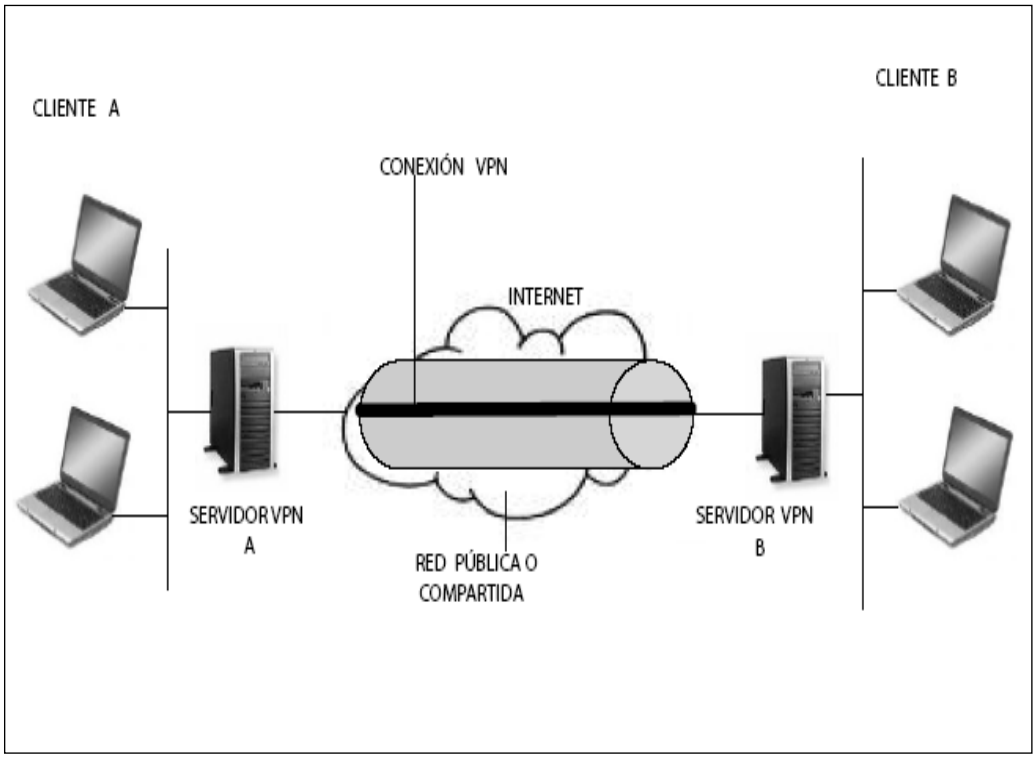
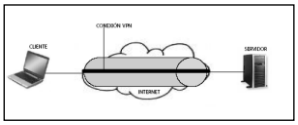
CAPÍTULO 3



INTRODUCCIÓN A LAS VPN'S



3.1 Definición De VPN

Una VPN (Virtual Private Network _ Red Privada Virtual) es una extensión de una red local y privada que utiliza un enlace de una red pública, por ejemplo Internet.

En una VPN normalmente se usa la red Internet como transporte para establecer enlaces seguros y una red WAN no tiene los suficientes elementos de seguridad en una red remota y es vulnerable que sea atacada por usuarios no conocidos, los dispositivos de una red WAN instalados en sus extremos también son encargados de realizar la conexión con los elementos de la red de área local en los puntos remotos a través de la WAN, pero los costos de estos equipos para diseñar una red WAN son altos y también se les tiene que dar un servicio de soporte técnico. Las VPN's se pueden enlazar en las oficinas corporativas con aliados comerciales o asociados de negocios, usuarios móviles, instituciones educativas y sucursales remotas mediante canales de comunicación seguros y utilizando protocolos de seguridad.

Una VPN no es más que una extensión de la red local de una entidad a la que se le agregan unas configuraciones y componentes de hardware y software que le permitan incorporarse a una red de recursos de carácter público como Internet y FrameRelay(El protocolo Frame Relay comparte varias características técnicas con el protocolo X.25, pero su comportamiento es más parecido al protocolo IP), pero manteniendo un entorno de carácter confidencial y privado que le permite al usuario trabajar como si estuviera en su misma red local. La comunicación entre los dos extremos de la red privada a través de la red pública se hace creando túneles virtuales entre esos dos puntos y usando sistemas de cifrado y autenticación que aseguren la

confidencialidad e integridad de los datos transmitidos a través de esa red pública.

3.2 Topologías VPN

Una VPN tiene distintas topologías que la conforman y se define según los requerimientos de la organización, institución educativa o laboratorio; existen tres tipos de topologías de una VPN que son: cliente a servidor, cliente a red interna y red interna a red interna , se puede utilizar cualquiera de las tres topologías para diseñar una VPN dentro de un modelo de seguridad.

a) **De cliente a servidor**: Un usuario remoto que sólo necesita servicios o aplicaciones desde el servidor o realizar una ejecución desde el mismo servidor VPN, esto puede realizarse tomando en cuenta que deben tenerse ciertos privilegios al momento de entrar al servidor VPN. (Figura 3.1).

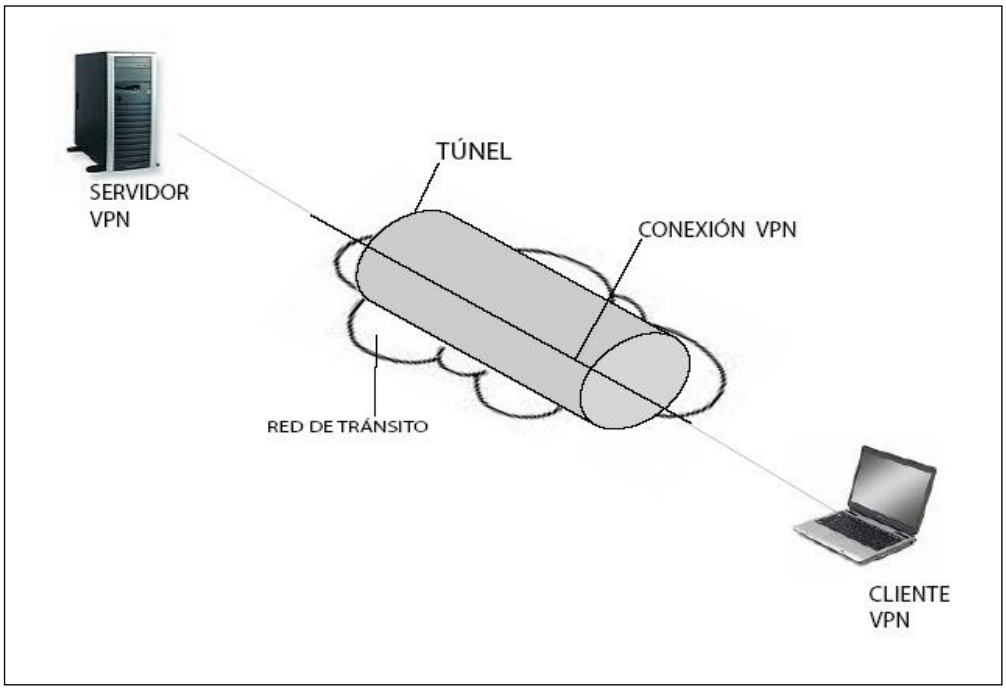


Figura 3.1 Una VPN de Cliente a Servidor

b) **De cliente a Red Interna (intranet)**: Un usuario remoto que requiere utilizar los servicios o aplicaciones que se pueden encontrar en uno o varios equipos de cómputo dentro de una misma red interna, este tipo de topologías se utiliza en las empresas, instituciones educativas, bancos etcétera, donde se realiza una infinidad de consultas que se requieren en un área de trabajo. (Figura 3.2).

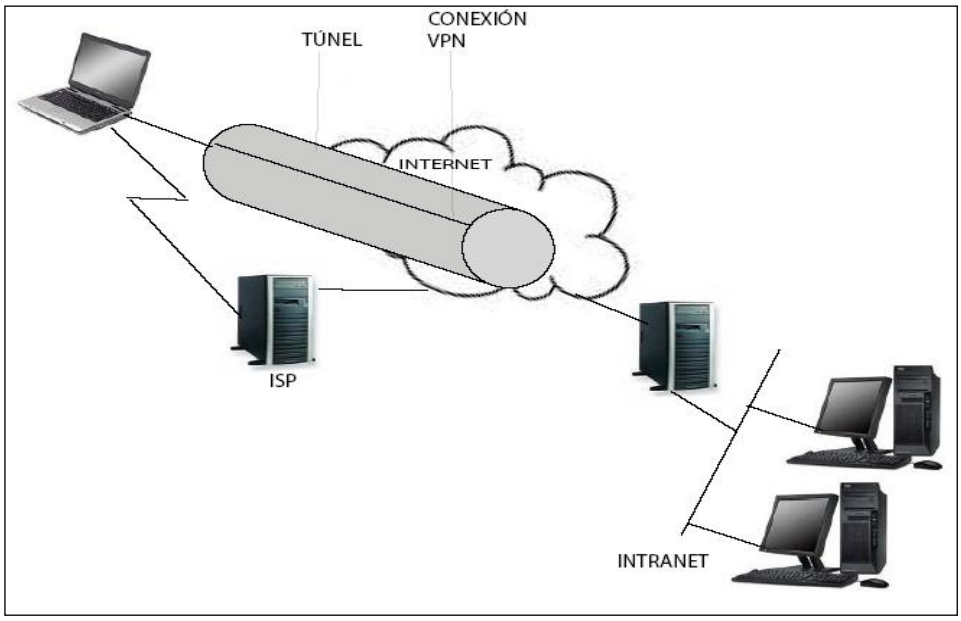


Figura 3.2 Una VPN de Cliente a Red Interna

c) **De Red Interna a Red Interna**: Tiene la posibilidad de unir dos intranets empleando dispositivos que son enrutadores, switches, etcétera, esto se puede hacer en las distintas áreas o departamentos que tienen su propia aplicación y sus servicios son distintos en ambos, esta conexión se puede hacer cuando se necesita de un dato desde un servidor VPN a otro servidor de una sucursal. (Figura 3.3)

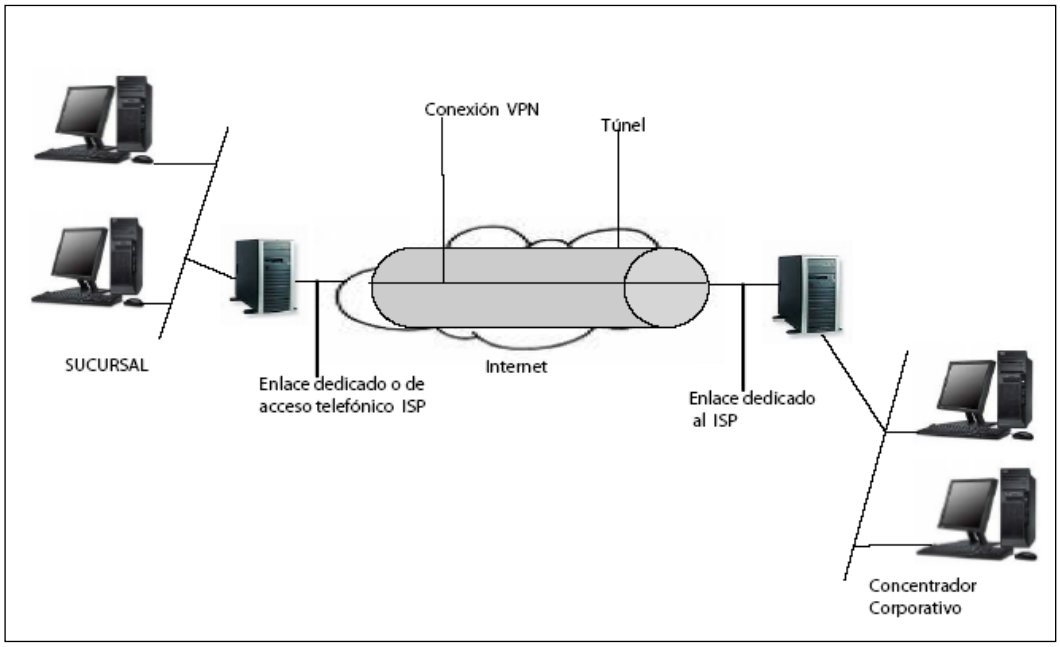
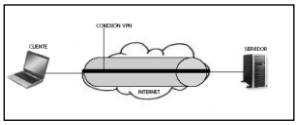


Figura 3.3 Una VPN de Red Interna a Red Interna

Las principales características de las topologías de las VPN´s son:

- **Un túnel**: Es aquella porción de la conexión en la que los datos están encapsulados. Los datos no tienen por qué estar forzosamente cifrados.
- **Protocolos de tonelaje**: Son estándares de comunicación utilizados para gestionar el túnel y encapsular los datos privados.
- **Red de Tránsito**: Es la red pública o compartida por lo cual circulan los datos. Puede tratarse de Internet o de una intranet basada en IP privada.
- **Un servidor VPN**: Es una computadora que acepta conexiones VPN de clientes VPN.
- **Un cliente VPN**: Es una computadora que inicia conexiones desde un enrutador o una computadora individual.



3.3 Ventajas y Desventajas de las VPN´s

3.3.1 Ventajas de las VPN's

Dentro de las numerosas ventajas que proporciona este protocolo, la más destacable es que permite construir una red segura sobre redes públicas, eliminando la gestión y el costo de las líneas dedicadas, ofreciendo al trabajador que se encuentra fuera de la sede, empresa o institución educativa, la misma seguridad que si realizara una actividad sobre una red de área local de la empresa. A continuación se mencionan algunas características principales que tienen las ventajas de las VPN´s.

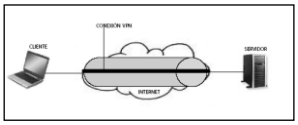
- **SEGURIDAD**: Provee cifrado y encapsulación de datos lo que permite que éstos viajen codificados y a través de un túnel seguro.

- **COSTOS:** Ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.

- **MEJOR ADMINISTRACIÓN**: Cada usuario que se conecta puede tener un número de IP fijo. Asignado por el administrador, lo que facilita algunas tareas, como por ejemplo: mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.

- **FACILIDAD**: Los usuarios con poca experiencia pueden conectarse a grandes redes corporativas transfiriendo sus datos de forma segura.

- **SIN CABLES**: A través de la red común sin tener que disponer de ningún dispositivo ni de ningún software complejo. Este avance ha



permitido que una persona con una portátil o PC y una conexión a la red pudiera operar con total tranquilidad sin temer que su información altamente confidencial pueda ser vista o alterada.

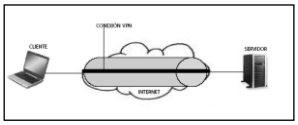
3.3.2 Desventajas de las VPN's

Las VPN's han representado una magnífica solución para las empresas, corporaciones, bancos e instituciones educativas en cuanto a la seguridad, confidencialidad e integridad de los datos, por esto se han vuelto tan importantes para las organizaciones, bancos, universidades, ya que reduce el costo de la transferencia de datos de un lugar a otro.

Es conveniente planear primero cómo se deben establecer las políticas de seguridad y el control de acceso porque al no estar bien definidos pueden existir serios problemas en el diseño de las VPN's. A continuación se menciona algunos puntos importantes:

a) No se garantiza la disponibilidad de Internet por medio de una VPN si no existe una planificación u organización en el diseño de una red segura.

b) No se garantiza la gestión de claves de acceso y autenticación, si no se plantea una política de crear claves con ciertas medidas de seguridad y especificar el tamaño de la contraseña.



c) Se debe diseñar una red bien definida, dependiendo de las necesidades de la organización o institución educativa; de la aplicación que se quiere instalar para poder procesar la información, por ejemplo: servidor de base de datos, correo, página Web.

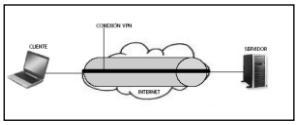
3.4 Tipos de VPN

Existen dos tipos de VPN que son: Hardware y Software, esto indica que existen implementaciones de mayor facilidad para el usuario que quiera diseñar una VPN, configurar y administrar los recursos de un servidor VPN. Se deben implementar algunos criterios de selección al momento de escoger el tipo de VPN que se quiere aplicar dentro de una empresa, negocio y escuela.

- **HARDWARE**

Las VPN's que se basan en hardware utilizan equipos dedicados como por ejemplo: los routers, switches, firewalls; son seguros y fáciles de usar para poder ofrecer un rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo, por lo cual utiliza muchos recursos del procesador para brindar otros servicios.

Los equipos dedicados son de fácil implementación y buen rendimiento, sólo que su costo es muy alto y poseen sistemas operativos propios; también se requiere de un servicio de soporte técnico con el proveedor del equipo que se compró para la organización. Además es responsabilidad del proveedor de darles algunas indicaciones de su manejo y uso y proporcionarles manuales de usuarios y técnicos.



- **SOFTWARE**

Las VPN's que están basadas en software se caracterizan por su flexibilidad, simplicidad en su configuración y adaptación a varias plataformas. Existen diferentes tipos de software libre para la implementación de una VPN que son: OPENVPN, OPENSWAN, STRONGSWAN, POPTOP, TRADEWARE y F-SECURE VPN. Dependiendo del software seleccionado para la implementación de una VPN en una empresa o institución educativa, lo primero que debe considerarse son las principales características de funcionamiento del equipo de cómputo, protocolo que se va a emplear, versión del kernel, las tarjetas de red alámbricas e inalámbricas, también se deben verificar si los controladores son compatibles con las distintas marcas de equipos de cómputo que existen en el mercado.

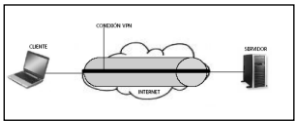
El Kernel de sistema operativo que tenga el Linux en sus distintas versiones que son: Fedora, RedHat, Suse, Ubuntu y otros más; es de suma importancia, porque el kernel es el núcleo principal de Linux, se puede definir como el corazón de este sistema operativo y es el encargado de que el software y el hardware de tu ordenador puedan trabajar juntos y que tenga una mejor administración en la memoria y en el procesador.

A continuación se nombran algunas de las principales características que tiene el software en general:

1) Soporta IP's dinámicas.

2) Adaptación para trabajar en redes remotas, tanto los clientes como los administradores pueden estar trabajando con IP's privadas.

3) Multiplataforma que se puede trabajar en diferentes sistemas operativos que son: Linux, Solaris, OpenBSD, FreeBSD, Mac OS X y Wndows 2000/XP/Server 2000/Server 2003.



4) Soporta múltiples conexiones, sólo con un puerto.

5) Requiere muy pocos parámetros de instalación para el administrador durante la instalación inicial.

6) Tiene un editor de red gráfico que permite configurar la totalidad de la red VPN desde una simple estación de trabajo.

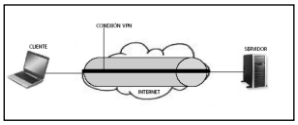
7) Las VPN's pueden aumentar la velocidad en las conexiones entre puntos empresariales gracias a que comprimen todo el tráfico añadiéndoles cifrado.

8) Usa una extensa variedad de algoritmos de cifrado para la selección de usuarios, incluyendo 3DES, RSA, DSA, AES.

3.5 Seguridad en las VPN's

La seguridad en las VPN's es el particionamiento de las redes públicas o de uso compartido para implementar las VPN's que son adjuntas. Esto se logra mediante el uso de túneles que son técnicas de encapsulado de tráfico. Las técnicas que se utilizan para que cualquier protocolo sea transportado entre dos puntos de la red encapsulado en otro protocolo son típicamente IP, L2TP(Layer 2 Tunneling Protocolo - Protocolo Túnel de Capa 2) que permite el armado de túneles para las sesiones PPP(Point to Point Protocolo - Protocolo Punto a Punto) remotas, y por último IPSEC para la generación de túneles con autenticación y cifrado de datos.

Se mencionan a continuación las principales características de la seguridad que brindan las VPN's para contar con una mejor administración en el servidor VPN y conocer los beneficios que brinda al negocio o a las dependencias públicas



A) Proveen seguridad en comunicaciones de voz, datos y video a través de redes públicas de datos como Internet al emplear túneles de IPSEC, servicios de cifrado y autenticación que logran mantener la integridad de las comunicaciones.

B) Los servicios de Firewall que crean una barrera segura contra ataques provenientes de Internet.

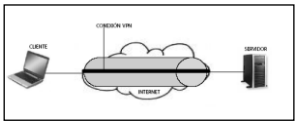
C) Cuentan con dispositivos que gestionan un acceso confiable a los usuarios de la red interna a través de servicios seguros de autentificación de ataques.

D) **"Los certificados de equipo son el método de autenticación recomendado ya que proporciona autenticación segura y son muy difíciles de suplantar o vulnerar. La autenticación de equipo requiere una infraestructura de claves públicas para emitir certificados de equipo al servidor VPN y a todos los equipos cliente VPN".**[1]

3.6 Decisiones al utilizar una VPN

Hace algunos años no era tan importante conectarse a Internet por motivos laborables, pero a medida que ha pasado el tiempo las corporaciones han requerido que las redes de área local (Local Area Network, LAN) trasciendan mas allá del ámbito local para incluir al personal y centros de información de otros edificios, ciudades, estados e incluso otros países. En contrapartida, era necesario invertir en hardware, software y en servicios de telecomunicaciones costosos para crear redes amplias de servicios (Wide Area Network, WAN). Sin embargo, con Internet, las corporaciones tienen la posibilidad de crear una red privada virtual (VPN) que demanda una inversión relativamente baja utilizando Internet para la conexión entre diferentes localidades o puntos. Las VPN's utilizan protocolos especiales de seguridad que permiten únicamente al personal

[1] http://openvpn.net/relnotes.html



autorizado, obtener acceso a servicios privados de una organización, cuando un empleado se conecta a Internet, la configuración VPN le permite conectarse a la red privada de la compañía o institución educativa y navegar en la red como si estuvieran localmente en la oficina o en algún otro sitio de la institución.

3.7 Protocolos VPN's

Los principales protocolos que se pueden implementar en un servidor VPN son:

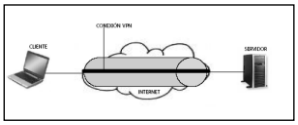
A) Protocolo PPTP

El protocolo fue originalmente designado como un mecanismo de encapsulamiento para permitir el transporte de protocolos diferentes del TCP/IP, como por ejemplo IPX sobre la red Internet. La especificación es bastante genérica y permite una variedad de mecanismos de autenticación y algoritmos de cifrado. El protocolo PPTP (Point-to-Point Tunneling Protocol - Protocolo de Túnel Punto a Punto) es un protocolo que permite establecer conexiones con túneles PPP, a través de una red IP, creando una VPN. La compañía Microsoft, ha implementado sus propios algoritmos y protocolos con soporte PPTP, es uno de los más ampliamente extendidos, por la popularidad de los productos Microsoft (Windows 98/ME/NT4/2000/XP/VISTA) los cuales llevan incluidos de serie estos protocolos.

Este protocolo fue desarrollado por el Forum PPTP que está constituido por las siguientes organizaciones: Ascend Communications, Microsoft Corporation, 3com/Primary Access, ECI Telematics and U.S Robotics.

B) Protocolo IPSec

El protocolo IPSec (Protocolo de Seguridad para Internet) proporciona confidencialidad e integridad de los paquetes IP. Los paquetes normales de IPv4 están compuestos de una cabecera y una carga, ambas partes contienen información útil para el atacante. La cabecera contiene la dirección IP, la cual es



utilizada para el encaminamiento, y puede ser aprendida para ser usada más tarde con técnicas de spooffing (suplantación).

"El protocolo IPSec proporciona seguridad mediante dos protocolos ESP (Encapsulating Security Payload - Cargar para el Encapsulamiento de la Seguridad) o AH (Authentication Header - Protocolo de Autenticación), básicamente ESP cifra los datos y los autentica, mientras que AH sólo los autentica. El IPSec es una buena solución para mantener la confidencialidad de los datos. Ofrece una comunicación segura host a host."[2]

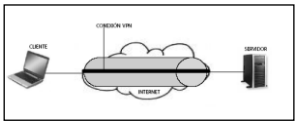
Este protocolo tiene dos modos de funcionamiento, modo transporte y modo túnel.

1. En el modo transporte el cifrado se realiza extremo a extremo, del host origen al host destino, por lo tanto, todos los hosts deben contar con IPSec.

2. En el modo túnel el cifrado se efectúa únicamente entre los routers de acceso a los hosts implicados. Con el modo túnel el cifrado se integra de manera eficiente, los mismos dispositivos que se encargan de crear los túneles integran el cifrado.

Los enlaces seguros de IPSec son definidos en función de SA (Segurity Associations - Asociaciones de Seguridad). Cada SA está definida para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo

[2] Markus Feilner, OpenVPN, Packt Publishing, Ed. 32, EUA, 2006, p17-20



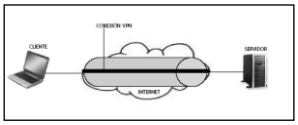
tráfico distinguible por un selector único. Todo el tráfico que fluye a través de una SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varias SA, cada uno de los cuales aplica cierta transformación. Los paquetes entrantes pueden ser asignados a una SA específica por los tres campos definidos por la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad.

C) Protocolo LTF

El protocolo LTF (Layer Two Forwarding - Protocolo de Envío de Dos Capas) fue desarrollado por Cisco y ha llegado a convertirse en uno de los protocolos de encapsulamiento más utilizados sobre todo a nivel hardware. La base sobre la que se asienta LTF es la misma que para PPTP, se trata de un verdadero protocolo de encapsulamiento que ha de efectuar incluso aquellas funciones que realiza PPP cuando viaja sin encapsulamiento alguno. Por lo general, LTF suele utilizarse para encapsular PPP, pero también existe la posibilidad de encapsular otros protocolos, como SLIP.

En términos generales, un paquete encapsulado con LTF se compone de una cabecera de paquete, una serie de datos y opcionalmente una firma que puede haber sido implementada o no por el fabricante de la solución VPN que se esté utilizando. La cabecera de un paquete LTF contiene, entre otras cosas, la prioridad del paquete que implementa en cierta forma un sistema QoS, además de otros elementos vistos antes en otros protocolos. Como el número de secuencia de los paquetes o su longitud del paquete.

Debido al encapsulamiento de PPP, LTF tiene que mantener ciertos servicios de cara a posibles problemas con el sistema de transmisión, algo que ya implementa de por sí PPP, pero que al estar éste encapsulado no puede utilizar. Entre las funciones de mantenimiento y sus características de LTF se encuentra la necesidad de mantener el flujo de datos dentro del túnel que funciona mediante este protocolo. El protocolo LTF debe ser capaz de reconocer un



retardo en el flujo de datos procedente de la red fuente, de un corte en el túnel que conforma la columna vertebral de la VPN.

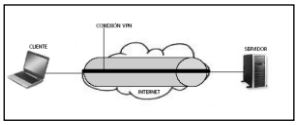
D) Protocolo L2TP

Todas las tecnologías de encapsulamiento que se han ido desarrollando en torno a PPP y que le han ido añadiendo nuevas características a la encapsulación real de PPP lo ha recogido L2TP, un nuevo protocolo que aún es desarrollado por L2TP y PPTP. El protocolo L2TP está pensado para acceder a entornos de traducciones de direcciones de red (NAT – Traducción de Direcciones de Red) desde clientes alejados geográficamente que no pueden mantener constantes llamadas internacionales. La solución más idónea a este tipo de situación es la utilización por parte del usuario de algún tipo de red global, ya sea Internet o la red de alguno de los muchos operadores de telecomunicaciones.

La arquitectura general de un sistema VPN basado en L2TP se basa en una red con tres nodos principales: el nodo de partida donde se sitúa el usuario que pretende enviar los datos, un nodo final o destino y un nodo intermedio encargado de transmitir los datos del usuario fuente al nodo de destino situado en un punto no accesible al usuario local, mediante el uso de una o varias redes públicas.

3.8 Categorías de las VPN’S

Las VPN’s se dividen en 3 categorías de acuerdo con el servicio de conectividad que pueden brindar las VPN’s :



1) **VPN de Acceso Remoto** : Provee acceso remoto a la intranet o extranet corporativa a través de la infraestructura pública, conservando las mismas políticas de seguridad y calidad de servicio que en la red privada, también permite el uso de múltiples tecnologías como ISDN, xDSL, cable UTP y una IP para la conexión segura de usuarios móviles o sucursales remotas a los recursos corporativos. (Figura 3.4).

Las principales características que tiene una VPN de acceso remoto son:

A) Outsourcing de acceso remoto.

B) Instalación y soporte del PS (Proveedor de servicio)

C) Acceso únicos al nodo central.

D) Tecnologías de acceso RTC, ISDN, xDSL.

E) Movilidad IP.

F) Seguridad reforzada por el cliente AAA (Autentificación, autorización y confidencialidad) en el ISP (Proveedor de servicios de Internet).

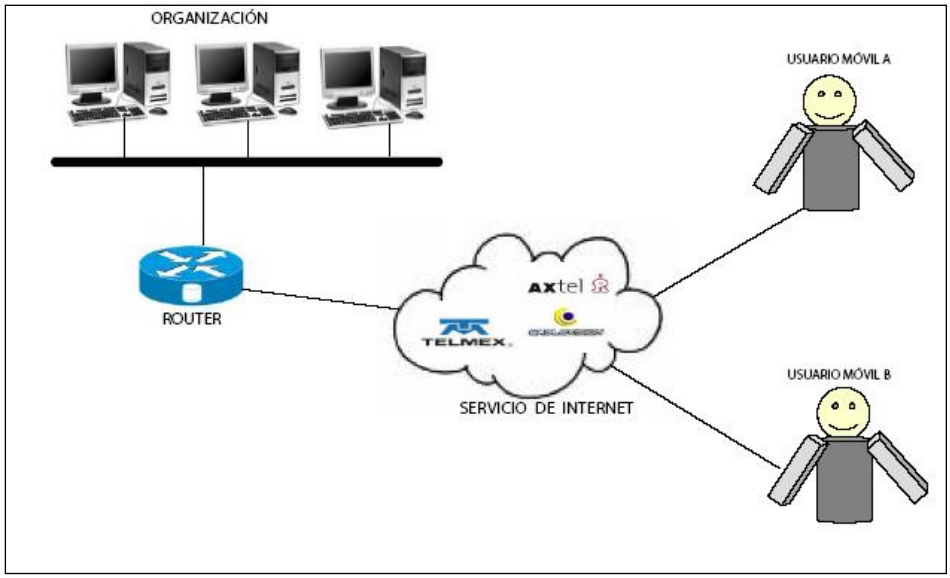
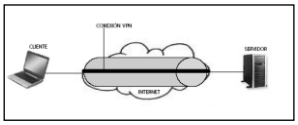


Figura 3.4 Una VPN de Acceso Remoto



2) **VPN de Intranet:** Vincula la oficina remota o sucursal a la red corporativa a través de una red pública, mediante un enlace dedicado al proveedor de servicio. (Figura 3.5).

La VPN goza de las mismas cualidades que la red privada que son: seguridad, calidad de servicio y disponibilidad. También extiende el modelo IP a través de la WAN compartida.

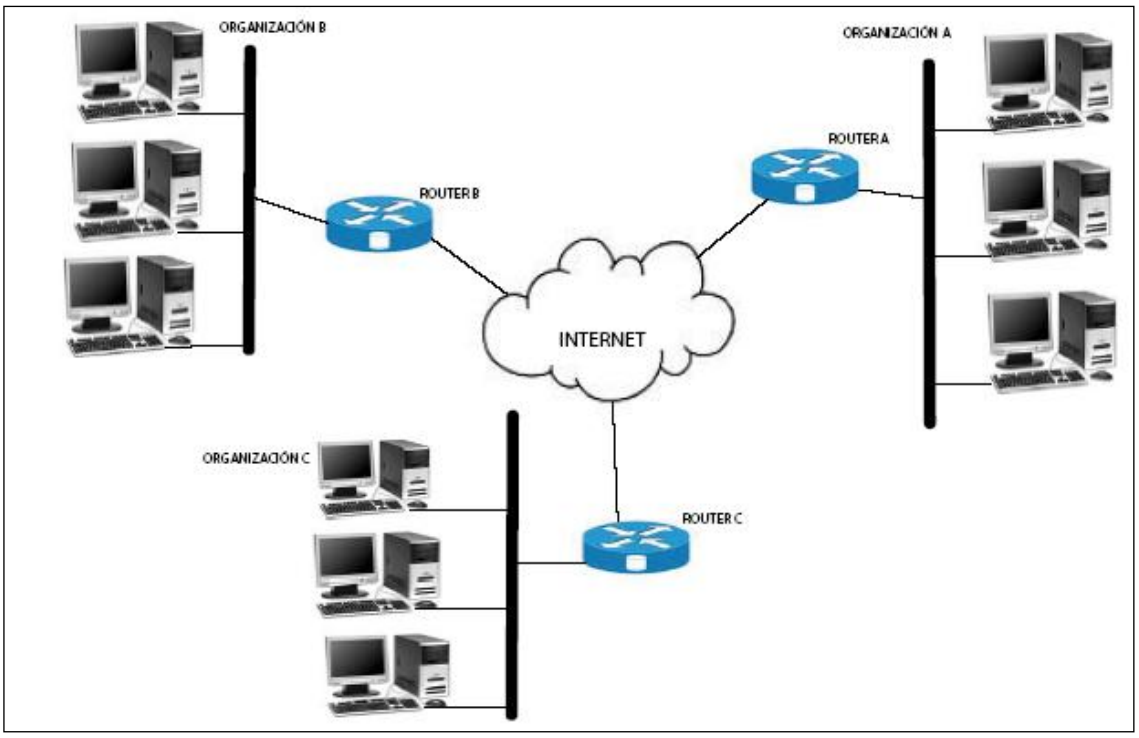
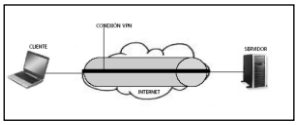


Figura 3.5 Una VPN de Intranet

3) **VPN de extranet:** Permite la conexión de clientes, proveedores, distribuidores o las demás comunidades de interés a la intranet corporativa a través de una red pública. (Figura 3.6).



Las principales características que tiene una VPN de extranet son:

A) Extiende la conectividad a proveedores y clientes:

- Sobre una infraestructura compartida.
- Usando conexiones virtuales dedicadas.

B) Los parámetros tienen diferentes niveles de autorización.

C) Listas de control de acceso, filtros, según decida la empresa.

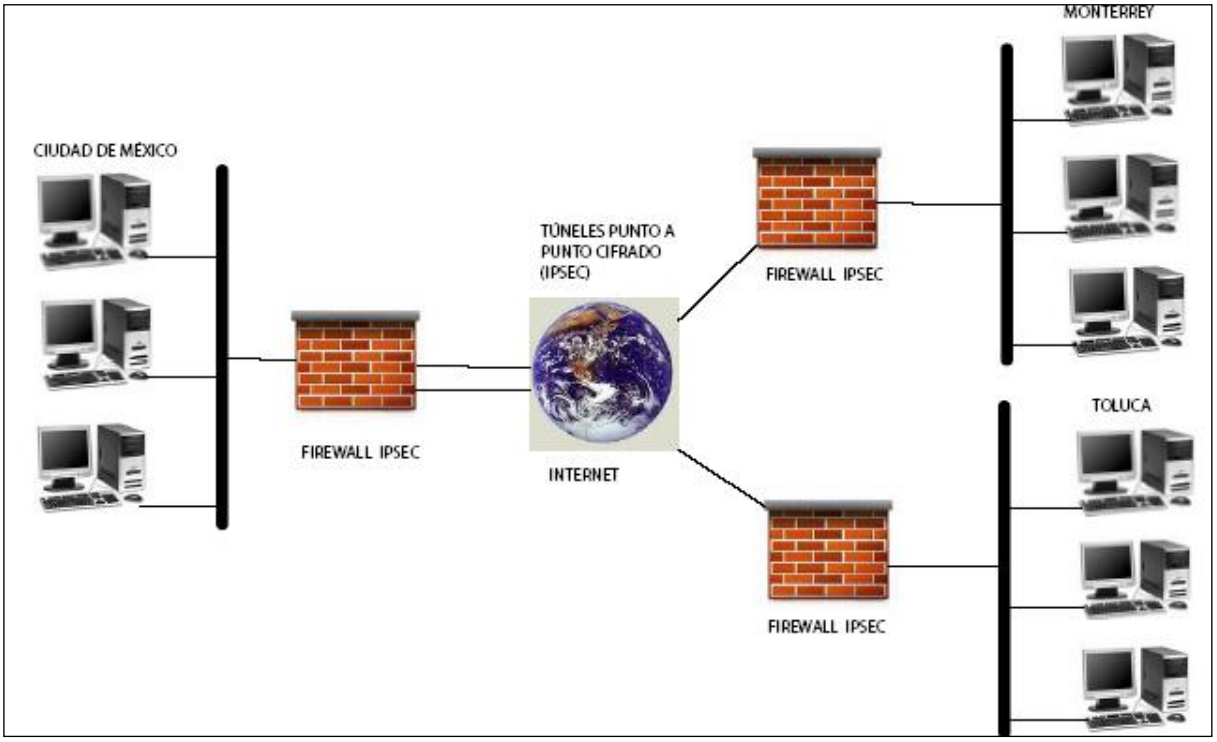
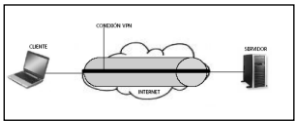


Figura 3.6 Una VPN de Extranet



3.9 Tecnología de las VPN'S

La arquitectura de las VPN's se debe basar en elementos esenciales de la tecnología para proteger la privacidad, mantener la calidad y confiabilidad, y asegurar la operación de la red en la organización o institución educativa. Estos elementos son:

- **SEGURIDAD**: Uso de los túneles cifrado de datos, autenticación de usuarios y paquetes, control de acceso.

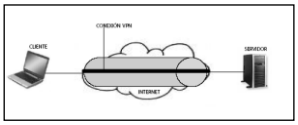
- **CALIDAD DE SERVICIO**: Uso de colas, manejo de congestión de red, prioridad de tráfico, clasificación de paquetes.

- **GESTIÓN**: Implementación y mantenimiento de las políticas de seguridad y calidad de servicio a lo largo de una VPN.

La tecnología de una VPN está basada en la idea de los túneles. La red de los túneles se involucra al establecer y mantener una conexión de la red lógica. En ésta se encapsulan paquetes construidos en una VPN en específico, entonces al transmitir la comunicación entre el cliente y el servidor VPN, finalmente se encapsulan en el lado del receptor.

Los protocolos de VPN también se apoyan en la autenticación y el cifrado para resguardar los túneles de seguridad.

La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados, con la tecnología de cifrada y encapsulamiento, una VPN básica, crea un sitio privado a través de Internet. Instalando VPN's se consigue reducir las responsabilidades de gestión de una red local.



3.9.1 Protocolos de túnel

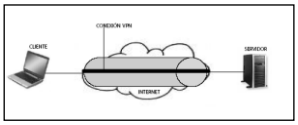
Dentro de los protocolos de implementación de las capas del modelo OSI se mencionan las cuatro principales: capa física, capa de datos, capa de red y capa de transporte. Dentro de estas capas se menciona la capa de datos por ser usada por el protocolo de túnel.

Las tecnologías de los túneles de capa 2 del OSI, se utilizan los métodos de cifrado y autenticación de usuarios, por ejemplo: PPTP,L2F y L2TP, dependiendo el tipo de estándar que se quiere aplicar en una IP y el protocolo de túnel, se podrá usar la capa de datos para crear un paquete de datos en forma segura y cifrada; si no cuenta el usuario con las siguientes condiciones asignadas a este servidor VPN que son: las variables de la configuración de su equipo de computo, la asignación de dirección IP y los parámetros de cifrado de datos; no podrá ser uso de la conexión hacía el servidor.

Los datos que se trasfieren a través del túnel se envían utilizando protocolos basados en datagramas y un protocolo de mantenimiento del túnel para administrar al mismo protocolo.

Las tecnologías que se implementan en los túneles de la capa 3 del OSI, suponen que se han manejado fuera de las bandas de comunicación relacionadas con la configuración, normalmente a través de procesos manuales, sin embargo, quizá no exista una fase de mantenimiento del túnel; para los protocolos de nivel 2 (PPTP y L2TP) se debe crear una estabilidad del túnel para enviar los datos a través del mismo. El cliente o el servidor utilizan un protocolo de transferencia de datos del túnel a fin de preparar los datos para su transferencia.

Se basan en protocolos PPP bien definidos, los protocolos de la capa 2 (PPTP y L2TP) heredan un conjunto de funciones útiles, como se señalan en las contrapartes de la capa 3 que cubren los requerimientos básicos de una VPN. Muchos de los esquemas de túnel de capa 3 suponen que los puntos finales han



sido bien conocidos antes de que se estableciera el túnel. Una excepción es la negociación IPSec que proporciona una autenticación mutua de los puntos finales del túnel.

Hay dos tipos de túneles VPN: Obligatorio y Voluntario.

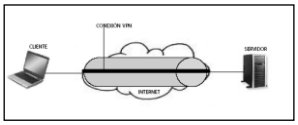
Los túneles voluntarios requieren que el cliente esté habilitado por una VPN, mientras que en los túneles obligatorios se utilizan cuando el cliente se conecta en un FEP (Procesador de Componente Frontal o Frente Externo del Procesador) habilitado por una VPN.

La conexión por el túnel voluntario es una metodología en la cual la estación de trabajo de cliente se ofrece como voluntaria para crear un túnel en la red. Para que exista una conexión por túnel, el cliente debe estar habilitado por una VPN con los protocolos PPTP, IPSec o L2TP y el software de soporte.

El cliente y el servidor deben utilizar el mismo protocolo de túnel para que tenga una conexión de red que puede proporcionar transporte entre la estación de trabajo y el servidor del túnel seleccionado. La estación de trabajo puede haber establecido una conexión de marcación a la red de transporte antes de que el cliente pueda configurar un túnel.

En la conexión por el túnel obligatorio el cliente desea conectarse a través de Internet, pero no está habilitado por una VPN, puede conectarse a un FEP habilitado en una VPN en un procesador de software independiente. Es evidente que el FEP y el servidor de túnel deben soportar y utilizar el mismo protocolo VPN que puede ser PPTP, IPSec y L2TP, para cualquier conexión específica.

Estos FEP's pueden establecer VPN's a través de Internet para un servidor de túnel en la red privada de corporación. Esta configuración es conocida como conexión por túnel obligatorio debido a que el cliente está obligado a utilizar la VPN. Una vez que se ha realizado la conexión inicial, automáticamente se encamina al cliente a través del túnel.



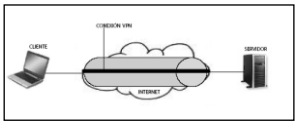
3.9.2 Interfaces del Túnel

Las interfaces de un túnel se pueden configurar con un software gráfico en cualquier sistema operativo en Linux y Windows; le permite al administrador del servidor VPN a configurar los siguientes puntos: editar la red, crear las políticas de red, creando un firewall de puertos, el método de cifrado y crear las carpetas de los archivos. La interfaz de un programa en ambiente gráfico se implementa a nivel administrador para poder configurar los parámetros de una VPN de cliente a servidor. El cliente que se quiere conectar al servidor VPN podrá acceder a la información de manera segura y confiable.

En la actualidad existen diferentes programas de software en ambiente gráfico para cualquier plataforma en donde se puede instalar esta herramienta para poder tener una conexión de Internet por medio de una VPN, se puede enviar programas o archivos de manera segura. Para que el usuario pueda tener una conexión de un lugar a otro sin tener problemas de envío de información hacia un lugar en específico.

La interfaz de usuario está compuesta por diferentes elementos:

1) La ventana principal de una configuración de una VPN
2) Un túnel desde el panel de configuración.
3) Configuración y selección de una nueva fase 1
4) Configuración de la fase de autenticación
5) La fase 1 debes de seleccionar una nueva fase 2 para configurar el protocolo IPSec.
6) Activación de los parámetros de configuración del protocolo IPSec.
7) Abertura del túnel para establecer la configuración de una VPN con IPsec.
8) Iconos de configuración en la barra de herramientas
9) Ventana de registros de la conexión de una VPN en accesos remotos.



3.10 Interacción entre una VPN y un Firewall

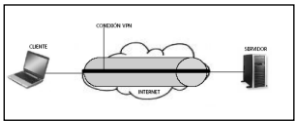
Las reglas del firewall deben permitir el tráfico PPTP, L2TP e IPSec con base en los puertos utilizados. El firewall y el servidor VPN incorporados en un mismo dispositivo de controles y riesgos asociados a la tecnología VPN cuando se desea implantar una VPN, se deben considerar las ventajas que van a aportar a la organización, sin embargo, es importante considerar los riesgos que implican en caso de no adoptarse las medidas necesarias al implantar una VPN segura.

Los estándares utilizados en la implementación de VPN's, garantizan la privacidad e integridad de los datos y permiten la autenticación de los extremos de la comunicación, para no tener errores en una VPN dentro de una organización o institución educativa. Se deben tomar las medidas necesarias para implementar una VPN segura que incluyan el uso de certificados digitales para la autenticación de equipos de cómputo con VPN's, tarjetas inteligentes para la autenticación de usuarios remotos y control de acceso al sistema; por eso es importante contar con un firewall y sistemas de autorización.

"Los certificados digitales, garantizan la autenticación de los elementos remotos que generan al túnel y elimina el problema de la distribución de claves. Se puede utilizar el sistema PKI (Infraestructura de Clave Pública) para emitir los certificados digitales, permite tener el control absoluto de la emisión, renovación y revocación de los certificados digitales usados en la VPN. El uso de PKI no se limita sólo a las VPN's sino que puede utilizarse para aplicaciones como firmas digitales, cifrado de correo electrónico." [3]

El certificado digital y la clave privada se almacenan en el propio CPU, no se está autenticando al usuario sino al CPU. Para poder autenticar al usuario, algunos fabricantes de sistemas VPN han añadido un segundo nivel de

[3] Richard Bejtlich, Monitorización de Seguridad en Redes, Pearson, ED. 2, México,2005,p216



autenticación. El uso de contraseñas es un nivel adicional de seguridad, pero no es el más adecuado, ya que carecen de los niveles de seguridad necesarios debido a que son fácilmente reproducibles, pueden ser capturadas y realmente no autentican al usuario.

El método más adecuado es autenticar a los usuarios remotos mediante la utilización de sistemas de autenticación de manera segura. Estos sistemas se basan en la combinación de dos factores: el Token y el PIN, de esta forma se asegura que sólo los usuarios autorizados acceden a la VPN de la organización o institución educativa.

El control de acceso se puede realizar utilizando firewalls y sistemas de autorización, de esta manera se aplican políticas de acceso a determinados sistemas y aplicaciones de acuerdo al tipo de usuarios o grupos de usuarios que están dentro del área de trabajo.