Universidad Central "Marta Abreu" de Las Villas
Facultad de Ingeniería Eléctrica
Dpto. Telecomunicaciones y Electrónica

Propuesta de implementación de la tecnología de Redes Privadas Virtuales en intranet de ETECSA

Tesis presentada en opción al Título Académico de Máster en Telemática

Autor : Ing. Ana Ivis Neyra Bencomo

Tutor : Dr. José Raúl Vento Alvarez

Villa Clara, Cuba
2004

RESUMEN

Las redes de comunicaciones han experimentado un desarrollo vertiginoso en los últimos años, sin embargo continúan enfrentando el factor seguridad que puede afectar su eficiente aprovechamiento. Entre las alternativas existentes para hacerle frente a dicho factor, se han destacado las llamadas Redes Privadas Virtuales (VPN), tecnología que proporciona un medio para usar una infraestructura pública de red para el transporte de datos privados con el objetivo de brindar acceso remoto a usuarios a sus redes privadas o brindar conexión a redes privadas distantes. Las Redes Privadas Virtuales no escapan a los riesgos de seguridad pero si cuentan con los elementos para minimizarlos. Dentro de estos elementos se encuentran algoritmos de encriptación, certificados digitales, protocolos de encapsulamiento, hardware, software, sistemas de autenticación y otros que son tratados en este trabajo.

Los problemas con la seguridad existen igualmente en una intranet y los mecanismos mencionados para contrarrestarlos son válidos. La red pública estaría conformada por un conjunto de subredes interconectadas de acceso libre y las redes privadas estarían conformadas por subredes que conforman una Red Privada Virtual. Este trabajo se orienta en el ambiente de Intranet brindando una propuesta de implementación de Red Privada Virtual en las redes de las Filiales Territoriales de ETECSA para dar conectividad a las redes de gestión territoriales así como una guía de pasos que tiene en cuenta criterios de implementación, elementos de seguridad y que puede ser muy útil al utilizar esta tecnología en Intranet.

Tabla de Contenidos

TABLA DE CONTENIDOS

Dedicatoria

...A ARLENA, MI TESORITO

Agradecimientos

A mi mamá, por su apoyo total y por cuidar de mi tesorito rubio con devoción.

A mi esposo que ha compartido conmigo todos estos meses ayudándome siempre en todo.

A mis abuelos, padre, tíos y primos porque siempre han estado prestos a apoyarme, animarme y cuidar de mi niñita en mis ausencias durante esta Maestría.

A todos mis compañeros de trabajo: Yanet, Casi, Mary, Grego, Yosmani, Rubén y Maykel que me han soportado y ayudado muchísimo en la realización de este trabajo; Magalys, Aníbal, Onel, Niurkita, Zoraida, Javier y Berli que me han sacado de grandes apuros.

A mi tutor, Raúl Vento, que a pesar de la distancia y el trabajo me ha dedicado mucho tiempo, facilitando información e importantes criterios.

A Efrén, todo un tutor, que ha contribuido muchísimo desde la concepción de este trabajo hasta la última prueba realizada.

A los profesores de la Maestría en Telemática de la UCLV, por su dedicación.

A Martica y Luis en el Centro de Capacitación, los trabajadores de la Escuela del PCC y de la Casa de Visitas de la CTC en Las Villas, a todos ellos por las atenciones y la paciencia que tuvieron con nuestro grupo.

A todos mis compañeros de grupo en esta Maestría por la ayuda que nos brindamos unos a otros, con los que compartimos viajes, estudios, risas y el teléfono; y especialmente dentro de ese grupo a las otras tres mosqueteras Mayra, Nora y Odalys (¡en orden alfabético!) por su magnífica compañía, por los trabajos que compartimos, por los momentos de nerviosismo (que fueron muchos), por los buenísimos momentos de conversaciones y risas (¡que también fueron muchos!!!) y finalmente por su ayuda y cuidado en la impresión de este trabajo.

A todos, muchas gracias!

Introducción

En los últimos años las redes se han convertido en un factor crítico para cualquier organización, cada día en mayor medida por ella se transmite información vital y por tanto dichas redes deben garantizar aspectos como seguridad, fiabilidad, alcance geográfico y efectividad en costos. Es entonces que existe la necesidad de instituciones y organismos de intercambiar información de forma segura.

Una alternativa para crear una red completamente privada es arrendar circuitos, o servicios dedicados similares, a los operadores de red públicos. Contar con enlaces dedicados privados es una alternativa muy segura, confiable y rápida pero que está dejando de ser la preferida en muchos sectores, principalmente por los costos que se asocian a este modo de conexión.

La seguridad en la red es cada vez más importante, tanto para proteger la información en tránsito en sesiones de acceso remoto, como en conexiones de redes internas, para ello son fundamentales las soluciones que garanticen esta seguridad y es aquí donde juegan su papel las Redes Privadas Virtuales (VPN, *Virtual Private Network*).

La tecnología de Redes Privadas Virtuales está diseñada para cubrir las necesidades de privacidad que se incrementan con la tendencia actual de las empresas hacia operaciones globales en donde ellas, sus sucursales y empleados deben conectarse a recursos centrales y comunicarse entre sí haciendo uso de accesos remotos confiables. Una Red Privada Virtual es una red de datos de gran seguridad que permite el transporte de información confidencial utilizando una red pública de datos como medio de transmisión, donde la transmisión de los datos se realiza creando túneles virtuales para asegurar la confidencialidad e integridad de los datos transmitidos apareciendo como una comunicación privada a pesar de estar soportada en una red pública.

En Cuba no existe aún un despliegue masivo de la tecnología de Red Privada Virtual, se han realizado algunas investigaciones al respecto pero los Proveedores de Servicio de Internet de nuestro país no ofrecen, hasta el momento, estas soluciones a los usuarios

que lo requieren por lo que estas tienen que ser implementadas y administradas por parte de los usuarios.

En estas condiciones identificamos la siguiente situación en las filiales territoriales de ETECSA: existen dos redes en una misma filial, la Red de Gestión (GesNet) y la Red Gerencial separadas físicamente como única vía para garantizar la seguridad requerida por la primera que se encarga del monitoreo, control y operación de la técnica de telecomunicaciones instalada en los territorios. Esto trae consigo que usuarios autorizados de la red gerencial, en su mayoría administrativos cuyas funciones no son exclusivas de la gestión, no tienen acceso a estudios de tráfico telefónico, completamientos de llamadas, estado de la técnica, y obtenerla se convierte en un proceso engorroso. Por otra parte, la GesNet de los territorios se encuentra aislada de las redes de los Centros de Gestión Regional y Nacional y en las condiciones actuales su conexión requeriría de otro backbone similar al existente para la Red Gerencial.

El problema que se plantea entonces es la dificultad para acceder a la información de gestión en las GesNet de los Centros de Supervisión y Gestión Territoriales de ETECSA desde las redes gerenciales de los propios territorios y desde los centros regionales debido a que no existe una solución de red segura como pudiera ser una Red Privada Virtual , así como la no existencia de una guía de pasos, aplicable para implementar Redes Privadas Virtuales seguras, teniendo en cuenta la variedad de tecnologías, productos, arquitecturas y disímiles necesidades en aspectos de seguridad.

En este contexto es posible, analizando las técnicas y variantes para la implementación de Redes Privadas Virtuales, dictar recomendaciones en forma de guía que contribuyan a una acertada implementación de la tecnología de Redes Privadas Virtuales así como proponer su implementación en las Filiales Territoriales de ETECSA, consistiendo el aporte de este trabajo en la utilización de esta tecnología en el ambiente de una Intranet empresarial

Para realizarla es necesario estudiar las técnicas, protocolos, arquitecturas que permiten la implantación de Redes Privadas Virtuales haciendo especial énfasis en el caso de su implementación sobre una Intranet.

En este trabajo se propone la utilización de la tecnología de redes privadas virtuales en los casos mencionados, teniendo como objetivos específicos:

1- Evaluar las Redes Privadas Virtuales en cuanto a tipos, tecnología de transporte, seguridad de la información, encriptación, calidad del servicio y protocolos.
2- Determinar que tipo de Red Privada Virtual y protocolos son factibles implementar en los casos descritos.
3- Establecer una guía de implementación de Redes Privadas Virtuales en las redes gerenciales de ETECSA.
4- Obtener una propuesta de implementación de la tecnología de Redes Privadas Virtuales en las redes gerenciales de ETECSA.

Para realizar este trabajo fue necesario llevar acabo las siguientes tareas:

- Estudiar alternativas de Redes Privadas Virtuales
- Estudiar los protocolos que se utilizan en las Redes Privadas Virtuales
- Estudiar los protocolos de seguridad
- Estudiar variantes de implementación
- Dictar una guía de pasos para la implementación de Redes Privadas Virtuales en intranets.
- Diseñar una Red Privada Virtual, para la GesNet sobre la Intranet de ETECSA en la Filial Territorial de Pinar del Río, aplicando la guía de pasos propuesta.

Se han empleado los siguientes métodos:

- Métodos Teóricos: Se ha realizado una extensa revisión bibliográfica en la búsqueda de información técnica referente a las Redes Privadas Virtuales
- Métodos Valorativos: Para proponer que protocolos y elementos de seguridad se utilizaran se ha procedido a la evaluación de las tecnologías de seguridad que se pueden aplicar en estas redes.
- Métodos experimentales: Para aplicar la guía al implementar a modo de prueba una Red Privada Virtual en la GesNet sobre la Intranet de ETECSA en Pinar del Río

El trabajo se presenta en tres capítulos.

En el Capítulo I se introducen los conceptos fundamentales de las Redes Privadas Virtuales y generalidades de este tipo de redes que incluye la protección y seguridad, y se hace un estudio de la situación actual en cuanto a la introducción de la tecnología de Red Privada Virtual analizando ventajas y perspectivas futuras.

En el Capítulo II se abordan las tecnologías Red Privada Virtual basadas en IP y los protocolos que se emplean en las mismas describiendo los mecanismos de encapsulamiento y encriptación así como aspectos de su implementación.

En el Capítulo III se expone una guía de pasos para lograr una fluida implementación de esta tecnología en ambiente de Intranet y se recoge la propuesta de implementación objeto de la investigación que cuenta con experiencias prácticas que avalan los resultados.

1. Capítulo I: Generalidades de las Redes Privadas Virtuales.

1.1 Introducción a las Redes Privadas Virtuales

Con el crecimiento que han experimentado en la actualidad las redes de computadoras, el intercambio de información a través de Internet se realiza de manera fácil y veloz reduciendo en tiempo y dinero los gastos de las empresas e instituciones aunque la seguridad en dicho intercambio de información se ha convertido en un factor preocupante.

Existen herramientas de seguridad como los firewalls que evitan la entrada o salida de datos de una red por usuarios no autorizados. Sin embargo, una vez que los paquetes están en Internet, datos como nombres de usuarios y contraseñas están al alcance de hackers e intrusos. En estas condiciones se hace necesario el uso de soluciones como la Red Privada Virtual.

Una Red Privada Virtual es una red privada que conecta, mediante un proceso de encapsulamiento y encriptación de los paquetes de datos, distintos puntos remotos mediante el uso de infraestructuras públicas de transporte como Internet. Esta tecnología posibilita intercambiar datos privados, previo proceso de encapsulado y cifrado, entre dos equipos a través de una red compartida o pública de forma que emula un vínculo privado punto a punto. [25]

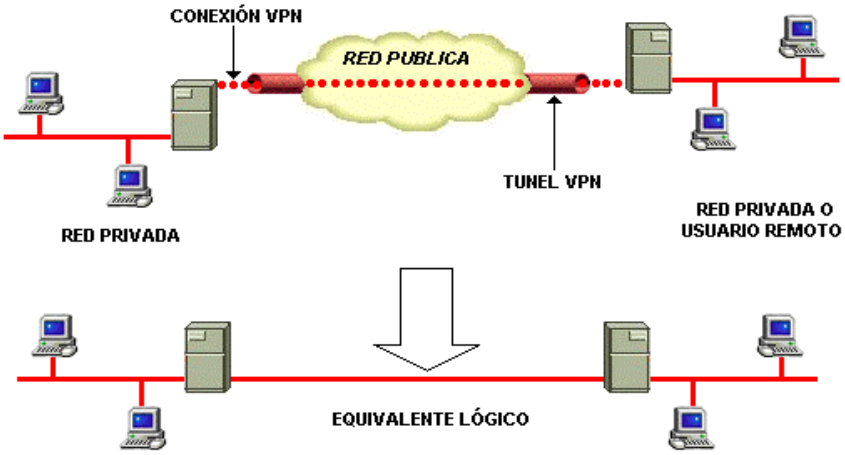

Fig. 1.1 Red Privada Virtual

La tendencia actual entre empresas e instituciones es mover sus aplicaciones críticas de negocio a Intranets para mantener unidas a oficinas regionales y usuarios móviles. Estas entidades requieren también extender su Intranet incorporando clientes, proveedores y socios vía Extranet. Para desarrollar estas infraestructuras competitivas y económicas que permitan incrementar la productividad y comunicación las compañías líderes valoran tres opciones:

1. **Conexión por módem telefónico: Las desventajas en que incurre este tipo de conexión están dadas por el costo de la llamada, que para el usuario sería una llamada telefónica convencional, por lo que se pagaría según el tiempo de conexión, esto empeoraría si la llamada es de larga distancia; por otra parte no se cuenta con la calidad y velocidad adecuadas que estaría poco más allá de los 40Kbps en orden descendente utilizando módems V90. [4]**

2. **Conexión por línea privada o arrendada: En este caso la conexión entre las dos entidades es por cables de pares de cobre o por fibra óptica de un punto a otro. El costo de este enlace es elevado, ya que esta dado por una tarifa mensual por kilómetro de distancia sin importar el tráfico cursado por el enlace.[4]**

3. **Conexión a través de una Red Privada Virtual: Esta opción ahorra en inversión de infraestructura tecnológica, administración y mantenimiento, integra varios servicios en un solo enlace, se eliminan las llamadas de larga distancia que son sustituidas por llamadas locales al proveedor local, o podría usarse un enlace dedicado a Internet ya establecido y se evitan otros pagos por concepto de enlaces dedicados para la interconexión de oficinas remotas. [4]**

La comparación de las opciones anteriores demuestra que la opción de conexión a través de una Red Privada Virtual es la más óptima dado los ahorros en inversión que ello implica. Este tipo de redes disminuye el costo del enlace seguro entre dos sitios remotos.

1.2 Clasificación de las Redes Privadas Virtuales

Las Redes Privadas Virtuales se pueden clasificar atendiendo a varios criterios:

- Red pública que la soporta
- Modo de transporte
- Uso de la Red Privada Virtual
- Si se implementan mediante software o hardware
- Según sus arquitecturas [25]

1.2.1 Red pública de soporte

Las Redes Privadas Virtuales pueden establecerse sobre diferentes redes públicas, Frame Relay, Internet, ISDN y en general sobre cualquier red de infraestructura pública aunque no se debe perder de vista que las Redes Privadas Virtuales son redes privadas construidas sobre la infraestructura de una red pública, por lo que es posible en lugar de utilizar enlaces dedicados a redes de paquetes (como X.25, Frame Relay) para conectar redes remotas, utilizar la infraestructura de Internet (o cualquier red pública), teniendo en cuenta que para los usuarios la forma en que están conectadas las redes es transparente.[4]

Este ejemplo ilustra la conveniencia de económica de la Red Privada Virtual sobre Internet:

Una red hipotética con 3 oficinas en Los Angeles, Houston y Boston y una en Londres con una velocidad de 64 kbits⁄ s. Los cálculos están basados en promedios de precios mensuales de un ISP en Estados Unidos [33].

	Líneas dedicadas	**VPN sobre Frame Relay**	**VPN sobre Internet**
Tarifas Anuales	$133,272	$89,998	$38,400
Instalación	$2,700	$5,760	4 dispositivos de encriptación VPN $16,000
Costo Total del 1er año	$135,972	$111,758	$54,400

Tabla 1. Ejemplo de conveniencia económica de las VPN

1.2.2 Modo de transporte

- Mediante circuitos virtuales ATM

  Para proveer Redes Privadas Virtuales con ATM (*Asynchronous Transfer Mode*, Modo de Transferencia Asíncrono) se reservan Circuitos Virtuales Permanentes (PVC) del ancho de banda deseado entre las sedes que se desean unir. Esta solución está entrando en desuso debido a las siguientes razones:

  - Tiene el problema de que si se cuenta con N centros, y se desea conectarlos unos con otros, hay que proveer N*(N-1)/2 enlaces que serían los PVCs, y esto puede llegar a una cantidad excesiva, por ejemplo para interconectar 50 nodos, se necesitan 2450 circuitos permanentes.
  - El tráfico actual mayoritario es IP. La gestión de las redes ATM es diferente del de las IP, con lo que se tienen que duplicar dichos sistemas. Esto supone duplicar esfuerzos tanto en operación y mantenimiento como en recursos humanos. [34]

- A través de túneles tradicionales (GRE, Encapsulamiento por enrutamiento genérico o túneles IP-IP)

  En las redes que no utilizan ATM como protocolo de transporte, se pueden implementar túneles IP. En este caso los datos viajan a través de la red como si hubiese un enlace virtual entre cada nodo origen y cada nodo destino. Los túneles IP aportan pocas ventajas sobre los PVC ATM salvo la independencia del medio. Los PVC sólo valen para ATM, y los túneles al ser IP están por encima del nivel físico y de enlace, siendo en teoría independiente del medio de transmisión.[6]

  El túnel más común es GRE el cual fue desarrollado por Cisco originalmente, constituyen túneles IP sobre IP cifrados, este tipo de túnel brinda más posibilidades que los túneles IP-sobre-IP digamos por ejemplo, se puede transportar tráfico multicast e IPv6 sobre un túnel GRE.

  Típicamente la arquitectura implementada cuando se usan túneles es hacer pasar estos por un “Concentrador de Túneles”, el tráfico tipo “túnel” no es observado por los

routers, con lo que se pierde la información de la cabecera IP como los bits de precedencia, impidiendo las políticas tradicionales de QoS. [6]

- Utilizando IPSec (Modo Túnel)

  El protocolo IPSec surgió a partir del desarrollo de IPv6. Empezó siendo una extensión de la cabecera en IPv6 y debido a que cubría las necesidades de un gran número de clientes, se decidió implementar en parte para IPv4.

  IPSec tiene como característica principal la posibilidad de encriptar los datos transmitidos, característica que ha permitido su rápida difusión en el mundo empresarial.

  Entre las desventajas que puede presentar se destacan las siguientes:
  - Es un protocolo complejo y de configuración complicada.
  - Requiere configuración en el cliente.

  A pesar de estos inconvenientes IPSec está teniendo una gran difusión en las redes actuales debido a la seguridad que proporciona tener los datos encriptados. [17]

- Implementando MPLS

  MPLS (*Multiprotocol Label Switching*, Conmutación por etiquetado multiprotocolo), es un protocolo de reciente creación que se encapsula por encima de los protocolos de nivel de enlace, pero por debajo de IP. Básicamente lo que se consigue es decrementar el tiempo de resolución del próximo salto para los paquetes IP. En la actualidad está teniendo un gran despliegue en el backbone de la red constituyendo una seria amenaza para las redes ATM pero que ha tenido que adaptarse a ésta para una correcta interoperación. [3]

  Este protocolo está siendo estandarizado por el IETF, y se ha definido un método para ofrecer IP Red Privada Virtual en la red utilizando MPLS, tratados en la RFC 2547 bis, que aborda los requisitos de los suministradores de servicios Red Privada Virtual.

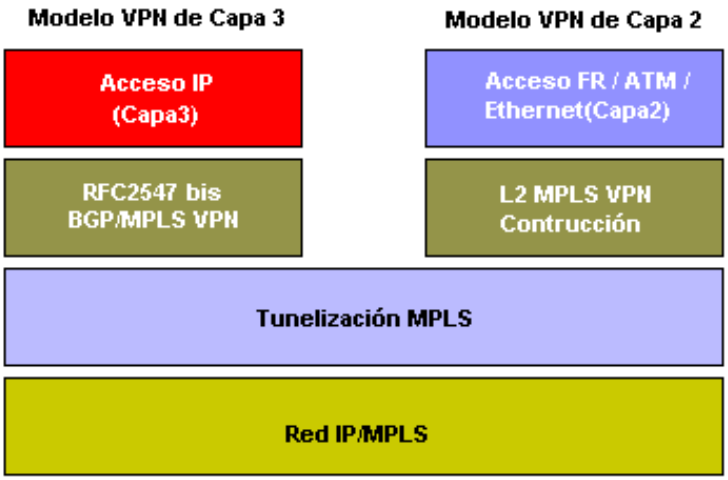

Fig. 1.2: Modelo MPLS VPN.

Usando este método se pueden suministrar túneles entre routers virtuales, instalados en los routers de extremo del proveedor que están dedicados a grupos cerrados de usuarios específicos, formando así la Red Privada Virtual.

El protocolo de señalización usado para MPLS es RSVP (Protocolo de Reservación de Recursos). Este es un estándar en Internet para la reserva de recursos que permite reservar anchos de banda mínimos, permite la gestión del tráfico según su origen y tipo. Actualmente representa la forma más completa y sencilla de implementación de técnicas de ingeniería de tráfico. [2]

1.2.3 Uso de la Red Privada Virtual

En este enfoque existen dos variantes:

- Red Privada Virtual para acceso remoto.
  La Red Privada Virtual para brindar acceso remoto es muy usada por usuarios móviles que requieren acceso remoto para conectarse. Los proveedores ofrecen este servicio para ayudar a los clientes a conectarse a intranets y extranets desde donde se encuentren situados.
- Red Privada Virtual como Intranet y Extranet
  Una Red Privada Virtual como extranet e Intranet enlaza oficinas remotas, socios comerciales, clientes y comunidades de intereses sobre una infraestructura

compartida con la misma política de una red privada. Ambos servicios crean túneles sobre la red IP, tomando los estándares para establecer una conexión punto a punto segura. [4]

Se pueden especificar los casos siguientes:

1. Acceso remoto a Redes Privadas Virtuales a través de Internet:

   Para la conexión de dos puntos remotos existen opciones como la conexión con modem por línea telefónica o mediante línea arrendada, con las desventajas imputables al costo de la llamada o del enlace respectivamente y a la velocidad posible a alcanzar. Con el uso de las Redes Privadas Virtuales se disminuye el costo de enlace privado entre dos sitios remotos, utilizando Internet para establecer el circuito virtual o túnel que conectará un local con otro y pudiendo ser utilizada para aplicaciones de Intranet o Extranet; los costos de Internet son independientes de las distancias entre los puntos. [7]

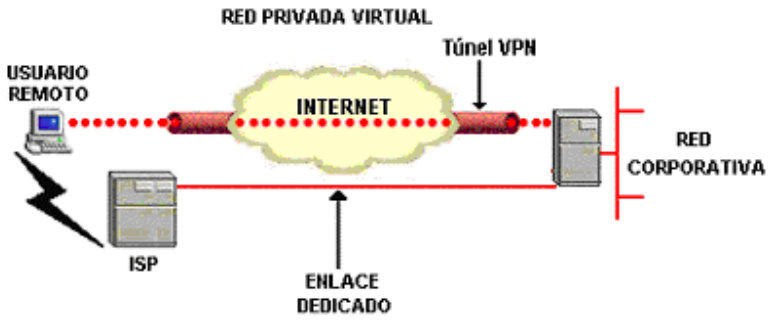

Fig. 1.3 Uso de VPN para conectar usuario remoto de una red a través de Internet

En este caso el usuario llama al número telefónico local correspondiente al NAS (Servidor de Acceso a la Red) de su ISP (Proveedor de Servicio de Internet), posteriormente, el software VPN crea una red privada virtual entre el usuario que marca y el servidor corporativo de VPN a través de Internet.

2. Conexión de Redes Privadas Virtuales remotas a través de Internet.

   La conexión de redes privadas virtuales remotas con una central se logra proveyendo en cada red un router que la conecta con el router del backbone sobre un enlace LAN o WAN.
   Los elementos de costos primarios incluirían:

   - Routers para el campo y el backbone.
   - Servicios de telecomunicaciones, en particular de larga distancia. El costo del backbone de la Intranet, en dependencia del volumen de tráfico puede saltar de

las decenas de miles de dólares mensuales a cientos de miles en igual periodo de tiempo.

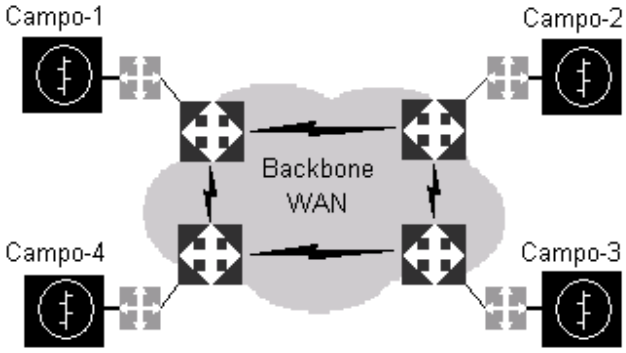

Fig. 1.4: Intranet de una compañía sin VPN.

Con una Red Privada Virtual, la Intranet backbone WAN es reemplazada por Internet. El nuevo costo para esta configuración incluye el despliegue y mantenimiento de compuertas VPN en los campos remotos y el despliegue y mantenimiento de un servidor VPN en la central. A esto se le suma aquello que debe pagar cada localidad por el acceso a Internet.

Los beneficios que ofrece el empleo de una Red Privada Virtual en este campo incluyen:

- La eliminación de los routers de backbone.
- La eliminación de la administración del sistema, configuración, y soporte técnico para routers, y de la necesidad de diseñar y darle mantenimiento a tablas de rutas.
- La eliminación de los servicios de larga distancia, que como mismo ocurre con el caso del acceso remoto, esto resulta en grandes ahorros.

En lugar de utilizar un vínculo WAN dedicado de larga distancia y caro entre las distintas redes, los enrutadores se conectan a Internet mediante vínculos WAN dedicados con un ISP local. Así, cualquiera de los enrutadores inicia una conexión VPN de enrutador a enrutador a través de Internet. Una vez conectados, los enrutadores pueden reenviarse entre sí transmisiones de protocolos enrutadas o directas mediante la conexión VPN. [4]

Existen dos métodos para utilizar las Redes Privadas Virtuales en la conexión de las redes de área local a sitios remotos.

- Uso de líneas dedicadas para conectar una sucursal LAN corporativa: tanto los routers de la sucursal como los de la intranet corporativa pueden utilizar la línea dedicada local al ISP para conectarse a Internet. El software de la Red privada

Virtual utiliza las conexiones de ISP locales e Internet para crear una red privada virtual entre el router de la sucursal y el router corporativo.

- Uso de una línea de marcación para conectar una sucursal a una LAN corporativa: el router en la sucursal puede llamar al ISP local. El software de la Red Privada Virtual utiliza la conexión al ISP local para crear una red privada virtual entre el router de la sucursal y el router de la central corporativa a través de Internet.

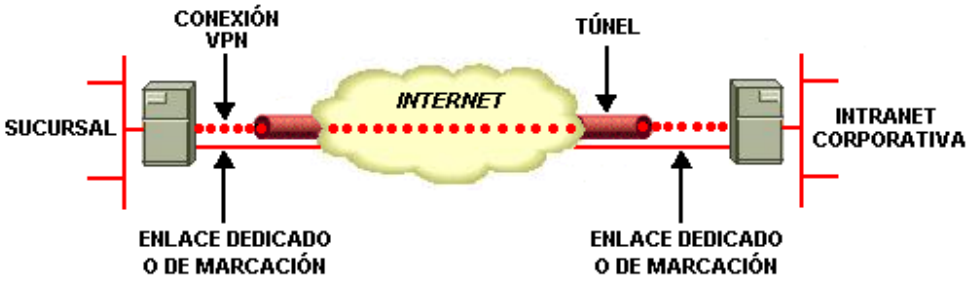

Fig. 1.5 Uso de una VPN para conectar dos sitios remotos.

1.2.4 Basada en software o hardware

Las Redes Privadas Virtuales pueden implementarse por hardware, con el encapsulamiento, la encriptación y otras funciones incluidas en el hardware o pueden ser implementadas por software ejecutándose en computadoras con buenas prestaciones, sobre sistemas operativos Linux, Windows NT, Windows 2000. Estas máquinas pueden estar funcionando como servidores de la red, como cortafuegos o máquinas dedicadas como servidores VPN. [4]

La solución por software consiste en instalar el software VPN en las computadoras que ya están funcionando como cortafuegos o servidores aunque esto trae como consecuencia la disminución del rendimiento de las mismas, por ejemplo, el proceso de encriptación es uno de los más importantes en una Red Privada Virtual y es un proceso que incluye una serie de operaciones matemáticas. Implementar una solución VPN que utilice el algoritmo DES trae como consecuencia una disminución del 40% en el rendimiento de la computadora que lo realice y usando Triple DES se afecta aún en mayor medida. Si la computadora se dedica solo a funciones VPN, la solución VPN puede tener ventajas sobre una solución hardware, la más importante es que ofrece flexibilidad pues si el tráfico

aumenta es relativamente fácil y barato instalar una computadora más rápida, instalar el mismo software VPN y cargar la configuración. [6]

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la Red Privada Virtual no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de Red Privada Virtual ofrece el método más flexible en cuanto al manejo de tráfico que puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en las Redes Privadas Virtuales por hardware, todo el tráfico es enrutado por el túnel. Permite hacer un enrutamiento inteligente de una manera mucho más fácil.[4]

Los sistema basados en Cortafuegos se implementan con software de cortafuegos (*firewall*). Tienen las ventajas de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna, realizan la traducción de direcciones NAT (*Network Address Translation*) y satisfacen los requerimientos de autentificación. Muchos de los cortafuegos comerciales aumentan la protección quitando al núcleo del Sistema Operativo algunos servicios peligrosos, y les provee de medidas de seguridad adicionales que son mucho más útiles para los servicios de Red Privada Virtual. El rendimiento en este tipo de implementación también decrece ya que no se tiene hardware especializado de encriptación. [17]

Existen “chips” con diseños específicos para encriptar y desencriptar datos así como para compactarlos. El hardware diseñado y desarrollado para la tecnología VPN ofrece ventajas significativas de rendimiento sobre una solución por software. La tendencia general va dirigiéndose a soluciones por hardware. Sin embargo, es más costoso actualizar el hardware aun cuando se aprecie que actualmente los precios del hardware VPN han descendido.

1.2.5 Arquitectura de la Red Privada Virtual

Según sus arquitecturas las Redes Privadas Virtuales se pueden clasificar en:

- Dependiente
- Independiente
- Híbrida

Dependiente: Son aquellas en las que el proveedor de servicios brinda completamente la solución VPN y se encarga de controlar el túnel, el rendimiento, la seguridad y los requerimientos de administración.

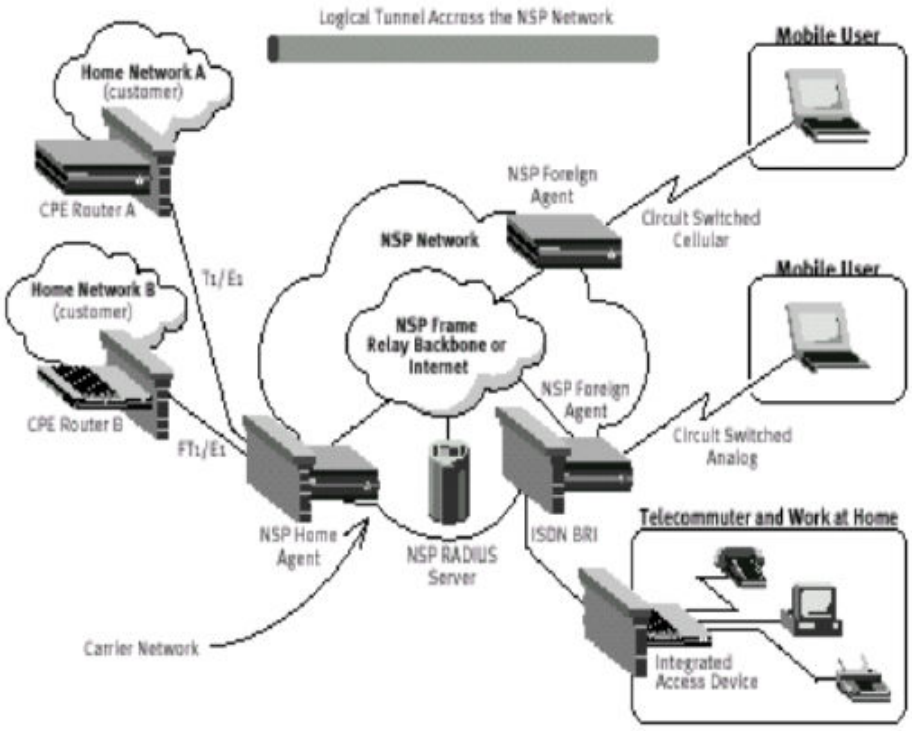

Fig. 1.8 VPN dependiente

Entre sus características se encuentran:

- Todos los sitios VPN tienen una interfaz con un punto de presencia del proveedor de servicios, ya sea mediante una línea arrendada o un servicio conmutado.
- Todo el tráfico de y hacia el usuario final es encapsulado/desencapsulado en el punto de presencia
- El proceso de túnel entre el usuario final y la infraestructura de Internet es transparente al usuario final quien solo ve el tráfico nativo, IP, IPX, NetBeui.
- La organización se encarga de la seguridad de los usuarios y de sus posibilidades de acceso [7]

Independiente: La organización se encarga de todos los requisitos de la Red Privada Virtual, dejándole al Proveedor de Servicios el transporte. El proveedor de servicios sólo

ve el tráfico de Internet , sin poder determinar cual pertenece a Internet y cual a la Red Privada Virtual.

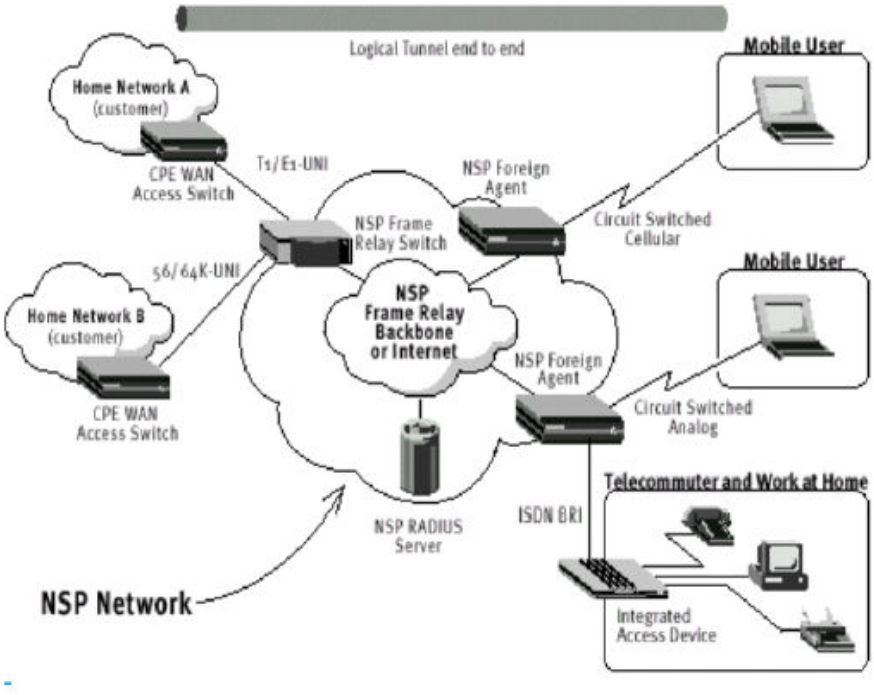

Fig 1.9 VPN independiente

Todos los sitios participantes intercambian tráfico IP con el punto de presencia del proveedor. El tráfico se encapsula/desencapsula en los sitios de la organización. Es útil para las organizaciones que deseen controlar el total de operaciones diarias, el total de los costos... [7]

Híbrida: Las Redes Privadas Virtuales híbridas son una combinación de las Redes Privadas Virtuales dependientes y las independientes, que pueden establecerse cuando el ISP implementa y administra algunos de los dispositivos VPN, mientras que otros los debe manipular la organización.

1.3 Encapsulamiento.

Las redes privadas virtuales crean un túnel virtual dedicado de un sitio a otro para transferir datos entre dos redes similares sobre una red intermedia. Se llama "encapsulamiento" a la tecnología que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, por ejemplo IPX dentro de IP, PPP dentro de IP o sea

involucra tres protocolos diferentes: el protocolo pasajero que representa el protocolo de nivel superior que debe encapsularse; el protocolo encapsulador que es el protocolo que será empleado para la creación, mantenimiento y destrucción del túnel de comunicación; y el protocolo portador será el encargado de realizar el transporte de todo el conjunto. [6]

La tecnología de túneles VPN añade otra dimensión al proceso de túneles antes nombrado encapsulamiento, ya que los paquetes encapsulados están encriptados de forma que los datos son ilegibles para los extraños y viajan a través de Internet hasta que alcanzan su destino donde se separan y vuelven a su formato original.

Se considera que las Redes Privadas Virtuales se encuentran en una zona de seguridad, con un túnel especial alrededor de ellas. Lo anterior se refiere desde el punto de vista lógico ya que en realidad no hay túneles y tampoco se les da a los paquetes de túnel virtual prioridades especiales, siguen siendo datagramas. Lo que añade seguridad son los procesos de encriptación y autenticación, que se pueden utilizar con los paquetes en el túnel. Algunos enfoques de VPN encapsulan todos los paquetes antes de encriptarlos, otros encriptan solo los contenidos de los paquetes encapsulados, no las cabeceras. Es la encriptación, no el encapsulamiento, el proceso que añade seguridad en las Redes Privadas Virtuales. [6]

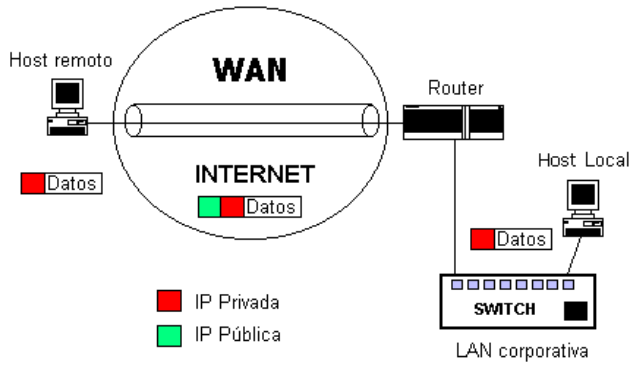

Fig. 1.10: Representación del proceso de encapsulamiento.

La figura anterior muestra cómo se encapsulan los0 datos en una conexión VPN donde un cliente que se encuentra fuera de su red y accede a la información del servidor de la red corporativa a través de Internet.

1.4 Encriptación.

Todas las Redes Privadas Virtuales tienen algún tipo de tecnología de encriptación que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación ya que protege los datos transportados de ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Las técnicas de encriptación de clave secreta y de clave pública son aplicables a las Redes Privadas Virtuales.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación tiene como desventaja el hecho de que al ser la contraseña compartida por todos los participantes, debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad. [18]

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.[18]

En las Redes Privadas Virtuales, la encriptación debe ser realizada en tiempo real, por lo que los flujos encriptados a través de una red se crean utilizando encriptación de clave secreta.

El protocolo más usado que provee encriptación dentro de las Redes Privadas Virtuales es IPSec, que consiste en un conjunto de propósitos del IETF que delinean un protocolo IP seguro para IPv4 e IPv6. [26]

1.5 Calidad de Servicio en las Redes Privadas Virtuales (QoS)

La calidad de servicio puede definirse como la posibilidad de asegurar y medir una serie de parámetros que describen el grado de servicio recibido por el usuario. Teniendo esto en cuenta, la problemática de la calidad de servicio en las Redes Privadas Virtuales está ligada al tipo de tecnología subyacente utilizada. Los parámetros que definen la calidad de servicio son básicamente: ancho de banda, retardo, variación de retardo, perdida de paquetes y disponibilidad. [30]

Las Redes Privadas Virtuales sobre servicios portadores de nivel 2 (ATM, FR) disfrutan de los mecanismos de estos protocolos para asegurar estos parámetros. Por tanto, la verdadera problemática, que no es exclusiva de las VPN, reside en la capacidad de IP para ir mas allá de un servicio best-effort (del mejor esfuerzo)

De manera sintética, es posible decir que existen dos aproximaciones para abordar la problemática de la calidad de servicio en redes IP:

1. El Modelo de Servicios Integrados (IntServ)
2. El Modelo de Servicios Diferenciados (Diffserv)

El modelo IntServ adopta lo que se puede denominar “aproximación por flujo”. Se envían peticiones de reserva de ancho de banda por cada petición o flujo que se establece. El requerimiento de que RSVP deba ser interpretado por el conjunto de equipos en medio y la carga que esta señalización puede suponer sobre los mismos ha hecho que se cuestione su capacidad para ser desplegado en redes grandes.

El modelo DiffServ adopta lo que se puede denominar “aproximación por Clase de Servicio”. Mediante la codificación del byte ToS de los paquetes IP (rebautizado DS), en los extremos de la red se clasifican los paquetes como pertenecientes a diferentes Clases de Servicios, cada una de las cuales está caracterizada por un tratamiento diferente en el núcleo de la red. Este tratamiento hace referencia a cómo se ubican en las colas, los paquetes en diferentes buffers, cómo se gestionan y priorizan cada uno de ellos por medio de una función de planificación y que política se sigue en caso de congestión de buffers (conformado de tráfico, descarte selectivo). [36]

Las limitaciones de escalabilidad del Modelo IntServ, hacen de DiffServ la opción más aceptada en el mercado. De hecho, su principio de funcionamiento es la base de las

políticas de gestión de trafico IP (clasificación de tráfico sobre la base de parámetros como dirección IP origen, dirección IP destino, puerto y tratamiento de buffers diferenciado) que actualmente implementan las redes de operadores y algunas corporaciones.

Lo fundamental a entender del modelo DiffServ, y de las técnicas empleadas actualmente, es que no se asegura de manera determinista para cada flujo determinados parámetros de QoS, como es el caso de un circuito ATM, sino que se forman agregaciones de tráfico. Así, un operador puede integrar las conexiones de usuarios pertenecientes a diferentes Redes Privadas Virtuales dentro del mismo agregado, teniendo por tanto todas ellas el mismo tratamiento a nivel de red. Este tratamiento podrá ser diferente al que tengan los usuarios de su oferta de acceso gratuito a Internet, pero actualmente sólo un trabajo de ingeniería de red y dimensionamiento correcto de la misma podrán hacer que se respeten determinados valores de retardo o pérdida de paquetes. MPLS-TE (*Trafic Engineering*) permitirá en el futuro el mapeo de los valores del byte DS en diferentes "trayectos virtuales" o LSPs *(Label Switched Paths)* que podrán ser enrutados selectivamente en la red del proveedor de servicios, pero todavía esta en fase de estandarización. [1]

Otro aspecto muy importante es el que hace referencia a la clasificación de los paquetes. Dado que el valor del byte DS puede ser modificado en cualquier equipo intermedio, una calidad extremo a extremo sólo será alcanzable cuando todos los elementos involucrados en la cadena (dominio DiffServ) actúen regidos por las mismas políticas, lo que de momento descarta Internet.

1.6 Ventajas de las Redes Privadas Virtuales.

La principal ventaja de usar una Red Privada Virtual es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de una computadora en esa red privada, pudiendo acceder a la información publicada en ella a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizaran usando los recursos y conexiones que tenga la red privada.

Otras ventajas que se pueden mencionar son:

- Privacidad y seguridad garantizada en sus comunicaciones.

- Altas prestaciones y fiabilidad.
- Integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla instalación del cliente bajo cualquier sistema operativo.
- Los algoritmos de compresión optimizan el tráfico del cliente. [7]

Desde el punto de vista económico, una red privada virtual ayuda en la reducción de gastos de administración pues el costo de una red se divide en: equipo 20%, implementación 30% y administración 50%, al utilizar una Red Privada Virtual se delega la administración y el mantenimiento de la red al proveedor de servicios. [35]

De esta forma una empresa se ahorra en inversión de infraestructura tecnológica, administración y mantenimiento, y además, puede integrar varios servicios en un solo enlace. Como ejemplo, se eliminan las llamadas de larga distancia, las cuales son sustituidas por llamadas locales al servidor de Internet, por lo que también desaparecen los pagos por concepto de enlaces dedicados para la interconexión de oficinas remotas.

Según estudios realizados por Forrester Research las organizaciones que adoptan Red Privada Virtual ahorran de un 30 – 80% a sus equivalentes redes privadas [12], ya que:

- Eliminan las líneas arrendadas entre sitios separados por largas distancias.
- Eliminan las llamadas de larga distancia a través de la red telefónica conmutada mediante modems.
- Les permite pagar sólo por el uso actual de la red o por el tráfico enviado.
- Minimiza el diseño de la red y las responsabilidades de administración.
- Explotan las nuevas generaciones de redes públicas de infraestructuras robustas para proporcionar más capacidades y alternativas confiables a las redes privadas.
- La presencia global de Internet hace a las Redes Privadas Virtuales más flexibles que las redes privadas.

En el caso de los Proveedores de Servicios de Internet adoptar esta tecnología le trae beneficios relacionados fundamentalmente con la ampliación de sus ofertas y el establecimiento de un ambiente seguro con poco costo y la gran dependencia de sus clientes que realizan comercio electrónico. Además puede agregarse:

- Posibilidad de brindar una gran cantidad de servicios de valor añadido.
- Una gran oportunidad de negocio con ingresos sustanciales

- Posibilidad para atraer y expandir clientes corporativos.
- Oportunidad para establecer relaciones con grandes organizaciones.
- Influencia de la infraestructura existente para el rápido establecimiento de nuevos servicios con poca inversión. [7]

Por otra parte los servicios de valor añadido sobre Red Privada Virtual dan más ganancias que los establecidos sobre líneas privadas.

1.7 Perspectivas futuras

La retransmisión de trama es el servicio de datos más ampliamente usado para las conexiones entre dependencias. Sin embargo, el uso de las tecnologías VPN IP para las dichas conexiones entre establecimiento está creciendo en importancia, debido a que en ciertos casos presentan una mayor rentabilidad económica con relación a las tecnologías tradicionales de las Redes Privadas Virtuales aunque frente a la caída de los precios de los servicios de retransmisión de tramas, la tecnología VPN IP debe solucionar un número de barreras si quiere competir en precio/rendimiento con la tecnología establecida basada en los circuitos. Estas barreras incluyen la ausencia de la Calidad de Servicio (QoS) extremo a extremo para el tráfico VPN IP. Los suministradores de servicios deben poder ofrecer a las empresas clientes contratos de niveles de servicio (SLA) en relación con los rendimientos de QoS de la Red Privada Virtual extremo a extremo, en vez de las garantías actuales en las estadísticas de perdidas de paquetes y de latencia en el centro de la red, debido a que estas últimas no se pueden correlacionar con el rendimiento de un servicio VPN particular. [4]

Actualmente las tecnologías preferidas para suministrar VPN son IPSec y MPLS que además son las estandarizadas por el IETF. Las operadoras están en un proceso de migración de redes ATM a redes IP puras con MPLS. Esta migración se aconseja por la rentabilidad económica que aporta MPLS y por las herramientas que proporciona para la realización de ingeniería de tráfico, QoS y el despliegue rápido y sencillo de Red Privada Virtual.

MPLS está adquiriendo protagonismo en los backbones e IPSec en los clientes. La tendencia a medio plazo será utilizar IPSec para encriptación de datos y MPLS para la provisión de servicios como Red Privada Virtual y la optimización de tráfico dentro de la red del proveedor.

Las VPN MPLS incluyen:

- Una oferta administrada escalable que puede soportar miles de sitios por VPN y centenares de miles de Redes Privadas Virtuales por proveedor de servicios.
- La asignación de ruta óptima de tráfico del cliente a través de la red del proveedor de servicios.
- La Clase del IP de Servicios (CoS) para clases múltiples de servicios y prioridades dentro de una Red Privada Virtual y entre ellas.
- El soporte para Redes Privadas Virtuales múltiples con el acuerdo de nivel de servicios (SLAs) para la calidad de servicios (QoS)
- Provisión inherente de la privacidad y QoS de ATM sin tunneling ni encriptación.
- La habilidad del proveedor de servicios de implementar servicios manejados económicos.
- La entrega de servicios independiente del acceso o tecnología de transporte.
- El apoyo transparente para direcciones IP privadas, sin requerir de traducción de direcciones para apoyar a sus subscriptores independientes que tienen un espacio de dirección de superposición.
- Una base para el despliegue futuro de servicios adicionales, como la voz y multimedia.
- La provisión de servicios es sencilla: una nueva conexión afecta a un solo enrutador.
- Tiene mayores opciones de crecimiento modular.
- Permite mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho de banda, retardo, fluctuación...), lo que sea necesario para un servicio VPN completo [3].

1.8 Conclusiones del capítulo

- Las Redes Privadas Virtuales se definen como redes que se extienden mediante procesos de encapsulamiento y encriptación de los paquetes de datos, a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte.
- Se clasifican según su uso, sobre que red pública funciona, según su arquitectura y si es implementada por software o hardware.

- En Cuba los Proveedores de Servicios de Internet (ISP) no ofrecen soluciones VPN y las empresas no las implementan debido al desconocimiento de esta tecnología, la ausencia de una guía de pasos que facilite el diseño e implementación de estas y la desconfianza, por parte de administradores y usuarios, de la seguridad en las Redes Privadas Virtuales.
- El protocolo de Red Privada Virtual más utilizado es el IPSec

2. Capítulo II: Encapsulamiento y encriptación en las Redes Privadas Virtuales

En las Redes Privadas Virtuales se aplican mecanismos de encapsulamiento para lo cual se hace uso de protocolos como PPTP y L2TP que crean túneles virtuales para la comunicación a través de la red pública y mecanismos de seguridad como la encriptación los cuales han ido evolucionando como certificados digitales, firmas digitales además de mecanismos de autenticación. El protocolo IPSec por las características de seguridad que garantiza es el más usado actualmente en las Redes Privadas Virtuales.

2.1 VPN IP

El enfoque general de VPN IP tradicional gira alrededor de tres procesos: encapsulamiento, encriptación y autenticación.

El encapsulamiento no es más que encapsular cada paquete IP en otro paquete IP antes de ponerlo en la Internet. Los protocolos de encapsulamiento VPN iniciales fueron L2F, desarrollado por Cisco, y PPTP, desarrollado por Microsoft. El IETF (Internet Engineering Task Force) diseñó un tercer protocolo, L2TP, como alternativa para el fabricante neutral. Debido específicamente a razones de seguridad, este último protocolo se adecuó a IPSec, también creado por IETF. [25]

La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de ser accedidos y entendidos en el transporte de un extremo a otro de la conexión. Todas las Redes Privadas Virtuales tienen algún tipo de tecnología de encriptación que esencialmente empaqueta los datos en un paquete seguro.

La autenticación en Redes Privadas Virtuales se realiza mediante un nombre de usuario y una contraseña pero con necesidades mayores de aseguramiento de validación de identidades. La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no exista un tercer participante que se haya inmiscuido en la comunicación. La autenticación también puede ser usada para asegurar la integridad de los datos que son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como una suma de comprobación. Cualquier desviación en esta suma, indica que los datos fueron corrompidos en la transmisión o interceptados y modificados. [6]

2.2 Mecanismos de seguridad.

Los mecanismos de seguridad de las Redes Privadas Virtuales se implementan mediante protocolos dentro de los que se relacionan:

- MPPE (*Microsoft Point-to-Point Encryption,* Cifrado punto a punto de MS): Se utiliza para encriptar los datos de las transmisiones. Es un algoritmo de cifrado de clave de 128 bits que utiliza RSA RC4. Proporciona confidencialidad de paquetes entre el cliente de acceso remoto y el servidor de acceso remoto o de túneles, y resulta útil cuando no hay seguridad IP (IPSec). MPPE es compatible con NAT (*Network Address Translation*).
- CHAP (*Challenge/Handshake Authentication Protocol*, Protocolo de autenticación por desafío mutuo): Los clientes de acceso remoto pueden enviar de forma segura sus credenciales de autentificación a un servidor de acceso remoto. Una variante implementada para los sistemas Windows de Microsoft es el MS-CHAP.
- IPSec (*Seguridad de protocolo Internet*):
  IPSec es un conjunto de recomendaciones y protocolos definidos para proteger intercambios de datos sobre IP mediante encriptación a nivel de red, lo que permite proveer una seguridad extremo a extremo. Incluye el soporte de servicios de confidencialidad (encriptación), autentificación (garantía de la identidad del emisor), integridad (garantía de que el contenido no ha sido modificado) y metodología para el intercambio de claves de encriptación. [11]

  El soporte de estas funcionalidades se realiza añadiendo a cada paquete IP cabeceras adicionales. La denominada AH (*Authentication Header),* se encarga de procurar la integridad y autenticidad de los datos, mientras que la cabecera ESP (*Encapsulation Security Payload)* se encarga de la confidencialidad, integridad y autenticidad de los mismos. AH y ESP proporcionan control de acceso. Pueden ser aplicados solos o en combinación para proporcionar la seguridad deseada.

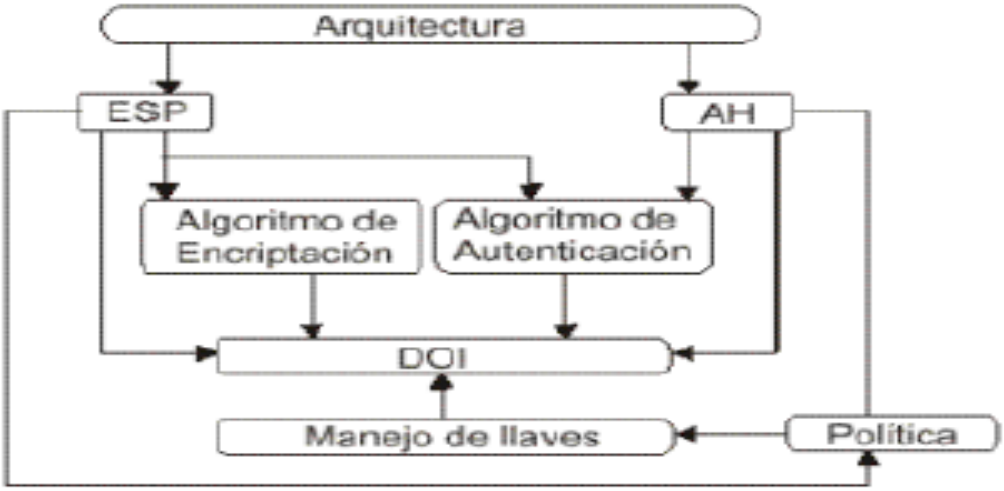

Fig. 2.1: Protocolos IPSec

IPSec puede proteger cualquier protocolo corriendo sobre IP, sobre cualquier medio sobre el que funcione IP y puede proteger cualquier mezcla de protocolos de aplicación corriendo sobre una combinación compleja de medios de comunicación. [9]

IPSec opera en dos modos posibles:

- El modo transporte (se emplea sobre los equipos terminales, sin modificar la cabecera original del paquete) es el que usa un anfitrión que genera los paquetes. En modo transporte, las cabeceras de seguridad se añaden antes que las cabeceras de la capa de transporte (ej., TCP, UDP), antes de que la cabecera IP sea añadida al paquete. En otras palabras, un AH añadido al paquete cubrirá el resumen criptográfico de la cabecera TCP y algunos campos de la cabecera IP de extremo a extremo, y una cabecera ESP cubrirá el cifrado de la cabecera TCP y los datos, pero no la cabecera IP de extremo a extremo.

- *El modo túnel (coloca una nueva cabecera IP que enmascara las direcciones de la cabecera original) se usa cuando la cabecera IP de extremo a extremo ya ha sido adjuntada al paquete y uno de los extremos de la conexión segura es solamente una pasarela. En este modo, las cabeceras AH y ESP se usan para cubrir todo el paquete, incluida la cabecera de extremo a extremo, y se añade una nueva cabecera IP al paquete que cubre sólo el salto al otro extremo de la conexión segura (aunque eso puedan ser varios saltos de distancia).*

Así mientras que en el modo Transporte sólo se encriptan los datos, en el Modo Túnel se encripta la cabecera IP original y se emplea cuando alguno de los extremos (IPSec Proxy) realiza la encriptación en vez de los equipos host. [26]

2.2.1 Asociaciones de Seguridad

IPSec define la posibilidad de utilizar diferentes algoritmos de encriptación o integridad, tanto de clave pública, también denominados de encriptación asimétrica porque se utilizan dos claves, una conocida o pública para encriptar y otra secreta para que el receptor pueda desencriptar la información, como de clave privada denominados de clave simétrica porque se utiliza la misma clave para encriptar y desencriptar la información). [11]

La provisión de nuevos usuarios dentro de la VPN se realiza mediante la definición y configuración de Asociaciones de Seguridad o SAs (Security Association) entre los extremos de la sesión IPSec.

Una SA la compone la información que necesita una entidad IPSec para soportar un sentido del tráfico (saliente o entrante) de una conexión de un protocolo IPSec. El contenido de una SA variará para cada conexión y puede incluir claves de autenticación o cifrado, algoritmos específicos, tiempos de vida de las claves, direcciones IP.

Una SA indica a un dispositivo IPSec cómo procesar paquetes IPSec entrantes o como generar paquetes IPSec salientes. Los dispositivos IPSec insertan un campo en la cabecera de IPSec (Indice de Parámetros de Seguridad) para asociar un cierto datagrama a la SA adecuada en las máquinas que los procesen. Los dispositivos IPSec almacenan las SAs en una base de datos (SAD). Los estándares definen diferentes SAs.

Ambos modos de IPSec ofrecen la posibilidad de cambiar el tiempo de vida de la Asociación de Seguridad (SA). Se puede considerar el tiempo de vida por defecto cuando

la sensibilidad de los datos en el túnel demanda la sustitución de las llaves de encriptación y la reautentificación de cada dispositivo con una actitud más agresiva.

Cambiando estos valores se incrementa los niveles de seguridad, pero también el procesamiento en el extremo VPN. El comportamiento por defecto del cambio de clave SA es para situar la nueva clave en parte de la vieja clave, para disminuir los recursos de procesamiento.

Perfect Forward Secrecy (PFS) genera una nueva llave sobre una nueva base mediante la exponenciación Diffie-Hellman (DH) cada vez que una nueva SA de modo rápido (QM) necesita una nueva generación de la llave. Así también, esta opción incrementa el nivel de seguridad pero al mismo tiempo aumenta el procesamiento.

La fortaleza de la exponenciación Diffie-Hellman es configurable; se soportan los grupos 1 (768 bits), 2 (1024 bits) y 5 (1536 bits). [9]

2.2.2 Protocolos que componen IPSec.

IPSec está compuesto por tres protocolos: AH (Authentication Header), que proporciona un servicio de autenticación a nivel paquete; ESP (Encapsulating Security Payload), que permite contar con encriptación más autenticación; e IKE (Internet Key Exchange), encargado de negociar parámetros de conexión, incluyendo llaves para los otros dos protocolos.

AH es el protocolo de IPSec utilizado para proveer servicios de integridad de datos, autenticación del origen de los datos. Es un estándar definido en el RFC 2402. La principal diferencia entre la autenticación provista entre ESP y AH tiene que ver con la cobertura, ESP no protege los campos del encabezado IP a menos que sean encapsulados por ESP (modo túnel). El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado AH contendrá el valor 51 en su campo de protocolo (IPv4) o siguiente cabecera (IPv6). Puede aplicarse solo o junto a ESP. [19]

Su propósito es:

- Detectar alteraciones del contenido de un paquete
- Autenticar la identidad del que lo envía, bien como usuario o por su dirección IP.

La siguiente figura muestra la cabecera AH, todos los campos son obligatorios y el campo reservado no se utiliza y su valor debe ser cero.

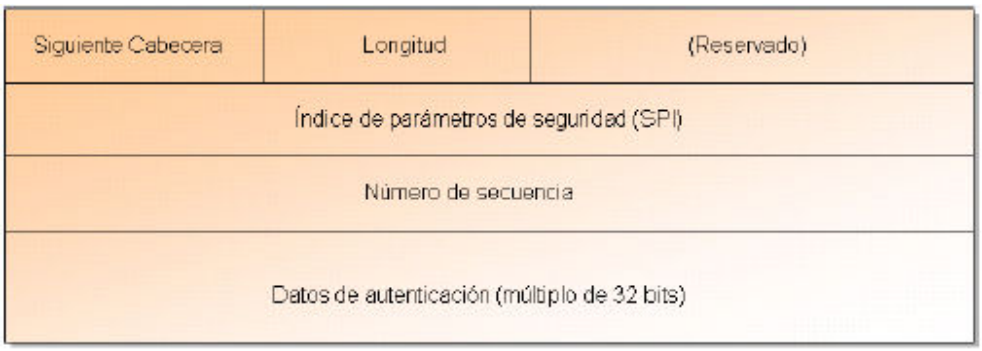

Fig. 2.2: Formato AH

- **Siguiente Cabecera**: Identifica el tipo de los siguientes datos después de la cabecera de autenticación.
- **Longitud**: Especifica la longitud de AH
- **Reservado**: Uso futuro
- **SPI**: En combinación con la IP de destino y protocolo de seguridad, únicamente identifica el SA para este datagrama. Normalmente es elegido por el destinatario cuando se establece la SA.
- **Número de secuencia**: Contador incremental. Se inicializa en cero al establecerse una SA. Uso: Evitar que alguien repita paquetes en la red (protección anti-repetición).
- **Datos de autenticación**: Es de tamaño variable. Contiene el ICV (Integrity Check Value). El algoritmo de autenticación que utilice MACs (Message Authentication Codes) MD5 o SHA –1. [19]

ESP es un encabezado de protocolo insertado en el datagrama IP para proveer servicios de confidencialidad, autenticación del origen de datos, anti-repetición e integridad de datos a IP [26]. Es un estándar definido en el RFC 2406. El encabezado ESP se inserta después del encabezado IP antes del encabezado del protocolo de capa superior (modo transporte) o antes del encabezado IP encapsulado (modo túnel) [20]

Su propósito es proporcionar:

- confidencialidad
- autenticidad
- integridad

- confidencialidad del flujo de tráfico (en modo túnel)

El formato ESP incluye todo el datagrama, excepto la cabecera IP.

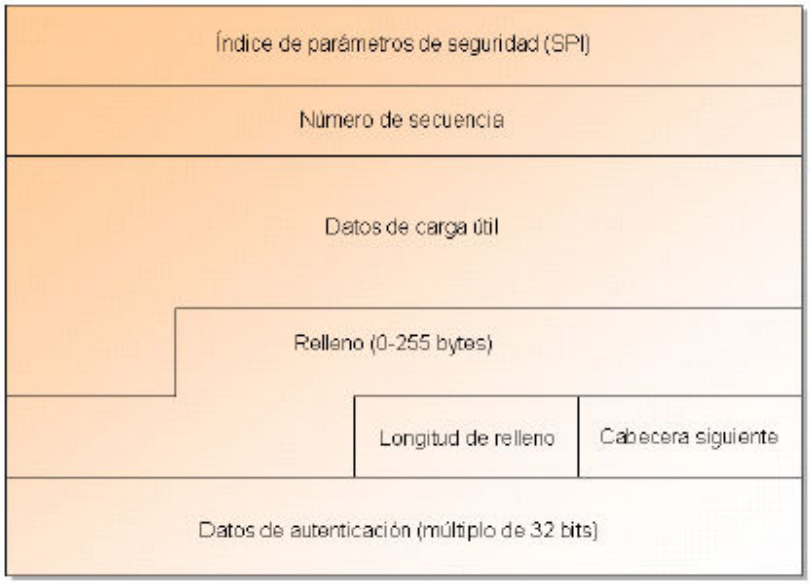

Fig. 2.3: Esquema representativo del funcionamiento de IPSec.

- **SPI** (Indice de parámetros de seguridad): En combinación con la IP de destino y protocolo de seguridad, únicamente identifica el SA (Asociación de seguridad) para este datagrama.
- **Número de secuencia**: Contador incremental. Se inicializa en cero al establecerse una SA (Asociacón de seguridad). Uso: Evitar que alguien repita paquetes en la red (anti-repetición)
- **Datos de carga útil**: Es de longitud variable, contiene los datos descritos por el campo Next Header. Datos que se trasnmiten
- **Relleno**
- **Longitud de Relleno**: Longitud de los bytes que le preceden
- **Siguiente cabecera**: Identifica el tipo de dato contenido en el campo de datos útiles. Número de la primera cabecera en los Datos de carga útil (IPv6), o número de protocolo de nivel superior en los Datos de carga útil (IPv4).
- **Datos de autenticación**: Es de tamaño variable. Contiene el ICV (Integrity Check Value). Opcional, sólo si lo establece la SA. En este caso, no se precisa AH. [20]

El encabezado ESP se inserta después del encabezado IP y antes del protocolo superior (TCP, UDP, ICMP, etc) o antes de cualquier encabezado IP que haya sido previamente insertado. En las figuras siguientes se muestran las posiciones de ESP en modo Transporte y modo Túnel.

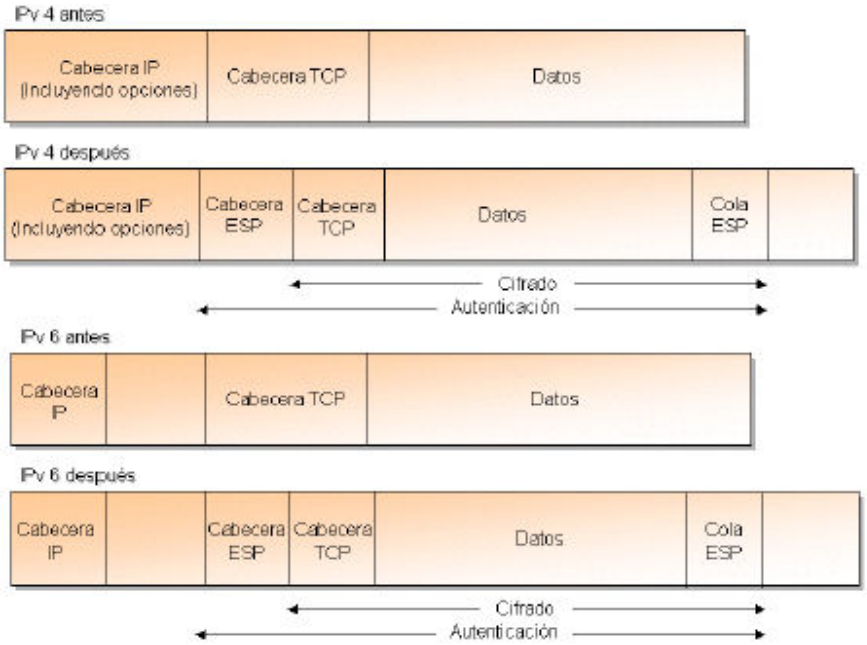

Fig. 2.4: Posición de ESP en modo transporte

- Sólo para implementaciones en máquinas finales.
- No da confidencialidad a la cabecera IP.

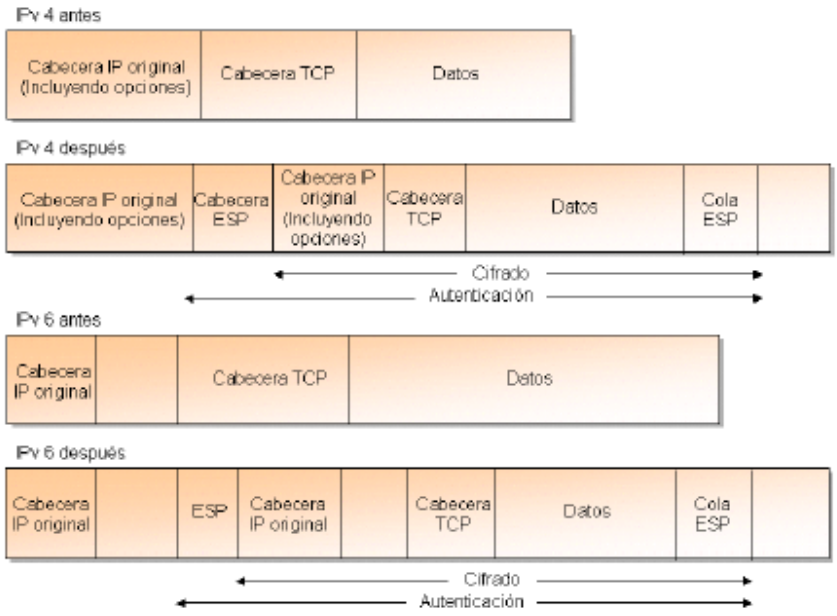

Fig. 2.5: Posición de ESP en modo túnel

- Para implementaciones en máquina finales o en pasarelas
- Da confidencialidad también a la cabecera IP. [20]

IKE (Internet Key Exchange): El IETF renombró la combinación ISKAMP/OAKLEY como IKE. ISAKMP combinado con el protocolo de intercambio de llaves OAKLEY, constituye uno de los más populares conjuntos de protocolos para la implementación y negociación de sesiones VPN. Este conjunto integrado de protocolos negocia automáticamente la conexión y manipula el intercambio de llaves entre el emisor y el receptor.

- ISAKMP (Internet Security Association and Key Management Protocol):
  Proporciona un marco de operación para la gestión de claves de Internet y el soporte de protocolo específico para negociar los atributos de seguridad. No establece las claves de sesión. Es el marco conceptual para la autenticación y el intercambio de claves y la negociación de una SA.[23]
- Oakley:
  Diffie-Hellman (DH) para establecer las claves de sesión en los routers o hosts puede utilizarse solo o con el ISAKMP se necesita negociación de atributos. [15]

  Características:

- Emplea mecanismos de *cookies* para prevenir el ataque de sabotaje del procesador.
- Habilita la negociación de grupos (parámetros globales de DH)
- Utiliza números únicos para protegerse del ataque de repetición
- Habilita el intercambio de valores públicos de DH.
- Protocolo que establece una clave compartida de forma segura entre dos partes
- Usa intercambio de claves Diffie – Hellman
- Encaja en el marco propuesto por ISAKMP para establecer asociaciones de seguridad (SA) IPSec.
- El protocolo establece una SA ISAKMP
- Una vez esta establecida, mecanismos ligeros para establecer más SAs.

La configuración de una SA puede ser, en función de las características del producto concreto utilizado, manual, mediante la configuración de sus parámetros descriptivos (claves a utilizar y protocolo de encriptación, principalmente) en cada extremo o dinámicamente mediante IKE.

IKE creará un túnel seguro entre las dos entidades que negocian la SA para IPSec. Este proceso requiere que ambas entidades se autentifiquen mutuamente y establezcan sus claves. Esta autentificación puede ser realizada por varios métodos. Uno de estos métodos requiere la preconfiguración en los equipos de lo que se denominan claves pre-compartidas (pre-shared keys), mientras que otros lo evitan mediante el uso de certificados digitales e interacción con una Autoridad de Certificación (CA, Certification Authority), lo que posibilita disponer de una solución mucho más escalable.

Una vez culminada esta etapa, se obtiene una SA para IKE, lo que permite el comienzo de la negociación de la SA para IPSec. Una vez establecida, ambos extremos podrán comenzar a comunicarse de una manera segura. [23]

2.2.3 Mecanismos de encriptación

La encriptación es básicamente transformar datos en alguna forma que no sea legible sin el conocimiento de la clave o algoritmo con el cual se realizó la modificación (un algoritmo es el proceso matemático mediante el cual se protege la información, la clave es el código o el número secreto necesarios para leer, modificar o comprobar los datos protegidos). El propósito es mantener oculta la información que se considera privada a cualquier persona

o sistema que no tenga permitido verla. La encriptación en general requiere el uso de información secreta para su funcionamiento la cual es llamada “llave” o “clave”. Algunos sistemas de encriptación utilizan la misma llave para cifrar y descifrar los datos, otros utilizan llaves diferentes.

Sólo las claves deben ser secretas pues la seguridad de un sistema estratégico se basa totalmente, o de forma esencial en el secreto de la clave [21]. El conocimiento del algoritmo empleado no permite acceder a la información protegida si se desconoce la llave utilizada. Por lo tanto se debe poner énfasis en el correcto almacenamiento, control, vida útil y destrucción de las claves generadas y utilizadas.

Algoritmos Simétricos: Utilizan la misma llave para encriptar y desencriptar. Estas claves cambian frecuentemente y se les conoce como claves de sesión cuando se generan aleatoriamente. Comparados con los algoritmos de claves públicas son mucho más rápidos y por lo tanto son utilizados para encriptar grandes cantidades de datos.

Existen diversos algoritmos de cifrado en bloques de llave única, entre ellos están:

- DES (Data Encryption Standard): esquema de encriptación simétrico desarrollado en 1977, posteriormente se desarrollo una versión DES implementada por hardware (DEA). En general, utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, los 8 restantes son de paridad y se usan para la detección de errores en el proceso.
- Triple-DES: aplica tres veces sucesivas el algoritmo DES con secuencia de cifrado y descifrado combinando la utilización de dos claves.
- Lucifer: precursor del DES
- NewDES: Utiliza bloque de 64 bits y llave de 120 bits
- IDEA: bloques de 64 bits con llaves de 128 bits
- MMB: bloques y llaves de 128 bits [R6]

Algoritmos asimétricos: Los algoritmos de clave pública (asimétricos) utilizan dos claves diferentes y relacionadas, una clave pública y otra clave privada, esta última es mantenida en secreto por dueño de la misma y la pública es distribuida a quien la requiera. Cuando una clave es utilizada para encriptar, se deberá utiliza la otra para desencriptar el mensaje.

Los algoritmos de clave pública son más lentos que los algoritmos simétricos en varios órdenes de magnitud. En consecuencia, se utilizan en forma combinada con un

algoritmo simétrico encriptando una clave de sesión con la clave pública del destinatario del mensaje. Estos sistemas se conocen como Híbridos. También se utilizan para firmar digitalmente un mensaje encriptando con la llave privada del emisor. De esta manera cualquier persona puede verificar el origen del mensaje. [R6]

2.2.3.1 Infraestructura de Claves Públicas (PKI)

En la práctica, no es razonable usar secretos compartidos con anterioridad por lo que es necesaria una PKI (*Public Key Infraestructure*). El término infraestructura de claves públicas (PKI) se utiliza para describir las directivas, los estándares y el software que regulan o manipulan los certificados y las claves públicas y privadas. En la práctica, PKI hace referencia a un sistema de certificados digitales, entidades emisoras de certificados (CA) y otras entidades de registro que comprueban y autentican la validez de cada parte implicada en una transacción electrónica. Los estándares de la infraestructura de claves públicas siguen evolucionando, aunque se estén implementando de forma generalizada como elemento necesario del comercio electrónico. [26]

2.2.3.2 Certificados digitales.

Un certificado de claves públicas se utiliza para autenticar y asegurar el intercambio de información en Internet, extranets e intranets. Al emisor y firmante del certificado se le conoce como entidad emisora de certificados (CA). Es una declaración firmada digitalmente que enlaza el valor de una clave pública a la identidad del tema que posee la clave privada permanente.

Al firmar el certificado, la entidad emisora (CA) atestigua que la clave privada asociada a la clave pública del certificado está en posesión del tema indicado en el certificado.

Una CA es una especie de notario público que se encarga de certificar la autenticidad y credibilidad de individuos, aplicaciones, entidades y datos. Una Infraestructura de Llave Pública (PKI, Public Key Infrastructure) está compuesta por una jerarquía de CAs que se certifican unas a otras. Un usuario o una aplicación confía en la jerarquía de CAs para establecer relaciones de confianza con otros usuarios o aplicaciones. [14]

Los certificados pueden emitirse con objetivos diferentes, entre ellos la autenticación de usuarios y servidores Web, la seguridad del correo electrónico (S/MIME), de IP, nivel de *sockets* seguros, seguridad en el transporte (SSL/TLS) y firma de código. En el

certificado, el tema puede especificarse con varios nombres, como nombre principal de usuario, de directorio, DNS. Los certificados también contienen:

1- Periodo de validez
2- Número de serie del certificado que la entidad emisora de certificados garantiza como único.
3- El nombre de la entidad que emitió el certificado y la clave utilizada para firmarlo.
4- Identificador de la directiva seguida por la emisora de certificados.
5- Los usos del par de claves.
6- La ubicación de la Lista de Revocación de Certificados (CRL). Una CRL se firma con la clave privada de la CA para garantizar su integridad.

El formato más común se define en la versión 3 del estándar internacional ITU-T X.509. RFC 2459, un perfil de X.509v3, clarifica los campos definidos en X.509v3

Uno de los primeros elementos a implementar para dar seguridad a una VPN sería aprovechar la capacidad que tiene IPSec de autenticar los extremos de la comunicación mediante certificados digitales. El uso de certificados digitales elimina el problema de la distribución de claves ya que un certificado digital, al ser público, puede ser distribuido por un canal inseguro.

Implantar un sistema PKI para emitir certificados digitales permite tener el control absoluto de la emisión, renovación y revocación de los certificados digitales usados en la VPN, su utilización no se limita sólo a las VPN sino que la misma infraestructura puede utilizarse para aplicaciones como cifrado de correo electrónico, firma digital, etc. [29]

2.3 Autenticación en las Redes Privadas Virtuales

Con el uso de certificados digitales, se garantiza la autenticación de los elementos remotos que generan el túnel, pero es necesario autenticar a los usuarios remotos y esto depende de dónde se almacene el certificado digital y la clave privada:

- Si el certificado digital y la clave privada se almacenan, protegidos por un PIN, en una tarjeta inteligente que el usuario lleva consigo, sí se está autenticando al usuario. Actualmente existen en el mercado Clientes IPSec compatibles con el

estándar PKCS#11 que permiten la lectura de una tarjeta inteligente para obtener un certificado.

- Si el certificado digital y la clave privada se almacenan en el propio equipo, no se está autenticando al usuario, sino al equipo. Para autenticar al usuario, algunos fabricantes de sistemas VPN han añadido un segundo nivel de autenticación. El uso de contraseñas (*passwords*) es un nivel adicional de seguridad, pero no es el más adecuado, ya que carecen de los niveles de seguridad necesarios en este tipo de entorno: son fácilmente reproducibles, pueden ser capturadas y realmente no autentican a la persona, ya que la autenticación se basa en un solo factor (lo que una persona conoce). La forma más adecuada de autenticar a los usuarios remotos, a falta de tarjetas inteligentes, es el uso de sistemas de autenticación fuerte. Estos sistemas se basan en la combinación de dos factores, lo que la persona tiene (un *token* o autentificador) y lo que la persona sabe (un PIN, *Personal Identification Number*). Por ejemplo, las tarjetas de cajero automático utilizan una forma simple de autenticación de dos factores porque para usarla es necesario tener la tarjeta (“algo que se tiene”) y saber el PIN (“algo que se sabe”). [29]

Autorización y control de acceso: Una vez que se conoce quien está al otro lado del túnel, mediante el uso de certificados digitales y sistemas de autenticación fuerte, es necesario, para ganar en seguridad, controlar donde están accediendo las oficinas y usuarios remotos. Este control de acceso se puede realizar utilizando sistemas de control de acceso o cortafuegos, y sistemas de autorización. De esta manera se aplican políticas de acceso a determinados sistemas en función de usuarios o grupos de usuarios.

Como cualquier otra red, una VPN, requiere de establecer políticas de seguridad lo que implica instalar, en diferentes partes de la red, herramientas de autentificación, sistemas de encriptación y detectores de intrusos [13]

2.4 Seguridad del protocolo IPSec

La Seguridad de Protocolo de Internet (IPSec) es una protección eficaz para las redes privadas contra ataques desde Internet. Define un conjunto de servicios de protección basados en criptografía y protocolos de seguridad. Los únicos equipos que deben saber sobre la protección de IPSec son el remitente y el receptor en la comunicación.

Los protocolos IPSec combinan IP tunneling con la autenticación reforzada, encriptación e integridad. La autenticación asegura que los remitentes y receptores son quienes ellos dicen ser, la encriptación mantiene en secreto datos de usuario y las verificaciones de integridad aseguran que nadie altera los datos del paquete que viaje por

la VPN. IPSec ofrece múltiples niveles de seguridad y varios algoritmos de encriptación y de enlace y los protocolos de intercambio de claves para negociar las conexiones e intercambio de las claves criptográficas.[11]

El diseño de TCP/IP (IPv4) no está concebido teniendo en cuenta aspectos de seguridad. Es por eso que la seguridad en IPv4 pasa por una de estas alternativas; Seguridad en las aplicaciones, uso de cortafuegos o uso de IPSec.

Existen tres característica de IPv4 que tienen implicaciones para la seguridad.

- Independencia del medio y/o protocolo (IP over everything): IP incluye un sistema de direccionamiento independiente del medio/protocolo. Incluyendo gestión de encaminamiento. El sistema de direccionamiento no asegura que las direcciones de emisor y receptor sean auténticas: Un datagrama IP, independiente de lo que diga su dirección de origen.
- Transporte de datos sin estado (orientado a datagrama): Cada paquete recibe tratamiento independiente. No hay reserva de recursos. Protocolos y aplicaciones por encima de IP
- Servicio no fiable: IP ofrece un servicio no fiable en dos sentidos, ya que no se garantiza la entrega de un datagrama y no se comprueba la integridad de los datos del datagrama. TCP se encarga de asegurar la entrega mediante asentimientos y retransmisiones.

La seguridad es una de las grandes ventajas que presenta IPv6. Este protocolo de comunicación incluye, de forma obligatoria e intrínseca en su núcleo, la especificación de seguridad IPSec. Con IPv6 todo el tráfico de la red va a ser autenticado. [9]

La implementación de IPSec en la capa de red habilita un nivel alto de protección sin demasiados problemas. Al desplegar IPSec no es necesario realizar ningún cambio en las aplicaciones existentes o sistemas operativos. Otros mecanismos de seguridad que operan por encima de la Capa de red, como *Secure Sockets Layer* (SSL), sólo proporcionan seguridad en las aplicaciones que saben cómo utilizar SSL, como por ejemplo los exploradores de Web.

La implementación de IPSec en la capa de red proporciona protección para todos los protocolos IP y de capa superior en el conjunto de protocolo TCP/IP, como TCP, UDP, ICMP e incluso en los protocolos personalizados que envían tráfico en la capa IP. La primera ventaja de asegurar información en esta capa es que todas las aplicaciones y

servicios que utiliza IP para el transporte de datos se pueden proteger con IPSec sin que se produzca ninguna modificación en estas aplicaciones o servicios. (para asegurar protocolos distintos a IP, se han de encapsular los paquetes mediante IP).

- Protección basada en criptografía

IPSec protege los datos de modo que a un intruso le resulte sumamente difícil o imposible interpretarlos. Para proteger la información se utiliza una combinación formada por un algoritmo y una clave. Mediante las claves y los algoritmos basados en criptografía se consigue un alto grado de seguridad. IPSec además reduce significativamente la posibilidad de que se produzcan ataques a través de la red gracias a características como las siguientes:

- Administración automática de claves

1- Generación de claves

Para habilitar una comunicación segura, dos equipos deben poder establecer la misma clave compartida, sin transmitirla a través de la red. IPSec utiliza el algoritmo Diffie-Hellman para posibilitar este intercambio de claves y proporciona el material para la generación de las demás claves de cifrado.

Los dos equipos inician el cálculo Diffie-Hellman y, después, intercambian un resultado intermedio de forma pública y segura (mediante la autenticación). Ninguno de los equipos envía la clave real. A partir de la información compartida en el intercambio, cada equipo genera una clave secreta, que es la misma en los dos casos. Los usuarios expertos pueden cambiar la configuración predeterminada de la clave de cifrado de datos y del intercambio de claves. [10]

2 - Longitud de las claves

Cada vez que se incrementa en un bit la longitud de una clave, el número de claves posibles se duplica, con lo que se dificulta exponencialmente el descubrimiento de la clave. La negociación de la seguridad IPSec entre dos equipos genera dos tipos de claves secretas compartidas: claves maestras y claves de sesión. Las claves maestras son largas, con 768 ó 1024 bits. Estas claves se utilizan como origen del que se derivan las claves de sesión. Las claves de sesión se derivan de la clave maestra de manera estándar, una clave de sesión para cada algoritmo de cifrado e integridad necesario. [10]

3- Generación dinámica de claves

IPSec puede generar automáticamente claves nuevas durante una comunicación. Así se evita que un intruso tenga acceso a toda la comunicación mediante una sola clave. Los usuarios expertos pueden cambiar los intervalos predeterminados para la generación de claves.[10]

- Servicios de seguridad

1 -Integridad

La integridad protege la información de la modificación no autorizada durante el tráfico, lo que garantiza que la información recibida coincida exactamente con la enviada. Se utilizan funciones de hash para marcar o señalar de forma única cada paquete. El equipo de destino comprueba la firma antes de abrir el paquete. Si la firma (y, por lo tanto, el paquete) ha cambiado, se descarta el paquete para evitar un posible ataque a través de la red.[10]

2 -Autenticación

La autenticación permite comprobar el origen y la integridad de un mensaje al asegurar la identidad genuina de cada equipo. Sin autenticación de alto nivel, un equipo desconocido es sospechoso, así como la información que envía.[10]

3- Confidencialidad (cifrado de datos)

Con la confidencialidad se garantiza que los datos sólo sean revelados a los destinatarios previstos. Cuando se selecciona, se utiliza el formato Carga de seguridad encapsuladora (ESP) de paquetes IPSec. Los datos de los paquetes se cifran antes de la transmisión, con lo que se asegura que no se pueden leer durante la misma, aunque el paquete sea supervisado o interceptado por un intruso. Sólo el equipo con la clave secreta compartida puede interpretar o modificar los datos. Los algoritmos del Estándar de Cifrado de Datos (DES, *Data Encryption Standard*) de Estados Unidos, DES y 3DES, se utilizan para proporcionar la confidencialidad de la negociación de la seguridad y del intercambio de datos de aplicaciones.

4- Aceptación (o imposibilidad de repudio)

Garantiza que el remitente de un mensaje sea la única persona que puede haber enviado el mensaje; el remitente no puede negar que ha enviado el mensaje.

5- Reproducción no permitida

También se conoce como impedimento de reproducción o protección frente a repetición. Garantiza la exclusividad de cada paquete IP. Los mensajes capturados por un intruso no se pueden volver a utilizar ni reproducir para establecer una sesión ni obtener acceso a la información ilegalmente.

- *Negociación de seguridad IPSec*

  Antes de que se pueda intercambiar información asegurada, ha de establecerse un contrato entre los dos equipos. A este contrato es al que se denomina Asociación de Seguridad (SA). En una SA, los dos equipos acuerdan el modo de intercambiar y proteger información. [10]

  1- Asociaciones de seguridad

  Esta combinación de una directiva y claves define los servicios, mecanismos y claves de seguridad comunes utilizados para proteger la comunicación de un lugar a otro. El SPI es un valor único e identificable en la SA utilizado para distinguir entre múltiples asociaciones de seguridad que existen en el equipo receptor. Por ejemplo, pueden existir múltiples asociaciones si un equipo se comunica con seguridad con múltiples equipos a la vez. Esta situación tiene lugar principalmente cuando el equipo es un servidor de archivo o un servidor de acceso remoto que sirve a múltiples clientes. Sin embargo, un equipo puede tener múltiples SA con un solo equipo. En estos caso, el equipo receptor utiliza el SPI (en combinación con la IP de destino y el protocolo de seguridad, únicamente identifica el SA para este datagrama) para determinar que SA se utilizará para procesar los paquetes de entrada.

  Para establecer este contrato entre los dos equipos, el IETF ha establecido un método estándar de asociación de seguridad y una resolución de intercambio clave que combina la Asociación de seguridad de Internet, el protocolo de administración clave (ISAKMP) y el protocolo de generación de clave Oakley. ISAKMP centraliza la administración de asociación de seguridad, reduciendo el tiempo de conexión. Oakley genera y administra las claves autenticadas utilizadas para asegurar la información.

  Este proceso protege no sólo las comunicaciones entre equipos, sino también los equipos remotos que solicitan el acceso seguro a una red corporativa o cualquier

situación en la que la negociación para el equipo de destino final (o punto final) se está realizando mediante un encaminador de seguridad u otro servidor proxy. En la última situación, a la que se denomina *Modo de cliente ISAKMP*, las identidades de los puntos finales se esconden para seguir protegiendo la comunicación.

Para asegurar una comunicación segura y con éxito, ISAKMP/Oakley (IKE, *Internet Key Exchange*) realiza una operación de dos fases. Se asegura la confidencialidad y la autenticación durante cada fase mediante la utilización del cifrado negociado y los algoritmos de autenticación acordados entre los dos equipos. Con las tareas divididas en las dos fases, se agiliza la escritura cuando resulte necesario. [10]

2- Intercambio de clave

Durante la fase inicial, los dos equipos establecen la primera SA, denominada ISAKMP SA. (Esta SA se nombra con el fin de diferenciar entre las SA establecidas en cada una de las dos fases). Oakley proporciona protección de identidad durante este intercambio, permitiendo una discreción absoluta. De esta manera, se ayuda a evitar los tipos de ataque de red más comunes que se centran en las identidades intrusas.

El proceso de negociación de seguridad durante esta fase comprende:

- Negociación de directiva.

  Determina:

  - El algoritmo de cifrado: DES, 3DES, 40bitDES o ninguno.
  - El algoritmo de integridad: MD5 o SHA.
  - El método de autenticación: Certificado con clave pública, clave compartida previamente o Kerberos V5 (la opción predeterminada en Windows 2000).
  - El grupo Diffie-Hellman.

- Intercambio de información clave:

  Tiene como resultado que cada equipo disponga de la información necesaria para generar la clave compartida secreta (la clave principal) para la ISAKMP SA. Las claves reales no se intercambian nunca, únicamente la información pública que necesita Diffie-Hellman para generar la clave secreta compartida. El servicio

Oakley de cada equipo genera la clave principal utilizada para proteger la autenticación. [9]

- Autenticación

  Si se produce un error en la autenticación, no se puede proceder con la comunicación. Independientemente del método de autenticación utilizado, la carga de identidad está protegida contra la modificación y la interpretación.

  La ISAKMP SA se utiliza para iniciar la segunda fase de las negociaciones de seguridas, combinado con el protocolo de intercambio de llaves Oakley: (IKE), es de los más populares protocolos para la implementación y negociación de sesiones VPN. [9]

- Protección de información

  Se negocia un par de SA en nombre del servicio IPSec y se les denomina IPSec SA. El proceso de negociación de seguridad durante esta segunda fase comprende:

  1. Negociación de directiva.

     Que determina:

     - El protocolo IPSec: AH, ESP.
     - El algoritmo de integridad: MD5, SHA.
     - El algoritmo de cifrado: DES, 3DES, 40bitDES o ninguno.

     Se llega a un acuerdo común, y se establecen dos SA: una para las comunicaciones de entrada y otro para las comunicaciones de salida.

     Oakley renueva el material escrito y se generan nuevas claves secretas compartidas para autenticar y, posiblemente, cifrar los paquetes. Si se necesita una nueva clave, se produce un segundo intercambio Diffie-Hellman. Si la clave o SA no ha caducado, Oakley renueva el material escrito procedente del intercambio Diffie-Hellman que se ha realizado durante el intercambio clave. [9]

  2. Las SA y las claves se pasan a la unidad IPSec, junto con el SPI.

     Toda la negociación está protegida por la ISAKMP SA. Excepto el encabezado ISAKMP de los paquetes, todos los paquetes de mensajes están cifrados y la firma de integridad que aparece tras el encabezado ISAKMP autentica el mensaje.

Oakley impide repeticiones de mensajes de negociación al proporcionar la protección de anti-repetición.

El proceso de reintento de mensaje automático es casi idéntico al proceso descrito en la negociación de intercambio de clave, con una excepción: si este proceso llega a finalizar por cualquier razón durante la segunda o más importante negociación de la misma ISAKMP SA, se intenta una nueva negociación de la ISAKMP SA. Si se recibe un mensaje para la fase de protección de información sin establecer una ISAKMP SA, se rechaza.

La capacidad de utilizar una única ISAKMP SA para las múltiples negociaciones de SA de IPSec agiliza el proceso de negociación de seguridad. [9]

2.4.1 Funcionamiento de IPSec

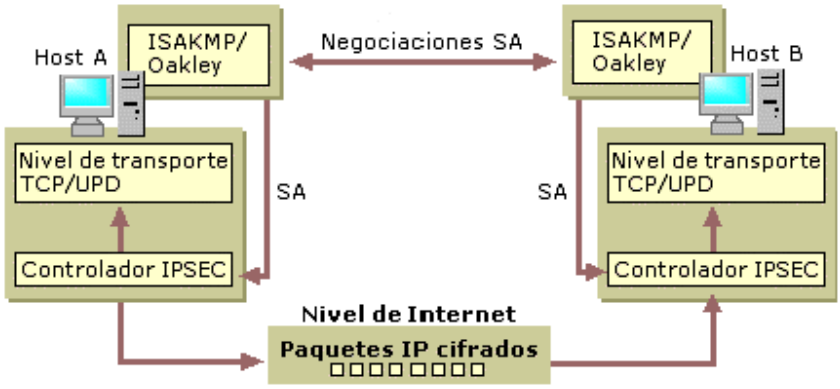

Fig. 2.6: Esquema representativo del funcionamiento de IPSec.

1. La unidad de IPSec en el equipo A comprueba la lista de filtro IP en una directiva para buscar la correspondencia con la dirección o el tipo de tráfico de los paquetes de salida.
2. La unidad de IPSec notifica a ISAKMP para iniciar las negociaciones de seguridad con el equipo B.
3. El servicio ISAKMP en el equipo B recibe una solicitud de negociaciones de seguridad.
4. Los dos equipos realizan un intercambio de clave, establecen un ISAKMP y una clave secreta compartida.
5. Los dos equipos negocian el nivel de seguridad para la transmisión de información, establecen un par de IPSec SA y las claves para asegurar los paquetes IP.

6. Al utilizar la IPSec SA y clave de salida, la unidad de IPSec en el equipo A firma los paquetes por integridad, y cifra los paquetes si se ha negociado la confidencialidad.
7. La unidad IPSec en el equipo A transfiere los paquetes al tipo de conexión apropiado para la transmisión al equipo B.
8. El equipo B recibe los paquetes asegurados y los transfiere a la unidad de IPSec.
9. Al utilizar la SA y la clave de salida, la unidad de IPSec en el equipo B comprueba la firma de integridad y descifra los paquetes.
10. La unidad de IPSec en el equipo B transfiere los paquetes descifrados a la unidad TCP/IP, que los transfiere a la aplicación de recepción.

    Los usuarios de A y B no ven ninguno de los procesos. Los enrutadores en la ruta de información entre los interlocutores no necesitan IPSec. De manera automática envían los paquetes IP cifrados al destino. Sin embargo, si un enrutador funciona como un cortafuego, puerta de seguridad o servidor proxy, debe habilitar el filtrado especial para habilitar los paquetes IP asegurados y poder pasar. [9]

2.5 Redes Privadas Virtuales con IPSec

El túnel es la ruta de información lógica a través de la cual viajan los paquetes encapsulados. Para los interlocutores de origen y de destino originales, el túnel suele ser transparente y aparece simplemente como otra conexión punto a punto en la ruta de acceso a la red. Los interlocutores desconocen los enrutadores, servidores proxy u otras puertas de enlace de seguridad entre los extremos del túnel. Cuando el túnel se combina con la privacidad que puede garantizar IPSec, se puede utilizar para implementar redes privadas virtuales (VPN).

Hay disponibles dos tipos de túneles que utilizan IPSec:

1. Protocolo de túnel de nivel 2 (L2TP/IPSec), con el que L2TP administra el encapsulamiento y el túnel para cualquier tipo de tráfico de red e IPSec en modo de transporte proporciona la seguridad de los paquetes de túnel L2TP.
2. IPSec en modo de túnel, con el que IPSec realiza la encapsulamiento del tráfico IP. [9]

2.6 Protocolos de encapsulamiento

El enfoque general de VPN IP tradicional es encapsular cada paquete IP en otro paquete IP antes de ponerlo en la red pública. El paquete saliente se dirige a la pasarela (gateway) VPN o cliente VPN creando un túnel a través de la red escondiendo la dirección del último destino.

Dos protocolos VPN iniciales son L2F, desarrollado por Cisco, y PPTP, desarrollado por Microsoft (basados en el Protocolo Punto a Punto, PPP). El IETF (Internet Engineering Task Force) diseñó un tercer protocolo, L2TP como una alternativa para el vendedor neutral. Posteriormente, debido mayormente a las preocupaciones de seguridad los tres protocolos se adecuaron a IPSec.

2.6.1 Protocolo Tunel Punto a Punto (PPTP)

Es una especificación de protocolos desarrollada por varias compañias, Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics. Su principal ventaja está en soportar protocolos no IP así como su principal inconveniente es su única encriptación y autenticación estándar. Este protocolo tiene problemas de seguridad y se aconseja implementarlo para evitar la entrada de intrusos nobles pero no es invulnerable. Se diseñó originalmente como una forma de encapsular protocolos no TCP/IP (como IPX) para poder ser transmitidos por Internet usando GRE (Generic Routing Encapsulation). Por tanto es una tecnología de red que admite VPNs multiprotocolo, permitiendo así a los usuarios remotos el acceso seguro a redes empresariales a través de Internet u otras redes al marcar el número de acceso a un ISP o al conectarse directamente a Internet. PPTP simula un túnel para el tráfico IP, IPX o NetBEUI en paquetes IP, esto permite ejecutar de forma remota aplicaciones que dependen de determinados protocolos de red.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser enrutado a través de una red IP, como Internet.

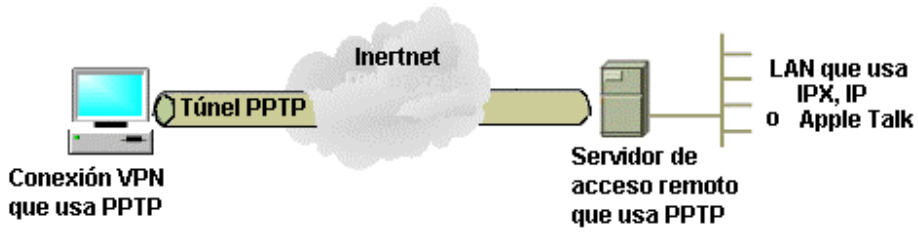

Fig. 2.7: Conexión VPN que usa PPTP.

Tipos de conexión para las VPN basadas en PPTP:

- El usuario remoto puede conectarse a un ISP que provee el servicio de PPTP hacia el servidor RAS (el usuario remoto establece una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS).
- El usuario remoto puede conectarse a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente. Esto es aplicable también en un ambiente Intranet (el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma)
- Conexión de dos redes privadas a través de Internet o una Intranet (existe una conexión PPTP preestablecida entre dos redes, por lo que los usuarios no tienen que establecer ninguna conexión con los servidores VPN) [16]

2.6.1.1 Técnica de encapsulamiento de PPTP

La técnica de encapsulamiento de PPTP se basa en el protocolo GRE, que puede ser usado para realizar túneles para protocolos a través de Internet. La versión para PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id (Identificador de llamada) y velocidad de conexión.

El paquete PPTP está compuesto de una trama PPP (que contiene el paquete de carga correspondiente a la red privada), por un encabezado GREv2 y un encabezado IP. El encabezado IP contiene las direcciones IP de origen y de destino que corresponden al cliente VPN y al servidor VPN. El encabezado GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que en el

caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. [16]

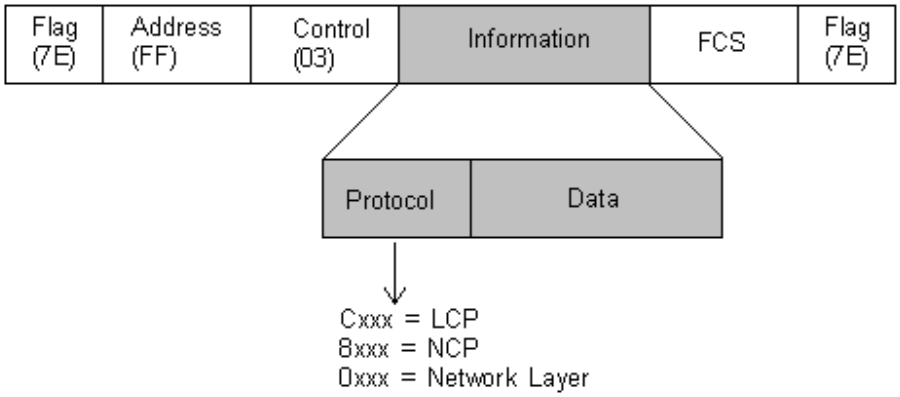

Fig 2.8: Formato de trama PPP.

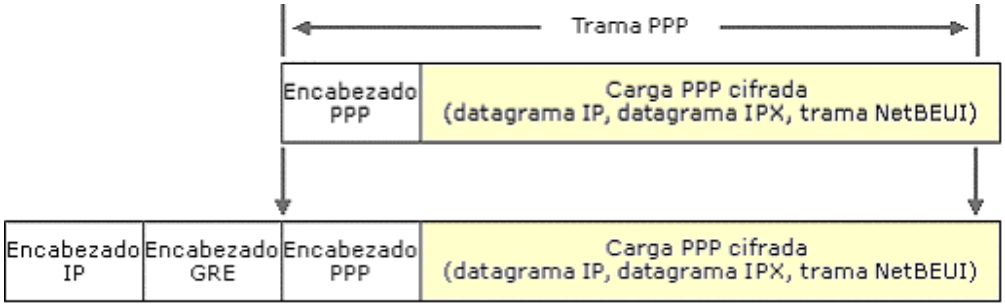

Fig. 2.9: Encapsulamiento PPTP para una trama PPP.

El paquete IP resultante se enmarca en un protocolo de enlace para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, Frame Relay, PPP, entre otros.

2.6.1.2 Cifrado de la trama PPTP

La trama PPP se cifra con el Cifrado punto a punto de Microsoft (MPPE, *Microsoft Point-to-Point Encryption*) que usa claves de cifrado de los procesos de autenticación MS-CHAP o EAP-TLS. Los clientes de red privada virtual deben utilizar el protocolo de autenticación MS-CHAP o el protocolo de autenticación extensible (EAP, *Extensible Authentication Protocol*), para poder cifrar las cargas de las tramas PPP. PPTP aprovecha el cifrado PPP subyacente y encapsula una trama PPP cifrada anteriormente.

Es posible utilizar una conexión PPTP no cifrada en la que la trama PPP se envíe como texto sin formato. Sin embargo, este tipo de conexión PPTP sin cifrado no se recomienda

en conexiones VPN a través de Internet, ya que las comunicaciones de este tipo no son seguras.

2.6.1.3 Opciones de PPTP para la autenticación.

Para la autenticación, PPTP tiene tres opciones: CHAP, MS-CHAP y aceptar cualquier tipo, incluso texto plano. Si se utiliza CHAP, estándar en el que se intercambia un "secreto" y se comprueba que ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña del sistema operativo como secreto. MS-CHAP es un estándar propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercera opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.

2.6.1.4 VPN de acceso remoto basadas en PPTP

Los servicios VPN proporcionan acceso a una intranet corporativa a los clientes de acceso remoto que establecen conexiones PPTP a través Internet.

Mediante los siguientes pasos se describe qué ocurre durante el intento de conexión de un cliente y un servidor VPN basados en PPTP:

1. El cliente VPN crea un túnel PPTP con el servidor VPN.
2. El servidor envía un desafío al cliente.
3. El cliente envía una respuesta cifrada al servidor.
4. El servidor contrasta la respuesta con la base de datos de cuentas de usuarios.
5. Si la cuenta es válida y tiene permisos de acceso remoto, el servidor acepta la conexión de acuerdo con las directivas de acceso remoto y las propiedades de la cuenta de usuario del cliente VPN.

En los pasos 2 a 4 el cliente VPN y el servidor VPN utilizan los protocolos de autenticación CHAP o para una mayor seguridad el MS-CHAPv2. El envío de las credenciales del cliente puede variar en otros protocolos de autenticación.

2.6.2 Protocolo túnel nivel 2 (L2TP)

El principal competidor de PPTP en soluciones VPN fue L2F. Con el objetivo de mejorar L2F se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP que opera en el nivel de enlace del modelo OSI y al igual que PPTP soporta clientes no IP y encapsula las tramas PPP, que a su vez encapsulan los protocolos IP, IPX o NetBEUI, con lo que permiten que los usuarios ejecuten de forma

remota aplicaciones que dependen de protocolos de red específicos. L2TP utiliza el protocolo de autenticación y cifrado IPSec para los servicios de cifrado añadiendo seguridad a la transmisión. La combinación de L2TP e IPSec se conoce como L2TP sobre IPSec. [13]

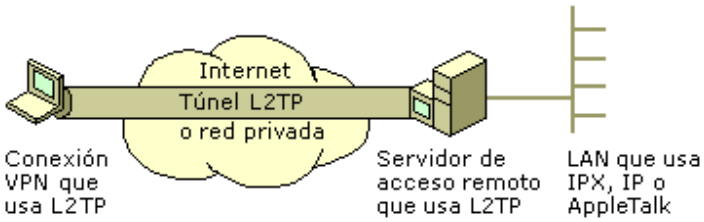

Figura 2.10: Representación del L2TP.

2.6.2.1 L2TP e IPSec

IPSec y L2TP se combinan para proporcionar túneles y seguridad para los paquetes IP, IPX y de otros protocolos que viajen por cualquier red IP. IPSec también puede realizar túneles sin L2TP, pero sólo se recomienda para la interoperabilidad, cuando una de las puertas de enlace no admite L2TP o PPTP.

- Encapsulamiento IPSec

  El mensaje L2TP resultante se empaqueta a continuación con un encabezado y un finalizador de Carga útil de seguridad de encapsulamiento (ESP, Encapsulating Security Payload) de IPSec, un finalizador de autenticación IPSec que proporciona autenticación e integridad de mensajes y un encabezado IP final. El encabezado IP contiene las direcciones IP de origen y de destino que corresponden al cliente VPN y al servidor VPN. [25]

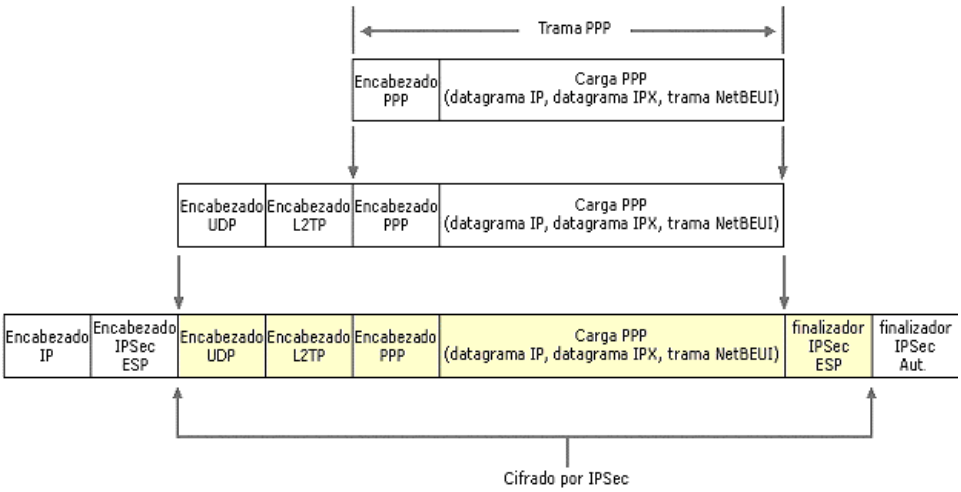

Figura 2.11: Encapsulamiento L2TP e IPSec para un datagrama PPP.

2.6.2.2 Túneles IPSec

El motivo principal por el que se utiliza el modo de túnel IPSec es para la interoperabilidad con otros enrutadores, puertas de enlace o sistemas finales que no admiten la tecnología de túneles de VPN L2TP/IPSec o PPTP. El modo de túnel IPSec se admite como característica avanzada sólo en casos de túneles de puerta de enlace a puerta de enlace y para determinadas configuraciones de servidor a servidor o de servidor a puerta de enlace.

El modo de túnel IPSec no se admite para casos de VPN de acceso remoto a clientes. Debe utilizarse L2TP/IPSec o PPTP para VPN de acceso remoto a clientes.

Los dos formatos de paquetes IPSec se pueden utilizar también en modo de túnel:

Modo de túnel ESP

El encabezado IP original (que es el encabezado del paquete original) contiene normalmente las direcciones de origen y destino definitivas, mientras que el encabezado IP externo contiene las direcciones de origen y destino correspondientes a las puertas de enlace de seguridad. El formato de túnel ESP siempre proporciona una gran integridad y autenticidad para el tráfico que pasa por el túnel. El túnel ESP se utiliza principalmente para ofrecer privacidad a los paquetes del túnel mediante el cifrado DES o 3DES. El nivel de cifrado se especifica en la acción de filtrado de la regla del túnel y, por tanto, también se puede configurar *sin cifrado* si el contenido del tráfico que pasa por el túnel no requiere privacidad.

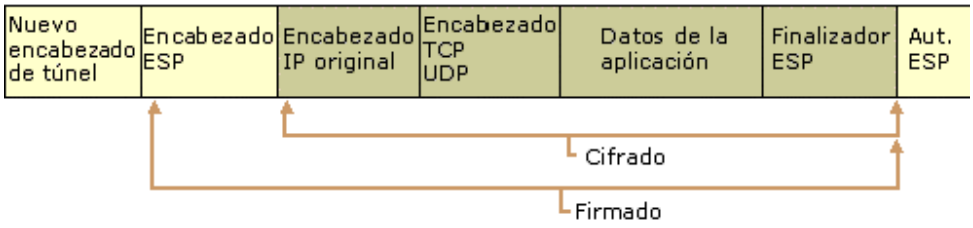

Fig. 2.12 : Representación de un túnel ESP.

En la figura anterior, el paquete original se encapsula mediante los nuevos encabezados IP y ESP entre el origen y el destino definitivos. El área *Firmada* indica dónde se ha protegido el paquete con integridad. El área *Cifrada* indica que puede estar cifrado el paquete original completo.

La información del encabezado IP nuevo se utiliza para enrutar el paquete desde el origen al extremo de destino del túnel, normalmente una puerta de enlace de seguridad. El encabezado IP ESP nuevo no está protegido por el hash de integridad. Éste es el diseño RFC de IETF que permite que los componentes de red modifiquen el encabezado de los paquetes según sea necesario a fin de ofrecer servicios adicionales, por ejemplo, cambiar las direcciones IP de origen y destino, o asignar una mayor prioridad a unos paquetes respecto a otros. [9]

Modo de túnel AH

El modo de túnel AH no proporciona la privacidad mediante el cifrado del contenido del túnel, sólo una gran integridad y autenticidad.

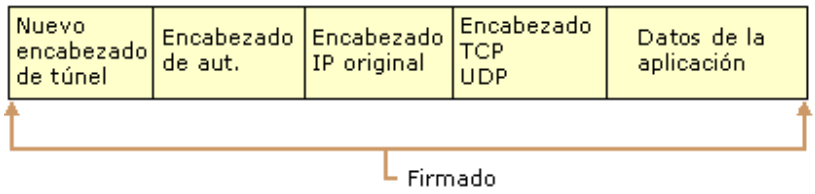

Figura 2.13: Representación de un túnel AH.

El paquete entero está firmado para la integridad, incluido el encabezado de túnel nuevo. Por tanto, no se pueden cambiar las direcciones de origen y destino una vez el paquete es enviado por el origen del túnel. El diseño RFC de IETF todavía permite que los componentes de red modifiquen algunos campos del encabezado IP nuevo para asignar prioridad a determinados paquetes y eliminar paquetes antiguos o extraviados. ESP y AH se pueden combinar para proporcionar túneles,

que incluyen tanto integridad para el paquete entero como confidencialidad para el paquete IP original. [9]

Como resultado, las conexiones de red privada virtual basadas en L2TP son una combinación de L2TP e IPSec, ambos protocolos deben ser compatibles con el cliente VPN y el servidor VPN.

El encapsulamiento de L2TP sobre paquetes IPSec consta de dos niveles:

1. Encapsulamiento L2TP
   Una trama PPP (un datagrama IP, un datagrama IPX o una trama NetBEUI) se empaqueta con un encabezado L2TP y un encabezado UDP.
2. Encapsulamiento IPSec
   El mensaje L2TP resultante se empaqueta a continuación con un encabezado y un finalizador de Carga útil de seguridad de encapsulamiento (ESP, Encapsulating Security Payload) de IPSec, un finalizador de autenticación IPSec que proporciona autenticación e integridad de mensajes y un encabezado IP final. El encabezado IP contiene las direcciones IP de origen y de destino que corresponden al cliente VPN y al servidor VPN.[251]

2.6.2.3 IPSec: Técnica de cifrado del protocolo L2TP

El mensaje L2TP se cifra con los mecanismos de cifrado IPSec que usan claves de cifrado generadas en el proceso de autenticación IPSec.

Es posible tener una conexión L2TP que no esté basada en IPSec (no cifrada) en la que la trama PPP se envía en texto sin formato. Sin embargo, este tipo de conexión L2TP sin cifrado no se recomienda en conexiones VPN a través de Internet, ya que las comunicaciones de este tipo no son seguras.

Las redes privadas virtuales (VPN) utilizan el cifrado en función del tipo de servidor al que se conecten. Si la conexión VPN está configurada para conectar con un servidor PPTP, se utiliza el cifrado MPPE. Si la conexión VPN está configurada para conectar con un servidor L2TP, se utilizan los métodos de cifrado IPSec.

2.6.2.4 VPN de acceso remoto basadas en L2TP

Se puede utilizar el acceso remoto para proporcionar acceso a una Intranet corporativa a los clientes de acceso remoto que establecen conexiones L2TP sobre IPSec a través de

una red pública, además el servidor de acceso remoto admite varias conexiones L2TP sobre IPSec, con una configuración determinada que incluye:

- Configurar la conexión a la red pública.
- Configurar la conexión a la Intranet.
- Configurar el servidor de acceso remoto como enrutador de una Intranet corporativa.
- Configurar el servidor de acceso remoto para clientes L2TP.
- Configurar los puertos L2TP.
- Configurar filtros L2TP sobre IPSec.

La figura muestra los elementos de un servidor de acceso remoto que proporciona acceso remoto basado en L2TP a una Intranet corporativa.

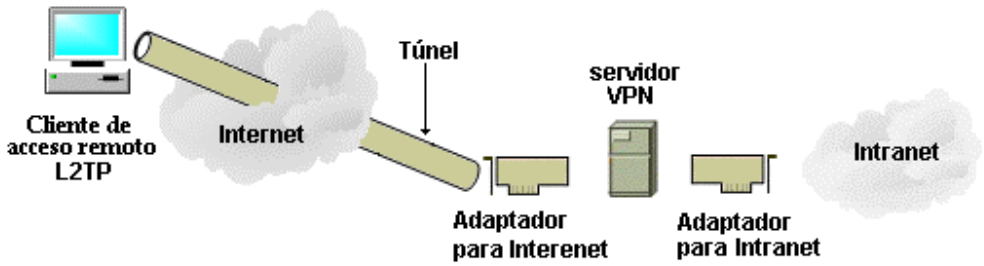

Fig. 2.14: Elementos de una VPN basada en L2TP.

En la configuración anterior se supone que los certificados de equipo ya están instalados en el servidor VPN y los clientes de acceso remoto. Los certificados de equipo son necesarios para las conexiones L2TP a través de IPSec.

Seguridad en el intento de conexión:

Los pasos siguientes describen qué ocurre durante el intento de conexión de un cliente VPN basado en L2TP a través de IPSec con un servidor VPN L2TP.

La asociación de seguridad IPSec se crea mediante certificados de equipo, ISAKMP (Protocolo de Administración de claves y asociación de seguridad Internet) y el protocolo de generación de claves Oakley.

1. El cliente VPN crea un túnel L2TP con el servidor VPN.
2. El servidor envía un desafío al cliente.
3. El cliente envía una respuesta cifrada al servidor.
4. El servidor contrasta la respuesta con la base de datos de cuentas de usuarios.

5. Si la cuenta es válida y tiene permisos de acceso remoto, el servidor acepta la conexión de acuerdo con las directivas de acceso remoto y las propiedades de la cuenta de usuario del cliente VPN.

El servidor de acceso remoto debe autenticar a los clientes VPN de acceso remoto para que éstos puedan tener acceso o generar tráfico en la red. Esta autenticación es un paso diferente del inicio de sesión. Después la autorización y la autenticación, y tras conectar a la LAN, los clientes VPN de acceso remoto están sujetos a la seguridad, tal como si estuvieran en la oficina. El administrador puede controlar con precisión la información disponible para los clientes VPN de acceso remoto y limitar su disponibilidad en caso de una ruptura de la seguridad.

2.7 Sistemas operativos para servidor VPN

2.7.1 Microsoft Windows 2000 Advanced Server

La característica VPN incluida en el sistema operativo Windows 2000 ofrece flexibilidad del servidor sin poner en peligro el rendimiento y la escalabilidad propios de los dispositivos hardware.

A petición de Microsoft Corporation, en diciembre de 1999 NSTL (National Software Testing Lab), la organización de pruebas de hardware y software independiente líder en el mundo, comprobó el rendimiento de la característica Red Privada Virtual (VPN) incluida en el sistema operativo Windows 2000 Server. Como resultados de estas pruebas se informó que, en cuanto al reenvío de paquetes, la característica VPN de Windows 2000 es comparable a los dispositivos VPN basados en hardware líderes de la industria. Las otras pruebas realizadas por NSTL confirman que Windows 2000 puede ofrecer un rendimiento adecuado como dispositivo VPN general. Si se agrega IPSEC se puede conseguir un rendimiento aún mayor con VPN de Windows 2000 utilizando L2TP/IPSec. [28]

En Windows 2000 Advanced Server se configura el servicio VPN a través del Servicio de enrutamiento y acceso remoto que incorpora el mismo, el cual proporciona:

- Servicios de enrutamiento de multiprotocolo LAN a LAN, LAN a WAN, red privada virtual (VPN, *Virtual Private Network*) y de traducción de direcciones de red (NAT, *Network Address Translation*).
- Servicios de acceso remoto de acceso telefónico y VPN.

2.7.1.1 Servicio de enrutamiento y acceso remoto

El Servicio de enrutamiento y acceso remoto es un servicio integrado único mediante el cual el servidor de Windows 2000 puede funcionar como un servidor de acceso remoto, un servidor VPN, una puerta de enlace o un enrutador (IP, IPX y AppleTalk).

Al proporcionar acceso remoto, el Servicio de enrutamiento y acceso remoto admite PPP (el protocolo de acceso telefónico estándar).

Si se utiliza como enrutador, el Servicio de enrutamiento y acceso remoto admite enrutamiento local (de LAN a LAN) y remoto (marcado a petición). Además de las conexiones de acceso telefónico, Frame Relay, ISDN o X.25, la conexión puede establecerse en la forma de una conexión directa a la red corporativa o de una conexión VPN de sucursal punto a punto a través de Internet. Este servicio admite los protocolos de control de enrutamiento OSPF y RIP2 para redes IP. [24]

2.7.1.2 Enrutamiento en MS Windows 2000 AS

Se le denomina enrutador de Windows 2000 al equipo que ejecuta Windows 2000 Server y el servicio de enrutamiento y acceso remoto, que suministra servicios de enrutamiento LAN y WAN.

Algunas características del enrutador de Windows 2000 relacionadas con VPNs:

- Filtrado de paquetes IP e IPX para seguridad y rendimiento.
- Enrutamiento de marcado a petición a través de vínculos WAN y LAN de acceso telefónico.
- Compatibilidad de la red privada virtual (VPN) con el Protocolo de túnel punto a punto (PPTP) y el Protocolo de túnel de capa 2 (L2TP) a través de la Seguridad de protocolos de Internet (IPSec).
- Compatibilidad estándar del sector con el Agente relé del Protocolo de configuración dinámica de host (DHCP) para IP.
- Compatibilidad con la creación de túneles mediante túneles IP en IP. [24]

2.7.1.2 Componentes de las redes privadas virtuales de MS Windows 2000 Advanced Server

Las redes privadas virtuales de Windows 2000 constan de los siguientes componentes:

- Servidores de red privada virtual (VPN): Puede configurar el servidor VPN para proporcionar acceso a toda la red o restringir el acceso a sólo los recursos del servidor VPN.
- Clientes VPN: Los clientes VPN son usuarios individuales que obtienen una conexión VPN de acceso remoto o enrutadores que obtienen una conexión VPN de enrutador a enrutador. Los equipos que ejecutan Windows 2000 Server con los Servicios de enrutamiento y acceso remoto (RRAS) pueden crear conexiones VPN de enrutador a enrutador. Los clientes VPN también pueden ser un cliente de PPTP o un cliente de L2TP sobre IPSec.
- Protocolos de LAN y de acceso remoto: Los programas de aplicación utilizan los protocolos de LAN para transportar información. Los protocolos de acceso remoto se utilizan para negociar conexiones y proporcionar el entramado para los datos del protocolo LAN que se envían a través de los enlaces de la red de área externa (WAN). Para las conexiones VPN, el acceso remoto de Windows 2000 admite el protocolo de acceso remoto PPP.
- Protocolos de túnel: Los clientes VPN utilizan los protocolos de túnel para crear conexiones seguras a un servidor VPN. Windows 2000 incluye los protocolos de túnel PPTP y L2TP.
- Compatibilidad con Internet: Las redes privadas virtuales Windows 2000 proporcionan servicios completos para VPN en Internet o Intranet. Puede configurar un equipo con Windows 2000 Server como servidor VPN, lo que ofrece conexiones seguras a los clientes de acceso remoto o a los enrutadores de marcado a petición.
- Opciones de seguridad: La seguridad de dominio e inicio de sesión de Windows 2000, la compatibilidad de host de seguridad, el cifrado de datos, el Servicio de usuario de acceso telefónico de autenticación remota (RADIUS, *Remote Authentication Dial-In User Service*), las tarjetas inteligentes, el filtrado de paquetes IP y el Id, del que llama proporcionan acceso de red seguro a los clientes VPN. [28]

La figura muestra todos los componentes de las redes privadas virtuales y las posibles configuraciones. Se tiene en cuenta que la implementación y la configuración real de una red privada virtual de Windows 2000 puede variar.

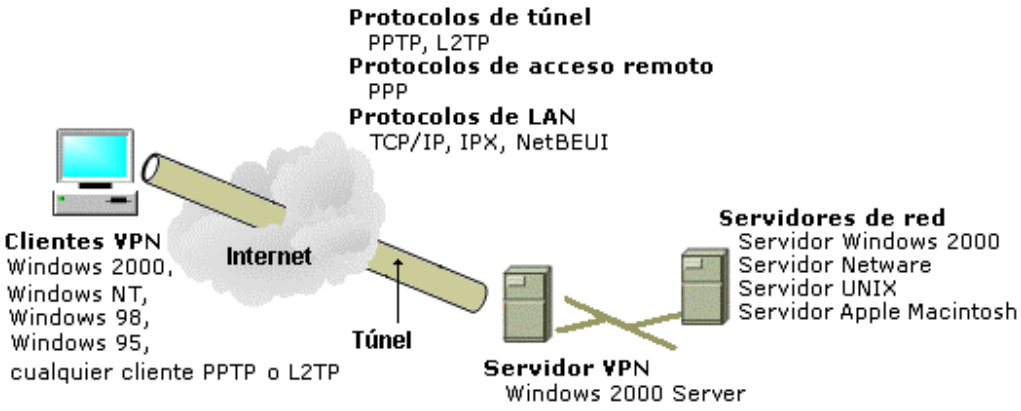

Figura 2.15 Componentes de las redes privadas virtuales de Windows 2000.

2.7.2 Linux

Para brindar soporte para el protocolo IPSec para el kernel de Linux actualmente existe una herramienta llamada FreeS/WAN (Free Secure over WAN) producto de la evolución de otras como S/WAN que funciona pasarela (gateway) VPN.

FreeS/WAN se ejecuta sobre varias versiones de Unix y Linux (Linux Red Hat v.8 es la recomendada) permite mantener un estándar que posibilita realizar conexiones hacia otras implementaciones FreeS/WAN, además de manejar con el estándar IPsec tantos puntos VPN como soporte el hardware y establecer Redes Privadas Virtuales con un alto nivel de encriptación en los datos y conexiones de gran ancho de banda. Cabe destacar que es posible utilizar FreeS/WAN con hardware dedicado para encriptación.

FreeS/WAN consta de 3 partes fundamentales:

KLIPS: es el soporte del protocolo IPsec dentro del kernel Linux. Implementa AH, ESP, y manejo de paquetes dentro del kernel. El protocolo AH provee autenticación de paquetes a nivel kernel. El protocolo ESP provee encriptación más autenticación.

PLUTO: Se encarga de negociar las conexiones con otros sistemas. El protocolo IKE es el encargado de negociar los parámetros de una conexión entre las dos partes participantes.

Diferentes scripts: Automatizan la tarea de administración del Gateway FreeS/Wan agregando rutas cuando sea necesario.
Existen tres formas de instalar FreeS/WAN en la computadora:

- Activando y probando FreeS/WAN sí está incluido en el sistema operativo (no son muchos los que lo incluyen; Debian, Mandrake, SuSE Linux, Coenctiva)
- Instalando los RPM
- Instalando desde fuentes

Tipos de Conexiones:

Punto a Red: Un usuario que soporta IPSec se conecta a una red. Puede acceder a cualquier punto de la misma de manera segura y confiable.

Red a Red: una red accede a otra conectándose con IPSec. Se puede acceder en cualquier maquina de ambas redes de manera segura y confiable.

Road-Warrior: Esta denominación es generalmente aplicada a host que se conectan a una red "segura" pero que tienen IP variable y el tipo de conexión es indiferente para FreeS/WAN, el único requisito es que este conectado a la misma red "insegura", en este caso la red pública, y una computadora que acceda a la misma a través de Dial-Up, ADSL, Cable-Módem, etc.

Uno de los puntos fuertes y diferenciadores de FreeS/WAN sobre otras implementaciones es el llamado OE (Oportunistic Encription). El mismo permite que dos gateways FreeS/WAN se comuniquen entre sí encriptando él tráfico, incluso si los administradores nunca han tenido contacto previo y ninguno de los sistemas tenga predefinido información del otro.

Para esto ambos sistemas deben tomar la información de autenticación que necesiten de DNS, así la administración, solo ingresa información en el sistema DNS y setean el gateway con OE. Para esto se necesita contar con algún servidor DNS que soporte DNSSEC. Esta técnica brinda dos grandes beneficios:

- Reduce el esfuerzo administrativo enormemente para IPSec. Un administrador configura el gateway FreeS/WAN, y todo lo demás es automático, la necesidad de configurar de manera "túnel" desaparece.
- Permite crear un ambiente en el cual la privacidad es un defecto. Todo él trafico será encriptado siempre que el otro lado lo permita.

OE no es todavía un estándar dentro del protocolo IPSec, pero, actualmente se encuentra en proceso de demostración para la futura incorporación dentro de IPSec. [22]

2.8 Conclusiones del capítulo

Las Redes Privadas Virtuales enfrentan riesgos de seguridad que pueden ser minimizados con una correcta aplicación de elementos como protocolos de encasulamiento, de encriptación, certificados digitales, sistemas de autenticación fuerte, control de acceso, topología de la red. Esto no garantiza que se eviten todas las penetraciones a la red, pero sí garantiza seguridad a la información que se intercambia, a través de tecnologías probadas, implementadas correctamente, con una adecuada política de seguridad, monitorización y gestión posterior.

3. Capítulo III: Propuesta de utilización de la tecnología VPN en intranets gerenciales de ETECSA.

3.1 Tendencias en las guías de implementación de Redes Privadas Virtuales.

Teniendo en cuenta la variedad de tecnologías, productos y arquitecturas que se involucran en la tecnología de VPN, el hecho de contar con una guía de implementación al implantar una VPN puede considerarse una gran ayuda para cualquier organización así como también lo son criterios para seleccionar dentro de un amplio rango de elementos de seguridad aquellos que le añaden seguridad a la información que se intercambia. [5]

La tendencia en cuanto a este tipo de guía es que las mismas sean específicas de un producto o de una solución, tanto de software como de hardware, dentro de estas se encuentran la guía de diseño de la compañía Netigy [27] y documentos de Cisco [9]. Para obtener esta guía se tomaron ideas de varias de ellas aunque la concepción no es similar pues esta no se ajusta ni recomienda ningún fabricante.

La guía obtenida constituye una orientación general que deja espacio a decisiones aunque se pretende siempre recomendar qué parámetro o elemento seleccionar.

Para la correcta aplicación de estas guías de implementación de Redes Privadas Virtuales, se requiere culminar una serie de etapas de análisis, diseño e implementación. [5]

Para conformar esta guía de pasos para ser utilizada en la implementación de una Red Privada Virtual soportada en Intranet se dividió la misma en tres etapas. La primera de estas etapas contiene un análisis de la situación que amerita la aplicación de esta tecnología, la definición de las características de la red a implementar así como las necesidades técnicas y organizativas. Una segunda etapa se encarga de definir el diseño de la red y los protocolos, mecanismos y configuraciones a implementar así como sus parámetros. La tercera etapa abarca la implementación y puesta a punto de la red.

3.1.1 Guía de implementación de Redes Privadas Virtuales en intranets

Etapa 1: Evaluación de necesidades

Paso 1- Evaluar la necesidad de implementación de la VPN.
Evaluar el problema a solucionar así como los servicios que se necesitan brindar y los niveles de seguridad que se requieren. Se considera necesario además realizar comparaciones, en cuanto a los aspectos mencionados anteriormente añadiendo el factor costo de implementación para comparar con otras variantes como enlaces conmutados o alquilados.

Paso 2- Definir clases de accesos que deben garantizarse
De acuerdo a las necesidades según las cuales se decide implementar una VPN en la intranet, pueden definirse tres tipos de conexión externas a la misma.

- Acceso remoto a la VPN mediante la línea telefónica conmutada o arrendada
- Acceso a la VPN desde la intranet "pública" que la soportará.
- Acceso desde otra VPN

Paso 3- Elegir si la VPN se implementa basada en software o en hardware

En una VPN a implementarse por software debe garantizarse compatibilidad entre el software cliente y el servidor, las facilidades de instalación de los software así como estandarizar las configuraciones para lo distintos accesos.

La VPN implementada por hardware ofrece mayor nivel de seguridad y rendimiento por lo que al tomar esta decisión el elemento principal a considerar es el económico, aunque también son muy importantes aspectos como compatibilidad entre los extremos en el caso de que la solución involucre hardware de varios fabricantes o integraciones de hardware o software. Por último también debe tenerse en cuenta la existencia de hardware en la red actual que pueda utilizarse para la VPN añadiéndole software específico.

Paso 4- Definir las necesidades técnicas (equipamiento, sistemas operativos de servidor y cliente, redundancia fuentes de alimentación).
Las necesidades de equipamiento para la implementación de una VPN y la redundancia requerida, los software a explotar así como la cantidad de usuarios dependen del tipo de VPN a implementar

Es necesario definir los niveles de redundancia que necesita la implementación a efectuarse, se debe considerar la redundancia para los dispositivos involucrados en forma

de duplicidad de componentes críticos (fuentes de alimentación, unidades centrales) o redundancia entre los enlaces, en esta decisión influirá el aspecto económico. Puede decidirse no incluir redundancia en el desarrollo inicial y hacerlo con posterioridad.

Paso 5- Garantizar la existencia de una política de seguridad

La existencia de una política de seguridad y su correcta aplicación es vital para garantizar los requerimientos de la seguridad en una VPN. En el caso de estar soportada por una intranet, la política de seguridad de esta contribuye a la seguridad y fiabilidad de la información en la VPN ya que existe la posibilidad de que usuarios de la intranet también lo sean de la VPN y en este caso es necesario minimizar los riesgos por ataques de virus, riesgos de operación o accesos sin autorización.

Etapa 2: Diseño

Paso 6- Esquematizar la topología de la red

Con el objetivo de colocar posteriormente los dispositivos VPN que se incorporarán es importante contar con un esquema de la red actual, especificando el hardware y el software que se utiliza hasta el momento.

Debe definirse además el tamaño de la VPN que se puede indicar como pequeña, mediana o grande. Para definir que tamaño tendrá la red que se implantará es necesario tener en cuenta la cantidad de usuarios que accederán por acceso remoto y la cantidad de sitios que se conectarán.

	Pequeña	Mediana	Grande
# de accesos simultáneos	hasta 50	hasta 500	más de 500
# de sitios remotos	hasta 20	entre 100 y 200	más de 200
Niveles de seguridad	altos	altos	altos

Tabla 2 Elementos para acotar el tamaño de la red

Paso 7- Definir el protocolo de encapsulamiento a utilizar.

Teniendo en cuenta la posibilidad de implementar los protocolos PPTP, L2TP e IPSec de acuerdo con las características de configuración y niveles de seguridad que proveen, se define el protocolo a utilizar en cada conexión.

PPTP: Protocolo de túnel que encapsula tramas PPP que a su vez encapsula datagramas de cualquier protocolo de red en datagramas IP y utiliza el cifrado MPPE.

L2TP: Protocolo estándar de túnel para Internet, encapsula tramas PPP que a su vez encapsula otros protocolos y utiliza IPSec para los servicios de cifrado para añadir seguridad a la transmisión.

IPSec: Proporciona seguridad para todos los protocolos IP y de capa superior en el conjunto de protocolos TCP/IP, permitiendo proteger todas las aplicaciones y servicios que utilizan IP para el transporte de datos. Se combina con L2TP para realizar túneles aunque puede realizarlos sin L2TP (IPSec modo túnel).

L2TP sobre IPSec: Es la combinación de estos protocolos para asegurar encapsulamiento y cifrado para los paquetes de cualquier protocolo que viajen por la red.

Parámetro	Valor recomendado
Encriptación de los datos	3DES
Integridad de los datos	SHA
Llaves de asociaciones de seguridad (SA)	Certificados Digitales
IKE	3DES
Diffie-Hellman	Grupo2 (1024 bits)
Modo	L2TP sobre IPSec

Tabla 3 Parámetro de IPSec [Kaufman, 1999]

Paso 8- Definir mecanismo de autenticación:

Para VPN IPSec hay dos métodos de autenticación: las llaves pre-compartidas (IKE) y los certificados digitales (PKI) por lo que debe escogerse entre uno de ellos.

La ventaja de usar las llaves pre-compartidas es que constituyen una manera relativamente fácil y barata pero no es muy escalable.

Por otra parte los certificados digitales son una opción más escalable para la autenticación del extremo de red pero requieren la implantación de una autoridad emisora de certificados o la compra de certificados a una tercera.

Servicios de autenticación externos deben ser empleados para la autenticación del usuario en un acceso remoto VPN. Esos servicios facilitan el desarrollo de un acceso remoto VPN y proporciona escalabilidad para que crezca el uso de la VPN dentro de la organización.

El uso de servicios de autenticación externos facilita el desarrollo permitiendo a la organización sincronizar las cuentas de usuarios con la autenticación del usuario VPN.

Se debe decidir entre:

- NT Domain Authentication
- RSA Escurrid
- LDAP
- RADIUS

Paso 9- Definir modo de asignación de direcciones IP a clientes

Se escoge entre:

1- Un servidor de DHCP existente: entre sus ventajas cuenta con la facilidad de configuración y de arrancada. La dirección IP del servidor de DHCP solo es necesario definirla en la pasarela VPN, la desventaja es que la información de responsabilidad es limitada y descentralizada y las trazas de los dispositivos de red incluirán la dirección IP de un cliente que sólo podrá resolverse analizando manualmente varias trazas (por ejemplo las trazas del servidor DHCP y las del fichero de trazas de la pasarela VPN).

2- Un rango de direcciones internas de la VPN: la ventaja de usar un rango de direcciones internas a la pasarela VPN es la relativa facilidad de configuración y el aumento de la limitación de responsabilidad. Como el rango de direcciones puede definirse fácilmente en la pasarela y ser distinto de aquellos definidos en el servidor DHCP, los eventos relacionados con el acceso remoto VPN pueden discernirse fácilmente de la actividad de la LAN simplemente por la dirección IP. La desventaja de este enfoque es la existencia de dos rangos de direcciones en dos dispositivos diferentes y la necesidad de revisar ambos ficheros de trazas para localizar la dirección IP de un usuario

3- Un servidor RADIUS: La ventaja de usar un servidor RADIUS para asignar direcciones estáticas a los usuarios VPN es que para localizar una dirección IP de un usuario no es necesario revisar varios ficheros de trazas. A cada usuario siempre se le asigna la misma dirección y localizarla se hace fácilmente analizando el servidor RADIUS. La desventaja está en la complejidad de configuración.

Etapa 3: Implementación

Paso 10- Análisis costo-beneficio

Después de realizar el análisis de los costos de brindar los servicios necesarios sin la VPN y los costos de instalación de la VPN, se debe realizar un análisis costos-beneficio así como de los nuevos servicios que se ofrecen para asegurar que ha sido correcta la elección de la tecnología en la solución del caso.

Paso 11- Implementación

La implementación depende de la solución escogida pues la configuración cambia según el software o hardware que se instale y los protocolos que se determine utilizar. Este implementación parte de la base de que los sistemas operativos y equipos están funcionando y que tienen configurados los elementos de red. Es en esta etapa donde se sigue los pasos de configuración y conexión del equipamiento específicos de cada solución.

3.2 Ejemplo de aplicación de la guía en el caso de las redes gerenciales de ETECSA.

Caso: Implementación de Red Privada Virtual en la Red de Gestión (GesNet) para ser soportada sobre la intranet de la Filial Territorial de ETECSA en Pinar del Río.

Etapa 1. Evaluación de necesidades

Paso 1- Evaluar la necesidad de implementación de la VPN.

En las condiciones actuales existe, en cada Filial de ETECSA en los territorios, una red gerencial y una red de gestión (GesNet), separadas físicamente debido a los requerimientos de seguridad de esta última que además de la supervisión de la técnica de

telecomunicaciones instalada se encarga de la operación y el mantenimiento de la misma, por lo que muchas de sus posiciones accionan sobre dicha técnica. La llamada red gerencial, cliente de CubaData, cuenta con un backbone FR a 128 kb/s y un backup X.25 a 64 kb/s que garantiza la conectividad con la WAN de ETECSA. Para garantizar la conexión nacional de la GesNet de los territorios se requerirá otro backbone con iguales características en cada territorio o la valoración de otras alternativas. Por otra parte, el personal vinculado a las actividades de supervisión y gestión no operativamente (personal administrativo) se encuentran en el compromiso de mantener su computadora en una u otra red, en un caso prescinden de la información de supervisión y gestión en tiempo real que se ha garantizado mediante aplicaciones en ambiente WEB y en otro caso prescinden de los servicios de la intranet que están implementados de forma tal que constituyen la principal herramienta para el intercambio de información dentro de la empresa.

Con el objetivo de garantizar accesos seguros de usuarios de la red gerencial a la información de gestión así como hacer un uso eficiente del backbone y el equipamiento instalado actualmente que permitirá la conexión de la GesNet del territorio con los Centros de Supervisión y Gestión Regional y Nacional, es que se considera proponer la implementación de una VPN en las GesNet siendo soportada sobre la intranet gerencial como una solución que permite la transmisión segura de datos.

Paso 2- Definir clases de accesos que deben garantizarse según las necesidades de acceso a la información

Necesidad	**Clase de acceso a garantizar**	**Seguridad requerida**	**Situación actual**
Acceso seguro a la información de gestión al personal autorizado no vinculado directamente con la supervisión u operación de la GesNet (personal administrativo)	Acceso a la información de la VPN (GesNet) desde la intranet Gerencial que la soportaría. Cliente - Servidor	Alta	No es posible
Acceso a la información de gestión al personal	Acceso remoto seguro a la	Alta	No es posible

autorizado de los centros telefónicos cuya técnica de telecomunicaciones se gestiona remotamente en el Centro de Supervisión y Gestión Territorial (GesNet).	información de la VPN (GesNet) mediante modems y enlaces conmutados o permanentes. Cliente - Servidor		
Acceso a la información de gestión de una GesNet territorial desde un Centro de Supervisión y Gestión Regional o Nacional	Acceso a la información de gestión territorial desde otras VPN. Servidor-Servidor (enrutador-enrutador)	Alta	No es posible

Tabla 4 Accesos necesarios a garantizar con la implementación de la VPN

Paso 3. Elegir el tipo de VPN a implementar

En el caso en cuestión valorando los requerimientos de seguridad y rendimiento de la VPN a implementar, teniendo en cuenta las posibilidades de administración del hardware (router) en las redes gerenciales y el aspecto económico se decide implementar la VPN por software. Se utilizarán las herramientas VPN que ofrece el Sistema Operativo Microsoft Window 2000 Advanced Server como servidor de VPN y Microsoft Window 2000 Professional como cliente VPN garantizando la compatibilidad entre cliente y servidor.

Paso 4. Definir las necesidades técnicas para la implementación.

Dado que se implementará una VPN por software las necesidades de equipamiento se minimizan identificándose las siguientes:

1- Computadora Pentium III o superior, 800MHz o más, 256 Mbyte de RAM. Fungirá como servidor de VPN que, aunque no tiene que ser específicamente para este propósito, es lo más aconsejable pues al priorizar las tareas como servidor de VPN

su rendimiento se ve seriamente afectado desde el punto de vista de otra aplicación que se ejecute.

2- Dos tarjetas de red (10/100 Mbps Fast Ethernet).
3- Tarjeta multipuerto y modems instalados en el servidor VPN.
4- Servicios telefónicos para el acceso conmutado
   (La cantidad de puertos, modems y servicios telefónicos necesarios en la implementación se definen en el paso 6)
5- Garantizar la conectividad del servidor de VPN hacia las dos redes, Red Gerencial y Red GesNet (VPN). 100 m Cable UTP categoría V, conectores RJ45, protectores de red.
6- Garantizar el funcionamiento óptimo del equipamiento activo actualmente instalado en las dos redes que será el utilizado para la implementación, en este caso dos switchs Horizon Modelo VH 2402S de 24 puertos (10/100) y router Cisco 3640.

La redundancia a implementar en este caso comprende la duplicidad de fuentes de alimentación implementada en el local de servidores de GesNet y la que se implementará en relación con el sistema operativo (Discos espejos, clones de particiones u otros).

Paso 5. Garantizar la existencia de una política de seguridad

Desde el momento en que usuarios de la intranet u otras VPN tendrán acceso a la VPN de la GesNet territorial resulta imprescindible el cumplimiento de las medidas de seguridad contempladas en el Plan de Seguridad Informática (confeccionado en cada entidad de ETECSA de acuerdo con sus particularidades) y en los reglamentos para el uso de las redes y sus recursos, debiendo cubrirse como riesgos principales aquellos que pueden tener lugar por ataque de virus, errores de operación por parte del usuario e incorrecto manejo de la política de complejidad e individualidad de nombres de usuarios y contraseñas.

Etapa 2: Diseño

Paso 6. Esquematizar la red

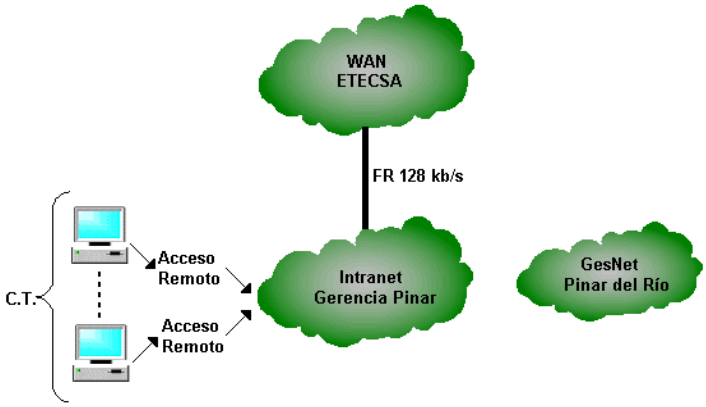

Fig. 3.1 Esquema de la red actual (sin VPN)

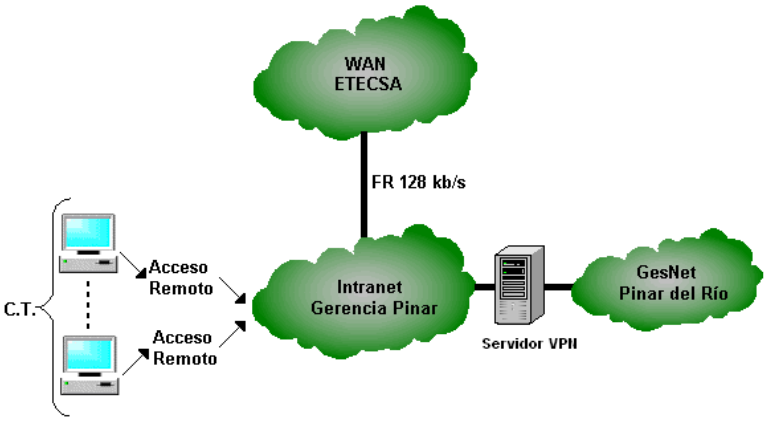

Fig. 3.2 Esquema de la red después de la implementación de la VPN

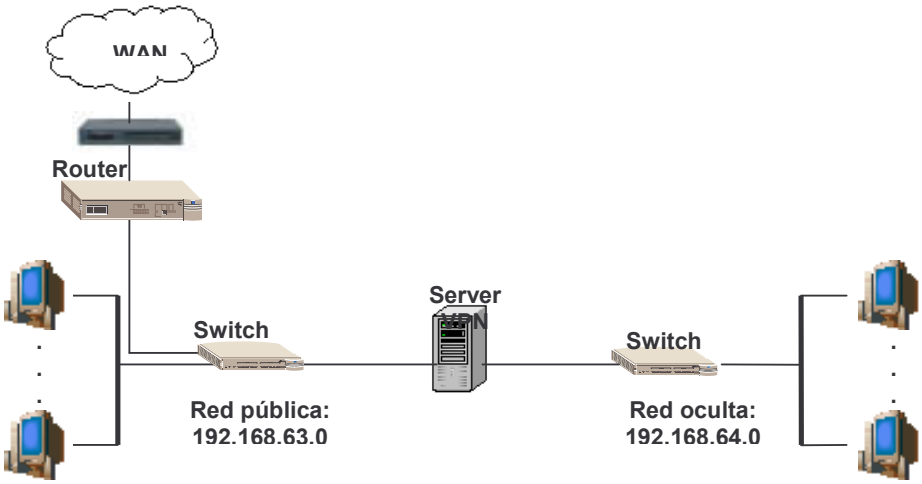

Fig. 3.3 Conexión de dispositivos después de la implementación de la VPN

El único cambio de hardware estará relacionado con la inclusión de la computadora que funcionará como servidor VPN y que estará conectada a las dos redes.

La red que se implementará estará dimensionada para soportar hasta 16 accesos remotos (8 accesos simultáneos), no más de 3 conexiones de Redes Privadas Virtuales remotas y 20 accesos desde la Intranet (todos con niveles altos de seguridad) por lo que clasifica como una red pequeña

Por tanto se necesitarán:

- Una tarjeta multipuerto de 8 puertos
- 8 modems instalados al servidor de VPN
- 8 servicios telefónicos

Paso 7- Definir el protocolo de encapsulamiento a utilizar.

Se utilizará la combinación de protocolos L2TP sobre IPSec para garantizar empaquetamiento y cifrado en la transmisión de los paquetes de datos.

Parámetros de IPSec.

Parámetro	Valor configurado
Encriptación de los datos	DES de 56 bits
Integridad de los datos	SHA-1
Llaves de asociaciones de seguridad (SA)	Certificados Digitales
IKE	DES de 56 bits
Diffie-Hellman	Grupo 2 (1024 bits)
Modo	L2TP sobre IPSec

Paso 8- Definir mecanismo de autenticación.

Al implementar L2TP sobre IPSec se determina utilizar como mecanismo de autenticación Certificados Digitales para lo cual se configurará una entidad emisora de certificados en el servidor de VPN. [Ver Anexo 3]

El servicio de autenticación externo que se usará será el NT Domain Authentication, el servidor de VPN se configurará como controlador de Dominio y contará con Directorio Activo.

Paso 9: Definir modo de asignación de direcciones IP a clientes

El modo de asignación de direcciones a implementar será la definición de un rango de direcciones internas a la pasarela VPN que se configura a la par que se configura el servidor de VPN para diferenciar los accesos por VPN de cualquier otro acceso que se implemente. [Ver Anexo 2]

Etapa 3: Implementación

Paso 10: Análisis costo-beneficio

Realizando una comparación entre la posible satisfacción de las necesidades según las condiciones actuales y una vez implementada la VPN:

Según condiciones actuales:

- No está implementada ninguna variante que permita el acceso a la GesNet por lo cual no existe una valoración económica pero tiene implicaciones negativas en el flujo de la información dentro de la empresa.
- Si se implementa un nuevo backbone para garantizar la gestión regional y nacional se necesitaría:

Concepto	**Costo**
Hardware	
- Router Cisco 3600	1699.00
- Modems FR	1417.50
- Redundancia . Modems Crocus . Interfaces V.35	 ~237.95 80.00
Puerta Nodo TX Datos CubaDATA	800.00 (600 + 200 del CIR 128)
Gastos de Instalación	1000.00
Total	4434.45 (Cada GesNet territorial,

	en total serian 19, por tanto 66516.75)

Implementando una VPN:

- Se garantizan los accesos a la GesNet para lo cual no existe una valoración económica pero tendrá implicaciones positivas en el flujo de la información dentro de la empresa.
- Si se implementa una VPN en la GesNet:

Concepto	**Observaciones**	**Costo (USD)**
Hardware		
- Computadora	P4 2.66GHz 256MB RAM HD 80GB	~ 700.00
- Tarjetas de Red	2 Tarjetas	~ 30.00
- Tarjeta Multipuerto RS232 (8 puertos)	1	~ 95.00
- Modems	8 Modems	~ 1200
Gastos de Conexión		~ 50.00
Autoridad de Certificado “CA” (si se decidió comprarla)	En esta implementación no se comprará sino que se configura una entidad emisora de certificados.	-
Contratar dirección IP real (si es necesario)	No es necesaria la contratación de una IP real	-
Gastos de Instalación		-
Total		2075 (Cada VPN, en

		total serian 15, por tanto 31125)

Se observa que la alternativa más atrayente desde el punto de vista económico es la implementación de la Red Privada Virtual. La cifra aproximada de implementación en todas las gerencias sería $31125, lo que representa un ahorro de $35391 si se comparan estas dos alternativas.

Paso 11: Implementación

En la computadora que realizará las funciones de servidor VPN:

1. Instalar el Sistema Operativo Windows 2000 Advanced Server y Directorio Activo (dominio: vpn.pri.tel.etecsa.cu). Crear usuarios en este dominio con permiso de acceso remoto que serían aquellos que accederían remotamente a la VPN
2. Configurar de las dos interfaces de red: para la red oculta (VPN, GesNet) y para la red pública (red gerencial).

   Detalles:

   Red Pública (Red ETECSA Gerencia Pinar del Río)

   - Red: 192.168.63.0
   - Dirección IP de la interfaz de red para la red pública: 192.168.63.30
   - Gateway: 192.168.63.1

   Red oculta (Red GesNet)

   - Red: 192.168.64.0
   - Dirección IP de la interfaz de red para la red oculta: 192.168.64.40
   - No se especifíca Gateway

   [Ver Anexo 1]
3. Instalar y configurar la tarjeta multipuerto (8 puertos) y modems.
4. Habilitar y configurar el Servicio de enrutamiento y acceso remoto del Sistema Operativo Windows 2000 Advanced Server.

   - Configurar el servidor como Servidor de VPN [Ver Anexo 2, figura 2]
   - Verificar los protocolos requeridos en este servidor para los clientes VPN. En este caso TCP/IP [Ver Anexo 2, figura 3]
   - Seleccionar cual de las dos interfaces se utilizará para acceder a VPN remotamente, desde la Intranet que la soporta o desde otra VPN: Se selecciona la interfaz de red pública. [Ver Anexo 2, figura 4]

- Seleccionar el método de asignación de direcciones IP a los clientes remotos. Para esta implementación se determina utilizar un rango de direcciones internas de la VPN. Rango: Dirección IP de inicio - 192.168.64.45
  Dirección IP final - 192.168.64.84
  Número total - 40 [Ver Anexo 2, figuras 5 y 6]
- Configurar puertos para permitir hasta 8 conexiones por acceso conmutado y 20 accesos desde la Intranet utilizando como protocolo de encapsulamiento el L2TP. [Ver Anexo 2, figura 7] (En el anexo solo se muestran 3 conexiones de acceso remoto y 3 puertos para que sea posible mostrar toda la ventana)
- Configurar las interfaces de conexión enrutador – enrutador para la conexión de hasta 3 Redes Privadas Virtuales remotas especificando que se utilizará como protocolo de encapsulamiento L2TP. [Ver Anexo 2, figuras 8 y 9]
- Configurar la ruta estática para cada conexión enrutador – enrutador. Cada conexión tendrá como credenciales el nombre de la cuanta de usuario autorizado en el servidor enrutador de la otra red oculta [Ver Anexo 2, figuras 10 y 11]

5. Instalar el servicio CA (Certification Authority, entidad emisora de certificados digitales) como componente del Sistema Operativo al ser el Certificado Digital el mecanismo de autenticación interno a emplear en esta implementación. Configurar este servidor como entidad emisora de certificados digitales. [Ver Anexo 3, figura1]

En los equipos remotos ya sean para el acceso remoto de clientes o el servidor enrutador de otra VPN:

6. Obtener en cada equipo que se conectará a la VPN el certificado digital desde la entidad configurada en el paso anterior mediante el ***Microsoft*** Certificate Services, especificando el Grupo DH (grupo 2, 1024 bits), y utilizar para la integridad de datos el algoritmo de autenticación SHA-1. [Ver Anexo 4] o mediante la Consola de Administración de Miscrosoft (MMC, Microsoft Management Console).
7. Configurar los acceso en los equipos ya certificados para la conexión a la VPN desde la Intranet. Probar la conexión [Ver Anexo 5]
8. Configurar los acceso remotos en los equipos clientes ya certificados para la conexión a la VPN por modem con las características del paso 7
9. Configurar los acceso de VPN remotas (conexión enrutador – enrutador) en el servidor VPN de la otra red. Desde la consola del servicio Enrutamiento y acceso

remoto se configuran las interfaces ya creadas durante la configuración del servicio [Ver Anexo 2, figura 9]

10. Pruebas de conexión [Ver Anexo 6]
11. Pruebas de captura de paquetes haciendo uso de la herramienta Sniffer Ethereal – Network Protocol Analyzer Versión 0.10. Se capturan paquetes en una comunicación entre estaciones de trabajo conectadas mediante una red pública y paquetes en una comunicación establecida entre dos estaciones de trabajo conectadas mediante una Red Privada Virtual soportada sobre una red pública. [Ver Anexo 7]

Con la aplicación de esta guía se implementó experimentalmente la Red Privada Virtual GesNet sobre la Intranet gerencial alcanzándose los resultados esperados desde el punto de vista de conectividad [Ver Anexo 6] y de seguridad, en este aspecto en cuanto al acceso a la red se requiere de un equipo certificado y de una cuenta de usuario en la VPN y en cuanto a integridad de la información con la captura de paquetes, estos no pudieron ser decodificados no siendo posible alterar la integridad de la información ni violar su confidencialidad. [Ver Anexo 7]

3.3 Conclusiones del capítulo

Con la aplicación de la guía obtenida en el epígrafe 3.1.1, se diseñó una Red Privada Virtual que garantiza la seguridad en los accesos remotos de clientes y de otras Redes Privadas Virtuales remotas a las redes de gestión de la Filial Territorial de ETECSA en Pinar del Río.

Se implementó una Red Privada Virtual experimental asegurando todo el tráfico hacía y desde la red de gestión permitiendo evaluar el concepto de VPN, su funcionamiento y pruebas de conectividad y seguridad que arrojaron los resultados esperados.

La guía obtenida permitió realizar la implementación de una VPN de forma rápida y organizada debido a que proporcionó una secuencia de pasos que facilitó dicha tarea tanto desde el punto de vista técnico como logístico.

Valoración económica

La implementación de Redes Privadas Virtuales, que se propone en las intranets de las redes territoriales de ETECSA con el objetivo permitir accesos autorizados a la Red de Gestión garantizando los requerimientos de seguridad, resulta una alternativa factible desde el punto de vista económico si se tiene en cuenta que la alternativa actual comprende la implementación de un segundo backbone en cada Filial Territorial con la consecuente utilización de puertas en los nodos provinciales de CubaData y de equipamiento costoso, routers y modems.

Comparación de variantes:

Implementación de un backbone

Concepto	**Costo**
- Router Cisco 3600	1699.00
- Modems FR	1417.50
- Redundancia . Modems Crocus . Interfaces V.35	 ~237.95 80.00
Puerta Nodo TX Datos CubaDATA	800.00 (600 + 200 del CIR 128)
Gastos de Instalación	1000.00
Total	4434.45

En la tabla anterior se reflejan los costos de la alternativa actual en una de las Filiales Territoriales de ETECSA, por lo que esto se repetirá en cada una de las Filiales alcanzándose la cifra aproximada de $66516.75

En la siguiente tabla se establece el costo de implementación de la VPN en una Filial Territorial

Concepto	Observaciones	Costo (USD)
Hardware		
- Computadora	P4 2.66GHz 256MB RAM HD 80GB	~ 700.00
- Tarjetas de Red	2 Tarjetas	~ 30.00
- Tarjeta Multipuerto RS232 (8 puertos)	1	~ 95.00
- Modems	8 Modems	~ 1200
Gastos de Conexión		~ 50.00
Autoridad de Certificado “CA” (si se decidió comprarla)	En esta implementación no se comprará sino que se configura una entidad emisora de certificados.	-
Contratar dirección IP real (si es necesario)	No es necesaria la contratación de una IP real	-
Gastos de Instalación		-
Total		2075

La cifra aproximada de implementación en todas las gerencias sería $31125, lo que representa un ahorro de $35391 si se comparan estas dos alternativas.

Conclusiones

- Habiendo estudiado documentación relacionada con el tema VPN, se evaluó la factibilidad de implementar VPNs en ambiente de Intranet para hacer uso de las diferentes tecnologías de seguridad lo que permite concluir que con la implementación de elementos como protocolos de encapsulamiento, protocolo IPSec (algoritmos de encriptación, certificados digitales), sistemas de autenticación fuerte es posible minimizar los riesgos de seguridad en las comunicaciones inter-redes.
- Se obtuvo una guía de pasos para la implementación de VPN en intranets que cuenta con tres etapas: Evaluación de la necesidad de implementación de la VPN, Diseño e Implementación.
- Se realizaron pruebas del funcionamiento de la tecnología de VPN en la Filial Territorial de ETECSA en Pinar del Río, teniendo por objeto la Red Gerencial como red pública y la GesNet (Red del Centro de Supervisión y Gestión Territorial) como red oculta, así también se simuló la conexión de dos VPNs (simulando la conexión de la red de un Centro de Supervisión y Gestión Regional con la de uno Territrorial) haciendo uso de las herramientas que para ello brinda el sistema operativo Microsoft Windows 2000 Advanced Server y la conectividad de la WAN de ETECSA
- Con la aplicación de la guía obtenida en el caso que se planteó y las pruebas realizadas quedó elaborada la propuesta de implementación de esta tecnología para las condiciones actuales de las redes gerenciales y GesNet en ETECSA.

Recomendaciones

- Incluir en la guía que se propone una etapa de verificación, durante la cual se hagan monitoreos a la Red Privada Virtual y se ataque su seguridad haciendo uso de herramientas como sniffers.
- Realizar las pruebas correspondientes a la simulación que se llevó a cabo conectando dos Redes Privadas Virtuales, para ello debe involucrarse la red del Centro de Supervisión y Gestión Regional y la red del Centro Territorial de Pinar del Río, las cuales se conectarían haciendo uso del backbone de la WAN de ETECSA.
- Implementar en las redes de ETECSA la propuesta correspondiente al uso de la tecnología de Redes Privadas Virtuales, que serían soportadas por las intranets.
- Difundir y aplicar la guía obtenida en las intranets de instituciones que se interesen por aplicar esta tecnología.

Referencias Bibliográficas

[1] **A. Mustapha**, H. Rudy, V. Sven, V. Gert, J. Arnold *Fundamentos de una Arquitectura QoS escalable para los servicios VPN IP.* Revista de Telecomunicaciones de Alcatel. 2003.

[2] **A. Mustapha**, H. Rudy, T. Tri. *MPLS: Valor añadido para la interconexión*. Revista de Telecomunicaciones de Alcatel. 2003.

[3] **Barbera**, José. *MPLS: A backbone architecture for the Internet of de 21 st Century.* http://www.rediris.es/rediris/boletin/53/enfoque1.html . Julio⁄2002

[4] **Broderick**, Stuart, *Implementando VPN en la empresa,* http://www.symantec.com/región/mx/entreprisesecurity/content/expert/LAM_1564.htm . Agosto/2002

[5] **Brown**, Brian. *Best Practices For VPN Implementation*. Bussiness Communications Review. Marzo 2001. pp. 24-30

[6] **Caire**, Ramiro. *Introducción a las Redes Privadas Virtuales* http://www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html Julio/2003

[7] **Céspedes** Morales, Lisset. *Redes Privadas Virtuales*, presentación en la Maestría en Telemática. 4ta Edición.

[8] Cisco**, *Technology Brief Layer 2 Tunnel Protocol*** http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm **. Julio 2002**

[9] **Cisco**, *IPSec Virtual Private Networks in Depth*, http⁄⁄www.cisco.com Septiembre⁄2001

[10] **Diffie – Hellman**, W. Diffie, M. E. Hellman, *New Directions in Cryptography, IEEE Transactions on Information Theory*, Vol. 22, No. 6, Nov. 1976

[11] **E. Kaufman**, A. Newman, *Implementing IPSec*. John Wiley & Sons, 1999

[12] **Forrester Research.** http://www.forrester.com/vpn.html . Julio⁄2002

[13] **García Gil**, Julio. *"¿Es segura nuestra VPN?"*, Comunicaciones World, , http://www.idg.es/comunicaciones/pdf/Soluzio08.pdf Noviembre 2003

[14] **Generalitat** Valenciana, *Manual de instalación de certificados digitales en fichero.* http://www.pki.gva.es/html-descargas/manualfichero_c.pdf Abril/2003.

[15] **Harkins** D., Carrel D., RFC 2409, *The Internet Key Exchange (IKE),* November 1998

[16] **Hamzeh,** K.**,** Verthein, W. ***P****oint to Point Tunneling Protocol (PPTP) Technical Specification,* *http://infodeli.3com.com/infodeli/tools/remote/general/pptp/pptp.htm* Junio, 1996

[17] **H. Brett**, P. Olivier, G. Bernhard. *Seguridad de la arquitectura de redes IP*. Revista de Telecomunicaciones de Alcatel. 2001.

[18] **Housley**, R., Ford, W. Polk,T., & Solo, D., RFC 2459, *Internet Public Key Infrastructure,* 1998

[19] **Kent** S., Atkinson R., RFC 2402, *IP Authentication Header*, November 1998

[20] **Kent** S., Atkinson R., RFC 2406, *IP Encapsulating Security Payload (ESP),* November 1998.

[21] **Kerchoffs**, Auguste. *La cryptographie Militaire*. http://www.geocities.com/sgrmatrix/kerchoffs.html?Nav Diciembre/2003

[22] **Linux FreeSWAN,** *FreeSWAN Documentation,* Abril 2003

[23] **Maughan** D., Schertler M., Schneider M., Turner J., RFC 2408*, Internet Security Association and Key Management Protocol (ISAKMP*), Noviembre 1998.

[24] **Minasi**, Mark ; Anderson, Christa*, WINDOWS 2000 SERVER*, Julio 2000

[25] **Miró**, José E, *VPN,* Revista en línea Teknokultura, Vol 2 Agosto 2003 http://teknocultura.rrp.upr.edu/teknotopia/vpn.htm

[26] **Naganad,** Doraswamy, Harkins Dan, IPSec *The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Prentice Hall. 1999

[27] **Netigy**, *Virtual Private Networks (VPN) Desing Guide*. http://www.netigy.com Septiembre/2002

[28] **NSTL** , *VPN de Windows 2000: rendimiento empresarial con la flexibilidad de los servidores*, http://www.microsoft.com/latam/technet/articulos/200103/ art07/ default.asp Febrero/2000

[29] **Olavsrud**, Thor. *Digital Certificates,* http://www.internetnews.com/dev-news/article.php/10_721571 Abril, 2001

[30] **Ramos,** Roberto. *Solución a los problemas de seguridad y calidad*. http://www.iies.es/teleco Septiembre/2003

[31] **Reynolds**, J., Postel, J., RFC1700, *Assigned Numbers, STD 2, Request for Comments 1700*, Octubre 1994. Información adicional: http://www.iana.org/numbers.html

[32] SafeNet, Inc. of Baltimore, *Microsoft L2TP/IPSec VPN*, htt://www.safenet-inc.com Junio, 2002

[33] **Wexler,** Joanie. *Frame Relay And IP VPNs: Compete Or Coexist*? Bussines Communications Review. Julio 1999, pp 28-32 www.bcr.com Septiembre⁄2002

[34] **Winkelstein**, Dan. *ATM Security Case Study*, http://www.acsac.org/1999/papers/thu-c-0830-winkelstein.pdf Agosto, 2002

[35] **Tremp**, Max. *Suplemento Especial: Redes Privadas Virtuales*. Revista Red. www.red.com.mx . Julio⁄2003

[36] **XIAO** X., NI L.,*Internet QoS: A Big Picture*, IEEE Network Magazine, marzo1999

Glosario de Términos

Algoritmo Asimétrico	Algoritmo que requiere dos claves diferentes, una para encriptar y otra para desencriptar. Una llamada clave pública y la otra clave privada. Un ejemplo es un algoritmo RSA
Algoritmo de Clave Pública	Ver algoritmo asimétrico
Algoritmo Simétrico	Algoritmo de encripción que se caracteriza por usar la misma clave para encriptar y desencriptar. Ejemplo de este tipo de algoritmo son: DES e IDEA
Algoritmo de Hashing	Son algoritmos que permiten verificar la integridad de un mensaje. Dado un mensaje de tamaño arbitrario produce una salida de tamaño fijo. Ejemplo de este tipo de algoritmo: SHA, MD5
ATM (Asyncronous Transfer Protocol)	Protocolo de transmisión orientado a la conexión basada en celdas de longitud fija (paquetes) de 53 bytes (incluyendo la cabecera de 5 bytes).
BGP (Border Gateway Protocol)	Protocolo para el intercambio de información de ruteo entre gateways y hosts en una red
CHAP	Protocolo de autenticación de intercambio de señales de reconocimiento.
Criptografía	Rama de la ciencia que estudia las técnicas por las cuales dos entes pueden comunicarse a través de un canal inseguro de una forma segura
Datagarama	Modo de transporte de paquetes donde los paquetes de una misma comunicación se enrutan independientemente y pueden seguir diferentes rutas, por lo cual no hay garantía en la secuencia de entrega
Encriptación	Acto por el cual un mensaje es codificado para transformarse en un mensaje cifrado
Firewall	Filtro de seguridad entra la red interna de una compañía e Internet, evitando el acceso de intrusos.
GRE, Generic Routing	Protocolo de encapsulamiento, que puede encapsular una amplia

Encapsulation	variedad de tipos de protocolos dentro de túneles IP
ISDN (Integrated Service Digital Network)	Sistema en el cual los datos digitales son transmitidos a 128kbps en un par telefónico desde un usuario hasta un destino pasando por la central telefónica que manipula la señal analógica
LAN (Local Area Network)	Red que interconecta computadoras, terminales, servidores, impresoras y otros periféricos sobre distancias cortas
RADIUS (Remote Authenticatión Dial In User Service)	Protocolo que permite al servidor RAS hacer la autentificación de un usuario a través de un servidor de atenticación.
Mensaje	Cualquier información ya sea un archivo o una cadena de caracteres
Router	Dispositivo que maneja la conexión entre dos o más redes de computadoras identificando las direcciones alas que cada paquete va dirigido y enrutándolo
Texto cifrado	Mensaje encriptado
Texto Plano	Mensaje sin encriptar

Glosario de Términos

Algoritmo Asimétrico	Algoritmo que requiere dos claves diferentes, una para encriptar y otra para desencriptar. Una llamada clave pública y la otra clave privada. Un ejemplo es un algoritmo RSA
Algoritmo de Clave Pública	Ver algoritmo asimétrico
Algoritmo Simétrico	Algoritmo de encripción que se caracteriza por usar la misma clave para encriptar y desencriptar. Ejemplo de este tipo de algoritmo son: DES e IDEA
Algoritmo de Hashing	Son algoritmos que permiten verificar la integridad de un mensaje. Dado un mensaje de tamaño arbitrario produce una salida de tamaño fijo. Ejemplo de este tipo de algoritmo: SHA, MD5
ATM (Asyncronous Transfer Protocol)	Protocolo de transmisión orientado a la conexión basada en celdas de longitud fija (paquetes) de 53 bytes (incluyendo la cabecera de 5 bytes).
BGP (Border Gateway Protocol)	Protocolo para el intercambio de información de ruteo entre gateways y hosts en una red
CHAP	Protocolo de autenticación de intercambio de señales de reconocimiento.
Criptografía	Rama de la ciencia que estudia las técnicas por las cuales dos entes pueden comunicarse a través de un canal inseguro de una forma segura
Datagarama	Modo de transporte de paquetes donde los paquetes de una misma comunicación se enrutan independientemente y pueden seguir diferentes rutas, por lo cual no hay garantía en la secuencia de entrega
Encriptación	Acto por el cual un mensaje es codificado para transformarse en un mensaje cifrado
Firewall	Filtro de seguridad entra la red interna de una compañía e Internet, evitando el acceso de intrusos.

GRE, Generic Routing Encapsulation	Protocolo de encapsulamiento, que puede encapsular una amplia variedad de tipos de protocolos dentro de túneles IP
ISDN (Integrated Service Digital Network)	Sistema en el cual los datos digitales son transmitidos a 128kbps en un par telefónico desde un usuario hasta un destino pasando por la central telefónica que manipula la señal analógica
LAN (Local Area Network)	Red que interconecta computadoras, terminales, servidores, impresoras y otros periféricos sobre distancias cortas
RADIUS (Remote Authenticatión Dial In User Service)	Protocolo que permite al servidor RAS hacer la autentificación de un usuario a través de un servidor de atenticación.
Mensaje	Cualquier información ya sea un archivo o una cadena de caracteres
Router	Dispositivo que maneja la conexión entre dos o más redes de computadoras identificando las direcciones alas que cada paquete va dirigido y enrutándolo
Texto cifrado	Mensaje encriptado
Texto Plano	Mensaje sin encriptar

Anexo 1: Configuración de las interfaces de Red del Servidor VPN

- Configurando la interfaz de red para la conexión a la red pública se mantiene la configuración normal de esta red.

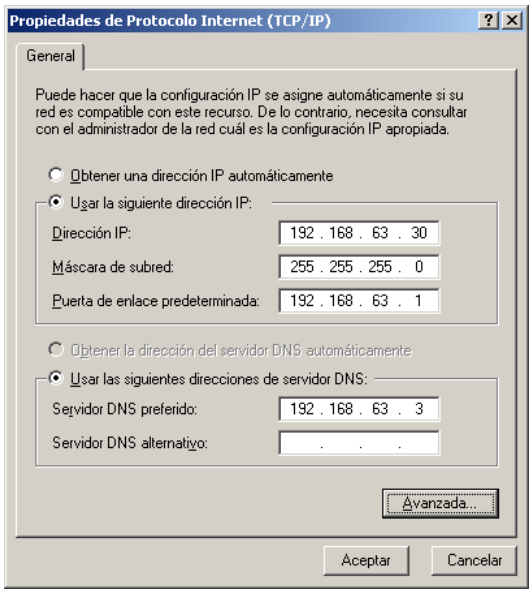

Figura 1. Configurando la interfaz de red para la conexión a la red pública

- Configurando la interfaz de red para la conexión a la red privada se configura según direcciones determinadas para esta red, no se configura Puerta de enlace y DNS en dependencia de si existe en dicha red o no.

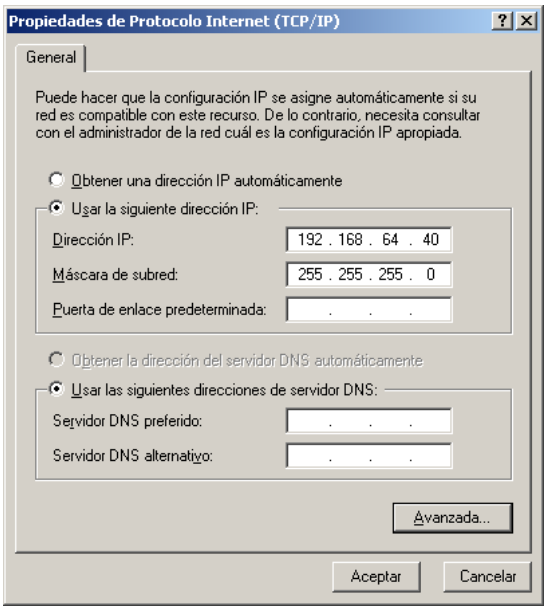

Figura 2. Configurando la interfaz de red para la conexión a la red oculta

Anexo 2: Configuración del Servicio de enrutamiento y acceso remoto

1- Ventana inicial.

Figura 1. Consola del servicio

2- Servidor VPN

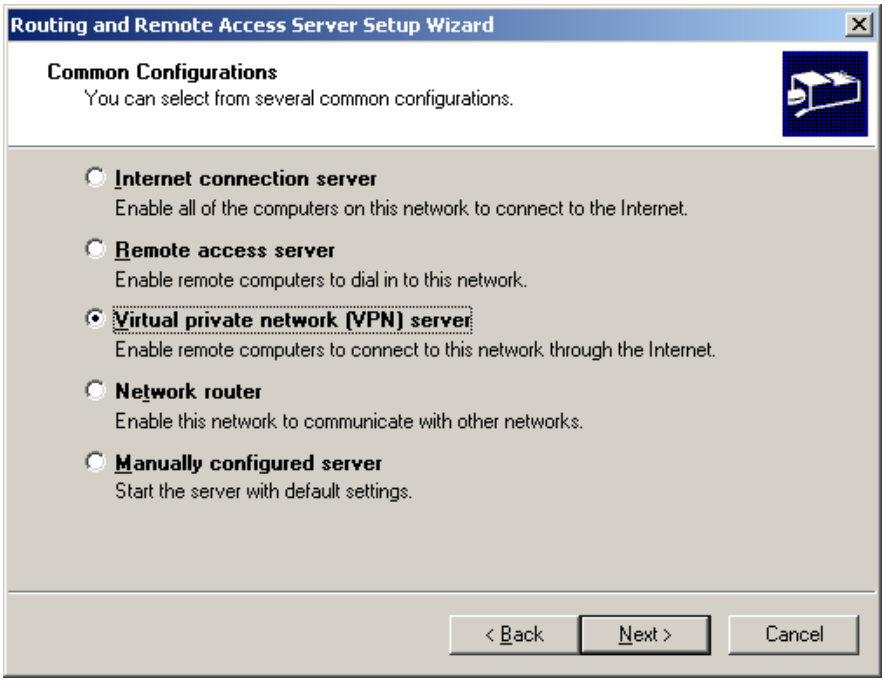

Figura 2. Servidor VPN

3- Verificar los protocolos requeridos en este servidor para los clientes VPN.

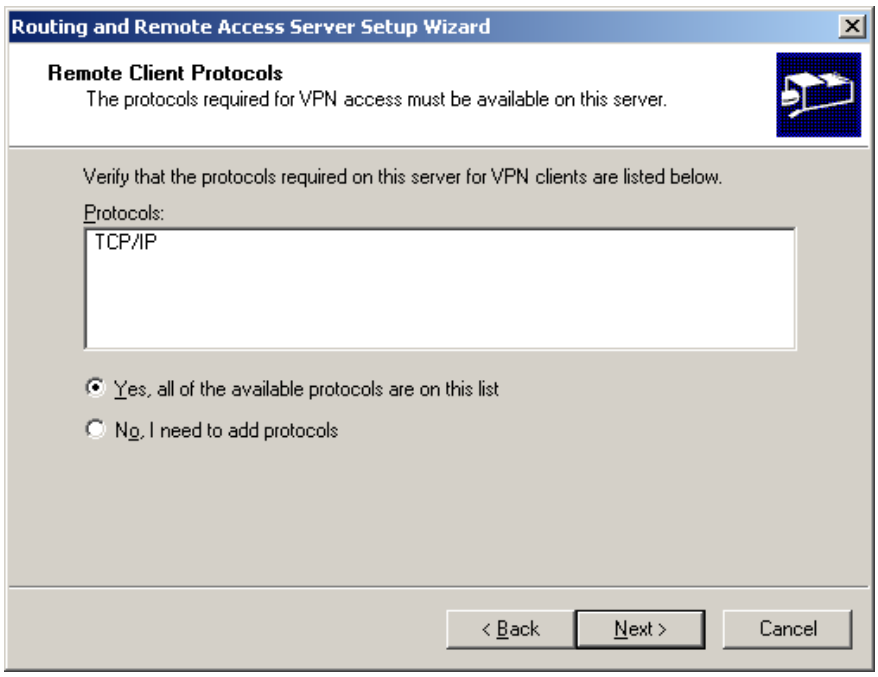

Figura 3. Protocolos del cliente remoto

4- Seleccionar la interfaz para acceder a la VPN remotamente, desde la Intranet que la soporta o desde otra VPN. Debe seleccionarse la interfaz de la red pública

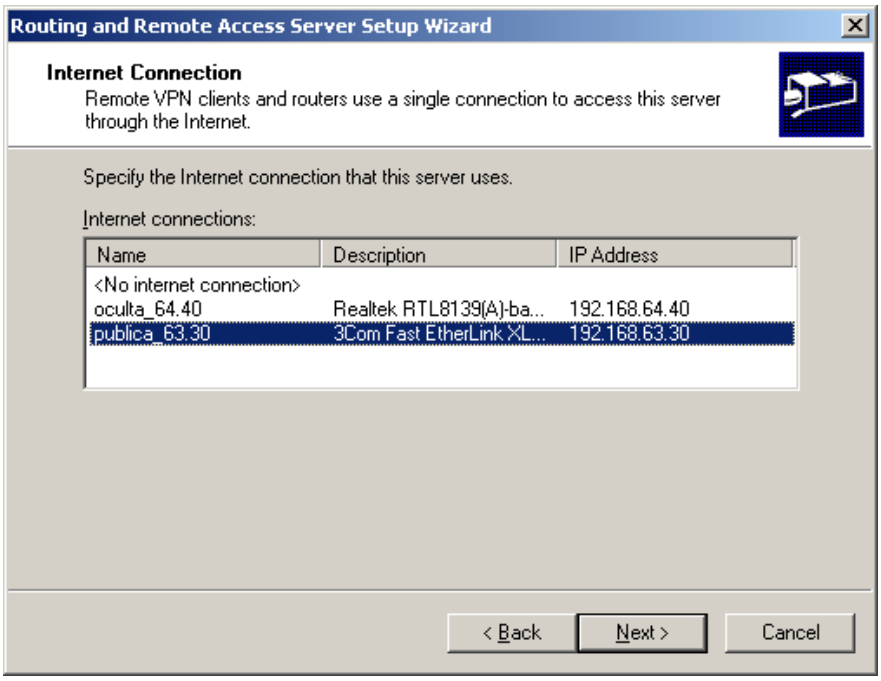

Figura 4. Interfaz para acceder a la VPN desde la red pública

5- Seleccionar el método de asignación de direcciones IP a los clientes remotos.

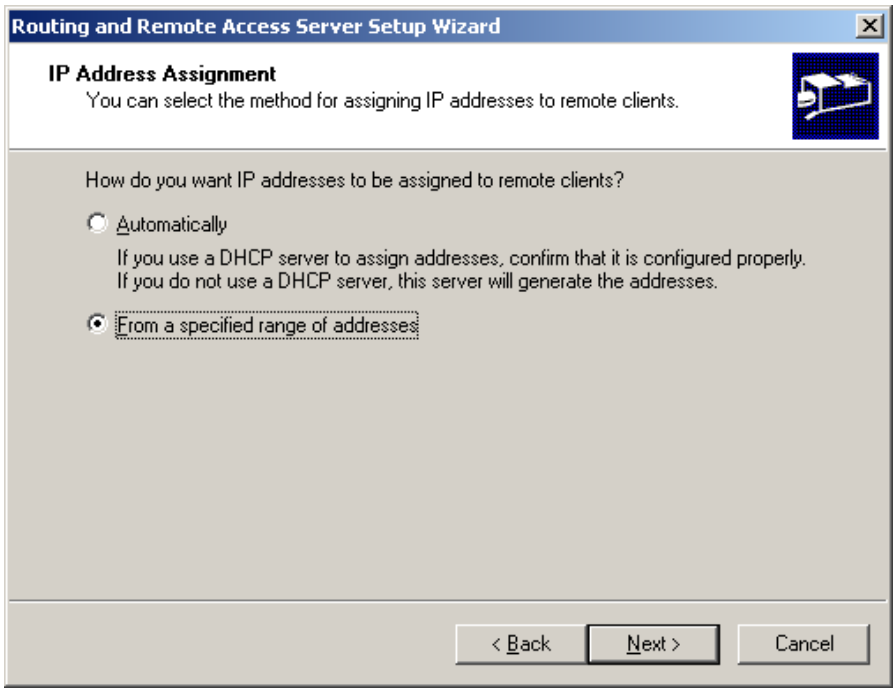

Figura 5. Asignación de direcciones

Rango: Para garantizar al menos 3 accesos desde otras VPNs, 8 accesos remotos simultáneos y hasta 20 accesos desde la Intranet que soporta la VPN.

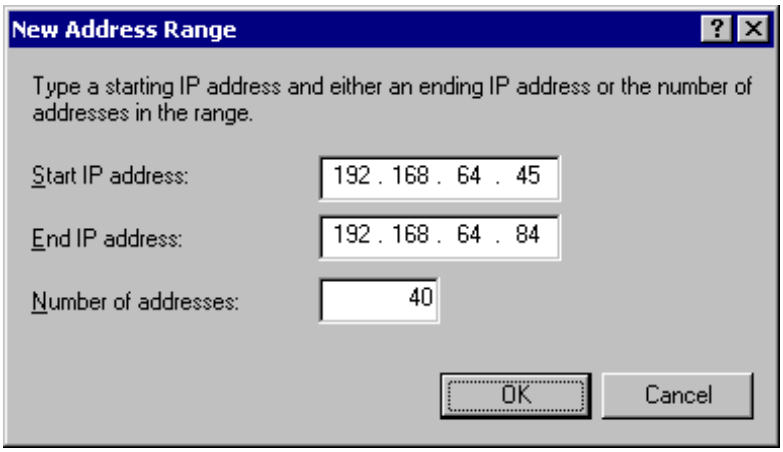

Figura 6. Rango de direcciones de la red oculta

6 - Configuración de puertos para accesos remotos y desde la Intranet que soporta la VPN.

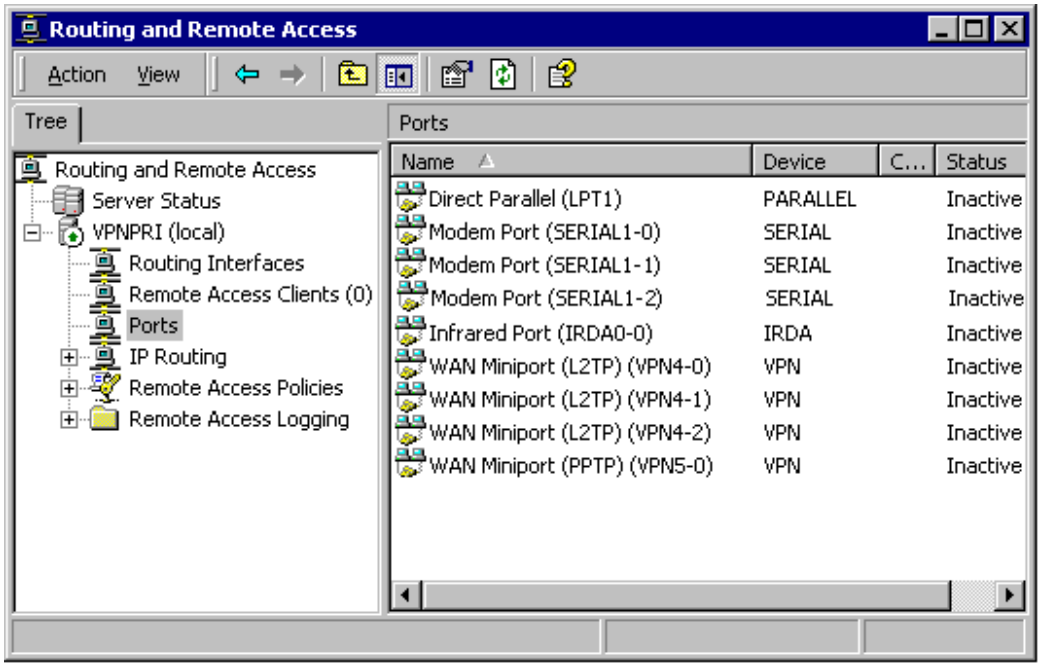

Figura 7. Vista de puertos

7- Configurar las interfaces para la conexión enrutador – enrutador. Selección del protocolo L2TP

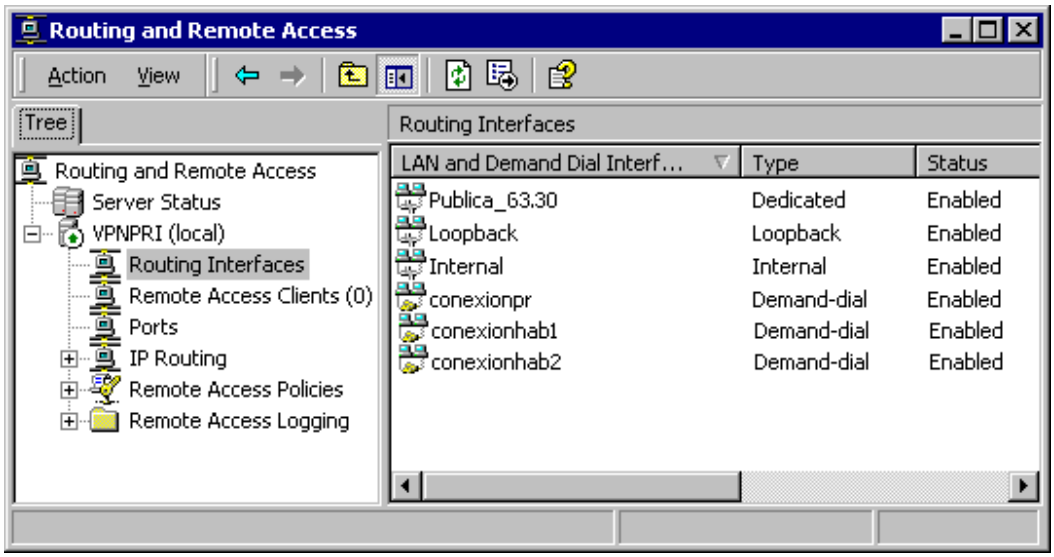

Figura 8. Interfaces

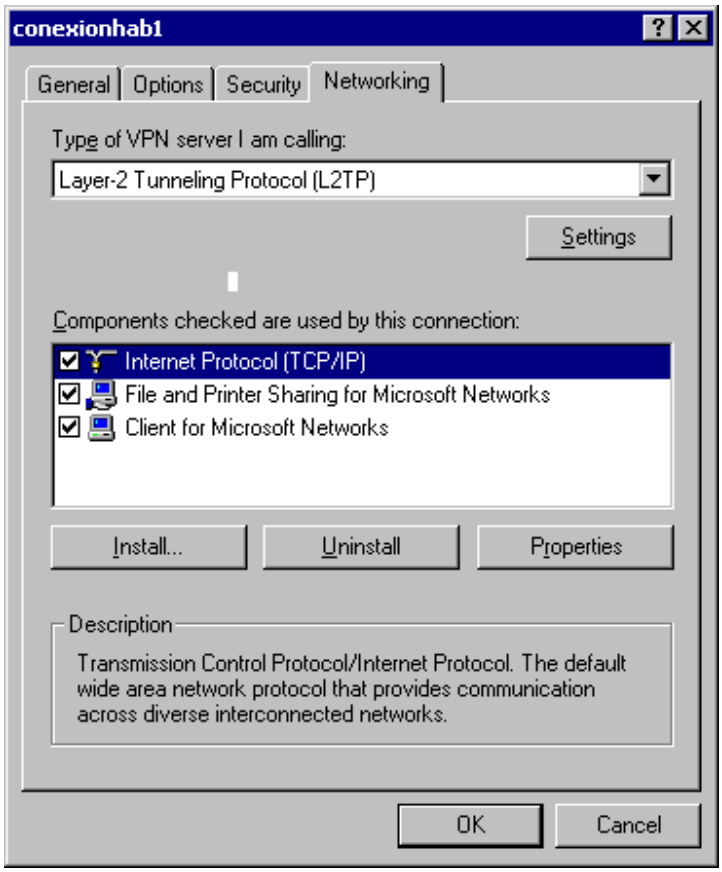

Figura 9. Tipo de servidor de VPN

8- Configurar la ruta estática para cada conexión enrutador – enrutador

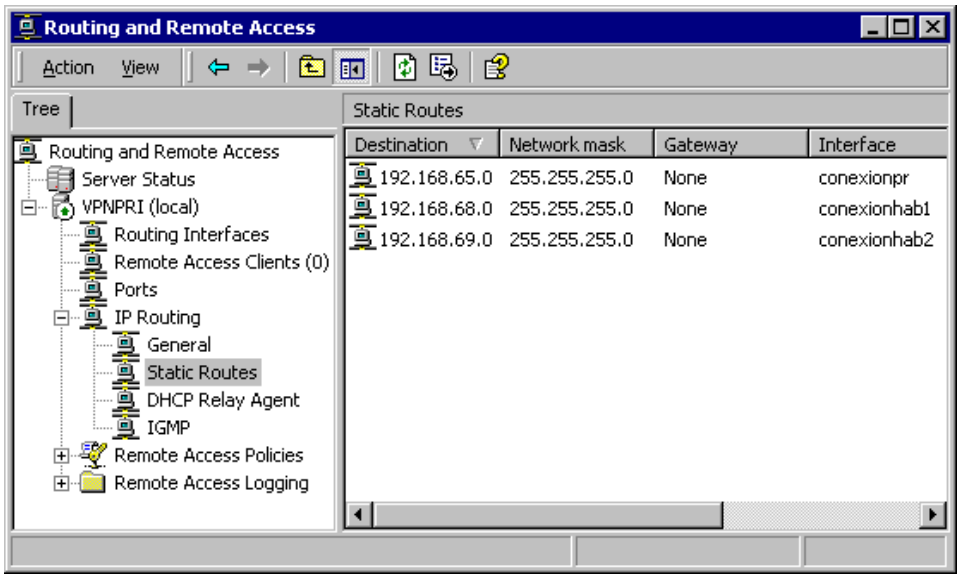

Figura 10. Rutas estáticas

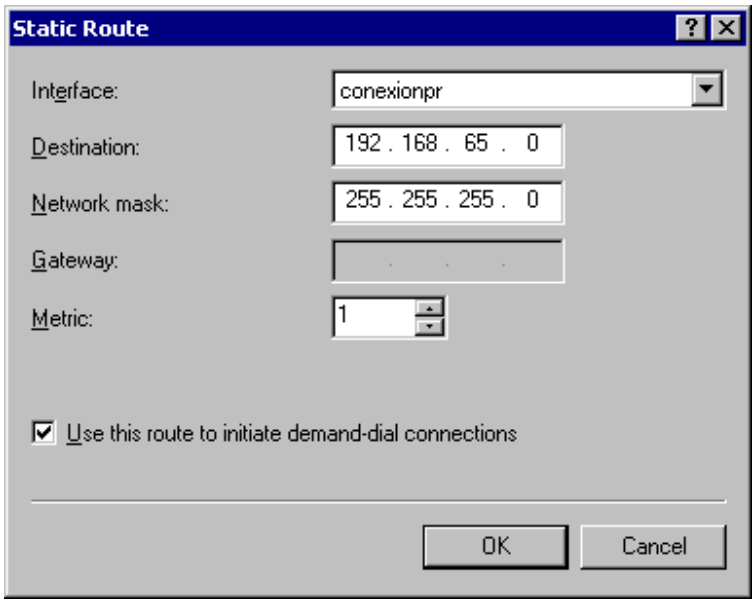
Static Route
Interface:
conexionpr
Destination:
192 . 168 . 65 . 0
Network mask:
255 . 255 . 255 . 0
Gateway:
Metric:
1
Use this route to initiate demand-dial connections
OK
Cancel

Figura 11

Anexo 3: Instalar CA

Este servicio se instala como componente del Sistema Operativo al ser el Certificado Digital el mecanismo de autenticación a emplear en esta implementación. Configurar este servidor como entidad emisora de certificados digitales.

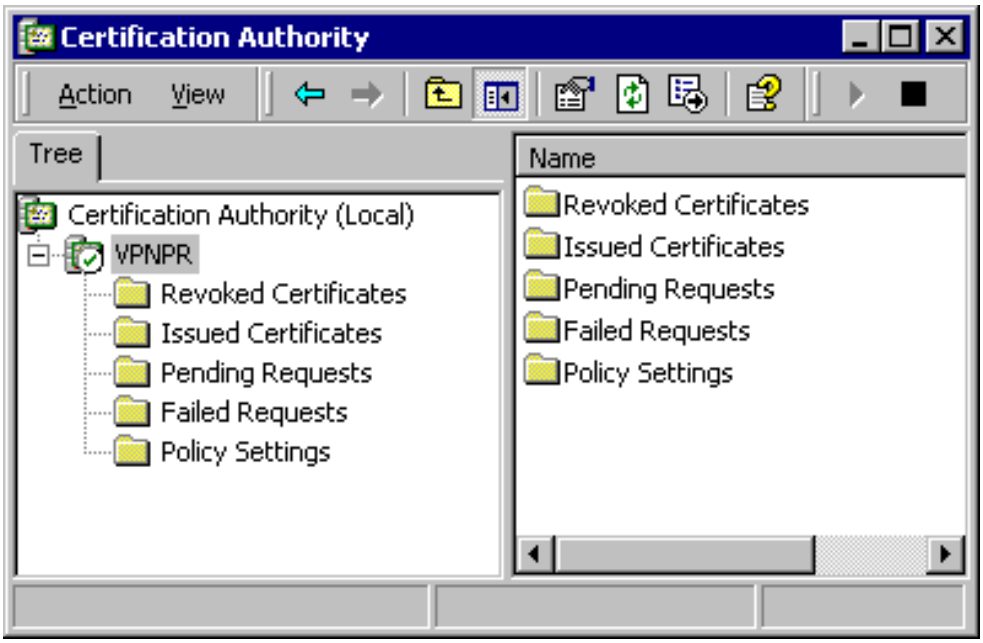

Figura 1

Anexo 4: Obtención del certificado digital en el equipo cliente

1- Solicitar un certificado a la entidad emisora VPNP

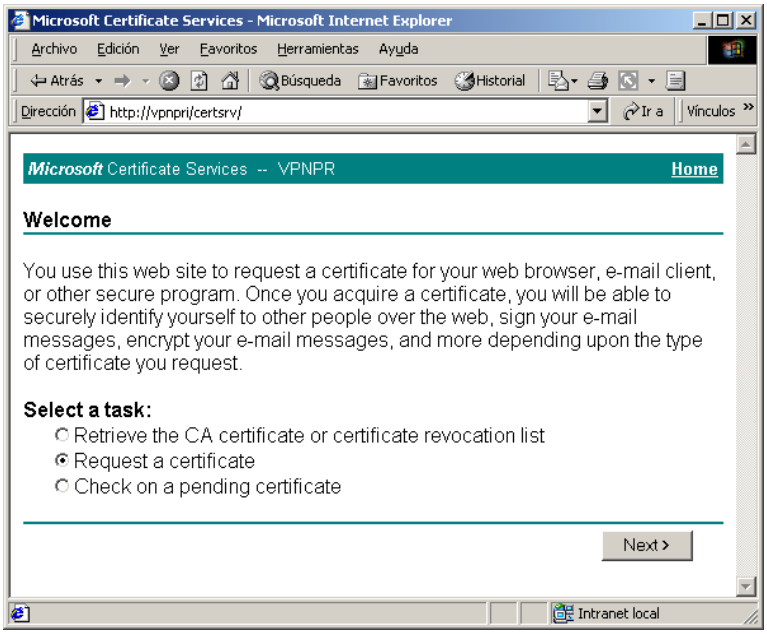

Figura 1. Sitio de la entidad emisora de certificados digitales

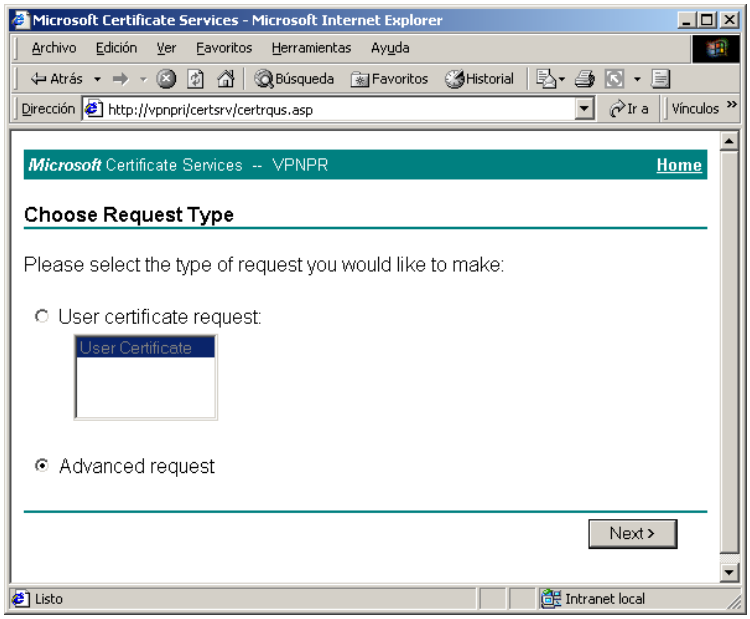

Figura 2.

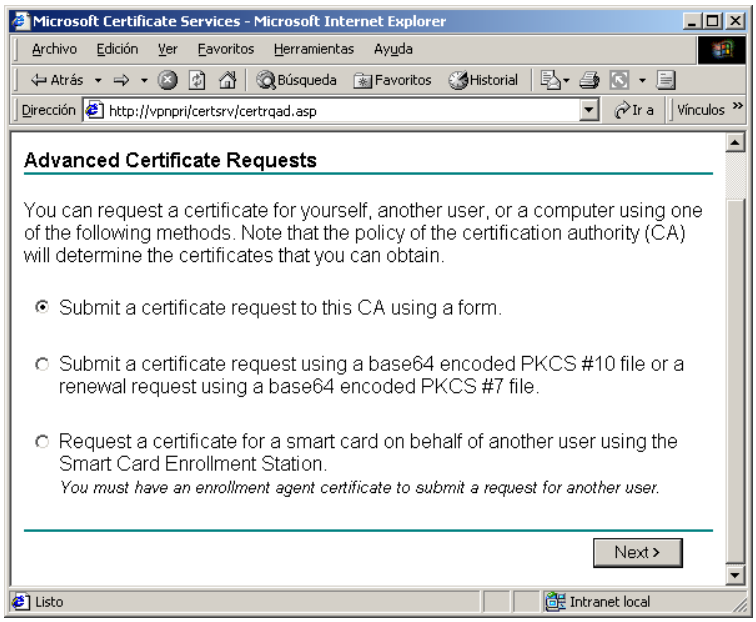

Figura 3.

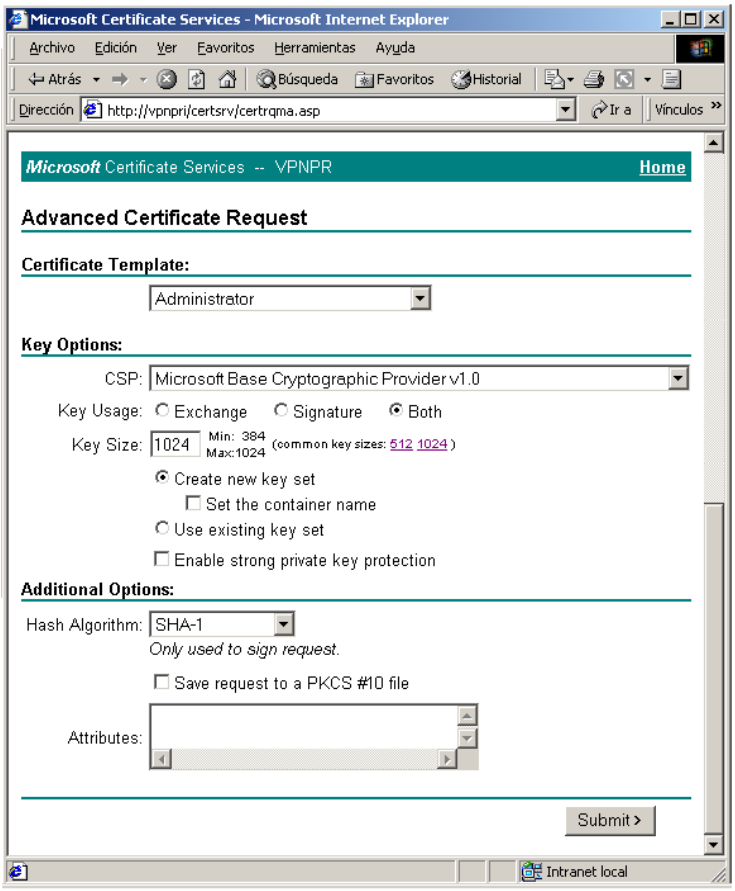

Figura 4.

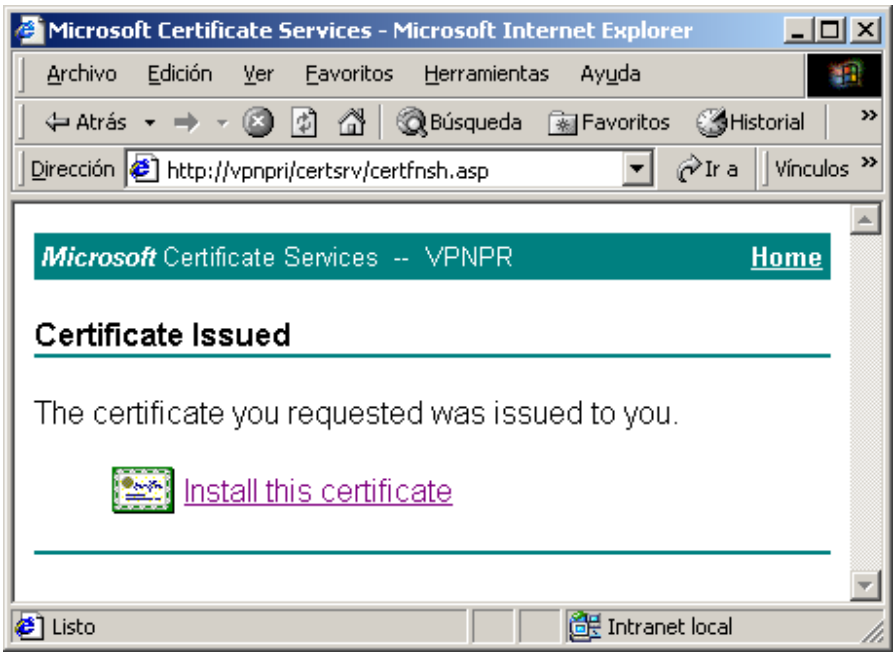

Figura 5.

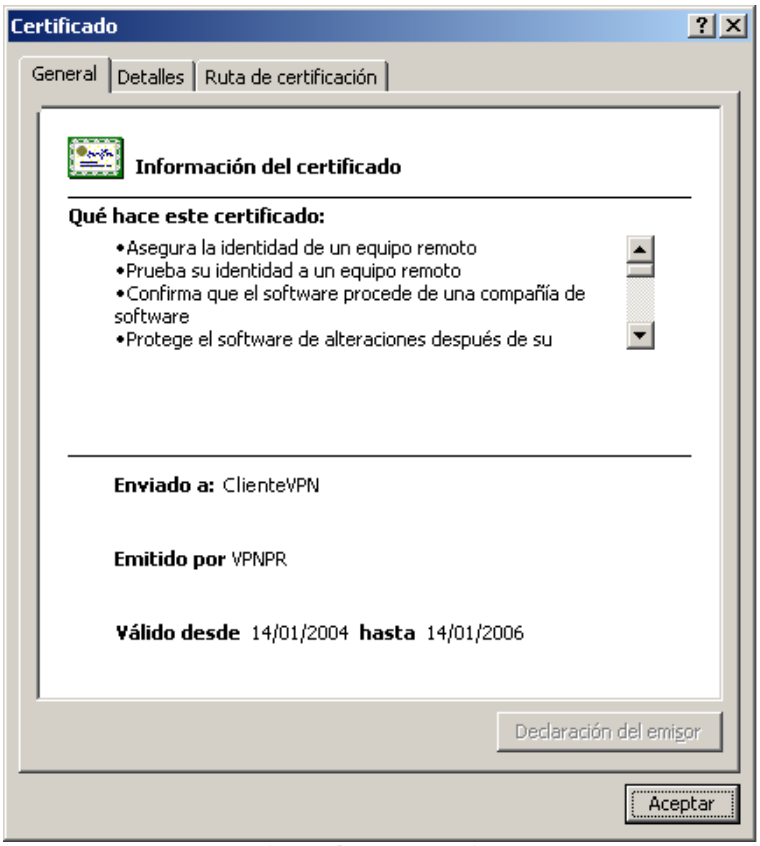

Figura 6. Verificación del certificado obtenido

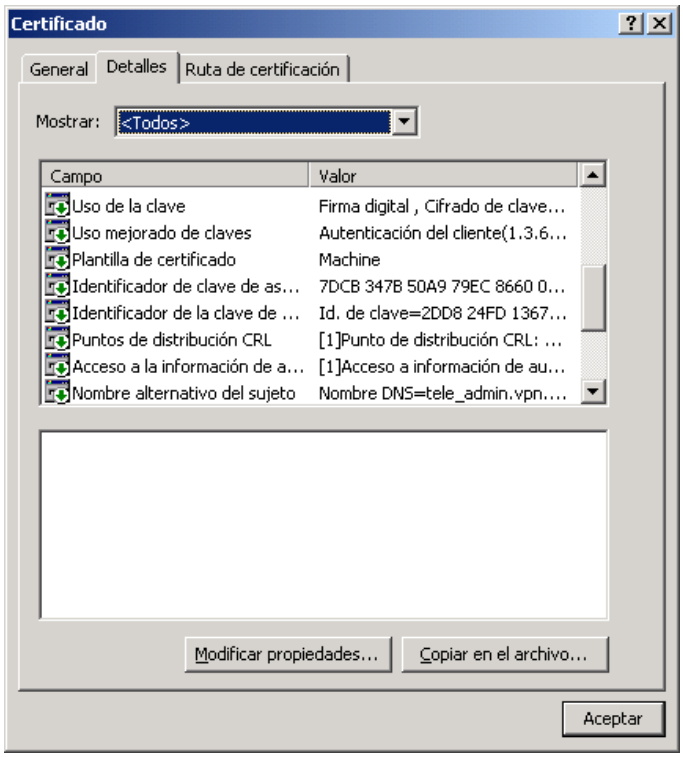

Figura 7. Detalles del Certificado obtenido

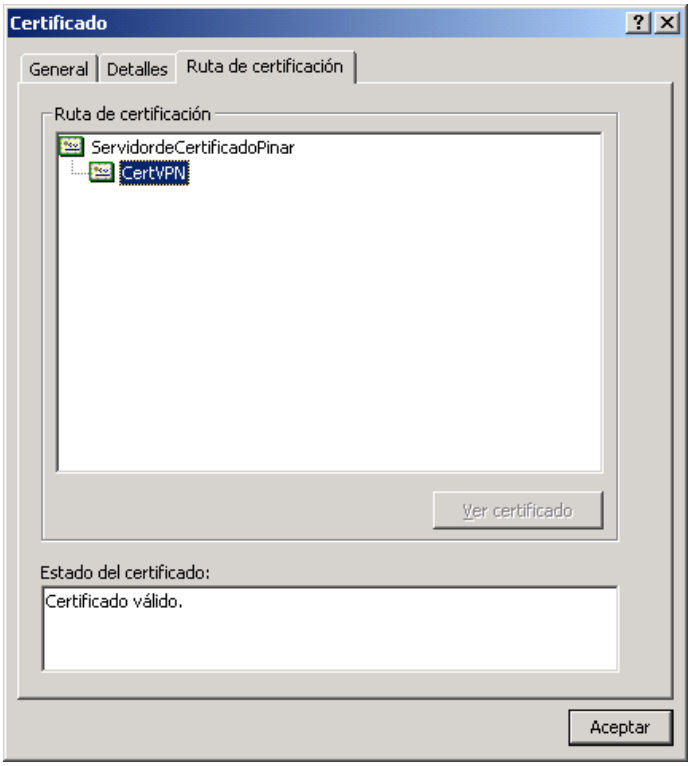

Figura 8. Ruta

Anexo 5: Configurar la conexión para el acceso a la VPN en los equipos clientes

Mediante el asistente para la configuración de conexiones:

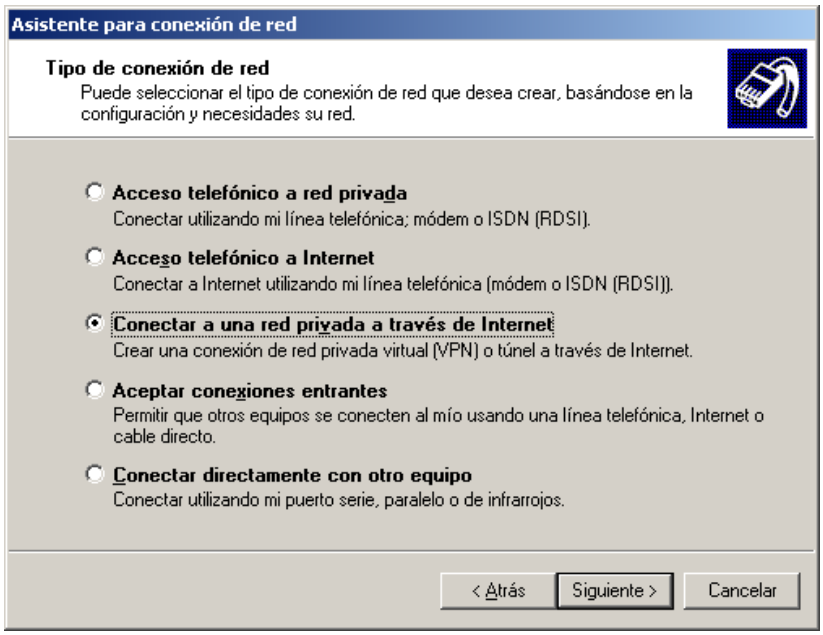

Figura 1. Seleccionar tipo de conexión

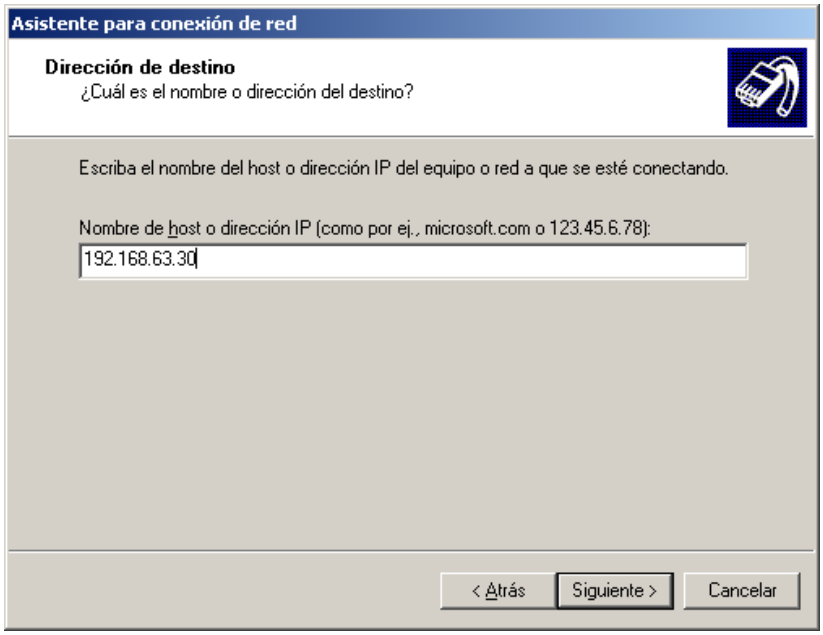

Figura 2. Dirección IP de la interfaz pública del servidor VPN

Figura 3. Autentificación para el acceso a la VPN

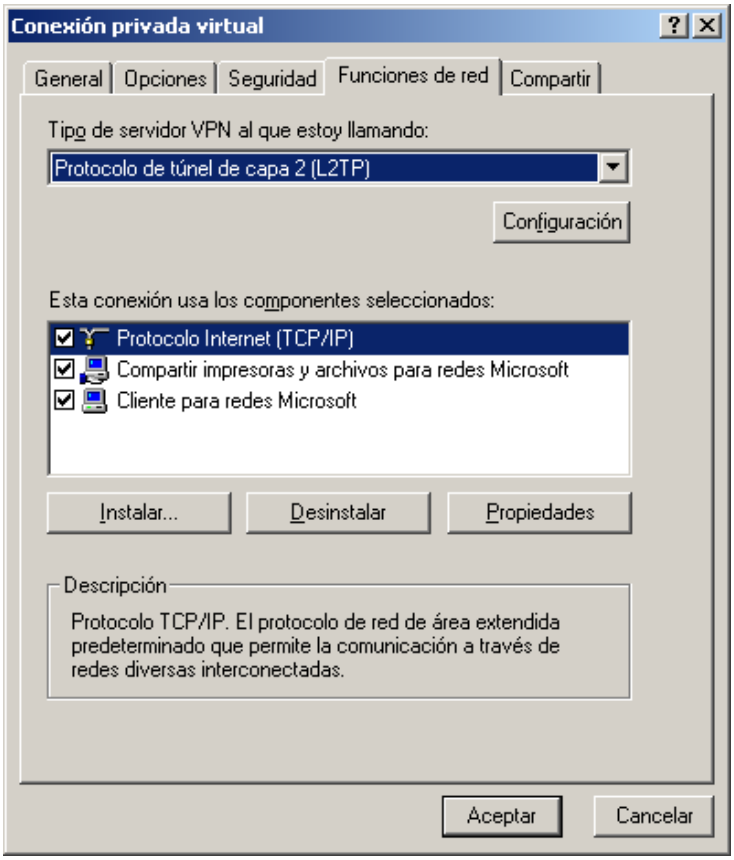

Figura 4. Propiedades de la conexión. Selección del protocolo L2TP/IPSec

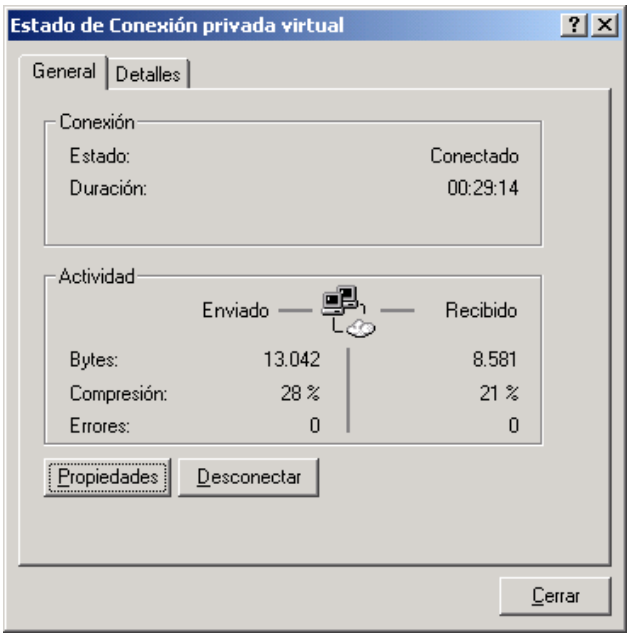

Figura 5. Conexión ya establecida

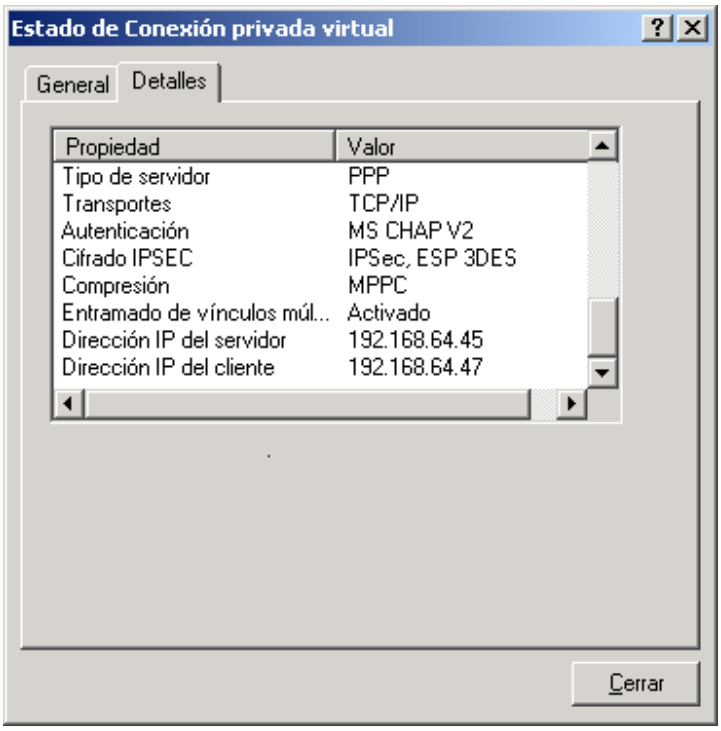

Figura 6. Detalles de la conexión. Protocolos usados