UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

E.A.P DE INGENIERÍA DE SISTEMAS

Implementación de una red privada virtual como alternativa para el acceso remoto a la red de datos de la Policía Nacional del Perú

Tesina

Para optar el Título de Ingeniero de Sistemas

AUTOR

Wilber Medina Jiménez

LIMA – PERÚ
2011

FICHA CATALOGRÁFICA

MEDINA JIMÉNEZ, Wilber

IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL COMO ALTERNATIVA PARA EL ACCESO REMOTO A LA RED DE DATOS DE LA POLICÍA NACIONAL DEL PERÚ

Redes de Computadoras (Lima, Perú 2011)

Tesina, Facultad de Ingeniería de Sistemas, Pregrado, Universidad Nacional Mayor De San Marcos

Formato 28 x 20 cm Paginas 115

DEDICATORIA:

"A todos los policías de vocación, que en su labor diaria tratan con dignidad e igualdad a la persona humana, sin distinción de raza, color, sexo, idioma, religión, opinión, política, origen nacional o social, posición económica, nacimiento o cualquier otra condición; plenamente convencidos que todos los hombres nacen libres e iguales".

AGRADECIMIENTOS

Primero y antes que nada, dar gracias a DIOS, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de esta etapa de mi vida.

A mis padres ***Roberto MEDINA RAMIREZ*** *y* ***Mery Luz JIMENEZ CARO*** *por su apoyo incondicional a lo largo de toda mi vida.*

A ***Miriam OJEDA JIMENEZ****, por ser la persona que comparte su vida y tiempo a mi lado, porque en su compañía las cosas malas se convierten en buenas, la tristeza se transforma en alegría y la soledad no existe.* ***TE AMO***

*A **Enrique SIERRA GOMEZ** por los momentos en los que más que un colega y compañero de trabajo, se comportó como un amigo.*

*Un agradecimiento especial al **Lic. Jorge Raúl DIAZ MUÑANTE** por la colaboración, paciencia, apoyo brindados en la elaboración del presente trabajo.*

En general quisiera agradecer a todas y cada una de las personas que han vivido conmigo la realización de esta tesina, con sus altos y bajos y que no necesito nombrar porque tanto ellas como yo sabemos que desde los más profundo de mi corazón les agradezco el haberme brindado todo el apoyo, colaboración, ánimo y sobre todo cariño y amistad.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADEMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL COMO ALTERNATIVA PARA EL ACCESO REMOTO A LA RED DE DATOS DE LA POLICÍA NACIONAL DEL PERÚ

Autor : MEDINA JIMÉNEZ, Wilber

Asesor : DIAZ MUÑANTE, Jorge Raúl

Titulo : Tesina, para optar el Título Profesional de Ingeniero de Sistemas

Fecha : Mayo del 2011

RESUMEN

La Policía Nacional del Perú se encuentra modernizando su red corporativa, y dentro de este proceso se halla mejorando y manteniendo en constante evolución los sistemas de información, seguridad y protección de su red.

Con este propósito y como una alternativa de acceso remoto a la red de datos policial se diseña Redes Privadas Virtuales para obtener conectividad entre los locales policiales a nivel nacional, partiendo del análisis de la red de datos existente.

La implementación contempla la selección de la tecnología, la adquisición, instalación, configuración de equipos y las pruebas de tráfico con los sistemas informáticos requeridos, con lo cual la VPN queda a disposición de los usuarios policiales.

Palabra Claves: Red Privada Virtual, VPN, Acceso Remoto, Red Corporativa.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADEMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

IMPLEMENTATION OF A VIRTUAL PRIVATE NETWORK AS AN ALTERNATIVE FOR REMOTE ACCESS TO DATA NETWORK OF THE NATIONAL POLICE OF PERU

Autor : MEDINA JIMÉNEZ, Wilber

Asesor : DIAZ MUÑANTE, Jorge Raúl

Titulo : Tesina, para optar el Título Profesional de Ingeniero de Sistemas

Fecha : Mayo del 2011

ABSTRACT

Peru's National Police is upgrading its corporate network, and within this process is constantly improving and maintaining information systems development, safety and security of your network.

To this end and as an alternative for remote access to police data network is designed for Virtual Private Network connectivity between local law enforcement nationwide, based on the analysis of existing data network.

The implementation includes the selection of technology, acquisition, installation, configuration and testing equipment for traffic information systems required, which the VPN is available to police users.

Key Words: Virtual Private Network, VPN, Remote Access, Corporate Network.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

CAPITULO II MARCO TEÓRICO

CAPITULO III ESTADO DEL ARTE METODOLÓGICO

CAPITULO IV DESARROLLO DE LA SOLUCIÓN O DEL ESTUDIO

INDICE DE TABLAS

INTRODUCCIÓN

En un pasado no muy lejano la prioridad era la necesidad de procesar y almacenar información, con lo que nacieron los equipos informáticos individuales entre otros, posteriormente surgió la necesidad no sólo de procesar y almacenar la información sino que además era preciso compartir la información en tiempo real entre distintos equipos informáticos, por ello surgieron las redes.

A medida que las redes de las organizaciones fueron creciendo se extendieron en distintos edificios, localidades, regiones y países, nuevamente surgió la necesidad de compartir la información entre los distintos puntos que se encontraban mucho más espaciados. Para cubrir esta demanda aparecen las redes de área extensa (WAN) implementándose las interconexiones de formas muy distintas (Conexión punto a punto, X25, Frame Relay, etc.). Finalmente aparece la red de redes, Internet, y rápidamente surgen aplicaciones que la utilizan como soporte para transmitir información bajo una cobertura de alcance mundial.

Las deficiencias en seguridad, falta de confidencialidad e integridad en las transmisiones sobre Internet, las costosas soluciones que implicaban los enlaces dedicados y nuevas necesidades como el Acceso Remoto a los recursos informáticos, provocaron el surgimiento de las Redes Privadas Virtuales (VPN - Virtual Private Network).

Una VPN es una tecnología que permite extender una red LAN como así también conectar distintas redes LANs para la transmisión segura de la información a través de un túnel, utilizando otra red como medio que generalmente es Internet.

Este Trabajo Final de Aplicación contempló el estudio de las tecnologías VPN, su aplicación a la solución de los principales problemas de conectividad remota segura en un caso concreto (La Red de Datos de la Policía Nacional del Perú) y la implementación de la solución propuesta.

CAPITULO I PLANTEAMIENTO METODOLÓGICO

1. ANTECEDENTES DEL PROBLEMA

La Policía Nacional del Perú (PNP), a través de la Dirección de Telemática, brinda soporte en el área de la informática y las telecomunicaciones a las Unidades Administrativas y Operativas policiales a nivel nacional, contribuyendo al mejoramiento de la eficiencia policial, mediante óptimo empleo de la tecnología. Para ello cuenta con una División de Informática la misma que administra la Red de Datos de la PNP (INTRANET PNP), cuyo Nodo Central o Centro de Cómputo está situada en la ciudad capital del país.

La INTRANET PNP interconecta Trescientos Sesenta y Ocho locales policiales a nivel nacional, los cuales el 70% se encuentran en la ciudad de Lima y el 30% en las principales ciudades del Perú. Cada local policial demanda el acceso a la INTRANET PNP y sus recursos informáticos que brinda: Sistema de Requisitorias de Personas, Sistema de Requisitorias de Vehículos, Sistema de Denuncias, Sistema de Planilla Virtual, Sistema Maestro Personal, entre otros. Tener acceso a estos sistemas de información sin duda elevaría la eficiencia y operatoria policial, contribuyendo a obtener una mejor calidad de vida para la sociedad y por ende realzar el prestigio e imagen institucional.

El problema es que los locales policiales interconectados constituyen sólo el 30% del total, Trescientos Sesenta y Ocho de Dos Mil aproximadamente, siendo en su mayoría los situados en provincias quienes requieren estar interconectados. Entonces surge la necesidad de ampliar la cobertura de la red a los locales policiales que lo demandan, pero el mayor problema está en la falta de presupuesto, pues interconectar los locales policiales faltantes con los tipos de enlace que actualmente se utiliza (Enlaces dedicados) resultaría un costo extremadamente elevado para la PNP.

Otro de los problemas que se tienen, es que se requiere interconectar a usuarios policiales móviles, posibilitando que tuvieran acceso a la red con independencia del tiempo o lugar donde se encontrarán; actualmente estos usuarios acceden a los datos que necesitan, mediante llamadas telefónicas dirigidas a locales policiales

interconectados, en ellos se encuentran operadores que se encargan de acceder a los datos de la red y comunicárselos a los usuarios móviles.

Por lo expuesto, es imprescindible la extensión de la INTRANET PNP, lo que permitiría la interconexión de locales policiales y usuarios móviles a nivel nacional.

2. DEFINICIÓN O FORMULACIÓN DEL PROBLEMA

Hoy en día, la información se ha convertido en el elemento más importante de una organización, sobre todo para aquellas que poseen sucursales o locales a nivel nacional, los cuales necesitan tener acceso a los sistemas de información y procesos en línea que reflejan la situación real de la misma.

La red de datos de la PNP no cuenta con las suficientes conexiones a nivel nacional, ya que resultan muy costosas, sobre todo cuando se trata de grandes distancias, y muchas veces el enlace no se encuentra disponible en el lugar de destino, lo que agrava la situación. Mantener este escenario disminuye la eficiencia, productividad y operatividad de la PNP, debido a que los recursos informáticos que brinda la INTRANET PNP se encuentran aislados.

Por tal motivo, se requiere la interconexión de los locales policiales y usuarios móviles que la conforman de manera que esto sean considerados parte de la red de datos de la PNP. Todo esto debe ser realizado sin afectar la seguridad de la institución, al garantizar que la información relacionada a los procesos claves, solo pueda ser solicitada por los miembros autorizados para tales fines. En tal sentido, la tecnología de Redes Privadas Virtuales surge como un medio económico al utilizar el canal público de internet para comunicar datos privados, proporcionando además seguridad a través de técnicas de encriptación y encapsulamiento.

3. OBJETIVOS

3.1 Objetivo General

Implementar una red privada virtual (VPN) como alternativa para el acceso remoto a la red de datos de la Policía Nacional del Perú.

3.2 Objetivos Específicos o Secundarios

- Identificar los requerimientos de conexión remota para garantizar que se satisfagan las necesidades de la PNP.
- Realizar un estudio comparativo de las diferentes tecnologías que se pueden utilizar para implementar una red privada virtual.
- Seleccionar la tecnología VPN que más se adapte a las condiciones de la red de datos de la Policía Nacional del Perú.
- Elegir, instalar y configurar el equipo de software y hardware necesario para implementar una red privada virtual y, configurar clientes VPN.

4. JUSTIFICACIÓN

A través de la implementación de una red privada virtual se pueden conectar locales policiales y usuarios móviles en una red corporativa ancha a través de Internet, disminuyendo los costos de largas distancias. Además, al utilizarse ciertos protocolos, permite una conexión segura similar a la existente en una red privada tradicional, por lo cual representa una opción atractiva para establecer conexiones remotas en la PNP.

Al igual, proporciona conocimientos a cerca de una nueva forma de establecer conexiones remotas económicas y seguras: las Redes Privadas Virtuales, y los resultados servirán de guía para que las organizaciones y/o empresas la consideren como alternativa en el momento de adquirir u optimizar sus conexiones remotas, facilitando así la toma de decisiones.

5. ALCANCE DEL ESTUDIO

La investigación se encuentra enmarcada en el campo de informática y las telecomunicaciones y se realizó tomando como modelo la Red de Datos de la Policía Nacional del Perú.

6. PROPUESTA METODOLÓGICA

Este trabajo se puede dividir en tres pasos fundamentales, para el logro de los objetivos:

- Se requiere de recolectar y sintetizar toda la documentación pertinente que nos permita identificar los requerimientos y necesidades de la PNP, respecto a la disponibilidad de información, reducción de costos, cobertura, plan de contingencias, etc.

- Se ampliará el conocimiento teórico de las VPN, centrándonos específicamente en las posibles soluciones actuales de esta tecnología.

- Desarrollar e implementar una solución VPN a fin de considerarlo y evaluarlo como una solución para el acceso remoto en el ámbito de la red de datos de la PNP.

7. ORGANIZACIÓN DE LA TESINA

El presente trabajo comprende la implementación de una red privada virtual como alternativa para el acceso remoto a la red de datos de la Policía Nacional del Perú. Ha sido estructurado en 5 capítulos, a continuación se describe una visión de los contenidos de cada sección:

Capitulo 1, presenta el planteamiento metodológico en el que se refiere al antecedente y formulación del problema, los objetivos, la justificación y alcance, y por último la propuesta metodológica.

Capitulo 2, se describe todo lo relacionado con las Redes Privadas Virtuales, como son los tipos, arquitectura y tecnologías; se hace un estudio de la situación organizacional y tecnológica de la Policía Nacional del Perú.

Capitulo 3, se hace un estudio de las tecnologías existentes en el momento para la posible realización del proyecto, y discerniremos entre una u otra, dependiendo de las, prestaciones, fiabilidad y posibles ampliaciones de servicios en el futuro.

Capitulo 4, se documenta la implementación de un prototipo de red privada virtual como alternativa de acceso remoto a la red de datos de la Policía Nacional del Perú, se hace un análisis de costos ventajas y desventajas respecto a las líneas dedicadas.

Capitulo 5, consta de las conclusiones y recomendaciones. Finalmente las *Referencias Bibliográficas* y los *Anexos*.

CAPITULO II MARCO TEÓRICO

1. REDES PRIVADAS VIRTUALES

1.1 Introducción

La implementación de una red privada virtual ha dejado de ser una necesidad exclusiva de las empresas grandes. Esta tecnología se ha transformado en un requerimiento para la mayoría de las empresas pequeñas y medianas, debido al gran valor agregado que aporta.

Es preciso tener en cuenta, además, que una VPN no se traduce simplemente en la configuración de un protocolo en particular, sino que concentra una gran cantidad de protocolos, algoritmos de encriptación, funciones de hash, dispositivos y programas.

En el transcurso de los últimos años, la implementación de VPNs se ha vuelto un hecho sumamente popular. Alentadas, en parte, por la potencialidad que brinda Internet como red pública portadora, estas redes privadas virtuales se han convertido en una herramienta fundamental a la hora de servir de vínculo de comunicación seguro a empresas de todos los tamaños. Si bien es cierto que estas implementaciones incluyen nuevos protocolos y novedosas funcionalidades, el concepto detrás de las VPNs lleva unos cuantos años junto a nosotros.

1.2 Red Privada Virtual

Red privada Virtual o Virtual Private Network (VPN) es un grupo de dos o más sistemas de ordenadores, generalmente conectados a una red corporativa privada, que se comunican con seguridad sobre una red pública. Es decir, para transmitir información a través de una red pública (insegura), en la VPN se aplican métodos de seguridad para garantizar la privacidad de los datos que se intercambian entre ambas, y protocolos de túneles.

A las Redes Privadas Virtuales, se les considera “Privadas” porque se establecen exclusivamente entre el emisor y el receptor de la información, y “Virtuales”, porque no se necesita un cable o cualquier otro medio físico directo entre los comunicantes. Las VPN extienden la red corporativa de una empresa a las

oficinas distantes, por ejemplo, en lugar de alquilar líneas dedicadas con un costo muy elevado, utilizan los servicios mundiales de IP, incluyendo la Internet.

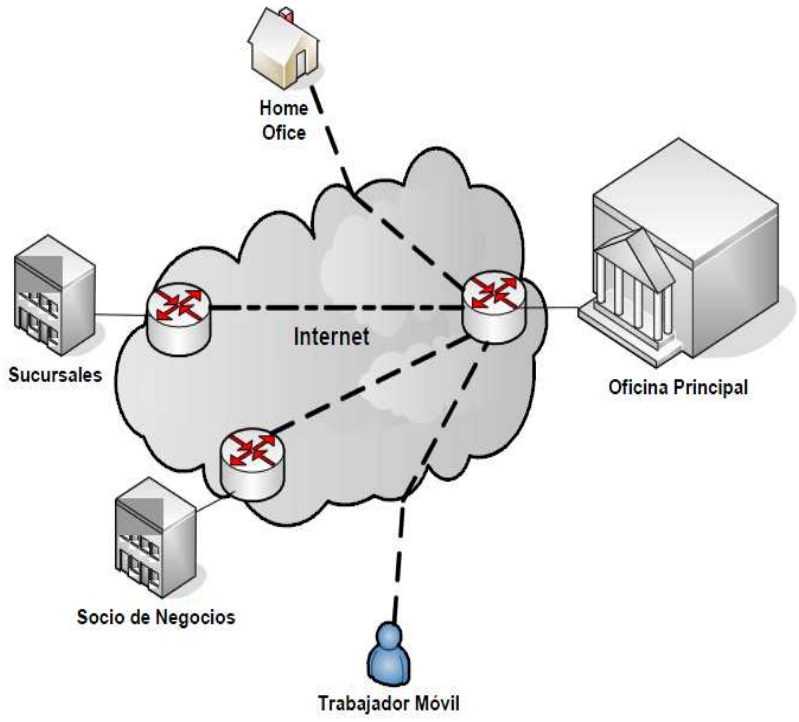

Figura 2.1 Diagrama de una VPN en una Organización

La VPN lo que hace es crear un túnel entre los dos puntos a conectar utilizando infraestructura pública, usa una técnica llamada entunelamiento (Tunneling), los paquetes de datos son enrutados por la red pública, tal como Internet, en un túnel privado que simula una conexión punto a punto.

Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. También hace universales para su trasporte los diferentes protocolos LAN entre los que se encuentran IP, IPX, Appletalk y Netbeui, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes privadas virtuales.

1.3 Requerimientos Básicos de una VPN

Una Red Privada Virtual ha de proveer de los siguientes mecanismos básicos, aunque en ocasiones y situaciones puede obviarse algunos.

- Autentificación de usuarios, verificar la identidad de los usuarios, para poder restringir el acceso a la VPN solo a los usuarios autorizados.
- Administración de direcciones, debe asignar una dirección del cliente a la red privada, y asegurar que las direcciones privadas se mantengan privadas.
- Encriptación de datos, los datos que viajan por la red pública, deben ser trasformados para que sean ilegibles por los usuarios no autorizados.
- Administración de claves, debe mantener claves de encriptación para los clientes y servidores.
- Soporte multiprotocolo, ha de ser capaz de manejar protocolos comunes usando la red pública, por ejemplo IPX, IP, etc.

1.4 Tipos de VPN

1.4.1 Sistemas Basados el Firewall

Estos se implementan con software de cortafuegos (Firewall). Tienen la ventaja de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna. También realizan la traducción de direcciones (NAT). Estos satisfacen los requerimientos de autentificación fuerte. El rendimiento en este tipo decrece, ya que no se tiene hardware especializado de encriptación.

1.4.2 Sistemas Basado en Hardware

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

La implementación entre ruteadores provee la capacidad de asegurar un paquete en una parte de la red, esta seguridad se logra a través del Tunneling

de paquetes. Las principales ventajas conseguidas con la implementación sobre routers son:

- Capacidad de asegurar el flujo de paquetes entre dos redes, a través de una red pública como internet.
- Capacidad de autentificar y autorizar a usuarios el acceso sobre redes privadas.

1.4.3 Sistema Basado 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 es enrutado por el túnel. Podemos hacer un enrutamiento inteligente de una manera mucho más fácil.

1.5 Arquitecturas VPN

1.5.1 VNP de Acceso Remoto

Las VPNs de acceso remoto suele ser consideradas la evolución natural de aquel tipo de conexiones dial-up tan frecuentemente utilizadas. Son la solución acertada a la hora de asegurar las conexiones de usuarios móviles, tele trabajadores o cualquier otro usuario tradicional que desea aprovechar las ventajas brindadas por la VPN. En este tipo de VPN, un usuario establece un vínculo a través de Internet por intermedio de su proveedor de servicios de Internet (ISP), para luego poner en funcionamiento el cliente instalado en su estación remota. Debemos aclarar, que hoy en día, el uso de un cliente por software en este tipo de esquemas ya no es una necesidad. En algunos casos, como WebVPN, bastará con un browser del lado del cliente para poder establecer el túnel VPN.

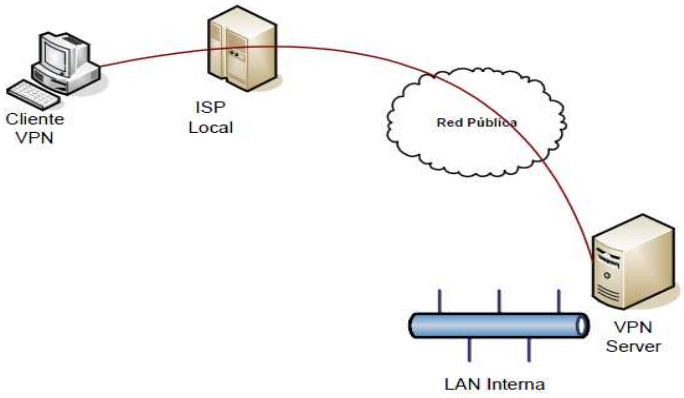

Figura 2.2 Diagrama de VPN por Acceso Remoto

1.5.2 VPN de Sitio a Sitio

Las VPNs site-to-site suelen implementarse a fin de establecer un vinculo seguro y confiable entre dos redes de distintas organizaciones (Extranet VPN), interconectando clientes, proveedores y socios de negocio; o bien entre redes distantes de una misma organización (Intranet VPN), interconectando oficinas centrales y remotas. En ambos casos, este tipo de conexión representa una evolución respecto al uso de líneas punto a punto o del tipo Frame Relay. De hecho, una VPN site-to-site suele ser considerada como una extensión de las clásicas redes WAN.

- ***Tipo Intranet***, si la empresa tiene una o más sucursales remotas que quiere unir en una única red privada, puede hacerlo creando una VPN para conectar ambas redes locales.

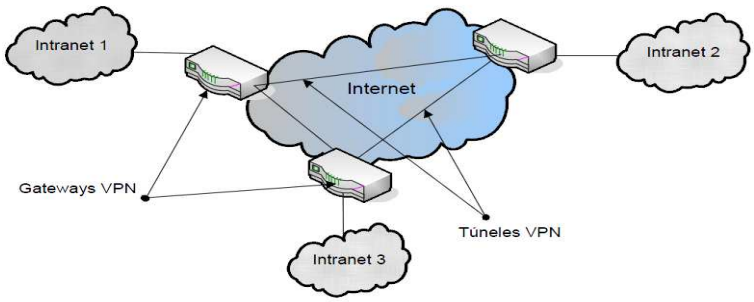

Figura 2.3 Diagrama de Intranet VPN

- ***Tipo Extranet***, cuando la empresa tiene una relación cercana con otra compañía (por ejemplo, una empresa asociada, un proveedor o cliente), entonces puede desarrollar una VPN que conecte sus redes y permita a estas empresas trabajar en un ambiente compartido. Con una arquitectura de Extranet VPN cada empresa tiene que controlar muy meticulosamente el acceso a los recursos de su red corporativa y a los datos que van a intercambiar con sus socios de negocios. Implementar una topología Extranet VPN implica incrementar la complejidad de los sistemas de control y acceso y de autenticación.

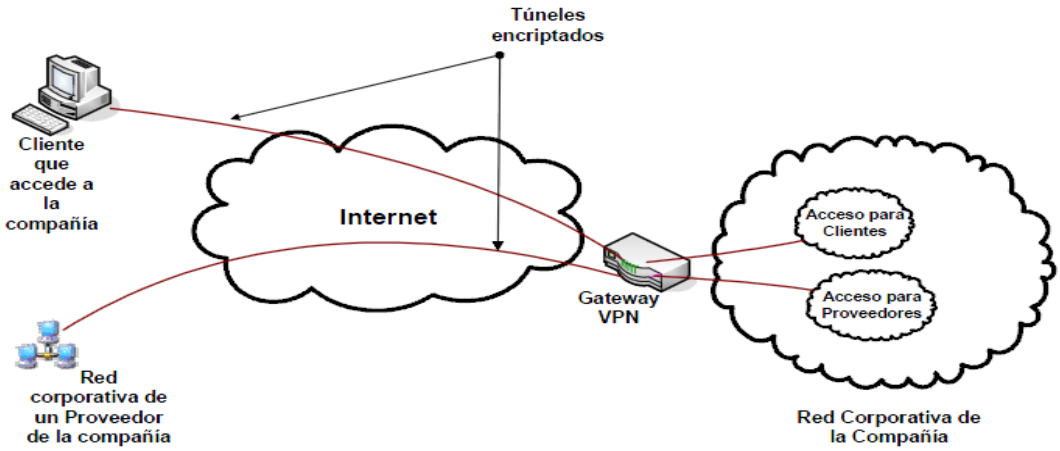

Figura 2.4 Diagrama de Extranet VPN

1.5.3 VPN Interna

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red LAN de la empresa. Sirve para aislar zonas y servicios de la red LAN interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas.

La mayoría de los incidentes de seguridad está relacionada con abusos dentro de la red de la compañía, por lo tanto a más de los ataques externos no hay que perder de vista los ataques internos. Dependiendo del tipo de

negocio o por asuntos legales, cierta información puede ser privada y confidencial a un nivel de departamento. Una VPN entre departamentos puede ayudar a encontrar esos requerimientos de confidencialidad. Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de RR.HH habilitado pueda acceder a la información. Otro ejemplo puede ser un requerimiento de email confidencial, como se muestra en la Figura 2.5.

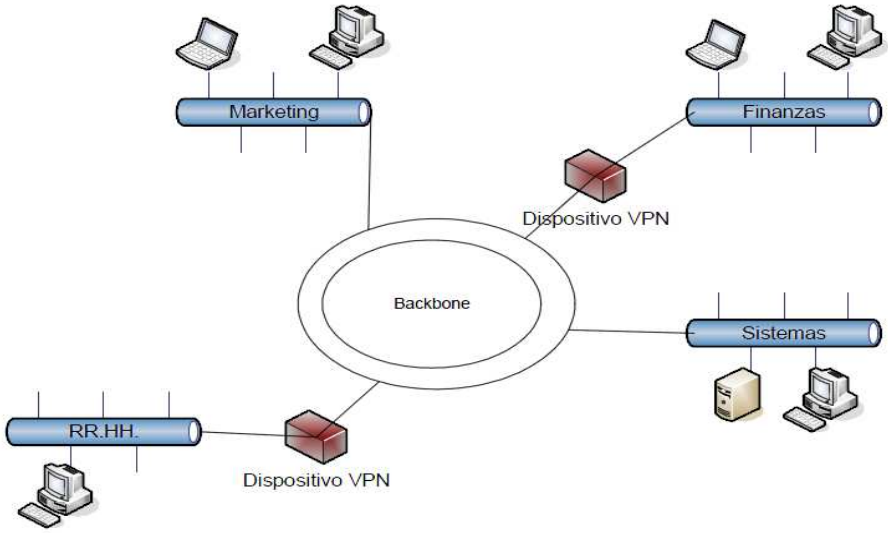

Figura 2.5 Arquitectura VPN Interna

1.6 Tecnologías VPN

Básicamente, y haciendo referencia al modelo OSI, se puede crear una VPN usando tecnologías de Tunneling de capa 2 (Enlace de Datos) y de capa 3 (Red).

1.6.1 Tunneling

Como parte de su funcionamiento, las redes privadas virtuales habilitan la creación de túneles o conductos dedicados de un sitio a otro. La tecnología de túneles, comúnmente conocida como **Tunneling**, representa un método válido para transferir datos entre dos redes similares sobre una red intermedia diferente. Por medio de una técnica conocida cono

encapsulamiento, estos túneles tienen la capacidad de encerrar un tipo de paquete de datos dentro del paquete de otro protocolo (en general, TCP/IP) y, en el caso particular de los túneles VPN, proceder a la encriptación de los datos trasmitido a través de él, de modo tal que si se produce algún tipo de intercepción sobre la red pública subyacente, estos resulten ilegibles a los ojos del atacante. De acuerdo con este procedimiento, los paquetes encapsulados viajan a través de Internet o de cualquier otro tipo de red pública hasta que alcanzan su destino, una vez allí, se separan y vuelven a su formato original.

Para llevar a cabo su función de manera segura, es necesario que una VPN provea los medios necesarios a la hora de garantizar aspectos tales como autenticación, integridad y confidencialidad de los datos que la atraviesan. Para comprender mejor este tema, utilizaremos como ejemplo la conexión de un cliente remoto a través de una VPN:

1- El usuario remoto llama a su ISP local y se conecta a su red de forma normal.
2- Cuando requiere conectarse a la red corporativa, el usuario inicia el túnel enviando una petición a un servidor VPN de la red corporativa.
3- El servidor VPN autentifica al usuario y crea el otro extremo del túnel.
4- El usuario comienza a enviar datos a través del túnel, los cuales generalmente son cifrados por el software VPN (del cliente) antes de ser enviados sobre la conexión del ISP.
5- En el destino, el servidor VPN recibe los datos, los descifra y los reenvía a la red corporativa. Cualquier información enviada de regreso al usuario remoto también es cifrada antes de enviarse por Internet, tarea que recae sobre el extremo contrario al cliente.

Tunneling incluye todo el proceso de encapsulado, desencapsulado y transmisión de los paquetes. Las tecnologías de Tunneling más conocidas son:

- PPTP (Point-to-Point Tunneling Protocol).
- L2F (Layer 2 Forwarding).

- L2TP (Layer 2 Tunneling protocol).
- IPSec (Internet Protocol Security Tunnel Mode).
- VPN-SSL

Referente a sus componentes, estructura, topología, formatos, etc., se explicaran con más detalle en el Capítulo III.

2. SITUACIÓN ACTUAL DE LA POLICÍA NACIONAL DEL PERÚ

2.1 Descripción

El Estado es la organización fundamental para la vida social estructurada, que materializa en lo cotidiano tanto al orden como a la justicia, a través de un marco legal por el que se regula la convivencia entre los miembros de una sociedad. El Estado crea a la Policía como Institución ejecutora de la facultad de coerción estatal, de acuerdo a las leyes dictadas en función del interés social; por lo que su actividad, función y finalidad deben ejecutarse dentro del marco de la ley, la doctrina y los principios generales del Derecho y de la Constitución, la cual se orienta hacia la persona humana como fin supremo del Estado:

- Función **PREVENTIVA** para garantizar la seguridad y tranquilidad pública.
- Función **INVESTIGATIVA** frente a la conexión de delitos y faltas.
- Función **PROTECTORA** de los derechos y patrimonios públicos y privados.
- Función de **AUXILIO** frente a pedidos de las actividades.
- Función **CONCILIADORA** frente a conflictos menores que se constituyen infracciones legales. Otra que la Constitución y las leyes le asignen.

2.2 Visión

Ser reconocida como una institución moderna, disciplinada y eficiente al servicio de la sociedad, con prestigio nacional e institucional:

- Por su respeto y defensa a los derechos humanos, la Constitución y las leyes, vocación democrática y compromiso por fomentar una cultura de paz.
- Por la vocación de servicio, honestidad, capacidad, profesionalismo y liderazgo de sus integrantes.

- Por su acercamiento e integración con la comunidad a la que sirve y su relación y colaboración con otras instituciones del Perú y el mundo.
- Por su estructura flexible y versátil, así como la incorporación y aplicación de tecnología de punta en su accionar.

2.3 Misión

La Policía Nacional tiene por finalidad fundamental garantizar, mantener y restablecer el orden interno. Presta protección y ayuda a las personas y la comunidad. Garantiza el cumplimiento de las leyes y la seguridad del patrimonio público y del privado. Previene, investiga y combate la delincuencia. Vigila y controla las fronteras. (Articulo 166 Constitución Política del Perú).

2.4 Presencia en el País

La Policía Nacional del Perú es una institución del Estado creada para garantizar el orden interno, el libre ejercicio de los derechos fundamentales de las personas y el normal desarrollo de las actividades ciudadanas. Es profesional y jerarquizada. Sus integrantes representan la ley, el orden y la seguridad en ***toda la República*** y tienen competencia para intervenir en todos los asuntos que se relacionan con el cumplimiento de su finalidad fundamental.

2.5 Organigrama Corporativo

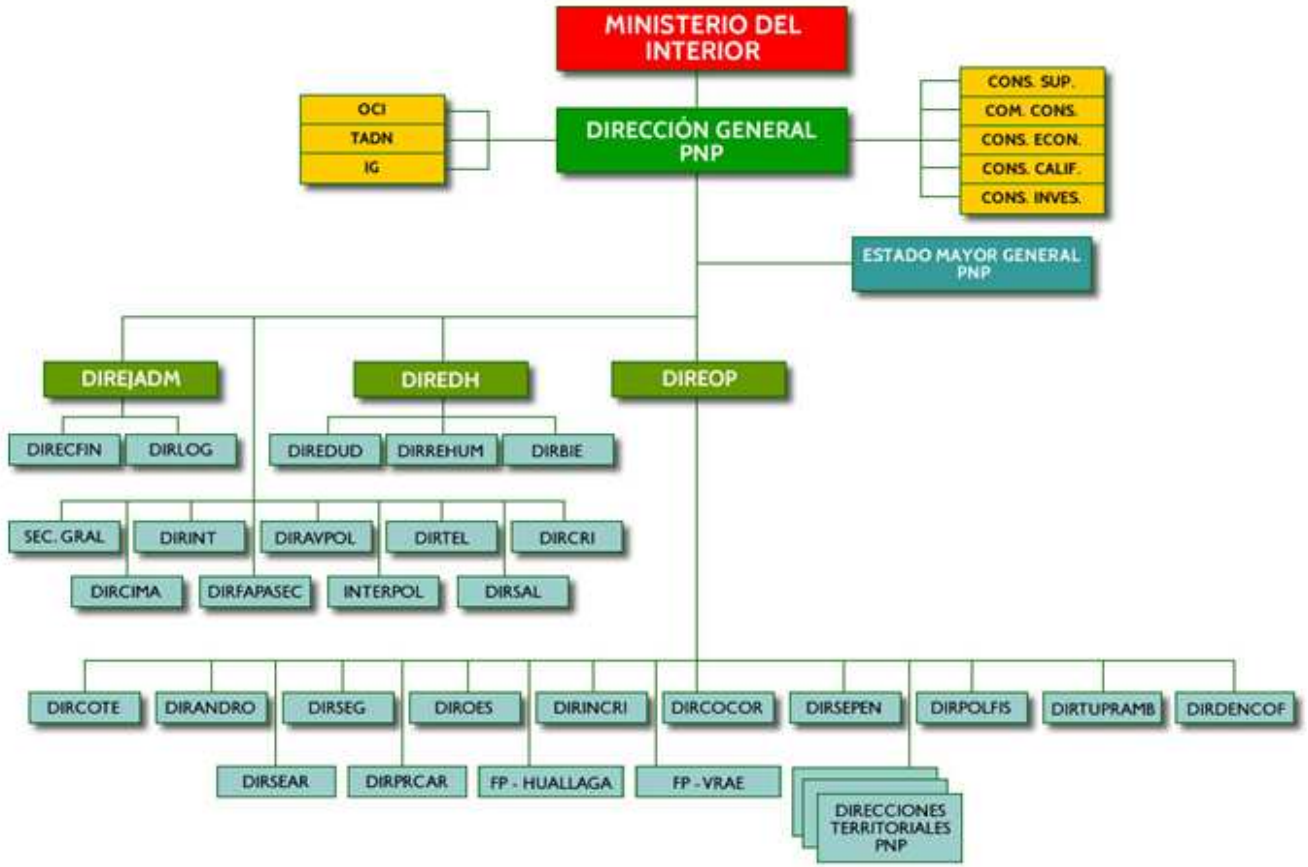

Figura 2.6 Organigrama Corporativo de la PNP

2.6 Soporte Informático y de Telecomunicaciones

La *Dirección de Telemática* es un órgano de apoyo de la PNP, cuya misión es la de brindar soporte técnico en la áreas de informática y telecomunicaciones. A través de su *División de Informática* brinda soporte técnico y soluciones tecnológicas a las Unidades Policiales, en tiempo real, coadyuvando a la eficiente gestión policial en la lucha contra la delincuencia común y el crimen organizado, terrorismo y narcotráfico, así como facilitar la comunicación de datos entre los miembros de la PNP, mejorando la calidad profesional del Policía.

2.7 Sistemas de Información

2.7.1 Datapol (Sistema de Requisitorias de Personas y Vehículos)

Sistema basado en Tecnología WEB que permite visualizar información:

- Consulta de Requisitoria de Personas
- Consulta de Antecedentes Policiales
- Consulta de Referencia de Investigación Criminal
- Consulta de Requisitorias de Vehículos
- Emisión de Certificados de Antecedentes Policiales
- Reportes Estadísticos.
- Noticias y Accesos a otras Páginas Web.

Figura 2.7 Sistema Datapol

2.7.2 Sistema de Denuncias Policiales

Consiste en la Automatización de todo el proceso de las denuncias Policiales, desde su registro en una Comisaría hasta sus conclusiones finales:

- Intercambio de información entre Comisarías.
- Explotación eficaz y oportuna de la información histórica que ingresa a la Comisaría PNP mediante estadísticas en tiempo real.
- Reducción de tiempo en el proceso de atención de denuncias y otros servicios a la comunidad.
- Mejor planeamiento del servicio policial al tener la información procesada por tipo de delitos y otros.
- Información oportuna al público

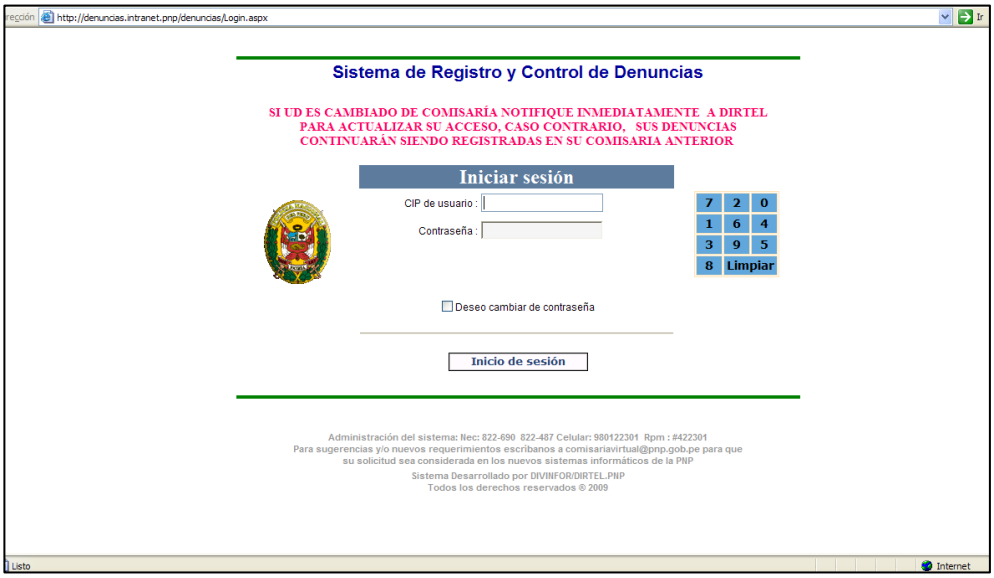

Figura 2.8 Sistema de Denuncias Policiales

2.7.3 Sistema de Personal Policial (Aguila6)

Sistema basado en Tecnología WEB que permite visualizar información del personal policial: Situación Profesional y Académica, Meritos, Deméritos, Condecoraciones, Situación Familiar y de Salud, etc.

Figura 2.9 Sistema de Personal Policial

2.7.4 Sistema de Planillas

Sistema basado en Tecnología WEB que permite visualizar información referente a las boletas de pago del personal policial.

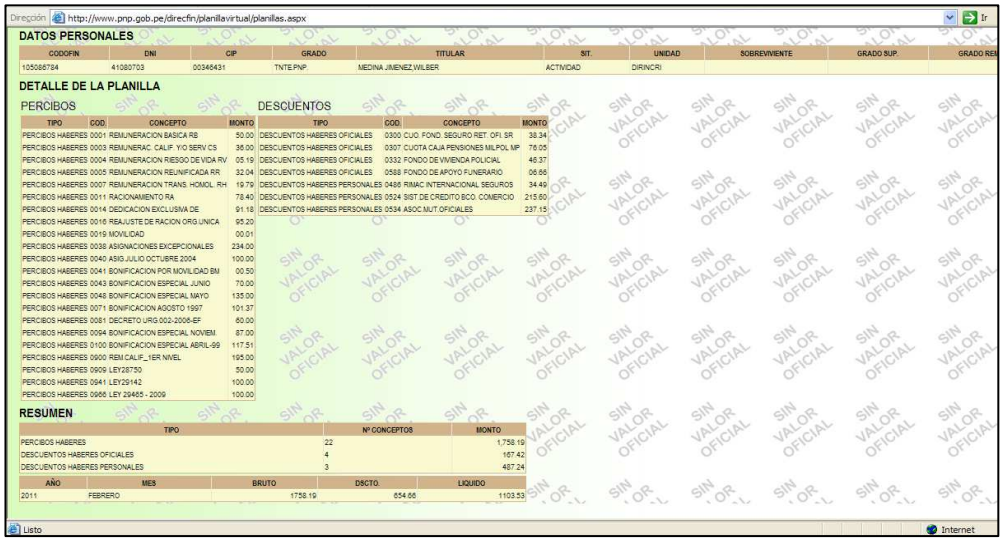

Figura 2.10 Sistema de Planillas

2.7.5 Servicio de Correo Electrónico de la PNP

Sistema basado en Tecnología WEB, implementado con Microsoft Exchange Server que permite la comunicación de los usuarios policiales:

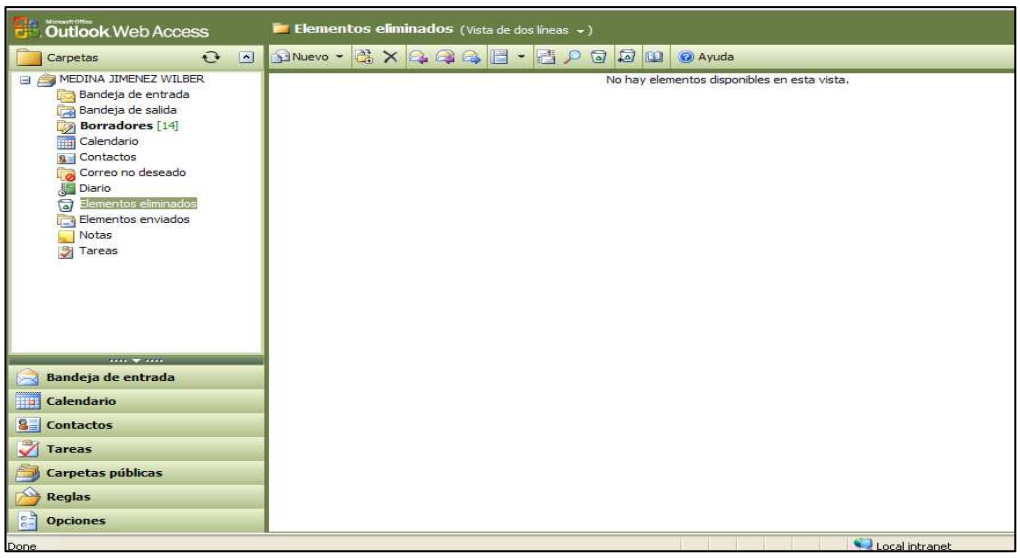

Figura 2.11 Servicio de Correo Electrónico

2.7.6 Sistema de Certificados y Antecedentes Policiales (CERAP)

Sistema que nos permite la automatización en los procesos de expedición de los Certificados de Antecedentes Policiales.

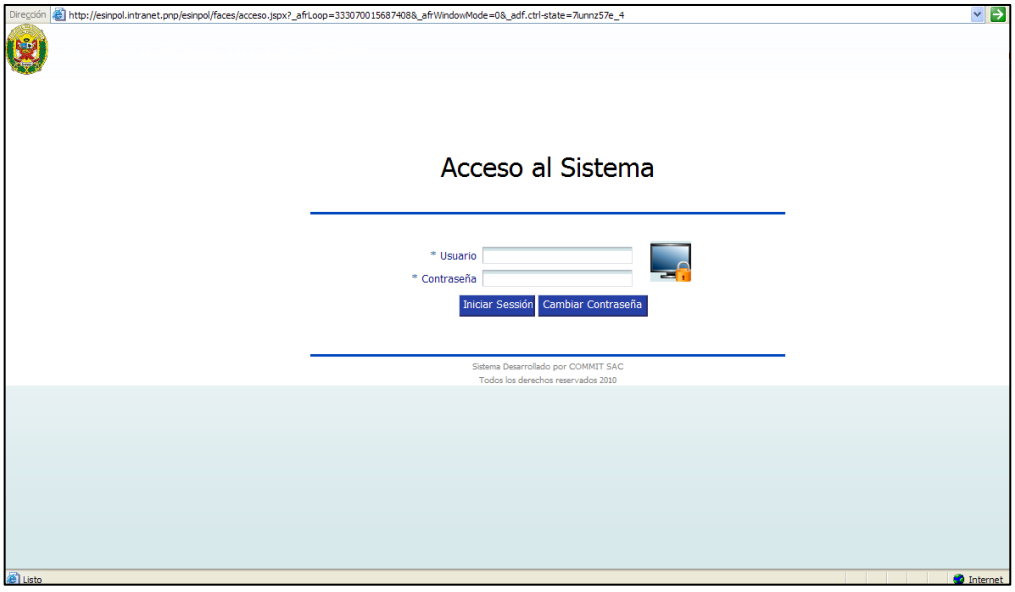

Figura 2.12 Sistema de Certificados y Antecedentes Policiales

2.7.7 Sistema de Comisaria Virtual

Sistema Web, que utilizando Internet permite:

- Conocer información de la Comisaría de cada jurisdicción: Historia, Misión, Funciones, Logros y servicios que se brinda a la colectividad.

- Acceder a una PRE DENUNCIA, con la cual se puede informar de hechos, presuntos autores, modalidades delincuenciales.

Figura 2.13 Sistema de Comisaría Virtual

2.7.8 Sistema de Tramite Documentario

Sistema que permite registrar todos los documentos que ingresan y se formulan en una dependencia policial, así como tener un control eficaz de los mismos, hecho que va a redundar en el adecuado y oportuno trámite de los documentos.

Figura 2.14 Sistema de Tramite Documentario

2.8 Infraestructura de Red

2.8.1 Red LAN

En la Figura 2.12 se muestra la red LAN en la Matriz, donde se puede apreciar las conexiones entre los Switch's de los pisos y el Switch central del Centro de Cómputo PNP. Para enlazar estos dispositivos se utiliza fibra óptica.

La topología de la red LAN es de tipo estrella, en este caso todos los mensajes deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado (Switch), el cual controla el flujo de datos. Tanto la matriz como los puntos remotos tienen la misma topología de red.

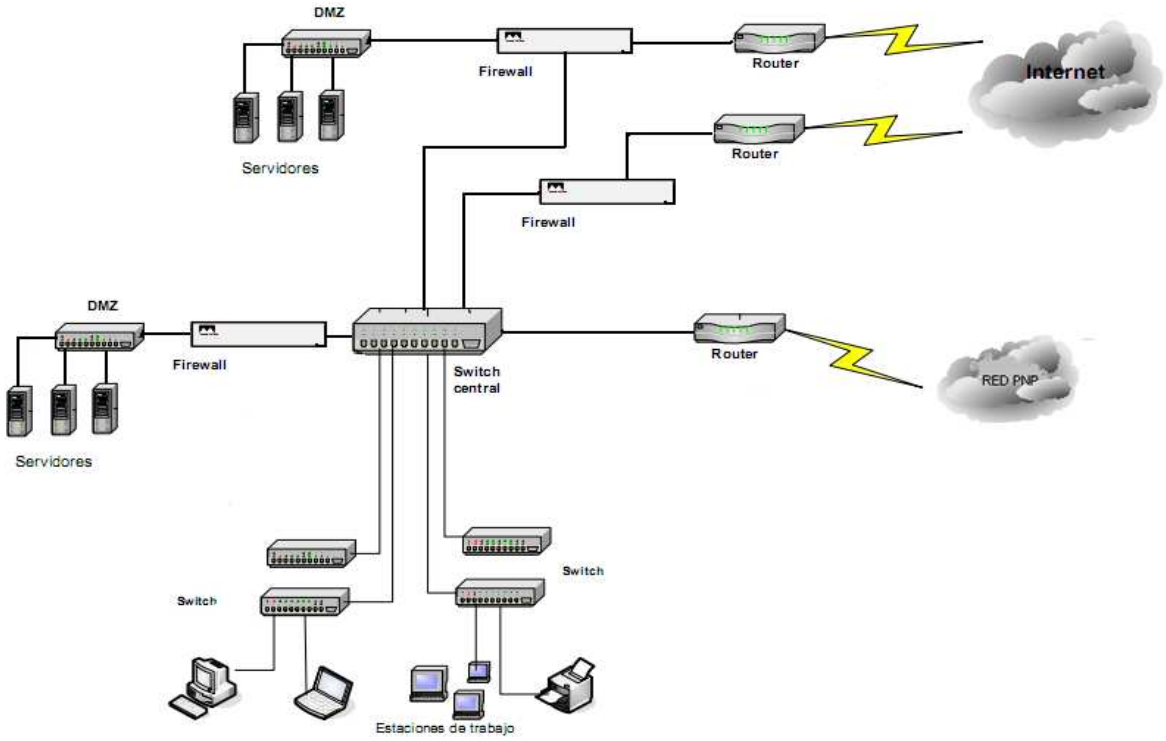

Figura 2.15 Red LAN del Nodo Central

En los puntos remotos la red de Área Local en realidad es pequeña Figura 2.13, constan de computadores, impresoras y los equipos de comunicaciones (Router y Switch).

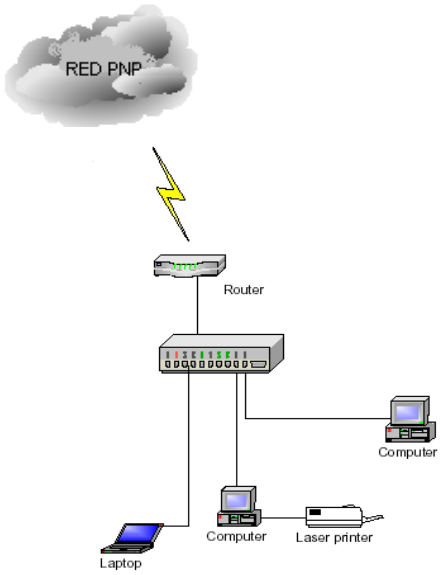

Figura 2.16 Red LAN de los Puntos Remotos

2.8.2 Red WAN

La red WAN enlaza computadoras que se encuentran geográficamente dispersas con la sede central, en la Red PNP la conexión entre las oficinas remotas se realiza a través de líneas dedicadas.

La red WAN de la PNP presenta una topología centralizada en donde las operaciones de cómputo primarias se realizan en un solo lugar Nodo Central, las estaciones distantes utilizan los recursos que brinda este Nodo Central. A menudo un sistema de este tipo es concebido como una red en estrella donde cada sitio remoto ingresa al sistema central vía una línea de comunicación.

En la Figura 2.14 se aprecia la red WAN formada por las sucursales y la matriz a través de los enlaces de la Red PNP, también consta la conexión a Internet con la empresa Telefónica.

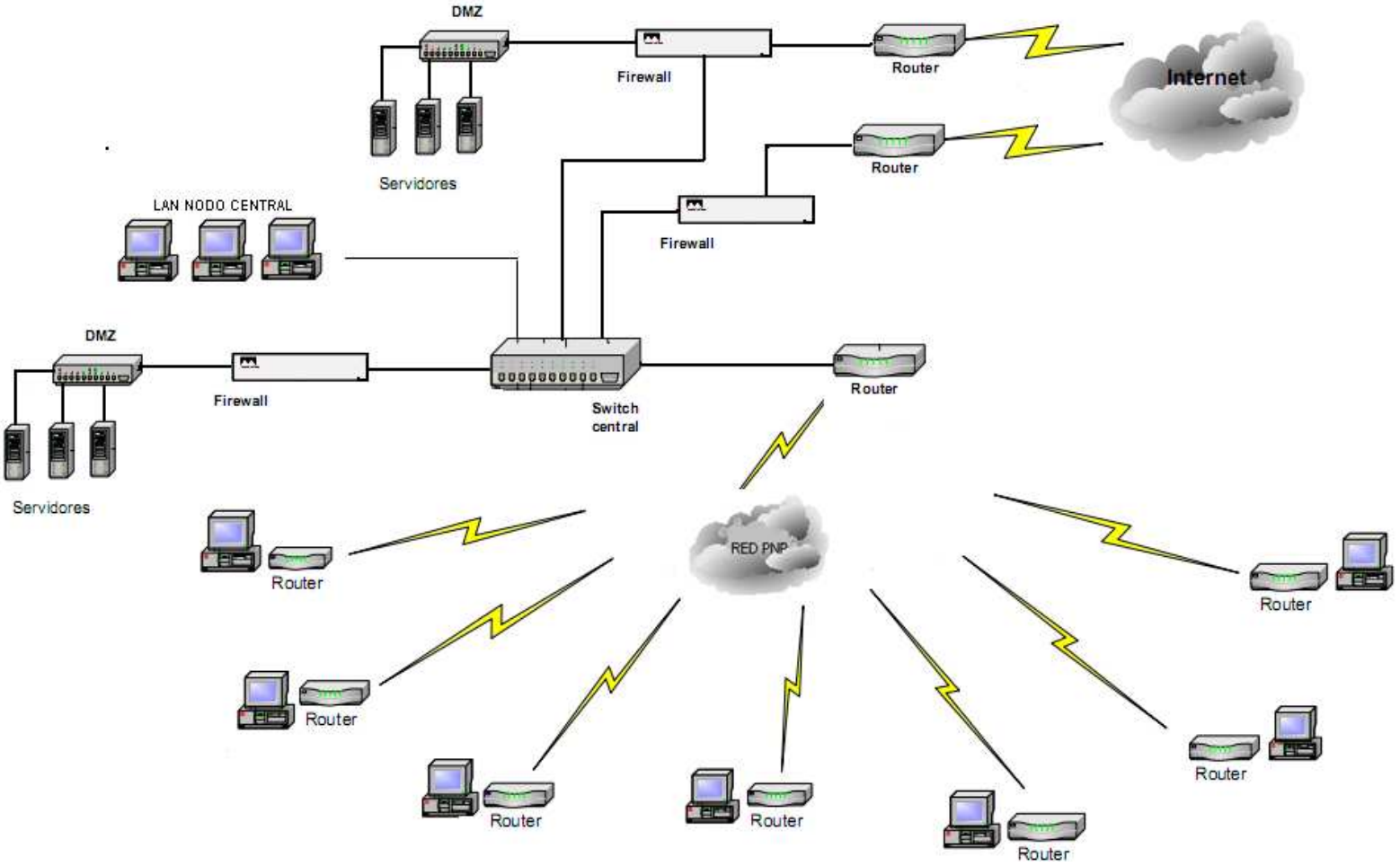

Figura 2.17 Grafica de la red WAN de la Red PNP

2.9 Infraestructura de Telecomunicaciones

2.9.1 Líneas Dedicadas

En la Policía Nacional actualmente se cuenta con Trescientos Sesenta y Ocho (368) Unidades Policiales interconectadas a la Intranet PNP mediante circuitos de datos, con los siguientes tipos de acceso:

- Un (01) circuito de datos en el Nodo Central, como línea dedicada principal, a través de fibra óptica. (34 Mbps)
- Cincuenta y tres (53) circuitos de datos, con acceso simétrico, a través de cobre y fibra óptica. (64, 128, 256 y 512 Kbps).
- Doscientos ochenta y cuatro (284) circuitos de datos, con acceso asimétrico de 600/256 Kilobits por segundo (Kbps), garantizando un 30%, cuando su red se encuentre congestionada.
- Treinta y uno (31) circuitos de datos satelitales, con acceso asimétrico de 256/128 Kbps, garantizando un 30%, cuando su red se encuentre congestionada.

CIRCUITO DE DATOS	LIMA	LIMA PROV	PROVINCIAS	SUBTOTAL
SIMETRICO	31	1	21	**53**
SATELITAL	7	15	9	**31**
ASIMETRICO	181	26	77	**284**
TOTAL	**219**	**42**	**107**	**368**

Tabla 2.1 Tabla Resumen de los Enlaces Dedicados

Los circuitos de datos con acceso simétrico permiten garantizar la comunicación de voz, video y datos, mediante la clasificación y priorización de los paquetes en todo el canal de comunicación, motivo por el cual son de mayor costo; mientras que los circuitos de datos con acceso asimétrico están orientados principalmente a la comunicación de datos, no garantizando la comunicación de voz ni video, siendo de menor costo.

DIRTEPOL	COMISARIA	UU.PP.	SUBTOTAL
I	2	6	8
II	6	7	13
III	2	7	9
IV	0	6	6
V	1	1	2
VI	1	3	4
VII			261
LIMA METROPOLIT.	**121**	**98**	**219**
LIMA PROVINCIAS	**38**	**4**	**42**
VIII	3	9	12
IX	2	2	4
X	1	10	11
XI	8	9	17
XII	1	4	5
XIII	2	4	6
XIV	4	1	5
XV	4	1	5
TOTAL	**196**	**172**	**368**

Tabla 2.2 Tabla de Locales Interconectados por Tipo de Unidad

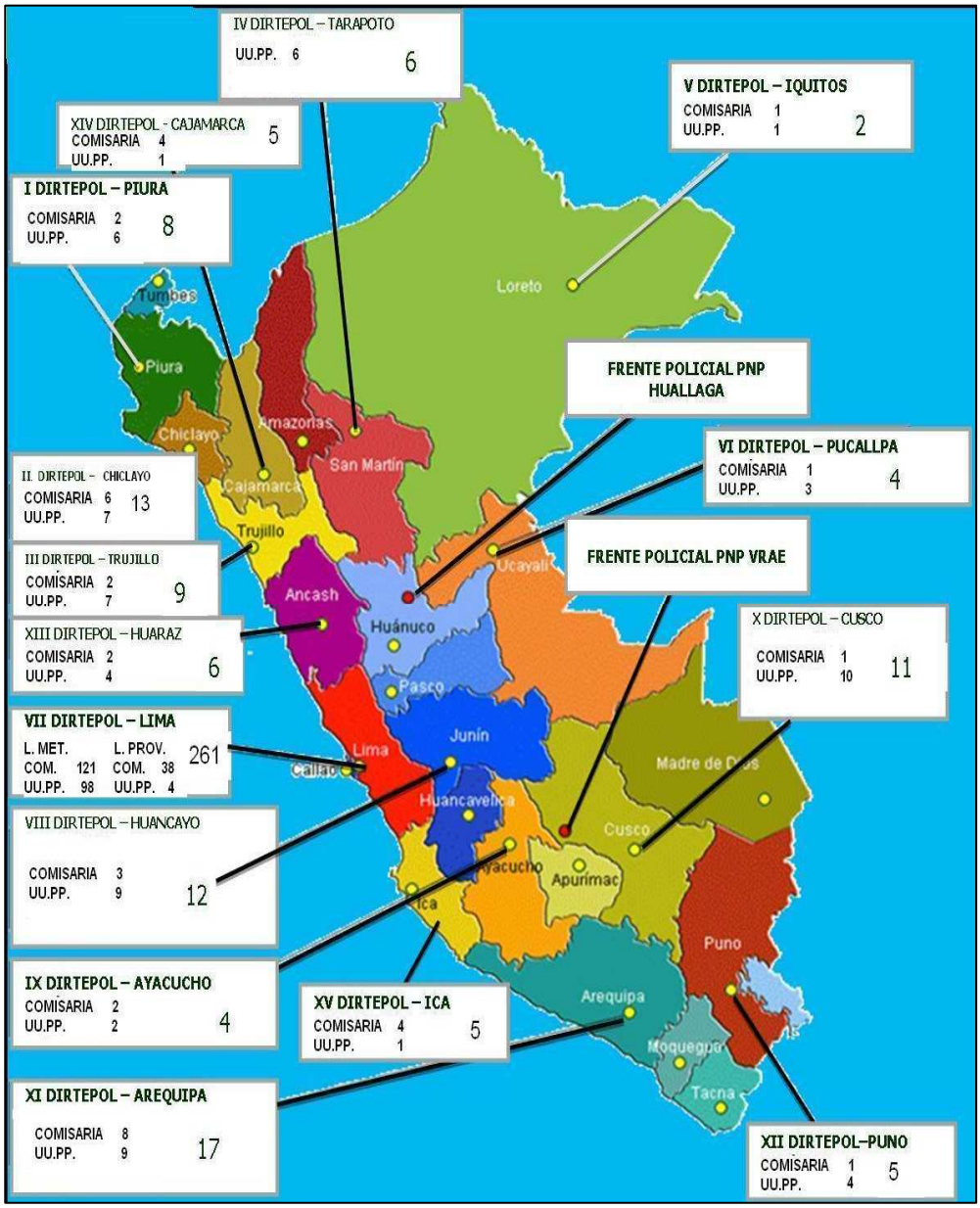

Figura 2.18 Interconexión a Nivel Nacional de 368 Unidades Policiales

2.9.2 Conexión a Internet

Para acceder al servicio de Internet, la Red de la Policía Nacional mantiene una conexión permanente de banda ancha de 8 Mbps con la empresa Telefónica del Perú. Esta conexión es aprovechada por casi todas las agencias del país, en el caso de los locales policiales situados en provincias, utilizan las líneas dedicadas para conectarse al servidor proxy que está en el

Nodo Central, de esta manera, los usuarios policiales se conectan sin tener que pagar un costo adicional por este servicio.

Asimismo se cuenta con un acceso Internet de 1Mbps con la empresa en mención, servicio que es utilizado exclusivamente para los enlaces VPN.

2.10 Plataforma de Software y Hardware

2.10.1 Sistema Operativo de Red

El software que se encarga de administrar y controlar en forma general la red es el sistema operativo de red de Microsoft Windows, el esquema de la red trabaja en modo dominio, soporta el protocolo TCP/IP y proporciona una interfaz amigable al administrador de la red.

2.10.2 Estaciones de Trabajo

Para las estaciones de trabajo se emplea sistemas operativos como Windows 98, Windows XP, Windows Vista, Windows 7, además de presentar una interfaz de fácil manejo a los usuarios, proporciona a éstos el soporte para ejecutar el conjunto de aplicaciones que cumplen con los requerimientos de información y trabajos que se manejan en la Policía Nacional.

2.10.3 Aplicaciones de Usuario

Para que los usuarios puedan realizar su trabajo de la mejor manera y de acuerdo al rango o las funciones que desempeña, se le instala todo o parte del software listado a continuación: Microsoft Office 2003/2007/2010, Internet Explorer, Messenger, Nod32 Antivirus, WinRar, Adobe Acrobat, etc.

2.10.4 Software de Desarrollo y Administración

Está formado por programas informáticos que permiten la administración de la red de datos, así como el desarrollo y gestión de sistemas de información: ISA Server 2006, TMG, Sharepoint Server, Websense Enterprise, MS SQL 2008 Server, My SQL, ORACLE Enterp, Visio 2007, JAVA, VISUAL STUDIO 2008, PHP, COREL DRAW, CRISTAL REPORT, RATIONAL ROSE, SPSS 16, Sniffer Portable, ARCGIS, etc.

2.10.5 Dispositivos de Interconexión

Constan de los equipos utilizados para la interconexión en las redes LAN y WAN, como son los ruteadores, módems, firewall, Gateway VoIP y switchs.

2.11 Requerimiento y Necesidades

- **Ampliación de Cobertura,** Requerimientos de las Unidades Policiales de interconectarse a la Red de Datos de la Policía Nacional (Intranet PNP). Además, existe la recomendación de la Defensoría del Pueblo y el requerimiento de la Comisión de Alto Nivel presidida por el Jefe del Estado Mayor General de la Policía Nacional del Perú, encargada de evaluar el funcionamiento del Sistema de Requisitorias de la Policía Nacional, así como efectuar las propuestas correspondientes, a fin de contar con un Sistema de Requisitorias interconectado a nivel nacional, solicitando la priorización de la interconexión de los Puestos de Vigilancia de Fronteras (PVF) y Aeropuertos donde existe tráfico de personas y vehículos.

- **Reducción de Costos en Telecomunicaciones,** En nuestro país el costo de las telecomunicaciones y en particular para las empresas sigue siendo elevado. El costo que representa el pago de líneas dedicadas es sin duda el mayor, de ahí la necesidad de buscar proveedores más competitivos y nuevas formas de interconexión que signifiquen un ahorro significativo para la organización. El costo mensual del servicio de Banda Ancha de la Red PNP asciende a $ 140,530.00 dólares americanos, el pago es integral, es decir incluye el pago por todos los enlaces de comunicaciones tanto para la Intranet como para el Internet.

- **Incrementar la Seguridad de la Información,** Al utilizar el sistema en una red estará a un nivel más alto de riesgo que si no estuviese conectado a una. La Red de datos de la Policía Nacional presenta un esquema de dominios que aporta grandes ventajas en la seguridad de la red gracias al control de usuarios y privilegios de acceso a los recursos del dominio, también se dispone de un Firewall para aislar la red de ataques externos. Pero se necesita implementar

más seguridades, especialmente políticas que ayuden a contrarrestar ataques internos y externos. La verdadera seguridad de un sistema va más allá de un Firewall o una actualización más reciente, la configuración de un cierto fichero, o la cuidadosa administración del acceso de los usuarios a los recursos del sistema. Las políticas de seguridad son una manera de ver diferentes amenazas que acechan al sistema y lo que se está dispuesto a hacer para evitarlas. Por lo tanto se hace necesario diseñar políticas de seguridad para el uso correcto del Internet, Correo Electrónico, entre otros.

- **Plan de Contingencias,** El Centro de Cómputo de la Policía Nacional del Perú puede quedar total o parcialmente inoperativo como consecuencia de un siniestro fortuito, esta suspensión afectaría directamente la operatoria policial y la imagen institucional, y consecuentemente en el Orden Interno y Seguridad Ciudadana. Es así que es necesario empezar a crear un plan de contingencias, el cual será un documento guía para prevenir desastres y actuar con eficacia cuando ocurran.

CAPITULO III ESTADO DEL ARTE METODOLÓGICO

En este capítulo discerniremos las tecnologías VPN más conocidas, respecto a sus prestaciones, fiabilidad y rendimiento. Básicamente, y desde el punto de vista de la torre OSI, se puede crear una VPN usando tecnologías de capa 2 (enlace de datos), de capa 3 (red) y de capa 4 (Transporte).

1. PPTP - PROTOCOLO DE TÚNEL PUNTO A PUNTO

Es quizá el protocolo más sencillo de entunelamiento de paquetes. Es usado, en general, por pequeñas empresas para realizar sus VPNs LAN-to-LAN, y en topologías de acceso remoto, para trabajadores teleconmutados (teleworkers), tales como vendedores externos o trabajadores que se mantienen en constante movimiento por fuera de sus oficinas.

El protocolo PPTP fue expuesto por el Foro PPTP (PPTP Forum), compuesto por 3Com, Ascend (ahora Lucent), Microsoft, ECI Telematics y USRobotics.

Debido a la integración que hizo Microsoft en sus sistemas operativos, PPTP tuvo gran acogida en el mercado mundial, a tal punto que un protocolo de capa 2 lanzado por Cisco Systems al mismo tiempo, prácticamente no se conoció, L2F (Layer-2-Forwarding).

El protocolo más comúnmente usado para acceso conmutado a Internet es el protocolo punto-a-punto (PPP). PPTP se soporta sobre toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de Internet. PPTP encapsula paquetes PPP usando una versión modificada del Protocolo de Encapsulamiento Ruteado Genérico (GRE – Generic Routing Encapsulation). Dado lo anterior, PPTP no sólo es capaz de encapsular paquetes IP, sino IPX y NETBEUI, los protocolos de red local más usados.

PPTP utiliza los mecanismos de autenticación que generalmente están asociados a PPP tales como PAP y CHAP, una versión mejorada de CHAP llamada MS-CHAP y desarrollada por Microsoft se encuentra en sus sistemas operativos Windows NT, 2000 y XP. Otra mejora que le ha hecho Microsoft al protocolo PPTP es la incorporación del método de cifrado MPPE (Microsoft Point-to-Point Encription).

Una de las ventajas que tiene PPTP por ser un protocolo de nivel 2, es que puede transmitir protocolos diferentes a IP en sus túneles, a diferencia de IPSec que se restringe a trabajar solamente con paquetes IP.

1.1 Relación Entre PPP Y PPTP

PPP es el protocolo más comúnmente usado para acceso a Internet, prácticamente el único, además es usado en algunos enlaces seriales punto a punto WAN. PPP trabaja en la capa 2 del modelo OSI, e incluye métodos para encapsular varios tipos de datagramas para ser transferidos sobre enlaces seriales, entre ellos IP, IPX y NETBEUI. El protocolo PPTP depende de PPP para crear la conexión conmutada entre el cliente y el servidor de acceso a la red. PPTP confía las siguientes funciones a PPP:

- Establecimiento y finalización de la conexión física.
- Autenticación de los usuarios.
- Creación de datagramas PPP.

Luego que el enlace PPP es creado, el protocolo PPTP define dos diferentes tipos de paquetes: paquetes de control y paquetes de datos, cada uno de los cuales es asignado a diferentes canales lógicos. PPTP separa los canales de control y de datos usando un flujo de control que corre sobre TCP y un flujo de datos que está encapsulado con cabeceras IP usando GRE.

La conexión TCP es creada entre el cliente y el servidor PPTP. Esta conexión es usada para intercambiar mensajes de control. Los paquetes de datos contienen los datos del usuario, es decir, los datagramas del protocolo de capa de red usado. Los paquetes de control (control del enlace) son enviados periódicamente para indagar sobre el estado del enlace y las señales de manejo entre el cliente y el servidor PPTP. Los paquetes de control también se usan para enviar información de manejo básica del dispositivo y de configuración. Los mensajes de control establecen, mantienen y finalizan un túnel PPTP.

Después de que el túnel PPTP se ha establecido, los datos del usuario son transmitidos entre el cliente y el servidor PPTP. Estos datos son transmitidos en datagramas IP contenidos dentro de los paquetes PPP.

Los datagramas IP son creados usando una versión modificada del protocolo GRE (Generic Routing Encapsulation); esta modificación consiste en incluir un identificador de los host que puede ser usado para controlar los privilegios de acceso y la capacidad de reconocimiento, la cual es usada para monitorear la velocidad de transferencia a la cual los paquetes están transmitiéndose en el túnel.

La cabecera GRE es usada para encapsular el paquete PPP dentro del datagrama IP. La información útil del paquete (payload) es esencialmente el paquete PPP original enviado por el cliente. Dado que PPTP opera con un protocolo de capa 2, debe incluir una cabecera que depende del medio en el cual el túnel está transmitiendo, esta puede ser Ethernet, Frame Relay o PPP. La Figura 3.1 muestra la estructura en los diferentes sitios de un túnel de un paquete IP usando encapsulación PPTP desde el sistema cliente hasta la LAN corporativa.

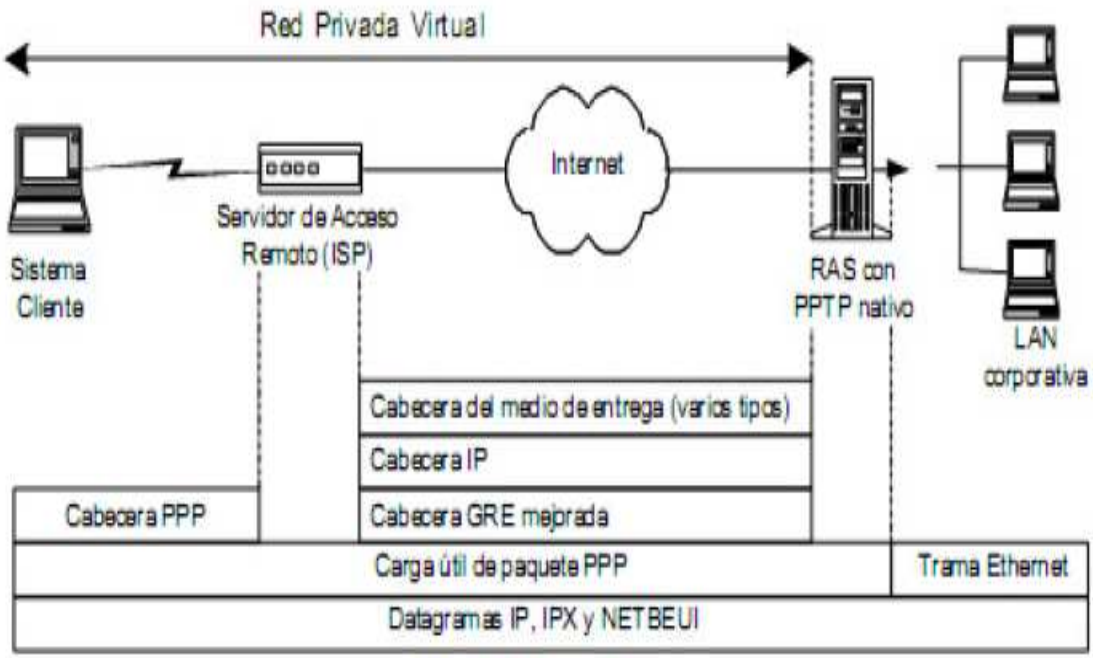

Figura 3.1 Estructura de un Túnel PPTP

1.2 Componentes de una VPN PPTP

Servidores PPTP**,** Un servidor PPTP tiene dos funciones básicas, la primera es actuar como el punto final del túnel PPTP y la segunda es reenviar los paquetes a y desde el computador en la red privada. Para reenviar los paquetes al computador destino, el servidor desencapsula el paquete PPTP obteniendo el nombre del computador o la dirección IP privada que se encuentra dentro de este. Una de las características de los servidores PPTP es la de poder filtrar únicamente el tráfico PPTP dependiendo de si esta condición aparece o no en el perfil del usuario, de esta manera, se puede restringir a un usuario para que se conecte a la red local o se conecte a Internet. Por lo general los servidores PPTP están en las premisas de la red corporativa, en algunos casos el servidor PPTP está ubicado dentro de la red privada y está protegido por el firewall (zona militarizada). Cuando esto ocurre, es necesario abrir el puerto TCP 1723, o si el firewall permite filtrar no por puerto sino por protocolo, se deberá permitir el protocolo GRE (puerto 47).

Software Cliente PPTP**,** Como se dijo anteriormente, si el NAS del ISP soporta PPTP no se necesita ningún software o hardware adicional en el extremo final del cliente, solamente que éste pueda establecer una conexión PPP. Por otro lado, si el ISP no soporta PPTP, el cliente deberá utilizar un software cliente PPTP en su computador para poder crear el túnel. La mayoría de los sistemas operativos cuentas con un cliente PPTP nativo.

Servidores de Acceso a la Red**,** Los servidores de acceso a la red también llamados servidores de acceso remoto o concentradores de acceso, son los encargados de soportar las conexiones PPP de una gran cantidad de clientes que se conectan a este por medio de enlaces telefónicos conmutados. Sus funciones van desde el establecimiento de la conexión física (modulación, demodulación, compresión de datos, corrección de errores, etc.) hasta labores de enrutamiento presentes en la capa 3 del modelo OSI. Dentro de un túnel PPTP se pueden encontrar NAS actuando como clientes PPTP o simplemente como un concentrador de acceso PPP. PPTP permite que las funciones realizadas por un servidor de acceso a la red (NAS) sean separadas usando una arquitectura cliente-servidor. Comúnmente, las siguientes funciones son implementadas por un NAS:

1. Brindar una interfaz física entre la red telefónica pública conmutada y los módems. Esto incluye conversiones A/D y D/A, conversiones síncronas a asíncronas y manipulaciones de flujos de datos.
2. Terminación lógica de enlaces PPP.
3. Autenticación de enlaces PPP.
4. Sumarización de canales (protocolo multilink PPP).
5. Terminación lógica de protocolos de control de red (NCP).
6. Enrutamiento multiprotocolo y bridging.

PPTP divide estas funciones entre los dos componentes que se definen en el protocolo, a saber PAC y PNS. El PAC o concentrador de acceso PPTP es el responsable de las funciones 1, 2 y algunas veces 3. El PNS o servidor de red PPTP, es el responsable de las funciones 3, 4, 5 y 6.

El protocolo PPTP es única y exclusivamente implementado entre el PAC y el PNS. Un PAC puede atender muchos PNSs. Un único PNS puede ser asociado a muchos PACs.

1.3 Estructura del Protocolo

PPTP define una conexión de control entre cada pareja PAC-PNS la cual opera sobre TCP; y un túnel IP operando sobre la misma pareja PAC-PNS el cual es usado para transportar paquetes PPP con encapsulamiento GRE.

1.4 Conexión de Control

Antes que el entunelamiento PPP ocurra entre un PAC y un PNS, una conexión de control debe ser establecida entre ellos. La conexión de control es una sesión TCP que mantiene control sobre la llamada e intercambia mensajes de información. Por cada pareja PAC-PNS debe existir una conexión de control y un túnel. La conexión de control es la responsable por el establecimiento, el manejo y la liberación de las sesiones que existen en el túnel, esto lo realiza a través del puerto 1723.

1.5 Operación del Túnel

PPTP necesita el establecimiento de un túnel por cada pareja PNS-PAC. Este túnel se utiliza para transportar todos los paquetes PPP de las diferentes sesiones involucradas en la pareja PNS-PAC. Una clave que se encuentra presente en la cabecera GRE indica qué paquetes PPP pertenecen a qué sesión. De ésta manera, los paquetes PPP son multiplexados y desmultiplexados sobre un único túnel existente entre una pareja PNS-PAC. El valor del campo Clave es definido dentro del proceso de establecimiento de la llamada.

La cabecera GRE también contiene información de reconocimiento y de secuencialización con la cual se realiza control de congestión y detección de errores en el túnel. Los datos del usuario transportados por el protocolo PPTP son esencialmente paquetes de datos PPP. Los paquetes PPP son transportados entre el PAC y el PNS, encapsulados en paquetes GRE los cuales a su vez son transportados sobre IP. Los paquetes encapsulados PPP son esencialmente paquetes de datos PPP sin ningún elemento de tramado de medio específico. Los paquetes IP transmitidos sobre los túneles entre un PAC y un PNS tienen la estructura general que se muestra en la Figura 3.2.

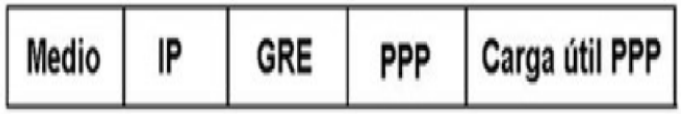

Figura 3.2 Formato del Paquete IP

1.6 Cabecera Mejorada GRE

La cabecera GRE usada por PPTP es una versión ligeramente mejorada de la especificación estándar del protocolo GRE. La principal diferencia es la definición de un nuevo campo de reconocimiento de número (acknowledgment number), usado para determinar si un paquete particular GRE o un conjunto de paquetes ha arribado al lado remoto del túnel. Esta capacidad de reconocimiento no es usada en conjunto con ningún tipo de retransmisión, en vez de eso, se usa

para determinar la velocidad de transferencia a la cual los paquetes de datos del usuario son transmitidos sobre el túnel.

1.7 Cifrado en PPTP

La trama PPP se cifra con el cifrado punto a punto de Microsoft (MPPE, Microsoft Point-to-Point Encryption) mediante claves de cifrado generadas en los procesos de autenticación MS-CHAP, MS-CHAP v2 o EAP-TLS. Los clientes de red privada virtual deben utilizar el protocolo de autenticación MSCHAP, MS-CHAP v2 o EAP-TLS para poder cifrar las cargas de las tramas PPP. PPTP aprovecha el cifrado PPP subyacente y encapsula una trama PPP cifrada anteriormente. Una llave de encriptación es generada usando una mínima parte del password situados en cliente y server. El RSA RC4 standard es usado para crear estos 40 bits (128 dentro de EEUU y Canadá) de llave de sesión basada en el password de un cliente. Esta llave es después usada para encriptar y desencriptar todos los datos intercambiados entre el server PPTP y el cliente. Los datos en los paquetes PPP son encriptados. El paquete PPP que contiene un bloque de datos encriptados es después metido en un datagrama IP para su enrutamiento.

1.8 Filtrado de Paquetes PPTP

Esta opción incrementa el rendimiento y fiabilidad de la seguridad de red si esta activada en el servidor PPTP. Cuando esta activa acepta y enjuta solo los paquetes PPTP de los usuarios autorizados. Esto prevé el resto de paquetes entren el red privada y en el servidor de PPTP.

1.9 Control de Acceso a los Recursos de la Red

Después de la autenticación, todo el acceso a la LAN privada continúa usando las estructuras de seguridad de la misma LAN. El acceso a recursos en devices NTFS u otros recursos de la red requieren los permisos correctos de cada usuario, tal como si estuvieses conectado físicamente dentro de la LAN. La existencia de un Controlador de Dominio por ejemplo, tiene validez en esta configuración.

2. L2TP - PROTOCOLO DE TÚNEL DE CAPA 2

L2TP fue creado como el sucesor de PPTP y L2F. Las dos compañías abanderadas de cada uno de estos protocolos, Microsoft por PPTP y Cisco porL2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 y así lograr su estandarización por parte de la IETF.

Como PPTP, L2F fue diseñado como un protocolo de entunelamiento usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el entunelamiento de éste último no depende de IP y GRE, permitiéndole trabajar con otros medios físicos por ejemplo Frame Relay. Paralelamente al diseño de PPTP, L2F utilizó PPP para autenticación de usuarios accesando vía telefónica conmutada, pero también incluyó soporte para TACKCS+ y RADIUS.

Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión. Hay dos niveles de autenticación del usuario: primero, por la ISP antes de crear el túnel; segundo, cuando la conexión está configurada y la autenticación la realiza el Gateway corporativo.

Todas las anteriores características de L2F han sido transportadas a L2TP. Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de Internet a un sitio destino. Sin embargo, como se ha mencionado anteriormente, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo transporte sobre una amplia variedad de medios de empaquetamiento tales como X.25, Frame Relay y ATM.

Dado que L2TP es un protocolo de capa 2, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI. Microsoft incluye L2TP a partir del sistema operativo Windows 2000, ya que las mejoras de L2TP con respecto a PPTP saltan a la vista.

2.1 Componentes Básicos de un Túnel L2TP

Concentrador de acceso L2TP (LAC)**,** es un nodo que se encuentra en un punto extremo de un túnel L2TP. El LAC se encuentra entre un LNS y un sistema remoto y reenvía los paquetes a y desde cada uno. Los paquetes enviados desde el

LAC hasta el LNS van tunelizados. En algunas ocasiones el sistema remoto actúa como un LAC, esto se presenta cuando se cuenta con un software cliente LAC.

Servidor de Red L2TP (LNS), es un nodo que se encuentra en un punto extremo de un túnel L2TP y que interactúa con el LAC, o punto final opuesto. El LNS es el punto lógico de terminación de una sesión PPP que está siendo tunelizada desde un sistema remoto por el LAC.

Túnel, un Túnel existe entre una pareja LAC-LNS. El túnel consiste de una conexión de control y de ninguna o más sesiones L2TP. El túnel transporta datagramas PPP encapsulados y mensajes de control entre el LAC y el LNS.

2.2 Topología de L2TP

La Figura 3.3 describe un escenario típico L2TP. El objetivo es tunelizar tramas PPP entre un sistema remoto o un cliente LAC y un LNS localizado en la LAN corporativa. El sistema remoto inicia una conexión PPP a través de la red de telefonía pública conmutada a un LAC. El LAC luego tuneliza la conexión PPP a través de Internet o una nube Frame Relay o ATM a un LNS por donde accesa a la LAN remota corporativa. La dirección del sistema remoto es dada desde la LAN corporativa por medio de una negociación PPP NCP. La autenticación, autorización y acoyuntan puede ser provista por el dominio de la red corporativa remota como si el usuario estuviera conectado a un servidor de acceso de la red directamente. Este escenario pertenece a una Sesión Obligatoria L2TP.

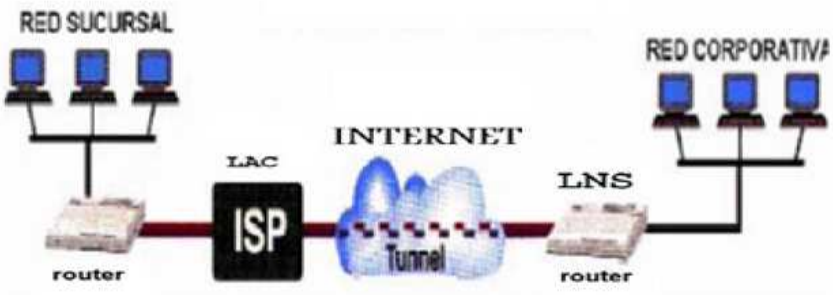

Figura 3.3 Escenario Típico L2TP

En una Sesión Voluntaria, un cliente LAC (un host que corre L2TP nativo) puede también crear un túnel hasta la LAN corporativa sin usar un LAC externo. En este

caso, el host tiene un software cliente LAC y previamente ha estado conectado a la red pública, tal como Internet. Una conexión PPP virtual es luego creada y el software cliente LAC hace un túnel hasta el cliente LNS. Como en el caso anterior, el direccionamiento, la autenticación y la autorización pueden ser provistos por el dominio de la LAN corporativa remota.

2.3 Estructura del Protocolo L2TP

L2TP utiliza dos tipos de mensajes, los mensajes de control y los mensajes de datos. Los mensajes de control son usados en el establecimiento, mantenimiento y finalización de túneles y llamadas. Los mensajes de datos son usados para encapsular tramas PPP que están siendo transportados sobre el túnel. Los mensajes de control utilizan un canal de control confiable con el cual L2TP garantiza la entrega. Los mensajes de datos no son retransmitidos cuando ocurren pérdidas de paquetes.

La Figura 3.4 muestra la relación de las tramas PPP y los mensajes de control con los canales de datos y control L2TP respectivamente. Las tramas PPP son transportadas sobre un canal de datos no confiable y son encapsuladas primero por una cabecera L2TP y luego por una cabecera de transporte de paquetes que pueden ser UDP, Frame Relay o ATM. Los mensajes de control son enviados sobre un canal de control L2TP confiable, el cual transmite paquetes en banda sobre el mismo transporte de paquetes. Para esto se requiere que números de secuencia estén presentes en todos los mensajes de control. Los mensajes de datos pueden usar esos números de secuencia para reordenar paquetes y detectar pérdidas de los mismos.

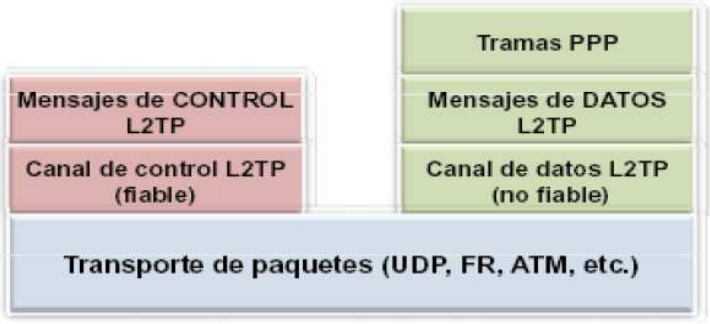

Figura 3.4 Relación Entre Tramas PPP y Mensajes L2TP

2.4 Formato de una Cabecera L2TP

Los paquetes L2TP para el canal de control y el canal de datos comparten un formato de cabecera en común, la Figura 3.5 muestra el formato dicha cabecera L2TP:

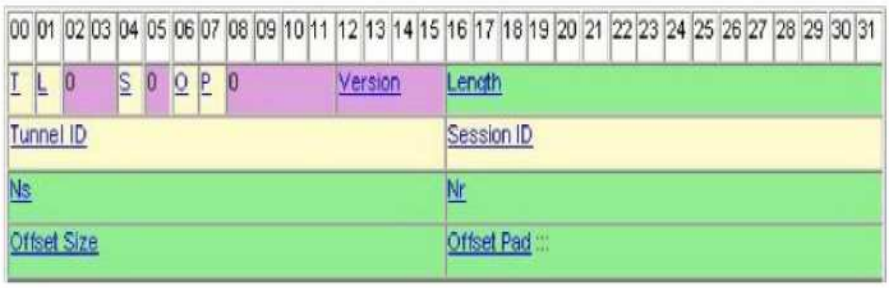

Figura 3.5 Formato de Cabecera L2TP

- T: Message Type. 1 bit. Especifica si es un mensaje de control (0) o datos (1).
- L: Used Length. 1 bit. Mensajes de Control deben tener configurado este bit.
- S: Used Sequence. 1 bit. Si está configurado, los campos Ns y Nr también deben estar configurados. Los mensajes de Control deben tener configurado este bit.
- O: Used Offset. 1 bit. Los mensajes de Control deben tener configurado este bit.
- P: Priority. 1 bit. Este debe recibir tratamiento especial en la cola local. Version: 4 bits. Indica la versión del protocolo L2TP. Debe ser configurado a 2, el valor 1 es reservado para detección L2F.
- Length: 16 bits. Opcional. El tamaño total del mensaje, este campo existe si L está configurado.
- Tunnel ID: 16 bits. Indica el identificador de control de la conexión, los túneles son nombrados por identificadores locales.
- Session ID: 16 bits. Indica el identificador de la sesión dentro de un túnel.
- Ns: Sequence Number. 16 bits. Optional. Indica el número de secuencia para el mensaje de control o los datos actuales.
- Nr: Sequence Number Expected. 16 bits. Optional. Indica el número de secuencia esperado en el siguiente mensaje de control a ser recibido.

- Offset Size: 16 bits. Optional. Especifica el número de bytes donde la cabecera finaliza y comienzan los datos.
- Offset Pad: Relleno.

Los componentes de mayor importancia son aquellos que definen el punto final de un túnel basado en este protocolo, entre los cuales se encuentra el concentrador de acceso L2TP (LAC) como parte del equipamiento del ISP, y el servidor de red L2TP (LNS).

En el caso de los ISPs además del hardware implementado en el mismo se tiene en cuenta el software necesario requerido que puede ser reducido para el enlace de los clientes móviles, los cuales necesitaran negociar en la primera fase de autentificación de usuarios. Por otro lado, el LNS deberá ser atendido y mantenido por el personal de la empresa, mientras que estas actividades son responsabilidad del ISP con relación al LAC.

2.5 Autenticación en L2TP

La autentificación de un usuario ocurre en 3 fases en L2TP. En la primera fase, el ISP puede usar el número de teléfono de la llamada recibida, el número llamado o el nombre del usuario determinado que el servicio de L2TP requiere y entonces iniciar un túnel de conexión al servidor de red apropiado. Cuando un túnel está establecido, el Concentrador de Acceso (LAC) del ISP asigna un nuevo ID de llamada para identificar la conexión con el túnel e inicia una sesión para devolver la información autentificada. El servidor de red corporativa emprende la segunda fase de autentificación para decidir si acepta o no la llamada. La llamada comienza indicando al ISP el método de autenticación o la información de autentificación de otros. El servidor de red usará esta información para decidir si acepta o rechaza la llamada.

Después que la llamada ha sido aceptada, el servidor de red puede iniciar la tercera fase de autentificación a la capa de PPP, la cual aporta una amplia gama de opciones, incluidos CHAP, MS-CHAP, MS-CHAPv2 y el Protocolo de autenticación extensible EAP (Extensible Authentication Protocol), que admite mecanismos de autenticación de tarjetas token y tarjetas inteligentes.

A través de estas 3 fases de autentificación L2TP garantiza que el usuario final, el ISP y el servidor de red están conectados con quien dicen ser.

2.6 Procesos de una Comunicación L2TP

1. Conexión y comunicación PPP: el cliente remoto usa el protocolo PPP para establecer la conexión con un IPS, la cual constituye la primera fase de autenticación L2TP.
2. Conexión de control L2TP (establecimiento del túnel): es la conexión inicial que hay que establecer entre el LAC y el LNS antes de que se puedan establecer sesiones. El establecimiento de la conexión de control incluye la autenticación de la entidad par por el LNS y la negociación de las facilidades soportadas.
3. Establecimiento de la sesión: una vez establecido el túnel entre el LAC y el LNS se establece una sesión dentro del túnel por cada conexión PPP existente entre LAC y LNS. Cada sesión se corresponde a un flujo de tramas PPP entre el LAC y el LNS. El LAC solicita al LNS que acepte una sesión para una llamada entrante y el LNS solicita al LAC que acepte una sesión para una llamada saliente. Seguidamente se completa el proceso de autenticación PPP entre el usuario remoto y el LNS. A continuación se inicia el envío de paquetes NCP para elegir y configurar uno o más protocolos de red:
   - Ej.: IPCP para indicar que el protocolo de red es IP.
   - Ej.: ECP para encriptar las tramas de la conexión PPP entre el usuario remoto y el LNS.
4. Envío de datos de usuario: el usuario puede empezar el envío de datos a través del túnel. Estos datos van cifrados.
5. Descifrado de los datos por el LNS: el LNS recibe los datos, los descifra y los entrega a la red corporativa. Si el LNS envía información al usuario también la cifra antes de enviarla a través del túnel.

2.7 Comparativa Entre PPTP y L2TP

- Con PPTP, el cifrado de datos comienza después de que la conexión se procese (y, por supuesto, después de la autentificación PPP). Con L2TP, el

cifrado empieza antes de la conexión PPP negociando una asociación de seguridad IPSec.

- Las conexiones PPTP usan MPPE, un método de cifrado basado en el algoritmo de encriptación Rivest-Shamir-Aldeman (RSA) RC-4, y usa llaves de 40, 56 o 128 bits. Las conexiones L2TP usan Data Encryption Standard (DES), con llaves de 56 bits para DES o tres llaves de 56 bits para 3-DES. Los datos se cifran en bloques (bloques de 64 bits para el caso de DES).
- Las conexiones PPTP requieren sólo autentificación a nivel de usuario a través de un protocolo de autentificación basado en PPP. Las conexiones L2TP / IPSec requieren el mismo nivel de autentificación a nivel de usuario y, además nivel de autentificación de máquina usando certificados digitales.
- PPTP requiere que el tránsito entre - redes sea una Internetwork IP. L2TP únicamente requiere que los medios de túnel proporcionen conectividad de punto a punto orientada al paquete. L2TP puede ejecutarse sobre IP (usando UDP), Frame Relay, X.25, ATM.
- PPTP sólo puede soportar un túnel entre dos puntos extremos. L2TP permite el uso de túneles múltiples entre puntos extremos. L2TP proporciona autenticación de túnel, mientras que PPTP no lo hace, sin embargo, cuando ya sea que PPTP o L2TP se ejecute sobre IPSec, la autenticación de túnel es proporcionada por IPSec para que no sea necesaria la autenticación de túnel nivel 2.

2.8 Problemas de L2TP

A pesar de que L2TP ofrece un acceso con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.

- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.
- A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

3. EL PROTOCOLO IPSEC

IPSec es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPSec existe en el nivel de red en OSI, para extender IP para el propósito de soportar servicios más seguros basados en Internet. Una de las características más importantes de IPSec es su compatibilidad con las redes IP actuales.

3.1 Descripción del Protocolo

IPSec en realidad es un conjunto de estándares para integrar en IP, funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales X509v3.

El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet.

Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de hash. Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno

específico: por ejemplo, como algoritmo de cifrado de clave simétrica IDEA, Blowfish y AES.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que proporcionan mecanismos de seguridad para proteger tráfico IP.
- Un protocolo de gestión de claves Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

***El Protocolo AH*,** El protocolo AH es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Esto es, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no has sido alterados en tránsito, sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser visto por terceros.

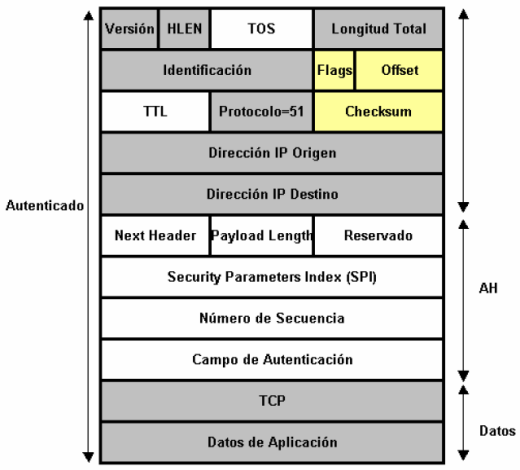

Figura 3.6 Estructura de una Datagrama AH

Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo (ver Figura 3.6).

El funcionamiento de AH se basa en un algoritmo HMAC, esto es, un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de unos datos de entrada y una clave, siéndola salida una pequeña cadena de caracteres que denominamos extracto. Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y a la persona que lo ha generado, puesto es la única que conoce la clave.

En la Figura 3.7 se muestra el modo que funciona el protocolo AH. El emisor calcula el extracto de mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete.

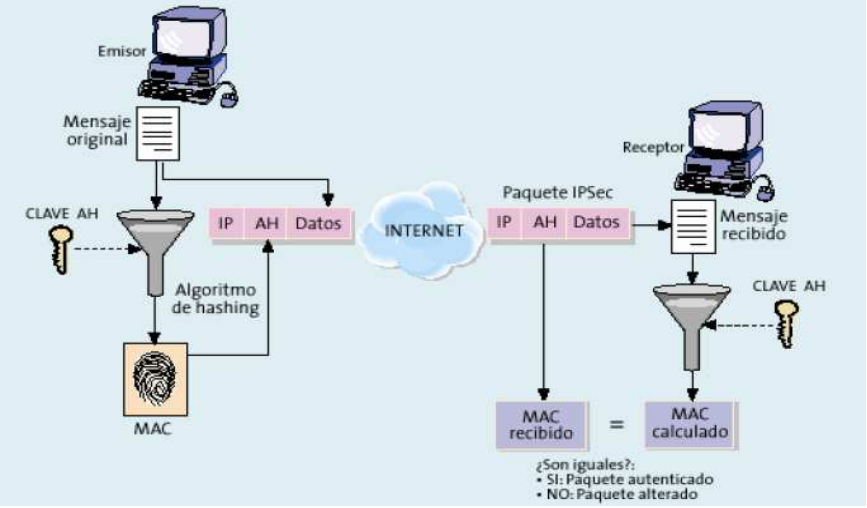

Figura 3.7 Funcionamiento del Protocolo AH

Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en tránsito y que procede efectivamente del origen esperado. Si analizamos con detalle el protocolo AH, podemos concluir que su seguridad reside en que el cálculo del extremo (MAC) es imposible sin conocer la clave, y que dicha clave (en la Figura 1.7, clave AH) sólo la conocen el emisor y el receptor.

***El Protocolo ESP*,** El objetivo principal del protocolo ESP (Encapsulating Security Payload) es proporcionar confidencialidad, para ello especifica el modo

de cifrar los datos que desean enviar y como este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo). En la Figura 3.8 se muestra la estructura de un datagrama ESP, en laque se observa cómo el contenido o carga útil viaja cifrado.

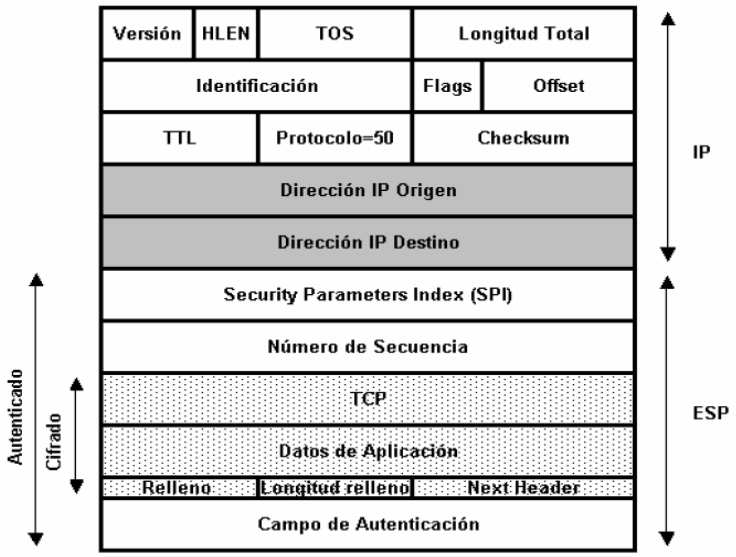

Figura 3.8 Estructura de una Datagrama ESP

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica, típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8º16 bytes, en la mayoría de los casos). Por esta razón existe un campo de relleno, tal como se observa en la Figura 3.8, el cual tiene una función adicional: es posible añadir caracteres de relleno al campo de datos para ocultar así su longitud real y, por tanto, las características del tráfico.

Un atacante suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque estén cifradas, tales como el retardo entre paquetes y su longitud. La función de relleno está pensada para dificultar este tipo de ataques.

En la Figura 3.9 se representa cómo el protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales.

Está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave así como en que la clave ESP únicamente la conocen el emisor y el receptor.

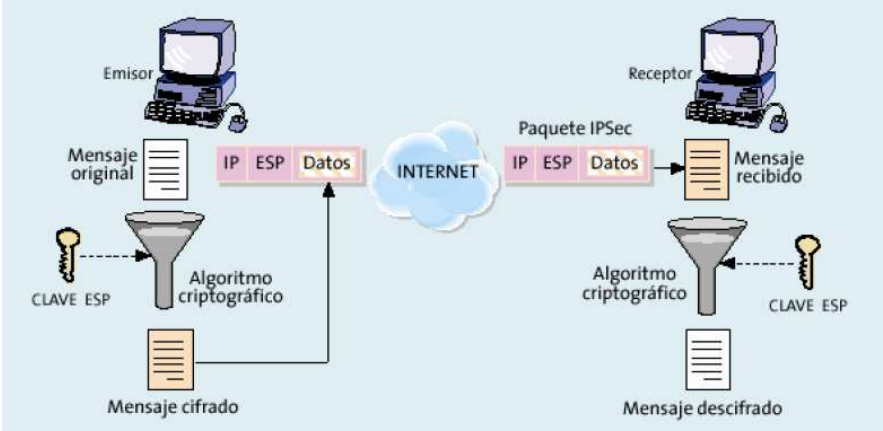

Figura 3.9 Estructura de una Datagrama ESP

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP y también de AH, como hemos visto anteriormente.

Asimismo, es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de hash como en el resto de parámetros comunes que

utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE, que se explicará más adelante.

3.2 Los Modos de Transporte y Túnel

Antes de entrar en los detalles del protocolo IKE es necesario explicar los dos modos de funcionamiento que permite IPSec. Tanto ESP como AH proporcionan dos modos de uso:

El Modo Trasporte**,** En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

El Modo Túnel**,** En éste contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

En la Figura 3.10a se representan dos host que entienden IPSec y que se comunican de forma segura. Esta comunicación se realiza en modo transporte, por tanto, la información que se protege es únicamente el protocolo TCP o UDP, así como los datos de aplicación.

En la Figura 3.10b se muestran dos redes que utilizan gateways IPSec para conectarse y, por tanto, emplean una solución en modo túnel. Se puede ver que la comunicación se realiza a través de una red de datos pública, entre un PC situado en una red local con otro PC situado en una red local remota, de modo que entre los gateways IPSec se establece un túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales.

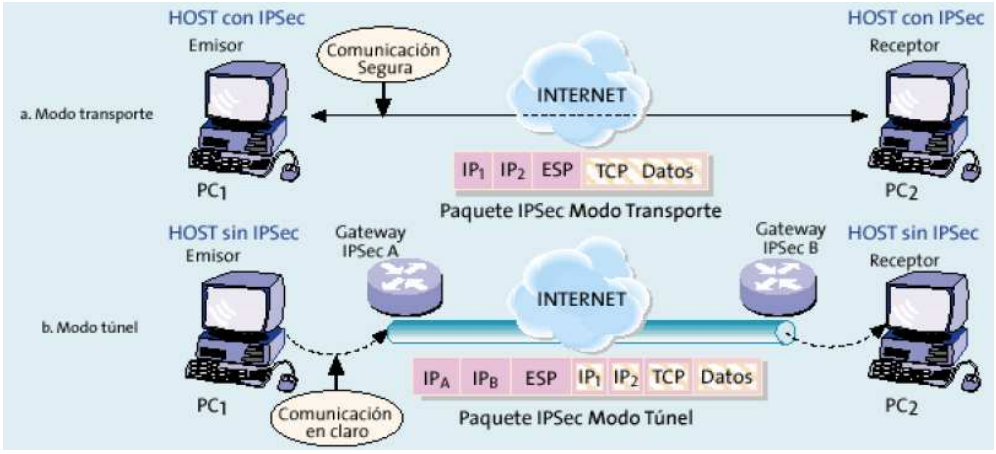

Figura 3.10 Modos de Funcionamiento Transporte y Túnel IPSec

Sin embargo ambos PCs envían y reciben el tráfico en claro, como si estuviesen situados en la misma red local. Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrándose, al mismo tiempo, las funciones de seguridad en un único punto, facilitando así las labores de administración.

3.3 IKE (Internet Key Exchange)

Un concepto esencial en IPSec es el de asociación de seguridad (SA), es una canal de comunicación que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SAs. Una característica importante de IKE es que su utilidad no se limita a IPSec, sino

que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación se lleva a cabo en dos fases:

Primera Fase IKE**,** La fase común a cualquier aplicación, en que ambos nodos establecen un canal seguro y autenticado. Dicho canal seguro consiste mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante el algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación.
Existen varios métodos de autenticación, los dos más comunes se describen a continuación:

- El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre lo indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer comunicación IPSec. Mediante el uso de funciones hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales.
- En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste pueda probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados

requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI (Infraestructura de Clave Pública), cuya integración se tratará con detalle más adelante.

Segunda Fase IKE**,** En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec. Durante esta fase se negocian las características de la conexión AH o ESP y todos los parámetros necesarios.

El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se haya configurado.

El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

Figura 3.11 Funcionamiento del Protocolo IKE

El funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH, se muestra en la Figura 3.11

3.4 Integración de IPSec con una PKI

El uso de una PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean

comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. La existencia de una PKI ofrece otras ventajas, ya que se centraliza el alta y baja de los usuarios, además se posibilita la introducción de tarjetas inteligentes para soportar los certificados, lo cual es muy interesante para la aplicación IPSec en un entorno de tele trabajadores o usuarios móviles.

Bajo el nombre de PKI se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y, eventualmente, renovar los certificados digitales para una comunicad de usuarios. En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras que la función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec. Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al dispositivo (tal como su nombre DNS, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la Autoridad de Certificación (CA) integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer una copia del certificado de la propia CA.

Los protocolos para la interacción de los dispositivos con una PKI no están especificados en ninguno de los protocolos de IPSec. Todos los fabricantes utilizan X.509v3 como formato común de los certificados, así como los estándares de la serie PKCS para la solicitud y descarga de certificados. Sin embargo, el protocolo de comunicaciones, mediante el cual de los dispositivos IPSec dialogan con la PKI, no está totalmente estandarizado. Esto hace que existan varias alternativas según el fabricante de que se trate.

En general los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido.

En la actualidad, la mayoría de los nodos IPSec realizan la validación de los certificados mediante consultas de la Lista de Certificados Revocados (CRL), que

se almacena en el directorio de la PKI. Para ello, cada uno de los nodos mantendrá una copia de la CRL, que actualizará periódicamente mediante una consulta LDAP al directorio PKI. Típicamente, los periodos de actualización de la CRL serán del orden de horas, de modo que existirá cierto retardo desde que la PKI revoca un certificado hasta que todos los dispositivos tengan constancia de dicha revocación.

Figura 3.12 Integración de una PKI con una IPSec

En la Figura 3.12 se representan los flujos de comunicación entre una PKI y un nodo IPSec. Inicialmente, cada uno de los nodos genera un par de claves (pública y privada) y envía una petición de certificado a la CA, en la que se incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la CA; a continuación, la CA genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros dispositivos. Periódicamente los dispositivos IPSec accederán al directorio de la PKI para actualizar la CRL.

3.5 Servicios de Seguridad Ofrecidos por IPSEC

***Integridad y Autenticación*,** El protocolo AH es el más adecuado si no se requiere cifrado. La opción de autenticación del protocolo ESP ofrece una funcionalidad

similar, aunque esta protección, a diferencia de AH, no incluye la cabecera IP. Como se comentó anteriormente, esta opción es de gran importancia para aquellas aplicaciones en las cuales es importante garantizar la invariabilidad del contenido de los paquetes IP.

Confidencialidad, El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autenticación, ya que si no se garantiza la integridad de los datos el cifrado es inútil. Esto es debido a que aunque los datos no pudiesen ser interpretados por nadie en tránsito, éstos podrían ser alterados haciendo llegar al receptor del mensaje tráfico sin sentido que sería aceptado como tráfico válido.

Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del paquete, de modo que se oculta la verdadera longitud del mismo. Esta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado.

Detección de Repeticiones**,** La autenticación protege contra la suplantación de la identidad IP, sin embargo un atacante todavía podría capturar paquetes válidos y reenviarlos al destino. Para evitar este ataque, tanto ESP como AH incorporan un procedimiento para detectar paquetes repetidos. Dicho procedimiento está basado en un número de secuencia incluido en la cabecera ESP o AH, el emisor incrementa dicho número dicho número por cada datagrama que envía y el receptor lo comprueba, de forma que los paquetes repetidos serán ignorados.

Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cualquiera de los dos protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.

Control de Acceso**,** Involucra autenticación y autorización, dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican

mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. Es conveniente aclarar que una autenticación valida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Por ejemplo, puede utilizarse IPSec para permitir el acceso desde una sucursal a la red local del centro corporativo, pero impidiendo el paso de tráfico hacia maquinas especialmente protegidas.

No Repudio, El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autenticación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo.

4. VPN-SSL

Combinar seguridad y sencillez es lo que prometen las Redes Virtuales Privadas basadas en SSL, La tecnología VPN-SSL (ó SSL-VPN) nació de las necesidades de las empresas que surgen a causa de estos problemas y limitaciones. Esto significó un cambio de paradigma en la propia percepción de la seguridad, acceso remoto, el objetivo de una VPN de acceso remoto ya no era sólo la construcción de los túneles de acceso seguro entre dispositivos remotos y redes de confianza, sino proporcionar a los usuarios autenticados autorizados y con acceso a la información confidencial. La introducción de VPN-SSL trajo una revolución hacia la transparencia en la entrega de soluciones de acceso remoto VPN.

Los objetivos iniciales de la primera generación de VPN-SSL son facilitar el acceso a través de cortafuegos y una solución de acceso remoto que trabaja desde cualquier lugar independientemente de los dispositivos NAT's y un clientes VPN's.

Tradicionalmente IP (IPSec) entre otras, requiere la instalación de software cliente un equipo remoto para poder establecer una conexión, mientras que SSL-VPN cliente no necesita instalación y ofrece la funcionalidad de un VPN clientes o Web VPN. Los usuarios pueden tener acceso a las aplicaciones o archivos compartidos sólo con

navegadores web estándares, esta es sin dudas una de las mayores ventajas de esta tecnología (se dice que si existe conexión HTTPS entonces debe funcionar).

Para las empresas, SSL-VPN ofrece versatilidad, facilidad de uso, seguridad y acceso remoto desde cualquier lugar a socios y clientes, usando los más variados dispositivos como computadoras portátiles, dispositivos móviles, equipos de casa y público. Las implementaciones por software más comunes bajo esta tecnología son SSTP (Secure Socket Tunneling Protocol) de Microsoft y Open VPN del movimiento Open Sourse, mientras que por hardware hoy en día existen muchos dispositivos que la soportan.

4.1 SSL/TLS Secure Sockets Layer/Transport Layer Security

TLS (Transport Layer Security - Seguridad de la Capa de Transporte) es el sucesor del SSL (Secure Sockets Layer). Ambos protocolos se utilizan para proporcionar comunicaciones seguras en Internet, usando un modelo de autenticación y privacidad de la información entre extremos sobre Internet mediante criptografía. Esto es fundamental para mantener la seguridad en el comercio vía Internet.

SSL fue diseñado de manera modular (extensible), con soporte para compatibilidad hacia delante y hacia atrás y negociación entre las partes (peer-topeer). Normalmente, en SSL sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (PKI) para los clientes. Esta tecnología permite permiten a las aplicaciones cliente servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente y mantener la integridad del mensaje.

Las primeras implementaciones de SSL sólo podían usar claves simétricas de 40 bits como máximo, ya que el gobierno de los EEUU imponía restricciones sobre la exportación de tecnología criptográfica. Esta clave era de 40 bits ya que las agencias de seguridad nacional americanas podían atacarla mediante fuerza bruta y poder leer así el tráfico cifrado, mientras que los posibles atacantes con menores recursos no podrían leerlo.

Finalmente, después de diferentes juicios y la aparición de mejores productos criptográficos diseñados en otros países, se rebajaron las restricciones de exportación de tecnología criptográfica, desapareciendo casi por completo la limitación de claves de 40 bits. Actualmente se usan claves de 128 bits, o incluso más, para las claves de cifrado simétricas. Las implementaciones actuales proporcionan las siguientes opciones:

- **Para criptografía de clave pública**: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.
- **Para cifrado simétrico**: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).
- **Con funciones hash**: MD5 o de la familia SHA.

4.2 Arquitectura de SSL

SSL trabaja sobre el protocolo TCP y por debajo de protocolos como HTTP, IMAP, LDAP, etc., y puede ser usado por todos ellos de forma transparente para el usuario. Opera entre la capa de transporte y la capa de sesión del modelo OSI (o entre la capa de transporte y la de aplicación del modelo TCP-IP) y está formado, a su vez, por dos capas y cuatro componentes bien diferenciados (ver Figura 3.15).

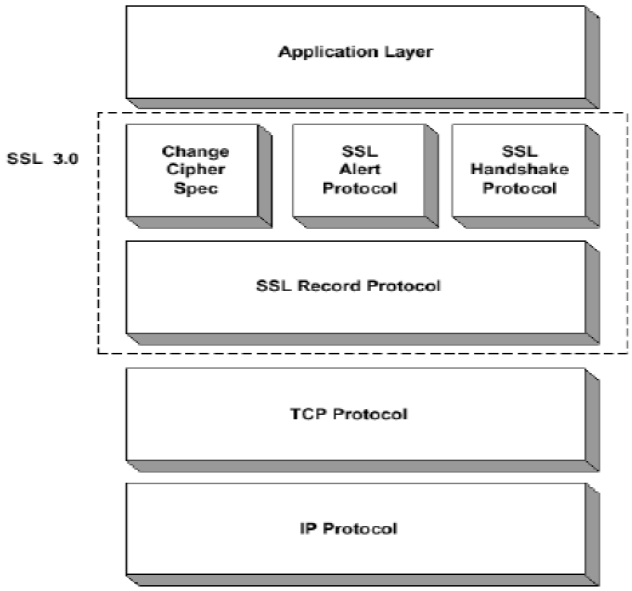

Figura 3.13 Estructura del Protocolo SSL

El protocolo de registro (Record Protocol) se encarga de encapsular el trabajo de los elementos de la capa superior, construyendo un canal de comunicaciones entre los dos extremos objeto de la comunicación.

El verdadero corazón de SSL está en ***el protocolo de Handshake*** que es el encargado de intercambiar la clave que se utilizará para crear un canal seguro mediante un algoritmo eficiente de cifrado simétrico. También es responsabilidad de este protocolo coordinar los estados de ambos extremos de la transmisión.

El protocolo de Alerta es el encargado de señalizar problemas y errores concernientes a la sesión SSL establecida.

Por último, el ***Change Cipher Spec Protocol*** está formado por un único mensaje consistente en un único byte de valor 1 y se utiliza para notificar un cambio en la estrategia de cifrado.

4.3 Funcionamiento Básico de SSL

El protocolo de Handshake es el encargado de negociar los atributos de la sesión SSL que permitirán construir un canal seguro de comunicaciones. En primer lugar el cliente envía un mensaje Client Hello al servidor el cual debe de responder con un mensaje similar de Server Hello. Estos mensajes son utilizados para dar a conocer ciertas características de ambos: versión del protocolo usada, algoritmos de cifrado conocidos y preferidos, funciones hash y métodos de compresión a utilizar. En este momento, además, el servidor asigna un identificador a la sesión y se hace constar la fecha y hora de la misma. Generalmente el servidor, que es el segundo en contestar, elige los algoritmos más fuertes de entre los soportados por el cliente. Si no hay acuerdo en este punto se envía un mensaje de error y se aborta la sesión.

A continuación del mensaje de Server Hello, el servidor puede envíar su Certificado (típicamente un X.509) de forma que sea autenticado por el cliente y que, además, este reciba su clave pública. Si no es así, le envía al cliente su clave pública mediante un mensaje de Server Key Exchange (o también si ha enviado su Certificado y este es únicamente para firma y autenticación). Está claro que al menos uno de estos dos mensajes es necesario para establecer el canal seguro. Un

último mensaje que puede enviar el servidor en esta fase de negociación es una solicitud de certificado al cliente. Por último, la fase concluye con el envío, por parte del servidor, de un mensaje de Server Hello Done.

Si el Servidor ha solicitado su certificado al cliente, este debe de responder con él o con un mensaje de alerta indicando que no lo posee. A continuación se envía un mensaje de Client Key Exchange donde el cliente envía al servidor la clave maestra cifrada mediante la clave pública, además un número aleatorio generado por él y que actuará como clave del algoritmo simétrico acordado para el intercambio de datos.

Por último, si el cliente ha enviado un certificado y éste tiene capacidades de firma, enviará adicionalmente un mensaje de Certificate Verify firmado digitalmente con objeto de que el servidor pueda verificar que la firma es válida. En este punto el cliente da por concluida la fase mediante un mensaje de Change Cipher Spec seguido, inmediatamente, de un mensaje de Finished que ya va cifrado mediante los algoritmos y claves recién negociados.

En respuesta, el servidor envía su propio mensaje de Change Cipher Spec y, a continuación, su mensaje de Finished cifrado con los parámetros negociados.

En este momento finaliza la fase de Handshake y cliente y servidor pueden intercambiar datos libremente. Podemos ver un esquema de este intercambio de mensajes en la Figura 3.16.

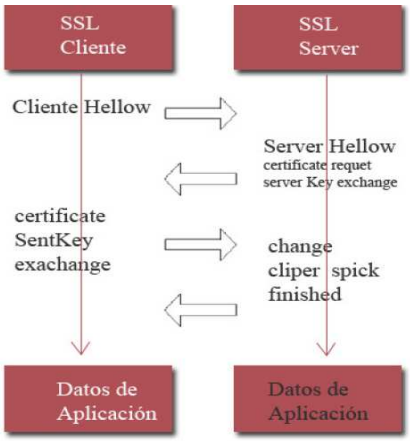

Figura 3.14 Intercambio de Mensajes en SSL

Durante la transmisión de datos los mensajes el protocolo de registro se encarga de fragmentar y comprimir cada mensaje, para luego aplicarle una función hash a cada uno de los bloques, proceso con el cual pretende asegurar la integridad de los mismos. Por último realiza el cifrado de los datos y los envía al otro extremo donde el mismo protocolo realizará un proceso inverso de reconstrucción.

Una sesión SSL puede comprender múltiples conexiones. Adicionalmente, se pueden establecer múltiples sesiones SSL simultáneas, cada una de ellas es controlada por una máquina de control de estados.

4.4 Aplicaciones e Implementaciones de SSL

Una de las ventajas de SSL es que es independiente del protocolo de aplicación, ya que es posible ubicarlo por encima del mismo en forma transparente. Este protocolo tiene multitud de aplicaciones en uso actualmente, la mayoría de ellas son versiones seguras de programas que emplean protocolos que no lo son. Hay versiones seguras de servidores y clientes de protocolos como el HTTP (HTTPS en este caso), NNTP, LDAP, IMAP, POP3, etc.

Existen multitud de implementaciones del protocolo, tanto comerciales como de libre distribución, una de las más populares es la biblioteca Open SSL, que constituye la base del software Open VPN, disponible bajo licencia GNU. El lenguaje Java también incluye soporte para el protocolo con la Extensión de Sockets Seguros de Java (JSSE).

Cada una de las aplicaciones SSL tiene las siguientes propiedades:

- ***Privada:*** después de un proceso inicial de handshake en el cual se define una clave secreta, se envía la información encriptada por medio de algún método simétrico (DES, RC4).
- ***Segura:*** aporta identidad de cada extremo, es autenticada usando métodos de cifrado asimétricos o de clave pública (RSA, DSS).
- ***Confiable:*** el transporte del mensaje incluye un control de la integridad del mismo usando una MAC cifrada con SHA y MD5.

4.5 Conceptos y Técnicas de VPN-SSL

El acceso remoto seguro basado en SSL aglutina diversas tecnologías, basados en cuatro conceptos básicos:

Proxy: todos los dispositivos y software SSL-VPN ofrecen al menos la función de proxy de páginas Web. Cuando el usuario se conecta a un servidor Web, éste descarga la página solicitada y se la envía a su navegador sobre una conexión SSL.

Conversión de aplicaciones: las cosas se complican cuando se trata de cualquier otro dato que no sean una página Web. Surge entonces la conversión de aplicaciones. Cuando, por ejemplo, los dispositivos SSLVPN han de tratar los servidores de ficheros, por lo general hablará como protocolo nativo CIFS (de Microsoft), o FTP. Por ello, habrá de convertirlos a HTTP y HTML, a fin de que el usuario final vea el servidor de ficheros como si fuera una página Web.

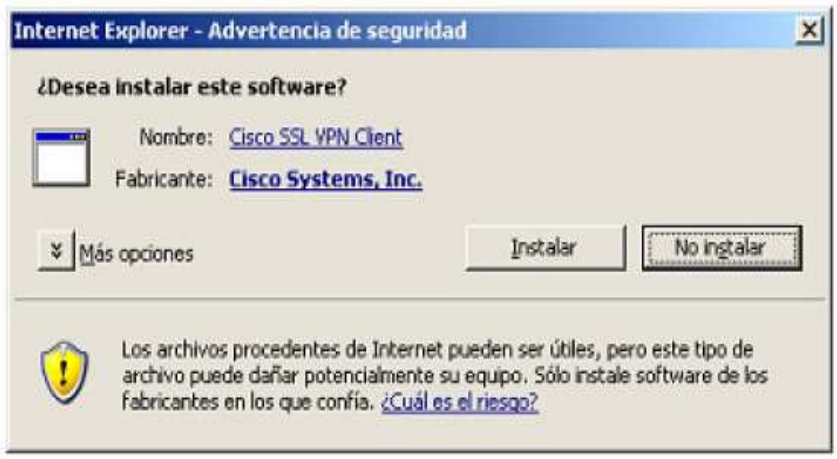

Figura 3.15 Advertencia de Instalación de Plugins en Internet Explorer

Port forwarding: pero la conversión de aplicaciones sólo funciona efectivamente con ciertas transacciones. Se impone, entonces, la técnica port forwarding, que requiere en el sistema cliente una herramienta del tipo Java o ActiveX (Pluning de Microsoft). Consiste en dedicar a cada aplicación un puerto determinado en el que se tunelizan los paquetes dentro de conexiones SSL. El server SSL-VPN los abre y los envía al servidor de aplicaciones. Se trata de una técnica muy efectiva pero

muestra serias limitaciones, por ejemplo, sólo funciona con aplicaciones muy predecibles en cuanto a sus requerimientos y necesidades de conectividad de red. La figura 3.17 muestra un mensaje de advertencia en el navegador Internet Explorer, antes la instalación de un ActiveX correspondiente al software cliente de un dispositivo de la empresa Cisco.

Extensión de red: conecta el sistema del usuario final a la red corporativa mediante controles de acceso exclusivamente basados en información de nivel de red, como dirección IP de destino y número de puerto. Dependen del sistema operativo que se utiliza y requiere acceso administrativo al sistema local. Las extensiones de red SSL-VPN corren en lo alto del protocolo SSL, sacrificando la mayor seguridad que ofrece IPSec.

4.6 Inconvenientes de las VPN-SSL

Secure Sockets Layer (SSL) para realizar el acceso remoto se basa en un concepto simple, utilizar la encriptación y capacidades de autenticación incorporado en todos los navegadores web para proporcionar acceso remoto seguro a aplicaciones corporativas.

Una ironía de las VPN-SSL es que su activo más importante es su aspecto más problemático. La libertad y la movilidad del navegador significa que los usuarios puedan ejecutar aplicaciones y recursos de la red de acceso desde cualquier parte, un kiosco del aeropuerto, un café Internet, incluso la casa de un amigo. Mientras que la libertad puede aumentar la productividad, también expone su red a un número ilimitado de equipos de seguridad cuyo estado es desconocido. Su red puede experimentar un mayor riesgo de virus, troyanos y otros códigos maliciosos, tales como capturadores de teclado.

El acceso basado en navegador tiene otras complicaciones también como la de autenticación de usuario, por defecto está limitado a un nombre de usuario y contraseña, que es notoriamente inseguro. Por último, los costos de los dispositivos VPN-SSL (Hardware) son elevados, aunque exista una variedad de precios entre las opciones que ofrecen los distintos fabricantes, existe una gran diferencia de precios con otros dispositivos que manejan protocolo como L2TP e IPSec. Esta última desventaja o inconveniente se podría decir que es relativa,

porque una implementación IPSec puede ser redituable en costos de hardware pero costosa en tiempo de configuración y mantenimiento.

4.7 Ventajas de SSL-VPN sobre IPSec

Las principales ventajas son las siguientes:

- SSL-VPN son a menudo mucho menos costoso que el despliegue de redes VPN IPSec. Esto se debe a que, con clientes SSL-VPN, no hay costo de licencias de software de propiedad del cliente, sin gastos generales de administración involucrados en la instalación de software cliente, y menos tiempo necesario para el apoyo técnico de clientes debido a la facilidad de uso.
- SSL-VPN permite a las organizaciones a crear la identidad del usuario de acceso basado en políticas, que ofrece acceso a la red granular a los empleados, socios y clientes sobre la base de la identidad del usuario y el perfil de trabajo.
- SSL utiliza el puerto TCP 443, que normalmente se abre en los cortafuegos, trabajará a través de firewalls sin ninguna configuración especial.
- IPSec usa puertos UDP específicos, si no están en uso, estos puertos estarán bloqueados por el servidor de seguridad.
- SSL-VPN también puede proporcionar una ventaja de seguridad. Cuando el acceso está restringido a aplicaciones específicas, las posibilidades de acceso no autorizado se reducen.
- Hoy en día, SSL-VPN ofrece también protección de datos en el navegador, después de que el usuario cierra la sesión, a fin de eliminar la información sensible que pueda haber sido utilizado durante el curso de un acceso seguro. Esto incluye la eliminación de cualquier caché las credenciales de usuario y la eliminación de la cola o temporal en caché de archivos. Algunos SSL-VPN pueden ser configuradas para evitar que un usuario realice copias locales de la información sensible de la empresa en un equipo de trabajo.
- Conexiones pobres, intermitentes e interrumpidas no causan la caída de la VPN.
- Permite mediante un certificado digital, usar su navegador para verificar la autenticidad del sitio y comunicarse con él en forma segura.

4.8 Software VPN-SSL

Aunque se emplea SSL para crear túneles no existe un estándar que especifique cómo funciona una VPN-SSL, sino que hay distintas implementaciones que funcionan bastante bien. Entre las más interesantes se encuentran Open VPN del movimiento Open Source y el protocolo SSTP (Secure Socket Tunneling Protocol) de Microsoft.

4.8.1 Open VPN

Open VPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) bajo la librería Open SSL y VPN Virtual Private Network (Red Virtual Privada). Soporta diferentes medios de autenticación como certificados, smart cards, y / o usuarios / contraseñas, y permite políticas de control de acceso para usuarios o grupos usando reglas de firewall aplicadas a las interfaces virtuales de la VPN.

Esta solución resulta una muy buena opción en tecnologías WiFi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas entre otras. Está publicado bajo licencia de código libre (Open Source). Es una solución multiplataforma que ha simplificado mucho la configuración de VPN's dejando atrás los tiempos de otras soluciones difíciles de configurar como IPSec haciéndola más accesible para gente inexperta en este tipo de tecnología.

Esta arquitectura está implementada sobre la capa 2 y capa 3 del modelo OSI, de esta manera los túneles de Open VPN pueden transportar tramas Ethernet, paquetes IPX, y los paquetes NETBIOS del navegador (Explorer) de la red Windows, que son un problema en la mayoría de las otras soluciones VPN.

Algunas de características de Open VPN son:

- **Protección de sesión con el cortafuego interno:** en una sesión conectada con la oficina central de su compañía mediante un túnel VPN puede cambiar el setup de su red en su ordenador portátil, para enviar

todo su tráfico de la red a través del túnel. Una vez que Open VPN haya establecido un túnel, el cortafuego central en la oficina central de la compañía puede proteger el ordenador portátil, aún cuando él no sea una máquina local. Solamente un puerto de la red se debe abrir de forma local para trabajar la sesión. El cortafuego central protege al empleado siempre que él o ella esté conectado a través del VPN. Las conexiones de Open VPN pueden ser establecidas a través de casi cualquier cortafuego, se dice que "si tienes acceso a Internet y si puedes tener acceso a la Web, los túneles de Open VPN deben poder trabajar".

- **Soporte de Proxy y configuraciones:** Open VPN tiene soporte de Proxy y se puede configurar para funcionar como un servicio de TCP o de UDP, y como servidor o cliente. Como servidor, Open VPN espera simplemente hasta que un cliente solicita una conexión, mientras que como cliente, intenta establecer una conexión según su configuración.

- **Apertura de un solo puerto en el cortafuego para permitir conexiones entrantes:** desde Open VPN 2.0, el modo especial del servidor permite conexiones entrantes múltiples en el mismo puerto del TCP o del UDP, mientras que todavía usa diversas configuraciones para cada conexión. Los interfaces virtuales permiten reglas muy específicas del establecimiento de una red y del cortafuego donde todas las reglas, restricciones, mecanismos de la expedición, y conceptos como NAT se pueden utilizar con los túneles de Open VPN.

Figura 3.16 Interfaz GUI de Open VPN Para Sistemas Windows

- **Alta flexibilidad con posibilidades extensas de lenguaje interpretado (scripting):** Open VPN ofrece numerosos puntos durante la conexión para la ejecución de los scripts individuales. Estos scripts se pueden utilizar para una gran variedad de propósitos de la autentificación, recuperación en caso de fallos (failover) entre otros.

- **Soporte transparente y alto rendimiento para IP's Dinámicas:** si se usa Open VPN, no hay necesidad de utilizar más IPs estáticas de cualquier lado del túnel. Ambas puntos finales del túnel pueden tener acceso barato de ADSL con el IPs dinámicas y los usuarios no notarán un cambio del IP de cualquier lado. Las sesiones del Terminal Server de Windows y las sesiones seguras de Shell (SSH) parecerán congeladas solamente por algunos segundos, pero no terminarán y continuarán con la acción solicitada después de una corta pausa.

- **Instalación simple en cualquier plataforma:** la instalación y el uso son increíblemente simples. Especialmente, si se ha intentado instalar IPSec con diversas configuraciones, se apreciará la facilidad de instalación de Open VPN. En plataformas Windows se cuenta con una interfaz gráfica muy amigable que permite el monitoreo de la Red Privada Virtual.

- **Diseño modular:** el diseño modular consta de un alto grado de simplicidad en seguridad y el establecimiento de una red virtual es excepcional. Ninguna otra solución VPN puede ofrecer la misma gama de posibilidades a este nivel de seguridad. Con respecto a la estabilidad, Open VPN es un programa muy robusto y ofrece la posibilidad de implementar esquemas de servidores redundantes y con balance de carga.

Las principales desventajas de Open VPN son las que se mencionan seguidamente:

- Todavía existe poca gente que conoce cómo usar Open VPN.

- Al día de hoy sólo se puede realizar conexiones entre computadoras. Pero esto empieza a cambiar, dado que ya existen compañías desarrollando dispositivos con clientes Open VPN integrados.
- No tiene compatibilidad con IPSec que justamente es el estándar actual para soluciones VPN.

4.8.2 SSTP (Secure Socket Tunneling Protocol)

El protocolo Secure Socket Tunneling Protocol (SSTP) de Microsoft es, por definición, un protocolo de capa de aplicación que encapsular tráfico PPP por un canal SSL del protocolo HTTPS. El uso habilita la compatibilidad con métodos de autenticación seguros, como EAP-TLS. El empleo de HTTPS significa que el tráfico pasa a través del puerto 443 (TCP), un puerto que se suele usar para el acceso web y eliminando así los problemas asociados con las conexiones VPN basadas en L2TP o PPTP (conocido error 800 – problemas de conectividad), que pueden ser bloqueadas por algunos proxies Web, firewall y routers en las configuraciones de los carrier's.

La Capa de sockets seguros (SSL) proporciona seguridad de nivel de transporte con negociación, cifrado y comprobación de integridad de claves mejorados.

SSTP se basa en el protocolo SSL en lugar de PPTP o IPSec, a pesar de que está estrechamente relacionado con SSL, no se puede hacer una comparación directa entre SSL y SSTP, porque SSTP es sólo una diferencia de protocolo de túnel SSL. Existen muchas razones para elegir SSL y no IPSec como base para SSTP, las ventajas mencionadas en el apartado anterior son validas también para este protocolo, otras razones son:

- Debido a que IPSec se ha desarrollado para conexiones seguras de sitio a sitio, es probable que presente problemas para usuarios remotos que intentan conectarse desde un lugar con un número limitado de direcciones IP.
- IPSec no soporta dinamic DNS.

Esta tecnología sólo está soportada por Windows Server 2008 y Windows Vista Service Pack 1; existen también paquetes de software como IAG 2007, un software que funciona como punto de bastión en interfaces de entrada a redes LAN's Corporativas.

Funcionamiento Básico de SSTP Cuando se inicia una conexión VPN-SSTP sucede lo siguiente:

1. EL software cliente (SSTP client) establece una conexión TCP con el servidor SSTP entre un puerto dinámico del cliente y el puerto 443 del servidor.
2. El cliente SSTP envía un SSL Client-Hello, indicando que el cliente quiere crear una sesión SSL con el servidor.
3. EL servidor SSTP envía su certificado de máquina al cliente.
4. El Cliente SSTP valida el certificado de equipo, determina el método de cifrado para la sesión SSL, genera una clave para la misma y cifra está con la clave pública del certificado del servidor SSTP, y a continuación lo envía al servidor.
5. El servidor SSTP descifra la clave de sesión SSL mandada por el cliente con su clave privada. Todas las comunicaciones posteriores se realizan ya con la nueva clave negociada.
6. El cliente SSTP envía una petición de HTTP sobre SSL al servidor de SSTP.
7. El cliente SSTP negocia un túnel SSTP con el servidor SSTP.
8. El cliente SSTP negocia una conexión PPP con el servidor SSTP. Esta negociación incluye las credenciales de autenticación del usuario, el método de autenticación y la configuración de IPv4 e IPv6.
9. El cliente SSTP comienza a enviar tráfico IPv4 o IPv6 sobre el enlace PPP.

5. ANÁLISIS DE LAS TECNOLOGÍAS VPN

En Resumen las siglas VPN se plasman en la realidad mediante una amplia variedad de tecnologías, de las que el *método de encapsulamiento* es la parte más esencial. Para encapsular un paquete en una VPN existe un gran número de técnicas, cada una de

ellas con sus propias características, lo que no siempre las hace excluyentes, sino más bien todo lo contrario.

Se pueden distinguir tres partes principales en una VPN: el ***Protocolo Original***, que se utiliza para navegar dentro de las redes locales; el ***Protocolo Portador o Carrier***, que se utiliza para transportar el paquete encapsulado a través de Internet y el ***Método de Encapsulamiento***.

Es el método de encapsulamiento la parte más esencial de la VPN, ya que determina sus características. Para encapsular un paquete en una VPN existe un gran número de tecnologías, cada una de las cuales dispone de una serie de características referidas, entre otros factores, a su nivel de seguridad o calidad del servicio. El uso de una u otra tecnología se debe a la naturaleza del problema a resolver, y cada vez es más frecuente la utilización de varias de ellas a la vez aunando lo mejor de cada una, algo que ya ha dado lugar incluso a nuevos protocolos de encapsulamiento, como L2TP.

Los principales protocolos de encapsulamiento, esto es, los que han sido seleccionados como más adecuados por consorcios como el VPN Consortium (VPNC), y que se encuentran entre los más habituales en el mercado son: PPTP, L2TP e IPSEC. Junto con estos protocolos, también se han desarrollado soluciones basadas en protocolos anteriores como SOCKS, SSL o SSH.

SSL	IPSEC	L2TP	PPTP	PPP
CONEXIÓN Y COMUNICACIÓN SSL: El protocolo de ***Handshake*** es el encargado de negociar los atributos de la sesión SSL que permitirán construir un canal seguro. **ESTABLECIMIENTO DEL TUNEL:** El cliente envía un mensaje Client Hello y el servidor responde con un mensaje Server Hello (Negocian la versión del protocolo usado, algoritmos de cifrado, funciones hash y métodos de compresión a utilizar). Si no hay acuerdo se aborta la sesión. A continuación el servidor envía su Certificado (X.509) la clave pública y una solicitud de certificado al cliente. Establecido el canal seguro el servidor envía un mensaje de Server Hello Done, luego el cliente envía los mensajes de Certificate Verify, Change Cipher Spec y Finished. En respuesta, el servidor envía su propio mensaje de Change Cipher Spec y su mensaje de Finished. En este momento finaliza la fase de Handshake y cliente y servidor pueden intercambiar datos libremente.	**CONEXIÓN Y COMUNICACIÓN IPSEC:** El ***PCA*** envía un paquete ala ***PCB***. Se encripta y se autentican los datos o paquetes usando lo protocolos **ESP** o **AH**, entonces se inicia el establecimiento del túnel VPN. (Algoritmos de encriptación: DES, AES, 3DES. Algoritmos Hash: MD5, SHA-1, Modos de IPSec). **MODOS DE FUNCIONAMIENTO IPSEC:** ***Modo Túnel***: Se encripta todo el paquete IP original. ***Modo Transporte***: Solamente se encripta la parte de datos. **ESTABLECIMIENTO DEL TÚNEL IPSEC:** La **fase 1 de IKE** crea un canal seguro y autenticado, en el cual se realiza la fase 2. Una vez establecida la fase 1, comienza la **fase 2 de IKE** que es negociar las **SA** de IPsec y establecer el túnel IPsec. Después que se estableció el túnel IPsec el tráfico encriptado se envía por el túnel seguro creado por IPsec.	**CONEXIÓN Y COMUNICACIÓN L2TP:** El ***cliente L2TP*** remoto usa el protocolo PPP para establecer la conexión con un IPS, la cual constituye la primera fase de autenticación L2TP. **CONEXIÓN DE CONTROL L2TP (establecimiento del túnel)**: Es la conexión inicial que hay que establecer entre el ***LAC*** y el ***LNS*** antes de que se puedan establecer sesiones. Esta conexión incluye la autenticación del cliente por el ***LNS*** y la negociación de las facilidades soportadas. **ESTABLECIMIENTO DE LA SESIÓN:** Establecido el túnel, se crea una sesión dentro del túnel por cada conexión PPP existente. Cada sesión se corresponde a un flujo de tramas PPP entre el LAC y el LNS (**Mensajes de Control y Datos**). El usuario puede empezar el envío de datos a través del túnel. Estos datos van cifrados **(DES)**. El LNS recibe los datos, los descifra y los entrega a la red corporativa. Si el LNS envía información al usuario también la cifra antes de enviarla a través del túnel.	**CONEXIÓN Y COMUNICACIÓN PPTP:** Un ***cliente PPTP*** utiliza PPP para conectarse a un ISP. Esta conexión usa el protocolo PPP para establecer la conexión. **CONTROL DE CONEXIÓN PPTP:** Usando la conexión a Internet establecida por el protocolo PPP, el PPTP crea una conexión controlada del ***cliente PPTP*** al server PPTP en Internet. Esta conexión usa **TCP** para establecer la comunicación y se denomina *PPTP Tunnel*. **ESTABLECIMIENTO DEL TUNEL PPTP:** El protocolo PPTP encripta los paquetes PPP (***estándar RSA RC4***), luego los encapsula en datagramas IP (***GRE***) que son enviados a través del ***Tunnel PPTP*** al ***PPTP server***. El *server PPTP* desensambla los datagramas IP y desencripta los paquetes PPP, los cuales son enrutados a la red privada. La seguridad de la red contra intrusos mejorada activando el filtrado de datos en el server PPTP.	**CONEXIÓN FÍSICA:** El protocolo PPP usa una secuencia definida para establecer, mantener y terminar la conexión entre dos ordenadores remotos. **AUTENTIFICA USUARIOS:** Los clientes PPTP son autentificados usando PPP. (MS-CHAP, EAP, CHAP, PAP). **CREACIÓN DATAGRAMAS PPP**: Que contienen paquetes IPX, Netbeui o TCP/IP. **FILTRADO Y CIFRADO DE DATOS:** El Protocolo PPP sólo proporciona filtrado de datos.

Tabla 3.1 Resumen de las Tecnologías VPN

Todos los protocolos y tecnologías analizados hasta aquí forman parte de diversas generaciones de tecnología VPN. IPSec es por hoy la opción más extendida entre los fabricantes VPN, sin embargo la tecnología PPTP dispone de un amplio parque de soluciones, y aún no han sido totalmente apartadas de la producción debido al conocimiento práctico adquirido sobre ellos.

Si bien cada protocolo es un mundo, las soluciones VPN suelen presentarse combinando dos o más protocolos de este tipo; tal es el caso del binomio L2TP/IPSec, o las distintas asociaciones que se ha establecido con diversos protocolos. Con todo, sólo IPSec dispone de todo lo necesario hoy en día para actuar en solitario, por lo que está siendo elegido por muchos fabricantes para sus dispositivos hardware y sus soluciones software.

Al respecto, los fabricantes de soluciones VPN distinguen principalmente tres categorías: *las redes VPN seguras, las redes VPN autenticadas y las híbridas*. La tecnología característica de las VPN seguras es IPSec, solo o junto con L2TP. Una vez seleccionado el grado de seguridad que se desea para la VPN, el siguiente paso es decantarse por una solución basada en software, una solución integrada en un sistema de cortafuegos o una solución basada en hardware. Por supuesto, si el servidor sobre el que va a recaer la administración de la VPN no dispone de suficiente potencia de cálculo, sobre todo en el caso de que vaya a utilizarse encriptación, lo mejor es olvidar las soluciones basadas en software y decidirse directamente por una solución hardware, ya que asume autónomamente esa función. Las soluciones VPN/firewall, por su parte, no hacen sino destacar la necesidad de disponer de un servidor seguro como columna vertebral de la red privada virtual.

CAPITULO IV. DESARROLLO DE LA SOLUCIÓN O DEL ESTUDIO

En este capítulo se describirá la forma de establecer VPNs combinando los protocolos **L2TP e IPSec**. L2TP, a diferencia de otros protocolos, es incapaz de garantizar la autenticación, el cifrado y la integridad de los paquetes que fluyen a través de un túnel. Por esta razón se utilizado junto con IPSec, ya que este último es el que verdaderamente se encarga de dotar al sistema de las carencias anteriormente mencionadas.

1. ESCENARIO DE IMPLEMENTACIÓN

1.1 Descripción del Escenario

El escenario implementado es "**VPN de acceso remoto"**, se utilizan productos de la línea "Microsoft"**,** en la Figura 4.1 se muestra la VPN desarrollada, en este caso se tienen dos componentes principales:

- El servidor o Gateway VPN, que es un Servidor con Sistema Operativo Windows 2008 R2 y software de seguridad (Firewall) MS Forefront Threat Management Gateway (siguiente versión de ISA 2006).
- El cliente VPN, que es el Sistema Operativo Microsoft en los equipos remotos (configuración).

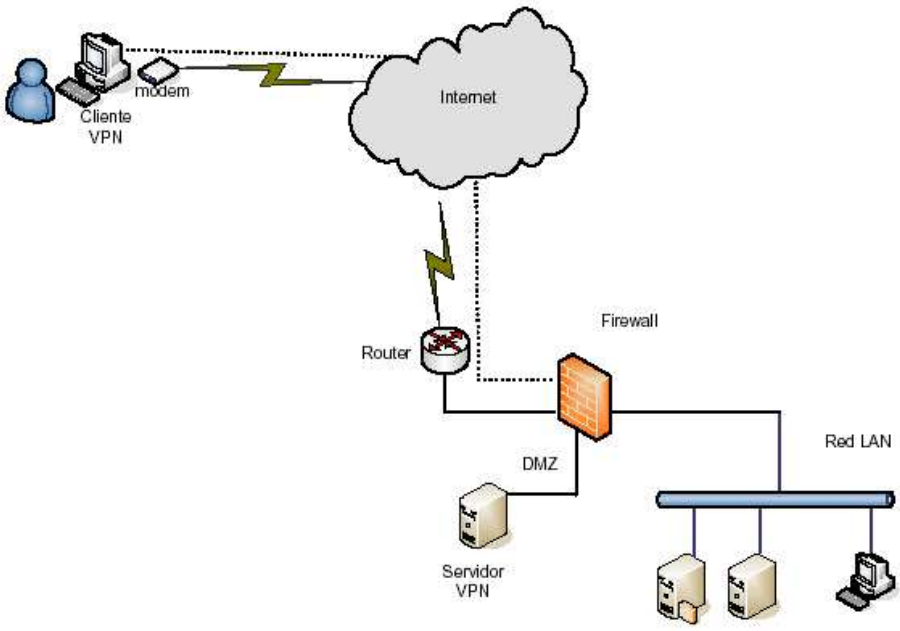

Figura 4.1 Escenario del Acceso Remoto del Prototipo VPN

Este escenario VPN permite a los usuarios móviles acceder de manera segura a los recursos de la red centralizada. El usuario necesita solo tener acceso a Internet, por cualquier medio.

El computador "Cliente VPN" es donde se configura la conexión cliente que permitirá conectar con el Servidor VPN, estableciendo una conexión segura sobre el Internet.

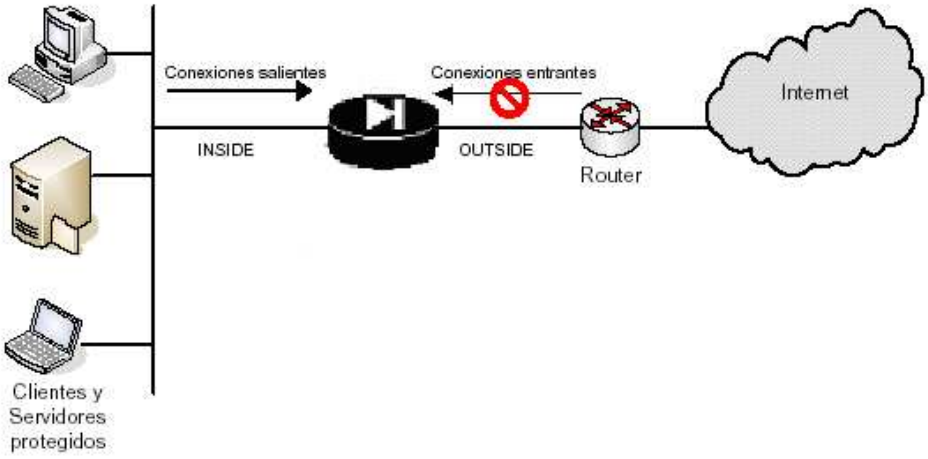

Figura 4.2 Interfaces del servidor VPN (Firewall)

El "Servidor VPN" con Firewall integrado, dispone de dos interfaces (NICs), uno de ellos está en la Red Interna y el otro conectado a Internet; éste exclusivamente atiende conexiones VPN, existiendo otro para permitir el acceso saliente a Internet.

1.2 Conexión a Internet

- **Servidor VPN**

Ancho de Banda Matriz	: 1024 Kbps
Proveedor	: Telefónica del Perú.
Servicio	: InfoInternet 1:1 simétrico
Tecnología Utilizada	: MPLS
Última milla	: Fibra Óptica.

- **Cliente VPN**
  Ancho de Banda Cliente: 256 Kbps como Mínimo.
  Proveedor: cualquiera.

1.3 Funcionamiento

El prototipo VPN implementado en la red de la PNP funciona de la siguiente manera:

- El cliente VPN se conecta al Internet.
- Ejecuta su conexión privada configurada mediante el acceso directo para ejecutar dicha conexión, para ello debe conocer la dirección IP o nombre del servidor VPN.
- El servidor VPN recibe la petición de conexión del cliente, reconoce que desea establecer una VPN, entonces inicia una conexión a través del Internet.
- En este momento se ha de negociar un proceso de confianza mutua que se consigue al verificar el método de autenticación, usuario, password, el algoritmo de encriptación.
- Cuando ambas máquinas confían una en la otra se establece un túnel, esto quiere decir que existe una comunicación constante entre ellas.
- El Servidor VPN asigna dinámicamente una dirección IP disponible del pool de direcciones destinadas para este propósito.
- Compara la lista de acceso de la VPN y establece el intercambio de información solo en los hosts y puertos permitidos.
- Ahora la red LAN de la PNP ya posee un brazo más que se extiende hasta el lugar donde está el cliente VPN.

2. CARACTERÍSTICAS DE HARDWARE Y SOFTWARE DE LOS DISPOSITIVOS

2.1 Servidor VPN

Se trata de un servidor marca HP Proliant ML370 G5 con:

- Procesadores: Intel(R) Xeon (TM) CPU 3.20GHz (8 CPUs), ~3.2GHz
- Memoria: 6142MB RAM.
- Sistema Operativo: Windows Server® 2008 Standard (6.0, Build 6002) Service Pack 2.

Dicho servidor tiene 02 interfaces de red:

- 1ra. Tarjeta de Red: 200.60.76.52 (externa), conectada a Internet.
- 2da. Tarjeta de Red: 172.31.1.79 (interna), conectada a la Red Interna.

2.2 Cliente VPN

Cualquier computadora personal, cuyas características técnicas mínimas en procesador sería similar o superior a: Intel Celeron 1.0GHz, memoria de 256MB, con Sistema Operativo con Windows XP o superior.

3. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS

3.1 Generación del Certificado L2TP/IPSec

La familia Windows Server 2008 admite dos métodos de autenticación para las conexiones VPN basadas en el Protocolo de túnel de capa 2 a través de seguridad de Protocolo Internet (L2TP/IPSec): Certificados de Equipo (también denominados certificados de máquina) y claves previamente compartidas.

Para crear una conexión L2TP/IPSec con el método de autenticación de Certificados de Equipo, debe instalar un certificado en el almacén de certificados del equipo local en el cliente VPN y en el servidor VPN. Para instalar un certificado de equipo, debe haber una entidad emisora de certificados. Una vez configurada la entidad emisora de certificados, podrá instalar certificados de tres formas distintas:

- Mediante la configuración de la inscripción automática de certificados de equipo en los equipos de un dominio de Windows Server 2008.
- Mediante el complemento Certificados para obtener un certificado de equipo.
- Mediante el explorador para conectarse a las páginas de inscripción en Web de la entidad emisora de certificados (CA) con el fin de instalar un certificado en el equipo local o almacenarlo en un disquete para su instalación en otro equipo, por ejemplo en el equipo doméstico de un usuario.

En función de las directivas de certificados establecidas en su organización, sólo debe realizar una de las asignaciones anteriores.

Como se va exportar certificados para importarlos en un equipo en el que se ejecuta Windows 7, PKCS #7 es el formato de exportación preferido. Este formato conserva la cadena de entidades de certificación (la ruta de certificación) de cualquier certificado que incluya contrafirmas asociadas a las firmas. Para exportar un certificado**:**

- Abra el complemento Certificados para un usuario, un equipo o un servicio.
- En el árbol de consola, en el almacén lógico que contiene el certificado que se va a exportar, haga clic en **Certificados**.
- En el panel de detalles, haga clic en el certificado que desee exportar.
- En el menú **Acción**, seleccione **Todas las tareas** y haga clic en **Exportar**.
- En el Asistente para exportación de certificados, haga clic en **No exportar la clave privada**. (Esta opción solo aparecerá si la clave privada está marcada como exportable y tiene acceso a ella).
- Proporcione la información siguiente en el Asistente para exportación de certificados:
- Haga clic en el formato de archivo que desee usar para almacenar el certificado exportado: un archivo codificado mediante DER, un archivo codificado base 64 o un archivo PKCS #7.
- Si exporta el certificado a un archivo PKCS #7, también puede incluir todos los certificados de la ruta de certificación.
- Si es necesario, en **Contraseña**, escriba una contraseña para cifrar la clave privada que va a exportar. En **Confirmar contraseña**, escriba la contraseña otra vez y haga clic en **Siguiente**.
- En **Nombre de archivo**, escriba el nombre y la ruta de acceso del archivo PKCS #7 en el que se almacenarán el certificado exportado y la clave privada. Haga clic en **Siguiente** y, después, en **Finalizar**.

3.2 Configuración del Servidor VPN

La configuración de un servidor VPN descrita en el presente trabajo, parte del hecho de tener Windows2008 R2 previamente instalado como servidor miembro de dominio. El soporte para realizar túneles bajo este Sistema Operativo está incluido como una función denominada ***Enrutamiento y Acceso Remoto (RRAS)***.

Se ha solicitado el registro de: vpn1.pnp.gob.pe en los servidores DNS de Internet, cuya resolución de nombre apunta al Servidor VPN.

Para mejorar la seguridad de nuestro Servidor de conexiones VPN se ha considerado la instalación de software Firewall ***MS Forefront Threat Management Gateway (TMG)*** de Microsoft. La configuración del Servidor VPN se realizará a través de la Consola de TMG, esto se hace siguiendo la ruta: *Inicio | Todos los Programas | Microsoft Forefront TMG | Forefront TMG Management***.** Ubicándonos en la raíz del Forefront TMG, seleccionados la opción *Configure el Acceso de VPN (Opción 5)*, luego procedemos a seguir el asistente que nos ayudará a definir y configurar como los clientes VPN tendrán acceso a la red corporativa usando una Red Privada Virtual (VPN).

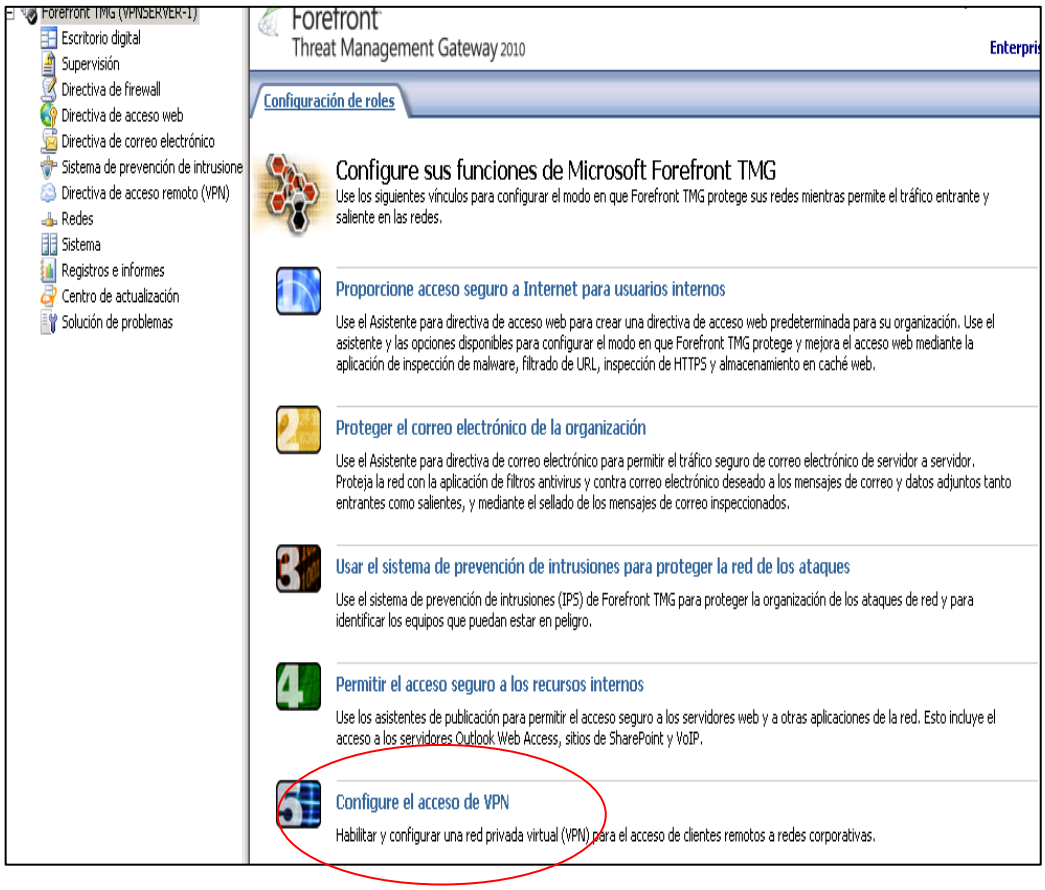

Figura 4.3 Consola del Forefront TMG Management

En la ventana que aparece empezamos la configuración paso a paso iniciando desde el número 1:

Figura 4.4 Pasos Configurar el Acceso de Clientes VPN

1. ***Configurar método de asignación de direcciones y Habilitar acceso de clientes de VPN,*** Permite que los clientes remotos se conecten a la red por medio de una conexión de VPN.

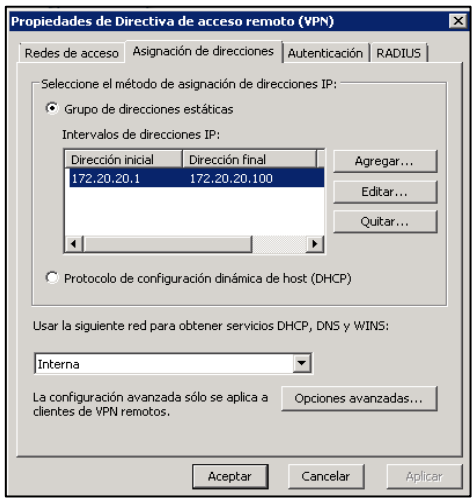

Figura 4.5 Asignación de Direcciones IP

En este caso se está seleccionando la opción que las direcciones IP sean asignadas desde un rango definido en el propio servidor VPN (172.20.20.1 al 172.20.20.100). Además se debe habilitar el *Acceso de Cliente VPN.*

Figura 4.6 Habilitar Acceso de Clientes VPN

2. ***Especifique usuarios de Windows o Seleccione un Servidor RADIUS,*** Especifique los usuarios de Windows (grupos de dominio) con acceso de VPN permitido, o si se usa la autenticación RADIUS, seleccione el servidor de autenticación RADIUS.

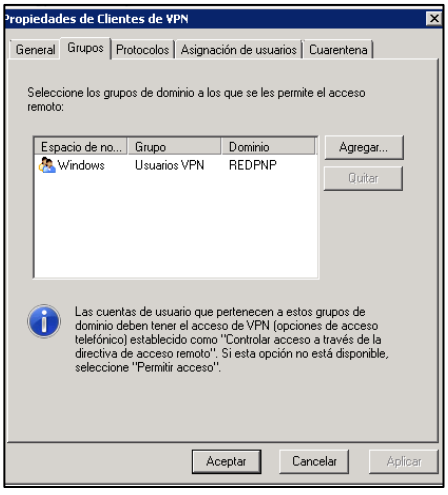

Figura 4.7 Grupo de Dominio con Acceso VPN

Aquí se permite el acceso al grupo denominado “Usuarios VPN” del dominio REDPNP. No se utilizará un Servidor RADIUS.

3. ***Comprobar Propiedades de VPN y Configuración de Acceso Remoto***, Compruebe que las propiedades de VPN, como protocolos y puntos de acceso, se definan de acuerdo con los requisitos de la red.

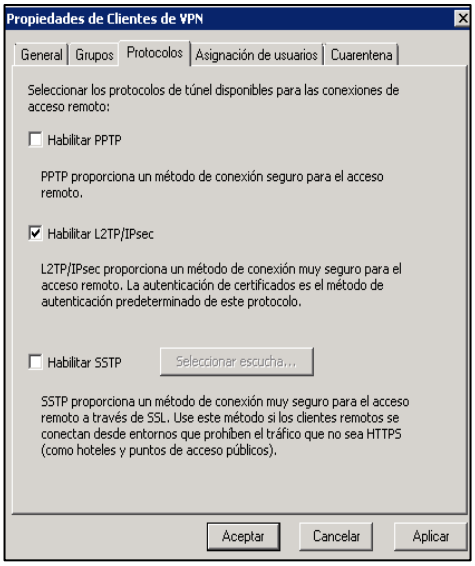

Figura 4.8 Interfaces del servidor VPN (Firewall)

Aquí se habilita el protocolo a utilizar para las conexiones VPN (L2TP/IPSec). En la siguiente imagen se selecciona la interface por el cual se atenderán las conexiones VPN, en este caso por la red externa.

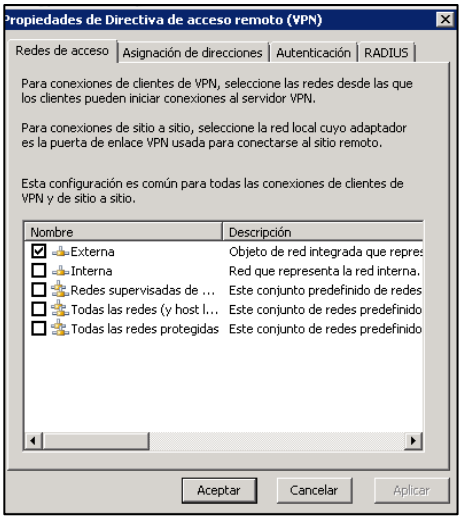

Figura 4.9 Redes de Acceso

4. **Vea la Directiva de Firewall para la Red de Clientes de VPN**, Compruebe que las reglas de directiva de firewall para la red de clientes de VPN se definan de acuerdo con los requisitos de seguridad de la red y corporativos.

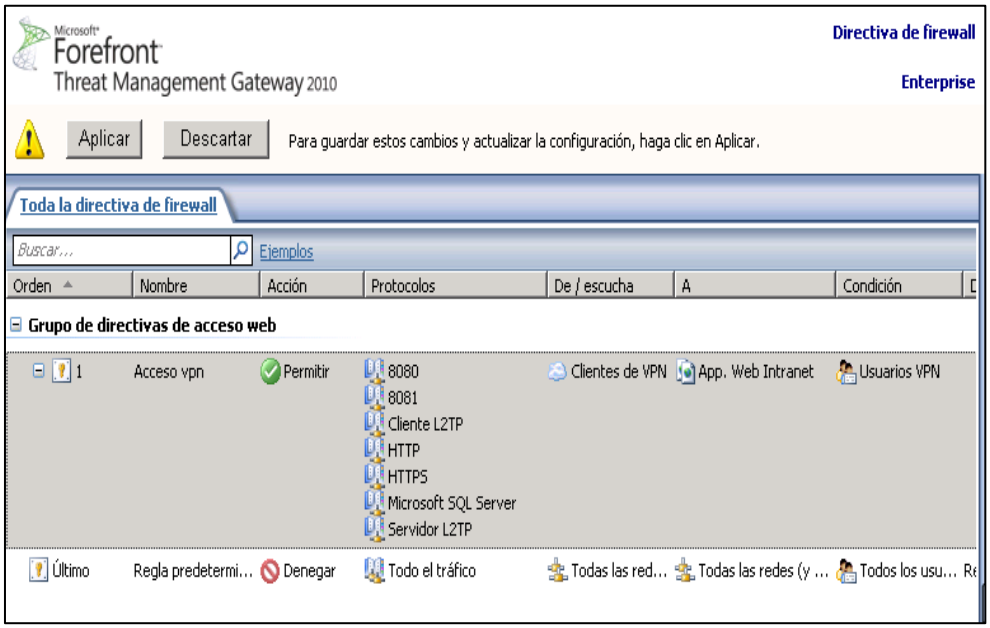

Figura 4.10 Directivas de Firewall VPN

5. **Vea las reglas de red**, Compruebe que las reglas que especifican las relaciones de redes entre la red de clientes de VPN y otras redes, como la interna, se definan de acuerdo con los requisitos de la red. Se mantienen los valores por defecto.

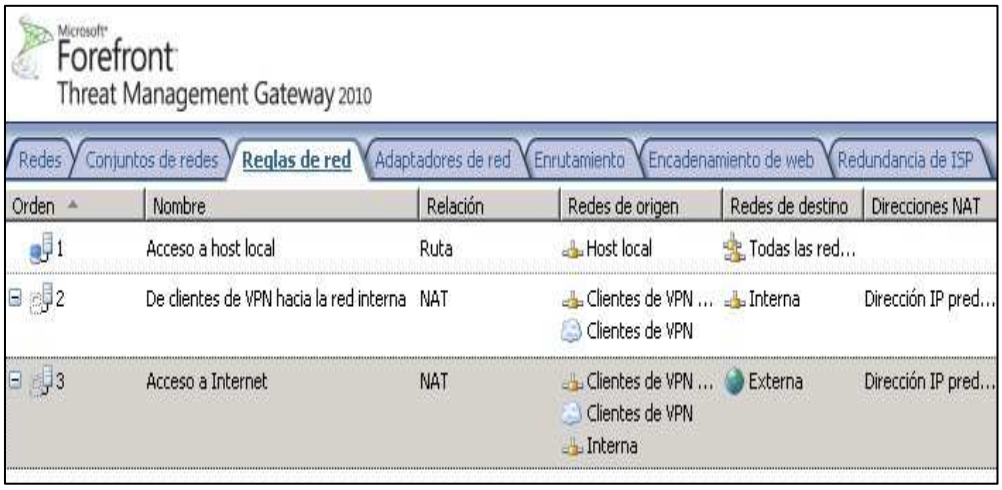

Figura 4.11 Reglas de Red

6. ***Configurar Cuarentena (opcional)***, Permite habilitar la compatibilidad con cuarentena, aplicar la directiva de cuarentena de Forefront TMG o RADIUS, y especificar si está habilitada la compatibilidad con clientes NAP.

En razón que se va a utilizar el protocolo L2PT/IPSec, se requiere generar el certificado L2PT/IPSec, el servidor VPN al pertenecer a un dominio incluye en su almacén de certificados digitales (Entidades de Certificación Raíz de Confianza) el que corresponde al dominio, tal como se parecía en la Figura 4.12.

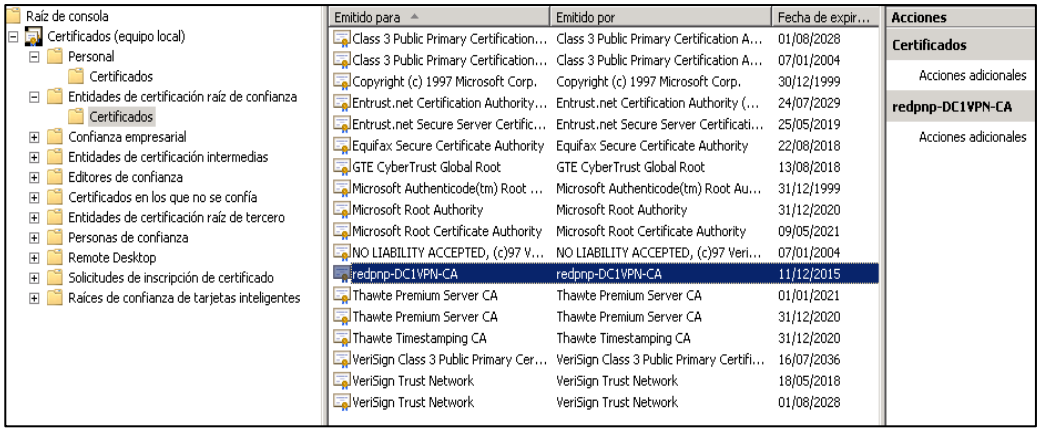

Figura 4.12 Certificado Digital del Dominio REDPNP

En base a esto generamos el certificado digital para el propio servidor VPN, exportándolo para luego importarlo y ubicarlo en el almacén de certificados (Personal), tal como se parecía en la Figura 4.13:

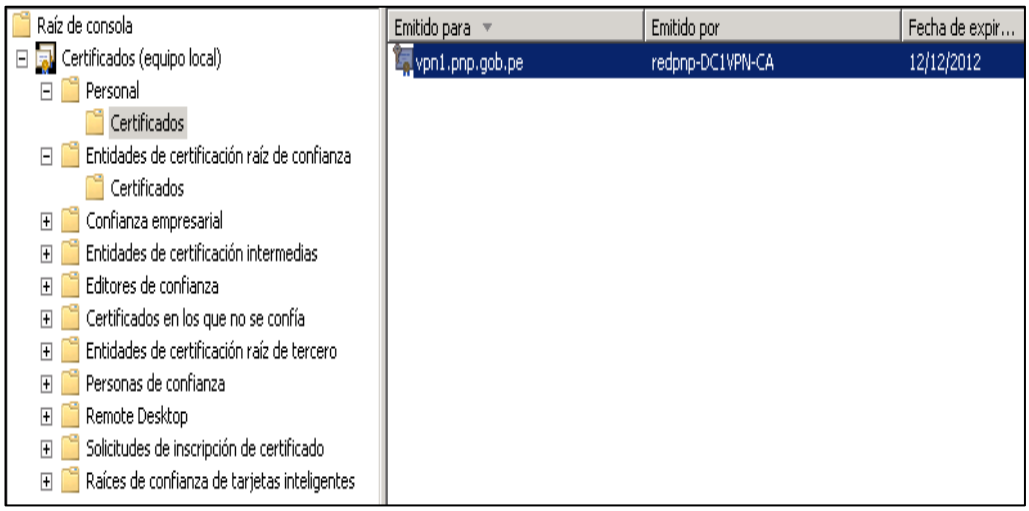

Figura 4.13 Almacén de Certificados (Personal)

3.3 Configuración del Cliente VPN

Sistema Operativo: Windows 7, El certificado antes mencionado requiere ser instalado en el equipo cliente a configurar, para ello se realiza lo siguiente:

1. Descargue el **Certificado** y guárdelo en el equipo cliente.
2. Abra la **Consola de administración de certificados**, para ello:
   - En la casilla Ejecutar del menú Inicio, escriba **"mmc"** y pulse **entrar**.
   - Desde el menú Archivo, seleccione **Agregar/Quitar Complemento...**
   - En las ventanas disponibles, lista, doble clic en **Certificados**.
   - En la siguiente ventana, seleccione **cuenta de equipo**, haga click en **Siguiente**, luego haga click en **Finalizar**.
   - Oprima **Aceptar** para cerrar la ventana.
3. Importar el Certificado
   - Haga click con el derecho en la ventana, luego vaya a **Todas las tareas**, luego haga click en **Importar...**

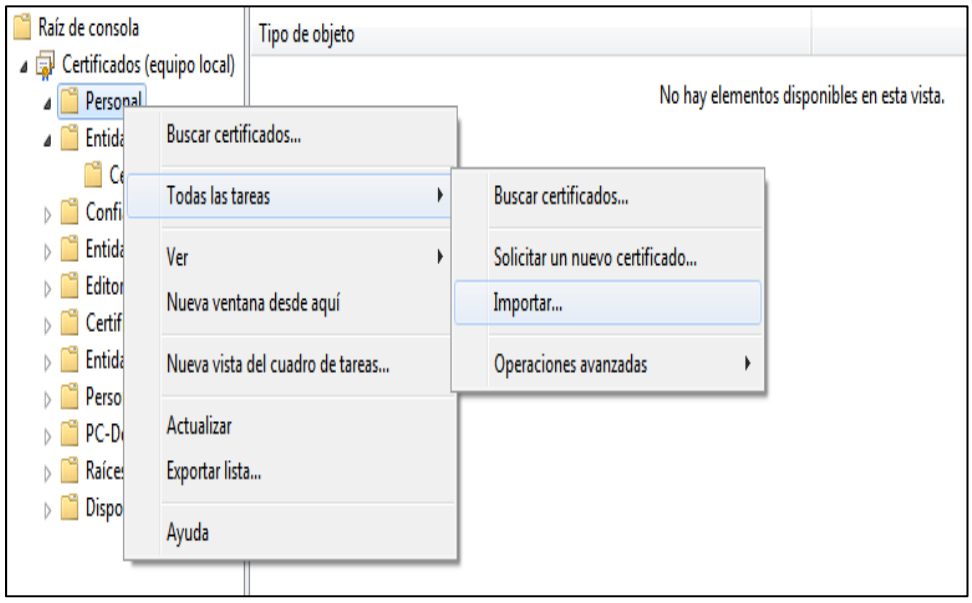

Figura 4.14 Importar Certificado Digital

- Haga clic en **Siguiente** luego **Navegar...**, y **ubique el Certificado** que usted descargó anteriormente.

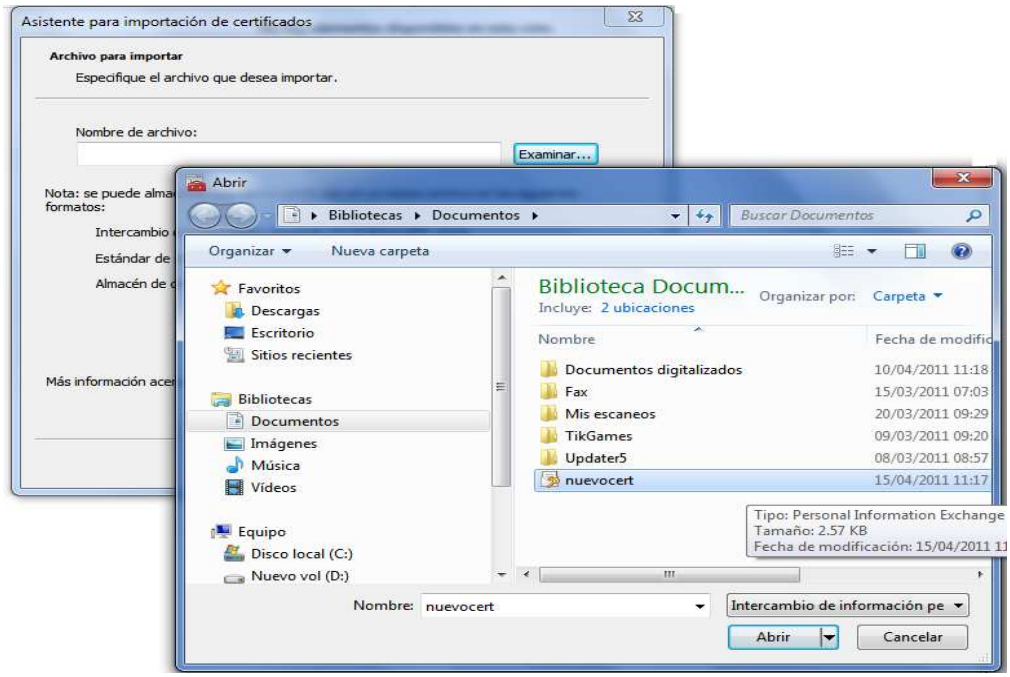

Figura 4.15 Ruta de Ubicación del Certificado Digital

- Haga clic en **Abrir**, escriba **la Contraseña** en el campo y haga clic en **Siguiente**:

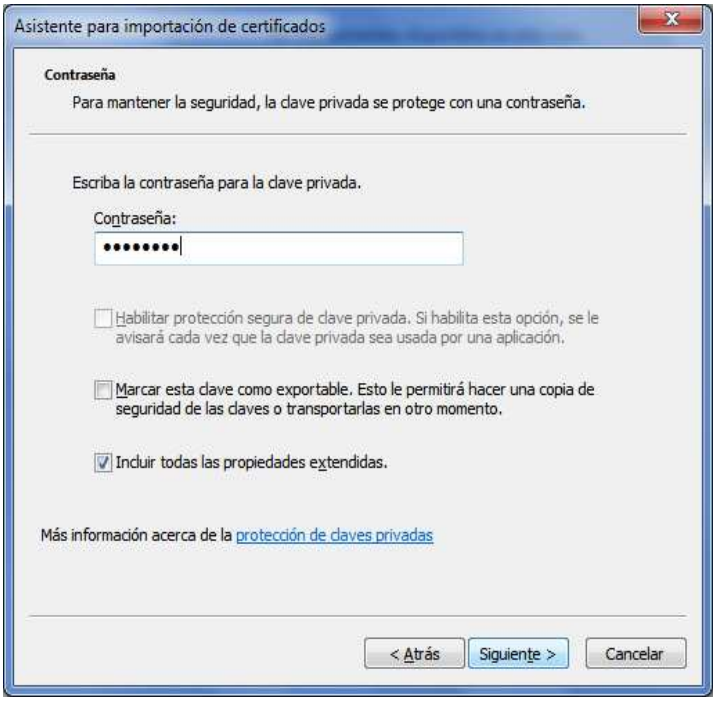

Figura 4.16 Contraseña Para la clave Privada

- Seleccionamos el **almacén** donde se guardará el certificado:

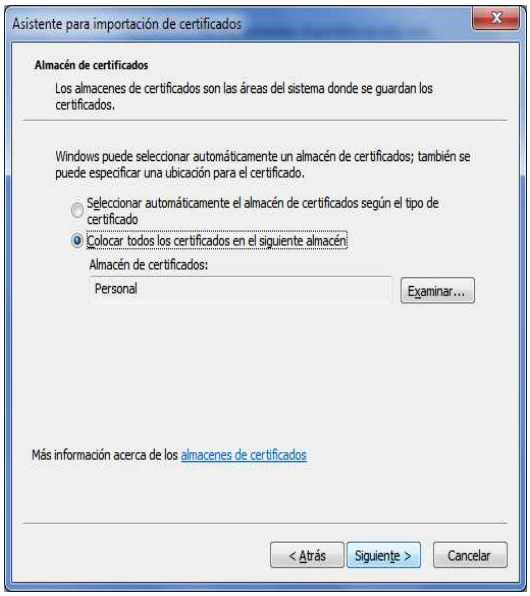

Figura 4.17 Almacén de Certificados

- Hacer clic en "Finalizar" para terminar con el asistente. Aquí vemos el certificado digital instalado:

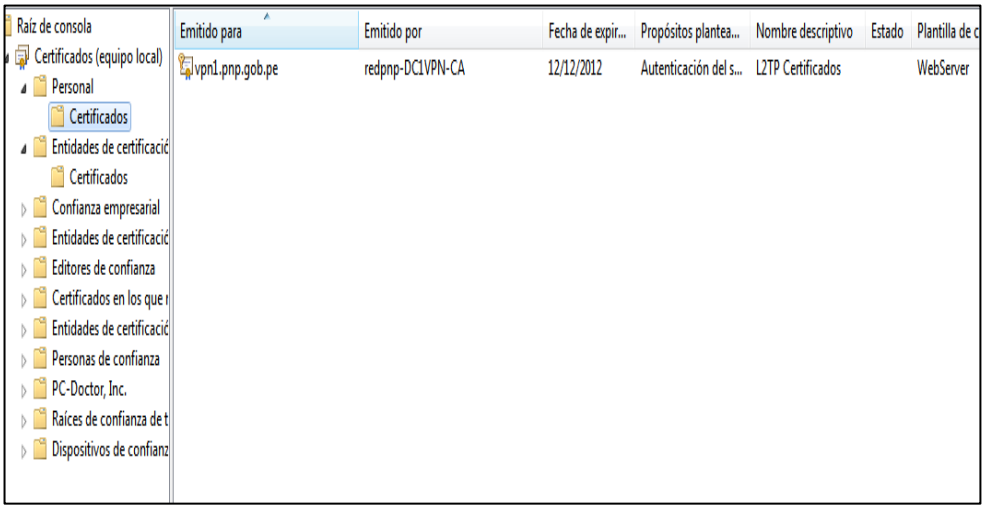

Figura 4.18 Certificado Digital Instalado en el Cliente VPN

Ahora el equipo ya se encuentra listo para iniciar la configuración de la Conexión Cliente de VPN:

1. Para crear una nueva conexión es necesario abrir la ventana donde aparecen las conexiones de red establecidas, para ello ingresamos al ***"Centro de Redes y Recursos Compartidos"*:**

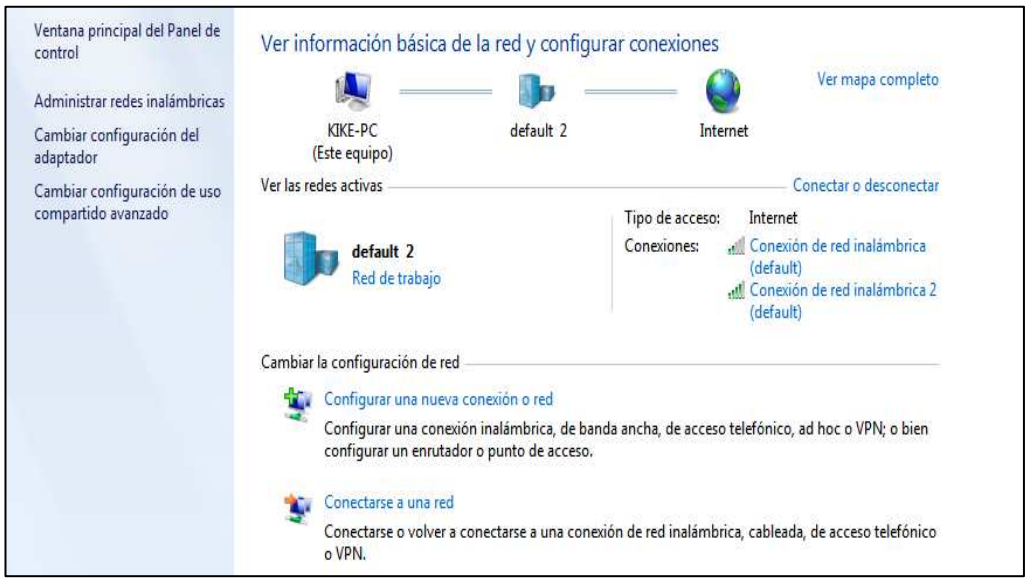

Figura 4.19 Centro de Redes y Recursos compartidos

2. Seguidamente hacemos clic en ***"Configurar una nueva conexión o red"*** y a continuación se despliega una ventana donde se escoge el tipo de conexión nueva que se quiere crear, en nuestro caso ***"Conectarse a un área de trabajo"***:

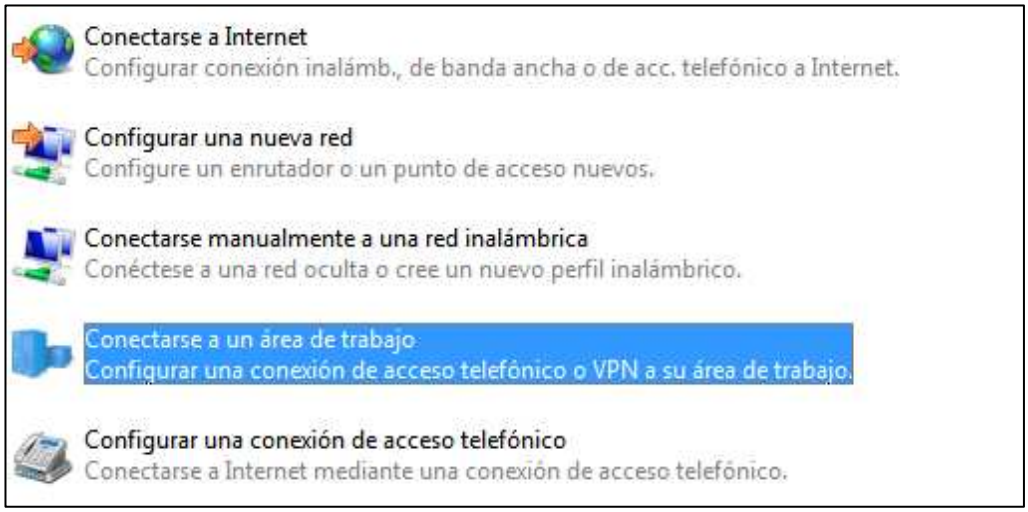

Figura 4.20 Conectarse a un Área de Trabajo

3. Se da clic en **"*Usar mi conexión a Internet (VPN)*"**:

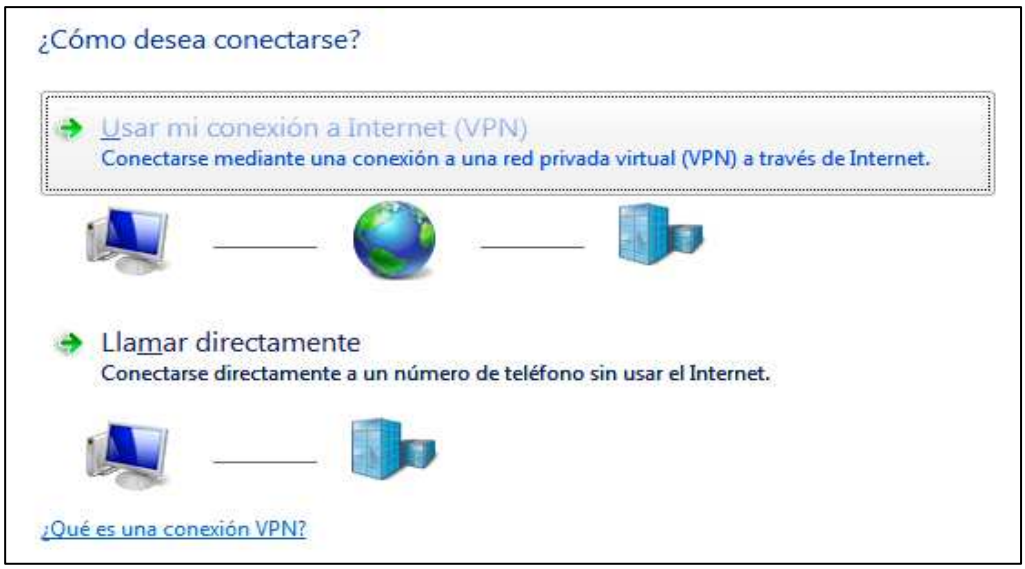

Figura 4.21 Usar mi conexión a Internet (VPN)

4. Escribir la dirección de Internet del Servidor VPN destino y marcar la opción *"No conectar ahora, configurar para conectarse más tarde",* se da clic en Siguiente:

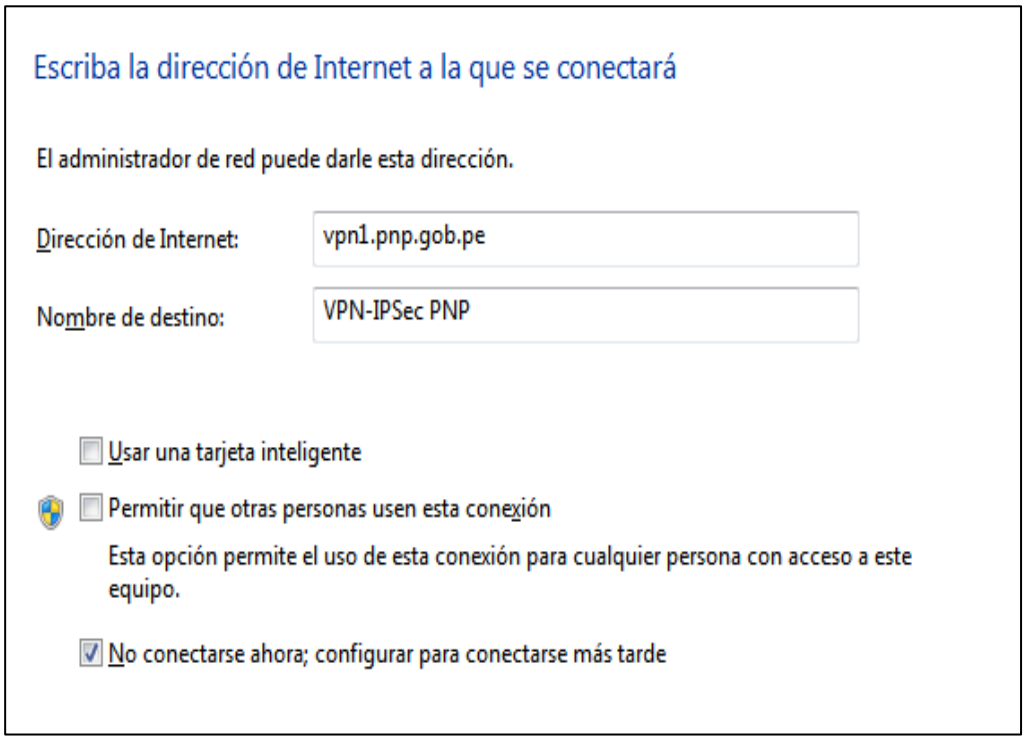

Figura 4.22 Dirección de Internet y Nombre de Destino

5. Escribir el nombre de usuario y contraseña. Hacer clic en *Crear*

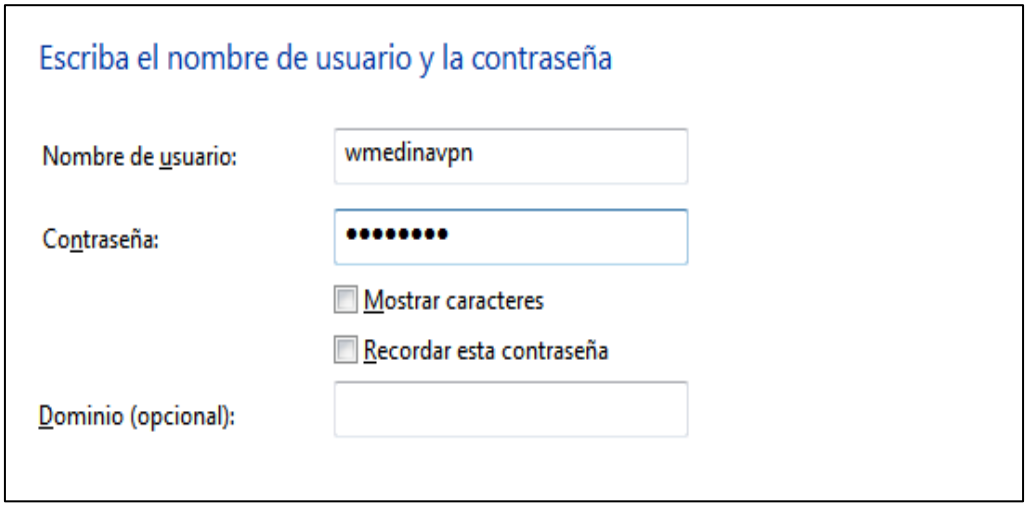

Figura 4.23 Nombre de Usuario y Contraseña

6. La siguiente ventana indica la creación correcta; haga clic en cerrar:

Figura 4.24 Conexión Lista para Usarse

7. En la lista de las redes creadas, hacer clic derecho en la Conexión VPN, luego escoger *Propiedades, Seguridad,* ***Escoger de Tipo de VPN***: Protocolo de túnel de nivel 2 con IPSec (L2TP/IPSec) y hacer clic en Aceptar.

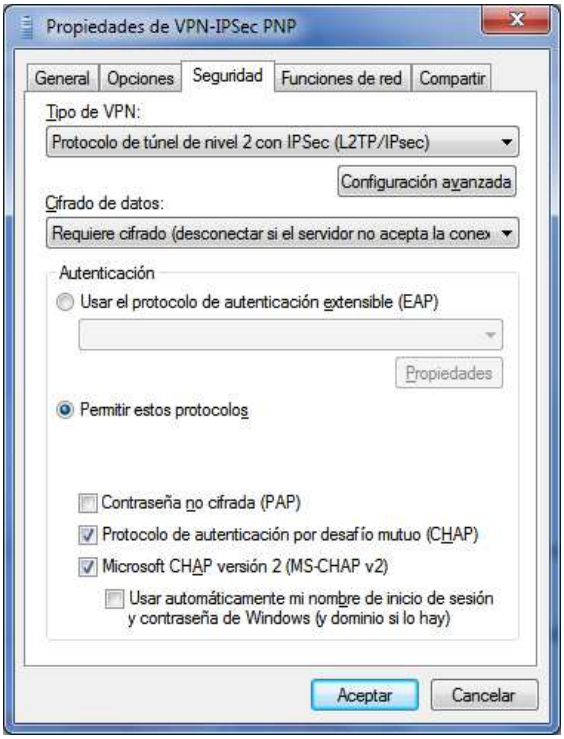

Figura 4.25 Tipo de VPN

4. PRUEBAS DE FUNCIONAMIENTO Y RESULTADOS

4.1 Conexión a Internet

Simplemente podemos ingresar a una página web para verificar que tenemos acceso a Internet. Por ejemplo aquí se muestra la web de google, por estar configurado como página inicial en el navegador.

Figura 4.26 Conexión a Internet}

4.2 Conexión de la VPN

Para iniciar la conexión VPN, hacemos clic en *Conectar a VPN-IPSec PNP, e*scribimos el nombre de usuario y contraseña y hacemos clic en *Conectar:*

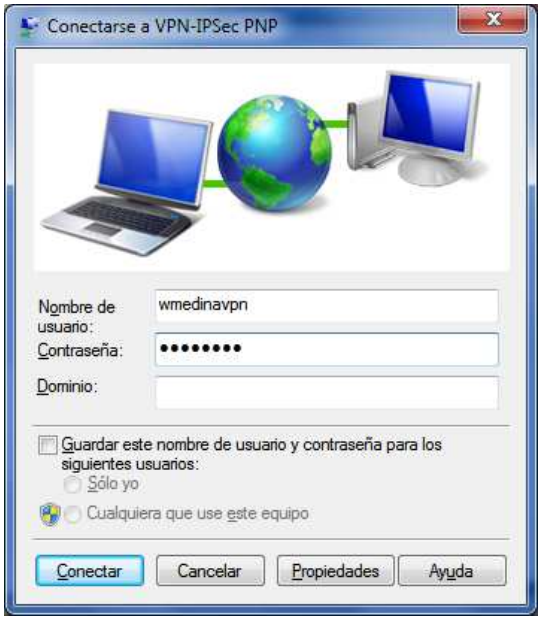

Figura 4.27 Tipo de VPN

Al revisar el estado de esta conexión, verificaremos que estamos conectados utilizando el protocolo L2TP/IPSec.

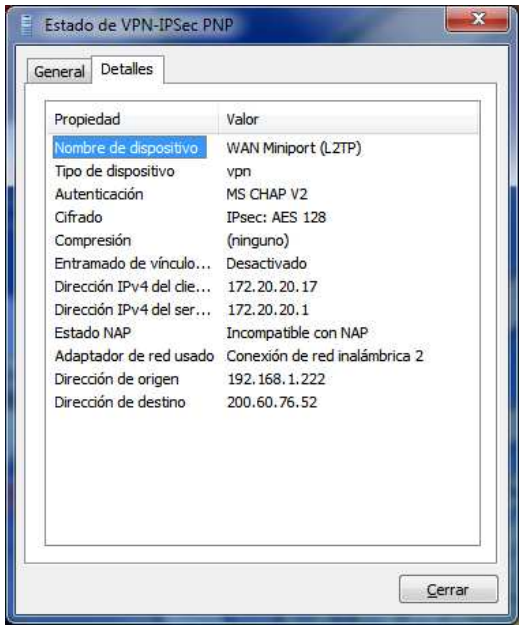

Figura 4.28 Estado de Conexión VPN

Ahora cuando abrimos nuestro navegador, como página inicial se mostrará la siguiente:

Figura 4.29 Red Privada Virtual PNP

5. ANÁLISIS DE COSTOS DE IMPLEMENTACIÓN

5.1 Costo del Prototipo de VPN

Para implementar el prototipo VPN dentro de la PNP se utilizaron recursos que ya dispone actualmente, por ejemplo la conexión a Internet, el servidor, firewall, la red. Sin embargo es importante mencionar el costo de estos los elementos. En el lado del cliente se invirtió en la conexión a Internet para las respectivas pruebas. Resumiendo, se invirtió en lo siguiente:

ITEM	DESCRIPCION	VALOR	
1	SERVIDOR	$	2,000.00
2	SOFTWARE FIREWALL	$	600.00
3	CONEXIÓN A INTERNET CORPORATIVO	$	1,000.00
TOTAL		$	3,600.00

Tabla 4.1 Costo del Prototipo VPN

El costo de **$ 3600.00** representa la inversión que implica construir una VPN. Claro que también hay que agregar las horas/hombre empleadas en la investigación y puesta en marcha. Si se considera ampliar este tipo de acceso VPN a más usuarios se debería considerar el costo que involucre para cada uno de ellos.

5.2 Análisis de Costos de Implementar VPN en Todos los Locales Policiales

En este punto se analiza los elementos que intervendrían en la implementación de una VPN global, de tal forma que integre locales policiales del país con la matriz. De esta forma se tendrá claro el panorama costo beneficio de la VPN en la PNP.

Gastos Actuales

Por concepto de 4 líneas dedicadas, la PNP paga mensualmente al proveedor de telecomunicaciones (Telefónica Empresas) los valores correspondientes que se muestran en la Tabla 4.1.

PUNTO A	PUNTO B	COSTO
NODO CENTRAL	DIRTEPOL PIURA	$ 600.00
NODO CENTRAL	DIRTEPOL CUSCO	$ 600.00
NODO CENTRAL	DIRTEPOL ICA	$ 550.00
NODO CENTRAL	DIRTEPOL AREQUIPA	$ 550.00
TOTAL		**$ 2,300.00**

Tabla 4.2 Gastos Actuales de Líneas Dedicadas

Entonces de acuerdo a las cantidades que se muestran en la tabla anterior, la PNP paga mensualmente por **$. 2,300.00** por las 4 líneas dedicadas.

Posibles Costos con Enlaces VPN

Para implementar una VPN, se debe tomar en cuenta las conexiones a Internet que se deberá invertir de acuerdo al caso que se elija, en este caso.

LOCAL POLICIAL	VELOCIDAD	COSTO
DIRTEPOL PIURA	2 Mbps	$ 150.00
DIRTEPOL CUSCO	2 Mbps	$ 150.00
DIRTEPOL ICA	2 Mbps	$ 100.00
DIRTEPOL AREQUIPA	2 Mbps	$ 100.00
TOTAL		$ 500.00

Tabla 4.3 Posibles Costos con Enlaces VPN

El costo mensual por Internet de los locales policiales en mención le representaría a la PNP **$ 500,00**. Se puede ver que es menor al valor que se paga por las telecomunicaciones actualmente, por lo tanto según este análisis de costos, al implementar las VPN en la PNP el ahorro mensual sería de **$ 1,800.00**.

6. ANÁLISIS COMPARATIVO CON LÍNEAS DEDICADAS

CRITERIO VPN	LINEAS DEDICADAS	VPN
Bajo Costo	Los proveedores de estos servicios tienen un costo mucho más elevado por un enlace dedicado.	Reduce el costo de la red y los cargos por accesos al sitio.
Escalabilidad	La escalabilidad es un reto muy grande para las redes.	Es altamente escalable sobre todo en una red VPN porque no se necesitan conexiones especiales de un lugar a otro. Simplifica las redes WAN
Despliegue del Servicio Rápido	Regularmente tardan de 1 a 7 semanas en instalar un nuevo enlace	No hay configuración demorada; rápido de implementar
Flexibilidad	Regularmente desarrollada para conexiones de un lugar a otro; de oficinas corporativas a sucursales. No permiten el acceso controlado de asociados de la red	Extiende la red a oficinas remotas, Extranet y trabajadores móviles con simple conexión. Permite conexiones seguras con asociados, proveedores y distribuidores

Soporte de Aplicaciones IP	Designada para transporte de capa 2. No tienen conocimiento de tráfico de capas más elevadas y ofrece poco valor agregado a capas superiores.	Provee las bases para desplegar servicios mejorados basados en IP tales como comunicaciones unificadas, video multicast, Extranet, acceso remoto y servicios de red seguros.
Cobertura Geográfica	Limitada al área de cobertura del proveedor.	Mayor cobertura geográfica y ofrece la estructura para una conectividad mundial.
Acceso Remoto	Regularmente no ofrece acceso remoto.	Extiende la seguridad de la red a trabajadores móviles.
Seguridad en la Red	Se basa en la separación de datos para la seguridad del transporte.	Provee una seguridad equivalente o mejor al Frame Relay ya que se utiliza IPSec.

Tabla 4.4 Análisis Comparativo con Líneas Dedicadas

CAPITULO V CONCLUSIONES Y RECOMENDACIONES

1. CONCLUSIONES

Luego de finalizar el trabajo, se puede concluir que se cumplieron con los objetivos propuestos para el mismo:

1.1 Se analizó que la tecnología VPN es una alternativa totalmente viable, la Policía Nacional del Perú está en la posibilidad de integrar sus locales policiales a nivel nacional a un costo efectivo, comparado con las tradicionales líneas dedicadas que alquila hasta ahora, ya que utilizaría el Internet que está creciendo notoriamente en nuestro país.

1.2 La disponibilidad de información en el ámbito nacional con un nivel de servicio razonable, son características indispensables para garantizar que la Policía Nacional cumpla con sus funciones a satisfacción de la Sociedad.

1.3 Las soluciones basadas en hardware resultan, en la mayoría de los casos, más costosas y con una mayor cantidad de características técnicas que las basadas en software, sin embargo, las últimas poseen también sólidas características de manejo de la seguridad que hacen factible su utilización. En el mercado existen numerosos recursos que cubren cada una de las soluciones.

1.4 La utilización de protocolos efectivos para el establecimiento de túneles y encripción y el empleo de adecuadas técnicas de autenticación garantizan la seguridad de una solución VPN. En este proyecto, el protocolo L2PT/IPSec es el encargado de brindar la seguridad necesaria a la información de la Policía Nacional dentro de la VPN.

1.5 Para el diseño se consideró a Sistema Operativo Windows 2008 R2 y el software de seguridad (Firewall) MS Forefront Threat Management Gateway como base para la VPN en la oficina principal y Windows de Microsoft (XP, 7) para el caso de los clientes. Como servidor se utilizó un equipo de marca HP Proliant ML370 G5.

1.6 Definitivamente las VPN seguirán siendo motivo de investigación, en un futuro no muy lejano, muchos estaremos utilizando esta tecnología incluso sin saberlo y el aporte que demos todos los profesionales involucrados en las redes de información será fundamental.

2. RECOMENDACIONES

2.1 Considerar y evaluar el diseño presentado como una solución para el acceso remoto en el ámbito corporativo.

2.2 Instalar y configurar la Red Privada Virtual con el objeto de otorgar a los miembros de la organización la conexión requerida.

2.3 Es recomendable que a la hora de escoger la opción entre software ó hardware para implementar una VPN, la decisión debe ser analizada en muchos aspectos como son: el número de usuarios, conocimientos del personal de Tecnología y los recursos para la inversión, de ello dependerá la opción correcta.

2.4 Diseñar el plan para la implantación de la red tomando en cuenta el recurso humano involucrado y el cronograma de actividades a seguir.

2.5 Asignar los niveles de acceso y derechos de usuario caso a caso, para garantizar que las personas autorizadas puedan llegar a consultar los datos correspondientes.

2.6 Se recomienda evaluar muy cuidadosamente el proveedor de Internet, la calidad y disponibilidad del servicio prestado es fundamental en el rendimiento de las Redes Privadas Virtuales.

BIBLIOGRAFIA

1. LIBROS

- Andrew S. Tanenbaum, Redes de Computadoras, USA, 2010.
- G. Brollo, Redes Privadas Virtuales, Argentina, 2009.
- Correa Ariel, Introducción a la Redes Fundamentos Teóricos, Argentina Banfield Lomas de Zamora, 2009.
- D. Piscitello, Completing the Secure Application Access Puzzle: SSL VP - Ns offer the Greatest Promise, but their Capabilities Still need some En-hancement Business Communications Review, USA, 2005.

2. TESIS

- Gerardo G. Brollo, Aplicación e-Learning para el Aprendizaje de Redes Virtuales Privadas, Argentina Corrientes, 2010.
- Edison Rafael Trujillo Machado, Diseño e Implementación de una VPN en una Empresa Comercializadora Utilizando IPSec, Ecuador Quito, 2006.
- Damian Rodríguez, Transmisión de voz, video y datos en Redes Privadas Virtuales VPN/MPLS, Argentina Buenos Aires, 2008.
- Leonardo Javier Uzcátegui Montes, Implementación de Redes Privadas Virtuales en la Red de Datos de la Universidad de los Andes, Venezuela Mérida, 2003.

3. REVISTAS ESPECIALIZADAS

- PC World en Español, La Nueva Forma de Trabajar, América Latina, 2000-2011.
- Users, Administración de Redes, Implementación de VPNs, Argentina, 2009.
- Network Magazine, Internet-based VPNs: Business or Cattle Class, USA, 2004.
- Red, El Futuro de las Comunicaciones, México, 1990.

4. DIRECCIONES ELECTRONICAS

- Wikipedia, Redes Privadas Virtuales, www.wikipedia.org, USA, 2009.

- Wikipedia, Protocolos VPN, www.wikipedia.org, USA, 2009.
- Microsoft, VPN en Windows Server 2008, www.microsoft.com, USA, 2010.
- Cisco, Seguridad y VPN, www.cisco.com,

ANEXOS

DIAGRAMA DE ACTIVIDADES PARA EL DESARROLLO DE LA TESINA

N°	ACTIVIDADES	HORAS	MARZO		ABRIL				MAYO			
			SEMANA		SEMANA				SEMANA			
			3	4	1	2	3	4	1	2	3	4
1	Presentación del Tema y Forma de Trabajo	2										
2	Definición de Problema y Objetivos, Documento de Planificación	2										
3	Revisión del Marco teórico: Tecnología, Arquitectura y Protocolos	2										
4	Análisis de la PNP: Sistema Actual y Requerimientos	2										
5	Documento de Análisis y Entrega	2										
6	Definición de la Plataforma (Hardware y Software)	3										
7	Documento de Diseño y Entrega	3										
8	Desarrollo de la Solución: Descripción del Escenario y Equipos	2										
9	Instalación del Hardware y Software	6										
10	Configuración del Prototipo	10										
11	Pruebas Preliminares y Documentación de los Resultados	3										
12	Documento de Desarrollo y Entrega	3										
13	Formulación de las Conclusiones y Recomendaciones	2										