y 191.255.255.255., y la mascara de subred será 255.255.0.0. La figura 2.4 ilustra la estructura de las direcciones de clase B.

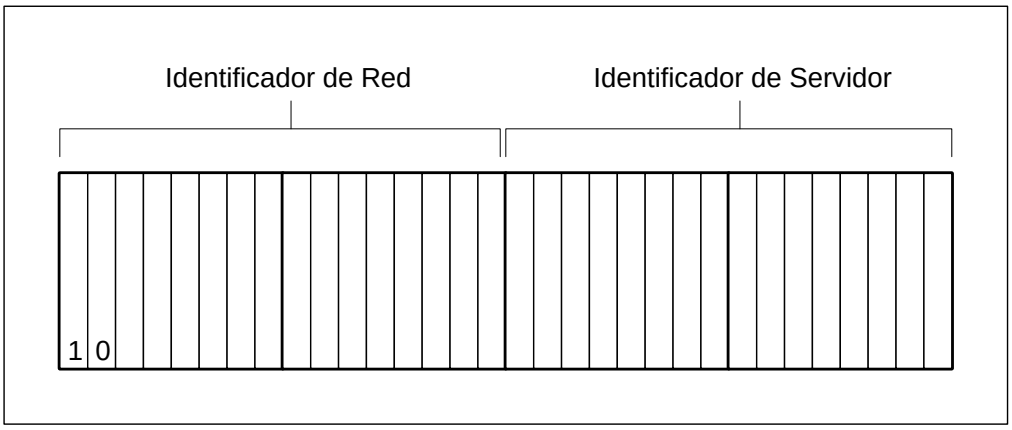


Figura 2.4.- Formato de Dirección IP Clase B

- ✓ La clase C contiene 21 bits para direcciones de red (los tres bits de orden más alto en una dirección de clase C son siempre iguales al binario 110) y 8 para hosts, lo que permite tener un total de 2.097.152 redes, cada una de ellas con 256 ordenadores. Las direcciones estarán comprendidas entre 192.0.0.0. y 223.255.255.255. y la mascara de subred será 255.255.255.0. La figura 2.5 ilustra la estructura de las direcciones de clase C.

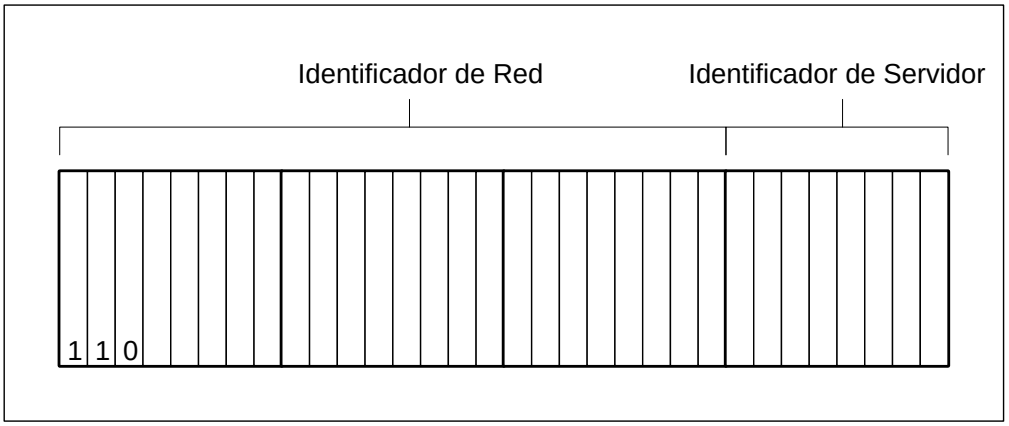


Figura 2.5.- Formato de Dirección IP Clase C

- ✓ La clase D se reserva todas las direcciones para multidestino (multicast), es decir, un ordenador transmite un mensaje a un grupo específico de ordenadores de esta clase. Los cuatro bits de orden más alto son siempre iguales al binario 1110. Las direcciones estarán comprendidas entre 224.0.0.0. y 239.255.255.255.

- ✓ La clase E se utiliza exclusivamente para fines experimentales. Los bits de orden más alto en la dirección de clase E son iguales a 1111. Las direcciones están comprendidas entre 240.0.0.0. y 247.255.255.255.

La tabla 2.1 es un resumen de las clases de direcciones A, B y C que pueden ser utilizados para direcciones de servidores IP [WWW02].

Clase	Valor para w	Porción del identificador de red	Porción del identificador de servidor	Redes disponibles	Servidores por red
A	1-126	w	x.y.z	128	16,777,216
B	128-191	w.x	y.z	16,384	65,536
C	192-223	w.x.y	z	2,097,152	256

Tabla 2.1. Resumen de las direcciones de clases IP

La dirección de clase A 127.x.y.z está reservada para las pruebas de loopback y para la comunicación interprocesos en la computadora local.

El identificador de red identifica a los servidores TCP/IP que están localizados en la misma red física. Todos los host en la misma red física deben tener asignado el mismo identificador de red para comunicarse unos con otros.

Siga estas guías cuando asigne el identificador de red:

- ✓ La dirección de red debe ser única dentro de la red IP. Si planea tener una conexión enrutada directa a Internet, el identificador de red debe ser único en Internet. Si no planea conectarse a internet, el identificador de red debe ser único en su red privada.
- ✓ El identificador de red no puede empezar con el número 127. El número 127 es una dirección de clase A reservada para funciones loopback internas.
- ✓ Todos los bits dentro del identificador de red no pueden ser iguales a 1. Todos los 1's en el identificador de red son reservados para una dirección de transmisión IP.
- ✓ Todos los bits dentro del identificador de red no pueden ser iguales a 0. Todos los 0's en identificador de red son utilizados para denotar un servidor específico en la red local y no serán enrutados.

La tabla 2.2 lista los rangos válidos de identificadores de red basados en las clases de direcciones IP. Para denotar identificadores de red IP, los bits del servidor son todos iguales a 0. Note que aunque esté expresado en notación decimal punteada el identificador de red no es una dirección IP.

Clase de dirección	Primer identificador de red	Ultimo identificador de red
Clase A	1.0.0.0	126.0.0.0
Clase B	128.0.0.0	191.255.0.0
Clase C	192.0.0.0	223.255.255.0

Tabla 2.2.- Rangos de las clases de identificadores de red

Los identificadores de servidor identifican un servidor TCP/IP dentro de una red. La combinación del identificador de red y del identificador de red IP es una dirección IP

Siga estas guías para asignar un identificador de servidor:

- ✓ El identificador de servidor debe ser único para el identificador de red.
- ✓ Todos los bits dentro del identificador del servidor no pueden ser iguales a 1, porque este identificador está reservado como una dirección de transmisión para enviar un paquete a todos los servidores de una red.
- ✓ Todos los bits en el identificador de red no pueden ser iguales a 0 porque este identificador de servidor está reservado para denominar el identificador de red IP.

La tabla 2.3 lista los rangos válidos de identificador de servidor basados en las clases de direcciones IP.

Clase de dirección	Primer identificador del servidor	Ultimo identificador del servidor
Clase A	w.0.0.1	w.255.255.254
Clase B	w.x.0.1	w.x.255.254
Clase C	w.x.y.1	w.x.y.254

Tabla 2.3. Rangos de clase de los identificadores de servidor

IP (Internet Protocol) Versión 6

Esta es una nueva versión del protocolo IP, llamada IPv6, aunque también es conocida como IPng (Internet Protocol Next Generation). Es la versión 6, debido a que la número 5 no pasa de la fase experimental. La compatibilidad con la versión 4 es prácticamente total, ya que se han incluido características de compatibilidad. Algunas de las modificaciones, están encaminadas a mejorar la seguridad en la red, que apenas existía en la versión 4.

Direcciones IP Versión 6 (Ipv6)

El cambio más significativo en las direcciones ha sido, que ahora, se refieren a una interfaz y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a estos mediante su interfaz.

El número de direcciones diferentes se ha multiplicado de una manera exagerada. Teóricamente, es posible tener 2128 direcciones diferentes. Este número quiere decir que se podrían llegar a tener más de 665.000 trillones de direcciones por metro cuadrado, aunque si siguieran una jerarquía, este número decrece hasta 1564 direcciones por metro cuadrado en el peor caso o tres trillones siendo optimistas [RFC2460].

En el IPv6 existen tres tipos básicos de direcciones:

- ✓ **Direcciones unicast:** Están dirigidas a una única interfaz en la red. Actualmente se dividen en varios grupos, y existe un grupo especial que facilita la compatibilidad con las direcciones de la versión 4.
- ✓ **Direcciones anycast:** Identifican a un conjunto de interfaces de red. El paquete se enviara a cualquier interfaz que forme parte del conjunto. En realidad son direcciones unicast que se encuentran asignadas a varias interfaces.

- ✓ **Direcciones multicast:** Identifican a un conjunto de interfaces de la red, de manera que cada paquete es enviado a cada uno de ellos individualmente.

Internet 2

El Internet de ayer

Tenía miles de usuarios, se utilizaba para conexiones remotas y transferencias de archivos, aplicaciones que capitalizaban la tecnología subyacente, era usada de manera experimental.

El Internet de hoy

Tiene cientos de millones de usuarios, sus aplicaciones principales son el web, el correo electrónico, así como audio y vídeo de baja calidad, adaptándose a la tecnología subyacente.

El Internet del mañana

Tendrá miles de millones de usuarios y dispositivos conectados, las aplicaciones de hoy serán complementadas con ambientes multimedia en tiempo real.

Las nuevas tecnologías posibilitarán aplicaciones hoy inimaginables, que crearán nuevos retos. Dado que la Internet actual no fue diseñada para millones de usuarios sin congestión, ni es capaz de manejar multimedia o interacción a tiempo real y sólo este medio puede permitir el crecimiento explosivo y permitir la convergencia de información, trabajo, medios masivos y colaboración humana, se han creado en varios países proyectos que nos pueden llevar a una nueva generación de Internet.

Internet 2, http://www.internet2.org/, es el nombre de un proyecto en los Estados Unidos de América que tiene como propósito crear una red avanzada para investigación y educación, que utilice tecnología de punta, para permitir el desarrollo de una nueva generación de aplicaciones. Se contempla una rápida

transferencia de tecnología de Internet 2 al Internet comercial. Por extensión, es el nombre genérico para redes avanzadas similares en otros países.

El desarrollo de nuevas capacidades requiere de un esfuerzo de experimentación, capacitación e innovación que posteriormente se incorporarán a las corrientes principales y a los servicios que se entreguen a los usuarios de Internet.

Este desarrollo de nuevas capacidades es el objetivo del Internet 2, que es el desarrollo y operación de una red de alta anchura de banda y controles avanzados, construida y operada en su inicio por universidades, gobierno y algunas empresas del ramo de tecnologías de la información, cuyos productos se incorporarán a las prácticas usuales de Internet en plazos que van de uno a cinco años, con el beneficio adicional de producir personal altamente calificado para la innovación y aplicación de estos productos y un alto grado de dominio nacional de los avances tecnológicos asociados.

Si bien el nombre corresponde inicialmente a un proyecto cuyo primer desarrollo ocurrió en Estados Unidos de América, se ha detonado también en otros países. Su avance en responde a necesidades nacionales bien identificadas y permite a las instituciones de educación superior incorporarse a la causa del desarrollo nacional de manera eficaz. Estos requerimientos se ubican principalmente en la educación a todos los niveles y modalidades, en la atención a la salud, el desarrollo tecnológico en otras ramas de la industria y los servicios, y la prestación amplia de servicios basados en información para la sociedad.

En octubre de 1996 se inició formalmente el proyecto Internet 2 (http://www.internet2.edu/). En octubre de 1997 se formó la UCAID (University Corporation for Advanced Internet Development), integrada por mas de 120 universidades en los Estados Unidos de América con la misión de facilitar y coordinar el desarrollo, implantación, operación y transferencia de tecnología de redes y aplicaciones avanzadas, enfocadas a la investigación y educación. Y acelerar la disponibilidad de nuevos servicios y aplicaciones en Internet. En abril de 1998 se lanzó Abilene, red avanzada desarrollada por UCAID en sociedad con Qwest Communications, Northern Telecom y Cisco Systems . Este proyecto proporcionará la red para soportar Internet 2, utilizando facilidades Sonet de alta

velocidad, ruteadores IP sobre Sonet y una red de fibras ópticas de amplia cobertura. En los Estados Unidos de América, existe además la red VBNS (Very High Speed Backbone Network Service) de la NSF (National Science Foundation), que es exclusiva para la investigación. Tanto Abilene como VBNS proporcionan conectividad para los llamados gigapops (puntos de presencia regionales para redes avanzadas) que están instalando las principales universidades de los Estados Unidos de América.

Inicialmente, los enlaces se plantearon de 2.4Gb/s (OC 48), para evolucionar en corto tiempo a 9.6 Gb/s (OC 192). Internet 2 contempla diseñar, construir y operar una red avanzada (que pueda soportar aplicaciones que requieren un ancho de banda mayor al soportado por las actuales) [WWW03].

2.4.2.- Fragmentación y ensamblado.

Las tecnologías de red, tales como Ethernet, especifican una Unidad de transferencia Máxima (MTU). La MTU define el tamaño máximo del paquete que puede transmitir la red. Cuando una aplicación transmite el paquete más grande que la MTU de la red, el software de red automáticamente divide el paquete en pedazos más pequeños y transmite los datos como múltiples paquetes. Los campos candidatos a ser fragmentados del encabezado IP, tales como identificación, Banderas y Reproducción de fragmentos, son actualizados para indicar que el paquete es un fragmento y en que orden debe ser reensamblado.

Cuando el anfitrión destino recibe los paquetes IP fragmentados, un contador de reensamble se inicia. Todos los fragmentos deben llegar antes que el contador expire, de otra forma el anfitrión descartará todos los fragmentos. Debido a que la fragmentación y reensamble ocurren entre las capas de red y enlace de su red, el proceso es normalmente transparente.

2.4.3.- Internet Control Message Protocol (ICMP).

El Protocolo de Mensajes de control de Internet (ICMP) proporciona servicios de resolución de problemas y de reporte de errores para los paquetes que no son entregables. Por ejemplo si el IP es incapaz de entregar un paquete al servidor destino, el ICMP enviará un mensaje de Destino Inalcanzable (Destination Unreachable) al servidor origen.

Internet es un sistema autónomo que no dispone de ningún control central. El protocolo ICMP (Internet Control Message Protocol), proporciona el medio para que el software de hosts y gateways intermedios se comuniquen. El protocolo ICMP tiene su propio número de protocolo (número 1), que lo habilita para utilizar el IP directamente. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Los mensajes de error de este protocolo los genera y procesa TCP/IP, y no el usuario[RFC792].

ICMP provee reporte de mensajes y errores. Por ejemplo, si IP no es capaz de entregar un paquete en el host destino, ICMP envía un mensaje de "destino no encontrado" (destination unreachable) al nodo emisor. Los mensajes más comunes de ICMP se podrá observar en la tabla 2.4.

Mensaje	Tipo	Función
Echo request	8	Mensaje simple para resolución de problemas. Usado por PING para encontrar un host.
Echo reply	0	Usado por PING para confirmar que un nodo ha sido encontrado.
Redirect	5	Enviado por un enrutador para informar a un host que envía de una mejor ruta hacia el IP destino. Informa al nodo de una ruta preferida.
Source quench	4	Informa al nodo disminuir la cantidad de datagramas debido a congestionamiento en la red.
Destination unreachable	3	Informa al nodo que el datagrama no pudo ser entregado.

Tabla 2.4.- Mensajes más comunes de ICMP

Hay una serie de mensajes Destination Unreachable del ICMP. La tabla 2.5 describe los mensajes Destination Unreachable del ICMP más comunes.

Mensajes *Destination Unreachable*	**Descripción**
Network Unreachable	Enviado por un enrutador IP cuando una ruta a la red destino no pudo ser encontrada.
Host Unreachable	Enviado por un enrutador IP cuando un servidor destino en la red destino no puede ser encontrado. Este mensaje solamente es utilizado con tecnologías de red orientadas a conexiones (enlaces WAN). Los enrutadores IP con tecnologías de red sin conexión (tales como Ethernet y Token Ring) no envían mensajes Host Unreachable.
Protocol Unreachable	Enviado por el nodo IP destino cuando el campo Protocolo en la cabecera IP no puede ser apareado con un protocolo del cliente IP a actualmente cargado.
Port Unreachable	Enviado por un nodo IP destino cuando el Puerto Destino (Destination Port) en la cabecera IP no puede ser apareado con un proceso que utilice ese puerto.
Fragmentation Needed and DF Set	Enviado por un enrutador IP cuando la fragmentación debe de ocurrir pero no es permitida debido a que el valor de la bandera No Fragmentar (Don't Fragment, DF) en la cabecera IP fue activada por el nodo origen.

Tabla 2.5.- Mensajes Destination Unreachable del ICMP comunes.

Los mensajes de ICMP están contenidos en datagramas IP. Esto asegura que el mensaje ICMP será ruteado al nodo apropiado. El destino de un mensaje ICMP es siempre un módulo de software de la capa de red. El módulo ICMP en la capa IP del destino determina si debe pasar el mensaje a cualquiera de los módulos de software del nivel superior.

ICMP sólo proporciona servicios para notificar errores, es decir que no proporciona ningún servicio de corrección de errores, además, no especifica ninguna acción que los módulos de software de la capa de red deben tomar en respuesta a los errores que reporta[WWW02].

2.4.4.- Protocolo de Manejo de Grupos De Internet (IGMP).

El Protocolo de Administración de Grupos de Internet (Internet Group Management Protocol, IGMP) es un protocolo que administra la membresía de

los host en los grupos IP multicast. Un grupo IP multicast, también conocido como un grupo de hosts (host group), es un conjunto de hosts que escuchan el tráfico IP destinado a una dirección IP multicast específica. El tráfico IP multicast es enviado a una sola dirección MAC pero es procesado por múltiples hosts IP. Un hosts dado escucha en una dirección IP multicast específica y recibe todos los paquetes de esa dirección IP.

EL IGMP (Internet Group Management Protocol) es un protocolo que funciona como una extensión del protocolo IP. Se utiliza exclusivamente por los miembros de una red multicast para mantener su status de miembros, o para propagar información de direccionamiento.

Un Gateway multicast manda mensajes una vez por minuto como máximo. Un Host receptor responde con un mensaje IGMP, que marca al Host como miembro activo. Un Host que no responde al mensaje se marca como inactivo en las tablas de direccionamiento de la red multicast.

Para aplicaciones como conferencias interactivas, se utiliza la transmisión múltiple, y de esta manera se puede enviar información a varios pero no necesariamente a todos los receptores en la red. Los anfitriones y los receptores que soportan la transmisión múltiple usan el módulo del Protocolo de Manejo de Grupos De Internet (IGMP) [RFC3228]

2.5.- Capa de Transporte.

La capa de transporte es responsable de proporcionar a la capa de aplicación los servicios de comunicación de sesión y datagrama. Los protocolos base de la capa de transporte son el TCP y el Protocolo de Datagramas de Usuario (User Datagram Protocol, UDP).

- ✓ El TCP (Transport Control Protocol) proporciona un servicio de comunicación confiable, orientado a conexión, uno a uno, este protocolo proporciona un circuito virtual para comunicaciones de red El TCP es responsable del establecimiento de una conexión TCP, la

secuenciación y la confirmación de los paquetes enviados, y de la recuperación de los paquetes perdidos durante la transmisión.

- ✓ El UDP (User Datagrama Protocol) proporciona servicios de comunicación no confiables, uno a uno o de uno a muchos, sin conexión. El UDP es utilizado cuando la cantidad de datos a ser transferidos es pequeña (tales como datos que pueden caber dentro de un paquete único), cuando la carga de establecer la conexión no es deseable o cuando la aplicación o los protocolos de capas superiores proporcionan una entrega confiable.

La capa de transporte comprende las responsabilidades de la capa de transporte OSI y algunas de las responsabilidades de la capa de sesión OSI.

Un puerto es como una dirección IP, excepto que TCP/IP asocia un puerto a un protocolo en lugar de a una computadora anfitrión. En la misma forma que los datagramas IP almacenan direcciones IP fuente y destino, los protocolos de transporte almacenan números de puerto fuente y destino. En pocas palabras, los programas de red asocian un puerto de protocolo Internet con una aplicación y función específicas.

Como protocolo sin conexión y no confiable, UDP simplemente deposita datos en el puerto. UDP no mantiene una conexión entre el emisor y el receptor. En contraste, TCP esta orientado a conexión. TCP mantiene una conexión mientras sé esta comunicando. Además, TCP puede abrir múltiples conexiones en el mismo puerto.

2.5.1.- Protocolo de Datagrama de Usuario (UDP).

El UDP proporciona un servicio de datagrama sin conexión que ofrece entrega no confiable, de mejor esfuerzo de los datos transmitidos en los mensajes. Esto significa que la llegada de los datagramas no está garantizada; ni que la entrega de los paquetes esté en la secuencia correcta. El UDP no se recupera de la pérdida de datos utilizando retransmisión. El UDP está definido en el RFC 768.

El protocolo UDP (User Datagram Protocol) proporciona aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio es muy parecido al protocolo IP en el sentido de que no es fiable y no esta orientado a la conexión. El UDP es simple, eficiente e ideal para aplicaciones como el TFTP, el DNS, el servicio de nombres NetBIOS, el servicio de datagramas de NetBIOS y el Protocolo Simple de Administración de Redes (Simple Network Management Protocol, SNMP). Una dirección IP sirve para dirigir el datagrama hacia una maquina en particular, y el número de puerto de destino en la cabecera UDP se utiliza para dirigir el datagrama UDP a un proceso específico localizado en la cabecera IP. La cabecera UDP también contiene un número de puerto origen que permite al proceso recibido conocer como responder al datagrama. La tabla 2.6 describe los campos clave en la cabecera UDP.

Campo	Función
Puerto origen	Puerto UDP del servidor que envía.
Puerto destino	Puerto UDP del servidor destino.
Suma de verificación UDP	Verifica la integridad de la cabecera UDP y de los datos UDP.
Número de confirmación	El número de secuencia del byte que el que envía espera recibir del otro lado de la conexión.

Tabla 2.6. Campos claves en la cabecera UDP.

Para usar el UDP, una aplicación debe proporcionar la dirección IP y el número de puerto UDP de la aplicación destino. Un puerto proporciona una localización para los mensajes que se envían. Un puerto funciona como una cola de mensajes multiplexada, significando que puede recibir múltiples mensajes a la vez. Cada puerto está identificado por un número único. Es importante notar que los puertos UDP son distintos y separados de los puertos TCP, incluso aunque algunos de ellos usen el mismo número. La tabla 2.7 lista algunos puertos UDP bien conocidos[RFC768].

Número de puerto UDP	Descripción
53	Petición de nombre para el Sistema de Nombres de Dominio (Domain Name System, DNS).
69	Protocolo Trivial de Transferencia de Archivos (File Transfer Protocol, TFTP).
137	Servicios de nombres NetBIOS.
138	Servicio de datagrama NetBIOS.
161	Protocolo Simple de Administración de Redes (Simple Network Management Protocol, SNMP).

Tabla 2.7.- Puertos UDP bien conocidos.

2.5.2.- Protocolo de Control de Transmisión TCP.

El protocolo TCP con el protocolo IP son los que con mayor frecuencia se utilizan en el conjunto de protocolos TCP/IP (de ahí el nombre)

El TCP es un servicio de entrega confiable, orientado a conexiones. Los datos son transmitidos en segmentos. Orientado a conexiones significa que una conexión debe establecerse antes de que el host intercambie datos. La confiabilidad es lograda asignando un número de secuencia a cada segmento transmitido. Se utiliza una confirmación para verificar que los datos fueron recibidos por el otro servidor. Para cada segmento enviado, el servidor que recibe debe regresar una confirmación (acknowledgment, ACK) dentro de un periodo específico de bytes recibidos. Si una ACK no es recibida, los datos son retransmitidos. El TCP está definido en el RFC 793.

El TCP utiliza comunicaciones de flujo de bytes (byte-stream), donde los datos dentro del segmento TCP son tratados como una secuencia de bytes sin límites de registro o de campo. La tabla 2.8 describe los campos claves en la cabecera TCP.

Campo	Función
Puerto origen	El puerto TCP del servidor que envía.
Puerto destino	El puerto TCP del servidor destino.
Número de secuencia	El número de secuencia del primer byte de datos en el segmento TCP.
Número de confirmación	El número de secuencia del byte que el que envía espera recibir del otro lado de la conexión.
Ventana	El tamaño actual de la memoria intermedia TCP en el servidor que envía este segmento TCP para almacenar segmentos que llegan.
Suma de verificación TCP	Verifica la integridad de la cabecera TCP y de los datos TCP .

Tabla 2.8.- Campos clave en la cabecera TCP.

Un puerto TCP proporciona una localización específica para entregar los segmentos TCP. Los números de puertos por debajo de 1024 son puertos bien conocidos y están asignados por la Autoridad de Número Asignados de Internet (Internet Assigned Numbers Authority, IANA) [RFC3232]. La tabla 2.9 lista algunos puertos TCP bien conocidos.

Número de puerto TCP	Descripción
20	FTP (Canal de datos).
21	FTP (Canal de control).
23	Telnet.
80	Protocolo de Transferencia de Hipertexto (HyperText Transfer Protocol, HTTP) utilizado para la Web.
139	Servicios de sesión NetBIOS.

Tabla 2.9.- Puertos TCP bien conocidos.

Para una lista completa de puertos TCP, referirise al RFC3232.

Al igual que el Protocolo de Datagrama de Usuario (UDP), TCP transporta datos entre las capas de red y de aplicación, pero es mucho más complejo que UDP, pues proporciona un servicio de entrega de datos confiable, de flujo de bytes y orientado a conexión; en otras palabras, TCP asegura la entrega, así como

también se encarga que la aplicación destino reciba los datos en la secuencia correcta. En contraste, UDP no garantiza la entrega de datagramas, ni que estos lleguen en la secuencia adecuada.

TCP también intenta optimizar el ancho de banda de la red. Para hacerlo, controla dinámicamente el flujo de datos entre las conexiones. Por lo tanto, si el buffer de datos en el lado receptor de la conexión TCP comienza a sobrecargarse, TCP indica al lado emisor que reduzca la velocidad de transmisión.

2.5.2.1.- Interfaces TCP.

Existen dos tipos de interfaces entre la conexión TCP y los otros programas:

- ✓ El primero es utilizar la pila de los programas de la capa de red. Como en esta capa solo esta el protocolo IP, la interfaz lo determina este protocolo.
- ✓ El segundo tipo es la interfaz del programa de usuario. Esta interfaz puede variar según el sistema operativo, pero en general tiene las siguientes características:

La interfaz envuelve el programa de usuario llamando a una rutina que introduce entradas en una estructura de datos llamada el Bloque de Control de Transmisión (TCB). Las entradas se realizan inicialmente en la pila de hardware y transferidas al TCB por medio de una rutina de sistema. Estas entradas permiten al TCP asociar un usuario con una conexión particular, de modo que pueda aceptar comandos de un usuario y mandarlos a otro usuario en la otra parte de la conexión. TCP utiliza unos identificadores únicos para cada parte de la conexión. Esto se utiliza para recordar la asociación entre dos usuarios. Al usuario se le asigna un nombre de conexión para utilizarlo en futuras entradas del TCB. Los identificadores para cada extremo de la conexión se llaman sockets. El socket local se construye concatenando la dirección IP de origen y el número de puerto de origen. El socket remoto se obtiene concatenando la dirección IP de destino y él número de puerto de destino.

El par de sockets de una conexión forman un único número en Internet. El UDP tiene los mismos sockets, pero no los recuerda. Esta es la diferencia entre un protocolo orientado a conexión y otro a no conexión. A continuación se explican los comandos más usuales:

- ✓ **Open:** Inicia una conexión o comienza a escuchar un socket. El usuario tiene un nombre de conexión local que actúa como un puntero dentro del TCB.
- ✓ **Send:** El comando Send manda datos del buffer especificado.
- ✓ **Receive**: El comando Receive es un mensaje de error si el nombre local proporcionado no es utilizado antes con el comando Open.
- ✓ **Close**: El comando Close hace que se cierre una conexión. Se produce un error si la conexión especificada no ha sido abierta, o si no se tiene autorización para cerrar la conexión.
- ✓ **Status**: El comando Status solo tiene una variable asociada, que es el nombre de la conexión.
- ✓ **Abort**: El comando Abort hace que todos los comandos Send y Receive asociados al nombre de la conexión local se interrumpan. La entrada del usuario del TCB se elimina y se envía un mensaje especial de reinicio a la entidad del otro lado de la conexión.

El TCP recuerda el estado de cada conexión por medio del TCB. Cuando se abre una conexión, se efectúa una entrada única en el TCB. Un nombre de conexión se le asigna al usuario para activar los comandos de la conexión. Cuando se cierra una conexión se elimina su entrada del TCB.

2.5.2.2.- Control de Flujo.

El protocolo TCP puede controlar la cantidad de datos que debe enviar mediante el campo Window. Este campo indica el número máximo de octetos que pueden ser recibidos. El receptor de un segmento con el campo window a cero, no puede enviar mensajes al emisor, excepto mensajes de prueba. Un mensaje de prueba es un mensaje de un solo octeto que se utiliza para detectar redes o hosts inalcanzables.

2.6.- Capa de Aplicación.

La capa de aplicación proporciona la habilidad de acceder a los servicios de otras capas y define los protocolos que las aplicaciones utilizan para intercambiar datos. Hay varios protocolos para la capa de aplicación y constantemente se están desarrollando nuevos protocolos.

Los protocolos de la capa de aplicación más ampliamente conocidos son aquellos usados para el intercambio de información del usuario, por ejemplo:

- ✓ El Protocolo de Transferencia de Hipertexto (HyperText Transfer Protocol, HTTP) es utilizado para transferir los archivos que componen las páginas de la Web. El servidor HTTP por defecto esta escuchando el puerto 80 y los datos son trasmitidos mediante el protocolo TCP.
- ✓ El Protocolo de transferencia de Archivos (File Transfer Protocol, FTP) es utilizado para la transferencia interactiva de archivos. Los servidores FTP son una forma conveniente de hacer disponibles al público informaciones, resúmenes de discusiones, investigaciones, programas y actualizaciones de software. El servidor FTP por defecto esta escuchando el puerto 21 y los datos son trasmitidos mediante el protocolo TCP.
- ✓ El Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol, SMTP) es utilizado para la transferencia de mensajes de correo y anexos. Por defecto el servidor SMTP esta escuchando el puerto 25 y los datos son trasmitidos mediante el protocolo TCP.
- ✓ POP3 (Protocolo de Oficina Postal) es un protocolo de correo Versión 3 (POP3), el cual fue creado para permitir a una red el acceso dinámico a una casilla sobre un servidor HOST de manera útil. Usualmente, esto significa que el protocolo POP3 es usado para dejar que una red recupere el correo que el servidor accionaría por él. normalmente, el correo es bajado y es borrado. Es un protocolo que fue diseñado para trabajar conjuntamente con el protocolo TCP, inicialmente el proceso está escuchando el puerto 110, a la espera de una conexión. La ventaja principal que tiene este protocolo es que

carpetas, mensajes, etc. se guardan en el computador, con lo que permite leer el correo recibido sin estar conectado a la red. Además, al leer los mensajes y bajarlos al computador, liberamos espacio en el buzón del Host, con lo cual se tiene menos probabilidades que se llene el buzón y no se pueda recibir más mensajes

- ✓ IMAP : Este protocolo es similar al protocolo POP pero sus diferencias radican en la forma en que almacena la información así de como se recupera el e-mail del servidor. La principal diferencia que encontramos respecto al anterior protocolo es que tanto los mensajes como las carpetas se guardan en el Host.
- ✓ NNTP (Network News Transfer Protocol) es un protocolo para la distribución, petición, recuperación y envío de news (noticias) entre los servidores de news de la comunidad ARPA-Internet a través de USENET utilizando un sistema cliente-servidor con intercambio fiable de información (TCP).
- ✓ El Telnet, un protocolo de emulación de terminal, es utilizado para el inicio de sesiones remotas en servidores de red. El programa servidor al que se quiere acceder está escuchando en el puerto 23 por defecto, y los datos son transmitidos mediante TCP.

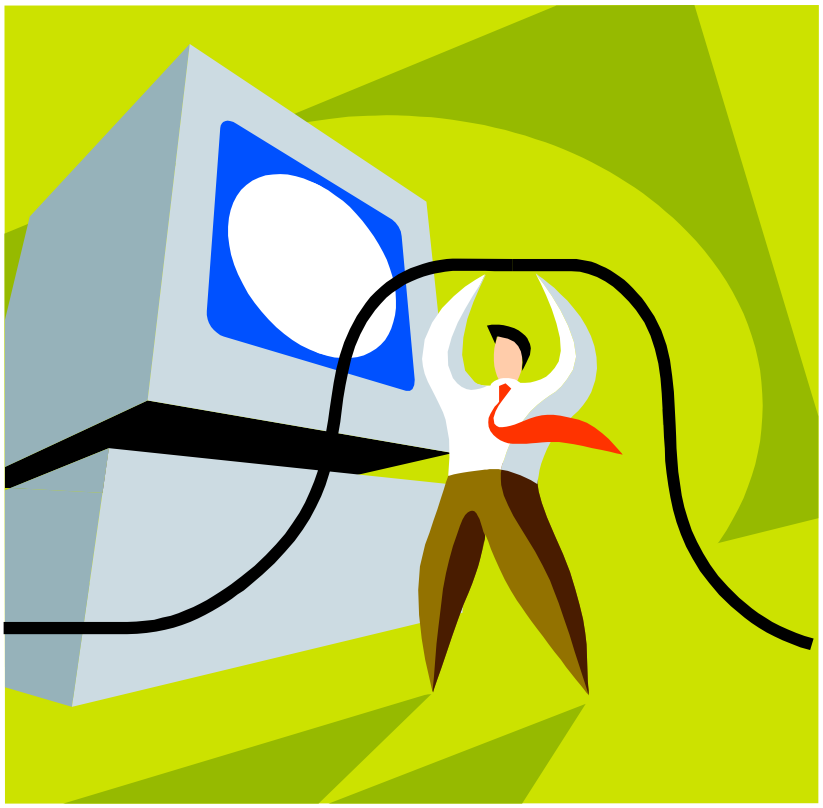
Adicionalmente, los siguientes protocolos ayudan a facilitar el uso y la administración de redes TCP/IP:

- ✓ El Sistema de Nombres de Dominio (Domain Name System, DNS) es utilizado para convertir un nombre de servidor en una dirección IP. El servidor DNS por defecto esta escuchando el puerto 53 y los datos son trasmitidos mediante el protocolo UDP.
- ✓ El Protocolo de Información de Enrutamiento (Routing Information Protocol, RIP) es un protocolo de enrutamiento que los enrutadores utilizan para intercambiar información de enrutamiento en una red IP.
- ✓ El Protocolo Simple de Administración de Red (Simple Network Management Protocol, SNMP) es utilizado entre la consola de administración de red y los dispositivos de la red (enrutadores, puentes y concentradores inteligentes) para recolectar e intercambiar información de administración de la red. El servidor SNMP por defecto

esta escuchando el puerto 161 y los datos son trasmitidos mediante el protocolo UDP.

Ejemplos de interfaces de la capa de aplicación para aplicaciones TCP/IP son Windows Sockets y NetBIOS. Windows Sockets proporciona una interfaz de programación para aplicaciones (API) estándar bajo el sistema operativo Microsoft Windows. El NetBIOS es una interfaz, estándar de la industria, para acceder servicios de protocolo tales como sesiones, datagramas y conversión de nombres.

CAPITULO III



PROTOCOLOS DE TUNEL

3.1.- Introducción
3.2.- Protocolos de Túnel
3.3.- Tipos de Túnel

3.1.- Introducción.

Un sistema de túnel, es un método para utilizar una infraestructura de red para transferir datos de una red sobre otra. Los datos que serán transferidos (carga útil) pueden ser tramas (paquetes) de otro protocolo. En lugar de enviar una trama a medida que es producida por el nodo originador, el protocolo de túnel encapsula la trama en un encabezado adicional. El encabezado adicional proporciona información de enrutamiento de tal manera que la carga útil encapsulada pueda viajar a través de la red intermedia.

Entonces, se pueden enrutar los paquetes encapsulados entre los puntos finales del túnel sobre la red. La trayectoria lógica a través de la cual viajan los paquetes encapsulados en la red se le llama un túnel. Una vez que las tramas encapsuladas llegan a su destino sobre la red se desencapsulan y se envían a su destino final. Note que este sistema de túnel incluye todo este proceso (encapsulamiento, transmisión y desencapsulamiento de paquetes) [WWW04].

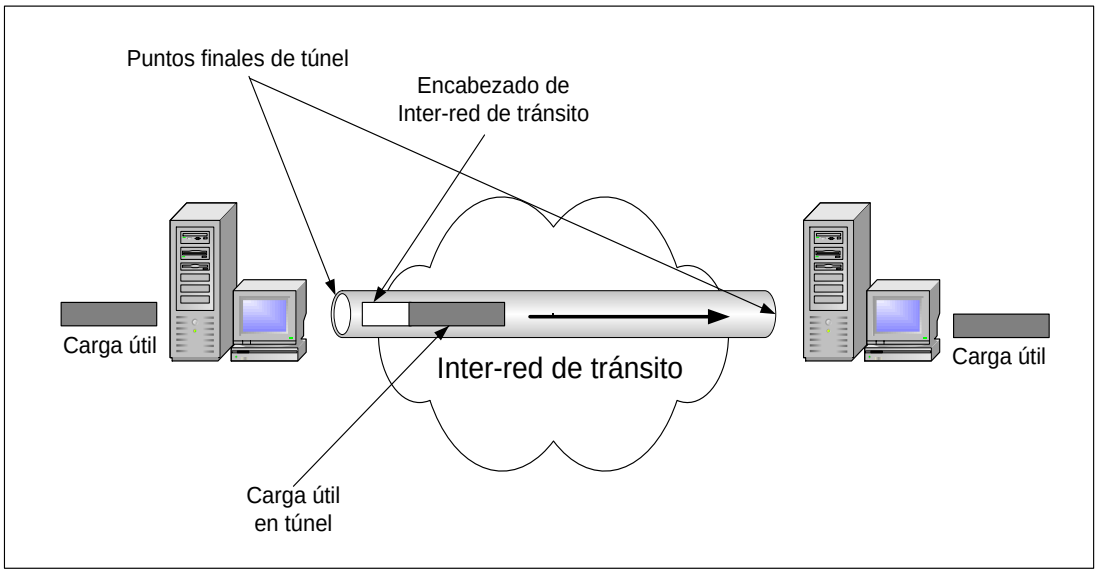


Figura 3.1.- Túneles

Tome en cuenta que la inter-red de tránsito puede ser el Internet, que es una inter-red pública y es el ejemplo del mundo real más conocido. Existen muchos

otros ejemplos de túneles que pueden realizarse sobre inter-redes corporativas. Si Internet proporciona una de las inter-redes más penetrantes y económicas, las referencias a Internet se pueden reemplazar por cualquier otra inter-red pública o privada que actúe como una inter-red de tránsito.

Las tecnologías de túnel han existido, pero algunos ejemplos de tecnologías maduras incluyen:

- ✓ **Túneles SNA sobre interredes IP**. Cuando se envía tráfico de la arquitectura de la red del sistema (SNA) a través de una inter-red IP corporativa, la trama SNA se encapsula en un encabezado UDP e IP.
- ✓ **Túneles IPX para Novell NetWare sobre inter-redes IP**. Cuando un paquete IPX se envía a un servidor NetWare o router IPX, el servidor o router envuelve el paquete IPX en un encabezado UDP e IP y, luego lo envía a través de una inter-red IP. El router IP a IPX de destino quita el encabezado UDP e IP, y transmite el paquete al destino IPX.

En los últimos años se han introducido nuevas tecnologías de sistemas de túneles. Entre las tecnologías más nuevas, enfoque principal de este capitulo, incluyen:

- ✓ **Protocolo de túnel de punto a punto (PPTP).** Permite que se encripte el tráfico IP, IPX o NetBEUI y luego se encapsule en un encabezado IP para enviarse a través de una red corporativa IP o red pública IP.
- ✓ **Protocolo de túnel de nivel 2 (L2TP).** Permite que se encripte el tráfico IP, IPX o NetBEUI y luego se envíe sobre cualquier medio que brinde soporte a la entrega de datagramas punto a punto, como IP, X.25, Frame Relay o ATM.
- ✓ **Modo de túnel de seguridad IP (IPSec)**. Permite que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP.

3.2.- Protocolos de túnel.

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

En la tabla 3.1 se puede observar los protocolos de túnel que se describirán más adelante.

Protocolo	Detalle
PPTP	Point to Point Tunneling Protocol (Microsoft)
L2F	Layer Two Forwarding (Cisco)
L2TP	Layer Two Tunneling Protocol (Cisco)

Tabla 3.1.- Protocolos de Túnel

También se describirán los protocolos PPP (Point to Point Protocol) y también el protocolo IPSec (IP Security), que aunque no pertenezcan al conjunto de protocolos de túnel, pero si tienen relación con éstos.

La tecnología de túnel se puede basar ya sea en el protocolo del túnel de Nivel 2 o de Nivel 3. Estos niveles corresponden al modelo de referencia de interconexión de sistemas abiertos (OSI). Los protocolos de nivel 2 corresponden al nivel de enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP y L2TP son protocolos de túnel de nivel 2; ambos encapsulan la carga útil en una trama del protocolo punto a punto (PPP) que se enviará a través de la red. Los protocolos de nivel 3 corresponden al nivel de la red y utilizan paquetes IP sobre IP y el modo de túnel de seguridad IP (IPSec); estos protocolos encapsulan los paquetes IP en un encabezado adicional IP antes de enviarlos a través de una red IP.

¿Cómo funcionan los túneles?

Para las tecnologías de túnel de nivel 2 como PPTP y L2TP, un túnel es similar a levantar una sesión de comunicación; los dos nodos finales del túnel deben estar de acuerdo al túnel y deben negociar las variables de la configuración, asignación de dirección, los parámetros de encriptación o de compresión. En la mayoría de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas. Se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar al mismo.

En general las tecnologías de túnel de nivel 3, suponen que se han manejado fuera de contexto los temas relacionados con la configuración, normalmente por medio de procesos manuales. Sin embargo una fase de mantenimiento de túnel bien puede no existir. Mientras para los protocolos de nivel 2 (PPTP y L2TP) se debe crear, mantener y luego dar por terminado un túnel.

Una vez que se establece el túnel, se puede enviar los datos a través del mismo. El cliente o el servidor del túnel utilizan un protocolo de transferencia de datos del túnel para preparar los datos para su transferencia. Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor del túnel, el cliente del túnel adjunta primero 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 cual lo enruta al servidor del túnel. El servidor del túnel acepta los paquetes, quita 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.

Los protocolos de túnel y los requerimientos básicos del túnel.

Debido a que los protocolos de nivel 2 (PPTP y L2TP) se basan en protocolos PPP bien definidos, heredan un conjunto de funciones útiles, estas funciones y sus contrapartes de nivel 3 cubren los requerimientos básicos de la VPN [WWW04].

- ✓ **Autenticación de usuario.** Los protocolos de túnel de nivel 2 heredan los esquemas de autenticación del usuario de PPP, incluyendo los métodos EAP (Extensible Authentication Protocol – *Protocolo de Autenticación Ampliable*). Muchos de los esquemas de túnel de nivel 3 suponen que los puntos finales han sido bien conocidos y autenticados antes de que se estableciera el túnel. Una excepción es la negociación IPSec ISAKMP, la cual proporciona una autenticación mutua de los nodos finales del túnel. (Note que la mayor parte de las implementaciones IPSec dan soporte sólo a certificados basados en equipo, más que en certificados de usuarios. Como resultado, cualquier usuario con acceso a uno de los equipos de nodo final puede utilizar el túnel. Se puede eliminar esta debilidad potencial de seguridad cuando se complementa el IPSec con un protocolo de nivel 2

como el L2TP.)

- ✓ **Soporte de tarjeta de señales.** Al utilizar el protocolo de autenticación ampliable (EAP), los protocolos de túnel de nivel 2 pueden dar soporte a una amplia variedad de métodos de autenticación, incluyendo contraseñas de una sola vez, calculadores criptográficos y tarjetas inteligentes. Los protocolos de túnel de nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define la autenticación de los certificados de claves públicas en su negociación ISAKMP/Oakley(protocolo de seguridad).
- ✓ **Asignación de dirección dinámica.** El túnel de nivel 2 da soporte a la asignación dinámica de direcciones de clientes basadas en un mecanismo de negociación de protocolo de control de la red (NCP). Por lo general, los esquemas de túnel de nivel 3 suponen que ya se ha asignado una dirección antes de la iniciación del túnel. Los esquemas para la asignación de direcciones en el modo de túnel IPSec están actualmente en desarrollo.
- ✓ **Compresión de datos.** Los protocolos de túnel de nivel 2 dan soporte a esquemas de compresión basados en PPP. Por ejemplo, las implementaciones de Microsoft tanto de PPTP como L2TP utilizan Microsoft Point-to-Point Compression (MPPC). La IETF se encuentra investigando mecanismos similares (como la compresión IP) para los protocolos de túnel de nivel 3.
- ✓ **Encriptación de datos**. Los protocolos de túnel nivel 2 dan soporte a mecanismos de encriptación de datos basados en PPP. La implementación de Microsoft de PPTP da soporte al uso opcional de Microsoft Point-to-Point Encription (MPPE), basado en el algoritmo RSA/RC4. Los protocolos de túnel nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define varios métodos de Encriptación opcional de datos que se negocian durante el intercambio ISAKMP/Oakley. La implementación de Microsoft del protocolo L2TP utiliza la encriptación IPSec para proteger el flujo de datos del cliente al servidor del túnel.
- ✓ **Administración de claves.** MPPE, protocolo de nivel 2, se basa en las claves iniciales generadas durante la autenticación del usuario y luego las renueva periódicamente. IPSec negocia explícitamente una

clave común durante el intercambio ISAKMP y también las renueva periódicamente.

- ✓ **Soporte de protocolo múltiple**. El sistema de túnel de nivel 2 da soporte a protocolos múltiples de carga útil, lo cual hace más fácil a los clientes de túnel tener acceso a sus redes corporativas utilizando IP, IPX, NetBEUI, etc. En contraste, los protocolos de túnel de nivel 3, como el modo de túnel IPSec, típicamente dan soporte sólo a redes objetivo que utilizan el protocolo IP.

3.2.1.- Protocolo de Punto a Punto (PPP).

El protocolo PPP, no es un protocolo de túnel, pero es la base para el protocolo PPTP, que es el protocolo de túnel punto a punto.

El protocolo PPP proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos "pares" (máquinas en los dos extremos del enlace). Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Consta de tres componentes principales:

- ✓ Un método de encapsulamiento que permite al software de red utilizar un solo enlace serial para múltiples protocolos y manejar la detección de errores.
- ✓ Un protocolo de control de enlace LCP (Link Control Protocol) que el software de red puede utilizar para establecer, configurar y probar las conexiones de enlace de datos. Ambos lados de la conexión PPP utilizan LCP para negociar las opciones de conexión.
- ✓ Una familia de protocolos de control de red NCPs (Network Control Protocols) que permita a las conexiones PPP utilizar diferentes protocolos de la capa de red.

Hay cuatro fases de negociación en una sesión de marcación de PPP. Cada una de éstas debe completarse satisfactoriamente antes de que la conexión de PPP esté lista para transferir los datos del usuario. Estas fases son:

Fase 1. Establecimiento del enlace de PPP: El PPP utiliza el protocolo de control de enlace (LCP) para establecer, mantener y terminar la conexión física. Durante la fase del LCP, se seleccionan las opciones de comunicación básica. Tome en cuenta que durante la fase de establecimiento del enlace (fase 1), se seleccionan los protocolos de autenticación, pero no se implementan realmente hasta la fase de autenticación de usuarios (fase 2). De manera similar, durante el LCP, se toma una decisión en cuanto a que si dos enlaces iguales negocian el uso de compresión y/o encriptación, la elección real de algoritmos de encriptación/compresión ocurre durante la fase 4.

Fase 2. Autenticación de usuarios: En esta fase, el computador que hace de cliente presenta la identificación del usuario al servidor de acceso remoto(RAS). Un esquema seguro de autenticación proporciona protección contra los ataques de contestación e imitación de clientes remotos.

Las implementaciones del PPP por lo general, proporcionan métodos limitados de autenticación, algunos de éstos son:

- ✓ **Protocolo de Autenticación de Contraseñas (PAP).** Es un esquema simple de autenticación de texto claro, es decir, que no está codificado. El servidor solicita el nombre y contraseña del usuario, y el PAP los entrega en texto claro. Indiscutiblemente, este esquema no es seguro debido a que puede ser interceptado el nombre y contraseña del usuario, y utilizarlos para obtener acceso al servidor y a todos los recursos suministrados por el mismo. El PAP no proporciona protección contra los ataques de reproducción o las imitaciones de cliente remoto, una vez que la contraseña del usuario ha sido violada.
- ✓ **Protocolo de Autenticación de Intercambio de Señales de Reconocimiento (CHAP).** Es un mecanismo de autenticación encriptado que evita la transmisión de contraseñas reales en la conexión. El NAS envía un desafío (challenge), que consiste de una identificación de sesión y una extensión challenge arbitraria al cliente

remoto. El cliente remoto deberá utilizar el algoritmo de control unidireccional MD5 para devolver el nombre del usuario y una encriptación del challenge, la identificación de la sesión y la contraseña del cliente. El nombre del usuario se envía sin verificar.

El CHAP es una mejora sobre el PAP en cuanto a que no se envía la contraseña de texto transparente sobre el enlace. En su lugar, se utiliza la contraseña para crear una verificación encriptada del desafío original. El servidor conoce la contraseña del texto transparente del cliente y por lo tanto puede duplicar la operación y comparar el resultado con la contraseña enviada en la respuesta del cliente. El CHAP protege contra ataques de reproducción al utilizar una extensión challenge arbitraria para cada intento de autenticación. El CHAP protege contra la personificación de un cliente remoto al enviar de manera impredecible desafíos repetidos al cliente remoto a todo lo largo de la duración de la conexión.

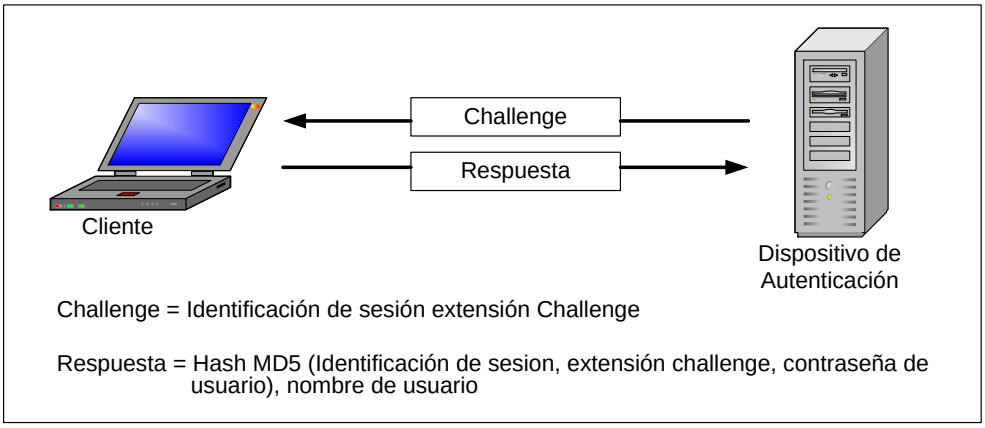


Figura 3.2.- El proceso CHAP

- ✓ **Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP):** El MS-CHAP (Protocolo de Autenticación por desafío mutuo de Microsoft) es un mecanismo de autenticación codificado muy similar al CHAP en donde, el servidor envía al cliente remoto una señal de reconocimiento, que consiste de una ID de sesión y de una cadena de reconocimiento arbitraria. El cliente remoto debe regresar el nombre

del usuario y un hash MD4 de la cadena de reconocimiento, la ID de sesión y de la contraseña con el algoritmo de control unidireccional hash MD4. Este diseño, que manipula una codificación del hash MD4 de la contraseña, proporciona un nivel adicional de seguridad porque permite que el servidor almacene contraseñas codificadas en lugar de contraseñas de texto claro. El servidor reúne los datos de autenticación y después los valida en su propia base de datos de usuarios o basándose en un servidor central de base de datos de autenticación, además, proporciona códigos de error adicionales, incluyendo un código de expiración de contraseña, y mensajes adicionales codificados de cliente-servidor que permiten que los usuarios cambien sus contraseñas.

Durante la fase 2 de la configuración del enlace del PPP, el NAS recopila los datos de autenticación y luego valida los datos contra sus propia base de datos del usuario o contra un servidor central para la autenticación de base de datos.

Fase 3. Control de retorno de llamada de PPP: La implementación del PPP de Microsoft incluye una fase opcional de control de retorno de llamada. Esta fase utiliza el Protocolo de Control de Retorno de Llamada (CBCP – Call Back Control Protocol) inmediatamente después de la fase de autenticación. Si la configuración es para retorno de llamada, después de la autenticación el cliente remoto y el servidor se desconectan. Después, el servidor llama otra vez al cliente remoto a un número telefónico especificado. Esto proporciona un nivel adicional de seguridad para las redes de marcación. El servidor permitirá conexiones de clientes remotos que residen físicamente sólo en números telefónicos específicos.

Fase 4. Invocación de protocolos de nivel de red: En esta fase, el PPP invoca a los protocolos de control de red (NCP) que fueron seleccionados durante la fase de establecimiento del enlace para configurar los protocolos utilizados por el cliente remoto.

Después de culminar las fases de negociación, el PPP comienza a transmitir los datos desde las dos partes. Cada paquete de datos transmitido se encapsula en un encabezado de PPP que es eliminado por el sistema receptor. Si la

compresión de datos se seleccionó en la fase del establecimiento del enlace PPP y se negoció en la fase de invocación de protocolos del nivel de red, los datos serán comprimidos antes de la transmisión. Si se seleccionaron y se negociaron de manera similar la encriptación de datos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

3.2.2.- Protocolo de Túnel de Punto a Punto (PPTP).

Point-To-Point Tunneling Protocol (PPTP) es una combinación del protocolo punto a punto(PPP) y del protocolo de control de transmisión/protocolo Internet (TCP/IP), el cual permite el seguro intercambio de datos de un cliente a un servidor formando una red privada virtual, basado en una red de trabajo vía TCP/IP[WWW04].

PPTP combina funciones del PPP como el multiprotocolo, la autenticación de usuarios y la privacidad con la compresión de paquetes de datos, y TCP/IP ofrece capacidad para enrutar esos paquetes por Internet. PPTP permite el encapsulamiento de datos con el uso de un túnel.

El PPTP es un protocolo de nivel de enlace del modelo de referencia OSI, el cual encapsula las tramas de PPP en datagramas de IP las cuales van a ser transmitidas a través de una red interna de IP, como Internet. (Sobre estos paquetes PPP pueden emplearse cualquiera de los siguientes protocolos: NetBEUI, IPX, SNA o TCP/IP). También se puede utilizar el PPTP en una red privada de LAN a LAN.

El protocolo de túnel de punto a punto (PPTP) utiliza una conexión de TCP (puerto 1723) para el mantenimiento del túnel y las tramas de PPP encapsuladas, las cuales a su vez son encapsuladas en paquetes de encapsulamiento de enrutamiento genérico (GRE) destinadas a los datos en el túnel. Las cargas de pago de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse.

PPTP permite crear conexiones entre un cliente y un servidor sobre redes IP públicas como puede ser Internet. Lo interesante es que estos enlaces se realizan a través de una especie de túnel que PPTP crea en la red IP y por el que viajan los datos de la conexión. Además este túnel es privado: nadie a excepción del cliente y el servidor viajan por él.

El tráfico PPTP consiste en dos tipos de tráfico para diferentes tipos de datos: paquetes de datos y paquetes de control. Los paquetes de control se emplean para cosas como el estado y la señalización, y los paquetes de datos se emplean para contener los datos del usuario. Los paquetes de datos son paquetes que han sido encapsulados con el protocolo de encapsulamiento para enrutamiento genérico versión 2 (GREv2) de Internet.

La conexión PPTP comienza primero como un reconocimiento entre las dos terminales remotas; éstas acuerdan el esquema de compresión y el método de encapsulamiento que van a usar. Si es necesario, durante la comunicación normal estos paquetes se pueden fragmentar y el encabezado PPP añade un número serial para detectar si se perdió un paquete.

La figura 3.3 muestra la forma en que se ensambla el paquete de PPTP antes de la transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de la red. El diseño de la trama final muestra la encapsulación para un cliente de marcación (controlador de dispositivo PPP).

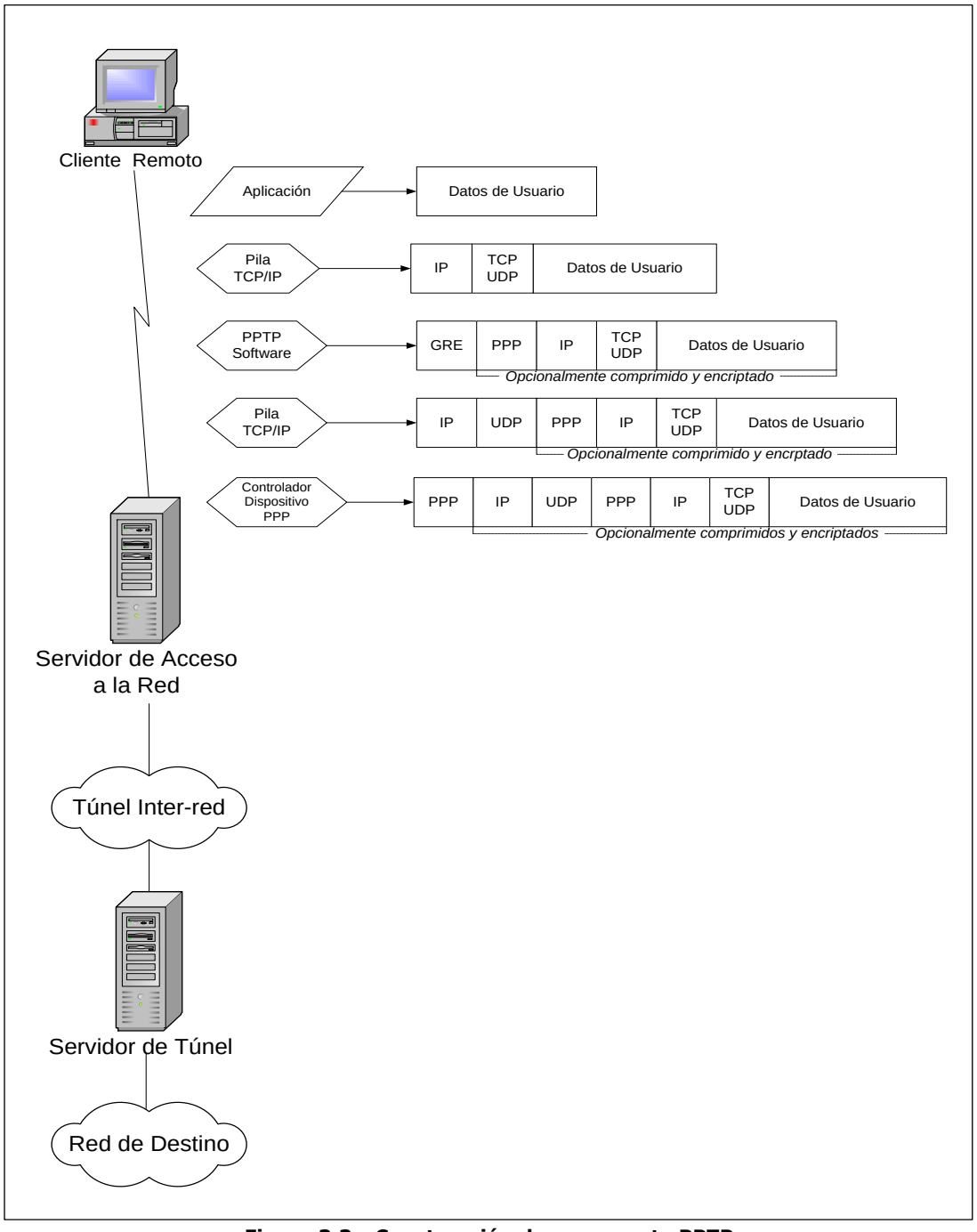


Figura 3.3.- Construcción de un paquete PPTP

La arquitectura del PPTP se compone de tres fases, cada una de las cuales necesita que el anterior haya tenido éxito:

Fase 1. Conexión PPP. Es la conexión con el ISP. PPP es un protocolo de acceso remoto que establece enlaces punto a punto sobre distintos medios

físicos. Normalmente, se emplea para establecer conexiones remotas a través de enlaces telefónicos (como por ejemplo conectar con nuestro ISP). PPP se encarga de las siguientes funciones:

- ✓ Establecer y mantener la conexión punto a punto a nivel físico.
- ✓ Autentifica a los usuarios mediante PAP, SPAP, CHAP ó MS-CHAP comentados anteriormente.
- ✓ Crea tramas que encapsulan paquetes NetBEUI, IPX o TCP/IP encriptados.

Fase 2. Control de la conexión PPTP. Una vez conectado a Internet, o a la red IP que hayamos elegido, debe establecerse conexión con el servidor y controlar la comunicación establecida. En una red TCP/IP, El protocolo TCP se encarga de este trabajo. Sin embargo, en los túneles PPTP, TCP no existe a nivel de transporte porque todo va encapsulado en marcos PPP sobre paquetes IP. Por este motivo PPTP asume este papel utilizando servicios TCP para ello. A esta conexión es a la que se le denomina túnel PPTP. Los principales mensajes empleados por PPTP para el control de la sesión entre los extremos del túnel son los siguientes:

Tabla 3.1.- Mensajes de Control de la sesión de PPTP

MENSAJE	FUNCION
PPTP_START_SESSION_REQUEST	Inicia la sesión
PPTP_START_SESSION_REPLY	Respuesta a la solicitud de inicio de sesión
PPTP_ECHO_REQUEST	Mantiene la sesión
PPTP_ECHO_REPLY	Respuesta a la solicitud de mantenimiento de sesión
PPTP_WAN_ERROR_NOTIFY	Notifica un error en la conexión PPP
PPTP_SET_LINK_INFO	Configura la conexión cliente/servidor PPTP
PPTP_STOP_SESSION_REQUEST	Finaliza la sesión
PPTP_STOP_SESSION_REPLY	Respuesta a la solicitud de finalización de sesión

Fase 3. Data Tunneling. Es el proceso de enviar los datos a través del túnel. Los datos se encapsulan y encriptan en paquetes PPP sobre datagramas IP. Como curiosidad, comentar que la creación de éste se realiza mediante una

versión modificada de GRE Protocolo de encapsulación y encaminamiento genérico.

De esta forma, pueden crearse conexiones WAN seguras y de bajo coste. Esta solución sólo tiene una restricción: el rendimiento. Si la red IP está muy saturada, el túnel sufrirá las consecuencias. Por tanto, puede no ser recomendable para aplicaciones que requieran fiabilidad y rapidez.

PPTP es, en la actualidad, un protocolo pendiente de estandarización y, por el momento sólo está disponible para plataformas Win32 (NT y 95/OSR2 y superiores). Sin embargo, goza del apoyo de las empresas integrantes del PPTP Forum, a saber: Ascend Communications, ECI Telematics, 3Com/US Robotics y, como no, Microsoft.

3.2.3.- Transmisión de nivel 2 (L2F).

En 1996, Cisco System desarrolló un protocolo que iba a emplearse en combinación con el protocolo PPTP de Microsoft. Con el crecimiento de los servicios por marcación y la disponibilidad de muchos protocolos diferentes, se necesitaba crear un escenario de marcación virtual donde cualquiera de los protocolos que no fueran IP pudiesen disfrutar de los servicios de Internet [WWW06].

Cisco definió el concepto de establecimiento de túneles, como el encapsulamiento de paquetes no IP; es decir los usuarios hacen una conexión PPP o SLIP a un proveedor de Internet por marcación, y con el uso de L2F, se conectan a las máquinas de sus empresas. Estos túneles se encuentran en los extremos de la conexión a Internet, y son enrutados con software para establecimiento de túneles, llamados interfaces de túnel. El reenvío de nivel 2 ofrece muchos beneficios como los siguientes:

- ✓ Independencia del Protocolo (IPX, SNA)
- ✓ Autenticación (PPP, CHAP, TACACS)
- ✓ Administración de direcciones (asignadas por destino)

- ✓ Túneles dinámicos y seguros
- ✓ Apertura de cuentas
- ✓ Independencia de medios, por ejemplo sobre L2F (ATM, X.25, tramas)
- ✓ Tanto el establecimiento de túneles L2F como el acceso local a Internet.

En la configuración básica, el usuario realiza una conexión PPP o una conexión similar al proveedor de Internet local. Con la solicitud del usuario, el servidor, mediante el software L2F, inicia un túnel al destino del usuario. El destino pide la contraseña del usuario y, una vez autorizado, le asigna una dirección IP al usuario, igual que un dispositivo de acceso por marcación típico. El punto terminal quita el encabezado del túnel, registra el tráfico y permite que haya comunicación.

A diferencia del PPTP y del L2TP, el L2F no tiene un cliente definido. Asimismo, el L2F sólo funciona en túneles obligatorios.

3.2.4.- Protocolo de túnel de nivel 2 (L2TP).

En 1996 surgieron los protocolos PPTP y L2F. Compañías como Microsoft, Ascend y 3Com trabajaron en PPTP, mientras que Cisco trabajó en L2F. Dos años más tarde, en 1998, estas compañías acordaron una nueva especificación de prueba para la IETF; el protocolo de establecimiento de túneles de nivel 2 (L2TP).

El L2TP esta compuesto por las mejores características del PPTP y del L2F. Este es un protocolo de red que encapsula las tramas de PPP para enviarlas a través de redes de IP, X.25, Frame Relay o modo de transferencia asíncrona (ATM).

L2TP utiliza dos funciones: una función de servidor de línea tipo cliente (LAC), que es concentrador de acceso L2TP, y una función de servidor de red del lado servidor (LNS). Cuando una computadora realiza una conexión a un proveedor de servicios de Internet, la función LAC inicia el túnel y luego agrega los distintos encabezados a la carga PPP. La LAC establece el túnel al dispositivo de terminación LNS; este dispositivo puede ser un enrutador, un servidor o un

dispositivo de acceso. Después de que se estableció el túnel, se configura un mecanismo de autenticación de usuario para establecer la identidad de los usuarios. L2TP utiliza mensajes de control para optimizar el túnel [RFC2661].

Cuando se configura para utilizar el IP y su transporte de datagrama, el L2TP puede utilizarse como un protocolo de túnel a través de Internet. Este también puede utilizarse directamente a través de varios medios de WAN media (como el Frame Relay) sin un nivel de transporte de IP.

El L2TP a través de redes internas de IP utiliza el UDP y una serie de mensajes L2TP para mantener el túnel. El L2TP también utiliza al UDP para enviar tramas de PPP encapsuladas L2TP como los datos en el túnel. Las cargas de pago de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse.

La Figura 3.4 muestra la forma en que se ensambla un paquete L2TP antes de su transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño final de trama muestra la encapsulación para un cliente de marcación (controlador de dispositivos PPP). La encapsulación supone el L2TP sobre IP.

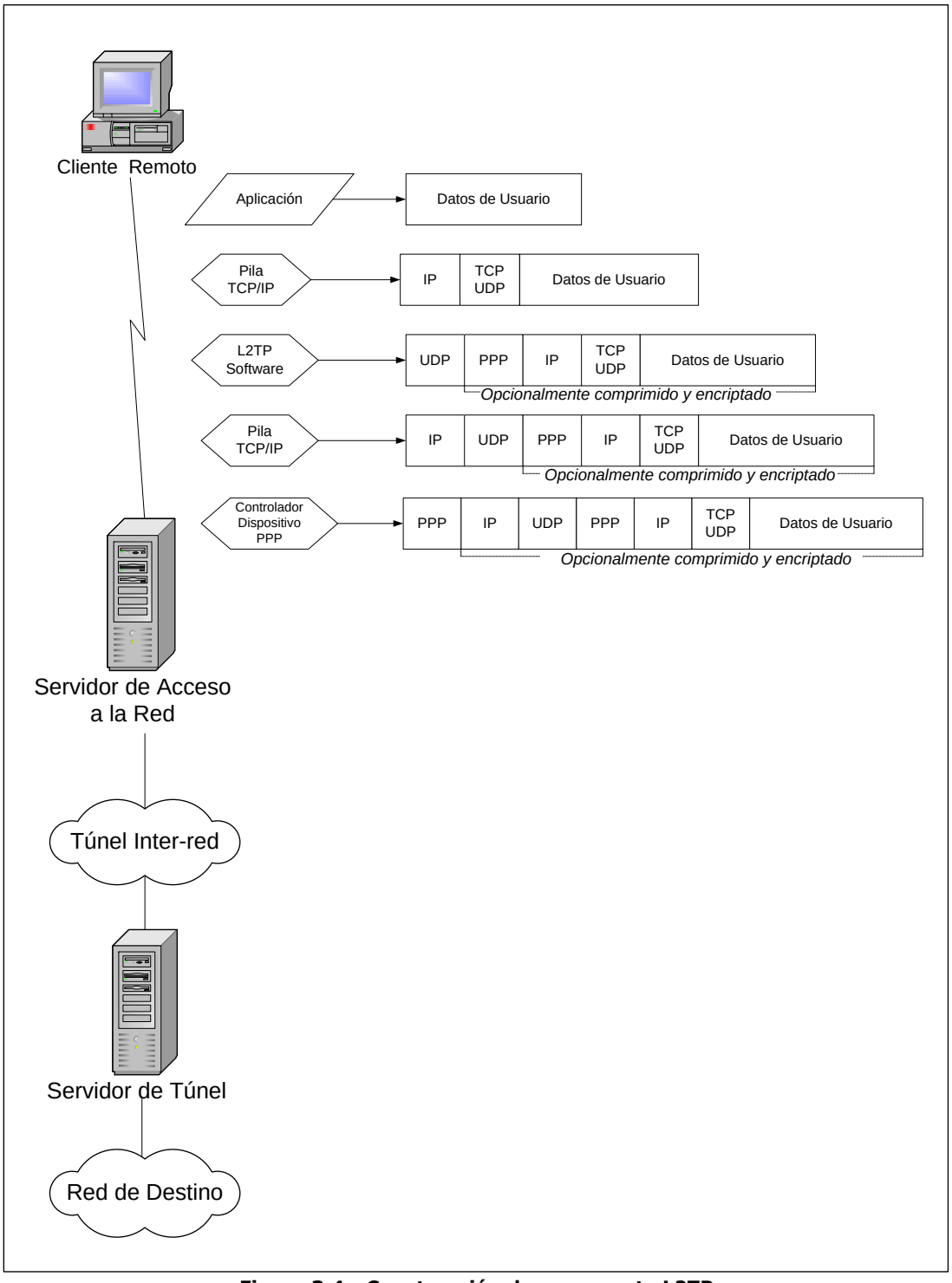


Figura 3.4.- Construcción de un paquete L2TP

PPTP y L2TP ofrecen compresión por software, lo cual reduce los paquetes de usuario, y también las técnicas de compresión añaden otro nivel de cifrado, aunque en pequeñas cantidades.

L2TP es un protocolo de nivel 2, diseñado para encapsular en el nivel 2, e IPSec, que es un protocolo de nivel 3. Por lo tanto IPSec se puede utilizar junto con L2TP para dar más seguridad. Esta es una configuración que se recomienda si se emplea L2TP para instalar seguridad IPSec en un entorno IP.

PPTP comparado con el L2TP

Tanto el PPTP como L2TP utilizan el PPP para proporcionar una envoltura inicial de los datos y luego incluir encabezados adicionales para transportarlos a través de la red. Los dos protocolos son muy similares [WWW04]. Sin embargo, existen diferencias entre el PPTP y L2TP:

- ✓ El PPTP requiere que la red sea de tipo IP. El L2TP requiere sólo que los medios del túnel proporcionen una conectividad de punto a punto orientada a paquetes. Se puede utilizar L2TP sobre IP (utilizando UDP), circuitos virtuales permanentes (PVCs), circuitos virtuales X.25 (VCs) o VCs ATM.
- ✓ El PPTP sólo puede soportar un túnel único entre puntos terminales. El L2TP permite el uso de varios túneles entre puntos terminales. Con el L2TP, uno puede crear diferentes túneles para diferentes calidades de servicio.
- ✓ L2TP proporciona la compresión de encabezados. Cuando se activa la compresión de encabezado, el L2TP opera sólo con 4 bytes adicionales, comparado con los 6 bytes para el PPTP.
- ✓ L2TP proporciona la autenticación de túnel, mientras que el PPTP no. Sin embargo, cuando se utiliza cualquiera de los protocolos sobre IPSec, se proporciona la autenticación de túnel por el IPSec de tal manera que no sea necesaria la autenticación del túnel nivel 2.

3.2.5.- Protocolo de Internet Seguro (IPSec).

El IPSec (IP Seguro) es un estándar de protocolo de nivel 3 que da soporte a la transferencia protegida de información a través de una red IP.

Se define como un conjunto de protocolos de seguridad que permite agregar encriptado y autenticación a las comunicaciones IP. Mientras el encriptado puede evitar que un usuario no autorizado como típicamente un hacker pueda leer un mensaje, el autenticado puede evitar los ataques a un sitio originados de sitios externos no deseados o hasta de dentro de la propia red del sitio [LIB01].

Las necesidades de privacidad, autenticación e integridad de un mensaje se cubren con dos de los protocolos incluidos en IPSec: AH y ESP. El primero provee autenticado y por extensión también integridad, y el segundo básicamente encriptado para asegurar la privacidad.

El encabezado de autenticación (AH) describe como autenticar paquetes de datagramas IP (autenticación de datos) y proporciona integridad sin conexión y, si esta implementada, protección contra ataques repetitivos. AH puede utilizarse en los modos de túnel y trasporte. 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.

La norma de Carga con seguridad de encapsulamiento (ESP) proporciona confianza, autenticación, integridad sin conexión y servicios contra repeticiones. Este conjunto de servicios en ESP se instala durante el establecimiento de la asociación de seguridad.

Si bien ESP también opcionalmente puede proveer autenticación, no encapsula todo el datagrama dejando abierto el primer encabezamiento, algo que puede ser una necesidad sin exponer mayormente la seguridad. Pero más recomendable resulta usar ambos protocolos juntos cada uno con sus funciones específicas.

IPSec es un protocolo de Capa 3 resultando totalmente transparente a las aplicaciones. Se viene usando cada vez más en las VPNs (Redes Privadas Virtuales) tanto para acceso remoto como intranets extendidas y especialmente en extranets.

Asimismo define los mecanismos de codificación para el tráfico de IP y el formato de un paquete para un IP a través del modo de túnel de IP, mejor conocido como modo de túnel de IPSec. Un túnel de IPSec consta de un cliente de túnel y de un servidor de túnel, los cuales se configuran para utilizar la transmisión en túnel de IPSec y un mecanismo de codificación negociado.

El modo de túnel de IPSec utiliza el método de seguridad negociada para encapsular y codificar todos los paquetes de IP con el fin de lograr una transferencia segura a través de las redes internas de IP públicas o privadas. Después, la carga de pago codificada se encapsula de nuevo en un encabezado de IP de texto plano, y se envía a través de la red interna para que lo reciba el servidor de túnel. Después de recibir este datagrama, el servidor de túnel procesa y descarta el encabezado de IP de texto plano y después decodifica su contenido para recuperar el paquete original de IP de carga útil. Posteriormente, el paquete de IP de carga útil es procesado normalmente y enrutado a su destino.

IPsec se puede usar directamente entre las máquinas que se comunican, o bien a través de un túnel entre los dispositivos periféricos, llamados gateways de seguridad, que las conectan a través de Internet. Las formas de conectividad resultantes se llaman así modo transporte y modo túnel respectivamente.

Un tercer protocolo integrante de IPSec llamado IKE (protocolo Internet Security Association Key Management conocido como ISAKMP/Oakley) se usa para un intercambio seguro de las claves con que se manejan los otros componentes de IPSec. IKE puede operar con claves precompartidas, firmas digitales o con claves públicas basadas en certificados digitales.

El modo de túnel IPSec tiene las siguientes funciones y limitaciones [LIB02]:

- ✓ Sólo da soporte a tráfico IP.

- ✓ Funciona en el fondo de la pila IP; por lo tanto, las aplicaciones y protocolos de niveles más altos heredan su comportamiento.
- ✓ Está controlado por una política de seguridad un conjunto de reglas que se cumplen a través de filtros. Esta política de seguridad establece los mecanismos de encriptación y de túnel disponibles en orden de preferencia y los métodos de autenticación disponibles, también en orden de preferencia. Tan pronto como existe tráfico, los dos equipos realizan una autenticación mutua, y luego negocian los métodos de encriptación que se utilizarán. En lo subsiguiente, se encripta todo el tráfico utilizando el mecanismo negociado de encriptación y luego se envuelve en un encabezado de túnel.
- ✓ Una limitación es que las claves son estáticas y, mientras dura la comunicación, no hay un mecanismo para intercambiar estas claves.
- ✓ Orto problema de IPSec es que cada paquete IP aumenta su tamaño una vez que pasa por el proceso de cifrado. En algunas LAN, el tamaño de MTU (Unidad de Transferencia Máxima) podría obligar a la fragmentación de estos paquetes, lo cual aumenta la carga de red en dispositivos como los enrutadores. La alternativa son los túneles cifrados.

3.3.- Tipos de túnel.

Se pueden crear túneles de 2 formas diferentes.

Tipo de Tunel	Descripción
Túneles Voluntarios	Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente del túnel
Túneles Obligatorios	Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con un túnel obligatorio, la computadora del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del túnel.

Tabla 3.2.- Tipos de Túnel

3.3.1.- Túneles voluntarios

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

Un túnel voluntario ocurre cuando una estación de trabajo o un servidor de enrutamiento utilizan el software del cliente del túnel para crear una conexión virtual al servidor del túnel objetivo. Para poder lograr esto se debe instalar el protocolo apropiado de túnel en la computadora cliente. Para los protocolos que se analizan en este documento, los túneles voluntarios requieren una conexión IP (ya sea a través de una LAN o marcación) [WWW04].

En una situación de marcación, el cliente debe establecer una conexión de marcación para conectarse a la red antes de que el cliente pueda establecer un túnel. Este es el caso más común. El mejor ejemplo de esto es el usuario de Internet por marcación, que debe de marcar a un ISP y obtener una conexión a Internet antes de que se pueda crear un túnel sobre Internet.

Para una PC conectada a una LAN, el cliente ya tiene una conexión a la red que le puede proporcionar un enrutamiento a las cargas útiles encapsuladas al servidor del túnel LAN elegido. Este sería el caso para un cliente en una LAN corporativa que inicia un túnel para alcanzar una sub-red privada u oculta en la

misma LAN (como sería el caso de la red de Recursos Humanos que se analizó previamente).

Es una equivocación común que las VPNs requieran una conexión de marcación. Sólo requieren de una red IP. Algunos clientes (como las PCs del hogar) utilizan conexiones de marcación al Internet para establecer transporte IP. Esto es un paso preliminar en la preparación para la creación de un túnel, y no es parte del protocolo del túnel mismo.

3.3.2.- Túneles obligatorios.

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

Varios proveedores que venden servidores de acceso de marcación han implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel para la computadora del cliente es conocida de varias maneras como: Procesador frontal (FEP) en PPTP, un Concentrador de acceso a L2TP (LAC) en L2TP o un gateway de seguridad IP en el IPSec. En este capítulo, el término FEP se utilizará para describir esta funcionalidad, sin importar el protocolo de túnel. Para llevar a cabo esta función, el FEP deberá tener instalado el protocolo apropiado de túnel y deberá ser capaz de establecer el túnel cuando se conecte la computadora cliente [WWW04].

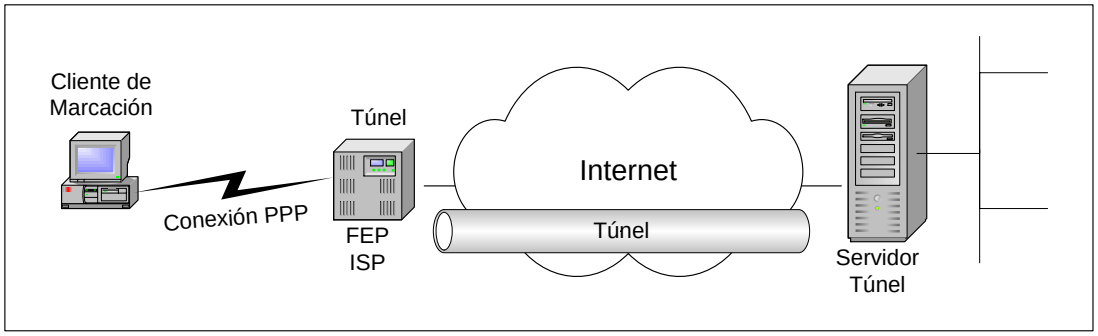


Figura 3.5.- Túneles obligatorios

En el ejemplo de Internet, la computadora cliente coloca una llamada de marcación al NAS activado por los túneles en el ISP. Por ejemplo, una empresa puede haber contratado con un ISP para instalar un conjunto nacional de FEPs. Estos FEPs pueden establecer túneles a través de Internet a un servidor de túnel conectado a la red privada de la empresa, consolidando así las llamadas de diferentes ubicaciones geográficas en una conexión única de Internet en la red corporativa.

Esta configuración se conoce como "túnel obligatorio" debido a que el cliente está obligado a utilizar el túnel creado por FEP. Una vez que se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel. En los túneles obligatorios, la computadora cliente realiza una conexión única PPP y, cuando un cliente marca en el NAS, se crea un túnel y todo el tráfico se enruta automáticamente a través de éste. Se puede configurar un FEP para hacer un túnel a todos los clientes de marcación hacia un servidor específico del túnel. De manera alterna, el FEP podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el FEP y servidor del túnel puede estar compartido entre varios clientes de marcación. Cuando un segundo cliente marca al servidor de acceso (FEP) para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el FEP y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya

que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel.

A la fecha, los túneles voluntarios han probado ser el tipo más popular de túnel.

CAPITULO IV

ARQUITECTURA DE RED PRIVADA VIRTUAL

4.1.- VPN proporcionada por un proveedor de servicios de Red
4.2.- VPN basada en cortafuegos
4.3.- VPN basada en caja negra
4.4.- VPN basada en Enrutador
4.5.- VPN basada en acceso remoto
4.6.- VPN basada con herramientas proxy
4.7.- VPN basada en software

Existen innumerables tipos de tecnología para la instalación de una VPN, cada una con su propio lugar y función, y cada uno con sus propias ventajas y desventajas asociadas. En el presente capitulo examinaremos algunas de las distintas arquitecturas de la tecnología VPN, incluyendo las VPN proporcionadas por los proveedores de servicio de red, las VPN basadas en cortafuegos, las VPN basadas en caja negra, las VPN basadas en acceso remoto / enrutador, las VPN consientes de las aplicaciones, las VPN de servicios múltiples y las VPN basadas en software. Con esta muestra de productos el lector podrá apreciar que existe una VPN para cada organización y cualquier infraestructura de red.

Parecería que en una VPN se podría instalar casi cualquier característica que deseara, desde la autenticación de usuarios y el filtrado en el web, hasta software antivirus. Lamentablemente, existen sacrificios entre el número de servicios disponibles en este tipo de productos, los requisitos de procesamiento necesarios para ejecutar esos servicios y el soporte final de los mismos.

Además se debería separar el servicio VPN de otros servicios de aplicaciones, por ejemplo, que se esté usando un cortafuego basado en sistema operativo y se decide instalar un producto VPN sobre el sistema operativo. Si se puede evitar el instalar una VPN en un servidor que ya tiene otros servicios de aplicaciones, es mejor hacerlo.

Ante la pregunta ¿Cuál es la mejor VPN para una organización? de entre las diferentes arquitecturas mencionadas anteriormente, es muy difícil y complejo dar una respuesta específica, sin embargo existen algunos lineamientos que permiten decidir cual VPN conviene a una organización específica.

A continuación se presentan una serie de preguntas que el grupo que esta implementando una VPN debe plantearse antes de decidirse por una solución VPN.

- ✓ Sabe que es una VPN?
- ✓ Los ahorros en el costo son el único propósito?
- ✓ Utilizará la VPN para comercio global?

- ✓ Instalará una extranet?
- ✓ Su organización posee la capacidad técnica adecuada para mantener e instalar una VPN?
- ✓ Que tipo de seguridad utilizará?
- ✓ Qué tipo de arquitectura de hardware soporta mi organización?
- ✓ Cuántos usuarios estima que utilizará esta VPN?

Estas preguntas son sólo un ejemplo de las muchísimas que pueden surgir y cada una puede ser de gran consideración para su organización. De igual manera pueden surgir preguntas que deben ser contestadas por el personal de Sistemas antes de decidirse por instalar una VPN.

A continuación empezaremos a describir cada arquitectura de las VPN más populares:

- ✓ VPN proporcionada por un ISP
- ✓ VPN basada en cortafuegos
- ✓ VPN basada en Caja Negra
- ✓ VPN basada en enrutador
- ✓ VPN basada en Acceso Remoto
- ✓ VPN con herramientas proxy
- ✓ VPN basadas en software

4.1.- VPN proporcionada por un Proveedor de Servicios de Red.

Este tipo de servicio son proporcionados por los Proveedores de Servicio de Internet (ISP), el cual se encarga de mantener el túnel entre nuestra organización y el ISP. Correspondería al ISP mantener la VPN funcionando adecuadamente, y para esto el ISP se haría cargo de la instalación y configuración de la VPN, y si así lo requiere el ISP puede instalar un dispositivo en las oficinas de nuestra organización o en su compañía, el cual creará el túnel por nosotros [LIB02].

El problema en este tipo de arquitectura es de quién se haría cargo de cada responsabilidad. Por ejemplo quién es responsable de la seguridad, nuestra organización o el ISP que nos ofrece el servicio de VPN; quién es el responsable de los equipos de comunicación, lógicamente si el ISP instala su propio equipo, entonces la responsabilidad sería del ISP, pero además de esto, hay que definir quién es el responsable de la comunicación entre nuestra red y el equipo que instaló el ISP para proporcionar la VPN. Ver figura 4.1

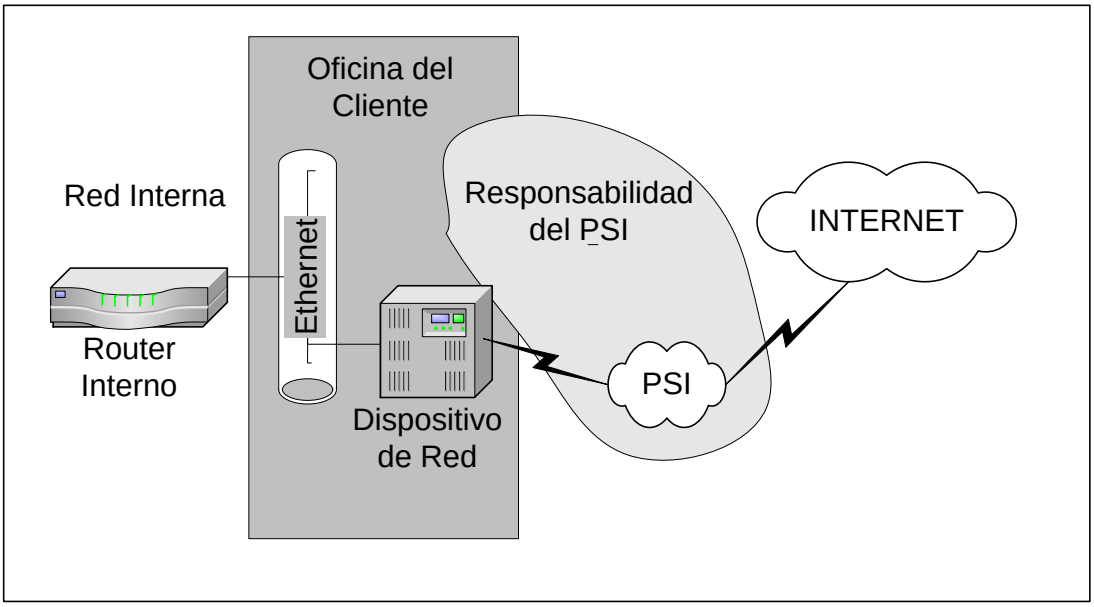


Figura 4.1.- VPN proporcionada por el proveedor de servicios de Internet

Para ilustrar un poco el panorama observemos algunos de los problemas que se tiene que esclarecer antes de instalar una VPN por parte de un PSI.

Seguridad.

La seguridad no debe estar en manos del proveedor de servicios de Internet, aún si proporciona el equipo para realizar la VPN. Tome en cuenta que los PSI primero proporcionan servicios de Internet y en segundo lugar servicios de VPN.

La seguridad debe estar en manos de la organización propietaria de la VPN, tomando en consideración que son las acciones de los propios usuarios los que pueden ocasionar los problemas de seguridad.

Control de cambios.

Antes de implementar una VPN con un PSI se necesita esclarecer quién hace los cambios en el control de la política de acceso y cuanto le toma implementar estos cambios. El proveedor de servicios de Internet no puede estar disponible o puede estar ocupado resolviendo otros problemas. Además al añadir nuevos servicios es posible que se requiera parar el funcionamiento de la VPN, de tal forma que eventualmente podría pasar por varios controles de cambios y necesitará seguirle la pista a cada uno de ellos y supervisarlos.

De igual forma necesita determinar como vigilar el control de cambios. Si solicitó un cambio en su arquitectura existente debe saber cómo y cuándo se implemento esa solicitud.

Solución de problemas.

En cualquier tipo de arquitectura de VPN, cuando las cosas van mal u ocurren problemas, ¿Quién puede ayudarle?. Es el proveedor de servicios de Internet el llamado a solucionar los problemas, y éste estará en la predisposición de solucionarlos si importarles el tiempo que le tome?

Autorización.

Usted necesita saber cómo y cuándo se añadieron usuarios a una base de datos lo cual les permitirá crear un túnel de VPN hacia su organización. ¿La base de datos esta en el dispositivo de la VPN proporcionado por el Proveedor de servicios de Internet o en algún servidor interno bajo su control? ¿Puede obtener acceso a él, de lo contrario, cuánto tiempo se requiere para que una autorización del usuarios se vuelva efectiva?. Esto es importante en el caso de un empleado despedido; si un empleado deja la compañía es muy importante que su acceso se restrinja de inmediato, no después de un día.

Utilización de la red

Es necesario estar consiente de cómo funciona la red en general. La organización o su Proveedor de servicios de Internet deben vigilar el enlace para el uso del tráfico en el ancho de banda.

Utilización de dispositivos

Su dispositivo VPN es justo como cualquier máquina o pieza de software ubicada en alguna parte de su organización. Alguien tendrá que mirar su desempeño, vigilar su salud y prevenir los problemas. Recuerde, la máquina no le pertenece, está en su sitio, pero bajo el control del proveedor de servicios de Internet.

4.2.- VPN basadas en Cortafuegos.

Las VPN basadas en cortafuego son la forma más común de implementación de VPN hoy en día, y muchos proveedores ofrecen este tipo de configuración; esto no significa que sean mejores, sino más bien se trata de una base establecida a partir de la cual crecer, como se indica en la figura 4.2 [LIB02].

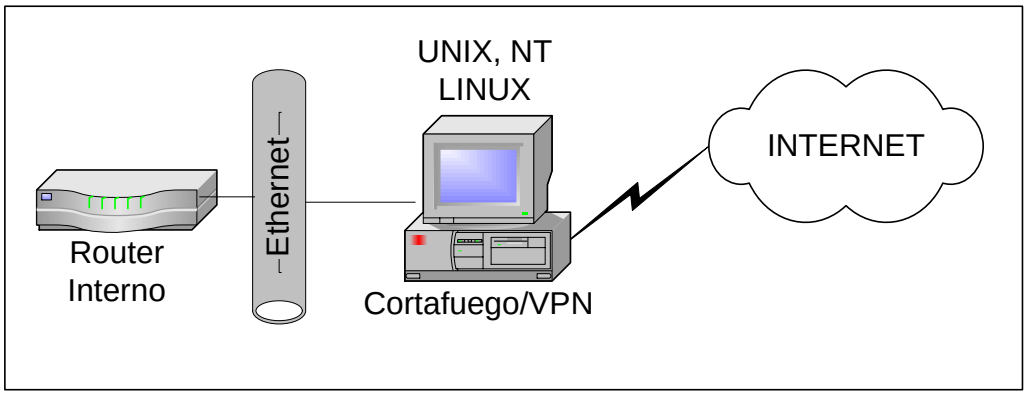


Figura 4.2: VPN basada en cortafuego

En la actualidad todas las organizaciones conectadas a Internet utilizan algún tipo de cortafuegos, lo que se trata es de utilizar esta infraestructura para crear la VPN, y lo único que se necesita es añadir software de cifrado. En estos días

casi la mayoría de software cortafuegos incluyen la capacidad para implementar tecnología de cifrado VPN.

Existen muchos proveedores entre los cuales elegir cuando se considera una VPN basada en cortafuego, y los productos están disponibles en todas las plataformas. Un aspecto importante de la seguridad es el sistema operativo en el cuál se esta ejecutando el cortafuegos, y hay que estar consientes de las vulnerabilidades de ese sistema operativo. No existe un dispositivo cien por ciento seguro, así que si crea la VPN en ese dispositivo, necesitará asegurarse de que el sistema operativo subyacente sea seguro.

Antes de instalar una VPN basada en cortafuego se cebe decidir la norma que se va a utilizar. Por ejemplo, se desea utilizar la norma PPTP, L2TP, o IPSec.

Hay que tener en consideración que los cortafuegos tienen tres tipos de implementaciones entre las cuales elegir: Inspección de estados, proxy y filtrado de paquetes, Un cortafuego de inspección de estados se ejecuta en los niveles dos y tres del modelo OSI, Un servidor Proxy se ejecuta en el nivel 7, el modelo de aplicaciones del modelo OSI, y el cortafuego de filtrado de paquetes también tiene que examinar el paquete completo cada vez que pasa.

Por la razón mencionada anteriormente, cuando se dice que se debería añadir tecnología VPN al cortafuego, se refiere a añadir tecnología VPN únicamente a un cortafuego de inspección de estados. De la misma manera que la tecnología VPN en sí misma se ejecuta en los niveles más bajos de la pila de OSI, el cortafuego también debe hacerlo, o de lo contrario podría caer en problemas de desempeño.

4.3.- VPN basadas en Caja Negra.

Se trata de un dispositivo cargado con software de cifrado para crear un túnel de VPN. Algunas cajas negras vienen equipadas con software que se ejecuta en el cliente, para ayudar a administrar el dispositivo, y otras se las puede administrar mediante el explorador de Internet. Por ser un dispositivo de hardware se cree que las VPN instaladas con estos equipos son mucho más rápidas que los tipos

basados en software, ya que crean túneles más rápidos bajo demanda y ejecutan el proceso de cifrado mucho más rápido. Aunque esto puede ser verdad, no todos ofrecen una característica de administración centralizada [LIB02].

Además se requiere otro servidor si se quiere llevar a cabo la autenticación de los usuarios, aunque algunos fabricantes si soportan la autenticación de usuarios, pero no es muy aconsejable tener todos los usuarios en el mismo equipo.

Un punto importante a tomar en consideración en este tipo de dispositivos es que debería soportar los tres protocolos para establecimiento de túneles, PPTP, L2TP e IPSec, además algunos de estos dispositivos están empezando a incorporar capacidades de cortafuego.

El dispositivo VPN de caja negra se sitúa por lo general detrás del cortafuego, aunque también puede situarse a un lado del mismo[1].

El cortafuego proporciona seguridad a su organización; pero no provee seguridad para sus datos. De igual manera el dispositivo VPN brindará seguridad a sus datos, pero no a su organización. La figura 4.3 muestra una solución de VPN de caja negra.

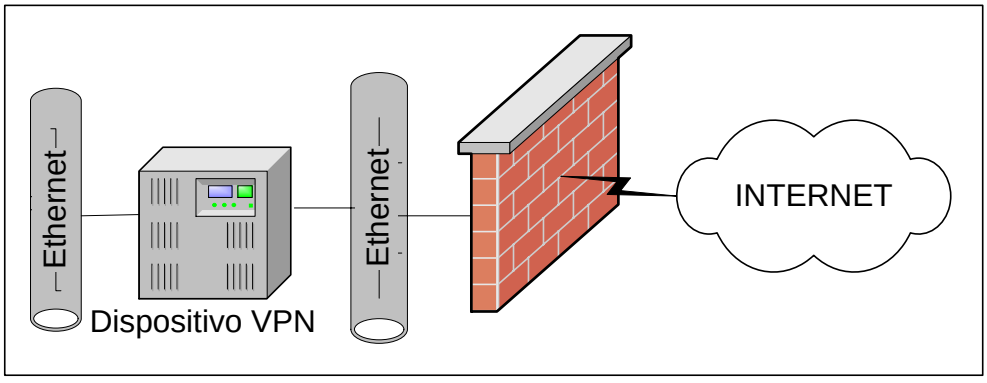


Figura 4.3: VPN de Caja negra

[1] Revise el capítulo correspondiente a Topologías de VPN

En la configuración del cortafuego hay que dejar pasar los paquetes cifrados. El cortafuego esta ahí para protección. Si usted esta filtrando en los puertos TCP y los paquetes vienen cifrados, el cortafuego tratará de examinar el paquete, se dará cuenta de que no puede hacerlo y lo soltará. Por consiguiente, debe asegurarse de que su cortafuego pasará esos paquetes.

4.4.- VPN basadas en enrutador.

Este tipo de arquitectura es adecuada para organizaciones que ya tiene instaladas una base de enrutadores, y que además soporten VPN. Existen dos tipos de VPN basadas en enrutadores. En uno de ellos el software se añade al enrutador para permitir que el proceso de cifrado ocurra. En el segundo método se inserta una tarjeta externa de otro proveedor en el mismo chasis del enrutador, este método esta diseñado para que la tarjeta insertada realice el proceso de cifrado y liberar de esta tarea al CPU del enrutador [LIB02].

Algunos enrutadores soportan intercambio en activo y redundancia, lo cual esta integrado en el producto, esto puede ser necesario para las organizaciones que sólo pueden permitir un tiempo de inactividad corto.

Se debe tener en consideración que el desempeño puede ser un problema en VPN basadas en enrutador, debido a la adición del proceso de cifrado al proceso de enrutamiento. Lo que estamos haciendo es agregar una carga más pesada al enrutador, especialmente si este esta manejando una gran cantidad de rutas o esta implementando un algoritmo de enrutamiento intensivo.

De igual manera como en los productos basados en caja negra, se debe tomar en consideración de que los enrutadores soporten todos los protocolos de seguridad de Internet y aquellos que se utilizan para el establecimiento de túneles de la VPN como por ejemplo PPTP, L2TP e IPSec, ya que estás nos garantizarán la interoperabilidad. Además, el enrutador implementará autenticación de usuarios, o para hacerlo necesitará un dispositivo independiente compatible con él. La figura 4.4 muestra una VPN típica basada en enrutador, en la cual los paquetes se cifran desde el origen hacia el destino.

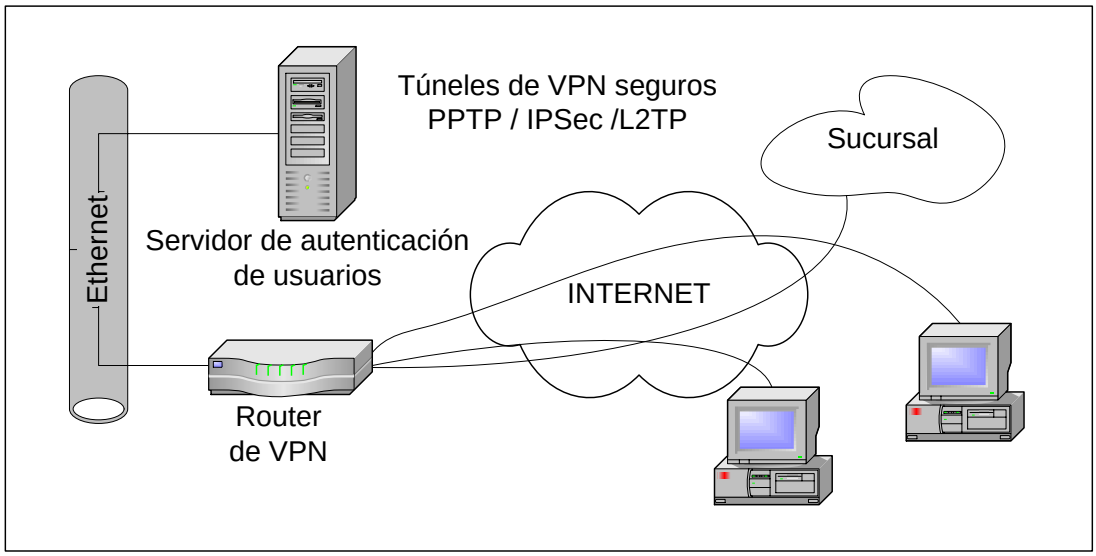


Figura 4.4.- VPN basada en enrutador

Existen dos inquietudes con las VPN basadas en enrutador:

- ✓ Interoperabilidad. Si desea conectarse a las VPN de los proveedores, su enrutador y el enrutador de sus proveedores trabajarán en conjunto y crean la VPN?
- ✓ Encapsulamiento. Van a transportar protocolos que no son IP, como IPX o SNA a otro sitio? Algunos fabricantes de enrutadores solo cifran y no encapsulan.

4.5.- VPN basadas en acceso remoto.

El acceso remoto significa que alguien de afuera esta tratando de crear un flujo de paquetes cifrados hacia su organización. Este túnel podría venir de Internet, pero también podría venir de una línea de marcación. La figura 4.5 muestra un escenario típico de acceso remoto [LIB02].

Este escenario tiene software que se ejecuta en una máquina remota en alguna parte y esa máquina intenta establecer una conexión a través de un túnel cifrado

al servidor interno de la organización, o desde una línea de acceso por marcación hacia un servidor de autenticación. Un servidor de acceso instalado en su red, ya sea un enrutador, un cortafuego, una caja negra o un servidor de autenticación independiente concede el acceso. Este dispositivo de acceso remoto reduce la cantidad de los costosos equipos de líneas rentadas y de acceso por marcación remota.

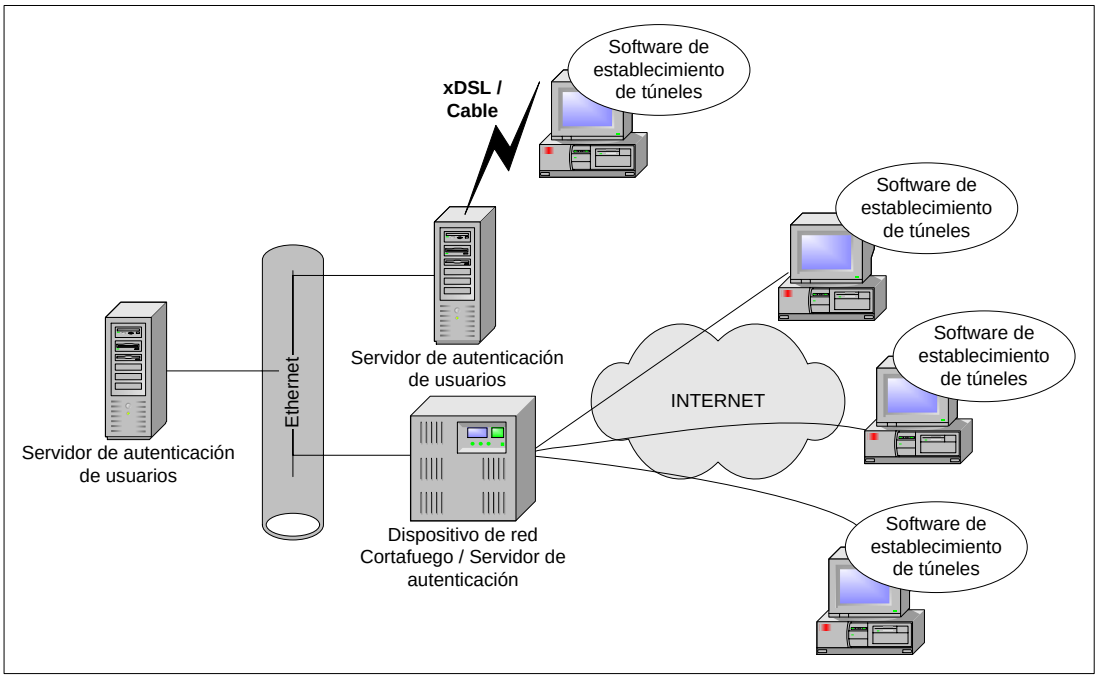


Figura 4.5.- Escenario de acceso remoto

4.6.- VPN con herramientas proxy.

En la actualidad con las aplicaciones recientes, como la telefonía IP y las tele conferencias, cuando se hace una conexión para una aplicación específica en un puerto determinado, la respuesta que el servidor envía de regreso llega a varios puertos. Así que, ¿cómo se debe configurar la VPN para que se maneje varias conexiones de entrada que se originan desde una solicitud de salida? ¿Qué sucede si se tiene un producto de cortafuego / VPN? ¿Qué puertos se abrirán? [LIB02].

La organización no desea abrir puertos innecesarios debido a posibles violaciones en la seguridad, pero en el caso de las tecnologías más nuevas, es necesario. Si no puede abrir estos puertos, se debe asegurar que la arquitectura de VPN soporte tecnologías nuevas como la telefonía IP, el envío de fax por Internet, entre otros.

Así que si esta haciendo una solicitud para una aplicación multimedia y la respuesta llega a varios puertos es necesario tener una arquitectura de VPN llamada Kit de herramientas proxy para VPN, la cual se indica en la figura 4.6.

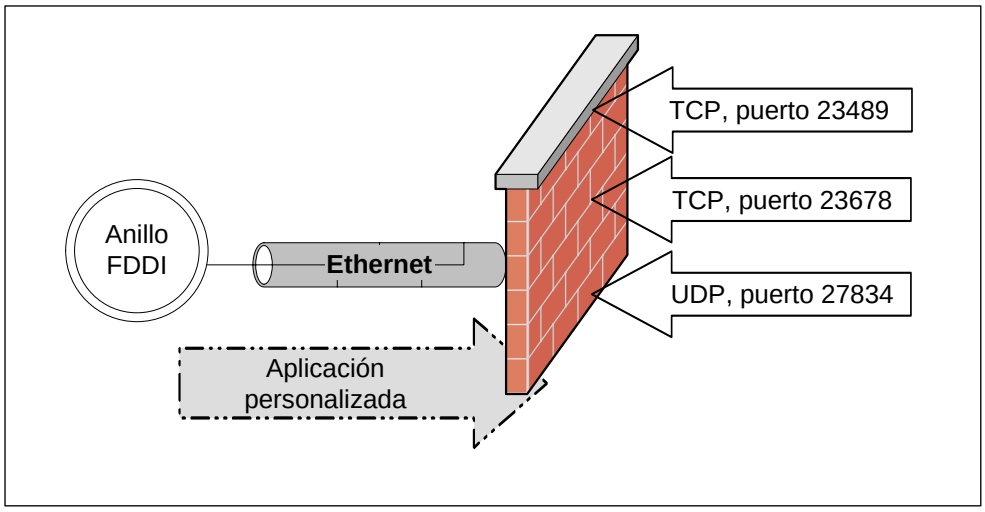


Figura 4.6.- Kit de herramientas de VPN

4.7.- VPN basadas en software.

Una VPN basada en software básicamente es un programa para establecer túneles o cifrado a otro anfitrión. Por lo general se utiliza desde un cliente a un servidor. Por ejemplo, en una VPN de PPTP, el software cargado en el cliente se conecta al software cargado en el servidor y establece una sesión de VPN [LIB02].

El tráfico inicia desde un anfitrión específico en su organización y establece una conexión a algún servidor en otra parte. El tráfico que sale desde el anfitrión se cifra o se encapsula, dependiendo de la VPN instalada, y se enruta hacia su destino. Lo mismo ocurre para alguien que esta tratando de conectarse a su red interna; una máquina cliente en alguna parte inicia una sesión de cliente VPN e instaura un diálogo de comunicación con el servidor VPN de su organización. Esta comunicación establece que tipo de cifrado y cuáles algoritmos de autenticación deben utilizarse y otros datos importantes para iniciar la comunicación. Después de que le proceso inicial se ha completado, comienza el flujo de datos. En la figura 4.7 se ilustra una VPN basada en software.

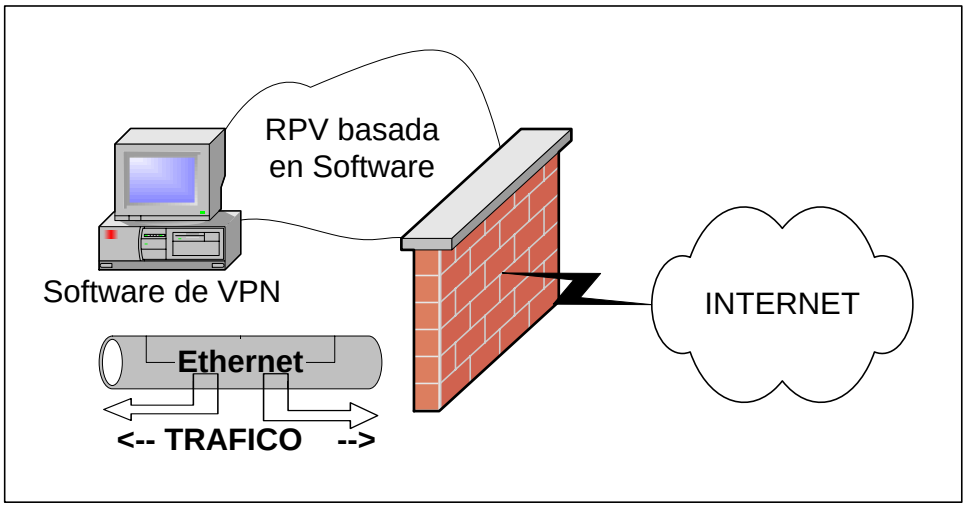


Figura 4.7.- VPN basada en software.

CAPITULO V

TOPOLOGIAS DE RED PRIVADA VIRTUAL

5.1.- Topología de Cortafuego/VPN a Cliente
5.2.- Topología de VPN/LAN a LAN
5.3.- Topología de VPN/Cortafuego a Intranet/Extranet
5.4.- Topología de VPN/Tramas o ATM
5.5.- Topología de VPN de hardware(Caja Negra)
5.6.- Topología de VPN/NAT
5.7.- Túneles de VPN anidados

En el presente capitulo se tratará de mostrar donde se debe colocar el dispositivo VPN en la topología de su red. Todas las opciones disponibles dan la oportunidad de aprovechar completamente la tecnología VPN. Los dispositivos VPN pueden ser internos, lo que significa que puede dejar que pasen los paquetes cifrados a su red sin necesidad de ser modificados por un enrutador o cortafuegos (Siempre y cuando el permiso este garantizado).

Además se tratará de explicar muchas de las topologías más comunes como por ejemplo: VPN de cortafuego a equipo portátil, VPN de LAN a LAN, topologías anidadas y topologías de túneles son sólo algunas de las configuraciones de topologías que se tratará de analizarlas.

Así como existen algunas maneras para adquirir e implementar una arquitectura de VPN, también existen muchas formas de colocar esta arquitectura en una topología de VPN, teniendo presente que las VPN y la seguridad van de la mano.

Al pensar en donde colocar su arquitectura VPN, observe primero la topología de la red de su conexión a Internet. Después examine las oficinas remotas que tendrán su propia conexión a Internet y dónde quiere crear el túnel de VPN.

Comenzar con lo básico ayudará a imaginar el flujo de datos y a determinar cuáles son los dispositivos de red por los que pasan los datos cifrados. Posiblemente los filtros colocados en algunos dispositivos bloquee los datos cifrados o, si el dispositivo tiene que examinar estos datos cifrados, tal vez reducirá el desempeño. Por lo tanto el primer paso consiste en examinar los flujos de datos cuando se estudia la topología.

Las topologías son las siguientes:

- ✓ Topología de cortafuego/VPN a Cliente
- ✓ Topología de VPN/LAN a LAN
- ✓ Topología de VPN/Cortafuego a Intranet / Extranet
- ✓ Topología de VPN/Tramas o ATM
- ✓ Topología de VPN de hardware (Caja Negra)
- ✓ Topología de VPN/NAT
- ✓ Túneles de VPN anidados

5.1.- Topología de cortafuego/VPN a Cliente.

Empezaremos con ésta ya que es la topología de uso más común y prácticamente todas las organizaciones que implementen una VPN utilizarán este tipo de configuración. En la actualidad casi todas las organizaciones conectadas a Internet tienen un cortafuego instalado, y todo lo que se necesita es agregar software de VPN al cortafuego. Este tipo de topología es la más común y posiblemente la más fácil de configurar para los que tienen un cortafuego colocado, y sólo desean aumentar la funcionalidad de la VPN[LIB02].

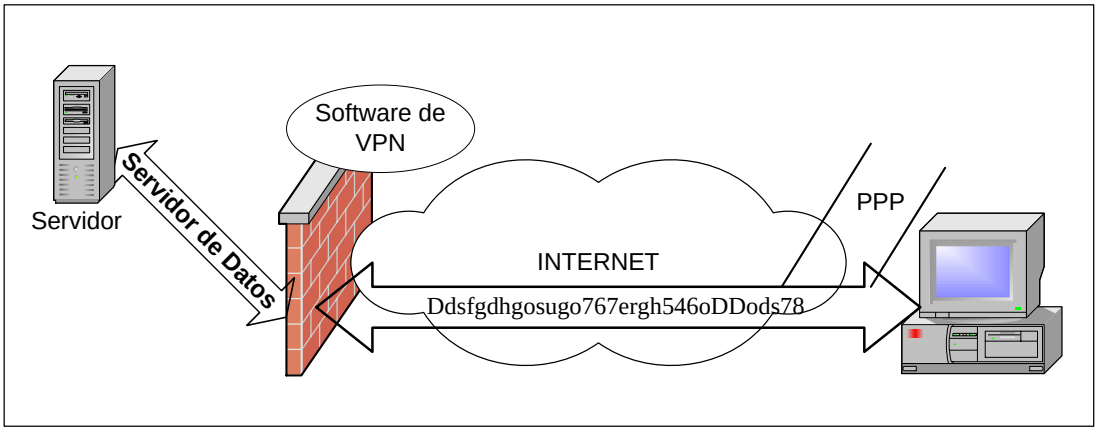


Figura 5.1.- Topología de Cortafuego[2]/VPN a Cliente

Como se indica en la figura 5.1 un usuario en su equipo portátil remoto necesita el acceso a un servidor que se encuentra dentro de la red de la organización, detrás de un cortafuego / VPN, para obtener un reporte confidencial. Esta es la configuración cliente / VPN típica. En ella existen dos componentes que deben habilitarse para establecer la comunicación:

- ✓ El dispositivo de cortafuego/VPN debe ejecutar algún tipo de código VPN, además de que deben agregarse algunas reglas al cortafuego

[2] El término **Cortafuego** se utiliza en español. El término **Firewall** se lo utiliza en Inglés

como por ejemplo para permitir el cifrado, y dejar pasar los datos cifrados, entre otras.

- ✓ El equipo portátil tiene una pila VPN instalada. Se trata de una pila de VPN puesto que una aplicación de VPN implicaría que el código corriera en el nivel 7 (aplicación) del modelo OSI, y la pila de VPN en realidad se encuentra en los niveles 2 (enlace de datos) y 3 (red).

También hay que tomar en consideración que si se utiliza el cifrado propietario de un fabricante y tiene un cifrado diferente en el cortafuego/VPN, no existirá una comunicación entre ambos. Si utiliza el encapsulamiento en el cortafuego / VPN, también deberá utilizarlo en el equipo portátil.

Los siguientes pasos describen el proceso de comunicación entre el equipo portátil y el servidor interno una vez que se han completado las configuraciones:

- ✓ El usuario en el equipo portátil marca a su proveedor de servicios de Internet local y establece una comunicación PPP.
- ✓ El equipo portátil solicita las claves del dispositivo del cortafuego/VPN.
- ✓ El cortafuego responde con la clave apropiada.
- ✓ El software de VPN instalado en el equipo portátil espera a que el usuario intente tener acceso al servidor interno (conocido como la dirección IP de destino). Si le usuario visita cualquier sitio distinto al de la red corporativa, no pasa nada. Pero si el usuario quiere realizar una conexión con el servidor interno, el software que se ejecuta en el equipo remoto ve la solicitud (conocida como una dirección IP), cifra el paquete y lo envía a la dirección IP pública de la combinación Cortafuego/ VPN.
- ✓ El dispositivo de Cortafuego/VPN le quita la dirección IP, descifra el paquete y lo envía al servidor dentro de la LAN local.
- ✓ El servidor interno responde la solicitud y envía el documento de regreso.
- ✓ El cortafuego /VPN examina el tráfico y por su tabla sabe que es una configuración de túnel de VPN. Así que toma el paquete, lo cifra y lo envía al equipo remoto.

- ✓ La pila de VPN en el equipo remoto ve el flujo de datos, sabe que viene del dispositivo de cortafuego/VPN, descifra el paquete y lo maneja en aplicaciones de niveles superiores.

Esta configuración es la que permite que la VPN tenga una gran flexibilidad, ya que se puede utilizar Internet como nuestra propia red privada, y muchos de los ahorros en los costos viene de esta configuración.

Hay que vigilar dos aspectos en este tipo de configuración:

- ✓ Las configuraciones del equipo remoto; este software tiene la tendencia a interactuar con otras aplicaciones y provoca problemas de interoperabilidad.
- ✓ Esta configuración añade una sobrecarga al proceso de cifrado / descifrado en el cortafuego. Se debe tomar en cuenta a ver si existen problemas de desempeño en el cortafuego.

5.2.- Topología de VPN/LAN a LAN.

Luego de haber utilizado la topología de Cortafuego/VPN a cliente las organizaciones se han dado cuenta que pueden extender sus VPN para brindar servicios a distintas oficinas remotas. Este tipo de topología es la segunda más comúnmente utilizada; teóricamente, se pueden utilizar tanto un cortafuego basado en Windows NT como uno basado en Unix, pero ambos utilizando un cifrado común, por ejemplo DES, y deberán ser capaces de comunicarse entre sí.

En la figura 5.2 aparece una organización con una oficina remota, las dos tiene su cortafuego propio, una es una máquina basada en Windows NT y la otra es una máquina basada en Unix. Ambas ejecutan software de VPN de distintos fabricantes y el algoritmo de cifrado utilizado en los productos VPN de los fabricantes es DES.

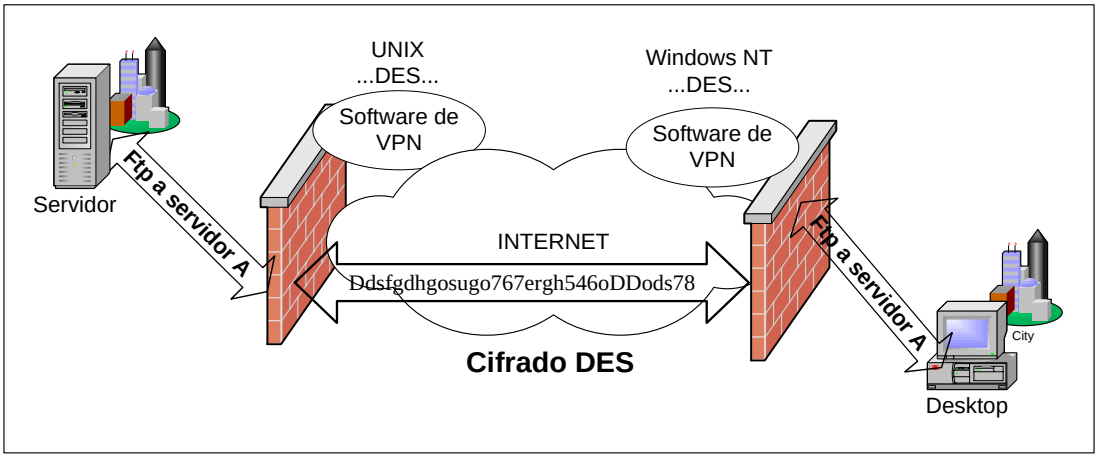


Figura 5.2.- Topología de VPN de LAN a LAN

El ejemplo [LIB02] presenta a un usuario de la oficina remota que necesita conectarse al servidor de la otra oficina y hacer una transferencia FTP para transferir un archivo: Antes de realizar la comunicación, los componentes que deben habilitarse son los siguientes:

- ✓ El administrador de cada sitio está de acuerdo con el cifrado DES. El software de VPN de cada dispositivo crea una clave única.
- ✓ Si se trata de un producto de cortafuego/VPN, el administrador de cada oficina establece una regla, por ejemplo, que todo el tráfico destinado a la otra terminal debe cifrarse.
- ✓ El usuario final utiliza una aplicación FTP en su escritorio para intentar conectarse al servidor.
- ✓ El paquete abandona el escritorio en texto sencillo y llega al dispositivo de cortafuego/VPN.
- ✓ El paquete es cifrado y se envía a la dirección IP pública del dispositivo de cortafuego/VPN de la otra oficina.
- ✓ El cortafuego/VPN acepta y descifra el paquete y lo reenvía a su destino final.
- ✓ El servidor recibe el paquete y responde.
- ✓ Envía un paquete en texto sencillo a su dispositivo de cortafuego/VPN local.
- ✓ Después, el cortafuego/VPN lo cifra y lo envía al otro cortafuego/VPN.

- ✓ El cortafuego/VPN lo descifra y finalmente lo envía de regreso al usuario original.

Lo importante aquí es que el usuario no tiene idea de que el cifrado se realiza. Además de esto el servidor no necesita una configuración especial, puesto que esta recibiendo solicitudes y respuestas normales. Los aspectos importantes aquí son los relacionadas con el enrutamiento; tanto la máquina del usuario como la red del servidor deben saber a que direcciones enrutar el dispositivo de cortafuego/VPN.

5.3.- Topología de VPN/Cortafuego a Intranet / Extranet.

En la actualidad las Intranet[3] y Extranet[4] son cada vez más populares. Normalmente las Intranet se utilizan internamente por el personal de la organización, y las Extranet se utilizan externamente por los clientes de la compañía [LIB02].

En la tecnología VPN estos servicios no han cambiado, pero ahora se ha agregado un nivel adicional de seguridad, y se puede tener acceso internamente o externamente a cualquier servicio. Esto tiene dos condiciones. En primer lugar se cuenta con flexibilidad para que una máquina se encargue de la Intranet y Extranet y por lo tanto se reduce la redundancia, y en segundo lugar se debe tener presente la seguridad, ya que existe una forma para que los usuarios externos tengan acceso a estos servidores.

La única diferencia entre las Intranets y Extranets VPN y no VPN es el punto donde se efectúa el proceso de cifrado. Si es en la máquina, piense en la seguridad como en u servidor Web típico. Si no, piense en que tanto permitirá que el tráfico externo penetre en su red.

[3] Intranet brinda lo mismos servicios de Internet (Por ejemplo servidor web, correo electrónico, servicios de noticias, entre otras), pero privadamente a una organización.
[4] Extranet brinda los mismos servicios de Internet pero el flujo de datos va de una organización hacia sus clientes.

La preocupación ahora es como identificar a los empleados que requieren los servicios de Intranet, pero que acceden a ellos externamente, y a los clientes externos a quienes sólo se les permite el acceso a la Extranet.

En la figura 5.3 se ilustra una posible solución para ubicar los servicios de Intranet y Extranet. En esta figura, el servidor web se mantiene en una red poco confiable, permitiendo que todos tengan acceso a este enlace de red. No importa que el dispositivo del cortafuego o de la VPN permita que los paquetes fluyan al servidor web sin modificación. (Aunque para implementar un nivel de seguridad más, el enlace DMZ1 del servidor web, sólo debe permitir que pase el tráfico HTTP del dispositivo VPN al servidor web, denegando los otros tipos de tráfico).

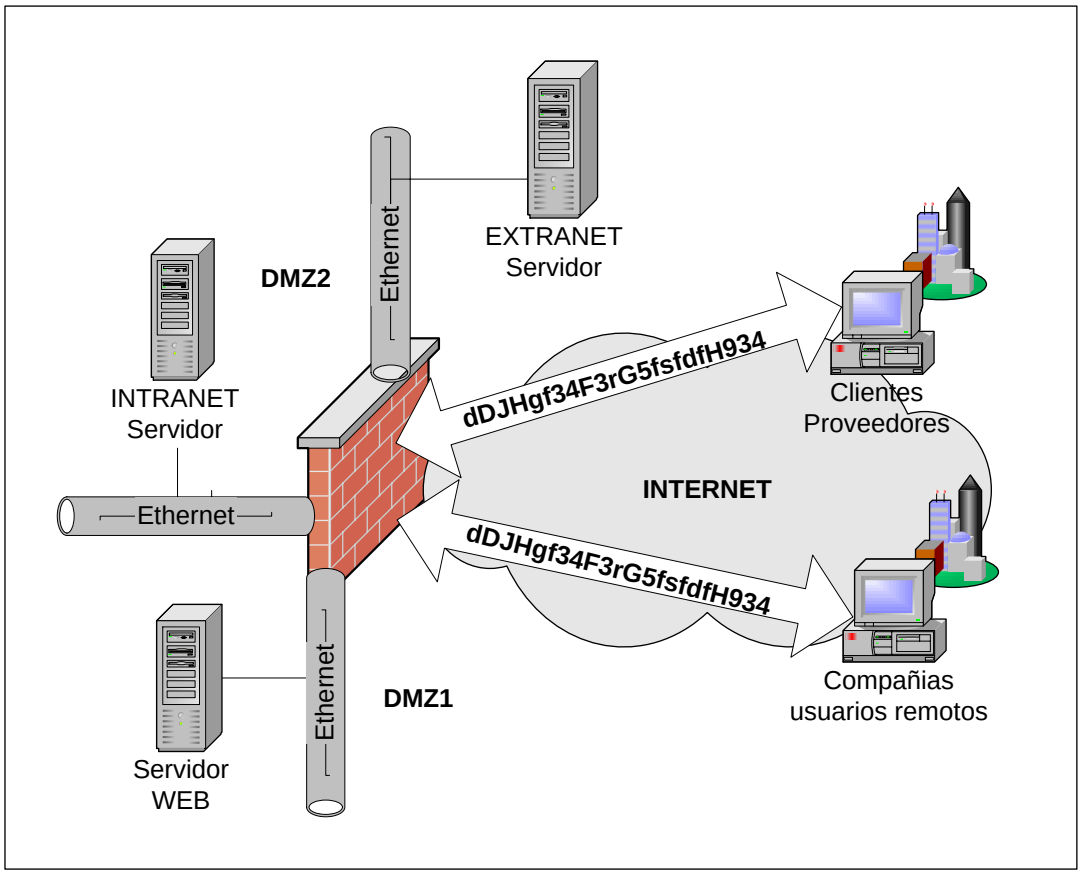


Figura 5.3.- Ubicación apropiada de la Intranet, Extranet y Servidor Web

La extranet se coloca en su propia red por separado. La seguridad que puede implementar aquí consiste en permitir que sólo aquellas direcciones de origen que considere necesarias pasen al dispositivo de cortafuego/VPN. Si su extranet se estableció entre varias compañías, es probable que lleguen desde sus propias redes internas (de las compañías), por lo tanto, se puede restringir el acceso sólo a esas redes. Pero, si alguien puede burlar las direcciones de origen, recuerde que cuando se estableció la comunicación se creo una VPN, por lo tanto los datos están cifrados y lo único que se esta haciendo es adicionando una restricción más.

Los clientes y los proveedores tienen permiso para conectarse al servidor de la extranet. El servidor web sólo es para tráfico web normal y esta disponible para todos. La Intranet se ubica detrás del dispositivo VPN y sólo los usuarios internos que llegan de Internet la usan.

Para concluir con este tipo de topología, es buena idea colocar los servidores de red de acuerdo con su función. Si está permitido el acceso público, colóquelo en una DMZ pública. Si hay clientes y proveedores externos, colóquelos en su propia DMZ. Si hay empleados, colóquelos en su propia DMZ. Con máquinas bien instaladas puede tener varias zonas DMZ; por ejemplo algunos fabricantes de cortafuego/VPN soportan hasta 32 DMZ.

5.4.- Topología de VPN/Tramas o ATM.

Si hay algo que agradecer a Internet es su flexibilidad casi en cualquier ámbito, y uno de ellos es la de habilitar comunicaciones instantáneas; pero siempre hay que tener en consideración un asunto de mucha importancia como es la seguridad. Es debido a la seguridad que muchas compañías construyen intranets empleando sólo líneas rentadas o enlaces basados en retransmisión de tramas para conectarse a sus sitios [LIB02].

Por lo tanto las VPN pueden configurarse sobre una infraestructura compartida tal como ATM o topologías de redes basadas en tramas. Loas organizaciones que ejecutan sus propias intranets sobre esta topología de VPN tienen la misma

seguridad, facilidad de administración y confiabilidad que en sus propias redes privadas.

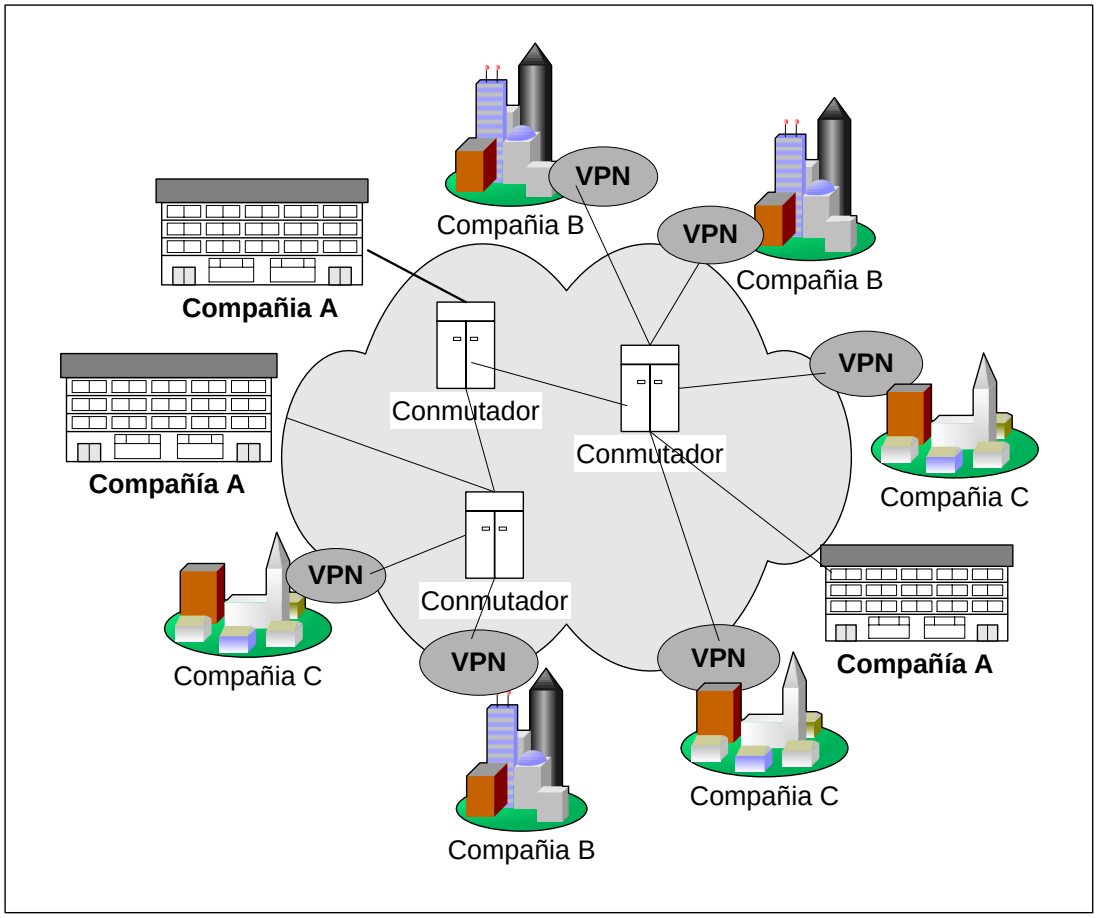


Figura 5.4.- VPN sobre un enlace ATM/tramas

En la figura 5.4 se muestra un ejemplo típico de una VPN sobre un enlace basado en tramas o ATM de algún proveedor de servicios de Internet. Este tipo de topología se configura de dos maneras:

La primera es IP sobre una infraestructura de red de tramas/ATM. Esta configuración combina el nivel de aplicación de los servicios IP sobre la capacidad de una red ATM. Dependiendo de la configuración del equipo, los paquetes IP se convierten en celdas y se transfieren sobre una red ATM. El

proceso de cifrado se ejecuta en estos paquetes antes de la conversión a celdas, y las celdas que contienen la carga IP cifrada se conmutan al destino final.

La segunda opción es la del grupo de trabajo de conmutación de etiquetas multiprotocolo (MPLS) del grupo de trabajo de Ingeniería de Internet (IETF). Esto permite que los proveedores de servicios busquen la integración de IP y ATM. En esta topología de red, los conmutadores inteligentes reenvían dinámicamente el tráfico IP en paralelo junto con el tráfico ATM en la misma red ATM. Al paquete se le aplica un campo que contiene un ID único que identifica al destino final. Todos los conmutadores de esta red ATM examinan este campo y lo reenvían a su destino apropiado. El atributo de seguridad de esto es que el paquete sólo se reenvía a su destino, evitando de esta manera su espionaje. Cualquier proceso de cifrado que pueda utilizarse aquí sólo se aplica a la porción de datos, antes de enviarlo a la nube de ATM. Debido a que esta configuración aplica un campo al paquete, no se pueden cifrar los encabezados del paquete; pero si se puede cifrar la carga útil, lo que implica que la funcionalidad completa de IPSec no se implementará. Sin embargo, al cifrar la carga y conmutarla sólo a su destino, si existe seguridad.

5.5.- Topología de VPN de hardware (Caja Negra).

Las VPN de hardware, o cajas negras, son dispositivos independientes que implementan algoritmos de tecnología VPN [LIB02].

Algunos soportan normas de cifrado como DES de 40 bits (internacional) y 3DES[5] (Estados Unidos y Canadá).

Muchas de las compañías dedicadas a ofrecer servicios de VPN, lo están haciendo tanto en hardware como en software, y a los dispositivos VPN basados en hardware les están añadiendo servicios adicionales como cortafuegos, antivirus, capacidad de enrutamiento, certificados digitales, soporte LDAP, la

[5] Lamentablemente el cifrado 3DES sólo se lo puede utilizar en los Estados Unidos, ya que este gobierno tiene prohibida su exportación.

vigilancia del correo electrónico y capacidades completas para Internet y para la marcación VPN.

Pero existe un par de problemas con los productos de hardware:

- ✓ Problemas de desempeño. Muchos dispositivos de hardware tiene problemas con los paquetes pequeños de 64 bytes.
- ✓ Funcionamiento limitado de subred. Algunos dispositivos presentan problemas para garantizar el acceso interno a los usuarios si la red está subdividida.

La figura 5.5 muestra una ubicación típica para estos dispositivos. El dispositivo se coloca detrás del cortafuego de la red interna.

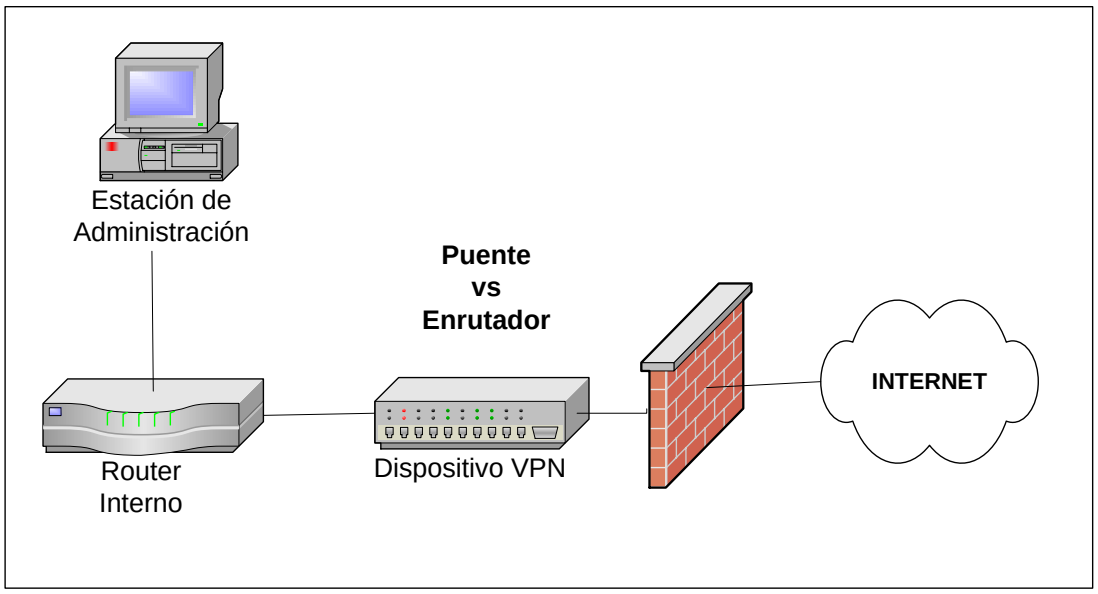


Figura 5.5.- VPN de caja negra detrás del cortafuego

Los paquetes de datos pasan por el cortafuego y por el dispositivo VPN. Conforme los paquetes de datos pasan por estos dispositivos, se mantienen intactos o se cifran, dependiendo de la configuración del dispositivo. La estación e administración se ubica en algún lugar de la red interna utilizada para

configurar el dispositivo, también existe la opción de utilizar un servidor web para configurar el dispositivo. Siempre hay que asegurarse tener creado un túnel para mantenimiento de estos dispositivos con la finalidad de modificarlos.

Otra ubicación para la VPN se indica en la figura 5.6 , en la cual el dispositivo VPN tiene el cortafuego junto a él, o en paralelo. A esto se le conoce como configuración de un brazo. Esta configuración le permite al dispositivo VPN crecer a cientos de túneles. El enrutador externo pasa el tráfico VPN al dispositivo VPN (por medio de la dirección de la VPN) y dirige todo el tráfico restante al cortafuego.

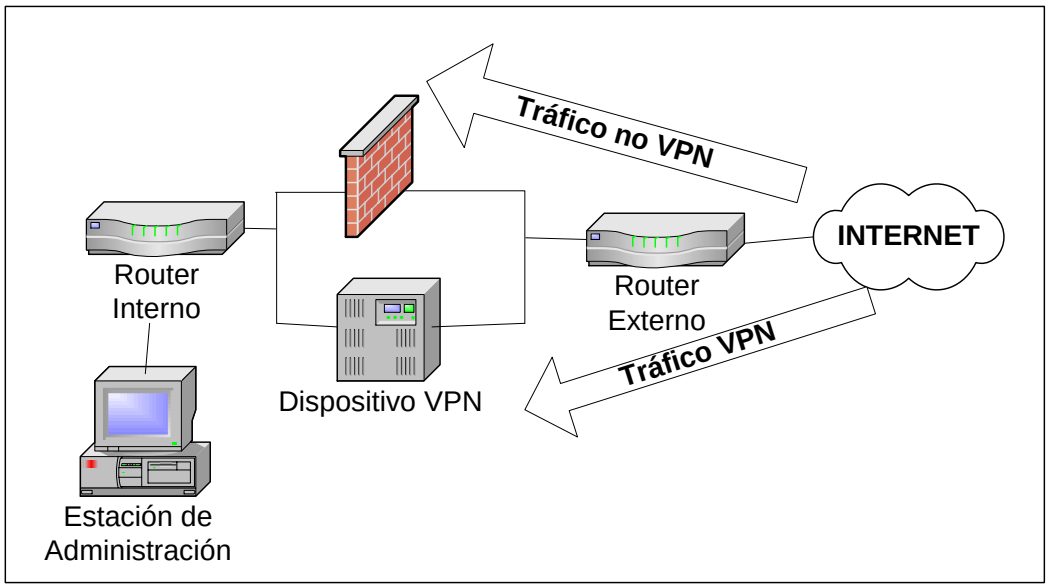


Figura 5.6.- VPN en paralelo con el cortafuego

Además como se muestra en la figura 5.7, también es posible agregar un cortafuego detrás del dispositivo de VPN en una configuración más elaborada. Cuándo se establecen túneles de VPN y se garantiza el acceso, estos se crean para destinos específicos. Si opta por hacerlo, después que el dispositivo VPN descifre el paquete, el cortafuego interno lo descifrara para ver su destino final y le permitirá o negará el acceso. También existe otra opción para que el dispositivo VPN reenvíe el tráfico a la interfaz de origen y pase por el otro

cortafuego. Se deberá configurar el enrutamiento en el dispositivo. Aunque no es una solución óptima, se puede realizar.

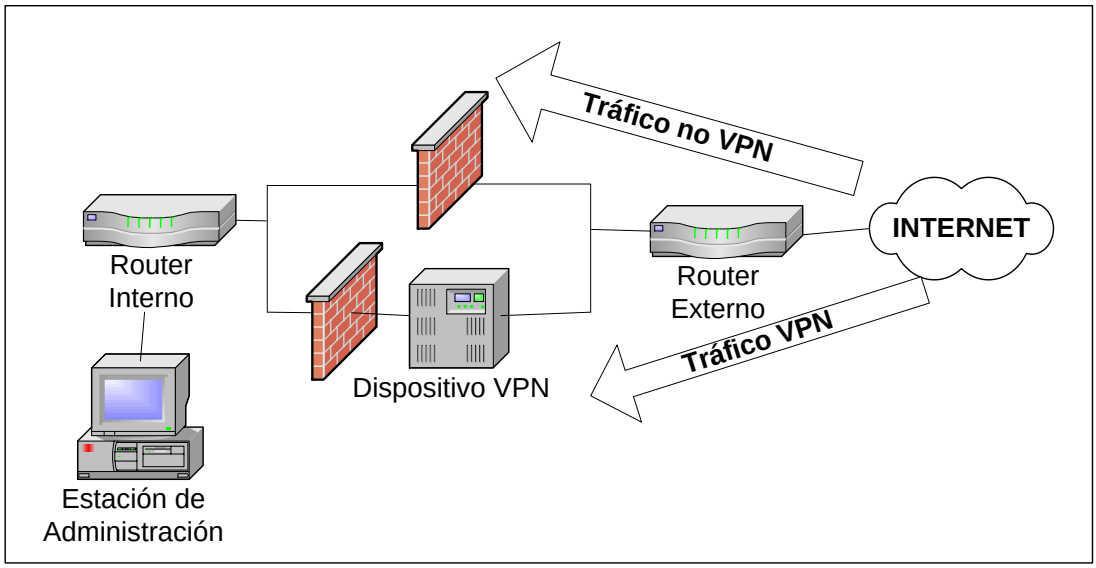


Figura 5.7.- Configuración VPN avanzada

5.6.- Topología de VPN/NAT.

Aunque la Traducción de Direcciones de Red (NAT) no es una VPN, se debe discutirla ya que muchas organizaciones lo tienen implementado, y los dispositivos VPN se ven afectados directamente por los procesos de NAT. La traducción de direcciones de red es el proceso de cambiar una dirección IP (por lo general la dirección privada de una organización) a una dirección IP pública enrutable. NAT proporciona un mecanismo para ocultar la estructura de la dirección privada de una organización. Utilizar la traducción de direcciones de red no es complicado, pero la ubicación del dispositivo VPN es importante [LIB02].

Si implementa a NAT en un paquete de VPN, ese paquete puede ser descartado; se debe recordar que una VPN es una configuración de IP a IP. La figura 5.8 muestra el flujo de tráfico que tiene lugar en un cortafuego que implementa a NAT mientras que el dispositivo VPN se encarga de la autenticación de usuarios.

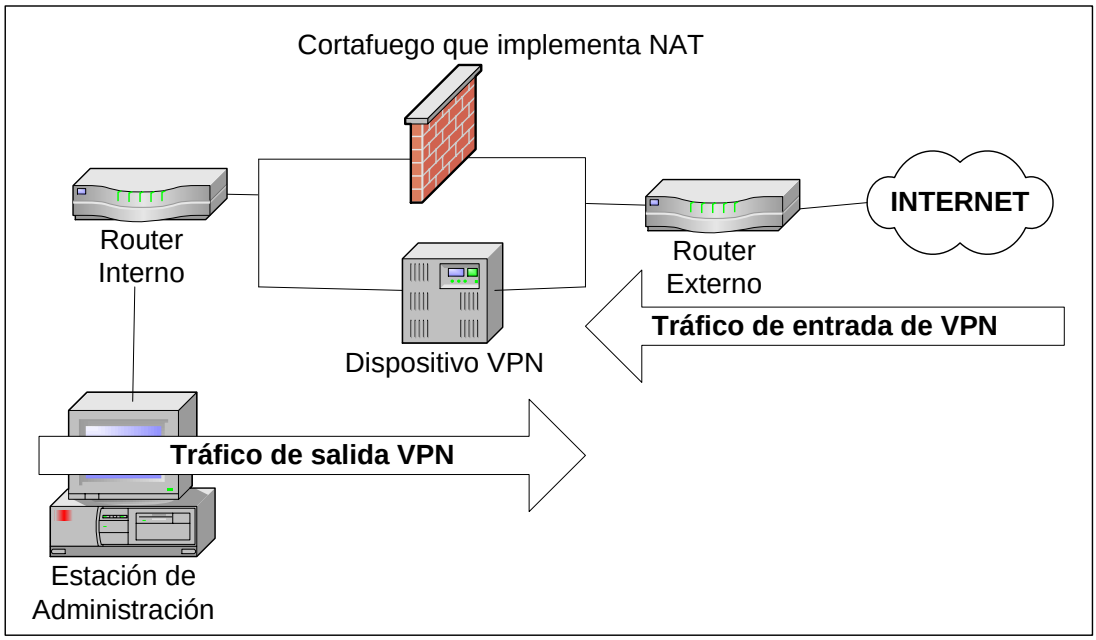


Figura 5.8.- Implementación de NAT con cortafuego y VPN

Estas dos reglas deben seguirse cuando se utilice NAT y VPN.

- ✓ Para paquetes de salida. Si tienen que pasar por NAT y ser parte de una VPN, NAT debe aplicarse antes de que el dispositivo VPN cifre los paquetes.
- ✓ Para tráfico de VPN entrante. NAT debe aplicarse después de que el cifrado de VPN se haya eliminado del paquete.

5.7.- Túneles de VPN anidados.

Los túneles de VPN anidados pueden considerarse como un túnel dentro de otro túnel. Existen muchas formas para hacer túneles anidados, una forma de emplearlos es cuando una organización requiere implantar seguridad punto a punto [LIB02].

La figura 5.9 muestra un túnel anidado, en la cual aparece un cliente PPTP que espera conectarse con el servidor PPTP. El proceso es el siguiente:

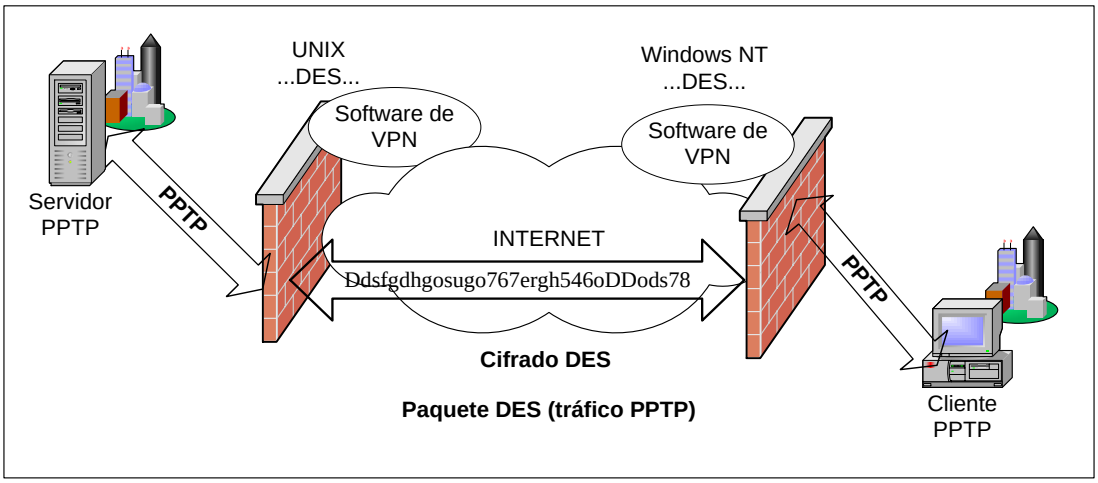
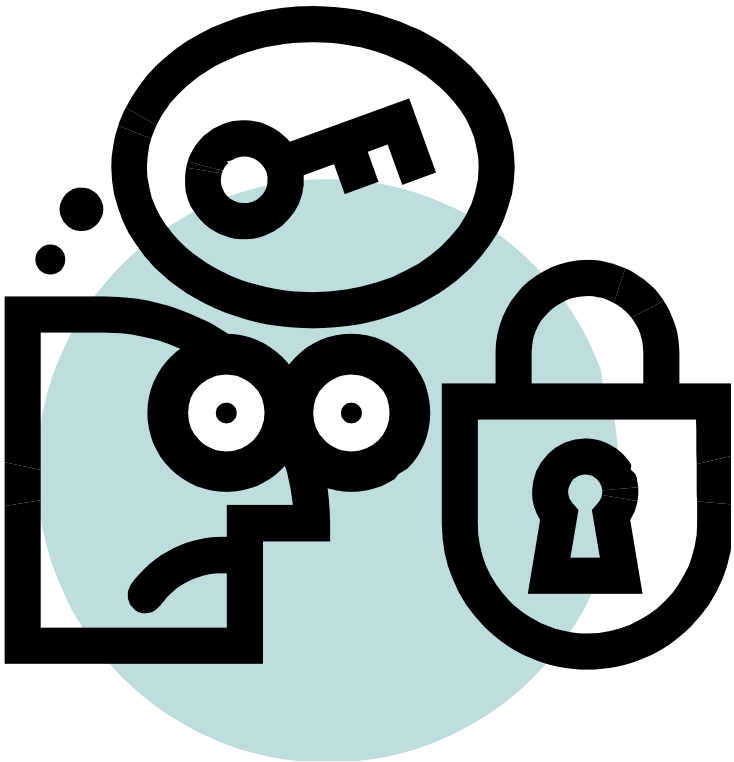


Figura 5.9.- VPN de túnel anidado

- ✓ El cliente PPTP realiza el proceso de cifrado en los datos desde la aplicación.
- ✓ Después, reenvía el flujo de datos cifrados al dispositivo de cortafuego/VPN, el cual añade cifrado DES al paquete. El cifrado DES puede implementarse como parte d la norma IPSec.
- ✓ El paquete es recibido por el dispositivo remoto de la VPN, el cual revisa la autenticación, quita el cifrado DES y lo envía a su destino final, que es el servidor PPTP.
- ✓ El servidor PPTP descifra el paquete PPTP y lo reenvía a las aplicaciones de nivel superior.

Antes de que dos dispositivos de cortafuego/VPN puedan realizar cualquier proceso de cifrado / descifrado, primero deben estar configurado entre ellos. Comúnmente se recomienda utilizar IPSec y PPTP en combinación.

CAPITULO VI



SEGURIDADES DE RED PRIVADA VIRTUAL

6.1.- Ataques a la red privada virtual
6.2.- Como identificar los ataques
6.3.- Importancia de la Seguridad en las VPN
6.4.- Requisitos de seguridad en las Redes Privadas Virtuales
6.5.- Sistemas Operativos

Los computadores son hoy en día una parte fundamental de la sociedad de la información en la que vivimos, han supuesto una revolución total en la forma de comunicarnos, de llevar a cabo nuestras necesidades básicas diarias, y que sin ellos la vida, tal como la concebimos hoy por hoy, sería imposible.

Resulta increíble que con tan sólo pulsar un botón podamos acceder a fuentes de información inmensas, situadas en cualquier parte del planeta y suministradas por personas de cualquier tipo. Que nuestro confort y bienestar dependan de máquinas que la gran mayoría ni conoce ni sabe cómo funcionan.

Pero esta facilidad de acceso a cualquier tipo de información y esta comodidad lograda con el uso de los computadores precisa que estas máquinas estén cada vez más interrelacionadas entre sí, comunicadas en todo momento con otras muchas, y sin lugar a dudas es Internet el mejor medio para conseguir esto.

Pero si esta apertura a la red de nuestras máquinas facilita la intercomunicación, también es cierto que con ella las situamos al alcance de todo tipo de ataques y contaminaciones externas, y es en este contexto en el que adquiere toda su magnitud la palabra clave SEGURIDAD.

La seguridad general abarca un sinnúmero de aspectos de la organización y este capitulo solo esta enfocado a la seguridad de la información, el cual abarca la seguridad de redes, la seguridad de las computadoras, la seguridad de acceso y la seguridad física, entre otras.

Con toda esta seguridad, es la administración superior de la organización quién decide que información es crítica y que información no lo es?,. Ya que es aquí donde se decide dar un valor a la información y proporcionar los recursos necesarios para protegerla. Además no todos los datos son confidenciales y no todos los datos comerciales son críticos.

La seguridad informática se ocupa de elaborar las normas y procedimientos que hacen al procesamiento seguro de la información en todos sus aspectos.

La seguridad persigue tres objetivos básicos:

Confidencialidad:

- ✓ Proteger la revelación de información a personas no autorizadas
- ✓ Restringir el acceso a información confidencial
- ✓ Proteger el sistema contra usuarios curiosos internos y externos

Integridad:

- ✓ Proteger los datos de cambios no autorizados
- ✓ Restringir la manipulación de datos a programas autorizados
- ✓ Proveer información verídica y consistente

Disponibilidad:

- ✓ Asegurar la continuidad operativa del sistema y proveer planes alternativos de contingencia
- ✓ Proteger el sistema contra acciones o accidentes que detengan los servicios o destruyan la información que brinda

La seguridad informática es asociada siempre con amenazas externas (como hackers o espías), pero la prevención de accidentes de usuarios autorizados (internos) es uno de los principales beneficios de una seguridad bien diseñada.

La seguridad es un gran problema, y lamentablemente pocos administradores de la seguridad están concientes de ello. Los sistemas informáticos están dispersos en toda la organización. Se dispone de numerosas máquinas de distinto tipo. Se interconectan en red con las sucursales y con otras empresas. Tenemos redes de área amplia, Internet, diversidad de plataformas, múltiples sistemas operativos, usuarios internos, externos, invitados, entre otros, computadoras personales, redes heterogéneas, computación móvil, virus, etc.

La seguridad es el tema central del tópico aplicaciones sobre Redes Privadas Virtuales, y cuando se piensa en la seguridad de redes, especialmente cuando se implemente en las Redes Privadas Virtuales, se debería revisar la pila de Interconexión de Sistemas Abiertos (OSI). La pila OSI consta de siete niveles:

aplicación, presentación, sesión, transporte, red, enlace de datos y físico. Cada nivel es responsable de su propio conjunto de funciones individuales, por ejemplo, confiabilidad, configuración, corrección, entre otras. Pero es aquí donde surgen problemas de seguridad, ya que los ataques más comunes en la actualidad suceden a través de todos estos niveles. Cada nivel puede atacarse y verse comprometido, por lo tanto, para que una red privada virtual sea segura es hacer que ésta se ubique en los niveles más bajos posibles de la pila OSI. La figura 6.1 muestra una ubicación óptima para la tecnología VPN [LIB02].

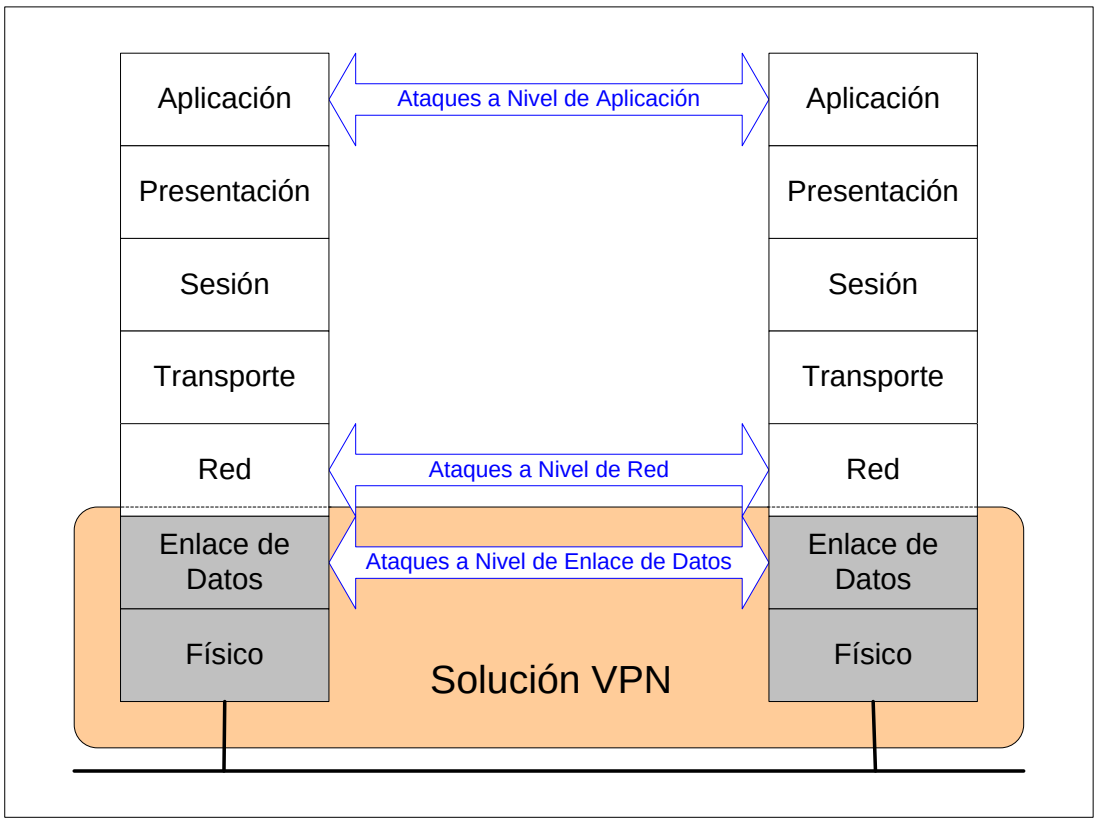


Figura 6.1.- Tecnología VPN en la pila de OSI

Pero hay que tener presente que esta ubicación puede provocar problemas de compatibilidad. Al implementar el software de red privada virtual en los niveles más bajos de la pila OSI, la tecnología tiene la posibilidad de interactuar más con los componentes específicos que forman el sistema operativo, y

lamentablemente, los controladores de dispositivos, los optimizadores y los módulos cargados pueden tener problemas de interoperabilidad con la tecnología de red privada virtual instalada y esto puede ser un problema más grave con los usuarios remotos que utilizan equipos portátiles y equipos de escritorio.

Control de acceso al usuario.

El modo de control de acceso al usuario solo admite los derechos y permisos de usuario requeridos para que realicen su trabajo. El control de acceso al usuario es extremadamente importante cuando se implementa una tecnología de Red Privada Virtual. Primero se tiene que asegurar de que sólo se concede permiso a los usuarios autorizados. Después debe asegurarse de que esos usuarios tienen concedido el acceso a aquellos recursos que usted considera necesarios para ese usuario.

Un comentario acerca de la seguridad es que siempre esta cambiando, y la implementación de sistemas de seguridad tiene que estar al día con esta manera de pensar. Durante años, las contraseñas simples fueron suficientes para las máquinas individuales y otros dispositivos de red, pero ahora han terminado con su vida útil.

La seguridad tiene un costo. Mientras más seguridad implementa en la organización, mayores serán los costos, además, los requisitos de mantenimiento y la experiencia técnica necesaria para administrar ese aumento de seguridad, no solo serán mayores, sino que también aumentará la irritación de los usuarios finales.

Es muy frustrante para el usuario final que el servidor de seguridad de la red se caiga, que el cortafuego no pase el tráfico, que el servidor de autenticación se venga abajo, o que los servidores web no acepten los certificados [WWW07].

6.1.- Ataques a la red privada virtual.

En esta parte se tratará de explicar rápidamente los tipos de ataques a las que pueden estar expuestas las redes privadas virtuales.

6.1.1.- Ataques a los algoritmos criptográficos.

Al igual que sucede en el software y el hardware, los algoritmos criptográficos también son vulnerables y están expuestos a ataques [WWW08], y generalmente existen tres formas de atacar un algoritmo de este tipo y son las siguientes: Ataques contra el protocolo, Ataques contra el algoritmo, Ataques contra la implementación.

Ataques contra el protocolo.- Si al realizar el cifrado no se utilizan los generadores de números aleatorio correctos, la reutilización de valores y demás funciones transformaciones de código, la integridad del protocolo será verá comprometida.

Ataques contra el algoritmo.- Uno de los principales problemas con los ataques criptográficos es que es posible que el usuario no este consciente de que ha sido atacado, lo que hace es depositar toda su confianza al algoritmo de cifrado. Pero hay que estar concientes que los algoritmos criptográficos también son sujetos de ataques. A continuación se presentan varias categorías comunes de ataque a algoritmos [LIB02].

Ataque de solo texto cifrado.- En un ataque de sólo texto cifrado, el agresor no sabe nada respecto al mensaje de texto simple, pero al obtener el texto cifrado, intenta obtener el texto simple. Lo que intenta el agresor es encontrar un patrón común donde puede identificar un conjunto de palabras de uso común. En la práctica esto es factible ya que la mayoría de documentos siguen ciertos formatos comunes, como por ejemplo, encabezados de formato fijo, las cartas, informes y memorando, comienzan de forma predecible.

Ataque de texto simple conocido.- En este ataque el agresor conoce parte del documento en texto simple o puede hacer conjeturas con cierta base sobre el

mismo. Este texto simple puede adivinarse debido a que es posible que sea un saludo, encabezado o sinopsis estándar. Debido a que el atacante tiene el texto cifrado, puede utilizar el texto simple para decodificar el resto del texto.

Ataque de texto simple seleccionado.- En este tipo de ataque, el agresor toma algún texto y lo cifra con la clave desconocida. En una inferencia, el atacante intenta adivinar la clave utilizada para ese cifrado.

Ataque de texto cifrado seleccionado.- El agresor tiene la ventaja de elegir un texto cifrado seleccionado arbitrariamente y puede encontrar el texto simple descifrado correspondiente.

Ataque de intermediario.- Es práctico para comunicaciones criptográficas y protocolos de intercambio de claves. Aquí dos partes intercambian sus claves para comunicaciones posteriores. El intermediario secuestra las claves del emisor y del receptor, y las sustituye por otras propias del intermediario, por lo cual tiene la capacidad de interceptar todas las comunicaciones futuras sin que el emisor y el receptor lo sepan. La única forma de impedir esto es con el uso de firmas digitales y con el mecanismo de claves secretas compartidas.

Ataque de sincronización.- Este tipo de ataque se basa en la medida de los tiempos de ejecución de una operación de exponenciación modular que se utiliza en los algoritmos criptográficos. Los criptosistemas toman cantidades de tiempo ligeramente diferentes para procesar entradas distintas. Cuando la CPU utiliza rutinas de optimización, ramificaciones, ciclos, instrucciones condicionales y demás, se utilizan distintas cantidades de ciclos de máquina. Es sabido que durante estos canales de sincronización los datos se pierden, aunque representan una cantidad mínima. Sin embargo los atacantes pueden explotar las medidas de tiempos o de sincronización de sistemas vulnerables para encontrar la clave secreta completa. Contra un sistema vulnerable, este ataque no es caro y a menudo requiere que se conozca el texto cifrado.

Ataque de fuerza bruta.- Un ataque de fuerza bruta es muy popular entre los agresores que tiene mucha capacidad de cómputo a su disposición. Lo que hace es simplemente tratar de ir probando una a una todas las claves posibles hasta encontrar la clave adecuada. Por ejemplo, el algoritmo DES tiene 2^{56} posibles

claves. ¿Cuánto tiempo nos llevaría probarlas todas si, supongamos, dispusiéramos de un computador capaz de hacer un millón de operaciones por segundo?. La respuesta es que tardaríamos más de 2200 años. Pero este algoritmo ya fue quebrantado por la Fundación de la Frontera Electrónica utilizando un método de fuerza bruta.

Criptoanálisis diferencial.- En los ataques de este tipo, el agresor utiliza la relación de la información que se basa en una información repetida. Al basar los resultados en un gran número de pares de texto cifrado, cuyas contrapartes de pares de texto simple satisfacen una diferencia XOR conocida en lo que respecta al componente, el atacante puede determinar la clave.

Solidez de los algoritmos criptográficos.- En teoría cualquier algoritmo criptográfico puede romperse al probar todas las claves posibles en secuencia (Un ataque de fuerza bruta). Pero para poder romper el algoritmo el número de pasos requeridos crece en forma exponencial con la longitud de la clave. A continuación se presenta el número de pasos requeridos [LIB02] para cada tamaño de clave.

- ✓ Clave de 32 bits requiere 2^{32} pasos
- ✓ Clave de 40 bits requiere 2^{40} pasos
- ✓ Clave de 56 bits requiere 2^{56} pasos
- ✓ Clave de 64 bits requiere 2^{64} pasos
- ✓ Clave de 80 bits requiere 2^{80} pasos
- ✓ Clave de 128 bits requiere 2^{128} pasos
- ✓ Clave de 160 bits requiere 2^{160} pasos

Las claves de 32 y 40 bits pueden ser quebrantadas para cualquiera que tenga acceso a un computador de alto rendimiento, la clave de 56 bits están comprometidas y las claves de 64 y 80 bits pueden ser quebrantas por los gobiernos y las universidades. Las claves de 128 y 160 bits probablemente sean seguras ahora.

En los sistemas criptográficos de clave pública las longitudes de clave son mayores de aquellas que se utilizan en las cifras simétricas. En los sistemas de clave pública, la mayoría de las fallas de seguridad no vienen del método de

fuerza bruta, sino de derivar la clave secreta de la clave pública. Por ejemplo, cualquiera con una computadora potente puede forzar un criptosistema de clave pública de un módulo de 256 bits con facilidad. Las universidades y gobiernos pueden forzar claves de módulos de 318 y 512 bits. Las claves con módulos de 768 y 1.024 bits probablemente son seguras por ahora.

Se debe tener presente que el algoritmo o las operaciones matemáticas que se ejecutan en los datos podrían debilitar todo el sistema, y por lo tanto los algoritmos de cifrado propietarios no hacen que un algoritmo sea seguro, la mayoría han mostrado ser débiles.

Ataques contra la implementación.- Este tipo de ataque es el más fácil de evitar, y se da cuando algunas implementaciones dejan archivos temporales, mensajes de texto simple y datos almacenados en la memoria intermedia de donde se puede extraer fácilmente.

6.1.2.- Ataques al generador de números aleatorios.

Un generador de números aleatorios es un dispositivo que genera números al azar, pero lamentablemente solo existen en la naturaleza, por ejemplo, en la electricidad estática y en el ruido blanco de los circuitos eléctricos. Debido a que no se puede utilizar un generador de números aleatorios de la naturaleza, se emplean los generadores de números pseudo aleatorios para generar valores supuestamente aleatorios.

Ya que un generador de números aleatorios es un común denominador en muchas funciones criptográficas, y si sus algoritmos no están diseñados correctamente pueden ser el eslabón más débil en la cadena de seguridad. Al igual que existen categorías de ataque en las funciones criptográficas, también se presentan categorías de ataques al generador de números aleatorios [LIB02], los cuales son:

Ataque criptoanalítico.- Este ataque ocurre si el agresor es capaz de observar una correlación entre el generador de números pseudo aleatorios y las salidas

aleatorias. Es factible en las funciones criptográficas donde las salidas del generador de números pseudo aleatorios son visibles.

Ataque de entrada.- Ocurren cuando el agresor puede tener conocimiento sobre la entrada del generador de números pseudo aleatorios con el fin de producir algunas salidas del generador de números pseudo aleatorios. Este tipo de ataque puede ocurrir en sistemas que utilizan los diversos tipos de entradas predecibles, como contraseñas y frases.

Ataque de sincronización.- Es similar al que ocurre en una función criptográfica. Durante las operaciones matemáticas que cuentan el número de ciclos de máquina para cada operación, el agresor puede tener alguna información. Se cree que el agresor puede determinar cuando ocurren ciertas operaciones booleanas. Por ejemplo, las adiciones referentes a los bits pueden detectarse al contar los ciclos de máquina.

Confidencialidad adelantada perfecta.- Es un mecanismo mediante el cual si una clave se roba en algún momento del futuro no se puede revelar ninguna comunicación que se ha conducido en el pasado. Todo algoritmo criptográfico debería estar diseñado para la confidencialidad adelantada perfecta. Lamentablemente la implementación de este tipo de algoritmos consume muchos recursos, ya que cada paquete requiere una nueva clave.

6.1.3.- Ataques a la recuperación de claves.

En este método de recuperación de claves que es exigida por los gobiernos, especialmente por el de los Estados Unidos, se construye una puerta trasera a propósito y, si existe tal puerta alguien más puede entrar. Este concepto elimina cualquier oportunidad de confidencialidad adelantada perfecta que se menciono con anterioridad [LIB02].

En la recuperación de claves, no solo esta en peligro la comunicación de datos futura sino cualquier información capturada previamente, ya que existe la clave para descifrarla. Los sistemas criptográficos confiables y seguros son muy

difíciles de diseñar, y la implementación de recuperación de claves lo han más difícil aún.

Otro problema con la recuperación de claves es quién guardará las claves, será el gobierno, cuál?, empresas privadas, quienes tendrán accesos a sus claves, esto es seguro?, y si lo fuera, que sucede en el momento de requerir una clave, la persona que tiene la clave viajaría por todo el mundo entregando claves o se enviarían por la misma red, en el momento que viajan por la red están seguras? De hecho ninguna solución se ve por el momento aceptable.

Y esto como le afecta a su Red privada Virtual?, de hecho es muy simple ya que es susceptible de que sus datos y claves sean amenazados, no sólo por el gobierno, sino por los atacantes que rompen los algoritmos que utilizan recuperación de claves, interceptando los datos conforme pasan del departamento encargado de custodiar las claves, al agente encargado de custodiar las mismas.

6.1.4.- Ataques al Protocolo de Seguridad de Internet (IPSec).

El protocolo de seguridad de Internet (IPSec) no es un algoritmo de cifrado y tampoco es un algoritmo de autentificación. IPSec es un paradigma en el cual otros algoritmos protegen datos. Los principales tipos de ataques que ocurrirán con IPSec serán aquellos que caen en la categoría de ataques contra la implementación[LIB02].

La norma IPSec solo requiere un algoritmo de cifrado (DES-CBC) y dos modos de autenticación (HMAC-MD5 y HMAC-SHA-1); sin embargo requiere los algoritmos NULL adicionales, ya que AH o ESP pueden ser opcionales, y cuando una norma requiere un algoritmo opcional está tratando de balancear la flexibilidad con la seguridad.

En el componente IKE del protocolo de administración de claves de IPSec, ambos extremos del canal de comunicación deciden que tan a menudo se deben cambiar las claves de cifrado. Debido a que muchos proveedores soportan claves

de 40 bits débiles que se usan para compatibilidad con productos anteriores, cambiar estas claves se vuelve crítico.

También en la especificación de IKE, cualquiera de las dos partes podría terminar una sesión, pero no hay forma de que el otro extremo sepa de la sesión se ha terminado; el extremo emisor seguirá enviando datos. Si la estación todavía envía datos, ¿Cómo dejaría otra estación de recibirlos y, si se utilizan claves débiles, cómo se burlaría la identidad del anfitrión original? Este tipo de ataque es similar a apropiarse de una sesión TCP.

Además IPSec no cuenta con ningún tipo de mecanismo para la autentificación de los usuarios: no incluye derechos de acceso, no existe verificación, etc. IPSec no se encarga del soporte para los clientes, ya que básicamente fue diseñado alrededor de una red privada virtual de LAN a LAN. Es por eso que queda la puerta abierta parea que los fabricantes ofrezcan su soporte de IPSec para la compatibilidad con los clientes.

La traducción de direcciones de red (NAT) existe en la norma IPSec. Cuando se utiliza el establecimiento de túneles en los modos ESP y AH, el encabezado IP original se reemplaza por uno nuevo encabezado IP. El problema es, ¿Dónde se esta ejecutando NAT? ¿En un enrutador, en un cortafuego o en un equipo de escritorio? ¿Qué dispositivo cambiará físicamente la dirección IP del paquete? ¿Este dispositivo deberá ser compatible con IPSec?

Una deficiencia de IPSec es que sólo soporta un conjunto muy pequeño de algoritmos y protocolos en su escenario predeterminado. Con el propósito de que IPSec se vuelva una entidad administrativa de corriente principal, tendrá que incluir más soporte, como el soporte para cliente, LDAP y múltiples algoritmos de cifrado predeterminados, así como otros mecanismos de autentificación. Al momento, IPSec sólo soporta firmas y certificados digitales. También tendrá que incluir un mayor soporte para los navegadores y equipos de escritorio con el fin de continuar haciéndolo una verdadera norma Internet interoperable. Lamentablemente la flexibilidad y la seguridad se sacrifican [WWW09].

6.1.5.- Ataques al protocolo PPTP.

El protocolo PPTP sufre ataques contra su implementación, y actualmente Microsoft, su diseñador, esta trabajando en esto. La red privada virtual de PPTP está formada por varios componentes y, de manera similar a IPSec, PPTP es un marco de referencia. No exige los algoritmos de cifrado y autentificación, esto se deja a los otros protocolos, como PAP, CHAP y MS-CHAP (detallados en el capitulo 3). Los protocolos utilizados son los siguientes:

- ✓ GRE. Protocolo de encapsulamiento de enrutamiento genérico.
- ✓ PPP. Protocolo de red punto a punto utilizado para proporcionar servicios TCP/IP sobre líneas de conexión serial por marcación.
- ✓ PPTP. Este protocolo utiliza GRE para establecer un túnel PPP y añade una instalación de conexiones y un protocolo de control.
- ✓ MS-CHAP. Es responsable del algoritmo de autentificación.
- ✓ MPPE. El protocolo de cifrado de punto a punto de Microsoft es el protocolo que se encarga de generar una clave y cifrar la sesión.

PPTP encapsula los paquetes PPP, los cuales a su vez son encapsulados en paquetes de encapsulamiento de enrutamiento genérico (GRE). PPTP crea una instalación de conexión y controla el canal al servidor PPTP sobre el puerto TCP 1723. Además esta conexión no se autentifica de ninguna forma.

Un tipo de ataque puede darse al encapsulamiento de enrutamiento genérico (GRE), ya que los paquetes GRE pueden trasportar un número se secuencia y un número de reconocimiento y pueden utilizar una ventana deslizable para evitar la congestión. Y esto tiene algunas implicaciones, ya que si se desea burlar los paquetes PPP encapsulados en GRE, simplemente se necesita desincronizar el canal de GRE. Esto puede evitarse con el número de secuencia, pero el GRE no tiene forma de que el anfitrión final reaccione ante un número de secuencia erróneo o duplicado. Es posible que simplemente se ignore y después, los paquetes PPP pueden burlarse.

La implementación de autentificación PPTP soporta tres tipos, de los cuales dos están relacionados con la seguridad y son: El método de transformación de código y le método de respuesta de pruebas. Cuando se utiliza el método de

transformación de código se esta exponiendo al los ataques de diccionario. Cuando se utiliza el método de respuesta de pruebas utilizando el protocolo de reconocimiento de pruebas (CHAP), el cual trabaja con el cliente contactando al servidor, y el servidor envía de regreso una prueba. El cliente entonces ejecuta una función de transformación del código, añade alguna información extra y la envía de regreso al servidor. El servidor busca en su propia base de datos y compara el valor de transformación del código con la prueba. Si son iguales, la autentificación es satisfactoria. Mientras esto elimina los ataques de diccionario, las funciones de transformación del código aún podrían ser atacadas.

Un punto vulnerable de PPTP es que se basa en PPP. Antes de cualquier comunicación, PPP establece e inicia los parámetros de comunicación, y debido a que no tiene autentificación contra estos paquetes, pueden ocurrir ataques como los de intermediario y de falsificación.

6.1.6.- Ataques a la autoridad emisora de certificados.

Las autoridades emisoras de certificados no son diferentes de cualquier otro dispositivo en la cadena de comunicación de terceras partes validadas. Si ocurre un ataque a una autoridad emisora de certificados, los agresores pueden hacerse pasar por quién ellos deseen, al unir cualquier clave de su elección al nombre de otro usuario, y utilizar a la autoridad emisora de certificados para verificarla.

6.1.7.- Ataques a radius.

El servicio de usuarios de autentificación remota por marcación (RADIUS) se diseño teniendo dos protocolos en mente, el de autenticación y el de asignación de cuentas.

En la tecnología RADIUS se encontró un punto débil que provocó un problema de desbordamiento de la memoria intermedia, el cuál permitía que un agresor obtuviera acceso de superusuario de forma remota a una máquina que ejecutará al servidor RADIUS. El problema se manifestó como resultado de una operación

de resolución inversa de direcciones IP a nombres de anfitrión. El software copiaría el nombre de anfitrión a una memoria intermedia en su pila sin revisar primer su longitud. En un ataque, un agresor establecería un nombre de anfitrión sumamente largo y el software RADIUS colocaría el nombre en la pila provocando que invadiera su memoria intermedia. Cualquier código malicioso podría entonces ejecutarse en el servidor.

6.1.8.- Ataques a kerberos.

Kerberos es un sistema de autentificación distribuida que permiten que las organizaciones manejen seguridad de contraseñas para toda una organización. Lamentablemente estos protocolos son vulnerables a los ataques de diccionario. Un atacante puede agredir a un sistema Kerberos con la ayuda de una máquina local y un husmeador de paquetes ayudará para el ataque.

6.1.9.- Ataques a pretty good privacy (PGP).

PGP es muy seguro, probablemente se trata de una de las mejores estructuras de seguridad. Lo más interesante sobre PGP no es su solidez, sino la actitud que tiene el gobierno de los Estados Unidos hacia él.

PGP utiliza cuatro componentes: una cifra simétrica (IDEA), una cifra asimétrica (RSA), una función de transformación de código (MD5) y un generador de números pseudoaleatorios (PRGN). Cada uno de estos dispositivos podría ser atacado [LIB02].

Idea.- La cifra de IDEA utiliza una clave de 128 bits, y la única forma de ataque conocida que podría intentarse contra ella sería un ataque de fuerza bruta. Por lo tanto, alguien tendría que intentar con al menos la mitad del espacio de clave, lo cual aproximadamente es 2^{127}.

RSA.- Obtiene su solidez de la dificultad que implica factorizar números primos grandes. Ningún ataque a RSA ha tenido éxito hasta ahora. Y con tamaños de clave lo suficientemente grandes, se espera que ningún ataque pueda lograrlo.

MD5.- Se encontró que la función de transformación del código MD5 es vulnerable si se utiliza un número de ciclos pequeños. Se han presentado intentos de forzar MD5 utilizando los métodos de criptoánalisis diferencial, de aniversario y de fuerza bruta. De éstos, el criptoanálisis diferencial ha tenido cierto éxito fuera del ciclo de MD5 y sólo afectó a una operación que no estaba relacionada con la seguridad de MD5.

PRNG.- PGP utiliza dos generadores de números pseudoaleatorios: el generador ANSI X9.17 y el generador trueRand. Este último mide la latencia de la entrada del usuario y después utiliza ese grupo para establecer una semilla en el generador X9.17. Al utilizar dos generadores, PGP ha añadido mecanismos de seguridad para producir una aleatoriedad verdadera.

Parecería que PGP es un algoritmo muy seguro que no ha experimentado ataques de ningún tipo; sin embargo esta es una suposición incorrecta. Después de todo, si no se puede atacar el protocolo, puede atacar la implementación.

6.1.10.- Ataques de negación de servicio.

Los ataques de negación de servicio provocan que el sistema o la red dejen de dar servicio a los usuarios legítimos, y entre los más conocidos se encuentran los siguientes:

Jamming o Flooding.- Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP. El sistema responde al mensaje, pero como no

recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas. Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

Syn Flood.- El protocolo TCP se basa en una conexión en tres pasos. Si el paso final no llega a establecerse, la conexión permanece en un estado denominado "semiabierto". El Syn Flood es el más famoso de los ataques del tipo Denial of Service. Se basa en un "saludo" incompleto entre los dos hosts.

El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

El problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones "semiabiertas" que pueden manejar en un momento determinado. Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando. Las conexiones "semiabiertas" van caducando tras un tiempo, liberando "huecos" para nuevas conexiones, pero mientras el atacante mantenga el Syn Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

La potencia de este ataque reside en que muchos sistemas operativos fijan un límite del orden de 5 a 30 conexiones "semiabiertas", y que éstas caducan alcabo de un par de minutos. Para mantener el servidor fuera de servicio, un atacante sólo necesita enviar un paquete SYN cada 4 segundos (algo al alcance de, incluso, un módem de 300 baudios).

Connection Flood.- La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza

ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del Syn Flood) para mantener fuera de servicio el servidor.

Land Attack.- Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows. El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al 113 o al 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino. Por ejemplo se envían un mensaje desde la dirección 10.0.0.1:139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados-recibidos la máquina termina colgándose.

E-Mail Bombing-Spamming.- El E-Mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así mailbox del destinatario.

El Spamming, en cambio se refiere a enviar el e-mail a miles de usuarios, hayan estos solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos. El Spamming esta siendo actualmente tratado por las leyes como una violación de los derechos de privacidad del usuario.

6.1.11.- Ataques de Autentificación.

Consisten en la suplantación de una persona con autorización por parte del atacante. Se suele realizar de dos formas: obteniendo el nombre y contraseña del atacado o suplantando a la víctima una vez ésta ya ha iniciado una sesión en su sistema. Para realizar ataques de este tipo se utilizan varias técnicas, las cuales pasamos a describir a continuación [WWW11].

Simulación de identidad.- Es una técnica para hacerse con el nombre y contraseña de usuarios autorizados de un sistema. El atacante instala un programa que recrea la pantalla de entrada al sistema, cuando el usuario intenta entrar en él teclea su login y password, el programa los captura y muestra una

pantalla de "error en el acceso" al usuario. El usuario vuelve a teclear su login y password, entrando esta vez sin problemas. El usuario cree que en el primer intento se equivocó al teclear, sin embargo, su login y password han sido capturados por el atacante.

Spoofing (Engaño).- Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Consiste en sustituir la fuente de origen de una serie de datos (por ejemplo, un usuario) adoptando una identidad falsa para engañar a un firewall o filtro de red. Los ataques Spoofing más conocidos son el IP Spoofing, el DNS Spoofing , el Web Spoofing y el fake-mail.

- ✓ **IP Spoofing.-** Sustituir una IP. El atacante logra identificarse con una IP que no es la suya, con lo que a ojos del atacado, el agresor es una tercera persona, que nada tiene que ver en el asunto, en vez de ser el atacante real.
- ✓ **DNS Spoofing.-** Sustituir a un servidor DNS (Domain Name Server) o dominio. Se usan paquetes UDP y afecta a sistemas bajo Windows NT. Se aprovecha de la capacidad de un servidor DNS resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos, ya que éste es su método de trabajo por defecto.
- ✓ **Web Spoofing.-** El atacante crea un sitio web (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorizar todas las acciones de la víctima: datos, contraseñas, números de tarjeta de créditos, etc. El atacante también es capaz de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.
- ✓ **Fake-mail.-** Es otra forma de spoofing y consiste en el envío de e-mails con remitente falso. Aquí el atacante envía E-Mails en nombre de otra persona con cualquier motivo y objetivo. Muchos de estos ataques se inician utilizando la Ingeniería Social para hacerse con el nombre y contraseña de una víctima.

Looping.- El intruso usualmente utiliza algún sistema para obtener información e ingresar en otro, que luego utiliza para entrar en otro, y así sucesivamente.

Este proceso se llama looping y tiene como finalidad hacer imposible localizar la identificación y la ubicación del atacante, de perderse por la red.

IP splicing-hijacking.- Es un método de sustitución que consiste en que el atacante espera a que la víctima entre en una red usando su nombre, contraseña y demás y una vez que la víctima ha superado los controles de identificación y ha sido autorizada la "saca" del sistema y se hace pasar por ella.

Utilización de backdoors (puertas traseras).- Las puertas traseras son trozos de código en un programa que permiten a quien los conocen saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo. No es por tanto un método de suplantación, si no de saltarse los controles de autentificación o, como su nombre indica, entrar por la "puerta de atrás".

Son fallas de seguridad que se mantienen, voluntariamente o no, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

Obtención de contraseñas.- Es la obtención por "Fuerza Bruta" de nombres de usuarios y claves de acceso. Casi todas las contraseñas que utilizamos habitualmente están vinculadas a nuestros nombres reales, nombres de familiares y/o mascotas, fechas significativas, ... etc. Además, no las solemos cambiar periódicamente. También se suele realizar este tipo de ataques usando una clase de programas llamados diccionarios.

Diccionarios.- Los Diccionarios son programas que en su base de datos contienen millones de palabras. Van probando con millones de combinaciones de letras y números encriptados, incluso con caracteres especiales hasta descubrir la combinación correcta de nombre y usuario de la víctima. Son entonces programas de fuerza bruta.

6.2.- Como identificar los ataques.

Una buena política de seguridad tiene auditorias y registros como pasos principales de sus procesos, ya que nunca se sabe de antemano cuando se va ha ser atacado. Es por esta razón que es bueno tener registros de quién ha ingresado o ha intentado introducirse y no tuvo éxito. Cuando se tiene intrusiones extrañas es necesario rastrear la intrusión y ver si los archivos de registro pueden identificar de donde vino el intruso, cuál es su dirección IP, y si es posible quién es su proveedor de Internet.

Las auditorias y los registros son herramientas adecuadas y necesarias para intentar revelar la identidad de potenciales violaciones a la seguridad. Sin embargo, el monitoreo es la vista en tiempo real de los paquetes mientras pasan el límite entre la red interna de la empresa y las redes externas. Este monitoreo controla que tráfico permite entrar, que tipo de tráfico permite salir, que servicios están permitidos. El monitoreo en tiempo real es la única forma efectiva de observar las desviaciones contra la política de seguridad establecida por la organización.

El problema con el monitoreo en tiempo real para un administrador de red es que pueden haber cientos de alertas, y es probable que el administrador se canse de todas estas alertas y desactive el monitoreo de una estación.

6.3.- Importancia de la Seguridad en las VPN.

Para que las Redes Privadas Virtuales puedan ser un medio efectivo para el comercio electrónico, para las aplicaciones de Intranet, Extranet y para las transacciones financieras a través de Internet, deben utilizarse tecnologías de autenticación seguras, las más recientes y sofisticadas, así como criptografía y cifrado en cada extremo del túnel de las Redes Privadas Virtuales. Por los motivos expuestos con anterioridad es importante para cualquier configuración de seguridad lo siguiente:

Acceso solo a personas autorizadas.- Sólo a las partes autorizadas se les permite el acceso a aplicaciones y servidores corporativos. Esté es un aspecto

importante de la tecnología Red Privada Virtual, ya que se permite que personas entren y salgan de Internet o de otras redes públicas y se les ofrece acceso a los servidores.

Imposibilidad de descifrar el mensaje.- Cualesquiera que pase a través del flujo de datos cifrados de las Redes Privadas Virtuales no debe estar capacitado para descifrar el mensaje, ya que los datos de las VPN viajarán a través de una red pública, y cualquiera tendrá la capacidad de interceptarlos. El resguardo de la información está en el cifrado, incluyendo su solidez y la implementación especifica del proveedor.

Datos íntegros.- Los datos deben permanecer intocables al cien por ciento, esto se debe a que algunas personas verán el tráfico cifrado e intentarán leerlo, sin embargo, otro problema, es que intenten modificarlo y enviarlo a su destino original. La integridad es un tema diferente cuando se trata de la tecnología VPN, ya que existen normas de cifrado que proporcionan autenticación, cifrado e integridad de datos.

Distintos niveles de acceso.- Los usuarios individuales deben tener un distinto nivel de acceso cuando entren al sitio desde redes externas.

Interoperabilidad.- Los aspectos de interoperabilidad deben tomarse en consideración, ya que es un problema cuando existen diferentes plataformas y sistemas operando en conjunto para lograr una meta común.

Las redes privadas virtuales deben funcionar en todas las plataformas y para logra este objetivo si es necesario, es probable que se tenga que instalar software adicional para estas plataformas, y se debe tener presente que cuando se aumenta algo nuevo, aumenta el riesgo de que se presenten consecuencias infortunadas.

Facilidad de administración.- Los dispositivos de las redes privadas virtuales deben proporcionar una administración fácil, la configuración debe ser directa, el mantenimiento y la actualización de las VPN deben estar asegurados. Una de estas facilidades de administración debe ser el acceso de los usuarios, es decir

debe haber una manera sencilla para agregar/eliminar usuarios sin esperar demasiado tiempo.

6.4.- Requisitos de seguridad en las Redes Privadas Virtuales.

Una red Privada Virtual esta basada en una red tradicional, así que los requisitos de seguridad son los mismos que se utilizan en las redes tradicionales y de algunas técnicas más, propias de la Red Privada Virtual. El mismo hecho de querer instalar una Red Privada Virtual significa que se quiere añadir un nivel más de seguridad a la red que se posee actualmente.

La seguridad de las Redes Privadas Virtuales es de suma importancia para cualquier compañía que realice negocios a través de Internet o de cualquier red pública. Estos requisitos de seguridad incluyen el cifrado, los dispositivos de Red Privada Virtual, la autenticación, el proceso sin rechazos, el cifrado punto a punto, la administración centralizada de la seguridad y los procedimientos de respaldo restauración. A continuación se revisarán algunos de estos componentes.

6.4.1.- Criptografía.[6]

Criptografía puede parecerse a magia negra para una persona promedio, pero en realidad está basada en principios matemáticos. El cifrado es sencillamente el procedimiento de convertir texto legible en un texto ilegible. La meta es permitir que sólo la persona a la que se le envía lo convierta en un texto legible. Un mensaje o archivo de datos es llamado texto-plano antes de ser encriptado y texto-cifrado luego de ser encriptado. El proceso de "scrambling" del texto-plano es llamado encriptación. El proceso de "Unscrambling" del texto-cifrado al texto plano original es llamado desencriptación. A veces las palabras cifrar y descifrar son usadas en su lugar.

[6] Criptografiar y cifrar un mensaje se considera lo mismo, por lo tanto se usarán estos términos indistintamente.

La ciencia de encriptar datos es llamada criptografía. La ciencia de romper datos encriptados es llamada criptoanálisis. La criptología es la ciencia combinada de estas dos.

Algunos de los mejores criptoanalístas del mundo trabajan en la Agencia nacional de Seguridad (NSA), una agencia muy secreta creada por el presidente Truman en 1952. Su propósito es desencriptar comunicaciones foráneas que son de interés para la seguridad nacional de los Estados Unidos.

Las claves se miden en bits. Una clave de un bit tiene dos combinaciones posibles 0 y 1. Cada bit adicional dobla la cantidad de combinaciones. Una clave de 8 bits tiene 256 combinaciones, una de 40 bits tiene más de un trillón de combinaciones y una de 160 bits tiene 10^{48} combinaciones. Probar cada posible clave hasta encontrar la correcta se denomina ataque de fuerza bruta. Una computadora personal que pueda probar 50.000 combinaciones por segundo puede testear todas las combinaciones de una clave de 40bits en alrededor de 255 días. Estadísticamente el usuario solo tendría que probar la mitad de las claves para encontrar la correcta. La clave de 40 bits puede ser clasificada como poseedora de seguridad casual. La clave de 160 bits usada en el algoritmo blowfish puede ser clasificada como poseedora de seguridad militar. Un trillón de supercomputadoras que pudieran probar cada una un trillón de claves por segundo demorarían cerca de 463 trillones de centurias para probar todas las combinaciones posibles de una clave de 160 bits.

La criptografía es clasificada como munición en la U.S. Munitions list (USML) y está contemplada en el International Traffic in Arms Regulations (ITAR). La NSA a través del Departamento de Estado, controla la tecnología de encriptación que es exportada desde los Estados Unidos. El Shareware[7] y las versiones internacionales registradas contienen la tecnología de encriptación más sólida permitida para exportar por los Estados Unidos (40 bits). Las versiones registradas en Canadá no están sujetas a estos controles y por consiguiente contienen mejor tecnología de encriptación.

[7] Shareware.- Palabra en inglés que significa software de evaluación

Básicamente hay dos tipos de algoritmos de encriptación en uso hoy, de clave privada o simétrico y de clave pública o asimétrico.

6.4.1.1.- Algoritmos Simétricos.

Son sistemas convencionales basados en password (clave) que la mayoría de la gente conoce. El usuario suministra una clave y el archivo es cifrado con la clave. Para descifrar el archivo, el usuario debe suministrar la misma clave nuevamente y el proceso es reversado. La clave es la llave de encriptación [WWW08]. El principal problema aquí es la clave; el emisor y el receptor no solamente deben de estar de acuerdo en usar la misma clave, sino que también deben idear alguna manera para intercambiarla, especialmente si están en diferentes áreas geográficas. En los sistemas de clave privada, la integridad de la clave es sumamente importante. Por lo tanto, es importante reemplazar periódicamente esta clave.

Ejemplos de los esquemas de encriptación simétrica son el algoritmo RSA RC4 (que proporciona la base de Microsoft Point-to-Point Encription (MPPE), el Estándar de encriptación de datos (DES), el Algoritmo de encriptación de datos internacional (IDEA) y la tecnología de encriptación Skipjack propuesta por el gobierno de Estados Unidos (e implementada en el Chip Clipper).

En este punto es necesarios aclarar que existen dos técnicas de cifrado simétrico, las cuales son: cifrado por bloques y cifrado por flujo.

6.4.1.1.1.- Cifras de bloque.

Una cifra de bloque es un cifrado que repite varias operaciones débiles como sustitución, transposición, adición modular, multiplicación y transformación lineal en un algoritmo mucho más sólido. Este algoritmo de cifrado se efectúa con la clave del usuario especificada. Una cifra de bloque codifica un bloque de datos, por ejemplo 64 bits a la vez, y luego va al siguiente bloque. DES es un ejemplo de una cifra de 64 bits. Una desventaja de la cifra de bloque es que el uso del

mismo algoritmo y la misma clave generan el mismo texto cifrado que se puede utilizar como un ataque de análisis de datos sostenido.

El cifrado Feistel.- Es una cifra de bloques que opera sobre la mitad del texto cifrado en cada repetición y luego intercambia las mitades del texto cifrado después de cada ciclo. Utiliza 64 bits con 16 ciclos.

DES.- La norma de cifrado de datos (DES) utiliza un tamaño de 64 bits y una clave de 56 bits durante la ejecución (los 8 bits de paridad se quitan de la clave de 64 bits completa). DES es un criptosistema simétrico, específicamente una cifra Feistel de 16 ciclos. En una cifra de ciclo se aplica el algoritmo varias veces; en este caso, el algoritmo se completa 16 veces. Durante cada ciclo (transformación) se utiliza una subclave con el proceso de repetición. Esta subclave es un derivado de la clave principal que el usuario suministró mediante una función especial en el algoritmo. Cabe aclarar que el cifrado DES de 56 bits fue violado en el lapso de un mes, por lo que el gobierno de los Estados Unidos permitió la exportación de DES de 56 bits.

El algoritmo Blowfish.- Fue desarrollado por Bruce Scheneir en 1993. Blowfish es un cifrador de bloque de tamaño de clave variable para usuarios registrados que residen en los Estados unidos o Canadá. El tamaño de la clave de Blowfish varía de 32 a 448 bits. El algoritmo en sí mismo consta de dos partes: una parte de expansión de subclave y una parte de cifrado. La parte de generación de claves es complejo, ya que debe ejecutarse en 521 repeticiones para generar todas las subclaves. Esto debe hacerse antes de que se realice el proceso de cifrado. Blowfish no requiere licencia para la implementación y su desempeño es superior al de DES y al de IDEA con el mismo tamaño de clave. La ventaja principal sobre otros algoritmos se deriva de sus tamaños de clave de longitud variable.

El algoritmo IDEA.- Es un cifrado de bloque que se creó en 1990 por una compañía suiza. Utiliza 64 bits con ocho ciclos. Este cifrado se diseño para una implementación fácil en hardware y software. La seguridad de IDEA se basa en la utilización de tres tipos incompatibles de operaciones aritméticas en palabras de 16 bits. En este algoritmo, las operaciones de tres grupos algebraicos diferentes se mezclan (XOR, modulo de adición 216 y módulo de multiplicación

216+1). IDEA utiliza 52 subclaves, cada una de las cuales comienza con una longitud de 16 bits. La generación de subclaves es como sigue: la clave de 128 bits de IDEA se utiliza como las primeras ocho subclaves K1 a K8. Las ocho siguientes se obtienen de la misma manera, después de una rotación circular a la izquierda de 25 bits. Este proceso se repite hasta que todas las subclaves de cifrado se hayan calculado.

IDEA es un cifrado sólido que ha enfrentado muchos retos en su contra. Se considera inmune al criptoanálisis diferencial y no se han reportado ataques criptoanalíticos lineales. De cualquier modo existen una gran clase de claves débiles, 2^{51}, que en el proceso de cifrado podrían permitir que se recuperara la clave. Sin embargo, IDEA todavía tiene 2^{128} claves posibles, lo que hace que sea seguro.

Skipjack.- El algoritmo de cifrado por bloques Skipjack utiliza una clave de 80 bits para cifrar bloques de 64 bits y emplea 32 ciclos. Se espera que Skipjack sea más seguro que DES en la ausencia de cualquier ataque analítico, ya que utiliza claves de 80 bits contra los 56 bits en DES.

6.4.1.1.2.- Cifras de flujo.

Una cifra de flujo son algoritmos simétricos que normalmente son más rápidos que los de bloque. Mientras que las cifras de bloque trabajan con partes de datos (64 bits), las de flujo trabajan sobre bits individuales, una buena característica de seguridad con las cifras de flujo es que aunque se utilice el mismo algoritmo y la misma clave, es posible que no aparezca el mismo texto cifrado; esto depende del momento en que los bits se encuentran en el proceso de cifrado.

RC4.- RC4 (una marca registrada de RSA Data Securities, Inc.), utiliza una cifra de flujo de tamaño de clave variable con operaciones algebraicas orientadas a bytes. El algoritmo se basa en la utilización de permutación aleatoria. El cifrado se diseño para ejecutarse rápidamente en el software y utiliza de 8 a 16 operaciones por byte. Fue desarrollado en 1987 por Ron Rivest. Este es un algoritmo no patentado que fue mantenido en secreto durante 7 años hasta que

fue sacado a la internet por una persona anónima a la lista de correo de Cypherpunks. RC4 posee un status de exportación especial. Es el único algoritmo (junto con el RC2) permitido para la exportación desde los Estados Unidos con un tamaño de clave de 40 bits usando el requerimiento del State Departament's Commodity Jurisdiction. Otros algoritmos (como el Blowfish) están actualmente limitados a claves de 32 bits para exportación.

6.4.1.2.- Algoritmos Asimétricos.

También se los conoce como algoritmos de clave pública. Cada parte obtiene un par de claves, una pública y una privada. La clave pública esta hecha para que todos la conozcan mientras que la privada no [WWW08]. La ventaja de utilizar criptografía de clave pública es la seguridad y la conveniencia. La clave privada nunca necesita transmitirse o confiarse a alguien más. Por lo tanto no hay ninguna posibilidad de que la clave se comprometa ni de que la transmisión sea interceptada o decodificada.

Es necesario aclarar que la clave privada utilizada en estos algoritmos no es la misma clave utilizada en los criptosistemas de clave privada; la clave privada sólo descifra los mensajes que han sido cifrados con la clave pública asociada.

Entre los algoritmos más representativos de esta categoría son el algoritmo Diffie-Hellman y el algoritmo RSA.

6.4.1.2.1.- Algoritmo Diffie-Hellman.

El protocolo de acuerdo de claves Diffie-Hellman es una generación de claves negociada. Su fortaleza radica en le campo matemático finito de exponenciación de los logaritmos. El protocolo permite que dos usuarios intercambien una clave secreta en un medio inseguro sin secreto previo alguno. El algoritmo Diffie-Hellman también ha establecido la función de seguridad de un acuerdo de claves secretas, por lo tanto aunque sea un algoritmo asimétrico (clave pública), tanto el emisor como el receptor pueden utilizar un cifrado simétrico.

Existen dos valores globales en el intercambio de claves Diffie-Hellman: P (que es un número primo) y G (llamado generador). G tiene una propiedad especial: es un entero menor que P y puede generar todos los números entre 1 y P-1 al multiplicarse por sí mismo. Se hace referencia a G como módulo de P. Antes de que los usuarios puedan comunicarse entre sí utilizando el intercambio de claves Diffie-Hellman necesitan acordar las claves secretas.

El intercambio de claves es vulnerable al ataque del intermediario, existe debido a que este algoritmo no autentifica a los usuarios. Por lo tanto, se necesitan otros pasos para evitar estos ataques, tales como el empleo de firmas digitales y las autoridades emisoras de certificados.

6.4.1.2.2.- Algoritmo RSA.

Este algoritmo fue ideado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman (RSA). Es sencillo de comprender e implementar, aunque las longitudes de sus claves es bastante considerable (ha pasado desde sus 200 bits originales a 2048 actualmente).

En este algoritmo se emplean las ventajas proporcionadas por las propiedades de los números primos cuando se aplican sobre ellos operaciones matemáticas basadas en la función módulo. En concreto, emplea la función exponencial discreta para cifrar y descifrar, y cuya inversa, el logaritmo discreto, es muy difícil de calcular [WWW10].

Los cálculos matemáticos de este algoritmo emplean un número denominado Módulo Público, N, que forma parte de la clave pública y que se obtiene a partir de la multiplicación de dos números primos, p y q, diferentes y grandes (del orden de 512 bits) y que forman parte de la clave privada. La gran propiedad de RSA es que, mientras que N es público, los valores de p y q se pueden mantener en secreto debido a la dificultad que entraña la factorización de un número grande.

La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta, el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la carga computacional lo suficientemente grande para que este tipo de ataque sea inviable.

6.4.1.3.- Algoritmo Híbrido (PGP).

Pretty Good Privacy (PGP) de Philip Zimmermann es un criptosistema híbrido, con todas las ventajas. Combina un algoritmo de clave privada con uno de clave pública. Esto le da tanto la rapidez de un sistema simétrico como las ventajas de un sistema asimétrico. PGP utiliza cuatro componentes: una cifra simétrica (IDEA), una cifra asimétrica (RSA), una función de transformación de código (MD5) y un generador de números pseudoaleatorios (PRGN)

PGP genera claves criptográficas fuertes, una privada, otra pública. El usuario guarda la clave privada, y distribuye la clave pública... insertada en el correo electrónico usando un fichero de firma, colocada en una página web, o en cualquier otro lugar. Asimismo es importante obtener las claves públicas de los contactos e importarlas en tu PGP. Cuando quieres enviar un correo cifrado, lo cifras usando la clave pública del receptor y sólo esa persona podrá descifrarlo usando su clave privada. También se puede firmar los ficheros y correos electrónicos para que cualquiera que tenga tu clave pública en su 'keyring' (anillo de claves) pueda comprobar si ese fichero en concreto proviene de ti y no de otra persona que se hace pasar por ti.

PGP generalmente comprime el texto plano antes de encriptar el mensaje (y lo descomprime después de desencriptarlo) para disminuir el tiempo de cifrado, de transmisión y de alguna manera fortalecer la seguridad del cifrado ante el criptoanálisis que explotan las redundancias del texto plano.

6.4.1.4.- Otros Cifrados.

Además de esos sistemas de cifrado basados en clave públicas o secretas existen otros sistemas de cifrado basados en algoritmos. Estos nuevos sistemas no emplean claves de ningún tipo, sino que se basan en extraer una determinada cantidad de bits a partir de un texto de longitud arbitraria. Esto es, cada cierta cantidad de texto elegido de forma arbitraria, se procede a realizar una transformación de bits, de esta transformación se obtiene una palabra longitud clave, esta palabra longitud tiene una extensión de x bits preestablecidos, de esta forma el texto es irreconocible ya que solo se pueden leer números secuénciales y no guardan relación alguna entre sí. Estos algoritmos normalmente se basan en complejas operaciones matemáticas de difícil resolución. Y el secreto esta en que operaciones matemáticas sigue el algoritmo.

Entre los sistemas desarrollados a partir de la creación de algoritmos cabe destacar al menos dos, por su complejidad e importancia: MD5 y SHA...

MD5.- Este algoritmo fue desarrollado por el grupo RSA y es un intento de probar con otros sistemas criptográficos que no empleen claves. El algoritmo desarrollado es capaz de obtener 128 bits a partir de un determinado texto. Como es lógico hasta el momento no se sabe cuales son las operaciones matemáticas a seguir, pero hay alguien que dice que es mas probable que se basen en factores de números primos [LIB03].

SHA, SHA-1. Es un algoritmo desarrollado por el gobierno de los Estados Unidos y se pretende implantar en lo sistemas informáticos de alta seguridad del estado como estándar de protección de documentos. El algoritmo obtiene 160 bits de un texto determinado. Aún cuando es más lento que otras funciones de transformación del código, se considera más seguro ya que tiene mayor longitud.

6.4.2.- Certificados Digitales.

Con la encriptación simétrica, tanto el remitente como el destinatario cuentan con una llave secreta compartida. La distribución de la llave secreta debe ocurrir

(con la protección adecuada) antes de cualquier comunicación encriptada. Sin embargo, con la encriptación asimétrica, el remitente utiliza una llave privada para encriptar o firmar digitalmente los mensajes, mientras que el receptor utiliza una llave pública para descifrar estos mensajes. La llave pública puede distribuirse libremente a todos los que necesiten recibir mensajes encriptados o firmados digitalmente. El remitente necesita proteger cuidadosamente sólo la llave privada.

Para garantizar la integridad de la llave pública se publica con un certificado. Un certificado (o certificado de llave pública) es una estructura de datos que está firmada digitalmente por una autoridad certificadora (CA); una autoridad en la que los usuarios del certificado pueden confiar. El certificado contiene varios valores, como el nombre y el uso del certificado, la información que identifica al propietario de la llave pública, la llave pública misma, una fecha de expiración y el nombre de la autoridad certificadora. La CA utiliza su llave privada para firmar el certificado. Si el receptor conoce la llave pública de la autoridad certificadora, el receptor puede verificar que el certificado sea, en efecto, de esa CA y, por lo tanto, que contiene información confiable y una llave pública válida. Los certificados se pueden distribuir de manera electrónica (a través de acceso al Web o correo electrónico), en tarjetas inteligentes o en discos flexibles.

6.4.3.- Autenticación.

La autentificación[8] es el segundo factor más importante en la configuración de una Red Privada Virtual. Pero así como existen distintas arquitecturas, topologías y esquemas de cifrado en las Redes privadas Virtuales, también hay muchos esquemas de autentificación. Además hay dos aspectos que son necesarios aclarar; la autentificación es quién tiene el permiso y la autorización es a que tiene acceso.

En este punto el usuario debe estar concientes de que en cualquier infraestructura de comunicaciones en red existe la necesidad de un proceso de autentificación que permita a que el usuario acceda a los servicios de red y que

[8] Autenticación y Autentificación tiene el mismo significado.

impida, al mismo tiempo, el acceso no garantizado de los usuarios sin autorización.

En un sistema de contraseñas normales, tanto el usuario como el servidor, conocen la contraseña, para el inicio de una sesión válida, el usuario ingresa la contraseña y el servidor la compra con la que tiene almacenada y si coinciden se permite el ingreso. Esto produce como resultado una debilidad en la seguridad, ya que si asumimos que el usuario no revela su contraseña, está permanecerá guardada en el servidor, y puede ser susceptible de ataques.

6.4.3.1.- CONTRASEÑAS DEL SISTEMA OPERATIVO.

En una organización existen varios servidores y aplicaciones protegidos con contraseñas [LIB02]. Los usuarios pueden tener varias contraseñas distintas para los diferentes servidores. A continuación se presentan algunas recomendaciones para utilizar en una Red Privada Virtual.

La identificación del usuario.- En lo posible debe ser Alfanumérica y de largo suficiente para que sea mnemotécnico, además, no deberían ser reutilizados en distintos usuarios ya que se pierde el control sobre las pistas de auditoria. Existen distintos métodos:

- ✓ Apellido del usuario, si hay repeticiones apellido y parte del nombre. Ejemplo: JATON, JATONRE, RAMIREZ, RAMIREZO
- ✓ Tres primeras letras del apellido y los nombres y el legajo (se utiliza en empresas grandes) Ejemplo: PAG81455 (Pablo Andrés Gietz)
- ✓ Tipo de usuario y legajo: ejemplo: EMP4517 (para empleado) GER7782 (para gerente). Desventajas: es difícil de administrar por que no se puede memorizar, además no permite el cambio de función sin cambiar el usuario.

Contraseñas.- La contraseña es el método que sirve para autentificar a los usuarios. Es por lo general uno de los eslabones más débiles de la seguridad, ya que los usuarios no la utilizan correctamente, o no le dan la debida importancia.

Las contraseñas deben ser secreta e intransferibles, mínimo de ocho caracteres, no debe ser escrita por el usuario para poder recordarla, el usuario puede cambiar su contraseña, debe caducar por lo menos en 45 días, el administrador del sistema no debe poder ver las contraseñas, y al tercer intento de ingreso no válido el sistema lo debe rechazar.

Log de seguridad.- Se deben proteger contra accesos no autorizados, se deben controlar y respaldar diariamente. No es necesario imprimirlos. Estos son los registros que se tiene de los accesos, para en posterior poder realizar auditorias.

6.4.3.2.- S/KEY.

Las contraseñas descartables del sistema S/KEY tienen una extensión de 64 bits. Esto se basa en la creencia de que son lo suficientemente extensas como para ser seguras y lo suficientemente cortas como para ser introducidas manualmente cuando sea necesario. El sistema S/KEY aplica funciones de transformación del código varias veces, produciendo una salida final de 64 bits. MD4 acepta un número arbitrario de bits como entrada y produce una salida de 128 bits. Las funciones de transformación del código seguras de S/KEY consisten en aplicar MD4 a una entrada de 64 bits y plegar la salida de MD4 con la función O exclusiva (XOR) para producir otra salida de 64 bits.

S/KEY, como se dijo anteriormente, es un sistema de contraseñas descartables, lo que significa que cada contraseña utilizada por el sistema se usa sólo para una autentificación. Las contraseñas no pueden volverse a utilizar, por lo tanto no pueden interceptarse ni usarse como una forma de predecir las contraseñas futuras.

6.4.3.3.- RADIUS.

El protocolo de servicio de autenticación de usuario remoto de marcación (RADIUS) es un método basado en el UDP para administrar la autenticación y

autorización de usuarios remotos. Los servidores de RADIUS pueden localizarse en cualquier lugar de Internet y proporcionan autenticación (incluyendo PPP PAP, CHAP, MSCHAP y EAP) para su NAS de cliente. Al mismo tiempo, los servidores de RADIUS pueden proporcionar un servicio proxy para transmitir las solicitudes de autenticación a servidores distantes de RADIUS.

6.4.3.4.- KERBEROS.

Kerberos[9] V5 es un protocolo de autentificación confiable fabricado por un tercero que permite que un proceso se ejecute en un cliente para demostrar su identidad frente a un servidor Kerberos [LIB02], sin tener que enviar los datos a través de la red, lo cuál permitiría que un atacante o un verificador se hiciera pasar por un director.

Kerberos es un sistema de cifrado DES simétrico. Utiliza una función de clave privada centralizada y en el núcleo del sistema se encuentra el centro de distribución de claves [RFC1510].

6.4.3.5.- LDAP.

El protocolo ligero de acceso a directorio (LDAP) [RFC2251] es un protocolo estándar en la industria para acceder a servicios de directorio. Este es extensible, independiente del distribuidor y se basa en los estándares. Permitiendo que un administrador asigne una variedad de propiedades de conexión para sesiones de marcación o de VPN destinadas a usuarios individuales o grupos. Estas propiedades pueden definir los filtros por usuario, la autenticación requerida o los métodos de codificación, entre otras.

[9] Kerberos viene de la mitología griega, del perro guardián de tres cabezas llamado Cancerbero que pertenecía a Hades.

6.4.3.6.- EAP.

El Protocolo de marcación extensible (EAP) es una extensión propuesta por la IETF para el PPP que permite que los mecanismos de autenticación arbitraria se utilicen para la validación de una conexión de PPP. EAP fue diseñado para permitir la adición dinámica de módulos de conexión de autenticación en ambos extremos de clientes y de servidor de una conexión, permitiendo a los distribuidores proveer un nuevo esquema de autenticación en cualquier momento, proporcionando la flexibilidad más alta en particularidad y variación de autenticación.

Con el EAP-TLS, un cliente presenta un certificado de usuario al servidor de marcación, al tiempo que el servidor presenta un certificado de servidor al cliente. El primero proporciona autenticación sólida de usuario al servidor y el segundo proporciona certeza de que el usuario ha contactado el servidor que esperaba. Ambos sistemas se basan en una cadena de autoridades confiables para verificar la validez del certificado ofrecido.

El certificado del usuario puede almacenarse en la PC de cliente de marcación o en una tarjeta inteligente externa En cualquier caso, el certificado no puede ser accesado sin alguna forma de identificación de usuario entre el usuario y la PC del cliente.

6.4.3.7.- ISAKMP/Oakley

ISAKMP/Oakley es el protocolo estándar para realizar una asociación de seguridad entre el transmisor y el receptor. Durante un intercambio de ISAKMP/Oakley, las dos máquinas acuerdan los métodos de autenticación y seguridad de datos, realizan una autenticación mutua y después generan una clave compartida para la codificación de datos subsecuente.

Después de establecer la asociación de seguridad, la transmisión de datos puede proceder para cada máquina aplicando tratamiento de seguridad de datos a los paquetes que transmite al receptor remoto. El tratamiento puede simplemente asegurar la integridad de los datos transmitidos o puede codificarlos también.

6.4.4.- Sin Repudio.

Debe existir alguna forma en que una parte esté completamente segura de que la otra parte ya envió el mensaje. Sin dicha garantía, las casas de finanzas, los bancos y las transacciones de ventas no podrían existir.

6.4.5.- Cifrado Punto a Punto.

Los túneles cifrados de Red Privada Virtual aseguran los datos conforme pasan a través de la red pública. Existen por lo general dos términos que se asocian con la tecnología VPN que son cifrado y encapsulamiento. La principal diferencia es que el cifrado solo codifica los datos, mientras que el encapsulamiento hace un paquete de datos del paquete original, lo envuelve en su propio paquete y después codifica todo el paquete.

6.4.6.- Administración de seguridad centralizada.

En cualquier momento en la arquitectura cliente/servidor hay distintas aplicaciones ejecutándose en varios servidores que soportan distintos clientes en redes diferentes. Imaginase lo que es administrar la seguridad en entornos tan heterogéneos y con varios tipos de aplicaciones corriendo en diferentes servidores.

Por las razones mencionadas anteriormente el ideal es poseer un especialista para cada Sistema Operativo o plataforma para administrar. La mayoría de las veces una persona puede atender varios sistemas operativos. La mínima dotación deseable es de dos personas altamente capacitadas que puedan sustituirse una a la otra. Una persona para administrar la seguridad es importante para que los otros puedan investigar y desarrollar nuevas implementaciones.

Tengamos en cuenta que si la política es que todos los nuevos productos de Informatización tengan seguridad, el sector debe tener recursos suficientes para acompañar los desarrollos desde el momento cero.

Existen algunas funciones que tradicionalmente entran en conflicto con los administradores de seguridad, estas son: el DBA (Data base administrator - administrador de base de datos) el NA (Administrador de red - Network administrator), el SA (Administrador de sistema - System administrator) y el administrador de seguridad. En todos estos casos el conflicto surge por que el Sistema Operativo no permite la adecuada separación de funciones de los distintos perfiles, lo que conduce a que cada uno de los mencionados pueda eventualmente realizar funciones solo autorizadas a otro. Por ejemplo en el Unix el root es el usuario con máximo nivel de autorización, pero no solo administra la seguridad, sino también la configuración, las bases de datos, etc. En el caso de Windows NT, el usuario Administrador, se debe utilizar para instalar o para realizar ciertas tareas de configuración, por lo que se debe compartir para las distintas tareas.

Desde el punto de vista de seguridad el sistema operativo debería permitir configurar los siguientes perfiles.

- ✓ **SecAdmin:** Administrador de seguridad. Administra altas, bajas, y cambios de perfiles de usuarios. Otorga, permisos de acceso a los recursos. Puede auditar a los usuarios.
- ✓ **System Administrator:** Instalación de software de base, administración de recursos (capacidad, performance no permisos), capacity planning, etc. Sin acceso irrestricto a los datos. Con utilización controlada de utilitarios sensitivos.
- ✓ **Network Administrator:** Atiende y monitorea la red. Instala y configura los componentes de software y hardware. Resuelve problemas de performance y conexiones.
- ✓ **DBA:** Administra la base de datos. Genera las estructuras, los índices, el diccionario de datos, administra los espacios, la performance, etc. Debe permitir al SecADmin la administración de permisos (Grant y Revoke).

- ✓ **Desarrollador:** Puede modificar programas, compilar en librerías de test, y probar con datos de prueba. EL desarrollador puede tener línea de comandos restringidos.
- ✓ **Implementador:** Debe pasar los programas de desarrollo a Producción mediante un mecanismo que asegure la transparencia. Puede intervenir operaciones. El implementador puede tener línea de comandos restringidos.
- ✓ **Operador del sistema:** Puede operar el sistema, prenderlo, apagarlo, descolgar usuarios por terminales, etc. El operador no debe tener línea de comandos.
- ✓ **Usuarios finales:** Solo deben acceder a las aplicaciones mínimas que necesitan para desarrollar su tarea.

6.4.7.- Procedimientos de respaldo/restauración.

Las claves de los dispositivos de las redes privadas virtuales son lo que hace que esta tecnología sea segura. Si los dispositivos de las redes privadas virtuales presentan problemas, ¿cómo pueden reinstalarse? Las claves de dichos dispositivos son conocidas por las personas que configuraron el servicio de las Redes Privadas Virtuales: Si no es posible restaurar las claves, entonces las comunicaciones con las otras partes no podrá restablecerse. Por lo tanto, su política de respaldo y restauración debería tomar en cuenta los sistemas operativos, los niveles de reparación, la política de reglas implementadas, y las claves asociadas con la solución particular de las Redes Privadas Virtuales.

6.4.7.1.- Planes de contingencia.

En lo posible se debe escribir uno, esto ayuda a pensar en como implementarlo, diseñarlo, entrenar al personal, implementarlo y probarlo.

Existe un equipo de especialistas que representa a las personas que conocen y que son imprescindibles para llevar adelante la ejecución del plan. Ellos entran en acción como un equipo del tipo SWAT.

Se debe poseer redundancia de los elementos críticos, array de discos, canales de comunicación, dispositivos de backup-restore de alta velocidad, o al menos contar con medios alternativos. Por ejemplo si no se pueden disponer de dos servidores funcionando a la par, acordar el proceso en un servidor de terceros, o disponer de un plan de recuperación acorde con los tiempos de la empresa (reparación o cambio del servidor) esto debe ser probado.

SI no se dispone de dos links de comunicaciones del mismo ancho de banda disponer de un alternativo y probarlo.

En empresas grandes se dispone de planes de continuidad de negocio que preparan a la organización para cualquier tipo de contingencia. Se determina por ejemplo: en caso de destrucción total de la casa matriz. Donde deben presentarse los empleados a trabajar. Donde se monta las oficinas de emergencia. Que se le debe decir a la prensa. Quien monta los sistemas de emergencia, etc.

6.5.- Sistemas Operativos.

Los sistemas operativos de cierto porte, incorporan en su diseño los elementos de seguridad necesarios para implementar la seguridad. El nivel de prestaciones varía con el sistema operativo. En flexibilidad y seguridad se puede destacar el Os/400 de IBM. En seguridad y robustez el sistema OS/390.

Existen muchas empresas que fabrican software de seguridad que se incorpora al software de base y complementa o reemplaza al sistema de seguridad nativo. Por ejemplo para OS/390 de Ibm, sistema RACF(IBM), TOP-Seret (Computer Associates).

En los sistemas operativos de escritorio los que poseen una buena seguridad son el OS/2 y el NT Workstation. El Windows 95/98 posee una seguridad relativa si se lo implementa en Red con un servidor seguro utilizando el Editor de Políticas.

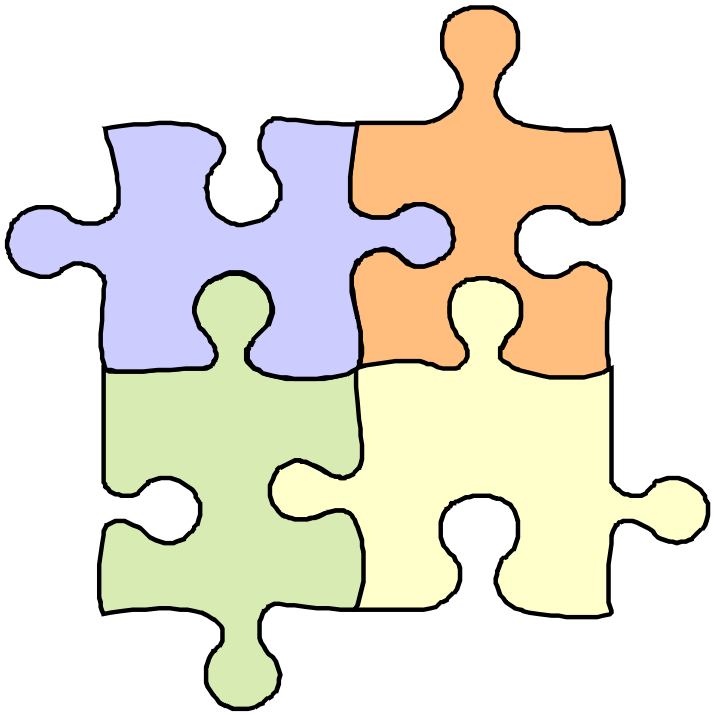
6.5.1.- Niveles de Seguridad C2 , B1 (Orange book).

EL Departamento de Defensa publicó en Diciembre de 1985 el "Trusted Computer System Evaluation Criteria" mas conocido como Orange book por el color de sus tapas en el que fija las pautas para evaluar la seguridad que brindan los Sistemas Operativos. Se establece una escala con las siguientes divisiones:

- ✓ **División D:** "Minimal Protection". Sistemas testeados pero que no pueden ser evaluados en la división siguiente:
- ✓ **Disivisión C:** Discretionary Protection. Protección discrecional (necesidad de conocer), inclusión de auditoria de los sujetos y las acciones que inician.
  - o **Clase C1:** Discretionary Security Protection. Capacidad para controlar acceso entre usuarios y objetos. El mecanismo debe permitir compartir objetos por individuo, grupos o ambos. Debe existir un proceso de Logon mediante usuario password. El Sistema Operativo debe mantener el dominio de su propia ejecución evitando la invasión de zonas de memoria, la toma de control, etc. Se debe poder verificar la integridad del sistema mediante herramientas de hardware o software provistas por el fabricante.
  - o **Clase C2:** Controlled Access Protection. Agrega a la clase anterior la capacidad de prevenir la propagación de derechos de acceso. Una mejor auditoria mediante el seguimiento de eventos de seguridad relevantes. El acceso a objetos protegidos debe ser dado por usuarios autorizados a nivel individual. La reutilización de objetos (reasignación) se hace previa revocación de todos los permisos cedidos antes a otro usuario. Los datos de auditoria deben estar protegidos y deben incluir uso de mecanismos de autenticación, operación con objetos, inicio de programas, borrado de objetos, acciones de los operadores, administradores y para cada evento fecha, hora evento, usuario, estado del evento (success o fail), terminal, nombre del objeto, etc.

- ✓ **División B:** Mandatory Protection. El sistema debe preservar la integridad de las etiquetas usadas para asegurar las reglas de control de acceso mandatorio.
  - o **Clase B1:** Labeled Security Protection Requiere todas las características requeridas en C2, más control de acceso mandatorio sobre sujetos y objetos, soporte para el etiquetado de sujetos y objetos bajo su control, es decir control de acceso basado en la sensibilidad de la información y el nivel de acceso del sujeto todo esto definible bajo una estructura combinada de jerarquía y clases. Test riguroso con corrección de errores y o fallas. Se somete a prueba el diseño del sistema el código fuente y los objetos.
  - o **Clase B2:** Structured Protection. El diseño del sistema está basado en un claramente definido y formalizado modelo de política de seguridad que requiere el control de acceso discrecional y mandatorio expresado en la clase B1. El sistema debe estar cuidadosamente estructurado en elementos de protección crítica y los otros. Posee mejores mecanismos de autenticación. Tests más rigurosos.
  - o **Clase B3:** Security Domains. El sistema debe mediar todos los accesos de sujetos a objetos, que sean a prueba de xx, y lo más pequeño posible. Para esto se debe eliminar todo el código no esencial a la seguridad, dirigiendo todo el esfuerzo de diseño en minimizar la complejidad.
- ✓ **División A:** Verified Protection.
  - o **Clase A1:** Verified Design. No se agregan características de seguridad, pero se realiza una verificación pormenorizada del diseño del sistema para asegurar que cumple con la política definida para su construcción. Debe probarse matemáticamente el modelo formal de seguridad.
  - o Mas allá de clase A1: Sistemas futuros.

CAPITULO 7



Metodología para la implementación de una VPN.

7.1. Formación de un Equipo Ejecutor
7.2. Fijación del Alcance
7.3 Estudio y Análisis
7.4. Elección de la Plataforma
7.5. Propuestas de Soluciones. (Diseño)
7.6. Seguridades.
7.7. Plan de Contingencia.
7.8. Costos.
7.9. Implementación
7.10. Mantenimiento
7.11. Medición de Resultados.

La información es una ventaja crítica para cualquier compañía, y poseer ésta a tiempo y con seguridad es fundamental para el desarrollo de cualquier organización. Además se debe tomar en consideración que la fuerza laboral del futuro será móvil, y una compañía u organización no estarán en capacidad de construir o rentar suficientes líneas a través de todo el mundo para garantizar conexiones seguras. Y es aquí donde toma importancia la implementación de una red privada virtual, ya que como se mencionó en los capítulos anteriores, una red privada virtual utiliza Internet como medio de transmisión de datos, lo que permite un considerable ahorro en términos económicos.

Se debe tener presente también que en la actualidad muchas compañías utilizan Internet para enviar correo electrónico; sin embargo, la gran mayoría no toma en consideración que ese correo se envía en modo texto, es decir sin ningún tipo de seguridad, y cualquiera que tenga acceso a Internet puede leerlo. Es por esta razón que el presente trabajo trata de familiarizar a los lectores con la tecnología de redes privadas virtuales, para hacer de sus redes más optimas y seguras al momento de transmitir y recibir datos desde el exterior, y por que no también desde el interior.

La metodología que a continuación se va a describir ha sido realizada tomando como experiencia organizaciones pequeñas y tiene como objetivo ayudar al entendimiento y mejor manejo de la teoría y la práctica en el desarrollo de Redes Privadas Virtuales.

Para obtener una Red Privada Virtual exitosa es necesario tomar en cuenta algunos factores que son de vital importancia los mismos que se convertirán en pasos para el análisis y posterior implementación de una Red Privada Virtual, los mismos que se describen a continuación:

1. Formación de un equipo de trabajo
2. Fijación del Alcance
3. Estudio y Análisis
4. Elección de la Plataforma
5. Propuestas de Soluciones
6. Seguridades

7. Plan de contingencia
8. Costos
9. Implementación
10. Mantenimiento
11. Medición

Cada uno de estos puntos serán detallados a continuación:

7.1. Formación de un Equipo Ejecutor

Si se toma en consideración de que una Red Privada Virtual es un conjunto de aplicaciones de software cliente-servidor basados en tecnología Internet[10] para la transmisión y recepción de datos, y que utilizan las plataformas de red local (LAN), redes a nivel mundial (WAN), protocolos TCP/IP y los servidores de su organización para prestar servicios de una red privada, entonces en el momento que se emprende la tarea de poner en marcha una Red Privada Virtual se hace necesario la formación de un Equipo Ejecutor, el cual debe ser conformado por un pequeño grupo de especialistas y a este agregar un número pequeño de personal con capacidad de decisión y conocimiento de la organización o empresa, de tal manera que se pueda asignar responsabilidades al personal, además que el equipo debe tener una gran capacidad de liderazgo y responsabilidad para asumir el reto de poner en marcha un proyecto de Redes Privadas Virtuales.

Los miembros recomendados para la conformación del Comité Ejecutor son: las direcciones de sistemas y recursos humanos. Deben concurrir además los gerentes cuyas divisiones vayan a tener contenido en la Red Privada Virtual. Se recomienda que al principio asistan todos los gerentes de la organización, para que estos decidan que tipo de información es confidencial y crucial para la compañía y encomienden ponerla en una red privada virtual, ya que como se

[10] La mayoría de los casos se utiliza Internet como medio de transmición, pero también se lo puede realizar en redes de área local.

explico en capítulos anteriores no es conveniente poner todo el tráfico de información que se genere en la organización en una Red Privada Virtual, ya que esta produce una sobrecarga de trabajo.

7.2. Fijación del Alcance

Una vez que se ha tomado la decisión de implementar una Red Privada Virtual es necesario definir argumentos que serán tomados en cuenta para la implementación, y que deberán cumplirse en lo posterior. Temas como los que se describen a continuación deberían ser tomados en consideración:

- ✓ ¿Para qué tener una Red Privada Virtual?
- ✓ ¿Quiénes serán los usuarios?
- ✓ ¿Qué conocimientos, información o datos se van a poner en la Red Privada Virtual?
- ✓ ¿Utilizará la Redes Privadas Virtuales para comercio global?
- ✓ ¿Instalará una extranet?
- ✓ ¿Su organización posee la capacidad técnica adecuada para mantener e instalar una Red Privada Virtual?
- ✓ ¿Cómo se integrará la Red Privada Virtual con la Red de la compañía?
- ✓ ¿Qué respuesta o resultados se desea obtener?
- ✓ ¿Qué tipo de seguridad de utilizara en la red privada virtual?
- ✓ ¿Cómo se construirá?
- ✓ ¿Qué servicios se colocarán primero, cuales después?
- ✓ ¿Su gobierno como considera al cifrado? . Se debe tener en cuenta que algunos gobiernos consideran al cifrado como arma, por lo tanto regula su uso.

El Comité Ejecutor será el organismo encargado de definir el "Por qué" y "Para qué" de una Red Privada Virtual. Para esto se analizará las expectativas creadas, las mismas que llevaron a la decisión de construirla, los problemas o retos que tienen factibilidad de resolverse con esta tecnología. Los objetivos buscados, a quienes se desea servir, el modelo administrativo con que se cuenta, y un punto muy importante a discutir, los parámetros que serán utilizados para medir el

éxito. En este paso se debe definir la política de tecnología, recursos necesarios y los responsables de obtener la información que será entregada a los creadores de la Red Privada Virtual.

Es importante recalcar que el éxito del proyecto se fundamenta en la calidad del análisis de factibilidad y éste determina el grado de participación y compromiso de los miembros del Equipo Ejecutor, esto con la finalidad de que tenga éxito la implementación de la red privada virtual. En algunos casos es necesario obtener el permiso de los altos ejecutivos con la finalidad de que exista mayor seguridad en las acciones y obtener éxito en este paso.

7.3 Estudio y Análisis

Luego de que se ha completado con la formación del equipo ejecutor, y la fijación del alcance del proyecto, es necesario realizar un estudio y análisis detenido para saber a ciencia cierta que parámetros deben cumplir las Redes Privadas Virtuales que se desea implementar.

Durante el análisis el equipo que desarrolla la Red privada virtual intenta identificar que información ha de ser procesada, que función y rendimiento se desea, cual será el comportamiento de la red, que interfaces van a ser establecidas, que restricciones se pondrán, que tipo de seguridad de necesita, que parámetros se sacrificarán a favor de la seguridad y que criterios de validación se necesitan para definir una red privada virtual correcta. Es decir durante el estudio y análisis deben identificarse los requisitos clave de la Red privada virtual.

El Análisis de factibilidad y la información en éste recolectada serán analizados por parte del Equipo Ejecutor asignado al proyecto y con esta base se propondrán los objetivos definitivos, como por ejemplo, que aplicaciones se pondrán en las Redes Privadas Virtuales, que servicios se brindarán en línea y en que fases se construirá.

Durante la fase de estudio y análisis también se deben estudiar los sistemas y soluciones utilizados por la organización y el manual de identidad corporativo.

7.4. Elección de la Plataforma

Para la implementación de una Red Privada Virtual es muy importante la elección de la plataforma en cual se la va ha desarrollar. En el mercado existe una gran variedad de soluciones, por lo que se hace necesario elegir una. También es necesario mencionar que las Redes Privadas Virtuales pueden ser construidas tanto por software, como por hardware o una combinación de éstas. Para realizar la elección de que tipo de Redes Privadas Virtuales instalar es necesario analizar los siguientes puntos:

- ✓ Software existente en la empresa.
- ✓ Aplicaciones existentes en la empresa.
- ✓ Plataforma existente en la empresa.
- ✓ Servicios que posee la plataforma.
- ✓ Seguridades que brinda la plataforma.
- ✓ Soporte técnico que posee la plataforma.
- ✓ Tipo de servidores que posee la empresa.
- ✓ Costo de la plataforma.

En el momento que se ha tomado la decisión de implementar una Red Privada Virtual, el Equipo Ejecutor deberá levantar un inventario del Hardware y Software existente en la empresa. Luego de levantado el inventario es necesario realizar un análisis para determinar que tipo de Red Privada Virtual se ajusta más a las necesidades de la organización.

Debido a que siempre será necesario contar con información y personal capacitado a tiempo y a mano, sobre todo en lo referente al manejo de la plataforma y a posibles dificultades que se encuentra en la configuración e implantación de una Red Privada Virtual, se ha visto necesario indicar que un punto de vital importancia para la selección de una Plataforma es el soporte

técnico que tienen cada una de las empresas distribuidoras y dueñas de las diferentes plataformas.

Generalmente para implantar una red privada virtual no se empezará desde cero en lo que se refiere a Hardware y Software, en la actualidad la mayoría de las empresas poseen equipos computacionales y en algunos casos se encuentra redes ya configuradas, en este caso se debe analizar que tipo de servidores tenemos y cual será la plataforma que se debe utilizar. Es necesario comprender que en algunos casos por costos de los servidores, o por que la tecnología es muy obsoleta, es muy probable que se tenga que empezar desde cero, es decir que se debe asumir que no existe nada.

Cuando se empieza desde cero el equipo ejecutor tiene más opciones para poder tomar la mejor decisión, ya que no se ve restringido a la tecnología existente, ya que si existe algo, en lo posible se debe tratar de que las Redes Privadas Virtuales sean compatibles.

7.5. Propuestas de Soluciones. (Diseño)

El diseño se lo pone como quinto punto, ya que luego de realizar el análisis se puede realizar el diseño, pero el diseño se ve afectado por la plataforma elegida, con esto se quiere decir que el diseño se lo debe realizar sólo después de haber realizado el análisis y de haber elegido una plataforma, ya que existen muchas opciones para instalar una red privada virtual.

Solo armados con el Análisis de factibilidad, la estructura general y la definición de los servicios a ser implementados, es posible acometer eficazmente la concepción, creación y construcción de la Red Privada Virtual.

En esta etapa se definirán la filosofía y enfoque globales; se concebirá la estructura lógica de la red privada virtual y se visualizará el conjunto general de la red, y esta deberá ser aprobada por el equipo ejecutor.

En la propuesta de soluciones se debe tener en consideración los siguientes aspectos:

- ✓ ¿Que aplicaciones van a pasar por la Red Privada Virtual?
- ✓ ¿Qué tipo de infraestructura de hardware soporta su organización?
- ✓ ¿Cuántos usuarios estima que utilizarán la Red Privada Virtual?
- ✓ ¿El tráfico que pasará por la VPN es pesado?
- ✓ ¿Qué tipo de seguridades se utilizarán en la Red Privada Virtual?

7.6. Seguridades.

Cómo la construcción de una Red Privada Virtual se basa en las seguridades, en este punto se debe ser muy exigente para poder disminuir a cero el riesgo de pérdida o daño de información en la Red Privada Virtual, y para esto se hace necesario la implantación de una política de Seguridad basándose en los siguientes parámetros:

- ✓ Fijación de Objetivos
- ✓ Relación Costos vs Riesgos

7.6.1. Fijación de Objetivos

Como se mencionó anteriormente, las seguridades es uno de los pasos de mayor importancia para la implantación de una Red Privada Virtual. Es necesario recalcar que con una buena política de seguridades se llegará al éxito en la propuesta, para lo cual se deben hacer algunas preguntas que permitirán conseguir el gran objetivo.

Si se toma en cuenta que es lo que se va a proteger, de que va a proteger y si se considera algunas sugerencias del equipo ejecutor (ya que éstos fueron escogidos precisamente para poder realizar un plan de seguridad), se encontrará en la capacidad de establecer cuales son las prioridades de seguridad corporativa, de tal manera que se pueda obtener una política de seguridad que brinde las mejores condiciones para la red implementada.

7.6.2. Relación Costos vs. Riesgos.

Antes de fijarse objetivos y prioridades de seguridad es necesario levantar un inventario de las posibles amenazas y debilidades que existen, luego se someterá a un análisis en el cual se debe comparar costo de implantar la seguridad con el costo de la información que se desea proteger, el mismo que brindará un panorama bastante amplio, y se debe tomar la decisión de que es lo que va a proteger, por que realmente sería innecesario proteger algo que tenga menos costo que el valor de la seguridad a implantar.

7.7. Plan de Contingencia.

Cuando se tiene grandes volúmenes de información, y es de vital importancia para la organización el correcto funcionamiento de la red privada virtual, resulta necesario, por no decir imprescindible, el tener un plan de contingencia tanto durante la fase de desarrollo y durante el funcionamiento de la red privada virtual.

Durante el desarrollo se debe considerar un plan que garantice finalizar con éxito la implementación de la red privada virtual y para ello se debe tener en cuenta los siguientes aspectos:

- ✓ ¿El personal encargado de desarrollar las Redes Privadas Virtuales tiene la suficiente capacitación y experiencia en este tema?
- ✓ ¿En el medio en el que nos encontramos existen varios proveedores de Internet que puedan brindar soporte para las Redes Privadas Virtuales?
- ✓ ¿Todo el proyecto se esta documentando?
- ✓ ¿Qué acciones se tomarán si el equipo de desarrollo se va?
- ✓ ¿Que riesgos podrían hacer que nuestro proyecto fracasará?
- ✓ ¿Qué métodos y herramientas deberíamos emplear?
- ✓ ¿Cuánta importancia hay que darle a la calidad?
- ✓ ¿Tenemos aplicaciones que entren en conflicto con las Redes Privadas Virtuales?

Estas y otras preguntas más deberán ser analizadas para poder finalizar con éxito la realización de las Redes Privadas Virtuales.

Para cuando la Red privada virtual este en funcionamiento también se deberá contar con un plan de contingencia, para garantizar a la organización su funcionamiento aún en casos extremos, para ello se deben analizar las siguientes preguntas.

- ✓ ¿Qué pasa si el proveedor de Internet cierra sus oficinas?
- ✓ ¿Qué acciones se realizarán en caso de que los servidores fallen?
- ✓ ¿El personal técnico que se tiene esta en capacidad de resolver los problemas?
- ✓ ¿Se tiene servicios de emergencia?
- ✓ ¿Quién administrará la red en caso de que el personal a cargo salaga de la organización?

7.8. Costos.

Puesto que la parte económica juega un papel muy importante en el éxito de una Red Privada Virtual, se considera muy importante analizar los siguientes puntos para determinar los costos de implementar una Red privada virtual.

- ✓ Hardware
- ✓ Software
- ✓ Capacitación
- ✓ Contratación de Servicios

7.8.1. Hardware

Como se había mencionado anteriormente es necesario saber con que Hardware cuenta la institución, de tal manera que después de haber levantado un inventario de los equipos existentes, se pueda determinar que equipos se van a adquirir y cuales son los equipos existentes que se podrán utilizar,

posteriormente se determina las características del hardware que se va adquirir de tal forma que se pueda hacer un concurso de ofertas para la adquisición de los diferentes implementos para la puesta en marcha de la Red Privada Virtual.

7.8.2. Software

Dependiendo de la plataforma elegida, los servicios y las aplicaciones que a determinado momento la Red Privada Virtual tenga a disposición de los usuarios, los costos de la implementación serán elevados, moderados o bajos, pero lo que si hay que estar muy consiente es que el servicio que brindará la Red Privada Virtual debe ser de óptima calidad de tal manera que haya valido la pena la inversión, por esto el Equipo Ejecutor tiene que tener la capacidad para demostrar a las autoridades de que el costo de la implementación no es un gasto más bien es una inversión que mejorará la rentabilidad y los servicios que brinda la empresa.

7.8.3. Capacitación

Uno de los rubros que se debe tener presente en la implementación de una Red Privada Virtual es la capacitación, en vista de que el personal técnico que se encargara de realizar la implementación necesitará que se le ponga al día en la tecnología de Redes Privadas Virtuales.

Además es necesario hacer conocer a las máximas autoridades que la capacitación siempre será una inversión y por tal motivo brindarle especial atención, para evitar posteriores inconformidades tanto de los usuarios como de las autoridades de la empresa.

7.8.4. Contratación de Servicios

Este es un rubro que en algunas empresas se lo puede evitar, en vista de que el personal existente en la institución puede estar en condiciones suficientes para llevar adelante un proyecto de esta magnitud. En el caso de no existir se hace

necesario la contratación de personal especializado, en este caso diremos que será el rubro más elevado, en vista de que obtener mano de obra calificada y cualificada llevará una inversión bastante elevada.

7.9. Implementación

Durante la implementación se utilizarán especialmente la fase del análisis y la fase del diseño, es necesario aclarar que antes de empezar con este punto, el personal que va a implementar la red privada virtual ya debe estar lo suficientemente capacitado acerca de esta tecnología para poder finalizar con éxito las Redes Privadas Virtuales.

En esta fase se configurarán los servidores, los clientes y demás equipos que sean necesarios para la red privada virtual.

7.10. Mantenimiento

El mantenimiento se centra en el cambio que va asociado a la corrección de errores, a las adaptaciones requeridas a medida que evoluciona el entorno de la red privada virtual, y a cambios debidos a las mejoras producidas por los requisitos cambiantes de la organización.

Por lo delicado del asunto, una red privada virtual debe ser administrado apropiadamente, es decir, debe ser mantenido, actualizado y además renovado con regularidad para garantizar su uso, ya que es fundamental que siempre los usuarios se fíen en la confidencialidad que proporciona la red privada virtual, ya que si un usuario sospecha que sus información no esta segura, talvez se restringa utilizar la Red Privada Virtual, especialmente si se esta realizando negocios a través de ella.

7.10.1. El Mantenimiento preventivo

En si, se refiere a las actividades de orden técnico al nivel de hardware y software en producción, para garantizar la integridad de los archivos y sus

respectivos enlaces y la verificación de la disponibilidad de la red privada virtual. Otra fase del mantenimiento consiste en la verificación constante de fallas en la seguridad, ya que es imposible determinar en un momento dado la inviolabilidad de la Red privada virtual.

7.10.2. El mantenimiento correctivo

En este punto nos referimos a que incluso llevando a cabo las mejores actividades de garantía de calidad, es muy probable que la organización descubra defectos en la red privada virtual. El mantenimiento correctivo modifica la red privada virtual para arreglar los defectos.

7.10.3. La Actualización

Se refiere a los pequeños cambios a servicios de acuerdo con la actualidad y el día a día de la organización, por ejemplo el cambio de contraseñas, la implementación de un protocolo más seguro para la autentificación, el crecimiento de la organización, entre otros.

7.10.4. La Renovación

Basados en la realimentación y análisis de resultados que se obtengan de la actividad de medición, se realizará la renovación de la red privada virtual. Esta, se refiere a los cambios más profundos en el contenido, servicios, topologías y arquitectura de la red privada virtual. La renovación lleva a las Redes Privadas Virtuales más allá de sus requisitos funcionales originales.

Tanto el Mantenimiento, la Actualización y la Renovación pueden ser subcontratados con Personal externo, pero sólo en un comienzo y con el apoyo activo de su personal, de lo contrario su organización se perderá la oportunidad de recorrer la curva de aprendizaje de esta tecnología o lo que también se podría

decir que el personal se perdería la oportunidad de capacitarse o de estar acorde a las necesidades actuales.

Esta tecnología está en su infancia, y como todo aquello que vale la pena, hay que comenzarlo temprano, antes que las barreras de entrada las construya su competencia.

7.11. Medición de Resultados.

Este punto es necesario para poder realizar una evaluación del trabajo realizado en la institución, por tanto la evaluación se realizará en todo momento, se evaluará a partir de la puesta en marcha del proyecto y se podrá medir como se está avanzando en la ejecución, en lo posterior se evaluará la utilización de los servicios y por defecto se estará evaluando la conformidad, la aceptación por parte de los usuarios hacia la nueva implementación.

COMPROBACION DE HIPOTESIS.

> **Hipótesis:** "Es posible desarrollar una metodología para la implementación de VPN´s que facilite integrar dos LAN mediante Internet con la finalidad de conseguir una WAN segura, de rendimiento aceptable y de bajo costo".

La hipótesis queda absolutamente comprobada, ya que si es posible utilizar Internet como medio de transmisión para unir dos redes LAN privadas, lo que da como resultado obtener una Red Privada Virtual segura, confiable y a bajos costos utilizando medios de transmisión públicos.

Además se desarrollo una metodología que ayude al mejor desarrollo e implementación de esta tecnología al igual que se implemento paso a paso el proceso de configuración de la VPN en el servidor y en el cliente utilizando como plataforma Windows 2000 Server, Windows XP profesional y Windows 98se.

Conclusiones

- ✓ Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro.

- ✓ Las VPN permiten una comunicación entre las oficinas centrales y las oficinas remotas, muy distantes geográficamente a través de internet de una forma segura, sin tener que depender de líneas rentadas o líneas dedicadas.

- ✓ Las VPN permiten brindar servicios a los clientes de la empresa en cualquier lugar del mundo, con lo que los clientes obtendrán la información que el necesita al instante, lo que generará una mayor productividad de la empresa.

- ✓ La implementación de una VPN, necesita de personal calificado para el análisis de requerimientos de la empresa y ver si es conveniente la implementación, para la misma. Este personal debe recibir la colaboración de cada uno de los departamentos de la empresa para que la implementación de la VPN sea óptima.

- ✓ Esta tecnología dispone de varias arquitecturas y topologías fácilmente adaptables a los diferentes tipos de empresas que puedan existir, ya que es una tecnología muy flexible y fácilmente acoplable al diseño de red de su empresa.

- ✓ La velocidad de comunicación a través de una VPN, se ve afectada considerablemente por la encriptación y encapsulación que los datos transferidos necesitan, para navegar seguros por la red pública.

- ✓ Windows 2000 Server, permite conexiones con los protocolos PPTP, y L2TP, pero las implementaciones más comunes se las realiza con PPTP porque es un protocolo que pone a la disposición Microsoft, en cambio L2TP no muy utilizable en la actualidad.

Recomendaciones

- ✓ Instalar y configurar una Red Privada Virtual, utilizando la metodología planteada en este trabajo y emitir las críticas respectivas sobre la eficiencia de la misma.

- ✓ Continuar con el estudio de la tecnología de VPN, ya que es una tecnología que va creciendo y que necesita de una constante actualización de conocimientos debido a las constantes actualizaciones en el software de soporte que se implementan en los sistemas operativos especialmente en Windows.

- ✓ Realizar una investigación sobre la compatibilidad de VPN con el nuevo proyecto de Internet 2, ya que VPN esta basado en IPv4 en cambio Internet 2 se basa en IPv6, conceptualmente similares pero diferentes en la implementación, tomando en cuenta que la tecnología de IPv6 será el futuro de internet.

- ✓ Se recomienda el estudio de implementación de VPN con el uso de dispositivos de Hardware, tema que a la finalización de este trabajo esta en sus principios, para lo cual será necesario buscar la colaboración de la empresa privada, debido a los altos costos que esto representaría.

- ✓ Como ya sabemos las VPN brindan seguridad y bajos costos en las comunicaciones, es recomendable que cuando usted necesite altas velocidades de comunicación no piense ni por un instante que la solución es una VPN porque no obtendrá excelentes velocidades de transmisión debido al encapsulamiento y encriptación de la información.

- ✓ Cabe anotar que la metodología expuesta, puede ser no acoplable para determinada situación o empresa, por lo que se recomienda plantear nuevas metodologías de acuerdo a las necesidades particulares que se presenten en cada empresa.

BIBLIOGRAFÍA

http://www.findvpn.com/	The WHIR´s FIND VPN.
http://vpn.shmoo.com/	VPN Information on the World Wide Web
http://www.cudi.edu.mx	CUDI – Corporación Universitaria para el Desarrollo de Internet
http://www.ciberhabitat.gob.mx	CiberHábit – Ciudad de la Informática
http://www.ietf.org	IETF - The Internet Engineering Task Force
http://www4.uji.es/~al019803/ip	Informática y Sociedad. Protocolos TCP/IP. Juan Salvador Miravet Bonet
http://www.microsoft.com/security/	Microsoft – Security & Privacy
http://www.microsoft.com/spain/seguridad/	Web de Recursos de Seguridad de Microsoft
https://www.vpn.net/	IMPERITO "Global Leaders in Manager Network and Client Security"

http://www.rediris.es/	Red Iris Española. Redes Privadas Virtuales Dinámicas.
ftp://ftp.rfc-editor.org/in-notes/tar/RFC-all.zip	RFC´s de la IETF. (Todos)
http://www.saulo.net/pub/tcpip/	Curso de protocolos TCP/IP. Saulo Barajas
http://www.monografias.com/	Monografías.com
http://www.infonetics.com	Infonetics Research
http://www.microsoft.com/articles/tcpip.htm	Instalación, introducción al TCP/IP en Windows NT. Microsoft. 2001
http://www.microsoft.com/serviceproviders/vpn_ras/vpnoverview.asp	Windows 2000 Server – Virtual Private Networking: An Overview. Microsoft Corporation.
http://www.microsoft.com/technet/vpnsolutions/index.htm	Virtual Private Networking – Microsoft Corporation 1999
http://www.microsoft.com/windows2000/technologies/communications /vpn/l2f_vpn.html	Layer Two Forwarding – Microsoft Corporation 2001. White Paper

www.iec.csic.es/criptonomicon/autenticacion Autenticación y autorización en Internet. 2001

http://rinconquevedo.iespana.es/rinconquevedo/Criptografia/autenticacion.htm

INTRODUCCIÓN A LA CRIPTOGRAFÍA. Aplicaciones criptográficas - Autenticación

http://www.infoapuntes.com.ar/Apuntes/seguridad.htm

SEGURIDAD EN REDES COMPLEJAS: EL CASO DE INTERNET. 2002

http://www.eff.org//Privacy/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html

RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF)

http://webs.ono.com/usr026/Agika2/3internet/autentificacion.htm

Ataques de Autenticación. Enlaces de Seguridad. 10-09-02

Microsoft Corporation Guía completa de Windows NT 4.0 Server Editorial McGraw-Hill , 591 páginas, © Microsoft Corporation

Microsoft Corporation http://www.microsoft.com /ecuador Microsoft Corporation del Ecuador Copyright © 1999.

	e-mail: e-cliente@microsoft .com
IETF	http://www.ietf.org The Internet Engineering Task Force
Bitway	http://www.bitway.com.ar/ products/POPMasterVPN Business Integration Product & Service. Copyright 1997-1998-1999
TCP/IP	http://emn.derecho.uma.es /grumetes/tcpip.htm Página de temas Interesantes
CINTEL	http://www.cintel.org.co Centro de Investigacion de las Teleco-municaciones Avenida 9 No. 118-85 PBX. (57-1) 6208307 FAX.(57-1)2144121 Santa Fe de Bogotá D.C., Colombia webmaste@cintel.org.co - cintel@impsat.net.co
King Adrian	Windows' 95, Editorial McGraw-Hill 1994, 1era Edición 411 páginas.
Richter Jeffrey	Windows NT Avanzado, Editorial McGraw-Hill 1994, 1era Edición, 654 páginas.
Microsoft Corporation	Microsoft Windows Paso a Paso, Editorial McGraw-Hill 1992, 1era Edición, 343 páginas.

Andrew S. Tanenbaum	Redes de Computadores, Editorial Prentice-Hall Hispanoamericana S.A., 813 páginas.
Steven Brown	Implementación de Redes Privadas Virtuales. Editorial McGraw-Hill Interamericana Editores, S.A. de C.V. 594 Páginas.
Feit Sidnie	TCP/IP. Arquitectura, protocolos e implementación. Editorial McGraw-Hill 1997. 623 Páginas.
Hernández Claudio	Hackers, los piratas del chip. Primera Edición. Libro digital. 2002.
Irving Reascos-Jaime Rivadeneira	Metodología para la Implementación de Intranets. Tesis de Grado para la obtención del Título en Ingeniería en Sistemas. Universidad Técnica del Norte.
IETF - RFC791	Internet Protocol. J. Postel. Sep-01-1981. (Format: TXT=97779 bytes) (Obsoletes RFC0760) (Updated by RFC1349) (Also STD0005)(Status: STANDARD)
IETF - RFC2460	Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998. (Format: TXT=85490 bytes) (Obsoletes RFC1883) (Status: DRAFT STANDARD)

IETF - RFC792	Internet Control Message Protocol. J. Postel. Sep-01-1981.(Format: TXT=30404 bytes) (Obsoletes RFC0777) (Also STD0005) (Status: STANDARD)
IETF - RFC3228	IANA Considerations for IPv4 Internet Group Management Protocol IGMP). B. Fenner. February 2002. (Format: TXT=6473 bytes) (Also BCP0057) Status: BEST CURRENT PRACTICE)
IETF - RFC768	User Datagram Protocol. J. Postel. Aug-28-1980. (Format: TXT=5896 bytes) (Also STD0006) (Status: STANDARD)
IETF - RFC793	Transmission Control Protocol. J. Postel. Sep-01-1981. (Format: TXT=172710 bytes) (Updated by RFC3168) (Also STD0007) (Status: STANDARD)
IETF - RFC2661	Layer Two Tunneling Protocol "L2TP". W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter. August 1999. (Format: TXT=168150 bytes) (Status: PROPOSED STANDARD)
IETF - RFC1510	The Kerberos Network Authentication Service (V5). J. Kohl, C. Neuman. September 1993. (Format: TXT=275395 bytes) (Status: PROPOSED STANDARD)

IETF - RFC2251 — Lightweight Directory Access Protocol (v3). M. Wahl, T. Howes, S. Kille. December 1997. (Format: TXT=114488 bytes) (Status: PROPOSED STANDARD)

IETF - RFC3232 — Assigned Numbers: RFC 1700 is Replaced by an On-line Database. J. Reynolds, Ed.. January 2002. (Format: TXT=3849 bytes) (Obsoletes RFC1700) (Status: INFORMATIONAL)

ANEXOS

Instalación y configuración del Servidor VPN en Windows 2000 Server.

Para la instalación y configuración de una Red Privada Virtual, debemos configurar primeramente el Servidor VPN, que en nuestro caso lo haremos en Windows 2000 Server. Además configuraremos los Clientes VPN, para lo cual tomaremos 2 plataformas que serán Windows XP Profesional y Windows 98se.

Las características de hardware que deben cumplir los equipos deben ser las mínimas recomendadas para la instalación de los diferentes sistemas operativos.

Requisitos del sistema.

Los requisitos mínimos de los sistemas operativos que vamos a utilizar se encuentran enmarcados dentro de los siguientes parámetros.

- ✓ Procesador Intel Pentium a 133MHz o Superior
- ✓ Se recomienda al menos 256Mb de memoria RAM, aunque lo mínimo admitido es 128MB.
- ✓ Espacio libre en Disco mínimo de 1GB, es posible que se necesite más espacio en disco dependiendo de los servicios adicionales que se deseen instalar para lo cual es recomendable tener previsto un espacio mínimo de 4GB.
- ✓ Monitor VGA o de mayor resolución
- ✓ Teclado y Mouse.
- ✓ FaxModem de 56600bps
- ✓ Tarjetas de Red 10/100 Mbps

Debido a los costos de hardware existentes en el mercado en la actualidad, es totalmente posible mejorar dichas características sin que la inversión sea alta, y tener un buen funcionamiento de la Red Privada Virtual.

Para la instalación y configuración del Servidor VPN, debemos realizar las siguientes configuraciones:

- ✓ Instalar y Configurar Active Directory
- ✓ Instalar y Configurar DNS
- ✓ Instalar y Configurar Enrutamiento y Acceso Remoto
- ✓ Instalar y Configurar Usuarios

Realizaremos la instalación y configuración de estos 4 componentes paso a paso.

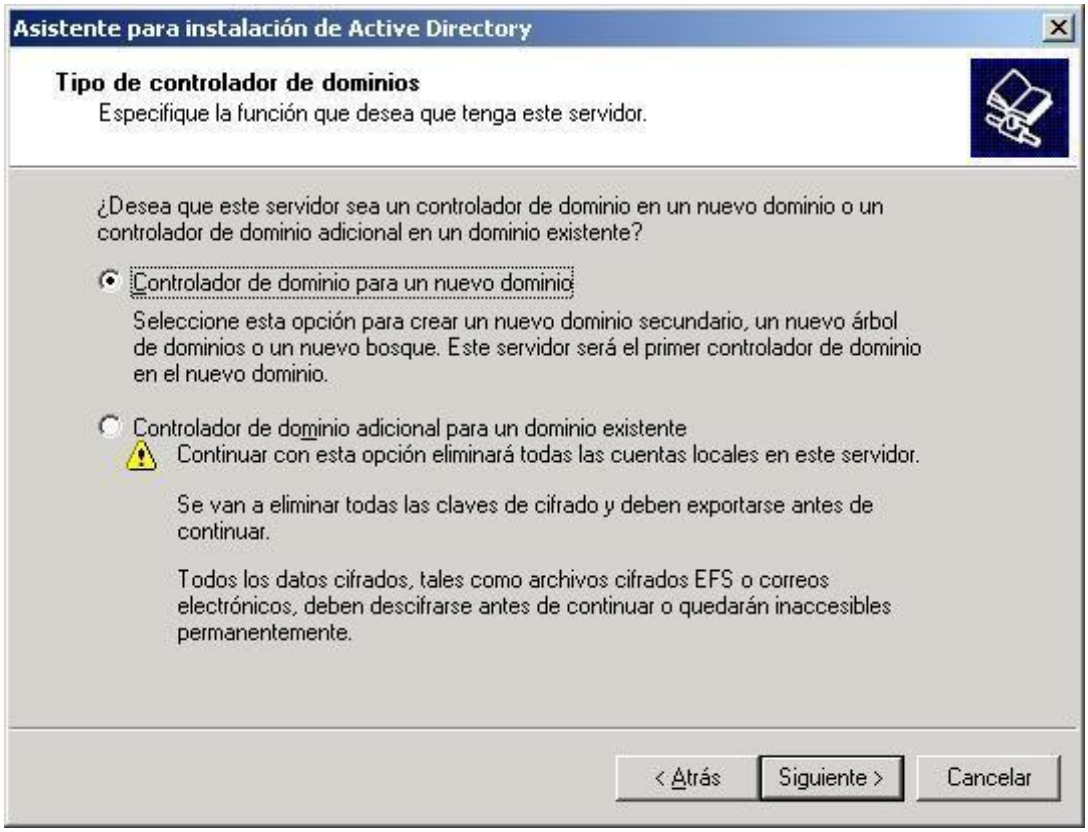
Instalar y Configurar Active Directory

El Active Directory, nos permitirá tener un controlador de dominio instalado en nuestro equipo, para lo cual necesitamos realizar los siguientes pasos:

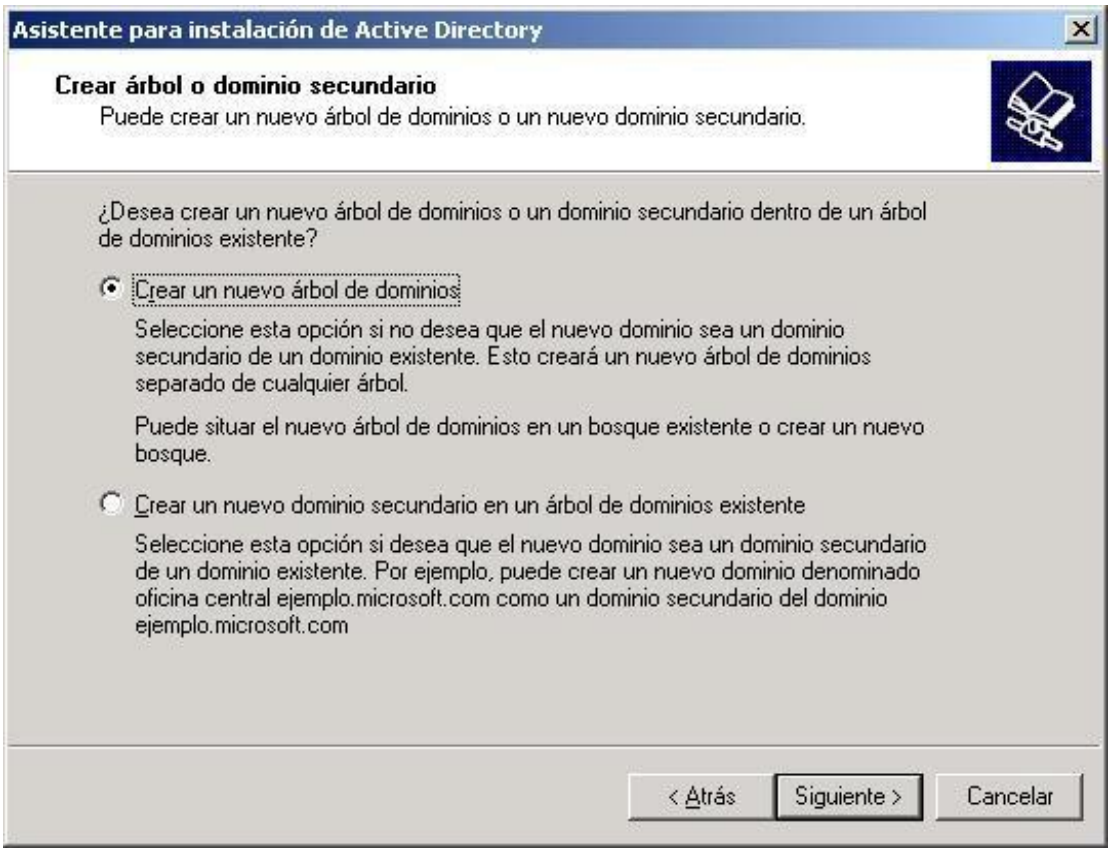
1. Una vez que instalamos Windows 2000 Server, tenemos la pantalla de Configurar el servidor de Windows 2000, y hacemos clic sobre **Active Directory**.

2. A continuación nos desplazamos hacia la parte final y pulsamos sobre el enlace **Iniciar**. Y comenzaremos el asistente para la instalación de Active Directory. Pulsamos sobre el botón **Siguiente**.

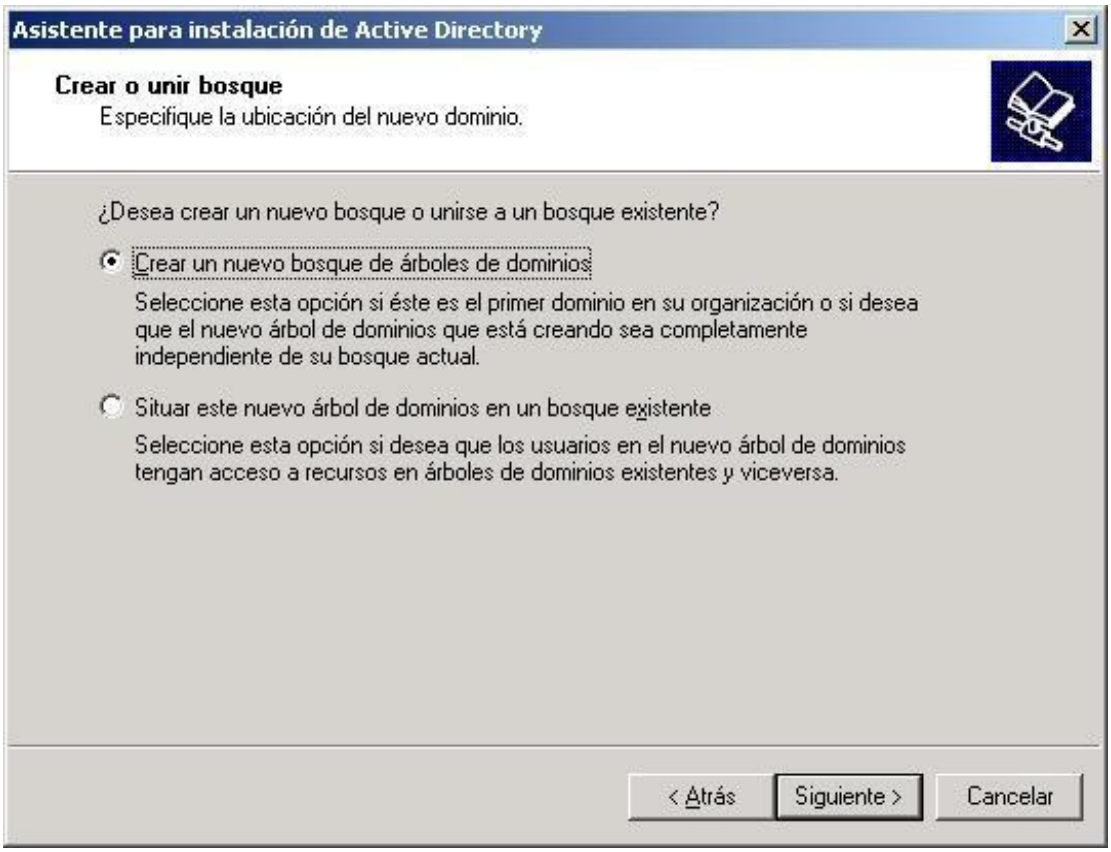
3. Escogemos la opción de Controlador de Dominio para un nuevo dominio y pulsamos sobre Siguiente.



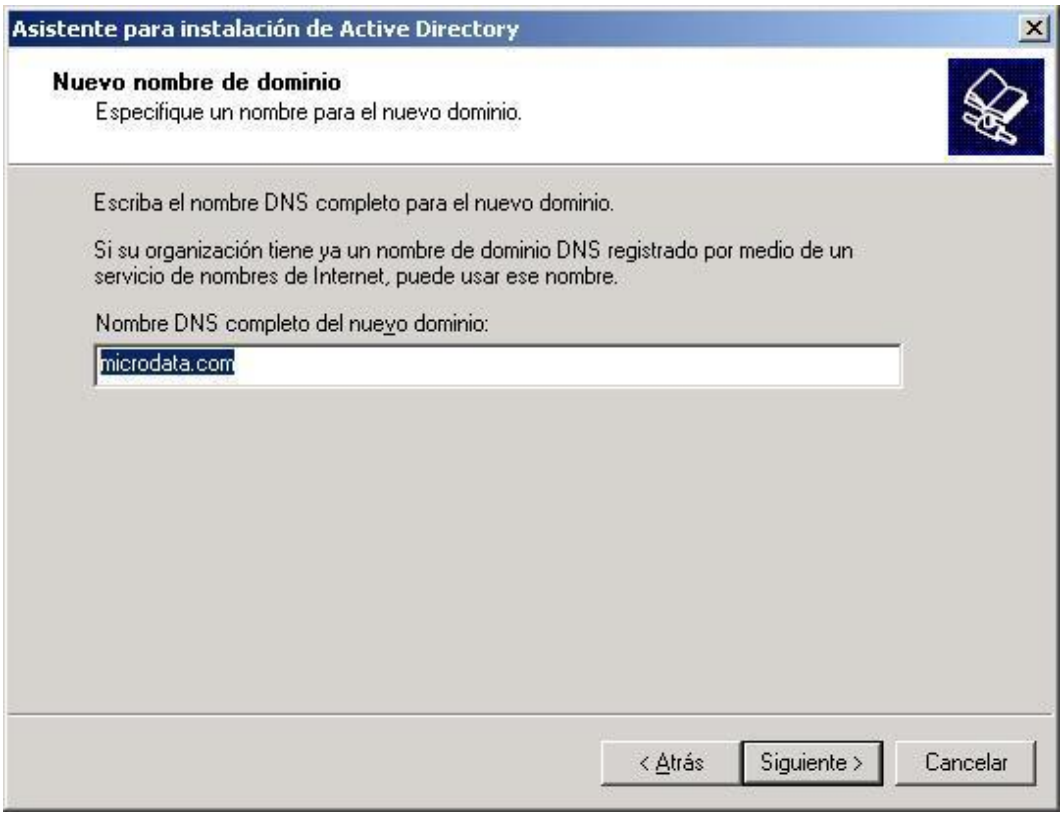
4. Marcamos la opción Crear un nuevo árbol de Dominio y pulsamos sobre Siguiente.



5. Seleccionamos la opción Crear un nuevo bosque de árboles de dominios y pulsamos sobre Siguiente.

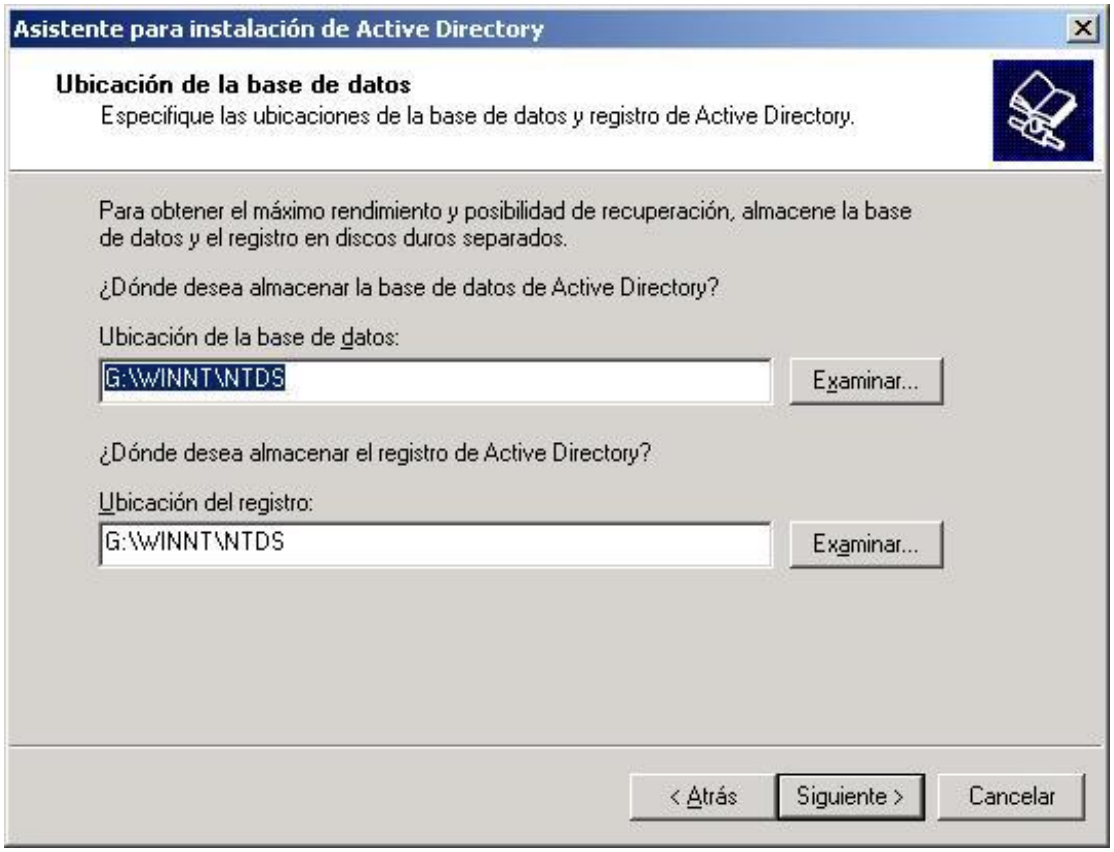


6. Ahora tenemos que escribir el nombre del Domino que deseamos crear, para lo cual en el recuadro escribimos del nombre completo de DNS, para nuestro ejemplo hemos escogido el nombre de microdata.com, seguidamente pulsamos sobre el botón **Siguiente**.

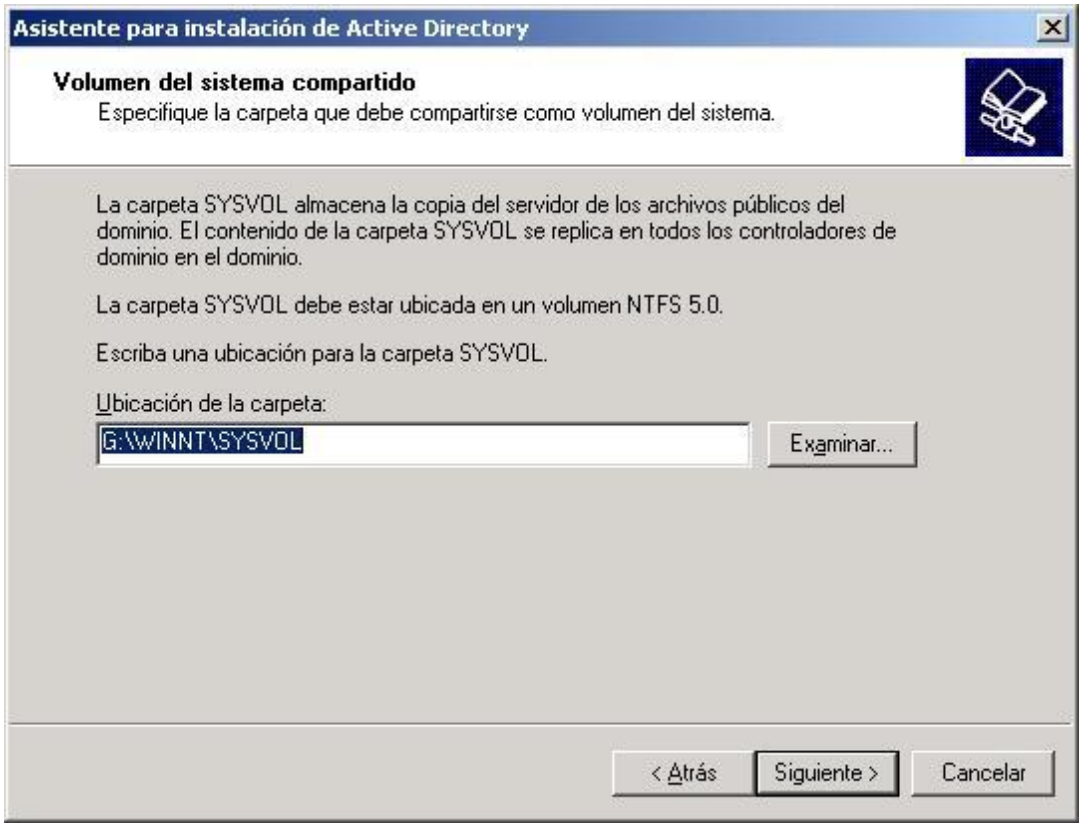


7. El nombre del NetBIOS, para las versiones anteriores de Windows en nuestro caso le hemos puesto como MICRODATA y pulsamos **Siguiente**.

8. La base de datos y registro de Active Directory, se encontraran en las ubicaciones por defecto que no da Windows 2000 Server que es \WINNT\NTDS, por lo tanto en la siguiente ventana únicamente pulsamos sobre el botón **Siguiente**.

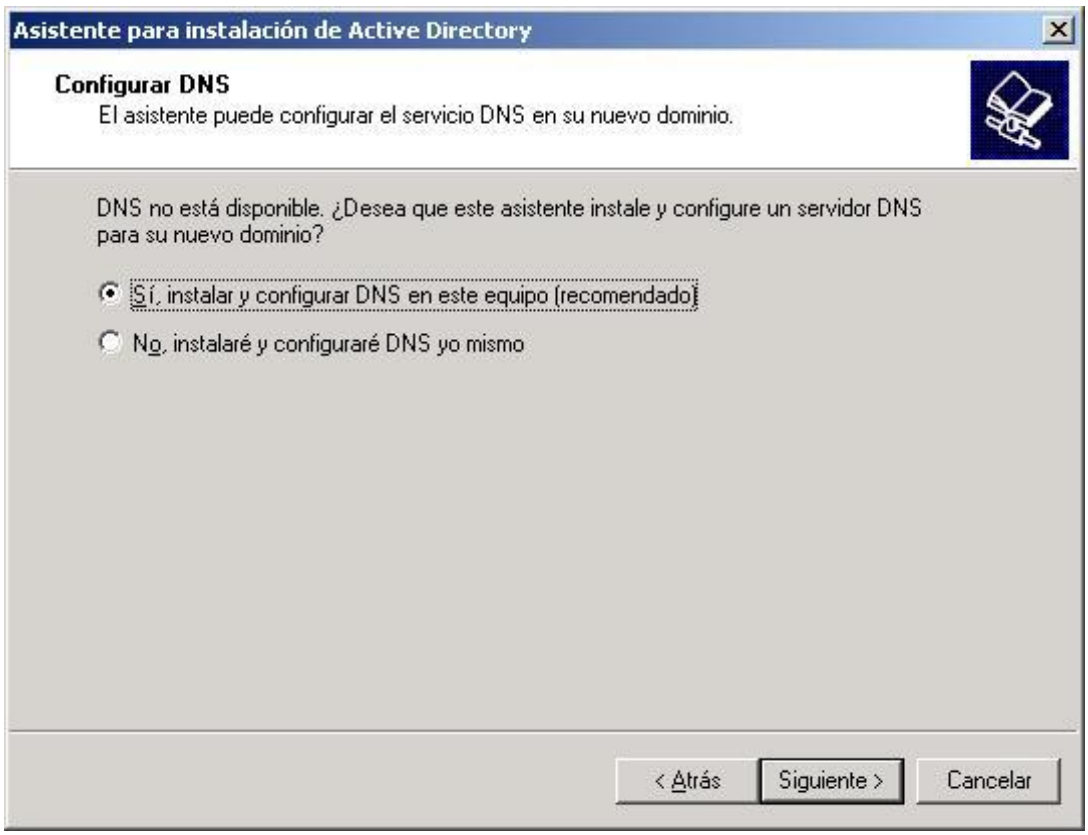


9. AL igual que en el paso anterior procedemos en este paso y únicamente pulsamos el botón **Siguiente**. Es lo posible es recomendable utilizar las carpetas que Windows nos ofrece para el caso.

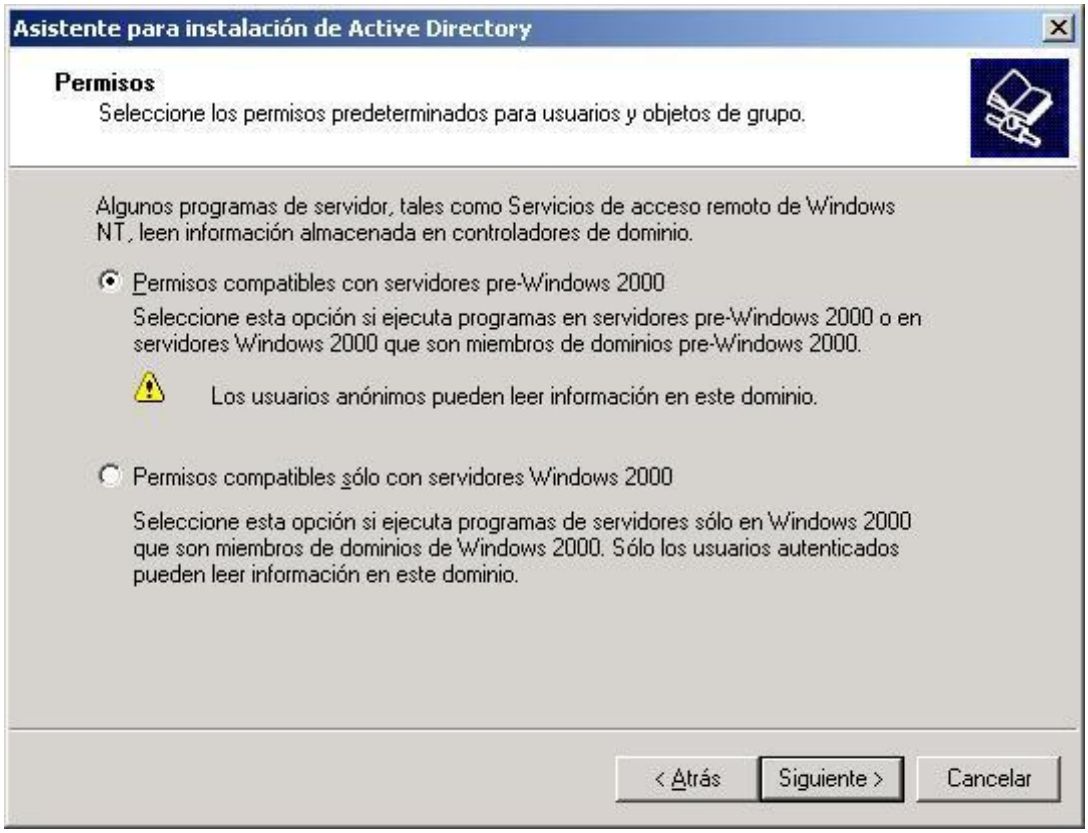


10. Como no existe el dominio MICROData.com, se nos presentará el siguiente mensaje en el cual nos limitaremos a pulsar sobre el botón de **Aceptar**.

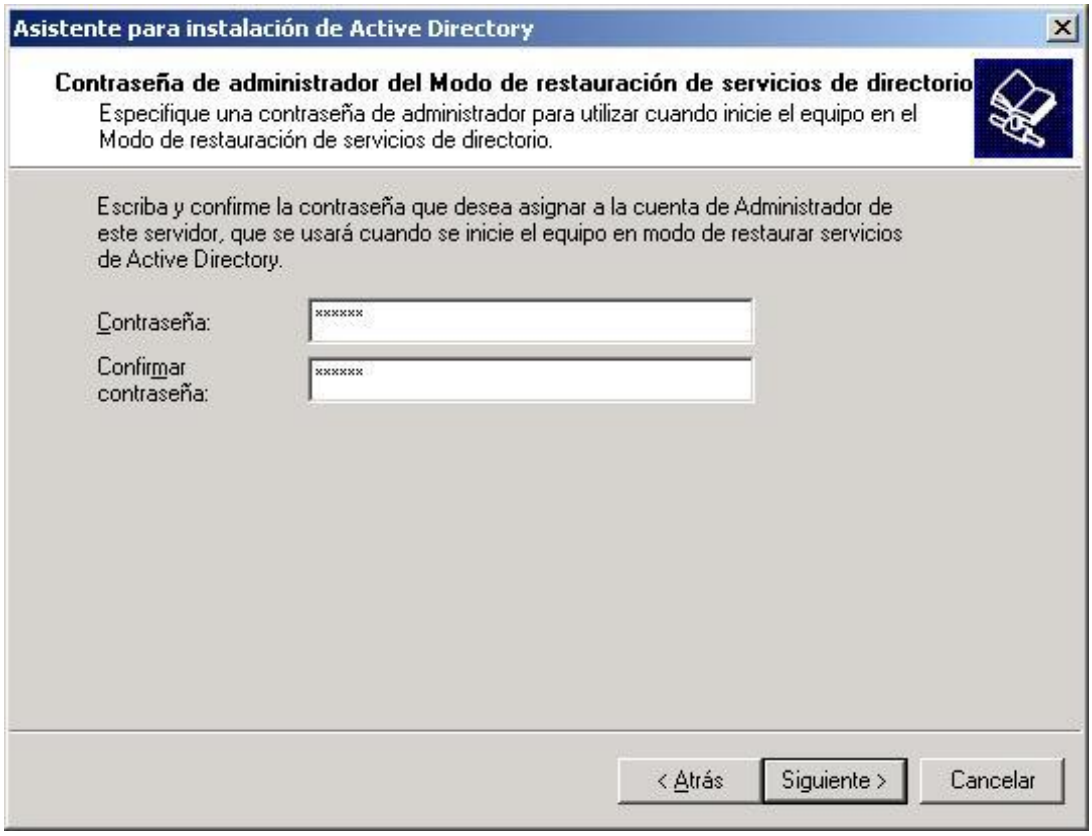
11. En la siguiente ventana escogemos la primera opción de **Si, instalar y configurar DNS en este equipo** y luego pulsamos sobre el botón **Siguiente**.



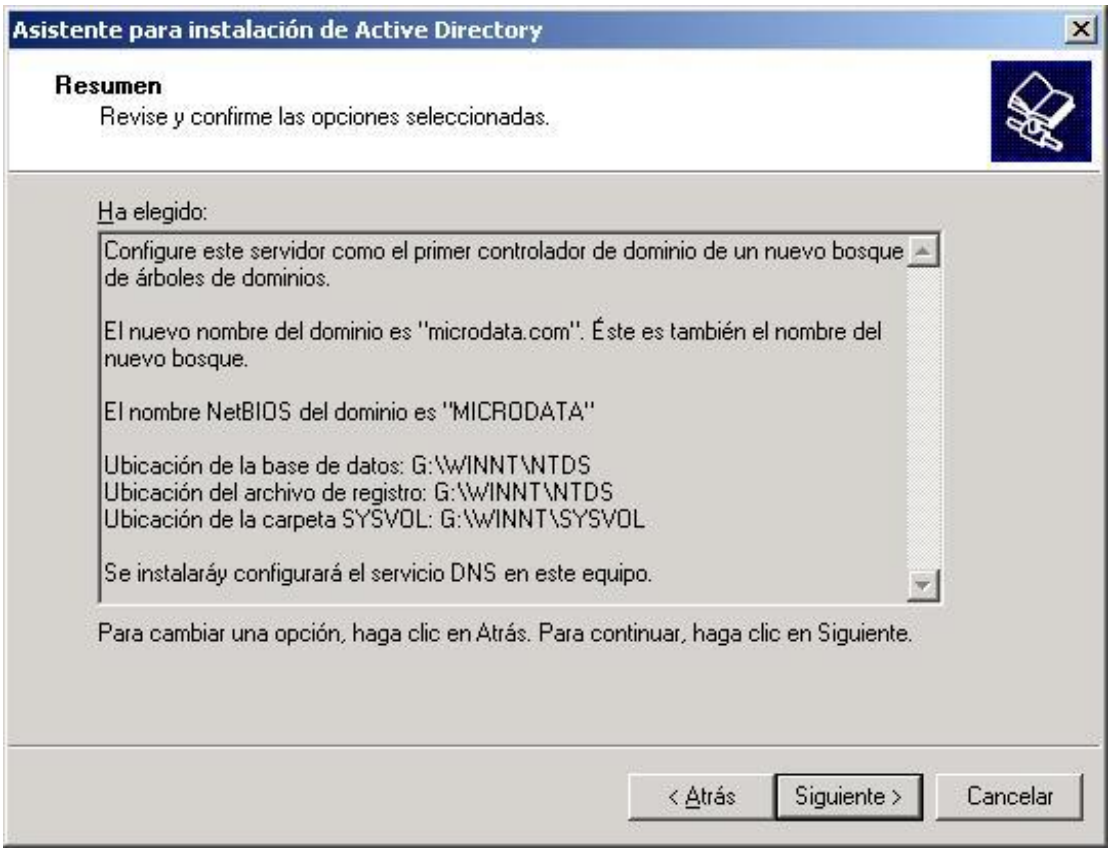
12. En esta ventana escogemos la opción de **Permisos compatibles con servidores pre-Windows 2000**, para obtener una mejor compatibilidad con sistemas anteriores a Windows 2000, y luego **Siguiente**.



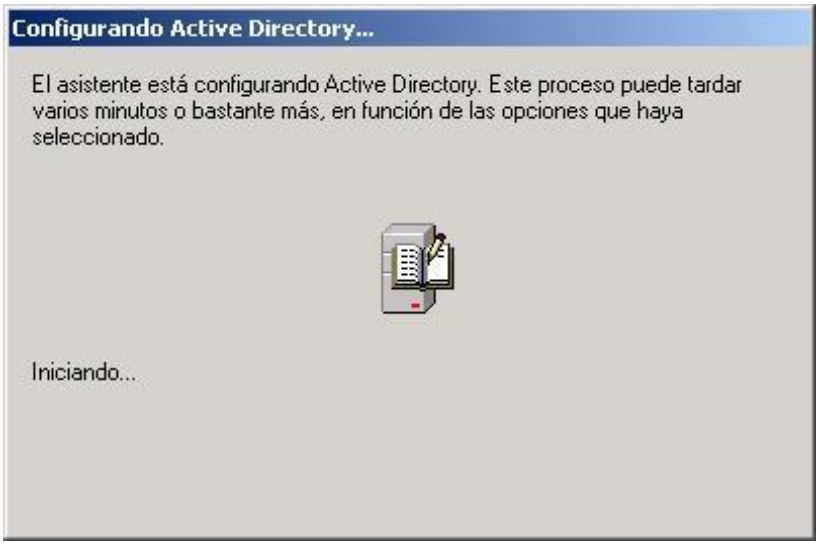
13. A continuación especificamos una contraseña para el modo de restauración de servicios de Active Directory, es conveniente que su contraseña sea fácilmente recordable, porque de olvidarse usted no podrá reconfigurar su Active Directory. Una vez ingresada y confirmada la clave pasamos a la siguiente ventana.



14. Esta ventana le presenta un resumen de todo lo que se configurará dentro del Active Directory. En este punto es el último en donde usted puede regresar a cambiar algún dato que no este de acuerdo, porque al pulsar en el botón Siguiente, comenzará a instalar y configurar automáticamente el Active Directory, este proceso puede tardar varios minutos (10apoximadamente) dependiendo de las características de su equipo. Si usted esta de acuerdo con todos los datos debe pulsar en **Siguiente**.



15. Se mostrará esta ventana en la que le indica las diferentes configuraciones que se van haciendo dentro del entorno Active Directory.



16. Una vez finalizada la instalación y configuración, aparece la siguiente ventana en la que debemos pulsar el botón de **Finalizar**.

17. Es recomendable que usted reinicie el equipo una vez que se haya finalizado todo el proceso. Pulse sobre el botón de **Reiniciar ahora**.

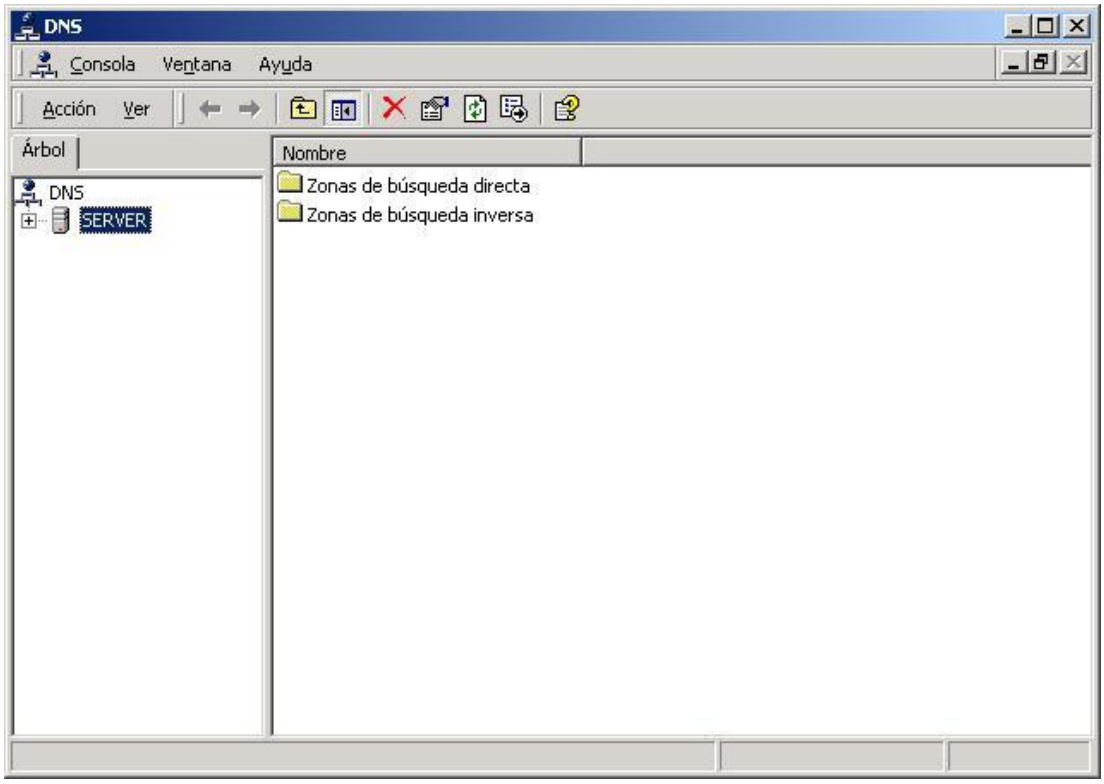
18. El momento que el equipo se reinicie estará instalado y configurado el Active Directory, que servirá como base para la instalación y configuración del Servidor VPN.

Instalar y Configurar DNS

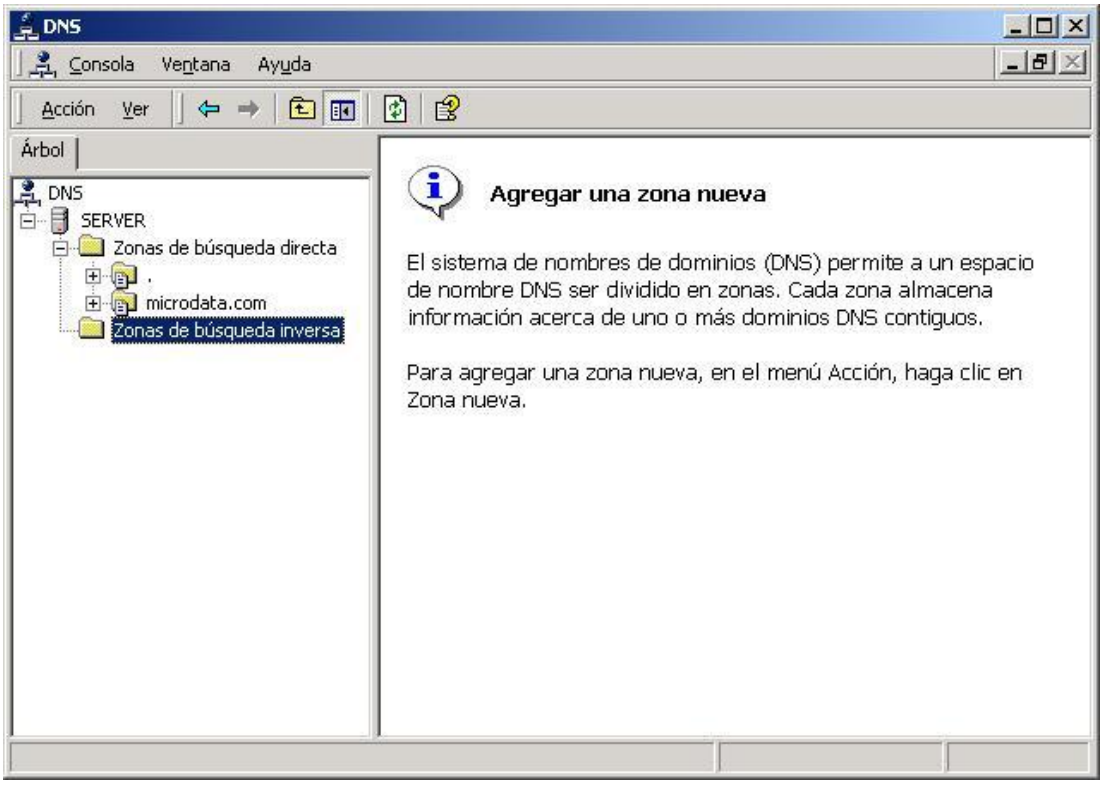
Realmente el la instalación del Active Directory ya instalamos parte del DNS, ahora lo que haremos a continuación es complementar dicha instalación.

1. Activamos la ventana de Configuración del DNS, que la encontramos en la siguiente ruta: **Inicio/Programas/Herramientas Administrativas/DNS**.

2. Una vez activada la ventana de configuración del DNS, podemos observar que se encuentra en la parte izquierda el nombre de nuestro servidor que en nuestro caso es **SERVER**, hagamos clic sobre el nombre del servidor y vayamos desplegando todo el árbol para obtener todas las zonas existentes en nuestro equipo.

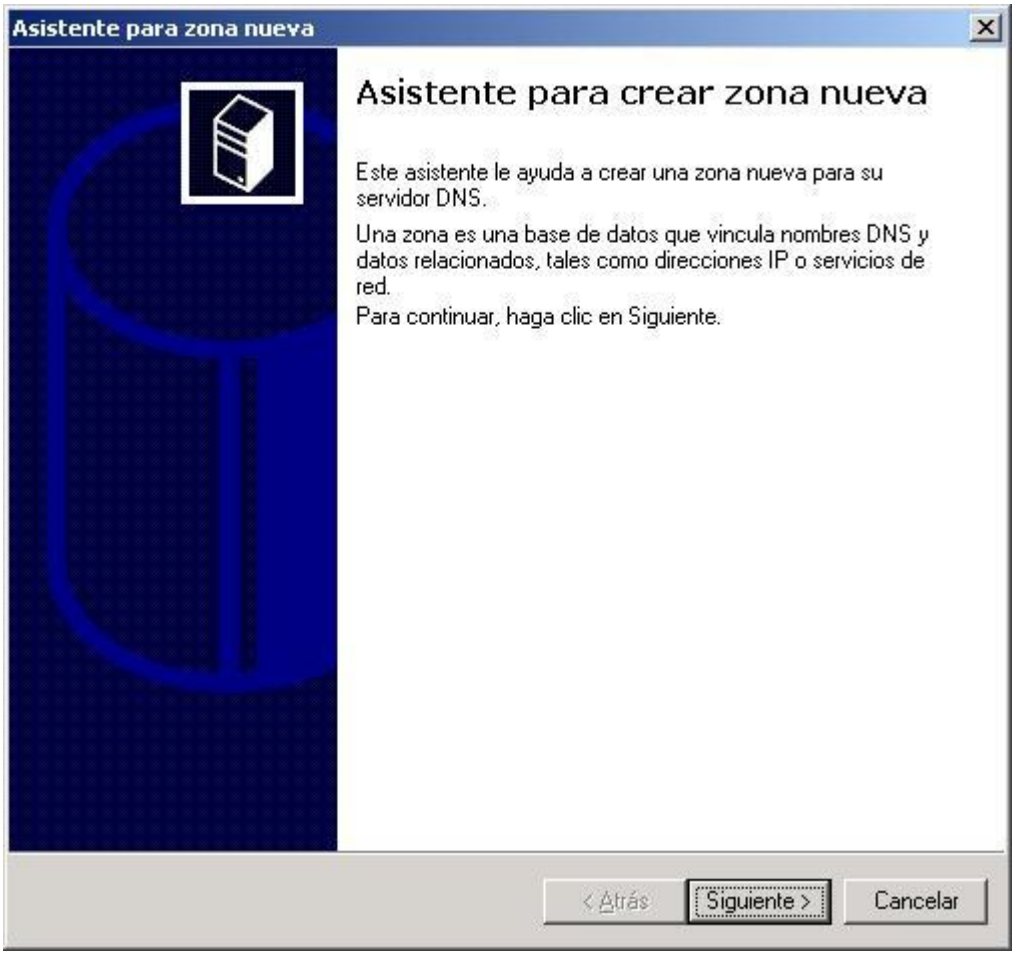


3. Podemos observar que existe una zona denominada microdata.com, que es la zona que fue creada en la instalación del Active Directory. En base a esta zona operaremos para la instalación de nuestro servidor VPN. Se recomienda revisar los datos de la zona microdata.com para observar como fue creada y tener en cuenta estos datos para usos futuros.

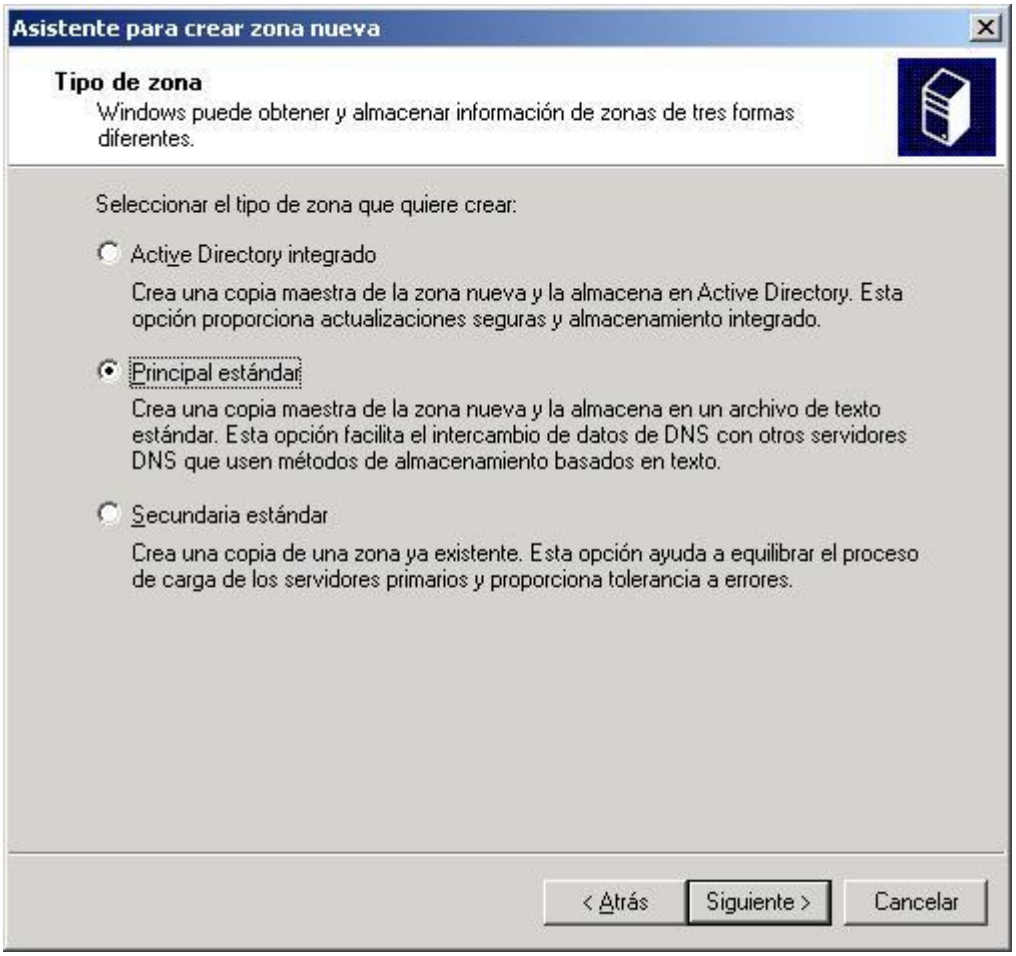


4. A continuación debemos hacer clic sobre el **Zonas de búsqueda inversa** y hacer clic con el botón derecho del mouse para activar el submenú y escogemos la opción de **Crear nueva zona**.

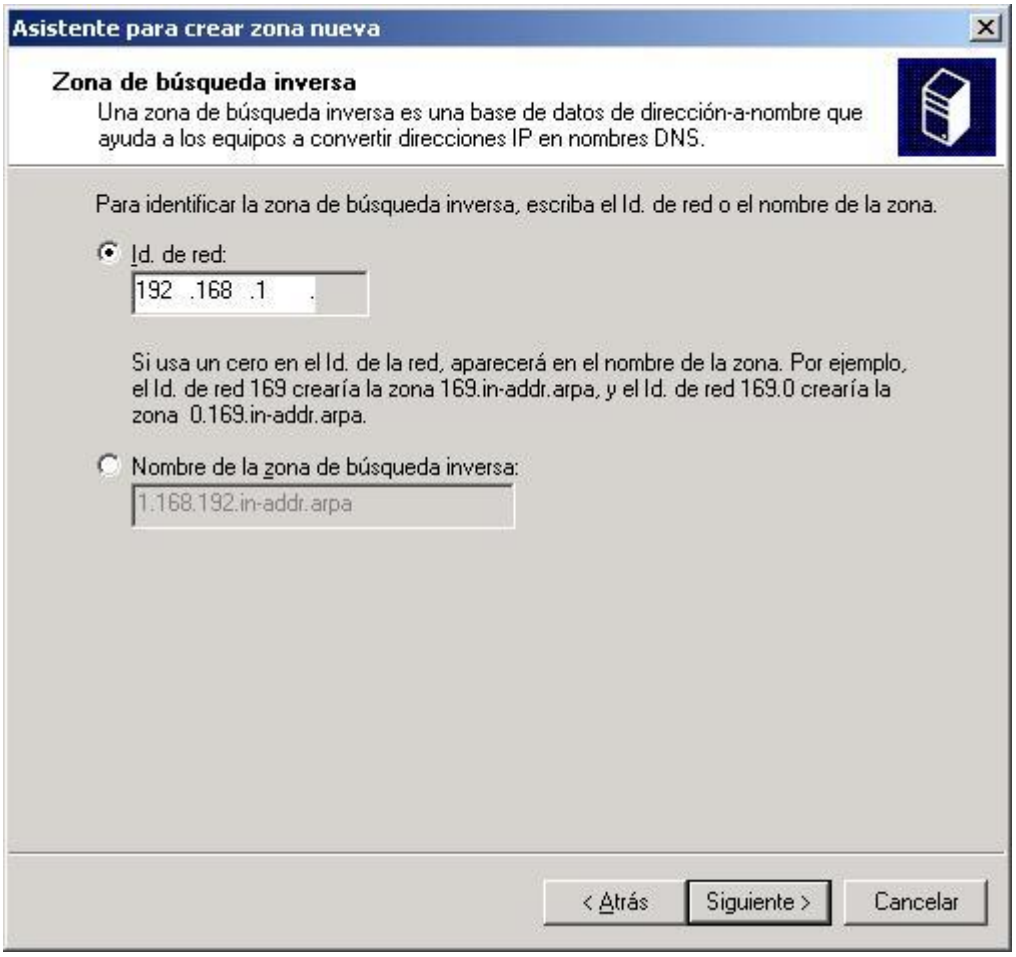
5. Se activa el Asistente para crear zona nueva, ventana en la cual debemos pulsar sobre el botón **Siguiente**, para iniciar el asistente.



6. En la siguiente ventana seleccionamos el tipo de zona con la opción **Principal Estándar** y pulsamos sobre el botón **Siguiente**.



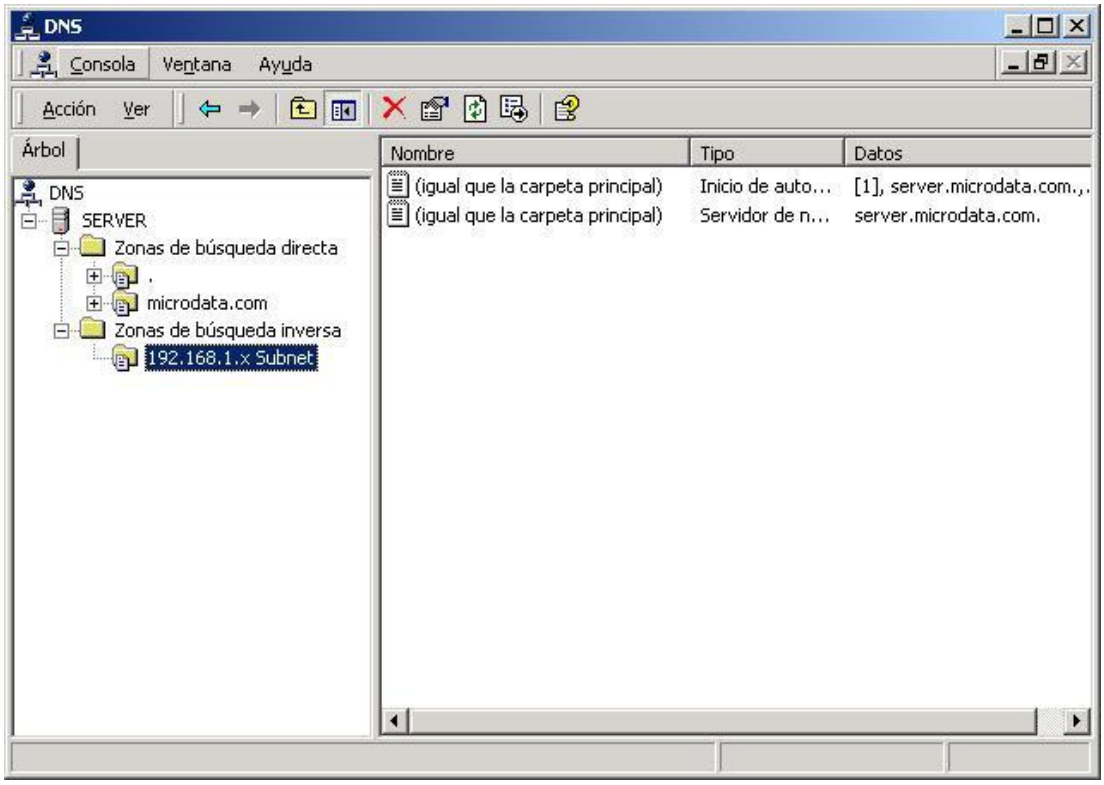
7. Ahora debemos ingresar el identificador de la red, únicamente los tres primeros bytes, en nuestro caso es 192.168.1, debido a que el identificador de la red es 162.198.1.1, dirección asignada a la tarjeta de red y al servidor. En este caso el nombre completo del equipo es server.microdata.com que corresponde a la dirección IP de la red. Una vez ingresado el identificador de Red debemos pulsar sobre el botón **Siguiente**.



8. En esta ventana anotamos el nombre del archivo en el que se creara la zona, como se anoto anteriormente es recomendable utilizar los datos que el propio Windows 2000 Server sugiere. Pulsamos sobre el botón **Siguiente**.

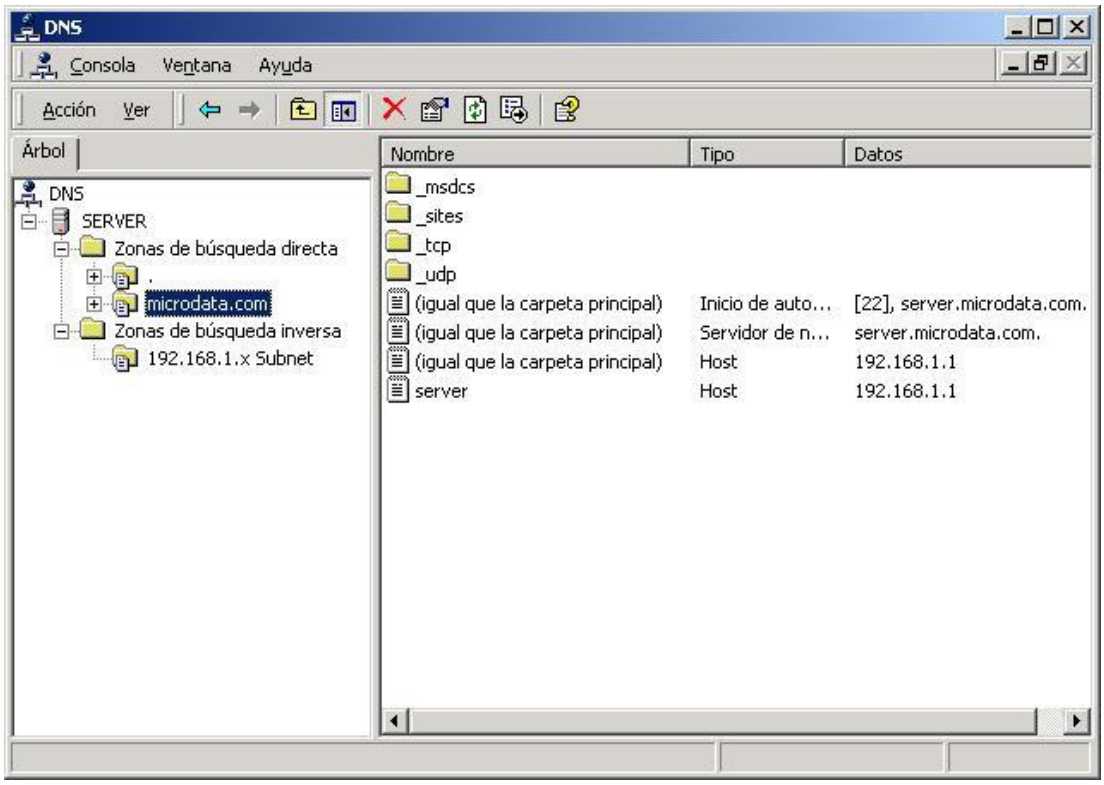
9. Una vez creada la zona, pulsemos sobre el botón de **Finalizar**. Recuerde que la zona de búsqueda inversa es para traducir una dirección IP en un nombre de dominio.

10. Abrimos la nueva zona creada como se observa en la siguiente venta, nos posesionamos sobre la nueva zona creada y hacemos clic con el botón derecho del mouse para obtener el submenú y escogemos la opción de **Nuevo Apuntador**, para crear un apuntador al servidor VPN que en este caso tiene la dirección 192.168.1.1

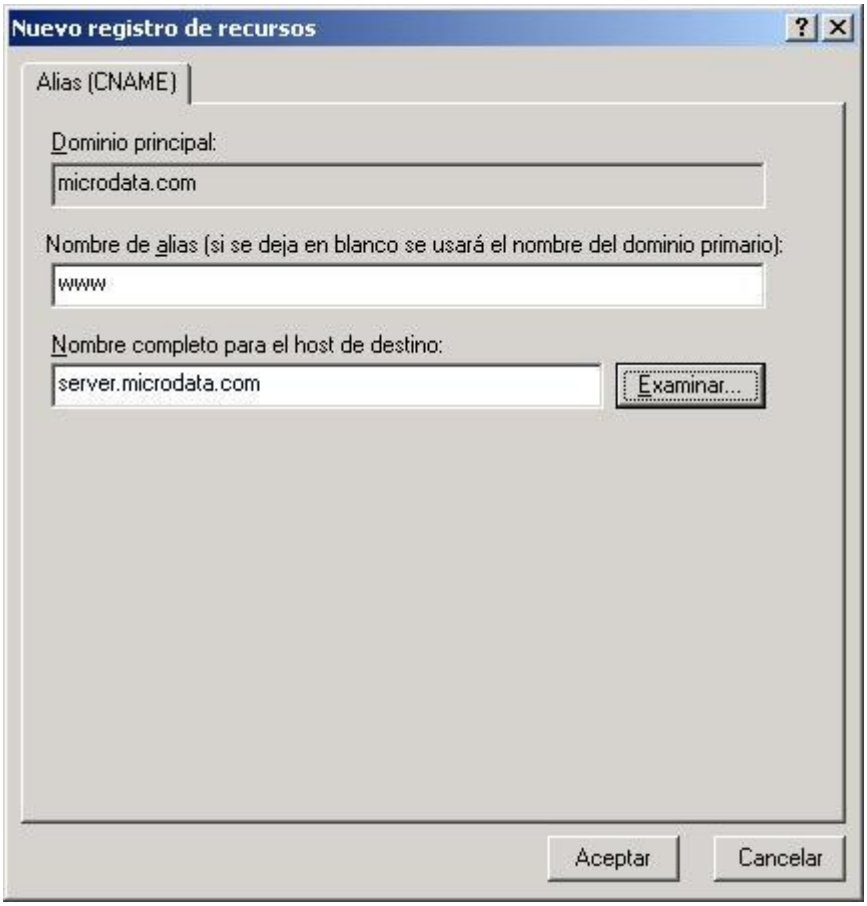


11. Como podemos observar en el recuadro **Número IP del Host** únicamente podemos escribir el último byte de la dirección IP del servidor, es por eso que los otros tres bytes, ingresados anteriormente deben ser correctos. Y en el segundo recuadro de **Nombre de host**, se debe ingresar el nombre del servidor que podemos escribirlo manualmente si lo tenemos claramente o podemos escogerlo con el botón **Examinar**. Una vez ingresado estos datos pulsamos sobre el botón de **Aceptar**.

12. Crearemos un alias para nuestro servidor VPN, el cual debemos crearlo de la siguiente manera. Abrimos la zona de **microdata.com**, haciendo clic con el botón derecho del mouse y pulsando sobre la opción de **Alias Nuevo**.



13. Sobre el cuadro **Nombre de Alias** ponemos el nombre que servirá de alias para nuestro servidor, como podemos observar le hemos puesto el nombre de www, y debemos escoger el Host al que hace referencia el alias. Ahora podemos decir que hacer referencia a www.microdata.com, es lo mismo que hacer referencia a server.microdata.com.

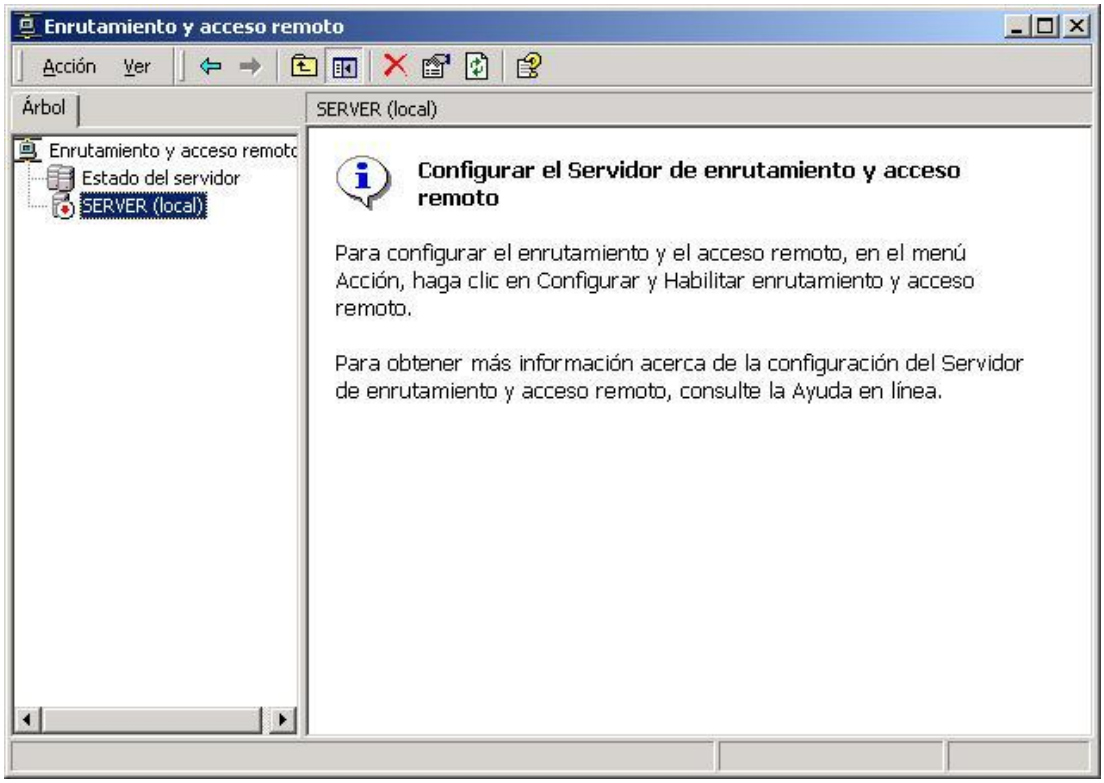


Instalar y Configurar Enrutamiento y Acceso Remoto

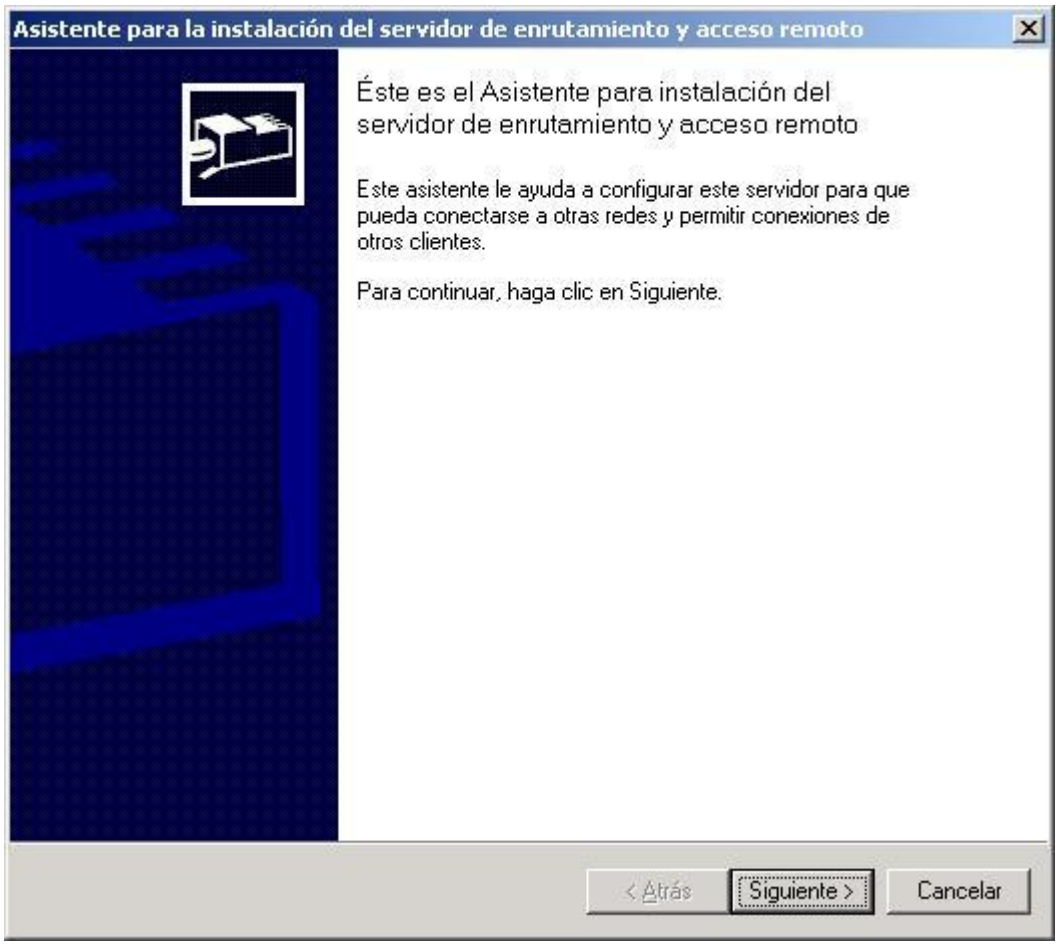
La instalación y configuración de Enrutamiento y Acceso Remoto es una de las partes principales de la configuración del Servidor VPN. Ya que aquí es donde configuraremos los protocolos de túnel para las conexiones VPN. Iniciamos ahora la Configuración del Enrutamiento y Acceso Remoto.

1. Inicialmente cargamos el programa de configuración del Enrutamiento y Acceso Remoto desde la siguiente ruta: **Inicio/Programas/Herramientas Administrativas/Enrutamiento y Acceso Remoto**

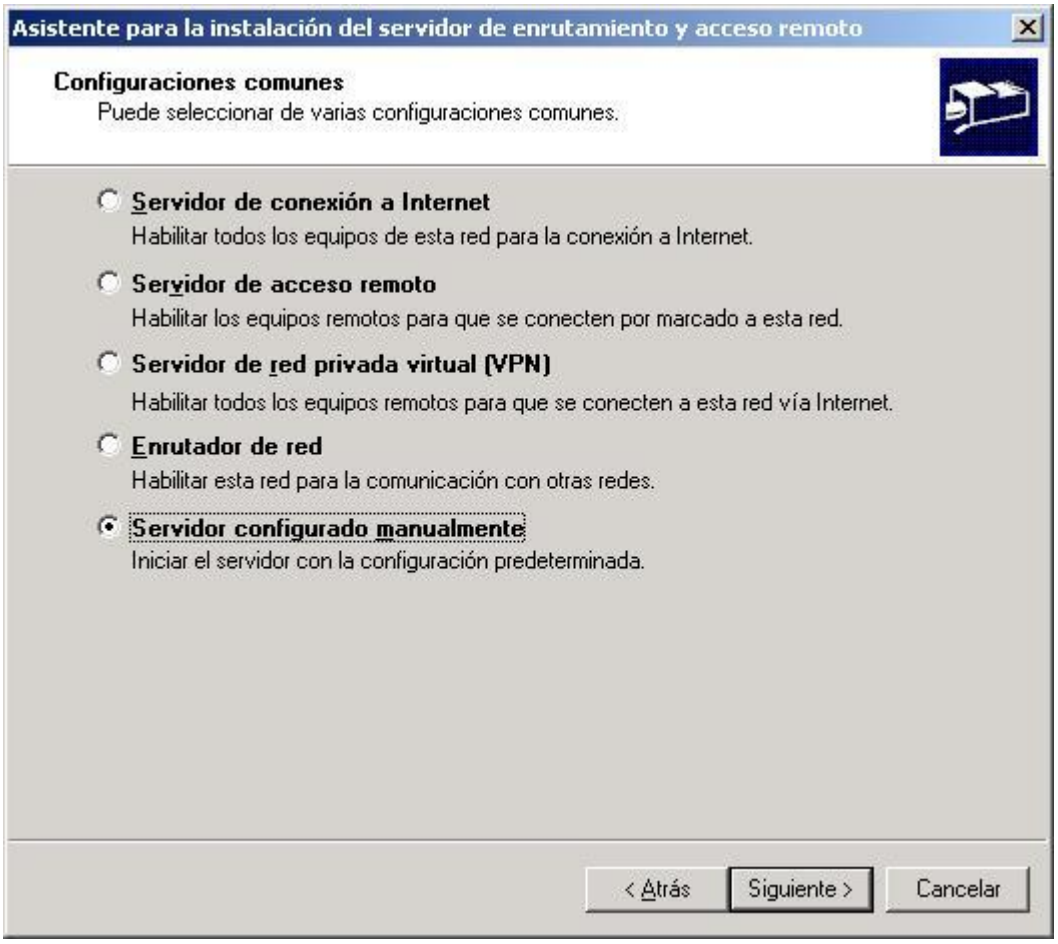
2. Pulsamos sobre el nombre de nuestro servidor (**SERVER**), y haciendo clic con el botón derecho del mouse escogemos la opción **Configurar y habilitar el Enrutamiento y Acceso Remoto**.



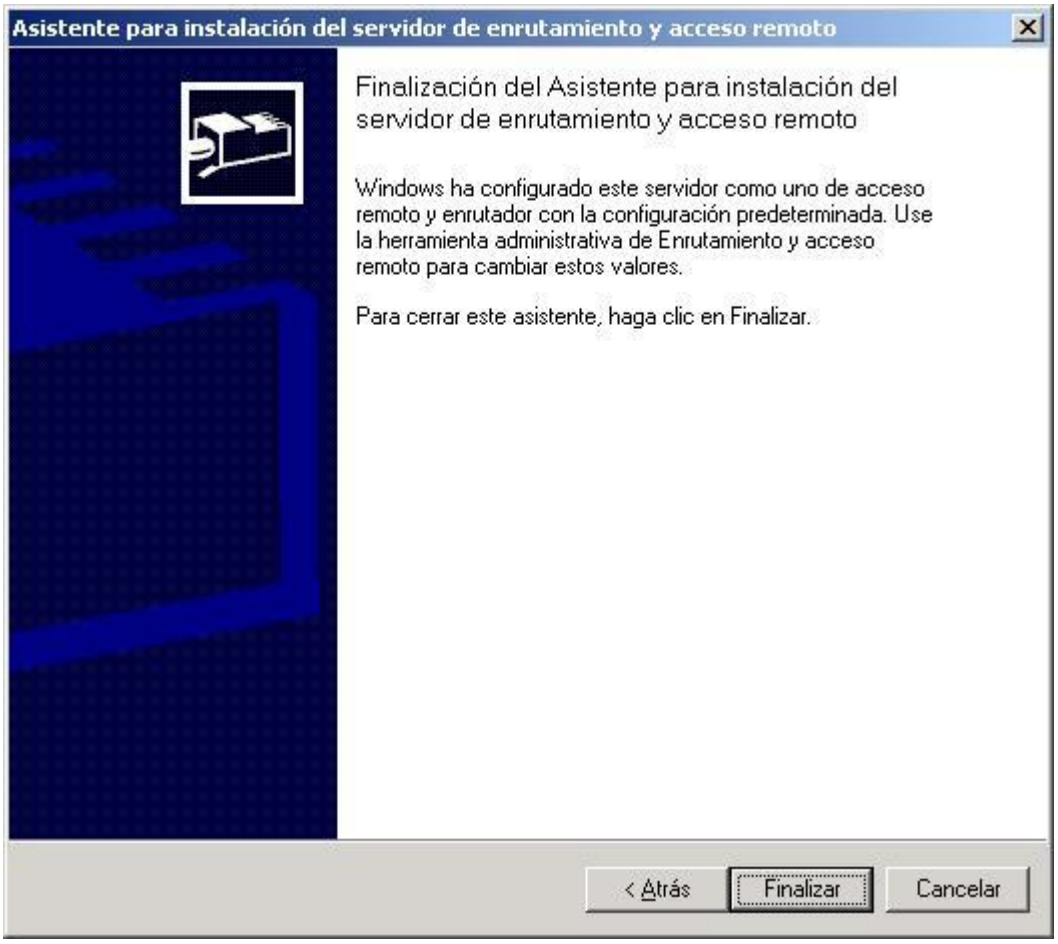
3. Así se inicia el Asistente para la instalación del servidor de enrutamiento y acceso remoto. Pulse sobre **Siguiente**.



4. En la siguiente ventana escogemos la opción **Servidor configurado manualmente**, no optamos por la opción de Servidor de red privada virtual (VPN), debido a que existe algún error en su configuración propio del Windows 2000, que se espera ser corregido mediante algún Service Pack. Ahora pulsamos sobre **Siguiente**.



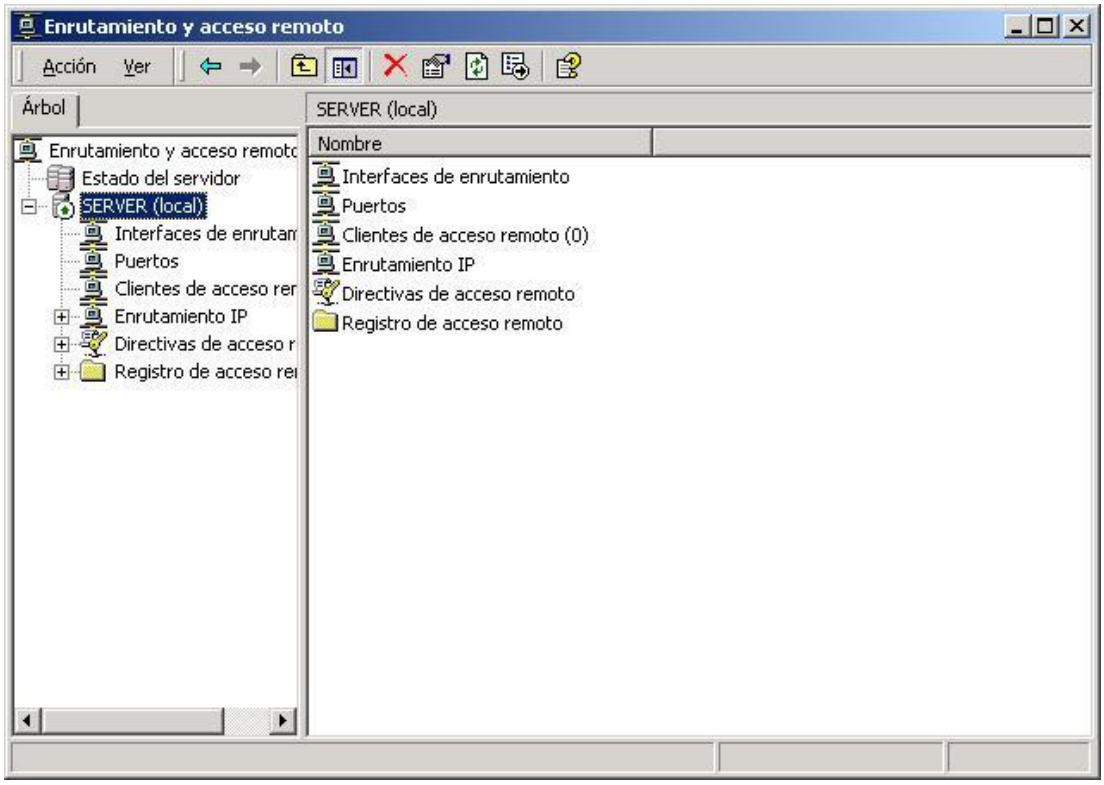
5. Pulsamos sobre **Finalizar** para terminar la instalación de enrutamiento y acceso remoto y proceder a su inicialización y configuración.



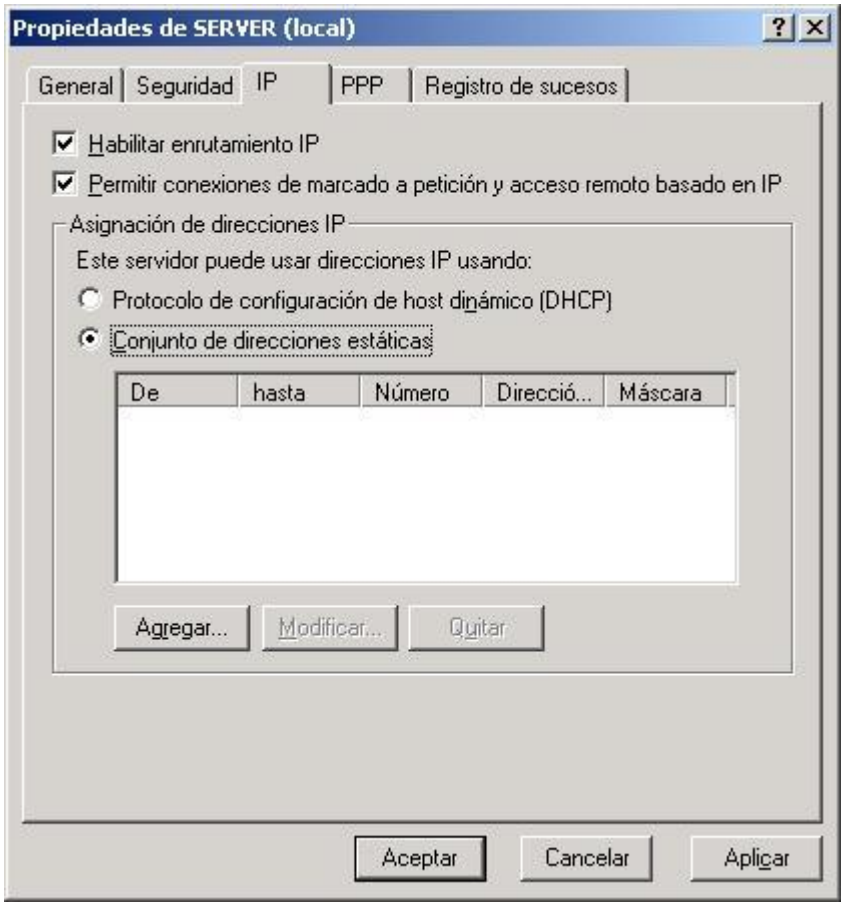
6. Procedemos ha iniciar el enrutamiento y acceso remoto, pulsando en la siguiente ventana el botón **Sí**.

7. El momento que obtengamos la siguiente ventana debemos esperar hasta que se inicie el servicio de Enrutamiento y acceso remoto.

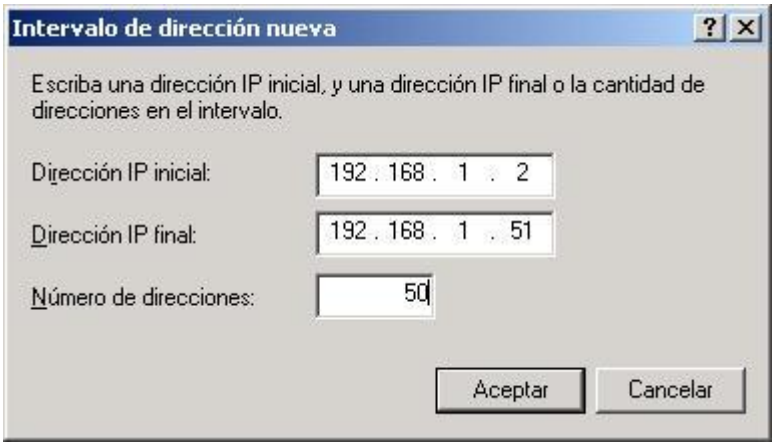
8. Una vez que se ha iniciado el servicio, es necesario que pulsemos sobre el nombre de nuestro servidor local y hagamos clic con el botón derecho del mouse para activar el submenú y escojamos la opción de **Propiedades**.



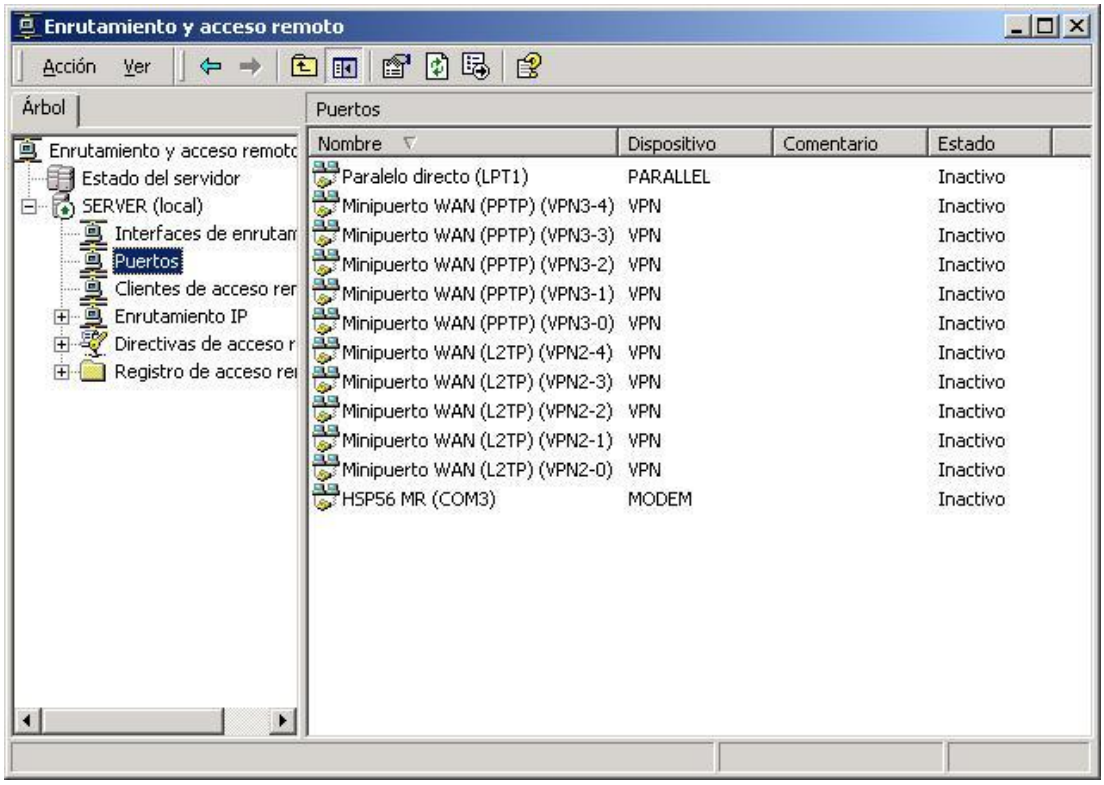
9. Escogemos la pestaña correspondiente a **IP** y activamos la opción de **Conjunto de direcciones estáticas**, y luego pulsamos sobre el botón **Agregar**.



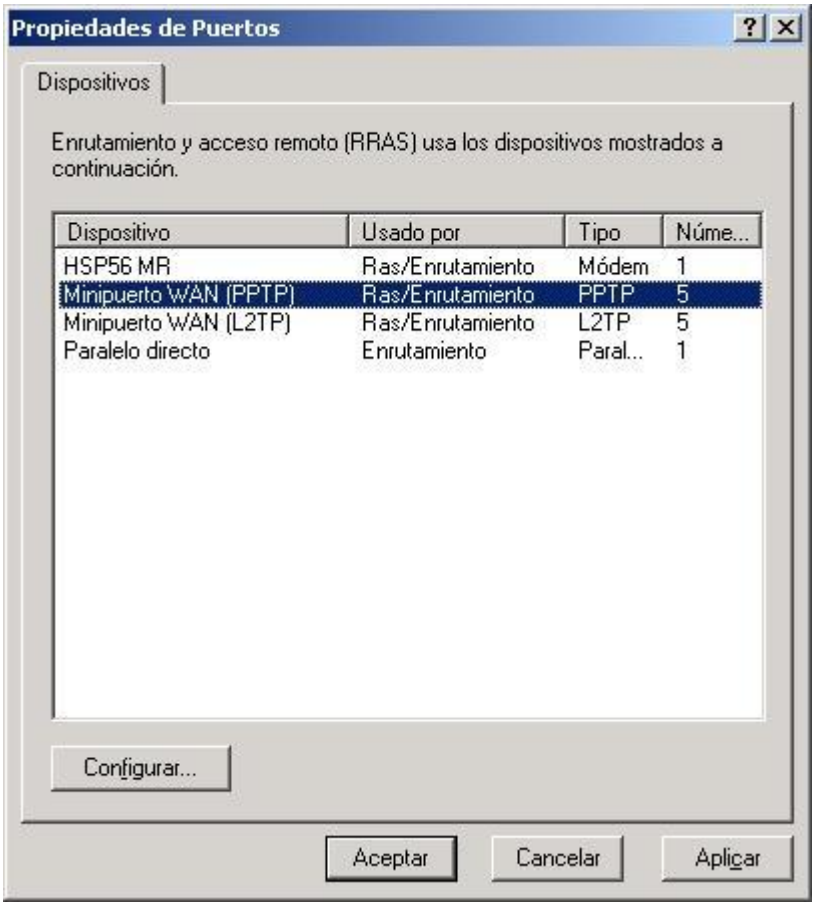
10. En esta ventana escribiremos un rango de direcciones IP, entre el cual estarán las direcciones IP de todas las conexiones que ingresen a esta máquina. Luego pulse sobre el botón **Aceptar**. Note usted que se puede ingresar únicamente la Dirección IP inicial y luego el Número de direcciones, y la Dirección IP final se calcula automáticamente.



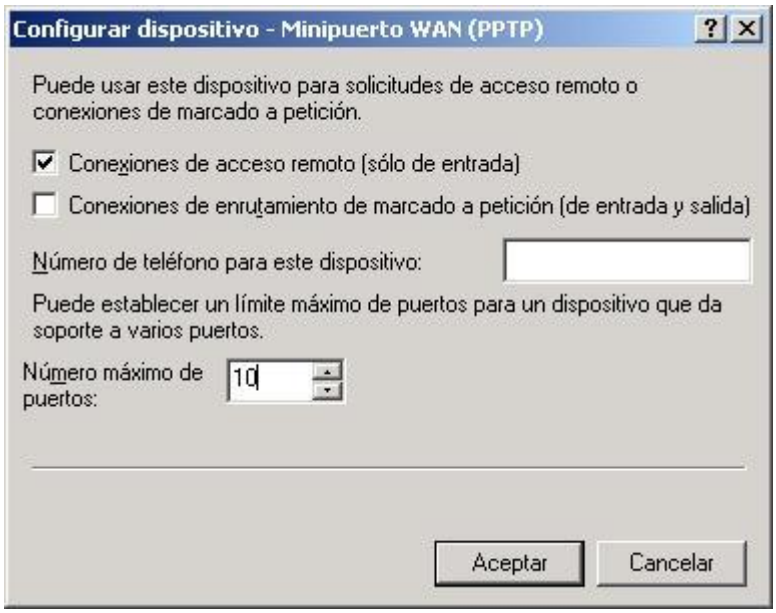
11. Ahora vamos a configurar los Puertos, pulsamos sobre **Puertos** y con el botón derecho del mouse hacemos clic para desplegar el submenú y escogemos la opción de **Propiedades**.



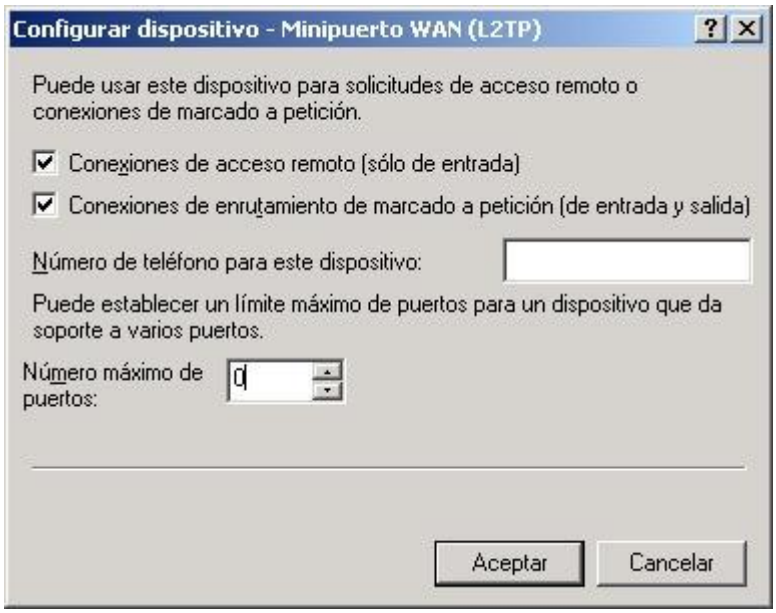
12. En la ventana de Propiedades de Puertos seleccionamos en **Minipuerto WAN(PPTP)** y hacemos clic en **Configurar**. Aquí configuraremos las opciones para las conexiones a través del protocolo PPTP.



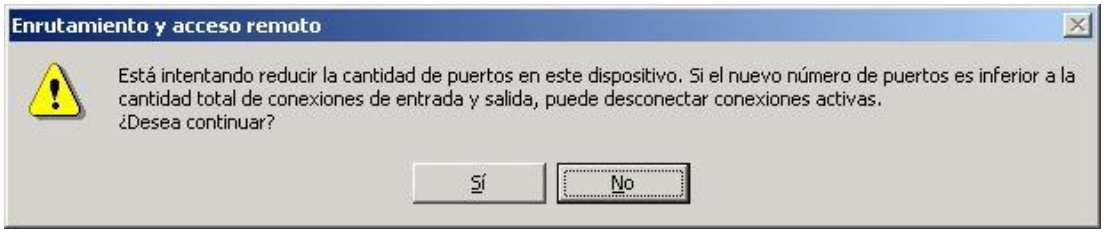
13. En esta ventana desactivamos la opción de **Conexiones de enrutamiento de marcado a petición (de entrada y salida)**, ya que este tipo de conexiones nosotros no las utilizaremos. Además en Número máximo de puertos debemos ingresar el número máximo de conexiones VPN que se pueden recibir al mismo tiempo en el servidor VPN. Para fines demostrativos hemos tomado la cantidad de 10 conexiones, puede ser menos como pueden ser más. Ahora pulsamos sobre el botón **Aceptar**.



14. Utilizaremos el mismo procedimiento para la configuración del **Minipuerto WAN(L2TP)**, pero en este caso vamos a desactivar las conexiones de L2TP, haciendo que el **Número máximo de puertos** sea igual a 0(cero), debido a que no tendremos conexiones de VPN con este tipo de protocolo, pero en caso de existir debemos poner el número máximo de conexiones que tendremos al mismo tiempo con el protocolo L2TP. Y luego pulsamos sobre el botón **Aceptar**.

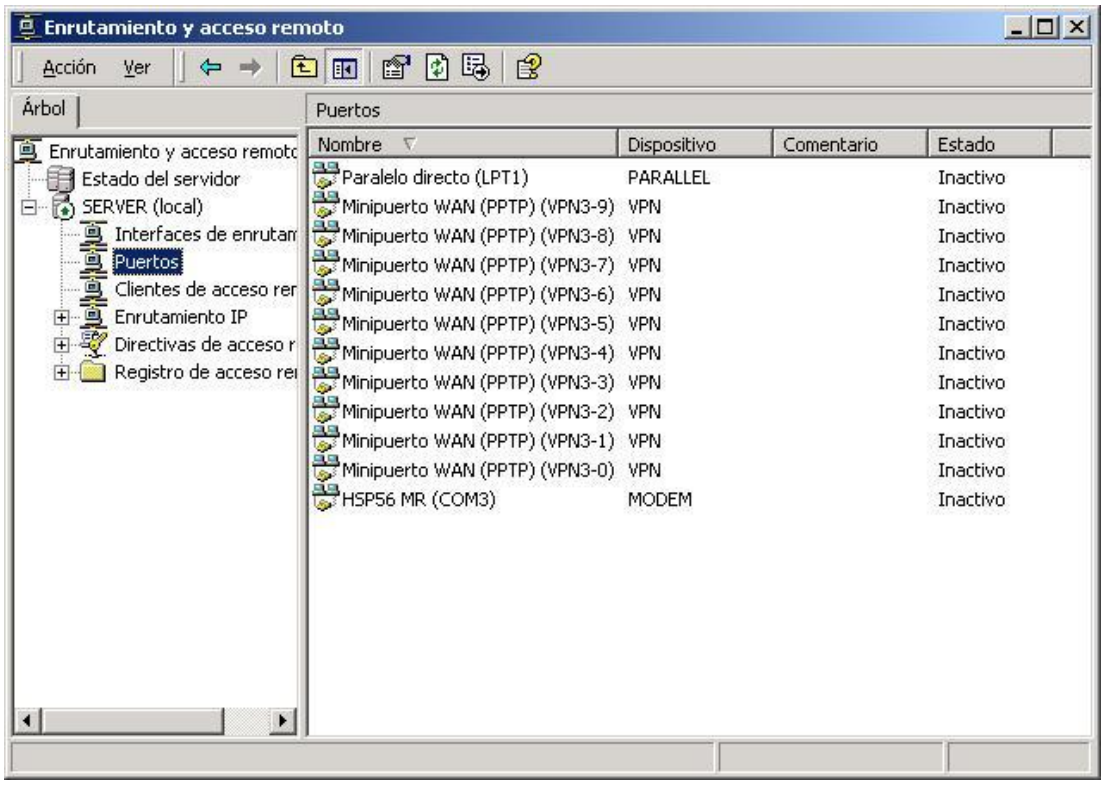


15. Si ponemos en cero el número máximo de conexiones o puertos tendremos el siguiente mensaje de información y debemos pulsar en el botón **Sí**.



16. Una vez que regresamos a la venta de Propiedades de Puertos debemos pulsar sobre el botón **Aceptar**.

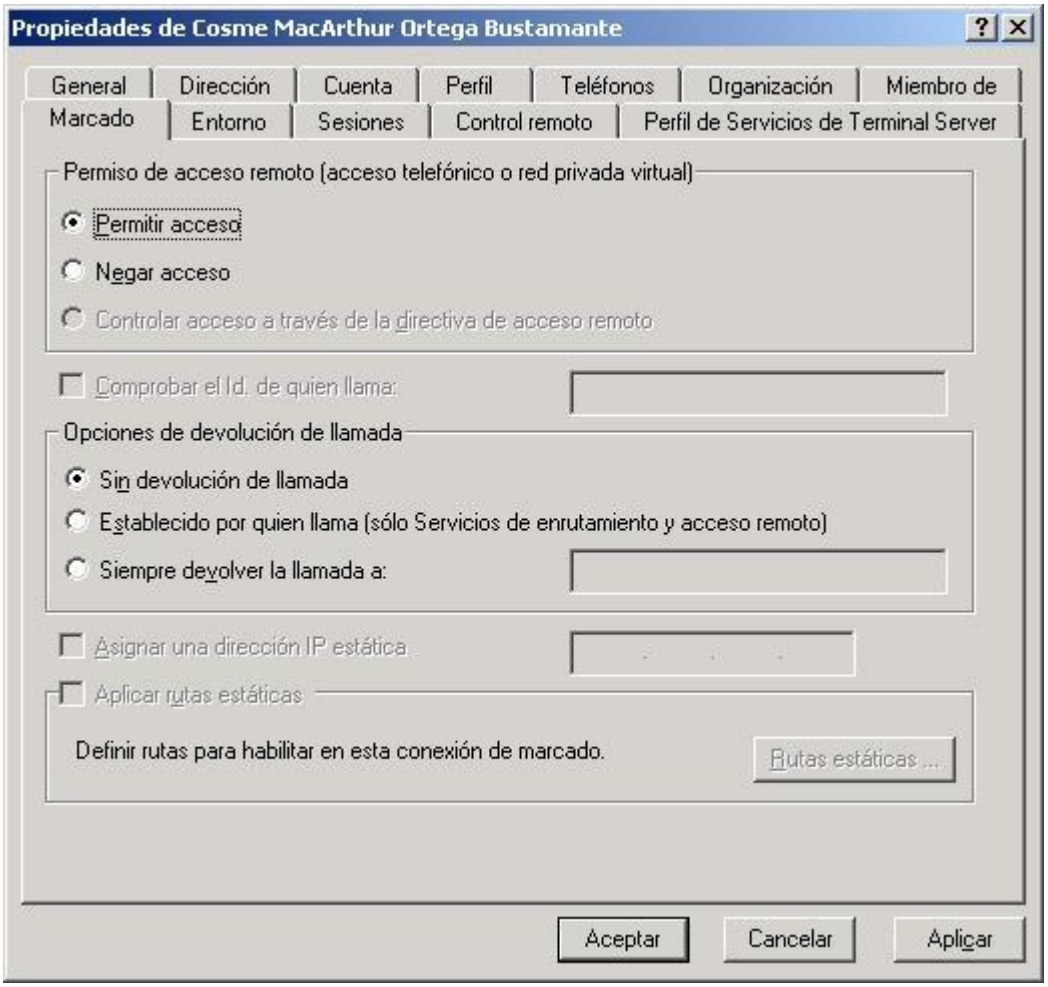
17. Como podemos observar en la siguiente ventana se obtendrá la nueva configuración de puertos que hemos realizado. Para finalizar podemos cerrar la ventana de Enrutamiento y Acceso remoto. Hemos terminado de configurar en su totalidad el Servidor VPN en Windows 2000, quedando pendiente un pequeñísimo paso que se debe tomar en cuenta en la creación y configuración de nuevos usuarios, datos que veremos a continuación.



Instalar y configurar Usuarios.

La creación y configuración de usuarios debe ser normalmente y de acuerdo a los requerimientos de los mismos como del administrador del sistema. Pero para permitir al nuevo usuario que tenga acceso al Servidor a través de una conexión VPN debemos considerar lo que detallamos a continuación.

1. Primeramente debemos activar las propiedades del usuario que deseamos configurar, en la pestaña de **Marcado** debemos seleccionar la opción de Permitir acceso, dentro del grupo de **Permiso de acceso remoto (acceso telefónico o red privada virtual)**. Esta opción permitirá al usuario que su petición de conexión sea permitida caso contrario no se podrá conectar aunque su Servidor y Cliente VPN estén configurados correctamente.

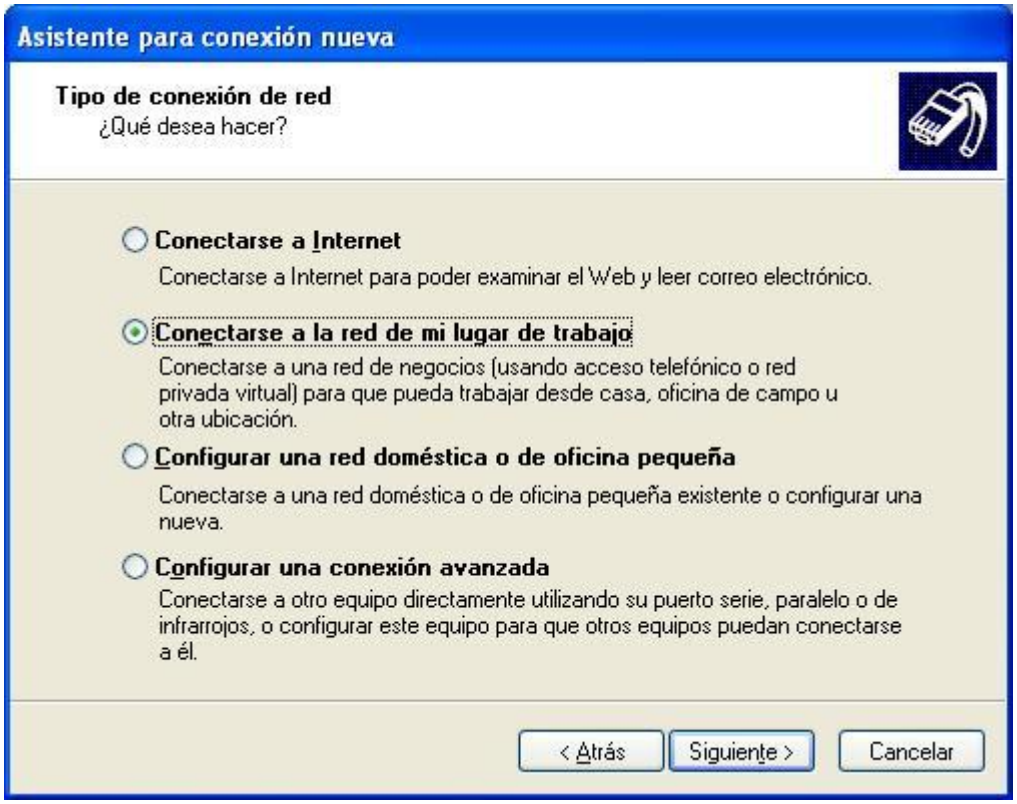


Instalación y configuración del Cliente VPN con Windows XP Profesional.

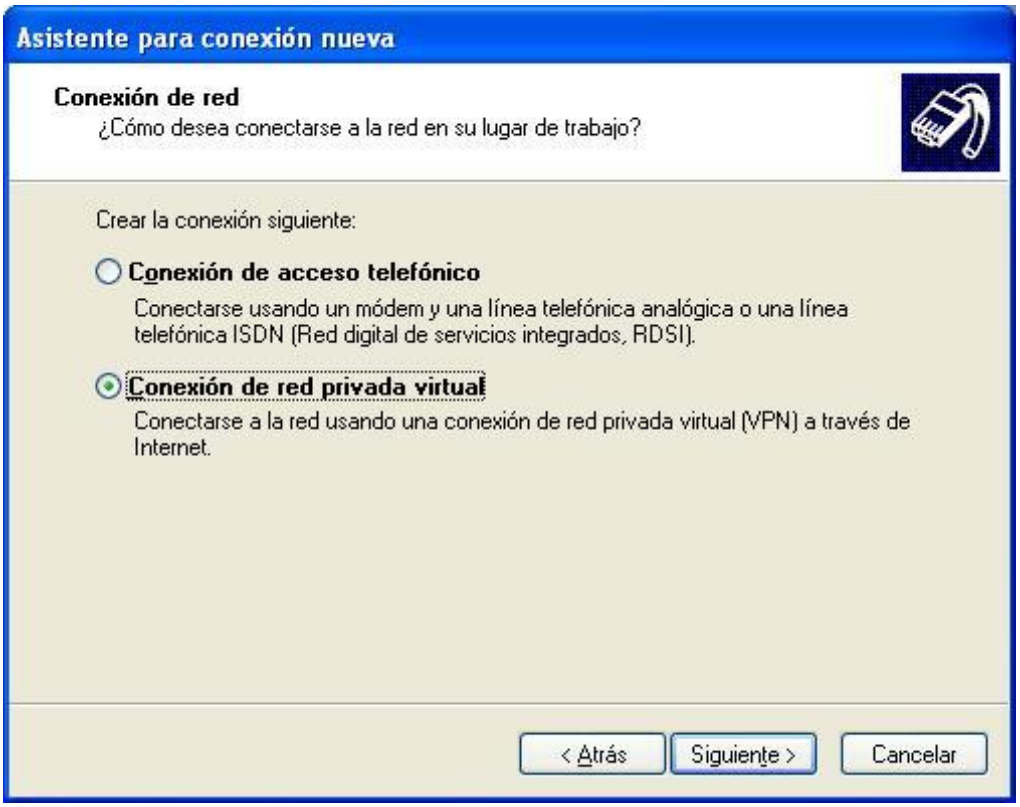
La configuración del Cliente VPN es más sencilla que la del Servidor VPN, pero igualmente debemos prestar mucha atención en los detalles para obtener una óptima configuración.

1. Debemos iniciar el Asistente para una conexión nueva, el cual nos ayudará en la configuración del cliente VPN. Seguidamente debemos pulsar el botón **Siguiente**.

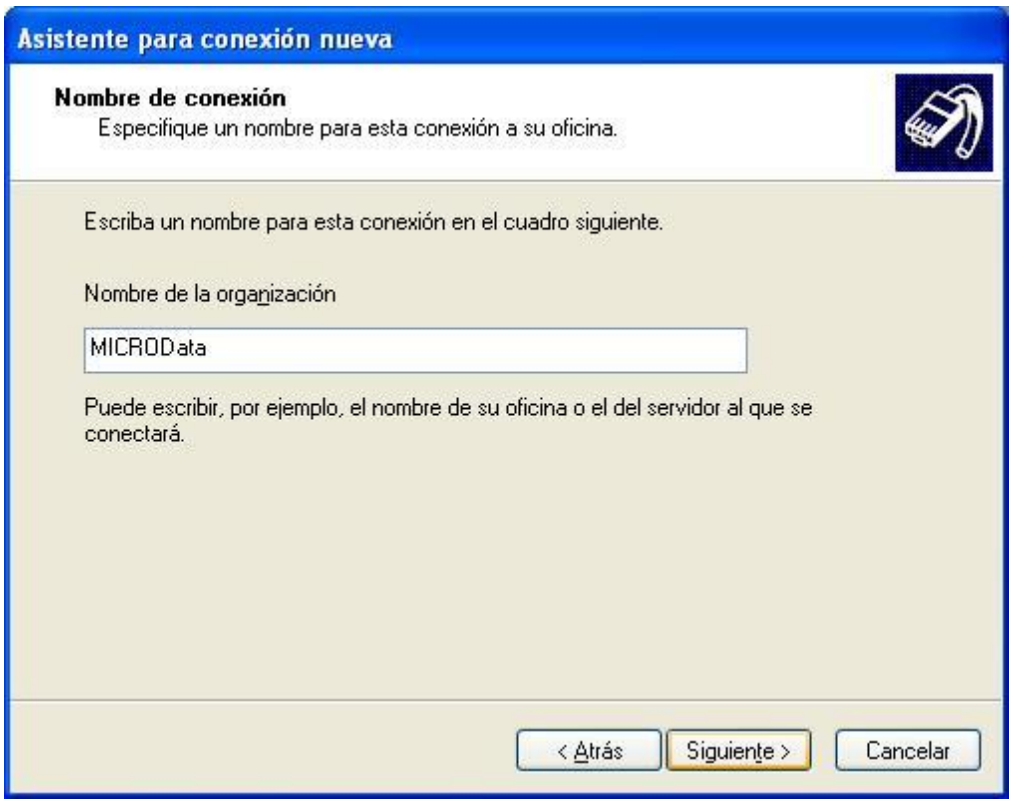
2. En la próxima ventana escogemos la opción de **Conectarse a la red de mi lugar de trabajo**, opción que es la que permite establecer a una conexión VPN. Y luego pulsamos sobre el botón **Siguiente**.



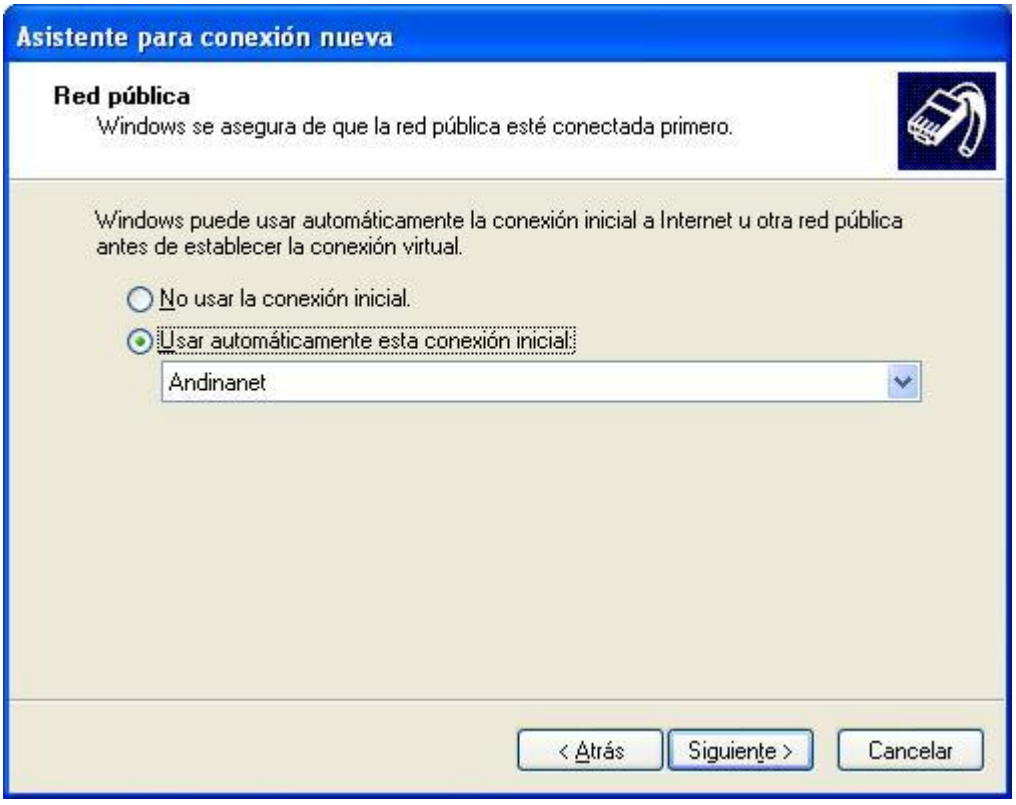
3. A continuación como es lógico seleccionamos la opción **Conexión de red privada virtual,** seguido del botón **Siguiente**.



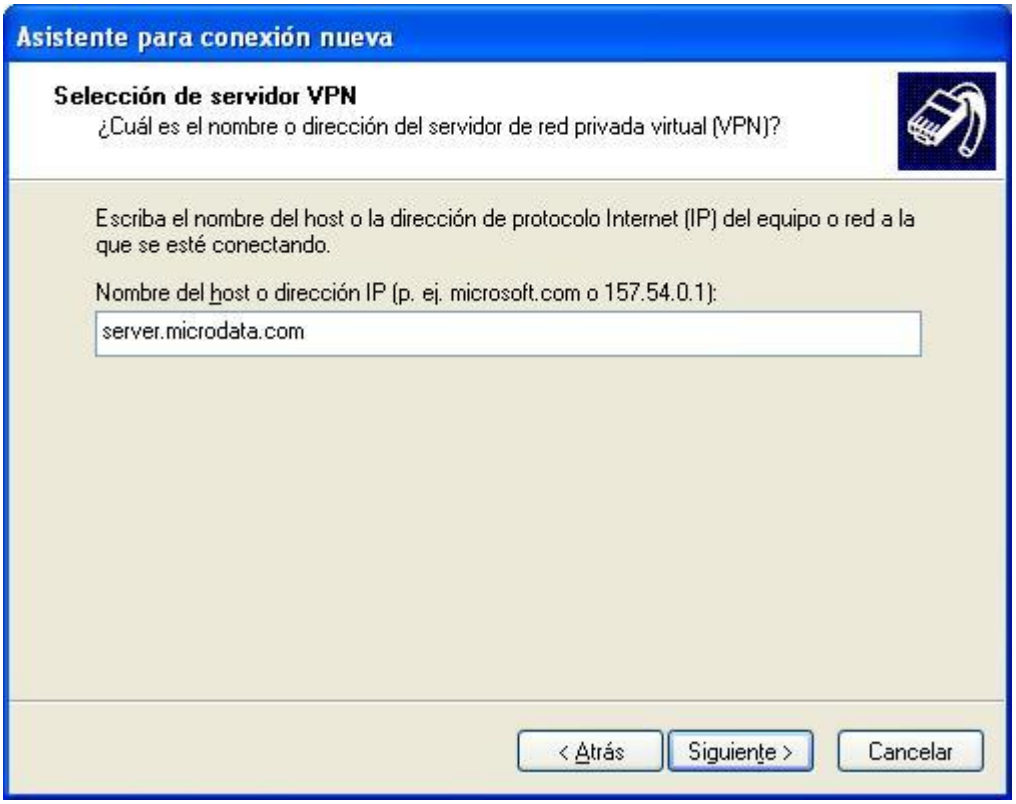
4. En la siguiente ventana ingresamos el **Nombre de la organización** a la que nos vamos a conectar, este nombre también es el nombre que tendrá la conexión. Y luego el botón de **Siguiente**.



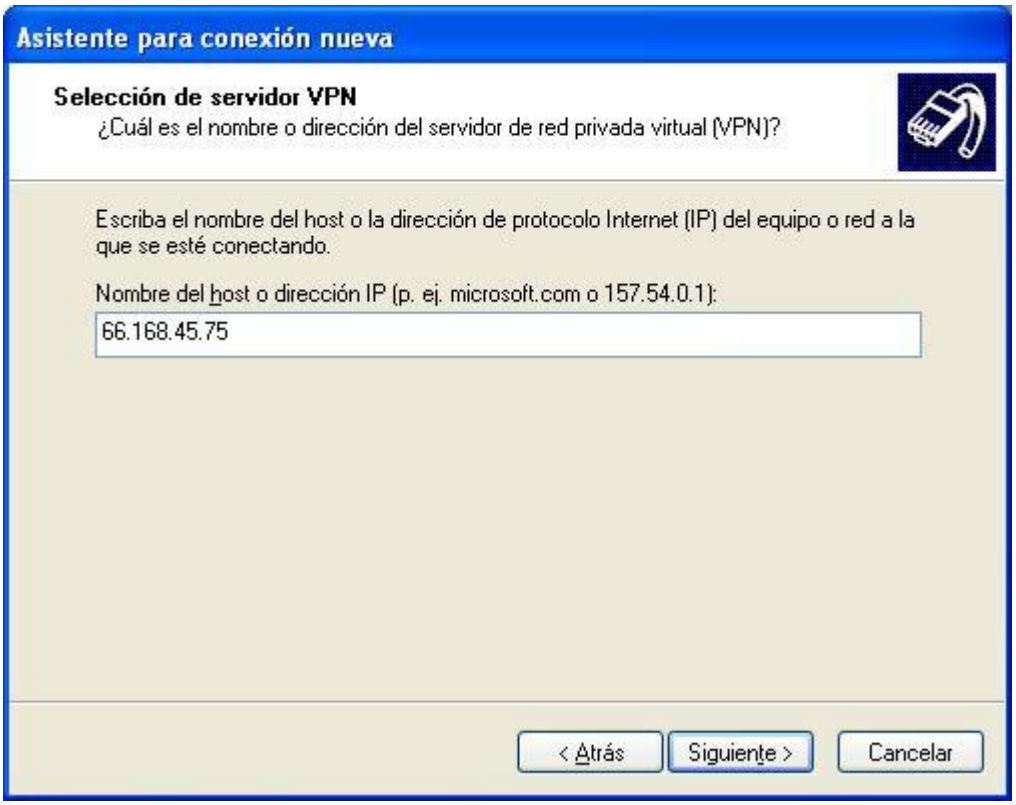
5. Al realizar la configuración de una conexión VPN, esta se asegura de que primeramente el equipo este conectado a Internet para lo cual escogemos la opción de **Usar automáticamente esta conexión inicial**, y escogemos una conexión a Internet disponible que en nuestro caso se denomina Andinanet, y luego pulsamos sobre el botón de **Siguiente**.



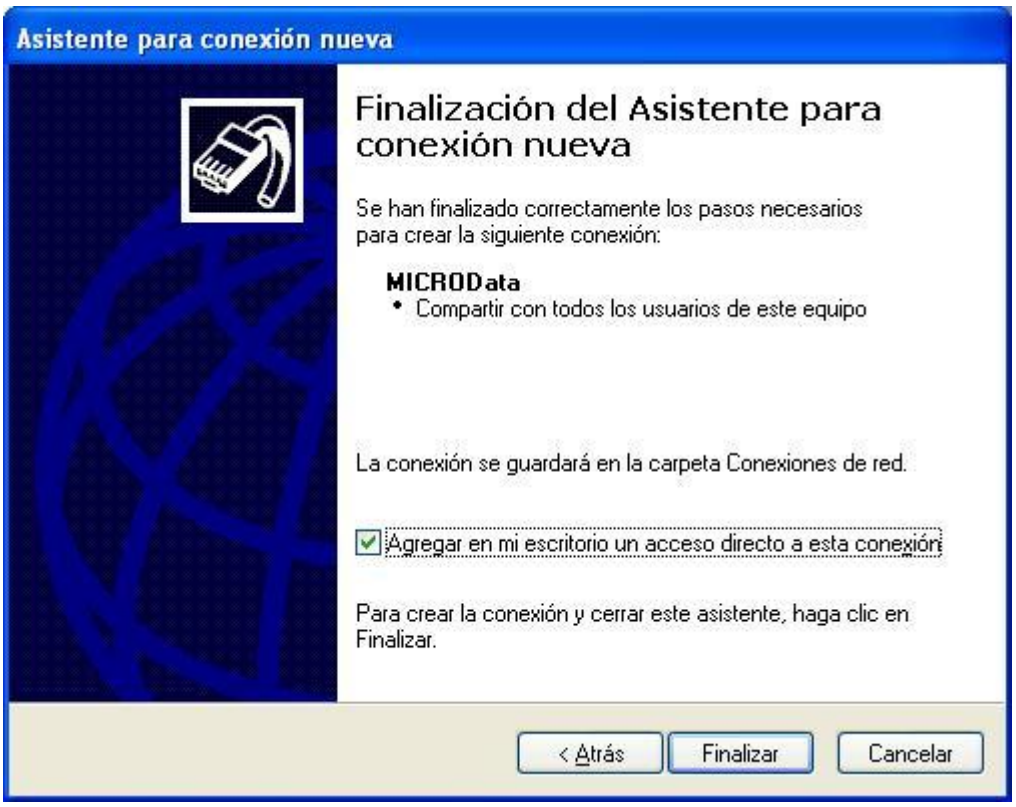
6. En la siguiente ventana en el recuadro de **Nombre de host o dirección IP** escribimos el nombre del servidor VPN al que nos vamos a conectar en este caso es server.microdata.com. Esto para cuando se tiene un Servidor VPN con una dirección estática.



7. En el caso de no poseer una IP fija para cada vez que el Servidor VPN se conecta a Internet, se debe buscar la manera de que el Cliente VPN obtenga la dirección del Servidor VPN que el ISP le asigno, este dato puede ser enviado por el Servidor VPN a todos sus Clientes VPN a través de correo electrónico o cualquier programa de mensajería instantánea. En este caso se anotará en el cuadro de **Nombre del host o dirección IP**, la dirección IP que se le asigno al Servidor VPN en Internet.



8. En la siguiente ventana marcamos la opción de **Agregar en mi escritorio un acceso directo a esta conexión** y luego pulsamos con el botón de **Finalizar**.



9. Ahora podemos ya establecer una conexión VPN pulsando sobre el icono de acceso directo a la conexión que se encuentra en el escritorio. Cuando lo haga por primera vez será necesario que ingrese en el cuadro **Nombre de usuario el nombre de usuario** que usted posee para acceder al servidor y en **Contraseña** su respectiva clave de usuario. Se le recomienda utilizar la opción de **Guardar este nombre de usuario y contraseña**, con la finalidad de no estar ingresando estos datos en cada conexión que usted desee efectuar. Y pulsamos con el mouse sobre el botón de **Conectar**.

10. Esta ventana se obtendrá el momento de que se este efectuando la conexión, nunca olvide de que el Servidor VPN debe estar ya conectado a la red pública (Internet) para poder efectuar la conexión.

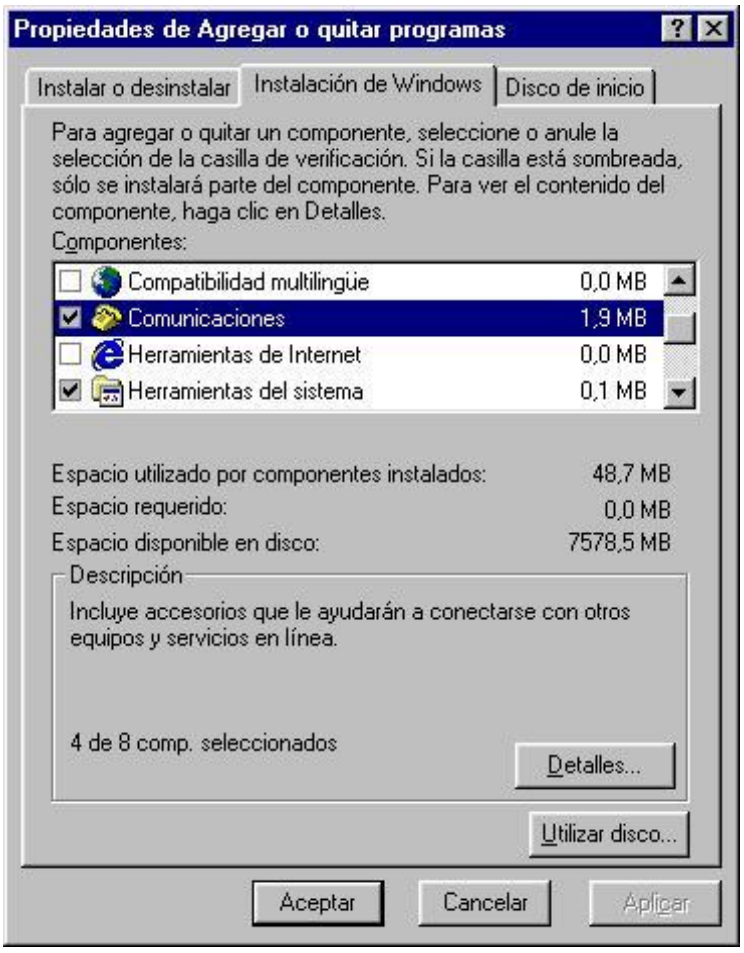
11. Si no existe ningún error, se realizará la conexión y se empezará la autenticación en el Servidor VPN por parte del cliente, como se puede observar en la siguiente ventana.

Instalación y Configuración del Cliente VPN con Windows 98se.

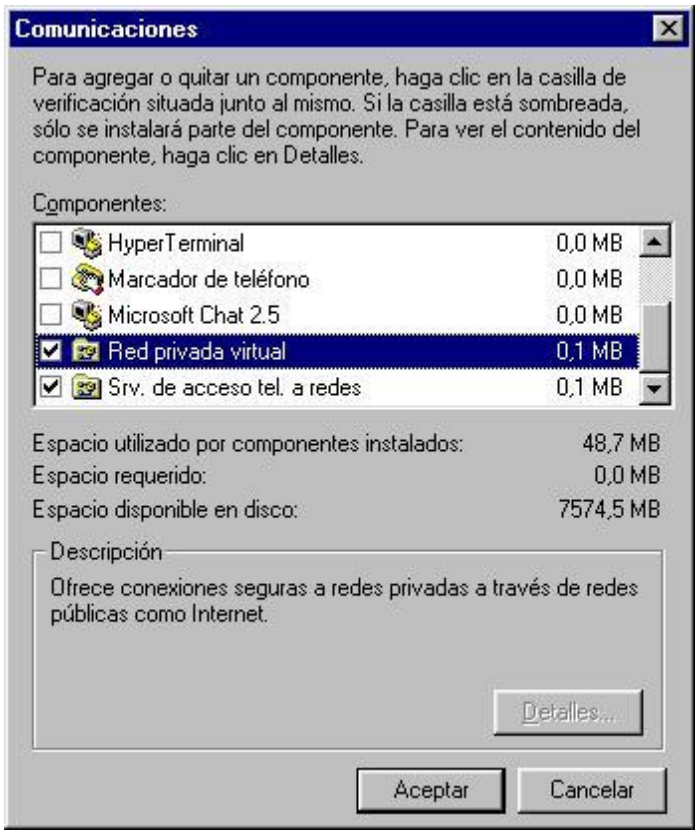
La instalación del cliente en Windows 98 segunda edición se procede de la siguiente manera:

1. Iniciamos el servicio de Agregar o Quitar Programas, que lo encontramos en la siguiente ruta: **Inicio/Configuración/panel de Control/Agregar o quitar programas**.

2. Activamos la opción de **Comunicaciones** y pulsamos sobre el Botón **Detalle**.



3. En la ventana de Comunicaciones debemos seleccionar el servicio de **Red privada virtual** y la opción **Srv. de acceso telefónico a redes**. El servicio de Red privada virtual es el servicio que nos permitirá crear las conexiones VPN. Seguidamente pulsamos sobre el botón **Aceptar**.



4. Es todo lo que debemos configurar en el Panel de control por consiguiente al volver a la plantilla de Propiedades de Agregar o quitar programas pulsamos sobre el botón de Aceptar e inmediatamente se instalará el Servicio de Red Privada Virtual, para lo cual debe asegurarse de poseer el disco original de Windows 98se que el sistema se lo solicitará, para la correcta instalación.

5. Agregamos una nueva conexión de la forma que siempre se la ha realizado, al igual que en la configuración que Windows XP, en el primer cuadro escribimos el nombre de la conexión, y en el menú de **Seleccione un dispositivo**, desplegándolo podemos observar que tenemos una opción adicional a la tarjeta de FaxModem que es **Microsoft VPN Adapter**, opción que nos permitirá hacer la conexión VPN, para lo cual la seleccionamos. Y seguidamente pulsamos sobre el botón **Siguiente**.

6. En la siguiente ventana en el cuadro de **Nombre del host o dirección IP**, debemos escribir el nombre del servidor al que estamos accesando siempre y cuando se tenga una dirección IP estática y conste el nombre en un DNS, de no ser así debemos ingresar la dirección IP con la que el Servidor VPN se encuentra en Internet en este momento. Esta situación es similar a la configuración que se realizo en el Cliente VPN con Windows XP. Profesional.

7. Listo, ha quedado configurado el Cliente VPN con Windows 98se, para concluir con el asistente debemos pulsar sobre el botón **Finalizar**.

8. En el momento de iniciar la conexión VPN, se le presentará la siguiente ventana, en donde se debe ingresar el Nombre de usuario y contraseña que se autentificarán en el Servidor VPN.

Referencias Bibliográficas

Referencias WWW.

[WWW01]

http://www4.uji.es/~al019803/ip — Informática y Sociedad. Protocolos TCP/IP. Juan Salvador Miravet Bonet

[WWW02]

http://www.microsoft.com/articles/tcpip.htm — Instalación, introducción al TCP/IP en Windows NT. Microsoft. 2001

[WWW03]

http://www.ciberhabitat.gob.mx — CiberHábit – Ciudad de la Informática

[WWW04]

http://www.microsoft.com/serviceproviders/vpn_ras/vpnoverview.asp

Windows 2000 Server – Virtual Private Networking: An Overview. Microsoft Corporation.

[WWW05]

http://www.microsoft.com/technet/vpnsolutions/index.htm

Virtual Private Networking – Microsoft Corporation 1999

[WWW06]

http://www.microsoft.com/windows2000/technologies/communications/vpn/l2f_vpn.html

Layer Two Forwarding – Microsoft Corporation 2001. White Paper

[WWW07]

www.iec.csic.es/criptonomicon/autenticacion

Autenticación y autorización en Internet. 2001

[WWW08]

http://rinconquevedo.iespana.es/rinconquevedo/Criptografia/autenticacion.htm

INTRODUCCIÓN A LA CRIPTOGRAFÍA. Aplicaciones criptográficas - Autenticación

[WWW09]

http://www.infoapuntes.com.ar/Apuntes/seguridad.htm

SEGURIDAD EN REDES COMPLEJAS: EL CASO DE INTERNET. 2002

[WWW10]

http://www.eff.org//Privacy/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html

RSA Code-Breaking Contest Again Won by Distributed.Net

and Electronic Frontier Foundation (EFF)

[WWW11]

http://webs.ono.com/usr026/Agika2/3internet/autentificacion.htm

Ataques de Autenticación. Enlaces de Seguridad. 10-09-02

Libros

[LIB01]

Feit Sidnie — TCP/IP. Arquitectura, protocolos e implementación, además de IPV6 y seguridad de IP. Editorial Osborne McGraw-Hill. 623 páginas. Primera edición año 1997.

[LIB02]

Steven Brown — Implementación de Redes Privadas Virtuales. Editorial McGraw-Hill Interamericana Editores, S.A. de C.V. 594 Páginas.

[LIB03]

Hernández Claudio — Hackers, los piratas del chip. Primera Edición. Libro digital. 2002.

Referencias RFC's

[RFC791]

IETF – RFC791 — Internet Protocol. J. Postel. Sep-01-1981. (Format: TXT=97779 bytes) (Obsoletes RFC0760) (Updated by RFC1349) (Also STD0005)(Status: STANDARD)

[RFC2460]

IETF – RFC2460 — Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998. (Format: TXT=85490 bytes) (Obsoletes RFC1883) (Status: DRAFT STANDARD)

[RFC792]

IETF – RFC792 — Internet Control Message Protocol. J. Postel. Sep-01-1981.(Format: TXT=30404 bytes) (Obsoletes RFC0777) (Also STD0005) (Status: STANDARD)

[RFC3228]

IETF – RFC3228 — IANA Considerations for IPv4 Internet Group Management Protocol IGMP). B. Fenner. February 2002. (Format: TXT=6473 bytes) (Also BCP0057) Status: BEST CURRENT PRACTICE)

[RFC768]

IETF – RFC768 — User Datagram Protocol. J. Postel. Aug-28-1980. (Format: TXT=5896 bytes) (Also STD0006) (Status: STANDARD)

[RFC793]

IETF – RFC793 — Transmission Control Protocol. J. Postel. Sep-01-1981. (Format: TXT=172710 bytes) (Updated by RFC3168) (Also STD0007) (Status: STANDARD)

[RFC2661]

IETF – RFC2661 — Layer Two Tunneling Protocol "L2TP". W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter. August 1999. (Format: TXT=168150 bytes) (Status: PROPOSED STANDARD)

[RFC1510]

IETF – RFC1510 — The Kerberos Network Authentication Service (V5). J. Kohl, C. Neuman. September 1993. (Format: TXT=275395 bytes) (Status: PROPOSED STANDARD)

[RFC2251]

IETF – RFC2251 — Lightweight Directory Access Protocol (v3). M. Wahl, T.

Howes, S. Kille. December 1997. (Format: TXT=114488 bytes) (Status: PROPOSED STANDARD)

[RFC3232]

IETF – RFC3232

Assigned Numbers: RFC 1700 is Replaced by an On-line Database. J. Reynolds, Ed.. January 2002. (Format: TXT=3849 bytes) (Obsoletes RFC1700) (Status: INFORMATIONAL)