DISEÑO Y CONSTRUCCIÓN DE UNA RED PRIVADA VIRTUAL (VPN) PARA LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

ANGÉLICA PATRICIA MENDOZA GONZÁLEZ

NIKKA MASSIEL MONTOYA RODRÍGUEZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

INGENIERÍA DE SISTEMAS

CARTAGENA

2004

DISEÑO Y CONSTRUCCIÓN DE UNA RED PRIVADA VIRTUAL (VPN) PARA LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

ANGÉLICA PATRICIA MENDOZA GONZÁLEZ

NIKKA MASSIEL MONTOYA RODRÍGUEZ

Monografía presentada para optar al

Título de Ingeniero de Sistemas

Director GIOVANNY VÁSQUEZ MENDOZA

Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

INGENIERÍA DE SISTEMAS

CARTAGENA

2004

Nota de aceptación

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, Junio 16 de 2004.

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

Comité de Evaluación de Proyectos.

Escuela de Ingenierías.

Ciudad.

Estimados Señores:

De la manera más cordial, nos permitimos presentar a ustedes para su estudio, consideración y aprobación el trabajo final titulado **"Diseño y Construcción de una Red Privada Virtual (VPN) para la Universidad Tecnológica de Bolívar"**, presentado para aprobar el Minor en Comunicaciones y Redes.

Esperamos que este proyecto sea de su total agrado.

Cordialmente,

Angélica Patricia Mendoza González	Nikka Massiel Montoya Rodríguez
Cod. 0005017	Cod. 0005010

Cartagena de Indias, Junio 16 de 2004.

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

Comité de Evaluación de Proyectos.

Escuela de Ingenierías.

Ciudad.

Estimados Señores:

Con el mayor agrado me dirijo a ustedes para poner a consideración el trabajo final titulado **"Diseño y Construcción de una Red Privada Virtual (VPN) para la Universidad Tecnológica de Bolívar",** el cual fue llevado a cabo por las estudiantes ANGÉLICA PATRICIA MENDOZA GONZÁLEZ y NIKKA MASSIEL MONTOYA RODRÍGUEZ, bajo mi orientación como Asesor.

Agradeciendo su amable atención,

Cordialmente,

_____

GIOVANNY VÁSQUEZ MENDOZA

Ingeniero de Sistemas.

AUTORIZACIÓN

Cartagena de Indias, D.T. y C.

Yo ANGÉLICA PATRICIA MENDOZA GONZÁLEZ, identificada con número de cédula 45.547.906 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catálogo on-line de la Biblioteca.

_____

Angélica Patricia Mendoza González
c.c. # 45.547.906 de Cartagena

AUTORIZACIÓN

Cartagena de Indias, D.T. y C.

Yo NIKKA MASSIEL MONTOYA RODRÍGUEZ, identificada con número de cédula 45.560.643 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catálogo on-line de la Biblioteca.

_____

Nikka Massiel Montoya Rodríguez
c.c. # 45.560.643 de Cartagena

DEDICATORIA

Dedico este trabajo de grado a Dios porque es el ser que siempre me brindó fortaleza y sabiduría para enfrentar los obstáculos durante esta etapa de mi vida que culmina.

Por último, sin ser ellos menos importante, a mi familia, mi mamá y mi abuelita, quienes con su tenacidad me ayudaron a salir triunfante en este proceso; a mi hermanito y a un gran amigo PLRS quienes nunca dejaron de apoyarme en los momentos más difíciles.

Y a mi papá... T.Q.M.

Angélica Patricia Mendoza González

DEDICATORIA

De Dios, gracias a Él y para Él. Sin duda alguna, es quien merece el mayor homenaje en medio de todo este trabajo.

A mis padres, que han dedicado sus vidas a mi formación y desarrollo personal, intelectual y social. Gracias por su sacrificio.

A mis hermanas, que me han apoyado y ayudado a salir adelante sin vacilaciones.

A mi familia, que son ellos junto con Dios, mi fuente de fuerzas.

A mis compañeros que han hecho miles de cosas para enseñarme a crecer, a caer y a levantarme. A quien me llena de esperanzas cada día, y me enseña a luchar por la felicidad sin desfallecer.

Nikka Massiel Montoya Rodríguez

AGRADECIMIENTOS

A **Giovanny Vásquez Mendoza**, por su apoyo incondicional durante el desarrollo de este trabajo. Su dirección fue muy importante y decisiva en la culminación del proyecto.

A **Humberto Marbello**, por prestarnos su ayuda incondicional en el área de desarrollo del proyecto de VPN.

TABLA DE CONTENIDO

INTRODUCCIÓN

Sin duda alguna, el concepto de redes ha penetrado en lo más profundo de la base tecnológica empresarial y se ha extendido considerablemente en todo tipo de negocio: pequeño, mediano o grande.

Las redes han representado intercomunicación, reducción de distancias, disminución de costos en envío de información, e innumerables cualidades más que les hacen ser muy apetecidas por cualquier organización.

Pero en medio de todo esto, nada más importante que la SEGURIDAD de la información.

INTERNET, la red más grande de todas, e igualmente de las más inseguras; uno de los medios más genialmente creados para el intercambio de ideas y que es usado por muchas empresas e instituciones para envío de datos. Por supuesto, estos datos pueden ser fácilmente capturados, transformados, y quién sabe cuántas cosas más.

Es por esto que se han desarrollado herramientas, que cada vez reducen más la inseguridad para el envío y recepción de información a través de la Internet.

Una de ellas, es la Red Privada Virtual (VPN), la cual permite crear un “túnel” que protege los datos mientras se dirigen a su destino, evitando así la intrusión.

El porqué de nuestro trabajo, radica en la explicación anteriormente dada: “interés por mantener la comunicación en un medio lo más seguro posible”.

Se considera entonces posible, aplicar estos conceptos al ámbito universitario y lograr tener acceso a información valiosa con restricciones de seguridad que la mantengan a salvo de intrusos.

1. CONCEPTOS BÁSICOS DE REDES PRIVADAS VIRTUALES (VPN)

1.1. Definición de VPN

Una Red Privada Virtual es la interconexión de dos o más redes a través de una infraestructura pública como Internet para compartir y transmitir información entre un circulo cerrado de usuarios que están situados en diferentes localizaciones geográficas.

También se puede definir como aquella Intranet que tiene una serie de subredes físicamente distantes y consigue que los recursos remotos se puedan ver como locales utilizando la Internet como canal global de comunicaciones.

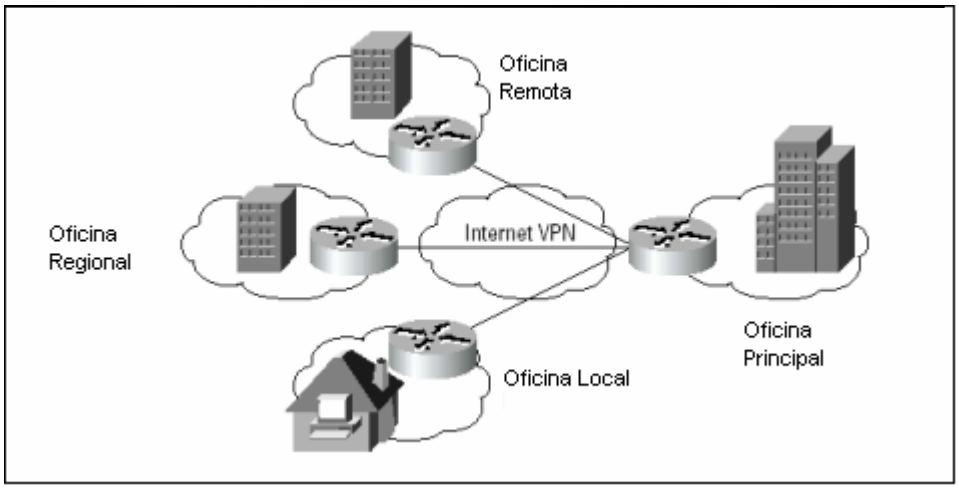


Figura 1. Diseño de VPN

Las *Redes Privadas Virtuales*, surgieron como respuesta a ciertos problemas que se presentaban en las Redes Privadas. El primero de ellos es que una Red Privada, nunca es lo suficientemente grande, por eso la Red Privada Virtual, es subyacente de la Internet, ya que ésta es una red de mucho alcance, y a través de ella se pueden compartir los recursos de comunicación y de datos. Para solucionar el segundo problema, el de que nunca se está en un entorno suficientemente compatible, se debe escoger una red de alcance global cuyos protocolos de transmisión sean estándares reconocidos y seguidos.

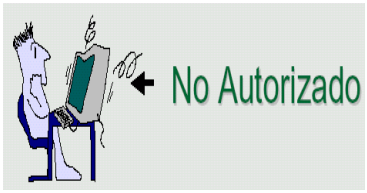
En la creación de Redes Privadas Virtuales es necesario tener en cuenta ciertos requerimientos que son importantes para la interconectividad:

- Políticas de seguridad
- Requerimiento de aplicaciones en tiempo real
- Compartir datos, aplicaciones y recursos
- Servidor de acceso y autenticación
- Aplicación de autenticación.

1.2. Características de las VPN´s.

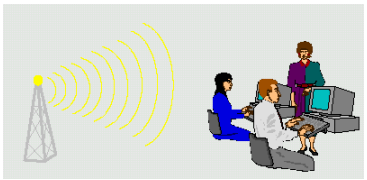
Para llevar a cabo los niveles de seguridad deseados es necesario que la red posea las siguientes características:

- *Confidencialidad o Privacidad*: Permite que la información transmitida sea accesible solamente en modo de lectura para usuarios autorizados.

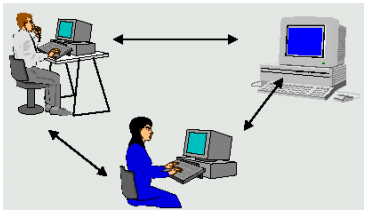


- *Integridad*: La información transmitida solo puede ser modificada (Escritura, borrado, creación y cambios) por los usuarios autorizados.

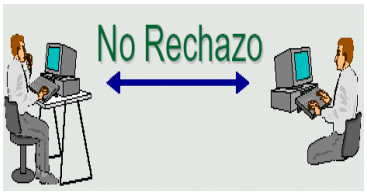
- *Autenticación*: Asegura que el emisor de la información esté correctamente identificado, con la certeza de que la identidad no sea falsa.



- *No repudiación o Disponibilidad*: Asegura la capacidad de acceder al servicio cuando el usuario lo necesite.



- *Control de Acceso*: Verifica el acceso a la información y a los recursos computacionales.



- *Viabilidad o No rechazo*: Evita que ni el receptor ni el emisor se nieguen a haber recibido o transmitido información.

Para este propósito se usa una técnica llamada *tunneling*, la cual se apoya en algoritmos de cifrado e intercambio de llaves públicas y encapsulamiento de paquetes.

1.3. Tipos de VPN

- *Sistemas basados en Hardware:* los sistemas basados en hardware son aquellos que utilizan los routers como encriptador. Estos son fáciles de instalar y de usar. Ofrecen un gran rendimiento, puesto que no necesitan ciclos de procesador haciendo funcionar un sistema operativo.
- *Sistemas basados en Cortafuegos:* son sistemas basados en mecanismos de protección contra accesos no autorizados procedentes de Internet. Estos sistemas surgen de la necesidad de resguardar la red privada ya que resulta imposible protegerla tomando medidas de seguridad en base a los

equipos por la gran cantidad de servicios que una red presta y que no tienen soporte de seguridad. Para ello los cortafuegos separa la red interna de Internet, monitorizando y filtrando todo el tráfico tanto entrante como saliente, en un único punto que será considerado como el punto fuerte de defensa. Existen tres técnicas de monitorización y filtrado del tráfico: Filtrado a nivel IP, filtrado a nivel de conexión y filtrado a nivel de aplicación (proxy):

- El filtrado a nivel IP consiste en analizar las cabeceras de los paquetes IP (dirección origen y destino, puerto destino y tipo de paquete transportado), el cual es desfavorable ya que tiene consigo ciertas desventajas como que posee una baja fiabilidad, por ello no resulta el más adecuado en los casos en los que el cortafuegos debe soportar autenticaciones de clientes externos. Además no permite la monitorización de los datos de niveles superiores intercambiados entre el cliente y el servidor. Por último las direcciones IP son visibles desde Internet por lo que deben ser los clientes internos los que se encarguen de resolver los nombres y direcciones IP de Internet y viceversa.
- El filtrado a nivel de conexión consiste en controlar la conexión entre un cliente y un servidor, y su principal problema radica en que la autenticación es muy débil y además no existe la posibilidad de realizar una monitorización de los datos que intercambian el cliente y

el servidor ya que cuando se realiza la conexión el cortafuegos actúa de manera transparente.

- El filtrado a nivel de aplicación (Proxy) consiste en bloqueo de todo el tráfico a nivel de IP entre la red interna e Internet. Los clientes internos establecen una conexión con el cortafuegos y a partir de allí un servidor Proxy actúa como intermediario comprobando los permisos de los clientes y realizando la conexión con el servidor remoto en Internet. Además el permite que la red se muestre oculta y que sólo sea visible su interfaz; también permite ejecutar software que realice conexiones con diferentes redes privadas en Internet con la utilización de líneas virtuales para que los datos viajen encriptados y autenticados. Las desventajas que nos muestra es que, los proxies no son mecanismos transparentes dado que las aplicaciones deben configurarse para que establezcan su conexión al cortafuegos en lugar de a los servidores externos.

  Realmente en la práctica se aplican las tres técnica de filtrado, teniendo en cuenta el grado de flexibilidad, transparencia y seguridad requerido.

- *Sistemas basados en Software:* estos sistemas permiten controlar el tráfico que se transmite a través del túnel de una manera más flexible ya que puede ser en función de las direcciones o de los protocolos. Son ideales

cuando los dos puntos extremos de la VPN no hacen parte de la misma organización o cuando los diferentes cortafuegos no son implementados por el mismo router o el mismo cortafuegos

1.4. Categorías de las VPN´s

- VPN Intranet: este tipo de red es creado entre una oficina central y una o varias oficinas remotas
- VPN Acceso remoto: es el que se crea entre las oficinas centrales y los usuarios situados remotamente, ya sea a través de dispositivos móviles o terminales fijas. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre.
- VPN Extranet: se forma entre dos organizaciones diferentes, o bien entre una corporación y sus proveedores o clientes. Se puede implementar una VPN Extranet mediante acuerdo entre miembros de distintas organizaciones.
- VPN Internas: con la migración hacia redes inalámbricas, como 802.11, es necesario incrementar las medidas de seguridad en una corporación. Actualmente se puede implementar una VPN interna cuando se tiene una LAN inalámbrica. En este caso la red pública es el espectro de frecuencia que se ocupa para comunicar un punto de acceso (AP) y un dispositivo

móvil. Muchos de los ataques son ejecutados desde el interior de las corporaciones, por los que una VPN interna elimina la posibilidad de que un usuario malintencionado logre acceder al servidor principal sin tener los permisos necesarios.

1.5. Tunneling

Es un método para transportar los datos de una red a otra utilizando la infraestructura de Internet o una interred cualquiera. Los datos pueden manejar protocolos distintos al que maneja la interred, ya que antes del paquete ser enviado es encapsulado por el protocolo de tunneling agregando un encabezado que pertenece al protocolo de interred sobre la cual se establece el túnel.

Luego estos paquetes son enrutados sobre la Internet entre los extremos del túnel y cuando llega a su destino es desencapsulado y reenviado a su destino final.

Las tecnologías de tunneling son:

- DLSW- Data Link Switching (SNA sobre IP)
- IPX para Novell Netware sobre IP
- GRE – Generic Routing Encapsulation (rfc 1701/2)
- ATMP – Ascend Tunnel Management Protocol
- Mobile IP – Para usuarios móviles
- IPSec – Internet Protocol Security Tunnel Mode
- PPTP - Point-to-Point Tunneling Protocol

- L2F – Layer 2 Forwarding
- L2TP – Layer 2 Tunneling Protocol

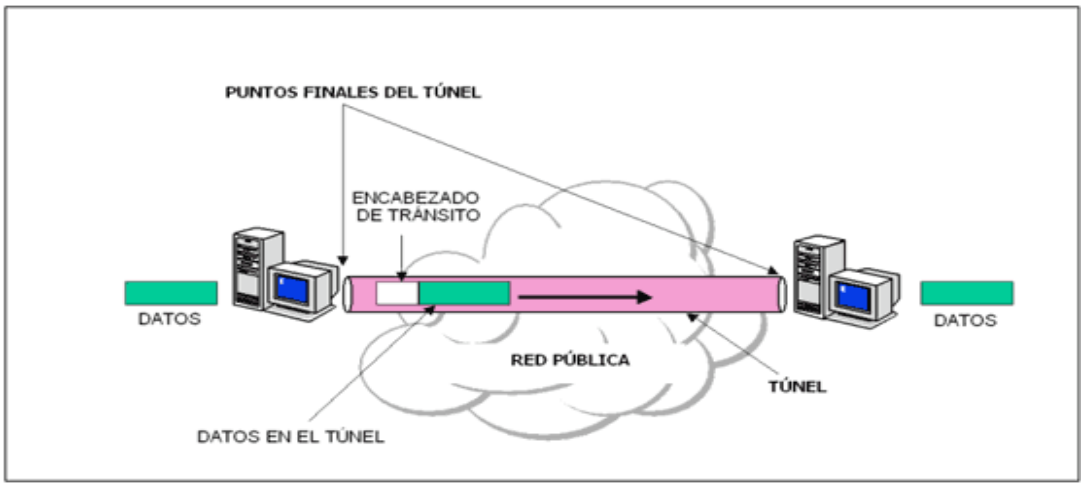


Figura 2. Tunneling

2. PROTOCOLOS PARA LA IMPLEMENTACIÓN DE REDES PRIVADAS VIRTUALES (VPN)

2.1. Point-to-Point Tunneling Protocol (PPTP)

Este protocolo diseñó hacia el año 1996 en un foro conformado por 3COM, Microsoft Corporations, Ascend Communications, E.C.I. Telematics, con el fin de proporcionar comunicaciones autenticadas y cifradas entre un cliente y una puerta de enlace o entre dos puertas de enlace, de una manera simple, compatible con variados protocolos y con la capacidad de cruzar una amplia gama de redes IP, utilizando una contraseña y un nombre de usuario, sin necesidad de claves públicas.

2.1.1. Requerimientos mínimos para el uso del PPTP

Generalmente para implementar una VPN basada en este protocolo es necesario tres computadores: Un cliente PPTP, un servidor de acceso a la red, el cual dentro de la LAN no es indispensable y un servidor PPTP.

Los servidores deben tener unos requerimientos mínimos de hardware como son: soportar Windows NT 4.0 Server o Windows 2000 Server en adelante, dos adaptadores de red, uno conectado a Internet y otro a la LAN.

El cliente puede ser un ordenador con Windows NT 4.0 Server o Workstation, Windows 2000 en adelante o Windows 95 con un MODEM. Si el cliente se encuentra en una LAN, es preciso una tarjeta de red.

2.1.2. Partes de un PPTP

- *PPP conexión y comunicación:* Inicialmente, un cliente necesita una conexión a Internet y usando PPP se contacta con un servidor de acceso a red. Además requiere de un nombre de usuario, una contraseña y un protocolo de autenticación para que le permitan o le denieguen el acceso. Luego de estar conectado puede enviar y recibir paquetes sobre Internet.
- *PPTP control de conexión:* Cuando el cliente tiene establecida la conexión PPP con el ISP, se realiza un segundo establecimiento de llamada, sobre la conexión PPP existente. Esto crea la conexión VPN (conexión de control) a un servidor PPTP de una LAN privada a una red corporativa y actúa como un túnel a través de la cual fluyen los paquetes de red. Un paquete de ocho mensajes de control establecerá, mantendrá y finalizara el túnel PPTP. Los mensajes son los siguientes:
    - PPTP_START_SESSION_REQUEST Inicia sesión
    - PPTP_START_SESSION_REPLY Responde a la solicitud de inicio de sesión
    - PPTP_ECHO_REQUEST Mantiene la sesión

- PPTP_ECHO_REPLY Responde a la solicitud de mantener la sesión
- PPTP_WAN_ERROR_NOTIFY Informa un error en la conexión PPP
- PPTP_SET_LINK_INFO Configura la conexión PPTP Cliente/Servidor
- PPTP_STOP_SESSION_REQUEST Finaliza sesión.
- PPTP_STOP_SESSION_REPLY Responde a la solicitud de fin de sesión.
- PPTP Data Tunneling

Después de establecer el túnel PPTP, los datos son transmitidos entre el cliente y el servidor PPTP. Los datos son enviados en formato de datagramas IP que contienen paquetes PPP, a los que nos referimos normalmente como paquetes PPP encapsulados. Los datagramas IP contienen paquetes IPX, NetBEUI, o TCP/IP y tiene el siguiente formato:

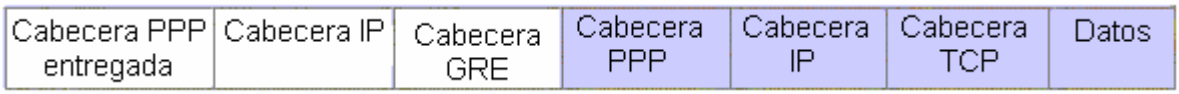


Figura 3. Datagramas IP que contienen paquetes PPP encriptados creados por PPTP

La cabecera IP de entrega proporciona la información necesaria para que el datagrama atraviese la red Internet. La cabecera GRE se usa para encapsular el

paquete PPP dentro de un datagrama IP y para contener la secuencia de información que ha sido usada para desempeñar algún nivel de control de congestión y detección de errores sobre el túnel. El área sombreada representa los datos encriptados.

Después de que la conexión VPN esta establecida, el usuario remoto (cliente) puede realizar cualquier operación como si fuera un usuario local.

2.1.3. ¿Cómo funciona?

Básicamente PPTP lo que hace es encapsular los paquetes del PPP (Protocolo Punto a Punto), los cuales ya vienen encriptados, luego es recibido por PPTP, quien utiliza una conexión de control para crear el túnel y una versión modificada de la Encapsulación de Enrutamiento Genérico (GRE), para enviar los datos en formato de datagramas IP, que serían paquetes PPP encapsulados, desde el cliente hasta el servidor y viceversa.

El proceso de autenticación de PPTP utiliza los mismos métodos, Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), que usa PPP al momento de establecer una conexión y el método de encriptación que utiliza PPTP es el MPPE (Microsoft Point to Point Encryption) y sólo es posible su utilización cuando se emplea CHAP como método de autenticación.

El servidor PPTP solo puede filtrar paquetes con filtros PPTP y con ellos puede restringir la conexión a la LAN o a Internet, lo que incrementa el rendimiento y la fiabilidad de la seguridad de red.

2.1.4. PPTP relacionado con Firewalls

PPTP complementa el uso de firewalls y cubre la necesidad de otro tipo diferente de seguridad. Los firewalls aseguran la red corporativa privada regulando estrictamente los datos que llegan desde Internet. PPTP asegura la privacidad de los datos intercambiados entre clientes y servidor a través de Internet.

El tráfico PPTP usa el puerto TCP 1723, y el identificador IP 47. Por tanto, un firewall puede configurarse para habilitar el tráfico a través de ellos. Un servidor PPTP situado detrás de él aceptará los paquetes PPTP que éste le envíe, extraerá el paquete PPP del datagrama IP, descifrará el paquete, y lo enviará a la máquina destino de la red privada.

Por tanto, se habrán combinado la seguridad del firewall en cuanto a la defensa de red privada de paquetes ajenos a ella, y la del PPTP, en lo que respecta a la seguridad con la que los paquetes de datos pertenecientes a la red privada han sido enviados a través de la red pública TCP/IP (Internet).

2.1.5. Ventajas

Una de las ventajas de este protocolo es la poca o nula necesidad del uso de equipos de telecomunicaciones que resultan costosos, para la interconexión con equipos portátiles y remotos. PPTP puede usar redes telefónicas normales de forma totalmente segura.

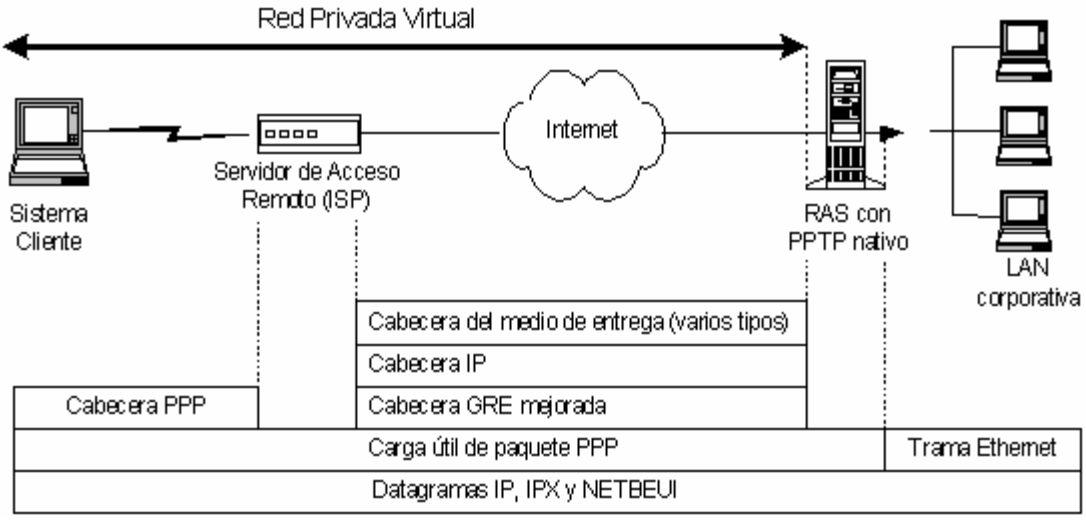


Figura 4. Red Privada Virtual basada en PPTP

2.2. Layer 2 Forwarding (L2F)

Es una tecnología propuesta por CISCO que tiene como objetivo proporcionar un mecanismo para el transporte de tramas a nivel de enlace: HDLC, PPP, SLIP, etc., sobre vínculos WAN a un servidor L2F desde un servidor de línea telefónica.

Este proceso de “tunneling” involucra tres protocolos diferentes: el protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (PPP,

SLIP, etc.); el protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y destrucción del túnel de comunicación (el protocolo encapsulador es L2F); y el protocolo portador será el encargado de realizar el transporte de todo el conjunto. Por lo general este protocolo suele ser IP dadas sus capacidades de enrutamiento, su acople a los diferentes medios y su estandarización dentro del ámbito de la Internet.

Entre las principales ventajas que ofrece este protocolo, cabe destacar el soporte multiprotocolo, la multiplexación de múltiples sesiones remotas (minimizando el número de túneles abiertos en un momento dado) y la gestión dinámica de los túneles en la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario. Además, por cada túnel L2F establecido, el proceso de seguridad genera una clave aleatoria como medida de prevención ante posibles ataques basados en *spoofing*. A su vez, en el interior de los túneles, cada una de las sesiones multiplexadas mantendrá un número de secuencia para evitar problemas debidos a la duplicidad de paquetes.

Este protocolo, a diferencia del PPTP y el L2TP no tiene un cliente definido.

00	01	02	03	04	..	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
F	K	P	S	0	0	0	C	Versión			Protocolo								Secuencia							
Multiplex ID											Client ID															
Length											Offset															
Key																										

Figura 5. Formato de Paquetes L2F

2.3. Layer 2 Tunneling Protocol (L2TP)

Éste protocolo se desarrolló con el fin de resolver los problemas de interoperabilidad que existen entre los protocolos L2F y PPTP; para eso se combinaron las mejores características de ambos.

L2TP existe en la capa de enlace de datos del modelo OSI y soporta clientes IP, Frame Relay, X.25 o ATM.

Cuando se configura para usar IP, L2TP puede ser usado como protocolo de Tunneling sobre Internet y también puede ser usado en la WAN sin capa IP de transporte. L2TP sobre interredes IP hace uso de UDP para mantener el túnel.

Para seguridad de los datos se apoya en IPSec.

PPTP	L2TP
Requiere una interred IP	Requiere que el medio de tunneling ofrezca conectividad punto a punto.
Soporta un solo túnel en los extremos	Soporta múltiples túneles en los extremos
No ofrece autenticación de túnel	Ofrece autenticación de túnel.

Figura 6. Diferencias entre PPTP y L2TP

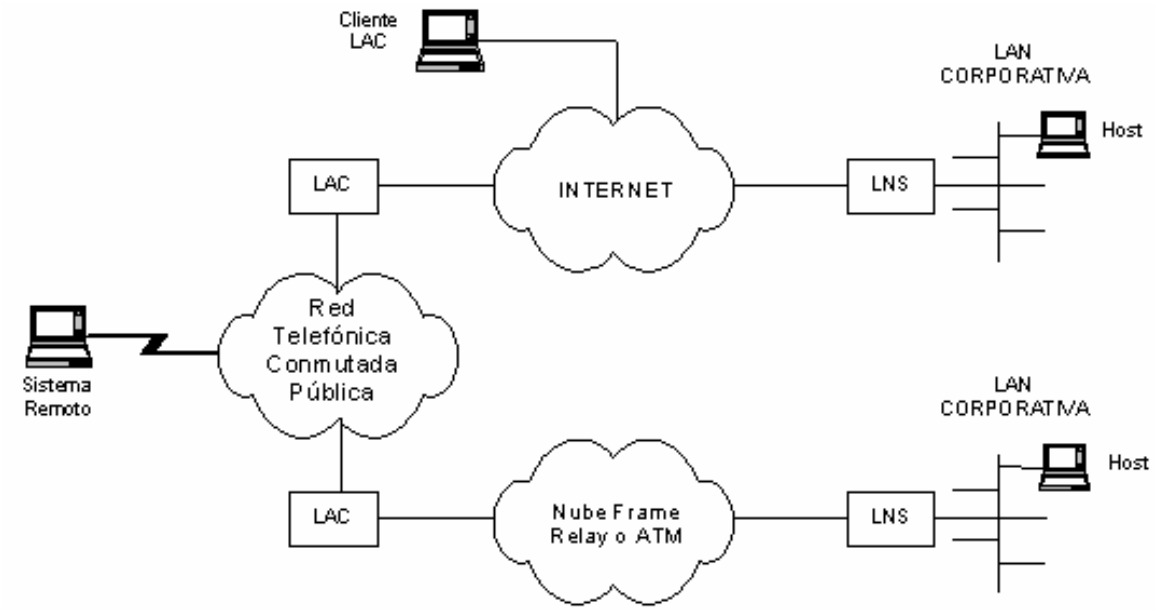


Figura 7. Red Privada Virtual basada en L2TP

L2TP esta compuesto de dos partes, el concentrador de acceso L2TP (LAC) y el servidor de red L2TP (LNS). El LAC se sitúa entre un LNS y un sistema remoto, manda paquetes a cada uno de los dos. El LNS es el par del LAC, y es un punto de terminación lógica de una sesión PPP a la cual se le esta siendo aplicado el túnel desde el sistema remoto por el LAC. El L2TP soporta dos modos de túneles, el modo Obligatorio y el Voluntario.

L2TP usa el Protocolo de Control de Red (Network Control Protocol, NCP) para asignar la IP y autenticar en PPP, llamados comúnmente, PAP o CHAP. La seguridad en L2TP requiere para el transporte seguro que estén disponibles los servicios de encriptación, integridad y autenticación para todo el tráfico L2TP. Este

transporte seguro opera en todo el paquete L2TP y es funcionalmente independiente de PPP y del protocolo que este transporta.

Túnel Obligatorio L2TP

1. El usuario remoto inicializa una conexión PPP a un ISP
2. El ISP acepta la conexión y el enlace PPP se establece
3. El ISP solicita la autentificación parcial para saber el nombre de usuario
4. El ISP mantiene una lista de todos los usuarios admitidos, para servir el final del túnel LNS
5. El LAC inicializa el túnel L2TP al LNS
6. Si el LNS acepta la conexión, el LAC encapsulara el PPP con el L2TP, y entonces enviara a través del túnel
7. El LNS acepta estas tramas, y las procesa como si fueran tramas PPP.
8. El LNS usa la autentificación PPP para validar al usuario y entonces asigna una dirección IP

Túnel Voluntario L2TP

1. El usuario remoto tiene una conexión a un ISP ya establecida
2. El cliente L2TP (LAC), inicializa el túnel L2TP al LNS
3. Si el LNS acepta la conexión, LAC encapsula con PPP y L2TP, y lo enviará a través del túnel

4. El LNS acepta estas tramas, y las procesa como si fueran tramas normales de entrada (PPP).
5. El LNS usa la autentificación PPP para validar al usuario y asignarle una IP

2.4. Internet Protocol Security (IPSEC)

Para una organización, la comunicación interna debe ser privada. La Internet, es todo menos privada.

Las redes privadas virtuales, o VPN (Virtual Private Network), crean conexiones seguras, llamadas túneles sobre infraestructuras de comunicación compartidas públicamente como la Internet. Estos túneles no son entidades públicas, sino construcciones lógicas, creadas usando encriptación, estándares de seguridad y protocolos.

Como estos estándares y protocolos han continuado evolucionando, varias tecnologías han surgido. IPSec es una de ellas, y de las más utilizadas en cuanto a VPN se refiere.

2.4.1. Beneficios de la Tecnología IPSec

- Las conexiones de VPN seguras a través de IPSec en la Internet, resultan ser beneficiosas increíblemente en cuanto a costos de comunicación se refiere, comparándolo específicamente con una conexión WAN. Además puede incrementar la productividad en una organización.

- A través de IPSec, una organización puede garantizar un acceso restringido a la red para trabajadores, clientes, o vendedores, incrementando la eficiencia velocidad de las comunicaciones de negocios, ventas y procesamientos, y manejo de servicios al cliente.
- Trabajadores desde casa, telecommutadores, y trabajadores en el campo de ventas y servicios pueden acceder a la red corporativa seguramente y económicamente con el acceso remoto de IPSec sobre la Internet pública.

Estos beneficios han hecho de IPSec una solución muy aplicada en las organizaciones globales. Esta representa un gran mercado potencial y creciente para los manufactureros y proveedores de productos y servicios relacionados con IPSec.

2.4.2. Limitaciones de IPSec

IPSec está diseñado para asegurar enlaces IP entre máquinas. Sin embargo posee varias limitaciones, como:

- IPSec no puede ser seguro si su sistema no lo es. El sistema de seguridad en las puertas de enlace es un requerimiento esencial si IPSec será aplicado.
- IPSec no es de extremo a extremo. IPSec no puede proveer la misma seguridad de extremo a extremo de los sistemas de trabajo en altos niveles.

IPSec encripta conexiones IP entre dos máquinas, lo cual es diferente a encriptar mensajes entre usuarios o entre aplicaciones.

- IPSec no lo puede hacer todo. No puede proveer todas las funciones de los sistemas de niveles altos. Por ejemplo se necesitan para hacer documentos firmados electrónicamente, firmas digitales.
- IPSec autentica máquinas no usuarios. IPSec utiliza mecanismos de autenticación para controlar qué mensajes van a las máquinas, pero no tiene el concepto de ID de usuario, que es vital para otros mecanismos y políticas de seguridad.

2.4.3. ¿Qué es IPSec?

Es un conjunto de estándares y protocolos abiertos para la creación y mantenimiento de comunicaciones seguras sobre redes IP. IPSec utiliza estos estándares y protocolos para asegurar la privacidad e integridad de la transmisión y comunicaciones de los datos sobre las redes públicas como Internet.

2.4.4. Servicios de Seguridad de IPSec

IPSec establece estándares para el manejo de riesgos de seguridad de todo el tráfico IP sobre la red pública.

- Confidencialidad. La encriptación protege la privacidad de las comunicaciones aún si estas son interceptadas.

- Control de acceso. El acceso a comunicaciones privadas sobre IPSec es restringido sólo a usuarios autorizados.
- Autenticación. La autenticación verifica la fuente de los datos recibidos (autenticación del origen de los datos), y confirma que el paquete IP original no fue modificado en transmisión.
- Rechazo de paquetes reenviados. Un servicio que evita ataques por reenvío, basado en la intercepción de una serie de paquetes por un intruso y que luego son reenviados.

2.4.5. ¿Cómo funciona IPSec?

Antes de que dos dispositivos puedan establecer un túnel IPSec y comunicarse seguramente a través de él, ellos deben ponerse de acuerdo en los parámetros de seguridad para usar durante la comunicación, estableciendo lo que es llamado Asociación de Seguridad (SA). La SA especifica los algoritmos de autenticación y encriptación para ser usados, las claves de encriptación para ser usadas durante la sesión, y cuánto tiempo son mantenidas las claves y la SA. El protocolo de Intercambio de Claves de Internet, IKE (Internet Key Exchange), es usado para instalar las asociaciones de seguridad necesarias para la comunicación segura a través de la VPN.

En el proceso de negociación, un punto final de IPSec actúa como el iniciador y el otro como quien responde. El que inicia ofrece un conjunto de parámetros de

autenticación, encriptación y otros, que está listo para usar con el otro punto final de la comunicación. Quien recibe, trata de que haga juego esta lista con su propia lista de técnicas soportadas. Si hay problemas, el envía su respectiva lista. El que inicia escoge una combinación de técnicas del que recibe y ellos proceden con la negociación.

La negociación IKE tiene dos fases:

- La *Fase 1*, permite a dos puertas de enlace de seguridad autenticarse entre sí y estableces parámetros de comunicación para las comunicaciones de la Fase 2. Al final de la fase, una Asociación de Seguridad (IKE SA) es establecida.
- La *Fase 2*, permite a dos puertas de enlace de seguridad estar de acuerdo con los parámetros de comunicación de IPSec en nombre de sus respectivos hosts. Al final de la fase, una SA IPSec es establecida.

IPSec utiliza dos protocolos para establecer servicios de seguridad, AH (Authentication Header) y ESP (Encapsulating Security Payload).

Authentication Header (AH). Provee integridad de datos y autenticación de origen de estos para paquetes IP. Incluye una suma de verificación criptográfica sobre todo el paquete. El receptor usa esta suma para verificar que el paquete no ha sido falsificado.

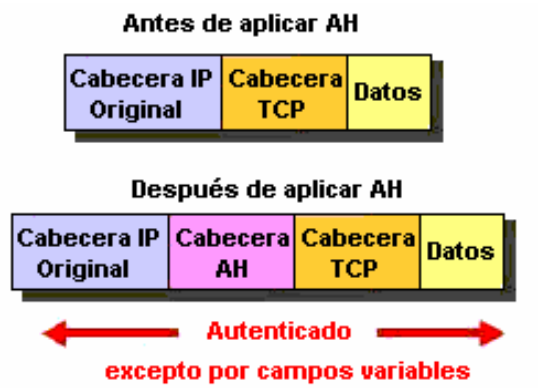


Figura 8. Formato de paquete antes y después de AH

Encapsulating Security Payload (ESP). Provee confidencialidad al tráfico IP sobre la encriptación. El estándar de algoritmos encriptación actual de IPSec incluye el 3DES (Triple Data Encryption Standard), y el AES (Advanced Encryption Standard).

Además de confidencialidad, ESP provee capacidades de autenticación y anti-reenvío. A diferencia de AH, los servicios de autenticación de ESP no protegen la cabecera IP del paquete. Actualmente, la mayoría de implementaciones de VPN usan ESP.

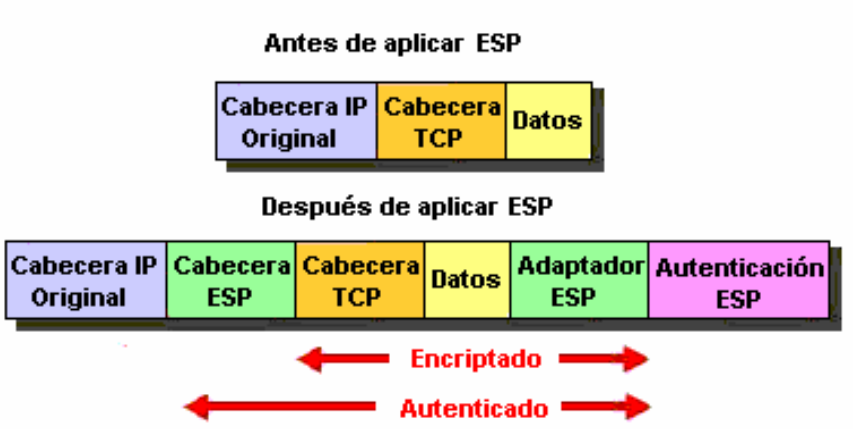


Figura 9. Formato de paquete antes y después de ESP

AH y ESP pueden ser usados separadamente o juntos. Como sean usados, depende del modo IPSec: Modo de Transporte o Modo de Túnel. Las conexiones de Cliente a LAN usan normalmente Modo de Transporte, mientras que de LAN a LAN el modo típicamente usado es el de Túnel.

En el ***Modo de Transporte***, sólo la carga IP es encriptada, y las cabeceras IP originales se dejan intactas. Este modo tiene la ventaja de agregar sólo unos poco bytes a cada paquete; además permite a los dispositivos de la red pública ver la fuente y destino final del paquete, permitiendo así habilitar procesamientos especiales como calidad de servicio. Desafortunadamente, permite el análisis del tráfico por parte de algún intruso, aunque esto sólo les permitiría saber que fueron enviados los paquetes IP.

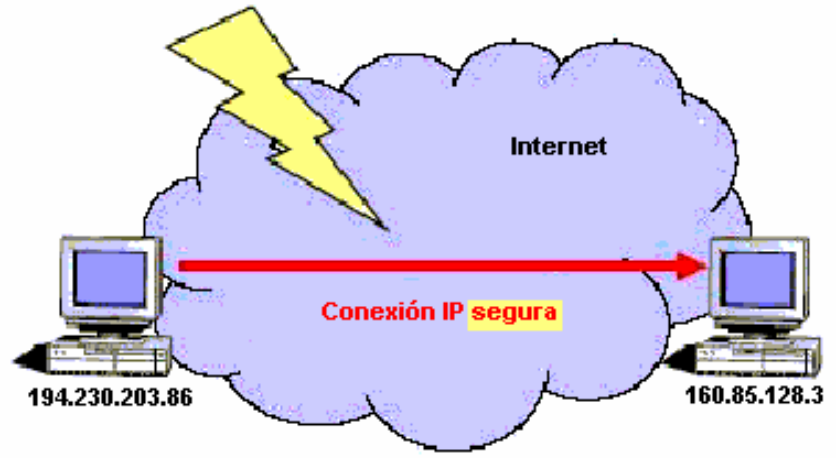


Figura 10. Modo de Transporte

En el ***Modo de Túnel***, todo el datagrama IP original es encriptado, y se convierte en la carga de un nuevo paquete IP. Este modo permite a un dispositivo de red, como un router, actuar como un proxy IPSec, lo cual permite la encripción en medio de los hosts. El router fuente encripta los paquetes y los envía a través del túnel IPSec. El router destino desencripta el datagrama IP original y lo envía al sistema destino. La mayor ventaja del modo de túnel es que los sistemas finales no necesitan ser modificados para disfrutar de los beneficios de IPSec. Además protege contra análisis de tráficos, puesto que el intruso sólo puede determinar los puntos finales del túnel, pero no los verdaderos fuente y destino de los paquetes.

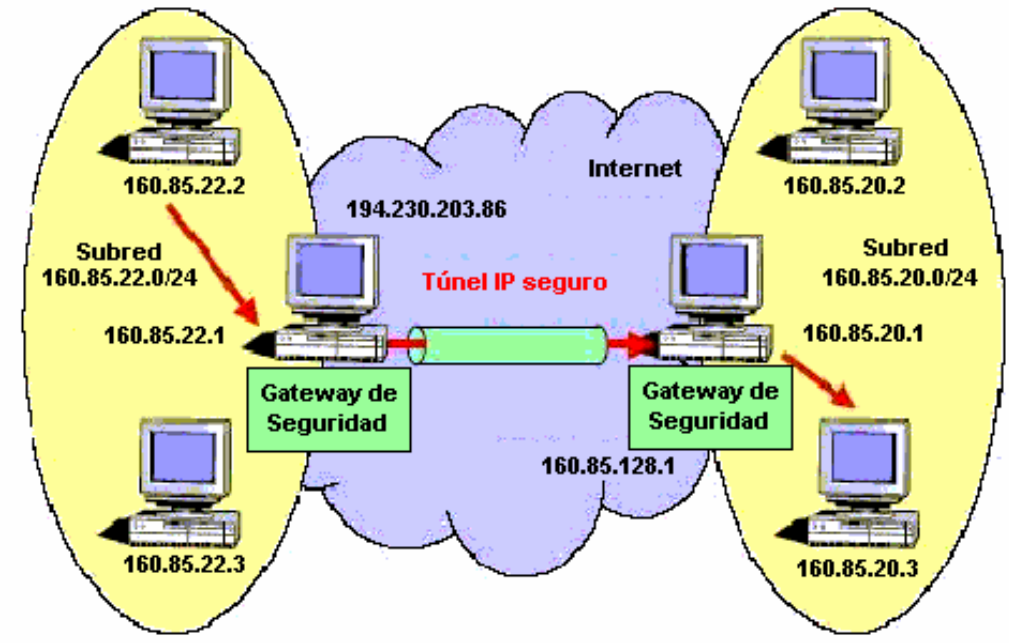


Figura 11. Modo de Túnel

2.4.6. FreeS/WAN

GNU/Linux ***FreeS/WAN ("Free Secure WAN")*** es una implementación gratis de IPSec (Seguridad para el Protocolo de Internet) e IKE para sistemas GNU/Linux. Esta utiliza una fuerte criptografía para proveer tanto autenticación como encriptación; la autenticación asegura que los paquetes provienen del emisor correcto y que no han sido alterados en la transmisión, y la encriptación previene la lectura desautorizada del contenido de los paquetes.

La filosofía de código abierto de Linux es lo que hace la existencia posible de FreeS/WAN, porque utiliza la posibilidad de modificar el código fuente del núcleo de Linux para incluir el soporte de IPSec. En realidad, FreeS/WAN puede ser vista como un paquete de dos partes: Un parche que hace modificaciones necesarias al núcleo para soportar IPSec, y un grupo de herramientas de software para controlar el manejo de claves.

2.4.6.1. Objetivos de FreeS/WAN

El objetivo principal de FreeS/WAN es hacer la Internet más segura y más privada. Algunos objetivos más detallados que los desarrolladores han manejado son:

- Extender IPSec para realizar encripción oportunística para:
  - ✓ Que dos sistemas cualesquiera puedan asegurar su comunicación sin haber tenido una pre-establecida

- ✓ Tener conexiones seguras por defecto, cambiándose a conexiones sin encriptación sólo si:
  - o Si los extremos no están dispuestos a realizar la conexión segura
  - o Si su política permite conexiones inseguras
  - o Una parte significante del tráfico en la Internet sea encriptado
  - o Sea imposible o difícil realizar monitoreos de la red
- Ayudar a hacer extensible IPSec proveyendo una implementación sin restricciones:
  - ✓ Disponible gratis en código fuente bajo GNU (General Public License)
  - ✓ Corriendo en un rango disponible de hardware
  - ✓ No sujeto a restricciones de exportación de USA u otras naciones
  - ✓ Portable a todas las CPUs con soporte de Linux
  - ✓ Interoperable con otras implementaciones de IPSec

FreeS/WAN es una solución ideal que le permite al administrador de la red, unir telecommutadores y equipos de oficina de todas partes sobre la Internet, y lo hace por el precio del hardware, con requerimientos sorprendentemente bajos.

Un escenario común crea un túnel seguro entre dos redes, sobre una red no confiable; otro escenario es la creación de una conexión segura entre una red y un host remoto.

Se puede decir que es una solución elegante para un serio problema en los negocios y el comercio - la naturaleza abierta de la Internet. Esto bueno en el intercambio de información e ideas, pero no lo es tanto para datos sensibles de clientes, transacciones financieras, y cosas por el estilo. La otra opción es crear una red privada física, con altos costos de construcción.

2.4.6.2. ¿Cómo funciona?

La arquitectura de FreeS/WAN consiste en dos partes importantes, el demonio de IKE (llamado Pluto) con un conjunto de utilidades que negocia las muchas conexiones con los otros sistemas y el Soporte del kernel de IPSec (llamado KLIPS, con dispositivos virtuales IPSec) que implementa AH (authentication header), ESP (encapsulating security payload) y paquetes de manejo en el núcleo.

2.4.6.3. KLIPS

Como ESP trabaja sobre IP para encapsular y encriptar paquetes TCP y UDP, debe colocarse dentro del código de enrutamiento del servidor. Es decir, se debe colocar dentro del código de transmisión y recepción de paquetes en la red. Por tanto, se debe adicionar al código del núcleo para aumentar la programación de red ya establecida allí.

Para esto, el código es incluido en una parte del paquete KLIPS (Kernel Level IP Security Support). Este es necesario para habilitar el uso de ESP. Requiere una

reconstrucción del núcleo y un rearranque de Linux y además, el uso de núcleos estables (2.2.18).

2.4.6.4. PLUTO

Como se usa IKE para instalar el SA, se necesita un programa basado en UDP para establecer el SA. Pluto, es el programa que escucha a través del puerto 500, las peticiones de IKE. No necesita ser parte del kernel, simplemente es otro demonio del sistema que escucha en un puerto como muchos otros servicios.

FreeS/WAN determina varios espacios en su funcionamiento:

ESPACIO DE USUARIO

Los programas y utilidades del espacio de usuario en FreeS/WAN son:

- Pluto, el demonio de IKE
- Un mecanismo de script
- Algunas utilidades para instalación y configuración

Pluto es responsable de negociar ISAKMP (Asociación de Seguridad en Internet y Protocolo de Manejo de Claves) y SA (Asociación de Seguridad) de IPSec con otros demonios IKE (de acuerdo a su SPD) y se encarga de instalar este SA de IPSec en KLIPS (con el uso de una interfaz de socket extendida PF_KEY)

ESPACIO DEL NÚCLEO

La parte del núcleo de FreeS/WAN contiene los dispositivos virtuales de IPSec (un máximo de 4), el SAD y los mecanismos de encriptado. Un dispositivo de IPSec es una interfaz virtual que puede ser establecida entre la capa IP y un dispositivo físico de red (ej. un dispositivo Ethernet). Con este diseño FreeS/WAN está habilitada para forzar el tráfico que debería hacer uso de IPSec para pasar a través de la maquinaria de KLIPS sin cambiar mucho en el código de enrutamiento de los núcleos.

PROCESAMIENTO DE SALIDA DE PAQUETES

Un buscador de rutas en la capa IP devuelve un dispositivo IPSec como interfaz de salida, así el código de enrutamiento IP llama la rutina de salida de KLIPS. Ahora la dirección IP de destino y el dispositivo virtual IPSec son usados para seleccionar el apropiado SA IPSec para ser aplicado. Entonces la rutina de salida del dispositivo físico adjunto de la red es llamada.

PROCESAMIENTO DE LLEGADA DE PAQUETES

Un paquete que llega es recibido por un dispositivo físico, y es pasado a la maquinaria de KLIPS sólo si tiene una cabecera ESP o AH, donde es asignado al dispositivo IPSec adjunto y procesado de acuerdo con el SA apropiado. Entonces es pasado arriba, hacia el próximo manejador del protocolo.

2.4.6.5. Configuración de FreeS/WAN

FreeS/WAN utiliza dos archivos que necesitan ser editados antes de que la primera comunicación tome lugar:

- */etc/ipsec.config,* usado para la configuración interna de FreeS/WAN (adjuntar dispositivo virtual de IPSec a un dispositivo físico de la red, manejo de nivel de depuración para Pluto y KLIPS, etc.), para la definición de "Conexiones" a otros gateways de seguridad, y para la determinación de cuáles conexiones deberían ser cargadas, o cargadas y negociadas en el inicio de Pluto. Las "Conexiones" es el término que utiliza FreeS/WAN para especificar parámetros (ej. Direcciones IP de puertas de enlace IPSec, redes IP detrás de puertas de enlace IPSec, mecanismos de autenticación para las puertas de enlace IPSec, tiempo de vida para el ISAKMP SA y para el SA de IPSec) que deben ser usados para negociar e instalar un ISAKMP y un SA de IPSec. Este contiene toda la información acerca de cómo son establecidos los túneles.
- */etc/ipsec.secrets,* manejado para autenticar la comunicación con otros IKE y (en las nuevas versiones) la clave RSA privada del sistema local. Este archivo contiene todas las contraseñas y cosas que se necesitan mantener en secreto.

El archivo ipsec.conf consiste en dos secciones, la sección config y la conn. Sin embargo la única sección de config reconocida por FreeS/WAN actualmente es

"setup config". Esta sección contiene toda la información que el software necesita saber en el momento de comenzar. Un ejemplo de esta sección es:

```
config setup
        interfaces=%defaultroute
        klipsdebug=none
        plutodebug=none
        plutoload=%search
        plutostart=%search
        uniqueids=yes
```

El valor más importante es el parámetro de interfaces; el valor especial %defaultroute significa que la interfaz que Pluto usa para establecer un túnel encriptado es uno de los que tiene la ruta por defecto del sistema. Los parámetros de debug, klipsdebug y plutodebug, necesitan cambiarse sólo cuando se tienen problemas. Los mensajes por defecto que se reciben en el registro, son en la mayoría de los casos, suficientes para comprender dónde está el problema.

La sección conn dice qué tipo de túneles puede aceptar o establecer Pluto. El siguiente ejemplo llama a "the concentrator", que es una puerta de enlace de seguridad en frente de la LAN y al cual todos quieren conectarse. Esta es la única

puerta de enlace que necesita una IP estática en el ejemplo, y también es el centro de la topología de red en estrella usada en este caso.

```
conn %default
        keyingtries=0
        authby=rsasig
        leftrsasig=%cert
        leftcert=hostBobcert.pem
        leftsubnet=192.168.1.0/24
        leftnexthop= el gateway por defecto (the concentrator)
        rightrsasig=%cert
```

Estos parámetros son establecidos para aplicar todas las secciones conn. La línea de keyingtries especifica cuántas veces Pluto trata de establecer un túnel especifico; un valor en cero significa seguir intentándolo. El parámetro authby puede contener uno de dos valores, secret, para la autenticación de claves secretas pre-compartidas y rsasig, que es usado para autenticar la puerta de enlace de seguridad usando una firma digital RSA. leftrsasig le dice a Pluto cómo obtener la firma RSA del lado izquierdo del túnel. %cert es un valor x509 (parche de FreeS/WAN) específico que dice la clave pública que debe ser extraída de un certificado X.509 enviado por el otro. leftcert es un parámetro x509 específico que

informa a Pluto cuál archivo tiene el certificado x509 en el lado izquierdo del túnel. En este caso “the concentrator“ certifica que es Bob.

La instalación inicial de FreeS/WAN inserta FreeS/WAN en el proceso de arranque del sistema Linux. Durante el arranque del sistema los dispositivos virtuales de IPSec son configurados poco después de la inicialización de la red (adjunto a su dispositivo de red físico, asignada la dirección IP del dispositivo físico de la red) y Pluto es iniciado. El diseño actual necesita manipular la tabla de ruteo así que el enrutamiento de paquetes por el cual existe SA IPSec, usa el dispositivo IPSec como interfaz de salida. Además, un SA IPSec debe ser instalado antes de ser usado. Esto significa que los SA son sólo negociados y establecidos por peticiones administrativas y no por mensajes de llegada.

El primer paso es la autenticación con las puertas de enlace, que son las que permitirán el enlace entre las subredes a comunicar. FreeS/WAN soporta manejo de claves manual y automático. Es preferible el manejo automático puesto que es más seguro. Dos sistemas se autentican entre sí y negocian sus propias claves secretas. Si una clave fuese interceptada de alguna manera por una persona con malas intenciones, no habría problema; nuevas claves son generadas periódicamente e intercambiadas, así que cualquier daño es automáticamente limitado. El equipo de FreeS/WAN prefiere usar un par de claves RSA, con los

estándares público/privado. Una vez que la conexión es validada y establecida, el tráfico encriptado viaja a través de la red.

Los paquetes son aún abiertos a la intercepción; no hay barrera para los sniffers. Sin embargo, FreeS/WAN usa la encripción 3DES - 168 bit, para que cualquier espía de sus paquetes no pueda ver nada de la información enviada. La encripción DES simple de 56 bit, ha sido probada de ser vulnerable a los ataques de fuerza bruta, y por tanto, no debería ser usada. Se debe ser cuidadoso porque algunas implementaciones de IPSec hacen uso del DES simple.

El proceso en resumidas cuentas, se realizaría de la siguiente manera:

- Los paquetes de nuestro equipo son enviados a través de IP al servidor de FreeS/WAN.
- Lo primero que él hace es enviar un paquete IKE sobre el puerto 500 UDP. Pluto está escuchando sobre este mismo puerto.
- Pluto responde y ahora sabemos cómo hablarnos.
- Enviamos un paquete ESP al servidor de FreeS/WAN. KLIPS en el núcleo del servidor de FreeS/WAN envía paquetes ESP devuelta.
- El paquete ESP es encriptado usando el método acordado por SA de la conversación de IKE con Pluto.

- La conversación continúa, usando ESP para encriptar y transmitir durante la conversación en la red desde su equipo hasta el KLIPS en el servidor de trabajo.
- Y de esta manera se continúa la comunicación entre los dispositivos.

3. IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL

3.1. Introducción a la implementación

Este capítulo, se dedica íntegramente a la descripción de los aspectos que tuvimos en cuenta para el desarrollo de nuestra red privada virtual, así como los pasos necesarios para lograr nuestro cometido.

Específicamente, hacemos una descripción de la topología básica que implementamos para nuestra prueba piloto, que será la base de posibles desarrollos de redes privadas virtuales en la comunidad universitaria.

Mostramos a su vez, las configuraciones necesarias para cada uno de los servidores que utilizaremos, en nuestro caso DNS, DHCP, VPN y de archivos, y la configuración del cliente final que hará uso de los servicios proporcionados por la red.

En esta prueba piloto, permitimos al cliente de una red cualquiera, tener acceso a la información que alberga un servidor de archivos, en nuestra prueba, el cual se encuentra en otra red.

El servidor VPN será el enlace entre estas dos redes, comunicado entonces con la de los servidores DNS, DHCP y de archivo, y a su vez, con la del cliente que accederá a la información; esto se llevará a cabo gracias a las dos tarjetas de red con que contará el servidor VPN.

Luego de esta prueba piloto, hemos considerado que se podría aplicar inicialmente para una red de profesores que necesiten acceder a información guardada en un servidor de archivos escogido para este fin, y luego, considerar extenderlo para la comunidad estudiantil en general, para efectos de provisión de talleres o exámenes que los profesores puedan proporcionarles.

Todo esto, en términos futuros.

Ahora nos concentraremos en el proyecto piloto desarrollado, que esperamos genere las expectativas necesarias para que se inicien las posibles implementaciones anteriormente mencionadas.

3.2. Diseño físico de la red privada virtual (VPN)

Esta Red Privada Virtual (VPN) que mostraremos a continuación, será la prueba piloto que nos permitirá profundizar en los conocimientos y aplicación de los conceptos sobre la seguridad que se logra a través de las VPN.

En nuestra prueba implementamos varios servidores que se encargan específicamente de varias tareas y son:

- **Servidor DNS**: permite establecer la correspondencia entre las direcciones IP y los nombres de los equipos. Este servidor posee una dirección estática, puesto que si es asignada dinámicamente los clientes podrían perder contacto con el servidor.

- **Servidor DHCP**: se utiliza para proveer automáticamente de direcciones IP a los diferentes equipos que se encuentran en la Intranet; además, actualiza la ubicación de las puertas de enlace por defecto y del servidor DNS para cada host.
- **Servidor de Archivos**: es aquel que permitirá albergar la información a la cual accederá nuestro cliente gracias al servidor VPN configurado.
- **Servidor VPN**: este servidor será el punto medio de la topología que implementamos en nuestra prueba, el cual servirá de enlace entre las redes establecidas (Intranet e Internet) y así prestará el servicio de intercomunicación entre el cliente y el servidor de archivos.

Igualmente habilitamos un cliente que a través de su configuración accederá al servidor VPN el cual le permitirá comunicarse con el servidor de archivos para tomar la información que requiera.

Se tiene convenciones específicas que hacen referencia a cada uno de los equipos que participan de la red, y se manejan dos segmentos de red definidos por distintas direcciones IP establecidas; uno de ellos representará el grupo de equipos perteneciente a la Intranet, que estará referenciada por los servidores que se utilicen, y el otro segmento que señalizará la conexión a Internet que se ha querido simular, y que estará determinando la ubicación del cliente que accederá a la Intranet, y más específicamente al servidor de archivos.

La topología a desarrollar en nuestra prueba es la siguiente:

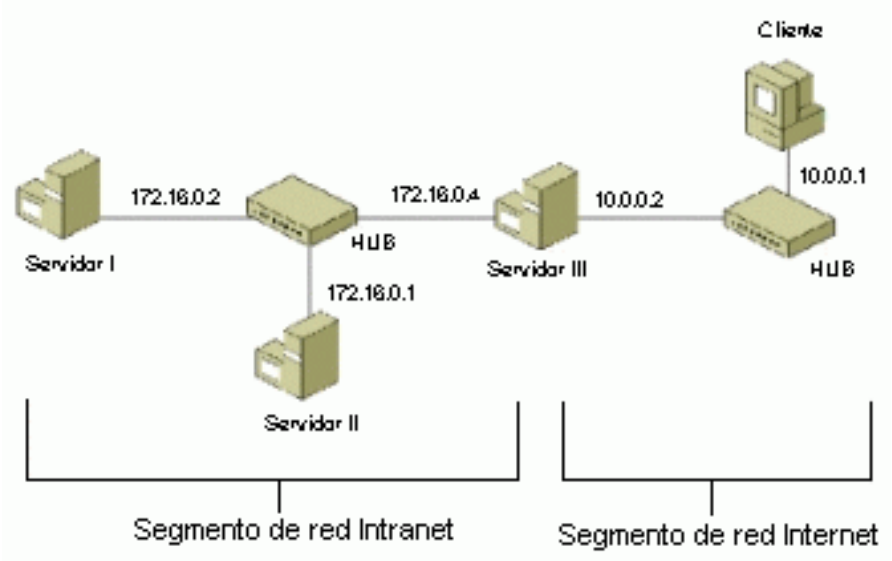


Figura 12. Topología de red de prueba

En la anterior gráfica se definieron varios dispositivos así:

- **Servidor I:** que estará realizando las veces del servidor de archivos, y al cual el cliente accederá desde donde se encuentre. Su dirección será asignada dinámicamente a través del servidor DHCP configurado.
- **Servidor II:** este equipo será configurado con los servicios de DNS, DHCP y controlador de dominio, y poseerá una IP estática, de acuerdo a las explicaciones anteriores.
- **Servidor III:** será el servidor VPN que establecerá el enlace entre las redes, y permitirá al cliente acceder a la información del servidor de archivos.

- **Cliente:** sin duda alguna, será el equipo que utilizará los servicios que proveerán los servidores de la Intranet.

Los hubs permitirán la interconexión de los diferentes equipos entre sí, para establecer las redes.

3.3. Configuración de servidores

Los detalles sobre la configuración de cada uno de los servidores, se presentarán a continuación, mostrando las pantallas más relevantes y que generan mayor comprensión ante el lector y posible desarrollador.

3.3.1. Configuración del Servidor II

Inicialmente, se explicará la configuración llevada a cabo en el **Servidor II**, el cual es un computador con el sistema operativo Windows Server 2003 instalado, el cual proveerá de los siguientes servicios:

- Un controlador de dominio para el dominio de Active Directory, que en nuestra prueba se denominará *ejemplo.com.*
- Un servidor DNS para el dominio *ejemplo.com.*
- Un servidor DHCP para el segmento de red de Intranet.

Para configurar los servicios anteriormente mencionados se llevan a cabo los siguientes pasos:

1. Se instala Windows Server 2003.
2. Se configura la dirección IP del servidor estáticamente, y será 172.16.0.1 con máscara de subred 255.255.255.0.
3. A través de la guía de instalación y administración de servidores que provee el sistema operativo, se crea el nuevo dominio *ejemplo.com* para un nuevo bosque. Además se instala el servicio DNS.
4. Hacemos uso del asistente y creamos una zona para la asignación de los nombres a los recursos, e indicamos el servidor que mantendrá los datos DNS para los equipos.

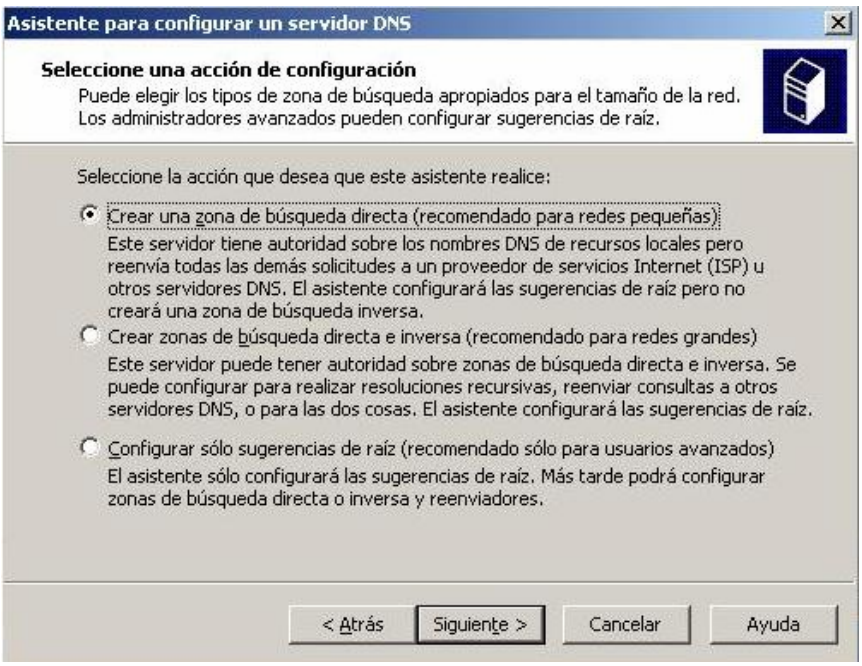


Figura 13. Creación de zona de búsqueda directa

Figura 14. Determinación de administrador de zona

5. Le damos el nombre a la zona que recientemente creamos, el cual es en nuestro caso el nombre de dominio.

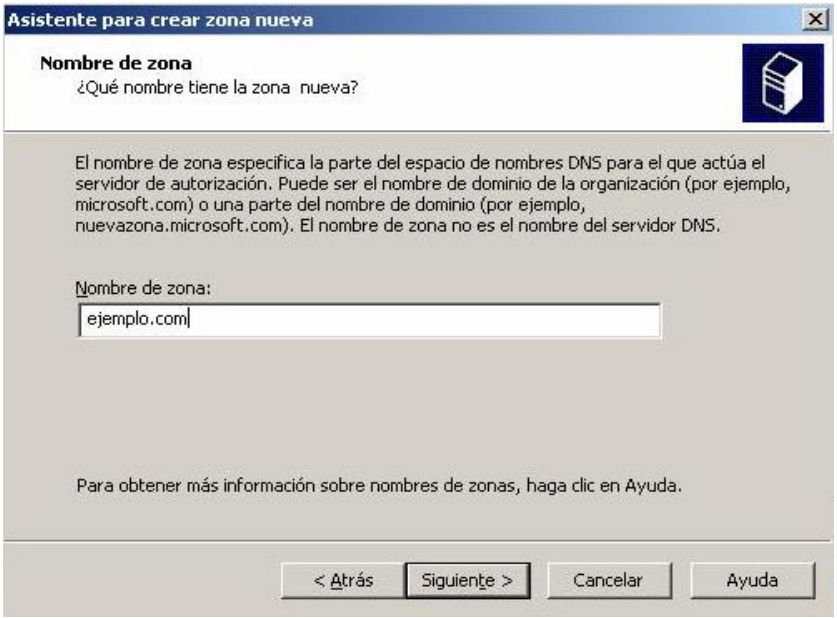


Figura 15. Establecimiento de nombre de zona

6. Luego el asistente nos permite configurar el archivo de la zona creada; además, se activan las actualizaciones de los registros.

Figura 16 Creación de archivo de zona

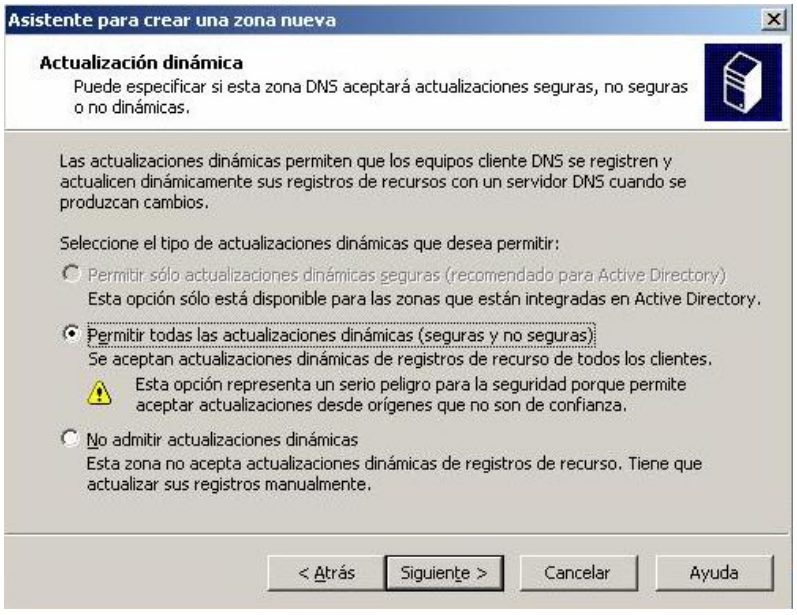


Figura 17 Actualización de archivos de recursos

7. En nuestro caso, decidimos no hacer reenvío de consultas, pero eso depende de si se tiene un servidor de apoyo que se pueda utilizar para la solución de respuestas para el usuario.

Figura 18 Determinación de reenvíos a otros servidores DNS

8. Con esto finaliza la configuración y nos define que somos servidores DNS.

Figura 19 Confirmación de servicio DNS configurado

9. En el servidor DNS, hacemos una configuración final de la zona para realizar la correspondencia entre la dirección IP y el nombre en el dominio.

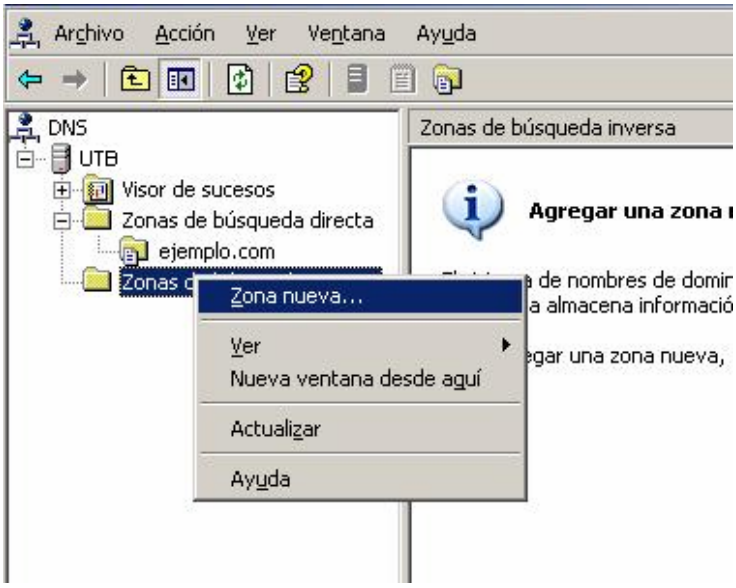


Figura 20 Creación de zona inversa

10. Creamos entonces una zona principal de actualización con el servidor.

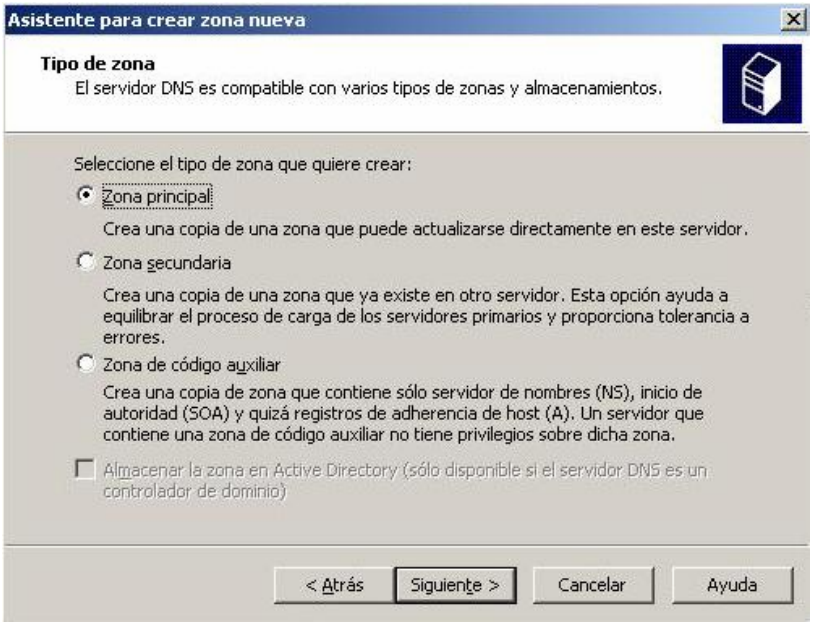


Figura 21 Determinación del tipo de zona inversa

11. Luego en la zona inversa colocamos la dirección de red, de los equipos que traducirá el servidor DNS, y luego se crean los archivos de zona; igual que en la anterior zona, se activan las actualizaciones de los equipos.

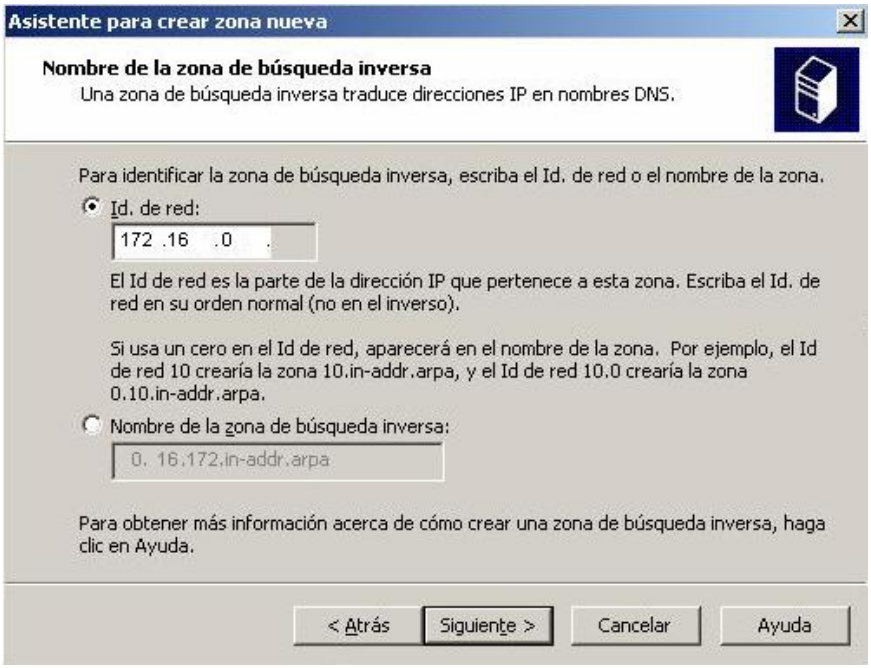


Figura 22 Especificación de nombre de zona inversa

12. De esta forma, luego de todas estas configuraciones, el asistente finaliza la creación de la zona inversa.
13. Luego utilizamos el asistente para la instalación del Active Directory que usaremos más adelante. Luego de unas ventanas iniciales, elegimos la opción para establecer el servidor como el nuevo controlador de dominio.

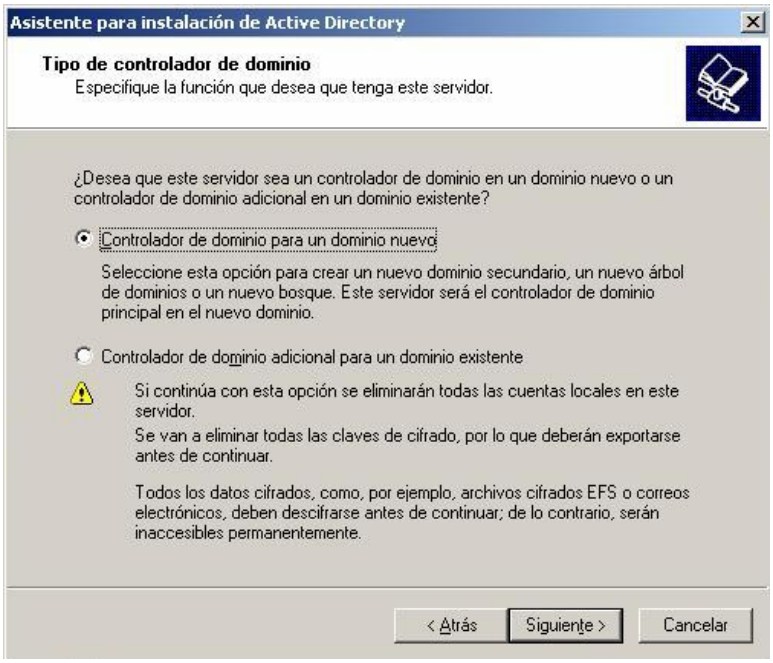


Figura 23 Determinación de función de controlador de dominio

14. Hacemos este, el dominio principal de la red que hemos configurado y colocamos el nombre del dominio que crearemos.

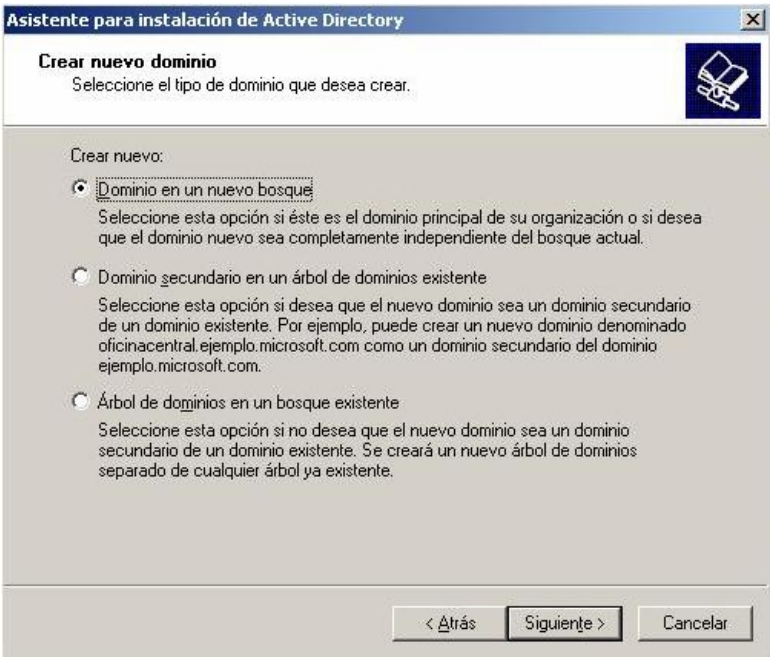


Figura 24 Establecimiento como dominio principal de la red

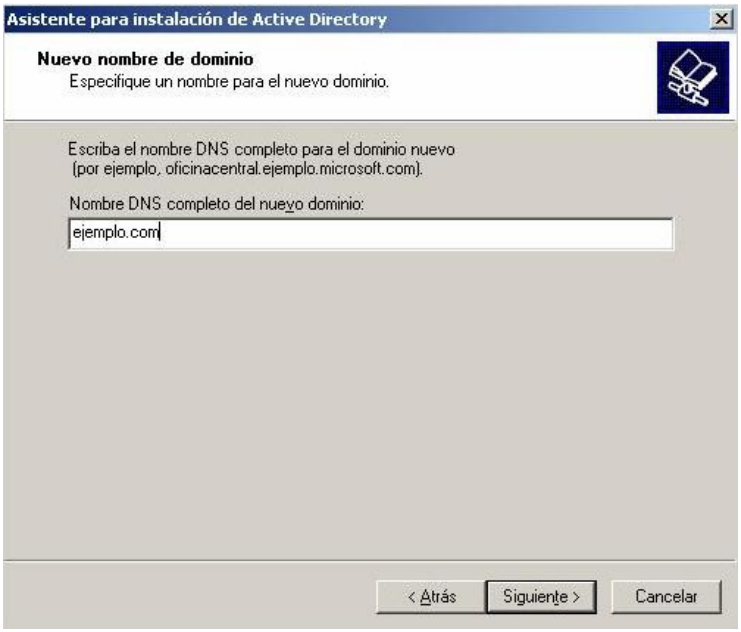


Figura 25 Establecimiento de nombre del dominio creado

15. Las otras ventanas, muestran la ubicación de los archivos de configuración., y por último se establecen los permisos a los usuarios dependiendo de la compatibilidad de su sistema operativo.

Figura 26 Determinación de permisos a usuarios

16. En este punto, finaliza la configuración del Active Directory, y podemos continuar con la creación de usuarios en nuestro dominio.
17. Utilizando la opción de Usuarios y equipos del Active Directory, se hace click derecho sobre el dominio y se hace click en Elevar nivel funcional del dominio.
18. Luego se escoge Windows Server 2003 y se eleva.
19. Igualmente se instala el servicio DHCP, agregando el componente a través del Panel de Control – Agregar o quitar programas – Agregar o quitar componentes de Windows. Allí en servicios de red, se escoge la opción de servidor DHCP y se habilita.
20. En la consola de DHCP, en Panel de Control – Herramientas administrativas, se click derecho sobre el dominio y se crea un nuevo ámbito. Además, se autoriza el servicio DHCP.
21. Cuando aparece la ventana del nombre de ámbito, se coloca el nombre que determinamos.

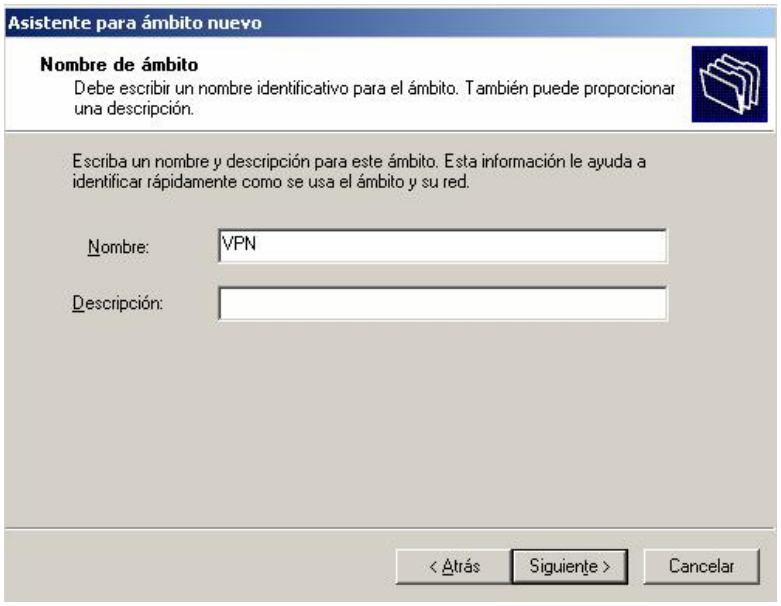


Figura 27. Nombre de ámbito a crear

22. Se hace click en Siguiente, y en la ventana mostrada se coloca el rango de direcciones IP que generará el servidor DHCP para los distintos equipos que hacen parte de la red. Para este efecto, la dirección IP inicial se consideró como la 172.16.0.2 y la final, 172.16.0.100.

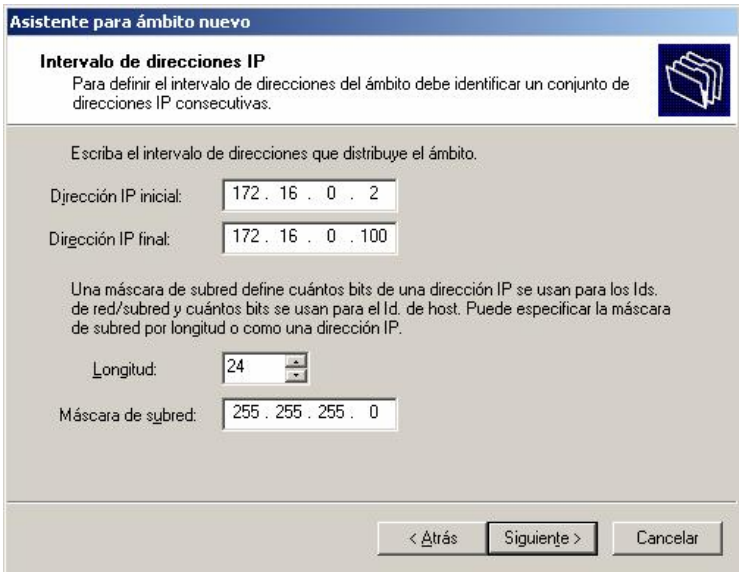


Figura 28. Determinación de rango de direcciones IP para asignación automática

23. Seguimos con el asistente y no configuramos las otras opciones, hasta que encontramos la ventana de Configuración de opciones DHCP, y se escoge la opción Sí, quiero configurar estas opciones ahora.

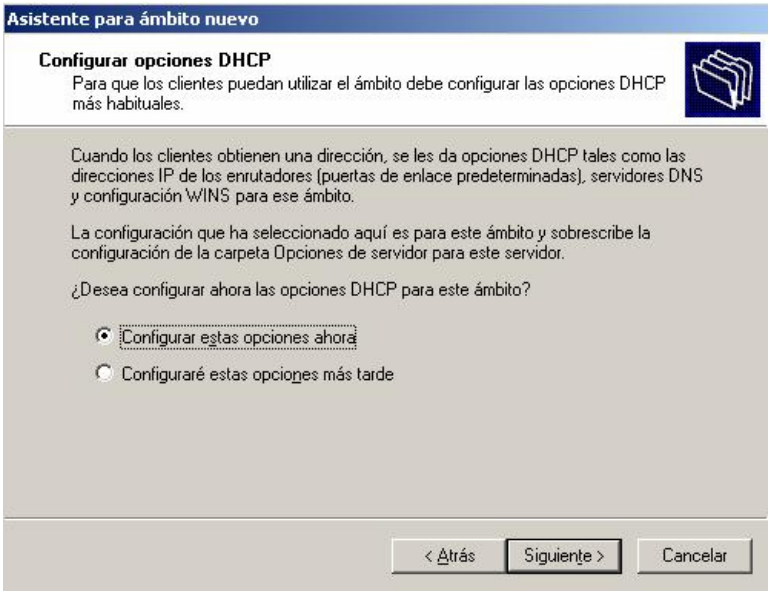


Figura 29. Configuración de opciones DHCP

24. Luego, se hace click en Siguiente y no se configura la opción de puerta de enlace por defecto. Es en la siguiente ventana, sobre servidores de nombre de dominio y DNS que se coloca el nombre del dominio que hemos escogido, en nuestro caso, *ejemplo.com*, y agregamos la dirección IP 172.16.0.1 que será la que maneje el servidor DNS.

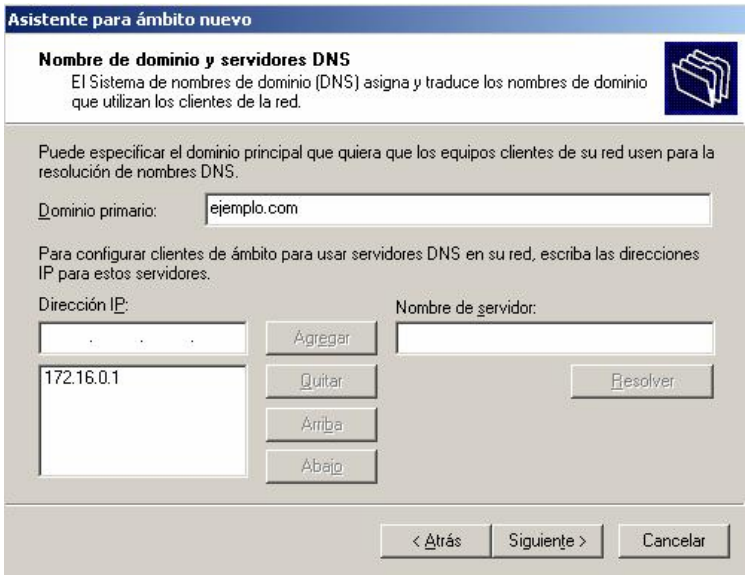


Figura 30. Especificación de servidores de nombre de dominio y DNS

25. Hace click en Siguiente y se pasa por alto la ventana sobre servidores WINS, puesto que no estamos configurándolos. En la ventana a continuación, se escoge la opción Sí, quiero activar el ámbito ahora.

Figura 31. Activar ámbito creado

26. Click en Siguiente, y aparece la ventana del asistente de nuevo ámbito completo. Se hace click en Terminar.

27. Luego se escoge la opción Usuarios y equipos del Active Directory y en la consola se expanden las opciones de nuestro dominio *ejemplo.com.*

28. Hacemos click en usuarios y luego en Equipo.

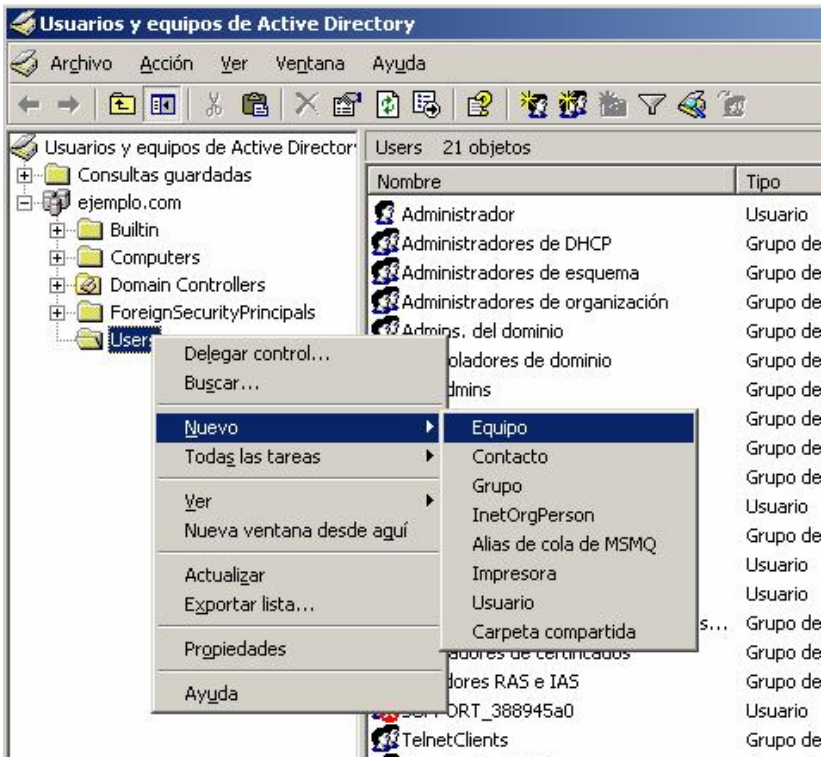


Figura 32. Creación de objeto Equipo en dominio ejemplo.com

29. En la ventana de diálogo del nuevo objeto, se coloca el nombre del equipo que se desea agregar a los usuarios del servidor.

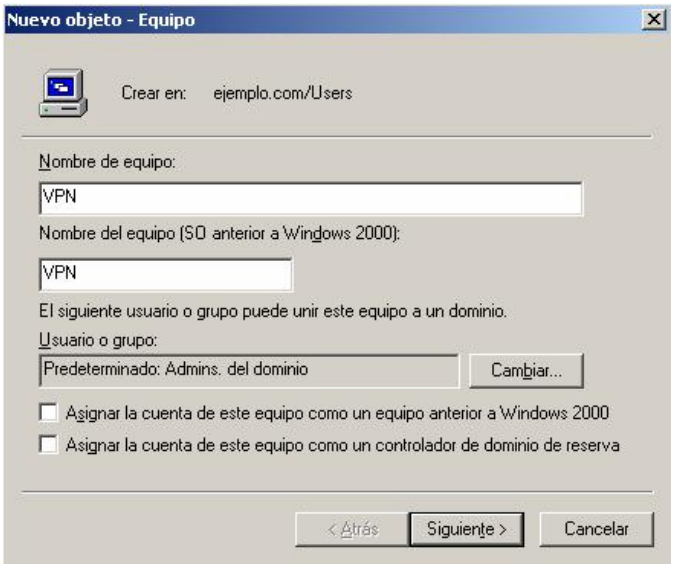


Figura 33. Crear un nuevo objeto (Computador)

30. Terminamos la configuración para este equipo, e igualmente lo hacemos con el cliente, y el servidor de archivos.

31. Además de este paso, volvemos a hacer click derecho sobre el dominio y nuevamente escogemos usuarios, y escogemos usuario.

32. Se coloca el nombre del usuario que se creará.

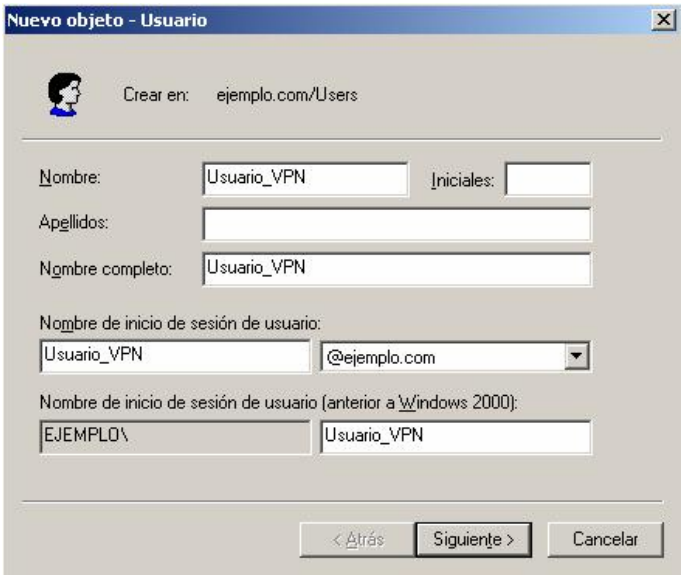


Figura 34. Crear un nuevo objeto (usuario)

33. Hacemos click en Siguiente. En la ventana continua aparece la opción de escribir la clave para acceder como ese usuario, y se especifica la característica de esta clave, que en nuestro caso es que nunca expira.

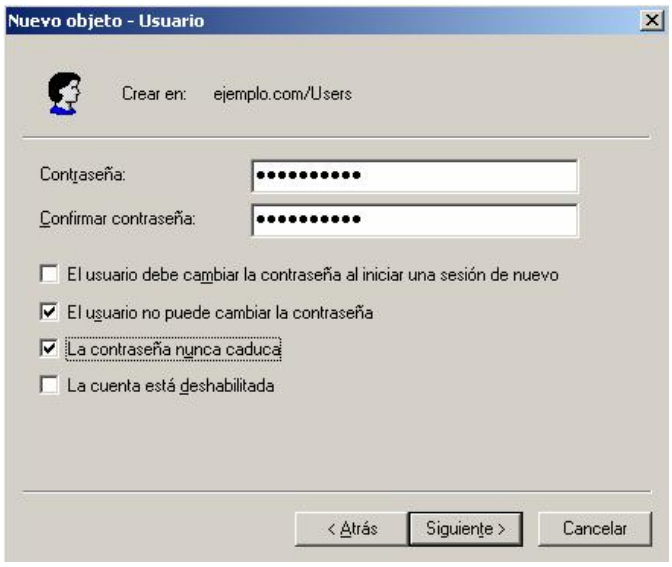


Figura 35. Establecer contraseña de usuario

34. Luego, hacemos click en Terminar, con el nuevo objeto creado.

35. Nuevamente, escogemos la opción usuarios, pero esta vez creamos un grupo.

36. En la ventana, colocamos el nombre del grupo, y le damos las opciones que consideremos necesarias.

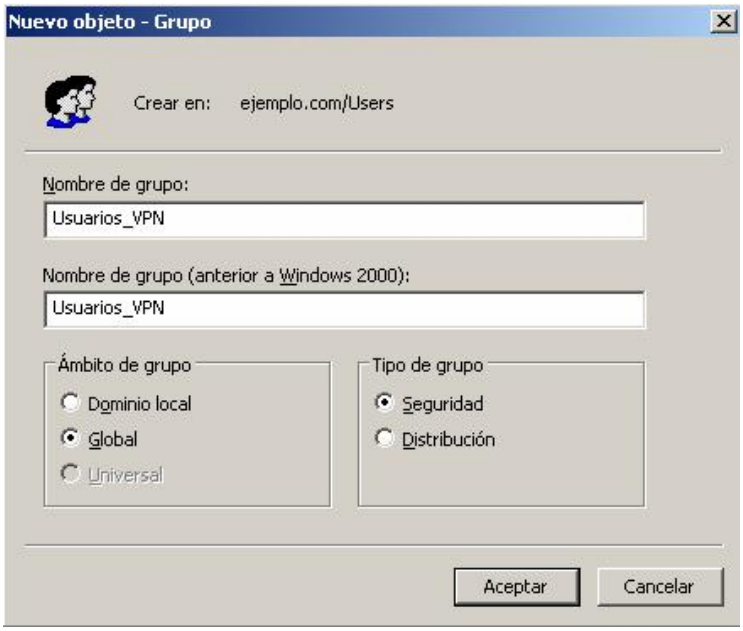


Figura 36. Crear un nuevo objeto (grupo)

37. En el panel detallado, se hace doble click sobre el grupo, y en la opción Miembros, se hace click en Agregar.

38. Escogemos el objeto que haremos miembro del grupo, escribiendo su nombre en la ventana, o buscándolo con la opción de Avanzadas.

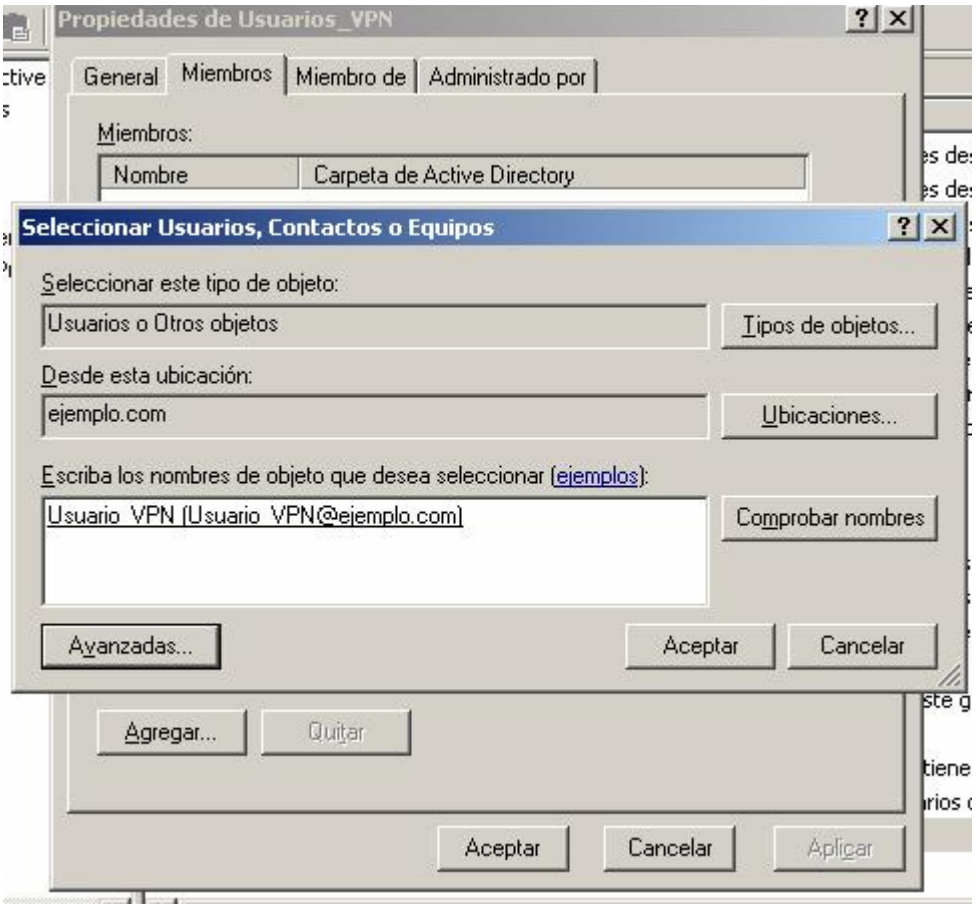


Figura 37. Selección de usuarios que pertenecerán al grupo

39. Continuamos la configuración y observamos como el usuario VPNUser que habíamos creado, es agregado al grupo que recientemente habilitamos.

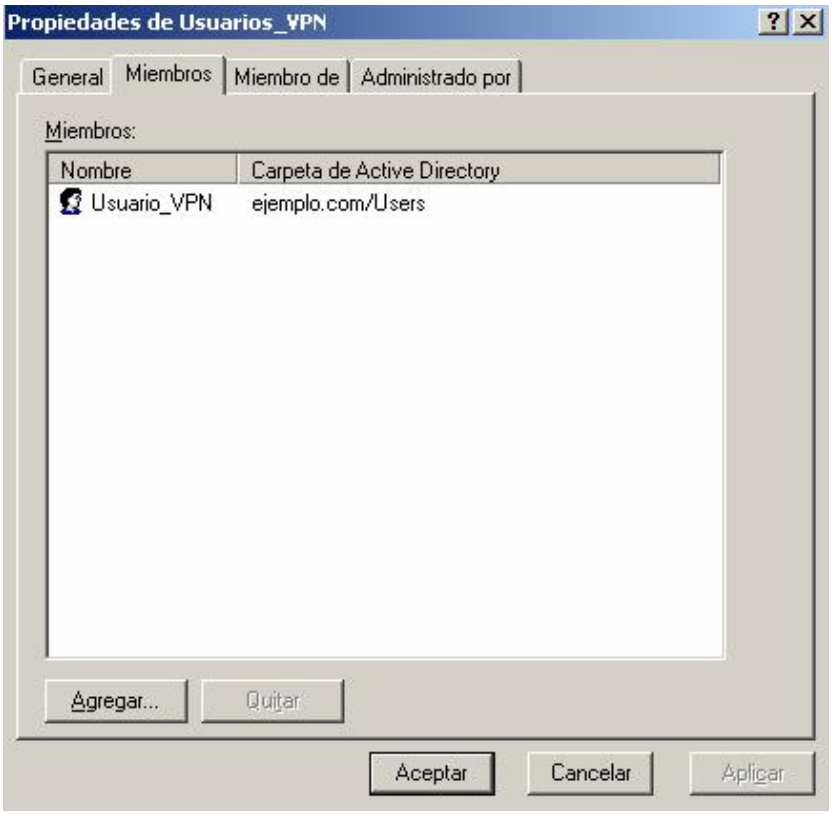


Figura 38. Usuarios miembros del grupo

27. Y luego terminamos para hacerlas actualizaciones en el nuevo grupo creado.

Así concluimos las configuraciones DNS y DHCP para el **Servidor II** de la Intranet.

3.3.2. Configuración del Servidor I

Ahora, la configuración del **Servidor I**, que va a ser quien esté haciendo las veces de servidor de archivos. Este servidor es un computador con el sistema operativo Windows Server 2003 instalado.

Para su configuración y habilitación, existen una serie de pasos:

1. Se instala el sistema operativo Windows Server 2003, y se hace miembro del dominio que estamos manejando, es decir, de *ejemplo.com.*
2. Se instala el componente de Windows IIS, perteneciente a Servidor de Aplicaciones en el Panel de Control.
3. En este equipo, utilizando el Explorador de Windows se crea una nueva carpeta compartida, que tendrá los permisos por defecto, y a la cual accederá nuestro cliente.
4. Si está trabajando bien el archivo compartido, se verifica en Inicio – Ejecutar – \\Nombre_maquina\Nombre_archivo, y listo. Esto debe permitir ver la información que fue compartida.

Así entonces, hemos configurado nuestro servidor de archivos.

3.3.3. Configuración del Servidor III

Ahora, el servidor más importante, puesto que es el centro de atención del proyecto será configurado: **Servidor III**.

Los requerimientos que precisa este equipo son esencialmente los siguientes:

- 2 tarjetas de red
- 1 dirección IP para realizar la conexión del servidor VPN a Internet. En nuestra prueba, trabajamos con una IP que para efectos del piloto nos permitió simular la red de Internet.

- 1 dirección IP fija para la tarjeta que se conectará a la Intranet.
- Instalar el sistema operativo Windows Server 2003.

Pasos para configuración:

1. Inicialmente hacemos uso del asistente para la instalación del servidor de enrutamiento y acceso remoto, seleccionando la opción de red privada virtual.

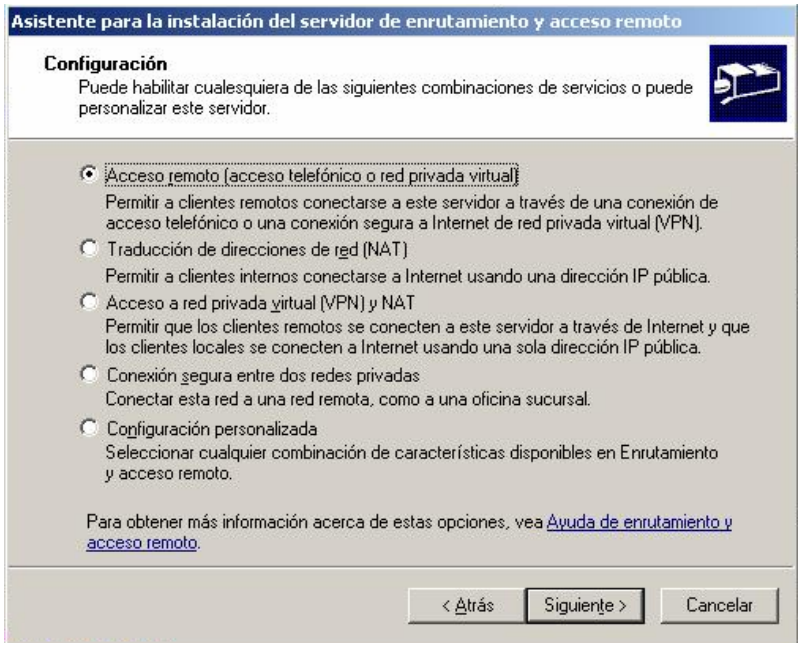


Figura 39 Configuración de servicio de acceso remoto a través de VPN

2. Se define la conexión que se quiere establecer.

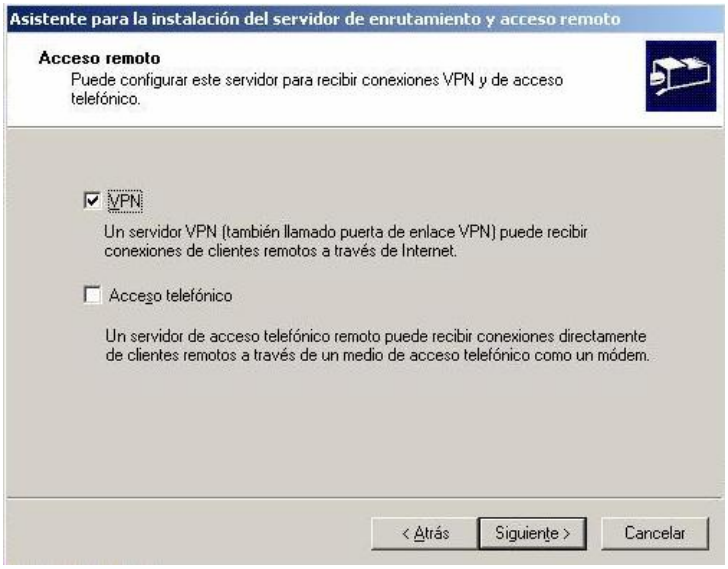


Figura 40 Tipo de conexión de acceso remoto

3. Se selecciona la tarjeta de red que estará conectada a la Internet que contacta al cliente. Se asignan y verifican las direcciones IP, siendo automáticamente en los clientes su determinación.

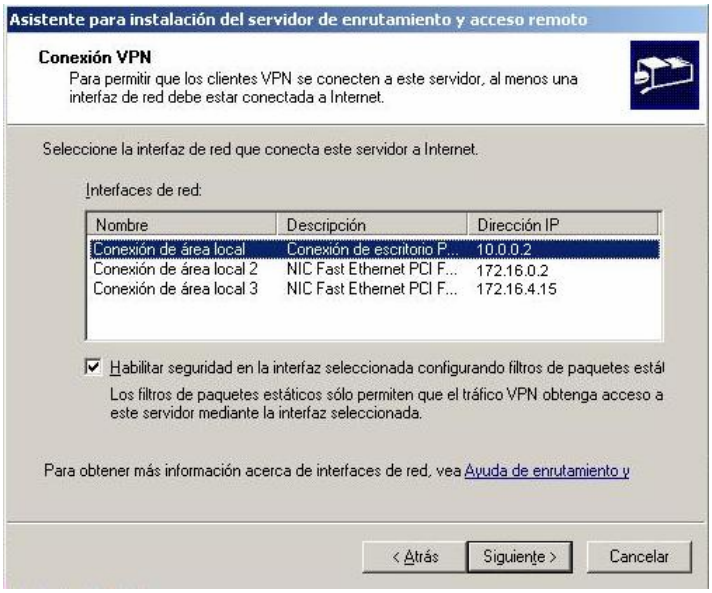


Figura 41 Determinación de tarjeta de red habilitada para conexión a Internet

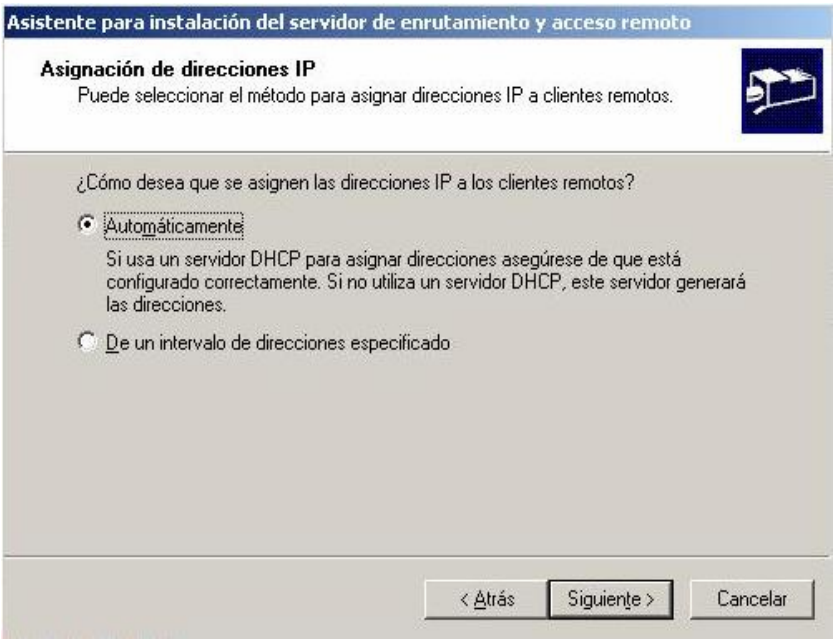


Figura 42 Especificación de asignación de direcciones IP a clientes remotos

4. Se establece la autenticación a través del mismo servidor de enrutamiento y acceso remoto, para los clientes.

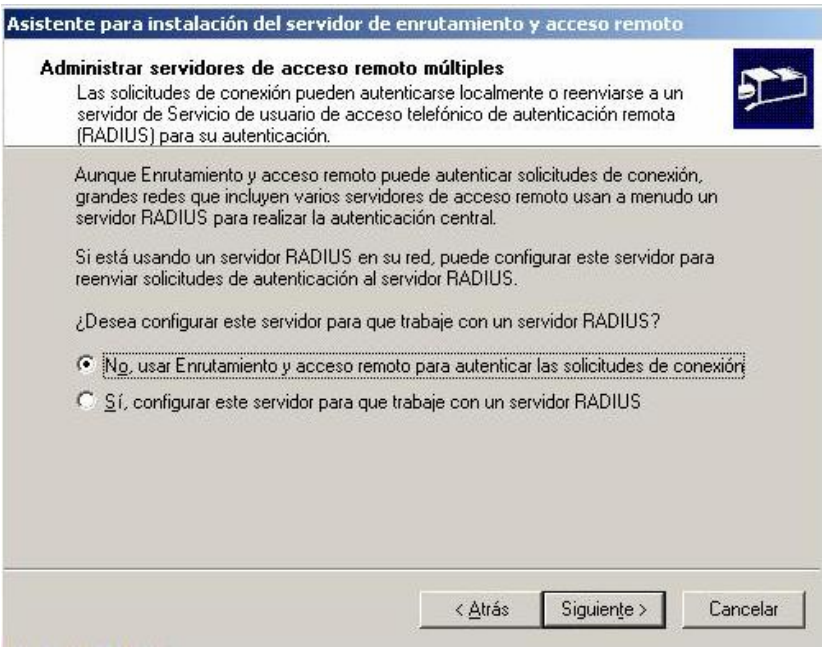


Figura 43 Servidor de autenticación para clientes

5. Luego en la consola, logramos observar que una flecha verde sobre nuestro servidor indica que éste está habilitado para trabajar, y se realizan varias configuraciones en el servidor que permitirán establecer las políticas que se utilizarán para su manejo.
6. Inicialmente se establece la Seguridad VPN donde se permite que las conexiones entrantes sean autentificadas, autorizadas y protegidas, al realizarse. Esto se puede implementar a través de la opción Directivas de acceso remoto de la consola, la cual posee por defecto dos reglas ya establecidas. Lo que se hará es crear una nueva política de acuerdo a las propias necesidades, y se borran las anteriores. Con un click derecho sobre las reglas, se eliminan, y click derecho sobre Políticas de acceso remoto, se crea una Nueva regla.

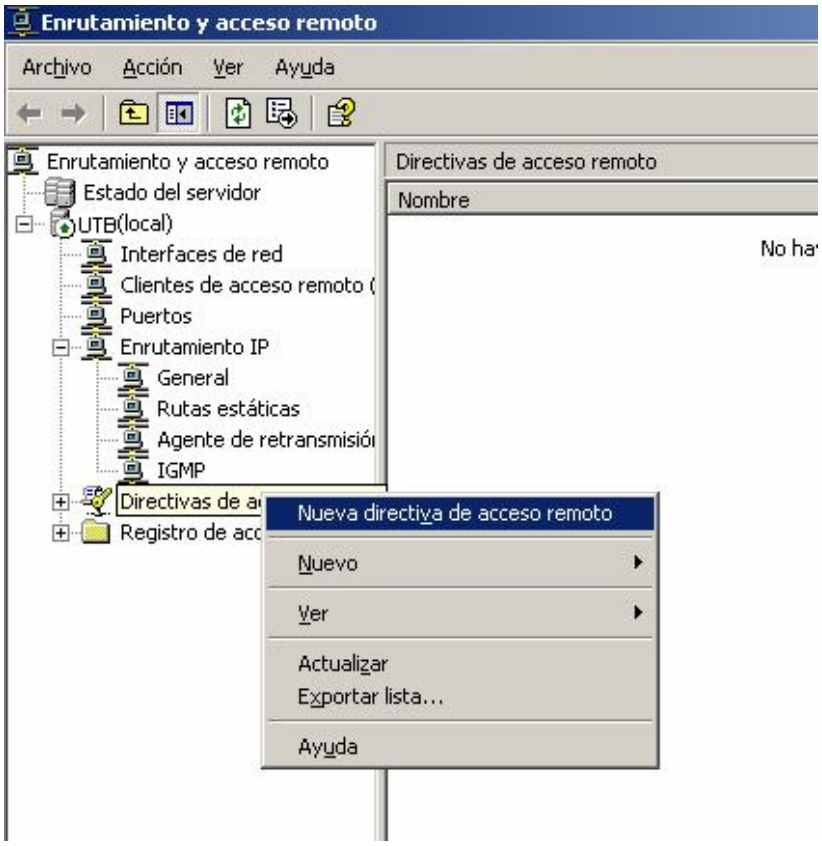


Figura 44. Creación de políticas de acceso

7. En el asistente que se presenta se configura una regla típica y le se le coloca un nombre que la logre identificar cuando se aplique.

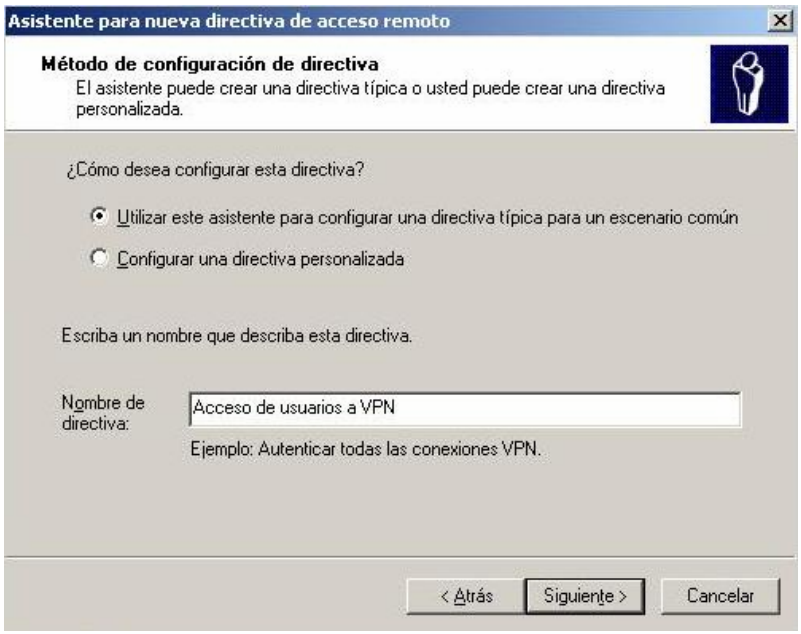


Figura 45. Asignación del nombre de la política a crear

8. En una ventana subsiguiente se muestran las posibles políticas de acceso, en la cual se escoge la interesada: VPN.

Figura 46. Especificación del método de acceso VPN

9. Se escogen los usuarios que pueden acceder al servicio y se agregan usuarios o grupos según el interés.

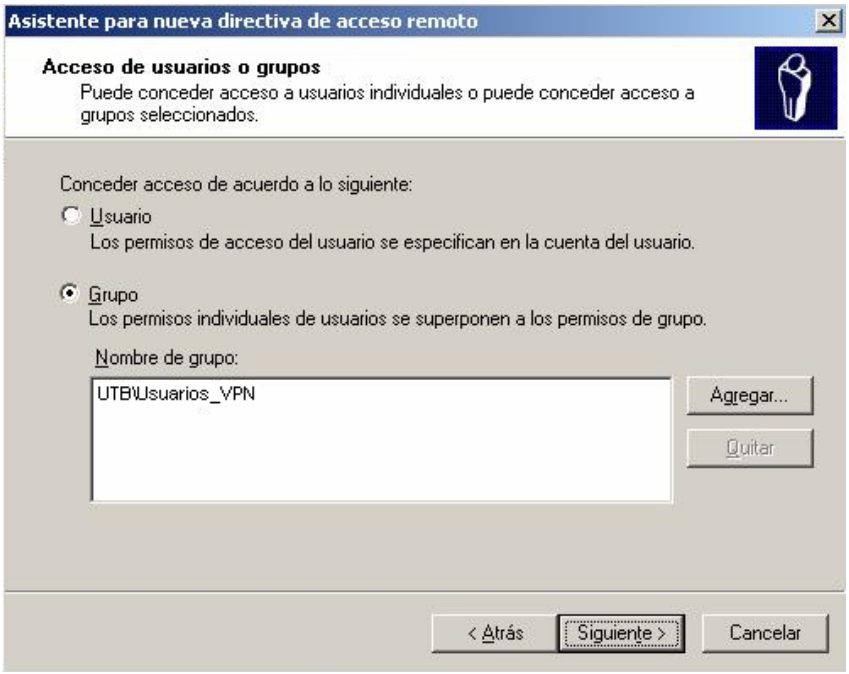


Figura 47. Concesión de acceso usuarios o grupos

10. Luego se presentan las opciones de escoger tanto el protocolo de encriptación, como el nivel que éste maneje. En este caso, se escoge el Microsoft Encrypted Authentication version 2 (MS-CHAPv2), que permite autentificar conexiones VPN. Y además, se selecciona el mayor nivel de encriptación.

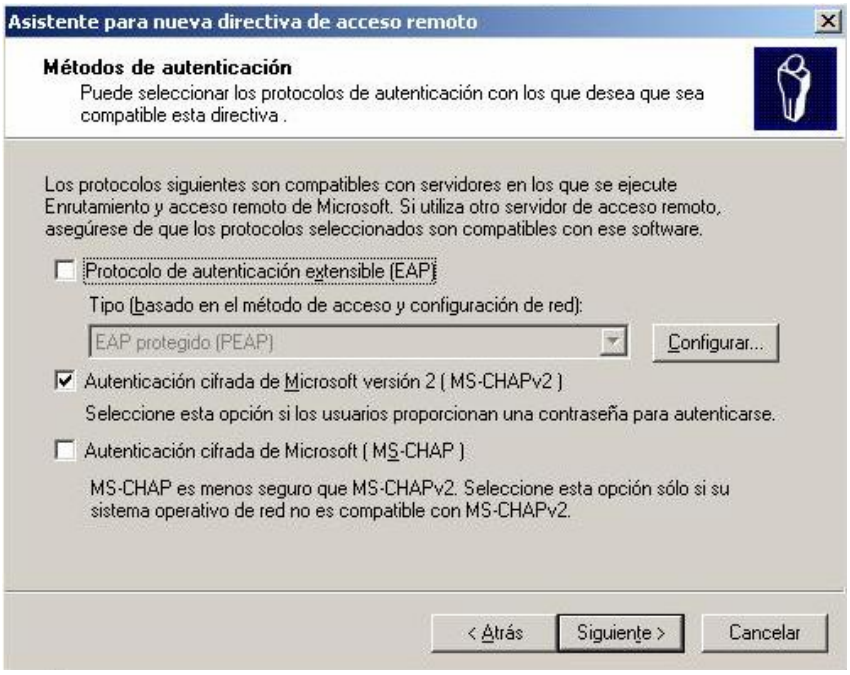


Figura 48. Selección de protocolo de autenticación

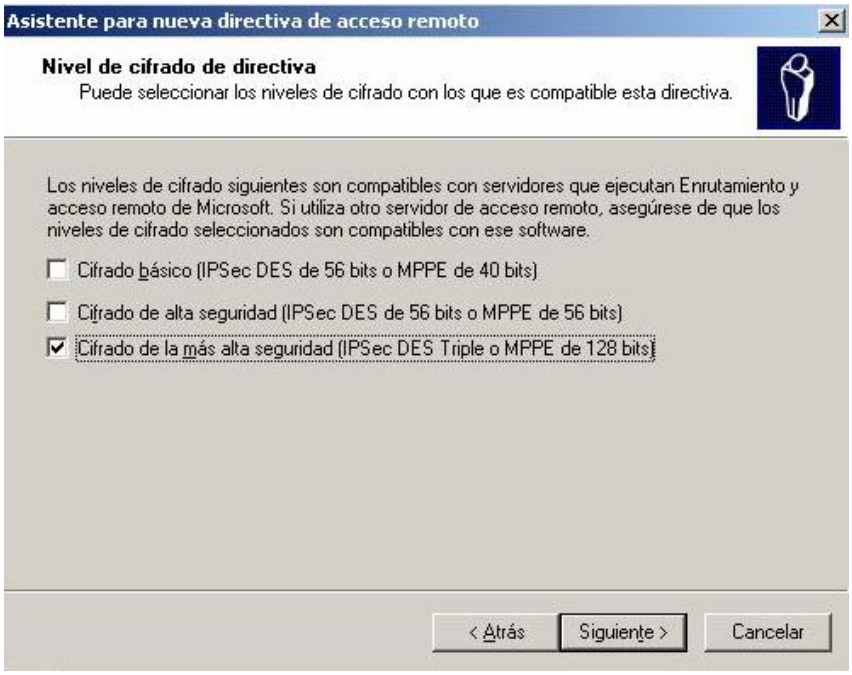


Figura 49. Selección de nivel de encriptación

11. En la consola al finalizar toda esta creación, nos muestra la regla que acabamos de configurar.

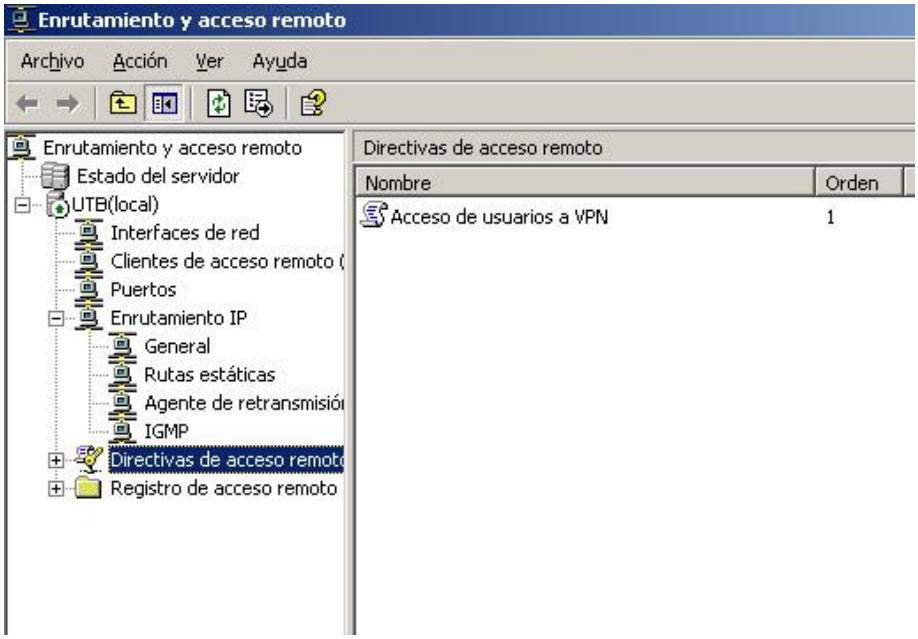


Figura 50. Vista de políticas creadas para el acceso al servidor VPN

12. Otra de las configuraciones es la de cantidad de conexiones concurrentes que se trabajarán. Para efectos de la prueba sólo se aplicaron 5 conexiones concurrentes. Para configurar la puerta se hace click derecho en Puertos y se seleccionan Propiedades.

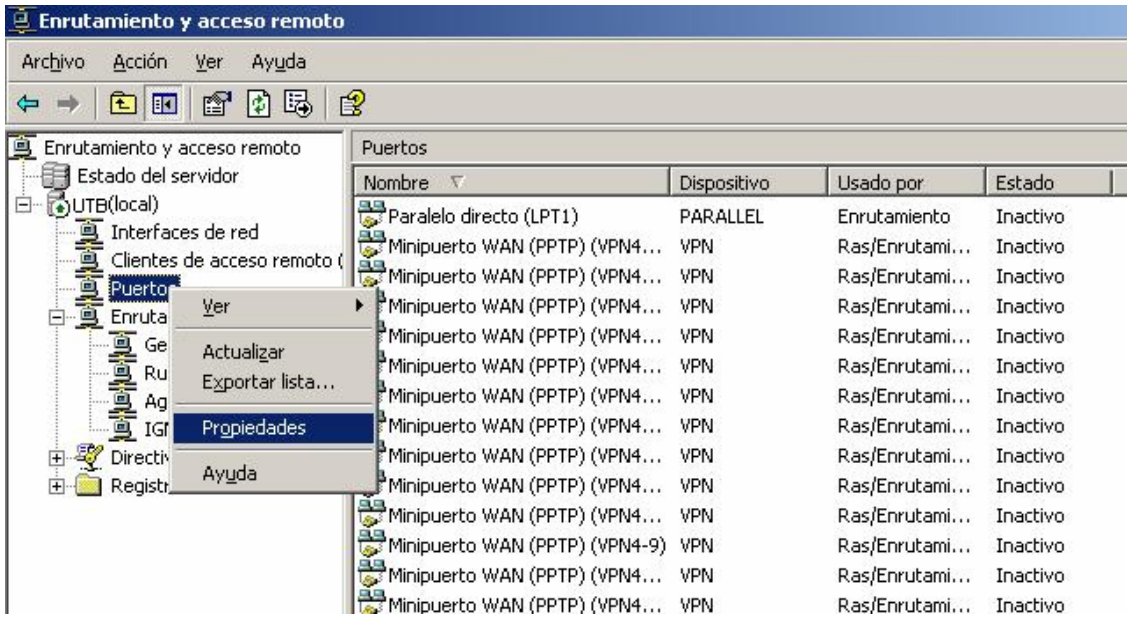


Figura 51. Verificación de puertos para conexión de clientes

13. En esta ventana se muestran los tipos de puertos que se habilitan y la cantidad que existe de ellos. Se escoge el puerto, en este caso el PPTP y se inicia la configuración, donde se especifican el número de conexiones y las conexiones que se pueden permitir.

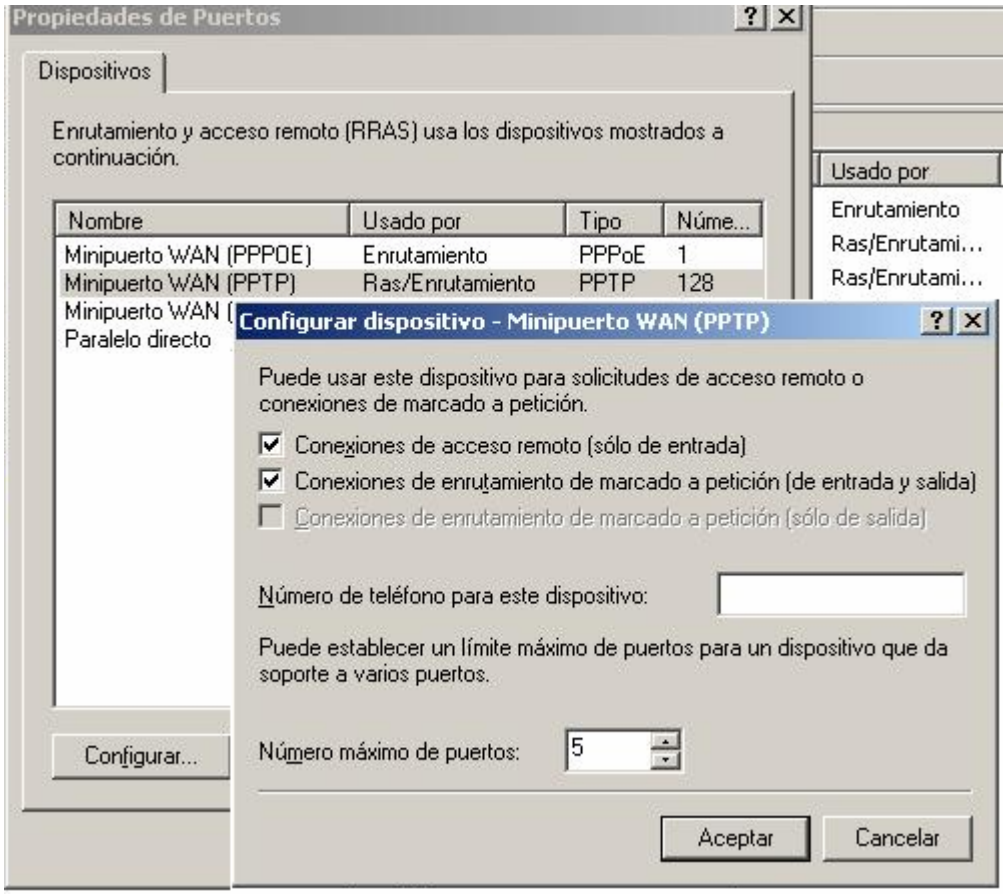


Figura 52. Selección de dispositivos y establecimiento de conexiones concurrentes habilitadas

14. En la ventana final se pueden ver los cambios que se realizaron y que permitirán el acceso de los clientes.

15. Otra configuración pertinente es para el seguimiento de las conexiones permitidas, como mecanismo de seguridad. Para esto, se hace click derecho en el servidor, y en Propiedades, se selecciona la pestaña referente al Inicio de Sesión, y se habilita la opción de registro de errores y advertencias.

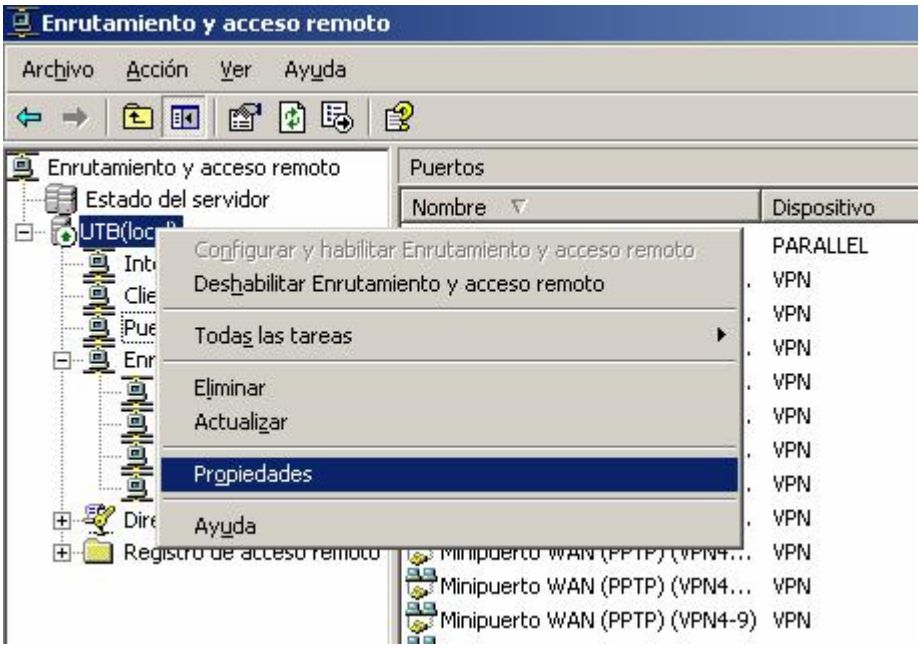


Figura 53 Configuración de propiedades del servidor VPN

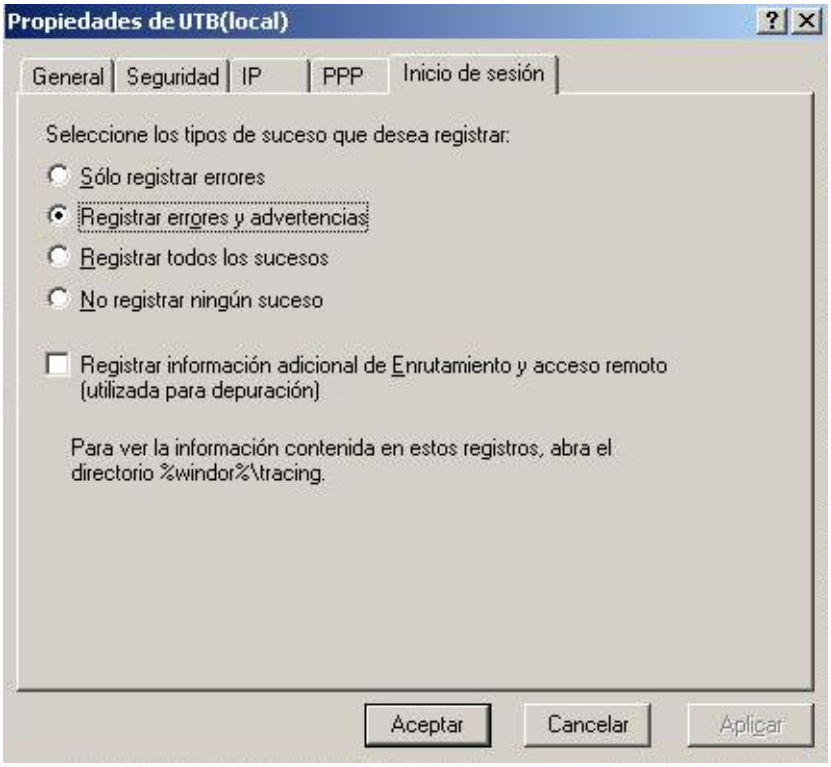


Figura 54. Registro de eventos durante la conexión

16. Como siguiente paso, se escoge en la última opción de Acceso Remoto de la consola principal con un doble click en Archivo Local, la ventana permite configurar la información a realizar el seguimiento. Y luego se configura el lugar en el disco donde se quiere guardar el archivo de seguimiento. Finalmente, se ha realizado la configuración del seguimiento satisfactoriamente.

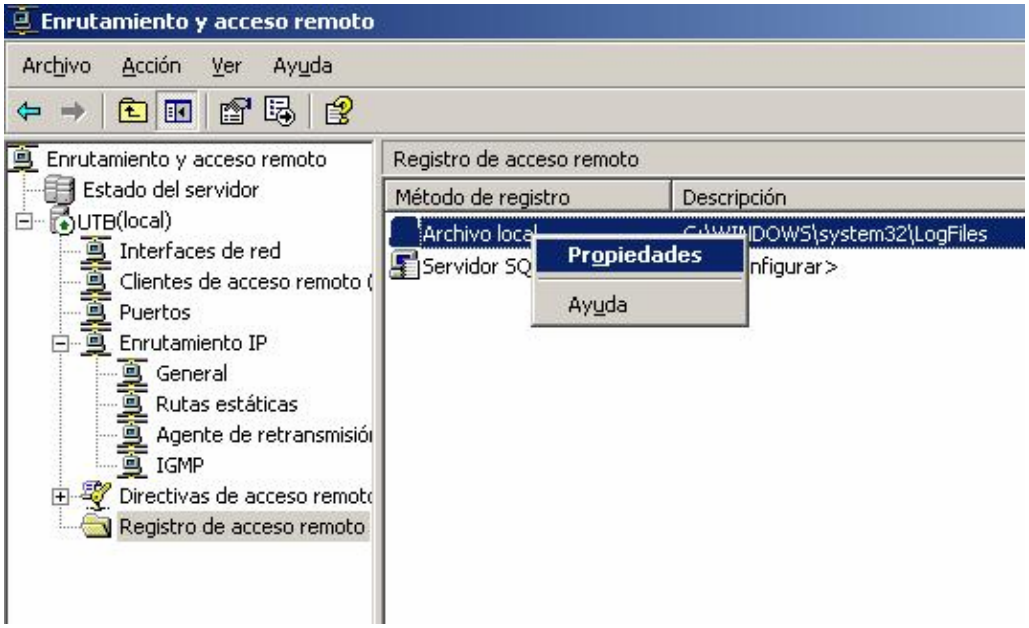


Figura 55 Configuración de propiedades del archivo local

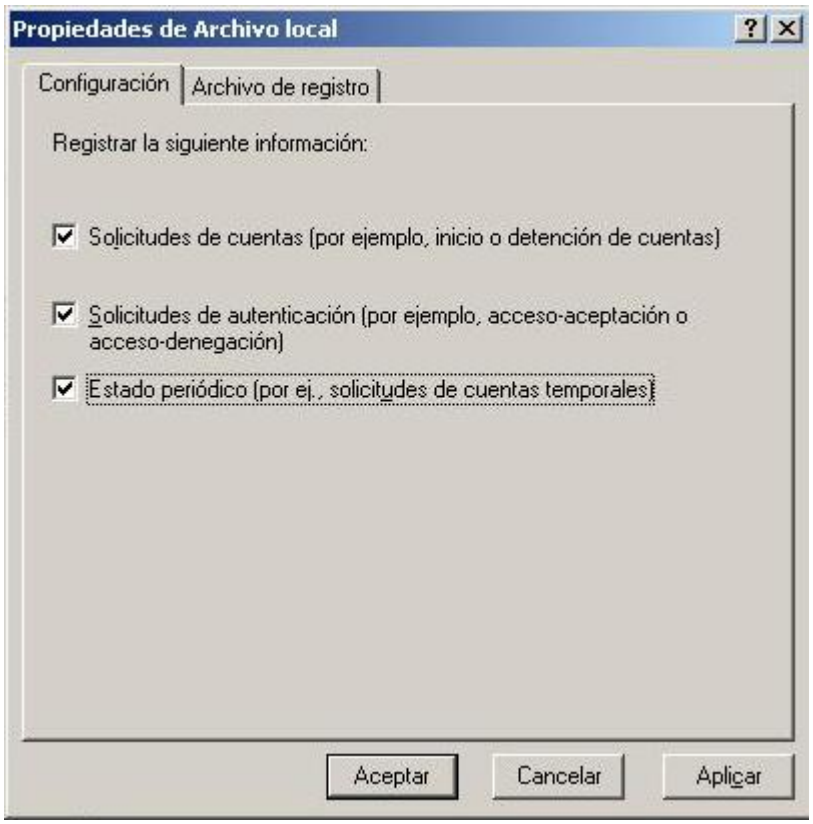


Figura 56. Selección de tipo de información en el registro

17. Igualmente, se realizan las configuraciones que corresponden al archivo de registro.

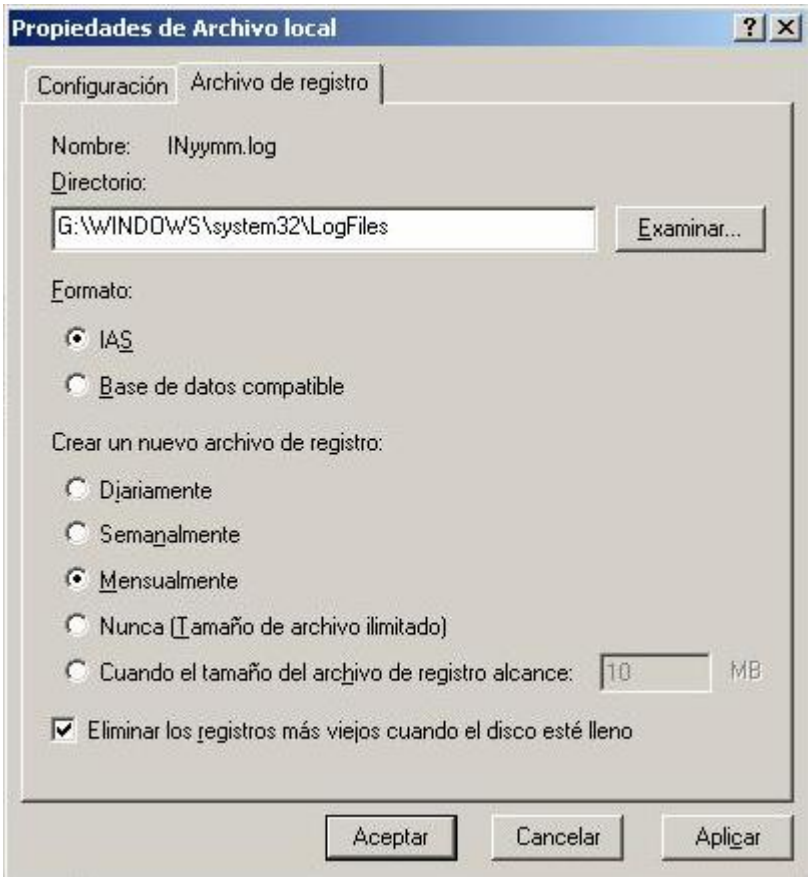


Figura 57 Propiedades del archivo de registro

18. Una nueva configuración a realizar será la de permisos para los usuarios. Para este efecto, en la consola se hace click derecho sobre el usuario y se escogen sus Propiedades.

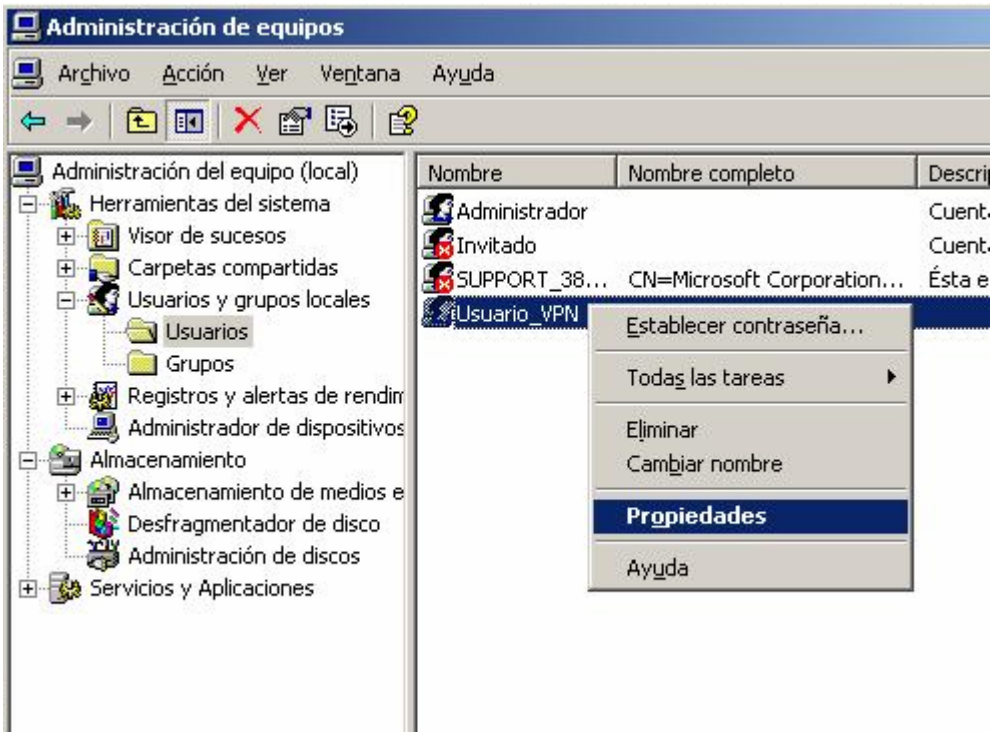


Figura 58. Determinación de permisos para cada usuario

19. En la pestaña de Marcado, se escoge el control a través de la política que anteriormente se creó y que permitirá conectarse al cliente con el servidor.

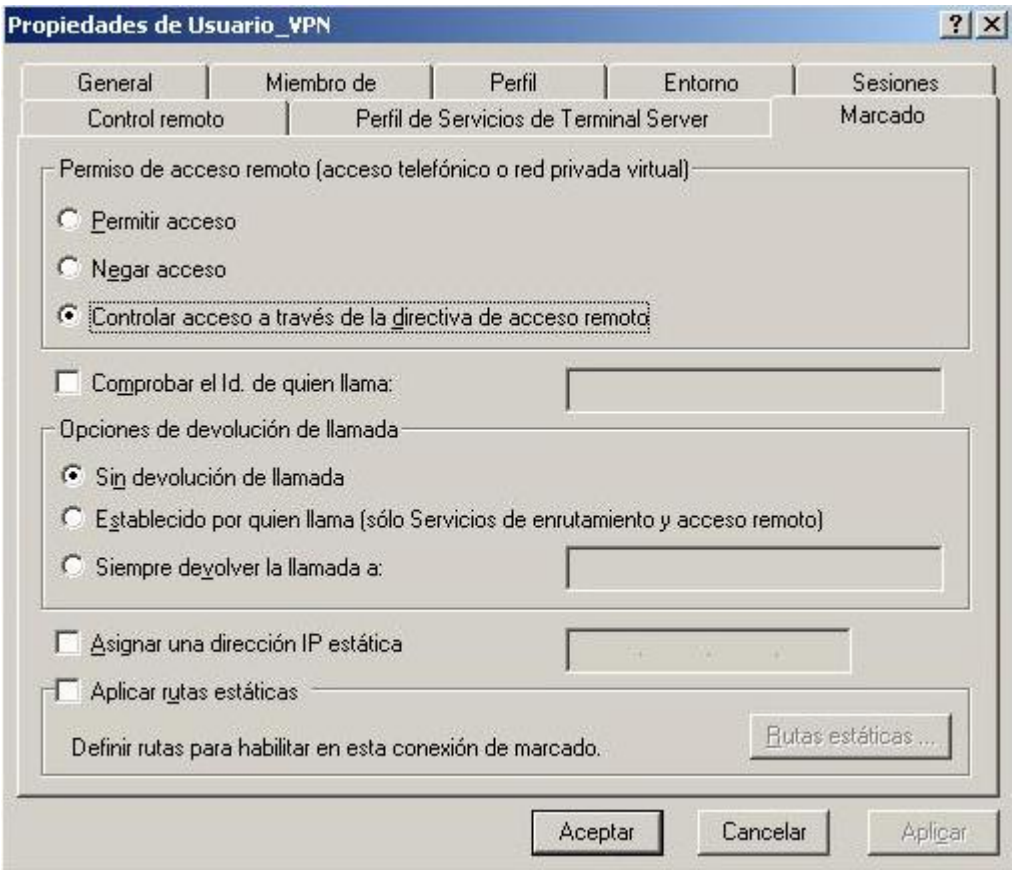


Figura 59. Control de acceso y establecimiento de permisos para usuarios

Así se ha logrado configurar el servidor VPN, y lo que haría falta es establecer la configuración del cliente que queremos conectar con la red.

3.3.4. Configuración del Cliente

El cliente que se conectará al servidor de archivos a través del servidor VPN, tendrá una estructura de conexión específica para permitir el acceso de éste a la información usando la herramienta de VPN.

Pasos para la configuración del **Cliente**:

1. Inicialmente se va al Panel de Control -- Conexiones de Red -- Asistente para nueva conexión. Se elige entonces la conexión que permita acceder a través de una VPN y se hace click en Siguiente.

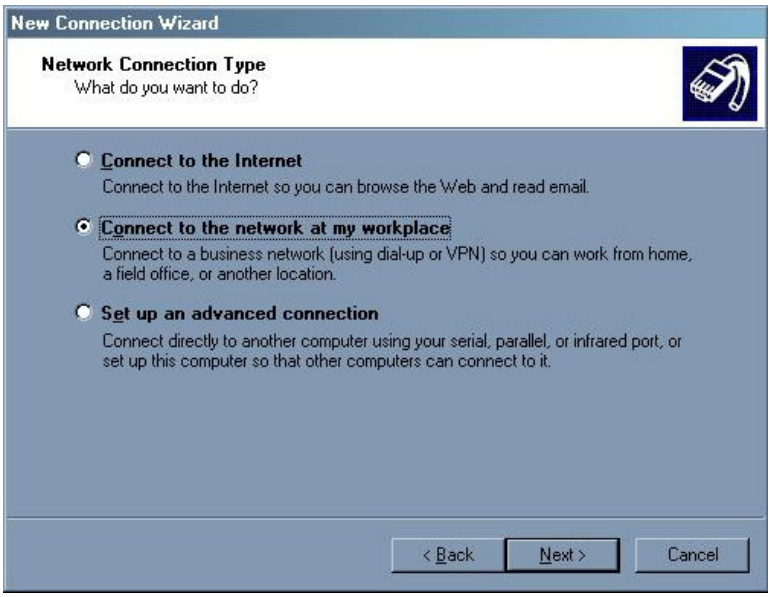


Figura 60. Tipo de conexión a establecer

2. La ventana nueva muestra el tipo de conexión que se establecerá como VPN para efectos de la prueba.

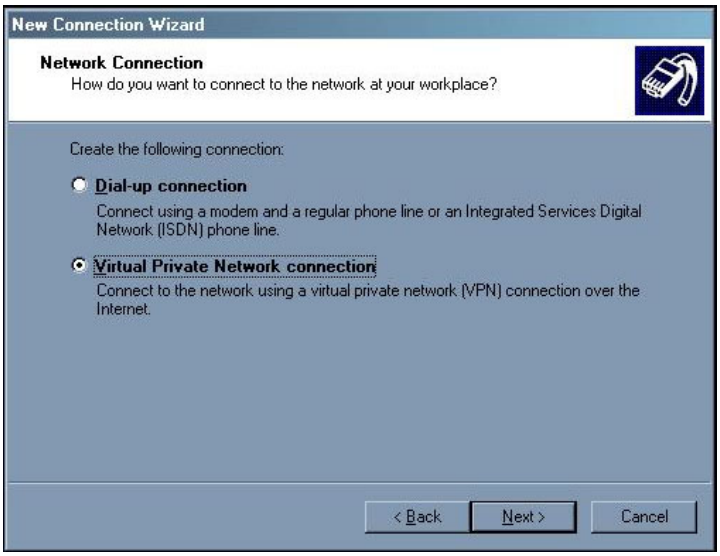


Figura 61. Creación de conexión a través de VPN

3. Luego se coloca el nombre de la conexión que se está configurando. Además, en la siguiente ventana se pide la IP o el nombre del host al que se desea conectar, en cuyo caso será el de la conexión a Internet del servidor VPN.

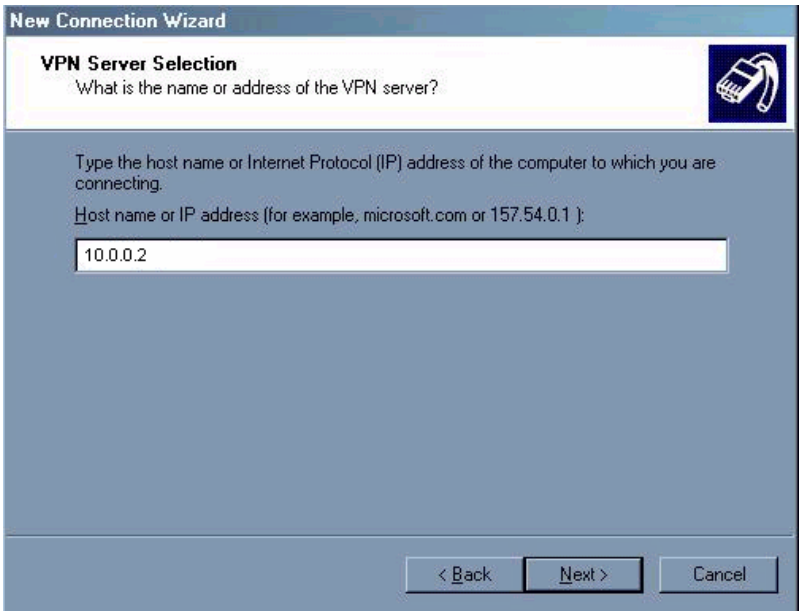


Figura 62. Selección del servidor VPN al cual conectarse

4. En la disponibilidad de la conexión se establece para uso personal, si el computador no es propio, para evitar así el acceso de usuarios no autorizados a la VPN. De esta manera se crea la conexión nueva a través de la VPN en el cliente. Cuando se hace click en Finalizar, enseguida se muestra la ventana para la conexión.

Figura 63. Conexión automática para la VPN

5. Se coloca el usuario que se creó para la VPN con la clave establecida y se inicia la conexión con el servidor.

Figura 64. Nombre de usuario y contraseña para acceder al servidor

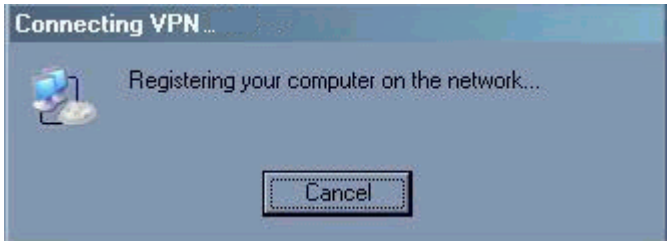


Figura 65. Ventana de conexión y registro del equipo en la red

Figura 66. Ventana de conexión a la VPN habilitada

6. En la consola principal se muestra la conexión del cliente remoto.

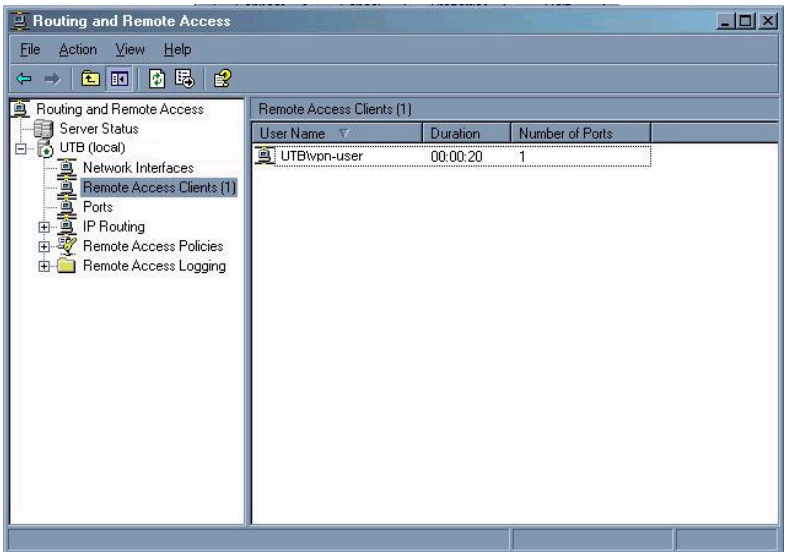


Figura 67. Registro de usuarios conectados al servidor VPN

De esta manera hemos terminado de configurar nuestro cliente y está listo para la conexión al servidor que se encuentra en la Intranet.

Esta prueba nos permite verificar la posibilidad de realizar conexiones del tipo VPN, con lo cual podemos iniciar alguna propuesta para implementarlo en la red de la Universidad Tecnológica de Bolívar, de acuerdo a las necesidades que se tengan y la disponibilidad de recursos con que cuente la institución.

4. CONCLUSIONES

El desarrollo de este trabajo de investigación ha permitido profundizar en conocimientos y experimentar físicamente con las Redes Privadas Virtuales (VPN), principalmente con las implementaciones en el sistema operativo Windows Server 2003.

Gracias a estos desarrollos se ha logrado concluir una vez más que las Redes Privadas Virtuales, son herramientas eficaces para la interconexión de equipos remotos, con un intercambio seguro de información que puede ser altamente confidencial.

Además, permiten ahorrar considerablemente dinero y esfuerzo en la construcción física de una infraestructura que permita enlazar dos redes lejanas geográficamente. Su implementación basada en el uso de una gran red ya constituida, Internet, le hacen una de las soluciones más apetecidas por el mercado empresarial para satisfacer sus necesidades de interconexión y seguridad.

Está de más, decir que en el ámbito universitario tiene aplicaciones válidas y que no generarán más gasto que el de los equipos necesarios para poner en marcha el diseño y montaje de la red.

Igualmente, estos conceptos permiten diferenciar las ideas de Red Privada y de Red Privada Virtual, haciéndose notoria su discrepancia por el concepto físico que ambas manejan: mientras que una Red Privada requiere expresamente interconexión física entre sus equipos, una Red Privada Virtual obvia este paso y utiliza un medio como la Internet, para realizar la conexión entre clientes y servidores.

Aunque las ventajas de las Redes Privadas Virtuales estén puestas sobre la mesa, con unas pocas desventajas, es una realidad que profundizará, igual que el concepto de red, en cada una de las pautas tecnológicas que rigen actualmente a las empresas e instituciones mundiales, pero por supuesto, POCO A POCO.

5. RECOMENDACIONES

Con respecto a las consideraciones de configuración e implementación de la red, recomendamos tener un esquema inicial sobre la topología que se desea desarrollar, lo cual permitirá tener una visión más amplia de los recursos que se requieren y las herramientas que faltan para poder lograr el establecimiento de la red sin contratiempos e interrupciones.

El servidor que se utilizará para trabajar la VPN, debe contar con dos tarjetas de red que manejen una misma velocidad de conexión. Se presentan algunos problemas para la visualización de las redes, si este punto no se considera. En este caso donde las velocidades manejadas son distintas, un ping entre los dispositivos de la misma red es posible, pero sólo con una de ellas, o la Intranet o la Internet. De otra forma, no es reconocido el dispositivo.

Con respecto a la configuración del servidor DNS, es importante que se lleve a cabo un *nslookup* para realizar la verificación de una configuración correcta, y que permita el manejo de los nombres de los equipos que pertenecen al dominio establecido.

No debe olvidarse, poner en marcha los servidores, principalmente el DHCP ya que sin éste es imposible que los dispositivos puedan obtener una dirección IP para conectarse a la red.

Con respecto a posibles usos, consideramos que este trabajo de investigación puede tener muchas aplicaciones, principalmente en nuestra institución universitaria.

Además de que permite la conexión segura a una red interna, puede permitir tanto a estudiantes como profesores valerse de este recurso para interactuar en la actividades académicas.

Muchas veces, es difícil la comunicación para envío de trabajos, talleres, tareas, etc.; esta sería una interesante solución virtual para aplicar. Con la disponibilidad de un servidor de archivos, los estudiantes y profesores podrían acceder a la información que compartan, sin que necesariamente alguien desconocido pueda ver también su información, situación que puede ocurrir muy a menudo en el envío de datos a través de la Internet.

Otra de las aplicaciones que consideramos como válidas, es para que los profesores mantengan un servidor disponible para ellos, o puedan acceder a la red en busca de información y que no necesariamente deban movilizarse hasta ella.

Recomendamos, tener en cuenta todos estos aspectos tratados, y hacer uso de ellos para la evolución de nuestra institución universitaria hacia la virtualización con seguridad.

6. GLOSARIO

A

AES (Advanced Encryption Standard): Es un algoritmo de cifrado por bloques destinado a reemplazar al DES como estándar.

AH (Authentication Header): Uno de los métodos usado por IPSec para brindar seguridad a los paquetes que se envían a través de Internet, autenticándolos, mediante la firma digital, con el fin de asegurar la identidad del emisor y del receptor.

ATM: Modo de transferencia asíncrona. Una conexión ATM, consiste en "celdas" de información contenidos en un circuito virtual (VC).

ATMP (Ascend Tunnel Management Protocol): Es un protocolo actual que permite conectarse a un software cliente y contactarse con un usuario remoto de una red doméstica.

Autenticación: Proceso para verificar que un objeto o entidad sea lo que dice ser. Aquí se confirma su origen e integridad de la información, como la firma digital o la identidad del usuario.

C

CHAP (Challenge-Handshake Authentication Protocol): Protocolo que ofrece un gran nivel de seguridad, debido a que la contraseña no viaja

ni siquiera cifrada durante la sesión PPP. Esto se logra mediante el mecanismo que este protocolo implementa que es a través de un mensaje de desafío, compuesto por un Id de Sesión y una cadena arbitraria (desafío), al cual el cliente debe responder con MD5 (id_sesión, desafío, password) y nombre de usuario y esto coincidir con la operación que hace el servidor.

Cortafuegos (Firewalls): mecanismos de protección contra accesos no autorizados procedentes de Internet.

D

Demonio: Es un programa que no está invocado explícitamente, pero duerme esperando que alguna condición ocurra.

DLSW (Data Link Switching): Surgió de la idea de IBM de transportar el tráfico NetBios y SNA (Sistema de arquitectura de red) a una red IP.

E

ESP (Encapsulating Security Payload): Protocolo que encripta y/o autentica datos

F

Filtrado: Software que extracta el contenido y las propiedades de un documento para clasificarlos.

Frame Relay: Es un estándar que se basa en la división de datos en paquetes para luego enviarlos a través de la WAN. Sus características principales son el manejo de circuitos virtuales y que es orientado a conexión.

FreeS/WAN (Free Secure WAN): Software que permite implementar de manera gratuita IPSec e IKE para sistemas GNU/Linux.

G

Gateway: Puerta de enlace.

GNU (General Public License): Es una parte de UNIX, no UNIX y se pronuncia “guh-New”.

GRE (Generic Routing Encapsulation): Es una cabecera que se usa para encapsular el paquete PPP dentro de un datagrama IP

H

HDLC: Control de enlace de datos de alto nivel. Es un protocolo de la capa de enlace de datos que se deriva del protocolo de encapsulamiento de control de enlace de datos síncrono (SDLC). No usa ventanas ni control de flujo y sólo se permiten las conexiones punto a punto.

I

IKE (Internet Key Exchange): Negocia los parámetros de conexión, incluyendo llaves.

IPSec (Internet Protocol Security): Es un protocolo de seguridad creado para establecer comunicaciones que proporcionen confidencialidad e integridad de los paquetes que se transmiten a través de Internet.

IPX: Es un protocolo no orientado a conexión que no requiere acuses de recibo para cada paquete (entrega de máximo esfuerzo).

ISAKMP (Internet Security Asociation and Key Management Protocol): *Ver IKE*

ISP (Internet Service Provider): Proveedor de servicio de Internet.

K

KLIPS (Kernel Level IP Security Support): Implementación del protocolo IPSec, incluida en FreeS/WAN, que permite establecer túneles seguros sobre redes no confiables

L

LAC: Es un concentrador de acceso, que se ubica entre un LNS y un sistema remoto y manda paquetes a cada uno de los dos.

LNS: es el par del LAC, y es un punto de terminación lógica de una sesión PPP a la cual se le esta siendo aplicado el túnel desde el sistema remoto por el LAC.

L2F (Layer 2 Forwarding): Es un protocolo de capa 2 que permite a un servidor dialup encuadrar tráfico dial-up en PPP y transmitirlo sobre vínculos WAN a un servidor L2F.

L2TP (Layer 2 Tunneling Protocol): Es un protocolo de red que facilita la creación de túneles para enviar tramas PPP. Encapsula las tramas PPP para que puedan ser enviadas sobre redes IP, X.25, Frame Relay o ATM.

M

Mobile IP: Estándar propuesto con el fin de resolver el problema de que a un nodo móvil se le permita dos direcciones IP

Modo de Túnel: *Ver Tunneling.*

MPPE (Microsoft Point-to-Point Encryption): Método de encriptación usado por PPTP, y solo es posible su utilización cuando se emplea CHAP, como medio de autenticación.

N

NCP (Network Control Protocol): Protocolo usado por L2TP para asignar la IP y autentificar en PPP, comúnmente conocido como CHAP y PAP.

P

PAP (Password Authentication Protocol): Es un protocolo de autenticación poco sólido. Las contraseñas se envían a través del enlace en texto no cifrado, y no hay protección contra la reproducción o los ataques reiterados de ensayo y error.

PLUTO: Demonio que maneja intercambio de claves, verifica identidades y establece una política de seguridad para KLIPS.

PPP (Point-to-Point Protocol): Es el protocolo WAN más popular y más ampliamente utilizado porque ofrece detección de errores, proporciona asignación dinámica de direcciones IP, etc.

PPTP (Point-to-Point Tunneling Protocol): Protocolo que permite que el tráfico IP, IPX o NETBEUI, sea encriptado y encapsulado en encabezados IP para ser enviado a través de una interred IP como Intenet.

S

SA (Security Asociation): Especifica los algoritmos de autenticación y encriptación para ser usados, las claves de encriptación para ser usadas durante la sesión, y cuánto tiempo son mantenidas las claves y la Asociación de Seguridad.

Sniffers: Intruso de la red, que husmea y nada más y no se conocen sus fines con certeza.

T

Triple Data Encryption Standard (3DES): Consiste en encriptar tres veces una clave DES. Existen 3 métodos: DES-EEE3, DES-EDE3, DES-EEE2 y DES-EDE2. Dependiendo del método elegido, el grado de seguridad varía; el método más seguro es el DES-EEE3.

Tunneling: Es un método que consiste en utilizar la infraestructura de una interred (como Internet), para transportar datos de una red a otra.

V

VPN (Virtual Private Network): Red Privada que trabaja sobre una red pública global e insegura como Internet, pero que al crear el túnel por el cual se enviarán los datos se convierte en un medio seguro y difícil de acceder.

X

X.25: Protocolo estándar para comunicaciones WAN que define la manera como se conectan los dispositivos de red y los dispositivos de usuarios. X.25 está diseñado para trabajar efectivamente en cualquier tipo de sistemas interconectados a la red

7. LISTA DE FIGURAS

BIBLIOGRAFÍA

Monografías

- ✓ **TORRES Martínez, Tania Margarita; CHARTUNI Castro, Yezid.** "Estudio y prácticas sobre redes privadas virtuales (VLAN y VPN) para los laboratorios de la CUTB".
- ✓ **VANEGAS Mattos, Enrique Carlos.** "Redes Privadas Virtuales (RPVs): Solución Integral de Seguridad".

Libros

- ✓ **LEÓN Clark, David; PINEDA Rojas, Eloy.** "Guía para el administrador de redes privadas virtuales". México D.F. Edit. McGrawHill 1999.
- ✓ **BROWN, Steven.** "Implementación de Redes Privadas Virtuales (RPV)". México D.F. Edit. McGrawHill 1999.

Páginas WEB

- ✓ **COLLADO Rodríguez, Mª Montserrat; CONDE Rey, Silvia; DAFONTE Pérez, Eva.** "Redes Privadas Virtuales".

http://ccia.ei.uvigo.es/docencia/SSI/VPN.pdf

- ✓ **PERT CONSULTORES SRL.** "i–VPN Servicio de Redes Privadas Virtuales dinámicas sobre Internet"

http://www.pert.com.ar/actual/productos/pdfs/i-VPN.pdf

- ✓ **GÓMEZ Cárdenas, Roberto.** "VPN sobre Linux"

http://www.netmedia.info/bsecure/articulos.php?id_sec=48&id_art=4493

- ✓ **XOMBRA TEAM.** "VPN o Redes Privadas Virtuales"

http://www.xombra.com/go_articulo.php?articulo=36

- ✓ **CANOVAS O. ; GÓMEZ A. F. ; LÓPEZ G. ; MARTÍNEZ G.** "Redes Privadas Virtuales Dinámicas"

http://www.rediris.es/rediris/boletin/54-55/ponencia2.html

- ✓ "Introduction to FreeS/WAN"

http://www.freeswan.org/freeswan_trees/freeswan-2.00/doc/toc.html

- ✓ **SCHRODER, Carla.** "Build a Flexible VPN with FreeS/WAN and Linux, Part1". Abril 17 de 2002.

http://www.rediris.es/rediris/boletin/54-55/ponencia2.html

- ✓ **GUY Briggs, Richard.** "FreeS/WAN IPSec for Linux". Julio 15 de 2000.

http://www.conscoop.ottawa.on.ca/rgb/freeswan/ols2k/pj.html

- ✓ **IETF Secretariat.** "IP Security Protocol (IPSec)". Noviembre 25 de 2003. http://www.rediris.es/rediris/boletin/54-55/ponencia2.html

- ✓ **STEFFEN, Andreas.** "Secure Network Communication Part IV IPSecurity (IPSec)". 2000 – 2002. http://www.strongsec.com/zhw/KSy_IPsec.pdf

- ✓ "HOW TO: Configure Packet Filter Support for PPTP VPN Clients in Windows Server 2003". Microsoft Knowledge Base Article 324262. 2004. http://support.microsoft.com/default.aspx?scid=kb;en-us;324262

- ✓ "HOW TO: Configure un servidor VPN para actuarlo como un enrutador en Windows Server 2003". Microsoft Knowledge Base Article 816573. 2004. http://support.microsoft.com/default.aspx?scid=kb;ES;816573

- ✓ "HOW TO: Configure DNS for Internet Access in Windows Server 2003". Microsoft Knowledge Base Article 323380. 2004. http://support.microsoft.com/default.aspx?scid=kb;en-us;323380

- ✓ "HOW TO: Install and Configure a DHCP Server in a Workgroup in Windows Server 2003". Microsoft Knowledge Base Article 323416. 2004.

http://support.microsoft.com/default.aspx?scid=kb;en-us;323416

- ✓ **El Taller Virtual.** "Creando una VPN en Ms Step-by-Step". 2004. http://www.eltallervirtual.cl/modules.php?name=News&file=article&sid=819&mode=&order=0&thold=0

- ✓ "Configuración de un servidor VPN para actuar como router en Windows Server 2003". Maxitrucos. 2003. http://www.maxitrucos.com/Truco_Del_Mes/Anteriores/2003/julio03.htm

- ✓ "Step-by-Step Guide for Setting Up Vpn-based Remote Access in a Test Lab". Microsoft Corporation. 2003. http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/networking/rmotevpn.mspx#XSLTsection122121120120