UNIVERSIDAD AMAZÓNICA DE PANDO

ÁREA DE CIENCIAS Y TECNOLOGÍA

CARRERA DE INGENIERÍA INFORMÁTICA

PROYECTO DE GRADO

IMPLEMENTACIÓN DE REDES PRIVADAS VIRTUALES (VPN) EN EL GOBIERNO AUTÓNOMO DEPARTAMENTAL DE PANDO PARA EL ACCESO A SISTEMAS INFORMÁTICOS CONTABLES DEPENDIENTES DEL MINISTERIO DE ECONOMÍA Y FINANZAS PÚBLICAS

Postulante: Univ. Eliot Darío Torrez Burgoa

Tutor: Ing. Juan Carlos Gallardo Jiménez

Asesor: Ing. José Balderrama Méndez

Cobija - Pando - Bolivia

2016

DEDICATORIA

A Dios por darme la oportunidad de vivir y 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 estudio.

A mi abuelo Félix Burgoa por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y por su amor.

A mi madre Rosario Burgoa por darme la vida, quererme mucho, creer en mí y porque siempre me apoyaste. Mamá gracias por darme una carrera para mi futuro, todo esto te lo debo a ti.

A mi hermano Edson por estar conmigo y apoyarme siempre.

Todos aquellos familiares y amigos que no recordé al momento de escribir esto. Ustedes saben quiénes son.

INDICE

INDICE DE FIGURAS

CAPITULO II

CAPITULO III

INDICE DE TABLAS

CAPITULO I

CAPITULO II

CAPITULO III

Capítulo I

INTRODUCIÓN

1 INTRODUCCIÓN

En los últimos años se han hecho cada vez más populares las redes entre PCs y dispositivos de tecnología, no sólo coexistiendo en el mismo lugar, sino también en ubicaciones remotas. Esto se debe a la necesidad surgida de compartir recursos, aplicaciones, sistemas, etc. Las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social. La informática y las redes se están convirtiendo en recursos omnipresentes. Por consiguiente, la seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que preocupa cada vez más a la sociedad, por la posibilidad de que surjan problemas en sistemas de información, como consecuencia el daño a la integridad de la información.

Es así que muchas empresas e instituciones en la actualidad tienen problemas en su seguridad por el tipo de sistemas de información financiera el cual manejan, considerando un problema en la tecnología actual en el área de redes, en ese sentido se propone un medio de comunicación seguro como son las redes privadas virtuales (Network Private Virtual VPN) por sus siglas en Ingles. Las Vpn permite una conexión segura entre una o varias redes LAN a través del internet, además todo el tráfico que pasa por esa red está asegurado y protegido.

Considerando a instituciones públicas a nivel nacional en su gran mayoría cuentan con la implementación de las redes privadas, como ser Gobierno Autónomo Departamental de La Paz, Gobierno autónomo Departamental de Tarija, etc. Tomando en cuenta los resultados y beneficios de las mencionadas Gobernaciones, hace que las redes privadas tengan el grado de importancia.

El Gobierno Autónomo Departamental de Pando (GADP), antes denominado Prefectura, hace años va trabajando con varios sistemas informáticos financieros, dichos sistemas son dependientes del Ministerio de Economía y Finanzas Públicas (MEFP).

El problema radica en que no existe ningún tipo de enlace como medio de transmisión segura, en ese sentido la implementación de la VPN es una de las alternativas para la solución a todos los inconvenientes en el manejo de los sistemas financieros en unidades descentralizadas del GADP. Tomando en cuenta el análisis diseño e implementación de las redes LAN de cada descentralizada.

El presente trabajo de grado propone ampliar los sistemas establecidos en el predio central del Gobierno Autónomo Departamental de Pando, a todas las unidades descentralizadas pertenecientes a la misma, a través de Redes Privadas Virtuales (VPN) utilizando como enlace de conexión el Internet, dispositivos de seguridad FIREWALL (hardware) y el mecanismo de seguridad IPSEC 1 (protocolo de seguridad de Internet).

1.1 DESCRIPCIÓN DEL PROBLEMA

De acuerdo al diagnóstico realizado a la institución y los distintos predios en los cuales se aplica los sistemas financieros, las causas que percutan para dicho acceso son, seguridad insuficiente en la red de enlace, predios aislados geográficamente, redes LAN independientes.

Esto constituye:

" Deficiente acceso a los sistemas informáticos contables dependientes del Ministerio de Economía y Finanzas Públicas en unidades descentralizadas del Gobierno Autónomo Departamental de Pando".

Este problema ha generado pérdida de datos, inestabilidad de los sistemas y recursos, extremada lentitud en el proceso de información y lo más importante la vulnerabilidad constante a la integridad de datos, así como ataques a la red y a los distintos servidores, colocando en riesgo la vital información contable de todo el Departamento de Pando.

1.2 OBJETIVOS

1.2.1 Objetivo General

Implementar Redes Privadas Virtuales (VPN) en las unidades descentralizadas del Gobierno Autónomo Departamental de Pando para el acceso a recursos y sistemas informáticos contables dependientes del Ministerio de Economía y Finanzas Públicas, utilizando tecnologías Firewall Físico IPsec.

---

1 IPsec Protocolo de seguridad (Vicente José Aguilar Roselló, 2002) (Solutions, 2013)

1.2.2 Objetivos Específicos

- Realizar un diagnóstico y requerimiento actual de todo el funcionamiento de las redes LAN, MAN, WAN del GADP.
- Analizar y elaborar el diseño de las redes VPN del GADP.
- Configurar e implementar las redes VPN en el GADP (firewall).
- Realizar pruebas de funcionamiento de todas las redes LAN, MAN, WAN, VLAN y VPN en el GADP.

1.3 JUSTIFICACIÓN

Con la implementación de esta tecnología el Gobierno Autónomo Departamental de Pando, tendrá la facilidad de compartir recursos e sistemas de información financiera con todas las unidades descentralizadas y al mismo tiempo con MEFP. Evitando demoras en el proceso de información, reduciendo costos en pasajes y el tiempo que es vital en el proceso y la elaboración de documentos emitidos por sistemas establecidos en la sede de Gobierno como en el predio Central de la institución.

En ese sentido la red privada virtual nos hace pensar en tres aspectos fundamentales y beneficiosos para el GADP que son: Seguridad, Bajos costos y Facilidad de uso.

1.4 METODOLOGÍA Y HERRAMIENTAS

Considerando que no existe una metodología estándar para la implementación de este tipo de proyectos se utilizará la siguiente metodológica como propuesta por el postulante, tomando en cuenta la técnica de Eclecticismo, una metodología mixta con la recomendación de los autores Ruixi Yuan, W. Timothy Strayer, en su publicación “Virtual Private Networks: Technologies and Solutions” y lo sugerido por Casey Wilson y Peter Doak en su libro “Creating and Implementig Virtual Private Networks”. el cual se refleja en el siguiente cuadro.

No	FASES	TECNICAS	HERRAMIENTAS	OBJETIVOS
1	Diagnóstico Y Requerimientos	Entrevistas Informes Evaluación	Solicitudes reuniones	Evaluar los diversos componentes de las redes, así como determinar aquellos componentes no presentes de la Red.

2	Análisis y Diseño	Análisis VPN Diseño de la red VPN	Tipo de encriptación Protocolo de Seguridad Topologías VPN Esquema de redes	. Desarrollo de Políticas de seguridad y Acceso a la VPN. . Determinación de la Estrategia para Implementar la VPN. . Diseño y desarrollo de la infraestructura tecnologías para la conexión segura a la VPN
3	Configuración e implementación	IPs, Nat, Rutas, Policy, Zone, Vlan. IPsec VPN Phase I Phase II	Firewall Físico	Implementación VPN
4	Pruebas	Pruebas de Funcionalidad	Comandos a nivel ICMP Cliente Http	Enlace Estable

Tabla 1-1: Metodología Propuesta por el Postulante

Fuente: Elaboración propia

Las herramientas que se utilizan para la implementación de las redes VPN se nombran a continuación:

IPSec es una plataforma de seguridad a nivel de red desarrollada por el IPSec Working Group de la IETF. Permite acomodar nuevos algoritmos de encriptación y autenticación de forma flexible y robusta. IPSec se concentra manejando en los problemas de seguridad, para ello maneja diferentes niveles y procedimientos de seguridad.

El firewall físico ofrece una amplia cartera de productos de seguridad a todos los niveles tomando en cuenta los algoritmos de encriptación.

- GNS3 Simulador de Redes (Software)
- IPsec: Internet Protocol security (mecanismo de seguridad)
- Dispositivo Firewall de alta Seguridad (hardware)
- Cliente Remoto. (Software)

1.5 ALCANCES

Se realizará de acuerdo a los objetivos del proyecto, se considera tener los siguientes alcances:

El diagnóstico y requerimiento elaborado demuestra el estudio del proyecto y la factibilidad para la implementación de las VPN.

Así mismo el análisis y diseño con su topología correspondiente posibilita a las redes privadas su ejecución.

La implementación de la VPN, se adecua a todas las redes operables de cada institución, tomando como referencia un segmento de red financiero.

Se considera que las nuevas unidades descentralizadas no contarán con la red VPN, porque no cuentan con la infraestructura adecuada ni el equipamiento correspondiente.

Las configuraciones de las VPNs están limitadas hasta el dispositivo de seguridad Firewall, la administración de LAN de SEDCAM, SEDES, SEDEGES estarán sujetos a su propio administrador.

Capítulo II

MARCO LEGAL
MARCO INSTITUCIONAL
MARCO TEORICO

2 MARCO LEGAL

Para la creación de los Gobiernos Departamentales de nuestro país se hace referencia a la Constitución Política del Estado Plurinacional (CPE). **(Ver Anexo 1)**

En la TERCERA PARTE, *Estructura y Organización Territorial del Estado*, Título I, Organización Territorial del Estado, CAPITULO PRIMERO: DISPOSICIONES GENERALES, Artículo 269 - Parágrafo I, Artículo 271 - Parágrafo I, CAPITULO SEGUNDO: AUTONOMIA DEPARTAMENTAL, Artículo 277, Artículo278 - Parágrafo I y II. Establece la organización territorial e instituye a la **ley Nº 031 de Autonomías y descentralización** como regulador de la elaboración de estatutos autonómicos y cartas orgánicas. Dicha ley tipifica en: TITULO III, Tipos de Autonomías, Capítulo I AUTONOMIA DEPARTAMENTAL, Artículo 30 **GOBIERNO AUTONOMO DEPARTAMENTAL** – parágrafo I y II. **(Ver Anexo 2)**

Es así que respaldado por las normas que rigen en nuestro país, nace el "***ESTATUTO CON JURISPRUDENCIA CONSTITUCIONAL PANDO***", por ende, el **"GOBIERNO ATONOMO DEPARTAMENTAL DE PANDO". (Ver Anexo 3)**

3 MARCO INSTITUCIONAL

Dentro de las competencias atribuidas en el Estatuto Departamental de Pando regidas por la ley 031 y la CPE, establece formar leyes, resoluciones, decretos, etc. Es así que se resuelve la Estructura Organizacional vigente del Gobierno Autónomo Departamental según el DECRETO DEPARTAMENTAL N° 09/2016. **(Ver Anexo 4)**

La estructura del Gobierno Autónomo Departamental de Pando (GADP) está conformada por Gobernador/a, Vicegobernador(a), Secretarías, Direcciones, Unidades y Servicios Departamentales. **(Ver Anexo 5)**

3.1 UNIDAD DE SISTEMAS

Esta área es la que tiene a cargo toda la administración referente al ámbito tecnológico del GADP, al mismo tiempo desempeña varias funciones en diferentes ramas de la informática como ser :

- Administración de la red de datos LAN, WAN, etc.
- Administración de sistemas
- Desarrollo de Software
- Soporte técnico en Hardware
- Soporte técnico ofimática, etc.

Dentro del organigrama estructural la unidad de sistemas se ubica bajo las siguientes dependencias.

Gobernador => Secretaría Departamental de Coordinación General => Secretaría Departamental de Economía y finanzas => Dirección Administrativa => *Unidad de Sistemas.* **(Ver Anexo 5).** El personal que trabaja en esta unidad está sujeto a responsabilidades y funciones según al cargo asignado. **(Ver Anexo 6).**

En las unidades descentralizadas o Servicios departamentales la unidad de sistemas está bajo las siguientes dependencias.

Director Departamental => Administrativo => Unidad de Sistemas.

4 MARCO TEORICO

4.1 ANTECEDENTES DE LA INVESTIGACION

El Gobierno Autónomo Departamental de Pando “GADP”, con el objeto de establecer un mecanismo de intercambio de información necesaria con las unidades descentralizadas, predispuso varios ambientes en su predio central en los años 2009 – 2010.

Asimismo, con el desarrollo de sistemas contables por parte del MEFP, el cual consolida una gran base de datos o repositorio de información contable, se establece un único punto de entrada a través del uso de redes LAN, para la operatividad de todas las unidades descentralizadas y el propio GADP en el área financiera.

Dichos sistemas de información SIIF – SIGMA están disponible a usuarios autorizados en la red local del GADP “Intranet”, a través de diversas aplicaciones cliente servidor. Sin embargo, el ámbito de interés para la consulta y acceso a los mencionados sistemas va mucho más allá de las fronteras del GADP. Dado a que el personal técnico lo requiere tanto dentro como fuera de la localidad de la institución.

Asimismo, existe un conjunto de usuarios que pertenecen a la institución tales como: SEDES, SEDEGES, SEDCAM, entre otros, con interés y necesidad de acceder y consultar a los diversos sistemas, a los fines de cotejar, validar y obtener información de acuerdo a su actividad o área de acción.

Por ello, la importancia de incorporar a la infraestructura tecnológica de los sistemas contables un componente que habilite y controle las conexiones y garantice la integridad, confiabilidad y estabilidad de los sistemas.

Por lo que, revisando la infraestructura de los sistemas el cual está adaptado a las tecnologías Telnet, Web (http) y otros, evaluando la plataforma para la conexión de Internet existente en GADP, es posible el establecimiento de una “Red Privada Virtual” como mecanismo de acceso a los sistemas.

Todo ello, sobre la base de consolidación y crecimiento que ha tenido lugar en la última década en los servicios, ancho de banda y disponibilidad de Internet, lo cual facilita hoy día el establecimiento de una “Red Privada Virtual” sobre protocolo IP.

4.2 BASES TEÓRICAS

En el marco tecnológico en el que tiene una Red Privada Virtual existen diversos componentes y configuraciones posibles de acuerdo al escenario y necesidad que exista, por lo que, dichos conceptos se revisarán a continuación con el objeto de establecer las bases teóricas donde se soportará el presente proyecto.

4.2.1 Marco para entender una red privada virtual

Una Red Privada Virtual, mejor conocida por sus siglas "VPN", es una red que utiliza recursos de transmisión y conmutación compartidos, de una red pública tal como el Internet, ATM y/o Frame, para disponer a usuarios remotos los recursos y servicios disponibles en una red ya sea corporativa o institucional, utilizando métodos de seguridad y protección para salvaguardar tanto la plataforma institucional como los datos intercambiados.

La esencia de ésta tecnología reside en que esa parte "pública" no será accesible por ningún usuario no autorizados, lo que la constituye en una red "privada virtual", dado a que no es una red privada real.

Una VPN posee ciertas ventajas sobre una red "privada real", tal como que ésta puede establecerse de manera más efectiva y expedita en términos económicos, y así incorporar en la red corporativa o institucional sitios remotos más pequeños. Los ahorros se estiman aproximadamente entre un 20% y 40% para la interconexión de las sedes principales con sus sucursales, y un 60% u 80% para la conexión de los usuarios móviles.

Otros Aspectos importantes que se deben considerar, son los aspectos técnicos que la institución o corporación requiere para establecer una conexión punto a punto entre sus sucursales y los usuarios móviles:

- Solicitar e instalar líneas telefónicas o troncales a los proveedores de servicio.
- Comprar, instalar y configurar equipos de acceso remoto, rack de módems, etc.
- Instalar en los equipos portátiles software capacitados para establecer la interconexión. Monitorear los patrones de tráfico sobre los puertos en los equipos de acceso remoto.

- Suplir suficientes puertos de acceso en relación con el número de personal móvil utilizando el servicio.
- Mantenerse actualizado con los cambios tecnológicos del mercado.

En los últimos años se ha observado una fuerte tendencia al desarrollo redes virtuales privadas utilizando Internet, ya que así se reducen aún más los costos de implementación y se alcanza la conectividad global. Por ello, se habla de intranet, donde se utilizan tecnologías de Internet a lo largo de la organización y de extranet, donde se extiende fuera de las fronteras de la organización el acceso a clientes, socios, proveedores, etc.

A continuación, se presenta una figura que muestra el esquema de conexión de una VPN utilizando una línea dedicada Vs la implementación que utiliza el Internet.

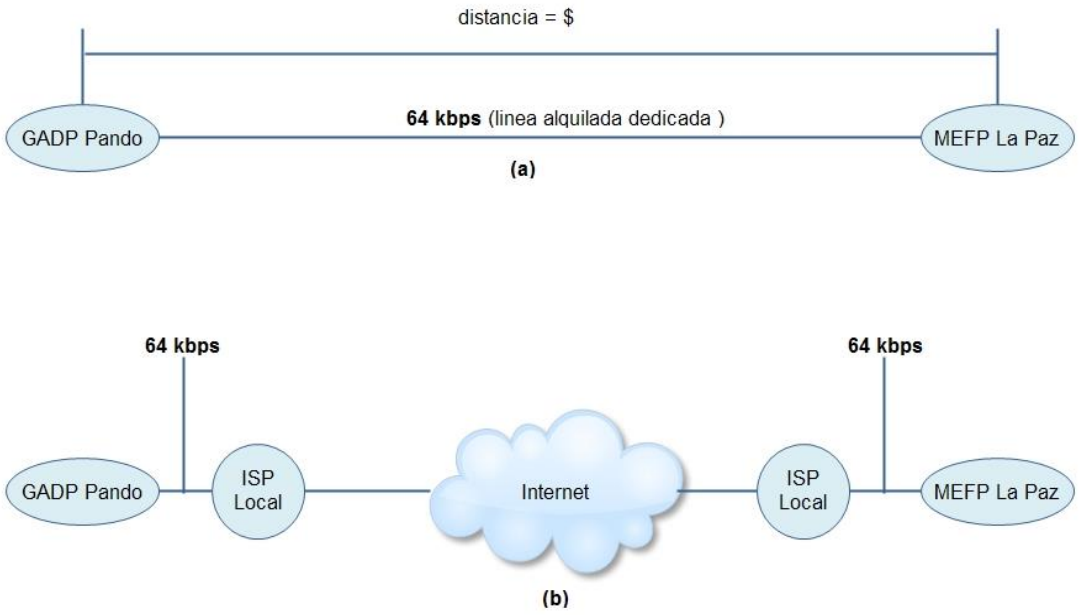


Figura 4-1: Comparación de interconexión de una VPN
Fuente: Elaboración propia

Como se observa en la gráfica anterior, utilizando líneas dedicada para el establecimiento de una VPN (a) existen las siguientes consideraciones:

- El costo de la línea dedicada depende de la distancia entre ambos extremos.

- El usuario cancela el costo total de la línea, a pesar de no haberla utilizado el 100%.
- Para cada nueva conexión (usuario) a la VPN debe contratarse una línea dedicada.

Asimismo, se observa en la gráfica anterior, utilizando el Internet para establecer una VPN (b) existen los siguientes beneficios:

- El costo de conexión y establecimiento de la VPN no está asociado a la distancia entre los extremos.
- El usuario sólo cancela el costo necesario de conexión para el establecimiento de la VPN.
- Cada nueva conexión (usuario) a la VPN puede efectuarse sólo si dicho usuario dispone del acceso a Internet y los programas de seguridad y autenticación.

Los requisitos para establecer una VPN basadas en Internet se pueden agrupar en cuatro áreas principales: compatibilidad, seguridad, disponibilidad e interoperabilidad.

Compatibilidad. Para establecer una VPN sobre Internet, debe ser compatible con el protocolo de Internet (IP). Resulta obvia esta consideración con el fin de poder asignar y, posteriormente, utilizar conjuntos de direcciones IP. Sin embargo, la mayoría de redes privadas emplean direcciones IP privadas o no-oficiales, provocando que únicamente unas pocas puedan ser empleadas en la interacción con Internet. La razón por la que sucede esto es simple: la obtención de un bloque de direcciones IP oficiales suficientemente grande como para facilitar un subnetting resulta imposible. Las subredes simplifican la administración de direcciones, así como la gestión de los routers y conmutadores, pero se desaprovechan direcciones muy preciadas.

Actualmente existen varias técnicas con las que poder obtener la compatibilidad deseada entre las redes privadas e Internet, por ejemplo, la conversión a direcciones Internet mediante NAT (Network Address Traslation) y el empleo de túneles para encapsulamiento.

En la primera de estas técnicas, las direcciones Internet oficiales coexistirán con las redes IP privadas en el interior de la infraestructura de routers y conmutadores de las organizaciones. De este modo, un usuario con una dirección IP privada puede acceder al

exterior por medio de un servidor de direcciones IP oficiales mediante la infraestructura local y sin necesidad de emplear ningún tipo de acción especial.

Con el túnel, la fuente encapsula los paquetes pertenecientes a otro protocolo en datagramas IP con el fin de poder atravesar la infraestructura de Internet. El proceso de encapsulación está basado en la adición de una cabecera IP al datagrama original, el cual representa la carga (payload). En el extremo remoto, el receptor desencapsula el datagrama IP (eliminando la cabecera IP) y entrega el datagrama original intacto. El uso de un túnel abarca todo el proceso de encapsulación, enrutamiento y desencapsulación.

El túnel envuelve, o encapsula, el paquete original dentro de un paquete nuevo. Este paquete nuevo puede contener nueva información de direccionamiento y enrutamiento, lo que le permite viajar por la red. Si el túnel se combina con la confidencialidad de datos, los datos del paquete original (así como el origen y el destino originales) no se muestran a quienes capturen el tráfico. La red puede ser cualquier conjunto de redes: una intranet privada o Internet. Cuando los paquetes encapsulados llegan a su destino, se quita la encapsulación y se utiliza el encabezado original del paquete para enrutar éste a su destino final.

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

Seguridad. Es un aspecto de séria consideración cuando se implementa una Red Privada Virtual utilizando como canal de comunicación el Internet. Las comunicaciones ya no van a estar confinadas a circuitos privados, sino que van a viajar a través de Internet, que es considerada una red “demasiado pública” para realizar comunicaciones privadas. Aunque puede parecer poco probable que alguien monitoreando una línea con un sniffer consiga capturar información y hacer uso de ella, la posibilidad existe, sin embargo y aplicando las correspondientes medidas de protección y seguridad, Internet puede convertirse en una red altamente privada y segura.

Para eso la encriptación es muy importante. Cuando la información está encriptada, se requiere una clave para desencriptarla. Los usuarios en cada extremo deben tener las claves adecuadas para encriptar y desencriptar los datos. Si se está configurando una conexión con una sucursal es fácil administrar este intercambio de claves. Sin embargo, si un usuario remoto accede a la red corporativa, se necesita un modo de verificar quién es (Identificación y Autenticación) y un modo de intercambiar las claves para la encriptación.

Las claves públicas basadas en certificados digitales son los que más se utilizan para este propósito.

Disponibilidad. La disponibilidad viene motivada principalmente por dos variables: una accesibilidad plena e independiente del momento y del lugar, y un rendimiento óptimo que garantice la calidad de servicio ofrecida al usuario final.

La calidad de servicio (QoS – Quality of Service) hace referencia a la capacidad que dispone una red para asegurar un cierto grado de operación de extremo a extremo. La QoS puede venir dada como una cierta cantidad de ancho de banda o un retardo que no debe sobrepasarse, o bien como una combinación de ambas.

Actualmente, la entrega de datos en Internet es realizada de acuerdo al mejor esfuerzo (best effort), lo cual no garantiza la calidad de servicio demandada.

Interoperabilidad. Las implementaciones de los tres primeros requisitos han provocado la aparición de un cuarto: la interoperabilidad. Los estándares sobre tunneling, autenticación, encriptación y modo de operación ya mencionados anteriormente son de reciente aparición o bien se encuentran en proceso de desarrollo. Por esta razón, previamente a la adquisición de una tecnología VPN, se debe prestar una cuidadosa atención a la interoperabilidad de extremo a extremo. Esta responsabilidad puede residir tanto en el usuario final como en el proveedor de red, dependiendo de la implementación deseada.

Una manera de asegurar una correcta interoperabilidad radica en la elección de una solución completa ofrecida por un mismo fabricante. En el caso de que dicho fabricante no sea capaz de satisfacer todos los requisitos, se deberán limitar los aspectos interoperaciones a un subconjunto que englobe aquellos que sean esenciales, además de utilizar únicamente aquel equipamiento que haya sido probado en laboratorios o bien sometido a pruebas.

En cualquiera de los casos, se deberán seleccionar fabricantes que se acoplen totalmente a los estándares VPN y adquirir únicamente aquel equipamiento que pueda ser actualizado tanto mediante software, firmware o módulos plug-in, con el fin de que puedan adecuarse a futuros estándares.

4.3 FUNDAMENTOS DE LAS VPN

4.3.1 Definición de red de computadoras

Según (Bruce A. Hallberg, 2007) Una red de computadoras es un grupo de computadoras interconectadas entre sí las cuales comparten información y recursos. La interconexión se puede realizar de diferentes maneras, ya sea cable de cobre, fibra óptica, rayos infrarrojos o microondas. Los recursos y la información que se pueden compartir pueden ser los siguientes:

- Archivos
- Aplicaciones
- Correo electrónico
- Impresoras, etc.

Las redes de computadoras ofrecen muchas ventajas. Sin ellas todo el envío de la información tendría que hacerse de forma manual, por medio de diskettes o CDs.

Esto haría el proceso algo muy lento. Con las redes no sólo se puede intercambiar información a nivel local, sino también a grandes distancias incluso mundiales y de forma instantánea.

4.3.2 Clasificación de las redes de computadoras

El mundo de las redes de computadoras es muy complejo, por lo que es necesario clasificarlas para facilitar su estudio, ya que existen muchos tipos de redes. Las redes pueden ser clasificadas en cuanto a cobertura, topología y propiedad.

4.3.2.1 **Cobertura**

La clasificación de las redes en cuanto a cobertura se refiere a la extensión que tiene una red dentro de un área geográfica. Utilizando este criterio, las redes de computadoras se pueden clasificar de acuerdo a la tabla 4.1

Distancia entre procesadores	Procesadores ubicados en el mismo	Clasificación
1 m	Metro cuadrado	Red de Área Personal (PAN)
10 m	Cuarto	Red de Área Local (LAN)
100 m	Edificio	
1 km	Campus	Red de Área Campus (CAN)
10 km	Ciudad	Red de Área Metropolitana (MAN)
100 km	País	Red de Área Amplia (WAN)
1000 km	Continente	
10000 km	Planeta	Internet

Tabla 4-1: Clasificación de las redes en cuanto cobertura
Fuente: Elaboración propia

Sin embargo, esencialmente las redes pueden clasificarse simplemente como Redes de Área Local (que abarcan desde un cuarto hasta un campus) y Redes de Área Amplia (que abarcan distancias mayores a un campus hasta abarcar todo el planeta). Resulta más práctico clasificarlas solamente así al momento de describirlas tecnologías y dispositivos de redes.

Red de Área Local (LAN). Es aquella red donde todas las computadoras conectadas en red están dentro de una habitación, un edificio e incluso varios edificios dentro de una localidad pequeña. Las LAN realizan lo siguiente:

- Operan dentro de una zona geográfica limitada
- Permiten a los usuarios acceder a medios de gran ancho de banda
- Proporcionan conectividad de tiempo completo a los servicios locales
- Conectan físicamente dispositivos adyacentes

Las principales tecnologías LAN son las siguientes:

- Ethernet
- Token Ring
- FDDI

Siendo Ethernet la más popular y más difundida de todas ellas.

Una LAN puede intercomunicarse por medio de un cableado que transmita señales punto a punto; o bien, por medio de una zona de influencia de un punto de acceso (access point) inalámbrico. La velocidad que se puede alcanzar en este tipo de red abarca desde los 10 Mbps hasta los 10 Gbps y se están desarrollando normas para 40 Gbps, 100 Gbps y 160 Gbps.

Red de Área Amplia (WAN). Es aquella red que está formada por la interconexión de varias LAN. Una WAN abarca una gran área geográfica de varios kilómetros. Las WAN son útiles cuando los usuarios de una red necesitan acceder a los recursos de otra red. Esto ocurre por ejemplo cuando las oficinas principales de una compañía necesitan utilizar recursos de la red que se encuentra en alguna de sus fábricas ubicada a varios kilómetros de distancia. Las WAN realizan lo siguiente:

- Operan sobre grandes áreas geográficamente separadas
- Permiten que los usuarios mantengan comunicación en tiempo real con otros
- Proporcionan acceso a los recursos remotos de una LAN
- Ofrecen servicios de correo electrónico, web, transferencia de archivos y comercio electrónico.

Las principales tecnologías WAN son:

- Módems
- Red Digital de Servicios Integrados (RDSI)
- Línea de Abonado Digital (DSL, Digital Suscriber Line)
- Frame Relay
- Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode)
- Portadoras T1, E1, etc
- Red Óptica Síncrona (SONET, Synchronous Optical Network).

En la figura 4.2 se pueden observar distintas redes LAN conectadas a una red WAN que puede utilizar diferentes tecnologías.

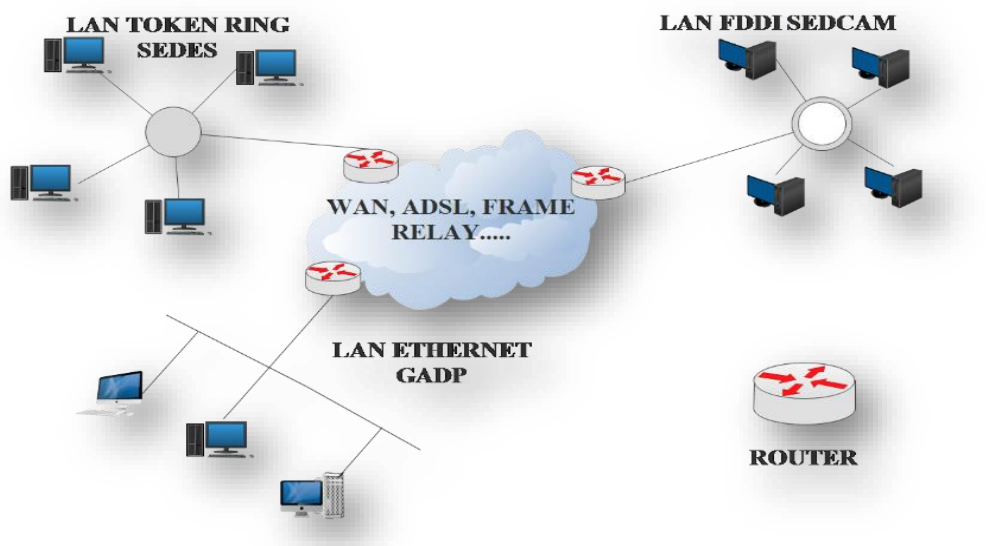


Figura 4-2: LAN y WAN
Fuente: Elaboración propia

4.3.2.2 **Topología**

Según (Cisco Networking Academy, 2015)En cuanto a la topología, como se muestra en la figura 4.3, existen básicamente cuatro tipos de redes de las cuales se desprenden varias combinaciones. Estas topologías son:

- Red tipo bus
- Red tipo estrella
- Red tipo anillo
- Red tipo malla
- Red tipo híbrida

Red tipo bus. En esta topología se utiliza un cable o serie de cables como eje central al cual se conectan todas las computadoras. En este conductor se efectúan todas las comunicaciones entre las computadoras. Esta red conviene usarse si no son muchas las computadoras que se van a conectar.

Red tipo estrella. Se caracteriza por tener un núcleo del cual se desprenden líneas hacía varias terminales. Fueron las primeras en utilizarse en el mundo de la computación. Esta topología es útil cuando se tiene una computadora central muy potente

rodeada de máquinas de menor potencia. Esta topología es la más común porque es la que más utilizan las redes Ethernet.

Red tipo anillo. Aquí también se utiliza un bus como eje central para conectar todos los equipos, sin embargo, dicho bus forma un anillo. Esta topología es utilizada en redes Token Ring y FDDI además de que es favorecida por los principales proveedores de acceso a Internet.

Red tipo malla. En esta topología, todos los dispositivos o algunos de ellos son conectados con todos los demás con el fin de conseguir redundancia y tolerancia a fallos. Si un enlace falla, la información puede fluir por otro enlace. Las redes de malla suelen implementarse solamente en redes WAN.

Red tipo híbrida. La topología híbrida es una red que utiliza combinaciones de las topologías anteriores.

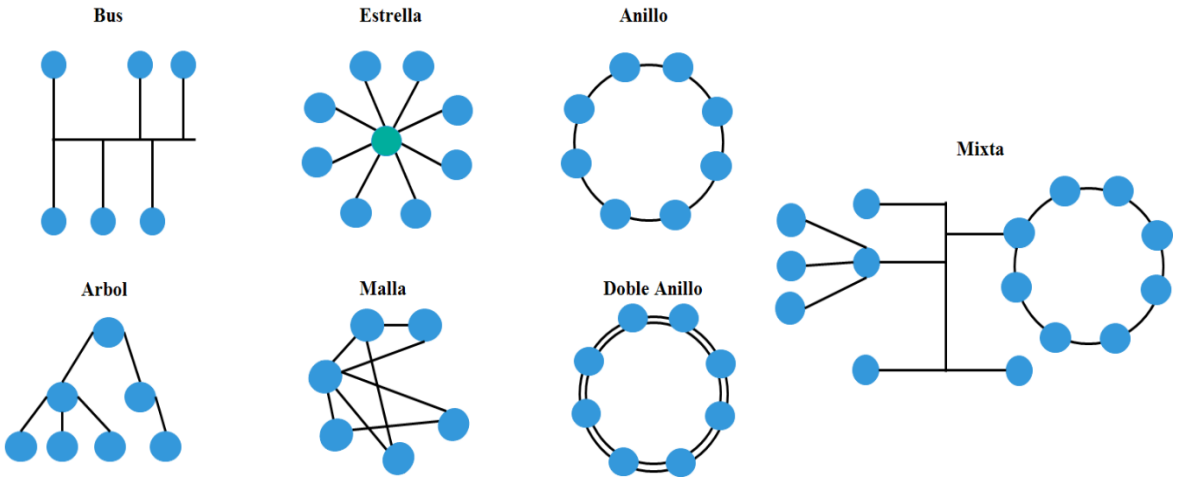


Figura 4-3: Topología de Redes
Fuente: Wikipedia

4.3.2.3 **Propiedad**

La clasificación de las redes en cuanto a propiedad se refiere a la forma de administración de la red. Así pues, como se muestra en la figura 4.4, las redes de computadoras se pueden clasificar de la siguiente forma:

- Redes privadas
- Redes públicas

Red privada. Es aquella red exclusiva de una sola compañía u organización en particular. La información no se comparte con otras compañías u organizaciones. En una red privada la información estará protegida, se podrá controlar el uso que se le da a la red y se podrá predecir el ancho de banda disponible.

Red pública. Es una red a través de la cual circula información de muchas compañías y organizaciones. Una red pública siempre será menos segura que una red privada, pero resultan ser más económicas y no se requiere que un administrador de red local de mantenimiento a una de estas redes. Como ejemplo de red pública tenemos a Internet.

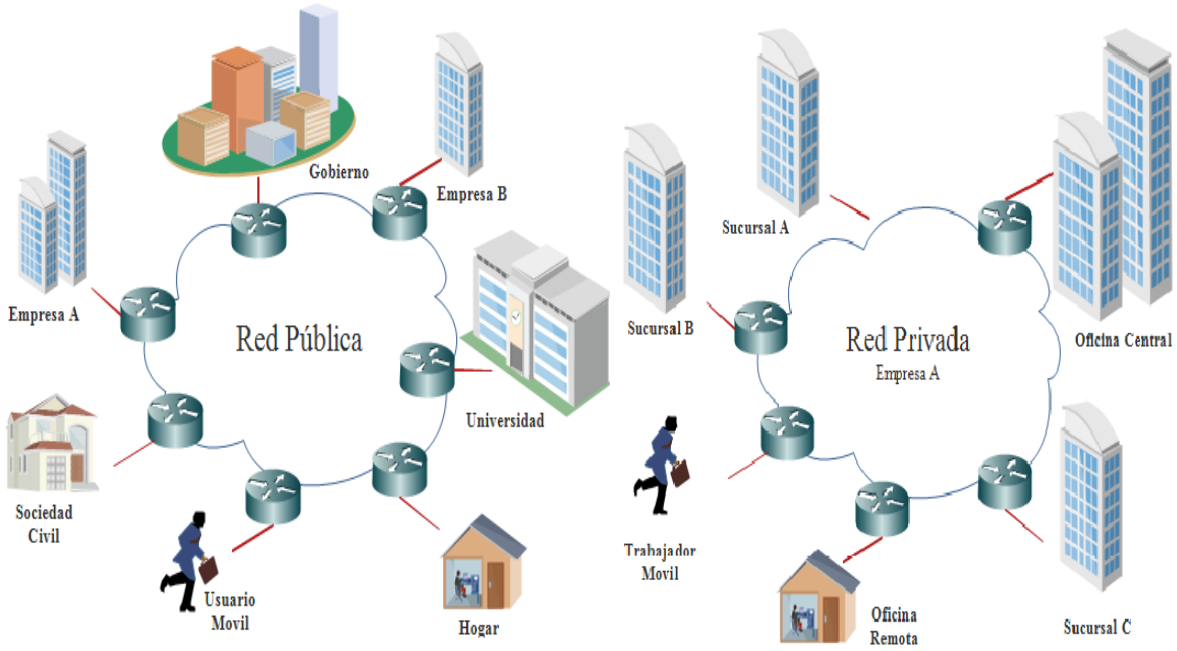


Figura 4-4: Red Pública y Privada
Fuente: Elaboración propia

4.3.3 Componentes de una red de computadoras

Según (Daniel Benchimol, 2010) Una red de computadoras consta de varios equipos necesarios para el correcto funcionamiento de la red. Entre los componentes de una red podemos encontrar el cableado y dispositivos de red como aparece en la figura 4.5.

4.3.3.1 Sistema de cableado

Éste se refiere al medio físico que se usa para conectar entre sí las estaciones de trabajo de los usuarios y con otros dispositivos o nodos de la red para lograr un intercambio

de información. La elección del sistema de cableado depende de varios factores, como los que se mencionan a continuación:

- Tipo de ambiente donde se va a instalar
- Tipo de equipo por conectar
- Tipo de aplicación y requerimiento
- Capacidad económica (relación costo/beneficio)

Se utilizan tres tipos de cables para instalar redes de cómputo, de los cuales los dos primeros son alámbricos y el tercero es óptico:

- Par trenzado
- Cable coaxial
- Fibra óptica.

El cable par trenzado es el medio de transmisión más utilizado actualmente. Se trata cuatro pares de dos conductores de cobre forrados con plástico, torcidos entre sí y protegidos por una cubierta de plástico. Existen dos clases de par trenzado: el UTP, que es el que más se usa y que tiene diferentes categorías que van desde la categoría 3 hasta la 7 con velocidades desde 10 Mbps hasta 1 Gbps y el STP, el cual tiene mayor resistencia al ruido y del cual hay cuatro tipos diferentes.

El cable coaxial es utilizado cada vez menos debido al auge del UTP. Existen dos tipos de cable coaxial: el delgado, el cual tiene un grosor de 6 mm. y puede transportar señales a distancias de hasta 185 m. y el grueso, el cual tiene un diámetro de 12 mm. y puede transportar señales a distancias de hasta 500 m.

La fibra óptica consiste en un núcleo central muy delgado de vidrio con alto índice de refracción de la luz. Alrededor del núcleo hay un revestimiento de vidrio, pero con un índice de refracción más bajo que protege al núcleo de contaminación. La fibra óptica posee un ancho de banda muy grande y poca pérdida de señal, lo que las hace ideales para transmitir un gran volumen de datos y a grandes distancias. La desventaja es que su instalación es muy costosa todavía.

4.3.3.2 **Dispositivos de interconexión de redes**

- Concentrador (hub)
- Conmutador (switch)
- Enrutador (router)

Concentrador o hub: Es un dispositivo que conecta varios cables de red que llegan desde computadoras cliente a la red. Existen concentradores de diferente tamaño en los cuales se puede conectar desde dos computadoras hasta más de 60 equipos. La información que llega al nodo de un hub es retransmitida a todos los demás nodos conectados a este equipo, lo que puede afectar el desempeño de una red.

Conmutador o switch: Se trata de un dispositivo que conmuta de forma dinámica sus distintos puertos para crear las conexiones. Un switch es un equipo semejante a un hub con la diferencia de que todas las conexiones de red tienen su propio dominio de colisión, esto hace que cada conexión de red sea privada, lo cual incrementa el desempeño de una red.

Enrutador o Router: Es un equipo que direcciona los paquetes de datos de una red a otra. Las dos redes se conectan al router usando sus propios cableados y tipos de conexión. Este dispositivo puede determinar cuál es la ruta más corta de un paquete hacia su destino, además de que también pueden optimizar el ancho de banda de la red y ajustarse de manera dinámica a problemas de patrones de tráfico cambiantes dentro de la red. Para que un router funcione de manera correcta, necesita ser programado, esto se puede realizar conectando una PC a una terminal del router y utilizando algún software de terminal o un programa en modo gráfico.

4.3.3.3 **Dispositivos terminales de redes o de usuario final**

Los dispositivos terminales de redes o de usuario final son aquellos que son conectados por los dispositivos de interconexión de redes y son los puntos finales de una red que transmiten o envían la información. Estos dispositivos son:

- Estación de trabajo (host)
- Servidor
- Tarjeta de Interfaz de Red (NIC)

Estación de trabajo. Son las computadoras que componen la red. Permiten a los usuarios crear, compartir y obtener información. A las estaciones de trabajo también se les denomina hosts y el término incluye a las impresoras en red.

Servidor. Es aquella computadora que proporciona funciones o servicios a otras computadoras. Existen diferentes tipos de servidores de acuerdo a la función que realizan como servidores de archivos, de red, de acceso remoto, de Internet, etc.

Tarjeta de Interfaz de Red (NIC, Network Interface Card). Es un dispositivo electrónico que permite a un ordenador o impresora acceder a una red y compartir recursos entre dos o más equipo.

Figura 4-5: Componentes de una red de computadoras
Fuente: Elaboración propia

4.3.4 El modelo OSI

4.3.4.1 Definición del modelo OSI

Según (Andrew S. Tanenbaum y David J. Wetherall, 2012)El modelo OSI (Sistemas Abiertos de Interconexión) define los métodos y protocolos necesarios para lograr la comunicación entre los equipos en una red. Fue desarrollado por la Organización Internacional de Estandarización (ISO) con el fin de proporcionar un modelo de referencia para la normalización y quedó definido en la norma ISO 7498.

El modelo divide las funciones en un conjunto jerárquico de capas. Cada capa realiza un conjunto de tareas necesarias para lograr la comunicación con otros sistemas. Cada

capa se sustenta en la inmediatamente inferior, la cual realiza funciones más primitivas ocultando los detalles a las capas superiores. El modelo define en términos generales las funciones que se deben realizar en cada capa. El modelo OSI consta de siete capas, e idealmente, cada sistema debe poseer las siete capas. Estas capas se muestran en la figura 4.6.

Figura 4-6: Las siete capas del modelo OSI
Fuente: Elaboración propia

4.3.4.2 **Las capas del modelo OSI**

Capa física. La capa física se encarga de la interfaz física entre los dispositivos, así como las reglas que rigen la transmisión de los bits. Esta capa tiene cuatro características importantes:

- Mecánicas
- Eléctricas
- Funcionales
- De procedimiento

Las características mecánicas definen las propiedades físicas de la interfaz con el medio de transmisión, como por ejemplo la especificación del conector que transmite las señales a través de los conductores. Las características eléctricas especifican la forma en

cómo se representan los bits, tales como niveles de voltaje, así como su velocidad de transmisión. Las características funcionales especifican las funciones que realiza cada uno de los circuitos de la interfaz física entre el sistema y el medio de transmisión. Por último, las características de procedimiento definen la secuencia de eventos que se llevan a cabo en el intercambio del flujo de bits a través del medio físico.

Capa de enlace de datos. La capa de enlace de datos proporciona los medios para activar, mantener y desactivar el enlace, así como intentar hacer que el enlace físico sea fiable. Uno de los principales servicios de esta capa es proporcionar detección y corrección de errores. Los elementos de información que circulan por esta capa se denominan tramas. En la mayor parte de los sistemas, los controladores de las NIC realizan el trabajo de esta capa.

Esta capa se divide normalmente en dos subcapas las cuales son LLC (Control de Enlace Lógico) y MAC (Control de Acceso a Medios). LLC realiza establecimiento y terminación de conexión, además de la transferencia de datos. MAC controla el ensamble y fragmentación de tramas, detección y corrección de errores, y direccionamiento. Los protocolos MAC más importantes son:

- 802.3 Ethernet
- 802.5 Token Ring
- 802.7 Banda Ancha
- 802.11 Inalámbrico
- 802.12 100BaseVBG.

Capa de red. La capa de red realiza la transferencia de información entre sistemas finales a través de algún tipo de red de comunicación. Aquí es donde se define la forma en que los paquetes llegan de un punto a otro dentro de una red y lo que lleva cada paquete. Esta capa define distintos protocolos de transmisión de paquetes. Estos protocolos definen las direcciones fuente y destino. Además, en esta capa se realizan las funciones de conmutación y enrutamiento de los paquetes. Los protocolos más importantes de esta capa son IP, IPX, AppleTalk y NetBIOS.

Capa de transporte. En la capa de transporte se proporciona un mecanismo para intercambiar datos entre sistemas finales. El servicio de transporte orientado a conexión asegura que los datos se entregan libres de errores, en orden y sin pérdidas ni duplicaciones. En esta capa se realiza también una optimización de los servicios de red. Algunos de los protocolos de transporte son TCP y UDP.

Capa de sesión. Esta capa proporciona los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales, es decir, se define la conexión de un usuario en un servidor de red o desde un punto de una red hasta otro punto. Estas conexiones virtuales se conocen como sesiones e incluyen la negociación entre el cliente y el anfitrión, la transferencia de información del usuario y la autenticación en la red.

Capa de presentación. La capa de presentación se encarga de definir el formato de los datos que se intercambian entre las aplicaciones y además ofrece un conjunto de servicios para transformar dichos datos. En esta capa se define la sintaxis utilizada entre las aplicaciones y proporciona los medios para seleccionar y modificar la representación utilizada. Las funciones que se realizan en esta capa pueden incluir el cifrado y la compresión de los datos.

Capa de aplicación. Esta capa proporciona a los programas de aplicación los medios necesarios para que accedan al entorno OSI, es decir, controla la forma en que el sistema operativo y sus aplicaciones interactúan con la red. En esta capa se encuentran las aplicaciones dedicadas a la transferencia de archivos (FTP), el correo electrónico (SMTP), el acceso remoto, etc.

4.3.5 Protocolo TCP/IP

Según (CCM, 2014), El Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP, Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos que permiten la comunicación a través de varias redes diferentes. TCP/IP fue creado por el Departamento de Defensa de Estados Unidos y se diseñó porque se quería un protocolo que fuera capaz de transmitir información en cualquier momento y bajo cualquier condición. Este protocolo tan popular dio origen a Internet, el cual ha posibilitado la interconexión de toda clase de redes a nivel mundial.

4.3.5.1 **El modelo TCP/IP**

TCP/IP fue diseñado en base un modelo de cuatro capas. Este modelo precedió al modelo OSI y fue muy importante. Aunque los nombres de algunas capas del modelo TCP/IP son iguales a las del modelo OSI no se debe confundirlas. Las funciones que realizan son diferentes. Estas capas se muestran en la figura 4.7.

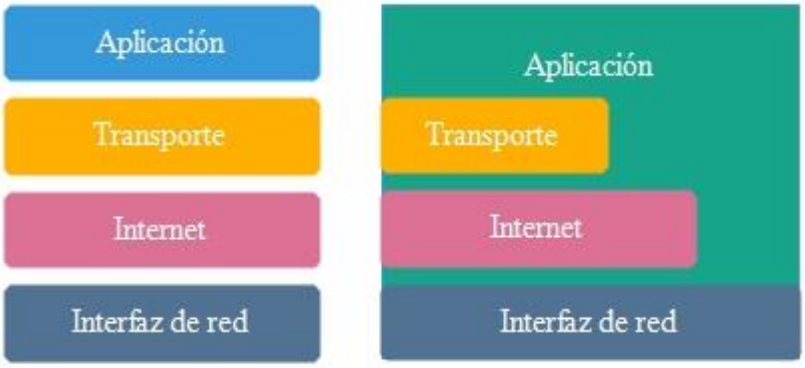


Figura 4-7: Las cuatro capas del modelo TCP/IP
Fuente: Elaboración propia

4.3.5.1.1 **Las capas del modelo TCP/IP**

Capa de Aplicación. Esta capa proporciona servicios que pueden ser utilizados por otras aplicaciones utilizadas para acceso remoto, correo electrónico, transferencia de archivos y administración de la red. La capa de aplicación de TCP/IP utiliza servicios de las tres capas superiores del modelo OSI (aplicación, presentación y sesión). Como podemos apreciar en la figura 4.7, TCP/IP no utiliza una estructura de capas rígida, ya que la capa de aplicación puede operar directamente sobre las capas de transporte, Internet y red. Los protocolos de la capa de aplicación son los siguientes:

- Protocolo de Transferencia de Hipertexto (HTTP, HyperText Transfer Protocol)
- Protocolo Trivial de Transferencia de Archivos (TFTP, Trivial File Transfer Protocol)
- Protocolo de Transferencia de Archivos (FTP, File Transfer Protocol)
- Sistema de Archivos de Red (NFS, Network File System)

- Protocolo Simple de Transferencia de Correo (SMTP, Simple Mail Transfer Protocol)
- Emulación de Terminal (Telnet)
- Protocolo Simple de Administración de Redes (SNMP, Simple Network Management Protocol)
- Sistema de Nombres de Dominio (DNS, Domain Name System).

Capa de transporte. La capa de transporte se encarga de controlar las conexiones lógicas entre las computadoras o hosts. Los protocolos de esta capa segmentan y reensamblan los datos que las aplicaciones de la capa superior envían. Los protocolos de la capa de transporte son los siguientes:

- Protocolo de Control de Transmisión (TCP, Transmission Control Protocol)
- Protocolo de Datagrama de Usuario (UDP, User Datagram Protocol)

Capa de Internet. Gestiona la transferencia de información a lo largo de varias redes mediante el uso de routers. La capa de Internet de TCP/IP es equivalente a la capa de red del modelo OSI, ya que se encarga de la transferencia de paquetes entre computadoras conectadas a distintas redes. En esta capa se determina la mejor ruta a seguir y la conmutación de paquetes. Los protocolos de la capa de Internet son los siguientes:

- Protocolo de Internet (IP, Internet Protocol)
- Protocolo de Mensajes de Control en Internet (ICMP, Internet Control Message Protocol)
- Protocolo de Resolución de Direcciones (ARP, Address Resolution Protocol)
- Protocolo de Resolución Inversa de Direcciones (RARP, Reverse Address Resolution Protocol).

IP es un protocolo que funciona en la capa de red del modelo OSI el cual define a forma en que se asignan las direcciones a los datos que van del origen hasta el destino y la

secuencia en que los datos deben ser reensamblados en el otro extremo de la transmisión. En la figura 4.8 se puede apreciar la forma en que está estructurado un datagrama IP.

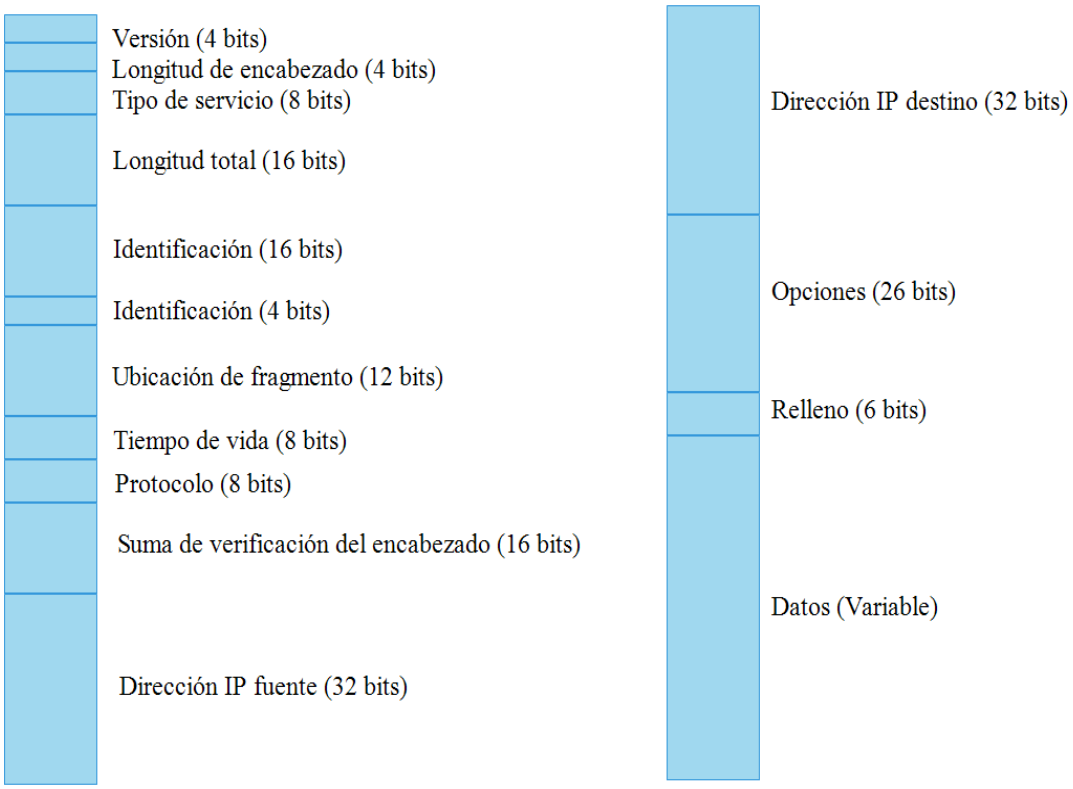


Figura 4-8: Estructura de un datagrama IP
Fuente: Elaboración propia

Capa de interfaz de red. Se encarga de todo lo relacionado con la transferencia de paquetes dependientes de la red. Realiza funciones que pertenecen a parte de la capa de enlace de datos y la capa física del modelo OSI. Se ocupa de los métodos utilizados para que un paquete IP pueda obtener un enlace físico con el medio de red. Los protocolos de la capa de interfaz de red son:

- Tecnologías LAN (Ethernet, Fast Ethernet, FDDI)
- Tecnologías WAN (ATM, Frame Relay)
- Protocolo Punto a Punto (PPP, Point-to-Point Protocol)
- ARP y RARP

4.3.6 Acceso remoto y conexiones WAN

4.3.6.1 Internet, intranets y extranets

Según (Cisco Networking Academy, 2015) Internet es una red de redes que ha proporcionado muchas ventajas a toda clase de organizaciones. A las empresas les aporta muchos beneficios económicos el hecho de conectarse a Internet y poder realizar ahí toda clase de negocios. Las corporaciones han descubierto también que llevar la tecnología sobre la cual se basa Internet a sus propias redes privadas les trae muchos beneficios a todos sus usuarios, de ahí el surgimiento de las intranets. Finalmente, las empresas requieren estar conectadas con sus socios y clientes, por lo que pronto surgen las extranets. Internet, intranet y extranet son conceptos muy importantes en el mundo de las VPN.

a) Internet. Internet conecta decenas de millones de computadoras en todo el mundo, permitiéndoles comunicarse entre sí y compartir recursos. Internet es una colección de redes organizada en una estructura multinivel las cuales usan toda una variedad de tecnologías para interconectarse. En el nivel más bajo se encuentra algunas decenas o cientos de computadoras conectadas a un router, formando una LAN. Otras computadoras se conectarán a un router a través de la red telefónica usando un módem. Una empresa o universidad podrá tener varios routers enlazados a un router principal. Estos routers se encuentran conectados mediante líneas alquiladas a un router de un Proveedor de Servicios de Internet (ISP, Internet Service Provider). A su vez, el proveedor conecta sus routers a una WAN de alta velocidad llamada backbone. Un país puede tener varios backbones que conectan a todos los ISP. Finalmente, los backbones de todos los países se interconectan en una malla usando líneas internacionales. Todo esto es lo que finalmente forma Internet.

La base de Internet es TCP/IP. El éxito de las redes basadas en IP se debe precisamente a Internet. Dos conceptos definen la tecnología de Internet: los paquetes y la forma de direccionamiento.

Paquetes. Internet transporta toda la información en unidades llamadas paquetes. Un paquete consta de dos partes: la información que contiene, la cual se llama carga útil y la información acerca de la información, llamada cabecera. La cabecera contiene información acerca de las direcciones origen y destino, longitud de los datos y tipo de éstos.

Direccionamiento. Las direcciones de la cabecera permiten el envío de la información a través de Internet. Los routers se encargan de realizar esto. Los paquetes

recorren diferentes caminos para llegar a su destino y eventualmente pueden ser almacenados dentro del router.

b) Intranet. Una intranet es una Internet orientada a una organización en particular. Los servidores web intranet difieren de los servidores web públicos en que estos últimos no tienen acceso a la intranet de la empresa sin los permisos y las contraseñas adecuadas. Una intranet está diseñada para que accedan a ellas sólo los usuarios con los debidos permisos de acceso a una red interna de una empresa. Una intranet reside dentro de un firewall y éste impide el acceso a los usuarios no autorizados.

c) Extranet. Una extranet es una intranet orientada a las personas u organizaciones que son externas a su empresa, pero necesitan acceder a alguna información, así se le permite el acceso a este contenido adicional, siempre bajo un sistema de autenticación y control de acceso.

La diferencia entre una intranet y una extranet es el método de acceso, siendo similares en cuanto a las facilidades y funciones, el tipo de recurso que utiliza y su filosofía general, de proporcionar acceso fácil, rápido y seguro a la información requerida.

El concepto extranet nace cuando una empresa quiere dar acceso a unas determinadas personas o grupos de personas a una determinada información de su intranet. Sin hacerla pública, la hace accesible a otras personas que puedan necesitarla o con quien mantienen relaciones comerciales.

El ejemplo más claro es la accesibilidad que una empresa da a una parte de sus clientes o proveedores.

4.3.6.2 **Acceso remoto**

Conectarse a una red desde una ubicación distante es lo que se denomina acceso remoto. El acceso remoto a una red ha sido algo de gran importancia en el mundo de las redes, ya que muchas compañías que promueven viajes de trabajo de sus empleados o el trabajo desde el hogar o desde una pequeña oficina remota. Y estos empleados necesitan conectarse a la red privada de la compañía para consultar ciertos archivos o correo electrónico. La necesidad del acceso remoto ha sido la causa principal del auge de las redes privadas virtuales, por lo que es preciso analizarlo un poco antes de verlo desde el punto de vista de las VPN.

4.3.6.2.1 **Necesidades de acceso remoto**

Con el incremento de las relaciones comerciales a nivel internacional, la movilidad geográfica de puestos de trabajo está llevando a las redes privadas a una situación bastante complicada. Los usuarios precisan conexiones que les permitan el acceso a las corporaciones desde cualquier lugar del mundo. Estas necesidades, unidas a las surgidas como consecuencia de la demanda de telecomunicaciones a tiempo completo, están aumentando drásticamente el número de oficinas remotas que una compañía debe interconectar. Como resultado, muchas redes privadas están convirtiéndose en redes muy complicadas de administrar.

El establecimiento de un sistema de acceso remoto en una red es algo que debe ser planeado cuidadosamente por lo que se debe definir claramente quiénes van a necesitar del acceso remoto y qué tecnología se utilizará para satisfacer las necesidades de esos usuarios.

De acuerdo a la figura 4.9, existen diferentes tipos de usuarios dependiendo de las necesidades de una organización y esto hará que las soluciones de acceso remoto también varíen de acuerdo a dichas necesidades. Los usuarios pueden ser clasificados de la siguiente forma:

- Usuarios móviles
- Usuarios de oficina remota

Usuarios móviles

Son aquellos que necesitan realizar viajes de trabajo a otro estado o país. Estos usuarios requieren de acceder a los recursos de la red de la oficina principal tales como su correo electrónico o sus archivos desde esa ubicación distante. Si el usuario viaja a otro país, entonces tiene que lidiar con diferentes sistemas telefónicos y compañías de telecomunicaciones, complicando la conexión a la red corporativa.

Usuarios de oficina remota

Son aquellos que acceden a la red corporativa desde una ubicación fija distante como puede ser una pequeña oficina o el hogar. El teletrabajo es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional en el domicilio del trabajador.

Engloba una amplia gama de actividades, e implica el uso de computadoras y la conexión permanente entre el trabajador y la empresa.

El usuario que trabaja desde su casa tiene su computadora conectada a la red privada y desde ahí tienen acceso al correo electrónico o algunas aplicaciones de la empresa.

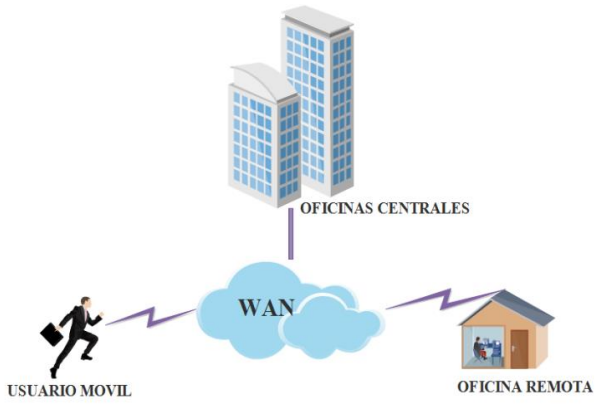


Figura 4-9: Acceso Remoto
Fuente: Elaboración propia

Si una compañía requiere de un sistema de acceso remoto lo primero que se tiene que evaluar es que tipo de usuarios tiene, ya sea móviles, de oficina remota o ambos. Una vez hecho esto, lo que debe hacerse es definir las necesidades de estos usuarios que se deben satisfacer. Estas necesidades pueden ser:

- Acceso remoto al correo electrónico
- Acceso remoto a los archivos del usuario
- Acceso remoto a una aplicación centralizada
- Acceso remoto a aplicaciones personalizadas o programas groupware
- Acceso remoto a la intranet o extranet, etc.

Después de examinar estas necesidades, el siguiente paso es estimar los requerimientos del ancho de banda para los diferentes usuarios. Esto es necesario para determinar qué tipo de conexión es necesaria para establecer el acceso remoto. También es importante determinar si dicha conexión es económicamente rentable para la empresa.

4.3.6.2.2 **Acceso remoto antes de las VPN**

Antes de que las VPN fueran tomadas como opción para el acceso remoto, era común que una corporación instalara módems desde los cuales el usuario remoto hacía una llamada para estar en conexión con la red corporativa. En redes donde no hay muchos usuarios remotos se pueden agregar sólo uno o dos módems a una computadora configurada como Servidor de Acceso Remoto (RAS, Remote Access Server). En el caso de organizaciones que mantienen muchos usuarios remotos, es preciso instalar desde decenas hasta cientos de módems y formar bancos o pilas de módems como se puede ver en la figura 4.10.

El acceso remoto así resulta ser caro y requiere de un gran soporte por parte de las empresas. Frecuentemente, los usuarios se encuentran muy alejados de las oficinas centrales de la compañía y tienen que realizar llamadas de larga distancia. Esto resulta ser especialmente caro si las llamadas son internacionales y si los teletrabajadores requieren estar conectados durante un tiempo largo. El acceso remoto requiere también del uso de los RAS que también son muy caros.

El uso de un módem desde otro país causa muchas dificultades ya que las velocidades de conexión son muy lentas, una línea telefónica no es buena y puesto que la mayor parte del tráfico internacional pasa a través de un satélite se producen muchos retrasos en la comunicación.

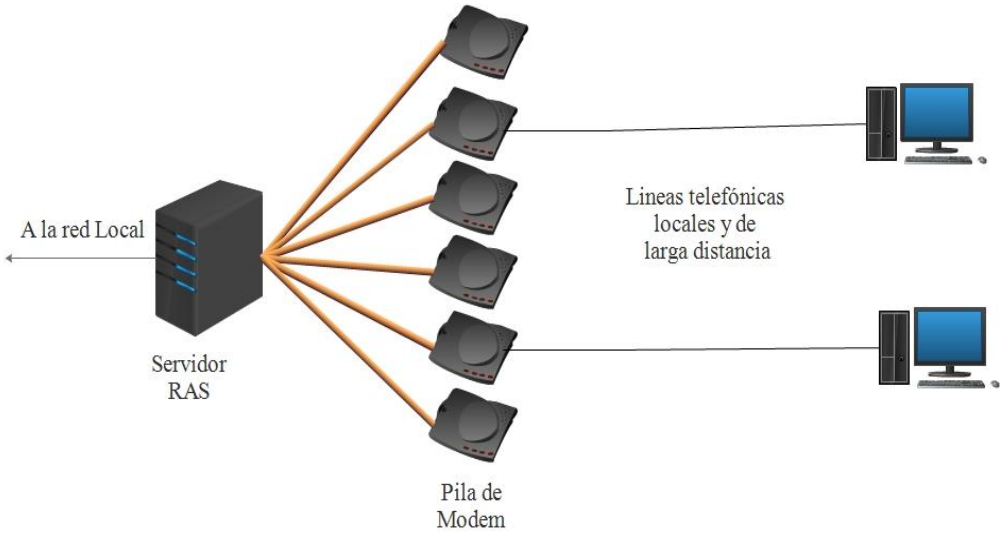


Figura 4-10: Acceso remoto sin una VPN
Fuente: Elaboración propia

4.3.6.3 **Conexiones WAN**

Según (William Satanllings, 2000) Existen diversas tecnologías o conexiones para poder unir diferentes LAN y crear una WAN. Un enlace WAN puede ser conmutado o dedicado. Por conmutado se entiende que es aquel que no está disponible todo el tiempo, la conexión se establece sólo cuando es necesaria. Un ejemplo de esto es una conexión de acceso telefónico a redes a través de un módem. Por otra parte, un enlace dedicado es aquel donde la conexión siempre estará disponible, incluso cuando no se esté utilizando. Como ejemplo podemos mencionar una conexión que utiliza tecnología xDSL. Las conexiones WAN se pueden clasificar de la siguiente manera:

- Servicios de conmutación de circuitos
- Servicios de conmutación de paquetes
- Servicios de conmutación de celdas
- Servicios digitales dedicados
- Servicios de marcación, cable e inalámbricos

4.3.6.3.1 **Servicios de conmutación de circuitos**

La conmutación de circuitos es un método en el que se establece, mantiene y termina un circuito físico dedicado a través de una red de proveedor para cada sesión de comunicación. Los servicios de circuitos conmutados utilizan Multiplexación por División del Tiempo (TDM) y son síncronos (utilizan STM). Los dos servicios de circuitos conmutados son POTS y RDSI.

Servicio Telefónico Analógico Convencional (POTS, Plain Old Telephone Service). Se trata de la red telefónica, también llamada Red Pública Telefónica Conmutada (PSTN, Public Switched Telephone Network). Aunque no es propiamente un servicio de datos de computadora, muchas de sus tecnologías son parte de la creciente infraestructura de datos y es una red de telecomunicaciones fiable, fácil de usar y de área amplia.

Red Digital de Servicios Integrados (RDSI o ISDN, Integrated Services Digital Network). Se trata del primer servicio de conexión telefónica digital. Es un sistema diseñado para integrar voz y datos en una sola conexión. Existen dos tipos principales de RDSI:

- Interfaz de servicio básico (BRI)
- Interfaz de servicio primario (PRI)

La interfaz de servicio básico (BRI) es una conexión que se puede tener en cualquier hogar o pequeña oficina. Consiste en dos conexiones simultáneas que pueden ser una mezcla de voz datos y fax. Cuando es usado como una conexión de datos BRI ofrece dos canales (llamados canales B) de 64 kbps o 128 kbps cuando se combinan en una sola conexión.

La interfaz de servicio primario (PRI) ofrece 24 o 30 canales de 64 kbps dando un total de 1.536 o 1920 kbps respectivamente. Al igual que en BRI, cada canal puede conectarse para un propósito diferente o combinarse para incrementar el ancho de banda.

Tanto BRI como PRI poseen un tercer canal llamado D el cual contiene la información de configuración de los canales B. El medio de transmisión más común para una red RDSI es el cable de cobre de par trenzado.

4.3.6.3.2 **Servicios de conmutación de paquetes**

La conmutación de paquetes es un método que enruta pequeñas unidades de datos denominadas paquetes a través de una red en base a la dirección de destino contenida en el paquete. Los dos servicios de paquetes conmutados son X.25 y Frame Relay.

X.25. Aunque se trata de una tecnología antigua, todavía sigue utilizándose en muchos lugares. X.25 tiene capacidades extensivas de comprobación de errores debido a que al principio las WAN eran muy propensas a fallar a causa de un error en la transmisión de información. Esto hace que sea una tecnología fiable, pero debido a esto su ancho de banda queda limitado lo que lo hace más lento que Frame Relay. El ancho de banda que puede alcanzar es de hasta 2 Mbps. X.25 es orientado a conexión y la comprobación de errores trabaja en las capas 2 y 3 del modelo OSI. El medio de transmisión más común para una red X.25 es el cable de cobre de par trenzado. El costo de X.25 es moderado.

Retransmisión de tramas (Frame Relay). Es una tecnología WAN de alto desempeño que opera en las capas 1 y 2 del modelo OSI y es de las tecnologías de redes más populares. Es una versión de paquetes conmutados del RDSI ya que originalmente fue diseñado para trabajar sobre este tipo de redes, aunque actualmente se utiliza en redes muy variadas. Frame Relay ofrece sus servicios en la capa 2, a diferencia de X.25 que también

proporciona servicios en la capa 3. Esto permite que las redes Frame Relay sean mucho más rápidas que las X.25.

Una red Frame Relay consta de dos tipos de dispositivos principales, tal como aparece en la figura 4.11. Estos son:

- Equipos Terminales de Datos (DTE, Data Terminal Equipment)
- Equipos Terminadores de Circuitos de Datos (DCE, Data Circuit-Terminating Equipment)

Los DTEs son considerados como equipos terminales de una red específica y están localizados en los dominios del cliente (corporaciones). De hecho, las corporaciones pueden ser propietarias de estos equipos. Ejemplos de DTEs son terminales, computadoras personales, routers y switches.

Los DCEs son dispositivos de redes portadores. El propósito de un DCE es proporcionar servicios de sincronización y conmutación en una red. Son dispositivos que transmiten datos a través de la WAN. Para el caso de Frame Relay, se trata de dispositivos de conmutación de paquetes.

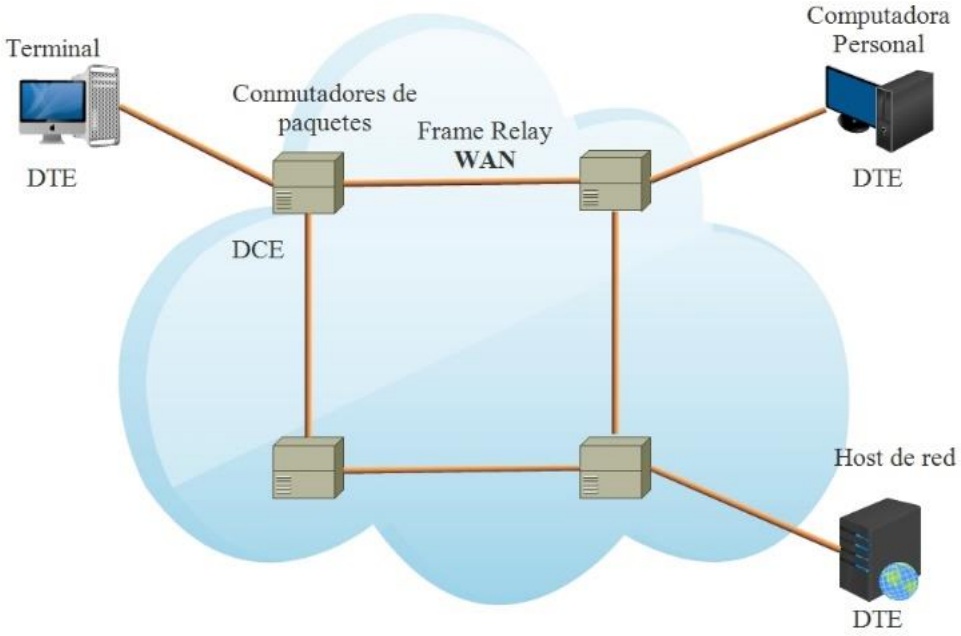


Figura 4-11: Red Frame Relay
Fuente: Elaboración propia

Frame Relay proporciona comunicación orientada a conexión en la capa de enlace de datos. Esto significa que una comunicación determinada existe entre cada par de dispositivos y que estas conexiones están asociadas con un identificador de conexión. Este servicio es implementado utilizando un circuito virtual, el cual es una conexión lógica creada entre dos DTEs a través de una red Frame Relay.

Los circuitos virtuales Frame Relay se dividen en dos categorías:

- Circuitos Virtuales Conmutados (SVC, Switched Virtual Circuits)
- Circuitos Virtuales Permanentes (PVC, Permanent Virtual Circuits)

Los SVCs son conexiones temporales utilizadas en situaciones que requieren sólo una transferencia de datos esporádica entre los DTEs a través de la red Frame Relay. Para transmitir datos se realiza una llamada y cuando se termina de transmitir la llamada es terminada.

Los PVCs son conexiones que son establecidas permanentemente las cuales son utilizadas cuando se desea transferencia de datos de forma continua entre los DTEs a través de la red Frame Relay. Un PVC no requiere el establecimiento y fin de llamadas como en los SVC.

Los circuitos virtuales Frame Relay son identificados por los Identificadores de Conexión de Enlace de Datos (DLCI, Data-Link Connection Identifiers). Los DLCI son asignados comúnmente por los proveedores de servicio Frame Relay.

El medio de transmisión más común para una red Frame Relay es el cable de cobre de par trenzado y la fibra óptica y el costo de este tipo de redes es de moderado a bajo.

4.3.6.3.3 **Servicios de conmutación de celdas**

Los servicios de conmutación de celdas proporcionan una tecnología de conmutación de conexión dedicada que organiza los datos digitales en unidades de celda y las transmite entonces por el medio físico utilizando tecnología de señal digital. Los dos servicios de celdas conmutadas son ATM y SMDS.

Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode). ATM surgió debido a las necesidades de crear un RDSI de banda ancha. Es un método de multiplexación y conmutación que permite varios servicios. Se trata de una técnica de

conmutación de celdas orientada a conexión y el cual combina varias de las características de la conmutación de paquetes y la conmutación de circuitos al utilizar TDM. ATM realiza un control dinámico del ancho de banda. De esta manera, si una fuente de datos deja de enviar información, el canal de comunicación se reasigna a otra fuente. El ancho de banda máximo que soporta es de 622 Mbps, pero se está trabajando para ofrecer soporte a velocidades más elevadas. En la figura 4.12 se muestra una red ATM típica.

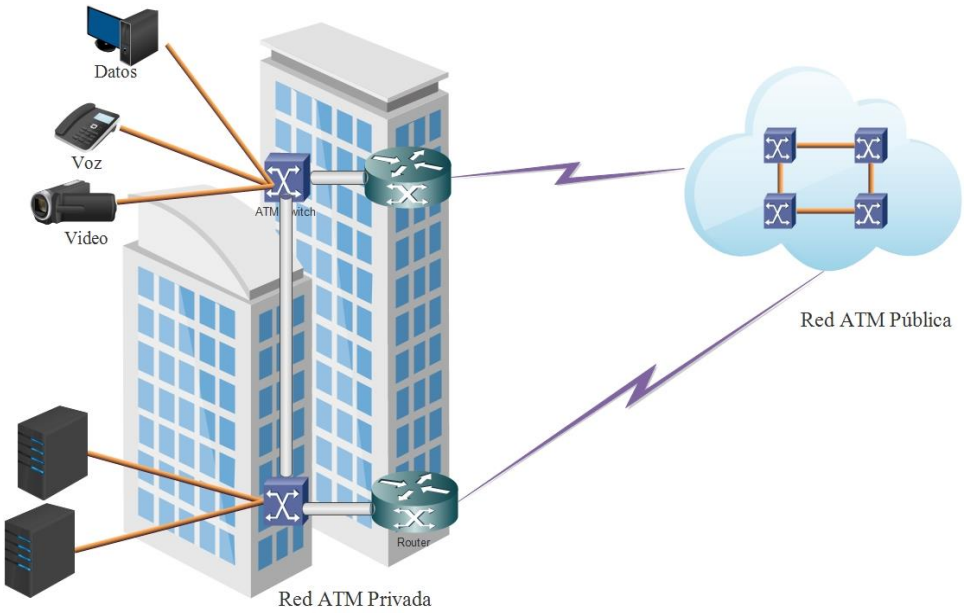


Figura 4-12: Red ATM
Fuente: Elaboración propia

ATM convierte todo el tráfico que fluye en la red a bloques de 53 bytes llamados celdas, de los cuales 48 son de carga útil y 5 son de la cabecera que contiene la información de destino de la celda, de acuerdo a la figura 4.13.

Figura 4-13: Estructura de una Celda ATM
Fuente: Elaboración propia

ATM no está limitada por la velocidad o distancia, la conmutación le permite operar a través de las LAN y redes de banda ancha mundiales. Estas velocidades permiten a ATM transportar voz, datos y video por lo que puede ofrecer soporte a una red de servicios integrados.

Al igual que Frame Relay, ATM proporciona dos tipos básicos de conexiones:

- Circuitos Virtuales Permanentes (PVC)
- Circuitos Virtuales Conmutadas (SVC)

El medio de transmisión más común para una red ATM es el cable de cobre de par trenzado y la fibra óptica. El costo de este tipo de redes es alto.

Servicio de Datos Multimegabit Conmutado (SMDS, Switched Multimegabit Data Service)

Es una tecnología muy relacionada con ATM y por lo general se utiliza en redes metropolitanas (MAN). Es una tecnología poco común, el medio de transmisión más común para una red SMDS es el cable de cobre de par trenzado y la fibra óptica. El costo de este tipo de redes es alto.

4.3.6.3.4 Servicios digitales dedicados

Los servicios digitales dedicados también proporcionan servicios de circuitos conmutados. Sin embargo, se trata de una conexión dedicada; es decir, siempre está disponible. Las series T y E, xDSL y SONET son las tecnologías de servicios digitales dedicados.

Series T y E (T1, T3, E1, E3,…)

La serie T de Estados Unidos, Canadá y Japón y la serie E de Europa y resto del mundo son de las tecnologías WAN más utilizadas. Los Laboratorios Bell desarrollaron una jerarquía de sistemas que pueden transportar señales digitales de voz.

En la capa más baja de esta jerarquía se encuentra una conexión llamado DS0 que transporta datos a 64 Kbps. 24 canales DS0 forman una conexión llamada DS1 o T1 a una velocidad de 1.544 Mbps.

Adicionalmente, existe una T1-C la cual opera a 3.152 Mbps. Existe también una T2 a 6.312 Mbps. Hay una T3, operando a 44.736 Mbps y finalmente, una T4 a 274.176 Mbps. El ancho de banda es de 2.048 Mbps para E1 y 34.368 Mbps para E3.

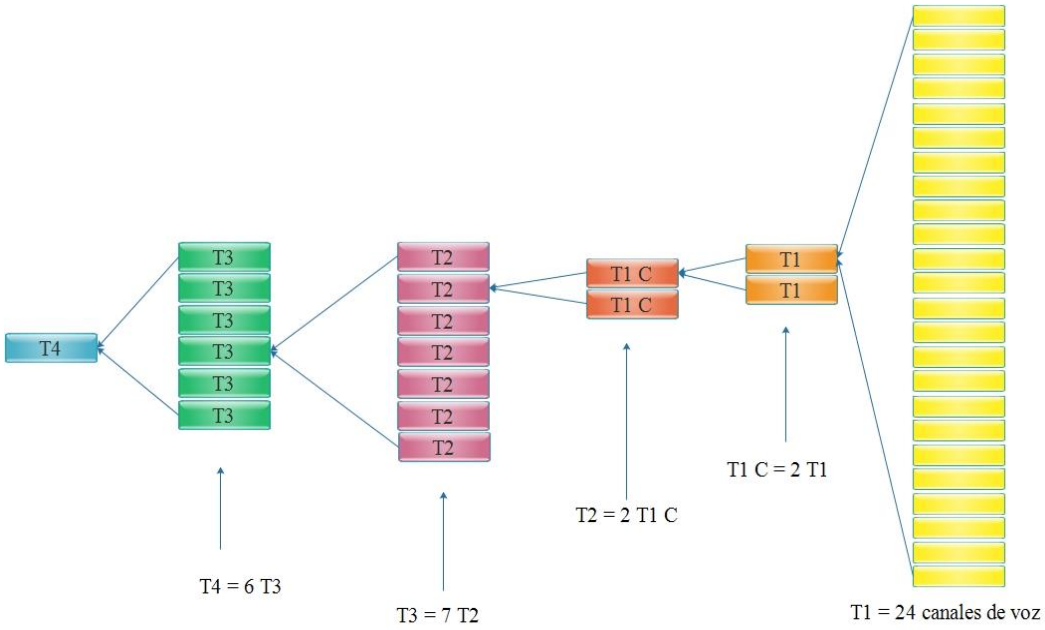


Figura 4-14: Jerarquía T
Fuente: Elaboración propia

En la tabla 4.2 se resume la jerarquía T y E:

Nivel de Señal (portadora)	Número de T1	Canales de Voz	Velocidad
DS0	1/24	1	64 Kbps
DS1(T1)	1	24	1.544 Mbps
DS1C (T1C)	2	48	3.152 Mbps
DS2 (T2)	4	96	6.312 Mbps
DS3 (T3)	28	672	44.736 Mbps
DS3C (T3C)	56	1344	89.472 Mbps
DS4 (T4)	168	4032	274.176 Mbps
Portadora	**Velocidad**		
E1	2 Mbps		
E2	8 Mbps		
E3	34 Mbps		
E4	139 Mbps		
E5	555 Mbps		

Tabla 4-2: La jerarquía T y E
Fuente: Elaboración propia

Una trama T1 se compone de 193 bits, de los cuales 192 son para datos y 1 bit extra llamado bit de trama es utilizado para sincronizar. El aspecto fundamental de una trama T1 se muestra en la figura 4.15.

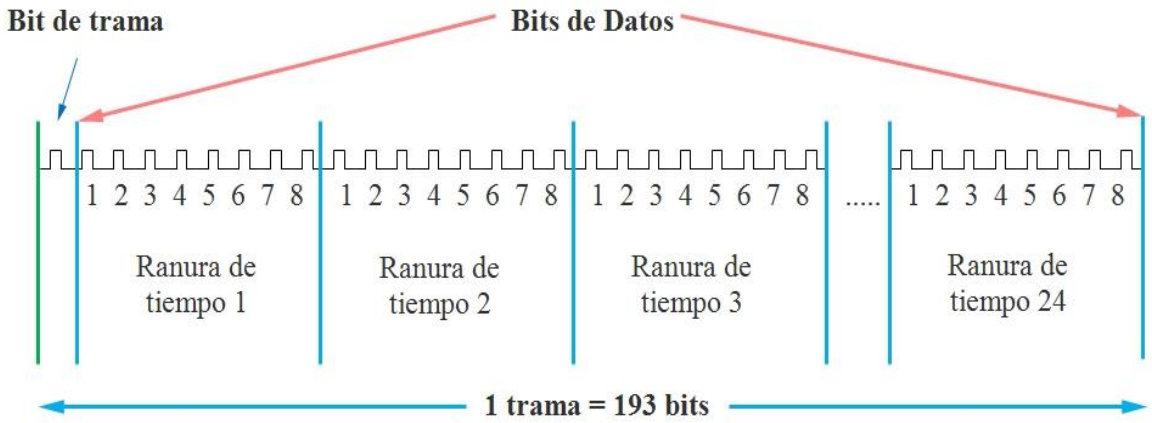


Figura 4-15: Estructura de una trama T1.
Fuente: Elaboración propia

T1 ha sido especificado por AT&T y por ANSI. El equivalente europeo, E1, es un estándar del Sector de Normalización de las Telecomunicaciones (UIT-T). E1 no utiliza un reloj maestro. En Estados Unidos, las tres portadoras mayores tienen cada una un reloj T1 maestro del cual se derivan las demás. Con estas tecnologías se pueden construir diferentes dispositivos tales como PBX, multiplexores T1, T1 fraccional, etc.

Las series T y E operan en la capa 1 y 2 del modelo OSI. Estas series utilizan TDM para asignar franjas de tiempo a la transmisión de datos. El medio de transmisión más común para las redes T y E es el cable de cobre de par trenzado y la fibra óptica y el costo de este tipo de redes es moderado.

Línea de Abonado Digital (DSL, Digital Suscriber Line). Es un conjunto de tecnologías y estándares utilizados para la transmisión de datos a alta velocidad utilizando el cableado telefónico normal. Para lograr las altas velocidades, DSL hace uso de todo el espectro de frecuencias que se pueden transmitir por una línea de cobre. La voz sólo utiliza bajas frecuencias por lo que las altas frecuencias son aprovechadas para la transmisión de datos. Los rangos de frecuencias son separados por un dispositivo especial (splitter) o por una serie de filtros que se conectan a cada socket en el que se va a conectar un teléfono. Para

lograr la conexión se utiliza un módem DSL. Existen diferentes tecnologías DSL, siendo algunas más útiles para la conexión a Internet y otras para interconectar dos o más LAN remotas. DSL se compone de las siguientes tecnologías:

- DSL Asimétrico (ADSL, Asymmetric DSL)
- DSL de Alta Velocidad (HDSL, High-bit-rate DSL)
- DSL de Velocidad Adaptable (RADSL, Rate Adaptable DSL)
- DSL Simétrico o de Línea Única (SDSL, Single-line DSL)
- DSL de muy Alta Velocidad (VDSL, Very-high-data-rate DSL).

ADSL es la tecnología más popular actualmente, debido a su amplio uso doméstico. Ofrece distintas velocidades que pueden alcanzar hasta 8 Mbps en recepción y 1 Mbps en envío de datos, aunque lo más común es una velocidad de 1.5 Mbps para la recepción y 256 kbps para el envío. El costo de las redes DSL es moderado, pero se está reduciendo cada vez más.

Red Óptica Síncrona (SONET, Synchronous Optical Network). Es un conjunto de tecnologías de capa física de alta velocidad diseñadas especialmente para la fibra óptica, aunque también pueden ser implementadas en cable de cobre de par trenzado. SONET define una tecnología para transportar muchas señales de diferentes capacidades a través de una jerarquía óptica, flexible y síncrona. Esto se cumple a través de un esquema de multiplexación de difusión de bytes. Esto simplifica la multiplexación y proporciona una administración de la red de punto a punto.

El primer paso en el proceso de la multiplexación SONET involucra la generación del nivel más bajo de la señal base. En SONET esta señal base es llamada Señal de Transporte Síncrono Nivel 1 (STS-1, Synchronous Transport Signal), la cual constituye el nivel eléctrico utilizado en los dispositivos de hardware. Las señales de niveles mayores son múltiplos enteros de STS-1, la cual crea toda una familia de señales STS-N. Una señal STS-N se compone de N señales STS de difusión de bytes. La parte óptica para cada señal STS-N se denomina Portadora Óptica Nivel N (OC-N, Optical Carrier), la cual es utilizada en las transmisiones por fibra óptica.

En la tabla 4.3 se muestra la jerarquía de señales SONET, su velocidad, así como la equivalencia con la serie T.

Nivel de Señal (Portad. óptica)	Velocidad	Capacidad
STS-1 (OC-1)	51.840 Mbps	28 DS1o 1 DS3
STS-3 (OC-3)	155.520 Mbps	84 DS1 o 3 DS3
STS-12 (OC-12)	622.080 Mbps	336 DS1 o 12 DS3
STS-48 (OC-48)	2.488 Gbps	1344 DS1 o 48 DS3
STS-192 (OC-192)	9.953 Gbps	5376 DS1 o 192 DS3
STS-768 (OC-768)	39.813 Gbps	21504 DS1 o 768 DS3

Tabla 4-3: La jerarquía de señales SONET
Fuente: Elaboración propia

El formato de una señal STS-1 se muestra en la figura 4.16. En general, la rama puede ser dividida en dos áreas principales: cabecera de transporte y Envoltura de Carga útil Síncrona (SPE, Synchronous Payload Envelope). El SPE se puede dividir también en dos partes: cabecera de ruta STS y la carga útil.

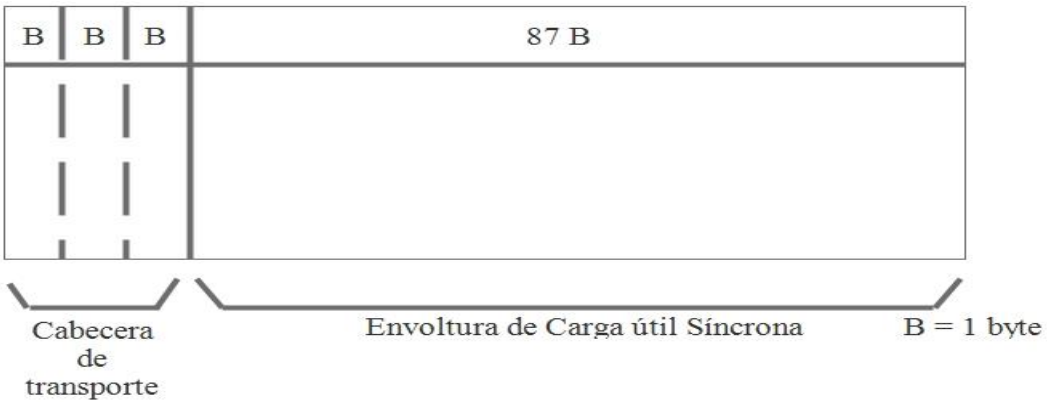


Figura 4-16: Estructura de una trama SONET.
Fuente: Elaboración propia

La carga útil tiene la capacidad de transportar arriba de 28 DS1s, 1DS3 o 21 señales de 2.048 Mbps o combinaciones de las anteriores. STS-1 es una secuencia específica de 810 bytes (6480 bits). Con una longitud de trama de 125µs (8000 tramas por segundo), STS-1 tiene una tasa de bits de 51.840 Mbps. El formato de una trama STS se compone de 9 filas de 90 columnas de bytes, es decir, 810 bytes. El orden de transmisión es de fila por fila, de izquierda a derecha.

Las redes SONET obtienen una alta velocidad de datos utilizando Multiplexación por División de Longitud de Onda (WDM, Wavelength Division Multiplexing). WDM es una tecnología que sincroniza los láseres a colores diferentes, lo que proporciona diferentes longitudes de onda y así poder enviar enormes cantidades de datos. SONET se utiliza principalmente en las entidades backbone de Internet. El costo de esta tecnología es alto.

4.3.6.3.5 **Servicios de marcación, cable e inalámbricos**

Existen otros servicios WAN diferentes a los explicados anteriormente. Se trata de los módems de marcación, los módems de cable y las redes WAN inalámbricas.

Módem de marcación. Esta tecnología funciona con la red telefónica existente. Su uso es extremadamente popular, sin embargo, está limitado en velocidad, ya que su ancho de banda máximo es de 56 kbps. El costo de esta tecnología es bajo.

Módem de cable. Esta tecnología coloca las señales de datos en el mismo cable que las señales de televisión. Es utilizado en zonas que poseen cable coaxial para televisión ya instalado. El ancho de banda máximo que puede alcanzar es de 10 Mbps, sin embargo, esta velocidad disminuye con el número de usuarios conectados a un mismo segmento de red. El costo de esta tecnología es relativamente bajo.

Redes WAN inalámbricas. Transmiten los datos por medio de ondas electromagnéticas que viajan por el aire. Los enlaces WAN inalámbricos se dividen en terrestres y satelitales. Los enlaces terrestres suelen utilizar microondas. El costo de esta tecnología es relativamente bajo y su uso es moderado. Los enlaces satelitales son utilizados por usuarios móviles en una red telefónica celular o por usuarios alejados de cualquier sistema de cableado. El costo de esta tecnología es alto, pero es ampliamente utilizado.

4.3.6.4 **Implementación de una WAN antes de las VPN**

Implementar una WAN requiere de una cuidadosa planeación debido a los costos ya a los tiempos requeridos para su instalación. Se debe analizar las aplicaciones que se le van a dar a la WAN con el fin de poder elegir una solución que pueda satisfacer las necesidades de una organización. Entre los aspectos que se deben analizar al elegir una solución WAN están los siguientes:

- Ubicación de las localidades (sucursales, oficinas remotas)
- Cantidad de datos a transmitir

- Velocidad de transferencia de la información
- Transmisión de datos en tiempo real (síncronos) o en un momento determinado (asíncronos)
- Restricciones

Algo muy importante a tomar en cuanta al crear una WAN es el costo. Tener una WAN implica costos de instalación y posteriormente gastos mensuales. Mantener un enlace WAN resulta costoso también porque las necesidades de ancho de banda se van incrementando con el tiempo. Entre más grande sea una red y más potentes sean sus componentes, mayores serán los costos de tener la red. Es necesario establecer un equilibrio entre el rendimiento de la red y los costos de ésta. Los costos de instalar un backbone privado por lo general van de los 100,000$ a 1’000,000$. dependiendo del tráfico y de las distancias geográficas.

Como se puede ver, el alto costo necesario para implementar y mantener redes privadas está llevando a éstas a una situación muy difícil. Las tecnologías WAN tradicionales, representan una serie de necesidades diarias. El personal de soporte necesario para gestionar estas tecnologías complejas conlleva un crecimiento continuo tanto en el número de personas como en su experiencia.

Igualmente, la dependencia de aplicaciones de red requiere un aprovisionamiento separado de respaldo además de una expansión de la infraestructura de la red privada ya existente.

4.4 FUNCIONAMIENTO DE LAS VPN

Es necesario comprender la definición, arquitecturas, tipos y topologías de una VPN. También se presenta el concepto de tunneling, que es la tecnología más importante sobre las que operan las VPN y se explican los métodos de seguridad (cifrado de datos, autenticación) que son utilizados para proteger los datos.

4.4.1 Introducción a las VPN

4.4.1.1 Definición de Red Privada Virtual (VPN)

Como se pudo leer en el capítulo anterior, los métodos tradicionales de acceso remoto y creación de WAN privadas resultan ser bastante costosos. Puesto que las redes

públicas resultan ser mucho más económicas que las privadas, se buscaron maneras de poder establecer una red privada dentro de una red pública. El resultado fue el surgimiento de las Redes Privadas Virtuales (VPN) las cuales han ofrecido ventajas muy amplias a las corporaciones siendo la principal de ellas la reducción de costos de instalación y mantenimiento de forma muy significativa. Se puede definir a una VPN de la siguiente manera:

Una Red Privada Virtual (VPN, Virtual Private Network) es una red privada que utiliza la infraestructura de una red pública para poder transmitir información.

Una VPN combina dos conceptos: redes virtuales y redes privadas. En una red virtual, los enlaces de la red son lógicos y no físicos. La topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla. Un usuario de una red virtual no será capaz de detectar la red física, el sólo podrá ver la red virtual.

Desde la perspectiva del usuario, la VPN es una conexión punto a punto entre el equipo (el cliente VPN) y el servidor de la organización (el servidor, firewall, etc. VPN). La infraestructura exacta de la red pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado. Esto se puede apreciar en la figura 4.17.

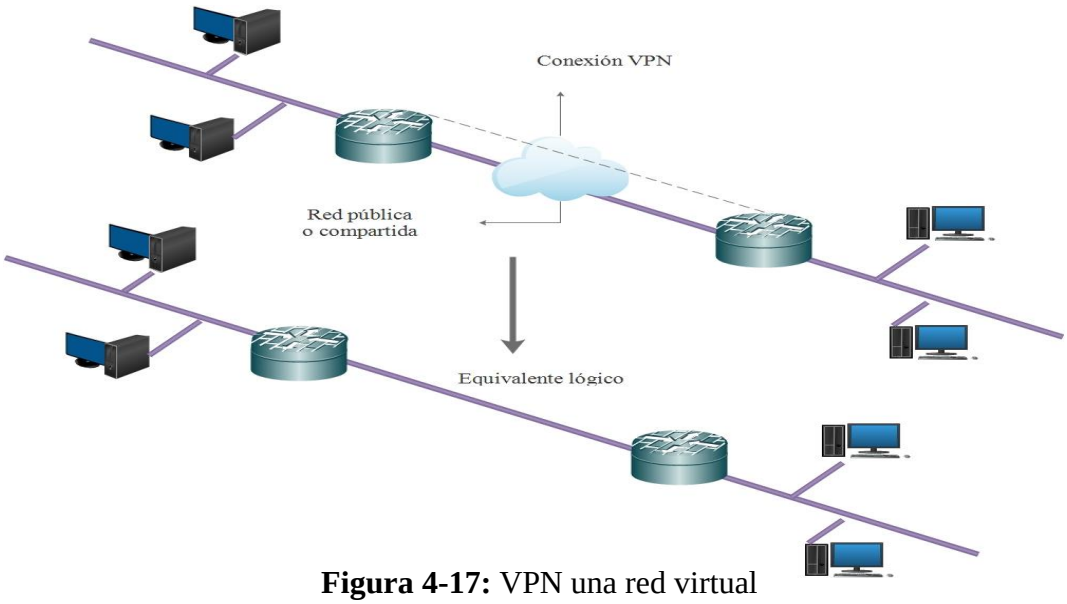


Figura 4-17: VPN una red virtual
Fuente: Elaboración propia

Las redes privadas son definidas como redes que pertenecen a una misma entidad administrativa. Un ejemplo típico de esta clase de red es una intranet corporativa, la cual puede ser utilizada sólo por los usuarios autorizados. De los conceptos de red privada y red virtual es como nace el concepto de red privada virtual.

Debido al hecho de ser una red privada que utiliza una red pública, la cuestión de la seguridad en una VPN es muy importante, ya que la información que circula en una red pública puede ser vista por cualquiera si no se toman las debidas precauciones. Y en una red pública como Internet existen muchas personas malintencionadas que siempre están dispuestas a robar información. Es por eso que una VPN debe de poseer excelentes mecanismos de autenticación y de encriptación de la información para que ésta viaje segura a través de una red pública.

4.4.1.1.1 **Historia del término VPN**

Resulta confuso definir el término VPN. El problema radica en que cada fabricante o proveedor de servicios VPN define a las VPN de diferentes maneras. No existen estándares que definan los componentes de software o hardware de una VPN o las tecnologías VPN, por lo que cada fabricante ofrece los servicios VPN que más se adaptan a sus propias plataformas de hardware y aplicaciones de software. Como la tecnología no está estandarizada, se ofrecen VPN en toda clase de formas diferentes, como pueden ser firewalls, sistemas operativos, etc. Respecto a la confusión para definir VPN un empresario de una importante empresa de telecomunicaciones mencionó: “Las VPN tienden a ser ahora lo que el mercado dice que son”.

El tiempo también ha modificado el concepto de VPN. El término VPN comenzó a aplicarse a las redes Frame Relay o ATM públicas, o a un servicio de acceso remoto basado en la red pública de telefonía conmutada (PSTN). En el capítulo anterior se explicó que las redes Frame Relay pueden implementarse de forma pública o privada. Pues bien, a las redes públicas Frame Relay se les dio el nombre de VPN, así como también a las redes públicas ATM. Estos servicios de VPN eran proporcionados por un proveedor de servicios, el cual conectaba las redes de diferentes organizaciones a su red ATM o Frame Relay.

Otros proveedores utilizan el término en referencia a los servicios provistos sobre sus redes de datos privadas (como es el caso de Tigo, Entel, Coteco). Pero las expectativas creadas por la utilización de Internet y de IP en general como medio de transporte son tan

altas que incluso algunos expertos han redefinido el concepto de VPN como una red que soporta transporte de datos privados sobre infraestructura IP pública. Y la infraestructura IP por excelencia es Internet, la red de datos más pública que existe. De esta forma, el término VPN se está aplicando cada vez más a las redes privadas que transportan datos utilizando Internet.

4.4.1.1.2 **Componentes de una VPN**

Según (Karen, 2012)Los componentes básicos de una VPN aparecen en la figura 4.18 y son:

- Servidor VPN, Firewall, etc.
- Túnel
- Conexión VPN
- Red pública de tránsito
- Cliente VPN

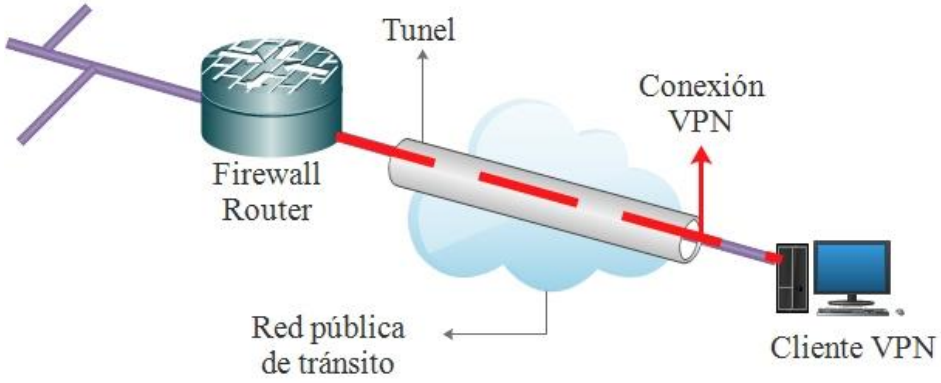


Figura 4-18: Componentes de una VPN
Fuente: Elaboración propia

Para emular un vínculo punto a punto en una VPN, los datos se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta alcanzar su destino. Para emular un vínculo privado, los datos se cifran para asegurar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar si no se dispone de las claves de cifrado. La parte de la conexión en la cual los datos privados son encapsulados es conocida como túnel.

La parte de la conexión en la que se encapsulan y cifran los datos privados se denomina conexión VPN.

4.4.1.1.3 **Utilizar Internet para crear una VPN**

El uso de Internet como una VPN permitió a los usuarios remotos acceder a la red corporativa utilizando a un ISP. Puesto que ahora muchos ISP ofrecen acceso ilimitado a Internet por un precio de $200 en promedio al mes para conexiones de módem, el uso de Internet puede proporcionar muchos beneficios económicos comparados con las tarifas de hacer llamadas de larga distancia. Por ejemplo, si la llamada de larga distancia cuesta $1 por minuto, una hora de acceso por día para un usuario viajero resultaría en un costo de $60 por día o $1200 al mes si se trabajan 20 días al mes. Por lo tanto, un costo de $200 al mes por tener acceso ilimitado a Internet claramente demuestra el ahorro considerable de dinero que se obtiene con el uso de una VPN.

Cuando una VPN es utilizada como un mecanismo para reemplazar redes privadas, también se pueden obtener bastantes beneficios económicos. La figura 4.19 muestra a dos sucursales conectadas con la oficina corporativa. En el inciso a) se muestra una red privada típica mientras que en el inciso b) se muestra una VPN que usa Internet como red pública.

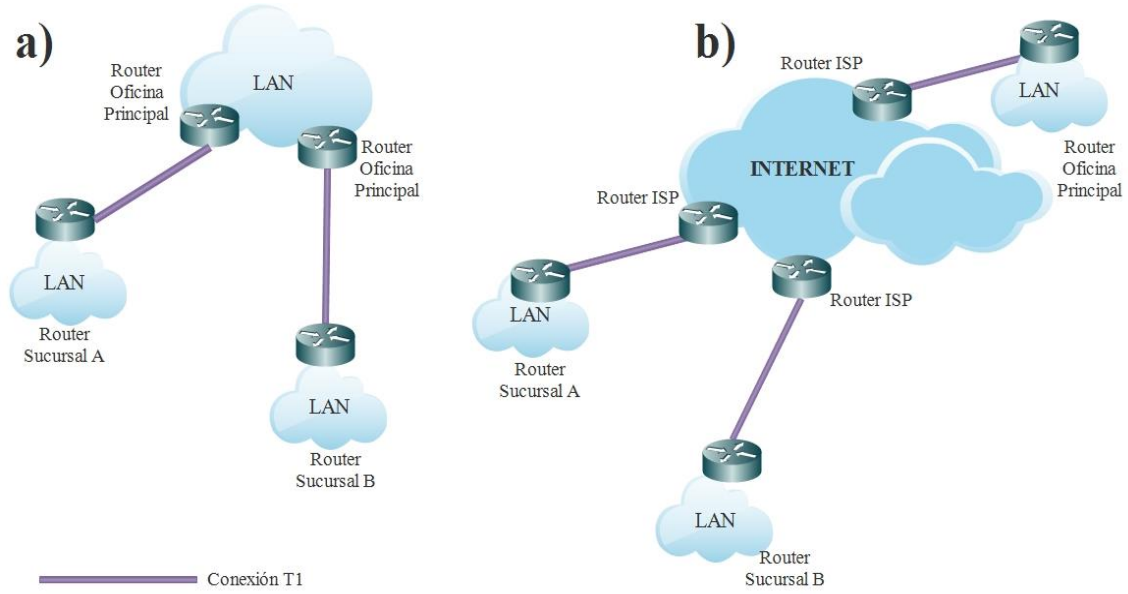


Figura 4-19: El uso de Internet para crear una VPN
Fuente: Elaboración propia

En el inciso b) se muestra que cada LAN de la empresa se conecta a Internet a través de un ISP local usando tres conexiones T1. La mayoría de los ISP tienen presencia en varias ciudades y cobrarán una tarifa de $10000 al mes por una conexión T1. Tanto las sucursales como la oficina principal utilizan una conexión T1 a Internet a través de un ISP con el fin de interconectar sus redes LAN a través de Internet.

Desde una perspectiva económica, se puede comparar el costo de usar Internet con el costo de mantener una red privada con dos conexiones T1 como aparece en el inciso a). Si se supone que cada red LAN se encuentra a 500 millas (804.67 Km.) de la otra, se requerirá de 1000 millas (1609.34 km.) de conexión T1 para interconectar los tres sitios.

Aunque el costo de los circuitos T1 puede variar por distintos factores, un costo de $30 por milla (1.61 km.) proporciona una aproximación razonable. De esta forma, interconectar tres sitios como aparece en el inciso a) con dos conexiones T1 costaría $30000, si existe una distancia de 500 millas entre sitios. Hay que notar que este costo iguala al costo de interconectar tres sitios utilizando Internet como aparece en el inciso b).

Sin embargo, si se asume ahora que cada uno de esos tres sitios se encuentran a una distancia de 3500 millas (5632.70 Km.) entre ellos; a un costo mensual de $30 por milla, el costo de dos líneas T1 para interconectar tres sitios como en el inciso a) se incrementaría en 3500*30, o $105,000. Ahora si se asume que cada sitio se interconecta con los otros usando la VPN del inciso b), el costo de conectar cada sitio seguiría siendo de $10000 al mes, puesto que cada sitio se conecta con el ISP local. Por lo tanto, el costo de usar la VPN del inciso b) permanecería en $30000, mientras que con la red privada del inciso a) el costo sería de $105,000. Está claro que con la VPN se lograría un ahorro de $75000.

4.4.1.2 **Arquitectura de una VPN**

Según (Wikispaces by TES, 2015)Existen básicamente dos tipos de arquitectura para una VPN. Estos son:

- VPN de acceso remoto
- VPN de sitio a sitio

La VPN de sitio a sitio también puede ser llamada VPN LAN a LAN o VPN POP a POP. Las VPN de sitio a sitio se dividen a su vez en VPN extranet y VPN intranet.

Las VPN de acceso remoto se dividen en VPN Dial-up y VPN directas.

4.4.1.2.1 **VPN de acceso remoto**

Esta VPN proporciona acceso remoto a una intranet o extranet corporativa. Una VPN de acceso remoto permite a los usuarios acceder a los recursos de la compañía siempre que lo requieran. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre. La figura 4.20 muestra una VPN de acceso remoto.

Las VPN de acceso remoto ahorran costos a las empresas ya que los usuarios sólo necesitan establecer una conexión con un ISP local, pagándose solamente la llamada local y olvidándose de realizar llamadas de larga distancia. El cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor, router, etc. VPN de la compañía. Una vez que se ha establecido el enlace, el usuario puede acceder a los recursos de la intranet privada de la empresa.

De acuerdo a la tecnología utilizada para establecer la conexión, las VPN de acceso remoto se puede dividir en VPN dial-up y VPN directas.

VPN dial-up. En esta VPN, el usuario realiza una llamada local al ISP utilizando un módem. Aunque se trata de una conexión lenta es todavía muy común. El uso de este tipo de VPN se da más entre los usuarios móviles, ya que no en todos los lugares a donde se viaja se pueden tener disponibles conexiones de alta velocidad.

VPN directa. En esta VPN, se utilizan las tecnologías de conexión a Internet de alta velocidad, tales como DSL y módem de cable las cuales ya ofrecen muchos ISP. Este tipo de VPN se puede encontrar principalmente entre los teletrabajadores. Actualmente se pueden obtener conexiones a Internet desde el hogar utilizando estas tecnologías.

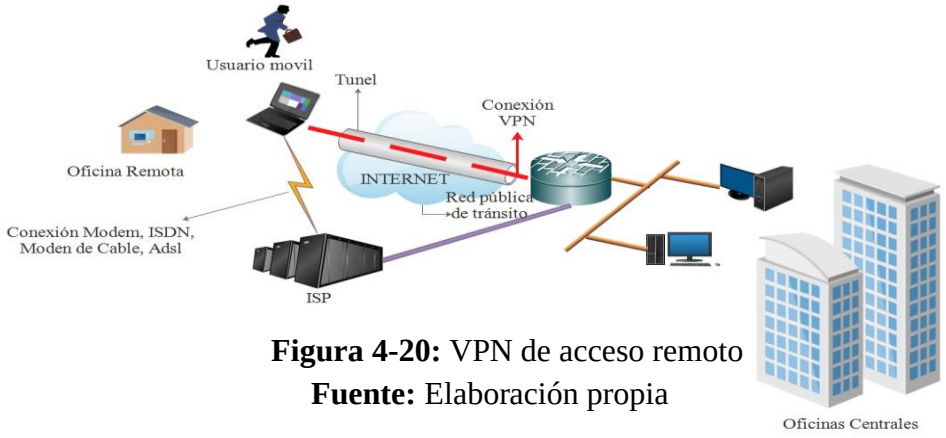


Figura 4-20: VPN de acceso remoto
Fuente: Elaboración propia

4.4.1.2.2 **VPN de sitio a sitio**

Las VPN de sitio a sitio son utilizadas para conectar sitios geográficamente separados de una corporación. Como ya se explicó anteriormente, en las redes tradicionales las distintas oficinas de una corporación son conectadas utilizando tecnologías como T1, E1, ATM o Frame Relay.

Con una VPN, es posible conectar las LAN corporativas utilizando Internet. El envío de información se realiza a través de una conexión VPN. De esta forma, se puede crear una WAN utilizando una VPN. Una empresa puede hacer que sus redes se conecten utilizando un ISP local y establezcan una conexión de sitio a sitio a través de Internet.

Los costos de la comunicación se reducen enormemente porque el cliente sólo paga por el acceso a Internet. Las oficinas remotas se conectan a través de túneles creados sobre Internet. Con el uso de la infraestructura de Internet, una empresa puede desechar la difícil tarea de tener que estar administrando los dispositivos como los que se utilizan en las WAN tradicionales.

En base a los problemas comerciales que resuelven, las VPN de sitio a sitio pueden subdividirse a su vez en VPN intranet y VPN extranet.

VPN intranet. Las VPN intranet se utilizan para la comunicación interna de una compañía, como aparece en la figura 4.21. Enlazan una oficina central con todas sus sucursales. Se disfrutan de las mismas normas que en cualquier red privada. Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN.

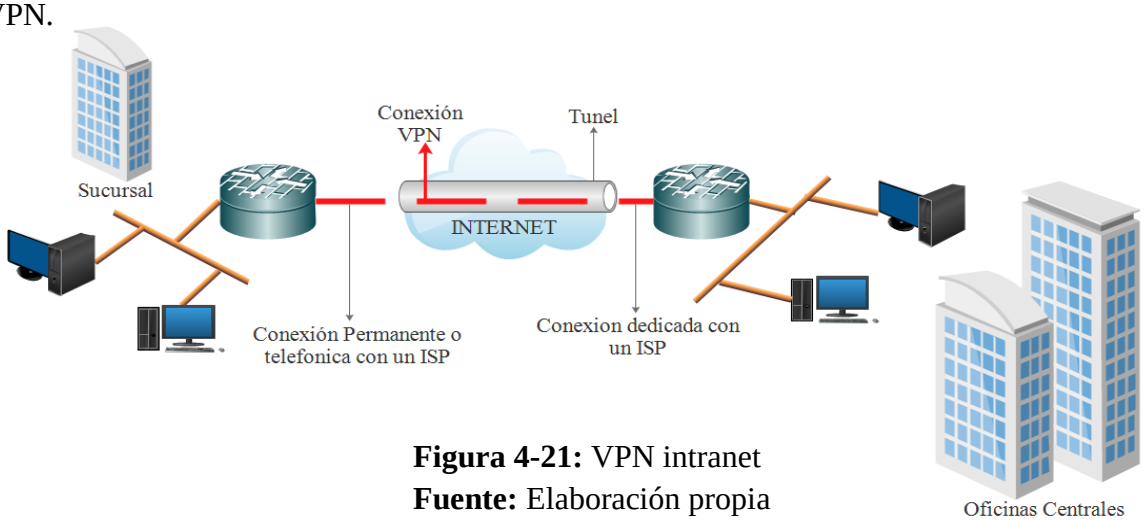


Figura 4-21: VPN intranet
Fuente: Elaboración propia

VPN extranet. Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa, como se muestra en la figura 4.22. Se puede implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones. Las empresas disfrutan de las mismas normas que las de una red privada. Sin embargo, las amenazas a la seguridad en una extranet son mayores que en una intranet, por lo que una VPN extranet debe ser cuidadosamente diseñada con muchas pólizas de control de acceso y acuerdos de seguridad entre los miembros de la extranet.

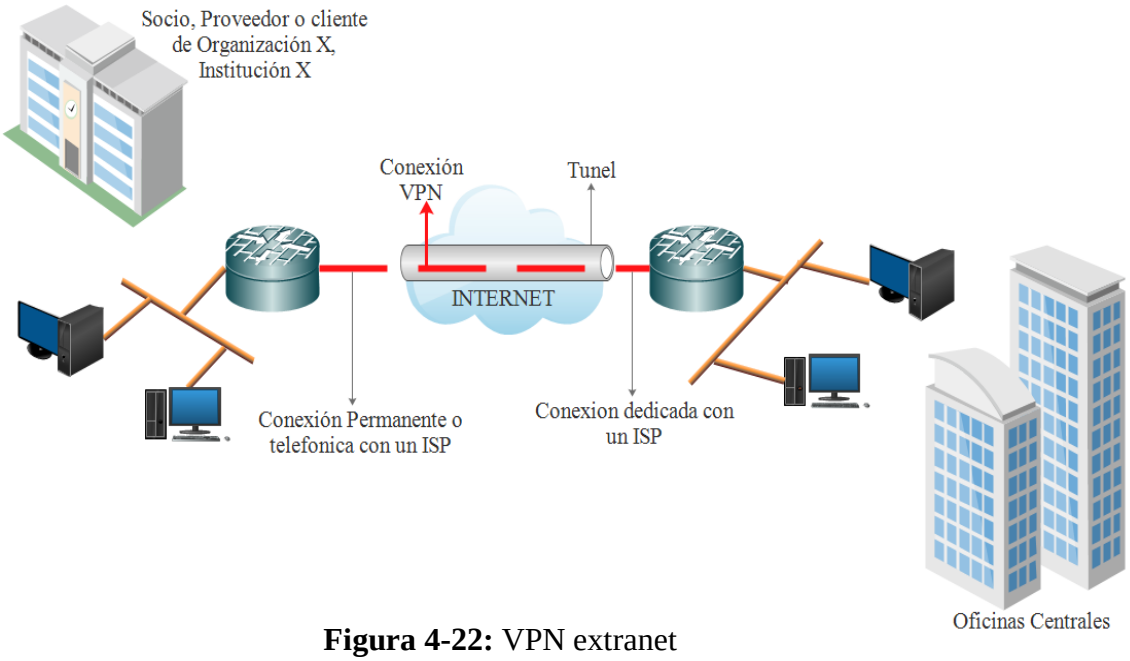


Figura 4-22: VPN extranet
Fuente: Elaboración propia

4.4.1.3 **Tipos de productos VPN**

Según (Wikispaces by TES, 2015) Existen diferentes formas de que una organización puede implementar una VPN. Cada fabricante o proveedor ofrece diferentes tipos de soluciones VPN. Cada corporación tendrá que decidir la que más le convenga. Los tipos diferentes de VPN son:

- VPN de firewall
- VPN de router y de concentrador
- VPN de sistema operativo
- VPN de aplicación

- VPN de proveedor de servicio

4.4.1.3.1 **VPN de firewall**

Un firewall (llamado también cortafuegos o servidor de seguridad) es un sistema de seguridad que implanta normas de control de acceso entre dos o más redes. Se trata de un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Un firewall puede ser un dispositivo software o hardware.

Es muy común que se utilice un firewall para proporcionar servicios VPN. Empresas como Cisco Systems, Nortel Networks, Juniper Network y otros ofrecen en muchos de sus dispositivos firewall soporte para VPN. Una VPN basada en firewall tiene la ventaja de que simplifica la arquitectura de la red al establecer un único punto de control de seguridad. Además, los ingenieros de redes sólo tienen que hacerse expertos en una tecnología, en lugar de tener que aprender a administrar un firewall y la VPN de forma separada.

Entre los inconvenientes se puede mencionar que tener la VPN en un firewall convierte al dispositivo en algo más complejo, por lo que se debe ser más cuidadoso en su configuración o de lo contrario cualquier intruso podría tener acceso no autorizado a la red. Otra desventaja ocurre debido a que tener firewall y VPN juntos, se ejerce presión al rendimiento del firewall. Esto ocurre principalmente si se tienen conectados cientos o incluso miles de usuarios.

4.4.1.3.2 **VPN de router y de concentrador**

Empresas como Cisco, Nortel y 3Com entre otros también ofrecen servicios VPN integrados dentro de un router o un dispositivo llamado concentrador VPN. Tanto el router como el concentrador VPN están especialmente diseñado para las conexiones VPN sitio a sitio y acceso remoto. Cuenta con las tecnologías VPN más importantes y los métodos de autenticación y cifrado para proteger los datos transmitidos.

Este dispositivo está especialmente diseñado para las VPN, por lo que se trata de la solución VPN más rápida. Resulta ser más fácil agregarles tarjetas con el fin de incrementar el rendimiento. Dependiendo de la implementación, estas VPN pueden configurarse para utilizar certificados, servicios de autenticación externos o claves de seguridad.

4.4.1.3.3 **VPN de sistema operativo**

Los sistemas operativos como Windows de Microsoft, Netware de Novell o Linux en sus diferentes distribuciones (Red Hat, Debian,…) ofrecen servicios de VPN ya integrados. La principal ventaja de esta solución es que resulta ser económica ya que en un mismo sistema operativo se pueden contar con una gran variedad de servicios (servidor Web, de nombres de dominio, acceso remoto, VPN) y además mejora los métodos de autenticación y la seguridad del sistema operativo. Tiene la desventaja de que es vulnerable a los problemas de seguridad del propio sistema operativo. Estas VPN se utilizan más para el acceso remoto.

4.4.1.3.4 **VPN de aplicación**

Este tipo de VPN es poco común. Una VPN de aplicación es un programa que añade posibilidades VPN a un sistema operativo. Sin embargo, este programa no queda integrado con el sistema operativo. La ventaja de este tipo de VPN es que la aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo. Un ejemplo de esta VPN es el programa ViPNet de Infotecs.

La desventaja es que estas VPN no soportan una gran cantidad de usuarios y son mucho más lentas que una VPN basada en hardware. Si se utilizan en Internet, son vulnerables a las fallas de seguridad del sistema operativo que contiene a la aplicación.

4.4.1.3.5 **VPN de proveedor de servicios**

Este tipo de VPN es proporcionada por un proveedor de servicios. Al principio las VPN de proveedor de servicios se basaban en tecnologías tales como X.25 y Frame Relay, posteriormente ATM y SMDS y finalmente se ofrecen redes basadas en IP. El proveedor de servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a sus clientes.

El cliente se conecta a la red del proveedor de servicios a través de un dispositivo de equipo terminal del cliente (CPE) como puede ser un router. El CPE se conecta a través

de medios de transmisión al equipo del proveedor de servicios, que puede ser X.25, Frame Relay, un conmutador ATM o un router IP. La línea virtual que se le proporciona al cliente mediante el proveedor de servicios se le llama circuito virtual (VC).

El proveedor de servicios puede cargar o una tarifa plana para el servicio VPN, que habitualmente depende del ancho de banda disponible para el cliente, o una tarifa basada en el uso, que puede depender del volumen de datos intercambiados o de la duración del intercambio de datos.

Acuerdos a nivel del servicio (SLA, Service Level Agreements). Los SLA son contratos negociados entre proveedores VPN y sus abonados en los que se plantean los criterios de servicio que el abonado espera tengan los servicios específicos que reciba. La SLA es el único documento que está a disposición del abonado para asegurar que el proveedor VPN entrega el servicio o servicios con el nivel y calidad acordados. Si se ha de implementar una VPN basada en proveedor de servicios, este documento es de vital importancia para asegurar un buen servicio.

4.4.1.4 Topologías de VPN

Según (Instituto de Ciencia Básicas e Ingeniería, 2007) La topología VPN que necesita una organización debe decidirse en función de los problemas que va a resolver. Una misma topología puede ofrecer distintas soluciones en diferentes compañías u organizaciones. En una VPN podemos encontrar las siguientes topologías:

Para las VPN de sitio a sitio:

- Topología radial
- Topología de malla completa o parcial
- Topología híbrida

Para las VPN de acceso remoto:

- Topología de acceso remoto

En las VPN basadas en ATM y Frame Relay, los enlaces que conectan las oficinas centrales con sus sucursales son circuitos virtuales (VC), mientras que en las VPN

basadas en IP como Internet, estos enlaces son los túneles que se establecen a través de Internet.

4.4.1.4.1 **Topología radial**

En una VPN de sitio a sitio, ésta es la topología más común. Aquí, las sucursales remotas se conectan a un sitio central, como se puede ver en la figura 4.23. Las sucursales podrían intercambiar datos entre ellas, sin embargo, este tipo de datos resulta ser muy insignificante. La mayor parte del intercambio de datos se da con las oficinas centrales de la compañía. Los datos intercambiados entre las sucursales siempre viajan a través del sitio central.

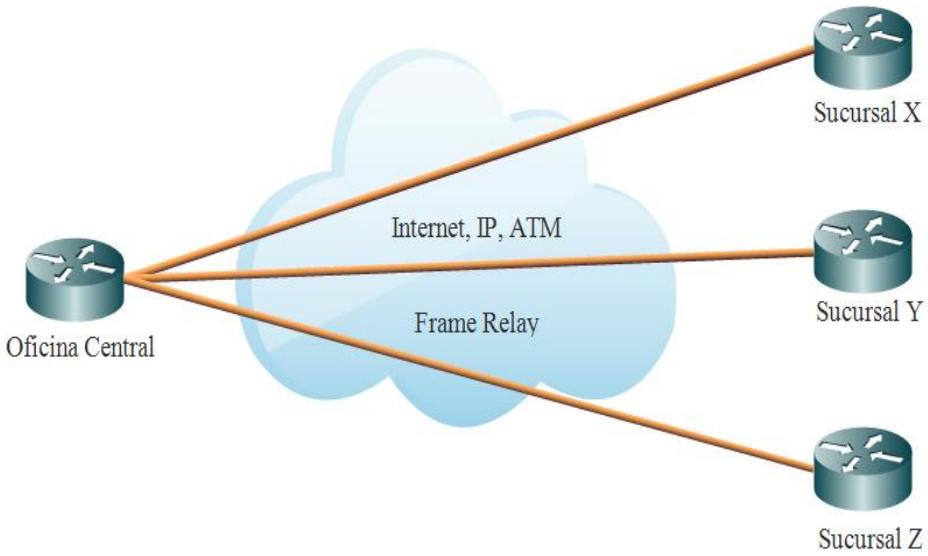


Figura 4-23: Topología radial
Fuente: Elaboración propia

4.4.1.4.2 **Topología de malla completa o parcial**

Esta topología es implementada en corporaciones que no tienen una estructura demasiado jerárquica. Aquí, las diversas LAN de la compañía pueden realizar un intercambio constante de datos entre ellas.

Dependiendo de sus necesidades, una empresa puede utilizar una topología de malla completa si todas las LAN se comunican entre sí o una topología de malla parcial, si

sólo algunas LAN mantienen intercambio de datos. En la gran mayoría de los casos se utiliza sólo malla parcial. La figura 4.24 muestra una topología de malla:

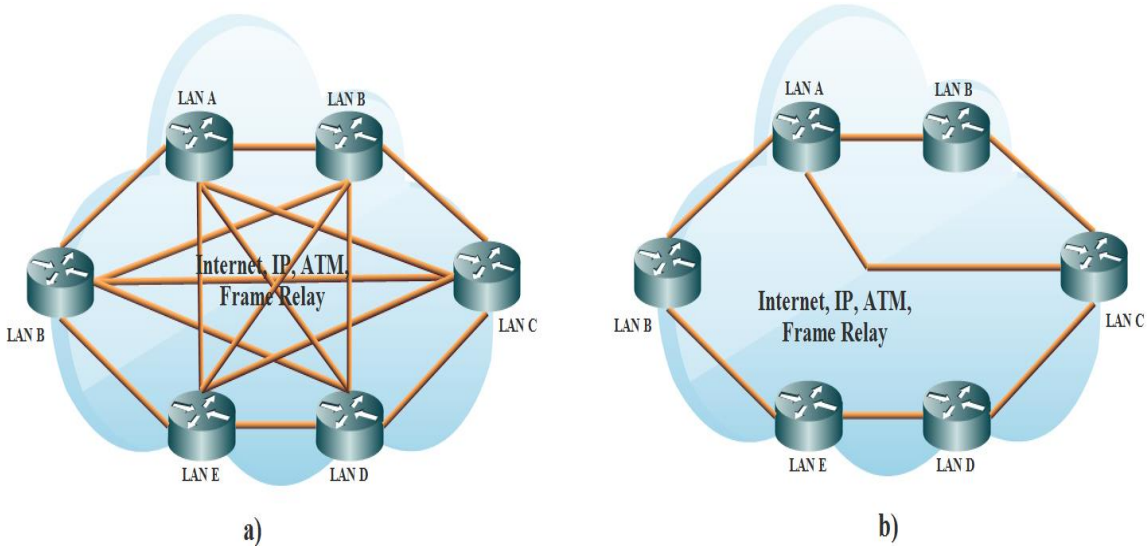


Figura 4-24: Topología de malla: a) completa b) parcial
Fuente: Elaboración propia

4.4.1.4.3 **Topología híbrida**

Las redes VPN grandes combinan la topología radial con la topología de malla parcial. Como ejemplo, una empresa multinacional podría tener acceso a redes implementadas en cada país con una topología radial, mientras que la red principal internacional estaría implementada con una tecnología de malla parcial.

4.4.1.4.4 **Topología de acceso remoto**

Esta topología consiste en un enlace punto a punto entre el usuario remoto la oficina central utilizando tramas tunneling PPP intercambiadas entre el usuario remoto y el servidor VPN o Firewall, etc. El usuario y el servidor establecen conectividad usando un protocolo de capa 3, siendo el más común IP, sobre el enlace PPP entunelado e intercambian paquetes de datos sobre él.

4.4.1.5 **Requerimientos de una VPN**

Según (Oviedo Miguel, 2012) Una VPN debe de contar con ciertos requerimientos que permitan que valga la pena el uso de esta tecnología. Sin estos requerimientos, las VPN no podrán ofrecer la calidad necesaria que requieren las

organizaciones para un desempeño óptimo. Una solución VPN debe ofrecer los siguientes requerimientos:

- Autenticación de usuarios
- Control de acceso
- Administración de direcciones
- Cifrado de datos
- Administración de claves
- Soporte a protocolos múltiples
- Ancho de banda

4.4.1.5.1 **Autenticación de usuarios**

La autenticación es uno de los requerimientos más importantes en una VPN. Cada entidad participante en una VPN debe de identificarse a sí misma ante otros y viceversa. La autenticación es el proceso que permite a los diversos integrantes de la VPN verificar las identidades de todos.

Existen muchos mecanismos de autenticación, pero el más popular de todos ellos es la Infraestructura de Claves Públicas (PKI, Public Key Infraestructure), el cual es un sistema basado en la autenticación por medio de certificados. Cada integrante de una VPN se autentica intercambiando los certificados de cada uno, los cuales están garantizados por una autoridad de certificación (CA, Certification Authority) en la que todos confían.

El proceso de autenticación también involucra el intercambio de información secreta, como una clave o un desafío ante un Servidor de Acceso a Red (NAS, Network Access Server), el cual consultará a un servidor, router, etc. Un servidor RADIUS administra la autenticación en una red que lo requiere.

4.4.1.5.2 **Control de acceso**

El control de acceso en una red está definido como el conjunto de pólizas y técnicas que rigen el acceso a los recursos privados de una red por parte de usuarios autorizados. Una vez que un usuario ha sido autenticado, se debe definir a qué recursos de la red puede tener acceso dicho usuario. Los diferentes tipos de VPN, ya sea de firewalls, sistemas operativos, etc; son responsables de gestionar el estado de la conexión del usuario.

La VPN debe administrar el inicio de una sesión, permitir el acceso a ciertos recursos, continuar una sesión, impedir el acceso de recursos y terminar una sesión.

El conjunto de reglas y acciones que definen el control de acceso se denomina póliza de control de acceso. Un servidor RADIUS puede administrar el control de acceso basándose en la póliza, así como los firewalls, routers, etc. Un ejemplo de una regla de control de acceso sería que el servidor o firewall permitiera el acceso sólo los usuarios de acceso remoto que no han rebasado un determinado uso de horas de la red.

El principal propósito de una VPN es permitir acceso seguro y selectivo a los recursos de una red. Con un buen sistema de cifrado y autenticación, pero sin control de acceso, la VPN sólo protege la integridad del tráfico transmitido y evita que usuarios no autorizados ingresen a la red, pero los recursos de ésta no quedan protegidos. Es por eso que el control de acceso es importante.

4.4.1.5.3 **Administración de direcciones**

Un servidor VPN o firewall, router, etc. Debe de asignar o establecer una dirección IP al cliente VPN y asegurarse de que dicha dirección permanezca privada. Está claro que IP no es un protocolo seguro y se puede ver esto en la inseguridad de Internet. Las direcciones deben ser protegidas con fuertes mecanismos de seguridad, deben usarse técnicas que permitan la ocultación de la dirección privada dentro de una red pública.

La tecnología más utilizada para ocultar la información es el tunneling. El tunneling es una técnica que encapsula los datos (incluyendo la dirección destino privada) dentro de otro conjunto de datos. Así, el contenido de los paquetes encapsulados se vuelve invisible para una red pública insegura como Internet. Existen muchas tecnologías de tunneling, cada una de ellas con sus ventajas y desventajas. Otra tecnología alterna al tunneling es MPLS, donde se hace uso de un sistema de etiquetas para transmitir información. MPLS es una tecnología que realizará grandes cambios a los métodos tradicionales de enrutamiento y de la forma de crear túneles.

4.4.1.5.4 **Cifrado de datos**

Cifrar o encriptar los datos es una tarea esencial de una VPN. Aunque se puedan encapsular los datos dentro de un túnel, estos todavía pueden ser leídos si no se implementan fuertes mecanismos de cifrado de la información. El cifrado es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. El texto sin cifrar se le

denomina texto nativo, mientras que el texto cifrado se le denomina texto cifrado. Antes de enviar la información, el servidor VPN o router, firewall, etc. cifra la información convirtiéndolo en texto cifrado. El receptor de la información descifra la información y la convierte en texto nativo.

Al principio los algoritmos de encriptación se mantenían en secreto. Sin embargo, cuando el algoritmo era roto, toda la información protegida con dicho algoritmo se volvía vulnerable. Por consiguiente, actualmente los algoritmos se hacen públicos. Existen muchos tipos de algoritmos de cifrado muy fuertes utilizados en las VPN entre los que podemos encontrar 3DES, Diffie-Hellman, MD5, RSA y SHA-1.

Puesto que el algoritmo de cifrado es conocido por todos, es necesario implementar técnicas para poder mantener los datos seguros. Esto se logra mediante el uso de claves. Una clave es un código secreto que el algoritmo de encriptación utiliza para crear una única versión de texto cifrado. Mientras la longitud en bits de esta clave sea más grande, más difícil será descifrar una información.

Las VPN requieren del uso de claves con una cierta longitud, de tal manera que resulta prácticamente imposible descifrar los datos (teóricamente tardaría millones de años, a no ser que se posean cientos de procesadores trabajando al mismo tiempo para encontrar la clave y aunque ésta se encontrara, los algoritmos están diseñados de forma que no se garantizaría totalmente el éxito). Aunque, de hecho, el uso de claves muy largas no es recomendable porque se afecta mucho el rendimiento de un procesador. Para eso se utilizan métodos como el uso de claves simétricas y asimétricas.

Con una clave simétrica, se usa la misma clave para cifrar y descifrar la información que viaja por un túnel. Tanto el emisor como el receptor de los datos poseen la misma clave privada. Con una clave asimétrica, la información se cifra con una clave y se descifra con otra diferente. Una de las claves sólo es conocida por el usuario, la cual es conocida como clave privada. La otra clave es conocida por todos y se le llama clave pública.

Las claves públicas permiten el uso de firmas digitales para autenticar información. Una clave pública es distribuida libremente a cualquiera que requiera enviar información cifrada o firmada. La clave privada debe ser bien resguardada por el usuario y no darla a conocer nunca.

4.4.1.5.5 **Administración de claves**

En una VPN, es importante la administración de claves. Para asegurar la integridad de una clave pública, ésta es publicada junto con un certificado. Un certificado es una estructura de datos firmada digitalmente por una organización conocida como autoridad de certificación (CA) en la cual todos confían. Una CA firma su certificado con su clave privada. Un usuario que utiliza la clave pública de la CA podrá comprobar que el certificado le pertenece a dicha CA y, por lo tanto, la clave pública es válida y confiable.

En una VPN pequeña no es muy necesario establecer una infraestructura de administración de claves. Sin embargo, las grandes compañías obtendrán muchos beneficios si hacen crean una Infraestructura de Claves Públicas (PKI) para poder crear y distribuir certificados. Una corporación puede crear su propia CA o confiar en una CA de terceros. Una PKI es muy útil en aquellas organizaciones que requieren de mucha seguridad y acceso limitado a sus usuarios.

4.4.1.5.6 **Soporte a protocolos múltiples**

Para que una solución VPN sea viable, es necesario también que ésta pueda ofrecer soporte a múltiples protocolos. Esto incluye el soporte a protocolos de red que no sean IP como pueden ser AppleTalk, IPX y NetBEUI. PPTP soporta varios protocolos de red. IPSec sólo puede ser utilizado en redes basadas en IP, pero siempre es posible encapsular los protocolos no compatibles dentro de un paquete IP, de modo que puedan ser transportados. En cuanto a L2TP, este protocolo VPN no sólo puede ser implementado en redes IP, sino también en ATM y Frame Relay.

4.4.1.5.7 **Ancho de banda**

El ancho de banda es también un requerimiento importante en una VPN. En el mundo de las redes existe un concepto que define la forma de administrar el ancho de banda con el fin de que el tráfico de una red fluya de forma eficiente. Dicho concepto es la Calidad de Servicio (QoS, Quality of Service). La QoS es una característica muy importante de una VPN. Una solución VPN no estará completa si no proporciona formas para el control y administración del ancho de banda.

La calidad del servicio también se refiere al número de conexiones simultáneas (la cantidad de túneles que pueden ser establecidos entre un sitio remoto y el sitio central) que puede soportar una VPN y la forma como ésta afecta al rendimiento de la VPN.

Es preciso también asegurarse que una VPN puede cifrar y descifrar los paquetes transmitidos a una velocidad adecuada, ya que algunos algoritmos de cifrado son lentos y si no se tiene un buen procesador el rendimiento se verá afectado. Es importante mencionar que el valor nominal de velocidad de los dispositivos de redes (por ejemplo 100 Mbps) nunca se cumple en la realidad y que eso habrá que tomarse en cuenta a la hora de implementar una VPN.

La calidad de las conexiones a Internet también es importante. Las técnicas de encriptación incrementan el deterioro del rendimiento de la comunicación por las sobrecargas. Las pérdidas de paquetes y la latencia en conexiones a Internet de baja calidad afectan más al rendimiento, que la carga añadida por la encriptación.

4.4.2 Tunneling

4.4.2.1 Definición de tunneling

Según (Cisco System, 2001) El tunneling es un método utilizado para encapsular paquetes (conocidos como datos de usuario) dentro de otros paquetes los cuales son enviados utilizando la tecnología de la red por la que viaja. Esto ofrece grandes ventajas, ya que permite el transporte de protocolos con diferente esquema de direccionamiento y que por lo tanto no son compatibles con una red que utiliza otros protocolos de direccionamiento dentro de paquetes que sí reconoce la red.

4.4.2.1.1 Funcionamiento del tunneling

Por ejemplo, un paquete IPX o AppleTalk no puede ser transportado en una red basada en IP, como Internet. Sin embargo, si este paquete es encapsulado dentro de un paquete IP, entonces podrá ser transportado como cualquier otro paquete IP. Lo que hace este proceso es simplemente agregarles un encabezado adicional.

Después de agregar el encabezado, se envía el paquete encapsulado a través de una ruta lógica denominada túnel. El túnel es la ruta de información lógica a través de la cual viajan los paquetes encapsulados. Para los interlocutores de origen y de destino originales, el túnel suele ser transparente y aparece simplemente como otra conexión punto a punto en la ruta de acceso a la red. A estos puntos que están en cada extremo del túnel se les denomina interfaces de túnel. Los interlocutores desconocen los routers, switches, servidores proxy u otras puertas de enlace de seguridad que pueda haber entre los extremos del túnel.

Cuando el paquete llega a su destino, éste es desencapsulado para que pueda ser utilizado. En resumen, el tunneling es un proceso que consta de los siguientes pasos:

- Encapsulación
- Transmisión
- Desencapsulación

El uso de un túnel abarca todo el proceso de encapsulación, enrutamiento y desencapsulación. El túnel envuelve, o encapsula, el paquete original dentro de un paquete nuevo. Este paquete nuevo puede contener nueva información de direccionamiento y enrutamiento, lo que le permite viajar por la red. Si el túnel se combina con la confidencialidad de datos, los datos del paquete original (así como el origen y el destino originales) no se muestran a quienes observen el tráfico en la red. Cuando los paquetes encapsulados llegan a su destino, se quita la encapsulación y se utiliza el encabezado original del paquete para enrutar éste a su destino final.

4.4.2.1.2 **Protocolo pasajero, encapsulador y portador**

El proceso de tunneling involucra tres protocolos diferentes (Ver Figura 4.25)

- **Protocolo pasajero:** Representa el protocolo que debe encapsularse. Como ejemplos de protocolos pasajeros tenemos PPP y SLIP.
- **Protocolo de encapsulamiento:** Es el que será empleado para la creación, mantenimiento y destrucción del túnel. Ejemplos de protocolo de encapsulamiento son L2F, L2TP, PPTP.
- **Protocolo portador:** Es el encargado de realizar el transporte del protocolo de encapsulamiento. El principal ejemplo de protocolo portador es IP puesto que este tiene amplias capacidades de direccionamiento y es en el que está basado Internet.

Figura 4-25: Estructura general de un paquete de tunneling
Fuente: Elaboración propia

4.4.2.2 **Tunneling y VPN**

Cuando el uso de túneles se combina con el cifrado de los datos, puede utilizarse para proporcionar servicios de VPN. Las VPN utilizan el tunneling para poder ofrecer mecanismos seguros de transporte de datos. Dentro del contexto de las VPN, el tunneling involucra tres tareas principales:

- Encapsulación
- Protección de direcciones privadas
- Integridad de los datos y confidencialidad de éstos

Para que el proceso del tunneling pueda ser llevado a cabo, existen diversos protocolos llamados protocolos de túnel los cuales se encargan de encapsular y desencapsular los datos que viajan dentro de una red privada virtual. Los protocolos de túnel usados por las VPN como PPTP y L2TP son usados para encapsular tramas de la capa de enlace de datos (PPP). Protocolos de túnel como IP sobre IP e IPSec en modo túnel son utilizados para encapsular paquetes de la capa de red.

Es posible colocar un paquete que utiliza una dirección IP privada dentro de un paquete que usa una dirección IP global única para poder extender una red privada sobre una red pública como Internet. Puesto que los contenidos del paquete entunelado sólo pueden ser interpretados por las interfaces de túnel, las direcciones IP privadas pueden ser ocultadas completamente de las redes IP públicas.

Los mecanismos de integridad y confidencialidad garantizan que ningún usuario no autorizado pueda alterar los paquetes entunelados durante la transmisión sin que el ataque pueda ser detectado y que los contenidos del paquete permanecen protegidos de acceso no autorizado. Además, el tunneling opcionalmente puede proteger la integridad de la cabecera del paquete IP externo, mediante técnicas de autenticación. Por ejemplo, si se utiliza IPSec los protocolos AH y ESP pueden proporcionar autenticación de los paquetes transmitidos.

Tres protocolos de túnel son los más usados para la creación de una VPN:

- Protocolo de Túnel punto a punto (PPTP)
- Protocolo de Túnel de Capa 2 (L2TP)
- Protocolo de Seguridad IP

Los protocolos PPTP y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN de sitio a sitio.

La figura 4.26 resume cómo se lleva a cabo el tunneling en una VPN.

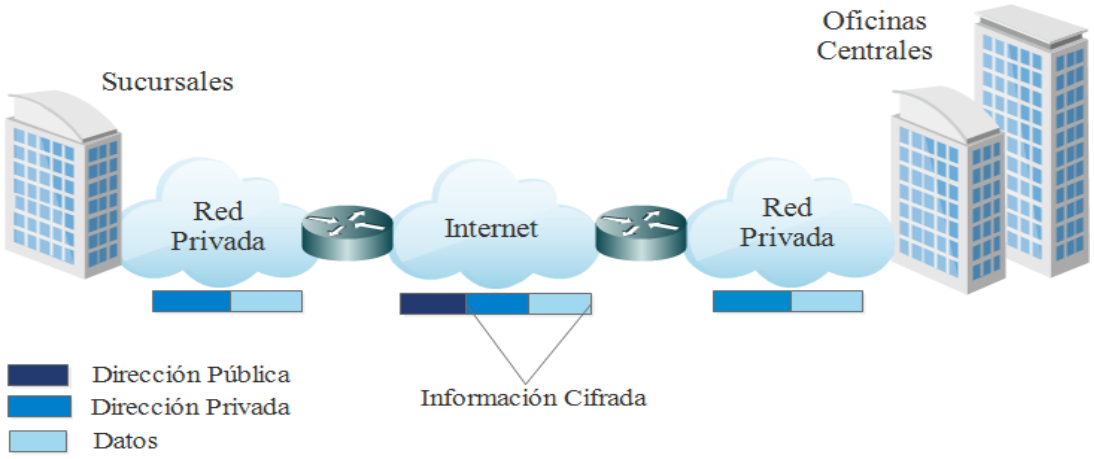


Figura 4-26: Tunneling en una VPN
Fuente: Elaboración propia

4.4.2.3 **Tipos de túneles**

Los túneles se clasifican de acuerdo a cómo se establece la conexión entre dos hosts. En base a esto, existen dos tipos de túneles. Éstos son:

- Túnel voluntario
- Túnel obligatorio

4.4.2.3.1 **Túnel voluntario**

Un equipo usuario o cliente puede emitir una petición VPN para configurar y crear un túnel voluntario. En este caso, el equipo del usuario es un extremo del túnel que funciona como cliente de túnel. El túnel voluntario se produce cuando una estación de trabajo o un router utilizan software de cliente de túnel para crear una conexión VPN con el servidor de túnel de destino. Para ello, debe instalar el protocolo de túnel correspondiente en el equipo cliente. Un túnel voluntario puede ser creado de dos maneras a través de una conexión dial-up o a través de una LAN. La figura 4.27 muestra un túnel voluntario.

A través de una conexión dial-up. En este caso, el usuario primero hace una llamada a su ISP para conectarse a Internet y entonces posteriormente podrá ser creado el

túnel. Esta suele ser la situación más común. La conexión a Internet es un paso preliminar para crear el túnel, pero no forma parte del proceso de creación del túnel.

A través de una LAN. En este caso, el cliente ya posee una conexión a la red, por lo que el túnel puede ser creado con cualquier servidor túnel deseado. Este es el caso de un usuario de una LAN que crea un túnel para acceder a otra LAN.

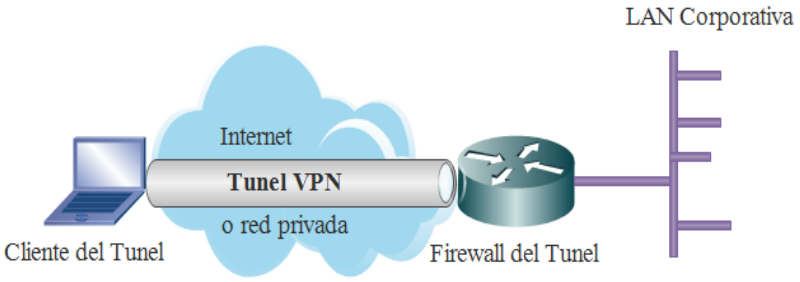


Figura 4-27: Túnel voluntario
Fuente: Elaboración propia

4.4.2.3.2 Túnel obligatorio

El túnel obligatorio es la creación de un túnel seguro por parte de otro equipo o dispositivo de red en nombre del equipo cliente. Los túneles obligatorios se configuran y crean automáticamente para los usuarios sin que éstos intervengan ni tengan conocimiento de los mismos. Con un túnel obligatorio, el equipo del usuario no es un extremo del túnel. Lo es otro dispositivo entre el equipo del usuario y el servidor de túnel que actúa como cliente de túnel.

Algunos proveedores que venden servidores de acceso telefónico facilitan la creación de un túnel en nombre de un cliente de acceso telefónico. El dispositivo que proporciona el túnel para el equipo cliente se conoce como procesador cliente (FEP) o PAC en PPTP, concentrador de acceso (LAC) de L2TP en L2TP o puerta de enlace (gateway) de Seguridad IP en IPSec. Para realizar su función, el dispositivo que proporciona el túnel debe tener instalado el protocolo de túnel adecuado y debe ser capaz de establecer el túnel cuando el equipo cliente intenta establecer una conexión.

Esta configuración se conoce como túnel obligatorio debido a que el cliente está obligado a utilizar el túnel creado por el dispositivo que proporciona el túnel. Una vez que se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel. En los túneles obligatorios, la computadora cliente realiza una conexión única PPP y, cuando un cliente se conecta en el NAS, se crea un túnel y todo

el tráfico se enruta automáticamente a través de éste. Se puede configurar en el dispositivo que proporciona el túnel para hacer un túnel a todos los clientes hacia un servidor específico del túnel. De manera alterna, el dispositivo que proporciona el túnel podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el dispositivo que proporciona el túnel y el servidor del túnel puede estar compartido entre varios clientes. Cuando un segundo cliente se conecta al dispositivo que proporciona el túnel para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el dispositivo que proporciona el túnel y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel.

Una compañía puede contratar a un ISP para que implemente un conjunto de dispositivos que proporcionen túneles por todos los territorios donde existan LAN de la compañía. Estos dispositivos pueden establecer túneles a través de Internet hasta un servidor VPN conectado a la red privada de la organización, consolidando así las llamadas de zonas geográficamente dispersas en una sola conexión a Internet en la red de la organización.

Existen dos formas de crear túneles obligatorios. En la primera forma, el túnel se crea antes de autenticar al cliente de acceso. Una vez creado el túnel, el cliente de acceso se autentica en el servidor de túnel. En la segunda forma, el túnel se crea después de que el dispositivo que proporciona el túnel autentica al cliente de acceso. La figura 4.28 muestra cómo se compone un túnel obligatorio.

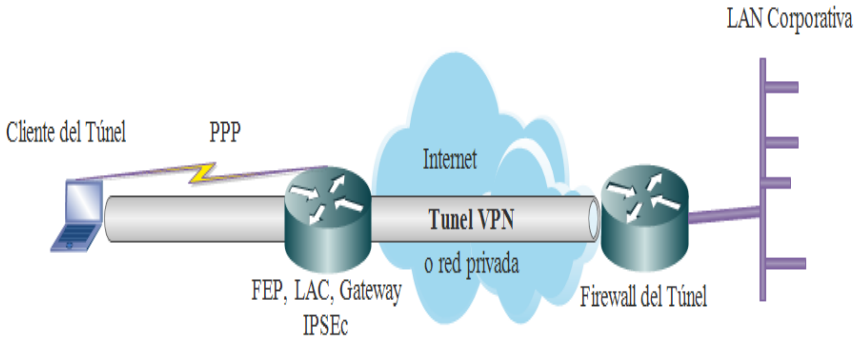


Figura 4-28: Túnel obligatorio
Fuente: Elaboración propia

4.4.3 Seguridad en una VPN

4.4.3.1 Necesidad de seguridad en una VPN

Cuando se diseñaron los primeros protocolos para redes, la seguridad no era un punto importante puesto que las redes sólo eran utilizadas por universidades e investigadores. Nadie pensaba en que alguien pudiera interceptar mensajes. Sin embargo, conforme las redes pasaron a tener un propósito comercial cuando las empresas las adoptaron y con la llegada de Internet, la seguridad pasó a ser una cuestión de vital importancia al momento de implementar redes.

Con la llegada de Internet, toda computadora conectada es susceptible de ser atacada por personas que no deben ingresar a ellas. Los ataques a redes provocan muchas pérdidas económicas a las empresas. Según una encuesta del Computer Security Institute (CSI), el 70% de las organizaciones encuestadas declararon que sus redes habían sido atacadas y el 60% afirmaba que los incidentes procedían de las propias empresas. Por lo tanto, es necesario tomar las medidas necesarias para proteger las redes.

La seguridad cobra especial importancia al momento de implementar una VPN. Puesto que la información privada de una organización atraviesa una red pública, es necesario proveer a la VPN de mecanismos que aseguren la confidencialidad y la integridad de los datos transmitidos y también para evitar el acceso a la red privada.

La seguridad de una VPN debe ir más allá que simplemente controlar el acceso seguro a los recursos de una red. También debe proveer mecanismos para administrar la implementación de pólizas de seguridad que garanticen el desarrollo exitoso de una VPN. La mejor opción es establecer también, antes de que se establezca la conexión cifrada con una oficina o LAN remota, unos niveles de seguridad que deben cumplirse. La comprobación de los niveles de seguridad que debe cumplir el equipo remoto que desea conectarse a la red corporativa debe ser lo más amplia posible.

Sin duda, es necesario establecer un sistema de chequeo del status de seguridad de los equipos remotos conectados mediante VPN a la red corporativa. Y el chequeo debe ser percibido por el usuario remoto como una ayuda a la seguridad general, no como una imposición corporativa y, además, debe hacerse con suficiente amplitud como para abarcar

productos y sistemas de seguridad no corporativos, sino elegidos por el teletrabajador en su ámbito doméstico.

La autenticación de usuarios y la encriptación de datos son características de seguridad muy fuertes. Y en una VPN la tecnología que podrá ofrecer mejor seguridad será IPSec.

4.4.3.2 **Ataques a la seguridad de las redes**

4.4.3.2.1 **Clasificación de las amenazas a redes**

Según (Álvaro Gómez Vieites, 2006) Existen cuatro posibles amenazas a la seguridad de las redes las cuales son descritas a continuación.

Amenazas no estructuradas. Esta clase de amenazas suelen ser originadas por personas inexpertas que utilizan herramientas de piratería en Internet. Aunque algunos actúan de forma malintencionada, la gran mayoría de ellos lo hace por puro reto intelectual. Se les conoce comúnmente como script kiddies.

A pesar de que no se trata de profesionales de las redes ni grandes programadores, son una amenaza muy seria para la seguridad. Pueden ser capaces de introducir un virus o caballo de Troya a una red sin saber exactamente lo que hacen y provocar graves pérdidas económicas.

Amenazas estructuradas. Estas amenazas son causadas por personas que sí tienen conocimientos de redes. Saben cómo están constituidas y conocen sus puntos débiles. Como conocen mucho de programación pueden crear programas que penetren en los sistemas. Son conocidos como hackers y si tienen malas intenciones se les llama crackers. Estas personas pueden ser contratadas por el crimen organizado para cometer robos y fraudes, por una empresa para dañar a la competencia o por agencias de inteligencia con el fin de desestabilizar un gobierno enemigo.

Amenazas externas. Son las amenazas causadas por personas ajenas a la red de una empresa. Son personas no autorizadas a ingresar a estos sistemas, pero pueden entrar a través de Internet o por medio de un RAS.

Amenazas internas. Son amenazas causadas por personas que sí tienen acceso autorizado a la red. Puede ocurrir que algún empleado despedido o descontento con la compañía introduzca un virus a la red como venganza. Este tipo de amenazas son las más frecuentes que existen.

4.4.3.2.2 Clasificación de los ataques a redes

Husmeadores (sniffers) de red. Este ataque tiene lugar cuando el usuario no autorizado utiliza un programa llamado husmeador o sniffer el cual puede leer todos los paquetes que circulan por una red con lo que se puede tener acceso a información privada. Si los paquetes no están cifrados, el sniffer proporciona una vista completa de los datos contenidos en el paquete. Incluso los paquetes encapsulados (enviados por un túnel) se pueden abrir y leer si no están cifrados.

Integridad de datos. Una vez que un atacante ha leído los datos entonces podrá tener la capacidad de modificarlos. Este ataque tiene lugar cuando alguien modifica o corrompe los datos que circulan por una red. Un atacante puede modificar los datos de un paquete sin que el remitente ni el receptor lo adviertan. Incluso cuando no se esté enviando información importante, nadie desea que la información enviada sea modificada en su camino.

Ataques de contraseña (diccionario). Un problema típico de seguridad tiene que ver con el control de acceso basado en contraseñas. El problema es que un sistema no puede saber quién está frente al teclado escribiendo la contraseña. Una forma de obtener una contraseña es si los nombres de usuario y contraseña no son cifrados al enviarse por una red, cualquier atacante podría apoderarse de ella y obtener acceso a una red haciéndose pasar por un usuario legítimo. Otra forma que se utiliza para obtener una contraseña es utilizar ciertas técnicas de criptoanálisis llamadas ataques de diccionario o fuerza bruta.

Ataque de denegación de servicio (DoS). Según (Capacity Academy, 2016) Este ataque tiene lugar cuando un atacante desactiva o corrompe las redes, los sistemas o los servicios para denegar el servicio a los usuarios. Se puede lograr enviando datos no válidos a aplicaciones o servicios de red, lo que puede hacer que el servidor se bloquee. Otro ataque DoS consiste en inundar de tráfico toda una red hasta hacer que se sature y sea imposible utilizarla o también se puede estropear un router con el fin de que los usuarios legítimos no puedan acceder a la red.

Ataque hombre en medio. Este ataque se produce cuando alguien se interpone entre dos usuarios que se están comunicando. El atacante observa activamente, captura y controla los paquetes sin que los usuarios lo adviertan. Por ejemplo, un atacante puede

negociar claves de cifrado con ambos usuarios. A continuación, cada usuario enviará datos cifrados al atacante, quien podrá descifrarlos.

Spoofing. Este ataque se basa en el uso de las direcciones IP. La mayoría de las redes y sistemas operativos utilizan la dirección IP para identificar un equipo como válido en una red. En algunos casos, es posible utilizar una dirección IP falsa. Esta práctica se conoce como suplantación. Un atacante podría utilizar programas especiales para construir paquetes IP que parezcan provenir de direcciones válidas dentro de la intranet de una organización. Una vez obtenido el acceso a la red con una dirección IP válida, el atacante podrá modificar, desviar o eliminar datos.

Ataque de clave comprometida. Una clave es un código o un número secreto necesario para cifrar, descifrar o validar información protegida. Averiguar una clave es un proceso difícil y que requiere grandes recursos por parte del atacante, pero no deja de ser posible. Cuando un atacante averigua una clave, ésta se denomina clave comprometida. El atacante puede utilizar la clave comprometida para obtener acceso a una comunicación protegida sin que el remitente ni el receptor lo perciban. La clave comprometida permite al atacante descifrar o modificar los datos. El atacante también puede intentar utilizar la clave comprometida para calcular otras claves que podrían suponer el acceso a otras comunicaciones protegidas.

4.4.3.3 **Seguridad de los datos**

Todas las tecnologías de seguridad en las redes se basan en técnicas criptográficas. Para dar seguridad a los datos, tres aspectos deben de proporcionar estas técnicas.

- Confidencialidad
- Integridad
- Autenticación.

Por confidencialidad se entiende como el hecho de ocultar los datos de usuarios no autorizados. Por integridad se refiere al hecho de asegurar que los datos no sean modificados mientras son transmitidos y la autenticación se refiere al hecho de poder comprobar que los datos provienen del lugar del que se supone deben venir. El cifrado

simétrico, el cifrado de clave pública y las funciones de dispersión (hash) son las técnicas utilizadas para proteger la información de todos los tipos de ataques ya mencionados.

4.4.3.3.1 **Criptografía y criptoanálisis**

Según (Bruce Schneier, 96) Criptografía y Criptoanálisis.

Criptografía. Es la ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. La criptografía abarca el uso de mensajes encubiertos, códigos y cifras, así como el uso de algoritmos matemáticos para poder proteger la información. La criptografía es el fundamento de todas las tecnologías de seguridad de las redes.

Criptoanálisis. Es la ciencia que analiza los algoritmos criptográficos, con el fin de poder obtener el texto nativo a partir de un texto cifrado. Hay ciertos algoritmos simples que son fáciles de romper, sin embargo, un buen algoritmo de encriptación sólo puede ser roto por medio de ataques de fuerza bruta o de diccionario.

El ataque de fuerza bruta consiste en probar cada posible clave sobre un fragmento de texto cifrado hasta que se obtenga un mensaje legible de texto nativo. Por otra parte, el ataque de diccionario se basa en estudiar la naturaleza del algoritmo junto a algún conocimiento de las características generales del texto nativo con el fin de deducir un texto nativo concreto o encontrar la clave que se esté utilizando. Si la clave es descubierta, todos los mensajes cifrados con esta clave quedan seriamente amenazados.

4.4.3.3.2 **Cifrado simétrico o de clave privada**

La técnica más utilizada históricamente para dar privacidad a los datos transmitidos es el cifrado simétrico o de clave privada. En el cifrado simétrico, las entidades de comunicación establecen y comparten una clave secreta que se utiliza después para cifrar y descifrar los mensajes. Un esquema de cifrado simétrico tiene los siguientes elementos (Ver figura 4.29).

- Texto nativo: Es el mensaje original que va a ser cifrado y que constituye la entrada del algoritmo.

- Algoritmo de cifrado: Es un algoritmo que realiza varias transformaciones del texto nativo en base a operaciones simples sobre patrones de bits.
- Clave secreta: Es una entrada del algoritmo de cifrado. Los cambios que realice el algoritmo al texto nativo dependen de la clave.
- Texto cifrado: Es el mensaje alterado que produce el algoritmo de cifrado. Claves diferentes producen cifrados diferentes para un mismo mensaje.
- Algoritmo de descifrado: Es esencialmente el algoritmo de cifrado ejecutado inversamente.

Figura 4-29: Modelo de cifrado simétrico
Fuente: Elaboración propia

Una clave es un código secreto que utiliza el algoritmo de encriptación para crear una única versión de texto cifrado. Mientras mayor sea la longitud de la clave, será más difícil averiguar ésta. Por ejemplo, una clave de 56 bits puede proporcionar 2^56 diferentes combinaciones.

Los algoritmos de encriptación simétrica más importantes son los llamados cifradores de bloque. Un cifrador de bloque procesa una entrada de texto nativo en bloques de tamaño fijo y produce un texto cifrado de igual tamaño por cada bloque de texto nativo. Los principales algoritmos de este tipo son DES y 3DES.

Estándar de Cifrado de Datos (DES, Data Encryption Standard). Creado en 1977, este algoritmo utiliza una clave simétrica de 56 bits para encriptar datos en bloques de 64 bits. Una computadora personal común tardaría años en probar todas las combinaciones usando la fuerza bruta. Sin embargo, utilizando computadoras especiales es posible romper

la encriptación en cuestión de segundos. Esto hace que DES ya no sea considerado un algoritmo seguro y no se debería usar en una VPN.

Estándar de Cifrado de Datos Triple (3DES). Debido a su debilidad, DES fue reforzado y se creó 3DES. Este algoritmo repite el algoritmo básico DES tres veces. Esto es, un texto es cifrado tres veces usando tres claves distintas. La longitud de la clave es de 168 bits. La desventaja de este algoritmo es que es lento, sin embargo, da buena seguridad y es muy utilizado por IPSec para cifrar los datos.

4.4.3.3.3 Cifrado asimétrico o de clave pública

El cifrado asimétrico o de clave pública fue propuesto por Diffie y Hellman en 1976. El cifrado asimétrico es un método donde cada usuario posee una pareja de claves relacionadas matemáticamente, donde se utiliza una clave para cifrar la información y la otra para descifrarla. Una de las claves se denomina clave pública, la cual puede darse a conocer ante todos los que quieran intercambiar información de forma segura con el usuario. La otra es la clave privada, la cual el usuario es dueño y no debe darla a conocer. Un esquema de cifrado asimétrico tiene los siguientes elementos:

- Texto nativo.
- Algoritmo de cifrado
- Clave pública y privada
- Texto cifrado.
- Algoritmo de descifrado.

El procedimiento para cifrar mensajes utilizando claves públicas se muestra en la figura 4.30 y es explicado a continuación.

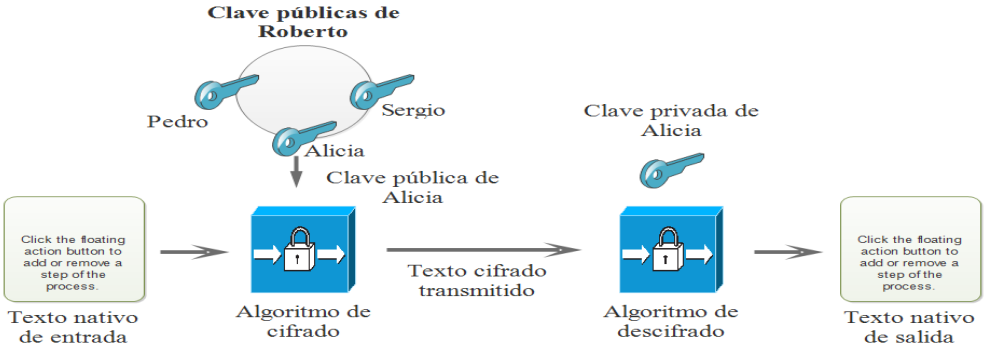


Figura 4-30: Modelo de cifrado de clave pública
Fuente: Elaboración propia

1. Cada usuario genera un par de claves que van a ser utilizadas para el cifrado y descifrado de los mensajes.
2. Cada usuario publica una de las dos claves de cifrado en un registro público. Esta clave se convierte en pública y la otra permanece privada.
3. Cada usuario puede tener las claves públicas de todos los usuarios con los que mantiene comunicación.
4. Si un usuario (Roberto) desea enviar un mensaje cifrado a otro (Alicia), él cifra el mensaje utilizando la clave pública de Alicia.
5. Cuando Alicia recibe el mensaje, lo descifra utilizando su clave privada. Nadie más puede descifrar el mensaje, ya que solamente Alicia conoce su propia clave.

Así, todos los participantes tienen acceso a las claves públicas y cada uno de ellos genera localmente su propia clave privada. Mientras la clave privada permanezca en secreto, las comunicaciones serán seguras.

Los algoritmos de cifrado de clave pública más importante son el RSA y Diffie-Hellman.

Rivest Shamir Adleman (RSA). Es un algoritmo de clave pública creado en 1977 por Ron Rivest, Adi Shamir y Len Adleman. Este algoritmo goza de mucha popularidad. La longitud de su clave varía desde 512 a 2048 bits haciendo que sea un algoritmo de encriptación muy seguro.

Este algoritmo utiliza un número conocido como módulo público para conseguir las claves pública y privada. Este número se forma multiplicando dos números primos. La seguridad de este algoritmo se encuentra en el hecho de que, aunque encontrar números primos grandes es relativamente fácil, hacer factor del resultado de multiplicar dos números primos resulta ser muy difícil. Si los números primos usados son muy grandes, el problema llega a ser computacionalmente imposible. RSA es ampliamente utilizado en certificados, los cuales utilizan muchas VPN para autenticar usuarios.

Diffie-Hellman (D-H). Es un método de encriptación de clave pública el cual permite a dos partes que se comunican usando IPSec establecer una clave simétrica que sólo ellos conocen, aunque se estén comunicando sobre un canal inseguro.

Con Diffie-Hellman, cada par genera una clave pública y otra privada. La clave privada se mantiene secreta y nunca es compartida. La clave pública se calcula de la clave privada por cada parte y se intercambia sobre el canal inseguro. Cada par combina la clave pública del otro con su propia clave privada y calcula el mismo número secreto compartido. El número secreto compartido es convertido entonces en una clave secreta compartida. Esta clave nunca se intercambia sobre el canal inseguro.

D-H es muy importante porque la clave secreta compartida es utilizada para cifrar datos usando los algoritmos de encriptación de clave secreta especificados en las SA de IPSec, tales como DES o MD5.

4.4.3.3.4 Funciones de dispersión (hash) unidireccionales

Las funciones de dispersión unidireccionales (one-way hash function) son muy utilizadas para la autenticación de datos, para la creación de firmas digitales y también son muy utilizadas por las tecnologías de autenticación de usuarios. Un conjunto de datos está autenticado si verdaderamente proviene del lugar de origen pretendido. La autenticación verifica que el mensaje sea auténtico y que no haya sido alterado.

Existen tres formas para autenticar un mensaje. La primera es utilizando cifrado simétrico. Si se supone que sólo el emisor y el receptor comparten la clave, se asegura la autenticación. El resumen del mensaje se puede cifrar usando cifrado de clave pública. Esto proporciona una firma digital, así como la autenticación de los mensajes y no requiere distribuir las claves a las partes que se comuniquen. La tercera forma es utilizando una función de dispersión.

Las funciones de dispersión operan sobre un mensaje de longitud variable y produce un resumen del mensaje de longitud fija (hash signature). Estas funciones crean una huella digital electrónica única para un mensaje dado. Para autenticar un mensaje se envía con él un resumen del mensaje de forma que el resumen sea auténtico. Una función de dispersión tiene las siguientes propiedades y atributos:

1. La función puede ser aplicada a un bloque de datos de cualquier tamaño.

2. La función produce una salida de longitud fija.
3. Para cualquier valor dado, es relativamente fácil calcular su función por lo que la función se puede implementar en software y hardware.
4. La función es unidireccional porque es fácil generar un código dado un mensaje, pero prácticamente imposible generar un mensaje a partir de un código. De esta forma, el mensaje se mantiene secreto.
5. No se puede encontrar un mensaje alternativo que produzca el mismo valor que un mensaje dado. Con esto se impide la falsificación de un mensaje.
6. Una función de dispersión es fuerte si resiste un ataque llamado "ataque del cumpleaños".

Las funciones de dispersión más importantes son MD5 y SHA-1.

Resumen de Mensaje versión 5 (MD5, Message Digest version 5). Es un algoritmo de dispersión que autentica los datos de los paquetes. Tuvo versiones anteriores llamadas MD2 y MD4. Este algoritmo toma un mensaje de longitud variable y produce un resumen del mensaje (hash) de 128 bits. MD5 es muy utilizado por IPSec para la autenticación de datos.

Algoritmo de Dispersión Segura versión 1 (SHA-1, Security Hash Algorithm). Es un algoritmo de dispersión el cual fue publicado como estándar en 1993. En 1995 se publicó una versión revisada conocida como SHA-1. Este algoritmo toma como entrada un mensaje con una longitud máxima de 2 ^ 64 bits y produce un resumen del mensaje (hash) de 160 bits. La entrada se procesa en bloques de 512 bits. IPSec y los certificados utilizan ampliamente SHA-1 para la autenticación y las firmas digitales.

4.4.3.3.5 **Firma digital**

Una firma digital es utilizada con las claves públicas y se trata de un medio por el que los autores de un mensaje, archivo u otro tipo de información codificada digitalmente enlazan su identidad a la información. El proceso de firmar información digitalmente implica la transformación de la misma y de algunos datos secretos que guarda el remitente en una etiqueta denominada firma.

Una firma digital es el equivalente electrónico de una firma manuscrita y tiene el mismo propósito. Las firmas digitales no deben ser falsificables, los receptores deben ser capaces de verificarlas y los firmantes no deben poder negarlas después. Una diferencia entre una firma manuscrita y una firma digital electrónica es que ésta última no debe ser constante y debe ser función de los datos que acompaña, de lo contrario una misma firma podría ser utilizada en cualquier mensaje y también se podría alterar cualquier mensaje firmado.

El cifrado de clave pública puede operar en conjunción con las funciones de dispersión unidireccionales para poder crear una firma digital. El proceso de creación de una firma digital y la verificación de su autenticidad usando estas técnicas criptográficas se muestra en la figura 4.31:

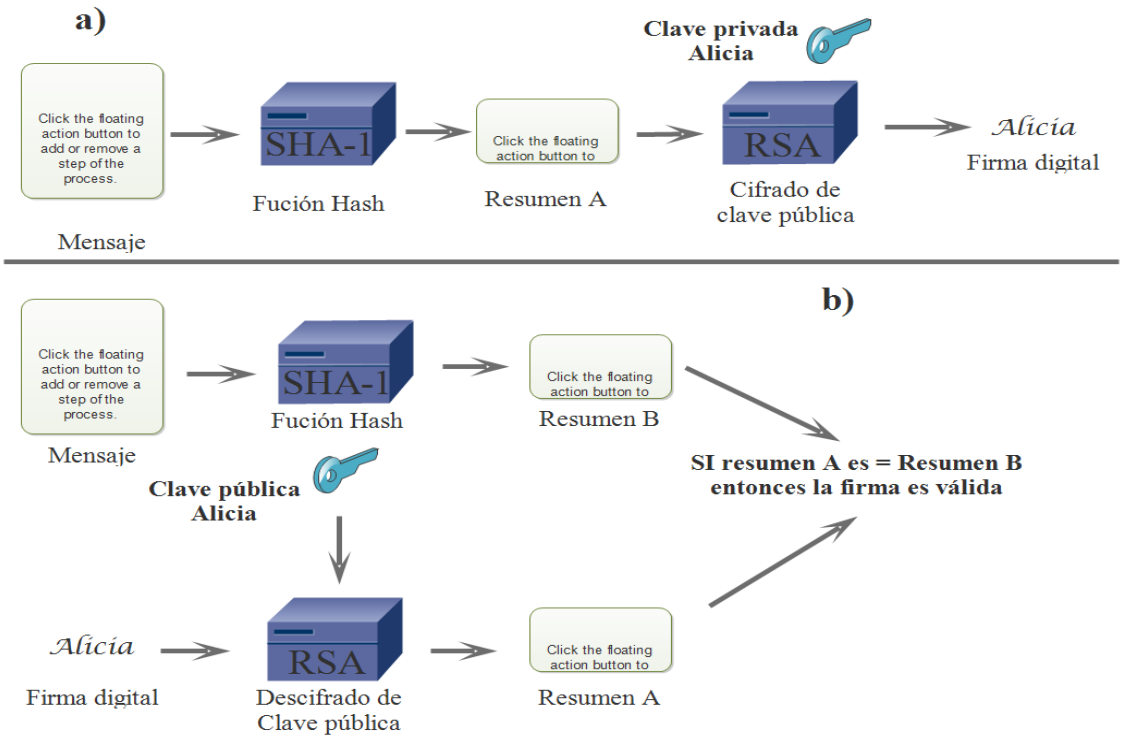


Figura 4-31: Firma digital a) Creación b) Validación
Fuente: Elaboración propia

El inciso a) muestra la creación de la firma digital. Alicia crea la firma cifrando el resumen del mensaje producido por la función de dispersión usando su clave privada. En el inciso b) se muestra la validación de la firma. Cuando Alicia le envía un mensaje firmado a Roberto, éste lo valida comparando el resumen del mensaje que él genera localmente con

el resumen obtenido al descifrar la firma usando la clave pública de Alicia. Si ambos resúmenes son exactamente iguales, entonces la firma es válida.

Es necesario tomar en cuenta que una firma digital no ofrece privacidad, ya que un mensaje firmado puede ser leído por cualquier persona. Incluso si se cifra el mensaje completo, cualquier intruso puede descifrar el mensaje utilizando la clave pública del autor. Lo único que hace la firma digital es demostrar que el mensaje pertenece al verdadero autor que lo creó.

4.4.3.4 **Sistemas de autenticación de usuarios**

Existen muchos mecanismos de autenticación de usuarios. Cada sistema de autenticación tiene sus ventajas y desventajas. Un sistema de autenticación es aquel donde un usuario se identifica ante un servidor remoto. En un VPN es muy importante identificar a los usuarios de la red para poder garantizar la seguridad. De los sistemas de autenticación aquí mencionados el más recomendable y utilizado en una VPN es PKI.

4.4.3.4.1 **Autenticación basada en contraseña**

La autenticación basada en contraseña es la más utilizada por los sistemas computacionales. En este mecanismo de autenticación, un usuario se identifica a sí mismo ante un servidor remoto al inicio de una sesión mediante una contraseña. La contraseña es un secreto compartido entre el usuario y el servidor remoto. El usuario recuerda la contraseña y el servidor almacena o una copia de ella o un valor calculado de la contraseña.

Aunque se trata de un método fácil de implementar y de usar, también resulta ser el más inseguro de todos. Si un intruso obtiene la contraseña, se puede hacer pasar como un usuario legítimo y entonces obtener todos los privilegios de acceso a la red que tenía el usuario legítimo. Cuando un usuario proporciona su nombre y su contraseña, cualquier atacante que esté observando (usando un sniffer) puede obtener la contraseña. Hasta que el usuario legítimo no cambie su contraseña, el atacante podrá hacer todo lo que quiera. Es por eso que muchas organizaciones insisten en que sus usuarios cambien continuamente de clave.

Una autenticación basada en contraseña no proporciona autenticación mutua. La contraseña de un usuario lo autentica ante el servidor. Si el servidor necesitara autenticarse ante el usuario, se necesitaría otra contraseña. El hecho de que no exista autenticación mutua proporciona otra ventaja a un atacante, ya que éste puede crear un servidor falso que se haga pasar por el legítimo y así obtener todas las contraseñas de los usuarios que se autentican con

el servidor. El principal protocolo de autenticación por contraseña es PAP el cual es utilizado por PPP.

4.4.3.4.2 **Autenticación basada en desafíos**

En este tipo de autenticación, el servidor genera un conjunto de datos aleatorio denominado desafío y se lo envía al usuario que desea autenticarse. En lugar de responder con una contraseña, el usuario cifra el desafío con una clave compartida sólo por el servidor y el usuario. El usuario envía su nombre y el texto cifrado al servidor. El servidor realiza la misma encriptación y entonces compara el texto cifrado enviado por el usuario con el texto cifrado generado localmente. Si ambos son iguales, la autenticación se lleva a cabo con éxito, de lo contrario el usuario será rechazado.

Se pueden utilizar las funciones de dispersión para este tipo de autenticación. Este mecanismo permite que un usuario se autentique ante un servidor y se basa en la existencia previa de un secreto compartido previamente por ambos como puede ser una contraseña. El usuario presenta su nombre y el servidor genera un desafío. Entonces el usuario combina el desafío con la clave, le aplica una función de dispersión y devuelve el resultado. El servidor repite el cálculo usando su propia versión del secreto compartido. Si ambos son iguales, se autentica al usuario y sin necesidad de enviar la contraseña.

Para prevenir los ataques de sniffers, este sistema de autenticación utiliza un secreto diferente por cada intento de autenticación. Este método es mejor que la contraseña porque un desafío diferente es enviado cada vez y así un atacante no podrá utilizar más de una vez el texto cifrado generado por el usuario para hacerse pasar por éste. Para que exista autenticación mutua, se requiere de un segundo desafío y su respectiva respuesta. El usuario puede proporcionar el segundo desafío junto con el primer desafío cifrado. Los protocolos de autenticación basados en este método son CHAP, MS-CHAP y EAP-MD5.

4.4.3.4.3 **Kerberos**

Kerberos es un conjunto de servicios que proporcionan un sistema de autenticación basado en un Centro de Distribución de Claves (KDC, Key Distribution Center). Un KDC determina a qué sistemas se les permite comunicarse entre ellos. Cuando a dos sistemas se les permite comunicarse entre ellos, el KDC proporciona una clave de sesión para esa conexión. Kerberos fue diseñado para las redes TCP/IP y se basa en el cifrado simétrico. Además, comparte una clave secreta diferente con cada entidad en la red.

Kerberos fue creado en el Instituto Tecnológico de Massachussets (MIT) en 1980 para un proyecto denominado Atenea. Kerberos es muy popular principalmente en escuelas y universidades y apenas está ingresando en el mundo de las empresas. La versión utilizada actualmente es Kerberos 5, el cual corrige ciertas deficiencias respecto al Kerberos original: Kerberos 4. Se puede utilizar Kerberos como forma de autenticación para IPSec en lugar de utilizar una PKI.

En un sistema Kerberos existen clientes y servidores. Los clientes pueden ser usuarios, sin embargo, también pueden ser aplicaciones que requieran de privilegios para acceder a un determinado sistema. Kerberos mantiene una base de datos de los clientes y de sus claves secretas. En el caso de un usuario se trata de una contraseña cifrada. Cualquiera que requiera autenticación necesita registrar su secreto con Kerberos.

Debido a que Kerberos conoce los secretos de todos, puede crear mensajes que convenzan a un usuario que en realidad se está autenticando con el servidor con el que pretende autenticarse. Kerberos también crea claves de sesión que les son dadas a cada cliente y al servidor (o a dos clientes) y a nadie más. Una clave de sesión es utilizada para cifrar mensajes entre las dos partes que se comunican, después de la cual es destruida.

4.4.3.4.4 **Infraestructura de Claves Públicas (PKI)**

Una Infraestructura de Claves Públicas (PKI, Public Key Infraestructure) basa su funcionamiento en el uso de certificados como sistema de autenticación de usuarios. Este es uno de los métodos de autenticación más utilizados en una VPN. Dada una clave pública, un usuario necesita saber quién posee la clave privada que está relacionada con dicha clave pública con el fin de poder comunicarse con él. La respuesta a este problema está en los certificados. La figura 4.31 muestra cómo se lleva a cabo la autenticación basada en certificados.

Una PKI consta de varios componentes que facilitan su administración. Cada componente tiene asignada una tarea específica y deben estar presentes en cualquier PKI. Los componentes de una PKI son:

- Certificados
- Autoridad de Certificación (CA, Certification Authority)
- Autoridad de Registro (RA, Registration Authority)

- Repositorio
- Archivo

Certificados: Un certificado es un objeto digital que relaciona una clave pública con una persona u organización. Con el fin de distribuir claves públicas de una forma segura y asegurar su integridad, se certifican las claves públicas que pertenecen a las personas, empresas y toda clase de organizaciones que se encuentran en Internet. Al usar certificados, un usuario puede estar seguro de que está utilizando la clave pública de otro usuario y que, por lo tanto, ese usuario firmó el mensaje.

Un certificado contiene el nombre del usuario y su clave pública. El certificado puede indicar la organización a la cual pertenece el usuario, así como también su correo electrónico. El certificado también posee la fecha de activación y la fecha en que caduca. También posee el nombre de la organización confiable que creó el certificado. Esta organización incluye un número de serie que identifica a cada certificado de manera única. Por último, la organización confiable firma digitalmente el certificado usando su propia clave privada. Un ejemplo de un certificado se muestra en la figura 4.32.

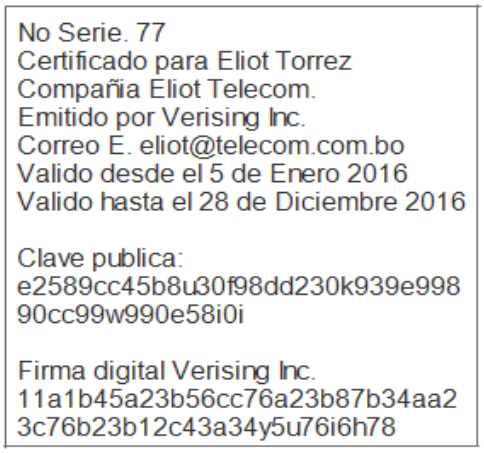


Figura 4-32: Ejemplo de un certificado
Fuente: Elaboración propia

Los certificados son muy importantes dentro de una VPN. Cuando un cliente inicia una sesión en la red de una empresa desde un sitio remoto a través de una VPN, el servidor VPN puede presentar un certificado de servidor para establecer su identidad. Dado que la entidad raíz corporativa es de confianza y la entidad emisora de certificados de raíz corporativa emitió el certificado del servidor VPN, el equipo cliente puede proseguir con la

conexión y el empleado sabe que su equipo está realmente conectado al servidor VPN de su organización.

El servidor VPN también tiene que poder autenticar al cliente VPN antes de empezar a intercambiar datos sobre la conexión VPN. Se puede dar la autenticación a nivel de equipo con el intercambio de certificados de equipo o la autenticación a nivel de usuario a través de un método de autenticación Protocolo punto a punto (PPP).

El certificado del equipo cliente puede servir para varios propósitos, la mayor parte de los cuales están basados en la autenticación, permitiendo que el cliente utilice muchos recursos organizativos sin la necesidad de certificados individuales para cada recurso. Por ejemplo, el certificado de cliente podría permitir conectividad VPN además de acceso al sitio intranet de la compañía, a servidores de productos y a una base de datos.

El certificado del servidor VPN también podría servir para varios propósitos. El mismo certificado podría tener el propósito de comprobar la identidad de servidores de correo electrónico, servidores Web o servidores de aplicaciones. La entidad emisora de certificados que emite el certificado determina el número de propósitos de cada certificado.

Para estandarizar el formato de los certificados, se ha diseñado un estándar conocido como X.509 el cual es ampliamente utilizado en Internet. X.509 es una forma de describir certificados. Lo hace utilizando varios campos entre los más importantes se encuentran en la tabla 4.4.

Campo	Significado
Versión	La versión del X.509
Número de serie	El número que identifica al certificado de forma única
Algoritmo de firma	El algoritmo utilizado para firmar el certificado
Emisor	El nombre X.500 de la CA
Valido desde	Fecha de inicio de validez del certificado
Válido hasta	Fecha de fin de validez del certificado
Asunto	La entidad cuya clave se está certificando
Clave pública	La clave pública del sujeto y el ID del algoritmo usado para crearla
Emisor	Un ID opcional que identifica de forma única al emisor del certificado
Sujeto	Un ID opcional que identifica de manera única al ID del certificado
Extensiones	Existen varias extensiones
Firma digital	La firma del certificado firmada por la clave privada de la CA

Tabla 4-4: Campos de un certificado según el estándar X.509

Fuente: Elaboración propia

Un certificado puede ser revocado cuando termina su validez o si una persona u organización hace un mal uso de él o si alguna clave privada se ha expuesto. La herramienta que utiliza una PKI para comprobar si un certificado es válido o no es la Lista de Revocación de Certificados (CRL, Certificate Revocation List) La CRL contiene la lista de todos los números de serie de certificados que ya han expirado o que ya no son confiables. La entidad confiable se encarga de publicar la CRL de forma frecuente para que cualquiera pueda verla.

Autoridad de Certificación (CA, Certification Authority). Es el componente más importante de una PKI. Una CA es la entidad confiable encargada de crear, firmar y distribuir certificados. Una CA es el conjunto de software, hardware y las personas que la operan.

Una CA tiene seis responsabilidades fundamentales que debe cumplir. La primera y la más importante es proteger su clave privada utilizando software o hardware como tarjetas inteligentes o de lo contrario la seguridad se verá comprometida. La segunda es verificar la información de un certificado antes de que sea distribuido, es decir, los datos del poseedor del certificado. La tercera es asegurar que todos los certificados y CRL cumplen con su perfil, esto es, si por ejemplo una CA sólo distribuye certificados para correo electrónico, no podrá existir un certificado de esa CA donde se autorice su uso para firmar un contrato. La cuarta es mantener una lista de los certificados que ya no son confiables, es decir que han expirado o han sido revocados. La quinta es distribuir los certificados y CRL para que puedan ser utilizados por los usuarios. La sexta y última responsabilidad es mantener un archivo de todos los certificados que ha tenido la CA. Las principales CA son las siguientes:

- Entrust
- GTE Cybertrust
- Network Associates PGP
- Baltimore
- Microsoft
- Verisign

Autoridad de Registro (RA, Registration Authority). Es la entidad que verifica el contenido de un certificado. El contenido de un certificado debe reflejar la información presentada por la entidad que solicita el certificado. Por ejemplo, una compañía puede solicitar un certificado para un usuario de cierto departamento y darle la autoridad para que firme algún contrato. Entonces la RA escribe en el certificado la información de la compañía, el departamento y la autoridad que tiene el usuario. Después, la RA proporciona esta información a la CA.

Repositorio. Un repositorio distribuye los certificados y las listas de revocación. Un repositorio acepta los certificados y CRL de una o varias CA y los hace disponibles a las organizaciones que los requieren para implementar servicios de seguridad.

Archivo. Se encarga de almacenar la información de los certificados de la CA. El archivo permite demostrar que la información es confiable al momento de recibirla y que no ha sido modificada mientras está en el archivo.

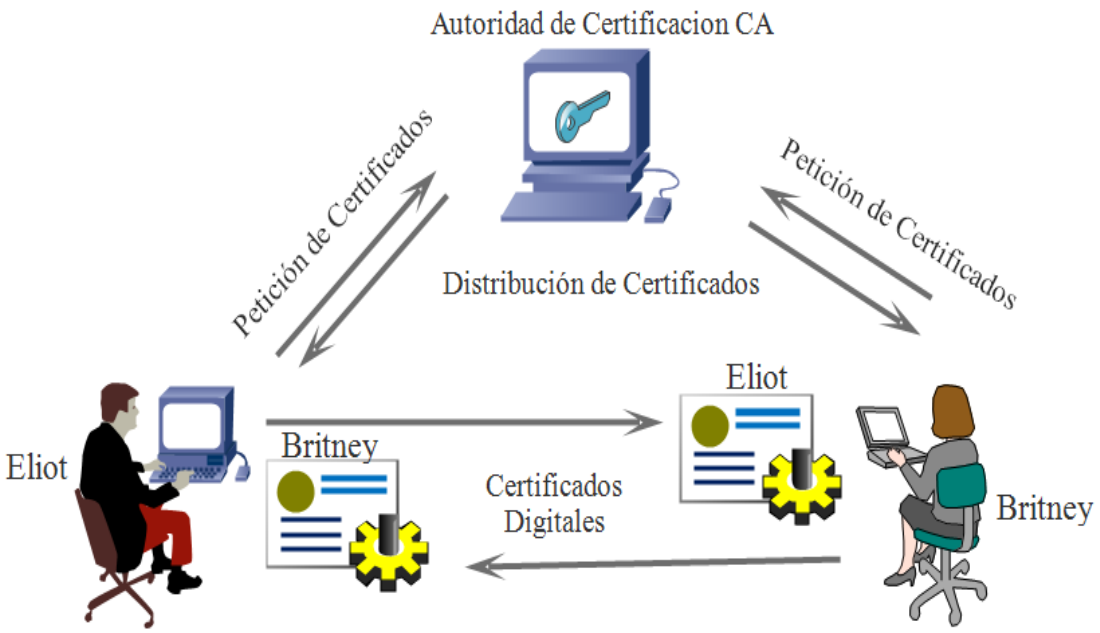


Figura 4-33: Autenticación basada en certificados
Fuente: Elaboración propia

4.4.3.4.5 **Servidores RADIUS**

El Servicio de Usuario de Marcación para Autenticación Remota (RADIUS, Remote Authentication Dial-In User Service) es un estándar para un sistema de autenticación de acceso remoto. Provee la funcionalidad de autenticación, autorización y contabilidad (AAA, Authentication, Authorization, Accounting) la cual es muy importante para el control de acceso.

RADIUS por sí mismo no provee buenos métodos de autenticación, sin embrago, RADIUS puede utilizar diferentes protocolos de autenticación para proveer mejor servicio como PAP, CHAP, MS-CHAP y EAP.

RADIUS es un protocolo y software cliente-servidor, el cual es utilizado por los dispositivos o aplicaciones NAS y servidores VPN para autenticar usuarios remotos y autorizarlos para que puedan acceder a los recursos de la red. Un servidor que ejecuta el servicio RADIUS es comúnmente conocido como servidor RADIUS. RADIUS es utilizado frecuentemente como Sistema de Autenticación Central el cual provee la autenticación, autorización y control para los usuarios remotos. Protocolos de autenticación.

4.5 TECNOLOGIAS DE LAS VPN

Analizando los protocolos más importantes que hacen que una VPN pueda funcionar. Existen varios, pero los más importantes son PPTP, L2TP e IPSec. Cada protocolo tiene sus ventajas y desventajas, así que corresponde al diseñador y administrador de la VPN determinar cuál es el más conveniente para una organización en particular.

4.5.1 Protocolo de Túnel Punto a Punto (PPTP)

4.5.1.1 **Definición de PPTP**

Según (Microsoft Corporation, 2016) El Protocolo de Túnel Punto a Punto (PPTP, Point-to-Point Tunneling Protocol) es un protocolo de red creado por Microsoft, Ascend Communications y US Robotics el cual permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet.

En el escenario típico de PPTP, el cliente establecerá una conexión dial-up con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP. Una vez conectado, el cliente establecerá una segunda conexión con el

servidor PPTP el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada. PPTP está documentado en el RFC 2637.

PPTP es una extensión de PPP, el cual es utilizado tradicionalmente para las conexiones dial-up. PPTP fue diseñado principalmente para las VPN de acceso remoto, sin embargo, también puede trabajar en las VPN de sitio a sitio. PPTP opera en la capa 2 del modelo OSI.

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y descifrados de acuerdo al protocolo de red transmitido. Por el momento, PPTP únicamente soporta los protocolos de red IP, IPX, y NetBEUI. PPTP especifica además una serie de mensajes de control con el fin de establecer, mantener y destruir el túnel PPTP. Estos mensajes son transmitidos en paquetes de control en el interior de segmentos TCP. De este modo, los paquetes de control almacenan la cabecera IP, la cabecera TCP y el mensaje de control PPTP.

En el caso de Microsoft, la autenticación utilizada para el acceso a los RAS soporta los protocolos CHAP, MS-CHAP, PAP, y debido a los problemas de seguridad, en versiones posteriores también se usa EAP. En cuanto a la encriptación de datos, PPTP utiliza el proceso de encriptación de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el protocolo MPPE a partir de la contraseña del usuario.

PPTP permanece como una opción popular para implementar VPN gracias a Microsoft. El cliente PPTP se distribuye gratuitamente en todas las versiones de estación de trabajo Windows, mientras que el servidor PPTP se instala junto con los sistemas operativos de servidor Windows. PPTP puede ser también implementado en sistemas Linux, así como en Macintosh. También diversos modelos de firewalls soportan PPTP, tales como servidores ISA, PIX de Cisco y SonicWall.

Una desventaja que tiene PPTP es que no posee un único estándar para la encriptación y la autenticación, ya que PPTP se ocupa únicamente de crear un túnel. Además, PPTP es el protocolo VPN menos seguro. L2TP e IPSec ofrecen mejores alternativas para garantizar la seguridad en una VPN.

4.5.1.2 **Estructura de PPTP**

4.5.1.2.1 **Concentrador de Acceso PPTP (PAC)**

El Concentrador de Acceso PPTP (PAC, PPTP Access Concentrator) es un dispositivo conectado a las líneas PSTN o ISDN capaz de realizar operaciones PPP y de manejar el protocolo PPTP. Lo único que necesita el PAC es implementar TCP/IP para transportar el tráfico hacia uno o más PNS. También puede entunelar protocolos que no son IP. Es también conocido como FEP o Procesador Final Frontal.

4.5.1.2.2 **Servidor de Red PPTP (PNS)**

El Servidor de Red PPTP (PNS, PPTP Network Server) es un dispositivo que opera como un servidor de túnel. Puesto que PPTP se basa completamente en TCP/IP y es independiente de la interfase de hardware, el PNS puede utilizar cualquier combinación de hardware incluyendo dispositivos LAN y WAN.

4.5.1.2.3 **Conexión de control**

Antes de que PPP pueda ser entunelado entre un PAC y un PNS, se debe establecer una conexión de control entre ambos dispositivos. La conexión de control es una sesión TCP estándar sobre la cual pasa el control de la llamada PPTP y la administración de la información. El control de la sesión está asociado lógicamente, pero separado de las sesiones que son entuneladas a través de un túnel PPTP. Para cada pareja PAC-PNS existe tanto un túnel como una conexión de control. La conexión de control es responsable de establecer, administrar y liberar las sesiones transportadas a través del túnel.

Mensajes de control. PPTP define un conjunto de mensajes enviados como datos TCP en la conexión de control entre un PAC y un PNS. La sesión TCP para establecer la conexión de control es establecida al iniciar una conexión TCP en el puerto 1723. La conexión de control puede ser establecido tanto por el PNS como por el PAC. Cada mensaje inicia con una cabecera de ocho octetos fija. Dicha cabecera contiene la longitud total del mensaje, el indicador del tipo de mensaje PPTP y una constante conocida como Magic Cookie.

La Magic Cookie es siempre enviada como la constante 0x1A2B3C4D. Su propósito es permitirle al receptor asegurarse de que está sincronizado adecuadamente con el flujo de datos TCP.

Los mensajes utilizados para mantener el control de las conexiones PPTP se muestran en la tabla 4.5.

Código	Nombre	Descripción
1	Start-Control-Connection-Request	Inicia el establecimiento de la sesión PPTP
2	Start-Control-Connection-Reply	Es la respuesta al mensaje 1. Contiene un código resultante que indica el éxito o el fracaso del establecimiento de la sesión, así como el número de la versión del protocolo
3	Stop-Control-Connection-Request	Es una petición para cerrar la conexión de control
4	Stop-Control-Connection-Reply	Es la respuesta al mensaje 3. Contiene el código resultante que indica el éxito o fracaso del cierre de la conexión
5	Echo-Request	Enviado periódicamente tanto por el cliente como por el servidor para mantener activa la conexión
6	Echo-Reply	Es la respuesta al mensaje 5 para indicar que la conexión sigue activa
7	Outgoing-Call-Request	Es una petición enviada por el cliente para crear un túnel
8	Outgoing-Call-Reply	Es la respuesta al mensaje 7, la cual contiene un identificador único para ese túnel
9	Incoming-Call-Request	Es una petición del cliente para recibir una llamada entrante por parte del servidor
10	Incoming-Call-Reply	Es la respuesta al mensaje 9. Esta indica si la llamada entrante debería ser contestada
11	Incoming-Call-Connected	Es la respuesta al mensaje 10. Provee parámetros de llamada adicionales al servidor
12	Call-Clear-Request	Es una petición para desconectar o una llamada entrante o saliente, enviada del servidor al cliente
13	Call-Disconnect-Notify	Es una respuesta al mensaje 12 para indicar que se realizará la desconexión y las razones para hacerlo
14	WAN-Error-Notify	Notifica que un error ha ocurrido en la conexión WAN, esto es, en la interfase que soporta PPP
15	Set-Link-Info	Notifica cambios en las opciones PPP

Tabla 4-5: Mensajes de control de conexión en PPTP
Fuente: Elaboración propia

Códigos de error. Los códigos de error determinan si ocurrió un error en la conexión PPTP. En la tabla 4.6 se muestra cuáles pueden ser estos errores.

Código	Nombre	Descripción
0	None	No hay error
1	Not-connected	Todavía no existe una conexión de control para este par PAC-PNS
2	Bad-Format	La longitud es errónea o el valor de la Magic Cookie es incorrecto
3	Bad-Value	Uno de los valores de algún campo está fuera de rango o un campo reservado no está en ceros
4	No-Resource	Recursos insuficientes para manejar este comando
5	Bad-Call-ID	El identificador de llamada es incorrecto
6	PAC-Error	Un error específico ocurrió en el PAC

Tabla 4-6: **Códigos de error en PPTP**

Fuente: Elaboración propia

4.5.1.2.4 Túneles en PPTP

PPTP requiere del establecimiento de un túnel para la comunicación entre una pareja PAC-PNS. Los datos de usuario que transporta PPTP son tramas PPP, las cuales son encapsuladas utilizando GRE. El túnel es utilizado para transportar todas las tramas PPP que pertenecen a una sesión entre una pareja PAC-PNS. Una clave presente en la cabecera GRE indica a cuál sesión pertenece una determinada trama PPP. De esta manera, Las tramas PPP son transportadas por rutas distintas, pero dentro de un único túnel. El proceso de ensamblado de un paquete PPTP al momento de ser transmitido se muestra en la figura 4.34.

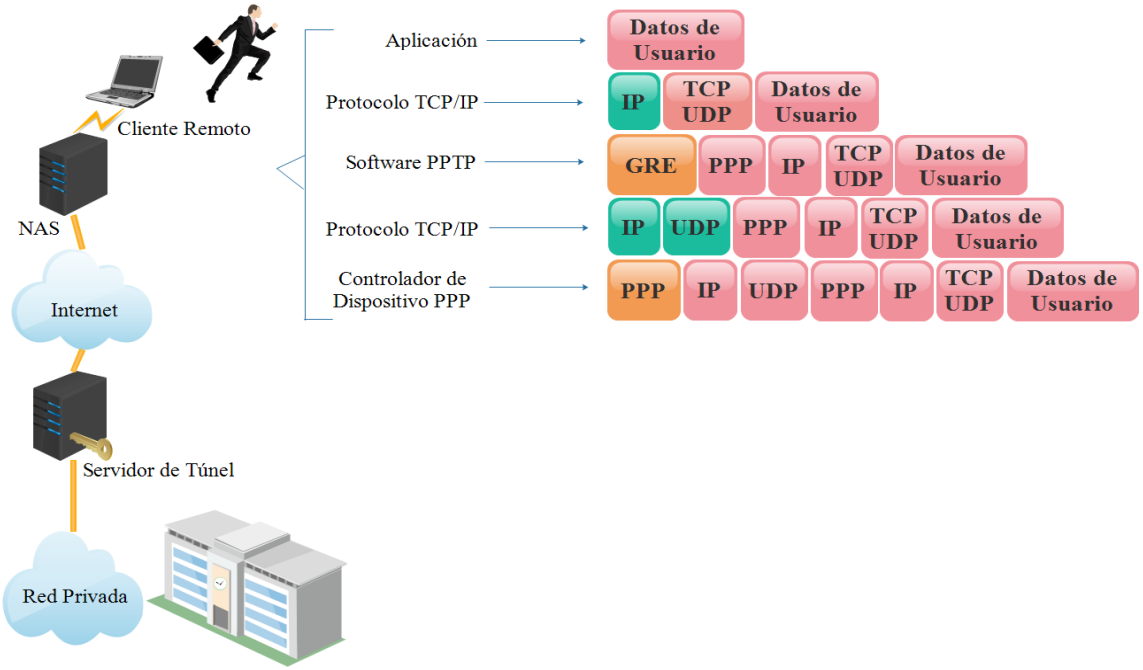


Figura 4-34: Construcción de un paquete PPTP

Fuente: Elaboración propia

Como se puede observar en la figura 4.34, el cliente crea los datos a enviar a los cuales se les asigna una dirección IP privada. Posteriormente, el software PPTP utiliza la cabecera GRE mejorada para permitir el transporte de la cabecera PPP privada y además encapsular el paquete dentro de otra cabecera IP la cual es pública. Finalmente, el controlador PPP añade la cabecera PPP pública la cual permitirá al paquete viajar al otro extremo del túnel. Tratándose de una VPN, la información debe ser cifrada para evitar que sea utilizada por usuarios no autorizados.

Encapsulación Genérica para Ruteo (GRE, Generic Routing Encapsulation). Es un protocolo para encapsular cualquier protocolo de la capa de red dentro de cualquier otro protocolo de la capa de red. El GRE es utilizado normalmente también para servicios VPN. GRE no posee mecanismos de seguridad y debe ser combinado por ejemplo con IPSec para que los datos viajen seguros.

La cabecera GRE utilizada en PPTP, la cual aparece en la figura 4.35, contiene una pequeña mejora que la hace diferente del protocolo GRE original. Esta diferencia consiste en incluir un número de reconocimiento el cual es utilizado para determinar si un paquete o grupo de paquetes GRE en particular ha alcanzado el otro extremo del túnel. Sin embargo, no se utiliza en la retransmisión de paquetes, sino que se utiliza para determinar la frecuencia con que deben ser transmitidos los paquetes a través del túnel para una determinada sesión.

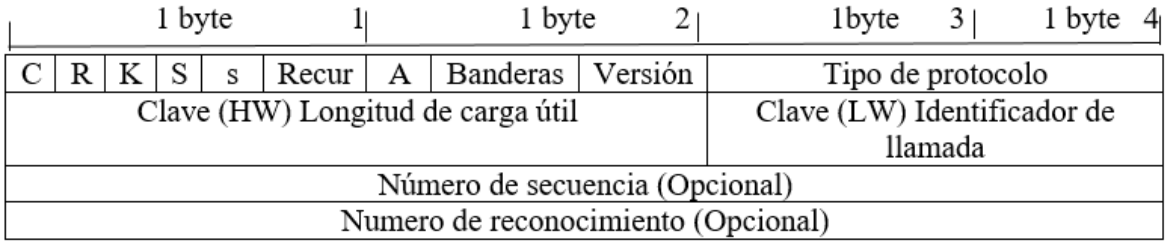


Figura 4-35: Cabecera GRE mejorada
Fuente: Elaboración propia

La cabecera GRE es descrita a continuación:

- C indica chequeo de suma presente. Se establece en 0.
- R indica ruteo presente. Se establece en 0.
- K indica clave presente. Se establece en 1.

- S indica número de secuencia presente. Se establece en 1 si un paquete de datos está presente, de lo contrario se establece en 0.
- s indica ruta de fuente estricta. Se establece en 0.
- Recur indica control de la recursión. Se establece en 0.
- A indica número de secuencia de reconocimiento presente. Se establece en 1 si el paquete contiene número de reconocimiento para ser usado en el reconocimiento de tramas previamente transmitidas.
- Banderas siempre están en 0.
- Versión siempre está en 1.
- Tipo de protocolo se establece en 880B hexadecimal.
- Clave (HW) indica tamaño de la carga útil.
- Clave (LW) contiene el indicador de llamada para la sesión a la cual pertenece el paquete.
- Número de secuencia contiene el número de secuencia de la carga útil. Presente si S está en 1.
- Número de reconocimiento contiene el número del paquete GRE con el número más grande recibido durante la sesión. Presente si A está en 1.

4.5.1.3 **Seguridad en PPTP**

PPTP por sí solo no proporciona ningún mecanismo de seguridad. Si los datos que atraviesan el túnel no son cifrados, cualquier usuario no autorizado puede apropiarse de la información. PPTP requiere de protocolos adicionales para poder autenticar usuarios y encriptar la información.

4.5.1.3.1 **Autenticación y control de acceso**

Un servidor PPTP actúa como una puerta de enlace a una VPN, es decir, se encarga de controlar todo el acceso a una VPN. La autenticación de los clientes remotos PPTP se realiza utilizando los métodos de autenticación de PPP. Como ya se vio anteriormente, los protocolos de autenticación que usa PPP son CHAP, MS-CHAP y PAP. En los sistemas Windows los clientes PPTP deben proporcionar un nombre de usuario y una clave para poder ser autenticados.

En cuanto a las cuentas de los usuarios, éstas son almacenadas en un directorio del servidor Windows y son administradas a través del administrador de usuarios para dominios, lo cual proporciona una administración centralizada. Sólo las cuentas que tienen permiso de acceso a la VPN a través de un dominio confiable son permitidas. Se requiere de una administración muy cuidadosa de las cuentas para reducir lo más posible los riesgos en la seguridad.

Después de la autenticación, todo el acceso a una LAN privada debe seguir un modelo de seguridad estricto. Todo acceso a los recursos de la red debe de tener los permisos apropiados.

Debido a problemas de seguridad que ha tenido PPTP, se ha incluido el uso de EAP para la autenticación. EAP mejora notablemente la seguridad de las VPN basadas en PPTP. Una ventaja de PPTP es que no requiere del uso de una PKI, sin embargo, EAP requiere de certificados digitales para la autenticación mutua y así elevar la seguridad al máximo.

4.5.1.3.2 **Cifrado de datos**

Para el cifrado de los datos, PPTP utiliza un modelo de cifrado simétrico, es decir, se utiliza una clave secreta compartida por ambas partes que se van a comunicar. La clave secreta es la contraseña de usuario. PPTP utiliza los esquemas de compresión y cifrado de PPP. El Protocolo de Control de Compresión (CCP, Compression Control Protocol) es utilizado por PPP para negociar la encriptación. PPTP hace uso del protocolo MPPE para poder cifrar la información.

Cifrado Punto a Punto de Microsoft (MPPE, Microsoft Point-to-Point Encryption). Es un protocolo que cifra los datos de las conexiones PPP de acceso telefónico o de las conexiones VPN basadas en PPTP. Los esquemas de cifrado MPPE compatibles son: de alto nivel (clave de 128 bits) y estándar (clave de 40 bits). MPPE proporciona seguridad a los datos entre la conexión PPTP y el servidor de túnel. Para crear la clave se utiliza el estándar de cifrado RSA RC4. Esta clave es utilizada para encriptar todos los datos que atraviesan Internet, manteniendo la conexión privada y segura.

La versión de 40 bits se puede utilizar en todo el mundo; está integrada en todos los equipos que ejecutan Windows. El nivel de cifrado de 128 bits sólo está disponible en

EE.UU. y Canadá. Es posible habilitar la versión de 128 bits si instala una versión de software específica en el cliente y en el servidor.

En un principio MPPE cambiaba la clave de encriptación cada 256 paquetes o cuando se perdía un paquete. Si el paquete perdido era detectado por el receptor, éste enviaba una solicitud autenticada al emisor para cambiar la clave a fin de resincronizar. Este comportamiento permitía que un intruso emprendiera un ataque de negación de servicio a través de la modificación del contabilizador en un paquete MPPE, o rechazando una petición de resincronización. Para manejar este problema, en PPTP de manera predeterminada las claves MPPE ahora se cambian de manera predeterminada en cada paquete. Este cambio evita el ataque a la resincronización de claves.

4.5.1.3.3 **Filtrado de paquetes PPTP**

El filtrado de paquetes PPTP es una característica muy importante. El administrador de red puede decidir que sólo los usuarios PPTP tengan permiso de conectarse a la red corporativa a través de Internet. Todos los paquetes que no son PPTP son filtrados lo que evita el riesgo de que alguien ataque la VPN a través del servidor PPTP.

Cuando el filtro de paquetes PPTP es activado, el servidor PPTP de la VPN acepta y enruta sólo los paquetes de usuarios autenticados. Esto evita que todos los demás paquetes que no son PPTP puedan ingresar a la VPN. Esto asegura que sólo los datos cifrados autorizados entran y salen de la LAN privada.

4.5.1.3.4 **Utilizar PPTP con firewalls y routers**

El tráfico PPTP utiliza el puerto TCP 1723, y el protocolo IP utiliza el ID 47, de acuerdo a la IANA. PPTP puede ser utilizado en la mayoría de los firewalls y routers al activar el tráfico destinado al puerto 1723 para que sea enrutado a través del firewall o router.

Los firewalls protegen la seguridad de una red empresarial a regular de forma estricta los datos que llegan a la VPN a través de Internet. Una organización puede desplegar un servidor Windows PPTP detrás del firewall. El servidor PPTP acepta los paquetes PPTP que llegan del exterior a través del firewall y extraer la trama PPP del datagrama IP, descifrar el paquete y enviarlo a la computadora destino dentro de la VPN.

4.5.2 Protocolo de Túnel de Capa 2 (L2TP)

4.5.2.1 Reenvío de Capa 2 (L2F)

El protocolo de Reenvío de Capa Dos (L2F, Layer 2 Forwarding) tiene como objetivo proporcionar un mecanismo de tunneling para el transporte de tramas a nivel de enlace de datos del modelo OSI (HDLC, PPP, SLIP, etc). L2F es un protocolo de encapsulamiento creado por Cisco Systems.

Entre las principales ventajas que ofrece el protocolo L2F cabe destacar el soporte multiprotocolo, la multiplexación de múltiples sesiones remotas (minimizando el número de túneles abiertos en un momento dado), y la gestión dinámica de los túneles, en la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario.

Además, por cada túnel L2F establecido, el proceso de seguridad genera una clave aleatoria como medida de prevención ante posibles ataques basados en spoofing. A su vez, en el interior de los túneles, cada una de las sesiones multiplexadas mantendrá un número de secuencia para evitar problemas debidos a la duplicidad de paquetes. L2F sólo puede funcionar en túneles obligatorios.

Este protocolo no fue muy popular y se comenzó entonces a trabajar en un nuevo protocolo que combinara las mejores características de L2F con PPTP. El resultado fue la creación de L2TP.

4.5.2.2 Definición de L2TP

Según (Teltad, 2007) El Protocolo de Túnel de Capa 2 (L2TP, Layer 2 Tunneling Protocol) es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de Internet. Aceptado ya por la mayoría de firmas y vendedores de productos de conectividad, se prevé que en un futuro inmediato constituya una de las funciones más revolucionarias, importantes, y usadas, por todo tipo de redes de datos mundiales en la creación de VPN.

L2TP es un protocolo estándar aprobado por el IETF (Internet Engineering Task Force), en oposición al protocolo propietario de Microsoft PPTP. L2TP se encuentra documentado en el RFC 2661. Es soportado prácticamente por la totalidad de firmas del mercado de la comunicación de datos, incluyendo Microsoft y Cisco. L2TP es una extensión del Protocolo Túnel Punto a Punto usado por los ISP para permitir la operación de VPN sobre

Internet. L2TP emerge de la fusión de las mejores características de los protocolos PPTP de Microsoft y L2F de Cisco. L2TP encapsula las tramas PPP que van a enviarse a través de redes IP, X.25, Frame Relay, o ATM.

Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN en Internet. L2TP utiliza UDP para mantener el túnel y para enviar tramas PPP encapsuladas en L2TP como datos del túnel. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, pueden hacer uso de IPSec, en una configuración denominada L2TP/IPSec, lo cual proporciona gran seguridad cuando se transportan datos en redes públicas IP.

L2TP se diseñó específicamente para conexiones de acceso remoto, así como para conexiones sitio a sitio. Mediante la utilización del protocolo PPP, L2TP gana compatibilidad multiprotocolo para protocolos como IPX y AppleTalk.

L2TP también proporciona una amplia gama de opciones de autenticación de usuario, incluidos CHAP, MS-CHAP, MS-CHAPv2 y EAP que admite mecanismos de autenticación de tarjetas token y tarjetas inteligentes. L2TP requiere preferentemente del uso de certificados digitales para la autenticación. L2TP es soportado por diferentes sistemas operativos, así como routers y firewalls.

4.5.2.3 **Estructura de L2TP**

4.5.2.3.1 **Concentrador de Acceso L2TP (LAC)**

Es un nodo que actúa en un extremo del túnel L2TP y trabajo junto con el LNS. El envío de paquetes entre el LAC y el LNS requiere de la creación de un túnel utilizando el protocolo L2TP. La conexión del LAC al sistema remoto puede ser local o a través de un enlace PPP.

El LAC es un dispositivo físico que se añade a los elementos de interconexión de la red conmutada; como lo es la red telefónica convencional RDSI, o se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP. Un LAC sólo necesita implementar el medio sobre el cual opera el L2TP para admitir el tráfico de una o más LNS. El LAC puede entunelar cualquier protocolo que incluya el PPP, además, es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. Un servidor de Acceso a la Red (NAS) es un LAC.

4.5.2.3.2 **Servidor de Red L2TP (LNS)**

Un LNS opera sobre cualquier plataforma con capacidad de terminación PPP. El LNS gestiona el lado del servidor del protocolo L2TP. Ya que L2TP se apoya sobre el medio al que llegan los túneles L2TP, LNS sólo puede tener una única interfaz LAN o WAN, aunque es capaz de terminar las llamadas entrantes en cualquiera de la amplia gama de las interfaces PPP LAC (asíncronos, RDSI, PPP sobre ATM, PPP sobre Frame Relay)

4.5.2.3.3 **Topología L2TP**

El objetivo de L2TP es entunelar tramas PPP entre el sistema remoto o cliente LAC y el LNS ubicado en una LAN privada. La topología típica de L2TP se muestra en la figura 4.36.

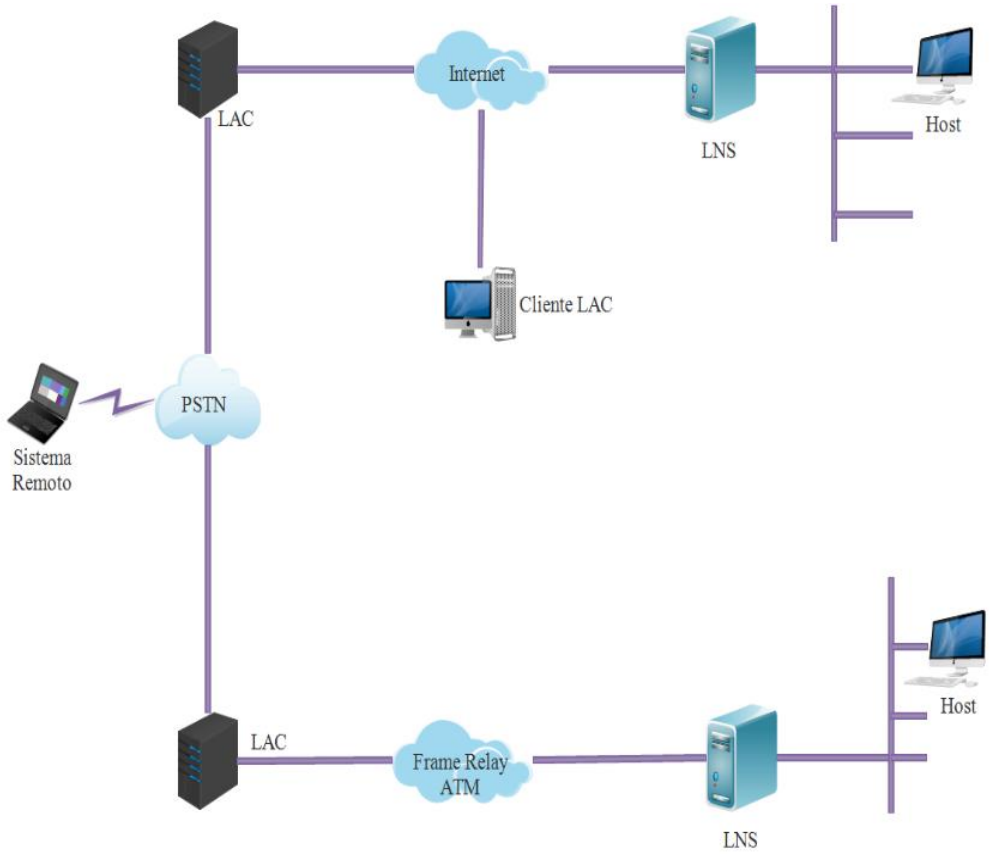


Figura 4-36: Topología de L2TP
Fuente: Elaboración propia

El sistema remoto inicia una conexión PPP a través de la nube PSTN hacia el LAC. Entonces, el LAC entunela la conexión PPP a través de Internet, Frame Relay o ATM hacia un LNS donde podrá tener acceso a una LAN privada. La autenticación, autorización y contabilidad son provistas por la LAN privada como si el usuario estuviera conectado a un NAS directamente.

Un cliente LAC (el cual es una computadora que ejecuta L2TP de forma nativa) participa en el tunneling hacia la red privada sin necesidad de usar un LAC separado. En este caso, el host que contiene el software L2TP cliente ya posee una conexión a Internet. Una conexión virtual PPP es creada entonces y el cliente LAC crea un túnel con el LNS o servidor L2TP. La autenticación, autorización y contabilidad son provistas por la LAN privada.

4.5.2.3.4 **Mensajes de control y de datos**

L2TP utiliza dos tipos de mensajes, mensajes de control y mensajes de datos. Los mensajes de control son utilizados para establecer, mantener y limpiar los túneles y las llamadas. Los mensajes de datos son utilizados para encapsular las tramas PPP que son transportadas a través del túnel. Los mensajes de control utilizan un canal de control confiable dentro de L2TP para garantizar el envío de la información. Los mensajes de datos, por el contrario, no son retransmitidos cuando ocurren pérdidas en los paquetes.

Figura 4-37: Estructura de mensajes L2TP
Fuente: Elaboración propia

En la figura 4.37 se puede observar la relación entre las tramas PPP y los mensajes de control sobre el control L2TP y los canales de datos. Las tramas PPP son transportadas sobre un canal de datos no confiable encapsulado primeramente por una cabecera L2TP y después por un medio de transporte como puede ser UDP, ATM o Frame Relay.

Los mensajes de control son enviados sobre un canal de control L2TP confiable el cual transmite los paquetes en el mismo medio de transporte que utilizan los mensajes de datos. Tanto los mensajes de datos como los de control comparten el mismo formato de la cabecera.

L2TP utiliza varios mensajes de control, los cuales se muestran en la tabla 4.7.

Código	Nombre	Descripción
0	(Reservado)	
1	Start-Control-Connection-Request (SCCRQ)	Inicia el establecimiento de la sesión L2TP y el proceso de autenticación del túnel
2	Start-Control-Connection-Reply (SCCRP)	Es la respuesta al mensaje 1. Indica el éxito o el fracaso del establecimiento de la sesión, así como la respuesta a la autenticación
3	Start-Control-Connection-Connected (SCCCN)	Es la respuesta al mensaje 2
4	Stop-Control-Connection-Notification (StopCCN)	Notifica el fin del túnel
5	(Reservado)	
6	Hello	Enviado periódicamente tanto por el cliente como por el servidor para mantener activa la conexión
7	Outgoing-Call-Request (OCRQ)	Es una petición enviada por el cliente para crear un túnel
8	Outgoing-Call-Reply (OCRP)	Es la respuesta al mensaje 7, la cual contiene un identificador único para ese túnel
9	Outgoing-Call-Connected (OCCN)	Es la respuesta al mensaje 8. Provee parámetros de llamada adicionales al servidor
10	Incoming-Call-Request (ICRQ)	Es una petición del cliente para recibir una llamada entrante por parte del servidor
11	Incoming-Call-Reply (ICRP)	Es la respuesta al mensaje 10. Esta indica si la llamada entrante debería ser contestada
12	Incoming-Call-Connected (ICCN)	Es la respuesta al mensaje 11. Provee parámetros de llamada adicionales al servidor
13	(Reservado)	
14	Call-Disconnect-Notify (CDN)	Notifica el fin de una sesión L2TP
15	WAN-Error-Notify (WEN)	Notifica que un error ha ocurrido en la conexión WAN, esto es, en la interfase que soporta PPP
16	Set-Link-Info (SLI)	Notifica cambios en las opciones PPP

Tabla 4-7: Mensajes de control en L2TP
Fuente: Elaboración propia

Formato de la cabecera L2TP. Los paquetes L2TP tanto de control como de datos comparten un mismo formato de la cabecera, el cual se muestra en la figura 4.38.

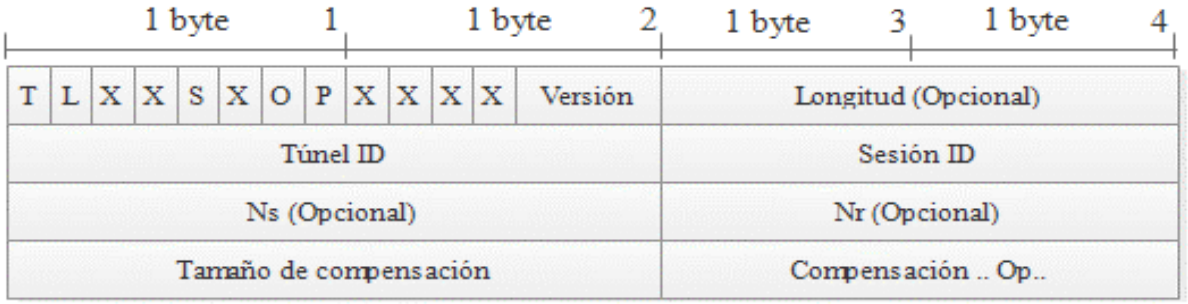


Figura 4-38: Formato de la cabecera L2TP
Fuente: Elaboración propia

- El bit T (tipo) indica el tipo de mensaje. Se establece en 0 si es de datos o 1 si es de control.
- Cuando está en 1 el campo Longitud (L) existe. En un mensaje de control L siempre está en 1.
- Los bits x están reservados para extensiones futuras. Permanecen en 0.
- Si el bit S (secuencia) está en 1 los campos Ns y Nr existen. En un mensaje de control S siempre es 1.
- Si el bit O (compensación) está en 1, el campo Tamaño de compensación existe. En un mensaje de control O siempre es 0.
- Si el bit P (prioridad) está en 1, este mensaje tiene prioridad durante latransmisión.
- El campo Versión indica la versión de la cabecera del mensaje L2TP.
- El campo Longitud indica la longitud del mensaje en octetos
- El túnel ID indica el identificador para la conexión de control. Los túneles L2TP son identificados con este campo.
- La Sesión ID indica el identificador para una sesión dentro de un túnel.
- Ns indica el número de secuencia para el mensaje. Inicia en 0 y cada mensaje enviado incrementa el número de secuencia.
- Nr indica el número de secuencia esperado en el siguiente mensaje.

- La compensación de relleno especifica el número de octetos después de la cabecera antes del inicio de los datos.

4.5.2.3.5 **Túneles en L2TP**

L2TP puede ser utilizado como protocolo de túnel en una red IP como Internet. Para el mantenimiento del túnel, L2TP sobre redes IP utiliza UDP y una serie de mensajes L2TP. Al igual que los datos entunelados, L2TP también utiliza UDP para enviar tramas PPP encapsuladas.

La carga útil de las tramas PPP encapsuladas puede ser comprimida al igual que cifradas. L2TP usa el puerto UDP 1701. El ensamblado de un paquete L2TP al momento de su transmisión se muestra en la figura 4.39.

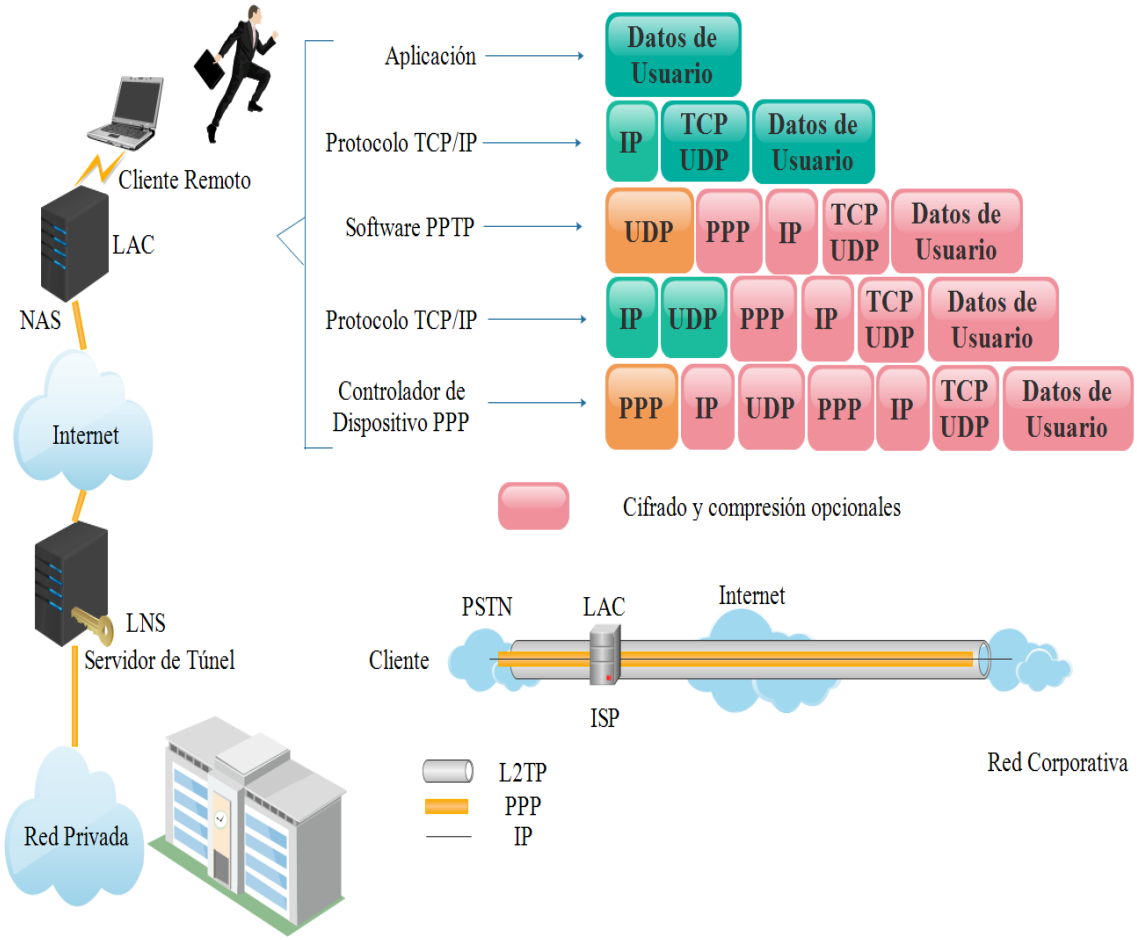


Figura 4-39: Construcción de un paquete L2TP
Fuente: Elaboración propia

4.5.2.4 **Funcionamiento de L2TP**

El túnel y su correspondiente conexión de control deben ser establecidas antes de que se inicien las llamadas entrantes o salientes. Una sesión L2TP debe ser establecida antes de que L2TP comience a entunelar tramas PPP. Sesiones múltiples pueden existir a través de un único túnel y múltiples túneles pueden existir entre el mismo LAC y LNS.

La operación del protocolo L2TP se lleva a cabo de la siguiente manera y se muestra en la figura 4.40.

1. Se establece la conexión de control inicial entre el LAC y el LNS intercambiando los mensajes SCCRQ, SCCRP y SCCCN.
2. Se lleva a cabo la autenticación del túnel utilizando CHAP para ello.
3. Después de que se establece la conexión de control, se crean sesiones individuales. Cada sesión corresponde a un único flujo de tramas PPP entre el LAC y el LNS. Se intercambian los mensajes ICRQ, ICRP, ICCN para llamadas entrantes y OCRQ, OCRP Y OCCN para llamadas salientes.
4. Una vez que se establece el túnel, las tramas PPP del sistema remoto son recibidas por el LAC, encapsuladas en L2TP y enviadas por el túnel apropiado. El LNS recibe el paquete y desencapsula la trama PPP.
5. Se utilizan números de secuencia con el fin de identificar los mensajes para mantener un transporte confiable de éstos.
6. Se emplea el mensaje Hello para mantener activa la conexión.
7. Para finalizar la sesión, o el LAC o el LNS envían un mensaje CDN.
8. Para finalizar la conexión de control, o el LAC o el LNS envían un mensaje StopCCN.

Se usa un mensaje ZLB ACK para indicar que ya no hay más mensajes que transmitir entre el par LAC-LNS.

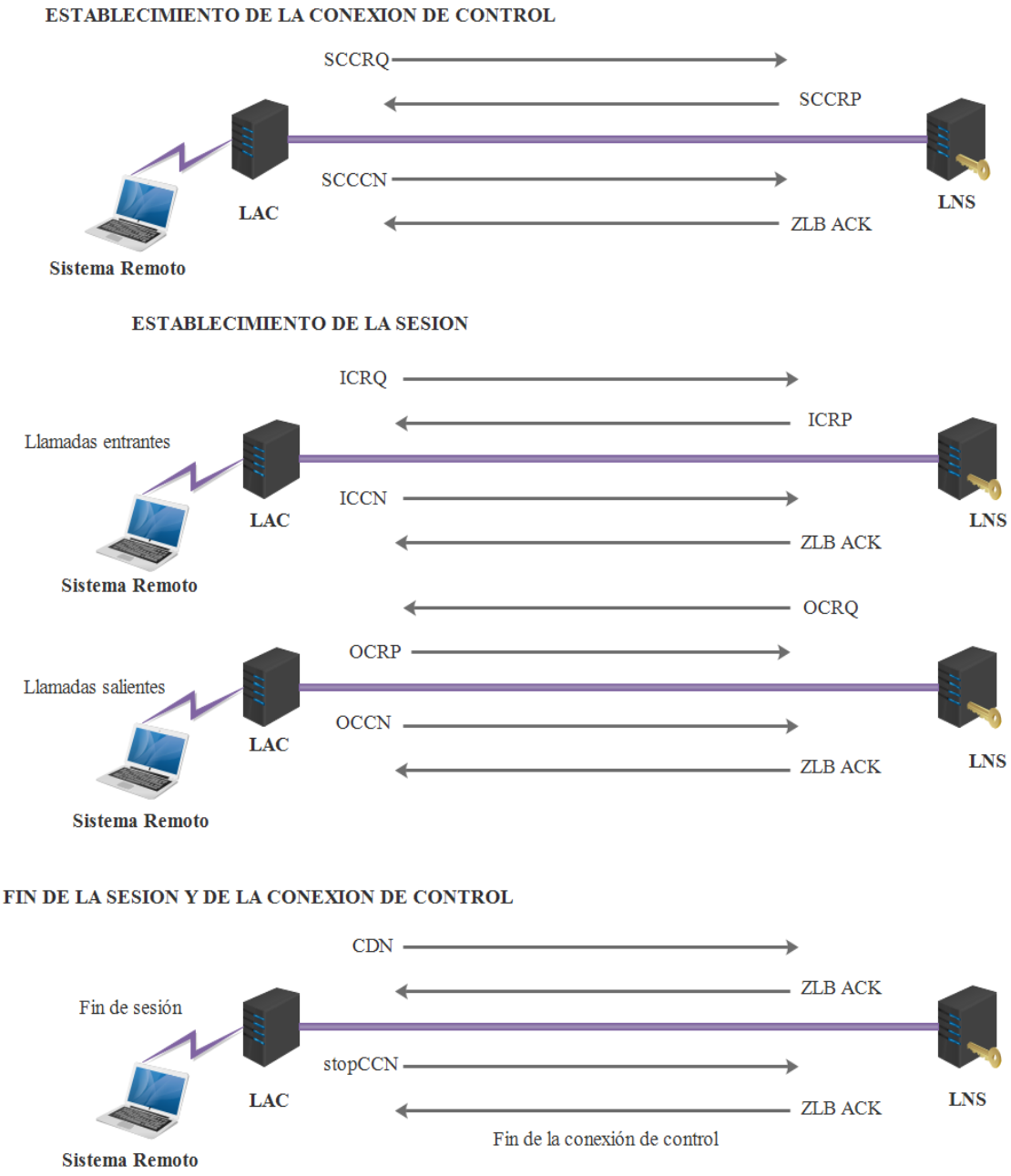


Figura 4-40: Funcionamiento de L2TP
Fuente: Elaboración propia

Para establecer una conexión entre un usuario remoto, un dispositivo LAC ubicado en el punto de presencia (POP) del ISP, y el LNS en la LAN destino usando un túnel L2TP se siguen los siguientes pasos descritos en la figura 4.41 y explicados posteriormente.

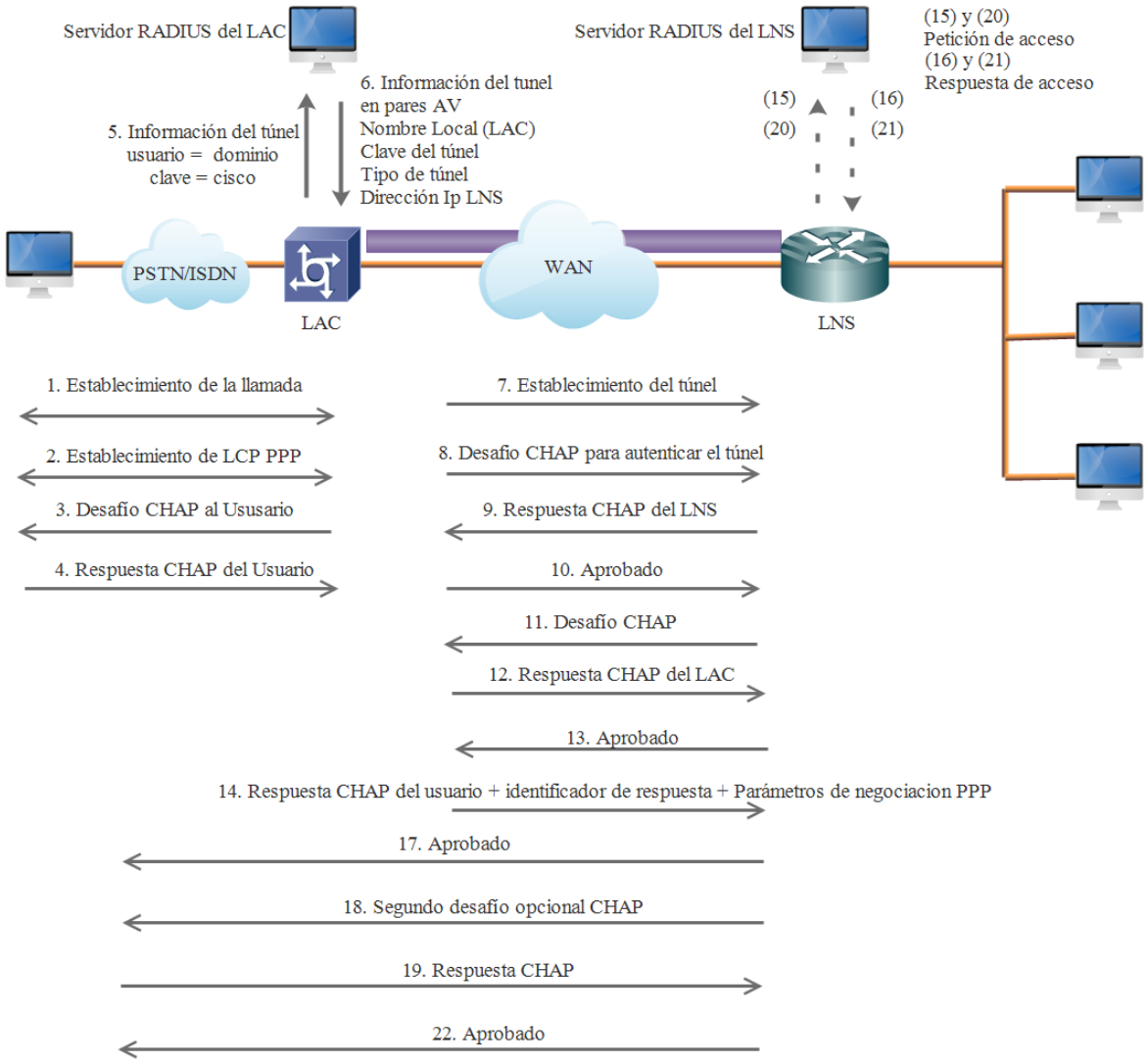


Figura 4-41: Establecimiento de una conexión L2TP
Fuente: Elaboración propia

1. El usuario remoto inicia una conexión PPP con el ISP, utilizando la red telefónica analógica o ISDN.
2. El LAC de la red del ISP acepta la conexión en el POP y se establece el vínculo PPP.
3. Después de que el usuario final y el LNS negocian LCP, el LAC autentica parcialmente al usuario final con PAP o CHAP. El nombre de usuario o nombre de dominio es utilizado para determinar si el usuario es cliente de la VPN.

4. Los extremos del túnel (LAC y LNS), se autentican mutuamente antes de que comience cualquier sesión dentro del túnel.
5. Una vez que el túnel existe, se crea una sesión L2TP para el usuario final.
6. El LAC propagará las opciones LCP negociadas y la información CHAP/PAP al LNS y establecerá la conexión.

4.5.2.5 **Seguridad en L2TP**

4.5.2.5.1 **Seguridad en los extremos del túnel**

Los extremos del túnel pueden opcionalmente ejecutar un procedimiento de autenticación durante el establecimiento del túnel. Esta autenticación tiene los mismos atributos de seguridad como CHAP y tiene protección razonable contra los ataques de repetición durante el proceso de establecimiento del túnel. Sin embargo, este mecanismo no está designado para proveer autenticación más allá del establecimiento del túnel. Para que exista la autenticación, tanto el LAC como el LNS comparten una misma clave.

4.5.2.5.2 **Seguridad a nivel paquete**

Para asegurar L2TP se requiere que el transporte proporcione servicios de encriptación, seguridad y autenticación para todo el tráfico L2TP. Este transporte seguro opera sobre el paquete L2TP completo y funciona independientemente de PPP y del protocolo que este siendo transportando por PPP. L2TP sólo se preocupa de la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los extremos del túnel (LAC y LNS).

4.5.2.5.3 **L2TP/IPSec**

Cuando L2TP opera sobre redes IP, el mejor método de proporcionar seguridad es utilizando IPSec en combinación con L2TP. IPSec provee seguridad a nivel paquete utilizando ya sea ESP, AH o ambos. Todos los datos L2TP de un túnel en particular aparecen como paquetes de datos UDP/IP para el sistema IPSec. L2TP se utiliza para enviar los datos por un túnel a través de una red compartida o pública como Internet, y ESP de IPSec para cifrar los datos.

Además de garantizar seguridad en el transporte de paquetes IP, IPSec define un modo de operación que permite entunelar paquetes IP. La autenticación y cifrado a nivel

paquete proporcionados por IPSec modo túnel y el proporcionado por L2TP/IPSec otorgan un nivel equivalente de seguridad tal como lo requiere una VPN.

IPSec también define características de control de acceso que son requeridas para una implementación de seguridad completa. Estas características permiten el filtrado de paquetes basado en las características de la capa de red y de transporte tales como dirección IP, puertos, etc. En el modelo de tunneling L2TP, un filtrado análogo es ejecutado lógicamente a nivel PPP o en la capa de red sobre L2TP.

Crear VPN de acceso remoto con L2TP/IPSec. Un requisito habitual es proteger las comunicaciones entre los clientes de acceso remoto y la red empresarial a través de Internet. Puede ser el caso de un consultor de ventas que pasa la mayor parte del tiempo de viaje o un empleado que trabaja desde casa.

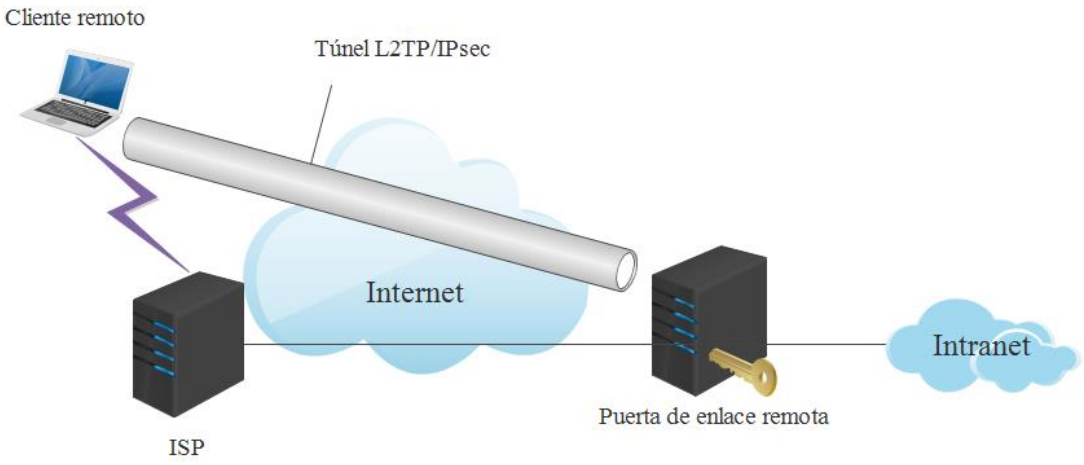


Figura 4-42: VPN de acceso remoto con L2TP/IPSec
Fuente: Elaboración propia

En la figura 4.42, la puerta de enlace remota es un servidor que proporciona alta seguridad para la intranet de la empresa. El cliente remoto representa un usuario itinerante que precisa obtener acceso frecuente a los recursos y la información de la red. En el ejemplo se utiliza un ISP para ilustrar la ruta de comunicación cuando el cliente utiliza un ISP para el acceso a Internet. L2TP se combina con IPSec para proporcionar un modo sencillo y eficaz de construir el túnel y proteger la información a través de Internet.

Crear VPN sitio a sitio con L2TP/IPSec. Una gran empresa a menudo dispondrá de varios sitios que precisan comunicarse, por ejemplo, una oficina corporativa en Nueva

York y una oficina de ventas en Washington. En este caso, L2TP se combina con IPSec para proporcionar la conexión VPN y proteger la información entre los distintos sitios.

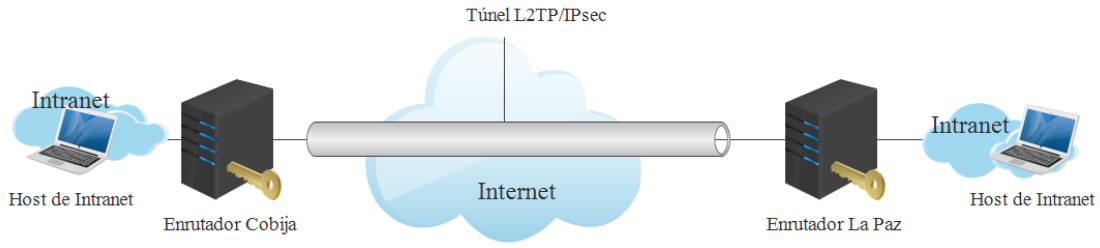


Figura 4-43: VPN de sitio a sitio con L2TP/IPSec
Fuente: Elaboración propia

En la figura 4.43, los routers VPN se encargan de la seguridad exterior. Es posible que los routers utilicen una línea alquilada, acceso telefónico u otro tipo de conexión a Internet. La SA de IPSec y el túnel L2TP se establecen entre los routers, y permiten la comunicación segura a través de Internet.

4.5.3 Seguridad IP (IPSec)

4.5.3.1 Definición de IPSec

Según (James S. Tiller, 2001)La Seguridad del Protocolo de Internet (IPSec, Internet Protocol Security) es un marco de estándares abiertos para lograr comunicaciones privadas seguras a través de redes IP mediante el uso de servicios de seguridad criptográfica. IPSec es la tendencia a largo plazo para las redes seguras. Proporciona una sólida protección contra ataques a redes privadas e Internet mediante la seguridad de extremo a extremo. Los únicos equipos que deben conocer que existe protección con IPSec son el remitente y el receptor de la comunicación. IPSec tiene dos objetivos:

- Proteger el contenido de los paquetes IP.
- Defender contra los ataques de red mediante el filtrado de paquetes y la exigencia de comunicaciones de confianza.

Ambos objetivos se alcanzan gracias al uso de servicios de protección criptográfica, protocolos de seguridad y administración dinámica de claves. Estos fundamentos proporcionan al mismo tiempo la capacidad y la flexibilidad para proteger las

comunicaciones entre equipos de redes privadas, dominios, sitios, sitios remotos, extranets y clientes de acceso telefónico. Incluso pueden utilizarse para bloquear la recepción o la transmisión de determinados tipos de tráfico.

IPSec se basa en un modelo de seguridad completo, y establece la confianza y la seguridad desde una dirección IP de origen hasta una dirección IP de destino. La dirección IP en sí no se considera necesariamente una identidad, sino que el sistema que hay tras la dirección IP tiene una identidad que se valida a través de un proceso de autenticación. Los únicos equipos que deben conocer que el tráfico está protegido son los equipos remitente y receptor.

Cada equipo trata la seguridad en su extremo respectivo y supone que el medio a través del cual tiene lugar la comunicación no es seguro. Los equipos que se limitan a enrutar datos desde el origen hasta el destino no necesitan ser compatibles con IPSec, salvo en el caso de que se filtren paquetes de tipo servidor de seguridad o se traduzcan direcciones de red entre los dos equipos. Este modelo permite implementar correctamente IPSec en los siguientes casos:

- Red de área local (LAN): cliente-servidor y entre homólogos
- Red de área extensa (WAN): entre routers y entre puertas de enlace
- Acceso remoto: clientes de acceso telefónico y acceso a Internet desde redes privadas

IPSec se basa en los estándares desarrollados por el grupo de trabajo de IPSec del IETF. IPSec se encuentra documentado en diversos RFC de los cuales el principal es el RFC 2401.

IPSec utiliza dos protocolos que proporcionan seguridad en el tráfico. Estos protocolos son:

- Cabecera de autenticación (AH, Authentication Header)
- Carga de Seguridad de Encapsulamiento (ESP, Encapsulating Security Protocol)

AH proporciona integridad en la conexión, autenticación de los datos de origen y un servicio opcional contra paquetes repetidos. ESP provee confidencialidad de los datos utilizando técnicas de encriptación. Opcionalmente puede proporcionar también autenticación, integridad y protección contra paquetes repetidos. Ambos protocolos son vehículos para el control de acceso, basado en la distribución de claves criptográficas y la administración de los flujos de tráfico relativos a estos protocolos de seguridad.

Cada protocolo soporta dos modos de uso: modo transporte y modo túnel. En el modo transporte los AH y ESP proveen protección a los protocolos de capas superiores. En el modo túnel AH y ESP son aplicados para entunelar paquetes IP.

También se utiliza un conjunto protocolos necesarios para la gestión de llaves criptográficas. La Asociación de Seguridad (SA), utilizada para llevar a cabo la autenticación, representa una conexión unidireccional para la cual se definen todos los servicios de seguridad que deben ser aplicados al tráfico de red. Las SA pueden ser creadas tanto automáticamente como manualmente, empleando para ello el protocolo ISAKMP/Oakley.

4.5.3.2 **Protocolos de IPSec**

4.5.3.2.1 **Cabecera de Autenticación (AH)**

La cabecera de autenticación (AH, Authentication Header) puede detectar paquetes alterados y puede autenticar la identidad del emisor basándose en el usuario final o en la dirección IP fuente. Las partes que se comunican en IPSec usando AH pueden utilizar diferentes algoritmos ya sea MD5 o SHA-1 con el fin de crear una firma hash utilizando un componente secreto de la SA, la carga útil del paquete y varias partes de la cabecera del paquete.

Contenido del paquete AH. La cabecera AH contiene esencialmente cinco campos los cuales se muestran a continuación en la figura 4.44.

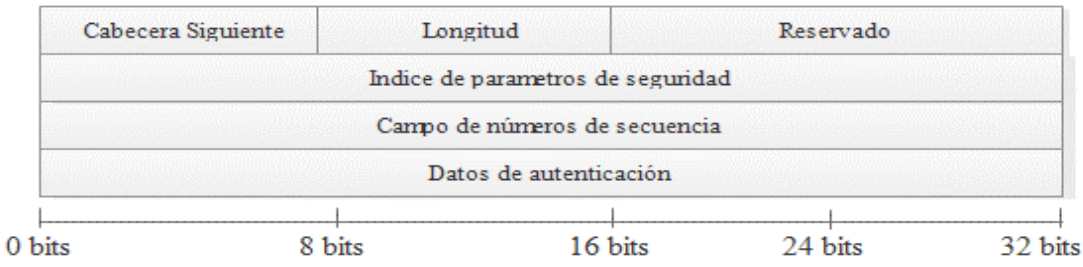


Figura 4-44: Contenido del paquete AH
Fuente: Elaboración propia

- La cabecera siguiente describe la cabecera de la capa 4 (TCP, UDP, ICMP) para un datagrama IPv4 (8 bits)
- La longitud de la firma hash (8 bits)
- El Índice de Parámetro de Seguridad (SPI) (32 bits)
- El campo de número de secuencia antirepetición, el cual evita los ataques de repetición (32 bits)
- La firma hash propiamente dicha (32 bits)

AH en modo transporte. En el modo transporte (Ver figura 4.45), los servicios AH protegen la cabecera IP externa junto con la carga útil de datos. Los servicios AH protegen todos los campos en la cabecera que no cambia durante el transporte. AH se coloca después de la cabecera IP y antes de la cabecera ESP si está presente, y antes de los protocolos de capas superiores.

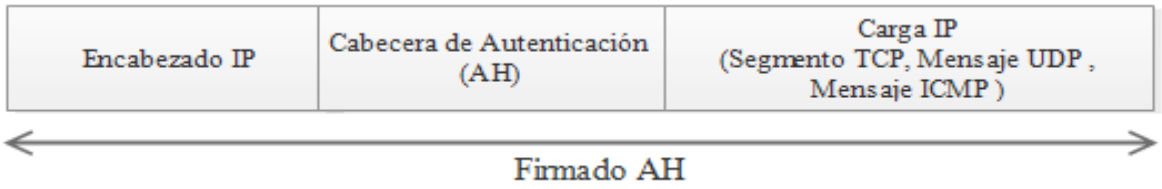


Figura 4-45: AH en modo transporte
Fuente: Elaboración propia

AH en modo túnel. En el modo túnel (Ver figura 4.46), la cabecera original entera es autenticada, se construye una cabecera IP nueva y la nueva cabecera IP es protegida de la misma manera que en el modo transporte.

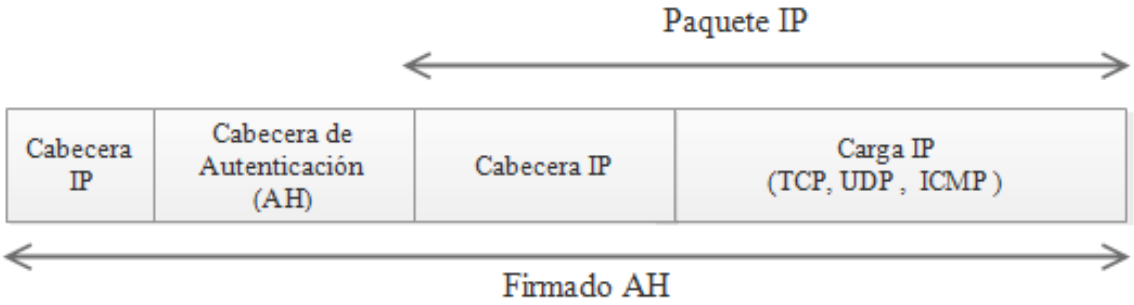


Figura 4-46: AH en modo túnel
Fuente: Elaboración propia

4.5.3.2.2 **Carga de Seguridad de Encapsulación (ESP)**

La Carga de Seguridad de Encapsulamiento (ESP, Encapsulating Security Protocol) puede proporcionar servicios de confidencialidad, autenticidad e integridad. El modo túnel ESP también ofrece confidencialidad en el flujo del tráfico. Las primeras versiones de ESP se enfocaron principalmente en la confidencialidad; sin embargo, el estándar final también incluye una gran funcionalidad como la que proporciona AH. Los estándares ESP soportan principalmente dos métodos de cifrado DES y 3DES.

Contenido del paquete ESP. Al igual que AH, la cabecera ESP contiene lo siguiente, como se muestra en la figura 4.47.

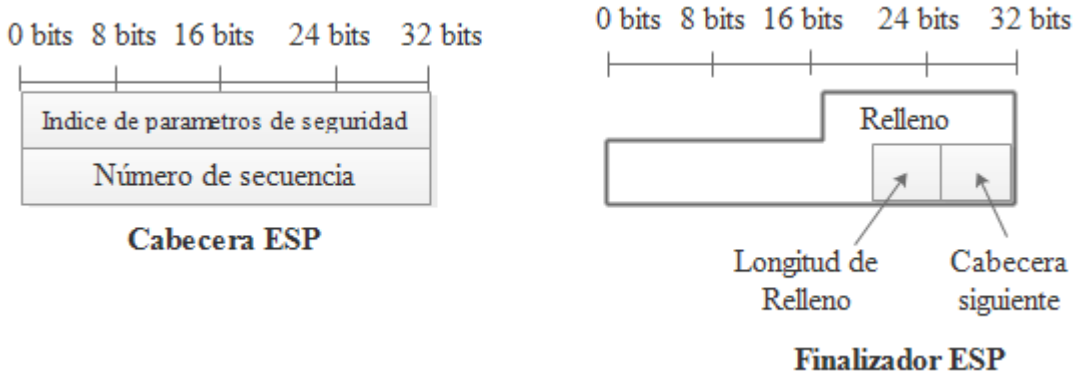


Figura 4-47: Contenido del paquete ESP
Fuente: Elaboración propia

- Índice de Parámetro de Seguridad (SPI) (32 bits)
- El campo de número de secuencia antirepetición (32 bits)
- Longitud de relleno (8 bits)
- Cabecera siguiente (8 bits)
- Relleno (0-255 bits)

A diferencia de AH, ESP también incluye el campo cabecera siguiente como una parte del finalizador del paquete. La carga del paquete debe incluir relleno para que pueda operar el algoritmo de cifrado. El finalizador también debe contener un monto variable de datos de autenticación.

ESP en modo transporte. En el modo transporte (Ver figura 4.48), la carga IP es cifrada y las cabeceras originales se dejan intactas. La cabecera ESP es insertada después de

la cabecera IP y antes de la cabecera del protocolo de capa superior. Los protocolos de capa superior son cifrados y autenticados utilizando la cabecera ESP. ESP no autentica la cabecera IP. También hay que notar que la información de capas superiores no está disponible debido a que pertenece a la carga cifrada.

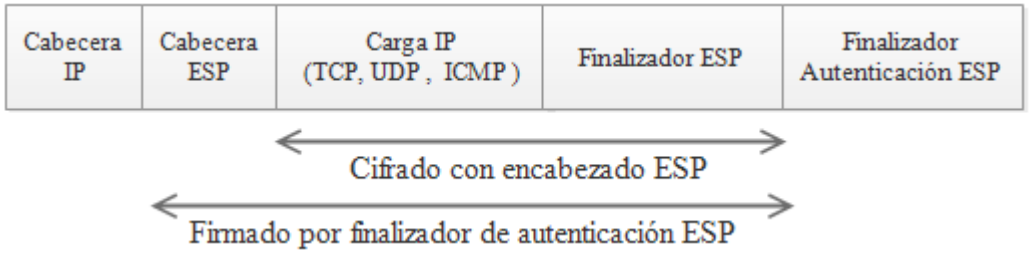


Figura 4-48: ESP en modo transporte
Fuente: Elaboración propia

ESP en modo túnel. En el modo túnel (Ver figura 4.49), la cabecera IP original se encuentra bien protegida debido a que el datagrama original IP completo se encuentra cifrado. Con el mecanismo de autenticación ESP, el datagrama IP original y la cabecera ESP son incluidas. Se construye una nueva cabecera IP, sin embargo, ésta no es incluida en la autenticación.

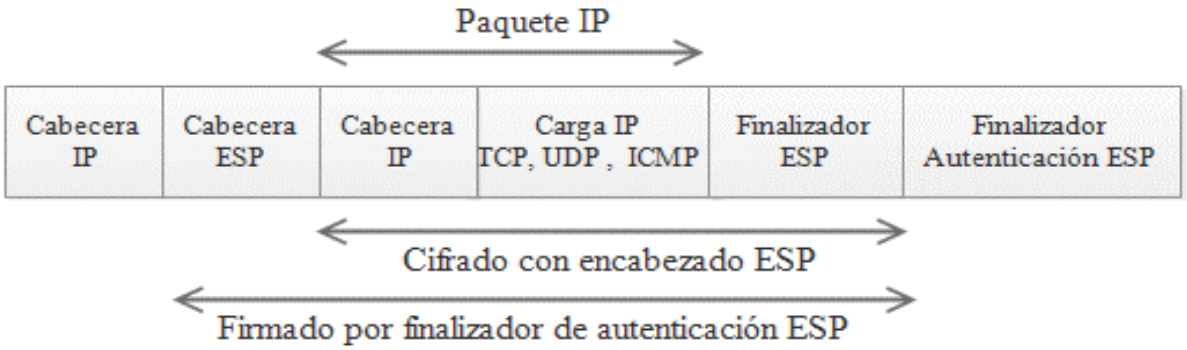


Figura 4-49: ESP en modo túnel
Fuente: Elaboración propia

4.5.3.3 **Asociaciones de Seguridad (SA)**

El concepto de Asociación de Seguridad (SA, Security Association) es fundamental en la arquitectura IPSec. Una SA es una conexión que permite servicios de seguridad para el tráfico transportado por ésta, dicho en otra forma, una SA es un acuerdo entre ambas partes acerca de cómo cifrar y descifrar los datos que se van a transmitir. Los servicios de seguridad son proporcionados a una SA utilizando AH o ESP, pero no ambos.

Si ambos protocolos son aplicados a influjo de datos determinado, entonces dos o más SA son creadas para dar protección a dicho flujo. Para asegurar una típica comunicación bidireccional entre dos hosts, o entre dos gateways de seguridad, dos SA (una en cada dirección) son requeridas.

Una SA es identificada de forma única por medio de valores diferentes tales como un Índice de Parámetro de Seguridad (SPI, Security Parameter Index), una dirección IP destino y un identificador del protocolo de seguridad (AH o ESP). Los estándares definen un riguroso mecanismo para asegurar que cada SA es única. Los dispositivos IPSec almacenan estas SA en una Base de Datos SA (SAD, SA Database). Un ejemplo de estos valores se muestra en la figura 4.50.

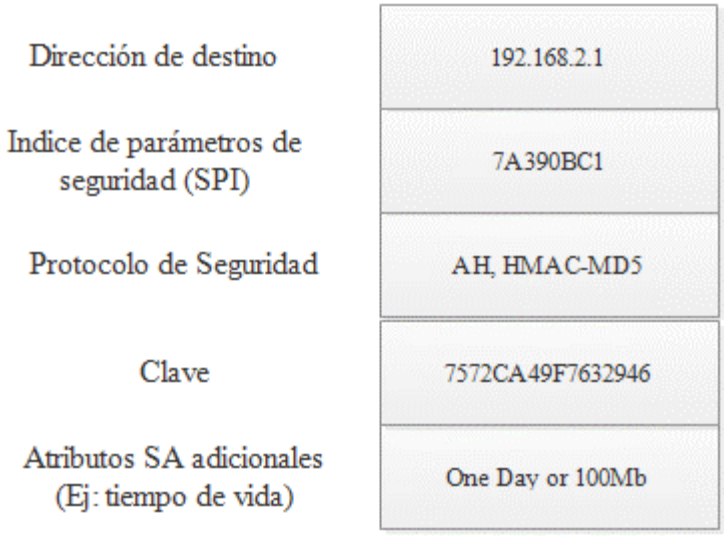


Figura 4-50: Asociación de Seguridad (SA)
Fuente: Elaboración propia

4.5.3.4 **Administración de claves en IPSec**

4.5.3.4.1 **Los protocolos ISAKMP/Oakley e IKE**

Puesto que IPSec es una arquitectura abierta, los protocolos de seguridad (AH y ESP) están diseñados para ser independientes con respecto a la administración de claves cifradas de forma automática. Sin embargo, las implementaciones de IPSec que cumplan con los estándares deben soportar tanto el uso de claves previamente compartidas como el mecanismo de administración de claves automatizado conocido como Intercambio de claves de Internet (IKE, Internet Key Exchange).

IKE es un diseño específico dentro de un sistema mayor conocido como Protocolo de Administración de Claves y Asociación de Seguridad de Internet (ISAKMP, Internet Security Association and Key Management Protocol). ISAKMP es un sistema de intercambio de claves y autenticación que es independiente de cualquier tecnología de claves específica. IKE trabaja con otro protocolo llamado Oakley, para el intercambio de claves seguro dentro del modelo ISAKMP.

ISAKMP/Oakley proporciona un mecanismo que permite a servidores VPN separados compartir información de claves de encriptación y hace que IPSec sea práctico en el entorno actual.

4.5.3.4.2 **Protocolo Oakley**

Oakley es un protocolo que utiliza un intercambio de claves Diffie-Hellman para establecer una clave compartida de forma segura entre las dos partes que se comunican. Oakley trabaja dentro del marco ISAKMP para establecer las SA de IPSec. El estándar de determinación de clave Oakley establece una SA de ISAKMP inicial, pero permite un mecanismo más ligero para permitir SA subsecuentes.

4.5.3.4.3 **Intercambio de Claves de Internet (IKE)**

El protocolo de Intercambio de claves de Internet (IKE) pertenece al conjunto ISAKMP/Oakley. Es un protocolo de administración de claves seguro diseñado para establecer las SA de IPSec y para permitir una rápida reasignación de claves para las SA existentes. IKE opera en dos fases, las cuales se describen a continuación.

Fase 1 de IKE. El objetivo básico de la fase 1 de IKE es autenticar ambas partes de IPSec. Durante esta fase se llevan a cabo las siguientes funciones:

- Identificar y proteger las identidades de ambas partes de IPSec
- Negociar una póliza SA de ISAKMP entre ambas partes para proteger el intercambio de IKE
- Ejecutar un intercambio Diffie-Hellman autenticado con el resultado final de tener claves secretas compartidas.
- Establecer un túnel seguro para negociar los parámetros de la fase 2 de IKE

Fase 2 de IKE. El propósito de la fase 2 de IKE es negociar las SA de IPSec para establecer el túnel IPSec. La fase 2 de IKE lleva a cabo las siguientes funciones como también se ve en la figura 4.51.

- Negociar los parámetros SA de IPSec protegidos por una SA de ISAKMP existente.
- Establece SA de IPSec
- Periódicamente renegocia las SA de IPSec para garantizar la seguridad
- Ejecuta opcionalmente un intercambio Diffie-Hellman adicional

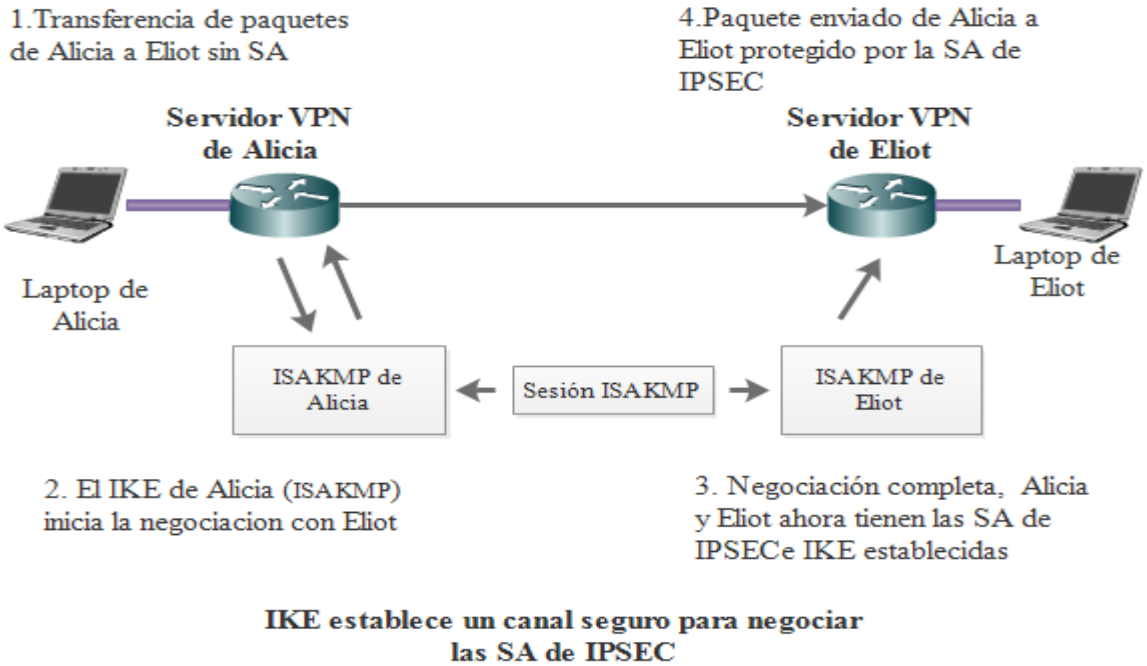


Figura 4-51: Funcionamiento de IKE
Fuente: Elaboración propia

4.5.3.5 **Funcionamiento de IPSec**

IPSec es una tecnología que envuelve muchos componentes tecnológicos y métodos de encriptación. Así pues, la operación de IPSec se puede descomponer en cinco pasos principales que se explican a continuación y que aparecen en la figura 4.52.

1. En este primer paso se determina el tráfico inicial IPSec. Determinar este tráfico inicial es parte de la formulación de una póliza de seguridad para

usar en una VPN. Esta póliza es implementada en ambas partes que se comunican.

2. El segundo paso consiste en ejecutar la Fase 1 de IKE, donde se autentican ambos extremos.
3. El tercer paso consiste en ejecutar la Fase 2 de IKE, donde se establecen las SA para crear el túnel.
4. El cuarto paso es donde se lleva a cabo la transferencia de datos por el túnel IPSec. Los paquetes son cifrados y descifrados de acuerdo con el método especificado en la SA de Ipsec.
5. El último paso consiste en la terminación del túnel IPSec, donde las SA expiran y se deben negociar nuevas SA para continuar transmitiendo datos. Entonces se regresa a la Fase 2 o a la Fase 1. Esto resulta en nuevas SA y nuevas claves.

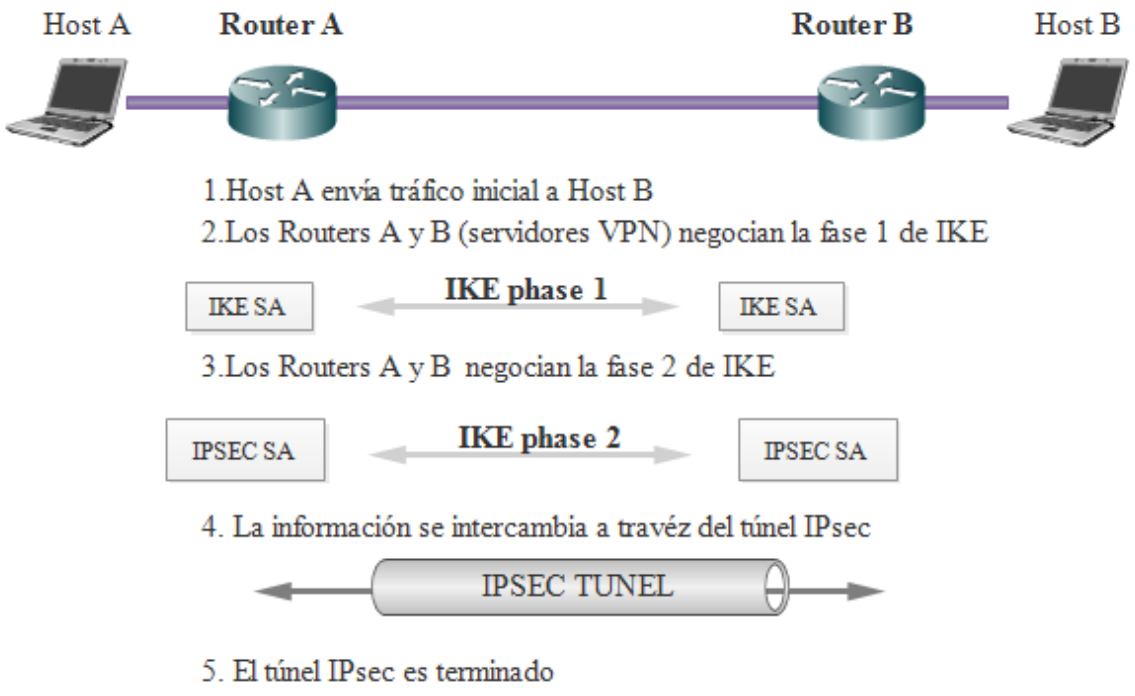


Figura 4-52: Funcionamiento de IPSec
Fuente: Elaboración propia

4.6 Metodología y Herramientas

4.6.1 Metodología

Dadas las características y objetivos planteados en la implementación de una VPN, es necesario definir un patrón metodológico que indique las fases ó pasos a seguir, en la búsqueda del alcance de dichos objetivos. En tal sentido se consideró seleccionar según la técnica de Eclecticismo, una metodología mixta con la recomendación de los autores Ruixi Yuan, W. Timothy Strayer, en su publicación "Virtual Private Networks: Technologies and Solutions" y lo sugerido por Casey Wilson y Peter Doak, en su libro "Creating and Implementing Virtual Private Networks".

Dado a que la VPN prevista para implantar en GADP prevé conexiones de unidades descentralizadas las cuales estarán enmarcadas bajo el método "Conectividad Sitio a Sitio" y las que tengan lugar entre usuario móviles, suscritas en el método "Acceso Remoto".

Lo cual hace que la Red Privada Virtual a implantarse disponga de ambos métodos de conexión. A continuación, se aplicará la metodología sugerida por el postulante el cual se describió en los anteriores capítulos.

4.6.1.1 **Fase (1): Diagnóstico y Requerimientos**

En ésta fase se evaluarán los diversos componentes que conforman las redes LAN, WAN, MAN de GADP y sus descentralizadas, para su efectiva integración y/o adecuación a los distintos esquemas de implantación de una Red Privada Virtual, así como determinar aquellos componentes no presentes en la configuración actual de la RED, para cada uno de los tipos de VPN de conformidad con lo descrito en las "Bases Teóricas".

4.6.1.2 **Fase (2): Análisis y diseño**

En ésta fase se definirá lo siguiente:

Desarrollo de las Políticas de Acceso y Seguridad a los recursos y servicios disponibles a los sistemas contables, en función de consolidar los aspectos susceptibles de control y/o restricción dentro de la Red Privada Virtual.

Determinación de la Estrategia para la Implantación de la VPN de acuerdo a la necesidad que poseen los distintos funcionarios para acceder a la información del el

GADP y evaluando las opciones y tecnologías existentes para la Implantación de una VPN, se determinará la estrategia para el diseño e implantación de la "Red Privada Virtual".

Diseño y Desarrollo de la infraestructura tecnológica para conexiones seguras en una VPN se llevará a cabo el trabajo de "Ingeniería de Detalle" propiamente dicho, es decir, de acuerdo a la estrategia de implantación adoptada se efectuará un "diseño concepto" de la Red Privada Virtual y se adicionarán, instalarán y ajustarán todas aquellas herramientas (hardware y software) previstos en el diseño.

4.6.1.3 **Fase (3) Configuración e implementación**

En esta fase se realiza las configuraciones e implementación de las Redes Privadas Virtuales.

4.6.1.4 **Fase (4) Pruebas**

Fase de comprobación del funcionamiento operativo y estratégico de la Red Privada Virtual que permite acceder los sistemas contables.

4.6.2 Herramientas

Firewall Dispositivo de seguridad que incorpora la administración de redes, así como un módulo de VPN basado en el protocolo de IPsec y entra funciones.

Switch Dispositivo de comunicación para conectar varios elementos dentro de una red.

ISP Internet Proveedor de servicio de internet con las configuraciones necesarias como modo bridge.

Servidores Ordenadores de alta gama que brindan continuamente algún tipo de servicio ejemplo: Http, Base de Datos, etc.

Estaciones de trabajo (host) Computadoras conectadas a la red para el acceso a los sistemas.

Pulse Secure Aplication Software para los clientes de acceso remoto.

GNS3 Software para realizar simulaciones y configuraciones networking.

Edraw Max Software de desarrollo de diagramas network

Capítulo III

IMPLEMENTACIÓN DE UNA VPN

5 CONFIGURACION DE UNA VPN

5.1 Configuración de una VPN en un Firewall

5.1.1 Fase (1): Diagnóstico y Requerimientos

Con el propósito de recabar información se estableció varias reuniones con los responsables en sistemas informáticos de cada unidad descentralizada, aplicando encuestas y entrevistas, así como informar los requisitos mínimos de una VPN. De esta manera tener un panorama y un diagnóstico general de cada red. Llegando a una evaluación final el cual deduciría la situación actual de cada una de ellas.

Dispositivos y estaciones Área Administrativa

	GADP	SEDCAM	SEDES	SEDEGES	DESCRIPCION
Servidores	5	1	0	0	Equipos que brindan algún servicio en la red
Estaciones de trabajo	50	4	4	2	Ordenadores conectados a la red para el acceso de información
Switch	5	1	1	1	Dispositivos de comunicación en la red
Firewalls y/o Routers	2	1	1	1	Dispositivos de seguridad y administración de la red

Tabla 5-1: Dispositivos y estaciones de trabajo
Fuente: Elaboración propia

a) Servidores y Estaciones de Trabajo

Está compuesta por 5 servidores configurados entre las plataformas Linux y Windows, brindando servicios de Aplicaciones Web, Base de Datos, Telnet y otros. Asimismo, existen 60 Estaciones de Trabajo que en su mayoría operan bajo los sistemas operativos Windows y a su vez tienen conexión a internet. Contando éstas con las características y capacidades técnicas (Hardware) para desempeñarse óptimamente con dichos sistemas.

a) Switch, Firewalls y Routers

Para mantener la conexión en la red LAN se utiliza como dispositivo de comunicación un aproximado de 8 switch. Asimismo, para establecer la conexión a Internet se ha venido contratando a un ISP con un aproximado de 20 Mb, lo cual lo administra el dispositivo Firewall/Router Juniper SRX, contando con un aproximado de 5 firewalls.

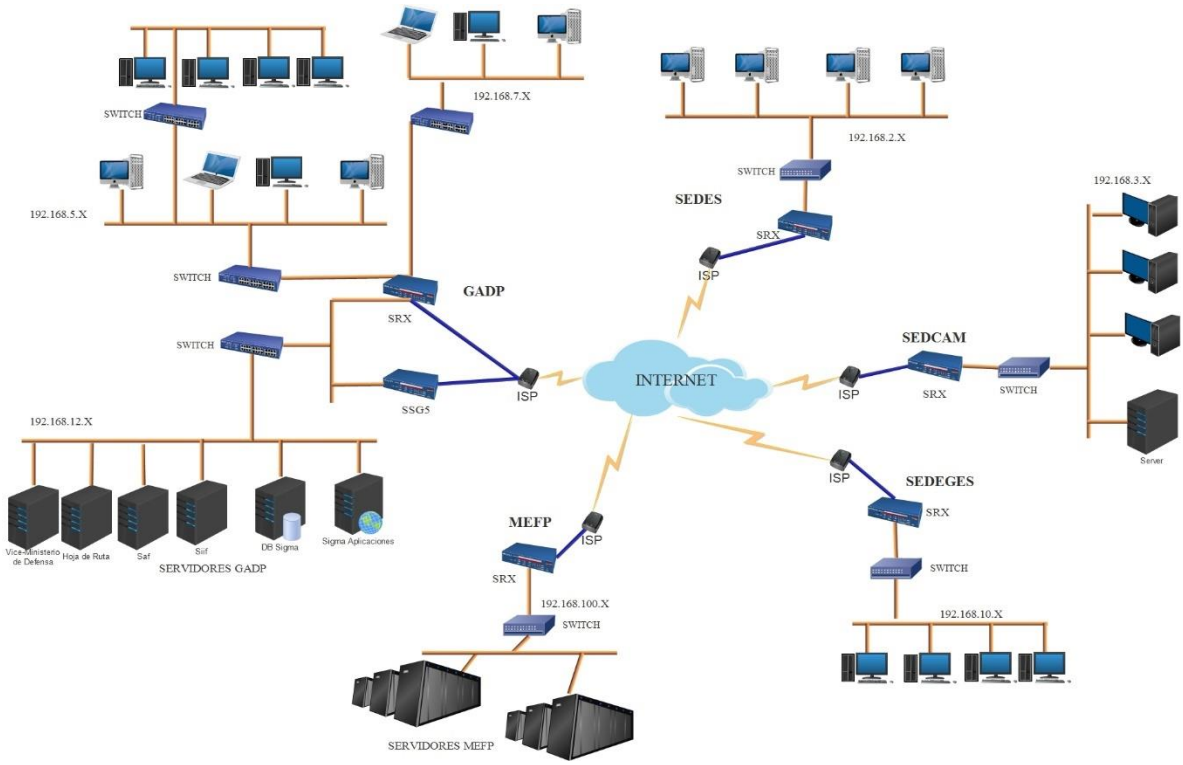


Figura 5-1: Diagrama General
Fuente: Elaboración propia

En la figura 5.1 se aprecia la interconexión de la red LAN Administrativa de cada descentralizada, así como la estructura de conexión a internet. Enfocándonos más al GADP se puede apreciar varios servidores y por otro lado su red LAN, al igual que el MEFP.

5.1.2 Fase (2): Análisis y diseño

5.1.2.1 Desarrollo de las Políticas de Acceso y Seguridad a la VPN

a) De los usuarios

1. El acceso a la información contenida en los sistemas SIGMA, SIGMA CENTRAL y SIIF que GADP considere de carácter privado y/o exclusiva estará disponible sólo a aquellos usuarios autorizados a través de la VPN.
2. Los usuarios remotos con privilegios exclusivos para acceder a los sistemas contables deben poseer una identificación electrónica (certificado y/o clave) como instrumento de autenticidad. Dicha Identificación será unipersonal.
3. Se establece perfiles de acceso que le permitirá acceder solo a las áreas de información, módulos y consultas prestablecidas, de acuerdo a su función e interés dentro de los sistemas.
4. Los certificados Digitales y llaves digitales tendrán una vigencia de uso según la consideración y aprobación de la junta coordinadora.

b) De la Plataforma informática

1. La infraestructura informática que soporta a la VPN debe proveer los mecanismos de seguridad (físico y lógico).
2. La plataforma para la conexión a los Sistemas Contables vía VPN debe ofrecer opciones alternas, para aquellos casos que por razones excepcionales no se tenga acceso a internet.
3. La infraestructura informática para atender a todos los usuarios debe de estar fuera del ámbito de la red LAN, de esta manera se tendrá acceso a la información necesaria de los Sistemas Contables.
4. La Red Privada Virtual debe ofrecer disponibilidad e interoperabilidad con los Protocolos TCP/IP a fines de ser compatibles con los estándares de comunicación utilizados en internet.

5.1.2.2 **Determinación de Estrategia para la Implantación de la VPN**

Para establecer la estrategia de implantación de una VPN, la cual dará acceso a los usuarios para el manejo de los sistemas contables, es importante determinar diferentes puntos que a continuación se describen.

Determinación Estratégica
4.4.1.1.2 Componentes de una VPN - Firewall - Túnel - Conexión VPN - Red Pública de tránsito - Cliente VPN **4.4.1.2 Arquitectura de una VPN** - VPN de Acceso Remoto - VPN de Sitio a Sitio - VPN Intranet **4.4.1.3 Tipos de VPN** - VPN Firewall - VPN Aplicación

Tabla 5-2: Resumen de determinación y estrategia
Fuente: Elaboración propia

a) Estructura física de la VPN

De acuerdo al análisis realizado en la figura 5.1 Diagrama General. Se observa la estructura física de la red del GADP. El cual se encuentra dividida en varias redes LAN, Zona de Servidores, donde se encuentran todos los servicios.

Deduciendo el análisis se presenta una tabla comparativa.

Conexión	Riesgos y Vulnerabilidades	Requerimientos	Disponible
Conexión VPN directo a la LAN	Todos los componentes de las redes LAN están comprometidos y confinados a la seguridad de la VPN, así como los sistemas en desarrollo	-Firewall	Si
		-Servicio de Internet	Si
		-Servicio VPN	No

Conexiones VPN directo al área de servidores.	Sólo la red de servidores está sujeta al establecimiento de control y seguridad	-Firewall	Si
		-Servicio de Internet	Si
		-Servicio VPN	Si

Tabla 5-3: Comparación de los esquemas de conexión VPN

Fuente: Elaboración propia

Como se observa en la tabla anterior, el esquema de conexiones VPN directo al área de Servidores, confiere solamente a los recursos de los sistemas contables.

b) Métodos de conexión de la Red Privada Virtual

La selección del tipo de tecnología a utilizarse para establecer el túnel Cliente-Servidor, es el aspecto más importante en el desarrollo de una VPN, dado que de ello depende la capacidad. Flexibilidad y seguridad de dicha red.

A continuación, se presenta una tabla de comparativa de los aspectos más importantes de los protocolos IPsec y SSL:

Protocolos / Características	SSL (Socket Secure Layer)	IPSec (IP Secure)
Maneja Tecnología PKI	SI	SI
Longitud de Clave	128 bits	128 bits
Presencia en el Modelo OSI	Capa 6 (Aplicaciones)	Todas las Capas
Acceso Subredes con control de Acceso Requerido	NO	SI
Típica implementación	Bancaria	Corporativa Militar Gubernamental
Clientes a conectarse	No controlado	Conocidos e identificados
Instalación en la del Cliente	Automático	Semiautomático

Tabla 5-4: Comparación entre los protocolos SSL - IPsec

Fuente: Elaboración propia

Como se muestra en la tabla anterior IPsec y SSL poseen características similares, sin embargo, existen diferencias según a la aplicabilidad que éstos tienen en distintos escenarios.

En el caso del acceso requerido por los usuarios remotos a la información financiera, donde es necesario la autorización y la autenticación para el establecimiento de sesión, se implementa el protocolo **IPsec** como método de implementación de VPN.

5.1.2.3 Diseño y Desarrollo de la Infraestructura Tecnológica para conexiones Seguras a una VPN

De acuerdo al análisis realizado en las secciones anteriores, el esquema de la conexión se desarrollará bajo el contexto de Conexiones VPN directo al área Servidores. En cuanto al método de conexión a la VPN, se seleccionó el protocolo de IPsec para el establecimiento del túnel. La topología el cual se utilizará se refleja en la sección 4.4.1.4.4 Topología de una VPN. Topología Radial y Topología de Acceso Remoto.

A continuación, se muestra diseño general de una VPN del GADP.

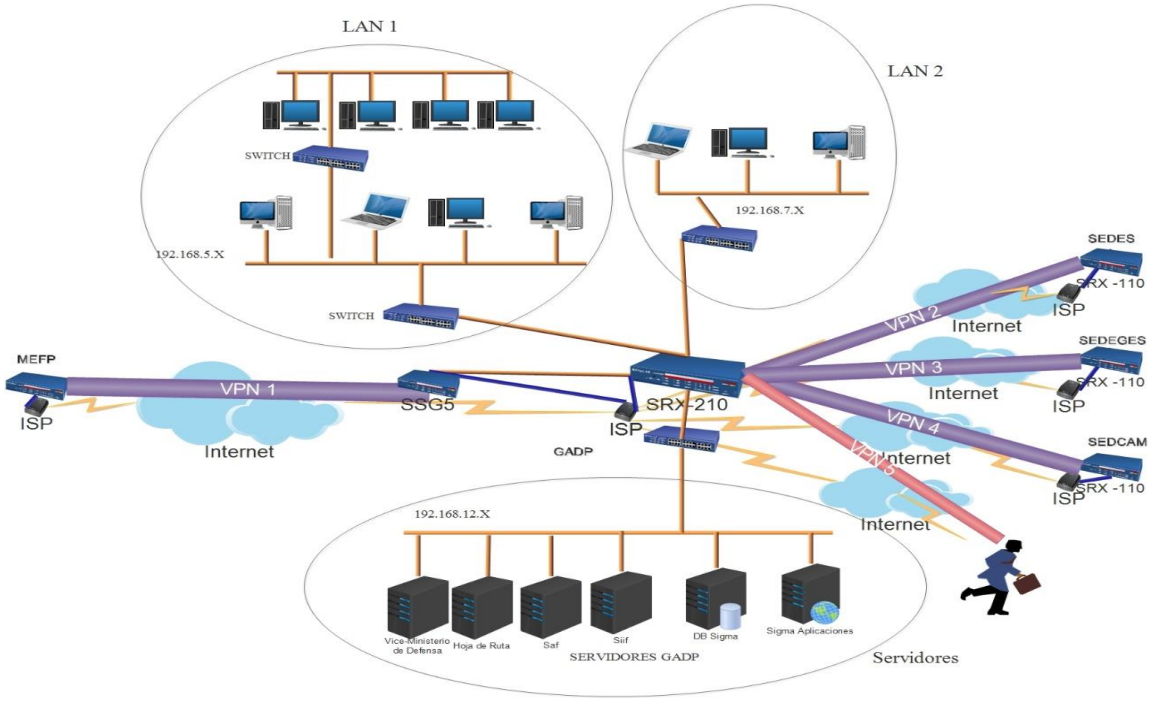


Figura 5-2: Estructura General de la VPN a implementarse en el GADP.
Fuente: Elaboración propia

a) Diseño detallado de la infraestructura para la implementación de la VPN

A continuación, se presentan cada uno de los componentes de Hardware y Software requeridos y disponibles en el GADP. Para la implementación de la red privada virtual.

	Componente	Disponible	Opción
Hardware	Firewall	SI	Juniper, Cisco, Mikrotik, otros compatibles con protocolo IPsec.
	Internet (ISP)	SI	Modem ADSL, Fibra Óptica, etc.
	Servidores	SI	Servidores que brindan algún servicio
Software	Tecnología de Cifrado y Enmascaramiento	SI	SHARED Simétrico
	Características del algoritmo de encriptamiento	SI	128 Bits
	Protocolo para establecimiento del túnel	SI	IPsec
	Ip Publica	SI	Ip Real
	Software del Cliente	SI	Conocidos e Identificados (Instalación Semiautomática)

Tabla 5-5: Resumen de componentes para la implementación de VPN
Fuente: Elaboración propia.

Firewall Dispositivo de seguridad que incorpora la administración de redes, así como un módulo de VPN basado en el protocolo de IPsec y entra funciones.

ISP Internet Proveedor de servicio de internet con las configuraciones necesarias como modo bridge.

Servidores Ordenadores de alta gama que brindan continuamente algún tipo de servicio ejemplo: Http, Base de Datos, etc.

Software y aplicaciones En cuanto al software se estableció el método de conexión con la tecnología Shared para los dispositivos Sitio a Sitio, y llaves privadas para los usuarios móviles. Así mismo se utiliza el protocolo IPsec, del mismo modo una aplicación del firewall a clientes móviles.

5.1.3 Fase (3) Configuración e implementación

Para instalar VPN con un Juniper Firewall Router se sigue los siguientes pasos.

5.1.3.1 **Paso 1: Instalación inicial física**

Asegurarnos que se encuentre en un lugar adecuado a temperaturas no más de los 20 grados, que tenga protección de UPS para salvaguardar altibajos de energía.

Dependiendo del modelo el dispositivo SRX210 cuenta con los dos primeros puertos para los ISP. Ya que ambos puertos 0/0 y 0/1 son de 10/100/1000 Mb, los puertos del 0/2 al 0/7 son para las diferentes LAN o segmentos de red que así uno lo utilice, también son usados para los Vlan internas. Así mismo se encuentra un puerto llamado CONSOLE es ahí donde se trabaja con un cable especial para configuraciones de comandos. También cuenta con dos puertos USB para otro tipo de configuraciones o actualizaciones. Y un botón RESET CONFIG para reestablecer en modo fabrica el dispositivo.

Si el dispositivo es un SRX110 a diferencia del anterior solo tendrá un solo puerto de 10/100/1000 para la conexión a ISP y un solo puerto de conexión USB.

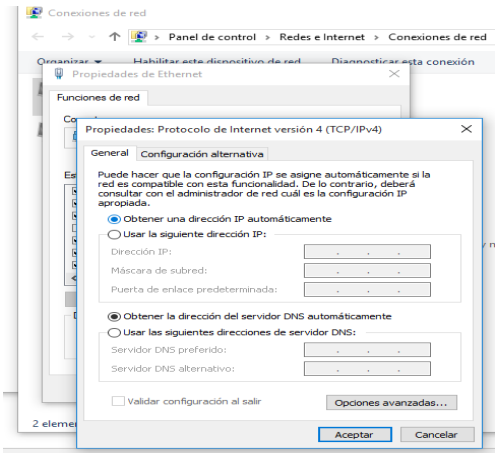
UPS 

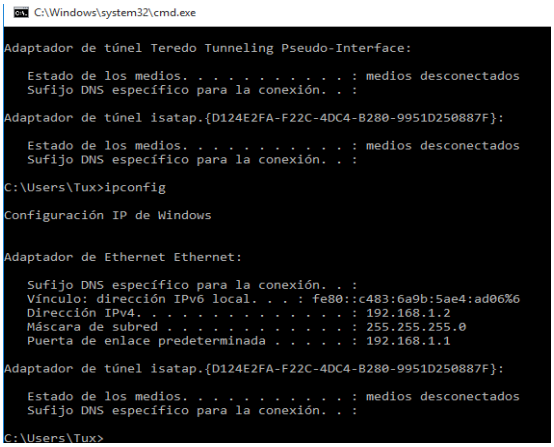
SRX 210

SR X110

Como se muestra en la figura 4.3 la conexión de un cable UTP se ubica en el puerto 0/3, por defecto viene configurado en modo Vlan los puertos 0/1 al 0/7 en cualquier de estos puertos se asignará una Ip DHCP en el segmento 192.168.1.0.

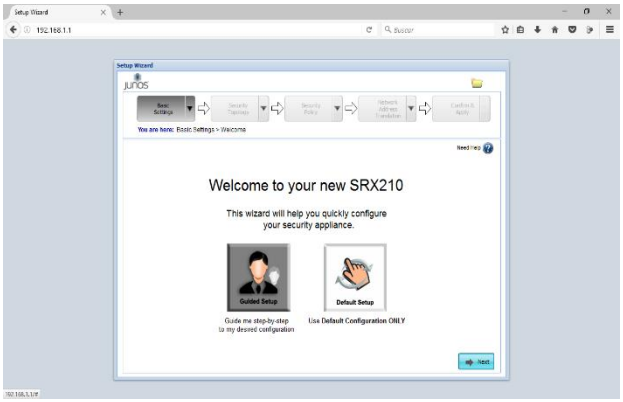
Configuración automática DHCP, IP asignada 192.168.1.X, mascara de red 255.255.255.0, Gateway 192.168.1.1. el cual será el acceso al dispositivo para su respectiva configuración. Para acceder a un dispositivo Juniper puede ser por puerto de consola, telnet, ssh, J-Web, snmp, JUNOScope, API JUNOSscript, API NETCONF y Sistemas de implementación de servicios SDX. Para su fácil manejo utilizaremos **J-Web (GUI WEB).**

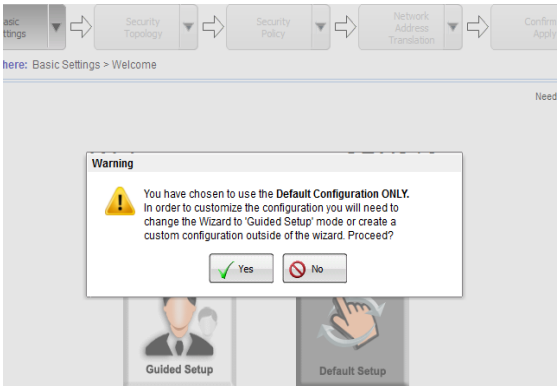




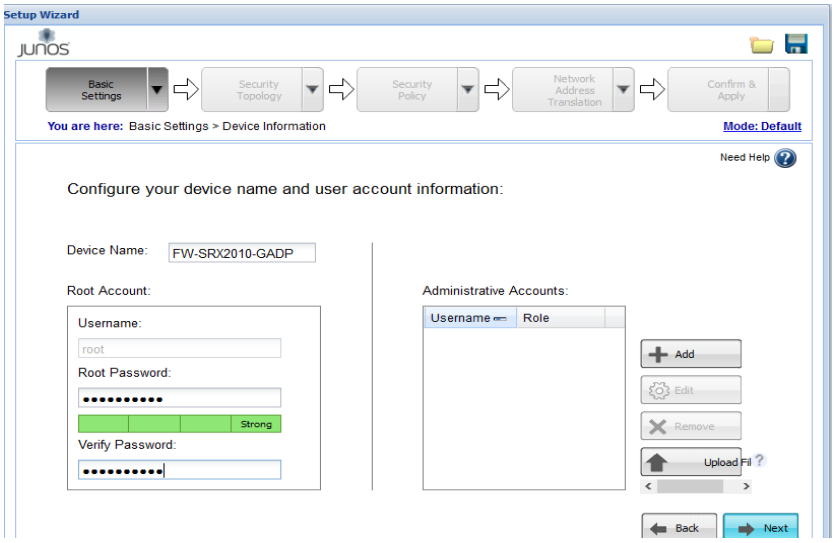
5.1.3.2 **Paso 2: Configuración básica**

Accediendo en un navegador a la dirección 192.168.1.1, seleccionamos ***instalación por defecto*** y ***Next.*** Aceptamos que la configuración será por defecto ***Yes.***

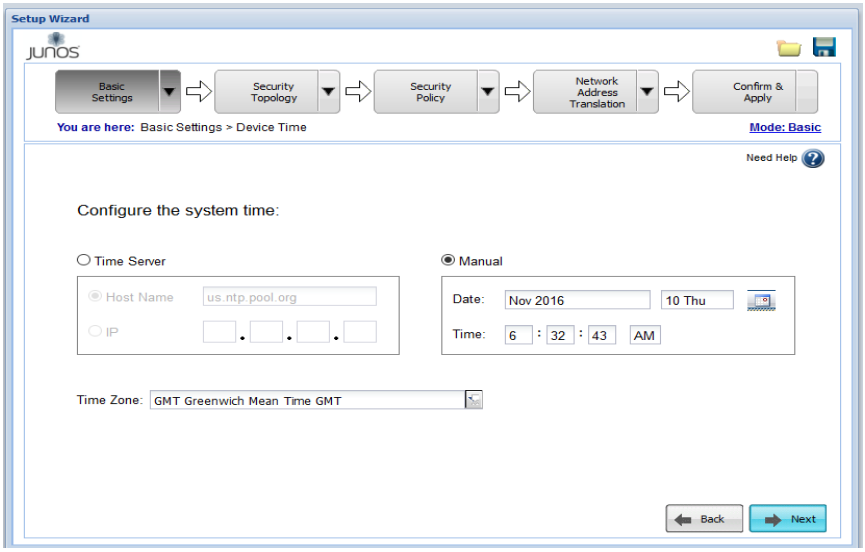




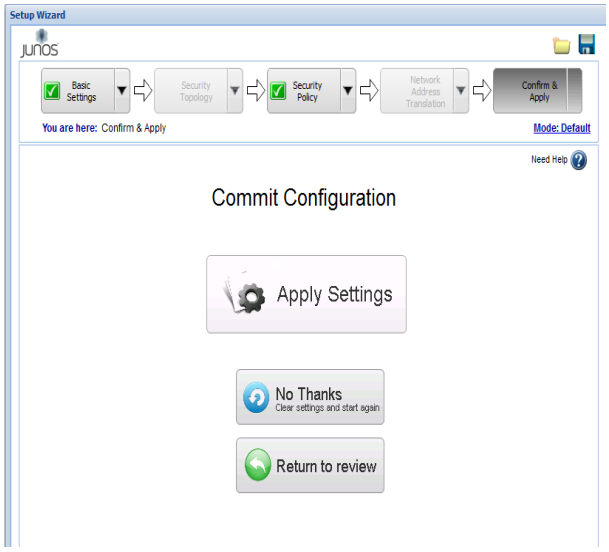
Asignando parámetros nombre y contraseña y ***Next***

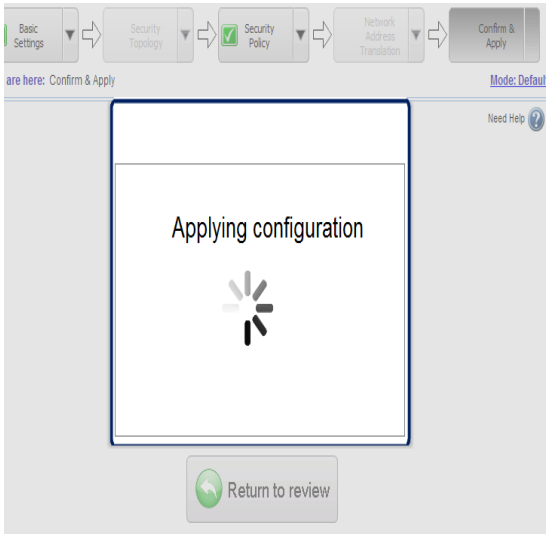


Asignamos fecha, mes y hora para el dispositivo clic ***Next.***

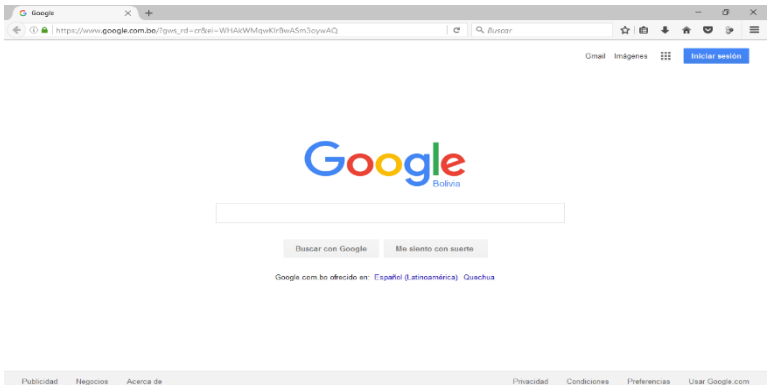


En las próximas opciones muestra el resumen de la configuración por defecto y la adquisición de la licencia en ambos casos hacemos clic en ***Next.*** Completando la configuración de las políticas de seguridad de las zonas trust / untrust o ahora bien llamado en las últimas versiones internal / internet. En ambos resúmenes hacemos clic en ***Next***. Para finalizar la instalación presionamos el botón ***Aplicar Configuración***. Si estuviese conectado a internet el puerto 0/0 ya se tendría por defecto internet, el sistema por primera vez crea automáticamente las reglas de políticas, nat, etc.





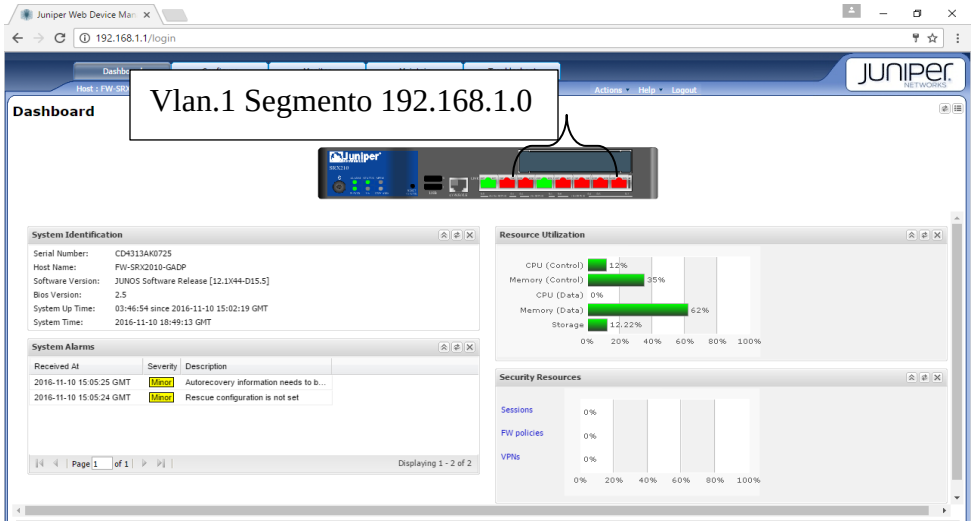
Una vez aplicada la configuración se tendría internet automáticamente.



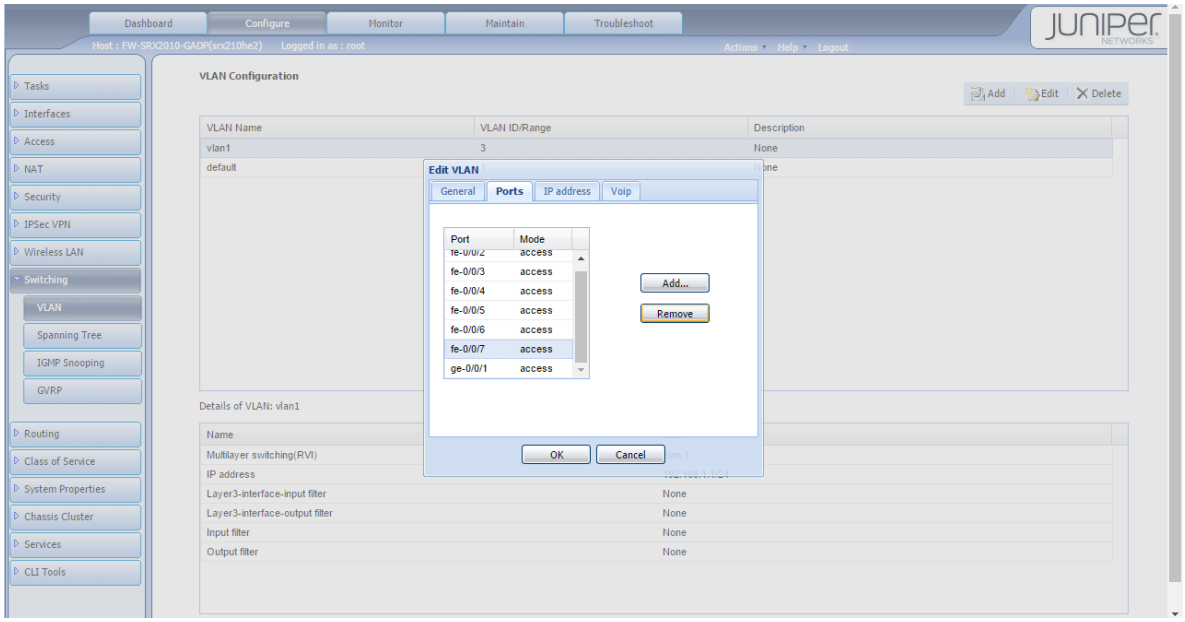
5.1.3.3 **Paso 3: Creación de Zonas en Vlans o interfaces**

Ingresamos con el usuario y contraseña que en la anterior sección configuramos. De hoy en adelante será de esta la manera de ingresar al dispositivo. Clic ***Login in***

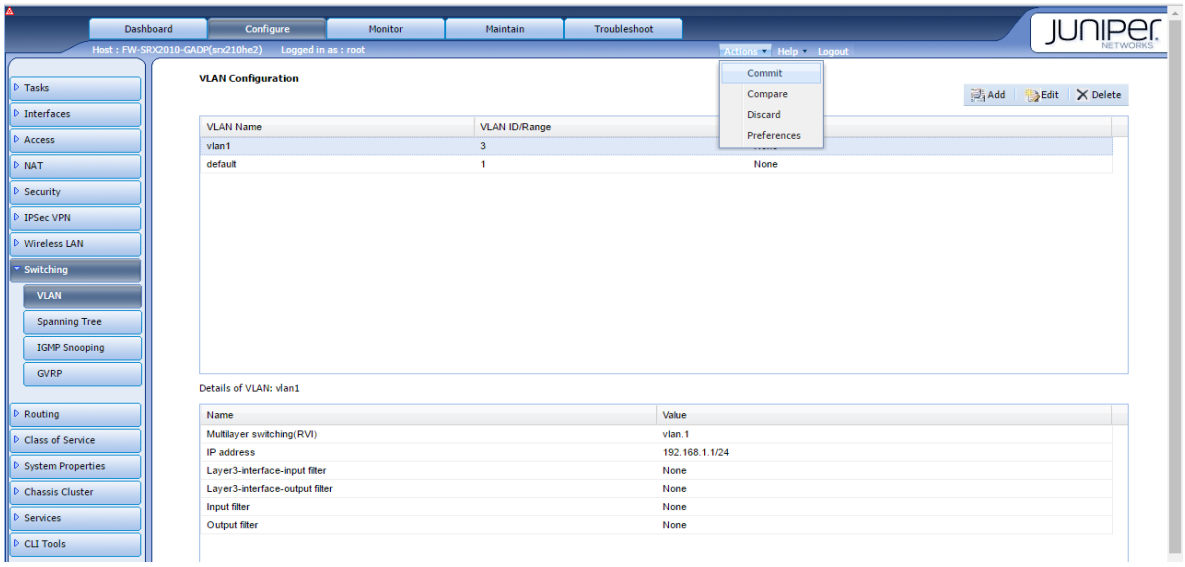
Como en la anterior sección se mencionó que las interfaces Ge-0/0/1 al Fe-0/0/7 por defecto están asignadas a una Vlan.0 o Vlan.1, en otros términos, en modo Switching.



Para crear una nueva VLAN tenemos que separar las interfaces de la Vlan que viene por defecto, esto se lo hace desde *Configure* > *Switching* > *Vlan*. Seleccionamos Vlan.1 que es por defecto pestaña Edit > Port y clic en los puertos a separar. En nuestro caso Fe-0/0/6 ***Remove*** y Fe-0/0/7 ***Remove***.

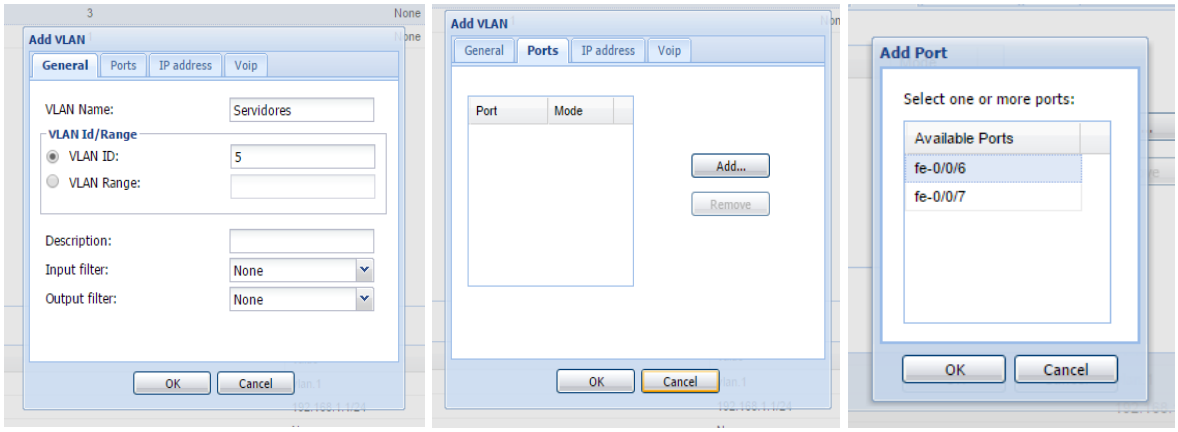


Una vez retirado los puertos, damos clic en ***Ok***, para luego guardar los cambios dando clic en la pestaña ***Actions y Commint.***

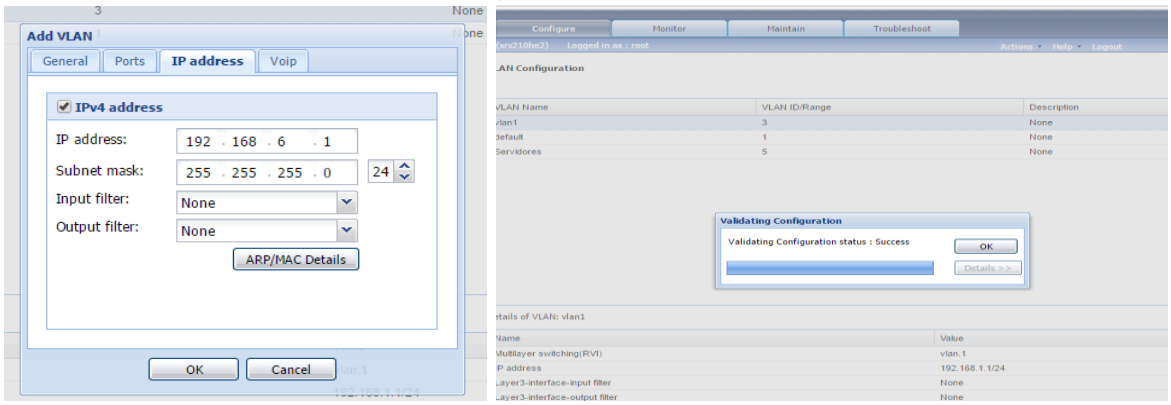


Para guardar los cambios de cualquier configuración en todo momento se utilizará Actions y ***Commint***. Es una manera de validar nuestra configuración y guardar los cambios efectuados, así sea modificar un pequeño parámetro.

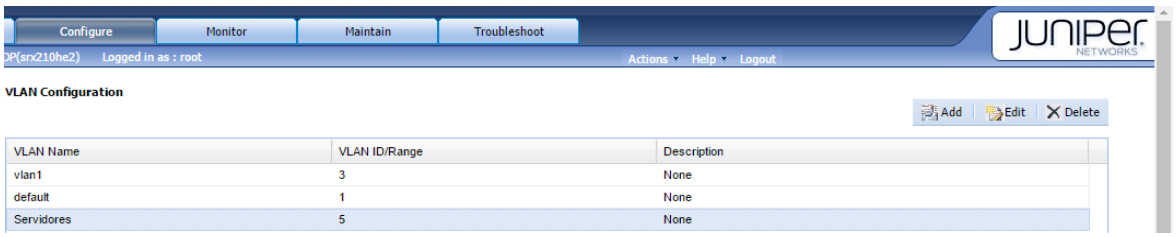
Creando una nueva VLAN, igual que el anterior nos ubicamos en *Configure>Switching>Vlan*, esta vez nos vamos a la pestaña *Add*, y en el cuadro de configuración *Add VLAN* en la pestaña *General*, ingresamos el nombre a la Vlan nueva y un ID que identificara de manera única Name: Servidores ID: 5. En la pestaña *Ports*, botón ***Add*** añadimos los puertos que formarán parte de nuestra Vlan clic ***OK.***



Continuando con nuestra configuración en la pestaña *IP address* en el mismo cuadro de configuración, Tildamos la opción *IPv4 address* seguidamente asignamos nuestro segmento de red 192.168.6.1/24 y la máscara de red correspondiente. Para luego pulsar el botón ***OK.*** Luego validamos y guardamos en Actions y ***Commnit.***

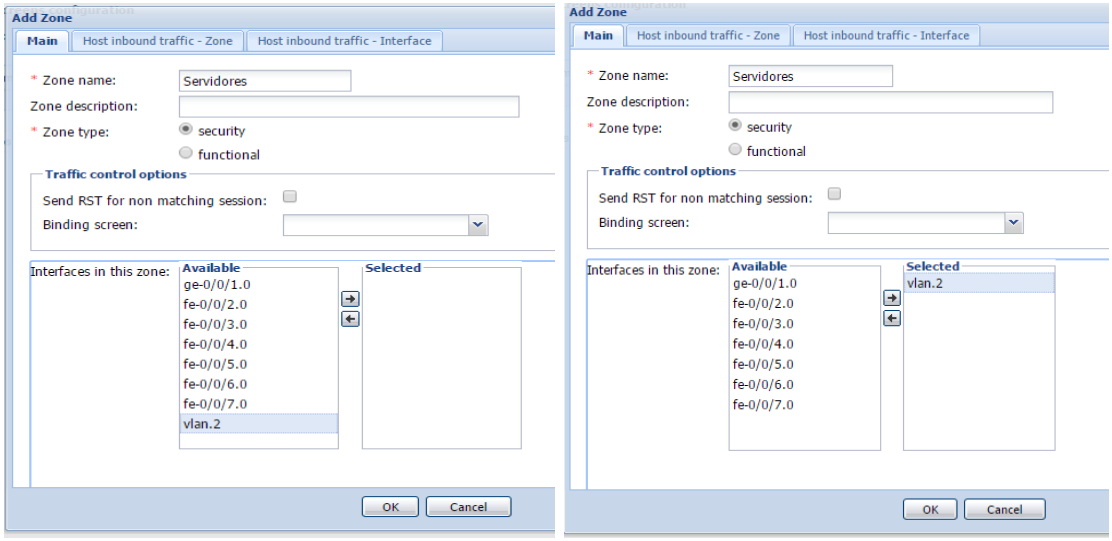


Verificamos nuestra Vlan creada: Servidores. Que corresponde a Vlan.2

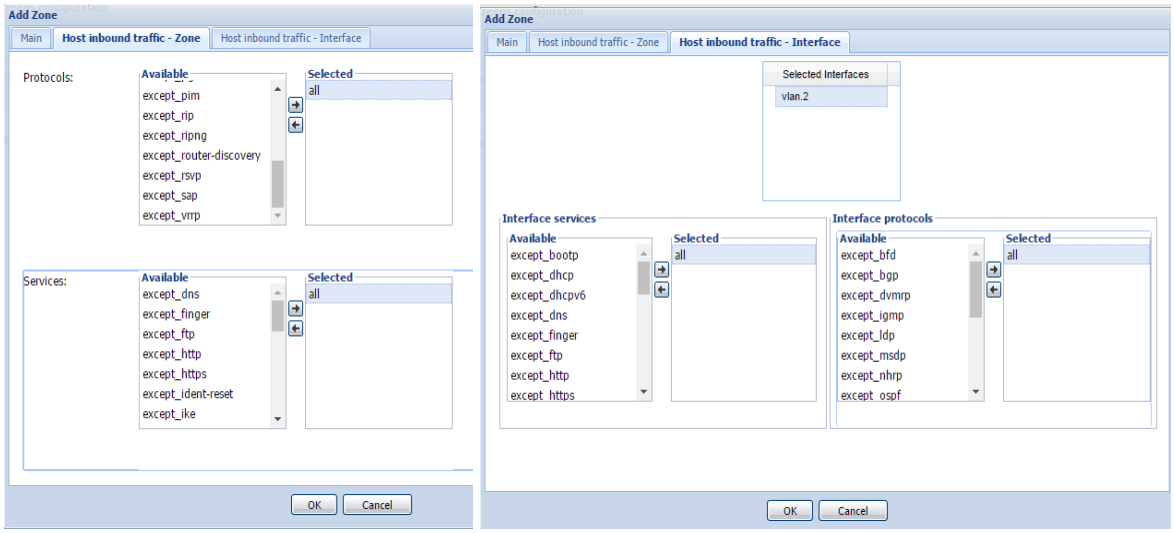


Para eliminar cualquier Vlan existe la opción ***Delete.***

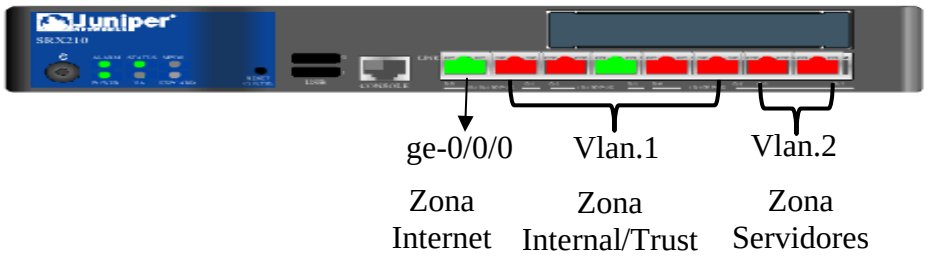
Ahora creamos la nueva Zona **Servidores** en *Security > Zones/Screens*, a primera vista se observa las dos zonas creadas por defecto internal y internet con su respectiva Vlan o interface. Para agregar la zona nueva seleccionamos la opción ***Add.*** Aparece el cuadro de configuración solicitando nombre, tipo de zona y la asignación de la Vlan. Name: Servidores Tipo de Zona: Security. En la parte inferior se encuentra las interfaces y Vlans habilitadas seleccionamos **Vlan.2** y asignamos a nuestra zona llevándolo a Selected.



En la pestaña siguiente de la misma configuración hacemos que escuchen todos los protocolos y servicios por zonas y en la última todos los protocolos y servicios por interface, de todas las listas habilitadas elegimos la opción **All** (todos). Y con las flechas de dirección llevamos al área de *selected.*

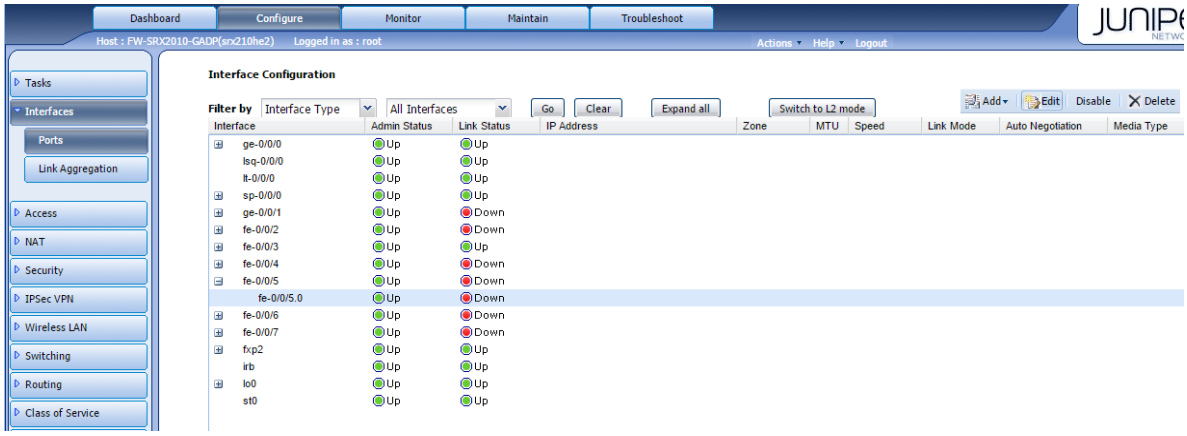


Y Presionamos el botón ***OK,*** para luego Guardar con *Actions y* ***Commint.***

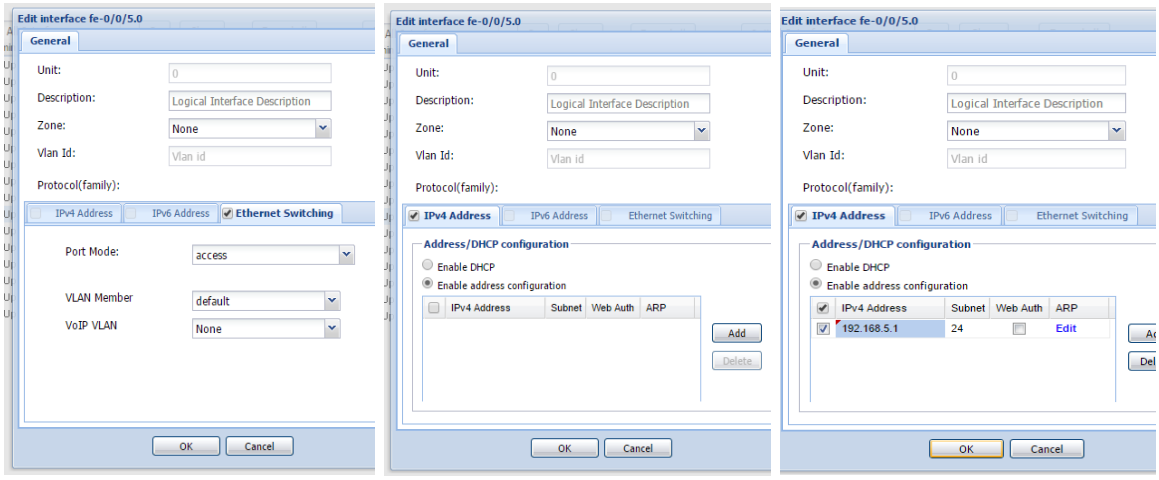


Así quedaría nuestro dispositivo con sus respectivas Vlans y Zonas.

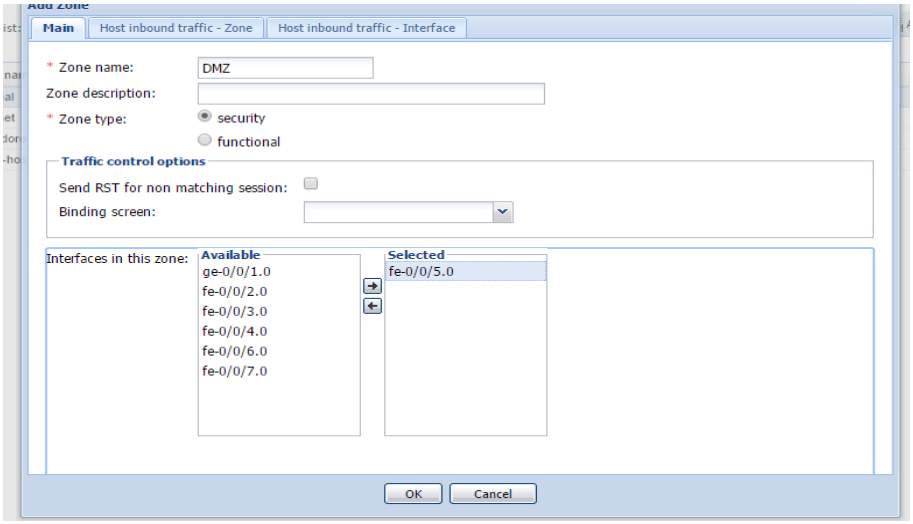
Agregando Zona a una interface. Para agregar una zona a una interface lo primero que se deber realizar separar un puerto de una de las Vlans. Como se explicó en la sección anterior *Configure* > *Switching* > *Vlan*, en nuestro caso f-0/0/5. Una vez que se tenga aislado el puerto se procede a la asignación de la zona a la interface en *Configure* >*Ports.* Seleccionamos el puerto libre y elegimos ***Edit.***



Automáticamente se nos abre el cuadro de configuración, desmarcamos *Ethernet Switching y* marcamos *IPv4 Address*. Luego elegimos ***Add*** y asignamos el nuevo segmento de red. Hacemos clic en ***OK*** y guardamos en *Actions* >**Commint.**

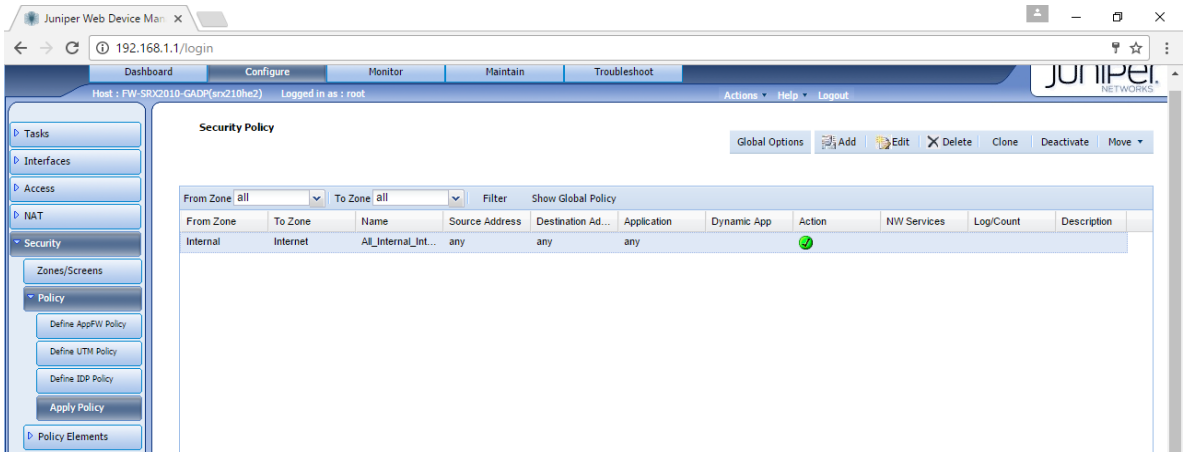


Como en la anterior sección aprendimos a crear zonas ahora asignamos a la interface fe-0/0/5 la zona DMZ. en *Configure* >*Security* > *Zones/Screens* luego aplicamos *Actions* > ***Commint.***



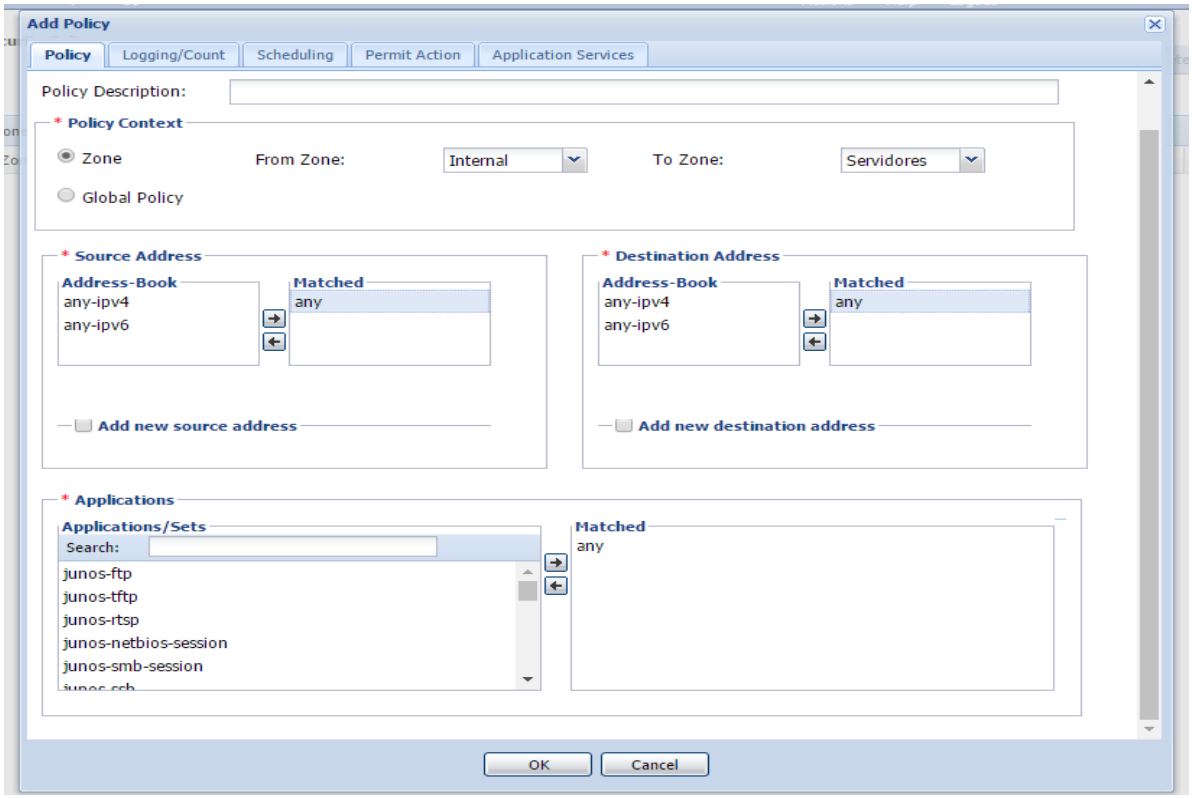
5.1.3.4 **Paso 4: Creación de políticas**

Las políticas son el control de tráfico que pasa de una zona a otra o de una interface a otra, de esta manera poder controlar los servicios puertos, protocolos, etc. Para configurar nos ubicamos en lo siguiente *Configure* > *Security* > *Policy* > *Apply Policy*.

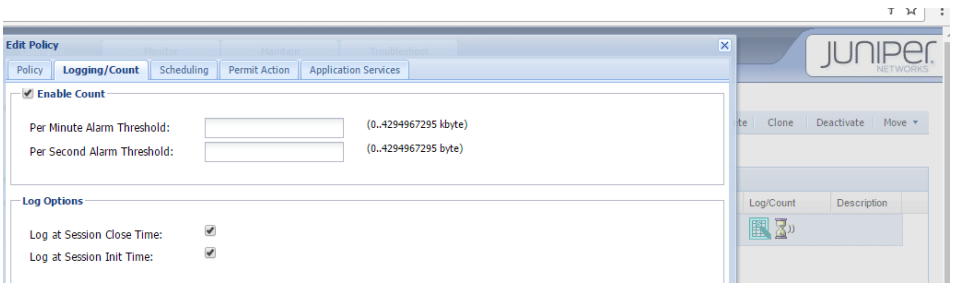


Las políticas pueden realizarse de manera viceversa dependiendo a las necesidades a configurar, una práctica útil es por vez primera sea cual sea la zona, pasar todo el tráfico correspondiente para luego ir restringiendo según las políticas establecidas, en nuestro caso crearemos una política de la Zona Internal/Trust a la Zona Servidores. Existe como en todas las configuraciones en la barra lateral superior derecha todas las opciones que describe en la mayoría por si solas Add, Edit, Delete, etc.

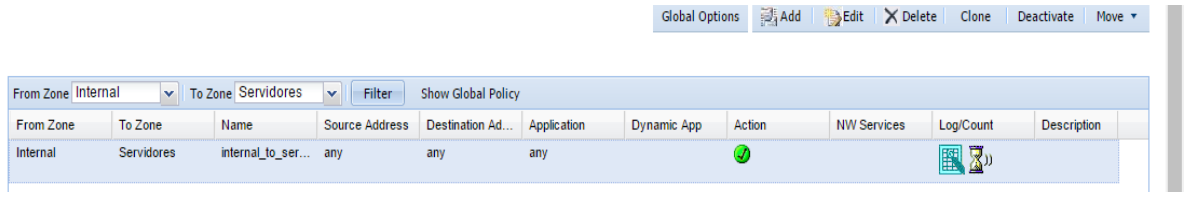
Creando Política de la Zona Internal/Trust a Zona Servidores *Configure > Security > Policy > Apply Policy*. ***Add***. Como es habitual aparece la ventana de configuración solicitando los parámetros a configurar. Nombre de la Política Policy Name: internal_to_servidores, tomar encueta que no acepta espacios en los nombres. Policy Action: Permit, en el contexto de Zona seleccionamos zona origen y zona destino. From Zone: Internal To Zone: Servidores. Automáticamente se habilita una lista de Source Address y Destination Address, direcciones origen y direcciones destino, en nuestro caso por el momento Any (todos) en ambos casos. en el sector Applications controlamos los protocolos, aplicaciones, puertos, etc. Por el momento any.



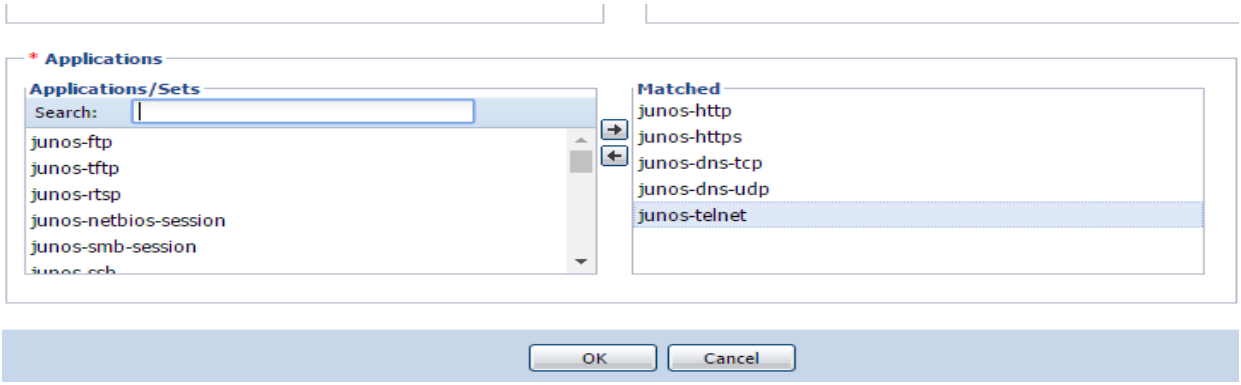
Para finalizar vamos a la pestaña Logging/Count para habilitar Enable Count y init time close time. Presionamos el botón ***OK*** par luego validar y guardar *Actions*> ***Commint***



Modificando los parámetros de nuestra política para permitir los protocolos HTTP, HTTPS, DNS, TELNET. *Security* > *Policy* > *Apply Policy*. Realizamos el filtro correspondiente con la herramienta *Filter* dependiendo de las zonas a las cual vamos a configurar Zona Internal – Zona Servidores, política internal_to_servidores, seleccionamos la política, y ***Edit.***



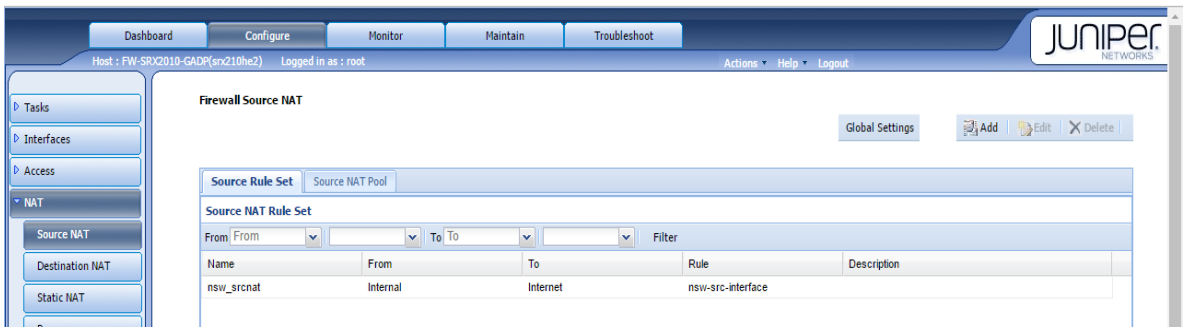
En la sección de Applications en el cuadro de configuración regresamos el parámetro *Any*, para dejarlo con los protocolos mencionados.



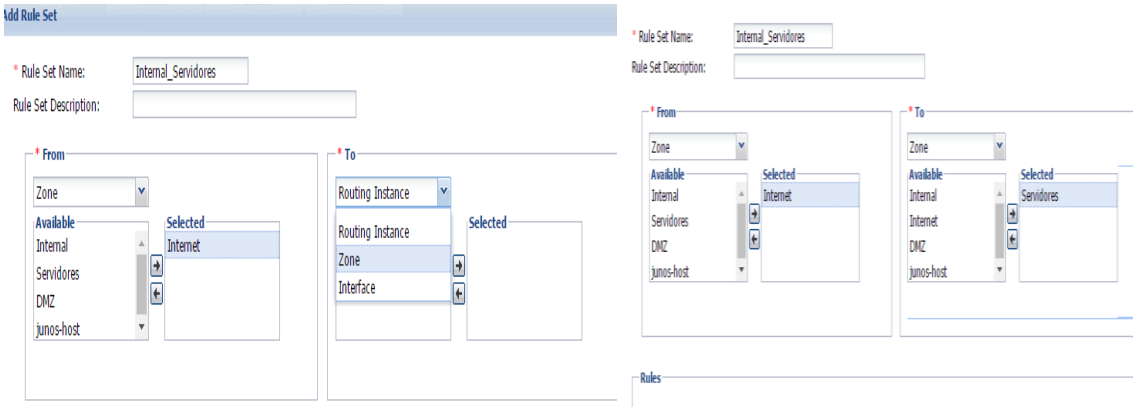
Luego presionamos el botón ***OK,*** para luego validar y guardar con *Actions*> ***Commint.***

5.1.3.5 **Paso 5: Creando source nat**

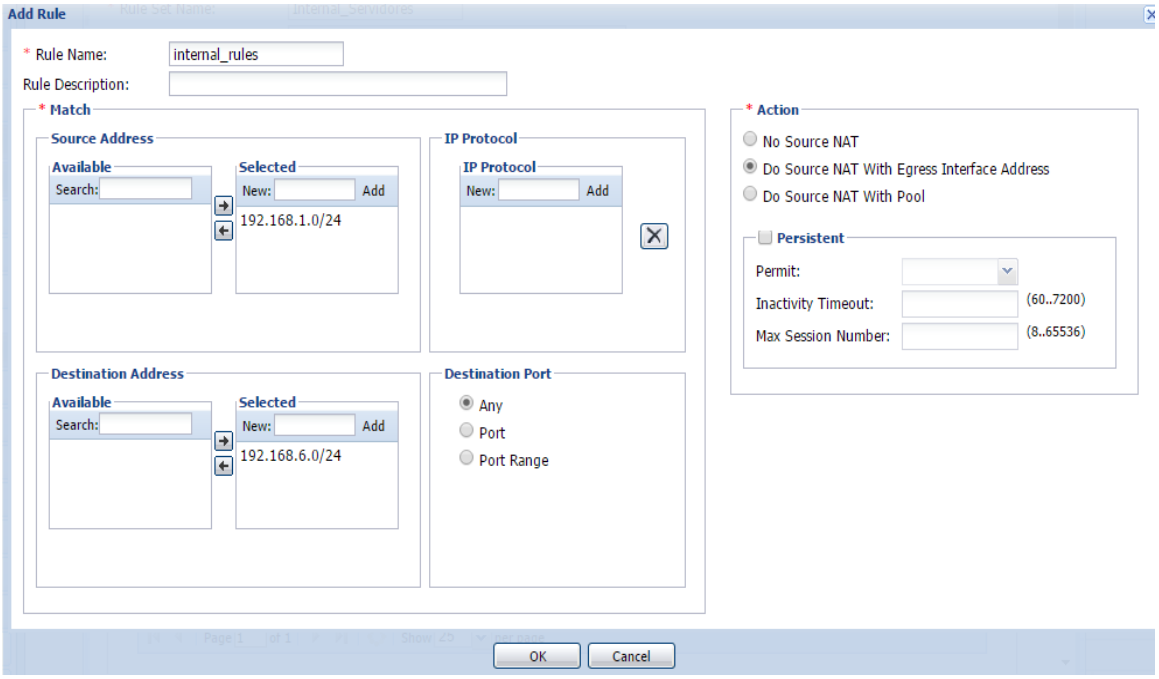
Como en todo dispositivo de seguridad existen varios tipos de nateo, se utiliza dependiendo de los requisitos o necesidades que se presente, en el caso específico de nosotros nos enfocaremos a Source NAT. Para configurar nos ubicamos en lo *siguiente Configure* > *NAT* > *Source NAT*.



Creando un nuevo Source NAT *Configure* > *NAT* > *Source NAT*, ***Add*** Inmediatamente empezamos asignar los siguientes parámetros, Rule Set Name: Internal_Servidores, Seleccionamos la zona origen y la zona destino.



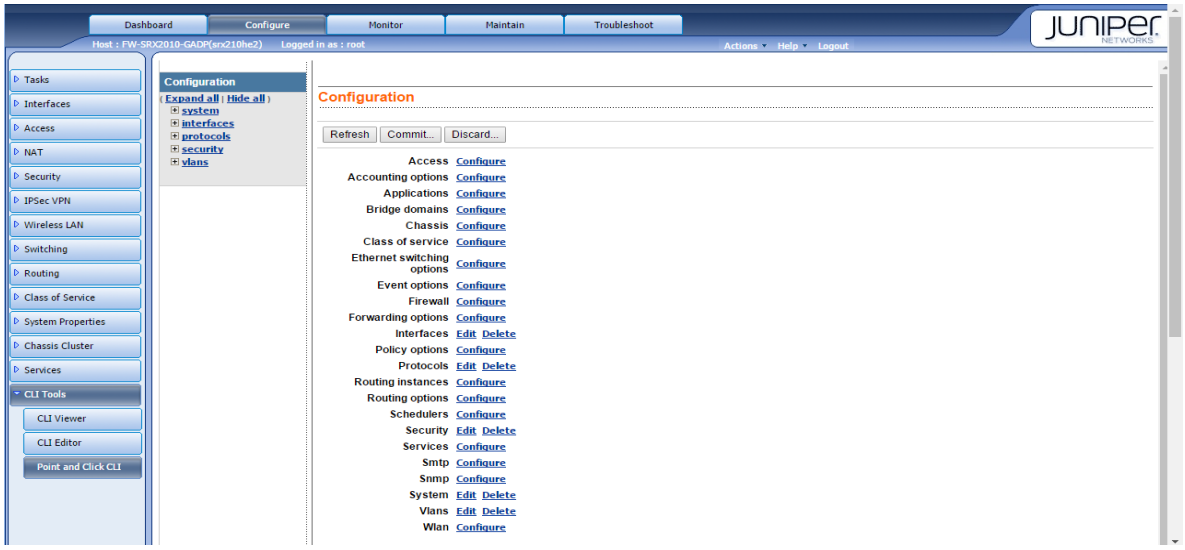
Ahora añadimos las reglas entre zonas en la seccion Rules en el boton ***Add***, Añadimos el nombre Rule Name: Internal_ Servidores, Source Address *Selected* Trafico origen (Segmento de la red de la zona Internal) 192.168.1.0/24 En Destination Address Selected Trafico destino (Segmento de la red Servidores) 192.168.6.0/24. Para finalizar vamos a la sección de Action y elegimos la segunda opción Do Source NAT Witch Egress Interface Address.



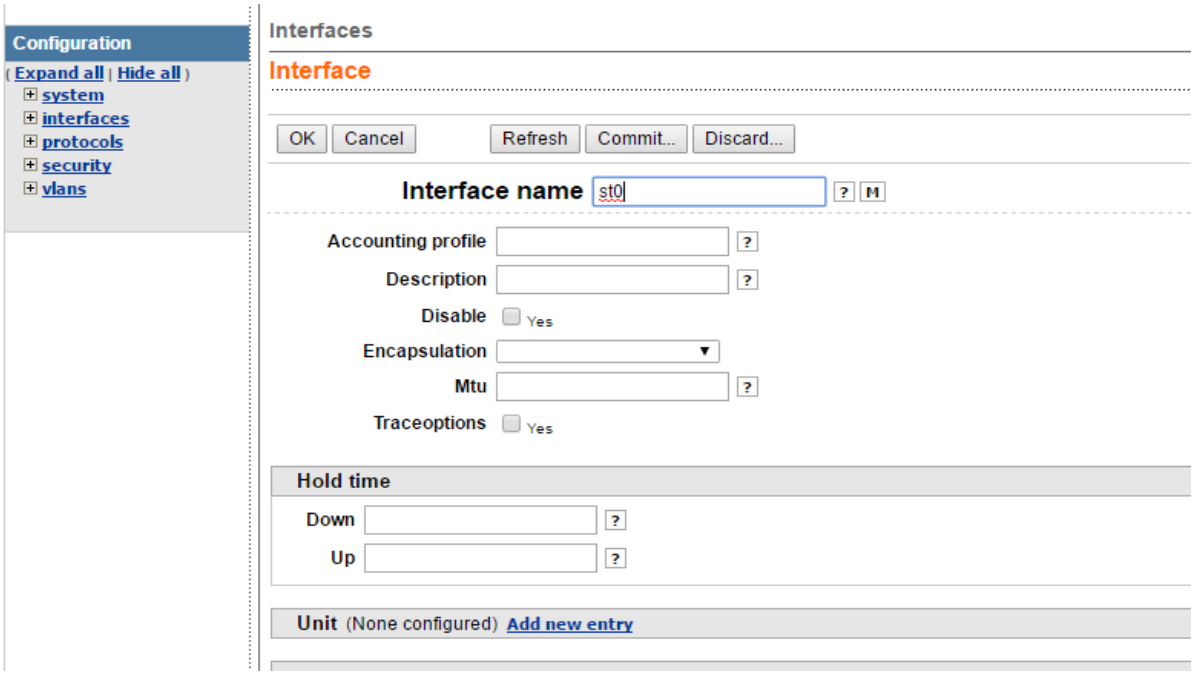
Para completar hacemos clic en ***OK*** en ambas ventanas y para guardar los cambios como es habitual en *Actions*> ***Commint.***

5.1.3.6 **Paso 6: Creación de una VPN Sitio a Sitio**

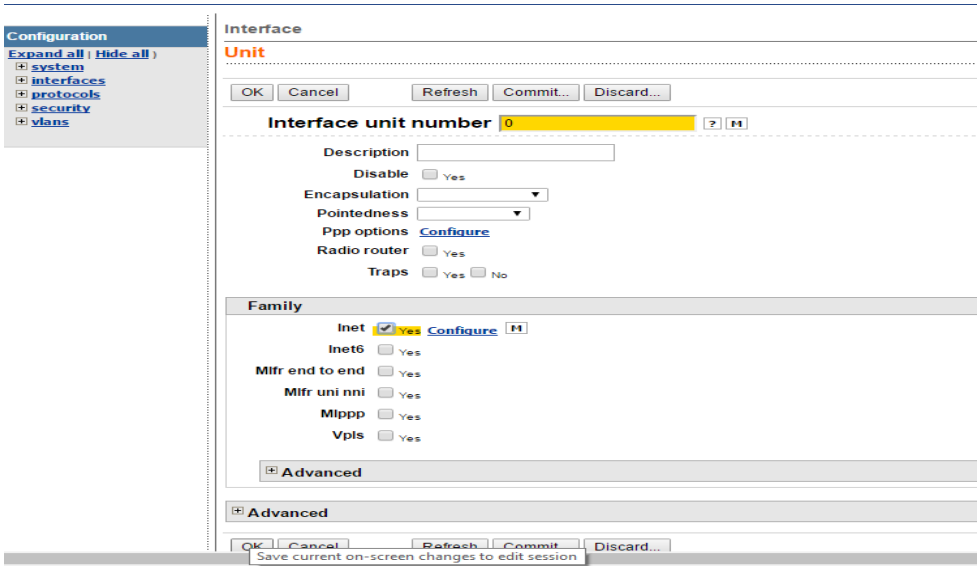
Lo primero es crear una **interface virtual** Configure > *CLI Tools* > *Point and Click CLI.*



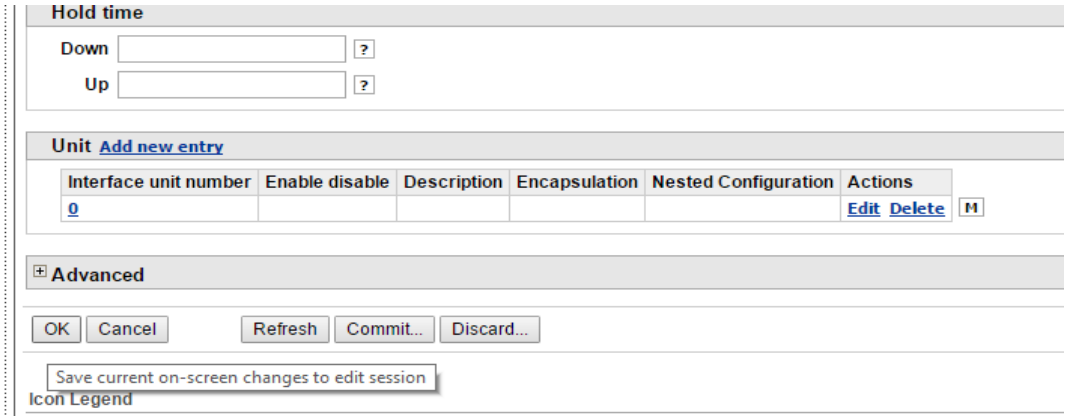
Elegimos la opción *interfaces* y Adicionamos nueva interface en ***Add new entry.*** Asignamos los parámetros requeridos Interface name: st0



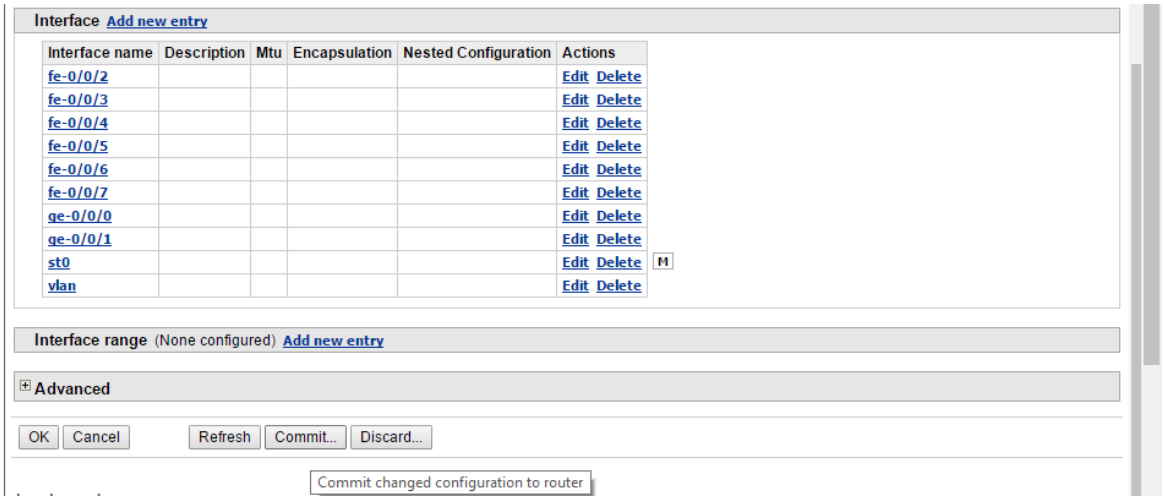
En *unit* elegimos ***Add new entry***, asignamos los parámetros Interface unit number:0 marcamos *inet* y guardamos la configuración en ***OK.***



Observamos que en la sección de unit aparece la interface y presionamos el botón ***OK***.



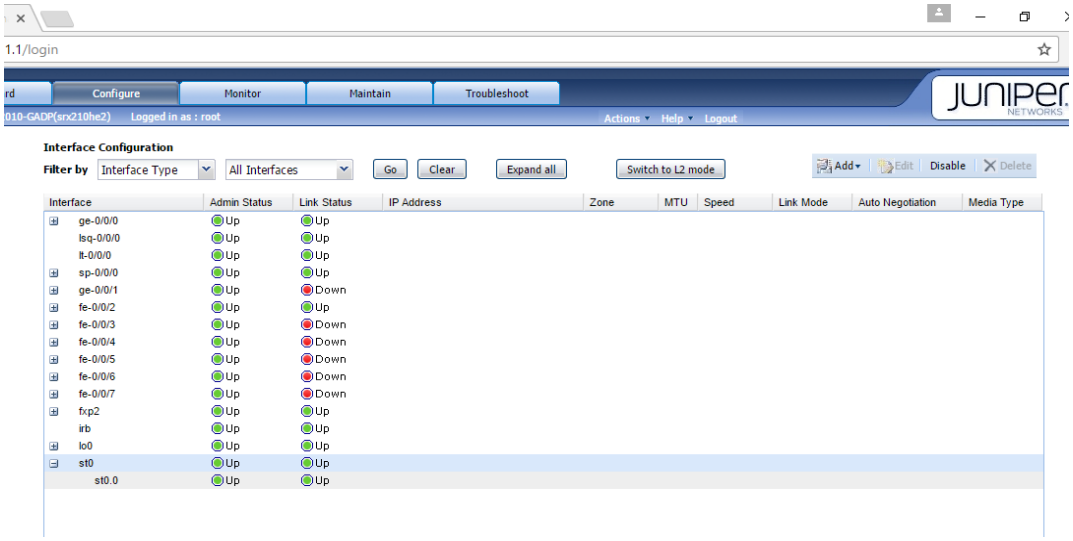
En la nómina de interfaces ya aparece st0. Presionamos el botón ***Commint***



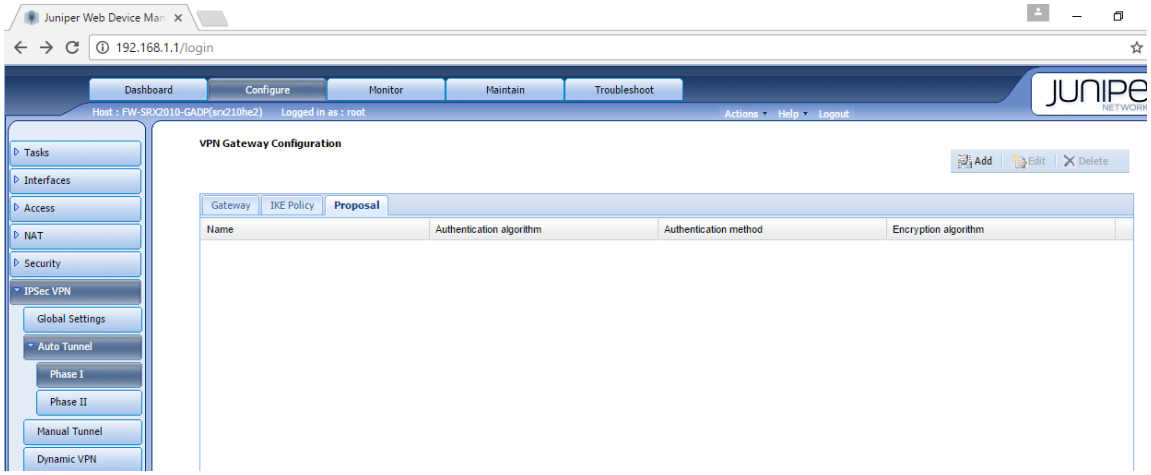
A continuación, aparece el resumen de cambios presionamos ***OK.***

La interface st0.0 se creó con éxito, presionamos el botón ***OK.***

Verificamos nuestra interface en *Configure >Interfaces > Ports.* y asignamos una Ip. Para nuestro control. Ejemplo segmento 10.0.10.0/24 en todos las Firewalls.

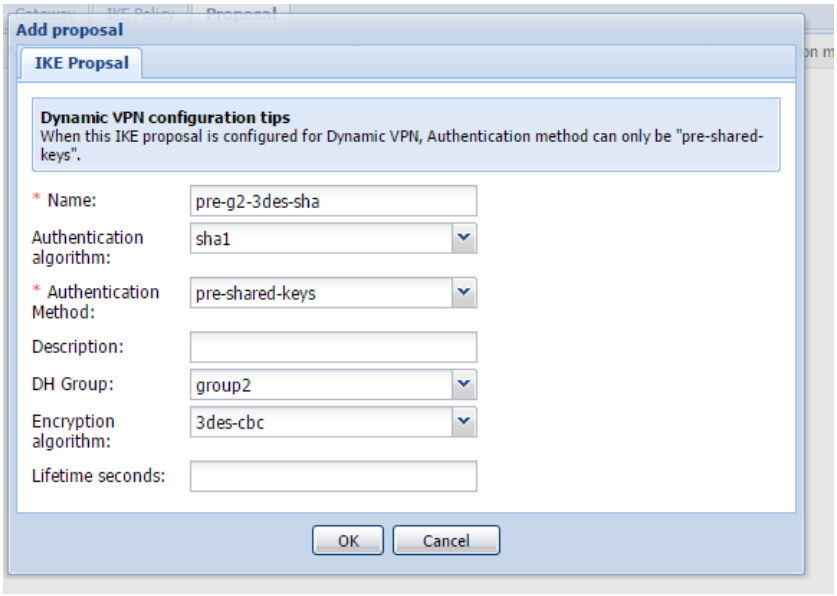


Creando VPN <u>Fase I</u> nos dirigimos a *Configure > IPSec VPN > Auto Tunel > Phase I,* comenzamos de derecha a izquierda (proposal).

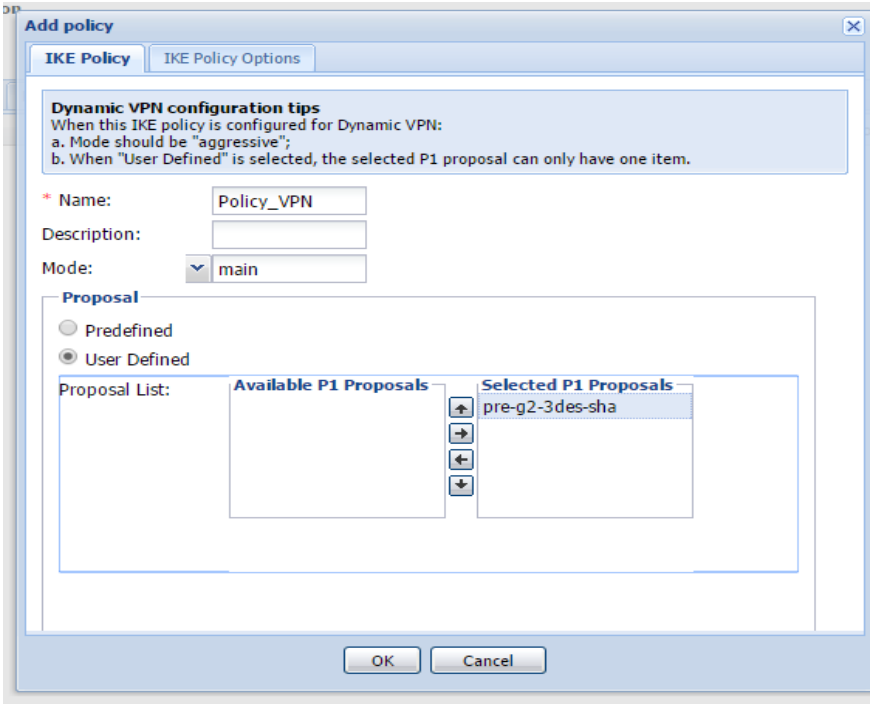


Presionamos en ***Add,*** y empezamos asignar parámetros Name: pre-g2-3des-sha

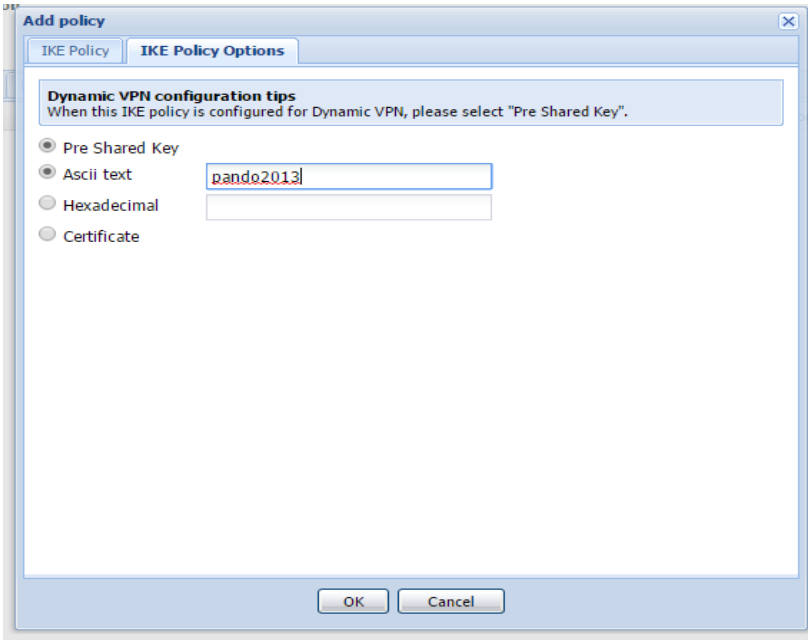
Algoritmo de autenticación sha1, Método de autenticación: pre-shared-key, Grupo: group2, Algoritmo de encriptacion 3des-cbc. Presionamos ***OK*** luego ***Commint.***



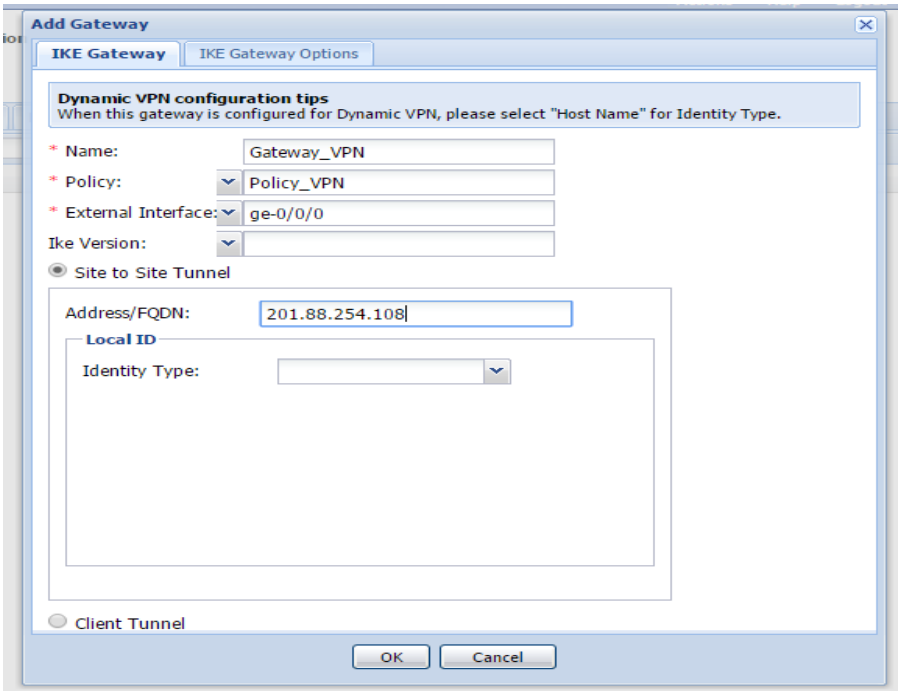
Añadiendo **IKE Policy,** presionamos ***Add*** configuramos Name: Policy_VPN, Metodo Main para las Ips públicas, en la sección de proposal podemos elegir uno ya predefinido, pero usaremos el que creamos.



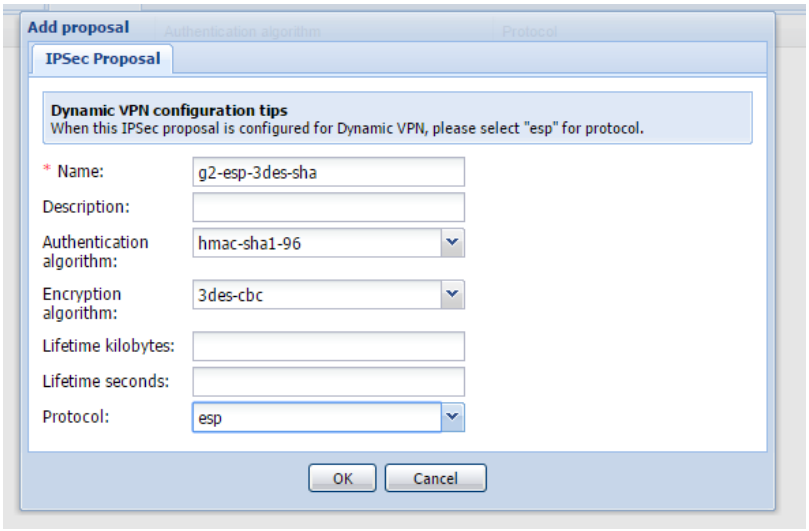
IKE Policy Options, ***Add*** aquí ingresaremos la llave que se encripta con el proposal elegido. Presionamos ***OK y Commint.***



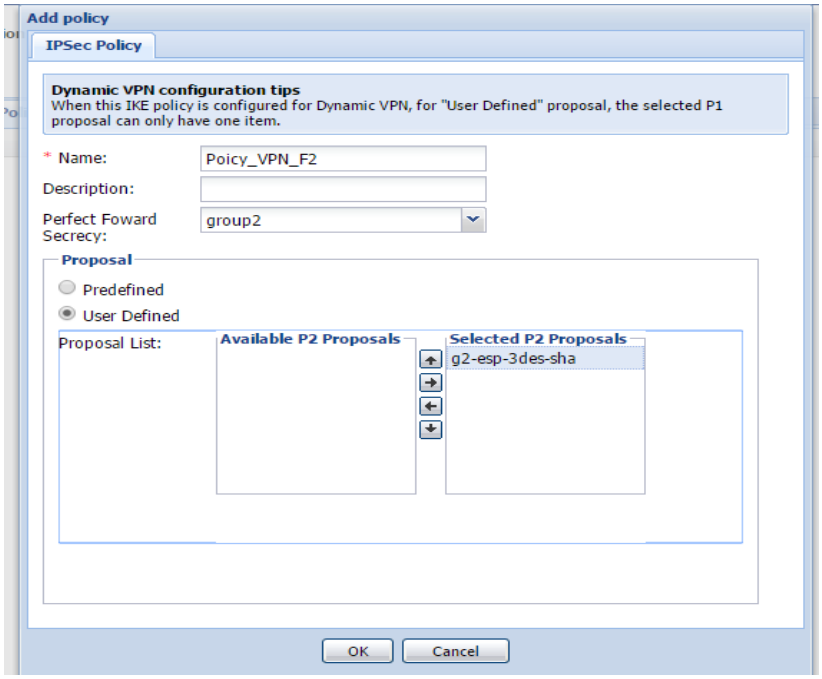
IKE Gateway, ***Add*** asignamos los parámetros como el nombre, elegimos la política anterior que creamos, escogemos la interface por donde saldrá la VPN (modem internet), marcamos túnel sitio a sitio, ingresamos la Ip publica del firewall del otro extremo de la VPN ejemplo 201.88.254.108. Presionamos ***OK y Commint.***



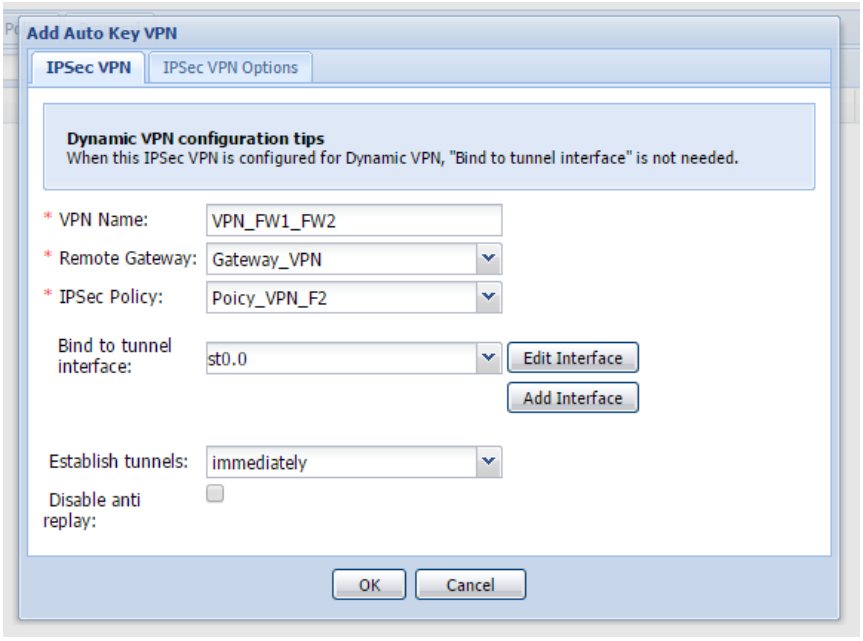
Fase II *Configure > IPSec VPN > Auto Tunel > Phase II*, del mismo modo que la primera Fase de derecha a izquierda *Proposal* > ***Add.*** Algoritmo de autenticación hmac-sha1-96, Algoritmo de encriptación 3des-cbc, Protocolo esp. Presionamos ***OK y Commint.***



IPSec Policy, ***Add*** agregamos Name:Policy_VPN_F2, Grupo: group2, del mismo modo que en la Fase I, usaremos el proposal que creamos manualmente y presionamos ***OK y Commint.***

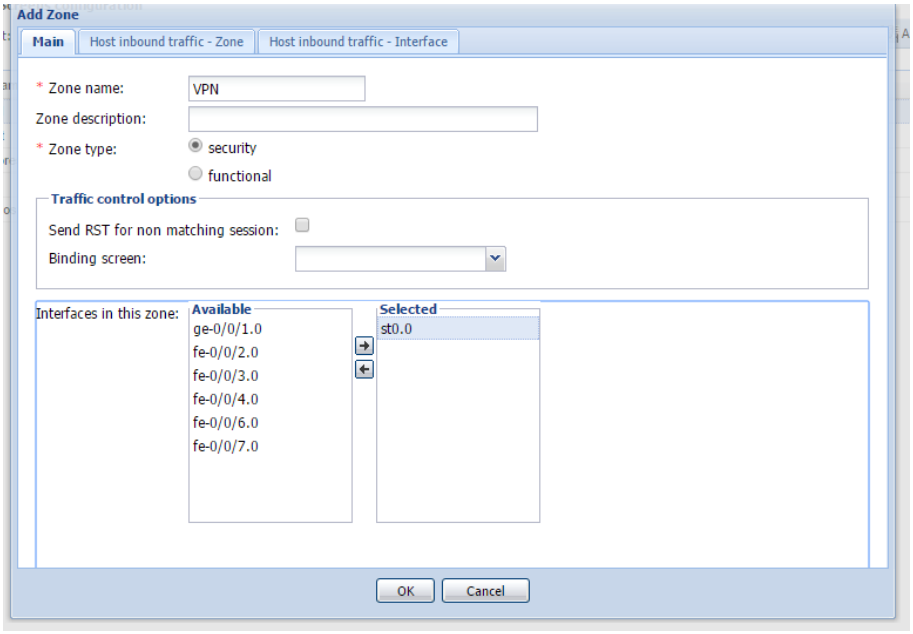


Auto Key VPN, ***Add*** Name: VPN_FW1_FW2, Remote Gateway: elegimos el que creamos anteriormente, IPSec Policy: el creamos anteriormente, Bind to túnel interface: st0.0, indicamos que el túnel se establecerá inmediatamente Establish tunnels: immediately.



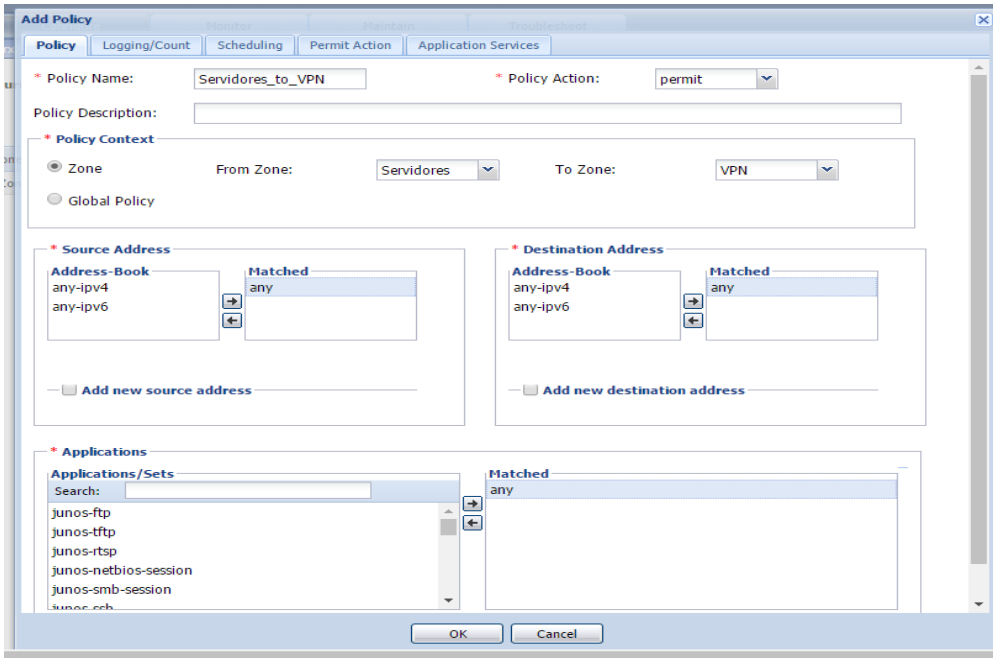
Habilitamos el monitoreo de la VPN en *IPSec VPN Options*, marcamos *Enable VPN monitor y Optimize.* y presionamos ***OK y Commint.***

Unas veces creadas la VPN se le debe asigna a una Zona, como aprendimos a asignar zonas en las secciones anteriores. Tomando en cuenta que la interface que se le asignará a la Zona es st0.0.

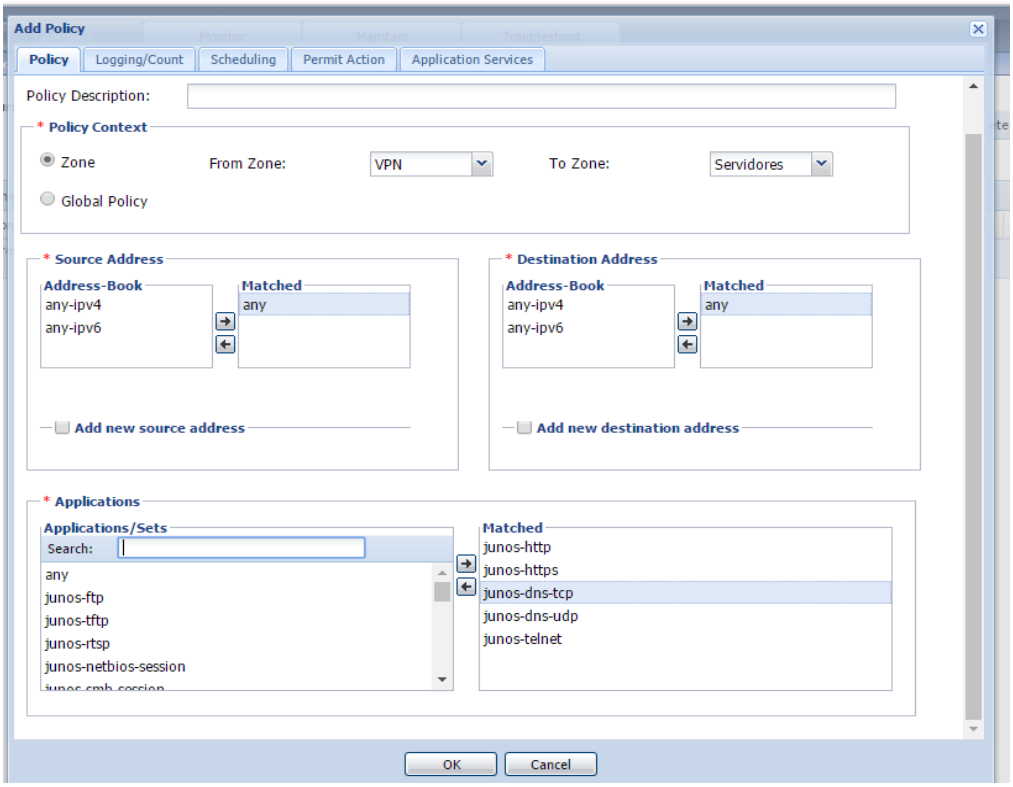


Como ya se lo tiene en una Zona ahora ya podemos crear políticas de entrada y salida como se aprendió en la sección anterior.

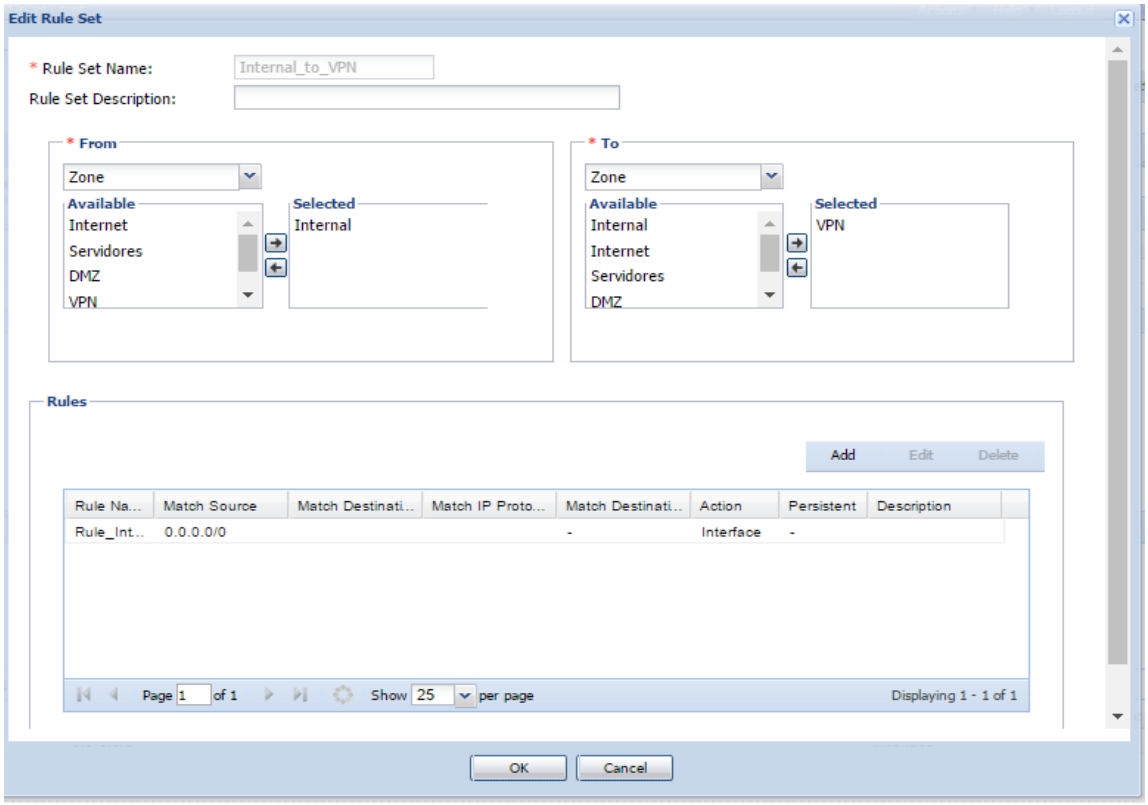
Política Servidores_to_VPN



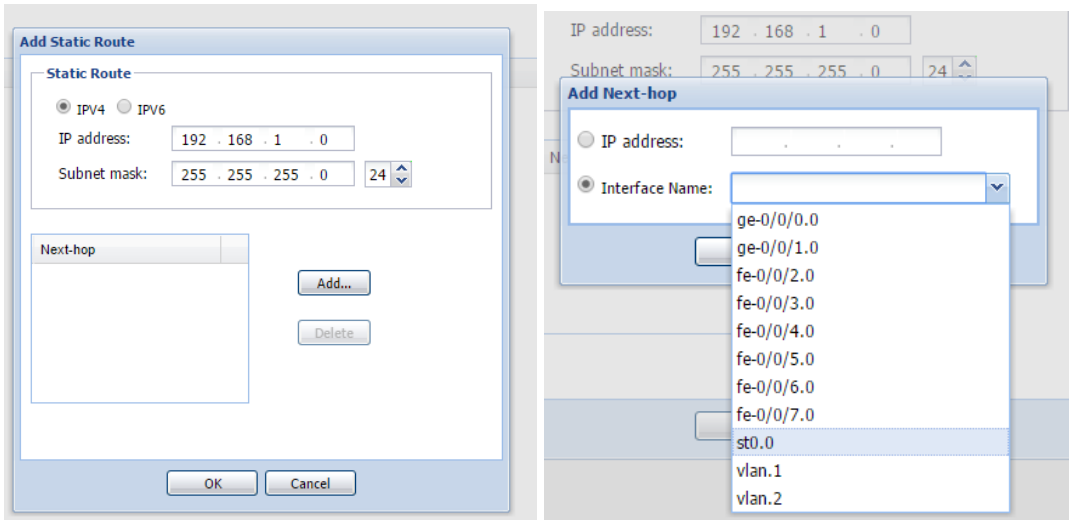
Política VPN_to_Servidores aquí se controla que puertos que protocolos y a que servidores se tendrá acceso



Una vez creada las políticas también se tiene que establecer el nateo correspondiste como se explicó en las anteriores secciones. Tomando en cuenta el análisis.

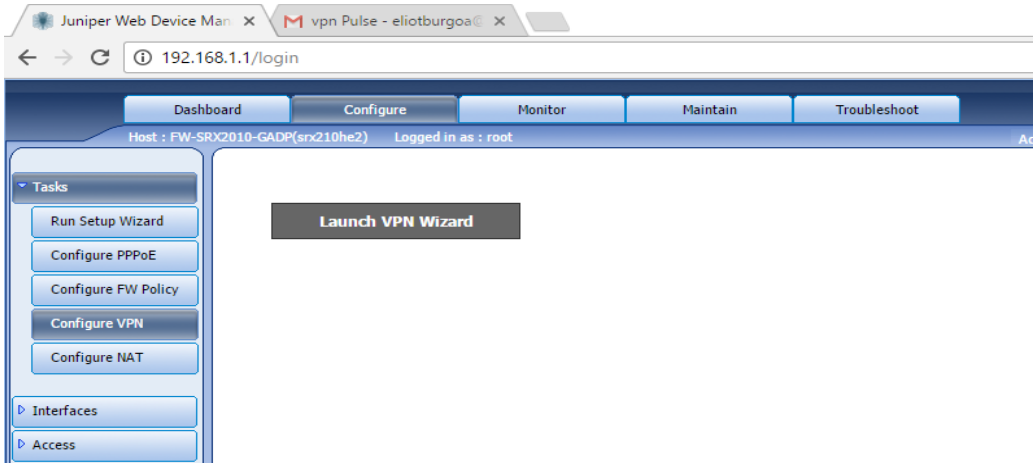


Creando rutas *Configure* > *Routing* > *Static Routing*, ***Add*** tenemos que indicarle que segmento de red realizará el salto correspondiente, cuando queremos ir a la red VPN tiene que ir por st.0.0 (zona VPN).

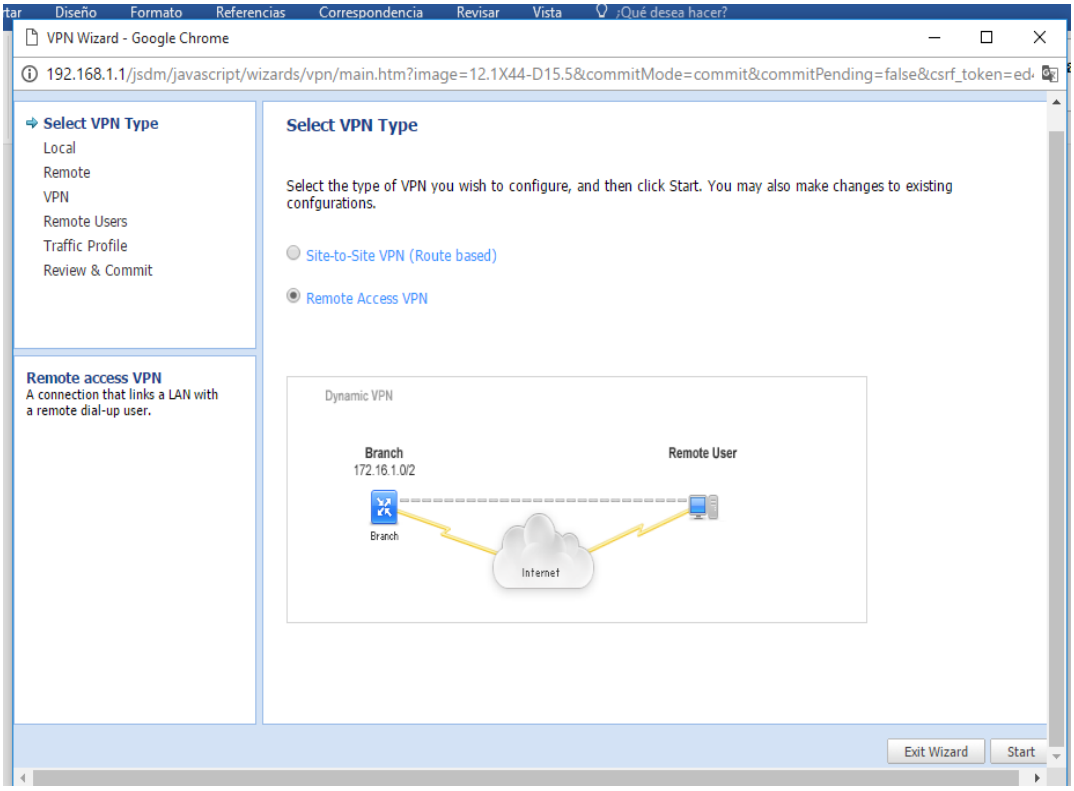


5.1.3.7 **Paso 7: Creación de una VPN para el Acceso Remoto**

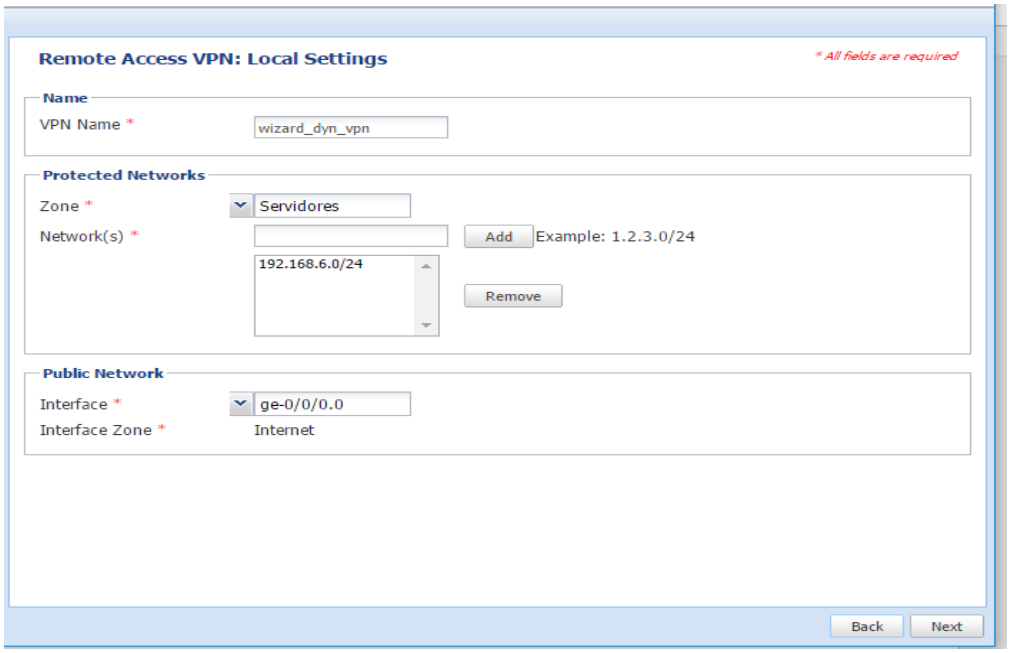
Para la creación de una VPN para los usuarios Remotos se configura lo siguiente *Configure* > *Tasks* > *Configure VPN* y presionamos ***Launch VPN Wizard.***



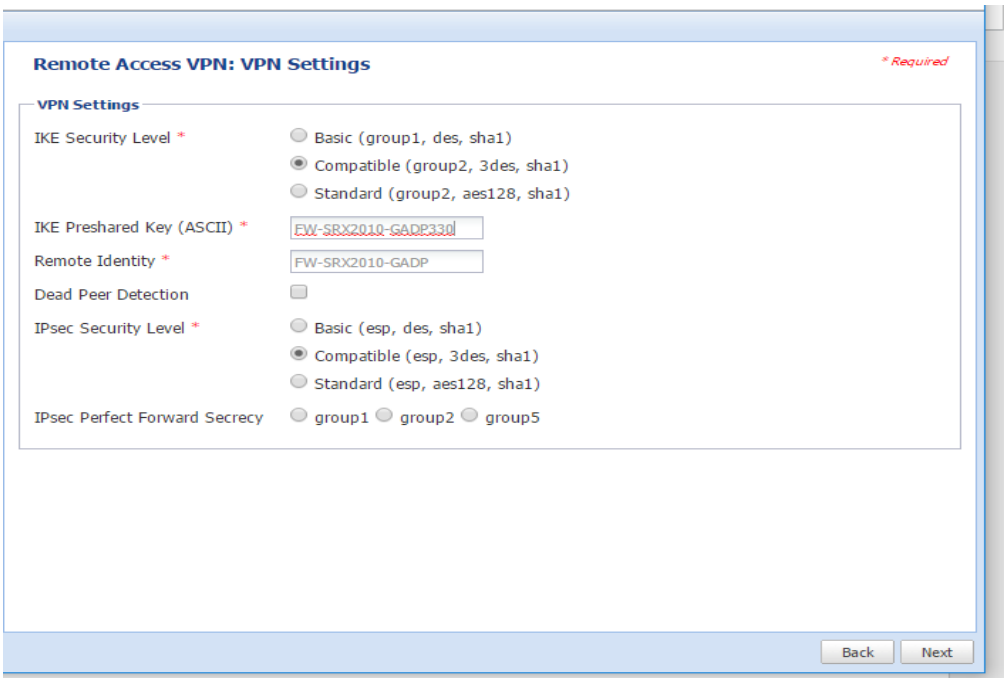
Elegimos la *Opción Remote Access VPN* y presionamos el Botón ***Start.***



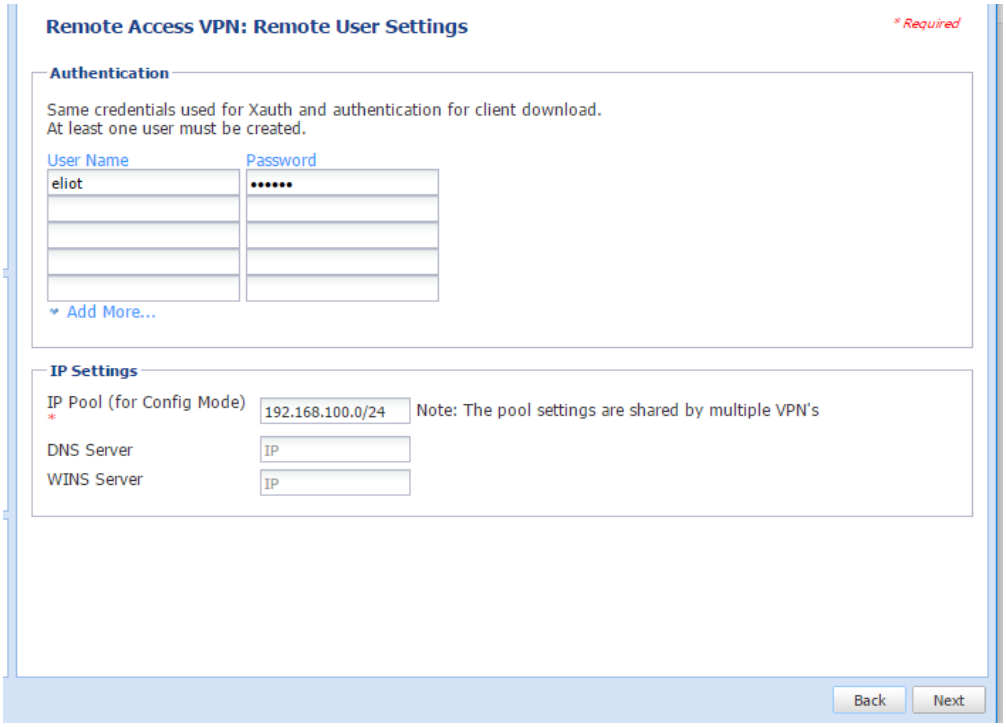
En la siguiente configuración asignamos los parámetros solicitados. En la sección Protected Network Zone: Servidores, Network: 192.168.6.0/24, y en la sección Public Network. interface por donde va ingresar la VPN Interface: ge-0/0/0.0 y la Zona: Internet. Luego pulsamos ***Next.***



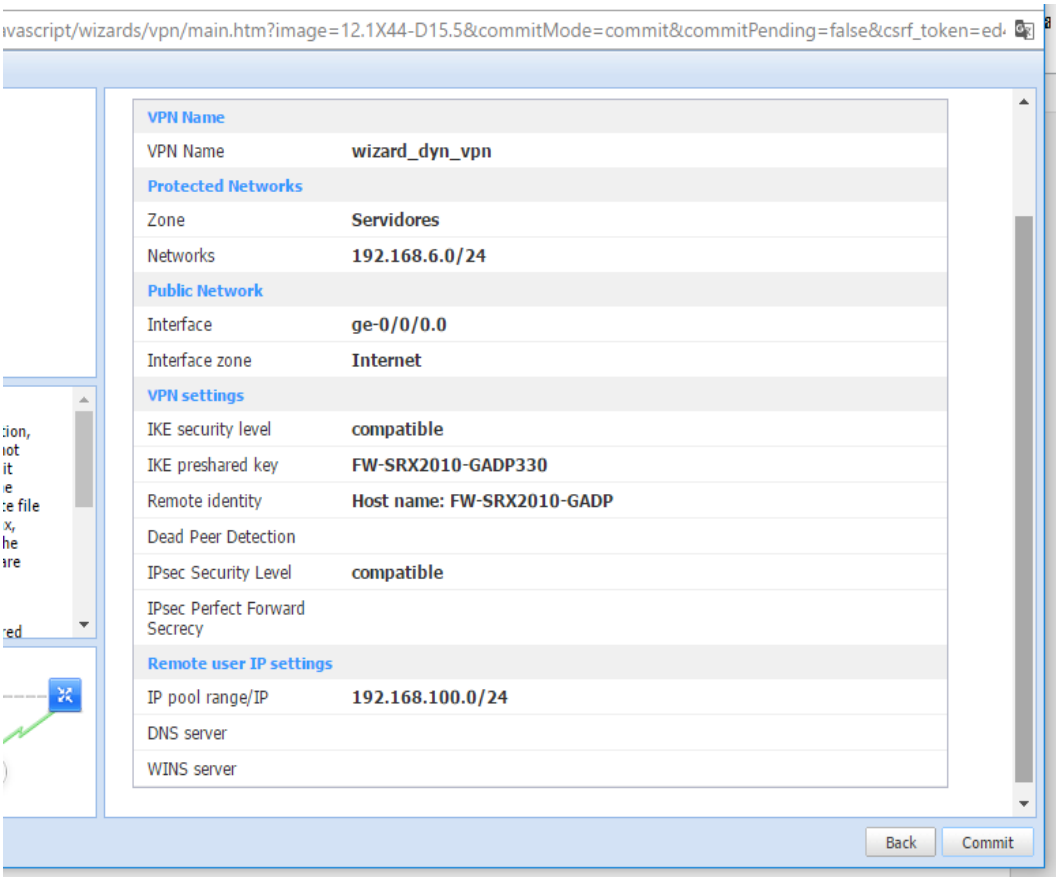
Algoritmos de encriptación y desencriptación se deja por defecto. Presionamos ***Next***.



Creación de usuarios y sus contraseñas, y en la sección IP settings *IP Pool (for Config Mode),* se asigna una red interna 192.168.100.0/24 para el nateo para poder ingresar a la zona deseada, eso significa que el trafico va ingresar nateando con ese segmento de red. Y presionamos ***Next***

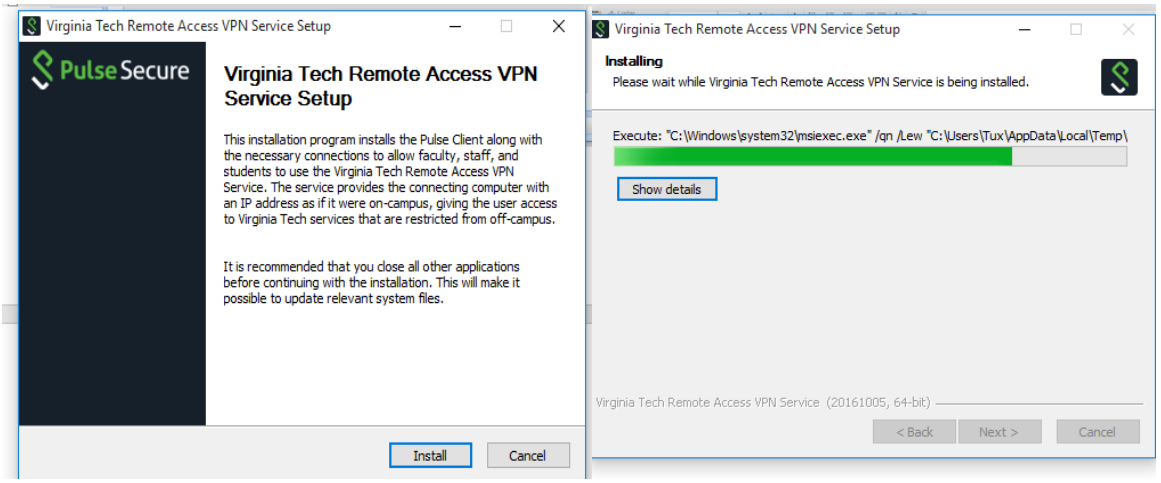


Finalmente, muestra un resumen y guardamos en ***Commint.***

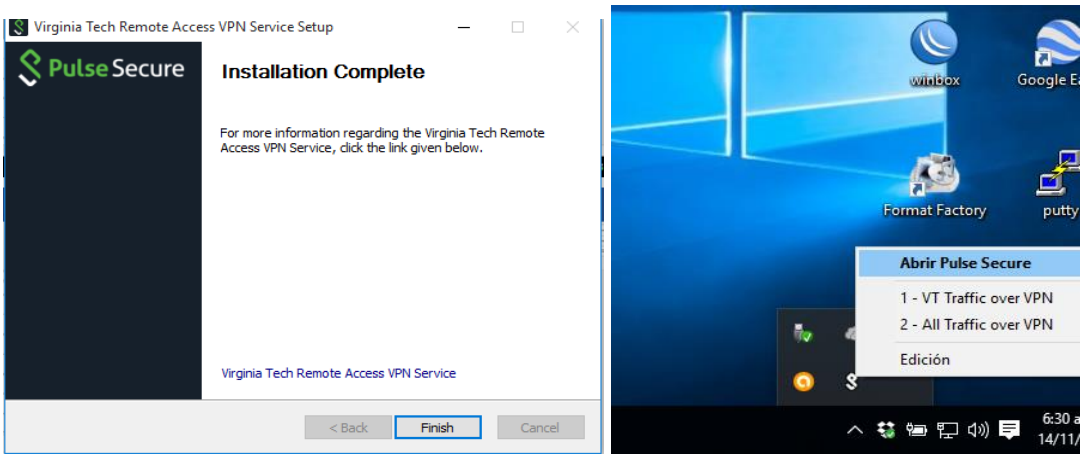


5.1.3.8 **Paso 8: Configuración de la aplicación Junos Pulse Cliente Remoto**

Clic derecho como administrador ejecutamos el instalador y presionamos ***Install***

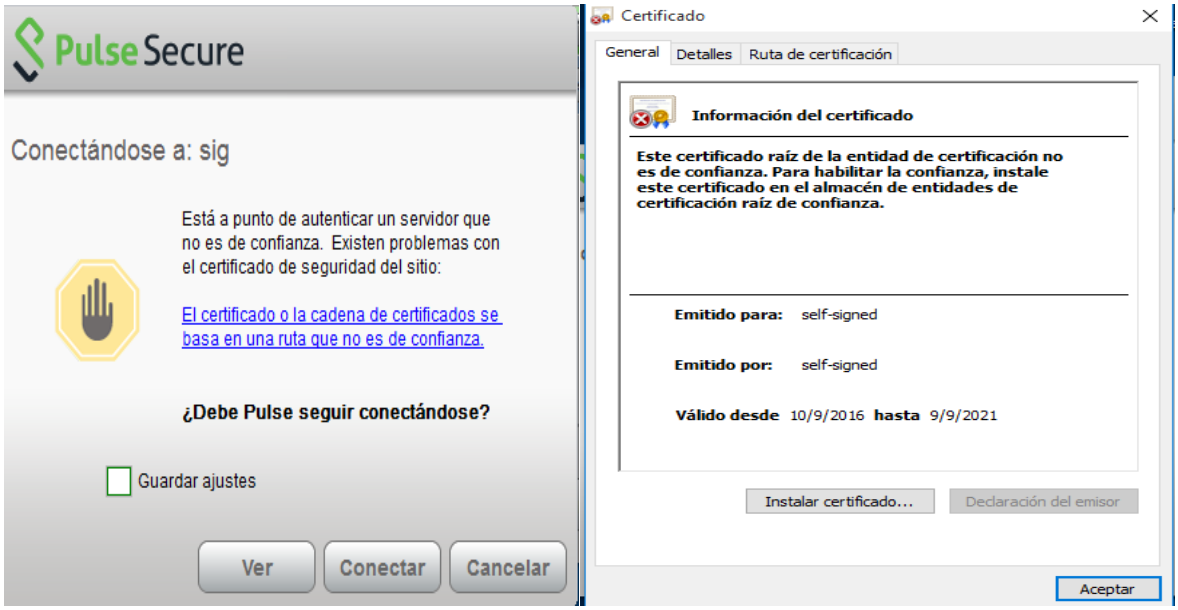


Finalizando la instalación y la ubicación para la configuración en la parte inferior derecha *Abrir Pulse Secure*

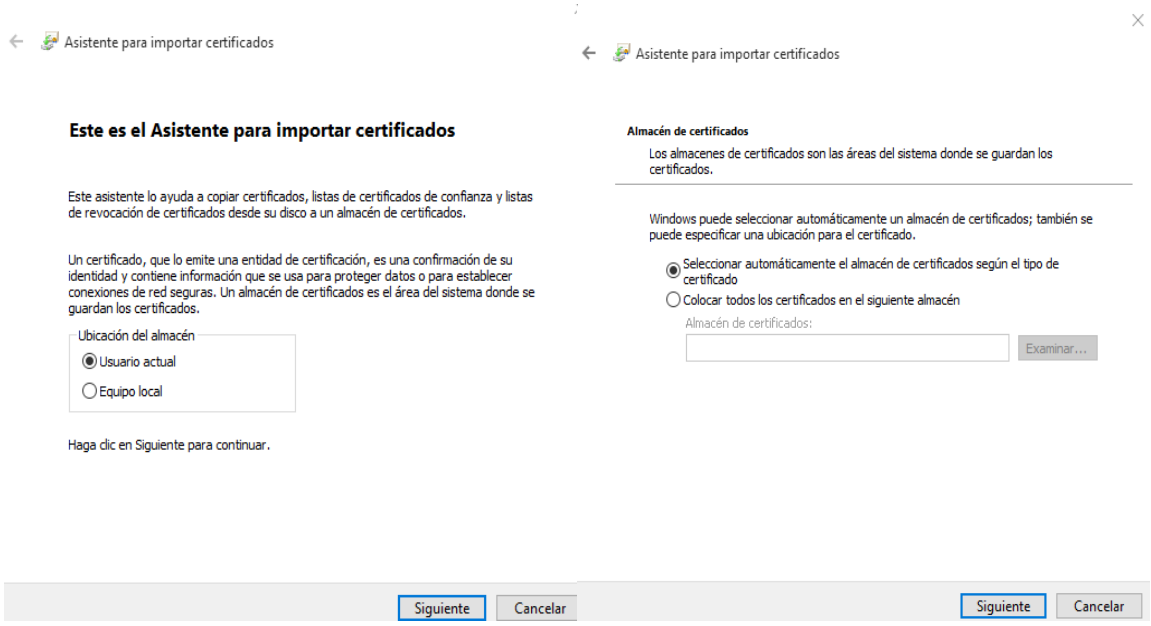


Añadimos una conexión para eso hacemos clic en el signo mas, tipo de conexión: SRX, asignamos un nombre: SIGMA y ingresamos la IP Pública del Firewall, ***Conectar.***

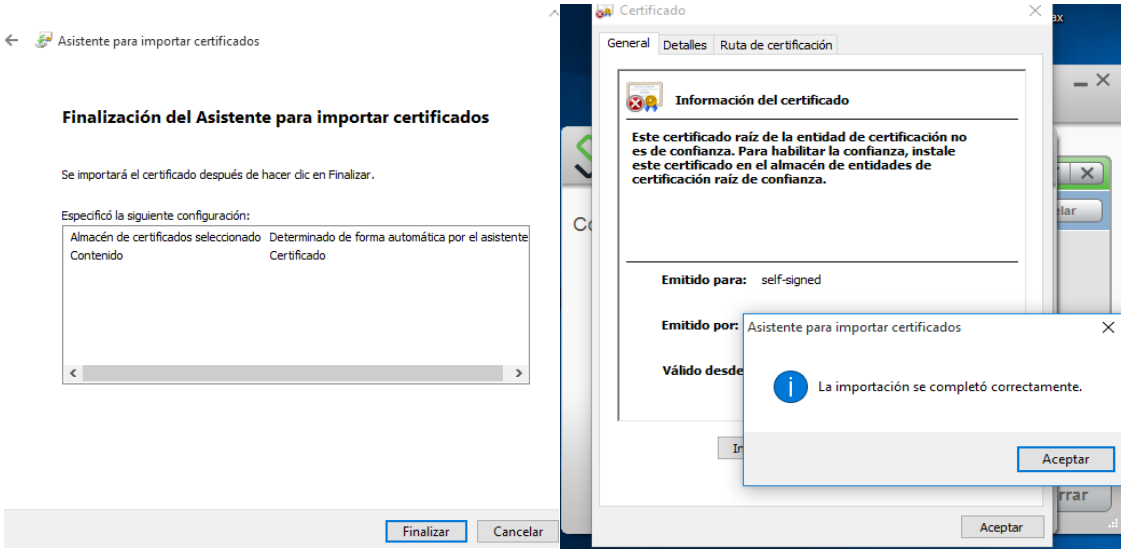
Automaticamente aparece el mensaje de autenticacion, pulsamos en el botón ***Ver.*** Despues aparcece el Certificado digital y presionamos el botón ***Instalar certificado.***



Ventana de asistente para importar el certificado lo dejamos por defecto y presionamos ***Siguiente.*** En la ventana de Alineación de certificados también se lo deja por defecto y clic en ***Siguiente.***



Para finalizar la instalación de los certificados presionamos el botón ***Finalizar***. Para confirmar aparece un mensaje y pulsamos en ***Aceptar***, y en la ventana de información del certificado presionamos ***Aceptar***.



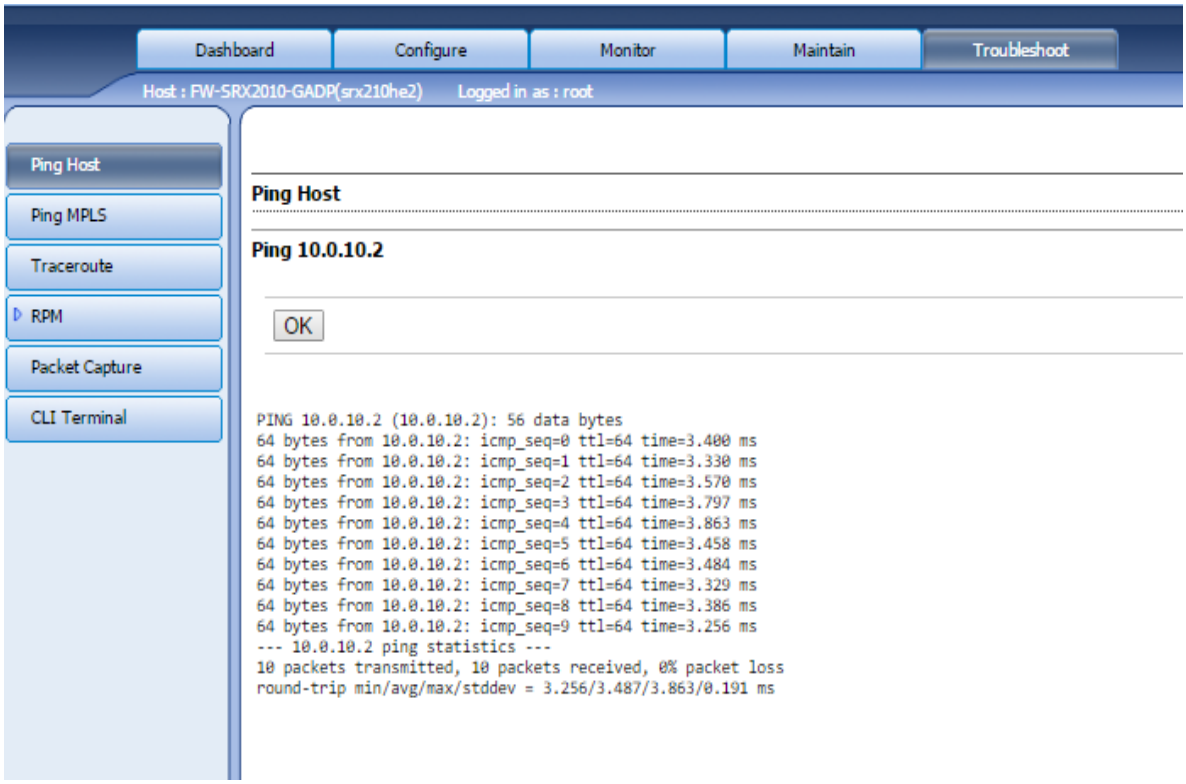
Empezamos a conectarnos pulsando el botón ***Conectar***. Una vez conectado en el siguiente cuadro solicitará el nombre del usuario y la contraseña establecida en el Firewall SRX establecidas en la anterior configuración.

Una vez finalizada la configuración del Firewall A, esa misma configuración se lo aplica a todos lo firewalls clientes, modificando los parámetros según lo requerido.

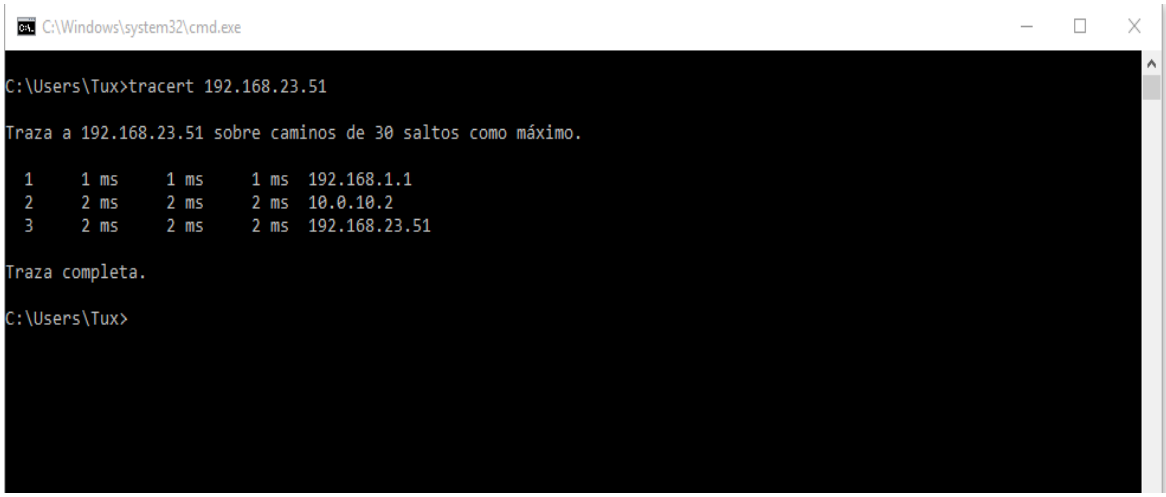
5.1.4 Fase (4) Pruebas

5.1.4.1 Prueba de Vpn sitio a sitio

Verificación ICMP a la otra interfaz virtual del Firewall B



Verificación de rutas.

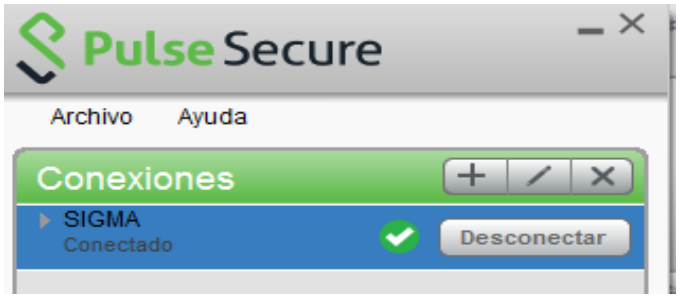


Verificación del servidor de aplicaciones SIGMA.

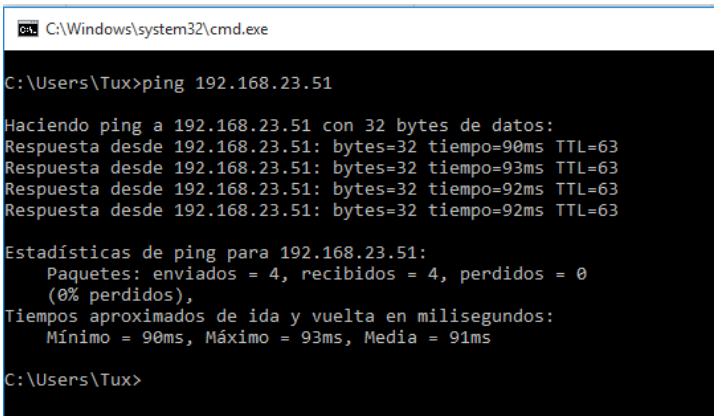
Verificación del servidor de SIGMA CENTRAL.

5.1.4.2 **Prueba de Vpn Aplicación**

Verificación de conexión de Vpn Usuarios móviles Acceso Remoto



Verificación ICMP



Verificación APLICACIÓN

Capítulo IV

CONCLUSIONES
RECOMENDACIONES
BIBLIOGRÁFICAS
ANEXOS

6 CONCLUSIONES

Debido a las ventajas económicas que ofrecen las Redes Privadas Virtuales se puede concluir que se trata de una excelente tecnología para el acceso remoto, puesto que el uso de una VPN constituye un sustituto indispensable a los métodos tradicionales caros de marcación telefónica de larga distancia. Además, constituye una buena solución alterna a los métodos de implementación de redes WAN tradicionales. Mientras mayor sea la VPN, el ahorro económico será mayor.

A lo largo del desarrollo del presente Trabajo de Grado, se ha estudiado la necesidad de disponer de la información contenida en los sistemas contables del GADP, a aquellos usuarios e instituciones descentralizadas que se encuentran aislados geográficamente del predio central de la Gobernación.

La cuestión de la seguridad en una VPN es muy importante. La gran mayoría de las organizaciones podrán ver satisfechas sus necesidades de seguridad con las tecnologías de seguridad existentes, pero siempre será necesario llevar un control estricto de la seguridad y mantener actualizada la VPN con los últimos avances en tecnología.

Una VPN podrá ser aplicada en todo tipo de entornos, desde las grandes empresas con sucursales en diversas partes del país o del mundo y varios trabajadores móviles hasta las pequeñas empresas que tengan una o dos sucursales en una sola ciudad; así como también las diversas dependencias del gobierno que necesiten intercambiar información entre ellas; e instituciones educativas como universidades y en general cualquiera que necesite acceder a sus archivos desde una ubicación remota de manera segura podrá obtener beneficios con esta tecnología.

7 RECOMENDACIONES

Al culminar este proyecto se plantea las siguientes recomendaciones a la institución:

- Implementación en las nuevas unidades descentralizadas creadas en los últimos años como ser SEDEPRO, SEDAGUA y otros.
- Aprovechar los beneficios del túnel para el acceso a nuevos sistemas implementados en la institución.

- Adquirir nuevos equipos de mayor capacidad para el buen funcionamiento
- Conseguir la licencia del módulo de VPN Acces Remote para más usuarios remotos.

8 BIBLIOGRAFÍA

Libros

Álvaro Gómez Vieites. (2006). *Tipos de Ataques e Intrusos en las Redes Informáticas.*

Andrew S. Tanenbaum y David J. Wetherall. (2012). *Redes de Computadoras 5 Ed.* México: Luis M. Cruz Castillo.

Arquitectura TCP/IP. (s.f.). Protocolo TCP/IP.

B., C. M. (2003). *Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de Enlace.* Ibarra.

Bruce A. Hallberg. (2007). *Fundamentos de Redes 4 Ed.* México: McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V.

Bruce Schneier. (96). *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source.*

Capacity Academy. (2016). *Técnicas y Mejores prácticas para la Seguridad Informática y el Hacking.* República Dominicana.

Cisco Networking Academy. (2015). *Principios básicos de enrutamiento y switching CCNA1 V5.*

Cisco Networking Academy. (2015). Principios básicos de enrutamiento y switching CCNA1 V5. En A. Ramirez.

Cisco System. (2001). *Ip Tuneling and VPN.*

Daniel Benchimol. (2010). *User Redes Cisco.* banfield lomas de zamora.

Gonzales, H. (2009). *Diseño de Topologia de Red VPN y VoIP para la Universidad Catolica Andres Bello.*

Instituto de Ciencia Básicas e Ingeniería. (2007). Implantación de una Red Privada Virtual. En E. A. Loa. México.

James S. Tiller. (2001). *IPSec Virtual Private Networks.* London: CRC Pres LLC.

Microsoft Corporation. (2016). *Point-to-Point Tunneling Protocol (PPTP).*

Ramírez, A. M. (2005). *ESTUDIO DE TECNOLOGIAS ENCONECTIVIDAD SEGURA Y SIMULACION DE LA TECNOLOGIA IPSEC PARA REDES DE COMUNICACION.* Santiago de Cali.

Teltad. (2007). *L2TP: Layer 2 Tunneling Protocol.*

Vicente José Aguilar Roselló, R. D. (2002). *Implementación de Redes Privadas Virtuales (VPN) Utilizando Protocolo Ipsec.*

William Satanllings. (2000). *Comunicaciones y Redes de Computadoras.* Granada.

Urls

CCM. (Junio de 2014). *TCP/IP*. Obtenido de CCM: http://es.ccm.net/contents/282-tcp-ip

Karen. (28 de Mayo de 2012). *Red Privada Virtual (VPN)*. Obtenido de http://karennz.blogspot.com/2012/05/componentes-de-una-vpn.html

MEFP. (noviembre de 2013). *http://www.economiayfinanzas.gob.bo/*. Obtenido de http://sigep.sigma.gob.bo/seguridad/faces/ingreso.jspx?_afrLoop=181776944032000&_afrWindowMode=0&_adf.ctrl-state=qz09gvqrp_4

Oviedo Miguel. (4 de Julio de 2012). *Redes Privadas Virtuales (VPN)*. Obtenido de http://redesprivadasvirtualesvpn.blogspot.com/2012/07/requerimientos-basicos-de-la-vpn.html

Publicas, M. d. (2010). *http://www.economiayfinanzas.gob.bo/*. Obtenido de http://sigma.gob.bo/produccion/php/index.php

Solutions, N. S. (22 de Octubre de 2013). *http://www.juniper.net/us/en/company/profile/*. Obtenido de www.juniper.net/us/en/ : http://www.juniper.net/es/es/products-services/routing/srx-series/

System, C. (s.f.). *http://www.cisco.com/*. Obtenido de http://www.cisco.com/web/LA/soluciones/la/vpn/index.html

Wikispaces by TES. (2015). *IW114GRUPO03*. Obtenido de http://iw114grupo03.wikispaces.com/2.+TIPOS+DE+ARQUITECTURA+VPN

ANEXOS

ANEXO 1

Constitución Política del Estado Plurinacional de Bolivia

TERCERA PARTE

Estructura y organización territorial del Estado

Título I

Organización Territorial del Estado

Capítulo Primero: Disposiciones Generales

Artículo 269. I. Bolivia se organiza territorialmente en departamentos, provincias, municipios y territorios indígena originario campesinos.

II. La creación, modificación y delimitación de las unidades territoriales se hará por voluntad democrática de sus habitantes, de acuerdo a las condiciones establecidas en la Constitución y la ley.

III. Las regiones formarán parte de la organización territorial, en los términos y las condiciones que determinen la ley.

Artículo 270. Los principios que rigen la organización territorial y las entidades territoriales descentralizadas y autónomas son: la unidad, voluntariedad, solidaridad, equidad, bien común, autogobierno, igualdad, complementariedad, reciprocidad, equidad de género, subsidiariedad, gradualidad, coordinación y lealtad institucional, transparencia, participación y control social, provisión de recursos económicos y preexistencia de las naciones y pueblos indígena originario campesinos, en los términos establecidos en esta Constitución.

Artículo 271. I. La Ley Marco de Autonomías y Descentralización regulará el procedimiento para la elaboración de Estatutos autonómicos y Cartas Orgánicas, la transferencia y delegación competencial, el régimen económico financiero, y la coordinación entre el nivel central y las entidades territoriales descentralizadas y autónomas.

Capítulo segundo: autonomía departamental

Artículo 277. El gobierno autónomo departamental está constituido por una Asamblea Departamental, con facultad deliberativa, fiscalizadora y legislativa departamental en el ámbito de sus competencias y por un órgano ejecutivo.

Artículo 278. I. La Asamblea Departamental estará compuesta por asambleístas departamentales, elegidas y elegidos por votación universal, directa, libre, secreta y obligatoria; y por asambleístas departamentales elegidos por las naciones y pueblos indígena originario campesinos, de acuerdo a sus propias normas y procedimientos.

II. La ley determinará los criterios generales para la elección de asambleístas departamentales, tomando en cuenta representación poblacional, territorial, de identidad cultural y lingüística cuando son minorías indígena originario campesinas, y paridad y alternancia de género. Los Estatutos Autonómicos definirán su aplicación de acuerdo a la realidad y condiciones específicas de su jurisdicción.

Fuente:

http://www.harmonywithnatureun.org/content/documents/159Bolivia%20Consitucion.pdf

ANEXO 2

LEY MARCO DE AUTONOMÍAS Y DESCENTRALIZACIÓN "ANDRÉS IBÁÑEZ"

LEY N° 031

LEY DE 19 DE JULIO DE 2010

TÍTULO III
TIPOS DE AUTONOMÍAS

CAPÍTULO I
AUTONOMÍA DEPARTAMENTAL

Artículo 30. (GOBIERNO AUTÓNOMO DEPARTAMENTAL). El gobierno autónomo departamental está constituido por dos órganos:

1. Una asamblea departamental, con facultad deliberativa, fiscalizadora y legislativa en el ámbito de sus competencias. Está integrada por asambleístas departamentales elegidos y elegidas, según criterios de población, territorio y equidad de género, por sufragio universal y por asambleístas departamentales representantes de las naciones y pueblos indígena originario campesinos. Las y los representantes de las naciones y pueblos indígena originario campesinos deberán ser elegidas y elegidos de acuerdo a sus normas y procedimientos propios.

2. Un Órgano Ejecutivo, presidido por una Gobernadora o Gobernador e integrado además por autoridades departamentales, cuyo número y atribuciones serán establecidos en el estatuto. La Gobernadora o Gobernador será elegida o elegido por sufragio universal en lista separada de los asambleístas.

Fuente:

http://www.ine.gob.bo/indicadoresddhh/archivos/alimentacion/nal/Ley%20N%C2%BA%20031.pdf

ANEXO 3

Estatuto Departamental de Pando

Fuente:

http://www.pando.gob.bo/wp-content/uploads/2015/09/EstatutoPando.pdf

ANEXO 4

Decreto Departamental N° 09/2016

ESTADO PLURINACIONAL DE BOLIVIA
GOBIERNO AUTÓNOMO DEPARTAMENTAL DE PANDO
Secretaría Departamental de Asuntos Jurídicos

DECRETO DEPARTAMENTAL N° 09/2016

Por la cual se aprueba la modificación de la Estructura Organizacional y el Manual de Funciones del Órgano Ejecutivo del Gobierno Autónomo Departamental de Pando.

Dr. Luis Adolfo Flores Roberts
GOBERNADOR DEL DEPARTAMENTO AUTONOMO DE PANDO

CONSIDERANDO:

Que, la Constitución Política del Estado en su Artículo 270, reconoce como principio el autogobierno a las Entidades Autónomas Departamentales.

Que, la Ley 031 del 19 de julio de 2010, Marco de Autonomías y descentralización "Andrés Ibáñez" en su Artículo 32 parágrafo I, señala que los órganos ejecutivos de los Gobiernos Autónomos Departamentales adoptarán una estructura orgánica propia de acuerdo a las necesidades de cada departamento.

Que, el Estatuto Autonómico Departamental de Pando en su Artículo 29, establece que corresponde al Gobierno Autónomo Departamental de Pando la elaboración de su propia estructura administrativa de acuerdo a sus necesidades, con apego a los principios generales contenidos en el Estatuto y las Leyes.

Que, la Ley Departamental Nº 025 del 03 de octubre de 2014 "Ley de Organización del Órgano Ejecutivo", establece la organización, composición, conformación del Órgano Ejecutivo Departamental, estableciendo sus atribuciones de acuerdo a normativa vigente. En su artículo 3 parágrafo IV, dispone que el Órgano Ejecutivo Departamental mediante Decreto Departamental establecerá la estructura jerárquica interna de las secretarías departamentales, entidades bajo su tuición y dependencia, autárquicas y Servicios departamentales, así como sus atribuciones específicas.

CONSIDERANDO:

Que, la Ley 1178, del 20 de julio de 1990 de Administración y Control Gubernamental, en su Artículo 7 inc. b), establece que toda entidad pública organizara internamente, en función de sus objetivos y la naturaleza de sus actividades, los sistemas de administración y control interno que trata la ley.

Que, las Normas Básicas del Sistema de Organización Administrativa, aprobada por Resolución Suprema N° 217055 de 20 de mayo de 1997, establece un conjunto ordenado de normas, criterios y metodologías que regulan el proceso de estructura organizacional de las entidades públicas. Así mismo manifiesta que la Estructura Organizacional es el conjunto de áreas y unidades organizacionales interrelacionadas entre sí, a través de canales de comunicación, instancias de coordinación interna y procesos establecidos por una entidad para cumplir con sus objetivos. La estructura organizacional se refleja en el Organigrama y Manual de Organización y Funciones.

Que, el artículo 9 de las Normas Básicas del Sistema de Organización Administrativa, dispone que el análisis, diseño e implantación de la estructura organizacional de la entidad es responsabilidad de la máxima autoridad ejecutiva y de los servidores públicos en su ámbito de competencia.

Que, el artículo 11 de las Normas Básicas del Sistema de Organización Administrativa, señala que la estructura organizacional de una entidad podrá adecuarse cuando se presenten circunstancias internas y/o del entorno que lo justifiquen, en el marco de las presentes normas y de las disposiciones legales vigentes en materia de organización.

CONSIDERANDO:

Que, el Informe U.D.O. Nº 11/2016, de fecha 20 de mayo de 2016, emitido por la Unidad de Desarrollo Organizacional del Gobierno Autónomo Departamental de Pando, en base al Informe Nº IN/UP14/Y15 U1 de fecha 20 de enero de 2016, emitido por la Contraloría General del Estado, producto de la evaluación de la Dirección de Auditoria Interna en la cual se recomienda, se ajuste la Estructura Organizacional, constituyendo una sola Unidad de Auditoria Interna bajo la dependencia del Gobernador y el Informe Cite D.A. Nº 33/2016, que identifica inconsistencias en relación a competencias, duplicidad de responsabilidades y funciones asignadas entre la Unidad de Bienes y Servicios y la Unidad de Activos Fijos; concluye que son justificativos técnicos para proceder a la modificación de la Estructura Organizacional y el Manual de Funciones del Órgano Ejecutivo del Gobierno Autónomo Departamental de Pando.

Que, el Informe Legal S.A.J/ D.G.A N° 204/2016 de fecha 23 de mayo de 2016, emitido por la Secretaria de Asuntos Jurídicos, concluye que los justificativos técnicos establecidos para la modificación a la Estructura Organizacional se enmarcan a lo establecido en el Artículo 11 de las Normas Básicas del Sistema de Organización Administrativa, siendo viable la modificación ya que el mismo no contraviene el ordenamiento jurídico y recomienda la aprobación de la modificación a la Estructura Organizacional y el Manual de Funciones del Órgano Ejecutivo del Gobierno Autónomo Departamental de Pando, mediante Decreto Departamental.

EN CONSEJO DE GABINETE,

DECRETA:

ARTICULO PRIMERO.- Aprobar las Modificaciones de la Estructura Organizacional y el Manual de Funciones del Órgano Ejecutivo del Gobierno Autónomo Departamental de Pando, aprobado mediante Decreto Departamental Nº 40/2015 en fecha 02 de junio de 2015 y que en anexo forman parte del mismo, de la siguiente manera:

1.- Se modifica el nivel de Dirección de Auditoria Interna por Unidad de Auditoria Interna, constituyéndose en una sola unidad bajo la dependencia del Gobernador, con responsables de Auditoria Interna en los Servicios Desconcentrados.

2.- Se suprime la Unidad de Activos Fijos.

ARTICULO SEGUNDO.- La Unidad de Desarrollo Organizacional deberá adecuar, actualizar y difundir las modificaciones a la Estructura Organizacional y Manual de Funciones del Órgano Ejecutivo del Gobierno Autónomo Departamental de Pando.

ARTICULO TERCERO.- El presente Decreto Departamental entrará en vigencia desde la fecha de su publicación en la Gaceta Oficial del Gobierno Autónomo de Pando.

Es dado en la sala de sesiones de la Gobernación del Departamento Autónomo de Pando, en la ciudad de Cobija a los veinticuatro días del mes de mayo de dos mil dieciséis años.

Dr. Luis Adolfo Flores Roberts
GOBERNADOR
DEPARTAMENTO AUTONOMO DE PANDO

Sr. Miguel García Bigabriel
SECRETARIO DEPARTAMAMENTAL
COORDINACIÓN GENERAL

Dr. Pedro Melgar Dorado
SECRETARIO DEPARTAMENTAL ASUNTOS JURÍDICOS

Ing. Gabriela Pereira Rosado
SECRETARIA DEPARTAMENTAL DE PLANIFICACION

Ing. Andróncles Puerta Velásquez
SECRETARIO DEPARTAMENTAL
ECONOMIA PLURAL

Dra. Katherine Shimekawa Von Boeck
SECRETARIA DEPARTAMENTAL
DESARROLLO HUMANO Y SOCIAL

Lic. Lizzy Yrene Herrera Pérez
SECRETARIA DEPARTAMENTAL
MADRE TIERRA

Ing. Oscar J. Terán Ayala
SECRETARIO DEPARTAMENTAL INFRAESTRUCTURA PARA EL DESARROLLO

Lic. José L. Dará Bazán
SECRETARIO DEPARTAMENTAL ECONOMÍAY FINANZAS

Sr. Pablo Rosel Marupa
SECRETARIO DEPARTAMENTAL ASUNTOS INDIGENAS

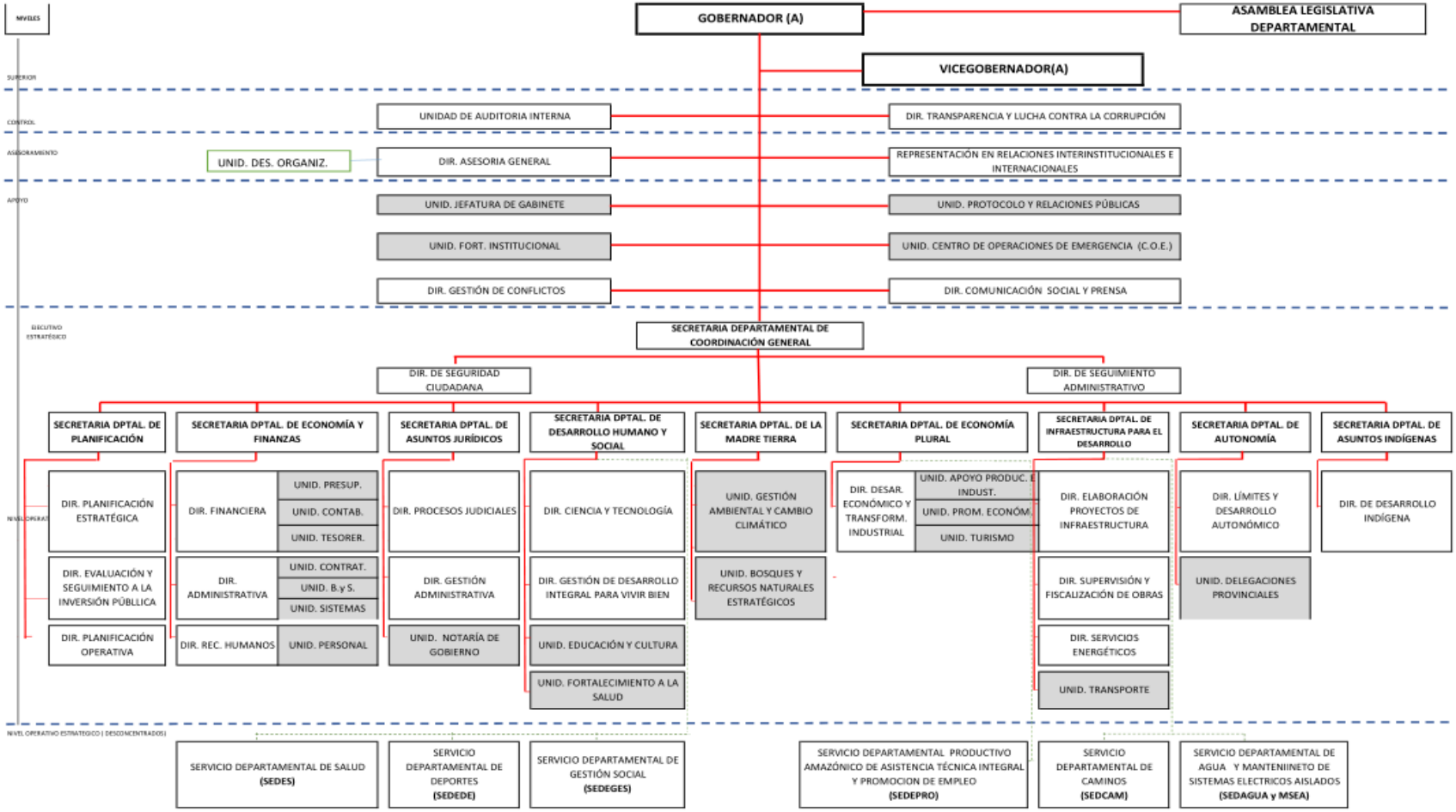
Lic. José L. Méndez Chaurara
SECRETARIO DEPARTAMENTAL DE AUTONOMÍA

Fuente:
http://www.pando.gob.bo/decretos-departamentales

ANEXO 5

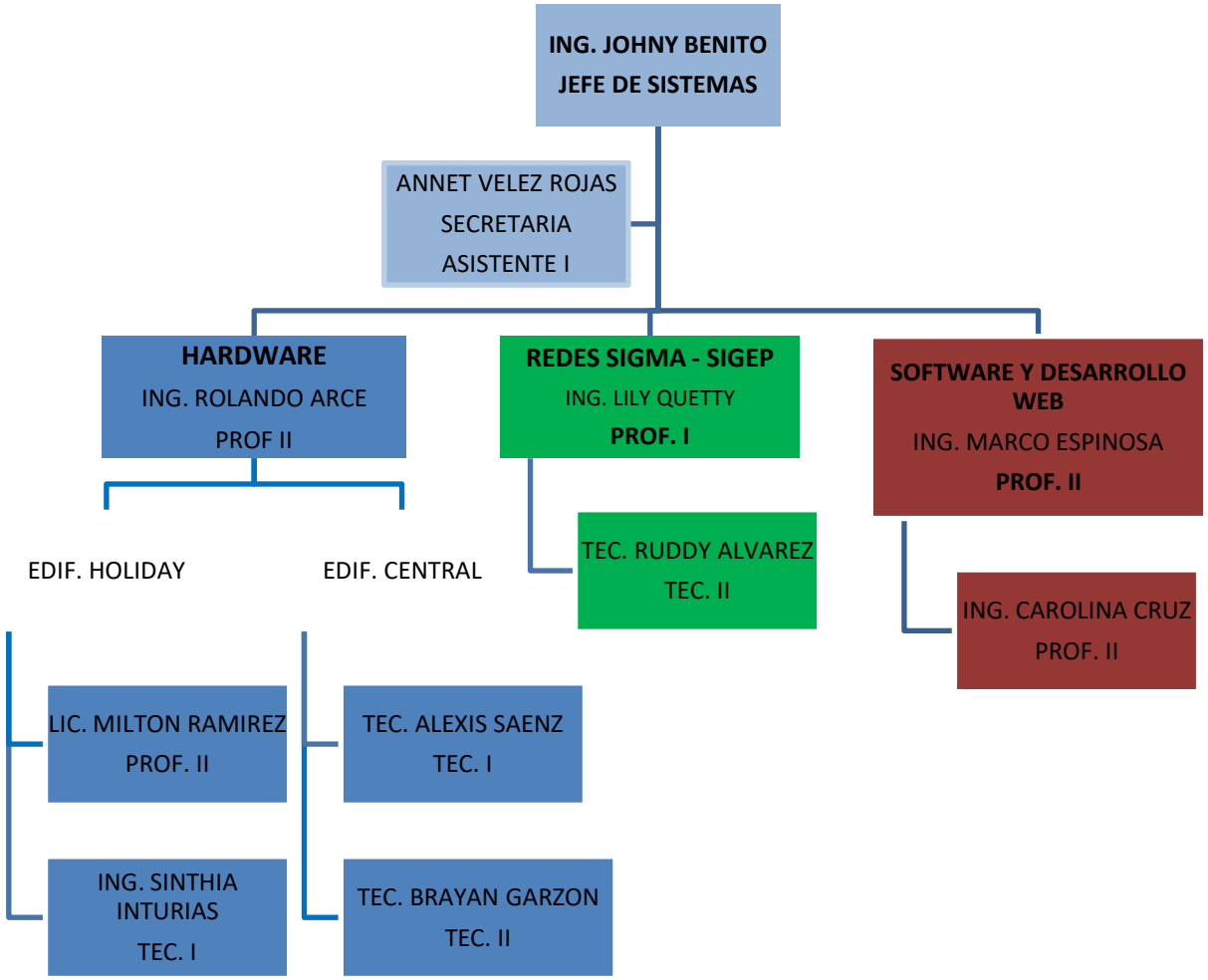
ESTRUCTURA ORGANIZACIONAL

GOBIERNO AUTÓNOMO DEPARTAMENTAL DE PANDO



ANEXO 6

PERSONAL DE LA UNIDAD DE SISTEMAS



JEFATURA	1
PROF. I	1
PROF. II	4
TEC. I	2
TEC. II	2
ASIST. I	1
TOTAL	11

ANEXO 7

Informe de entrega VPN de la configuración SEDEGES

ESTADO PLURINACIONAL DE BOLIVIA

GOBIERNO AUTONOMO DEL DEPARTAMENTO DE PANDO

S.S.S.S. Nº 17/2013

INFORME

GOBIERNO AUTONOMO DE PANDO
UNIDAD SISTEMAS INFORMATICOS
RECIBIDO
Hora: 11.00
Fecha: 27-03-2014
Firma

A : Lic. Milton Ramirez Linares
JEFE DE SISTEMAS INFORMATICOS
GOBIERNO AUTONOMO DE PANDO

DE : Eljot Dario Torrez Burgoa.
RESPONSABLE DE SIGEP-SIGMA-SIIF

FECHA : Cobija, 27 de noviembre 2013

REF : **CONFIGURACION JUNIPER SRX110 SEDEGES**

Por intermedio de la presente me dirijo a su autoridad, para informar la implementación del dispositivo Juniper SRX110 en las oficinas de la unidad descentralizada SEDEGES con las diferentes características requeridas para el uso de los Sistemas del Gobierno Autónomo Departamental de Pando y Sistemas del Ministerio de Economía y Finanzas.

Por otro lado también informarle que ya está en funcionamiento todos los sistemas y el mismo equipo firewall el cual permite acceder y manipular cada uno de los sistemas financieros que se maneja en la institución como en la sede de Gobierno.

A continuación presento a detalle cuadros relacionados con la configuración.

Es en cuanto informo para fines consiguientes.

ESTADO PLURINACIONAL DE BOLIVIA

GOBIERNO AUTONOMO DEL DEPARTAMENTO DE PANDO

CARACTERISTICAS DE IMPLEMENTACION JUNIPER SRX110

DATOS Y CARACTERISTICAS BASICAS	
Usuario de login	[redacted]
Passwd	[redacted]
Ip Real proporcionado por ISP	201.88.254.108
Mascara de sub red	255.255.255.0
Gateway	201.88.254.1
Dns	201.88.254.4 201.88.254.7

CARACTERISTICAS AVANZADAS			
Zonas, vlan e interfaces			
Zonas	Untrust	fe-0/0/0.0	
	Trust	vlan.0	fe-0/0/0.1 fe-0/0/0.2 fe-0/0/0.3
	sedeges	vlan.1	fe-0/0/0.4 fe-0/0/0.5 fe-0/0/0.6 fe-0/0/0.7
	Vpn	st0.0	

Ips y zonas		
Zonas	untrust	201.88.254.108/24
	trust	192.168.1.1/24
	sedèges	192.168.12.0/24
	vpn	10.0.10.0/24

Políticas establecidas						
From zone	To zone	Sourse address	Destination address	aplication	action	Log/count
trust	untrust	any	any	any	permit	yes

Interfaz enlace fe-0/0/0.0	Interfaz enlace ge-0/0/0.0
Ips real 201.88.254.108	Ip real 201.88.254.90
Instancias creadas Pashe I Pashe II	Instancias creadas Pashe I Pashe II
Ip intercambio 201.88.254.90	Ip intercambio 201.88.254.108

Observaciones
Implementación de las rutas, políticas, zonas, vlan, ips, nateo, routing, vpn. Son parte de la configuración para el funcionamiento del juniper. Sin embargo la configuración de la administración de la red, se tiene que añadir otras opciones más según a lo requerido de la institución. Por otro lado también se configuro un modem. El cual enlaza con el proveedor de servicio de internet dando de baja a un dispositivo y cambiando por otro que en la actualidad está en funcionamiento wan modo briged y lan dhcp. También se configuro su router WIFI en el rango que estable el juniper Otra de las observaciones y vale la pena resaltar que el ancho de banda no le favorece mucho.

ANEXO 8

Acta de conformidad SEDCAM

GOBIERNO AUTÓNOMO DEL DEPARTAMENTO DE PANDO
SERVICIO DEPARTAMENTAL DE CAMINOS

ACTA DE CONFORMIDAD

De fecha: 08 de Septiembre de 2011

En la institución del Sedcam en fecha 08 de septiembre 2011 en el Área de Sistemas se realizó un acta de conformidad del funcionamiento del sigma en el servicio departamental de caminos, Realizando la verificación y prueba del equipo del sigma se pudo evidenciar que están en funcionando con el ingreso al programa sigma que se menciona anteriormente.

Es por cuanto firmamos al pie del documento de conformidad.

Ing. Efraín Vásquez Pérez
RESPONSABLE DE SISTEMAS

Tec. Eliot Torrez Burgoa
TÉCNICO SISTEMAS

ANEXO 9

Acta de conformidad SEDES

MINISTERIO DE SALUD
Y DEPORTES

GOBIERNO AUTÓNOMO DEL DEPARTAMENTO DE PANDO
SERVICIO DEPARTAMENTAL DE SALUD
COBIJA - PANDO – BOLIVIA

SERVICIO DEPARTAMENTAL DE SALUD PANDO

Cobija, 08 de Septiembre del 2010

ACTA DE CONFORMIDAD

En las Instalaciones del Servicio Departamental de Salud en dependencias de la Unidad de Sistemas en fecha 08 de Septiembre del 2011, conste por la presente acta de conformidad, que a hasta la fecha el Sistema integrado de Gestión para la Modernización Administrativa (SIGMA), esta funcionando correctamente después de haber realizado las configuraciones pertinentes..

Es por cuando firmamos al pie del documento de conformidad.

RESPONSABLE DE SISTEMAS Y CONTROL DE PERSONAL
SEDES -PANDO

TÉCNICO DE SISTEMAS
GOBIERNO AUTÓNOMO DE PANDO

Av. 9 de febrero, Plaza Humbert Terrazas
Teléfono: (591) 3 - 842- 2502. Tel - Fax. 3 - 842-7473

ANEXO 10

Personal MEFP y GADP

ANEXO 11

Personal Configurando Firewall