UNIVERSIDAD TÉCNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

ESPECIALIDAD INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

UNIVERSIDAD DE PINAR DEL RÍO

"Hermanos Saíz Montes de Oca"

Facultad de Informática y Telecomunicaciones
Departamento de Telecomunicaciones y Electrónica

PROYECTO DE DIPLOMA

Título: *Propuesta para la implementación de una Red Privada Virtual para el Instituto Superior Pedagógico en Pinar del Río*

(Proyecto de Diploma presentado en opción al título de Ingeniero en Sistemas)

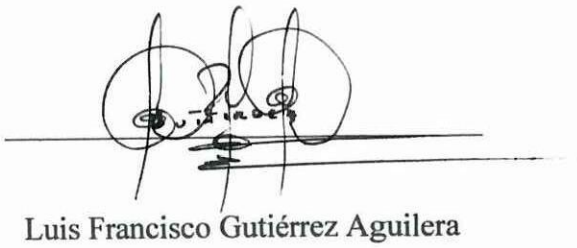
Autor: *Luis Francisco Gutiérrez Aguilera*

Tutores: *Ing. Abel Lorenzo*
Ing. Yoan Fustes
Ing. Michel Falcón Domínguez

Declaración

DECLARACIÓN DE AUTORIDAD.

Declaro que soy el autor de este Trabajo de Diploma y autorizo a la Universidad de Pinar del Río Hermanos Saíz Montes de Oca a hacer uso del mismo con la finalidad que estime conveniente.



Luis Francisco Gutiérrez Aguilera

Opinión del Tutor

OPINIÓN DE LOS TUTORES

El Estudiante Luis Francisco Gutiérrez Aguilera ha desarrollado y concluido satisfactoriamente este trabajo, en cuya realización ha puesto a prueba su laboriosidad, sacrificio y dedicación.

El desarrollo del mismo se caracterizó por:

- Alto rigor científico.
- Importante recopilación bibliográfica.
- Independencia del estudiante.
- Capacidad de integrar conocimientos.

Ha puesto de manifiesto su creatividad y capacidad para engranar todo el conocimiento adquirido, que hace demostrar que está listo para desempeñarse como profesional, capaz de asumir y llevar exitosamente hasta el final cualquier empresa. La investigación sobre las Redes Privadas Virtuales, un tema completamente nuevo para él y en cierta medida para muchos, pues en este centro solamente existe un proyecto de diploma anterior a este, y su implementación de seguro apoyará el aprendizaje del estudiantado en la Universidad de Pinar del Río y contribuirá a la formación de profesionales más integrales.

Ha sobrado también la calidad humana, con la que logramos crear un verdadero equipo de trabajo y donde la amistad y el respeto mutuo, jugaron un papel fundamental para lograr los objetivos propuestos.

Por las razones antes expuestas, la calidad técnica del trabajo y la magnífica edición consideramos que el diplomante es merecedor de la calificación de cinco puntos.

Ing. Yoan Fustez Pérez

Ing. Michel Falcón Domínguez

Ing. Abel Lorenzo Morera

Opinión del Opositor

UNIVERSIDAD DE PINAR DEL RÍO
"HERMANOS SAÍZ MONTES DE OCA"
FACULTAD DE INFORMÁTICA Y TELECOMUNICACIONES
DPTO. DE TELECOMUNICACIONES Y ELECTRÓNICA.
CALLE MARTÍ No. 270 FINAL. CP. 20100 PINAR DE RÍO, CUBA.
TELEF: (53) (82) 5453.
Email: dptotele@tele.upr.edu.cu

27 de Noviembre de 2004

A quien pueda interesar:

El proyecto de Diploma titulado "Propuesta para la implementación de una Red Privada Virtual para el Instituto Superior Pedagógico "Rafael María de Mendive" de Pinar del Río", del autor Luis Francisco Gutiérrez Aguilera, constituye una herramienta de gran ayuda para la comprensión de los contenidos relacionados con las VPN, y forma parte de una ayuda bibliográfica para todos aquellos interesados en adentrarse en el bello y amplio mundo de las redes de computadoras. Además, este Proyecto de Diploma contribuye a implementar una aplicación real en una institución educacional en nuestra provincia, permitiendo configurar una red para la transferencia confiable, segura y eficiente de datos importantes en dicho centro. Cabe además resaltar que la exposición del diplomante fue excelente, y se evidenció un profundo conocimiento de los temas abordados, igualmente fueron respondidas de forma clara y precisa las preguntas de la oponencia. Por lo anterior planteado, así como la calidad humana evidenciada en dicho diplomante para enfrentar los retos en el camino hacia su preparación, la oponencia decide proponer la calificación de 5 puntos .

Ing. Luis Ernesto García Concepción
Departamento de Telecomunicaciones y Electrónica
Facultad de Informática y Telecomunicaciones
Universidad de Pinar del Río, Cuba

Página de Aceptación

PÁGINA DE ACEPTACIÓN.

El proyecto de diploma constituye una herramienta de gran importancia para la comprensión del funcionamiento de las Redes privadas virtuales (VPN) e igualmente constituye una aplicación práctica de suma eficiencia para un centro educacional de nuestro país. Constituye además una herramienta bibliográfica para todos aquellos estudiantes o profesionales del ramo. Por todo lo anterior y atendiendo a los resultados se otorga la calificación de 5 ptos.

FACULTAD DE INFORMÁTICA Y TELECOMUNICACIÓN UPR
DECANATO
PINAR DEL RÍO

Presidente

Secretario

Vocal

Pensamiento

PENSAMIENTO

Vive tu vida como si subieras una montaña. De vez en cuando mira hacia tu alrededor y admira las cosas bellas en el camino. Sube despacio, firme y disfruta cada momento hasta llegar a la cumbre.

(Harold V. Melchert)

Dedicatoria

DEDICATORIA

Dedico este trabajo a mi madre y a mi hermana María del Carmen, que siempre han estado y están presentes en cualquier acto de mi vida, así como también a todas aquellas personas que de una forma u otra contribuyeron con la realización del mismo.

Agradecimiento

AGRADECIMIENTO

Un agradecimiento al pueblo Cubano y en particular a la Universidad Pinar del Río, por haberme abierto las puertas desde el inicio hasta la culminación de la presente investigación.

En especial a mis tutores quienes impulsaron este proyecto sobre las Redes Privadas Virtuales, con sus conocimientos aportaron de manera muy significativa dentro de todo el desarrollo de este proyecto.

Gracias a todas aquellas personas que de forma directa o indirecta han contribuido en el desarrollo del proyecto.

Resumen

RESUMEN

La tecnología de Redes Privadas Virtuales (VPN) proporciona un medio para usar una infraestructura pública de red, como Internet, para el transporte de datos privados, con el objetivo de brindar acceso remoto a usuarios a sus redes privadas cooperativas, o para brindar conexión a dos redes privadas distantes. Una pregunta surgiría entonces, ¿cómo proteger esos datos que viajan sobre la red pública? Para lograrlo, las VPN emplean tecnologías de encriptación y encapsulamiento, que aseguran la integridad de los datos. Las definiciones anteriores son válidas también en un ambiente Intranet, donde la red pública consistiría en un conjunto de subredes interconectadas de acceso libre, y las redes privadas, en subredes igual que las otras pero protegidas por una VPN. Esta investigación se enfoca en éste último ambiente brindando una propuesta de implementación de VPN para los departamentos del Instituto Superior Pedagógico que requieran proteger sus datos.

Summary

SUMMARY

The technology of Virtual Private Nets (VPN) provides a way to use a public infrastructure of net, as Internet, for to transport private data, with the aim to remote access to users to their cooperative private nets, or to connection for two distant private nets. A question come out, how to protect those data that travel above the public net? To achieve it, the VPN uses codify and save technologies to assure the data integrity. The previous definitions are valid also in an Intranet environment, where the public net would consist on a group of interconnected free subredes access, and the private nets, in subredes the same as the other ones but protected by a VPN. This research is focused in the last atmosphere offering an implementation proposal of VPN to the departments of the Pedagogic Superior Institute that require to protect its data.

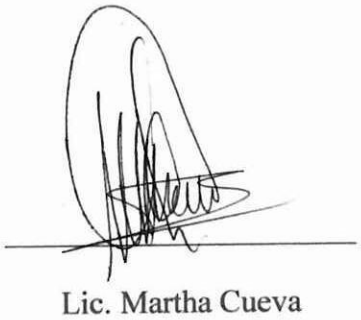
Certificación de Traducción

CERTIFICADO DE TRADUCCIÓN

En calidad de Licenciada de la especialidad de Ingles, CERTIFICO, que he realizado una exhaustiva revisión de la traducción al idioma ingles de la tesis realizada por el egresado: Luis Francisco Gutiérrez Aguilera, portador de la cédula de identidad N° 050160622-2, con el tema:"Propuesta para la implementación de una Red Privada Virtual para el Instituto Superior en Pinar del Río".

Es cuanto puedo certificar en honor a la verdad.

Latacunga, 12 de Diciembre del 2005



Lic. Martha Cueva

Índice

ÍNDICE.

ÍNDICE.

ÍNDICE.

ÍNDICE.

Introducción

INTRODUCCION

Los países y sociedades dependen fuertemente de la información para estimular su crecimiento económico, el ordenador ha sido el catalizador de esta revolución de la información, la sociedad de la información esta basada en datos que es la materia prima que contiene información. La esencia de la automatización y la sociedad de la información es el procesamiento manipulación y generación de datos para suministrar algo inteligible como es la información.

Esta poderosa capacidad se ve fortalecida por el uso de sistemas de comunicaciones de datos. Estos sistemas se encargan del transporte de datos e información entre los ordenadores las comunicaciones de datos proporcionan las conexiones entre ordenadores de un país y del mundo situados a grandes distancias, los recursos informáticos están unidos mediante sistemas de comunicación de datos formando una red de recursos automatizados.

Las redes de computadoras de hoy ofrecen muchos beneficios ya que durante las primeras décadas de su existencia, las redes de computadoras fueron utilizadas solamente por investigadores; universitarios para el envío de correo electrónico y por empleados corporativos para compartir impresoras, por lo que la seguridad no tenía mucha importancia pero ahora cuando millones de ciudadanos comunes usan redes para sus múltiples actividades diarias ya que estas reducen gastos de tiempo y dinero a las empresas, dando una gran ventaja para estas organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, por lo que las ventajas de las redes en Informática son evidentes, pero muchas veces se minusvaloran ciertos riesgos, circunstancia que a menudo pone en peligro la seguridad de los sistemas. En unos pocos años la inmensa mayoría de las empresas operaran a través de la Red, y esto solo será

posible si los profesionales de la Informática saben aportar soluciones que garanticen la seguridad de la información, Por tal motivo la seguridad de las redes es de suma importancia, y es aquí donde aparece la VPN (*Virtual Private Network*, Red Privada Virtual).

Antecedentes

En Cuba no ha existido aun un despliegue masivo de las Redes Privadas Virtuales y es en el año 2003 que se ha realizado algunas investigaciones al respecto, en la capital del país así como también en el resto de universidades.

Los Proveedores de Servicios de Internet, no ofrecen hasta el momento soluciones VPN, para los usuarios que requieran, por lo que estas tienen que ser implementadas y administradas por parte de los usuarios.

De aquí surge el problema que se quiere resolver que es el siguiente:

Problema

Necesidad de implementación de una red segura en el Instituto Superior Pedagógico, que provea protección, a las Pcs que manejen información confidencial, garantizando una transmisión confiable entre las mismas y los clientes que la usen.

De esta forma el objeto sobre el cual se trabaja sería:

Objeto

Las redes de computadoras y sus configuraciones

INTRODUCCION

Objetivos

1. Evaluar las diferentes tecnologías de seguridad presentes en las Redes Privadas Virtuales.
2. Lograr la implementación de Redes Privadas Virtuales basadas en IP
3. Demostrar, una vez implementada las Redes Privadas Virtuales, que se logra la privacidad y seguridad de la información transmitida por la red.
4. Definir una propuesta de VPN para la implementación en el Instituto Superior Pedagógico, para los departamentos Económico y de Recursos Humanos.

Hipótesis

La implementación de VPN en el Instituto Superior Pedagógico, para la protección de información confidencial de los departamentos Económico y de Recursos Humanos, garantizando la seguridad requerida por tales entidades.

Estructura del trabajo

El trabajo se presenta en tres capítulos organizados de la siguiente manera:

El Primer Capítulo contiene los conceptos fundamentales de las Redes Privadas Virtuales y sus clasificaciones teniendo en cuenta detalles de implementación.

El segundo capitulo hace referencia en las tecnologías de Redes Privadas Virtuales basadas en IP y los protocolos que se emplean en las mismas describiendo algunos pasos interesantes para su implementación.

El tercer y último capitulo trata sobre la propuesta realizada en la investigación, luego de haber realizado distintas implementaciones prácticas que avalan los resultados.

Capítulo I

1.1. Concepto de Red Privada Virtual.

Una VPN es una red privada que se extiende, mediante un proceso de encapsulación, y en su caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte como Internet. Eso indica que con una red privada virtual, se pueden enviar datos entre dos equipos a través de una red compartida o pública, de forma que emula un vínculo privado punto a punto.

Para emular un vínculo punto a punto, los datos de la red privada se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red compartida o pública hasta alcanzar su destino, formando un "túnel (Encapsulación)" que queda definido en la red pública por donde viajan los datos. Para emular un vínculo privado, los datos se cifran para asegurar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar si no se dispone de las claves de cifrado. El vínculo en el que se encapsulan y cifran los datos privados es una conexión de red privada virtual (VPN).

La Figura 1.1 muestra el equivalente lógico de una conexión VPN.

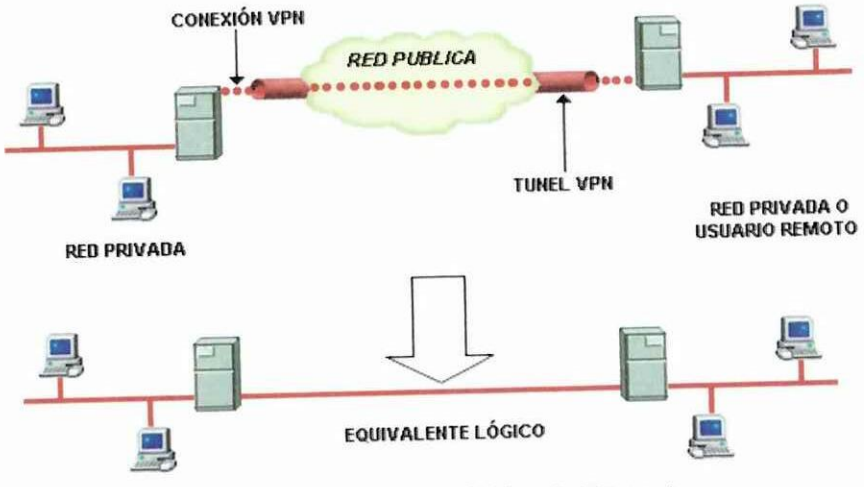


Figura 1.1: Red Privada Virtual.

1.2. Importancia de las VPN's

La importancia de las VPNs radica fundamentalmente en el hecho de lograr disminuir el costo del enlace entre dos sitios remotos.

Cuando se desea conectar las oficinas centrales de una empresa con alguna de sus sucursales u oficinas remotas, o los usuarios remotos conectarse con la misma, se tienen tres opciones de conexión fundamentales:

I. **Conexión por módem telefónico:** Las desventajas en que incurre este tipo de conexión están dadas principalmente 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.

II. **Conexión por línea privada o arrendada:** En este caso la conexión entre las dos entidades generalmente es por cables de pares de cobre o por fibra óptica de un punto a otro. Aquí el costo del enlace entre la oficina central y una sucursal es elevado, ya que esta dado por una tarifa mensual por kilómetro de distancia, sin importar el tráfico cursado por el enlace.

III. **Conexión a través de una Red Privada Virtual:** En el caso de una conexión por VPN, una empresa se ahorra en inversión de infraestructura tecnológica, administración y mantenimiento, 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 proveedor local, o podría usarse un

enlace dedicado a Internet ya establecido por lo que desaparecen los pagos por concepto de enlaces dedicados para la interconexión de oficinas remotas.

Las comparaciones anteriores demuestran que la opción de conexión a través de una VPN constituye la más óptima dado los ahorros en inversión que ello implica.

1.3. Ventajas y desventajas de las VPNs

Ventajas

La principal ventaja de usar una VPN 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 un ordenador en esa red privada, pudiendo acceder a la información publicada para esa red privada (bases de datos, documentos internos, etc.) a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizarán 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.
- La integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente bajo cualquier sistema operativo.

- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

Desventajas

Entre los inconvenientes se pueden citar: una mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce una mayor congestión en la mayoría de conexiones. También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP).

1.4. Tipos de VPN según el modo de conexión

Las VPN se pueden clasificar de acuerdo a quiénes son las entidades que se conectan, encontrándose las siguientes alternativas:

1.4.1. Redes privadas virtuales basadas en Internet

Acceso de usuario remoto a través de Internet

Las VPNs deben proporcionar acceso remoto a los usuarios de la corporación a través de Internet, y al mismo tiempo conservar la privacidad de la información. En la Figura 1.2 se representa este caso.

En este caso, en vez de utilizar una línea arrendada o hacer una llamada de larga distancia a un servidor de acceso a red corporativo (NAS, Network Access Server, Servidor de Acceso a Red), el usuario debe llamar a un número telefónico local correspondiente al NAS de su Proveedor de Servicio de Internet (ISP, *Internet Service Provider*, Proveedor de Servicio a 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.

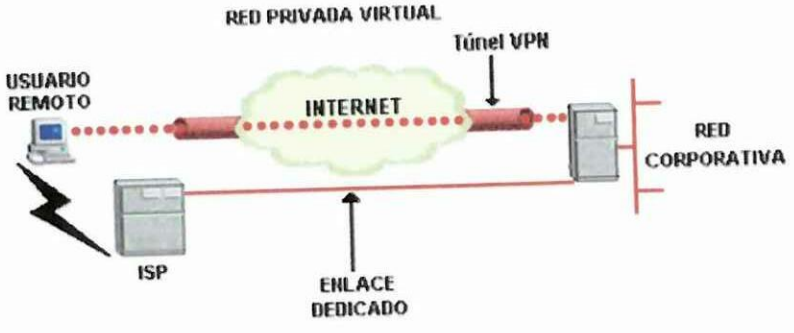


Figura 1.2: Uso de una VPN para conectar a un usuario remoto a una Intranet corporativa a través de Internet

Conexión de redes empresariales a través de Internet

Existen dos métodos para utilizar las VPNs y permitir la conexión de las redes de área local a sitios remotos (Figura 1.3):

1. Uso de líneas dedicadas para conectar una sucursal LAN corporativa: En este caso, 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 VPN utiliza las conexiones de ISP locales e Internet para crear una red privada virtual entre el router de la sucursal y el router corporativo.

2. Uso de una línea de marcación para conectar una sucursal a una LAN corporativa: En este caso, el router en la sucursal puede llamar al ISP local. El software de la VPN 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.

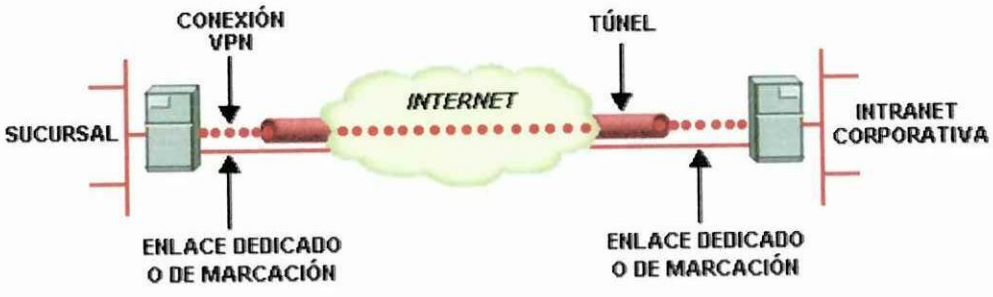


Figura 1.3: Uso de una VPN para conectar dos sitios remotos.

1.4.2. Redes Privadas Virtuales basadas en Intranet

Acceso remoto a través de una Intranet

En las Intranets de algunas organizaciones, los datos de un departamento, por ejemplo, el departamento económico o el de recursos humanos, son tan confidenciales que la red del departamento está físicamente desconectada de la Intranet del resto de la organización. Aunque así se protegen los datos del departamento, se crea un problema de acceso a la información por parte de aquellos usuarios autorizados que no están físicamente conectados a la red independiente.

Mediante una conexión VPN, la red del departamento está físicamente conectada a la Intranet de la organización pero se mantiene separada gracias a un servidor VPN. El servidor VPN no proporciona una conexión enrutada directa entre la Intranet de la

organización y la red del departamento. Los usuarios de la Intranet de la organización que disponen de los permisos apropiados pueden establecer una conexión VPN de acceso remoto con el servidor VPN y tener acceso a los recursos protegidos de la red confidencial del departamento. Adicionalmente, para mantener la confidencialidad de los datos, se cifran todas las comunicaciones realizadas a través de la conexión VPN utilizando algún mecanismo de encriptación estándar. Para aquellos usuarios que no tienen permisos para establecer una conexión VPN, la red del departamento está oculta a la vista.

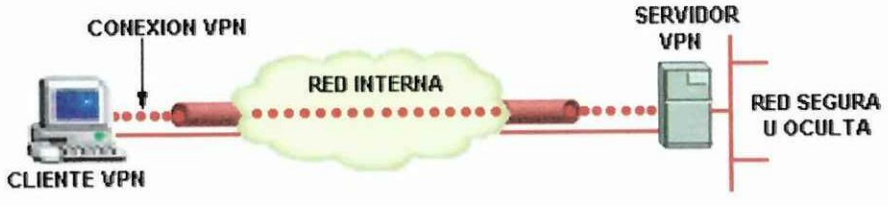


Figura 1.4: Uso de una VPN para conectar dos computadoras en la misma LAN.

Conexión de redes a través de una Intranet

Análogo al segundo caso, dos redes se pueden conectar a través de una Intranet mediante una conexión VPN de enrutador a enrutador. Las organizaciones que tienen departamentos en diferentes ubicaciones, cuyos datos son altamente confidenciales, pueden utilizar una conexión VPN de enrutador a enrutador para comunicarse entre sí. Por ejemplo, el departamento económico podría necesitar comunicarse con el departamento de recursos humanos para intercambiar información acerca de las nóminas.

El departamento económico y el departamento de recursos humanos están conectados a la Intranet común, con equipos que pueden actuar como clientes VPN o servidores VPN. Una vez establecida la conexión VPN, los usuarios de los equipos de ambas redes pueden intercambiar datos confidenciales a través de la Intranet corporativa.

La figura 1.5 muestra la conexión de redes a través de una Intranet.

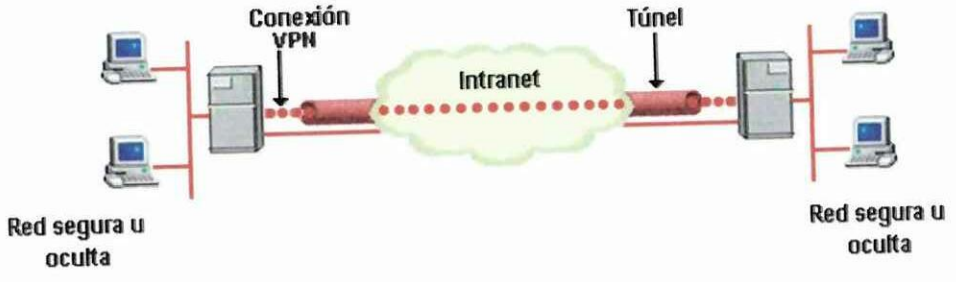


Figura 1.5: Conexión de redes a través de una Intranet.

1.5. Tipos de VPN según la tecnología de transporte

En este tema se pretende describir algunas de las tecnologías VPN analizando sus funcionalidades y realizando una comparación entre las tecnologías existentes para implementarlas.

Estas tecnologías son usadas por los proveedores para ofrecer el servicio a los clientes, y en función del tipo de implementación escogida, se les ofrecerá uno u otro tipo de servicio.

La forma de brindar este servicio por parte de los proveedores está muy condicionada por la infraestructura de sus redes de datos.

Las soluciones más comunes son las siguientes:

- ✓ Mediante circuitos virtuales ATM
- ✓ A través de túneles tradicionales (GRE *Generic Routing Encapsulation*, Encapsulación por enrutamiento genérico o túneles IP-IP)
- ✓ Utilizando IPSec
- ✓ Implementando MPLS

Se analizan a continuación cada una de estas opciones.

1.5.1. VPNs basadas en circuitos virtuales ATM

ATM son las siglas de (*Asynchronous Transfer Mode*, Modo de Transferencia Asíncrono). La tecnología ATM está ampliamente extendida, principalmente en el backbone de la red aunque actualmente se está sustituyendo por medios de transmisión síncronos y ópticos.

Para proveer Redes Privadas Virtuales con ATM lo que se hace es reservar Circuitos Virtuales Permanentes (PVC) del ancho de banda deseado entre las sedes que se desean unir. Esta solución está empezando a entrar en desuso por varias 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) enlaces, que serían los PVCs, y esto puede llegar a suponer una cantidad excesiva. Así para interconectar 80 nodos, se necesitan 6320 circuitos permanentes.
- El tráfico actual mayoritario es IP. La gestión de las redes ATM es diferente del de IP, con lo que se tienen que duplicar dichos sistemas (uno para IP y otro para ATM). Esto supone duplicar esfuerzos tanto en operación y mantenimiento como en recursos humanos.

1.5.2. Túneles IP-IP

En las redes que no utilizan ATM como protocolo de transporte, se pueden realizar 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.

El túnel más común es GRE el cual fue desarrollado por Cisco originalmente, y constituyen túneles IP sobre IP cifrados. Este puede hacer unas cuántas cosas más que los túneles IP-sobre-IP. Por ejemplo, se puede transportar tráfico multicast e IPv6 sobre un túnel GRE.

Una arquitectura típica cuando se usan túneles es hacer pasar estos por un "Concentrador de Túneles". Este equipo suele ser de gran potencia y bastante costoso. Además el tráfico tipo "túnel" no suele ser 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.

1.5.3. Túneles IPSec

Este protocolo está siendo desarrollado por el grupo de trabajo de seguridad del IETF (*Internet Engineering Task Force*, Grupo de Trabajo de Ingeniería Internet).

El protocolo IPSec surgió a partir del desarrollo de Ipv6. Empezó siendo una extensión de la cabecera en Ipv6, pero debido a que cubría las necesidades de un gran número de clientes, se decidió implementar en parte para Ipv4.

IPSec tiene como característica más importante la posibilidad de encriptar los datos transmitidos. Esta cualidad es hoy en día el gran valor que tiene este protocolo y es lo que está permitiendo su rápida difusión en el mundo empresarial.

Entre las desventajas que puede presentar se destacan las siguientes:

- Es un protocolo complejo.
- Su configuración es complicada.
- Requiere configuración en el cliente.
- Tiene una provisión lenta y complicada.

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. En el Capítulo 2 se abordará más en este protocolo.

1.5.4. 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.

Este protocolo está siendo estandarizado por el IETF, y se ha definido un método para ofrecer IP VPN en la red utilizando MPLS, tratados en la RFC 2547 bis, que aborda los requisitos de los suministradores de servicios VPN (Figura 1.6).

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 VPN.

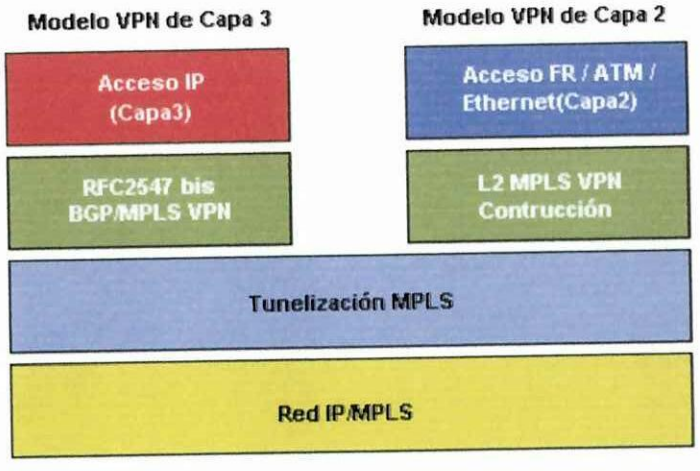


Figura 1.6: Modelo MPLS VPN.

El protocolo de señalización usado para MPLS es RSVP (Protocolo de Reservación de Recursos). Éste es un estándar en Internet para la reserva de recursos. Con RSVP se pueden reservar anchos de banda mínimos, se 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.

1.6. Tipos de VPN según el modo de aplicación

Según el modo de aplicación las VPN se pueden clasificar en sistemas basados en Hardware, Cortafuegos, y Software.

1.6.1. Sistemas basados en Hardware

Los sistemas basados en hardware, son routers que encriptan. Son seguros y fáciles de usar, puesto que son *plug and play*. Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido, y de fácil instalación.

1.6.2. Sistema basados en Cortafuegos

Estos 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. También realizan la traducción de direcciones NAT (*Network Address Translation*) Estos 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 VPN. El rendimiento en este tipo decrece, ya que no se tiene hardware especializado de encriptación.

1.6.3. Sistema basados en Software

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPN ofrece el método más flexible en cuanto al manejo de tráfico. Con este tipo, el tráfico puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en los VPN por hardware, todo el tráfico era enrutado por el túnel. Podemos hacer un enrutamiento inteligente de una manera mucho más fácil.

1.7. Encapsulamiento o Túnel *(tunneling)*

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. La tecnología de túneles "*Tunneling*" es un modo de transferir datos entre dos redes similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado "encapsulación", ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original.

Hay varios usos para el término "*tunneling*" en las redes. El significado más común y técnico de los túneles en Internet, se refiere a introducir un paquete dentro de otro; IPX dentro de IP, PPP dentro de IP. En este proceso el "*tunneling*" es meramente un proceso de transporte. El IP no añade seguridad al IPX o al PPP cuando se encapsula, meramente los porta.

La definición mezcla un concepto técnico, el encapsulamiento, también llamado "*tunneling*", con el concepto de la seguridad, dando como resultado la connotación de que las VPN se encuentran en una zona de robustez, con un túnel especial alrededor de ellas. Esto es desde el punto de vista lógico, ya que en realidad, mientras que las VPN son seguras contra piratas de la red (*hackers*) e intrusos, no hay túneles, y circuitos virtuales a través de Internet, tampoco se les dan, por ahora, a los paquetes de túnel prioridades especiales, siguen siendo datagramas como los otros paquetes

Lo que añade seguridad son los procesos de encriptación y autenticación, que se pueden utilizar con los paquetes en el túnel y con los paquetes cuando no hay túnel. Algunos

enfoques de VPN encapsulan todos los paquetes antes de encriptarlos. Otros encriptan solo los contenidos de los paquetes y los contenidos de los paquetes encapsulados, no las cabeceras. De cualquier manera es la encriptación, no el encapsulamiento la que añade seguridad.

En la Figura1.7 se muestra cómo se encapsulan los datos en una conexión VPN donde un cliente que se encuentra fuera de su red, desea acceder a la información del servidor de su red corporativa a través de Internet.

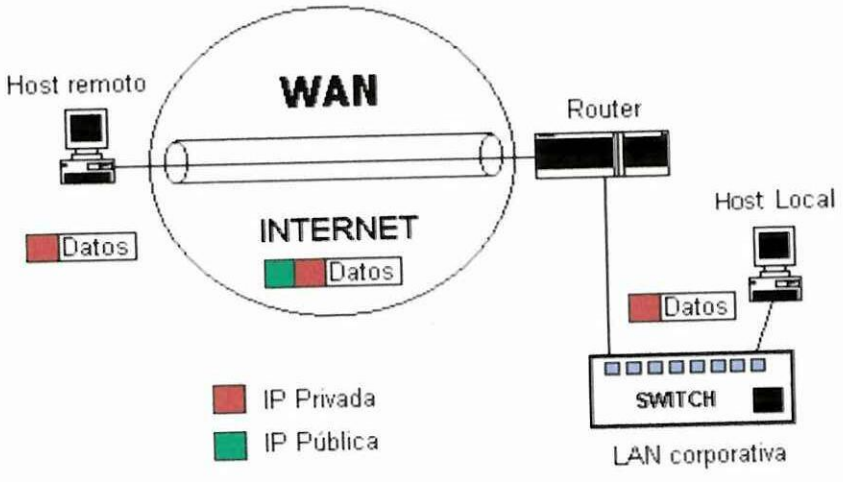


Figura 1.7: Representación del proceso de encapsulación.

1.8. Principios de seguridad y encriptación en las VPNs

Hay bastante área independiente de investigación y de tecnología relacionadas con la seguridad de los recursos de información. No obstante, las "tres más importantes" son la confidencialidad, la integridad y la autenticación.

- **Confidencialidad:** consiste en mantener la información oculta a la curiosidad de las personas a la que no está destinada.
- **Integridad:** trata de mantener la información intacta o, al menos, detectar si se ha alterado eventualmente.
- **Autenticación:** consiste en identificar el origen de la información.

Estos tres principios son independientes, pero complementarios. Ejemplo de esto puede ser una transacción enviada desde una sucursal bancaria a la oficina central con la orden de transferir 10.000 dólares a la cuenta X del banco. El banco puede no estar especialmente preocupado con la confiabilidad de este mensaje, pero la sucursal si estará preocupada por su integridad y por el origen correcto.

Estos principios se aplican por igual a los mensajes entre personas que a los paquetes enviados de una máquina a otra. De esta forma, es importante saber qué técnicas existen para contrarrestar las amenazas que puedan dañar el proceso de comunicación.

1.8.1. Técnicas de seguridad

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, con el propósito de mantener oculta la información que se considera privada a cualquier persona o sistema que no se le tenga permitido verla.

La técnica de encriptación a aplicar se basa en la sensibilidad de la información a ocultar, es decir, mientras más sensible sea la información se debe aplicar un sistema de encriptación más robusto.

Existen varias herramientas de seguridad y criptografía, éstas se pueden agrupar en varias categorías, que corresponden con los principios descritos anteriormente y que se muestran en la Tabla 1.1.

Codificación

La codificación es una de las más antiguas formas de criptografía, habiéndose utilizado durante siglos para enviar mensajes secretos que van desde tácticas de guerra a operaciones clandestinas. Los sistemas modernos usan potentes algoritmos de codificación y claves para codificar y descodificar la información. Estos sistemas se pueden clasificar en varias categorías: bloque o continuo, y simétrico o asimétrico.

Principio	Técnica	Descripción
Confidencialidad	Codificación	Estos sistemas codifican la información (normalmente por medio de claves) de forma que sólo los destinatarios legales (poseedores de la clave correcta) pueden ver (descodificar) la información.
Integridad	Resumen de mensajes	Estos crean una potente suma de controles criptográficos o impresión digital de un bloque de información. La naturaleza de estos resúmenes (a diferencia de las suma de control típicas) hace imposible modificar un mensaje para que tenga un valor particular.
Autentificación	Firmas digitales	Estos sistemas emplean normalmente un par de claves,

		una privada que se usa para firmar un mensaje y otra que se puede distribuir y que sirve para verificar la firma. Los sistemas de firma de dos claves (o asimétricos) asumen que el destinatario tiene acceso a la clave de verificación (o pública) del remitente.

Tabla 1.1: Herramientas de seguridad y criptografía.

La gran mayoría de los sistemas instalados actualmente son simétricos por bloques, y funcionan partiendo un mensaje en partes de tamaño fijo que se codifican a continuación con una clave. La misma clave se usa para decodificar el mensaje aplicando el algoritmo de decodificación a los mismos bloques creados durante la etapa de codificación.

La Figura 1.8 muestra un sistema de codificación que utiliza el cifrado simétrico por bloque. Hay docenas de algoritmos a elegir, cada uno con sus propias características: nivel de seguridad, velocidad de cálculo, tamaño de los bloques y tamaño de clave. Por ejemplo el DES (*Data Encryption Standard*, Estándar de Encriptación de Datos) es sólo medianamente seguro para los estándares actuales, relativamente lento para correr a nivel de lógica (pero eficiente a nivel de equipo). El tamaño de bloque es 64 bits y el de clave 56 bits.

Los algoritmos de cifrado continuos producen un flujo codificado de bits pseudo-aleatorios que se usan para codificar el flujo de datos claros (utilizando una operación OR-exclusivo), y decodificándolo utilizando un mecanismo inverso (sincronizado) en la parte receptora.

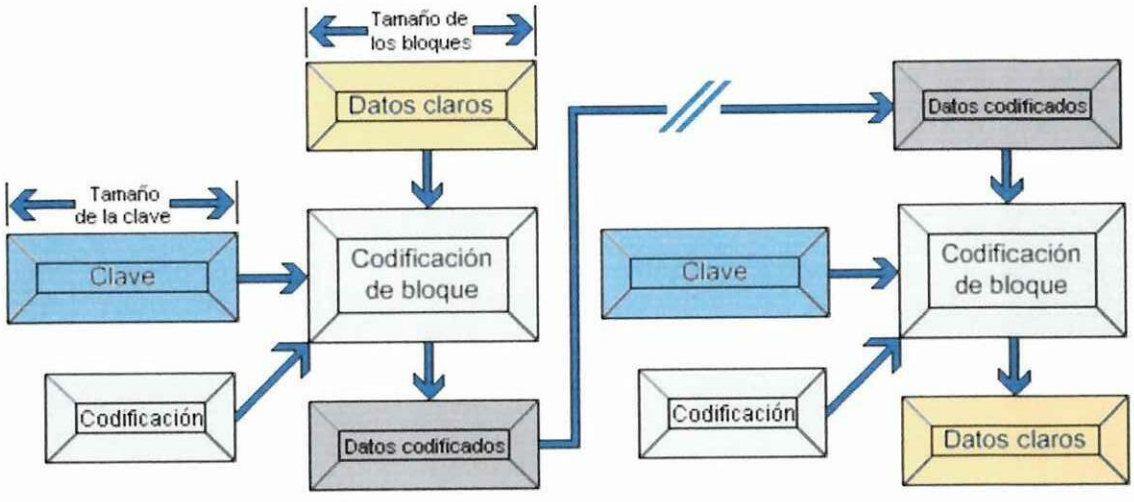


Figura 1.8: Principio de codificación y decodificación.

No obstante, hay una importante salvedad para todos estos tipos de sistemas. El remitente y el receptor de un mensaje deben compartir antes una clave (cosa que no pasa en el caso de los sistemas asimétricos).

Los sistemas de codificación asimétricos usan dos claves. Una, que se distribuye públicamente, se usa para codificar los datos que su homólogo privado puede usar para decodificar. Estos sistemas funcionan por bloques, pero en general son lentos. Como hay importantes ventajas con los sistemas de dos claves, con frecuencia se usan conjuntamente con sistemas de una clave. Por ejemplo, supongamos que de la oficina central desea enviar a la sucursal bancaria un e-mail grande codificado. Si no comparten una clave en común, entonces tienen un problema. Necesitan usar un sistema asimétrico para resolver el problema de clave compartida. No obstante, para codificar un fichero grande se necesitaría mucho utilizando un sistema como este. En consecuencia, usan un sistema asimétrico para codificar una clave simétrica, que después se usa por el sistema simétrico más rápido, como se muestra en la Tabla 1.2.

Ahora la oficina central ha enviado con éxito su fichero grande a la sucursal bancaria usando la eficiencia de un cifrado simétrico, a pesar de no haber compartido antes alguna información de claves.

Oficina Central		Sucursal Bancaria
Envía su clave pública	→	
		Inventa una clave simétrica *"K"*
		Codifica *"K"* usando la clave pública de la oficina central para producir *"K_e"*
	←	Envía *"K_e"*
Descodifica *"K_e"* usando su clave privada para producir *"K"*		
Codifica el *"fichero"* utilizando un sistema simétrico rápido y la clave *"K"* para producir un *"fichero$_e$"*		
Envía *"fichero$_e$"*	→	
		Descodifica el *"fichero"* usando *"K"* para producir el *"fichero"* original

Tabla 1.2: Uso combinado de la codificación simétrica y asimétrica.

El método más popular de intercambio de clave pública es el Diffie-Hellman. En este proceso de dos etapas, las partes intercambian claves que se inventan dinámicamente, y con la ayuda de un poco de magia matemática son capaces de proporcionar un número común que un espía no puede descubrir.

La Tabla 1.3 lista algunos de los algoritmos de codificación por bloques disponibles.

	Simétrico	**Asimétrico**
Bloques	DES, 3DES, RC2, RC5, AES, CAST, IDEA, Skipjack, Safer, Blowfish, FEAL	RSA

Tabla 1.3: Principales algoritmos de codificación simétricos y asimétricos.

Resumen de mensajes

Hay un gran número de aplicaciones que utilizan resúmenes (o hashes), pero la mayoría de ellas se encargan de detectar si la información está intacta. Un resumen criptográfico toma bloque de datos de cualquier tamaño como entrada y produce una impresión digital de un tamaño específico, dependiendo del algoritmo utilizado. La naturaleza del algoritmo es tal que no es posible proporcionar un bloque de datos de entrada que dé lugar a una salida determinada. Esto previene contra un atacante que desea modificar o sustituir un fichero que un destinatario va a verificar contra un valor conocido del resumen.

Los sistemas de resumen más populares son: MD4, MD5 y SHA-1.

Firma digital

En general, un sistema de firma digital utiliza claves asimétricas para realizar sus operaciones: una función de firma usa una clave privada, y una función de verificación usa una clave pública. Normalmente, el objeto que se está firmando se pone primero en una operación de resumen para darle un tamaño que pueda manejarse con la operación de firma.

La Figura 1.9 muestra un remitente en la parte izquierda enviando un fichero autentificado al destinatario de la parte derecha. Para hacer esto, el remitente firma el resumen del fichero usando una clave privada (conocida sólo por el remitente) y envía la firma (normalmente una serie de bits de tamaño fijo) junto con el fichero. El destinatario controla el fichero, la firma y la clave pública del remitente por una función de verificación que determina si la firma es válida o no. Si es válida el destinatario sabe que el propietario de la clave privada corresponde a la clave pública que firmaba el mensaje.

Hay que hacer notar que una aplicación interesante de firmas digitales es similar a distribuir software sin virus. Si un ejecutable está firmado por una compañía de confianza, se puede asegurar que no ha sido infectado desde su creación verificando la firma.

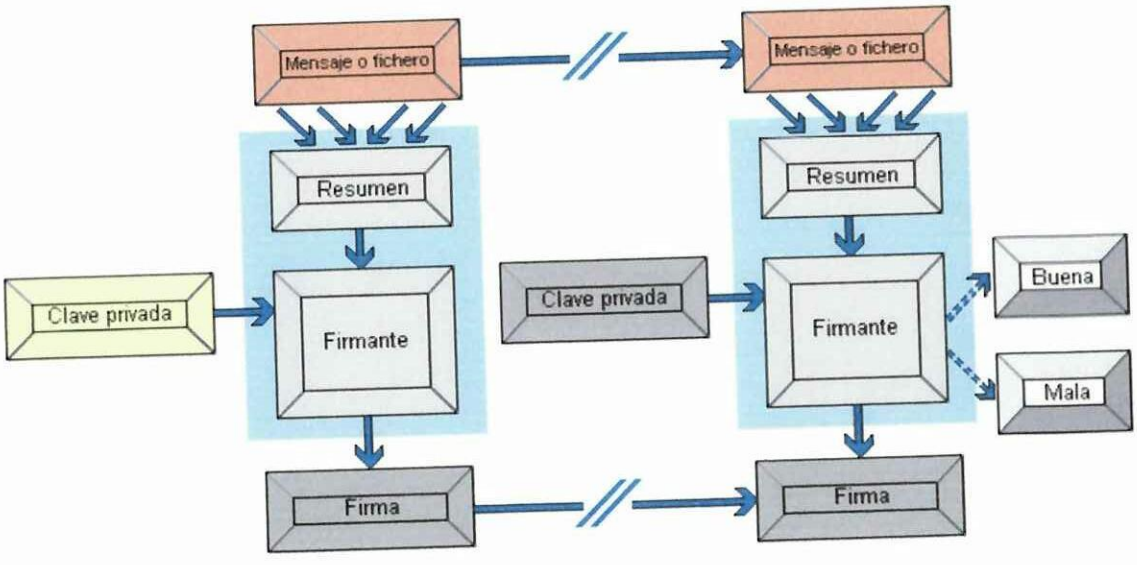


Figura 1.9: Uso de una forma digital.

RSA y DSA son los sistemas de firmas que se utilizan con mayor frecuencia.

Certificado de clave pública

Las firmas digitales se utilizan para suministrar autentificación. Al recibir un documento firmado, solo hay que pasar la clave pública del remitente por un algoritmo de verificación que dice "Sí" o "No". El problema es cómo obtiene el receptor la clave pública en primer lugar. Se puede imaginar que se encuentra disponible en un directorio (como una guía telefónica), pero así el receptor no puede estar seguro de que la clave pública no se ha sustituido en el tránsito.

Un certificado es una identidad digital autorizada por alguien en quien confiamos, conocido como una Autoridad de Certificación. Por lo general sirve para asociar digitalmente el propietario a una clave pública. Al estar el certificado firmado, no se puede usurpar ni modificar. Al usar certificado el receptor de un mensaje firmado puede

ahora buscar con total seguridad la clave pública del remitente, ya que se puede verificar su autenticidad en la recepción. Los certificados normalmente se estructuran de acuerdo a la recomendación X.509 de la UIT. Están formados por un identificador (nombre), una clave pública, un número de serie, las fechas de validez y una firma generada usando la clave privada de la Autoridad de Certificación (ver Figura 1.10).

La popularidad de los certificados de clave pública está aumentando a gran velocidad ya que se utilizan para el comercio electrónico para el e-mail seguro, para los formularios electrónicos, para auditorias, y para las Redes Privadas Virtuales.

Nombre:	"Efrén Cordovez Rodríguez"
Clave pública:	RSA-1024: 451f6c882..8b
Número de serie:	2772-18811
Fecha de expiración:	Junio 27, 2004
Emisor:	2770-19199
Firma AC:	DSA: 177f31cbe94..1f

Figura 1.10: Certificado de clave pública.

1.8.2. Aplicación de la encriptación en las VPNs

Todas las VPNs 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 vistas anteriormente son aplicables a las VPNs.

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 posee el problema que, como la contraseña es compartida por todos los participantes y 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.

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.

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

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

1.9. Calidad de Servicio en las VPN (QoS)

Es posible definir calidad de servicio 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 VPN 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.

Las VPN 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 establece. Este modelo RSVP como protocolo de señalización. El requerimiento de que RSVP deba ser interpretado por el conjunto de equipos atravesados 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).

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, por ejemplo, sino que se forman agregaciones de tráfico. Así, un operador puede integrar las conexiones de usuarios pertenecientes a diferentes VPN 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, por ejemplo, pero actualmente, sólo un trabajo de ingeniería de red y dimensionamiento correcto de la misma podrá 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 a 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.

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.

Capítulo II

2.1. Descripción de algunos protocolos utilizados en las VPN IP

MPPE (*Microsoft Point-to-Point Encryption*): Cifrado punto a punto de Microsoft, protocolo que se utiliza para encriptar los datos de las transmisiones. Es un algoritmo de cifrado de clave de 128 bits o clave de 40 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. Es un protocolo de autenticación donde 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.

IPIP (Protocolo de Encapsulamiento de IP sobre IP): Este protocolo, como se vio en el Capítulo I, sirve para hacer el *tunneling* que se marca como uno de los requisitos de VPN.

IP-GRE (Protocolo de Encapsulamiento de otros protocolos sobre IP): En un principio el tráfico que puede encapsular IP-GRE sería cualquiera. Es útil en el sentido de que se puede tener redes de otro tipo además de IP (como por ejemplo IPX) y funcionar con una VPN de igual manera. Más adelante se verá como IPSec sirve para este mismo fin (a la vez que proporciona otros muchos servicios).

PPP (*Point-to-Point Protocol*): Protocolo Punto a Punto, fue diseñado para enviar datos a través de conexiones punto a punto de marcación o dedicadas. El PPP encapsula

paquetes IP, IPX, y NetBEUI dentro de las tramas del PPP, y después los transmite a través de un enlace punto a punto. El PPP se utiliza entre un cliente de marcación o dedicado y un NAS.

PPTP (*Point-to-Point Tunneling Protocol*): Protocolo de encapsulado de PPP sobre IP. Es una especificación desarrollada por un consorcio de fabricantes, entre los que estaban gente como Microsoft, 3Com y U.S. Robotics. El protocolo se diseñó originalmente como una forma de encapsular protocolos no TCP/IP (como IPX) para poder ser transmitidos por Internet usando GRE. Es una especificación genérica, que permite la adición de diversos mecanismos de autentificación y algoritmos de encriptación. Nótese que estas técnicas de seguridad no están dentro del protocolo, sino que se añaden. 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 (o encapsula) para el tráfico IP, IPX o NetBEUI en paquetes IP. Esto significa que los usuarios pueden ejecutar de forma remota aplicaciones que dependen de determinados protocolos de red.

IPSec (*Seguridad de protocolo Internet*): IPSec es un grupo de extensiones de la familia del protocolo IP. IPSec provee servicios criptográficos de seguridad. Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad. IPSec provee servicios similares a SSL (*Secure Socket Layer*, Capa de Socket Segura), pero a nivel de red, de un modo que es completamente transparente para sus aplicaciones y mucho más robusto. Es transparente debido a que sus aplicaciones no necesitan tener ningún conocimiento de IPSec para poder usarlo. Se puede usar cualquier protocolo

basado en IP sobre IPSec. Se pueden crear túneles cifrados (VPN), o simple cifrado entre computadoras. Debido a que dispone de tantas opciones, IPSec es muy complejo.

L2TP (*Layer Two Tunneling Protocolol*): Protocolo de túnel de nivel 2. Con L2TP se puede tener acceso a una red privada a través de Internet o de otra red pública mediante una conexión VPN. L2TP es un protocolo estándar de túnel para Internet que tiene casi la misma funcionalidad que PPTP. Al igual que PPTP, L2TP 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 nuevo protocolo de autenticación y cifrado IPSec para añadir seguridad a la transmisión.

En las secciones siguientes se detallará en los protocolos PPP, PPTP, L2TP e IPSec dado su importancia en la creación de VPNs.

2.2. Protocolo Punto a Punto (PPP)

El Protocolo punto a punto (PPP, *Point-to-Point Protocol*) es un conjunto de protocolos estándar que permiten la interacción de software de acceso remoto de diversos proveedores. Una conexión habilitada para PPP puede conectar con redes remotas a través de cualquier servidor PPP normalizado. PPP también permite que un equipo que ejecute un servicio de acceso remoto reciba llamadas y proporcione acceso de red al software de acceso remoto de otros proveedores que cumpla los estándares de PPP.

Los estándares de PPP también permiten características avanzadas, no disponibles en estándares más antiguos como SLIP (Protocolo de línea serie). PPP acepta varios

métodos de autenticación, así como compresión y cifrado de datos. En la mayor parte de las implementaciones de PPP, se puede automatizar todo el proceso de inicio de sesión.

PPP también admite múltiples protocolos de LAN. Puede utilizar TCP/IP, IPX o NetBEUI como protocolo de red.

PPP es la base de los protocolos PPTP y L2TP, que se utilizan en las conexiones protegidas de Redes Privadas Virtuales.

En la Figura 2.1 se muestra el formato de la trama PPP. El primer y último campo constituyen banderas de inicio y fin de trama respectivamente. Contiene además un campo de Dirección, de Control, de Información donde están encapsulados los paquetes de nivel superior como IP, y un campo de suma de comprobación (FCS).

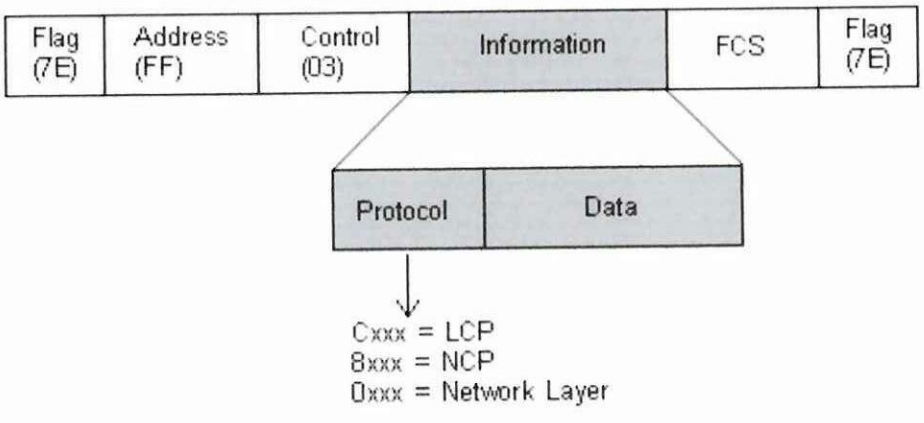


Figura 2.1: Formato de trama PPP.

Fases de negociación en una sesión de marcación PPP

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

Estas fases son:

Fase 1

Establecimiento del enlace de PPP: El PPP utiliza un protocolo de control de enlace (LCP, *Link Control Protocol*) para establecer, mantener y terminar la conexión física. Durante la fase del LCP, se seleccionan las opciones de comunicación básica. Hay que tener en cuenta que durante la fase de establecimiento del enlace (fase 1), se seleccionan los protocolos de autenticación, pero no se implementan realmente hasta la fase de autenticación de usuarios (fase 2).

Fase 2

Autenticación de usuarios: En esta fase, la PC que hace de cliente presenta la identificación del usuario al servidor de acceso remoto. Un esquema seguro de autenticación proporciona protección contra los ataques de contestación e imitación de clientes remoto.

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

Protocolo de autenticación de contraseñas PAP, (*Password Authentication Protocol*): El PAP es un esquema simple de autenticación de texto claro, es decir, que no está codificado. El NAS solicita el nombre y contraseña del usuario, y el PAP los regresa en texto claro. Indiscutiblemente, este esquema no es seguro debido a que puede ser interceptado el nombre y contraseña del usuario, y utilizarlos para obtener acceso al NAS y a todos los recursos suministrados por el mismo. El PAP no proporciona

protección contra los ataques de reproducción o las imitaciones de cliente remoto, una vez que la contraseña del usuario ha sido violada.

Protocolo CHAP: El CHAP es un mecanismo de autenticación codificado que evita la transmisión de la contraseña real a través de la conexión y utiliza tres pasos para el establecimiento de la conexión. Es una mejora del PAP ya que la contraseña del texto claro no se envía a través del enlace. En lugar de eso, la contraseña se utiliza para crear un hash codificado a partir de la señal de reconocimiento original. El cliente remoto debe utilizar el algoritmo unidireccional de hashing MD5 para regresar el nombre del usuario y una codificación de la señal de reconocimiento, ID de sesión y de la contraseña del cliente. El nombre del usuario se envía sin hashing.

El servidor sabe la contraseña del texto claro del cliente y, por lo tanto, replica la operación y compara el resultado con la contraseña enviada en la respuesta del cliente. CHAP protege en contra de los ataques de reproducción utilizando una cadena de reconocimiento arbitraria para cada intento de autenticación y protege además de la imitación de clientes remotos al enviar impredeciblemente señales de reconocimiento repetidas al cliente remoto durante la conexión.

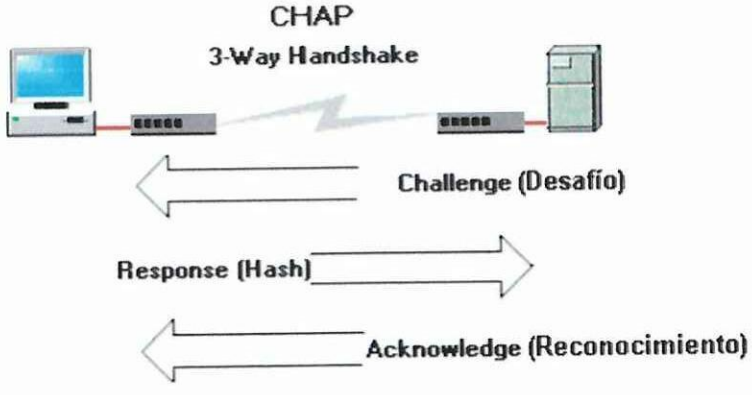


Figura 2.2: El proceso CHAP.

Protocolo MS-CHAP *(Microsoft CHAP)*: El MS-CHAP es un mecanismo de autenticación codificado muy similar al CHAP creado por Microsoft. Al igual que en el CHAP, el NAS envía al cliente remoto una señal de reconocimiento, que consiste de una ID de sesión y de una cadena de reconocimiento arbitraria. El cliente remoto debe regresar el nombre del usuario y un hash MD4 de la cadena de reconocimiento, la ID de sesión y de la contraseña con hash MD4. Este diseño, que manipula un hash del hash MD4 de la contraseña, proporciona un nivel adicional de seguridad porque permite que el servidor almacene contraseñas con hash en lugar de contraseñas de texto claro. El NAS reúne los datos de autenticación y después los valida con base en su propia base de datos de usuarios o basándose en un servidor central de base de datos de autenticación, además, proporciona códigos de error adicionales, incluyendo un código de expiración de contraseña, y mensajes adicionales codificados de cliente-servidor que permiten que los usuarios cambien sus contraseñas.

Fase 3

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

Fase 4

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

Después de haber culminado las cuatro fases de negociación se empiezan a transmitir los datos, esto se conoce como la fase de transferencia de datos.

Fase de transferencia de datos: Después de culminar las fases de negociación, el PPP comienza a transmitir los datos para y desde las dos partes. Cada paquete de datos transmitido se encapsula en un encabezado de PPP que es eliminado por el sistema receptor. Si la compresión de datos se seleccionó en la fase del establecimiento del enlace PPP y se negoció en la fase de invocación de protocolos del nivel de red, los datos serán comprimidos antes de la transmisión. Al culminar la transferencia de datos, cualquiera de los dos terminales puede terminar la conexión PPP.

2.3- Protocolo de túnel punto a punto (PPTP)

El Protocolo de túnel punto a punto (PPTP, *Point-to-Point Tunneling Protocol*) fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics, para proveer una red privada virtual entre usuarios de acceso remoto y servidores de red.

Este protocolo es, de hecho, un protocolo de túnel estándar del sector que se incorporó por primera vez en Windows NT 4.0. PPTP es una extensión del Protocolo punto a

punto (PPP) y aprovecha las ventajas de los mecanismos de autenticación, compresión y cifrado de PPP.

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.

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

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS (Servidor de Acceso Remoto) desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un módem conectado al servidor RAS, los usuarios se conectan a su proveedor ISP y luego "llaman" al servidor RAS a través de Internet utilizando PPTP. La Figura 2.3 muestra el escenario de una conexión remota VPN utilizando PPTP.

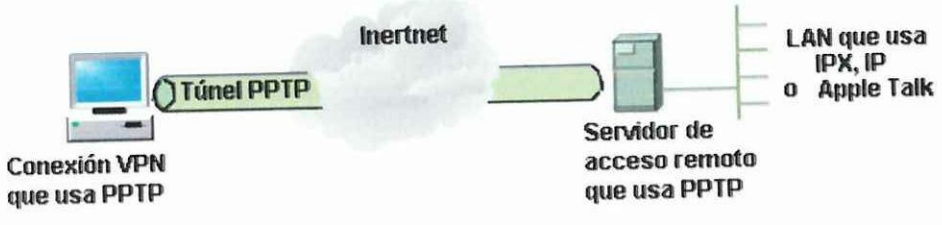


Figura 2.3: Conexión VPN que usa PPTP.

2.3.1. Tipos de conexión para las VPN basadas en PPTP

Entre los tipos de conexión VPN basadas en PPTP están los siguientes:

- El usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- El usuario remoto se conecta 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.
- Conexión de dos redes privadas a través de Internet o una Intranet.

Para el primero de los casos, el usuario remoto establece una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo caso, 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. En el tercer caso existe una conexión PPTP preestablecida entre dos redes, por lo que los usuarios no tienen que establecer ninguna conexión con los servidores VPN.

2.3.2. Técnica de Encapsulación

La técnica de encapsulación de PPTP se basa en el protocolo Generic Routing Encapsulation (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, 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. La siguiente figura ilustra las capas del encapsulamiento PPTP.

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.

En la siguiente Figura 2.4 se muestra la encapsulación PPTP para una trama PPP.

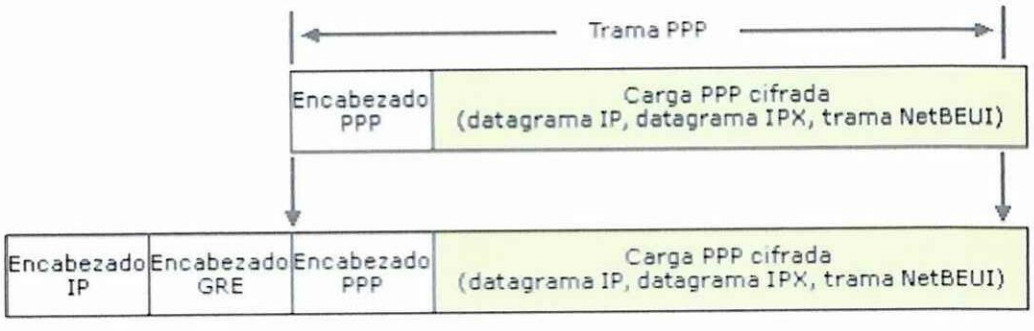


Figura 2.4: Encapsulación PPTP para una trama PPP.

2.3.3. Técnica de Cifrado

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.

2.3.4. Técnica de Autenticación

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive 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 de Windows 2000, en el caso de usar este 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.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

2.3.5. 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. Para que el servidor

de acceso remoto admita varias conexiones PPTP, se deben realizar los siguientes pasos:

- Configurar la conexión a Internet.
- 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 PPTP.
- Configurar los puertos PPTP.
- Configurar filtros PPTP.

La Figura 2.5 muestra los elementos de un servidor de acceso remoto que proporciona acceso remoto basado en PPTP a una Intranet corporativa.

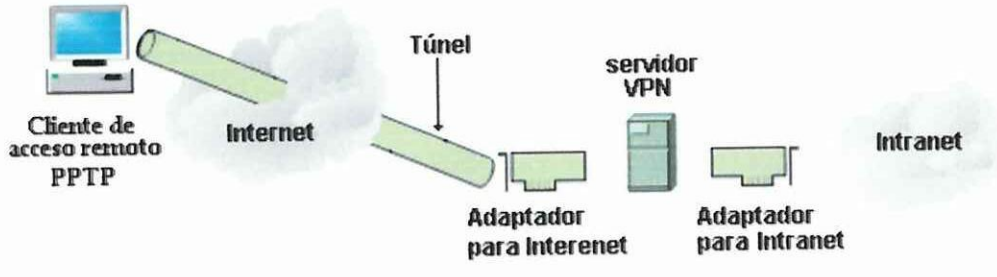


Figura 2.5 Elementos de una VPN basada en PPTP.

A continuación se explican cada uno de los pasos anteriores.

Configurar la conexión a Internet

La conexión a Internet desde el servidor VPN es una conexión dedicada: un adaptador para WAN instalado en el equipo. Normalmente, el adaptador para WAN es un adaptador T1, T1 fraccionario, Frame Relay o DSL.

Debe configurar TCP/IP de la siguiente forma en el adaptador para WAN:

- La dirección IP y la máscara de subred asignadas por InterNIC o por un proveedor de servicios Internet (ISP).
- La puerta de enlace o gateway predeterminado del enrutador del ISP.

Configurar la conexión a la Intranet

La conexión a la Intranet se establece a través de un adaptador de LAN instalado en el equipo servidor.

Necesita configurar TCP/IP con los siguientes valores en el adaptador para LAN:

- La dirección IP y la máscara de subred asignadas por el administrador de la red.
- Los servidores de nombres DNS de los servidores de nombres de la Intranet corporativa.

Configurar el servidor de acceso remoto como enrutador de una Intranet corporativa

Para que el servidor de acceso remoto reenvíe el tráfico correctamente en la Intranet corporativa, debe configurarlo como un enrutador con rutas estáticas o protocolos de enrutamiento de manera que se pueda tener acceso a todas las ubicaciones de la Intranet desde el servidor de acceso remoto.

Configurar el servidor de acceso remoto para clientes PPTP

En primer lugar, debe habilitar el servidor de acceso remoto para su configuración. Si desea permitir que varios clientes PPTP tengan acceso a la Intranet corporativa, debe configurar los valores siguientes:

- **Seguridad**
  - **Métodos de autenticación**

    Seleccione los métodos de autenticación que admite el servidor de acceso remoto para autenticar las credenciales de los clientes de acceso telefónico. Normalmente, los clientes de acceso telefónico a redes utilizan la autenticación MS-CHAP. Los clientes de acceso telefónico a redes que no son de Microsoft utilizan la autenticación CHAP, SPAP y PAP. En las conexiones PPTP cifradas, debe utilizar MS-CHAP como método de autenticación.

  - **Proveedor de cuentas**

    Puede registrar la actividad de los clientes de acceso telefónico para realizar el análisis o la contabilidad, si selecciona y configura un proveedor de cuentas.

- **IP**

  Si se encuentra disponible algún servidor DHCP que asigne direcciones IP de Intranet, deberá seleccionar uno para la asignación a los clientes VPN. En caso contrario, se deberá configurar un conjunto de direcciones estáticas y máscara que se asignan dinámicamente a los clientes VPN basados en PPTP.

  Si el conjunto de direcciones IP estáticas representa una subred independiente, debe agregar una ruta IP estática compuesta por {dirección IP, máscara} del conjunto de direcciones de acceso remoto a los enrutadores de la Intranet. Si no se

agrega esta ruta, los clientes VPN basados en PPTP no podrán recibir tráfico de los recursos de la Intranet.

Configurar los puertos PPTP

Todos los puertos PPTP se enumeran como puertos independientes en una lista de Puertos de Enrutamiento y acceso remoto. Todos los puertos PPTP se deben configurar para el acceso remoto.

Configurar filtros PPTP

Para proteger al servidor de acceso remoto del envío o recepción de tráfico de la interfaz de Internet que no sea tráfico PPTP procedente de los clientes de acceso remoto, es necesario configurar filtros de entrada y salida PPTP en la interfaz del servidor de acceso remoto que corresponde a la conexión a Internet.

Puesto que el enrutamiento IP está habilitado en la interfaz de Internet, si no se configuran filtros PPTP en la interfaz de Internet del servidor de acceso remoto, todo el tráfico recibido en la interfaz de Internet se enruta, por lo que posiblemente se reenviará tráfico de Internet no deseado a la Intranet.

2.3.6. Funcionamiento de la seguridad en el intento de conexión

Los pasos siguientes describen qué ocurre durante el intento de conexión de un cliente VPN basado en PPTP con un servidor VPN basado 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 se supone que 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.

2.4. Seguridad del protocolo Internet IPSec

La Seguridad de protocolo de Internet (IPSec) es una protección eficaz para las redes privadas contra ataques desde Internet, a la vez que se facilita el uso. 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.

IPSec provee la capacidad de proteger la comunicación entre grupos de trabajo, equipos de redes de área local, clientes y servidores, sucursales físicamente remotas, extranets, clientes itinerantes y administración remota de equipos.

Seguridad de red

La implementación de IPSec en el nivel de transporte IP (capa de red 3) 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 3, como *Secure Sockets Layer* (SSL), sólo proporcionan seguridad en las aplicaciones que saben cómo utilizar SSL, como por ejemplo los exploradores de Web. Debe modificar todas las demás aplicaciones para proteger las comunicaciones con SSL.

La implementación de IPSec en la Capa de red 3 proporciona protección para todos los protocolos IP y de capa superior en el conjunto de protocolo TCP/IP, como por ejemplo 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 utilizan 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.)

2.4.1. 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. 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.

IPSec reduce significativamente la posibilidad de que se produzcan ataques a través de la red gracias a características como las siguientes:

Administración automática de claves

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.

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.

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.

Servicios de seguridad

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 matemáticas 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.

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.

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.

Encadenamiento de bloques de cifrado (CBC, *Cipher Block Chaining*) permite ocultar modelos de bloques de datos idénticos en un paquete sin aumentar el tamaño de los datos después del cifrado. Los modelos de cifrado repetidos pueden comprometer la seguridad al proporcionar una pauta que puede utilizar un intruso para intentar descubrir la clave de cifrado. Como primer bloque aleatorio se utiliza un vector de inicialización (un número aleatorio inicial) para cifrar y descifrar un bloque de datos. Para cifrar cada bloque se utilizan distintos bloques aleatorios junto con la clave secreta. Así se garantiza que se transformen conjuntos de datos idénticos no seguros en conjuntos únicos de datos cifrados.

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.

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.

2.4.2. Protocolos de seguridad de IPSec

Los protocolos de seguridad proporcionan protección de información e identidad para cada paquete de IP. IPSec define nuevos formatos de paquete: la cabecera de autentificación (AH), y el ESP (Carga útil de seguridad de encapsulación, *Encapsulating Security Payload*).

Encabezado de autenticación (AH)

AH proporciona autenticación, integridad y anti-repetición para el paquete entero (ambos el encabezado de IP y la información incluida en el paquete), AH firma el paquete entero. No cifra la información, por lo que no proporciona confidencialidad. La información es legible, pero está protegida contra modificaciones. AH utiliza algoritmos HMAC(Hash con claves para la autenticación de mensajes) para firmar el paquete.

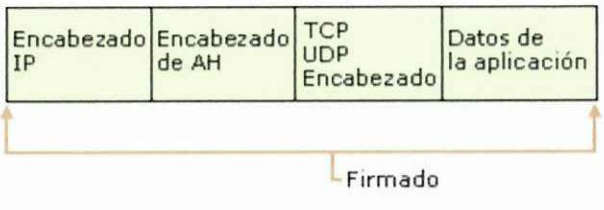


Figura 2.6: Ubicación del encabezado AH.

La Figura 2.6 muestra la ubicación del encabezado AH. La integridad y la autenticación se consiguen al situar el encabezado de AH entre el encabezado de IP y el encabezado de protocolo de transporte (TCP o UDP).

Carga de seguridad de encapsulación (ESP)

ESP proporciona confidencialidad, además de autenticación, integridad y anti-repetición. ESP no firma normalmente el paquete entero a no ser que se esté realizando un túnel. Por lo general, sólo se protege la información y no el encabezado de IP.

La seguridad se consigue al situar el encabezado de ESP entre el encabezado de IP y el encabezado de protocolo de transporte (TCP o UDP).

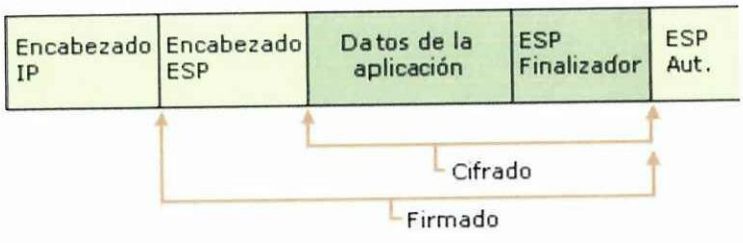


Figura 2.7: Ubicación del encabezado ESP.

2.4.3. Negociación de seguridad IPSec

Antes de que se pueda intercambiar información asegurada, ha de establecerse un contrato entre los dos equipos. A este contrato se le denomina asociación de seguridad (SA). En una SA, los dos equipos acuerdan el modo de intercambiar y proteger información.

Asociaciones de seguridad

Una asociación de seguridad (SA) es una combinación de una directiva y claves que definen los servicios, mecanismos y claves de seguridad comunes utilizados para proteger la comunicación de un lugar a otro. El índice de parámetros de seguridad (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 para determinar qué 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 y el Protocolo de administración clave (ISAKMP) y el protocolo de generación 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 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.

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:

1. **Negociación de directiva. Que 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.

2. **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.

3. **Autenticación**

   Los equipos que intentan autenticar el intercambio de información clave. Si se produce un error en la autenticación, no se puede proceder con la comunicación. Se utiliza la clave principal, junto con los algoritmos negociados en el Paso 1. 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 seguridad.

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.

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 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.

2.4.4. Funcionamiento de IPSec

Para simplificar el funcionamiento, este ejemplo ilustra el IPSec de un equipo a otro. Usuario1, que utiliza una aplicación en el equipo A, envía un mensaje a Usuario2 en el equipo B (Ver Figura 2.8).

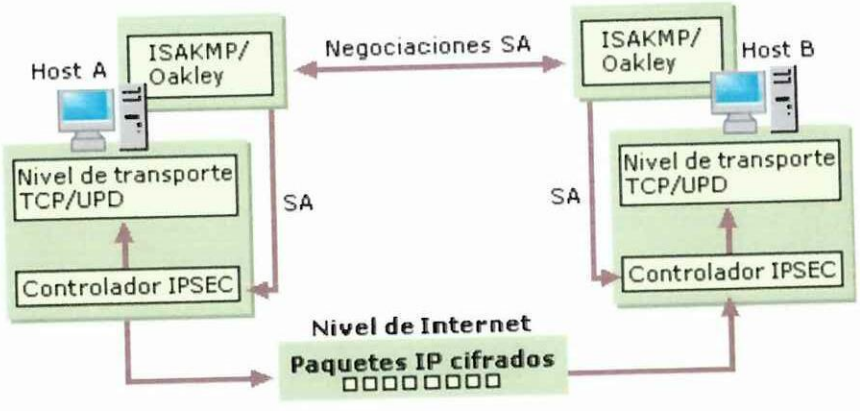


Figura 2.8: Esquema representativo del funcionamiento de IPSec.

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.

Usuario1 y usuario2 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.

2.4.5. Modos de IPSec

IPSec define dos modos de operación los cuales se explican a continuación:

- El modo **transporte** 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** 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).

2.4.6. Redes Privadas Virtuales con IPSec

Todo el proceso de encapsulación, enrutamiento y desencapsulación se denomina *túnel*. El túnel oculta, o encapsula, el paquete original dentro de un paquete nuevo. Este paquete puede contener información nueva de dirección y enrutamiento, que permite al nuevo paquete viajar a través de redes. Si el túnel se combina con la privacidad, los datos del paquete original (así como el origen y el destino originales) no se muestran a los que escuchan el tráfico en la red. La red puede ser cualquier conjunto de redes: una red Intranet privada o Internet. Cuando los paquetes encapsulados llegan a su destino, se quita el encabezado de encapsulación y se utiliza el encabezado original del paquete para enrutar éste a su destino final.

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, se puede utilizar para proporcionar 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 la encapsulación 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 sólo la encapsulación del tráfico IP.

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.

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.

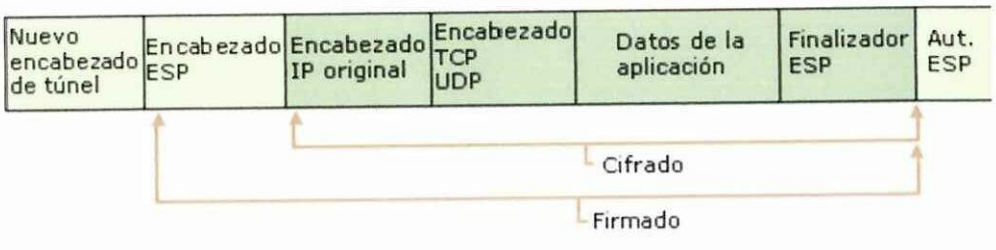


Figura : Representación de un túnel ESP.

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.

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.

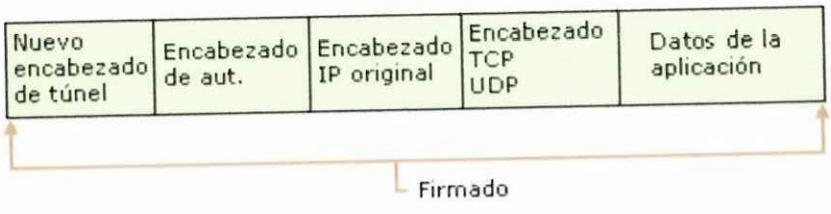


Figura 2.10: Representación de un túnel AH.

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.

Los túneles IPSec ofrecen seguridad sólo para el tráfico IP. El túnel está configurado para proteger el tráfico entre dos direcciones IP o dos subredes IP. Si

se utiliza el túnel entre dos hosts en lugar de entre dos puertas de enlace, la dirección IP externa será la misma que la dirección IP interna.

2.5. Protocolo de túnel de capa 2 (L2TP)

El Protocolo de túnel de capa 2 (L2TP), *Layer Two Tunneling Protocol*) es un protocolo de túnel basado en RFC destinado a convertirse en el estándar del sector. A diferencia de PPTP, L2TP no utiliza el Cifrado punto a punto de Microsoft (MPPE, *Microsoft Point-to-Point Encryption*) para cifrar datagramas PPP. L2TP utiliza la Seguridad de protocolos Internet (IPSec) para los servicios de cifrado. La combinación de L2TP e IPSec se conoce como L2TP sobre IPSec.

La Figura 2.11 muestra la representación del L2TP

Figura 2.11: Representación del L2TP.

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

L2TP sobre IPSec proporciona los servicios VPN principales de encapsulación y cifrado de datos privados. sobre IPSec proporciona los servicios VPN principales de encapsulación y cifrado de datos privados.

2.5.1. Técnica de Encapsulación del protocolo L2TP

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

1. Encapsulación 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. Encapsulación IPSec

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

La Figura 2.12 muestra la encapsulación L2TP e IPSec para un datagrama PPP.

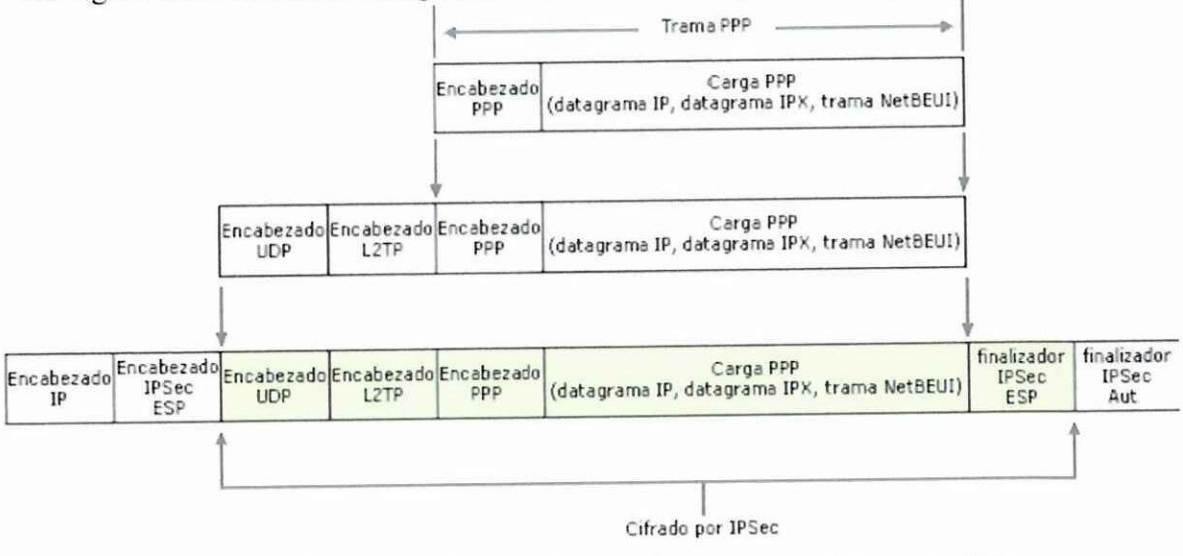


Figura 2.12: Encapsulación L2TP e IPSec para un datagrama PPP.

2.5.2. 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.

2.5.3. VPN de acceso remoto basadas en L2TP

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 Internet. Si desea que el servidor de acceso remoto admita varias conexiones L2TP sobre IPSec, realice los pasos siguientes:

- Configurar la conexión a Internet.
- 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 2.13 muestra los elementos de un servidor de acceso remoto que proporciona acceso remoto basado en L2TP a una Intranet corporativa.

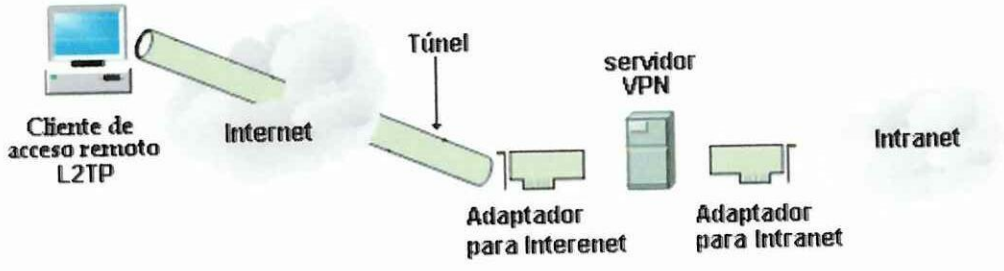


Figura 2.13: Elementos de una VPN basada en L2TP.

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. A continuación se explican cada uno de los pasos anteriores

Configurar la conexión a Internet

La conexión a Internet desde el servidor VPN es una conexión dedicada lo que significa que un adaptador para WAN está instalado en el equipo. Normalmente, el adaptador para WAN es un adaptador T1, T1 fraccionario, Frame Relay o DSL.

Se necesita establecer la siguiente configuración de TCP/IP en el adaptador para WAN:

- La dirección IP y la máscara de subred asignadas por InterNIC o por un proveedor de servicios Internet (ISP).
- La puerta de enlace o gateway predeterminado del enrutador del ISP.

Configurar la conexión a la Intranet

La conexión a la Intranet desde un Servidor VPN se establece a través de un adaptador de LAN instalado en el equipo.

Necesita configurar TCP/IP con los siguientes valores en el adaptador para LAN:

- La dirección IP y la máscara de subred asignadas por el administrador de la red.
- Los servidores de nombres DNS y WINS de los servidores de nombres de la Intranet corporativa.

Configurar el servidor de acceso remoto como enrutador de una Intranet corporativa

Para que el servidor de acceso remoto reenvíe el tráfico correctamente a la Intranet corporativa, se debe configurar como un enrutador con rutas estáticas o protocolos de enrutamiento de manera que se pueda tener acceso a todas las ubicaciones de la Intranet desde el servidor de acceso remoto.

Configurar el servidor de acceso remoto para clientes L2TP

En primer lugar, hay que habilitar el servidor de acceso remoto. Si desea permitir que varios clientes L2TP tengan acceso a la Intranet corporativa, se configuran los valores siguientes:

- **Seguridad**

- **Métodos de autenticación**

  Seleccionar los métodos de autenticación que admite el servidor de acceso remoto para autenticar las credenciales de los clientes de acceso remoto. En el caso de que sean clientes de acceso remoto de Microsoft, utilizan normalmente la autenticación MS-CHAP.

- **Proveedor de cuentas**

  Para registrar la actividad de los clientes de acceso remoto para propósitos de análisis o de contabilidad se selecciona y configura un proveedor de cuentas.

- **IP**

Si se encuentra disponible algún servidor DHCP que asigne direcciones IP de Intranet, deberá seleccionar uno para la asignación a los clientes VPN. En caso contrario, se deberá configurar un conjunto de direcciones estáticas y máscara que se asignan dinámicamente a los clientes VPN basados en L2TP.

Si el grupo de direcciones IP estáticas está compuesto por intervalos de direcciones IP que constituyen una subred independiente, tendrá que habilitar un protocolo de enrutamiento IP en el equipo servidor de acceso remoto o agregar rutas IP estáticas que consten de {Dirección IP, Máscara} de cada intervalo para los enrutadores de la Intranet. Si no se agregan estas rutas, los clientes VPN basados en L2TP no podrán recibir transmisiones de los recursos de la Intranet.

Configurar los puertos L2TP

Todos los puertos L2TP se enumeran como puertos independientes en una lista de Puertos de Enrutamiento y acceso remoto. Todos los puertos L2TP se deben configurar para el acceso remoto.

Configurar filtros L2TP sobre IPSec.

Para proteger al servidor de acceso remoto del envío o recepción de tráfico de la interfaz de Internet que no sea tráfico L2TP sobre IPSec procedente de los clientes de acceso remoto, es necesario configurar filtros de entrada y salida L2TP sobre IPSec en la interfaz del servidor de acceso remoto que corresponde a la conexión a Internet.

Puesto que el enrutamiento IP está habilitado en la interfaz de Internet, si no se configuran filtros L2TP sobre IPSec en la interfaz de Internet del servidor de acceso remoto, todo el tráfico recibido en la interfaz de Internet se enruta, por lo que posiblemente se reenviará tráfico de Internet no deseado a la Intranet.

2.5.4. Funcionamiento de la 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, el Protocolo de administración de claves y asociación de seguridad Internet (ISAKMP, *Internet Security Association and Key Management Protocol*) 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.

En los pasos 3 a 5 se supone que 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.

La seguridad una vez realizada la conexión

Después de pasar la autorización y la autenticación, y tras conectar a la LAN, los clientes VPN de conexiones VPN de acceso remoto sólo pueden tener acceso a los recursos de la red para los que tengan permisos. Los clientes VPN de acceso remoto están sujetos a la seguridad, tal como si estuvieran en la oficina. Es decir, los clientes VPN de acceso remoto no pueden hacer nada para lo que no tengan los derechos suficientes ni pueden tener acceso a los recursos para los que no tienen permisos.

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.

Puede restringir el acceso de los clientes VPN de acceso remoto a sólo los recursos compartidos del servidor VPN y no a la red a la que está conectado el servidor VPN.

Por lo tanto, un 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.

Capítulo III

3.1. El sistema operativo Windows 2003 Advanced Server como servidor VPN

En Windows 2003 Advanced Server se configura el servicio VPN a través del Servicio de enrutamiento y acceso remoto que incorpora el mismo, el cual proporciona lo siguiente:

- 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.

En la siguiente sección se aborda con mayor profundidad las características del servicio anterior.

3.1.1. Servicio de enrutamiento y acceso remoto

El Servicio de enrutamiento y acceso remoto es un servicio integrado único que finaliza las conexiones procedentes de clientes de acceso telefónico o VPN, o proporciona enrutamiento (IP, IPX y AppleTalk), o realiza ambas tareas a la vez. Mediante el Servicio de enrutamiento y acceso remoto, el servidor de Windows 2003 puede funcionar como un servidor de acceso remoto, un servidor VPN, una puerta de enlace o un enrutador de sucursal.

Cuando se proporciona 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 físico, relé de trama, 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. El Servicio de enrutamiento y acceso remoto admite los protocolos de control de enrutamiento OSPF y RIP2 para redes IP. El intervalo de servicios de enrutamiento y de puerta de enlace incluido en Windows 2003 Advanced Server permite crear conexiones flexibles entre las sucursales

(o redes periféricas) y la red corporativa y también entre enrutadores internos de una Intranet.

Información general acerca del enrutamiento en Windows 2000

Se le denomina enrutador de Windows 2000 al equipo que ejecuta Windows 2003 Server y el servicio de enrutamiento y acceso remoto, que suministra servicios de enrutamiento LAN y WAN.

El enrutador de Windows 2000 está diseñado para ser usado por administradores de sistema familiarizados con los protocolos y servicios de enrutamiento. Mediante el enrutamiento y acceso remoto, los administradores pueden ver y administrar enrutadores y servidores de acceso remoto en sus redes.

A continuación se mencionan 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.

3.2. Componentes de las redes privadas virtuales de Windows 2000

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 2003 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 Protocolo de túnel punto a punto (PPTP, *Point-to-Point Tunneling Protocol*) o un cliente de Protocolo de túnel de capa 2 (L2TP, *Layer Two Tunneling Protocol*) con seguridad de Protocolo Internet (IPSec, *Internet Protocol Security*) que no sean de Microsoft.

- **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 2003 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.

La Figura 3.1 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.

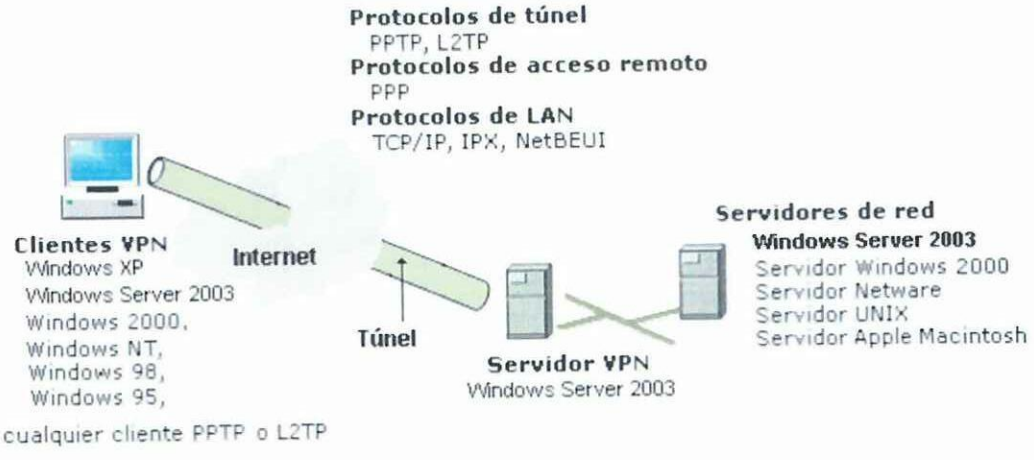


Figura 3.1 Componentes de las redes privadas virtuales de Windows 2000.

En las secciones siguientes se describirán todos los posibles tipos de conexiones VPN en una Intranet basadas en los protocolos PPTP y L2TP, los cuales se implementaron obteniendo magníficos resultados. Estos tipos son los de acceso de clientes VPN de acceso remoto a redes privadas y conexión de redes privadas virtuales de enrutador a enrutador. En los ejemplos, las redes privadas corresponderán con la parte segura de las redes de los departamentos de Recursos Humanos.

3.3. Conexión de clientes de acceso remoto a VPNs mediante PPTP

La Figura 3.2 muestra el esquema representativo de la VPN de acceso remoto basada en PPTP.

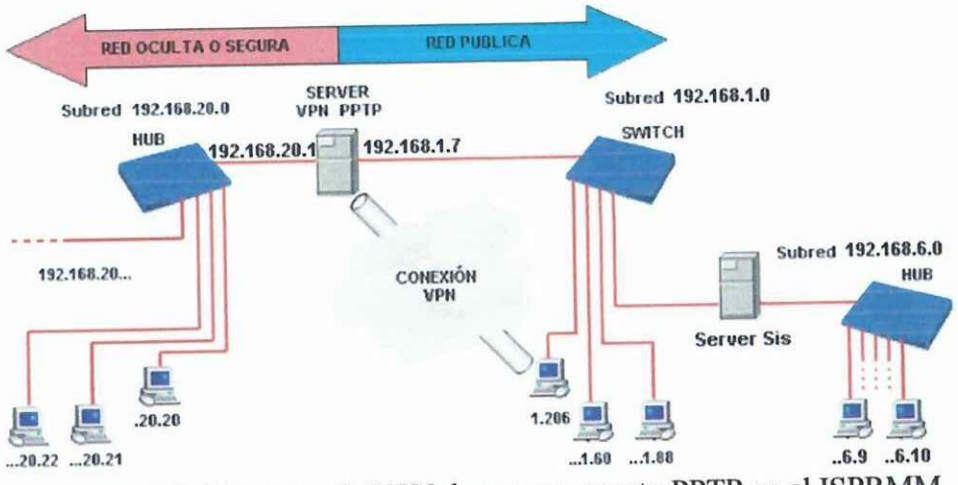


Figura 3.2: Esquema de VPN de acceso remoto PPTP en el ISPRMM

La subred 192.168.20.0/24 representa la red del departamento de Recursos Humanos, y constituye la red a proteger. La red restante, constituye la red pública, que incluye, entre otras, las subredes 192.168.1.0 y la 192.168.6.0.

El servicio de enrutamiento y acceso remoto tiene varias opciones de configuración. Para configurar un servidor VPN, en todas las implementaciones se deberá escoger la opción *Servidor de Red Privada Virtual* como muestra la Figura 3.3. En estos casos como el objetivo es acceder a una red privada desde una red pública, el servidor de Windows 2003 Server tendrá que ser un sistema multitarjeta, o sea, dispondrá de dos tarjetas interfaces de red para su conexión con cada red.

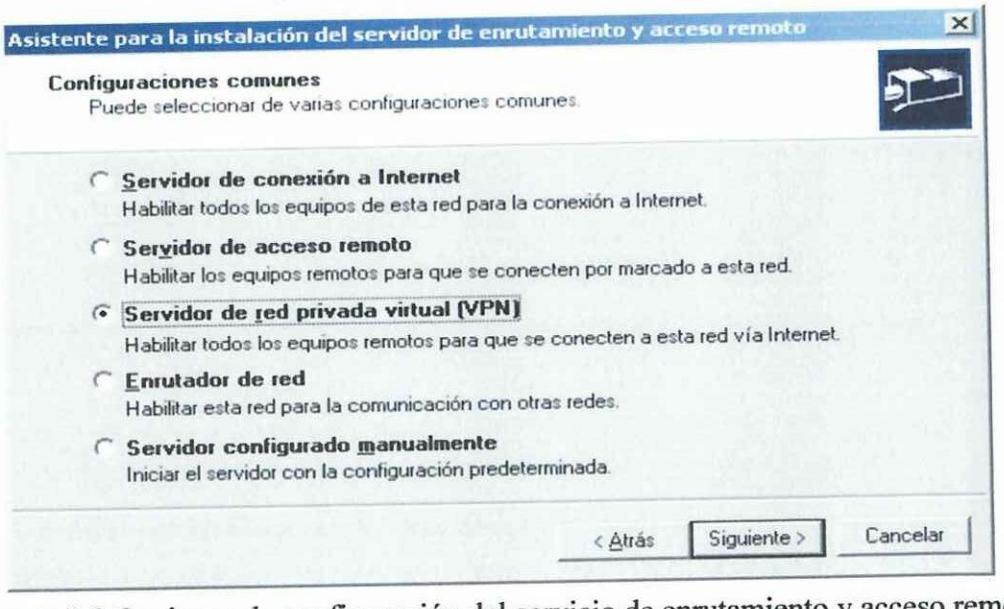


Figura 3.3 Opciones de configuración del servicio de enrutamiento y acceso remoto.

Los clientes VPN deben estar asignados a una red para el direccionamiento, el acceso por marcado telefónico y otros propósitos, por lo que se deberá escoger la conexión de red apropiada para tal objetivo. La conexión de red a escoger tendrá que ser aquella que da la cara a la red pública, que es la subred con dirección de red 192.168.1.0/24, por lo que se escoge la interfaz con dirección IP 192.168.1.7 (Figura 3.4). A esta interfaz solo tendrán acceso los clientes VPN.

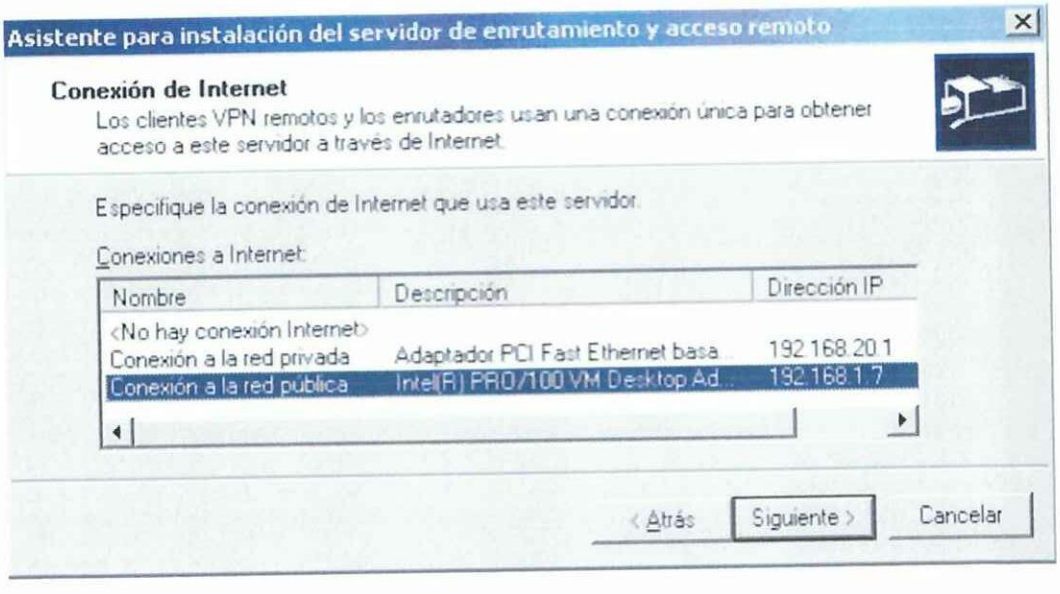


Figura 3.4 Selección de la interfaz para el acceso VPN.

Adicionalmente se deberá escoger el método de asignación de las direcciones IP a los clientes, que puede ser de forma automática o a través de un intervalo de direcciones especificado de forma manual. En el primer caso, que es la opción escogida para la implementación, puede usar un servidor DHCP para asignar las direcciones en cuyo caso se debe asegurar de que está configurado correctamente, si no se utiliza este servidor generará las direcciones de forma aleatoria. Hay que tener en cuenta que para que el relevo de mensajes DHCP desde un cliente de acceso remoto sea compatible, se deberán configurar las propiedades del **Agente de retransmisión DHCP** con la dirección IP del servidor DHCP. El agente de retransmisión DHCP es el componente del servicio de **RRAS** que le indica al servidor VPN cual va a ser el servidor DHCP que brindará servicio a los clientes de acceso remoto VPN.

El servicio DHCP para la red privada va a estar corriendo en el mismo servidor VPN pero sobre la interfaz de red con dirección IP 192.168.20.1. Las opciones configuradas son las siguientes:

- Rango IP: 192.168.20.40 a 192.168.20.80
- Máscara: 255.255.255.0
- Puerta de enlace: 192.168.20.1
- Servidor DNS: 192.168.20.1
- Servidor WINS: 192.168.20.1

En la Figura 3.5 se ilustra la ventana de administración del servicio de enrutamiento y acceso remoto una vez terminado el proceso de configuración.

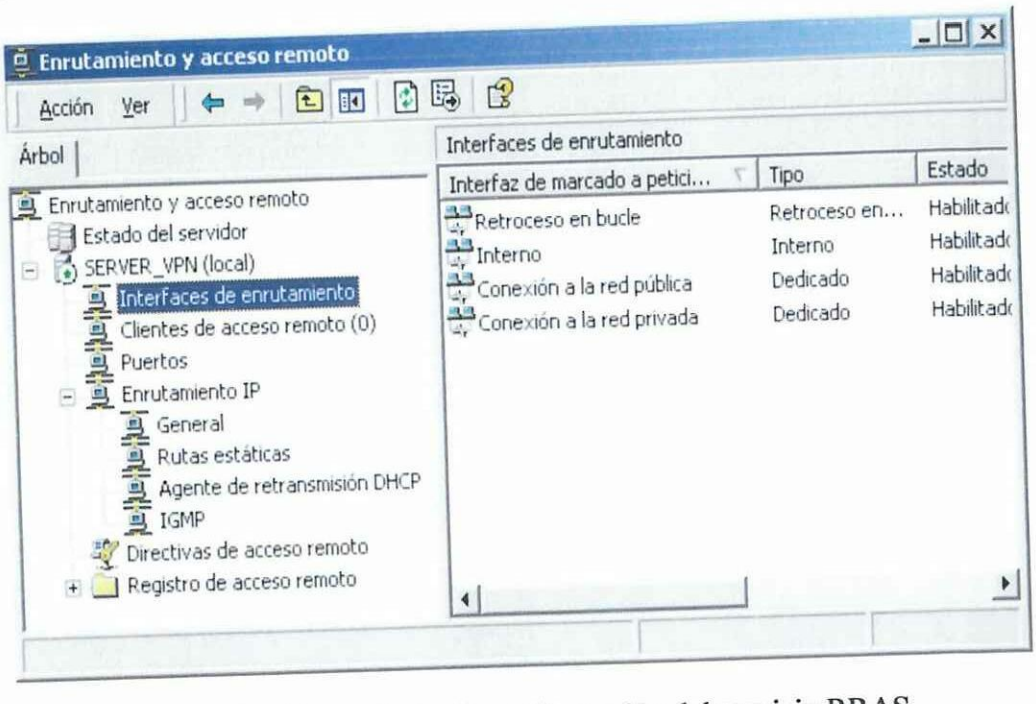


Figura 3.5 Herramienta de configuración del servicio RRAS.

El número de puertos PPTP y L2TP predeterminado es cinco. Para varios clientes VPN de acceso remoto, es posible que cinco puertos no sean suficientes por lo que se deberán agregar los puertos suficientes mediante la opción *Puertos.*

Mediante las directivas de acceso remoto, se crea una directiva que requiera que las conexiones VPN de acceso remoto utilicen un método de autenticación y refuerzo de cifrado específicos.

Por ejemplo, se puede crear un grupo de Windows 2000 llamado *Usuarios VPN* cuyos miembros sean las cuentas de los usuarios que crean conexiones VPN de acceso remoto a través de Internet. A continuación, se puede crear una directiva que contenga las siguientes condiciones: **Tipo de puerto NAS** establecido como **Virtual (VPN)** y **Grupo de Windows** establecido como **Usuarios VPN,** y la condición **Tunnel-Type** en **Protocolo de túnel punto a punto.** Finalmente, debe configurar el perfil de la directiva para seleccionar un método de autenticación, un método de cifrado y un nivel de cifrado específicos. La configuración predeterminada de cifrado admite todos los niveles de cifrado y permite que no haya cifrado.

Para requerir el cifrado, hay que desactivar la opción **Sin cifrado** y seleccione los niveles de cifrado adecuados en la ficha **Cifrado** del perfil de la directiva de acceso remoto. Los niveles de cifrado son:

- **Básico:** Esta opción se utiliza si establece comunicaciones con clientes de acceso telefónico a redes de Microsoft antiguos. En esta opción se utiliza el Cifrado punto a punto de Microsoft (MPPE) y una clave de cifrado de 40 bits.
- **Seguro**: Esta opción se utiliza si establece comunicaciones con clientes de acceso telefónico a redes de Windows 2000 y Windows 98. En esta opción se utiliza MPPE y una clave de cifrado de 56 bits.
- **El más seguro**: Con esta opción se utiliza MPPE y una clave de cifrado de 128 bits por lo que se añade mayor seguridad. Esta opción sólo está disponible en las versiones de Windows 2000 para Norteamérica

Una vez hecho esto el servidor VPN ya está listo para brindar servicio a clientes VPN de acceso remoto PPTP.

3.3.1. Comprobaciones realizadas

Primeramente se configuró en una PC de la red pública, con dirección IP 192.168.1.25 (206)una conexión de red con la opción **Conectar a una red privada a través de Internet**, en este caso Internet es la Intranet ISPRMM, por ser conexiones basadas en Intranet (Figura3.6).

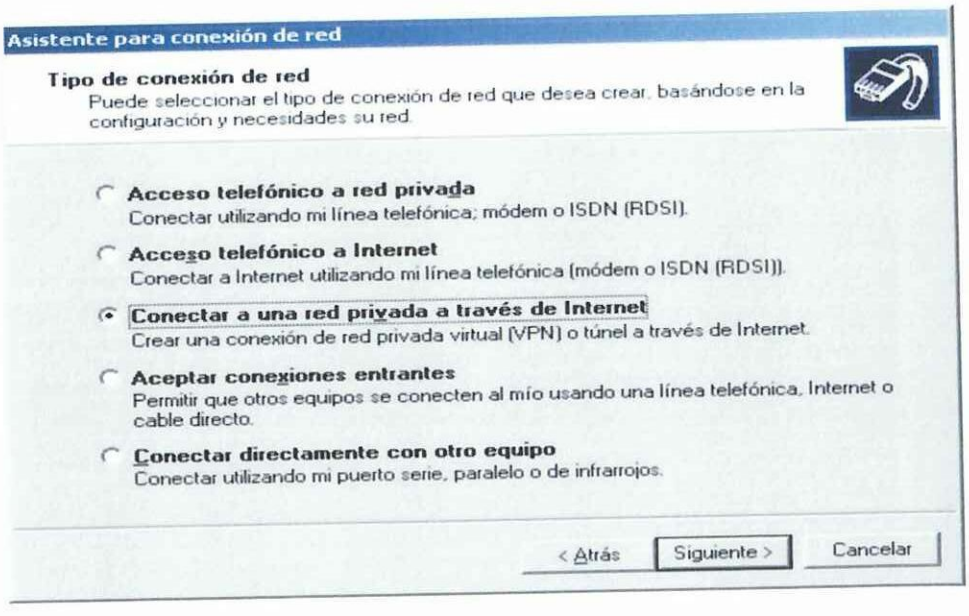


Figura 3.6 Opciones de configuración del cliente de acceso remoto.

Posteriormente se elige el nombre o la dirección IP del servidor VPN que sería la 192.168.1.7 (Figura 3.7).

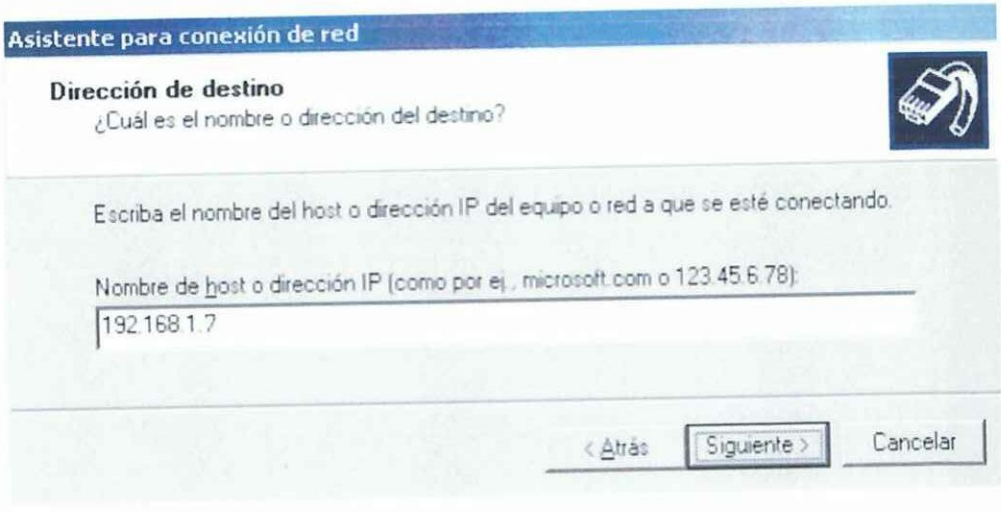


Figura 3.7 Selección del servidor VPN PPTP.

En las propiedades de la conexión creada en la ficha **Funciones de red** se escoge el tipo de servidor al que se llama, en este caso PPTP, y los protocolos de red disponibles para la conexión VPN (Figura 3.8).

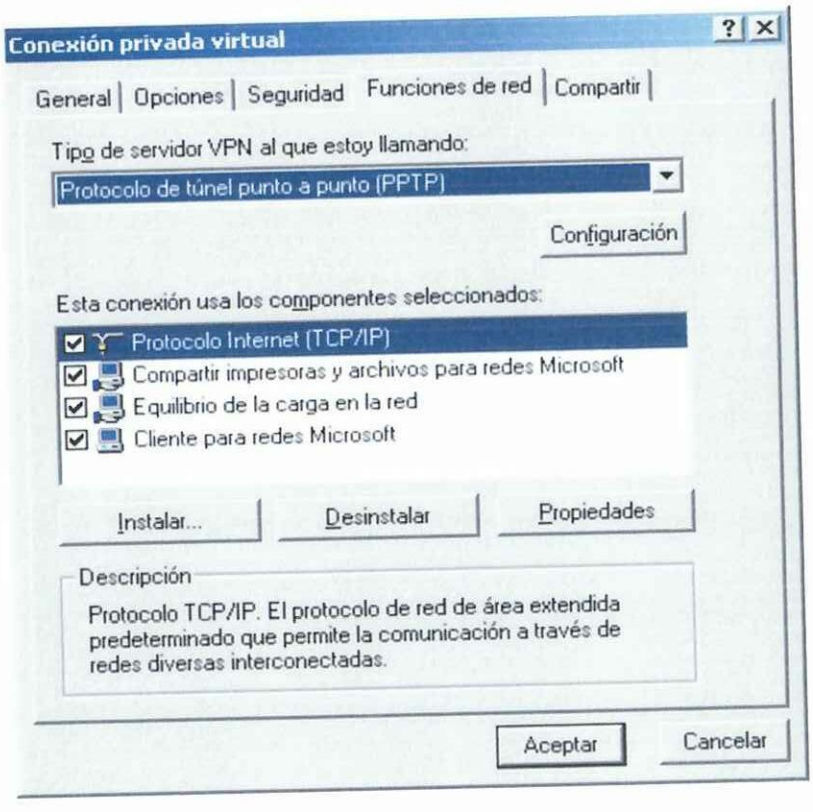


Figura 3.8 Selección del tipo de servidor VPN.

Una vez hecho esto solo basta poner las credenciales y conectar. Si todo ha funcionado bien, se indica que se ha establecido la conexión.

Los resultados de la conexión, como Tipo de servidor, transporte, autenticación, cifrado, IP del servidor y del cliente, entre otros, se muestran en la Figura 3.9. Como se puede observar, la dirección IP asignada pertenece a la subred oculta o segura y ésta fue asignada por el servidor DHCP corriendo en el mismo equipo que el servidor VPN; esto, dado porque en la lista de servidores DHCP en el ***Agente de retransmisión DHCP*** se encuentra la dirección IP 192.168.20.1.

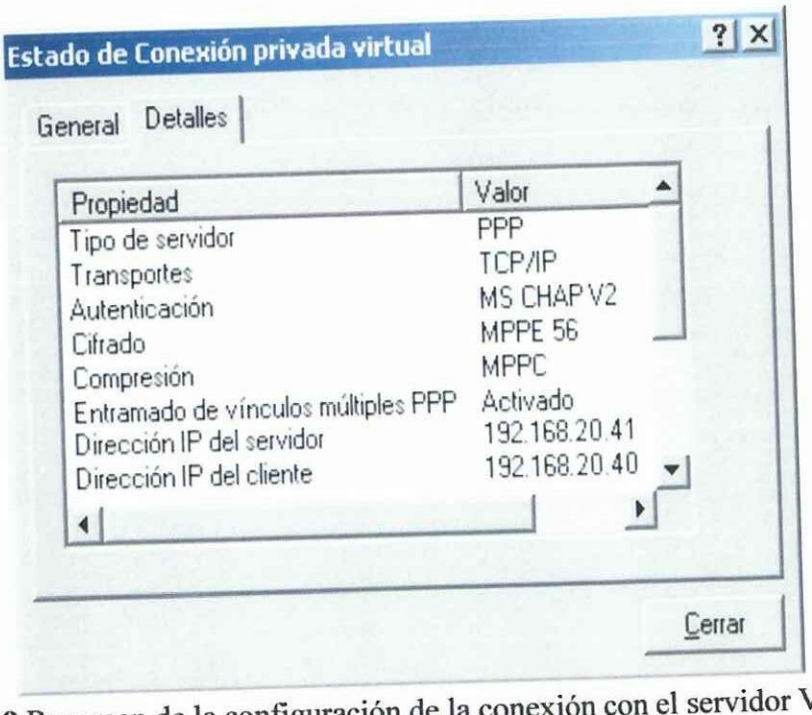


Figura 3.9 Resumen de la configuración de la conexión con el servidor VPN PPTP.

Antes de la conexión se pudo comprobar, a través de comando **ping**, que no existía conexión, como es lógico, con ninguna de las PCs de la red segura, con dirección IP de la red 192.168.20.0 (Figura 3.10).

Después de la conexión ya se cuenta con una conexión a la máquina destino como muestra la Figura 3.11.

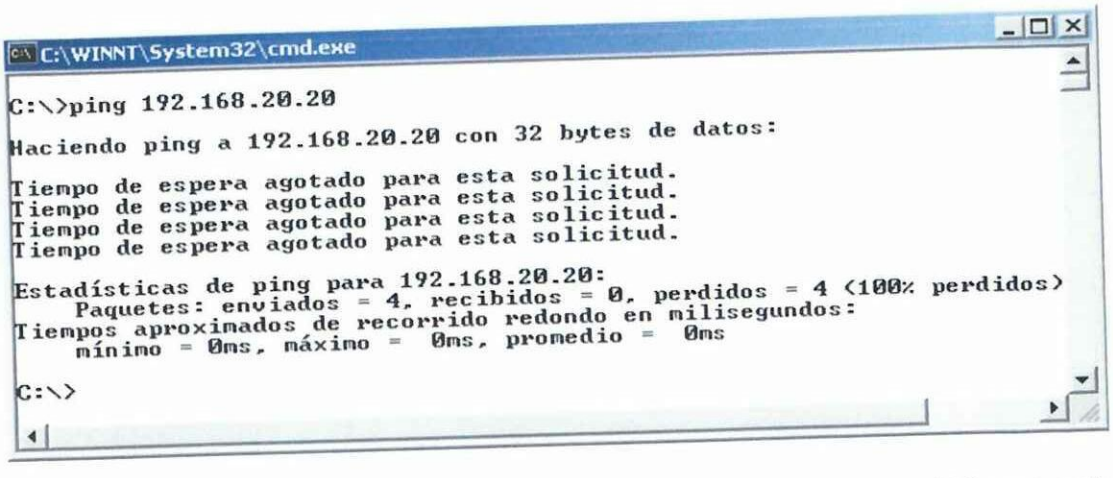


Figura 3.10 Respuesta del comando ping cuando intenta conectarse a una PC segura sin establecer la conexión VPN.

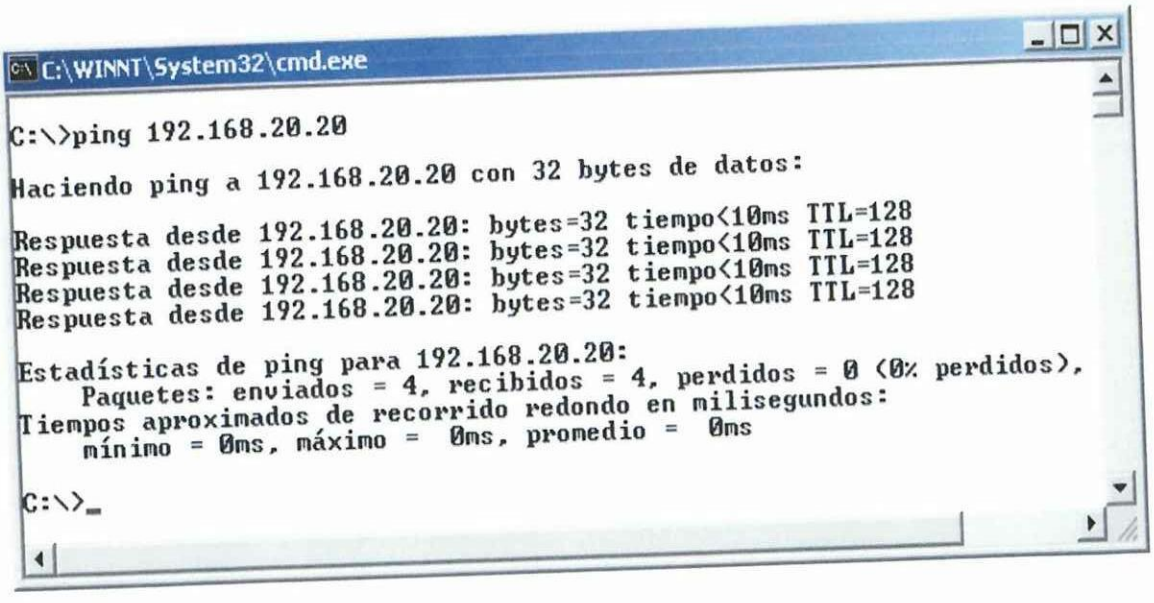


Figura 3.11 Respuesta del comando ping cuando intenta conectarse a una PC segura, una vez establecida la conexión VPN.

De esta forma se demuestra que solo a través de una conexión VPN se tiene acceso a todas las PCs de la red segura.

3.4. Conexión de dos redes privadas virtuales de enrutador a enrutador basada en PPTP

La Figura 3.12 muestra el esquema representativo de la VPN de enrutador a enrutador basada en PPTP, planteada en esta investigación. En este caso van a existir dos redes privadas con direcciones de red 192.168.20.0 y 192.168.6.0 que representan, respectivamente, las redes de Recursos Humanos y del departamento Económico.

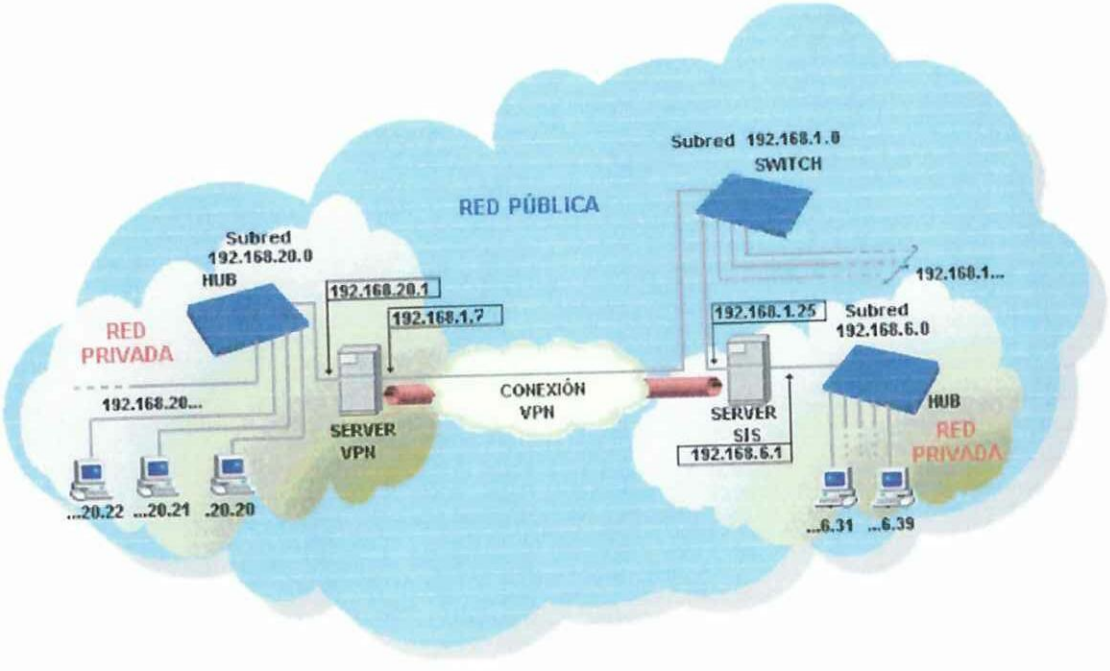


Figura 3.12 Esquema de VPN PPTP de enrutador a enrutador en ISPRMM.

Las dos redes privadas se conectan, utilizando sus enrutadores VPN, mediante un túnel VPN PPTP que se extiende sobre la subred pública 192.168.1.0.

Para crear esta conexión VPN de enrutador a enrutador basada en PPTP y enviar datos privados a través de la red pública en la Intranet ISPRMM (red 192.168.1.0/24), hay que seguir los siguientes pasos:

1. Configurar el enrutador de Windows 2000 que se encuentra en el departamento económico para que reciba conexiones PPTP desde el enrutador del departamento de recursos humanos.
2. Configurar el enrutador de Windows 2000 del departamento de recursos humanos para que inicie una conexión PPTP con el enrutador del departamento económico.
3. Iniciar la conexión PPTP desde cualquier enrutador, en este caso se escogió el de recursos humanos.

En las siguientes secciones se describen los pasos anteriores.

3.4.1. Configurar el enrutador del departamento económico

Para que el enrutador de Windows 2000 del departamento económico admita la conexión PPTP del otro departamento hay que realizar lo siguiente:

- Configurar la conexión a la Intranet.
- Configurar la conexión a la red privada.
- Configurar el enrutador del departamento económico.
- Configurar los puertos PPTP.
- Configurar las interfaces de marcado a petición.
- Configurar las rutas estáticas.
- Configurar las directivas de acceso remoto.

Configurar la conexión a la Intranet

Se configuran los siguientes valores en la configuración de TCP/IP:

- Dirección IP: 192.168.1.98
- Máscara de subred:255.255.255.0
- Puerta de enlace: Nula, puesto que los dos servidores están conectados directamente a la misma subred (192.168.1.0/24)

Configurar la conexión a la red privada

Se configuran los siguientes valores en la configuración de TCP/IP:

- Dirección IP: 192.168.20.1
- Máscara de subred:255.255.255.0
- Servidores DNS y WINS: 192.168.20.1

Configurar el enrutador del departamento económico

Para permitir que el enrutador de recursos humanos tenga acceso a la red privada, se debe configurar los valores siguientes:

- Activar casillas de verificación ***Enrutador y Enrutamiento LAN y de marcado a petición*** (Figura 3.13).

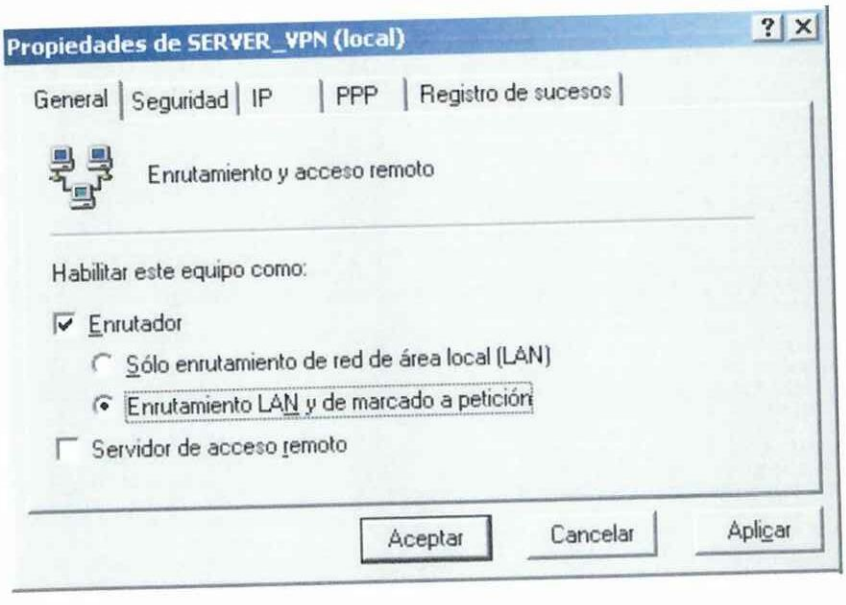


Figura 3.13 Modos de funcionamiento del enrutador de Windows 2000 Server.

- **Elementos de Seguridad**
    - **Métodos de autenticación:** Aquí se seleccionan los métodos de autenticación que admite el enrutador de recursos humanos para autenticar las credenciales de los enrutadores de marcado a petición. Se selecciona la autenticación MS-CHAPv2 preferiblemente o EAP-TLS (si se dispone de tarjetas inteligentes o certificados de equipo).
- **Elementos del protocolo IP:** Activar casillas de verificación ***Habilitar enrutamiento IP y Permitir conexiones de marcado a petición y acceso remoto basado en IP***. En caso de utilizar asignación estática de direcciones IP se debe seleccionar ***Conjunto de direcciones estáticas*** y configurar los intervalos de direcciones IP que se asignan dinámicamente a los clientes VPN basados en PPTP. En este caso se seleccionó DHCP.
- **Protocolo PPP:** Se debe activar la casilla de verificación ***Extensiones del Protocolo de control de vínculos*** (LCP) y ***Compresión de software.***

Configurar los puertos PPTP

De manera predeterminada, todos los puertos de un enrutador de Windows 2000 están configurados para **Conexiones de enrutamiento de marcado a petición (de entrada y salida)**, por lo que no es necesario establecer ninguna configuración adicional.

Configurar la interfaz de marcado a petición

Las interfaces de marcado a petición vienen siendo el elemento fundamental para lograr la conexión. Éstas se crean con el Asistente para interfaz de marcado a petición, donde se configuran los valores siguientes:

- **Nombre de interfaz:** Es el nombre de la interfaz que representa la conexión al departamento de recursos humanos. En este caso, se nombró ***conexiónvpnRH***.
- **Tipo de conexión:** Se selecciona ***Conectar usando red privada virtual (VPN).***
- **Tipo de VPN:** Se selecciona Protocolo de túnel punto a punto (PPTP).
- **Dirección de destino:** Puesto que el enrutador del departamento económico no iniciará la conexión VPN, no se requiere ninguna dirección IP.
- **Credenciales de acceso telefónico de salida**: Puesto que el enrutador del departamento económico no iniciará la conexión VPN, escriba cualquier nombre, dominio y contraseña.
- **Credenciales de acceso telefónico de entrada**: Se escribe el dominio y la contraseña de la cuenta que se utilizará para autenticar el enrutador de recursos humanos. El Asistente para interfaz de marcado a petición crea automáticamente la cuenta y configura su permiso de acceso remoto como **Permitir acceso**. El nombre de la cuenta es el mismo que el de la interfaz de marcado a petición. Por ejemplo, para el enrutador del departamento de recursos humanos, el nombre de la cuenta es ***conexiónvpnRH***.

Configurar rutas estáticas

Se necesita agregar rutas estáticas para que se reenvíe el tráfico al departamento de recursos humanos mediante la interfaz de marcado a petición apropiada. Se debe

seleccionar la interfaz de marcado a petición que corresponda al departamento de recursos humanos. Los valores de la ruta estática son los siguientes:

- Interfaz: conexiónvpnRH
- Destino: 192.168.6.0
- Máscara de red: 255.255.255.0
- Métrica: 1

Puesto que la conexión PPTP es una conexión punto a punto, no es posible configurar la dirección IP de la puerta de enlace.

Configurar directivas de acceso remoto

Si se desea conceder acceso remoto al enrutador de recursos humanos basado en PPTP, en función de la pertenencia a grupos, hay que hacer lo siguiente:

1. Crear un grupo de Windows 2000 cuyos miembros puedan crear conexiones de redes privadas virtuales con el servidor VPN. Por ejemplo, EnrutadorRemoto.
2. Agregar al grupo de Windows 2000 las cuentas de usuario que correspondan a las cuentas que utilizan enrutador remoto.
3. Crear una nueva directiva de acceso remoto con las propiedades siguientes:
    - En **Nombre de directiva** escribir **Acceso VPN si es miembro de EnrutadorRemoto** (por ejemplo).
    - Asignar **EnrutadorRemoto** a la condición **Grupos-Windows** (ejemplo).
    - Asignar **Virtual (VPN)** a la condición **Tipo de Puerto NAS.**
    - Asignar **Protocolo de túnel punto a punto (PPTP)** a la condición **Tipo de túnel.**
    - Activar la opción **Conceder permiso de acceso remoto.**
4. Si este equipo sólo se utiliza para proporcionar conexiones VPN de enrutador a enrutador, debe eliminar la directiva predeterminada de acceso remoto llamada **Permitir el acceso si está habilitado el permiso de acceso telefónico.** En caso

contrario, mueva la directiva de acceso remoto predeterminada para que se evalúe en último lugar.

La configuración predeterminada no permite cifrado a ningún nivel. Para requerir el cifrado, desactive la opción **Sin cifrado** y seleccione los niveles de cifrado apropiados en la ficha **Cifrado** del perfil de directiva de acceso remoto que utilizan los enrutadores de llamada.

3.4.2. Configurar el enrutador del departamento de recursos humanos

El enrutador de Windows 2000 del departamento de recursos humanos iniciará la conexión PPTP con el enrutador del departamento, para ello se ejecutan los pasos siguientes:

- Configurar la conexión a la Intranet.
- Configurar la conexión a la red privada del departamento de recursos humanos.
- Configurar la interfaz de marcado a petición.
- Configurar las rutas estáticas.

Configurar la conexión a la Intranet

Se configuran los siguientes valores en la configuración de TCP/IP:

- Dirección IP: 192.168.1.25
- Máscara de subred:255.255.255.0
- Puerta de enlace: Nula, puesto que los dos servidores están conectados directamente a la misma subred (192.168.1.0/24).

Configurar la conexión a la red privada del departamento de recursos humanos

Se configuran los siguientes valores en la configuración de TCP/IP:

- Dirección IP: 192.168.6.1
- Máscara de subred:255.255.255.0

- Sevidores DNS y WINS: 192.168.6.1

Configurar la interfaz de marcado a petición

- **Nombre de interfaz:** Es el nombre de la interfaz que representa la conexión al departamento económico. En este caso, se nombró ***conexiónvpnECO***.
- **Tipo de conexión:** Se selecciona ***Conectar usando red privada virtual (VPN).***
- **Tipo de VPN:** Se selecciona Protocolo de túnel punto a punto (PPTP).
- **Dirección de destino:** 192.168.1.7
- **Credenciales de acceso telefónico de salida**: Escribir el nombre, el nombre de dominio y la contraseña de la cuenta de usuario correspondiente al enrutador de la sucursal. Las credenciales son las mismas que se incluyeron en la opción. **Credenciales de acceso telefónico de entrada** del Asistente para la interfaz de marcado a petición, al crear la interfaz de marcado a petición correspondiente a este departamento en el enrutador del departamento económico. Por tanto el nombre sería ***conexiónvpnRH***, con la clave correspondiente

Configurar las rutas estáticas

Se necesita agregar una ruta estática para que se reenvíe el tráfico al departamento económico mediante la interfaz de marcado a petición apropiada. Se debe seleccionar la interfaz de marcado a petición que corresponda al departamento económico creada anteriormente. Los valores de la ruta estática son los siguientes:

- Interfaz: conexiónvpnECO
- Destino: 192.168.1.0
- Máscara de red: 255.255.255.0
- Métrica: 1

Puesto que la conexión PPTP es una conexión punto a punto, no es posible configurar la dirección IP de la puerta de enlace

3.4.3. Iniciar la conexión VPN PPTP de enrutador a enrutador

Para conectar el enrutador de recursos humanos con el enrutador del departamento económico, se deberá seleccionar la opción **Conectar** sobre la interfaz de marcado a petición creada que conecte con este último.

3.4.4. Comprobaciones realizadas

En este caso como se explicó anteriormente, las conexiones se realizan a través de las interfaces de marcado a petición creadas en ambos servidores. La interfaz en el enrutador de recursos humanos es quien inicia la conexión, conexión ésta que se vuelve bidireccional (en ambos sentidos) cuando se comprueba la identidad del enrutador que llama. La bidireccionalidad permite que ambas redes seguras tengan conexión, si ésta no se consigue el enrutador que llama será quien tenga conexión solamente.

Cuando se establece la conexión en ambos servidores VPN aparecen las interfaces de marcado a petición en modo ***Conectado*** (Figura 3.14 y 3.15). Al servidor de Recursos Humanos le es asignada por parte de su homólogo, la dirección IP 192.168.20.49. En la dirección opuesta, se le asignó al servidor del departamento Económico, la dirección IP 192.168.6.98.

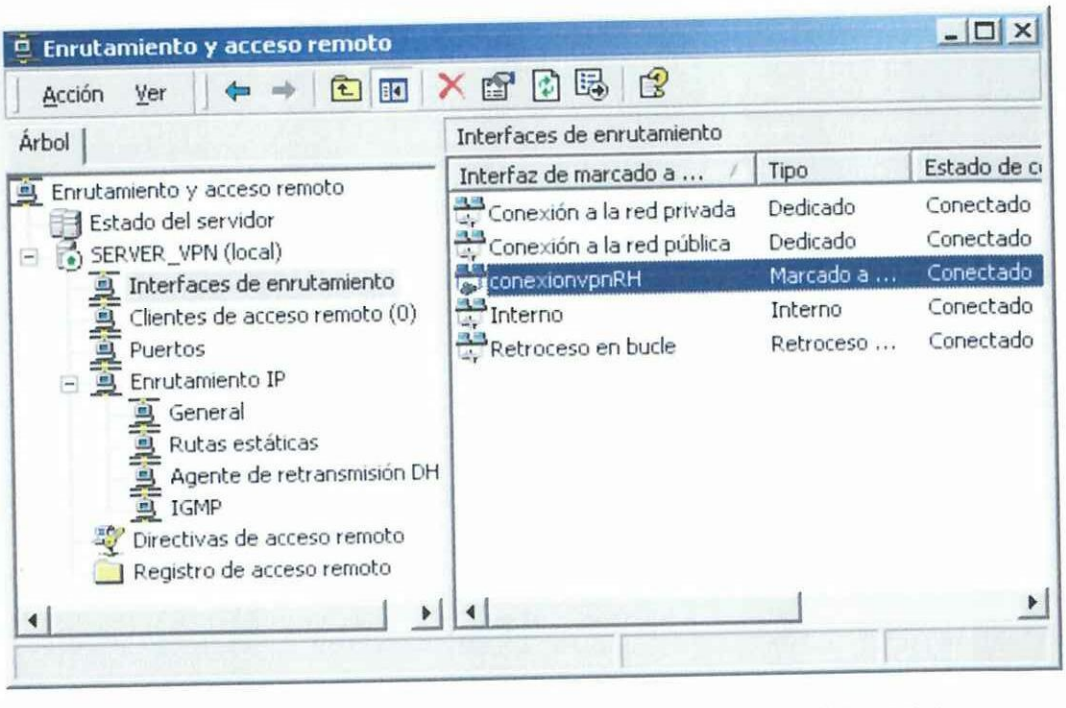


Figura 3.14 Estado de la interfaz de marcado a petición en el servidor del departamento Económico.

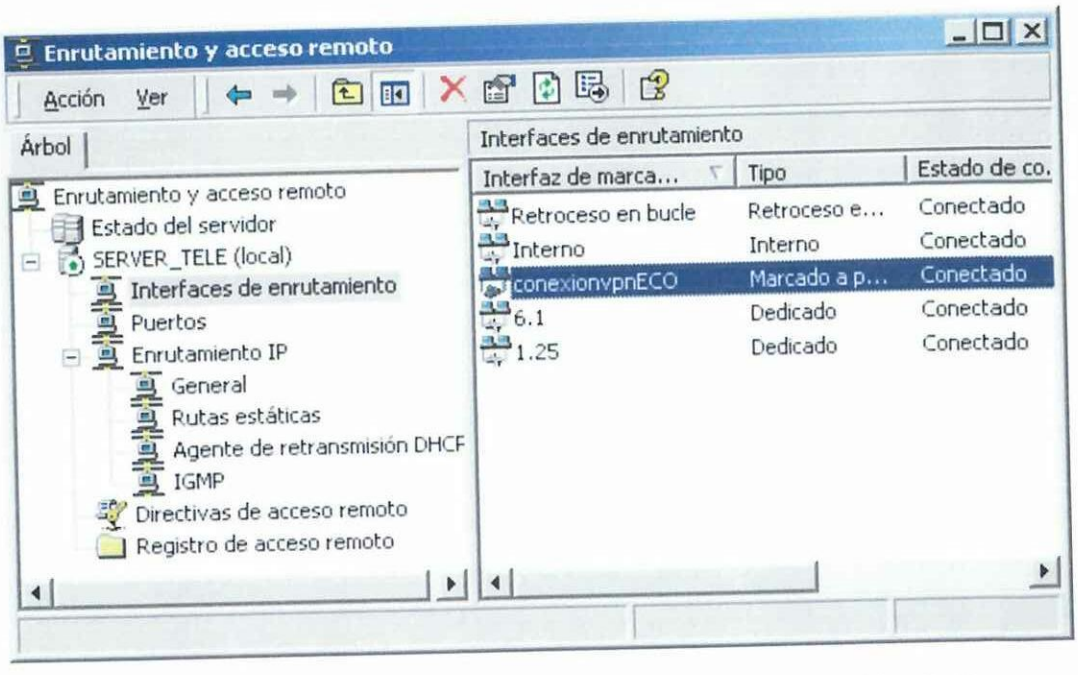


Figura 3.15 Estado de la interfaz de marcado a petición en el servidor de Recursos Humanos

La Figura 3.16 muestra la respuesta que se tiene con el comando ping que comprueba la conexión entre una PC de la subred segura 192.168.20.0 con otra de la subred 192.168.6.0. Dada la característica de éste comando se deduce la conectividad a la inversa. De esta forma se demuestra que solo a través de una conexión VPN ambas redes mantienen una conexión segura.

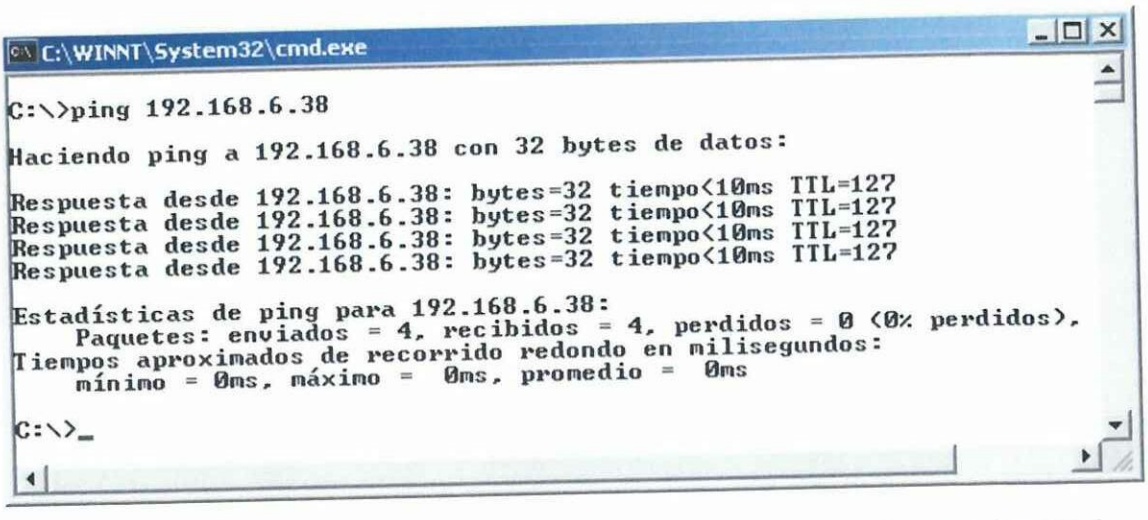


Figura 3.16 Respuesta al comando ping, al comprobar una conexión entre dos PC de redes privadas distintas.

Red Segura 1: 192.168.6.0	Red Segura 2: 192.168.20.0
PC Segura 1: 192.168.6.38 ServidorRH con conexión VPN: 192.168.20.49 (Asignada por servidor VPN ECO)	PC Segura 2: 192.168.20.20 ServidorECO con conexión VPN: 192.168.6.98 (Asignada por servidor VPN RH)
Cantidad de saltos entre redes seguras, en dirección a la red 192.168.20.0 1. ServidorRH 192.168.6.1 2. ServidorECO 192.168.6.98 3. Eco1 192.168.20.20	
Cantidad de saltos entre redes seguras, en dirección a la red 192.168.6.0 1. ServidorECO 192.168.20.1 2. ServidorRH 192.168.20.49 3. Eco2 192.168.6.38	

Tabla 3.1 Resumen de saltos IP de red segura a red segura.

En la Tabla 3.1 se muestra un resumen de las direcciones IP de clientes y servidores y la cantidad de saltos que da un paquete desde una red privada hasta la otra; estas pruebas se hicieron con el comando tracert que marca la ruta que toma el paquete entre una estación de la red privada 192.168.6.0 hasta la otra red privada 192.168.20.0.

3.5. Conexión de clientes de acceso remoto a VPNs mediante L2TP

La Figura 3.17 muestra el esquema representativo de la VPN de acceso remoto basada en L2TP. El enfoque en este ejemplo es el mismo que en el caso de acceso remoto VPN por PPTP visto en la sección 3.4.

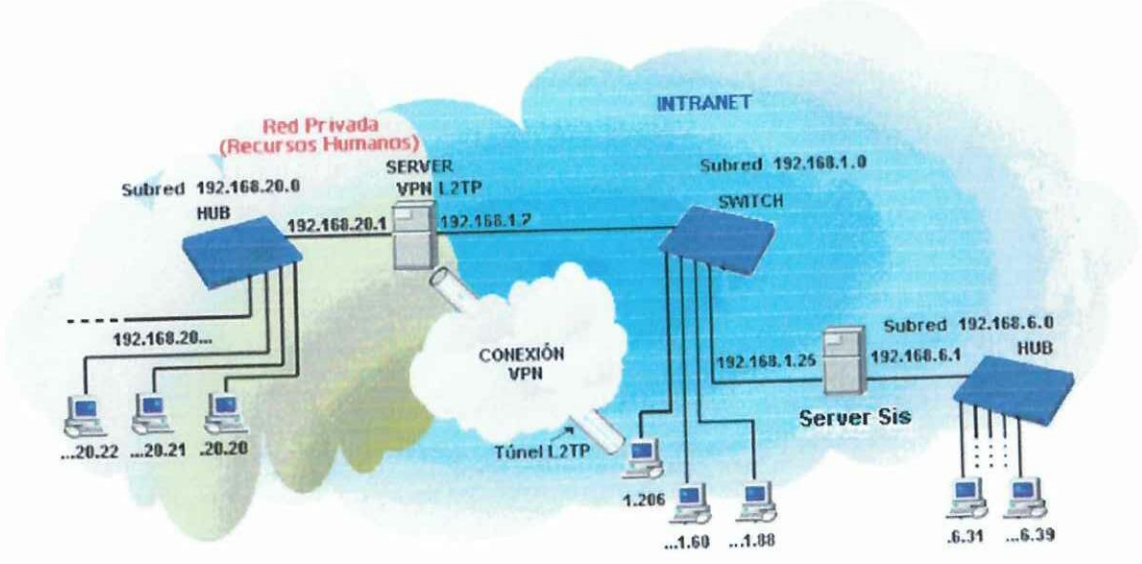


Figura 3.17 Esquema de VPN de acceso remoto PPTP en ISPRMM.

La configuración de un servidor VPN de acceso remoto basado en L2TP es muy parecida al de PPP por lo que se detallarán las diferencias medulares.

Todos los puertos L2TP se enumeran como puertos independientes en la lista **Puertos** de Enrutamiento y acceso remoto, por lo que se debe configurar todos los puertos L2TP para el acceso remoto, también es posibles nuevos puertos L2TP adicionales.

Para configurar una directiva de acceso remoto que controle las opciones de autenticación y cifrado para las conexiones VPN, se crea una directiva de acceso remoto con la configuración siguiente:

- Opción **Nombre de directiva: Acceso VPN** (ejemplo).
- En las condiciones, se establece la condición **Tipo-Puerto-NAS** en **Virtual (VPN)** y la condición **Tunnel-Type** (Tipo de túnel) en **Protocolo de túnel de capa 2**.
- Para la configuración de los perfiles, seleccione las opciones de cifrado y autenticación adecuadas.

La configuración predeterminada de cifrado admite todos los niveles de cifrado y permite que no haya cifrado. Para requerir el cifrado, hay que desactivar la opción **Sin**

cifrado y seleccionar los niveles de cifrado adecuados en la ficha **Cifrado** del perfil de la directiva de acceso remoto. Los niveles de cifrado son:

- **Básico:** Se utiliza cifrado DES de 56 bits.
- **Seguro:** Se utiliza cifrado DES de 56 bits.
- **El más seguro**: Esta opción utiliza cifrado DES triple (3DES) y ofrece el mayor grado de seguridad. Esta opción sólo está disponible en las versiones de Windows 2000 para Norteamérica

Cómo se explicó en el Capítulo II en configuraciones VPN con L2TP es necesario que cada equipo, cliente y servidor, tengan al menos un certificado digital de equipo instalado asignados por una entidad emisora de certificados de confianza. En una red Microsoft se puede configurar un servidor *Windows 2003 Server* como una entidad emisora de certificados que puede brindar servicio a toda la institución. El componente administrativo que implementan estos servidores para tal objetivo son los *Servicios de Certificate Server.*

3.5.1. Solicitud de certificados a un servidor con Servicios de *Certificate Server*

Las solicitudes de certificados las debe hacer el usuario, el equipo o el servicio que tiene acceso a la *clave privada* asociada con la *clave pública* que formará parte del certificado. Dependiendo de las directivas de clave pública establecidas por el administrador del sistema, los equipos y servicios pueden solicitar automáticamente certificados sin la intervención del usuario. Principalmente, hay dos formas de solicitar, explícitamente, certificados en Windows 2000.

Solicitar certificados mediante el Asistente para petición de certificados

Cuando solicite certificados de una *entidad emisora de certificados de empresa* de Windows 2000, se puede utilizar el Asistente para petición de certificados que se encuentra en el complemento Certificados. Este asistente establece los siguientes pasos:

- Seleccionar la entidad emisora de certificados a la que enviará la solicitud. Sólo las entidades emisoras de certificados de empresa que estén disponibles en un

dominio de Windows podrán emitir certificados mediante el Asistente para petición de certificados.

- (Opcional) Utilizar **Opciones avanzadas** en el Asistente para petición de certificados con el fin de seleccionar el proveedor de servicios criptográficos (CSP) para la pareja de claves asociada con la solicitud de certificados.

Solicitar los certificados mediante las páginas Web de los Servicios de Certificate Server de Windows

Cada entidad emisora de certificados instalada en un servidor de Windows 2000 tiene páginas Web a las que los usuarios tienen acceso para enviar solicitudes de certificados básicas y avanzadas. De forma predeterminada, estas páginas se encuentran en http://*nombreServidor*/certsrv, donde *nombreServidor* es el nombre del servidor de Windows 2000 que aloja a la entidad emisora de certificados.

Cuando solicite certificados de una entidad emisora de certificados independiente de Windows 2000, utilice las páginas Web de los Servicios de Certificate Server. También se pueden utilizar las páginas Web para solicitar certificados de las entidades emisoras de certificados de empresa de Windows 2000 si desea establecer características de solicitud opcionales que no estén disponibles en el Asistente para petición de certificados.

Procesar solicitudes de certificados

Cuando envíe una solicitud de certificado a una entidad emisora de certificados de empresa de Windows 2000, se procesará inmediatamente, en lugar de dejarse "pendiente". La solicitud de certificado fracasará o se concederá inmediatamente. Si se concede, se emite el certificado y se le pide que lo instale.

Cuando envíe una solicitud de certificado a una entidad emisora de certificados independiente de Windows 2000, se procesará inmediatamente o, de forma predeterminada, se considerará pendiente hasta que el administrador de la entidad emisora de certificados apruebe o rechace la petición. En el caso de una petición pendiente, el solicitante del certificado tendrá que utilizar las páginas Web de los Servicios de Certificate Server para comprobar el estado de los certificados pendientes.

Una vez obtenidos los certificados por las partes involucradas y establecer las configuraciones al servidor VPN ya se está listo para brindar servicio a clientes VPN de acceso remoto PPTP.

3.5.2. Comprobaciones realizadas

La configuración del cliente en este caso es análoga al caso de utilizar el protocolo PPTP, solo cambia el tipo de servidor al que se está llamando, o sea, L2TP. Otro elemento importante es que se deben contar con los certificados de equipos correspondientes.

Los resultados de la conexión, como Tipo de servidor, transporte, autenticación, cifrado, IP del servidor y del cliente, entre otros, se muestran en la Figura 3.18. La dirección IP, fue asignada por el servidor DHCP corriendo en el mismo equipo que el servidor VPN, y pertenece a la misma red que la red oculta o segura.

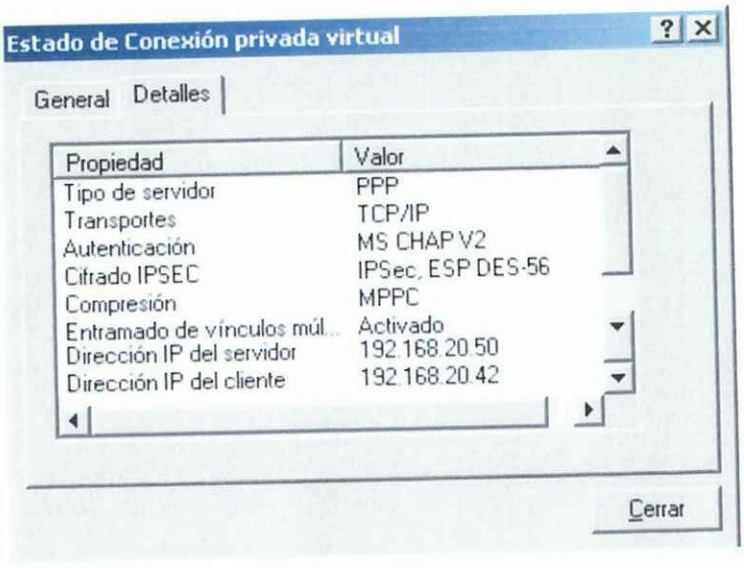


Figura 3.18 Resumen de la configuración de la conexión con el servidor VPN L2TP.

Igual se pudo comprobar a través del comando *ping* que solo mediante una conexión VPN se tiene acceso a las PCs privadas de la red segura.

3.5.3. Conexión de dos redes privadas virtuales de enrutador a enrutador basada en L2TP

La Figura 3.19 muestra el esquema representativo de la VPN de enrutador a enrutador basada en L2TP, planteada en esta investigación. La configuración es exacta al caso visto en la sección 3.5, solo cambia el tipo de túnel creado.

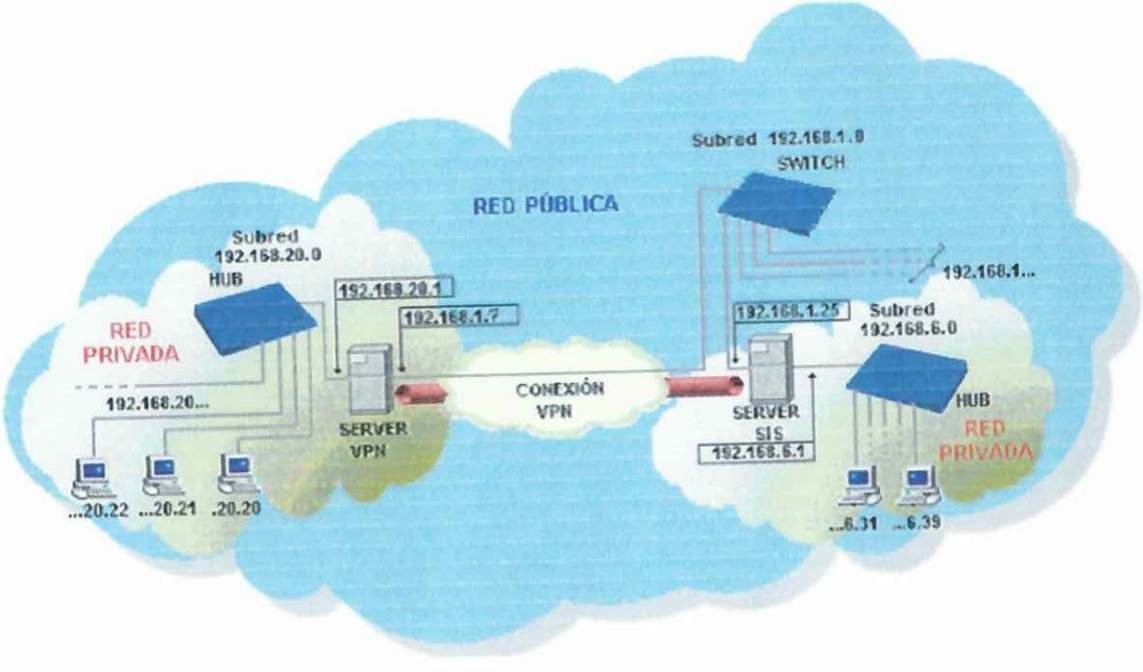


Figura 3.19 Esquema de VPN L2TP de enrutador a enrutador en la ISPRMM.

Los pasos a seguir para crear esta conexión VPN de enrutador a enrutador basada en L2TP y enviar datos privados a través de la red pública en la Intranet ISPRMM (red 192.168.1.0/24), son análogos a los de la conexión de enrutador a enrutador basada en PPTP, estos son los siguientes:

1. Configurar el enrutador de Windows 2000 que se encuentra en el departamento económico para que reciba conexiones L2TP desde el enrutador del departamento de recursos humanos.
2. Configurar el enrutador de Windows 2000 del departamento de recursos humanos para que inicie una conexión L2TP con el enrutador del departamento económico.

3. Iniciar la conexión L2TP desde cualquier enrutador, en este caso, como en el caso anterior se escogió el de recursos humanos.

En aras de no reiterar en las configuraciones de estos, solo se detallarán los aspectos medulares que lo diferencian de la conexión basada en PPTP.

Primeramente se deben instalar los certificados de equipo como se describió en la sección anterior.

En la configuración de ambas interfaces de marcado a petición, una en cada extremo de la conexión, se deberá escoger en **Tipo de VPN**, el tipo **Protocolo de túnel de capa 2 (L2TP)**.

En cuanto a las directivas de acceso remoto, si se desea conceder acceso remoto al enrutador de recursos humanos basado en L2TP, en función de la pertenencia a grupos, su configuración será igual al caso homólogo PPTP solo cambiaría el valor de la condición **Tipo de túnel** que sería **Protocolo de túnel de capa 2 (L2TP)**.

3.5.4. Comprobaciones realizadas

La conexión es análoga al caso visto con anterioridad basado en PPTP y se comprobó la conectividad en ambas direcciones mediante el comando ping.

3.6. Propuesta de VPN escogida

La ubicación real de los departamentos de recursos humanos y económicos hace que estos formen una única red de computadoras debido a que se encuentran en la misma edificación, pero en diferentes plantas, lo cual no es inconveniente por la cercanía en el plano vertical de los mismos.

Lo anterior hace descartar las posibilidades de conexión VPN del tipo enrutador a enrutador, quedaría escoger entre las opciones de acceso remoto VPN basado en PPTP o L2TP. La opción de configuración propuesta es la de conexión de acceso remoto VPN L2TP por ser ésta, como se explicó en el capítulo II, la que implementa mayor seguridad, al basarse en el protocolo IPSec.

Hay que destacar que no todas las máquinas de estos departamentos manejan información confidencial por lo que éstas pueden pertenecer a la red pública. Esto

podría ser muy importante puesto que las máquinas que pertenecen a la red privada nunca podrán acceder a los servicios públicos dentro de los que se destacan el Web, FTP, e-mail, entre otros, lo que podría traer inconvenientes a los trabajadores.

Una configuración más exacta para ésta red sería la representada en la Figura 3.21.

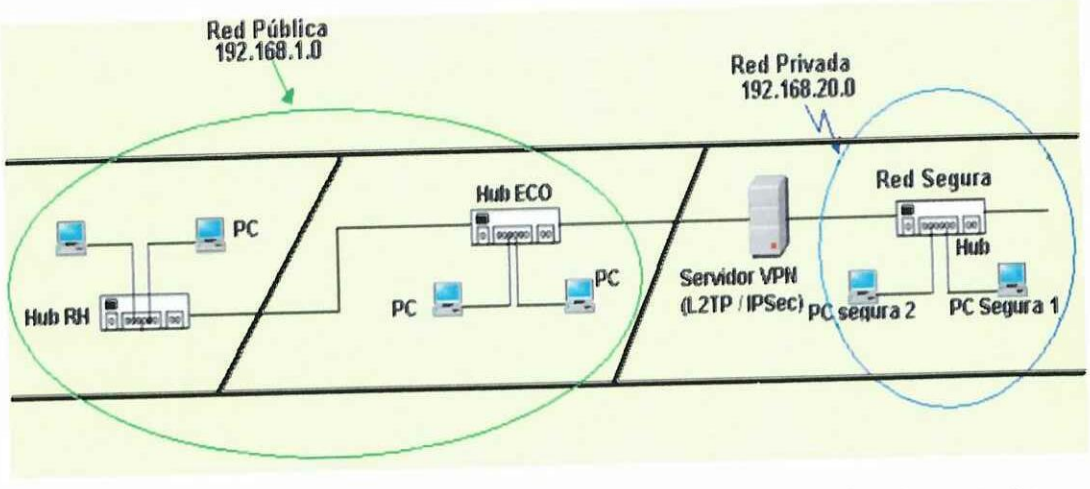


Figura 3.21 Configuración de Red VPN propuesta para su implementación.

Los componentes principales de la red de estos departamentos incluyendo la parte pública y la privada serían los siguientes:

- Tres Hubs (Hub1, Hub2, Hub3): Los dos primeros le dan conectividad a las PCs no seguras de cada departamento, por lo que están conectadas a la parte pública de la Intranet ISPRMM. El Hub3 le brinda conectividad a todas las PCs seguras y al servidor VPN.
- Servidor VPN multitarjeta: El servidor VPN se conecta a la red pública a través de una conexión con el Hub1 y a la red Privada mediante el Hub3.

En la figura anterior las PCs seguras se ubican a la derecha En caso de que la aplicación ASSETSS lo permita, los usuarios de recursos humanos que la utilicen podrían convertirse en clientes VPN del servidor y así ejecutar la aplicación de forma remota y segura.

Conclusiones

Conclusiones

Durante el desarrollo de este proyecto se han planteado los ejemplos necesarios que justifican y demuestran el cumplimiento de los objetivos trazados inicialmente, por lo que se pueden citar las siguientes conclusiones:

1. Los requerimientos de seguridad en las redes de datos han sido y serán uno de los factores esenciales para las empresas, en su elección de una arquitectura de red determinada.
2. Los servicios VPN IP tienen el potencial para convertirse en una solución viable para la consolidación de la seguridad en ambientes de Internet e Intranet.
3. La propuesta planteada de VPN para su implementación en el Instituto Superior Pedagógico, responde a las necesidades actuales con un mínimo de recursos.
4. Los escasos recursos con que cuenta el ISPRMM, unido a la mala concepción sobre seguridad, que implica un uso incorrecto de una PC que maneja información confidencial, harán difícil la temprana implementación de la propuesta dictada.
5. Dado que las VPN's utilizan una infraestructura pública de transporte, se tiene que implementar fuertes mecanismos de seguridad y encriptación para mantener la integridad de los datos.
6. Las VPN IP representan una solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos por lo que algunas organizaciones están implementando este tipo de tecnología.

Recomendaciones

Recomendaciones

1. Capacitar, en los principios básicos de seguridad informática, al personal de la institución que maneje información confidencial.

2. Implementar la propuesta planteada, como una solución a los requerimientos de seguridad existentes en el ISPRMM.

Bibliografia

Bibliografía

- Manuel J. Lucena López Criptografía y Seguridad en Computadores.
- Redes de Computadores tomo III Tercera edición Tanenbaum.
- Uyless D. Black, Redes de transmisión de datos y proceso distribuido, Edición Revolucionaria
- 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 año 2003.
- A. Mustapha H. Rudy, T. Tri. "MPLS: Valor Añadido para la interconexión", Revista de Telecomunicaciones de Alcatel año 2003.
- http://www.uv.es/ciuv/cas/vpn/
- http://www.google.com.cu/search?q=cache:ppW7hwjdCE8J:www.uniboyaca.edu.co/facingenieria/vpn.pdf+historia+vpn&hl=es&lr=lang_es&ie=UTF-8
- http://dis.eafit.edu.co/cursos/st-051/encapsulamiento.html
- http://tiny.uasnet.mx/prof/cln/ccu/marioREDES/node162.html
- http://www.portalmundos.com/software.htm
- http://www.portalmundos.com/mundogratis/encriptacion.htm
- http://www.ciberconta.unizar.es/LECCION/web/encriptar.htm.
- http://www.vpnsystems.com/main.htm
- http://www.monografías.com/trabajos11/intru/intru.shtml
- http://www.monografías.com/trabajos12/monvpn/monvpn.shtml

Bibliografía

- http://www.monografías.com/trabajos11/repri/repri.shtml
- http://www2.monografías.comcomputación/redes
- http://www.techidata.com.mx/servicios/att/vpn
- http://www2.ecocomputer.com/empresas/vpn/default.asp
- http://www.frases.org
- http://www.proverbia.net/citas_tematicas.asp?tematica=308