UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTARCION

ESCUELA DE INGENIERÍA DE SISTEMAS

ELABORACION DE UN TUTORIAL PARA LA CONSTRUCCION DE UNA RED VIRTUAL PRIVADA (VPN)

TRABAJO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

AUTORES:

DIANA CAROLINA FLORES MOGROVEJO

MELISSA MARIA SANGURIMA GALLARDO

DIRECTOR:

ING. LUIS CALDERON

CUENCA – ECUADOR

2008

Las opiniones y contenidos vertidos en este proyecto de monografía son de exclusiva responsabilidad de sus autores.

Diana Flores Mogrovejo

Melissa Sangurima Gallardo

DEDICATORIA

Dedico esta monografía con mucho cariño a Dios porque sin El nada hubiera sido posible, a mis padres Alfredo y Rosa, a mi hermana Carolina, a mi tía Maruja, a mis abuelitos y a toda mi familia que a pesar de la distancia fueron mi gran apoyo y guía en todo momento especialmente cuando las cosas no iban tan bien. Además a la Sra. Jackelyne Barriga y a todos mis amigos que han sido muy importantes en mí vivir diario.

Melissa

Dedico esta monografía primero a Dios porque hizo posible mi realización profesional y me permitió compartir este momento con mis seres queridos, luego a mis padres por brindarme todo su amor y apoyo en los instantes buenos y malos durante mis estudios, a mi hermana por sus palabras de aliento cuando la situación se tornaba difícil, y a todas esas personas que siempre estuvieron presentes y pendientes de mi.

Caro

AGRADECIMIENTOS

Especialmente a Dios por ser un ser extraordinario y permitirnos culminar exitosamente esta etapa estudiantil, a nuestros padres que han sido un pilar fundamental en el desarrollo de nuestras vidas y un apoyo incondicional en los estudios, a todos los profesores especialmente Ing. Luis Calderón, Ing. Oswaldo Merchán, que fueron forjadores de nuestra formación académica, a nuestra universidad por darnos la oportunidad de conocer, compartir y vivir experiencias que quedarán como recuerdos inolvidables en nuestras mentes, a quienes conforman los laboratorios de la Escuela de Ingeniería en Sistemas , Sr. Felipe Merchán, Sr Julio Bustos y Sr. Alfredo Chiriboga, por su apoyo sincero en la realización del presente trabajo.

RESUMEN

La presente investigación tiene por objeto conocer las Redes Privadas Virtuales, y los protocolos de tunneling para su implementación, y a partir de esto la elaboración de un tutorial para la construcción de una VPN, con la finalidad de que este material facilite y aporte en el aprendizaje de los estudiantes de la materia de Redes de la Universidad del Azuay, ya que se dará paso a paso una guía de cómo configurar un servidor VPN con L2TP/IPSec, un cliente de acceso remoto, y la red por la cual se comunicarán, al concluir las practicas los estudiantes realizarán la captura de tráfico, comprobando la diferencia de los datos cuando viajan encriptados y cuando viajan en claro, destacando la importancia de que la información viaje en forma segura.

ABSTRACT

The aim of this research work is to know the Virtual Private Networks and the tunneling protocols for their implementation leading to the development of a tutorial for the construction of a VPN.

The purpose is to use this material to facilitate and contribute to the learning of students of Networks, a subject offered by the University of Azuay. It will provide a step-by-step guide on how to configure a VPN server with L2TP/IPSec, a remote access user, and the net through which they will communicate.

When the practice ends, the students will do the traffic capture, checking the difference of the information when it travels encrypted or unencrypted, and highlighting the importance of having the information travel safely.

INDICE DE CONTENIDOS

Diana Carolina Flores Mogrovejo
Melissa María Sangurima Gallardo
Trabajo de Graduación
Ing. Luis Calderón
Abril 2008

ELABORACION DE UN TUTORIAL PARA LA CONSTRUCCION DE UNA RED VIRTUAL PRIVADA (VPN)

INTRODUCCIÓN

Diversas organizaciones se han visto atraídas por la idea de implementar VPN's (Virtual Private Network), ya que desean ampliar las capacidades de sus redes y reducir costos.

La nueva economía y avance tecnológico requiere, no como un lujo sino más bien como una necesidad, una cobertura global entre oficinas locales y remotas de una misma empresa. Una red privada virtual es la interconexión de varias redes locales (LAN) que se encuentran en lugares remotos. Estas pueden encontrarse en la casa o lugares de trabajo y brinda a los empleados seguridad en sus comunicaciones. Los trabajadores y aquellos que viajan con frecuencia, encuentran que las redes VPN son una forma más provechosa de permanecer conectados con la red que laboran, por lo que en este tutorial se encuentra toda la información necesaria para lograr un alto nivel de conocimiento y poder aplicarlo.

Las VPNs utilizan protocolos de tunneling para su seguridad como PPTP, L2TP, IPSec, etc, para garantizar la seguridad de los sistemas. En este tutorial encontraremos ventajas, desventajas, características, y mediante el estudio de estas se decidirá cuál es el protocolo que nos brinda la seguridad más óptima y éste será el que se utilice para la parte práctica del tutorial.

CAPITULO I

1. VPN (REDES PRIVADAS VIRTUALES)

1.1 INTRODUCCION

En este capítulo se hablará sobre las VPNs, que no son más que dos redes locales comportándose como si se trataran de una única red local; sin embargo por diversas razones, esencialmente de índole económica, la interconexión entre dichas redes se efectúa a través de medios que suelen ser inseguros como Internet. Además muestra su funcionamiento, los elementos necesarios para su construcción, las características y ventajas que se obtienen si decidimos implementar una VPN.

1.2 CONCEPTO

VPN, es una tecnología de red que permite conectar varias redes y emula ser una sola red privada como si fuera una conexión punto a punto entre los ordenadores remotos del usuario (cliente VPN) y el servidor de la organización (servidor VPN), para esto hace uso de una infraestructura pública de telecomunicaciones como podrían ser Internet, Red telefónica conmutada, ATM RDSI, X.25, FRAME RELAY, etc; en lugar de utilizar líneas privadas rentadas, por lo que se puede decir que una VPN es una forma de red WAN (Wide Area Network), aunque no es más que la creación de una red de carácter confidencial en una red pública.

Los paquetes de datos de la red privada viajan por un túnel definido en esta red, permitiendo compartir y transmitir información entre un grupo de usuarios que se encuentran en diferentes ubicaciones geográficas, de manera que podrán trabajar como si estuvieran en una misma red local.

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

Autenticación y autorización: Verificar que una entidad (usuario/equipo)es quien dice ser y qué nivel de acceso debe tener.

Integridad: Que los dato se mantengan intactos y no sean modificados.

Confidencialidad: que los datos sean vistos solo por quien tiene permisos

No repudio: Si determinada entidad genero un documento/transacción no lo podrá negar.

Control de Acceso: Autenticada la persona o entidad, a que recursos puede acceder.

Cabe mencionar que para poder construir una VPN es necesaria la implementación de protocolos como L2TP, IPSec, PPTP. En el Gráfico #1 podemos observar cómo sería una conexión VPN.

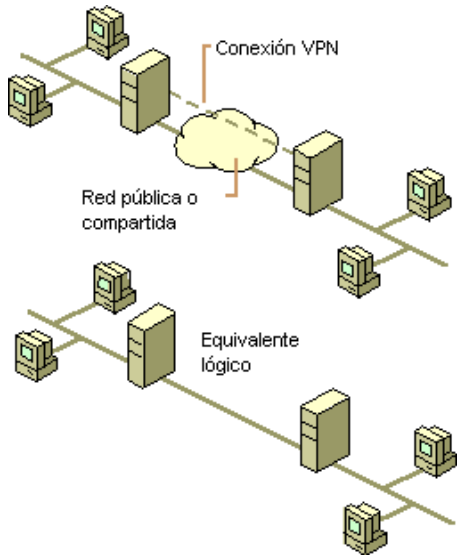


Gráfico 1. Equivalente lógico de una Conexión VPN

1.3 FUNCIONAMIENTO

El proceso de una VPN es totalmente transparente para el usuario y para la mayoría de las aplicaciones. En el interior de la Red Virtual Privada cada equipo tendrá una IP, todas las conexiones que usen esta IP estarán funcionando dentro de la VPN y estarán de forma encriptada, para el uso

de la VPN el usuario tendrá que usar sus IPs, y no preocuparse de nada más, el resto ya lo hace el cliente VPN y el servidor VPN.

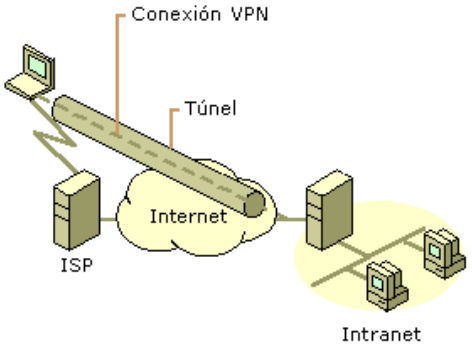


Grafico 2. Funcionamiento de una VPN

El funcionamiento se da de la siguiente manera:

Cuando un paquete es transmitido, éste es enviado y se le añade el Encabezado de autenticación (AH) para enrutamientos y autenticación. Posteriormente los datos son encriptados y cerrados con una Carga de seguridad de encapsulación (ESP) y es aquí donde están las instrucciones de control y desencriptación.

El receptor VPN:

1. Extrae la información.
2. Desencripta los datos.
3. Enruta la información a su destino.

El equipo receptor recibe los paquetes descifrados que están listos para ser procesados.

Al manejar este nivel de seguridad, cualquier intruso que se presente no sólo debe interceptar un paquete, sino también descifrarlo, es decir, debe también conocer la llave para la autenticación de sesiones.

1.4 ELEMENTOS DE UNA VPN

- **Servidor VPN:** Este elemento es el responsable de aceptar la conexión VPN de un cliente.
- **Cliente VPN:** Es el computador que da inicio a una conexión VPN. El cliente VPN puede ser un computador individual o formar parte de una red distinta de la que intenta conectar.
- **Túnel:** Por medio de este elemento se transmite los datos encriptados. Podríamos crear un túnel y por medio de este enviar información sin encriptar, pero no sería una VPN ya que la información privada es enviada por un medio público, es decir, todo el mundo puede acceder, por no tener encripción esta información estaría disponible para todos.
- **Protocolos de Tunneling:** Son los estándares de comunicación que rigen los túneles y la trasmisión de datos privados encriptados.
- **Datos de Túnel:** Son los datos que se envían a través del túnel.
- **Red de Tránsito:** Es la red pública compartida por medio de la cual los datos encapsulados son transmitidos, por ejemplo Internet.
- **Conexión Vpn:** La creación de una conexión VPN es similar a establecer una conexión punto a punto mediante el acceso telefónico a redes.

  Existen 3 tipos de conexiones:

  - **Acceso Remoto:** Este tipo de conexión la realiza un cliente remoto o una computadora individual que pueden estar ubicados en casas, oficinas, aviones, hoteles, etc. En esta comunicación el servidor VPN provee acceso a recursos del servidor o de la red conectada permitiendo así que los empleados teletrabajen. Los paquetes enviados por la VPN se originan en el acceso remoto del cliente.

    Cuando el cliente desee conectarse, primero se conecta con ISP, luego inicia la conexión VPN, luego cuando se establece la conexión, los clientes podrán acceder a su red.

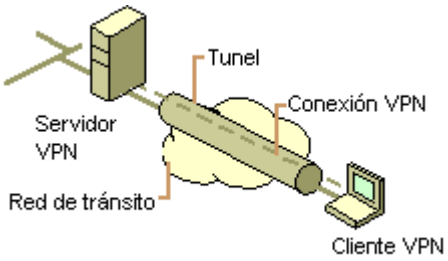


Grafico 3. Conexión VPN de acceso Remoto

- **Router a Router:** Esta comunicación es establecida por 2 ruteadores que unen 2 partes de red o 2 redes distintas. El primero es el cliente que llama y el segundo es el servidor que autentica y provee los recursos del servidor o de la red.
  En esta conexión se establece el Túnel VPN mediante internet. Al usar esta tecnología nos ahorraríamos las costosas conexiones punto a punto, sobre todo si son internacionales. Esta es una conexión de servidor VPN a servidor VPN.

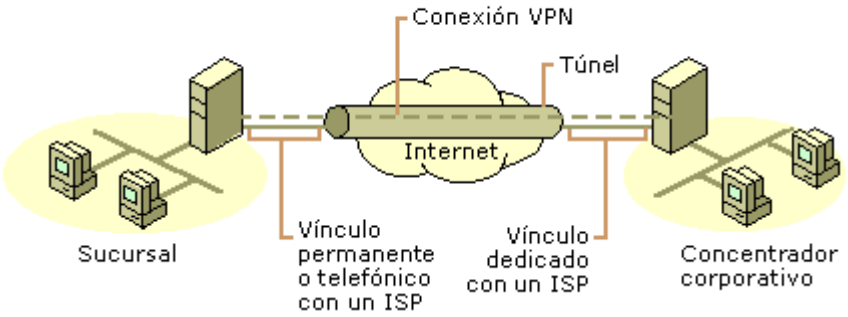


Grafico 4. Conexión VPN de Router a Router

- **VPN Interna:** Estas redes son las más eficaces para utilizar dentro de una empresa. Es una variante de las de "acceso remoto" pero, en vez de utilizar Internet para conectarse, utilizan la propia LAN de la empresa (intranet). Es una forma de aislar zonas o departamentos de la LAN interna, de esta

manera solo el personal autorizado podrá tener acceso a cierta información.

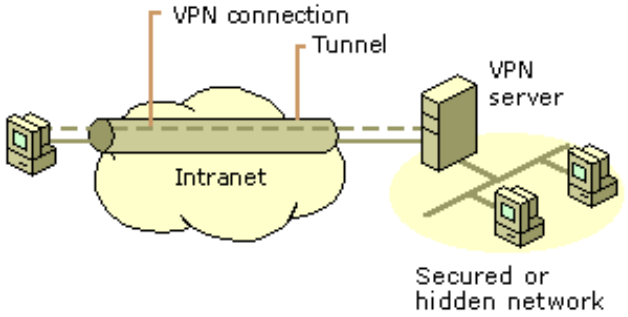


Grafico 5. Conexión VPN Interna

1.5 PROPIEDADES DE UNA VPN

Una VPN debe cumplir al menos con los siguientes puntos:

- **Autenticación de usuarios:** Debe verificar la identidad de quien se conecta, y también determina las restricciones de acceso que exista. Además el cliente tiene que verificar que el servidor que contesta es el que realmente el que dice ser.
- **Administración de direcciones:** Debe asignar una dirección IP de la red al cliente que se conecta, con el objetivo de que esta dirección sea privada.
- **Encripción de datos:** Los datos que se envían por la red pública son indescifrables para aquellos usuarios que no cuentan con los permisos necesarios.

  La información es encriptada por el que la envía y desencriptada por quien la recibe. El proceso de encriptar y desencriptar depende de quien envía y del que recibe, ambos deben conocer la llave que les permita realizar este proceso. El tamaño de la llave es un aspecto importante para la encripción de datos, mientras Mayor es el tamaño de la llave, mayor es el grado de seguridad que se da a los datos y a la conexión.

- **Administración de Llaves:** Este elemento es de vital importancia para la encripcion y desencripción. Este aspecto es primordial para mantener la privacidad y la seguridad de la VPN, lo hace generando nuevas llaves tanto para el cliente como para el servidor a intervalos regulares de tiempo.
- **Soporte de Múltiples Protocolos:** La solución debe soportar varios protocolos usados en las Redes Públicas, como por ejemplo TCP/IP, IPX, etc.

1.6 CARACTERÍSTICAS

- Permite extender redes internas en Internet sobre entidades remotas o usuarios móviles.
- Además se pueden crear vínculos entre distintas redes (extranet) que unan empresas con clientes, proveedores, etc.
- Admite el acceso a la red a usuarios remotos desde sus casas, oficinas, hoteles, etc.
- Estas redes proporcionan conectividad hasta en distancias muy grandes.
- Tienen la capacidad de trabajar ya sea sobre redes privadas como en públicas como el Internet.
- Cuando utilizan un método llamado "tunneling", las VPN pueden usar la misma infraestructura de hardware de las conexiones de Internet o Intranet que ya existen.
- Estas tecnologías incluyen algunos mecanismos de seguridad para proteger las conexiones virtuales privadas.
- Con las VPN se puede compartir archivos, video conferencias y servicios de red afines.
- Las VPN habitualmente no ofrecen ninguna funcionalidad que otras opciones no ofrezcan, pero una VPN implementa los mismos servicios con mayor eficiencia y economía en casi todos los casos.

1.7 VENTAJAS DE UNA VPN

Con el pasar de los días las empresas van descubriendo las ventajas que trae el uso de las VPN para la conexión de sucursales, de socios empresariales, proveedores y fabricantes (incluso de empleados).

- Brinda a los datos integridad, confidencialidad y seguridad.
- Es fácil de usar.
- La instalación del cliente en cualquier PC Windows se realiza de forma sencilla.
- El Acceso es controlado por las políticas de la organización
- En lo que se refiere a las actualizaciones y mantenimiento de las PC's remotas evita el costo alto.
- Garantiza una conexión de red con las características de la red privada a la que se quiere acceder.
- El cliente VPN adquiere la condición de miembro de esa red, y con esto se le aplican todas las directivas de seguridad y permisos de un ordenador en esa red privada, de esta forma puede acceder a los datos publicados para esa red privada: bases de datos, documentos internos, etc. mediante un acceso público.
- Los recursos y conexiones de la red privada son utilizados para realizar las conexiones de acceso a Internet desde el ordenador cliente VPN.

1.8 CONCLUSIONES

Las Redes privadas Virtuales VPNs son una alternativa de gran ayuda tanto en lo económico como en lo que se refiere a seguridad, debido a que su implementación no requiere de componentes costosos y la seguridad que éstas ofrecen es confiable para cualquier tipo de uso que se les quiera dar.

CAPITULO II

2. TUNNELING

2.1 INTRODUCCION

En este capítulo se habla de la tecnología de tunneling y como gracias a esta podemos construir las VPNs, además nos explica su funcionamiento, y nos da una información completa de los protocolos de tunneling (PPTP, L2TP, IPSec…); concepto, funcionamiento, características, ventajas, y al final se realiza la selección del protocolo más adecuado y seguro para la elaboración de la práctica de laboratorio.

2.2 CONCEPTO

Aplicando esta tecnología se transmiten los datos de una red hacia otra, utilizando como medio una red que puede ser pública o compartida. Se pueden usar distintos protocolos de tunneling para la transmisión. Lo que hacen estos protocolos es que antes de enviar los datos le añaden una cabecera adicional al paquete. Esta nueva cabecera suministra la información para que la carga útil del paquete que va encapsulado pueda pasar por la red sin dificultades.

Estos paquetes viajan por un camino lógico que es el túnel, una vez que han localizado su destino son desencapsulados y entregados a su destinatario final.

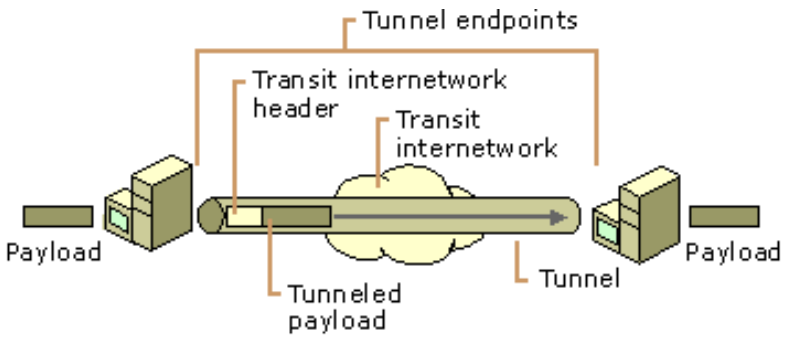


Grafico 6. Tunelling

2.3 FUNCIONAMIENTO DEL TUNNELING: Si hablamos de protocolos de tunneling de capa 2 como PPTP y L2TP es como si estableciéramos una sesión en la que los dos extremos aceptan y negocian las variables de configuración (asignación de direcciones, encripción de parámetros). A diferencia de los protocolos de capa 2 en los de capa 3 no hay fase de mantenimiento.
Al enviar la información por el túnel, tanto el servidor como el cliente hacen uso de un protocolo.

Así por ejemplo cuando un cliente envía datos por el túnel, el cliente debe agregar al paquete una cabecera del protocolo utilizado para realizar la transferencia de datos. Resultado de esto el cliente envía el paquete encapsulado por la red. El momento que llega al servidor, este retira la cabecera antes agregada par encapsular la información, para después enviar el paquete a su destino final, y de igual forma cuando la información se envía del servidor al cliente.

2.4 PROTOCOLOS DE TUNNELING Y SEGURIDAD

Es necesario para poder establecer un túnel que el cliente y el servidor utilicen el mismo protocolo de Tunneling.
Las tecnologías tunneling pueden basarse en los protocolos de capa 2 (enlace) o de capa 3 (red).
Dentro de los protocolos de capa 2 tenemos al PPTP y L2TP, el funcionamiento de estos protocolos consiste en encapsular los datos en frames PPP (Punto a Punto) los cuales serán enviados por medio de la red pública

Entre los protocolos que se ubican en la capa 3 encontramos a IP Security (IPSEC). El funcionamiento de este protocolo consiste en encapsular los paquetes IP en cabeceras IP adicionales previo al envío que se realiza por la red pública.

2.4.1 PPP (Point to Point Protocol)

2.4.1.1 CONCEPTO

PPP es la base de PPTP y L2TP. Es un protocolo de capa de enlace (Nivel 2 del Modelo OSI) que permite establecer una conexión entre dos puntos (dos computadoras o nodos), y requiere del protocolo TCP/IP (Transport Control Protocol / Internet Protocol) para realizar la transferencia de datos. Este protocolo fue diseñado para el envío de datos a través de línea telefónica o conexiones dedicadas punto a punto. PPP encapsula paquetes multiprotocolo IP, IPX, y NetBEUI en frames PPP, para luego transportarlos sobre un enlace serial entre el usuario y el proveedor de servicios de Internet (ISP). Este trasporte se realiza bidireccional y full-duplex.
Además del transporte de datos, permite autentificación a través de una clave de acceso y asignación dinámica de IP.
PPP también dispone de:

- Un mecanismo para encapsular los paquetes y manejar la detección de errores
- Un protocolo de control de Enlace (LCP) para establecer, configurar y probar la conexión de datos.
- Una serie de protocolos de control de red (NCP), para establecer y controlar los diversos protocolos de la capa de red

PPP tiene las siguientes fases:

a) **Establecimiento del enlace y negociación:** Durante esta fase un equipo o nodo PPP envía tramas LCP (Link Control Protocol) para configurar y establecer el enlace de datos. LCP es un protocolo fundamental en PPP.
b) **Determinación de la calidad del enlace:** Esta es una fase opcional, y aquí se prueba el enlace para ver si son adecuados para establecer los protocolos de capa de red.
c) **Autenticación:** No es una fase obligatoria. PPP tiene los siguientes protocolos de autenticación: PAP CHAP, EAP y MS-CHAP.

PAP (Protocolo de autenticación de contraseña): Proporciona un método de autenticación simple utilizando un intercambio de señales de dos vías, se realiza durante el establecimiento de inicial del enlace. No es un método seguro ya las contraseñas se envían en modo abierto.

CHAP (Challenge Handshake Authentication Protocol): Más segura que PAP, La contraseña es encriptada utilizando MD5 (Message-Digest Algorithm 5), una vez establecido el enlace el router agrega un mensaje que es verificado por ambos routers, si ambos coinciden se acepta la autenticación de lo contrario la conexión se cierra inmediatamente.

EAP (Protocolo de autenticación extensible): Este protocolo admite métodos de autenticación arbitrarios. A cada usuario se le proporciona una clave nueva cada vez que se conecta, y éstas son regeneradas cada cierto intervalo de tiempo durante su sesión.

MS-CHAP (Microsoft Challenge Handshake Authentication Protocol): Es un protocolo de autenticación de contraseña de cifrado no reversible, funciona de la siguiente manera:

- El autenticador envía al cliente de acceso remoto un mensaje formado por un identificador de sesión y una cadena arbitraria.
- El cliente de acceso remoto envía una respuesta que contiene el nombre de usuario y un cifrado no reversible, el identiicador de sesión y la contraseña.
- El autentificador comprueba la respuesta y, si es válida, se autentica las credenciales del usuario.

d) Configuración del protocolo de la capa de red: El computador o nodo PPP envía tramas NCP para escoger y configurar los protocolos de capa de red. Después, se pueden enviar datagramas de cada protocolo de red configurado.

e) **Transferencia de Datos:** Durante esta fase se manda y recibe la información de red.
f) **Terminación del enlace:** El LCP es quien termina el enlace, puede ser por petición del usuario o por expiración de tiempo.

2.4.2 PPTP (Point to Point Tunneling Protocol)

2.4.2.1 CONCEPTO

PPTP es un protocolo punto a punto de capa de enlace de datos (Nivel 2 del Modelo OSI). Permite construir VPN simples (túneles) dentro de una red (IP, IPX, netBEUI), en este caso hablaremos de una red IP. Se basa en encapsular los paquetes (frames) del protocolo PPP con datagramas IP, para que después sean transmitidos por una red pública como internet, o una privada como una intranet.

Una conexión de este tipo se establece entre un cliente y servidor (ambos utilizando el protocolo PPTP). Al servidor se lo identificará como PNS (PPTP Network Server) y al cliente como PAC (PPTP Access Concentrator).

Cada conexión PPTP consta de:

- Una conexión de control que se debe establecer antes del túnel IP entre un PAC y un PNS, como es TCP que le permite crear, mantener y terminar el túnel.
- Un túnel IP entre el PAC y PNS, que se usa para transportar los mensajes PPP encapsulados mediante el protocolo GRE (Encapsulación de Enrutamiento genérico, protocolo que encapsula un paquete dentro de un protocolo de transporte. La carga útil será encapsulada dentro del paquete GRE).

La carga útil de los paquetes encapsulados puede estar encriptada o comprimida o ambas cosas, y estos datos, como las direcciones de los equipos que se encuentran en el encabezado del mensaje, se encapsulan

en un mensaje PPP, el que al mismo tiempo está encapsulado dentro de un mensaje GRE y un mensaje IP, ver Gráfico 7.

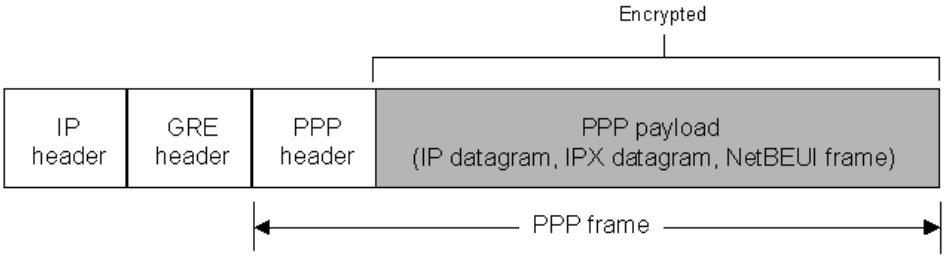


Grafico 7. Estructura del paquete PPTP

2.4.2.2 FUNCIONAMIENTO

La función de PPTP es crear un túnel dentro de una red (IP para el ejemplo), y permite que el tráfico multiprotocolo que viajara por este túnel sea cifrado y encapsulado en un encabezado IP para que de este modo pueda ser enviado por la red.

Una vez establecida la conexión (que puede ser realizada por el PAC o PNS) mediante PPP se presentan dos opciones, que el Servidor de Acceso Remoto (RAS) del ISP soporte PPTP ,entonces el mismo RAS establece el túnel, o si no se establece una conexión PPTP con el servidor PPTP de la red a la que queremos acceder de la siguiente manera: en primer lugar se crea un paquete PPP y la carga útil se cifra con MPPE (cifrado punto a punto de Microsoft) y hace uso de las claves de cifrado generadas por un protocolo de autenticación como puede ser MS-CHAP o EAP, de esta manera la trama PPP es encriptada y/o comprimida en una cabecea PPP, creando un paquete (frame) PPP. Luego se realiza la encapsulación de los paquetes PPP con una cabecera GRE, esto se hace usando el protocolo GRE; y después la carga resultante (PPP + GRE) es encapsulada con una cabecera IP que contiene las direcciones IP destino y origen adecuadas para el cliente y el servidor PPTP.

Finalmente para que sea enviado por un enlace LAN o WAN, el datagrama

IP es encapsulado con una cabecera y una cola según la tecnología de la capa del enlace que se esté usando por ejemplo Ethernet.

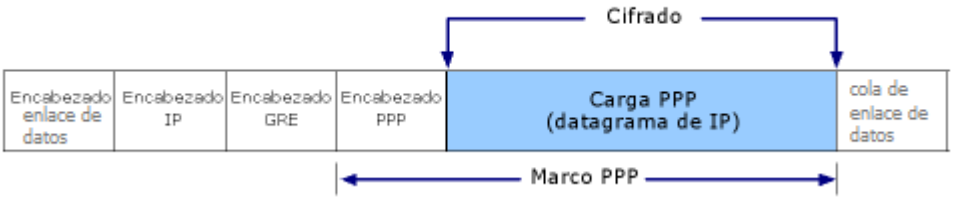


Grafico 8. Estructura de un paquete PPTP que contiene un datagrama IP

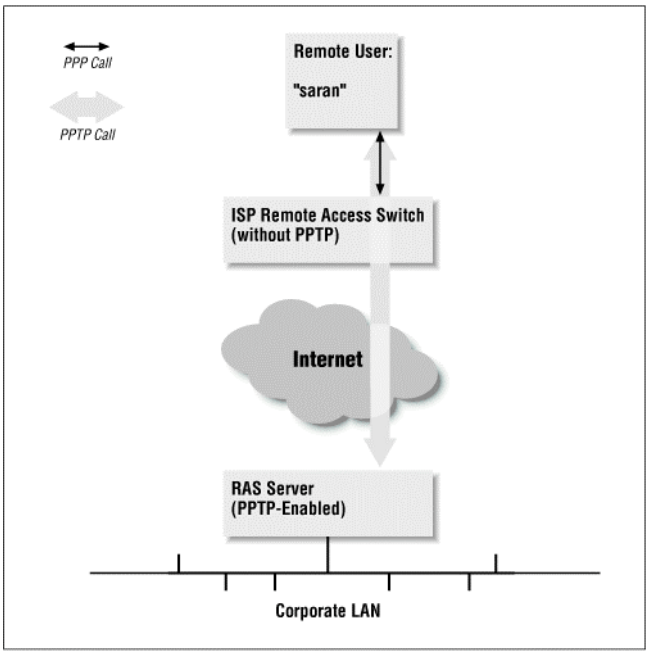


Grafico 9. Túnel mediante PPTP

Como hemos visto para realizar el envío de datos con PPTP se logra con múltiples niveles de encapsulación. A continuación se detalla el procesamiento de los datos enviados con este protocolo, al ser recibidos por el cliente o el servidor PPTP:

- Procesa y elimina la cabecera y la cola del enlace de datos.
- Procesa y elimina la cabecera IP.
- Procesa y elimina las cabeceras GRE y PPP.
- Desencripta y/ o descomprime la carga PPP.
- Procesa la carga para recepción o reenvío.

2.4.2.3 CARACTERISTICAS

- PPTP es una mejora del protocolo básico PPP.
- Se lo suele asociar con Microsoft, ya que forma parte de los sistemas operativos de Windows.
- Posee la habilidad de soportar protocolos no IP, la cual es su mejor característica, ya que también usa los protocolos IPX y NetBEUI.
- Usa el protocolo TCP para el mantenimiento del túnel.
- Para la encapsulación de las tramas PPP usa el protocolo GRE
- No permite múltiples conexiones.
- Las conexiones PPTP utilizan para su autenticación los mismos mecanismos de autenticación del protocolo PPP, tales como PAP, MS-CHAP, CHAP y EAP.
- PPTP puede utilizarse para el acceso remoto y las conexiones VPN enrutador a enrutador.
- Los servidores PPTP poseen la capacidad de filtrar paquetes.
- El servidor asigna una dirección IP al cliente, por lo que permite usar direcciones de la propia red
- La seguridad que brinda PPTP no es tan fuerte como la que ofrece IPSec.

2.4.3 LAYER-2 TUNNELING PROTOCOL (L2TP)

2.4.3.1 CONCEPTO

Este protocolo tiene casi la misma funcionalidad que el protocolo túnel Punto a Punto (PPTP), es un protocolo estándar de túnel para internet. Fue aprobado por el IETF en contra al protocolo propietario de Microsoft PPTP.
Este protocolo encapsula las tramas PPP que serán enviadas mediante redes IP, X.25, Frame Relay, o ATM. Brinda opciones de autenticación.

Gracias a L2TP, los datos no TCP/IP pueden ser transportados a través de Internet (ya que las tramas PPP son multiprotocolo).

L2TP sobre redes IP usa UDP y una serie de mensajes de L2TP para el mantenimiento del túnel. También usa UDP para enviar los paquetes PPP encapsulados por L2TP como datos del túnel. La carga útil de los paquetes puede ser cifrada y/o comprimida.

El Gráfico. 10 muestra la estructura de un paquete L2TP, donde vemos que la cabecera del protocolo L2TP es parte del conjunto de cabeceras de un datagrama IP:

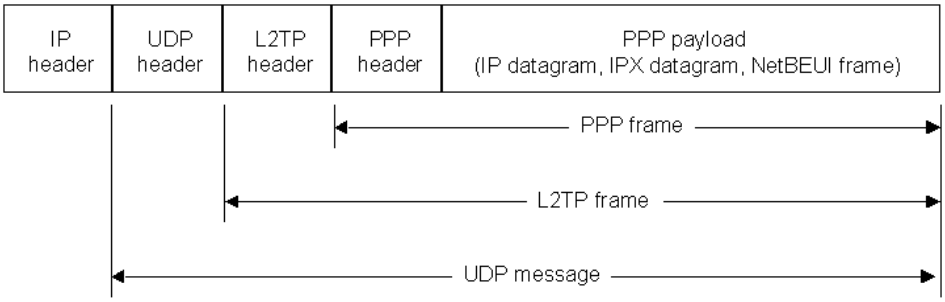


Grafico 10. Estructura del paquete L2TP

La cabecera de L2TP consta de 128 bits y queda estructurada de esta manera:

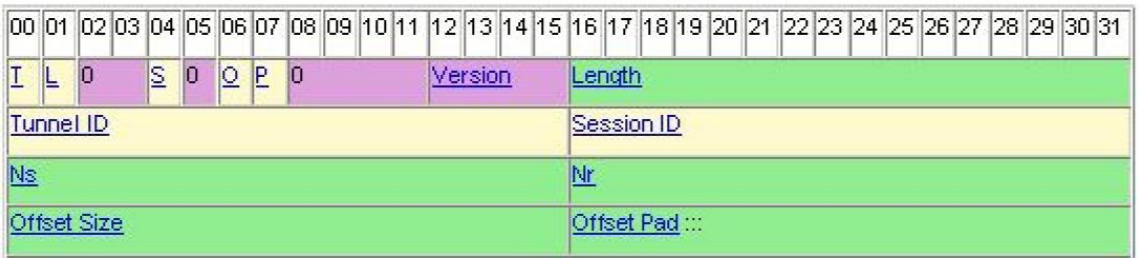


Grafico 11. Cabecera de L2TP

T: Especifica si es un mensaje de control (0) o datos (1).

S: (mensajes de control): Si el valor que tiene es 1, los campos Ns y Nr deben estar configurados.

P: Este mensaje debe recibir tratamiento especial en la cola local.

Version. 4 bits. Indica la versión del protocolo L2TP. Debe ser configurado a 2.

Tunnel ID. 16 bits. Indica el identificador de control de la conexión, los túneles son nombrados por identificadores locales.

Session ID. 16 bits. Indica el identificador de la sesión dentro de un túnel.

Ns, Sequence Number. 16 bits. Opcional. Indica el número de secuencia para el mensaje de control o los datos actuales.
Nr, Sequence Number Expected. 16 bits. Opcional. Indica el número de secuencia esperado en el siguiente mensaje de control a ser recibido.

2.4.3.2 FUNCIONAMIENTO

El funcionamiento de este protocolo tiene como fin facilitar el entunelamiento de paquetes PPP mediante una red teniendo como objetivo que sea lo más transparente posible a los usuarios que estén en los extremos del túnel y para los usos que éstos le den. Una conexión L2TP consta de:

L2TP Network Server (LNS): Es un extremo de la conexión L2TP y es la pareja de un LAC. Opera sobre cualquier plataforma con capacidad de terminación PPP. LNS gestiona el lado del servidor del protocolo L2TP.
Cuando el sistema remoto pone en el túnel una sesión punto a punto por medio del LAC, el LNS indica su terminación lógica, ver Gráfico 12.

L2TP Access Concentrator (LAC): Es un nodo que actúa como el otro extremo del túnel L2TP y hace pareja de un LNS. Éste se ubica y manda paquetes entre un LNS y un sistema remoto. Para el envío de paquetes entre un LAC y un LNS se utiliza un túnel L2TP y para el envío de paquetes entre un LAC y un sistema remoto se realiza mediante una red local o una conexión PPP, ver Gráfico 12.

PC + LAC: Cuando una máquina corre naturalmente L2TP, también puede participar en el túnel, sin la necesidad de un LAC separado, es decir, estará conectado directamente a Internet, ver Grafico 13.

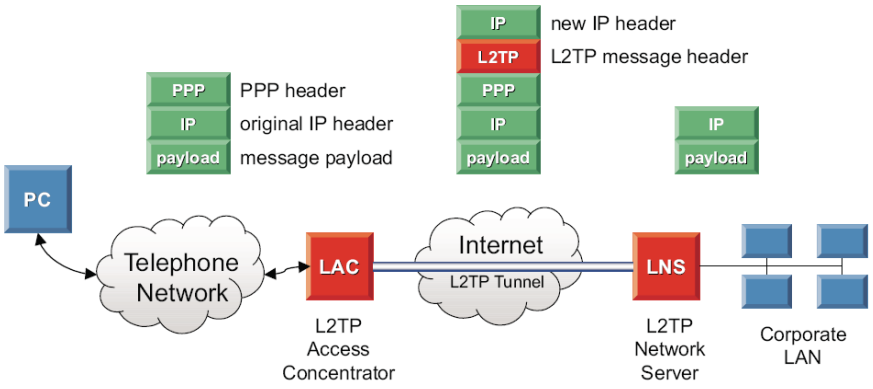


Grafico 12. Conexión L2TP

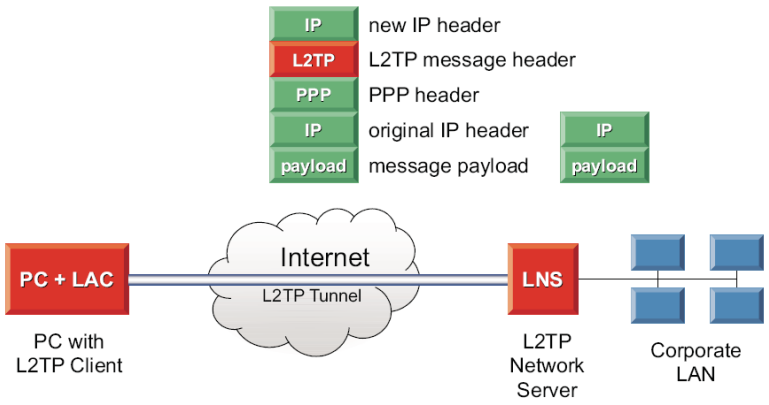


Grafico 13. Conexión L2TP con PC +LAC

L2TP utiliza dos tipos de mensajes:

De Control: Se utiliza para el establecimiento, mantenimiento y borrado de los túneles y llamadas. Para garantizar el envío utilizan un canal de control confiable dentro de L2TP.

De Datos: Estos mensajes encapsulan los marcos PPP y los envía a través del túnel.

El Gráfico 14 muestra la relación entre los paquetes PPP y los mensajes de control a través de los canales de control y datos de L2TP.

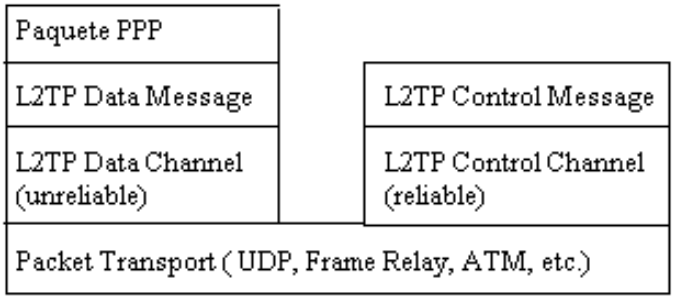


Grafico 14. Relación entre paquetes PPP y mensajes de control

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

2.4.3.3 L2TP – Autenticación/Encriptación

La autentificación se realiza en 3 fases:

- **Primera Fase:** El LAC inicia un túnel de conexión al servidor de red y da inicio a una sesión con el fin de devolver la información autentificada.
- **Segunda Fase:** A la segunda fase le da inicio el servidor de red y en ésta se decide si acepta o no la llamada. Al iniciar la llamada se indica al ISP que autenticación se va a utilizar como: CHAP, PAP, EAP u otra. Esta información será utilizada por el servidor de red para decidir si acepta o rechaza la llamada.
- **Tercera Fase:** Una vez aceptada la llamada el servidor de red inicia la tercera fase de autenticación a la capa PPP.

Mediante estas 3 fases de autenticación el protocolo L2TP garantiza al usuario final, ISP y al servidor de red que están con quien dice ser.

2.4.3.4 CARACTERISTICAS.

- Es estándar aprobado por la IETF (Internet Engineering Task Force).
- Progreso combinado de PPTP y L2F.
- Este protocolo no posee el cifrado y la autenticación por paquete, esto puede dar lugar a suplantaciones de identidad en algún punto interior del túnel, razón por la cual tiene que combinarse con otro protocolo, por ejemplo IPSEC.
- Al estar combinado con el protocolo IPSEC L2TP ofrece integridad de datos y la confidencialidad que exige una VPN.
- Permite el encapsulado de los protocolos como IP, IPX, NetBEUI….
- L2TP usa la funcionalidad de PPP para realizar la autenticación, es decir, PAP y CHAP.
- Brinda la opción de gestionar múltiples sesiones sobre un mismo túnel.
- Establecimiento de múltiples túneles a un mismo sitio, pero con calidad de servicio diferente, en función del medio, por ejemplo, y permite asignar dichos túneles a usuarios o clases de usuarios.

2.4.4 L2TP/IPSec

A pesar de que PPTP y L2TP son los primordiales protocolos de túneles que se utilizan en Windows 2000 o Windows 2003, se puede construir una VPN utilizando el protocolo IPSec que es usado para encriptar los paquetes L2TP. Este protocolo utiliza un modo específico el modo de túnel ESP que ofrece al datagrama IP un fuerte encapsulado y cifrado cuando es enviado en una red IP pública. El datagrama IP es encapsulado con una nueva cabecera IP y el nuevo datagrama que se obtiene se envía a través de la red. Al recibir el datagrama L2TP, el receptor procesa los datos para autenticar el contenido y envía los datos al lugar de destino.

El resultado después de aplicar ESP se muestra en el Gráfico 15.

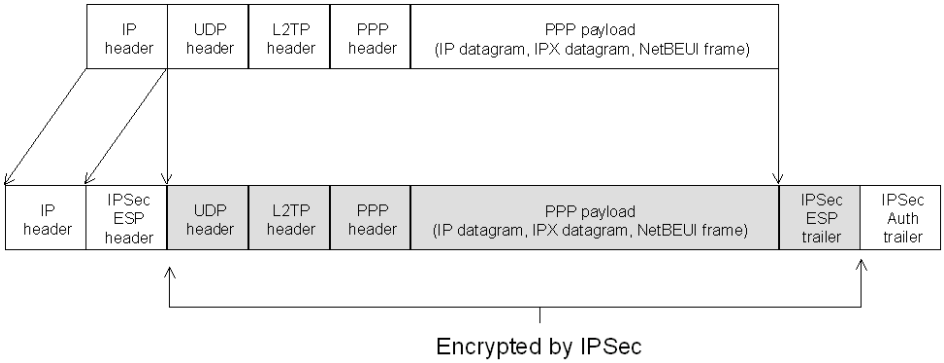


Gráfico 15. Encriptación de un paquete L2TP con IPSec ESP

2.4.5 IPSEC (IP SECURITY PROTOCOL)

Es un protocolo de la Capa de Red (Nivel 3 Modelo OSI) que proporciona seguridad a IP y a los protocolos de capas superiores basadas en IP (TCP, UDP, entre otros). Fue desarrollado para IPv6 pero se a implementado también en IPv4.

Realmente IPSec mejora la seguridad del protocolo IP para garantizar la privacidad, integridad y autenticación de los datos enviados por una red privada o pública como internet.

Se lo puede utilizar como una solución completa de protocolo VPN o brindar encriptación para L2TP o PPTP.

Ipsec provee Autenticación de usuario, Confidencialidad de datos y Administración de claves, pero no está atado a ningún algoritmos de cifrado, seguridad, método de autenticación, o alguna tecnología de claves en concreto; ya que es un protocolo estándar que permite que cualquier nuevo algoritmo sea utilizado.

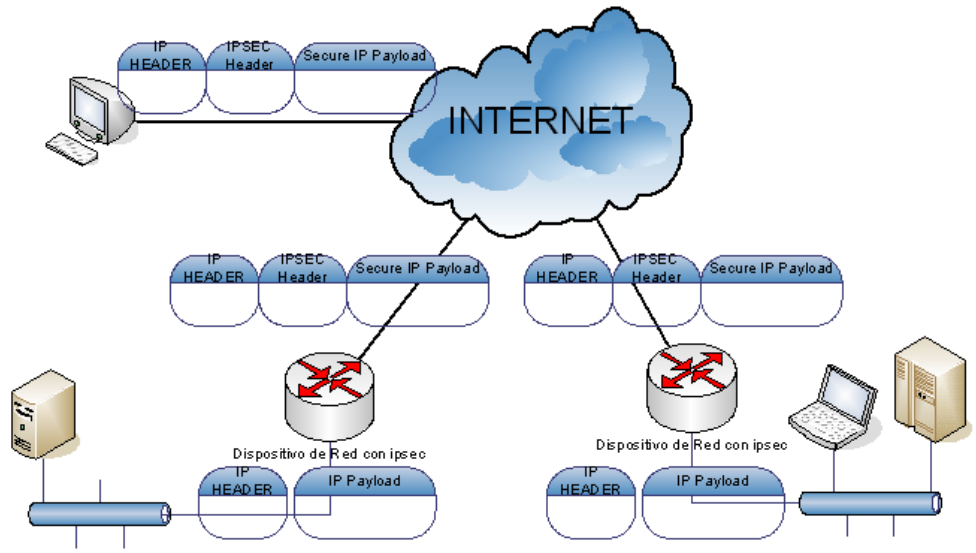


Gráfico 16. Escenario de uso IPSec

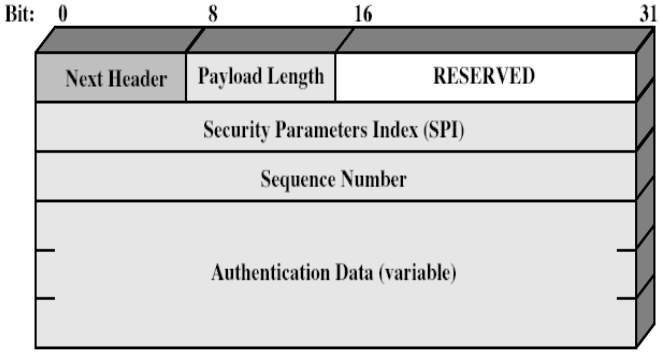
Brinda los siguientes servicios:

- Control de Acceso
- Autenticación de Origen y destino de los datos
- Rechazo de paquetes reenviados
- Confidencialidad (encripción)
- Creación de VPNs seguras

El concepto más importante que define IPSec es el de Asociación de Seguridad (SA) que ofrece servicios de seguridad al tráfico que viaja por ella, estos servicios son suministrados por dos cabeceras que son añadidas al nivel IP, estas vienen de los dos protocolos que tiene IPSEC: AH (Authentication Header) y ESP (Encapsulating Security Payload).
Ambos protocolos se basan en la utilización de varios algoritmos criptográficos previamente negociados que proporciona integridad de los datos y autenticación del origen de los mismos, como HMAC para la integridad y autenticación; y NULL, DES, 3DES para la encripción.

Cabecera de Autenticación (Authentication Header, AH): Suministra autenticación e integridad de datos, un servicio opcional anti reenvío de mensajes, pero no confidencialidad (es decir, los datos transmitidos pueden ser vistos por terceros). Este protocolo calcula una HMAC basada en la

clave secreta, el contenido del paquete y las partes inalterables de la cabecera IP, a continuación se añade la nueva cabecera AH al paquete.



17. Formato de Cabecera AH

CAMPO	BITS	DESCRIPCION
Next Header	8	Identifica el tipo de header del paquete
Payload Length	8	Largo del AH en multiplos de 32 bits
Reserved	16	Para uso futuro
SPI	32	Identifica el SA en la tabla SAD
Sequence Number	32	Numero de secuencia que crece con cada paquete
Authentication Data	Var	Contiene el MAC del paquete (Integrity Check Value)

Tabla 1. Descripción de campos de cabecera AH

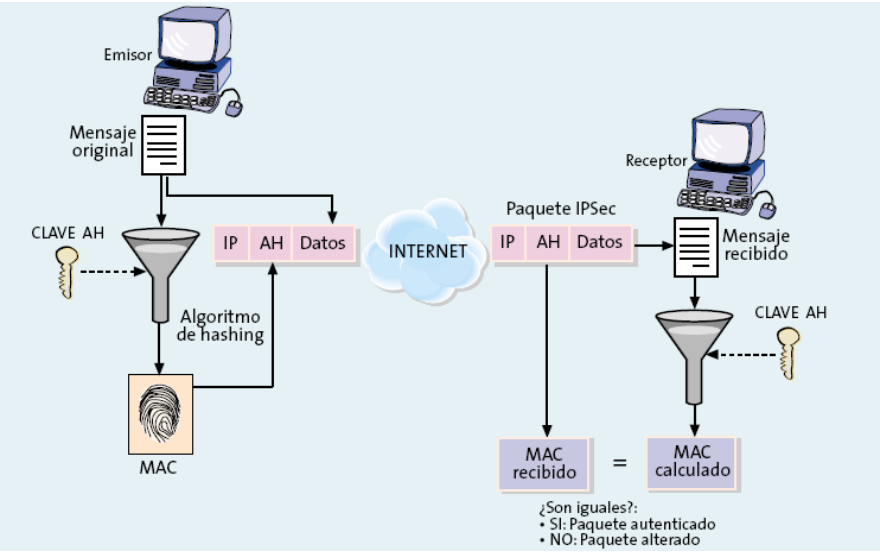


Gráfico 18. Funcionamiento del protocolo AH

Encapsulado de Seguridad de la Carga (Encapsulating Security Payload, ESP): Provee principalmente confidencialidad de los datos ya que los encripta (soporta varios cifradores como: Triple-DES, RC5, IDEA, etc), y además autenticación e integridad de la carga útil empleando una HMAC (Hash Message Authentication Codes). La cabecera ESP es generada y luego añadida al paquete después de cifrarlo y calcular su HMAC.
Para cifrar utiliza algoritmos como: DES, Triple-DES, RC5, IDEA, CAST, etc.

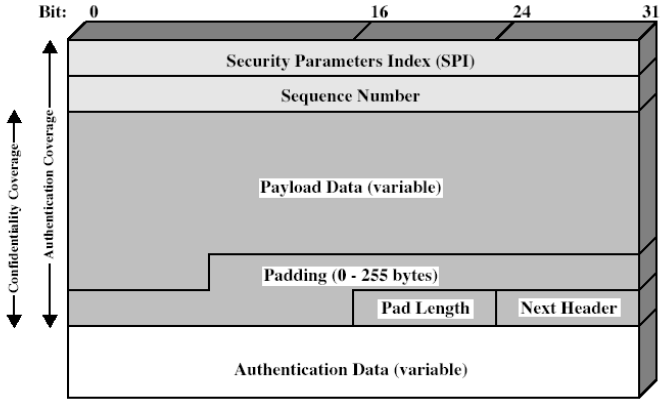


Gráfico 19. Formato de cabecera ESP

CAMPO	BITS	DESCRIPCION
SPI	32	Identifica el SA en la tabla SAD
Sequence Number	32	Numero de secuencia que crece con cada paquete. Para el servicio de anti reenvío
Payload Data	Var	Es el paquete TCP (transporte) o IP (túnel) encriptado
Padding	Var	0-255 bytes se lo alinea a multiplo de 32 bits.
Pad Length	8	Longitud del relleno
Next Header	8	Identifica el tipo de los datos contenidos en el campo "payload"
Authentication Data	Var	Contiene el MAC (opcional)

Tabla 2. Descripción de campos de cabecera ESP

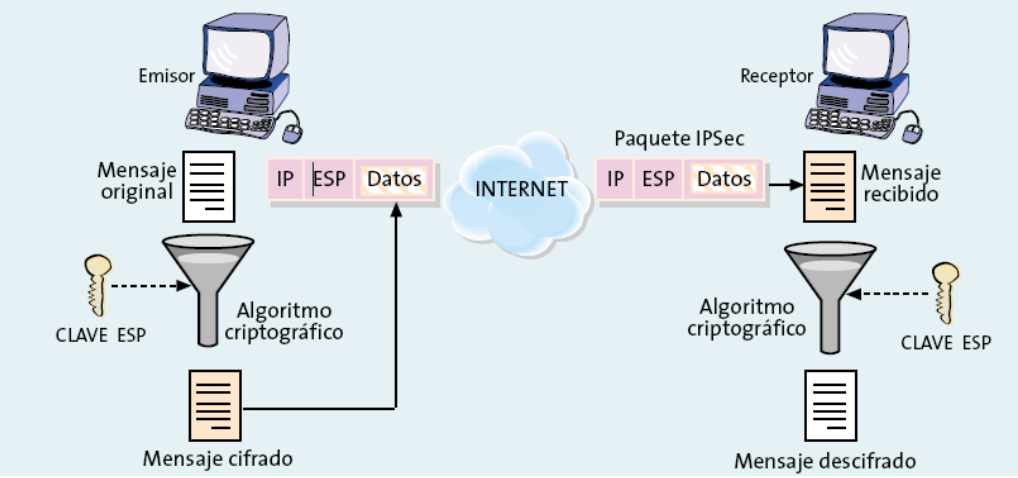


Gráfico 20. Funcionamiento del protocolo ESP

2.4.5.1 FUNCIONAMIENTO

IPSec tiene dos modos de funcionamiento para sus protocolos: Modo de transporte y Modo de Túnel.

Modo Túnel: Usando este modo se protege todo el datagrama IP, es decir éste es encapsulado íntegramente dentro de un nuevo datagrama IP que utiliza el protocolo IPSEC (AH o ESP). Cuando se usa ESP se encripta el paquete original y si utilizamos AH se autentifica también la parte del header.

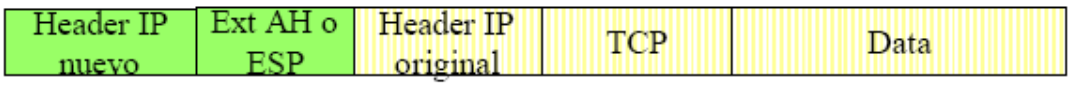


Gráfico 21. Paquete en Modo Túnel

Modo Transporte: Usando esta modo solo se protege la carga útil del datagrama IP, ésto se hace insertando la cabecera del protocolo IPSec (AH o ESP) entre la cabecera IP y la cabecera de las capas superiores de (TCP, UDP, ICMP).

Cuando este modo usa el protocolo ESP se encripta la carga (IP Payload) y si se utiliza AH autentifica los headers y la carga (IP Payload).

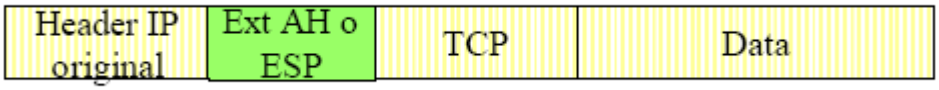


Gráfico 22. Paquete en Modo Transporte

Asociación de Seguridad (SA)

Son relaciones unidireccionales entre un emisor y un receptor, que son muy importantes, ya que permiten conocer la información de cómo se van a procesar los paquetes: los algoritmos de seguridad, las claves utilizadas, protocolos AH y/o ESP, el modo de trasporte o túnel, etc.

Si se necesita proteger ambos sentidos de la comunicación son necesarios dos SA. La administración de las claves se puede realizar manualmente o con el protocolo de intercambio IKE (la mayoría de veces), esto permite que ambas partes se escuchen entre sí.

SA Bundle es la asociación de varias SA. A cada paquete se puede aplicar más de un SA.

Ejemplo: ESP para asegurar el contenido y AH con el header.

- EL primer SA es para el ESP
- EL segundo para el AH

Las Asociaciones de Seguridad (SA) están definidas principalmente por 3 parámetros:

SPI (Security Parameters Index): Es un campo de 32 bits, permite identificar la entrada en la tabla de SA, es enviado en el paquete de AH o ESP para que la otra parte identifique el SA asociado.

Este e s enviado con el paquete, y una entrada del SA está compuesto por:

SPI + IP Destination Address + IPSec Protocol (AH o ESP).

IP Destination Address: IP destino del SA.

Security Protocol Identifier: Identifica si la asociación es un AH o un ESP.

Pero además tiene otros parámetros:

Contador de número de secuencia: utilizado para generar el número de secuencia en header AH o ESP.
Desbordamiento del contador de secuencia (Flag de overflow): Detiene la SA.
Ventana de Anti repetición: Evita la repetición de mensajes
Información AH: algoritmos de autentificación, llaves, tiempo de vida de llaves y otros parámetros.
Información ESP: algoritmos de encriptación y autentificación, valores de inicialización, llaves, tiempo de vida de llaves y otros parámetros.
Tiempo de vida de la SA: tiempo de vida del SA luego del cual se debe abrir un nuevo SA o terminar el actual.
Modo del protocolo IPSEC: Túnel o Transporte
Unidad de Trasmisión máxima de camino (MTU): Máximo MTU sin fragmentación observado.

SAD (Security Asocciation Databases): Las SA se almacenan en Base de datos de Asociaciones se Seguridad (SAD), en cada implementación IPSec hay una única SAD que por cada entrada tiene los mismos parámetros de una SA.
Las entradas se identifican por la trupla: Dirección de destino IP, Protocolo PSec y SPI.

SPD (Security Policy Database): Las asociaciones de seguridad especifican como vamos a proteger el tráfico, pero para definir qué tráfico vamos a proteger, necesitamos más información que se almacena en la Política de Seguridad (SP - Security Policy), que a la vez se almacenan en la Base de Datos de políticas de Seguridad SPD (Security Policy Database).
SPD es algo parecido a un filtro de paquetes que permite seleccionar entre los que deben pasar directamente y los que deben ser protegidos por IPSec (de éstos paquetes muestra que servicios brindan y de qué manera los van a ofrecer).

Una **SP** tiene los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transporte son las mismas direcciones que las de un SA, mientras que en modo túnel pueden ser distintas.

- Protocolos y puertos a proteger.
- La AS a utilizar para proteger los paquetes.

Las bases de datos de políticas de seguridad se utilizan para paquetes salientes. Se ingresa al SPD por medio de los campos del IP (Selector fields), éstos son:
Dirección de destino (Dest IP), Dirección de origen (Source IP), Capa de Transporte de Protocolo (Transport Protocol), Protocolo IPSEC, Puertos origen y destino (Source & Dest Ports), etc.

Una SPD contiene entradas que definen subconjuntos del trafico IP y apuntan a uno o más SA (que se encuentran en una SAD) para ese tráfico, es decir cada entrada de SPD tiene asociada la entrada a SAD; en caso de que no haya ninguna entrada SAD que se esté disponible, se creará una nueva SA.

PROCESAMIENTO IPSEC DE SALIDA

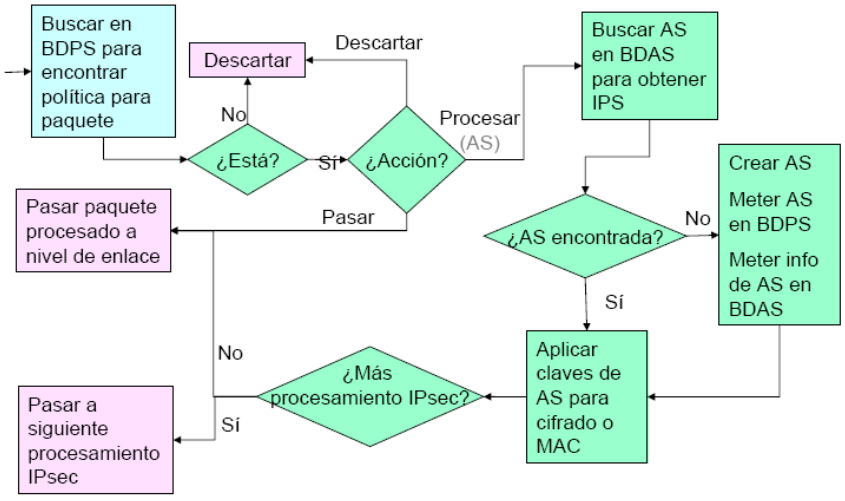


Gráfico 23. Procesamiento IPSec de salida

PROCESAMIENTO IPSEC DE ENTRADA

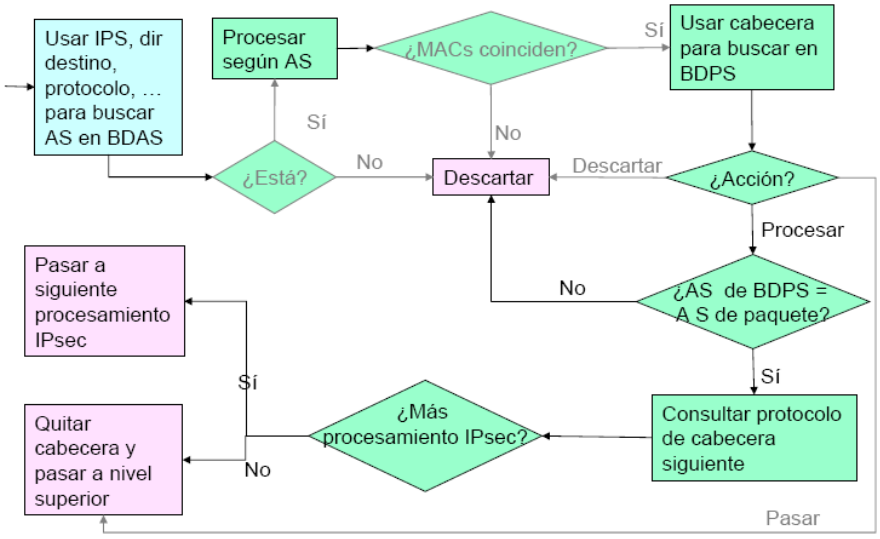


Gráfico 24. Procesamiento IPSec de entrada

COMBINACIONES DE SA

Los SAs pueden implementar AH o ESP, para implementar ambos se deben combinar las SAs.

Existen 4 tipos de combinaciones:

- **Entre sistemas finales**: Con IPSec y clave secreta compartida, en este caso pueden haber una o más ASs, usando:
  - AH o ESP en modo transporte
  - AH seguida de ESP, ambos en modo transporte
  - Cualquiera de las anteriores, dentro de AH o ESP en modo túnel

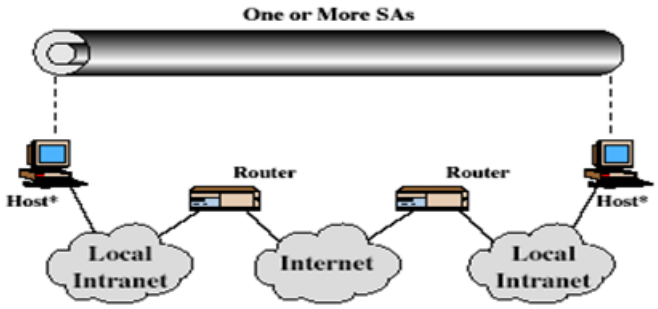


Gráfico 25. Combinación de SAs entre sistemas finales

- **Entre gateway/routers:** En este caso IPSec está solo en el túnel, no en los sistemas finales. Se trata de una Red privada virtual (VPN).
  Una AS en modo túnel que permita:
  AH, ESP (sólo confidencialidad) o ESP (confidencialidad + autenticación)

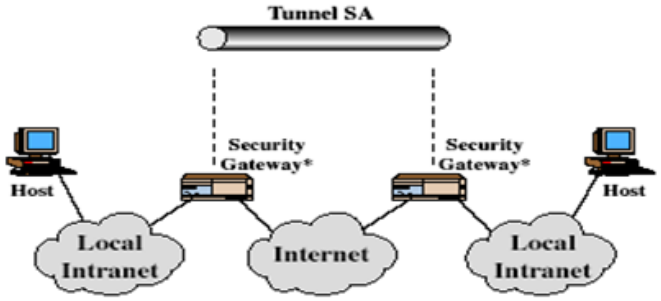


Gráfico 26. Combinación de SAs entre gateway/routers

- **Combinación de 1 y 2:** En este caso tenemos un túnel entre los 2 gateway/routers; y seguridad adicional en las redes locales, un ejemplo puede ser ESP en modo túnel y llevando AH en modo trasporte.

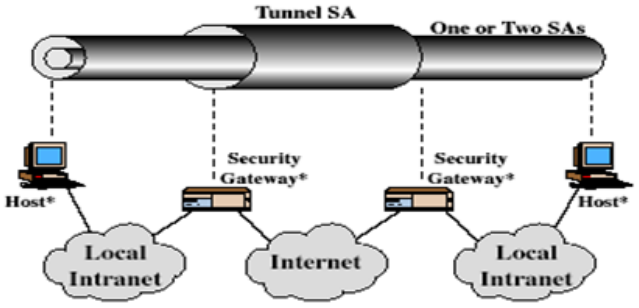


Gráfico 27. Combinación de SAs de paso 1 y 2

- **Soporte para sistema remoto**: En este caso el tráfico es protegido por el túnel interior hasta el servidor (como en el caso1), y el túnel externo protege el tráfico interno por internet.

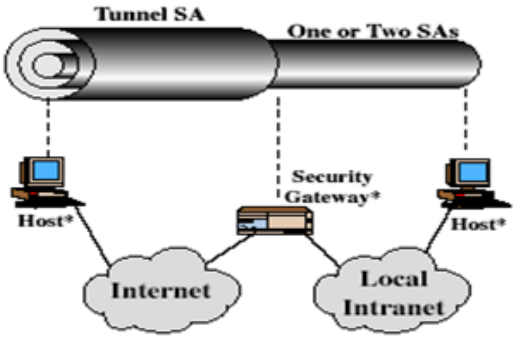


Gráfico 28. Combinación de SAs para sistema remoto

2.4.5.2 ADMINISTRACION DE CLAVES

Las SAs pueden ser definidas en forma manual o dinámica, los protocolos AH y ESP necesitan de claves de autenticación y de cifrado, a través de este proceso las partes negocian y establecen las SAs que necesita IPSec.
Típicamente se requieren cuatro claves para la comunicación entre dos nodos: un par (AH, ESP) para cifrar cuando se transmite y otro par para autentificar cuando se recibe.
La criptografía (cifrado) puede ser de dos tipos:

Criptografía simétrica: Usan una única clave (secreta) que deben conocer emisor y receptor, con ésta se cifra y se descifra.

Criptografía asimétrica: Utilizan un par de claves, una privada y otra pública, lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa.

Manejo manual: En esta forma es una persona la que se encarga de configurar manualmente en ambos nodos los sistemas con claves y SAs. Es útil para redes pequeñas y estáticas puesto que en estos casos no se tiene que proteger todo el tráfico. Utiliza claves simétricas, no es escalable y no es seguro, ya que las claves secretas y algoritmos de cifrado deben ser conocidas por todos los que formen parte de la VPN.

Manejo Automático: En este caso el sistema crea automáticamente en demanda de claves para los SA.

El protocolo por defecto para la gestión de claves que utiliza es el Intercambio de Claves por Internet (IKE, Internet Key Exchange), se basa en el protocolo UDP y utiliza cifrado de clave pública para realizar el intercambio seguro de claves de sesión y otros atributos en un dominio de direcciones. Se utiliza para establecer las SAs.

IKE tiene 2 fases:

Fase 1: Establece una asociación de seguridad ISAKMP (Internet Security Association Key Management) entre los extremos, y se establece un secreto del que se derivan las claves. Utiliza criptografía asimétrica.

Fase 2: En esta fase se utiliza la asociación de seguridad ISAKMP para crear la asociación de seguridad IPSec definitiva, que es la que establecerá las claves y otros parámetros a utilizar en la sesión. Además se negociará dos SAs, ya que éstas son unidireccionales.

2.4.5.3 CARACTERISTICAS DE IPSEC

- Ipsec es el estándar que proporciona seguridad en el nivel de red.
- Es el más conveniente para crear VPN, debido a sus poderosas medidas de seguridad y a los mecanismos de gestión de claves.
- Funciona directamente sobre IP y no sobre TCP/UDP, está diseñado para tráfico IP exclusivamente.
- Provee validación de usuarios
- Claves secretas compartidas por ambos extremos
- Es complejo de configurar
- Cuando se implementa en los Routers o Firewalls les brinda seguridad a los paquetes que circulan por ellos.
- Puede ser transparente a las aplicaciones y al usuario final
- Es aplicado para usuarios individuales
- La negociación de la conexión utiliza el protocolo ISAKMP

2.4.6 SELECCION DE PROTOCOLOS DE TUNEL

El momento que se necesite implementar una VPN se debe seleccionar el protocolo a utilizar para la creación del túnel y darle seguridad; IPSec, L2TP y PPTP proporcionan los mecanismos para eso. Esta selección se realizará en base a las ventajas e inconvenientes de cada uno, además de las diferencias entre ellos.

La diferencia entre estos protocolos de nivel 2(PPTP, L2TP) y nivel 3 (IPSec), radica en el mantenimiento del túnel, ya que los de nivel 2 necesitan que éste sea creado, mantenido y terminado; mientras que los capa 3 no necesitan de esto.

Si hablamos de seguridad los protocolos de nivel 2 no son suficientes para la creación de una VPN, ya que ninguno suministra las funciones de integridad, encriptación y autenticación que son realmente necesarias para mantener la privacidad de la conexión.

Entre las particularidades que aparecen cuando se usa IPSec tenemos:

- IPSec es un protocolo de capa de Red y fue diseñado para tráfico IP exclusivamente
- IPSec se puede instalar en tres partes: gateways de seguridad, clientes fijos y clientes móviles
- Conecta redes a través de gateways/routers de seguridad
- Facilita la gestión de claves, puesto que solo se necesitan claves entra las SAs de los routers.
- Permite elegir modo transporte o modo túnel, de acuerdo al grado de seguridad o privacidad que se quiera alcanzar.

PPTP, L2TP son muy similares (ambos se basan en el protocolo PPP), sin embargo existen ciertas diferencias significativas:

- PPTP necesita que la red sea IP, L2TP necesita que sólo el túnel provea conexión punto a punto orientada a paquetes. Además como L2TP utiliza UDP puede ser utilizado sobre Circuitos virtuales permanentes (PVC's) en Frame Relay, Circuitos virtuales en X.25 o ATM.

- PPTP únicamente soporta un túnel simple entre dos puntos, al contrario de L2TP que permite la utilización de múltiples túneles entre 2 puntos. Además se pueden crear distintos túneles de acuerdo a la calidad de servicio.
- L2TP permite compresión de cabeceras. Cuando esta compresión está habilitada, L2TP trabaja con 4 bytes de overhead en comparación con los 6 bytes de PPTP.
- L2TP puede aplicarse sólo cuando los equipos cliente ejecuten Windows 2000, Windows XP o Windows Vista.
- Aunque PPTP puede ser apto para impedir intrusiones de principiantes, es posible que los especialistas puedan acceder fácilmente a la información que viaja por el túnel.

Las siguientes son las ventajas de usar L2TP / IPSec sobre PPTP en Windows 2003:

- IPSec provee la autentificación de datos (la prueba de que los datos fueron enviados por el usuario autorizado), la integridad de datos (la prueba de que los datos no fueron modificados en el viaje), la protección de repetición (la prevención de reenviar un flujo de paquetes capturados), y la confidencialidad de datos (la prevención de interpretar paquetes capturados sin la clave de encriptación) por paquete. Al contrario de PPTP que provee sola la confidencialidad de datos de paquete.
- Las conexiones de L2TP / IPSec proveen la autentificación más fuerte requiriendo tanto autentificación de nivel de computadora por certificados como de nivel de usuario a través de un protocolo de autentificación de PPP.

Por todo esto podemos asegurar que IPSec es la mejor opción cuando se desea construir una VPN, ya que proporciona un marco de trabajo estándar y completo; y además porque otros protocolos suelen incorporar a IPSec para complementarse y cubrir las deficiencias de seguridad que tienen. Finalmente hemos decidido para la práctica usar en conjunto los protocolos L2TP/IPSec.

2.5 CONCLUSIONES

La aplicación de la tecnología de tunneling es muy ventajosa y permite establecer túneles por los que la información se transporta utilizando algunos protocolos que son importantes en el uso de las vpns, ya que cada uno de ellos con sus características y ventajas ayudan a que el envió de datos se realice de una manera segura ya que van encriptados, garantizando de esta forma que la información que se reciba sea confiable.

CAPITULO III

3. PRACTICAS DE LABORATORIO

3.1 INTRODUCCION

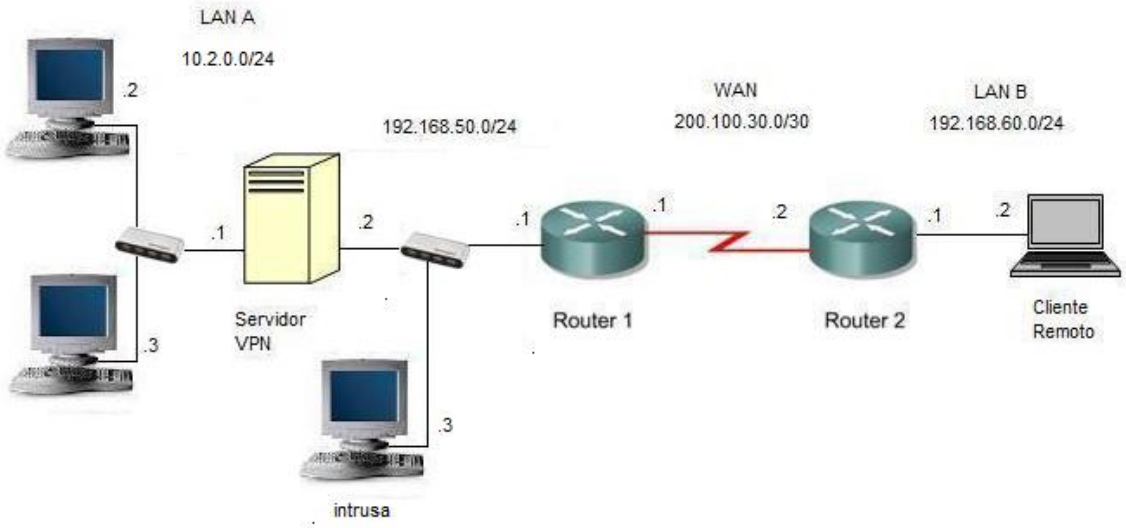
En este capítulo se muestra paso a paso las configuraciones necesarias para realizar una Red privada virtual, como son la configuración de la red que simulará a Internet, la configuración del servidor VPN con L2TP/IPSec en Windows Server 2003, la del cliente VPN en Windows Vista, y finalmente la captura de tráfico con la última versión de la herramienta Ethereal (Wireshark) que comprueba la diferencia de la información cuando viaja encriptada y cuando no.

3.2 PRACTICA 1: CONFIGURACION DE LA RED

Objetivo

Configurar la interfaz serial y Ethernet en cada uno de los dos routers para que se puedan comunicar entre sí, y de esta manera simulen al internet para que los usuarios se puedan conectar con la VPN.

El esquema que vamos a armar en esta práctica es el siguiente:



Paso1. Especificar el nombre de los routers, usando el siguiente comando:

(config)#**hostname** <nombre>

Router1:
(config)#**hostname** router1
Router2:
(config)#**hostname** router2

Paso 2. Configurar los interfaces que se vayan a utilizar en el router, realizando los siguientes pasos:

- Entrar en modo interfaz
  (config)#**interface** <tipo> <número>
  Para pasar del modo usuario al modo privilegiado, se escribe lo siguiente:
  (config)#**enable**
- Asignar una dirección IP al interfaz:
  (config-if)#**ip address** <dir_IP_interfaz> <máscara_red>
- Habilitar el interfaz para que esté operativo (config-if)#**no shutdown**
- Para los interfaces seriales, que hagan de extremo DCE, se debe especificar un reloj, para esta práctica el Router1:
  (config-if)#**clock rate** <velocidad_línea>

Router1:
(config)#**interface** ser1
(config-if)#**ip address** 200.100.30.1 255.255.255.252
(config-if)#**no shutdown**
(config-if)#**clock rate** 72000

(config)#**interface** eth0
(config-if)#**ip address** 192.168.50.1 255.255.255.0
(config-if)#**no shutdown**

Router2:
(config)#**interface** ser0
(config-if)#**ip address** 200.100.30.2 255.255.255.0
(config-if)#**no shutdown**

(config)#**interface** eth0
(config-if)#**ip address** 192.168.60.1 255.255.255.0
(config-if)#**no shutdown**

Paso 3. Ahora procedemos a configurar las tablas de ruteo para que ambas redes puedan verse entre sí:

Router1:
(config-if)#**Ip route** 0.0.0.0 0.0.0.0 200.100.30.2
(config-if)#**Ip route** 0.0.0.0 0.0.0.0 192.168.50.1

Router2:
(config-if)#**Ip route** 0.0.0.0 0.0.0.0 200.100.30.1

Paso 4. Para visualizar la configuración que se acaba de realizar se utiliza el comando:
#**show running-config**

Paso 5. Una vez configurado, para probar la conectividad con otros equipos de la red, se usa el comando:
ping

Paso 6. El momento que todo funcione correctamente con la configuración realizada, guardamos la configuración permanentemente en el router:

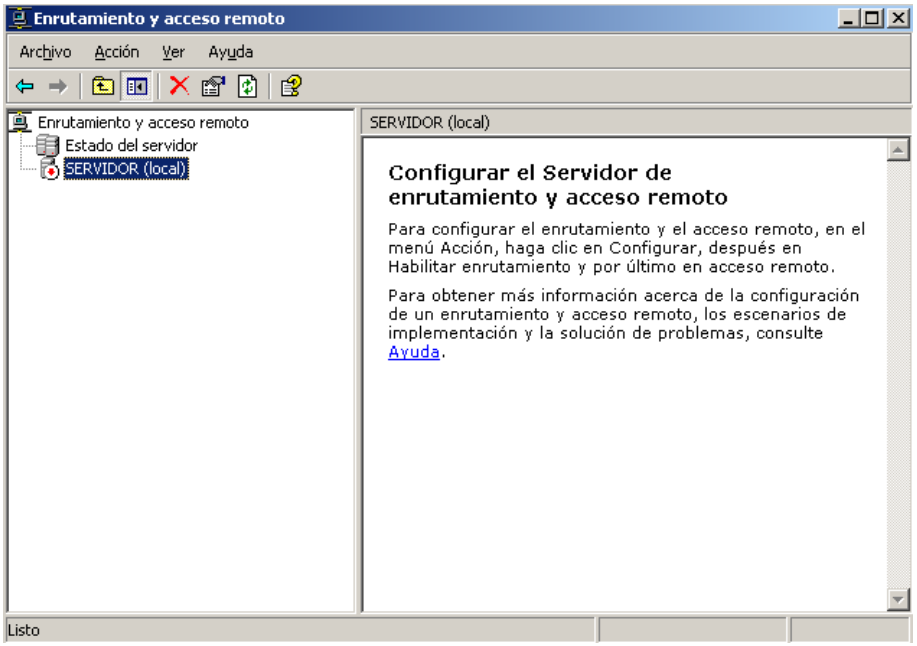
#**copy running-config startup-config**

PRACTICA 2. CONFIGURACIÓN DEL SERVIDOR

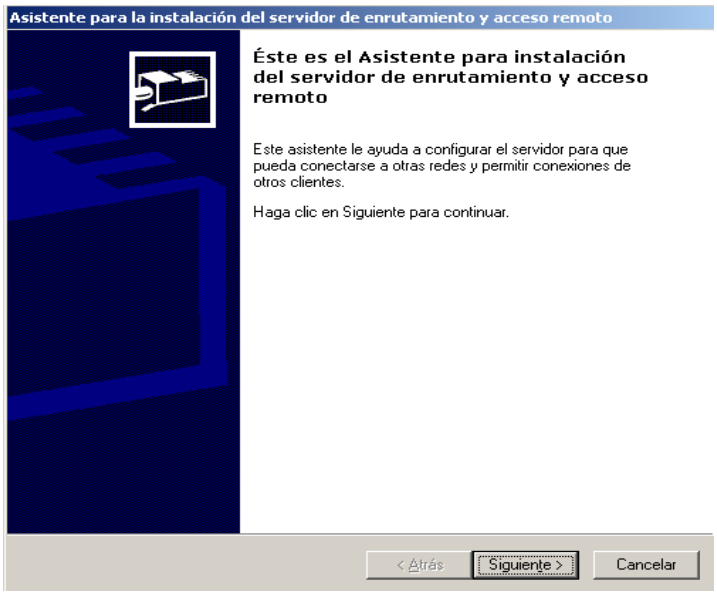
Objetivo

Configurar el servidor VPN con L2TP/IPSec en Windows Server 2003, además crear los usuarios que tendrán acceso a la red privada virtual.

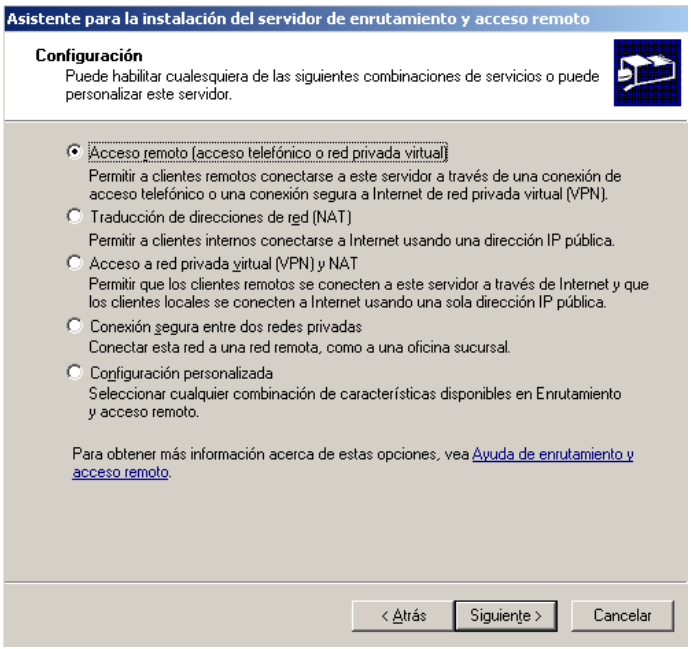
Paso 1. Hacemos clic en **Inicio > Herramientas administrativas > en Enrutamiento y acceso remoto**,



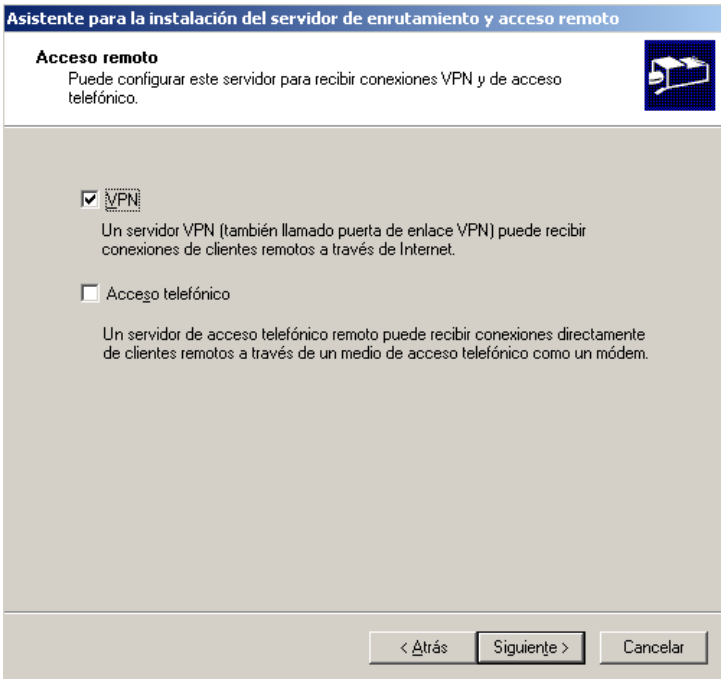
Paso 2. Luego hacemos clic derecho en el icono del servidor y seleccionamos **Configurar y habilitar Enrutamiento y acceso remoto**, esto iniciara el Asistente para instalación del servidor de enrutamiento y acceso remoto. Click en **Siguiente** para continuar.



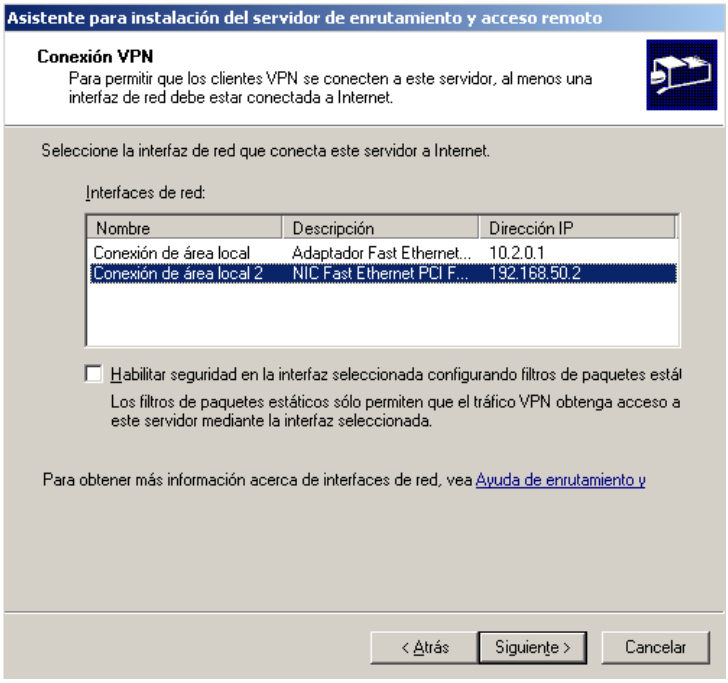
Paso 3. Click en **Acceso remoto (acceso telefónico o red privada virtual)** para activar los equipos remotos de forma que puedan marcar o conectarse a esta red a través de Internet. Click en **Siguiente** para continuar



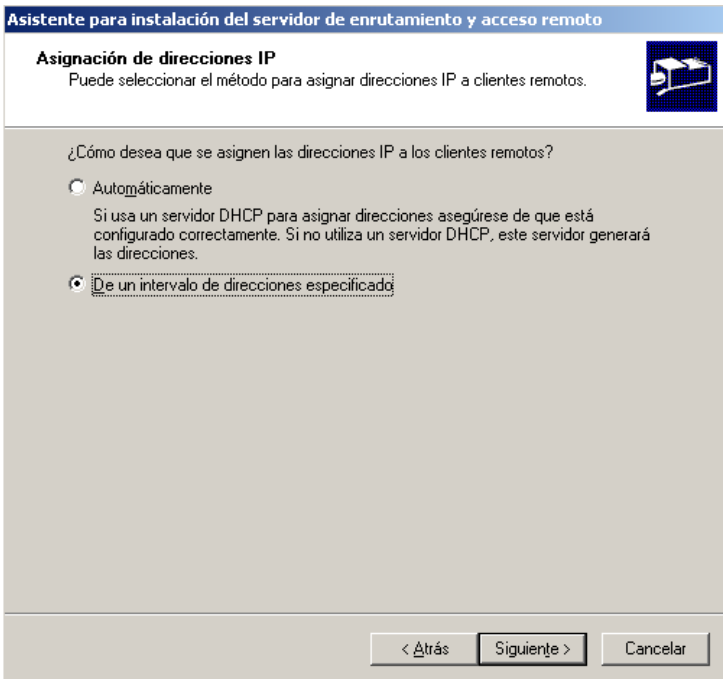
Paso 4. Ahora seleccionamos VPN



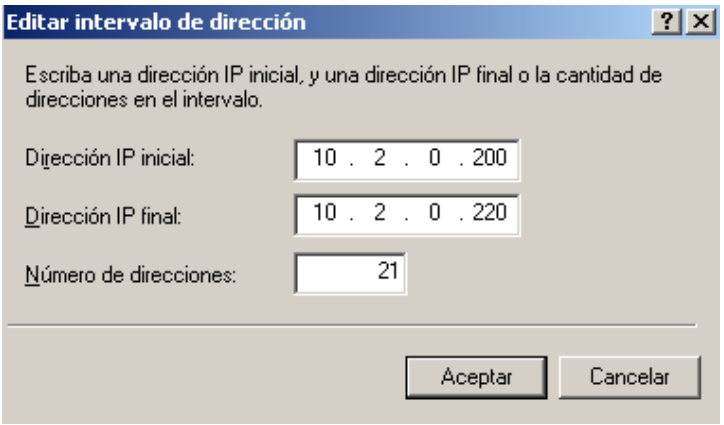
Paso 5. En esta ventana de Conexión VPN damos Click en la interfaz de red conectada a Internet, desactivamos la casilla que aparece y, después, hacemos Click en **Siguiente**.



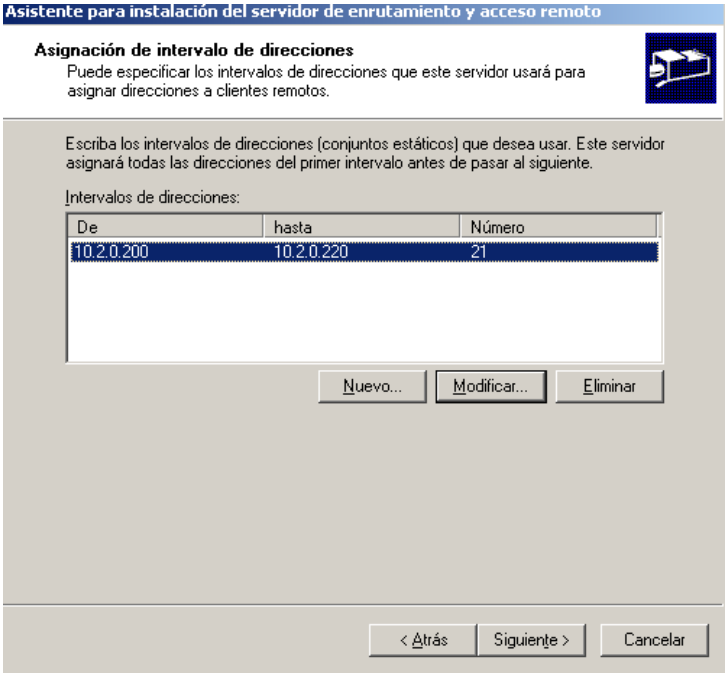
Paso 6. Luego aparece la ventana de Asignación de direcciones IP, se presentan dos opciones **Automáticamente** si se va a utilizar un servidor DHCP, o **De un intervalo de direcciones especificado**, que es el que vamos a utilizar para esta práctica, donde los clientes remotos sólo deben recibir direcciones de un conjunto predefinido, damos Click en **Siguiente:**



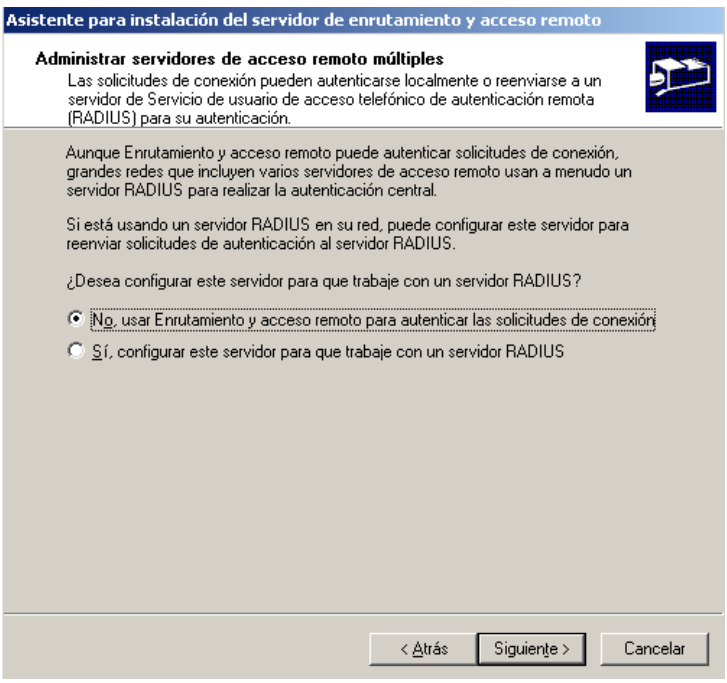
Paso 7. A continuación se abre un cuadro de Asignación de intervalos de direcciones, damos clic en **Nuevo** y escribimos el rango de direcciones que se van a asignar a los clientes remotos, hacemos Click en **Aceptar**



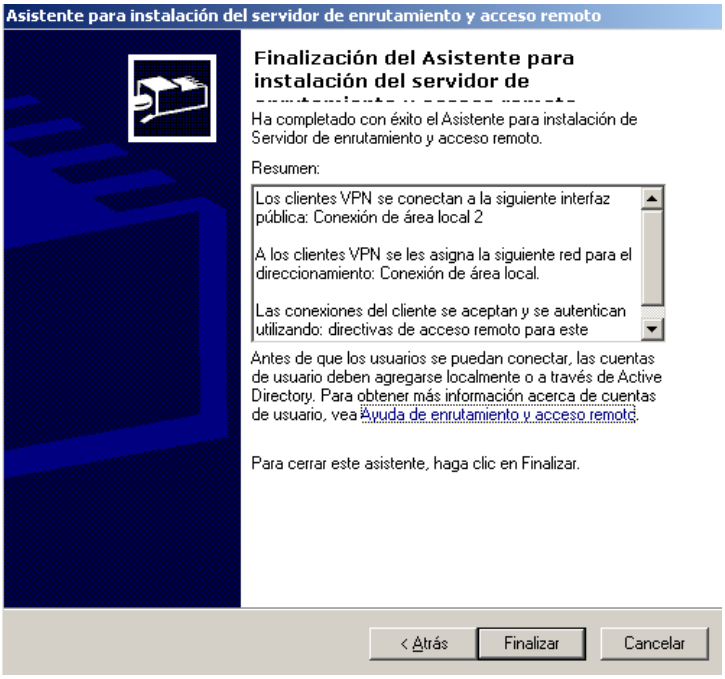
Paso 8. Damos Click en **Siguiente:**



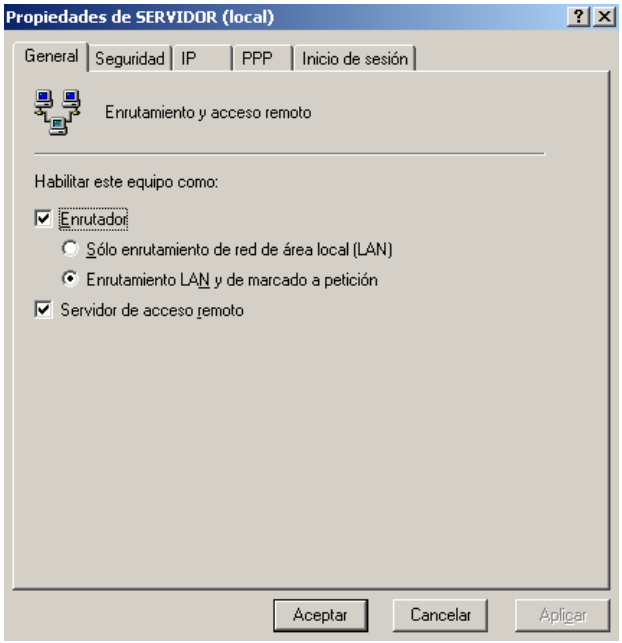
Paso 9. Aceptamos la opción predeterminada **No, usar Enrutamiento y acceso remoto para autenticar las solicitudes de conexión.** Click en **Siguiente** para continuar.



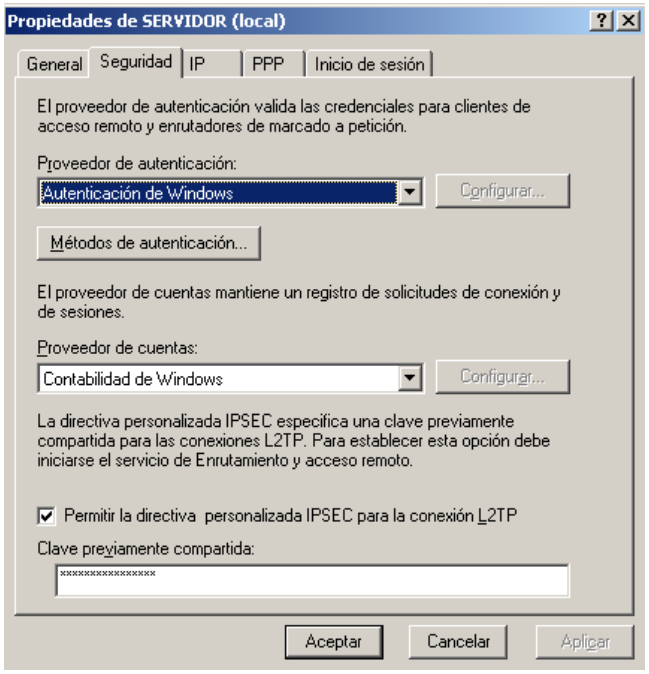
Paso 10. Hacemos click en **Finalizar** para activar el servicio Enrutamiento y acceso remoto, y para configurar el servidor como servidor de acceso remoto.



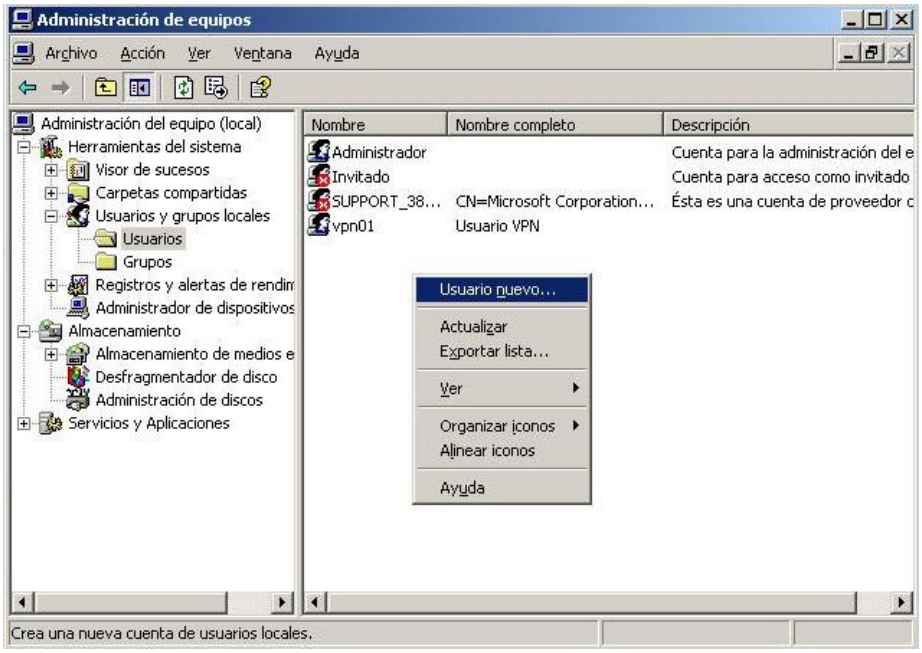
Paso 11. Ahora vamos a configurar el servidor como enrutador, para esto hacemos click con el botón secundario del mouse en el nombre del servidor y, a continuación, hacemos clic en **Propiedades**. En la pestaña **General** activamos **Enrutador** bajo Habilitar este equipo como, y hacemos clic en **Enrutamiento LAN y de marcado a petición**



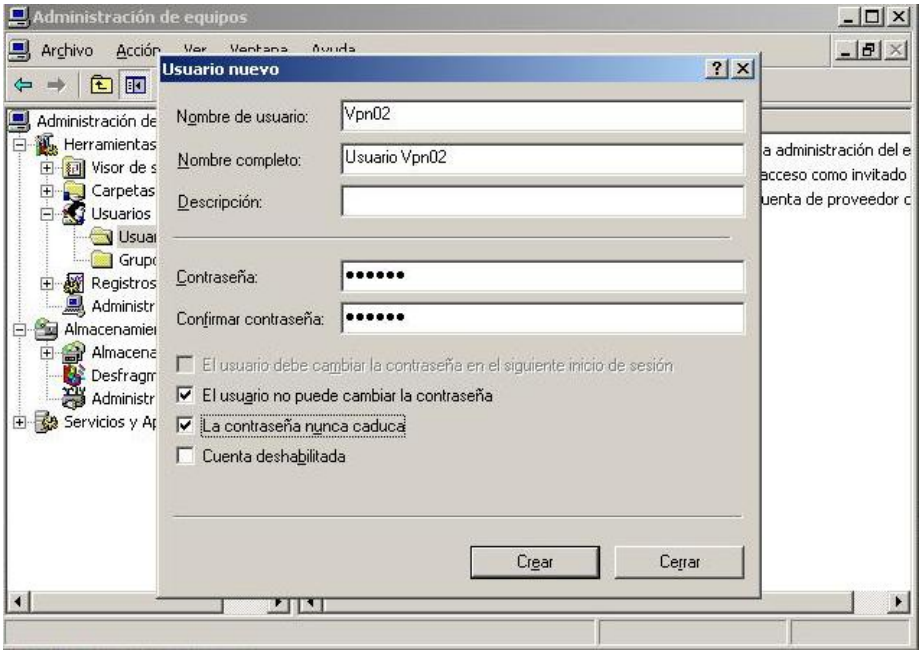
Paso 12. Ahora en la pestaña de **Seguridad** especificaremos que vamos a utilizar L2TP/IPSec, marcamos la opción **Permitir la directiva personalizada Ipsec para la conexión L2TP** y escribimos la clave que va a ser compartida entre el servidor y el cliente, damos click en **Aceptar:**



Paso 13. Después de haber configurado el servidor para que permita el enrutamiento y acceso remoto, vamos a configurar los usuarios que van a tener acceso a la VPN, vamos a **Inicio> Administración de equipos** seleccionamos **Usuarios y grupos locales** y damos click derecho en **Usuarios> Usuario nuevo:**

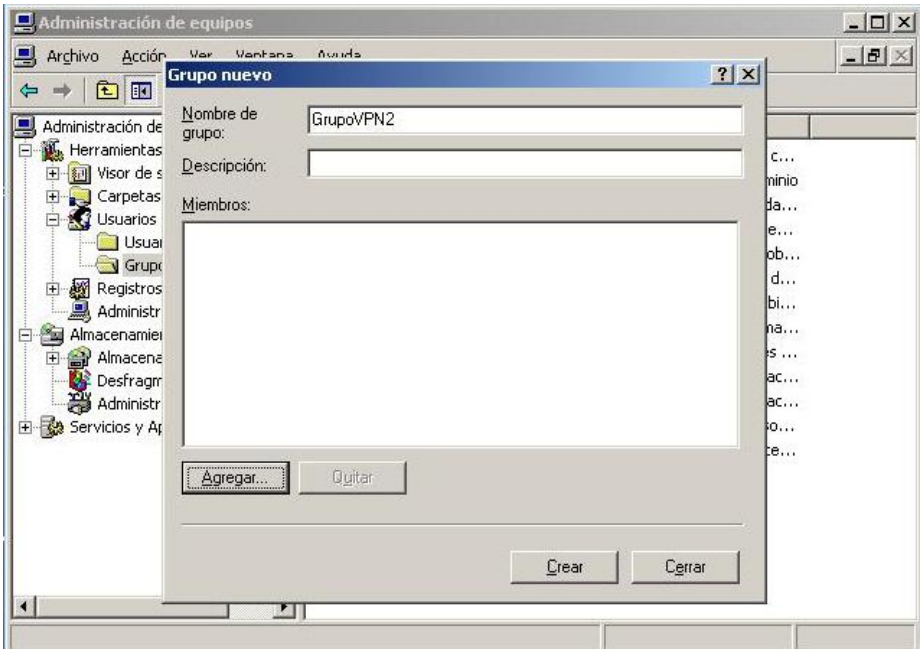


Paso 14. Escribimos el nombre y contraseña del usuario y habilitamos las opciones que se muestran a continuación, click en **Crear**:

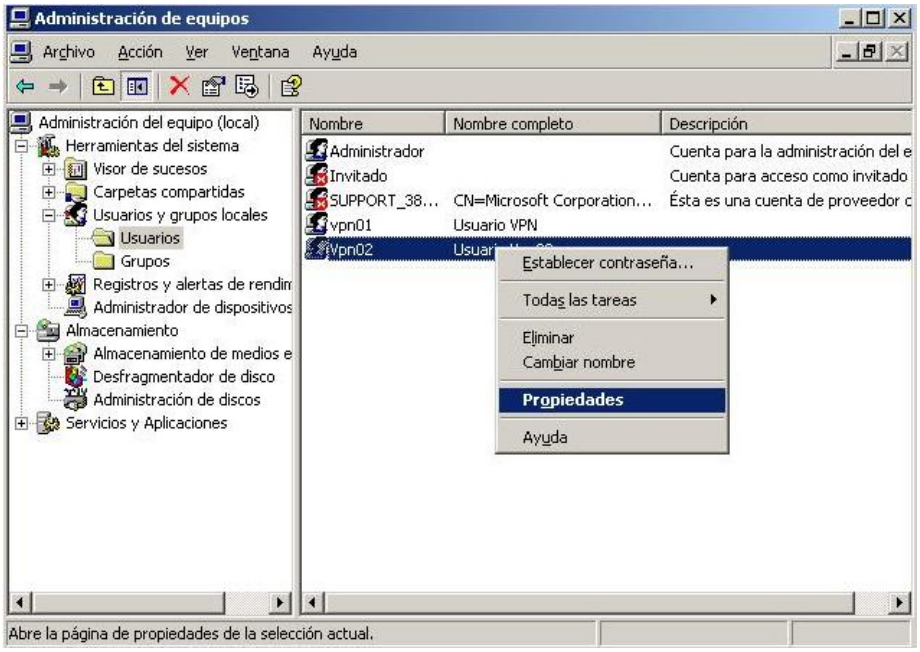


Paso 15. A continuación hacemos click derecho en **Grupos** y seleccionamos **Grupo nuevo**

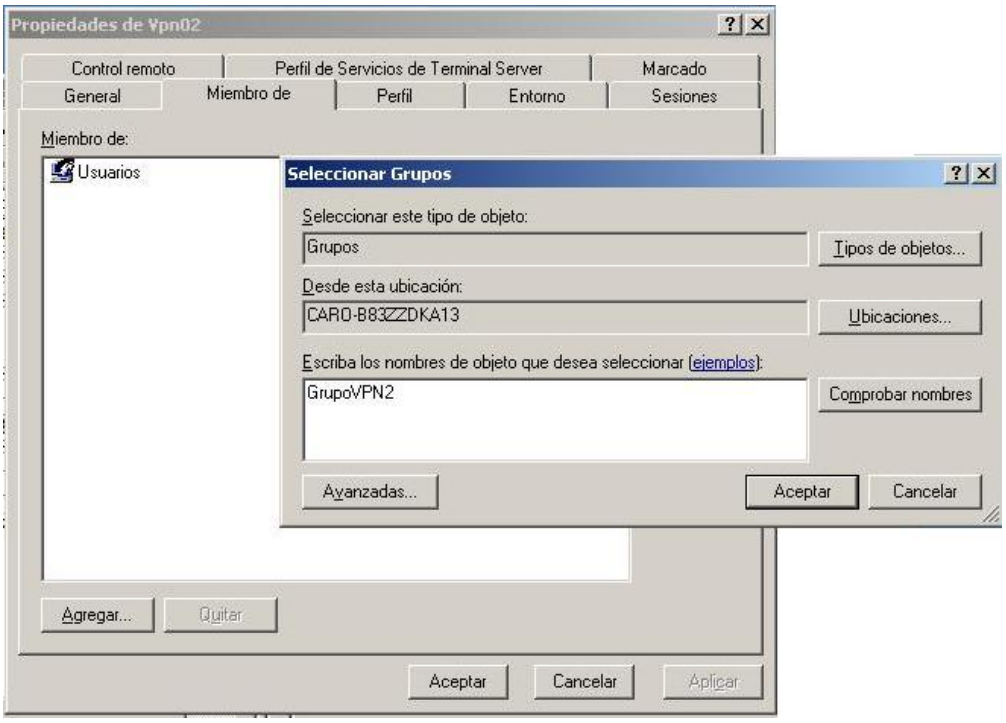
Paso 16. Escribimos el nombre del nuevo grupo al que va a pertenecer el usuario VPN. Click en **Crear:**



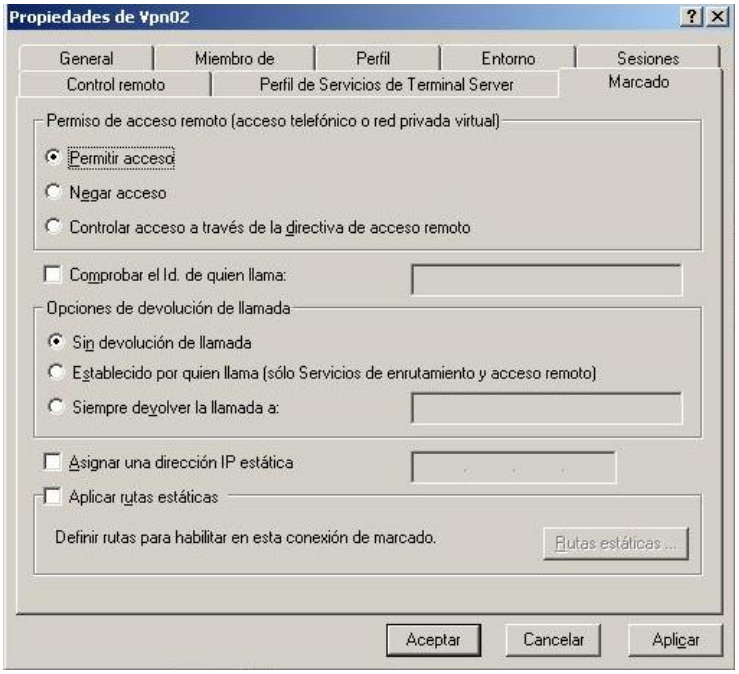
Paso 17. Una vez que se ha creado el usuario y el grupo, damos click derecho sobre el usuario y elegimos **Propiedades:**



Paso 18. En la pestaña **Miembro de**, escribimos el nombre del grupo que creamos y hacemos click en **Aceptar:**



Paso 19. En la pestaña **Marcado** seleccionamos lo siguiente, damos click en **Aceptar**:



Paso 20. Finalmente en **MiPc** hacemos clic en **propiedades** y en la pestaña **Acceso Remoto**, marcamos lo siguiente:

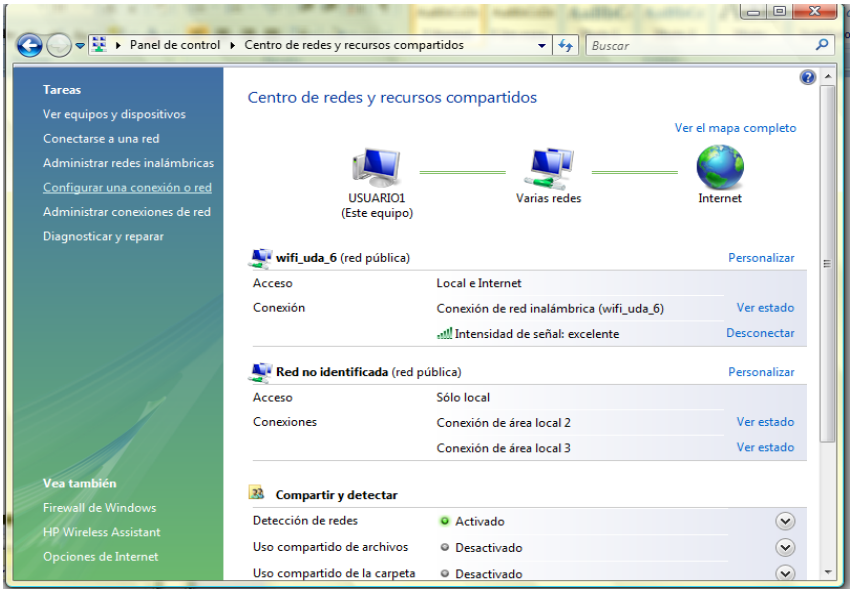
3.4 PRACTICA 3: CONFIGURACION DEL CLIENTE

Objetivo

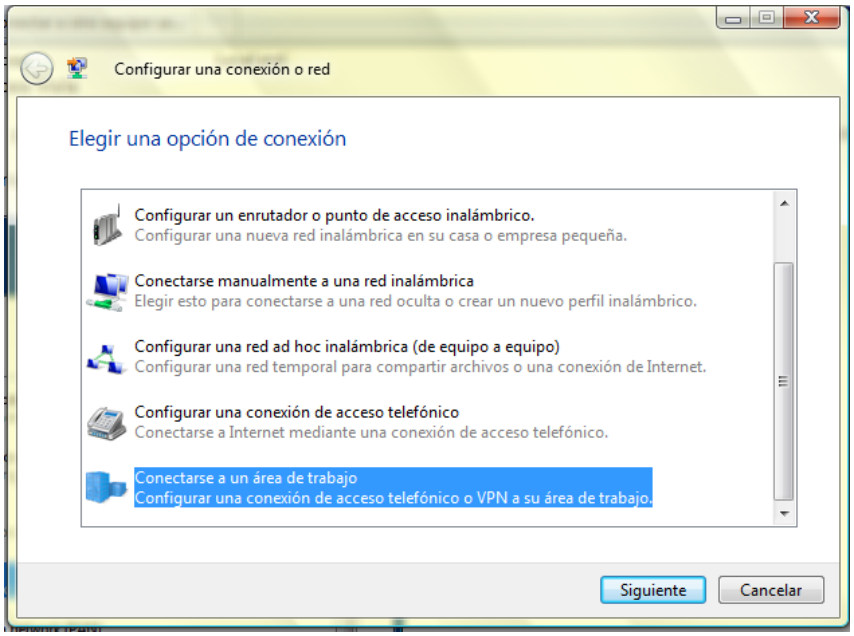
Crear una conexión de cliente VPN, para esto existen diferentes softwares, pero para la práctica usaremos Windows Vista que permite realizarlo de una manera rápida.

Los pasos a seguir son los siguientes:

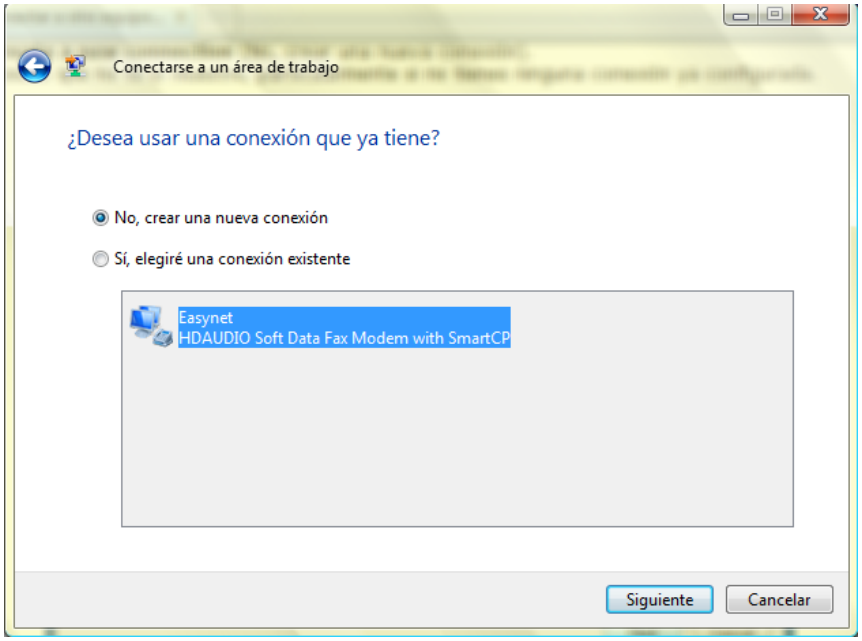
Paso1. En el panel de control, seleccionar **Centro de redes y recursos compartidos,** en las opciones de la izquierda, pulsamos **Configurar una conexión o red** tal como vemos a continuación:



Paso2. Esto hará que se inicie el asistente de nueva conexión, y tal como vemos en la siguiente figura, seleccionamos **Conectarse a un área de trabajo** y pulsamos en **Siguiente**

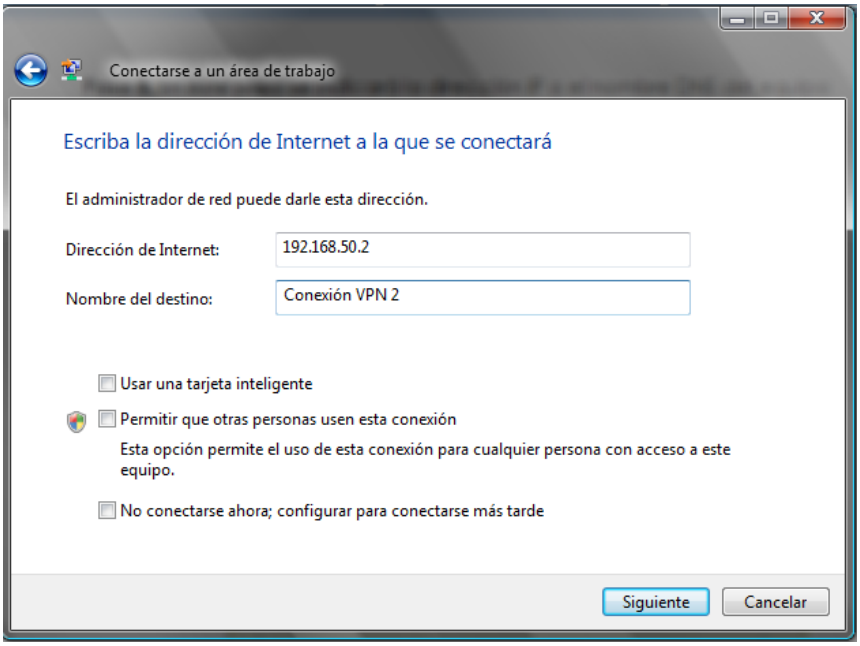


Paso 3. En el siguiente paso se mostrarán las conexiones que tengamos, aquí marcamos la opción **No, crear una nueva conexión** (es posible que este paso no se muestre si no se tiene una conexión configurada).

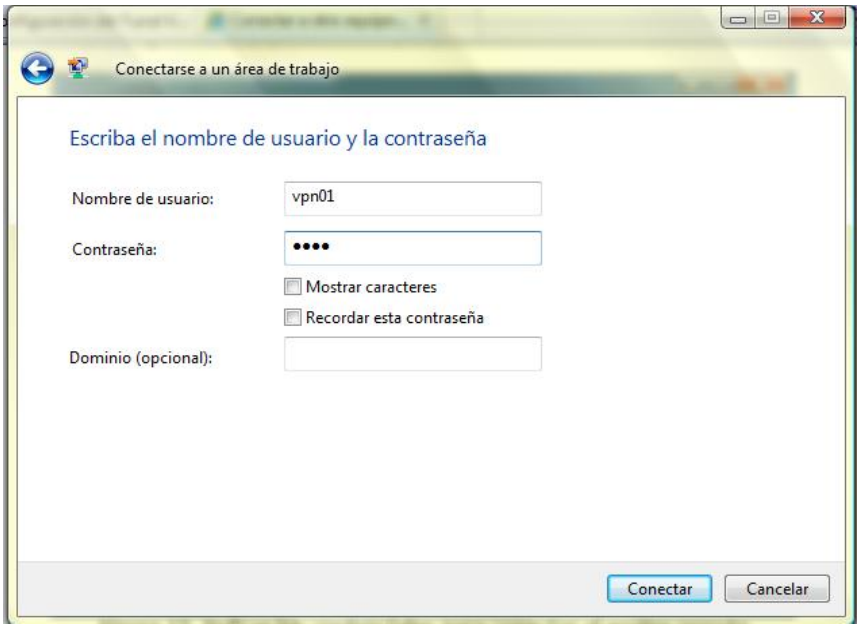


Paso 4. A continuación vamos a usar la conexión VPN, seleccionamos la opción que muestra **Usar mi conexión a Internet**.

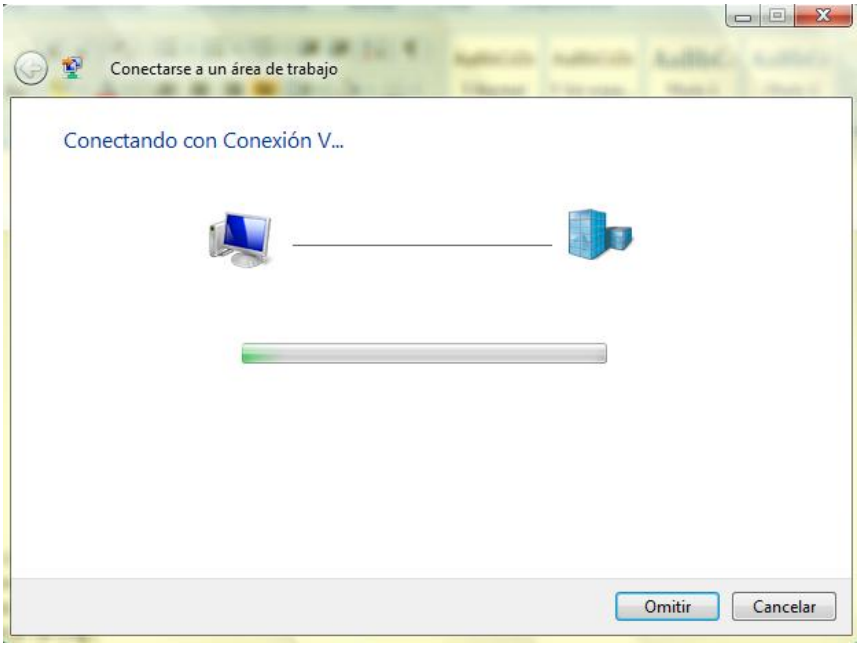
Paso 5. En este paso se indicará la dirección IP o el nombre DNS del equipo remoto al que nos queremos conectar:



Paso 6. Aquí indicamos el nombre de usuario y la contraseña; éstos deben coincidir con los datos que se tengan en el servidor (equipo remoto) al que queremos conectarnos.

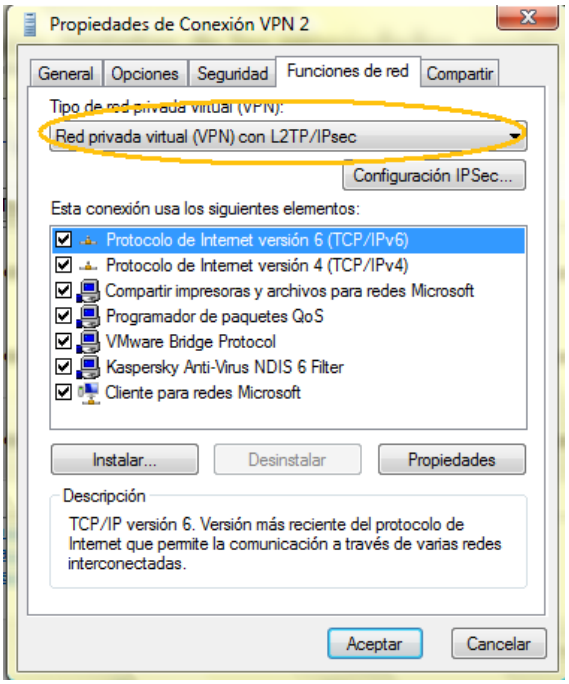


Y ya estaría lista la configuración del cliente, y empezará la conexión:

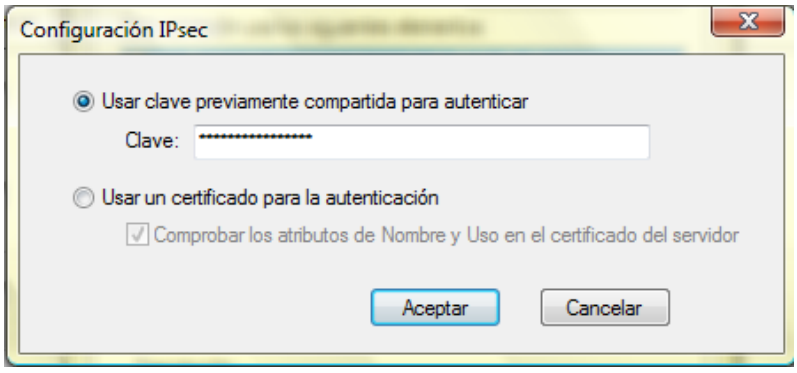


De esta manera tenemos configurado el cliente, pero hace falta especificar que protocolo de tunneling se va a utilizar, para esta práctica será L2TP/IPSec, debemos hacer lo siguiente:

Paso 7. Damos click derecho en la conexión VPN, seleccionamos **Propiedades** y en la pestaña de **Función de red** en **Tipo de red privada virtual (VPN)** elegimos lo siguiente:



Y luego en la misma ventana pulsamos **Configuración IPSec y** seleccionamos **Usar clave previamente compartida para autenticar** y escribimos la misma clave que indicamos en el servidor (Practica 2: Paso 11):

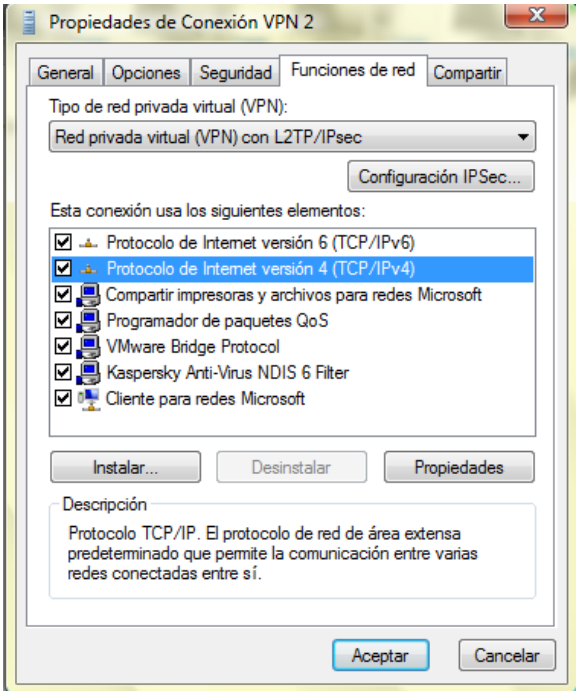


Finalmente, la forma de conectarse normalmente se la hace de la siguiente manera: **Panel de control > Centro de redes y recursos compartidos** y pulsamos en la opción **Administrar conexiones de red o simplemente vamos a INICIO> Conectar a, seleccionamos la conexión y pulsamos Conectar**. Hacemos doble clic en el icono de la conexión VPN y se mostrará la siguiente ventana de conexión:

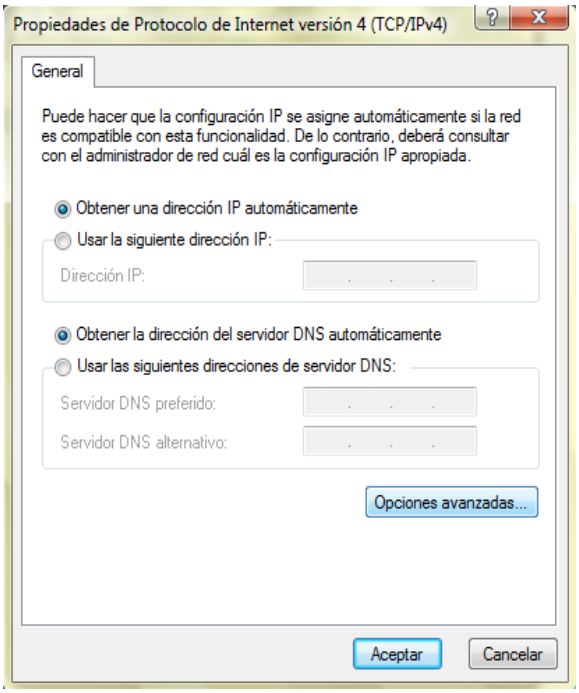
El momento de la conexión se puede presentar algún problema, como que se pierda la conexión a Internet, es decir que no se puedan abrir páginas web, no que se pierda la conexión con el equipo remoto.

Si este es el caso debemos seguir los siguientes pasos:

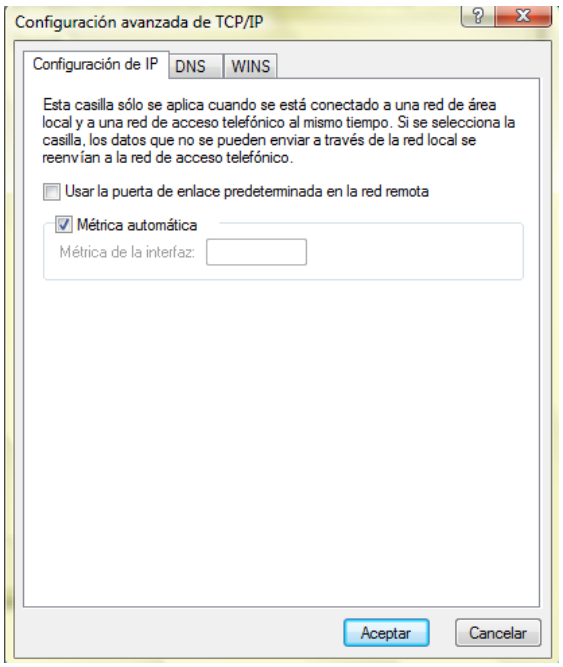
Vamos a la conexión VPN y **Propiedades** en la pestaña **Funciones de red** secciona **Protocolo de Internet versión 4 (TCP/IPv4)** y pulsa en el botón de **Propiedades**.



En la siguiente ventana dejamos todo automático y seleccionamos **Opciones avanzadas.**

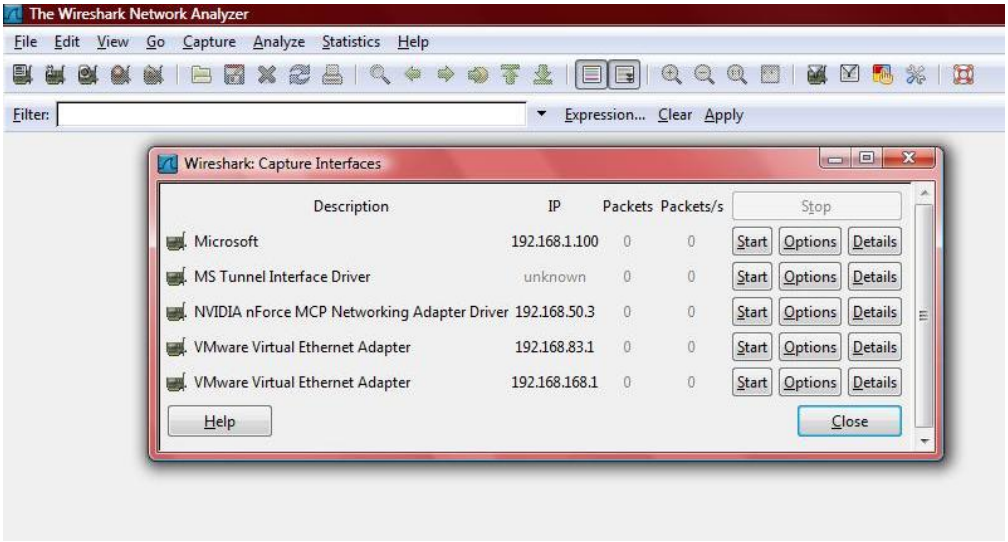


Y en avanzadas, nos aseguramos que la opción **Usar la puerta de enlace predeterminada en la red remota** no esté marcada.

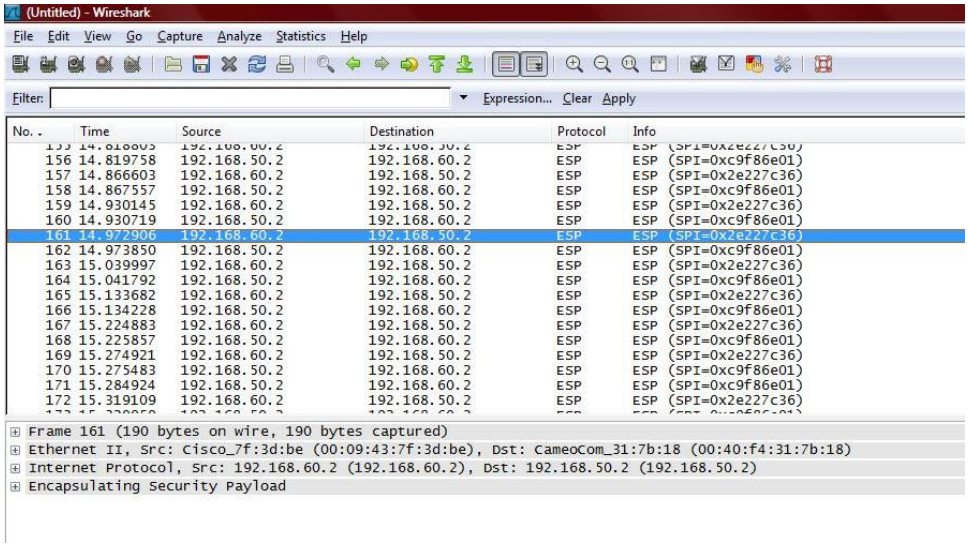


Ahora que ya hemos configurado todo lo necesario para crear una VPN, realizaremos la captura de tráfico utilizando la herramienta Wireshark para poder comprobar la seguridad que brinda al utilizar L2TP/IPSec. La captura la realizaremos desde la máquina intrusa con IP 192.168.50.3.

Vamos a **Capture> Interfaces** seleccionamos la interfaz y **Start**



Como podemos observar a continuación todo el tráfico viaja encriptado con el protocolo ESP (Encapsulating Security Payload), solo se puede ver las direcciones Ip y la asociación de seguridad SPI (una para los paquetes entrantes, y otras para los paquetes salientes), por lo que será imposible leer su contenido.



Si quitamos el protocolo L2TP/IPSec, esto lo hacemos en la Practica 2 en el Paso 12 y en la Práctica 3 en el Paso 7, ya no observaremos la encriptación con ESP.

Ahora realizaremos la captura desde la máquina con IP 10.2.0.3 y aquí si podremos ver el contenido de la información.

3.5 CONCLUSIONES

Estas prácticas nos permitieron comprobar que al construir una VPN el envió de información resulta muy eficiente utilizando L2TP/IPSec como protocolo de seguridad, puesto que solo el usuario autorizado será capaz de leer la misma, incluso en el caso que un tercero quiera intervenir no le será posible recuperar la información original.

CONCLUSIONES

La utilización de las Redes privadas Virtuales (VPNs) se presentan en la actualidad como una buena alternativa para las empresas debido a que mediante el tunneling se suministra la confianza y la certeza que en todo momento las comunicaciones sean fiables, además gracias a la tecnología que brindan las VPNs se puede obtener un considerable ahorro económico, al reducir los costos de la transmisión de los datos, puesto que no hace falta hacer uso de una línea dedicada muy costosa, por el contrario nos permite usar una red pública como el internet.

Usar una VPN es ventajoso porque además nos da a elegir el nivel de seguridad que el usuario requiere en su conexión, para esta elección existen protocolos como por ejemplo: PPTP, L2TP e IPSec. Cabe destacar que individualmente la seguridad que brindan no es completa, razón por la cual lo más optimo es juntar las características que brinda un protocolo con las que brinda otro, de esta forma podemos estar seguros que tenemos la información correcta y protegida de terceros.

Este tutorial reúne toda la información necesaria para la elaboración de una red privada virtual con L2TP/IPSec, de esta manera los estudiantes que precisen de él, puedan enriquecer sus conocimientos tanto prácticos como teóricos de una forma didáctica y la vez sencilla.

BIBLIOGRAFIA

Actualización de NAT-T de L2TP/IPsec para Windows XP y Windows 2000, Microsoft Ayuda y soporte técnico, http://support.microsoft.com/kb/818043/es [consulta: febrero del 2008]

CARRO DÍAZ Santiago, Redes privadas virtuales, conexión sin límites: las VPN conectan cualquier centro de trabajo con total seguridad, PC world profesional, ISSN 1886-8843, Nº. 238, 2007, pgs. 146-149, Universidad de La Rioja, http://dialnet.unirioja.es/servlet/articulo?codigo=2198214 [consulta: febrero del 2008]

CLERENCIA Isaac, Redes privadas Virtuales, Warp Networks S.L., 17 de junio de 2005, http://people.warp.es/~isaac/openvpn.pdf

DE LOS SANTOS Sergio, Redes privadas virtuales (VPN): Solución a la comunicación remota segura, http://mundoinformatica.portalmundos.com/redes-privadas-virtuales-vpn-solucion-a-la-comunicacion-remota-segura/ [consulta: enero del 2008]

DE SAINT PIERRE Thierry, IPSec: Seguridad IP, http://www.dcc.uchile.cl/~cc51d/docs2001/c9-IPSEC.pdf [consulta: febrero del 2008]

EGEA LÓP EZ Esteban, Universidad Politécnica de Cartagena, Redes Privadas Virtuales, http://www.teleco.upct.es/Docencia/Asignaturas/103113004/Curso0203/Tema5.pdf [consulta: febrero del 2008]

FERRER Damián, VPN: Una introducción a las Redes Privadas Virtuales, 2004, Kritópolis, http://www.kriptopolis.org/vpn-una-introduccion-a-las-redes-privadas-virtuales.htm [consulta: enero del 2008]

FERNÁNDEZ GARZA Juana María, Redes privadas Virtuales, Octubre de 1998 http://www.aaapn.org/aaapn/boletin/1998/pbol44a.htm [consulta: enero del 2008]

ILERBAIG ADELL Vicente, Transmisión de Vídeo sobre IP s través de Redes Privadas Virtuales, Valencia, 12 de noviembre de 2004, http://www.ralco-networks.com/pdf/VBvpn.pdf [consulta: enero del 2008]

INTERIANO Eduardo, MONTES DE OCA Faustino, Redes de Computadoras, http://www.ie.itcr.ac.cr/faustino/Redes/Clase6/3.2PPP.pdf [consulta: febrero del 2008]

INTRODUCCIÓN A L2TP, http://docente.ucol.mx/al971854/public_html/tarea7.htm [consulta: febrero del 2008]

ICONO TECNOLOGÍA, http://www.icono-computadoras-pc.com/redes-vpn.html [consulta: enero del 2008]

LAYER 2 TUNNELING PROTOCOL, Interpeak network Security, 2001, http://adsl.cutw.net/l2tp/l2tp.pdf [consulta: abril del 2008]

NADER CARREON Roberto, VPN o Redes Privadas Virtuales (Parte II), 2003, http://www.pc-news.com/detalle.asp?sid=&id=11&lda=1178 [consulta: abril del 2008]

PÉREZ IGLESIAS Santiago, Análisis del protocolo IPSec: el estándar de seguridad en IP, http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/ipsec.pdf

PROTOCOLO DE TÚNEL DE CAPA DOS (L2TP), 2005, http://technet2.microsoft.com/WindowsServer/es/Library/04bd5817-0e41-46b7-9dda-d6340fce514f3082.mspx?mfr=true [consulta: febrero del 2008]

PTPP (Microsoft Point-To-Point Tunneling Protocol), http://www.textoscientificos.com/redes/redes-virtuales/tuneles/ptpp [consulta: febrero del 2008]

REDES PRIVADAS VIRTUALES, http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/COMUNW01/Tema_4_Desarrollado.htm [consulta: enero del 2008]

REDES PRIVADAS VIRTUALES (RPV), http://asignaturas.diatel.upm.es/seguridad/RPV.htm#protocolos [consulta: enero del 2008]

RUIZ GONZÁLEZ José Luis, VPN - Redes Privadas Virtuales, Marzo 2002, http://isa.uniovi.es/~sirgo/doctorado/VPN.pdf [consulta: enero del 2008]

SALAVERT CASAMOR Antonio, LOS PROTOCOLOS EN LAS REDES DE ORDENADORES, Ediciones UPC, Publicado en 2003, http://books.google.com/books?id=utSDd87gmdYC&pg=RA1-PA146&lpg=RA1-PA146&dq=caracteristicas+de+pptp&source=web&ots=X_r3-ldsWh&sig=M6K8FfvIL-qGw6W3DtbK8mSjJoA#PRA1-PA146,M1 [consulta: febrero del 2008]

TORRES L., BALUJA W., Elementos de seguridad en redes privadas virtuales sobre internet, Ingeniería Electrónica, Automática y Comunicaciones, 2003, http://revistas.mes.edu.cu:9900/EDUNIV/03-Revistas-ientificas/Ingenieria-Electronica-Automatica-y-Comunicaciones/2003/3/10303305.pdf [consulta: marzo del 2008]

VPN - REDES PRIVADAS VIRTUALES, Socier Empresas, http://www.sorcier.com.pe/empresas/vpn [consulta: enero del 2008]

VPN: SEGURIDAD EN SUS COMUNICACIONES, http://www.proxia.es/docs/Hojas%20de%20Aplicacion/VNPs%20y%20Redes%20Seguras_v.2.0_.pdf [consulta: enero del 2008]