UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERíA

"MECANISMOS DE SEGURIDAD PARA UN SERVIDOR VPN EN LINUX EN EL LABORATORIO DE REDES Y SEGURIDAD"

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTAN:

MEJÍA RIVERA JOSÉ FRANCISCO

TEODORO CRUZ JORGE ENRIQUE HOMERO

DIRIGIDA POR:

M.C. CINTIA QUEZADA REYES

CIUDAD UNIVERSITARIA 2012

AGRADECIMIENTOS

AGRADECIMIENTOS

A DIOS Y A LA VIRGEN DE GUADALUPE

Por la ayuda divina que he recibido al permitirme terminar una etapa muy importante en mi vida y así seguir con otras etapas que espero sean muy satisfactorias para mí. Les doy las gracias porque tengo una familia maravillosa que siempre me ha apoyado y que tengo la fortuna de verlos todos los días. Gracias porque también ha puesto en mi camino a muchas personas que han sido muy valiosas para mí.

A la M.C. CINTIA QUEZADA REYES

Por cada una de las clases que impartió y en donde tuve la oportunidad de estar presente y que nos compartiera su gran conocimiento por cada asignatura, por la paciencia, la asesoría y el tiempo dedicado que nos brindó para poder terminar este trabajo.

A LA COORDINACIÓN DE MATEMÁTICAS

Por haberme dado la oportunidad de trabajar en dicho lugar y permitirme aprender muchas cosas, un agradecimiento especial a la M.I. María Sara Valentina Sánchez Salinas y la M. en E. Rosalba Rodríguez Chávez por sus valiosos consejos, la ayuda que siempre me brindaron y su gran amistad.

A LA FACULTAD DE DERECHO

Por darme la oportunidad de trabajar con ellos, por la ayuda brindada, por los buenos compañeros que he conocido, por los consejos que me han dado, el agradecimiento en especial es para el Ing. Héctor Javier Correa Peragallo**,** Christian Aguilar Díaz y Enrique Díaz Martínez.

A TODOS Y CADA UNO DE MIS PROFESORES

Porque con los conocimientos que nos compartieron a lo largo de la carrera, nos han dado herramientas para poder defendernos en el aspecto laboral.

AGRADECIMIENTOS

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Por permitirme ser parte de tan honorable institución y poder tener una educación de gran nivel, muchísimas gracias por todo.

A NUESTROS SINODALES

M.C. Ma. Jaquelina López Barrientos, Ing. Edgar Martínez Meza, Ing. Rafael Sandoval Vázquez y el Ing. Cruz Sergio Aguilar Díaz por sus observaciones a este trabajo.

José Francisco Mejía Rivera

AGRADECIMIENTOS

Padres

Queridos padres, les agradezco su gran amor, cariño, apoyo social y económico para darme la oportunidad de seguir estudiando una carrera profesional. También les doy las gracias por brindarme la mano para poder emprender un proyecto de vida, desde que inicié mis primeras clases en la escuela.

Hermanos

Le agradezco a mis hermanos que estuvieron conmigo, porque cuando entré a estudiar la universidad, me dieron todo su apoyo en la parte económica, me brindaron amor, alegría y me alentaron con frases positivas que son: empeño, audacia, confianza, ser constante, perseverante, guardar la calma, escuchar a los demás, trabajar duro y ser feliz.

También le doy gracias a Dios que me permitió concluir mi carrera profesional con mucho esfuerzo y el empeño que le puse en estudiar duro durante 6 años largos que no fueron fáciles, pero me llevo una gran satisfacción en el corazón por ser un estudiante egresado de la máxima casa de estudios, la UNAM.

Jorge Enrique Homero Teodoro Cruz

DEDICATORIAS

DEDICATORIAS

PARA MIS PADRES

Laura Rivera y Pablo Pedro Mejía, por el amor, el apoyo incondicional que siempre me brindan, que gracias a los valores que me enseñaron he sido una gran persona, hoy con éste trabajo dedicado a ustedes, las personas más importantes de mi vida, a las que más admiro y que siempre llevo en mi corazón, ya que sin su apoyo no hubiera llegado a este momento.

PARA MIS HERMANOS

Eva, Rosy, Pablo y Luis, éste trabajo va dedicado a ustedes con mucho cariño porque cada uno es un ejemplo a seguir, cada quien tiene cualidades sobresalientes y espero algún día tener un poco de cada uno para ser una mejor persona. Muchas gracias por los buenos momentos que hemos pasado y por el infinito cariño que siempre me brindan.

PARA MIS CUÑADOS

Javier muchas gracias por el apoyo que recibí cuando apenas entré a la carrera, gracias por la asesoría que me dabas de matemáticas y también para Mayra, este trabajo está dedicado a ustedes.

PARA MIS SOBRINITOS

Wendy Aracely, Oswaldo Xavier y Christopher Joshua, que espero lleguen hasta donde ustedes lo deseen, que desde muy pequeños han demostrado que son muy inteligentes.

DEDICATORIAS

PARA MIS TÍAS

Hortensia Cervantes Rivera y María Luisa Cervantes Rivera por el apoyo que he recibido de su parte.

A LA MEMORIA DE MI ABUELITA †

Maura Rivera Roa por el cariño que siempre me diste, el cuidado que siempre recibimos mis hermanos y yo. Muchas gracias por esos momentos tan agradables, éste trabajo también está dedicado a tu memoria abuelita.

PARA MIS COMPADRES

Jesús Alfredo Zárraga Martínez y Miriam Pavón Marín. Gracias por todo su apoyo.

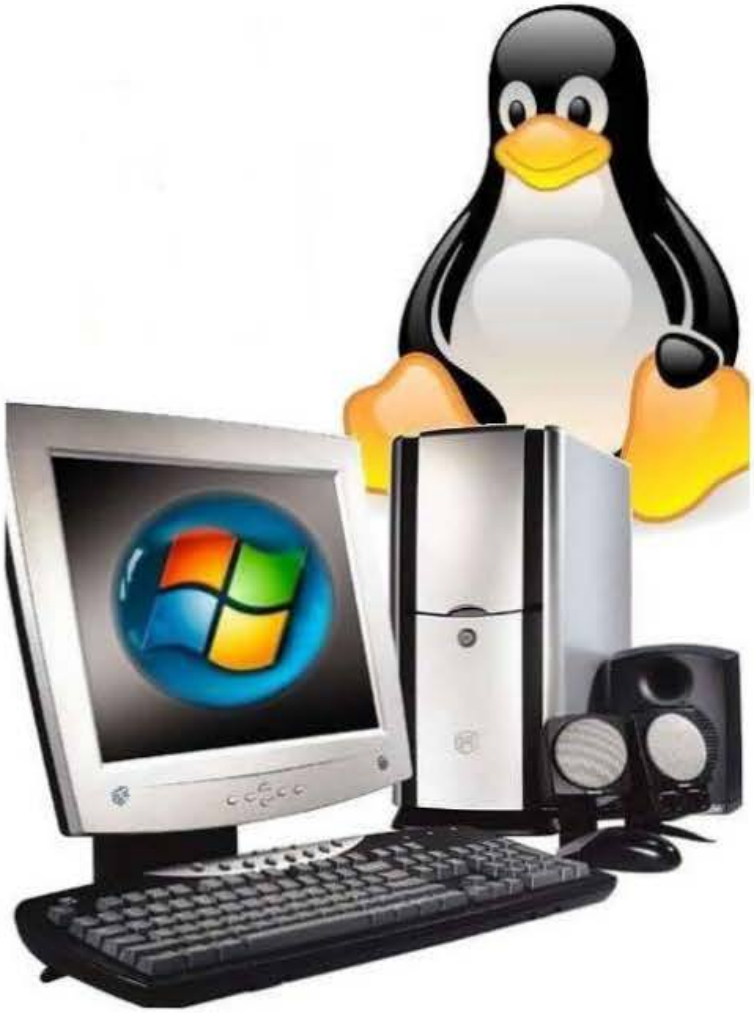
PARA MI AHIJADO

Santiago Zárraga Pavón

PARA MIS AMIGOS

Norma Martínez Quiroz, José Carlos Gutiérrez Vera, Roberta Magali Vargas Carapia, Juan Armando Romero Guadarrama, Geovani Javier Flores Cruz, Luis Alberto Villanueva Juárez, María del Rocío Pérez Pérez, Lilia Inés Sánchez Vargas, Fernando Sánchez Cervantes, Alondra Rebolledo Trejo, Roberto Carlos Gama Gómez, Eraim Ruiz Sánchez, Edgar Gúzman Maldonado.

José Francisco Mejía Rivera



ÍNDICE

Índice Temático

OBJETIVO

OBJETIVO

Objetivo General

Con base en los conocimientos adquiridos, diseñar un servidor VPN en el Laboratorio de Redes y Seguridad.

Objetivos Particulares

- Una vez diseñado, implementar mecanismos de seguridad en dicho servidor.
- Además, contar con una herramienta de seguridad para el laboratorio, que permita una mayor protección lógica de los equipos.
- Que el alumno tenga conocimientos de cómo proteger un servidor VPN, que alimente más sus conocimientos de seguridad informática, que sepa qué requerimientos se necesitan para poder proteger un conjunto de equipos de cómputo en un área específica.

INTRODUCCIÓN

INTRODUCCIÓN

Hace algunos años, poder comunicarse con otra persona era un hecho muy difícil de lograr, ¿Qué se podría decir de comunicarse desde una empresa a cualquier lugar?, eso era imposible para esos tiempos. Hoy en día los avances tecnológicos están dando pasos agigantados y la comunicación entre computadoras se ha hecho cada vez más fácil y rápida.

Mencionando un poco de historia, con la llegada del internet se facilitaron algunas actividades para las empresas, sin embargo, existía la problemática que no cualquiera podía tener acceso a ella. Las empresas necesitaban tener comunicación con otras corporaciones y para poder tener acceso a sus datos les era indispensable comprar costosos equipos para tener una conexión. A medida que ha pasado el tiempo, las corporaciones han requerido que las redes de área local trasciendan más allá de la cobertura local para incluir al personal y a los centros de información ubicados en otros edificios, ciudades, estados e incluso también otros países.

Una VPN (Virtual Private Network) es una estructura de red corporativa implantada sobre una red de transmisión y comunicación ante el público en general que tenga permisos de uso del servicio, básicamente es una red remota que se conecta en forma segura para evitar una conexión insegura como puede ser el Internet. Se usan algoritmos de cifrado y claves, ya que ofrecen seguridad sobre los datos que se transmiten en la red, pues se crea un túnel cifrado entre los puntos que participan en la comunicación y sólo los clientes autorizados pueden acceder a él.

Las ventajas que tiene el usuario al contar con una VPN son la seguridad, la integridad, el menor costo, mejor administración y la facilidad de transferencia

de archivos de un equipo a otro sin necesidad de estar en la misma empresa y con la garantía de contar con un respaldo íntegro de información.

La seguridad brinda un mejor cifrado y encapsulación de datos que viajan codificados a través de un túnel. Los costos de una VPN son muy bajos en su implementación y diseño, no se necesitan grandes sumas de dinero para comprar líneas dedicadas o enlaces físicos de muy altos costos. Las VPN's principalmente brindan autenticidad, autorización, integridad y confidencialidad.

Para contar con estas ventajas se configuran los mecanismos de seguridad de un servidor VPN en Linux en el laboratorio de redes y seguridad, y posteriormente se verifica la identidad de los usuarios para acceder al sistema del servicio de Internet, esto último se hace por medio de las contraseñas para implementar un control de acceso y la autenticación de cada usuario.

Dependiendo del usuario, éste tendrá ciertos permisos para acceder al sistema o servicio de Internet que se esté manejando en el laboratorio de redes y seguridad; la principal idea es contar con un mecanismo de seguridad en el servidor VPN para evitar un sabotaje o robo de información.

CAPÍTULO 1

REDES DE DATOS

1.1 Introducción a las redes

Se le llama red de computadoras al conjunto de elementos que interaccionan entre sí con el propósito de compartir recursos e intercambiar información. Se consideran elementos aquellos que sirven de propósito especial como lo son los nodos, las terminales, los servidores, las computadoras, entre otros.

Una de las razones por la cual es muy frecuente el uso de las redes es por la flexibilidad con la que se cuenta, ya que la forma de comunicarse con otra persona es más fácil y se presenta rapidez que se tiene al transferir cualquier documento vía internet.

Otra de las razones por la cual se incrementó el uso fue el gran ahorro económico que se obtuvo al compartir recursos tanto lógicos como físicos, permitiendo así un gran porcentaje de aceptación para el usuario general. Las redes se clasifican de acuerdo con su alcance geográfico y se muestra esta clasificación a continuación en la tabla 1.1.

Tabla 1.1 Clasificación de las redes

Tipo de red	Distancia	Lugares donde se utiliza
PAN (Personal Area Network – Red de Área Personal)	≤ 10 m.	Espacio personal (oficina, cubículo)
LAN (Local Area Network – Red de Área Local)	≤ 1 Km.	Escuelas, habitación, edificios, universidad
CAN (Campus Area Network - Red de Área de Campus)	≤ 10 Km.	Universidad, base militar
MAN (Metropolitan Area Network - Red de Área Metropolitana)	≤ 100 Km.	La ciudad
GAN (Global Area Network- Red de Área Global)	< 100 Km.	El Mundo (con retraso en la comunicación)
WAN (Wide Area Network – Red de Área Amplia)	≤ 1000 Km.	El mundo

Es importante mencionar que existen dos formas para que los equipos se interconecten, con base en ello se puede hacer una clasificación en redes cableadas y redes no cableadas:

a) Redes Cableadas (Guiadas). Son las que tienen la capacidad de transferir información de manera rápida, segura y efectiva, además de que su implementación es de menor costo que las redes inalámbricas.

Para llevar a cabo una conexión de este tipo se hace uso de medios de transmisión guiados o terrestres, entre ellos se encuentran los de tipo coaxial, par trenzado y fibra óptica.

El cable coaxial tiene un hilo de cobre en la parte central el cual está rodeado por una malla metálica y una cubierta protectora de plástico en forma cilíndrica. Una de las ventajas del cable coaxial es la resistencia a interferencias y atenuación. (Figura 1.1)

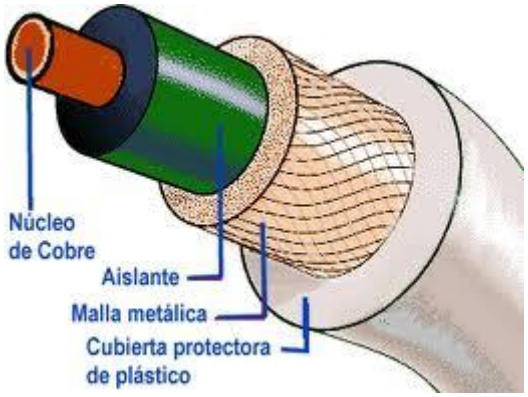


Figura 1.1 Cable Coaxial

El cable de par trenzado UTP (unshielded twisted pair- par trenzado no apantallado) está formado por un conductor interno protegido por una capa de polietileno y un grupo de pares de diferentes colores dentro de la capa se cuenta con tres pares. (Figura 1.2)

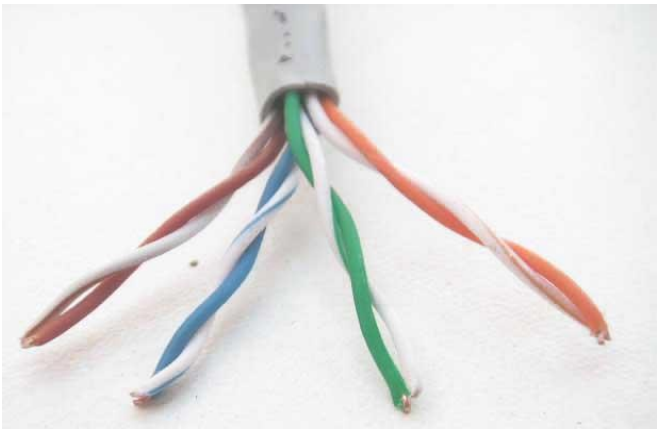


Figura 1.2 Cable UTP

Una de las ventajas de utilizar este cable es su bajo costo, además de que su uso es sencillo, sólo que tiene un problema el cual es la limitación para trabajar a largas distancias (máximo 100m). Este cable cuenta con diferentes categorías que van desde la categoria1 hasta la 7. Actualmente se utiliza en su mayoría el cable UTP categoría 5e que puede transmitir datos hasta de 100Mbps y consta de 4 pares trenzados de hilo de cobre. El cable UTP utiliza conectores RJ-45.

La fibra óptica es un hilo muy fino y por medio de estos hilos se envían pulsos de luz, es el mejor medio de transmisión ya que no hay problemas de interferencia, la velocidad con la que se trasmiten los datos es alta. (Figura 1.3)

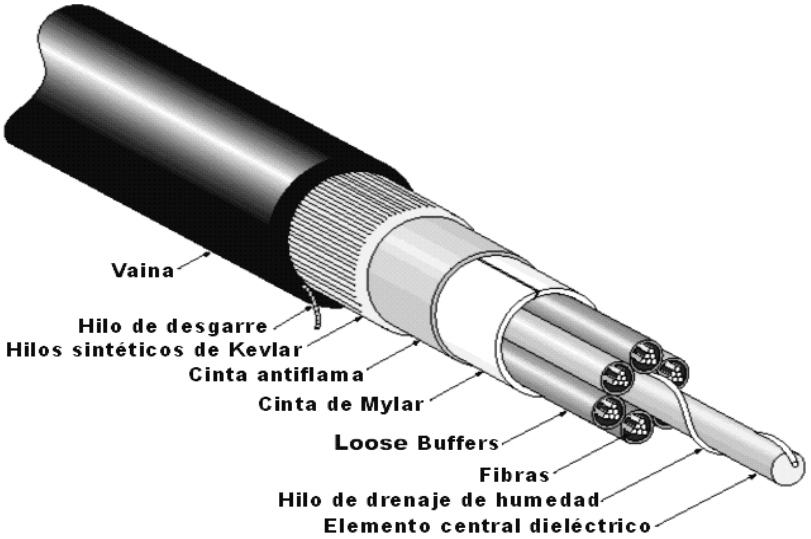


Figura 1.3 Cable de Fibra Óptica

Para realizar la comunicación se emplean fibras multimodo y monomodo, las multimodo se utilizan para distancias cortas que puede considerarse de hasta 5000 m. las fibras monomodo se emplean para distancias más largas.

La desventaja es su alto costo, además de que la fibra es muy frágil y se debe tener mucho cuidado en su utilización.

b) Redes no cableadas (Inalámbricas). Son aquellas que se comunican mediante ondas electromagnéticas y para la trasmisión y recepción se necesita una antena.

Entre las ventajas que tienen las redes inalámbricas es la rápida instalación de la red, la movilidad que se tiene, además del bajo costo en su mantenimiento.

Los medios de transmisión se encargan de propagar las señales libremente a través del medio y se clasifican en 3 tipos: ondas de radio, microondas e infrarrojo. (Figura 1.4)

Figura 1.4 Medios de transmisión de una red inalámbrica

Las ondas de radio son ondas electromagnéticas de menor frecuencia ya que su rango se encuentra entre 3 a 30 Hz. Estas ondas son omnidireccionales por lo tanto no necesitarán de un aparato que se encargue de dirigir la señal ya que habrá varias antenas que la reciban.

En la transmisión por microondas la señal va viajando en línea recta entre las estaciones repetidoras hasta llegar a su destino, al llegar a éste, se amplifica la señal y se retransmite a otros puntos.

El infrarrojo se utiliza para una comunicación a corta distancia y tanto el transmisor como el receptor deben estar alineados directamente para lograr una

buena transmisión. La gran desventaja de este medio de transmisión es que no puede atravesar las paredes.

1.2 Topologías de las redes

La topología hace referencia a la forma de una red, muestra cómo los diferentes nodos se encuentran conectados entre sí y la forma de comunicarse. Las topologías pueden ser físicas o lógicas, existen diversos tipos:

a) Topología Bus

En esta topología las computadoras se encuentran conectadas en línea recta, es decir, todas las máquinas se encuentran conectadas a un cable en común, esto permite que se puedan comunicar directamente. El tipo de medio de transmisión (cable) que se utiliza en este tipo de conexión es el cable coaxial. La gran desventaja de este tipo de conexión es que la ruptura del cable hace que todos los nodos pierdan la comunicación.

A continuación se presentan dos tablas (1.2 y 1.3) con las características del cable coaxial delgado y del cable coaxial grueso, ambos permiten realizar con la que se hace una conexión tipo bus.

Tabla 1.2 Especificaciones del cable coaxial delgado

CABLE COAXIAL DELGADO RG-58	
Velocidad de operación	10 Mbps
Tipo de transmisión	Banda Base
Distancia máxima del segmento	185 m
Distancia mínima entre nodos	0.5 m
Diámetro del cable	¼ pulg
Material que se utiliza para la conexión	Conector BNC-T(del inglés Bayonet Neill-Concelman), Terminador

Tabla 1.3 Especificaciones del cable coaxial grueso

CABLE COAXIAL GRUESO RG-8	
Velocidad de operación	10 Mbps
Tipo de transmisión	Banda Base
Distancia máxima del segmento	500 m.
Distancia mínima entre nodos	2.5 m
Diámetro del cable	½ pulg
Material que se utiliza para la conexión	Transceiver tipo vampiro, terminador

La topología tipo bus emplea el cable coaxial delgado o grueso y puede observarse en las figuras 1.5 y 1.6

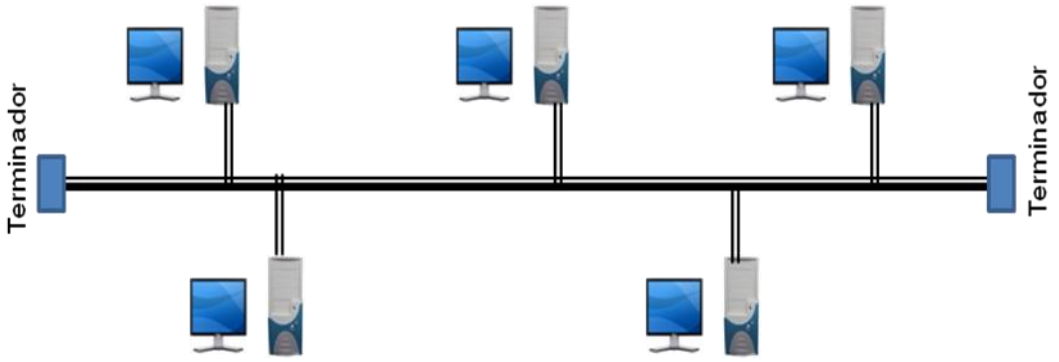


Figura 1.5 Topología en bus con cable coaxial delgado

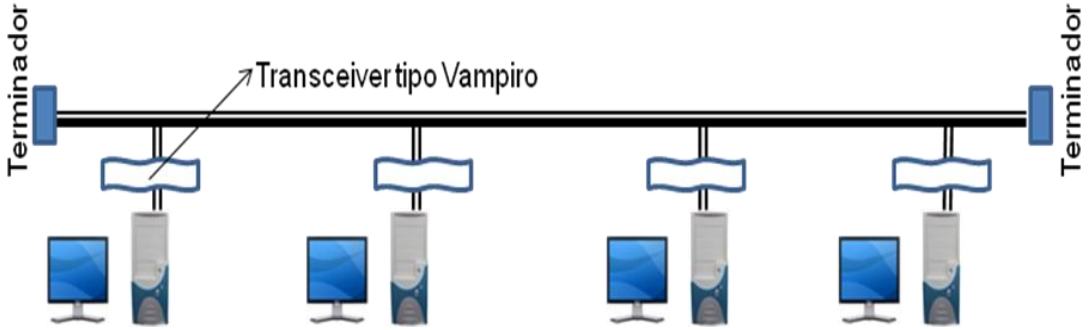


Figura 1.6 Topología en bus con cable coaxial grueso

Una de las ventajas de esta topología es que todos los dispositivos de la red pueden verse entre sí y compartir la información de manera que puede simularse que ésta se encuentra residente de manera local en el equipo que la solicita, otra gran ventaja es que se permite conectar un gran número de

equipos. La desventaja es que al compartir la información, como sólo se utiliza un canal de comunicación, esto provoca problemas de tráfico y colisiones.

b) Topología Anillo

Este tipo de topología se compone de un solo anillo cerrado donde los dispositivos se conectan directamente entre sí por medio de cables, la diferencia que se tiene con la topología bus es que las puntas no están conectadas a un terminador. Las ventajas que se observan en esta topología son las siguientes:

- Se tiene un acceso equitativo para todas las computadoras.
- El rendimiento del sistema no se altera demasiado cuando muchos usuarios están utilizando la red.

La desventaja de este tipo de conexión es que al cortar la cadena se interrumpe la conexión o si existe alguna distorsión afecta a toda la red, La figura 1.7 muestra cómo es la conexión tipo anillo.

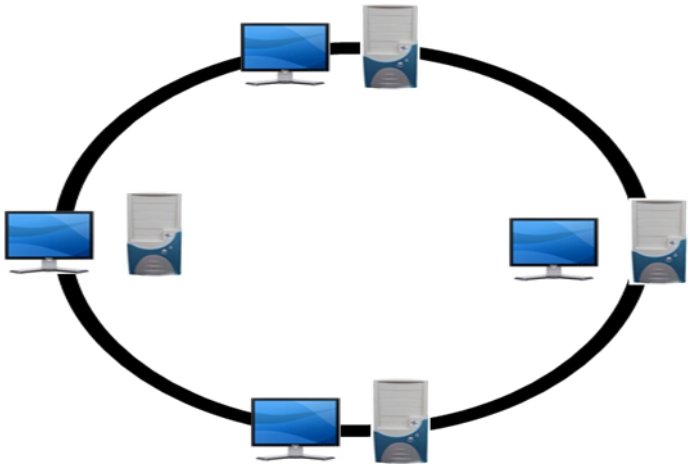


Figura 1.7 Topología en Anillo

c) Topología Estrella.

En este tipo de topología los dispositivos se encuentran conectados a un concentrador (hub) o conmutador (switch).

La ventaja de este tipo de conexión es que si un cable falla no afecta a los demás nodos ya que están conectados mediante un concentrador y sólo falla el equipo del cable dañado, otra ventaja es la administración y monitoreo centralizado.

Entre las desventajas se puede encontrar el alto costo en el cableado que se hace, así como las conexiones que se utilizan y en caso de que el concentrador presente alguna falla, la red queda inutilizable. (Figura 1.8)

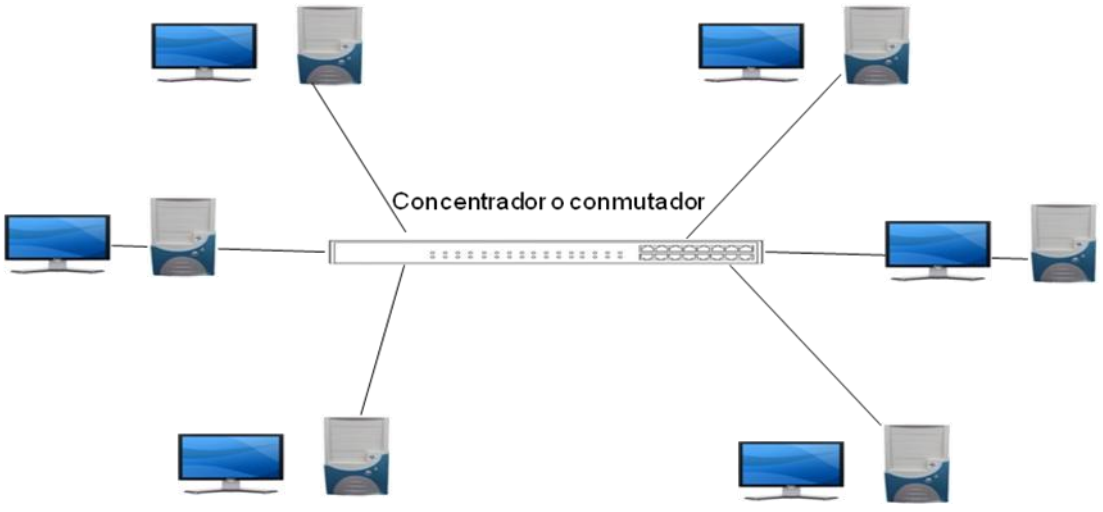


Figura 1.8 Topología en Estrella

d) Topología Malla

En esta topología cada nodo está conectado a todos los nodos, por lo que la comunicación entre un equipo y otro es de manera eficiente debido a que se cuenta con varios enlaces disponibles. Como ventaja es posible mencionar que si uno de los cables falla, la comunicación no se pierde, pues habrá otros cables disponibles para ese equipo, otra ventaja es el grado de confiabilidad, pues se tiene independencia en cada uno de los equipos conectados aunque estén conectados todos entre sí.

La gran desventaja es la parte económica, ya que conlleva un gasto enorme comprar demasiado cable para conectar todos los equipos. Otra de las desventajas que se tiene es el grado de complejidad en la realización de este tipo de conexión. La figura 1.9 muestra cómo es una topología malla.

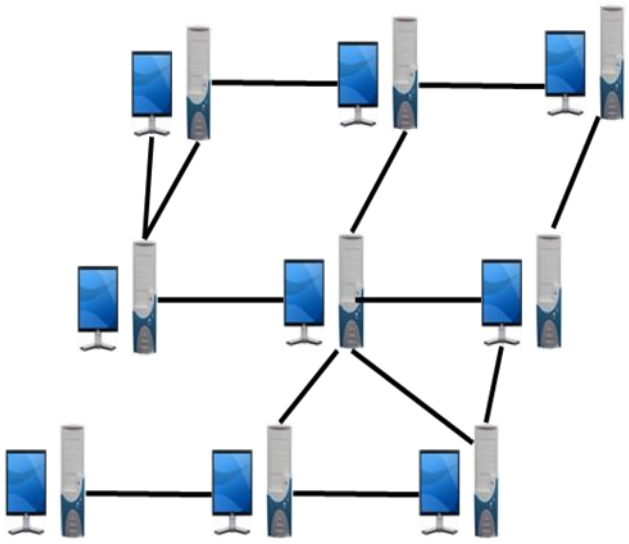


Figura 1.9 Topología Malla

e) Topología Híbrida

El término híbrido describe que está formada con diferentes protocolos, sistemas operativos y distintas plataformas, en este caso esta topología indica que está formada mediante la combinación de topologías básicas.

1.3 Estándares de las redes

Los estándares de las redes se realizan por medio del comité 802 del IEEE (Institute of Electrical and Electronic Engineers- Instituto de Ingenieros Eléctricos y Electrónicos) donde se definen los estándares para las redes LAN (Local Area Network – Redes de Área Local). La mayoría de los estándares se desarrollaron en la época de los 80 cuando apenas comenzaban a surgir las redes en los equipos de cómputo y telecomunicaciones, fue un desarrollo impresionante para todo el mundo, algunas empresas e instituciones gubernamentales de los países de primer mundo ya tenían esta tecnología, sin embargo, era muy caro el servicio de las telecomunicaciones y la instalación de las redes LAN y sus variantes en cuestión de tecnología en redes WLAN.

Dentro de los estándares de las redes de área local que fueron definidas por el comité 802, surgieron las diferentes categorías de las especificaciones 802 por su avance tecnológico y crecimiento de los servicios de Internet y telefonía móvil.

El comité 802 clasifica en 11 categorías los avances de los estándares, esto se observa a continuación:

a) Definición internacional de redes (802.1)

Establece los estándares de interconexión relacionada con la gestión de redes por IEEE y el modelo de referencia para la interconexión de sistemas abiertos (OSI – Open Systems Interconennection), de la Organización Internacional de Estándares (ISO - Internacional Standards Organization). El comité definió las direcciones para las estaciones LAN de 48 bits para todos los estándares 802, de modo que cada adaptador puede tener una dirección única.

b) Control de enlaces lógicos (802.2)

Se define el estándar general para el nivel de enlace de datos. El IEEE divide este nivel en dos subniveles: Los niveles LLC y MAC. El LLC (Logical Link Control - Control de Enlace Lógico) asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación y la MAC (Media Access Control - Control de Acceso al Medio) provee la dirección física de red de un dispositivo.

c) Redes CSMA/CD (Carrier Sense Multiple Access / Collision Detection – Acceso Múltiple con Detección de Portadora y Detección de Colisiones). (802.3)

El estándar 802.3 define cómo opera el método de acceso múltiple con detección de colisiones sobre varios medios. Este estándar define la conexión de redes sobre el cable coaxial, cable de par trenzado y medios de fibra óptica.

d) Redes token bus (802.4)

El estándar 802.4 define el esquema de red de amplios anchos de banda en la Industria, también se deriva del MAP (Manufacturing Automation Protocol - Protocolo de Automatización de Manufactura). Los tokens son pasados en orden lógico basado en la dirección del nodo, pero este orden puede no relacionarse con la posición física del nodo como se hace en una red token ring.

e) Redes token ring (802.5)

El estándar 802.5 de las redes token ring es también llamado ANSI (American National Standards Institute – Instituto Nacional de Estándares Norteamericanos)/IEEE 802.5, se creó en 1985 en donde se definieron los protocolos de acceso, cableado e interfaz para las LAN Token Ring, este estándar lo hizo popular IBM para el método de acceso de paso de tokens y físicamente es una conexión con topología estrella, pero lógicamente forma un anillo.

f) MAN (Metropolitan Area Network - Redes de Área Metropolitana) (802.6)

El estándar 802.6 trata de redes de área metropolitana definidas como redes de datos diseñadas para poblaciones o ciudades. Se define un protocolo de alta velocidad donde las estaciones enlazadas comparten un bus dual de fibra óptica usando un método de acceso llamado DQDB (Distributed Queued Dual Bus - Bus Dual de Cola Distribuida).

El DQDB es una red repetidora que conmuta celdas de longitud fija de 53 bytes; por lo consiguiente, es compatible con el ancho de banda ISDN (Integrated Services Digital Network - Red Digital de Servicios Integrados) y ATM (Asynchronous Transfer Mode - Modo de Transferencia Asíncrona)

g) Grupo asesor técnico de ancho de banda (802.7)

Este comité brinda consejos técnicos a otros subcomités en técnicas sobre anchos de banda en redes.

h) Grupo asesor técnico de fibra óptica (802.8)

Este consejo brinda asesoría de redes por fibra óptica a otros subcomités como una alternativa a las redes basadas en cable de cobre.

i) Redes integradas de datos y sonido (802.9)

Define la integración de tráfico de sonido, datos y video para las LAN, también existe una especificación llamada IVD (Integrated Voice Data - Datos y Voz Integrados), este servicio provee un flujo multiplexado que pueda llevar canales de información de datos y sonido conectando dos estaciones sobre un cable de cobre o un par trenzado.

j) Grupo asesor técnico de seguridad en redes (802.10)

Se trabaja en la definición de un modelo de seguridad estándar que opera sobre una variedad de redes e incorpora métodos de autenticación y cifrado para redes LAN Y WLAN.

k) Redes inalámbricas (802.11)[1]

Conocido también como WIFI, es una familia de estándares, especificaciones o protocolos de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y enlace de datos), especificando las normas de funcionamiento en una WLAN.

Se han desarrollado diversas especificaciones en esta familia debido a que han surgido nuevas necesidades para utilizar los medios más adecuados para lograr la implementación de una red inalámbrica en cualquier lugar.

[1] Para mayor información ver el apéndice A

1.4 Protocolos utilizados en las redes

Un protocolo es un conjunto de reglas que permite la comunicación entre ambos procesos que se ejecutan en diferentes equipos de cómputo, es un conjunto de reglas y procedimientos que se deben respetar para poder enviar y recibir los datos a través de la red.

Los protocolos son los encargados de establecer la forma en que se enviarán los paquetes de información considerando las necesidades de las organizaciones, éstos acoplan la información para su transmisión entre redes con diferentes protocolos, de esta manera se garantiza la comunicación entre redes, logrando así que los datos puedan llegar a su destino.

Los protocolos se pueden clasificar en protocolos orientados a la conexión y protocolos no orientados a la conexión.

a) Protocolos orientados a la conexión

Permiten el control de la transmisión de datos durante una comunicación establecida entre 2 equipos de cómputo. El equipo receptor se encarga de enviar los datos de recepción durante la comunicación y el equipo remitente es el responsable de validar los datos que está enviando. La lista de protocolos orientados a la conexión son: TCP, FRAME RELAY Y ATM.

Las características de los protocolos orientados a la conexión son:

1) Una red orientada a conexión cuida bastante los datos del usuario.

2) Exige una confirmación explícita de que se ha podido establecer esa conexión.

3) Si no se cumple lo anterior, la red informa al usuario solicitante que no ha podido establecer esa conexión.

4) Se intenta asegurar que los datos no se pierdan en la red.

b) Protocolos no orientados a la conexión

Método de comunicación por el cual el equipo remitente envía datos sin avisarle al equipo receptor, esto indica que recibe los datos sin enviar una notificación de recepción al remitente. Los protocolos no orientados a la conexión son: IP, UDP, ICMP, IPX Y TIPC.

Las características de los protocolos no orientados a la conexión son:

1) Las redes no orientadas a conexión pasan directamente del estado libre al modo de transferencia de datos.

2) Las redes no ofrecen confirmaciones, control de flujo, ni recuperación de errores aplicables a la red.

3) El costo de una red no orientada a conexión es mucho menor.

Las principales implementaciones en los protocolos definen que únicamente se deben comunicar los equipos, es decir, indican el formato y la propia secuencia de datos que van a intercambiar, por el contrario, un protocolo no define cómo se debe programar el software para que sea compatible con el protocolo adecuado dependiendo del sistema operativo y el hardware.

Las especificaciones de los protocolos nunca son exhaustivas, es común que las implementaciones estén sujetas a una determinada interpretación de las especificaciones, lo cual genera ciertas implementaciones; incompatibilidad o fallas de seguridad, por las características propias de cada protocolo conviene mencionar éstos a continuación: educativa.

a) HTTP

Desde 1990 se creó el protocolo HTTP (Hyper Text Transfer Protocol - Protocolo de Transferencia de Hipertexto), es el protocolo más utilizado en el servicio de Internet.

El principal objetivo de este protocolo es permitir la transferencia de archivos entre un navegador cliente y un servidor web localizado mediante una cadena de caracteres denominada dirección URL , el modelo del protocolo se muestra en el siguiente diagrama (Figura 1.10)

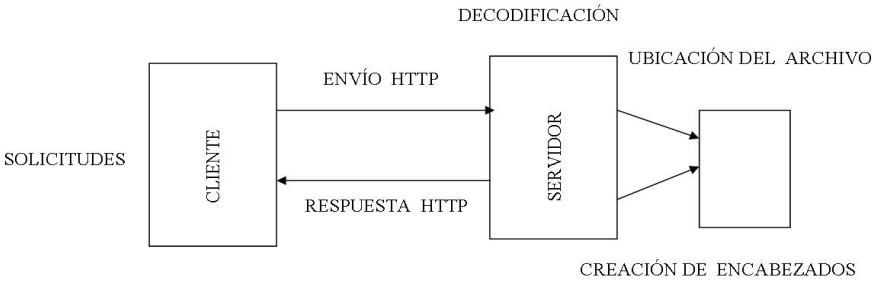


Figura 1.10 Modelo del protocolo HTTP

La manera de realizar una solicitud mediante el protocolo HTTP es un conjunto de líneas que el navegador envía al servidor con los siguientes puntos:

1. **Una línea de solicitud**. Es una línea que especifica el tipo de documento que se quiere solicitar, el método que se aplica y la versión del protocolo utilizado. La dirección está formada por tres elementos que deben estar separados por un espacio.
2. **Los campos del encabezado de solicitud**. Es un conjunto de líneas que permite aportar información a la solicitud y al cliente (navegador, sistema operativo, etcétera).Cada línea está formada por un nombre que describe el tipo de encabezado.
3. **El cuerpo de la solicitud**. Es un conjunto de líneas opcionales que deben estar separadas por una línea en blanco. Por ejemplo, permiten que se envíen datos mediante un comando POST durante la transmisión de datos al servidor.

b) FTP

El protocolo FTP (File Transfer Protocol – Protocolo de transferencia de archivos), como su nombre lo indica, es un protocolo para transferir archivos. El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP. El principal objetivo del protocolo FTP es permitir que los equipos remotos puedan compartir archivos y también permitir la comunicación entre los sistemas de archivos del equipo del cliente y del servidor.

El protocolo FTP está dentro del modelo cliente - servidor, es decir, cuando una aplicación cliente FTP inicia una conexión a un servidor FTP, abre el puerto 21 en el servidor conocido como el puerto de comandos. Se utiliza este puerto para

arrojar todos los comandos al servidor y para cualquier petición de datos desde el servidor se devuelve al cliente a través del puerto de datos. El número de puerto varía dependiendo si el cliente solicita los datos en modo activo o en modo pasivo. (Figura 1.11)

- **Modo Activo**: El modo activo es el método original utilizado por el protocolo FTP para la transferencia de datos a la aplicación cliente. Cuando el cliente FTP inicia una transferencia de datos, el servidor abre una conexión desde el puerto 20 en el servidor para la dirección IP y un puerto aleatorio sin privilegios especificado por el cliente.

- **Modo Pasivo**: La aplicación FTP cliente es la que inicia el modo pasivo de la misma forma que el modo activo. El cliente FTP indica que desea acceder a los datos en modo pasivo y el servidor proporciona la dirección IP y el puerto aleatorio sin privilegios en el servidor y luego el cliente se conecta al puerto en el servidor y descarga la información requerida.

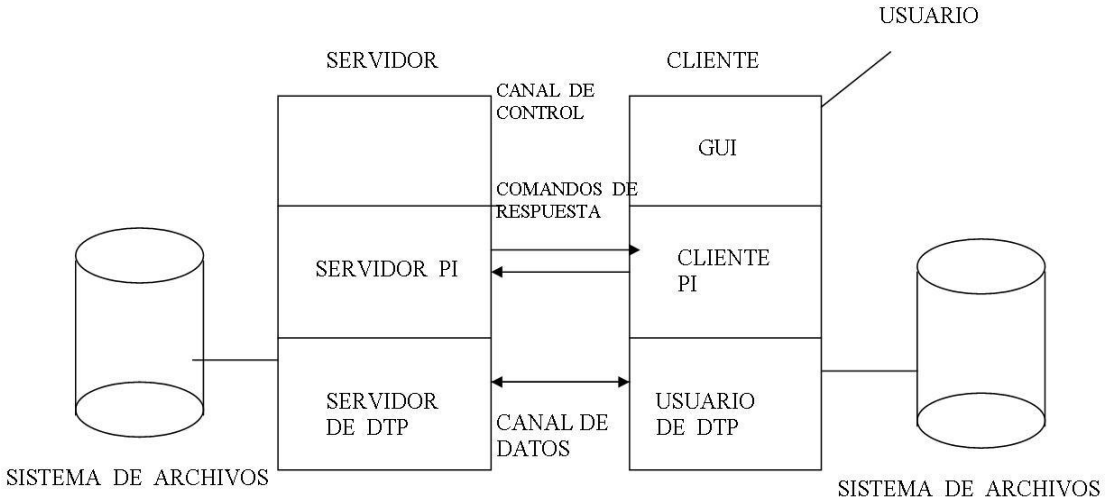


Figura 1.11 Modelo del protocolo FTP

Donde:

- DTP (Proceso de Transferencia de Datos) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina servidor de DTP y del lado del cliente se denomina usuario DTP.

- PI (Intérprete de Protocolo) es el que interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control.

- GUI(Interfaz Gráfica de Usuario) el usuario puede interactuar directamente con el proceso servidor FTP y el diseño del protocolo está orientado a la utilización de los lenguajes autómatas.

c) ARP

El protocolo ARP (Address Resolution Protocol - Protocolo de Resolución de Dirección) tiene un papel clave entre los protocolos de la capa de Internet del modelo TCP/IP, ya que le permite que se conozca la dirección física de una tarjeta de interfaz de red asociada a una dirección IP.

La direcciones físicas se puedan asociar con las direcciones lógicas, el protocolo ARP se comunica con los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda de direcciones lógicas y físicas en una memoria caché. Si la dirección requerida no se encuentra en la tabla, entonces el protocolo ARP envía una solicitud a la red. Si todos los equipos en la red comparan esta dirección lógica con la suya, entonces se identificará con esta dirección al equipo que le confirme al protocolo ARP.

Existe otra variante del protocolo, éste es llamado RARP que consiste en un tipo de directorio inverso de direcciones lógicas y físicas. En realidad el protocolo RARP se usa esencialmente para las estaciones de trabajo sin discos duros que desean conocer su dirección física.

El protocolo RARP (Protocolo de Resolución de Dirección Inversa) es de un tipo de directorio inverso de direcciones lógicas y físicas. Este tipo de protocolo le permite a la estación de trabajo investigar su dirección IP desde una tabla de búsqueda entre las direcciones MAC y las direcciones IP alojadas en la misma red de área local (LAN).

d) ICMP

El protocolo ICMP (Internet Control Message Protocol - Protocolo de Mensajes de Control de Internet) permite administrar información relacionada con errores de los equipos en la red. El ICMP no permite corregir los errores sólo los notifica a los protocolos de capas cercanas. Por lo tanto, el protocolo ICMP es empleado por todos los routers para indicar un error.

e) IP

El protocolo IP (Internet Protocol - Protocolo de Internet) utiliza direcciones numéricas denominadas direcciones IP compuestas por cuatro bytes o cuatro números enteros decimales entre 0 y 255, están escritas en el formato xxx.xxx.xxx.xxx, por ejemplo, 146.153.205.26 es una dirección IP en formato técnico.

Los equipos de cómputo de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva. La organización ICANN (Internet Corporation for Assigned Names and Numbers – Corporación de Internet para la Asignación de Nombres y Números) es la responsable de asignar direcciones públicas de IP, es decir, direcciones IP para

los equipos de cómputo conectados directamente a la red pública de Internet, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.

Existen diferentes clases de redes con el protocolo IP y se clasifican de acuerdo con la cantidad de bytes que representan a la red, las clases se muestran a continuación:

1. Clase A

Es una dirección IP de clase A cuando el primer byte representa a la red (considerando los bytes de izquierda a derecha). El bit más importante es el primer bit a la izquierda que está en cero, lo que significa que hay 2^7posibles redes, es decir, 128, considerando el rango del primer byte de 0000001 a 01111111, en decimal y con el formato técnico para representar las direcciones IP se tiene las redes disponibles de clase A que van desde 1.0.0.0 a 127.0.0.0.

2. Clase B

En una dirección IP de clase B, los primeros dos bytes representan a la red. Los primeros dos bits siempre son 10; esto significa que existen 2^{14} posibles redes, es decir, 16384 redes posibles, considerando el rango de los primeros dos bytes de 10000000 00000000 a 10111111 11111111, en decimal y con el formato técnico para representar las direcciones IP se tiene que las redes disponibles de la clase B van de 128.0.0.0 a 191.255.0.0.

3. Clase C

En una dirección IP de clase C, los primeros tres bytes representan a la red. Los primeros tres bits siempre son 110; esto significa que hay 2^{21} posibles redes, es decir,2097152, considerando el rango de los primeros tres bytes de 11000000 00000000 00000000 a 11011111 11111111 11111111, en decimal y con el

formato técnico para representar las direcciones IP se tiene que las redes disponibles de la clase C van desde 192.0.0.0 a 223.255.255.0

4. Clase D

Se caracterizan porque su dirección comienza con la secuencia de bits 1110 y corresponden a las direcciones desde la 224.0.0.0 a la 239.255.255.255. Estas direcciones reciben el nombre de multicast, es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Un paquete dirigido a una dirección multicast es entregado a todas las máquinas que componen al grupo.

5. Clase E

Se caracterizan porque su dirección comienza con la secuencia 1111 y van desde la 240.0.0.0 hasta la 255.255.255.255. Son direcciones especiales reservadas por la IANA (la Autoridad Administradora de Dominios) y sólo está asignada la 255.255.255.255 que corresponde a todas las máquinas conectadas a un soporte físico.

El principal objetivo de dividir las direcciones IP en las clases comerciales A, B y C es facilitar la búsqueda de un equipo en la red, la asignación de una dirección IP se realiza de acuerdo con el tamaño de la red (Tabla 1.4)

Tabla 1.4 Clasificación de las Distintas Clases de Redes

CLASE	CANTIDAD DE REDES POSIBLES	CANTIDAD MÁXIMA DE EQUIPOS EN CADA RED
A	126	16777214
B	16384	65534
C	2097152	254

f) TCP

TCP (Transmission Control Protocol - Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo OSI, es un protocolo orientado a la conexión que proporciona fiabilidad, control de flujo y recuperación de errores; protocolo punto a punto que suministra una conexión lógica entre pares de procesos, identificados cada uno de ellos por un socket, utilizando los números de puertos de éstos como comunicación con los procesos de nivel superior. El protocolo TCP es un protocolo orientado a la conexión, es decir, permite que dos computadoras estén en comunicación y tengan un control de estado de la transmisión.

Las principales características que tiene el protocolo TCP son las siguientes:

- TCP permite colocar los datagramas nuevamente en orden cuando provienen del protocolo IP.
- TCP permite el monitoreo del flujo de los datos y así evita la saturación de la red.

- TCP permite que los datos se formen en segmentos de longitud variada para entregarlos al protocolo IP.

El principal objetivo del protocolo TCP está en las aplicaciones que pueden comunicarse en forma segura con el sistema de archivos que manejan al protocolo TCP independientemente de las capas inferiores. El protocolo TCP garantiza la transferencia de datos confiable.

La conexión que se establece en el protocolo TCP entre las dos aplicaciones a menudo se realiza siguiendo el siguiente esquema:

- Los puertos TCP deben estar abiertos.
- La aplicación en el servidor es pasiva, es decir, que la aplicación escucha y espera una conexión.
- La aplicación del cliente realiza un pedido de conexión al servidor

El TCP debe realizar también el control de flujo. Para ello el módulo receptor va informando al módulo emisor de la cantidad de octetos que puede recibir sin problemas en cada lapso de tiempo, mediante un mecanismo llamado ventana deslizante. A fin de utilizar más eficientemente los recursos disponibles TCP ofrece la posibilidad de múltiple acción entre distintos procesos de usuario, transmisión simultánea y la posibilidad de especificar niveles de seguridad o prioridad para las comunicaciones que asegura que la conexión no se cierra hasta no haber recibido confirmación de la recepción de todos los datos enviados.

La estructura general del encabezado del protocolo TCP se observa en la figura 1.12

<table>
<tr><td colspan="6">Puerto de origen (16</td><td colspan="3">Puerto de destino (16 bit)</td></tr>
<tr><td colspan="9">Número de orden (32 bit)</td></tr>
<tr><td colspan="9">Número de reconocimiento (32 bit)</td></tr>
<tr><td>Desplazamiento de los datos (4 bit)</td><td>Reservado (6 bit)</td><td>U R G</td><td>A C K</td><td>P S H</td><td>R S T</td><td>S Y N</td><td>F I N</td><td>Ventana (16 bit)</td></tr>
<tr><td colspan="6">Código de verificación (16 bit)</td><td colspan="3">Puntero a datos urgentes (16 bit)</td></tr>
<tr><td colspan="7">Opciones (Variable)</td><td colspan="2">Relleno</td></tr>
<tr><td colspan="9">Datos (Variable)</td></tr>
</table>

Figura 1.12 Estructura del encabezado del protocolo TCP

Donde:

1. Puerto de origen: Identifica al proceso de un puerto de origen.

2. Puerto de destino: Identifica al proceso de un puerto de destino.

3. Número de orden: Número de orden del byte que identifica la posición inicial de los datos del segmento con respecto al flujo de bytes original del emisor.

4. Número de Reconocimiento: Indica el número de orden del byte que el receptor espera.

5. Desplazamiento de los datos: Indica la longitud de la cabecera de TCP medida en palabras de 32 bits.

6. Reservado: Campo reservado para el uso futuro que debe llevar todos sus bits a 0.

7. Banderas: Los siguientes seis campos son indicadores para solicitar servicios o marcar la validez de otros campos de la cabecera.

8. Ventana: Indica el número de octetos que el receptor podría aceptar.

9. Código de verificación: Se usa para verificar la corrección de los datos contenidos en el segmento incluida la cabecera.

10. Puntero a datos urgentes: Este campo, válido sólo si el URG está a 1, indica los datos considerados urgentes que cada implementación tratará de manera diferente.

11. Opciones: Un campo para implementación de opciones que funciona de manera similar a como lo hace el campo opciones del datagrama IP. Cada opción tiene tres campos, un octeto que contiene el código de opción, un campo que indica la longitud de la opción y el tercer campo que incluye los valores propios de la opción. Las tres opciones disponibles actualmente son: fin de lista de opciones, código 0, sin operación, código 1, y longitud máxima del segmento, código 2.

12. Relleno: Relleno de bit a cero para completar palabra de 32 bit.

g) UDP

UDP (User Datagram Protocol - Protocolo de Datagrama de Usuario) es un protocolo del modelo OSI. Este protocolo es muy simple, ya que no proporciona

detección de errores, a continuación se muestra encabezado del segmento UDP en la Figura 1.13

Puerto de origen (16 bits)	Puerto de destino (16 bits)
Longitud total (16 bits)	Suma de comprobación del encabezado (16 bits)
Datos (Longitud variable)	

Figura 1.13 El encabezado del segmento UDP

Donde:

1. Puerto de origen: Es el número de puerto relacionado con la aplicación del remitente del segmento UDP.

2. Puerto de destino: Este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.

3. Longitud: Este campo especifica la longitud total del segmento con el encabezado incluido. Sin embargo, el encabezado tiene una longitud de 4^{16} bits, por lo tanto, la longitud del campo es necesariamente superior o igual a 8 bytes.

4. Suma de comprobación: Es una suma de comprobación realizada de manera tal que permite controlar la integridad del segmento.

h) SMTP

SMTP (Simple Mail Transfer Protocol - Protocolo Simple de Transferencia de Correo) es el protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión de punto a punto. Este protocolo funciona en línea, encapsulado en una trama TCP/IP. El correo se envía directamente al servidor de correo del destinatario.

El protocolo SMTP funciona con comandos de texto enviando al servidor SMTP vía el puerto 25 de manera predeterminada. A cada comando enviando por el cliente le sigue una respuesta del servidor SMTP compuesta por un número y un mensaje descriptivo.

i) POP

El protocolo POP (Post Office Protocol - Protocolo de Oficina de Correos), permite descargar el correo electrónico desde un servidor remoto. Es adecuado para las personas que no están permanentemente conectadas a Internet, ya que así pueden consultar los correos electrónicos recibidos sin que estar conectados.

Existen dos versiones principales de este protocolo, POP2 y POP3, y se encuentran asignadas a los puertos 109 y 110 respectivamente, para establecer una conexión a un servidor POP2 el cliente de correo abre una conexión TCP en el puerto 109 del servidor. Cuando la conexión se ha establecido, el servidor POP2 envía al cliente POP2 una invitación y después las dos computadoras se envían entre sí otras órdenes y respuestas que se especifican en el protocolo. Como parte de esta comunicación, al cliente POP2 se le pide que se autentique, el nombre de usuario y la contraseña del usuario se envían al servidor POP2. Si la autenticación es correcta, el cliente POP2 pasa al estado de transacción.

El POP3 está diseñado para recibir correo, no para enviarlo. La mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de

manera tal que un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta.

j) TELNET

Telnet es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente en el sistema (compuesto de una pantalla y un teclado) con el intérprete de comandos en la parte del servidor.

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII, éste se codifica en 8 bits, entre los cuales se encuentran secuencias de verificación del Telnet.

El protocolo Telnet se basa en tres conceptos básicos:

- El paradigma terminal virtual de red NVT (Network Virtual Terminal - Terminal Virtual de Red).
- El principio de opciones negociadas.
- Las reglas de negociación.

Las especificaciones de Telnet no mencionan la autenticación por parte del protocolo, éste no es un protocolo de transferencia de datos seguro ya que los datos que transmite circulan en la red como texto sin codificar. Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funcione como servidor, el puerto que utiliza es el 23.

El protocolo Telnet consiste en crear una abstracción de la terminal que permita a cualquier host de cliente a servidor comunicarse con otro host sin conocer sus características

1.5 Modelo OSI

Modelo de Interconexión de Sistemas Abiertos por sus siglas en inglés (Open System Interconnection). Este Modelo se vio impulsado por la ISO (International Organization for Standardization - Organización Internacional para la Normalización) y el motivo de éste es una definición de procedimientos estandarizados que permitan la interconexión de información entre usuarios.

Cabe aclarar que el modelo OSI no trata sobre ninguna implantación tecnológica, sólo muestra la forma de interoperar sistemas abiertos.

El modelo OSI está formado por 7 capas (Ver figura 1.10)

7.- Aplicación
6.- Presentación
5.- Sesión
4.- Transporte
3. Red
2.- Enlace
1.- Física

Figura 1.10 Capas del Modelo OSI

1. Capa Física

Esta capa es la que se ocupa de la interfaz física entre los dispositivos, entre otras funciones, las cuales son la transmisión de los bits a lo largo del canal de comunicación.

Las características más importantes de esta capa son el aspecto mecánico que está relacionado con la especificación del conector que transmite las señales a través de los conductores.

La siguiente característica es la eléctrica en la cual se especifica cómo se representan los bits.

Entre los medios de transmisión se observan dos tipos:

- Medios guiados: cable coaxial, cable de par trenzado no apantallado (UTP), fibra óptica.
- Medios no guiados: radio, infrarrojos, microondas, láser, satelital.

En los medios guiados la trasmisión es por medio de impulsos eléctricos, mientras que los medios no guiados emplean la transmisión por impulsos electromagnéticos.

2.- Capa de Enlace

Esta capa se encarga del direccionamiento físico, de la detección y control de errores, esto quiere decir que el emisor segmenta la información en tramas de datos y las transmite.

El Instituto de Ingenieros Eléctricos Electrónicos (IEEE) subdividió la capa de enlace en dos subcapas:

- *Control de Enlace Lógico (LLC).* Define cómo serán transferidos los datos sobre el medio físico, además de manejar el control de errores de transmisión, regular el

control de flujo de las tramas y encargada del direccionamiento de la subcapa MAC. En esta subcapa se ofrecen servicios orientados a conexión(garantizar la entrega de los datos) y los servicios orientados a no conexión (los datos no pueden ser entregados en su totalidad por no haber una conexión al momento)

- *Control de Acceso al Medio(MAC).* Se encarga de controlar el acceso al medio físico que los dispositivos comparten al mismo canal de comunicación, agregar nodo fuente y nodo destino a cada una de las tramas que se transmiten, detección y corrección de errores de transmisión y descartar tramas duplicadas o tramas que tienen fallas.

3.- Capa de Red

En esta capa el principal objetivo es hacer que los datos lleguen desde el origen hasta el destino, todo esto se hace mediante un encaminador comúnmente llamado router. Esto indica que se busca la mejor ruta para que el paquete llegue a su destino

Esta capa también cuenta con el control de congestión, pues en un momento determinado existen demasiados paquetes en la subred y se tiene que dar lugar a un cuello de botella.

4.- Capa de Transporte

La función de esta capa es aceptar todos los datos de la capa de sesión y a su vez dividirlos en unidades muy pequeñas para que pasen a la capa de red. También debe asegurar que estas unidades lleguen al otro extremo de la comunicación.

5.- Capa de Sesión

En esta capa se establecen las conexiones entre usuarios finales, a través de una sesión se puede permitir al usuario acceder al sistema.

En esta capa se proporcionan los siguientes servicios:

- Control de diálogo. Aquí la comunicación puede ser en dos sentidos o se puede ir alternando en los dos sentidos.
- Agrupamiento. De diferentes sistemas se puede agrupar la información para obtener un resultado final.
- Recuperación. Si hay alguna falla en el envío de información, la capa de sesión permite retransmitir todos los datos desde el punto de comprobación.

6.- Capa de Presentación

Esta capa se encarga de la presentación, es decir, de los aspectos de sintaxis y semántica de la información que se transmite, esto se debe a que hay distintos equipos que cuentan con diferentes formas de caracteres y la capa se encarga de mostrarlos de una manera entendible al usuario.

Además de contar con la función de formateo de datos (presentación), se tienen otras dos funciones importantes en esta capa que son el cifrado y la compresión de datos.

El cifrado se lleva a cabo para proteger la información que se trasmite, esto es, los datos no viajan en claro para que sólo sean entendidos por las personas autorizadas.

La compresión se lleva a cabo para reducir el tamaño de los datos que son transmitidos y funciona mediante el uso de algoritmos, en esta función todos los bits repetidos son reemplazados por un token (patrón de bit mucho más corto).

7.- Capa de Aplicación

Encargada de sincronizar las aplicaciones, además de controlar la integridad de los datos.

La función principal que se presenta en esta capa es la de dar servicio de correo electrónico, HTTP, FTP, SSH, FTP, TELNET.

Esta capa cuenta con funciones de implementación de aplicaciones distribuidas.

CAPÍTULO 2

SEGURIDAD INFORMÁTICA

2.1 Definición de Seguridad Informática

Antes de definir el concepto de Seguridad Informática se mencionan algunos términos importantes que se ven involucrados.

Se entiende por datos a todas aquellas cifras y hechos sin analizar. La información se define como el conjunto de datos que han sido analizados u organizados de manera lógica.

"***El concepto de seguridad se refiere a todo tipo de precauciones y protecciones que se llevan a cabo para evitar alguna acción que comprometa a la información***"[2]

Entonces, la seguridad informática consiste en un conjunto de herramientas que permita proteger la información de cualquier peligro que se presente.

La seguridad informática se relaciona con la seguridad de la red, ya que la información necesita de un canal de transporte y las computadoras transmiten información por medio de la red, de esta manera, el objetivo principal es que los datos lleguen seguros a su destino.

La palabra seguridad es un concepto que brinda protección y confianza, la protección se orienta a todos los bienes mientras que la confianza la tiene quien esté operando ese recurso.

Se tiene que instalar una serie de herramientas necesarias para obtener la seguridad deseada, para saber qué herramientas son útiles es necesario contestar tres preguntas:

- *¿Qué se quiere proteger?* Es importante identificar qué recursos se van a proteger de los riesgos que puedan presentarse.
- *¿De qué se quiere proteger?* Cualquier recurso es vulnerable, por lo cual es necesario que los dueños de los bienes le pidan ayuda a

[2] López Barrientos María Jaquelina, Quezada Reyes Cintia. *Fundamentos de seguridad informática*. UNAM, Facultad de Ingeniería, 2006, p23.

especialistas para que analicen las posibles amenazas o peligros de su entorno.

- *¿Cómo se va a proteger?* Una vez contestadas las dos preguntas anteriores se plantearán las políticas de seguridad, pues esto permitirá contrarrestar las amenazas y vulnerabilidades.

Es importante señalar que la seguridad no está garantizada al 100% puesto que el eslabón más débil es la gente, siendo ésta la que manipula los sistemas informáticos, a pesar de este problema, se buscan reducir las probabilidades de que las fallas se presenten en el sistema.

2.2 Amenazas y vulnerabilidades.

Las amenazas y vulnerabilidades son dos términos que no hay que confundir, ya que generalmente se piensa que ambos tienen el mismo significado.

Se le llama amenaza a todo aquello que intente, pueda o pretenda destruir o dañar un recurso, el peligro está latente. Ésta se puede presentar por personas o cualquier otra circunstancia que pueda provocar el daño.

Las vulnerabilidades son aquellas debilidades que tiene el recurso activo donde se le permite al atacante quebrantarlos. Las vulnerabilidades pueden ser aprovechadas por las amenazas para dañar total o parcialmente los bienes.

A continuación se menciona la clasificación de las amenazas y las vulnerabilidades

2.2.1 Clasificación general de las amenazas

Las amenazas se clasifican en los siguientes tipos:

a) De humanos

Este tipo de amenaza ocurre cuando la persona no tiene cuidado con la información que posee, las causas pueden ser por un descuido, inconformidad, ignorancia, etcétera. Como algunos ejemplos pueden mencionarse la ingeniería social, la ingeniería social inversa, el robo, el fraude, el sabotaje, el chantaje, el terrorismo.

b) Errores de hardware

La amenaza se presenta por fallas físicas en cualquier dispositivo de la computadora, la falla de las computadoras ocasionan en algunos casos pérdida de información, mal funcionamiento del equipo, pérdida del dispositivo.

c) Errores de la red

Esta amenaza se presenta cuando hay alguna falla en la red, ya sea por el mal diseño de la red y se satura el canal de comunicación llegando a bloquear el sistema, dejando como consecuencia que se pierda información o que otro usuario entre a datos no autorizados.

d) Problemas de tipo lógico

Esta amenaza se presenta cuando el diseño de un mecanismo de seguridad no fue bien implementado en el sistema. El usuario al desconocer lo que debe tener instalado en lo referente a software puede dar entrada a códigos maliciosos, el código malicioso es un programa que entra al sistema de cómputo provocando fallas en el sistema, algunos códigos maliciosos que se pueden mencionar son los caballos de Troya, los gusanos, los virus.

e) Naturales

Se refiere a las acciones provocadas por la naturaleza y donde los humanos no tienen participación alguna, en este tipo de amenazas se encuentran las inundaciones, los terremotos, incendios, vientos muy fuertes. Si se presenta algún tipo de éstas en cualquier empresa, repercute en el funcionamiento de los equipos, la red, las instalaciones.

El fuego es la amenaza principal en cuanto a desastres naturales, ya que por cualquier descuido se puede dar con facilidad, como instalaciones eléctricas mal diseñadas que no soporten determinados números de equipos conectados, dejar conectado algún aparato que se caliente demasiado, un cable en mal estado.

2.2.2 Clasificación general de las vulnerabilidades

Existen seis tipos de vulnerabilidades:

a) Física

Este tipo de vulnerabilidad hace mención a la posibilidad de tener acceso físico al lugar, todo esto con el fin de poder dañar, modificar o robar información importante del sistema que se encuentre en dicho lugar. Por ejemplo, el no contar con buena seguridad en el área, como sería tener chapas frágiles donde éstas se puedan abrir fácilmente.

b) Natural

Los sistemas se ven afectados cuando ocurren desastres naturales, ocasionado por el descuido, por la falta de precauciones que debe tomar cada empresa respecto a la ubicación de la empresa.

Por ejemplo, la falta de extinguidores en cada piso, el no tener un espejo del sistema en otra ubicación, el no contar con ventiladores para evitar que los equipos no se sobrecalienten, un buen sistema de drenaje en caso de inundaciones, entre otras variadas causas de desastres naturales.

c) Software

Las vulnerabilidades que se encuentran en este tipo se deben a que existen programas mal diseñados y programados, carentes de seguridad siendo un programa con errores en la configuración y que cualquier ente no autorizado pueda acceder al sistema.

La mayoría de los programas que son controlados desde la red suelen ser inseguros debido a que no cumplen con todos los protocolos de comunicación y la operación de ese sistema no suele ser monitoreado constantemente.

d) Hardware

Una de las causas principales que da origen a este tipo de vulnerabilidad es el ignorar los manuales donde vienen las características técnicas de cualquier dispositivo, siendo a la larga un serio problema, ya que al no leer el manual se comenten errores como un mal armado del equipo, el no tomar en cuenta cómo llevar a cabo su mantenimiento para que dure, el saber qué otras tecnologías soporta, el comprar equipo de mala calidad o simplemente hacer mal uso de él al no saber su funcionamiento correcto, exponerlo a fuertes cargas estáticas.

e) De red

El tener conectados equipos a la red provoca una gran probabilidad de que sea muy vulnerable el sistema, ocasionando que las personas que entran al sistema puedan interceptar la comunicación.

A esto añadirle otros problemas como sería un mal diseño de la red, un cableado con pésima calidad que no cumpla con los estándares, el no contar con equipo adecuado como lo son la falta de placas en el área y si hay alguna falla eléctrica no contar con un no- break en el servidor.

f) Humana

Se sigue con la misma línea que las amenazas, siendo que la gente es el eslabón más débil y la mayoría de las vulnerabilidades es a causa del descuido de la persona a cargo, como el no contratar gente con aptitudes para el puesto, ni contar con el personal necesario, que la gente no pida una identificación al querer entrar a un área restringida.

Que no se le dé capacitación al personal así como cursos de actualización pues si se quedan con el conocimiento estancado no sabrán de las nuevas tecnologías existentes para su empresa.

Los malos tratos que se dan dentro de la organización y peor aún hacia gente ajena a la empresa, el no contratar servicio de seguridad para la empresa, el no tener ética profesional, y algunas otras causas que provoque este tipo de vulnerabilidad.

2.2.3 Clasificación general de amenazas en la red

Existe una clasificación general de las amenazas en ésta se pueden observar cuatro categorías:

a) Interrupción: el sistema puede ser destruido o bien no estar disponible, este tipo de amenaza es en contra de la disponibilidad. (Véase figura 2.1)

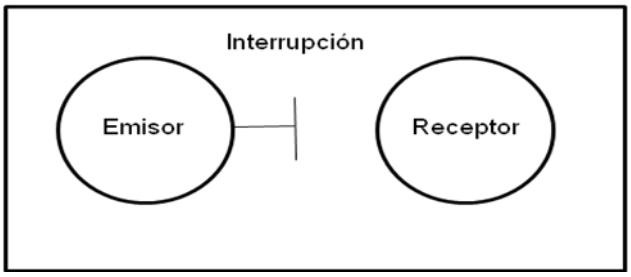


Figura 2.1 Flujo de Interrupción

b) Intercepción: algún usuario no autorizado puede tener acceso al recurso provocando una amenaza contra la confidencialidad. (Véase figura 2.2)

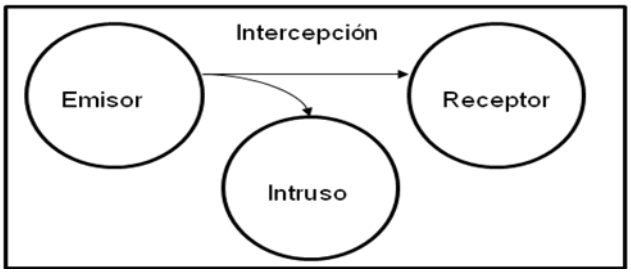


Figura 2.2 Flujo de Intercepción

c) Modificación: el usuario no autorizado puede acceder al sistema para manipularlo a su beneficio, esta amenaza es contra la integridad. (Véase figura 2.3)

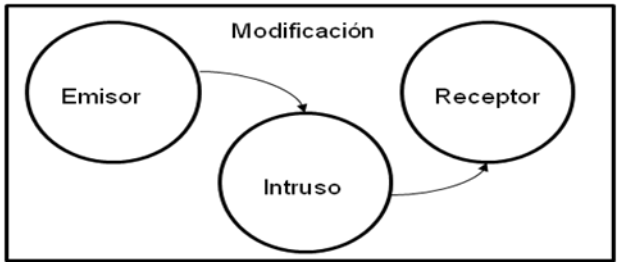


Figura 2.3 Flujo de Modificación

d) Suplantación o fabricación: el intruso puede insertar información falsa en el sistema siendo esto una amenaza contra la autenticidad. (Véase figura 2.4)

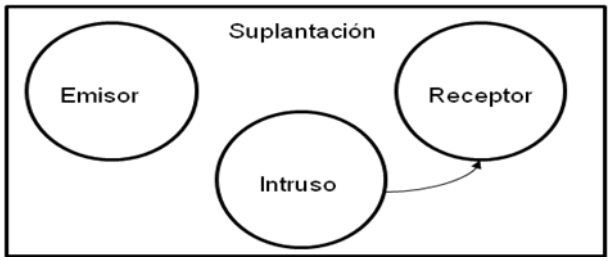


Figura 2.4 Flujo de Modificación

Un ataque es la realización o culminación de una amenaza. Es posible clasificar a los ataques dentro de las mismas cuatro categorías descritas anteriormente, considerando que la descripción no es sólo una posibilidad sino un hecho. También los ataques se engloban en dos grandes categorías.

- Ataque pasivo: aquí el atacante no altera ninguna información, sólo la observa o escucha, un ataque de tipo intercepción se encuentra en este rubro. Los ataques pasivos pueden prevenirse empleando herramientas adecuadas contra el análisis de tráfico.

- Ataque activo: el atacante modifica la información dentro de este rubro se encuentran la interrupción, la suplantación y la modificación. Es posible detectar y prevenir este tipo de ataques, sin embargo la detección puede presentarse de manera extemporánea.

Independientemente del tipo de ataque que se esté realizando, es menester mencionar que cuenta con tres etapas identificables:

1) Preparación: en esta etapa el perpetrador plantea los objetivos deseados, algunas formas que se utilizan para realizar esta etapa son:

- Recolección de información: La forma con la que se obtendrá la información de otros usuarios sin la necesidad de ser administradores. La ingeniería social es de mucha utilidad para el perpetrador, aunque algunas veces recibe ayuda del administrador del sistema, no siempre es así.

- Puerta trasera: Se instala un software que contiene mecanismos escondidos que permiten desviar información confidencial a otro lugar en donde el perpetrador sepa la ubicación.

- Exploración: Se busca información básica de la víctima para obtener datos importantes como lo es la contraseña que utiliza, el número telefónico, entre otra información que le sea de utilidad al perpetrador.

- Mal uso de la autoridad: Cuando el perpetrador logra tener acceso al sistema sin necesidad de utilizar algún método especial para lograrlo significa entonces que se carece de autoridad dentro de la organización.

2) Activación: esta etapa se puede llevar a cabo de las siguientes maneras:

- Si el sistema sufre una interrupción en el sistema operativo, posiblemente el código de ataque se llevará a cabo, si no sucede así, el perpetrador utilizará un programa que le permita interrumpir el sistema.

- Si el programa de ataque es más sofisticado, éste ocasionará que su identificación sea tardía, provocando en algunas ocasiones que el sistema sufra un daño más destructivo.

3) Ejecución: Esta etapa depende del objetivo que se quiera lograr, entre los cuales se pueden mencionar:

- Mal uso activo: se afecta cualquier tipo de información, generalmente los archivos son destruidos o en algunas ocasiones alterados.

- Mal uso pasivo: este objetivo no afecta de ninguna manera al sistema, ni los archivos son modificados, esto es porque el perpetrador sólo quiere fisgonear qué tipo de información se encuentra en dicho equipo.

- Robo del servicio: cuando se llega a robar el servicio, éste se puede utilizar para mandar correo electrónico a ciertas personas, mandar información confidencial de ese sistema, jugar con ciertos datos, etcétera.

2.3 Servicios de seguridad

Un servicio de seguridad se encarga de mejorar la seguridad del sistema de información, así como la manera en que será difundida en la organización. Este servicio protege contra ataques de seguridad y para poder brindar este servicio es necesario utilizar en ocasiones más de un mecanismo de seguridad.

A continuación se mencionan los diferentes servicios de seguridad:

1) Confidencialidad

   Se le considera confidencial a aquello que mantiene en secreto cualquier tipo de información, la confidencialidad protege información secreta de cualquier persona que no esté autorizada para manipularla.

Es de suma importancia para cualquier empresa mantener la confidencialidad de su información, ya que al ser descubierta por gente no autorizada, provocaría un gran daño para la empresa, pues el intruso tendría acceso a datos financieros, información confidencial de los recursos que se poseen, información personal.

Es conveniente contar con un buen control de seguridad para evitar problemas, ya que muchas personas intentan acceder la información confidencial.

El servicio de confidencialidad se encarga de asegurar que nadie pueda leer o copiar cualquier información sin autorización, tampoco que se pueda interceptarla.

2) Autenticación

Se trata de la forma en que uno verifica la identidad de un proceso o una persona.

El servicio de autenticación se encarga de asegurar que la comunicación se lleve de manera correcta, que lo que se espera recibir sea lo acordado. La autenticación se realiza a través de:

a) Algo que se sabe: cualquier sistema requerirá de algún dato que permita identificar que tal usuario es el indicado para acceder a la información, tales datos pueden ser una contraseña o algún número de validación.

b) Algo que se tiene: la forma para verificar la identidad se puede realizar por algún tipo de credencial que sea de utilidad y que sea aceptada por el sistema.

c) Algo que se es: se refiere a algo que puede indicar la identidad de manera más avanzada, como es la voz, la retina, huella digital, esto se realiza con aparatos especiales.

3) Integridad

La integridad se encarga de proporcionar controles que aseguren que el contenido de dicha información no ha sido modificado y que se mantenga intacta al ser transmitida a otro lugar. Si la integridad no existiera, la información sería manipulada a conveniencia de cualquier persona.

Para verificar que un producto llega completo, se comprueban los sellos que le colocan, si están intactos el producto no sufrió ningún altercado.

Para llevar a cabo la verificación de integridad en los sistemas de información es más difícil, ya que cualquier individuo puede cambiar los datos si logra acceder al sistema y si su intención es perjudicar a la empresa.

Se cuenta con dos tipos de servicio de integridad:

a) Servicio de integridad del contenido: ofrece pruebas de que el contenido no ha sido modificado.

b) Servicio de integridad de la secuencia del mensaje: se ofrecen pruebas de que el orden de la secuencia de mensajes se mantuvo intacta durante su trasmisión.

4) No repudio

Este servicio se encarga de que no se niegue que un mensaje ha sido transmitido. Esto es, encargarse de que se pueda demostrar recepción y envío de información a un tercero. Y los siguientes servicios son los que podrían ser proporcionados:

a) No repudio de origen: que se pueda probar que el emisor niegue haber mandado un mensaje con base en pruebas del origen de los datos.

b) No repudio de envío. Que se puedan dar pruebas de que se han enviado los datos.

c) No repudio de transporte: el probar que los datos fueron transportados y evitar la negación de que se hizo.

d) No repudio de recepción: que se pueda probar que se ha recibido el mensaje.

5) Control de acceso

Éste se encarga de limitar el acceso a la organización o al sistema de información de personas que no estén autorizadas. Para tener este control es necesario pedir que el usuario se identifique, una vez hecho esto le será permitido el acceso a su lugar de trabajo.

Los derechos de acceso son los que describen hasta qué grado tiene privilegios cierto usuario. Los privilegios son designados por el administrador y éste puede revocarlos o cambiarlos.

El control de acceso es diferente de acuerdo con el nivel de seguridad, variando desde una entidad individual hasta la administración de la red.

6) Disponibilidad

Como su nombre lo indica este tipo de servicio permite que las personas autorizadas tengan acceso a la información deseada independientemente del día y la hora.

2.4 Políticas de seguridad

Las políticas de seguridad son aquellas que tienen consideradas leyes, reglas y prácticas que regulen la forma de dirigir y proteger cualquier recurso en una organización.

Una empresa debe tener bien planteadas su misión y visión, pues las políticas de seguridad reflejan fielmente los objetivos de la organización, protegiéndola de amenazas y vulnerabilidades.

Si la organización plantea reglas que no le son útiles y están mal elaboradas las políticas de seguridad, tendrá una tarea muy difícil ya que no visualiza claramente lo que debe proteger.

Una organización con reglas bien plateadas podrá gestionar la seguridad de la información de manera eficiente, confiable y ordenada.

Es necesario que las políticas de seguridad se desarrollen en pequeños grupos, por ejemplo, en las oficinas y en los centros de cómputo, las políticas tendrán que cambiar ya que cada lugar tendrá diferentes tipos de vulnerabilidades y amenazas. Esto no representa la inexistencia de un reglamento general que se debe cumplir en toda la empresa, independientemente de cada departamento y diferente a las políticas de seguridad. Existen principios que se aplican en las políticas en general, a continuación se mencionan a detalle:

1) *Responsabilidad individual*: este principio hace referencia al hecho de que toda persona debe estar consciente de lo que hace, ya que cualquier acción que realice quedará registrada y será examinada.

2) *Autorización*: las reglas que establecen quién o quiénes pueden utilizar los recursos dados.

3) *Mínimo privilegio*: las personas sólo están autorizadas para utilizar las herramientas necesarias que permitan hacer su trabajo.

4) *Separación de obligaciones*: debe existir una separación de las funciones que realizan la misma actividad, ya que con esto se evita que una persona cometa un ataque sin ser detectado.

5) *Auditoría*: el trabajo que se realiza debe ser monitoreado desde el principio con el fin de tener registrado lo que cada persona realiza en sus funciones.

6) *Reducción de riesgos*: se debe contar con una estrategia para reducir riesgos a un nivel aceptable.

La redacción de las políticas de seguridad requiere de un compromiso serio por parte de la organización, pues se deben establecer las fallas y vulnerabilidades que existen en ella y actualizarse o modificarse de acuerdo con el dinamismo que exista en la empresa. Estos cambios pueden ser el aumento de personal, cambio en la infraestructura, creación de nuevos servicios, cambios de ubicación de la empresa, etcétera.

Las políticas de seguridad ofrecen una explicación sobre por qué se están tomando ciertas decisiones y demostrar qué tan importante son los recursos que se encuentran en la organización. Las políticas deben redactarse de forma clara y entendible, siguiendo una estructura positiva y haciendo referencia a alguna de las dos filosofías existentes que son la prohibitiva y la permisiva:

- La prohibitiva dice que todo está prohibido a excepción de lo que específicamente está permitido.
- La permisiva dice que todo está permitido a excepción de lo que específicamente está prohibido.

Al formular las políticas de seguridad es necesario considerar los siguientes aspectos:

- Se debe realizar un análisis de riesgos para valorar los activos de la organización y así redactar políticas que se apeguen al funcionamiento de la empresa.
- Una vez identificados los riesgos, se deben reunir las personas que redactarán las políticas con los dueños de dichos recursos y de esta manera proponerles las políticas pues estas personas poseen experiencia y se las harán hacer saber a los dueños.
- Las políticas deben cubrir todos los aspectos que se relacionen con el sistema, también deben protegerlo en los niveles físico, humano, lógico y logístico.
- Comunicar a todo el personal sobre el desarrollo de las políticas y el por qué se redactaron estas políticas, qué beneficios y riesgos tiene cada recurso activo.

- Las políticas de seguridad se deben adecuar a las necesidades y recursos de la empresa e identificar quién tiene la autoridad para tomar decisiones en cada departamento.
- Verificar que se cumplan las políticas así como revisar periódicamente las operaciones de la empresa y los cambios que puedan hacerse de forma que sea benéfica para la organización.

Aunque actualmente cada vez son más organizaciones que se preocupan por establecer políticas de seguridad, aún el porcentaje es muy poco ya que el primer obstáculo que se puede observar es que los altos ejecutivos difícilmente se convencen de lo benéfico que es tener políticas de seguridad en la empresa.

Las políticas de seguridad deben integrarse a las estrategias de la empresa, a su misión y visión con el propósito de que ésta funcione adecuadamente.

Para la realización de políticas de seguridad es necesario recordar tres preguntas básicas que anteriormente se mencionaron:

- ¿Qué se quiere proteger?
- ¿De qué se quiere proteger?
- ¿Cómo se va a proteger?

2.5 Algoritmos de cifrado

Con el paso del tiempo el manejo de información por medio de la red fue creciendo cada vez más hasta convertirse hoy en día en el medio principal para el transporte de mensajes, esto a su vez trae peligros ya que hay intrusos que desean obtener información de utilidad para ellos mismos o simplemente para ver qué tipo de documentos tiene determinado usuario, violándose así los servicios de seguridad como la integridad, autenticación, no repudio y control de acceso. Para evitar este tipo de sucesos es necesario proteger la información por medio de la criptografía.

La criptografía se encarga de estudiar las técnicas para convertir cualquier tipo de información a una forma que no se podrá entender sin tener el conocimiento del método y la clave que sirvan para su transformación. Esto se hace con el fin de ocultar información y de esta forma protegerla de cualquier intruso.

La ciencia que se encarga de estudiar las escrituras ocultas se llama criptología, en ella se incluye la rama de la criptografía y la esteganografía, este método se encarga de ocultar el contenido de un mensaje en un canal diferente, ya sea el sonido o una imagen.

La criptografía tiene por objetivo lograr la disponibilidad, la integridad y la confidencialidad en un mensaje. Cumpliendo lo anterior se asegura que el mensaje sólo sea leído por el personal autorizado.

En la criptografía se le llama texto en claro a aquel mensaje que se quiere transmitir de forma confidencial, el cifrado es el proceso que transforma el texto en claro en un texto que no cualquiera pueda interpretar, este texto recibe el nombre de texto cifrado. Al proceso de volver a transformar el texto cifrado en el texto en claro se le llama descifrado. La clave es la parte más importante de este proceso, ya que aquí se encuentra la seguridad de un sistema de cifrado, es por esto que debe mantenerse en resguardo para evitar que algún ente no autorizado se apropie de ella. El tamaño de la clave varía dependiendo de las características del proceso de cifrado.

En la figura 2.5 Se observan los elementos que intervienen en el proceso de cifrado.

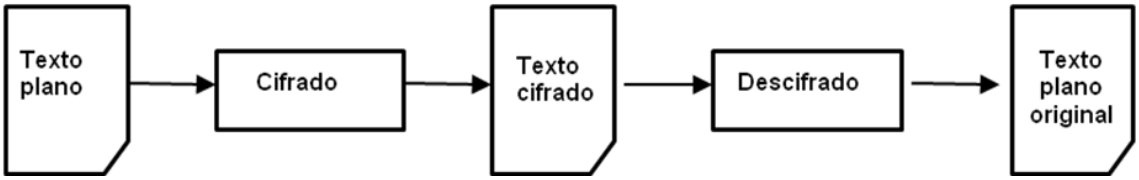


Figura 2.5 Elementos de un sistema criptográfico

En la antigüedad se utilizaban dos principios o técnicas de cifrado:

a) La sustitución consiste en cambiar cada carácter del texto plano por otro elemento, es decir, existe una correspondencia entre las letras del alfabeto que se encuentran en el texto original con los elementos de otro conjunto que puede ser de la misma forma o con diferente alfabeto y cada letra se va sustituyendo por el símbolo definido en dicho proceso. El destinatario debe saber la clave que se utilizó para poder descifrar y volverlo a su forma original.
b) La transposición consiste simplemente en cambiar el orden de las letras, a diferencia del método por sustitución éste sólo va reordenando las letras.

Existen 2 tipos de algoritmos de cifrado, si el emisor y receptor utilizan la misma clave de cifrado, se le conoce como cifrado simétrico, pero si el emisor y el receptor utilizan claves de cifrado diferentes, se le conoce como cifrado asimétrico.

a) Cifrado simétrico

Al cifrado simétrico se le llama de clave secreta o de clave privada ya que dicha clave la conoce tanto el emisor como el receptor únicamente. Es por eso que

se debe tener cuidado en la forma en la que se acordó la clave, ya que no importa que se sepa el método que se utilizó, sino la forma de cómo se protegió el mensaje y esto es a base de las claves.

La clave debe ser utilizada una sola vez cuando se cifran mensajes diferentes, es decir, una vez utilizada cualquier clave, habrá que modificarla ya que se corre el riesgo de que se descubra el mensaje por algún intruso.

Esta forma de cifrado se usa generalmente cuando el volumen de los datos es demasiado grande.

Existen diferentes algoritmos que a continuación se enuncian:

- DES (Data Encryption Standard – Estándar de cifrado de datos). Fue creado en los años 70, el método utiliza un cifrado por bloques en donde se tiene una longitud de bloque de 64 bits y una longitud de la clave de 56 bits, consiste en 16 iteraciones de la misma función
- 3DES. Este método recibe el nombre porque se hace tres veces el cifrado del DES y su creación se debe a que se quiso agrandar la clave sin necesidad de cambiarse de algoritmo de cifrado. Con este método se logró hacer el DES más seguro, aunque está desapareciendo lentamente debido a la creación de otros métodos más eficientes. Aunque la mayoría de las tarjetas de crédito manejan este algoritmo.

- RC4. Fue diseñado por Ron Rivest en 1987 y el nombre completo del método es Ron Cipher (cifrado de Ron), el número 4 se debe a la versión del diseño, también se le conoce como ARC4.

  Para usar este método se combina con el mensaje en claro usando la función XOR, se emplea una permutación de todos los 256 posibles símbolos de un byte de longitud, la permutación se inicializa con una clave de longitud variable entre 40 y 256 bits.

a) AES (Advanced Encryption Standard - Estándar de Cifrado Avanzado). Publicado por el NIST (National Institute for Standard and Technology-Instituto Nacional de Estándares y Tecnología) en el año 2001, con la finalidad de sustituir al DES. El AES maneja bloques de 128 bits, soporta el manejo de claves de diferentes longitudes (128, 192 y 256 bits). El AES hace uso de matemáticas polinomiales en estructuras de campos finitos.

b) Cifrado asimétrico

El cifrado asimétrico utiliza algoritmos donde la clave de cifrado es distinta a la de descifrado, además de que las operaciones matemáticas que realiza no son simples, ocasionado que los algoritmos sean de proceso lento al momento de descifrar en comparación con los algoritmos de cifrado simétrico.

Entre las partes que integra un cifrado asimétrico se encuentran el mensaje en claro, el algoritmo de cifrado, una clave pública y una privada, el mensaje cifrado y el algoritmo de descifrado.

Ejemplos de algoritmos asimétricos:

- RSA. Por las siglas de sus creadores Ronald Rivest, Adi Shamir y Leonard Adelman. Desarrollado en 1977, realiza la factorización de un número de gran tamaño.

  Entre las desventajas de este algoritmo es que requiere mayor tiempo de ejecución en comparación con el cifrado simétrico, la seguridad del cifrado depende de la eficiencia computacional y por último la clave privada debe ser cifrada por algún algoritmo simétrico.

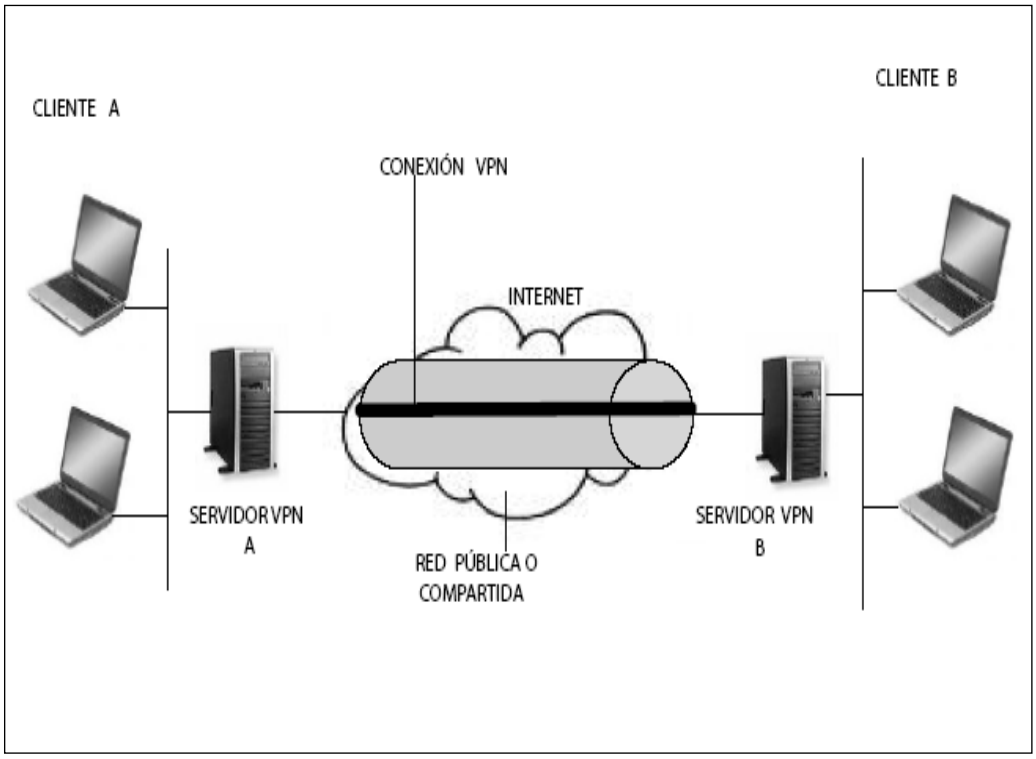
- Diffie-Hellman. Este método fue desarrollado por Whitfield Diffie y Martin Hellman en 1975. Este método consiste en intercambiar claves entre dos partes que previamente no han tenido contacto, utilizando un canal inseguro y de manera anónima.

En cuestiones matemáticas este método se basa en las potencias de los números y en la función mod (módulo discreto). Esto es la potencia discreta de un número como $Y = X^a \bmod q$.

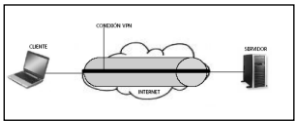
- MD4 (Message Digest Algorythm 4 – Algoritmo de Publicación de Mensaje). Desarrollado por Ron Rivest en el cual se hace una manipulación de bits para que se pueda obtener el hash (método para generar claves) para el uso en comprobaciones de integridad de mensajes, la longitud del mensaje es de 128 bits.

  En 1991 se desarrolló el MD5 como mejora del MD4 permitiendo la seguridad a la integridad de la información. La codificación del MD5 de 128 bits se representa como un número de 32 dígitos hexadecimales y así la obtención del valor hash se considera más segura.

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).

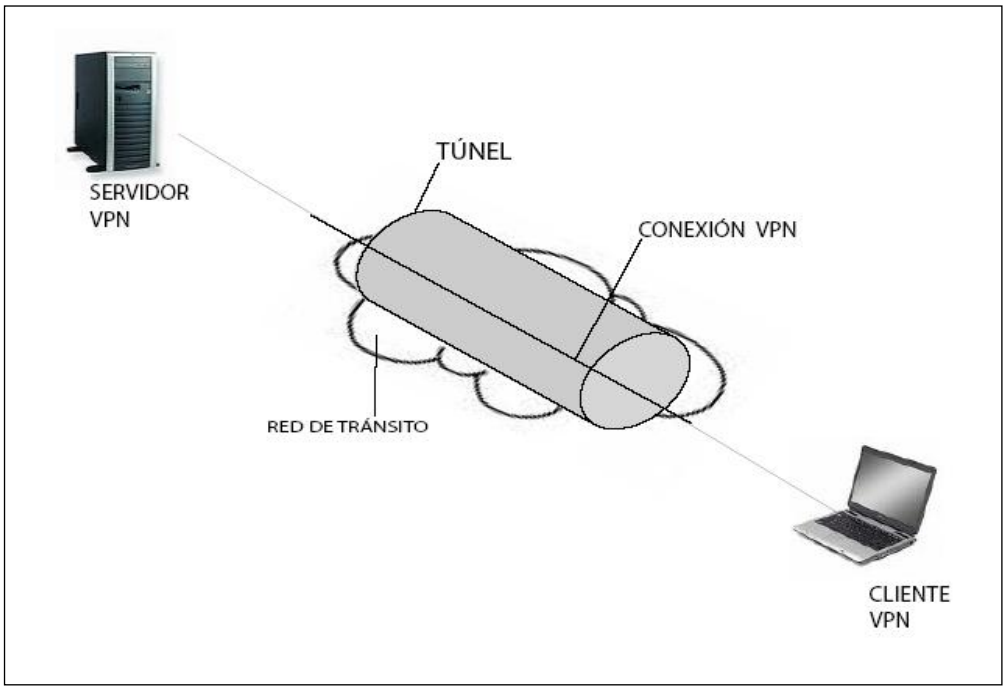


Figura 3.1 Una VPN de Cliente a Servidor

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).

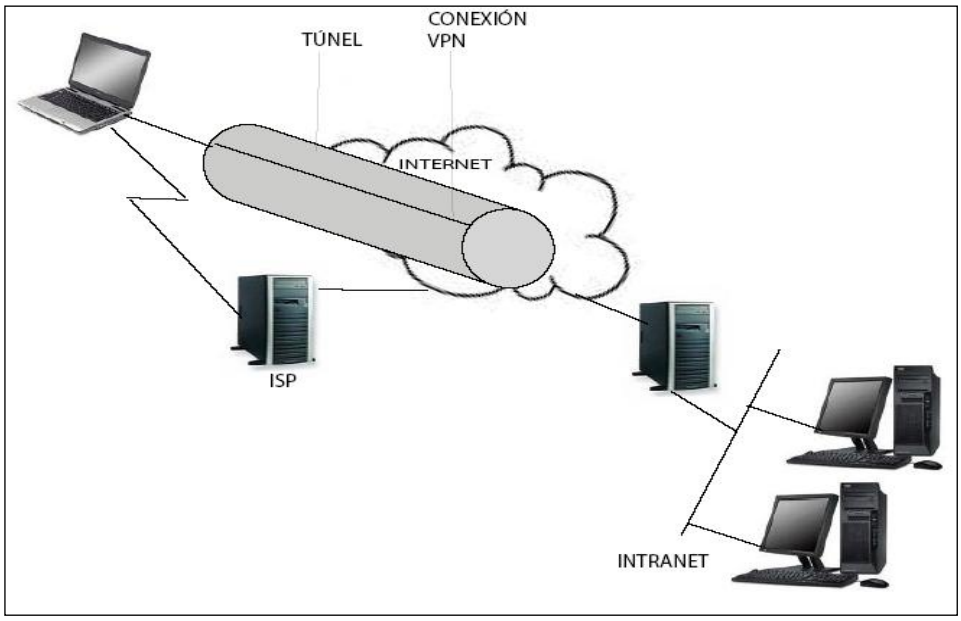


Figura 3.2 Una VPN de Cliente a Red Interna

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)

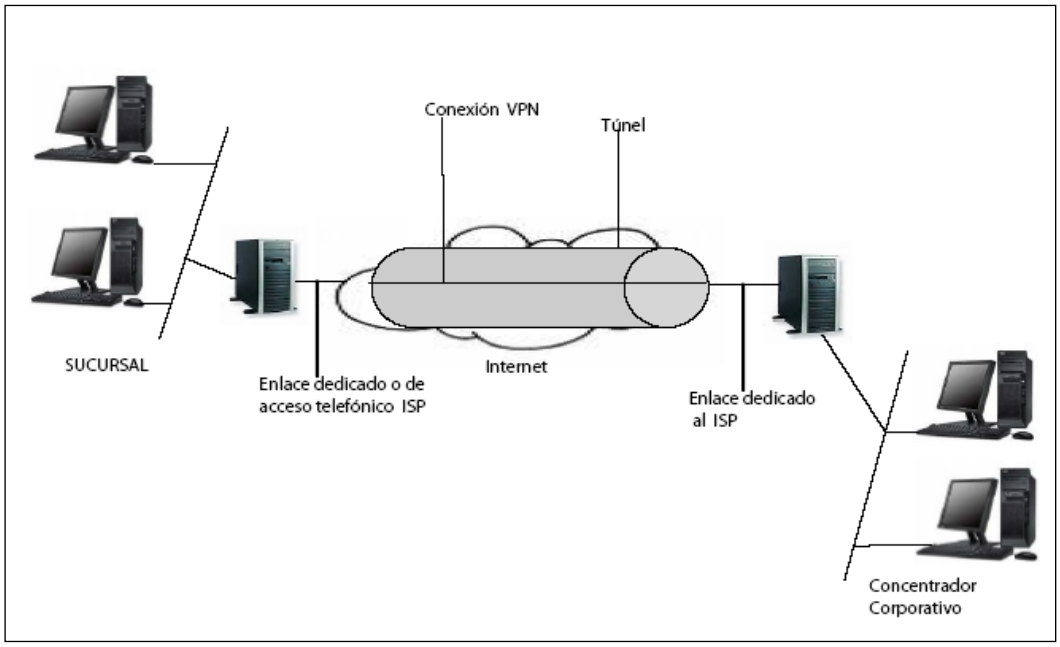
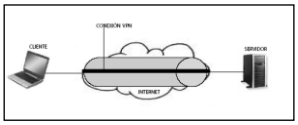


Figura 3.3 Una VPN de Red Interna a Red Interna

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.

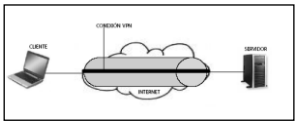
- **SEGURIDAD**: Provee cifrado y encapsulación de datos lo que permite que éstos viajen codificados y a través de un túnel seguro.

- **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.

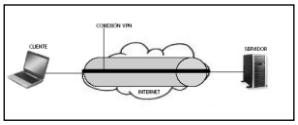
3.3.2 Desventajas de las VPN's

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.

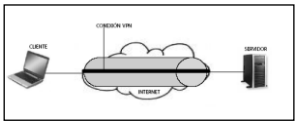
3.4 Tipos de VPN

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.

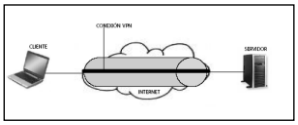
El Kernel de sistema operativo que tenga el Linux en sus distintas versiones que son: Fedora, RedHat, Suse, Ubuntu y otros más; es de suma importancia, porque el kernel es el núcleo principal de Linux, se puede definir como el corazón de este sistema operativo y es el encargado de que el software y el 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.

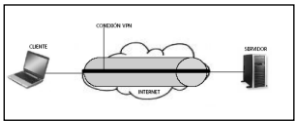
7) Las VPN's pueden aumentar la velocidad en las conexiones entre puntos empresariales gracias a que comprimen todo el tráfico añadiéndoles cifrado.

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.

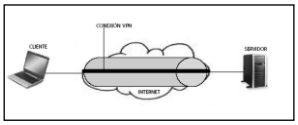
C) Cuentan con dispositivos que gestionan un acceso confiable a los usuarios de la red interna a través de servicios seguros de autentificación de ataques.

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".**[3]

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

[3] 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:

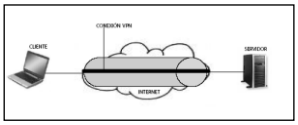
A) Protocolo PPTP

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 Securidad) 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."[4]

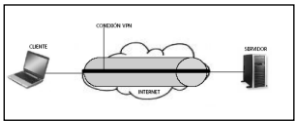
Este protocolo tiene dos modos de funcionamiento, modo transporte y modo túnel.

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

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



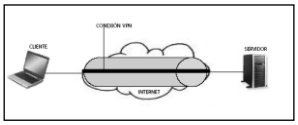
tráfico distinguible por un selector único. Todo el tráfico que fluye a través de una SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varias SA, cada uno de los cuales aplica cierta transformación. Los paquetes entrantes pueden ser asignados a una SA específica por los tres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

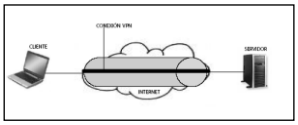
D) Protocolo L2TP

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).

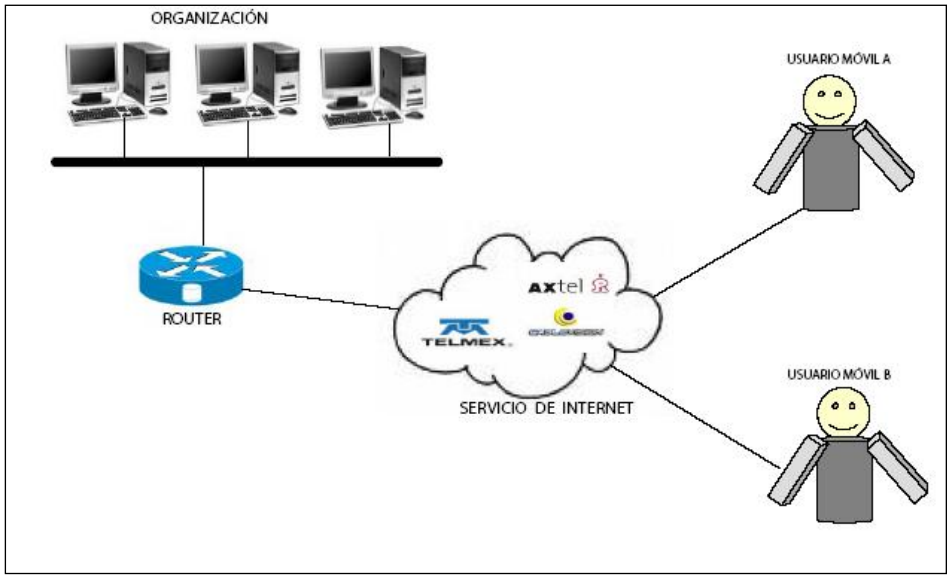
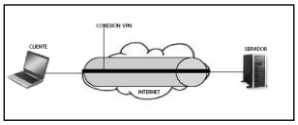


Figura 3.4 Una VPN de Acceso Remoto



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.

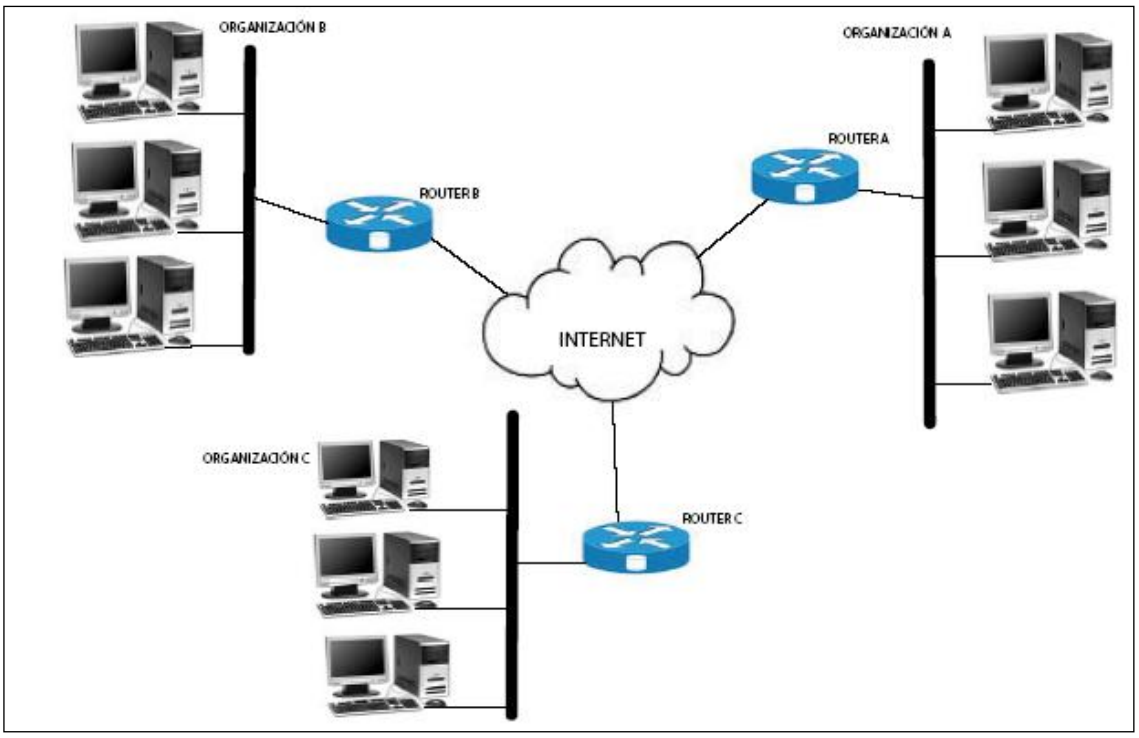
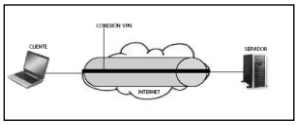


Figura 3.5 Una VPN de Intranet

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.

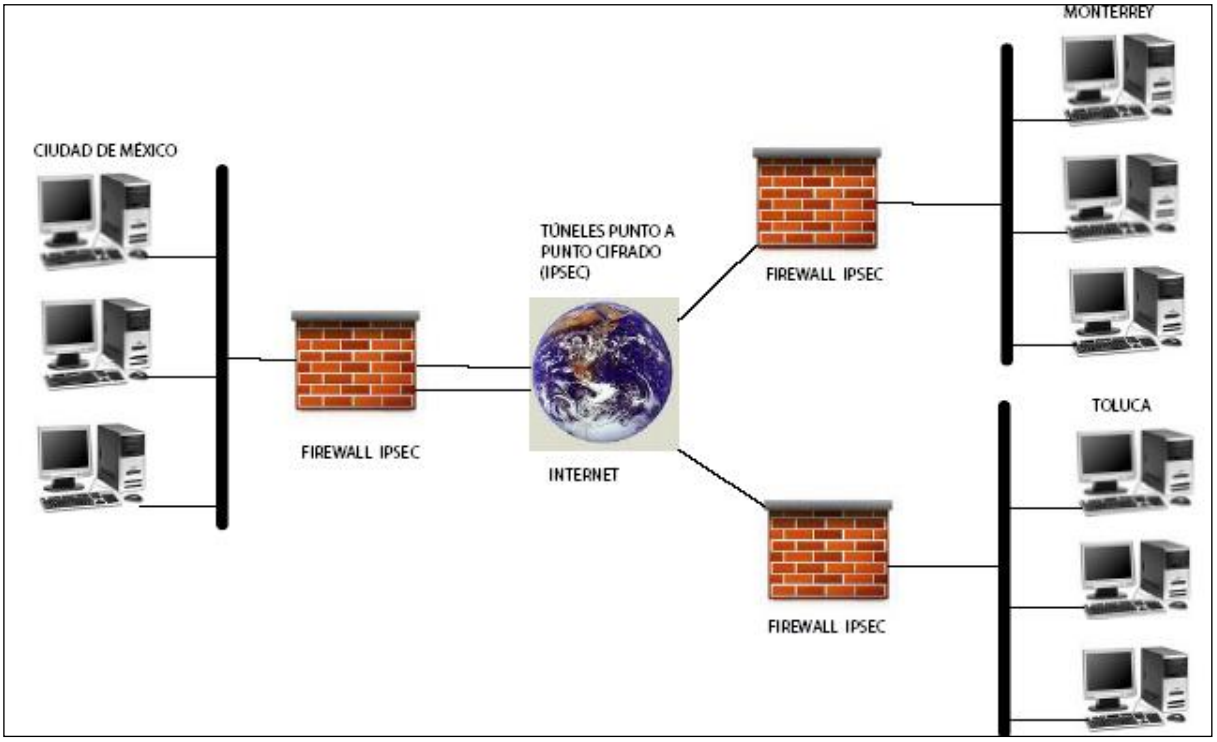
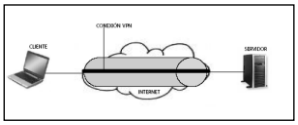


Figura 3.6 Una VPN de Extranet



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.

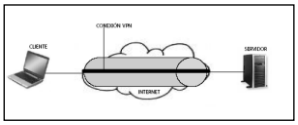
- **CALIDAD DE SERVICIO**: Uso de colas, manejo de congestión de red, prioridad de tráfico, clasificación de paquetes.

- **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

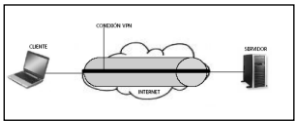
Dentro de los protocolos de implementación de las capas del modelo OSI se mencionan las cuatro principales: capa física, capa de datos, capa de red y capa de transporte. Dentro de estas capas se menciona la capa de datos por ser usada por el protocolo de túnel.

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.

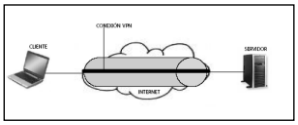
Los túneles voluntarios requieren que el cliente esté habilitado por una VPN, mientras que en los túneles obligatorios se utilizan cuando el cliente se conecta en un FEP (Procesador de Componente Frontal o Frente Externo del Procesador) habilitado por una VPN.

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.



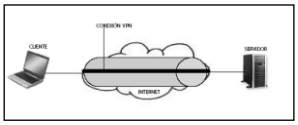
3.9.2 Interfaces del Túnel

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.

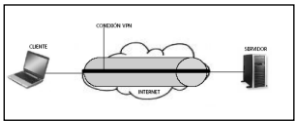
La interfaz de usuario está compuesta por diferentes elementos:

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.



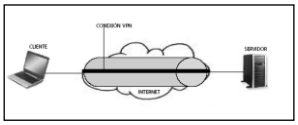
Los estándares utilizados en la implementación de VPN's, garantizan la privacidad e integridad de los datos y permiten la autenticación de los extremos de la comunicación, para no tener errores en una VPN dentro de una organización o institución educativa. Se deben tomar las medidas necesarias para implementar 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." [5]

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 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

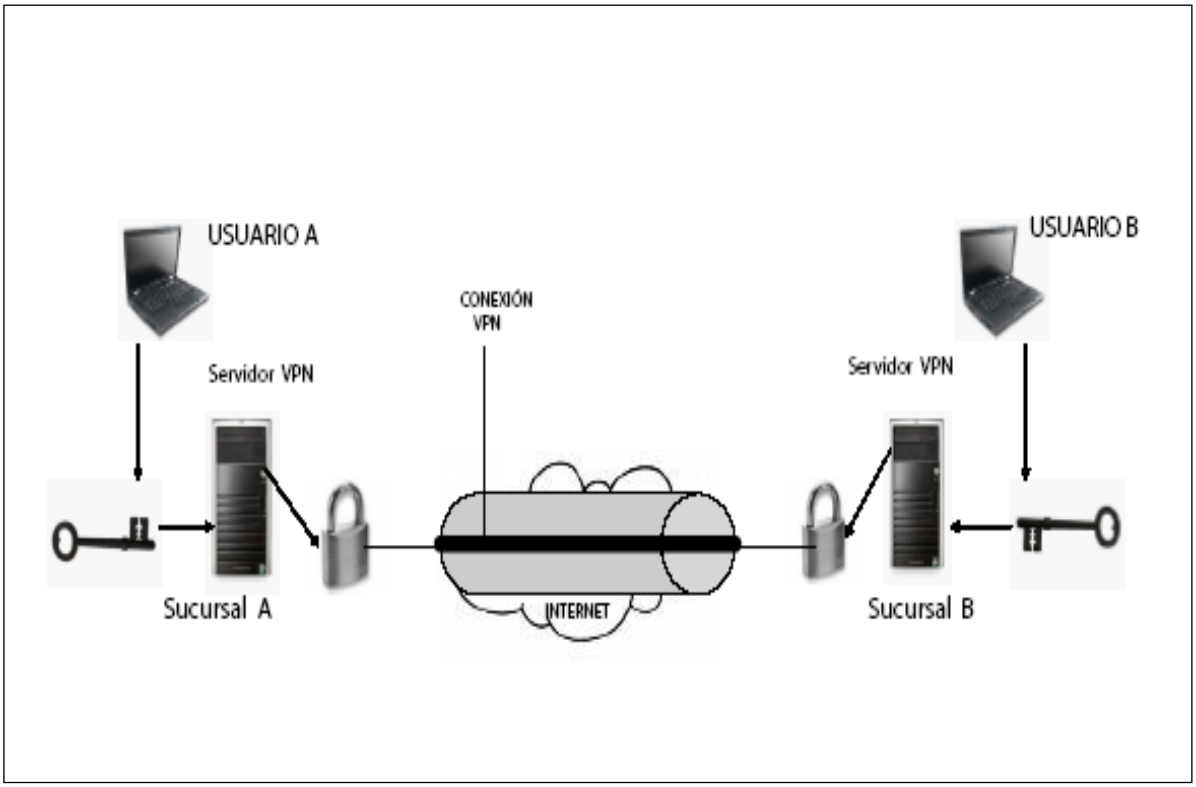
[5] Richard Bejtlich, Monitorización de Seguridad en Redes, Pearson, ED. 2, México,2005,p216



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.

CAPÍTULO 4



DISEÑO DE UNA VPN

Este capítulo aborda los elementos importantes que deben tomarse en cuenta para poder llevar a cabo el diseño de una VPN en el laboratorio de Redes y Seguridad.

4.1 Ubicación

El modelo VPN se va a implementar dentro de una de las dependencias de Ciudad Universitaria (UNAM), que está ubicada en la delegación Coyoacán en Universidad Nº. 3000 (Figura 4.1)

Figura 4.1 El mapa de Ciudad Universitaria (UNAM)

Para ser exactos el proyecto se desarrolla en el laboratorio de redes y seguridad ubicado en el primer piso del edificio de posgrado de ingeniería (edificio Bernardo Quintana Arrioja). (Figura 4.2)

Figura 4.2 Ubicación del Edificio; del Posgrado de Ingeniería

En el primer piso del edificio de posgrado también se encuentran los laboratorios de UNICA e IBM, como se muestra en la figura 4.3

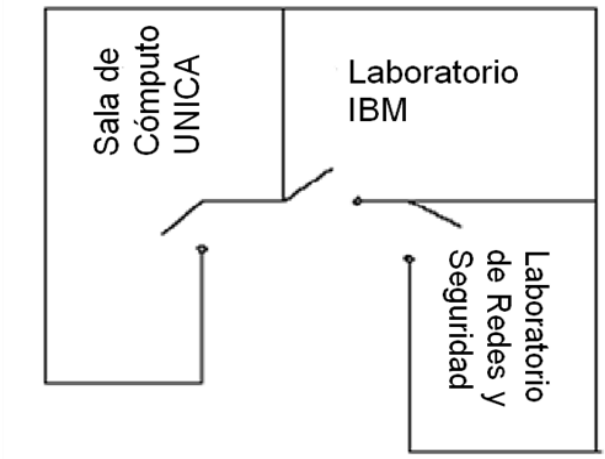


Figura 4.3 Ubicación del Laboratorio de Redes y Seguridad

El laboratorio de redes y seguridad cuenta con equipo de cómputo y de red, es indispensable mencionar que uno de ellos fungirá como servidor (Figuras 4.4, 4.5, 4.6)

Figura 4.4 Equipo de red

Figura 4.4 Servidor

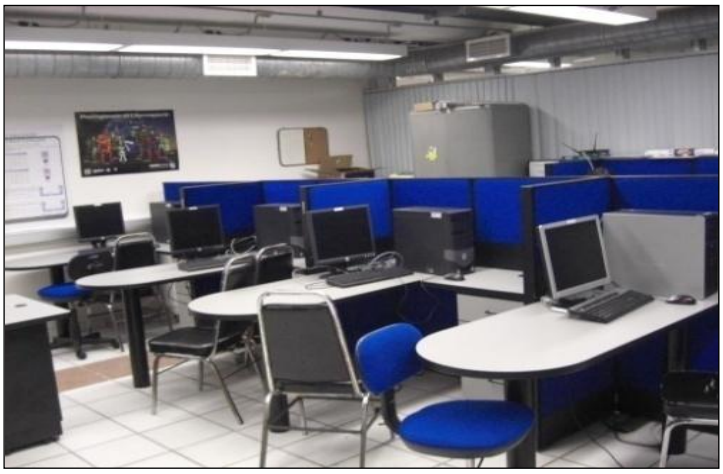


Figura 4.4 Equipo de cómputo

4.2 Metodología

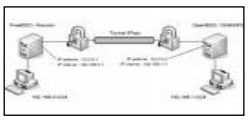
El siguiente paso para el diseño de una VPN, es la selección de la metodología. Es indispensable considerar que las metodologías se pueden clasificar en dos tipos:

a) Modelos de control de acceso.
b) Modelos de integridad.

Estos modelos indican de manera particular, la forma en la que se implementa la configuración de los equipos de cómputo.

Los modelos de control de acceso se encargan de proporcionar la autorización de acceso a los recursos que se manipulan en los servidores o aplicaciones; se clasifican de la siguiente manera:

a) Modelo de la matriz de acceso: Este modelo expresa varias políticas de protección y control de acceso, entre la más sobresaliente se encuentra el control de acceso directo (DAC), refiriéndose a que la matriz de acceso es cambiada de manera discreta por la persona que tiene la autorización para



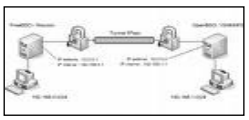
hacerlo. El modelo de la matriz de acceso se encarga de especificar quién eres y qué tienes permitido hacer.

b) Modelo Harrison Ruzo Ullman(HRU): Define un sistema de protección mediante un conjunto de derechos genéricos y un conjunto de comandos que cuenta con una parte principal y una condicional. En la parte condicional se verifica si los derechos de la matriz de acceso son correctos, si la prueba es exitosa, la parte principal realizará operaciones de cambio en la configuración de protección.
c) Modelo Bell - LaPadula: Modelo creado por D.E. Bell y L.J. Lapadula en 1976 y sirvió para resolver vulnerabilidades del control de acceso directo (DAC). El Modelo Bell-Lapadula recurre a un modelo mandatario de control de acceso (MAC), éste se encarga de restringir lo que puede hacer un usuario. Además de contar con una política multinivel que consiste en 4 niveles, no clasificado, confidencial, secreto y ultrasecreto.

Cada modelo tiene sus propios parámetros que se caracterizan por su originalidad, es decir, cada uno trata de manera diferente la forma de proteger los equipos de cómputo y quienes tiene el permiso de manipular la información, aunque el modelo que tiene política multinivel no es tan preciso.

Los modelos de integridad se identifican por ser los más estrictos y tienen como función evitar que existan modificaciones sobre la información que se maneja en una organización tanto pública como privada.

La principal característica de los modelos se identifica por los avances históricos que indican la evolución de las metodologías, las cuales fueron desarrolladas para mejorar las políticas de seguridad en cómputo.



a) Modelo Biba: Indica las políticas de integridad, esto para evitar robo de información que existe en los sistemas de cómputo de una organización.
b) Modelo Clark-Wilson: Un modelo que demostró que la integridad de los datos comerciales es más importante que la confidencialidad y se enfocaban en dos controles que son las transacciones bien formadas y la separación de las obligaciones.

4.2.1 Selección del modelo

Se seleccionó el modelo HRU para el diseño de la VPN debido a que es de gran utilidad para definir los mecanismos de seguridad y el control de la configuración en la matriz de acceso para los usuarios que van a estar asignados en el servidor VPN.

Michael Harrison, Walter Ruzzo y Jeffrey Ullman propusieron un modelo en 1976, que es popularmente referenciado como el modelo HRU, esta propuesta trató de mejorar el modelo de la matriz de acceso que es un modelo débil respecto a la seguridad. La definición formal del modelo es la siguiente: "**Se analiza el problema de filtración de acceso en la matriz de control de acceso (ACM) y garantía de confidencialidad."**[6] En otras palabras, este modelo solo se preocupa por la protección informática.

En la figura 4.7 se puede ver el funcionamiento del modelo HRU

[6]. Tomas and Michael A. " Protection in Operating Systems", Communications of the ACM, Vol. 19, No. 8, pag. 461-471, 1977.

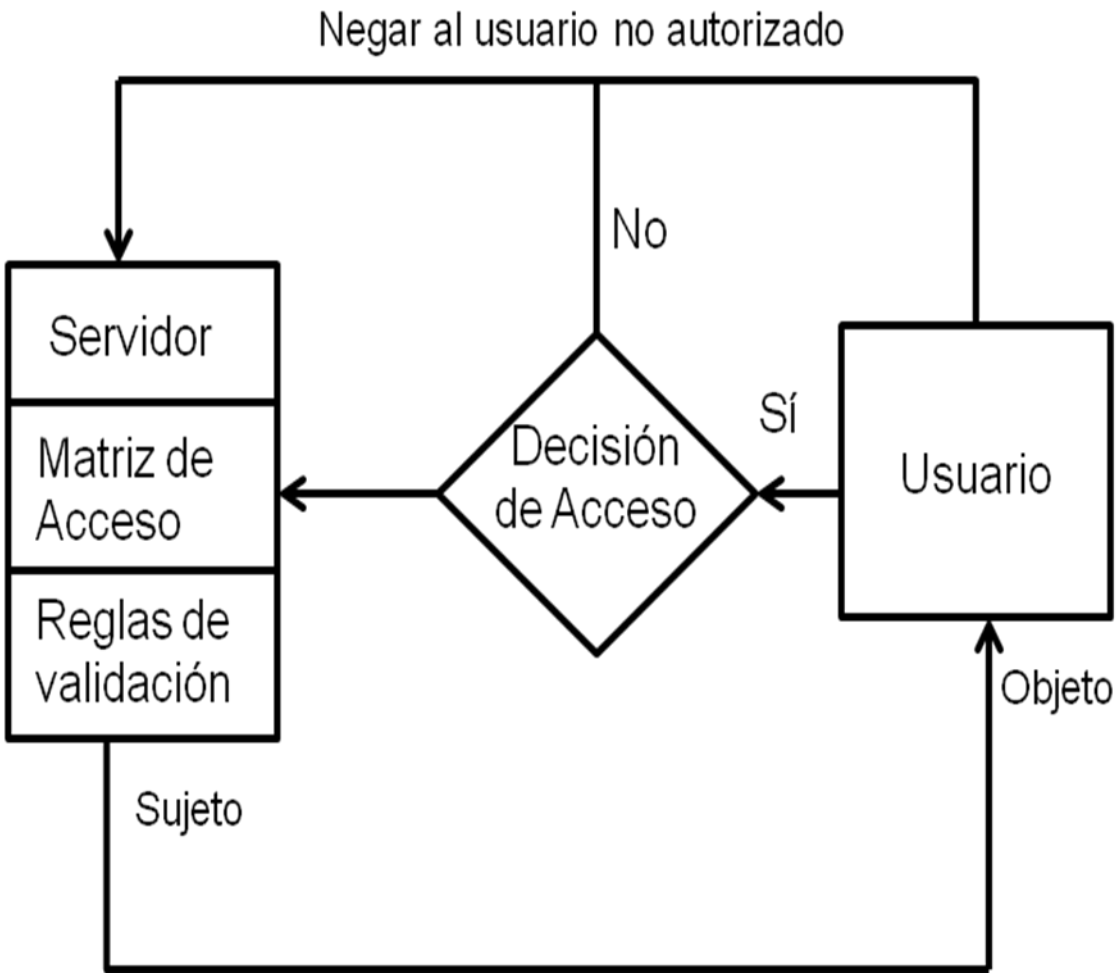
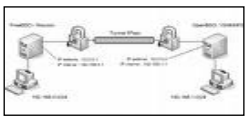


Figura 4.7 Modelo HRU

A continuación se explica detalladamente en qué consiste la figura:

- Reglas de validación: especifica cómo la decisión de acceso decide el destino de la petición, es decir, se tienen los parámetros de configuración para que el usuario tenga acceso al servidor o en caso contrario se le niegue la autorización para entrar al servidor.
- Matriz de acceso: Modelo que se está ejecutando con ciertas restricciones.
- Usuario: se encargará de hacer una petición en la cual la decisión de acceso tendrá la opción a cargo.



- Servidor. Dependiendo de la respuesta de la decisión de acceso se permitirán o se negarán los derechos de acceso a la información.

El modelo HRU es sencillo de implementar en una organización, en cuanto a controles de acceso y confidencialidad.

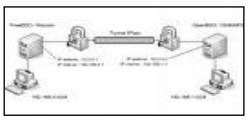
4.3 Selección del hardware

El equipo necesario que se requiere para poder llevar a cabo el diseño de la VPN es el siguiente:

a) Equipo de cómputo

Los requerimientos mínimos que necesita la computadora para que se pueda implementar el modelo VPN, es que cuente con:

- Una memoria RAM de 512 MB.
- Un procesador con una frecuencia de 266 MHz
- Una tarjeta de red Ethernet
- Un disco duro de 250 GB.



Para un servidor, las características son las siguientes:

- Procesador Dual-Core AMD Opteron 2220 (2,8 GHz, 1 MB L2 de caché, 1 GHz HyperTransport).
- Chipset Dual Intel® 5520
- Memoria máxima hasta 192 GB DDR3 1333 MHz ECC
- SATA (de 7.200 rpm) 160 GB
- Ranuras: 1 PCI, 1 PCI Express Gen1 (x8 mecánicamente, x4 eléctricamente).

b) Cable cruzado

El cable cruzado se utiliza para conectar dos computadoras directamente o bien conectar equipos activos entre sí, como hub con hub, switch con switch o router con router, etcétera.

Se le llama cable cruzado a aquel que cuenta con una configuración de los extremos diferente, se le da el nombre porque cruza las terminales de transmisión de un lado para que llegue al otro extremo de recepción, y la recepción del origen a la transmisión del final.

El cable cruzado, utiliza cable par trenzado "UTP" con conectores RJ45 (macho). El cable cruzado usa la misma instalación tanto para velocidad Base T, como para velocidad 100 Base TX.

El cable cruzado puede ser usado indistintamente ya que con la configuración de la salida de red “A” o “B” funciona perfectamente.

En la figura 4.8 se observa la forma de configuración de colores del cable cruzado.

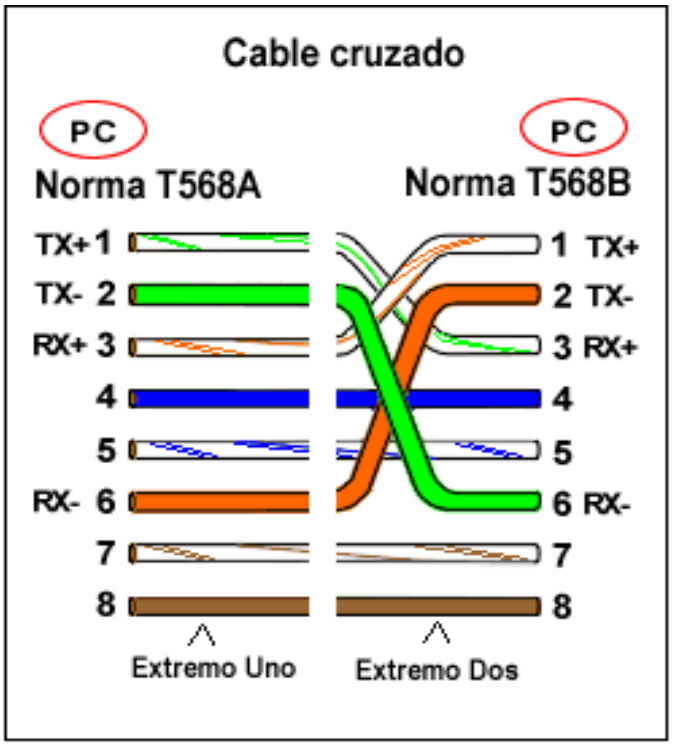


Figura 4.8 Configuración de colores de un cable cruzado

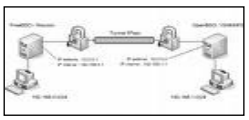
4.4 Sistema Operativo

El sistema operativo es la parte más importante de la computadora, ya que como se sabe, actúa como interfaz entre los dispositivos de hardware y el software que utiliza el equipo de cómputo.

Las tareas más importantes que realiza el sistema operativo son:

- Compartir recursos entre los mismos usuarios.
- Facilitar el acceso a los recursos de entrada y salida.
- Recuperarse de errores o fallas que se puedan presentar.
- Llevar el control de uso de los recursos.
-

Existen diferentes tipos de sistemas operativos, entre los que son más mencionados se encuentra el Dos, Windows, GNU/Linux y Mac.



El sistema operativo puede clasificarse de 4 formas:

a) Multiusuario. El sistema permite que 2 o más usuarios puedan utilizar al mismo tiempo sus programas.
b) Multiprocesador. En esta categoría se puede abrir el mismo programa en más de un procesador.
c) Multitarea. Se ejecutan varios programas al mismo tiempo sin ningún problema.
d) Tiempo Real. Responden a cualquier petición al mismo tiempo.

El sistema operativo puede ser presentado en forma gráfica o en modo consola, la interfaz gráfica del usuario, mejor conocida como GUI, le permite al usuario enviar comandos a la computadora al hacer clic en iconos o al seleccionar elementos en los menús que se encuentren en el sistema. Un ejemplo de la interfaz gráfica es Windows 7. En modo de consola o por caracteres se tiene MS-DOS.

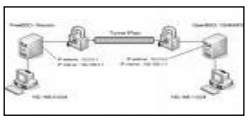
Algunos ejemplos de sistemas operativos son:

1. Familia Windows

- Windows 95
- Windows 98
- Windows ME
- Windows NT
- Windows 2000
- Windows 2000 server
- Windows XP
- Windows Server 2003
- Windows CE
- Windows Mobile
- Windows XP 64 bits
- Windows Vista (Longhorn)
- Windows 7

2. Familia Macintosh

- Mac OS 7



- Mac OS 8
- Mac OS 9
- Mac OS X

3. Familia UNIX

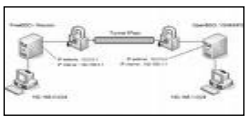
- AIX
- AMIX
- GNU / Hurd
- HP-UX
- Irix
- Minix
- System V
- Solaris
- UnixWare

4. Familia GNU/Linux

- Debian
- Suse
- Mandrake / Mandriva
- Fedora
- Ubuntu
- Gentoo

Existen algunas diferencias entre Linux y Unix, ya que aunque sean bastante semejantes, cada uno está hecho para un propósito diferente, en el caso de Unix es un sistema que en la mayoría de sus distribuciones no es gratuita, es decir, habría que pagar la licencia para obtener dicho software caso contrario con Linux, ya que la mayoría de las distribuciones son gratuitas y además su código fuente puede ser proporcionado con el fin de que cualquier desarrollador pueda hacerle mejoras al sistema y que sean beneficiados varios usuarios con dichos avances .

Otra de las diferencias es que Unix fue desarrollado principalmente para el uso de la red, además de existir primero y por esa razón es que el código fuente de Linux está basado en el sistema Unix.



Linux es más utilizado en las universidades y en las compañías por la funcionalidad de trabajo que existe en este sistema

4.4.1 Selección del Sistema Operativo

Para este proyecto se seleccionó el sistema operativo Debian, ya que es de libre uso y cuenta con un conjunto de programas básicos y utilidades que permiten el buen desempeño de la computadora.

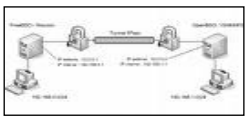
El sistema operativo está formado por una organización voluntaria con documentos fundadores.

- El contrato social de Debian. Que está encargado de definir las bases del proyecto y tratar los detalles del desarrollo.
- Las directrices de software libre de Debian. Se definen cuáles serán los criterios del software libre, además de analizar el software que será instalado en la distribución.
- La constitución de Debian. En este documento se describe la estructura de la organización para la toma de decisiones de manera formal dentro del proyecto.

El proyecto Debian está cargo de más de mil desarrolladores. Cada uno con sus respectivas funciones de las cuales se puede mencionar: mantenimiento, documentación control de calidad, traducciones, etcétera.

El proyecto Debian fue creado por Ian Murdock en el año 1993, dentro de los puntos importantes que se destaca en este sistema era la distribución de manera abierta y que tuviera coherencia con Linux y GNU.

El apelativo se basa en la combinación del nombre de su entonces novia Deborah con su propio nombre Ian, formando *Debian*.



Debian es un sistema operativo que soporta arquitecturas de hardware: x86 y x86-64, cuenta con una interfaz gráfica amigable con el objetivo de que el usuario no se le haga difícil su uso.

El sistema operativo no cuenta con un firewall predeterminado debido a que no hay algún tipo de servicio que puede afectar la seguridad puesto que entre sus funciones cuenta con la no activación de procesos latentes al momento de la instalación.

Entre las especificaciones mínimas que se deben tener para poder contar con este sistema operativo son los siguientes:

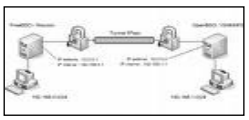
Un procesador: 700 MHz x86, una memoria RAM de 384 MB, un Disco Duro de 8GB, una tarjeta gráfica que soporte una gran resolución, un lector de CD-ROM, tarjeta de sonido y conexión a internet.

4.5 Dirección IP

Existen dos tipos de direccionamiento de IP que son: IP Estática y dinámica, todo esto depende del proveedor de los servicios de internet (ISP).

El direccionamiento IP estático indica que se cuenta una sola dirección IP, se deben configurar los parámetros de red de manera manual permitiendo que se identifique de manera diferente a otra dirección IP, evitado así que se tengan repeticiones de la dirección en los diferentes equipos de cómputo dentro del mismo grupo de trabajo.

Las direcciones IP estáticas son utilizadas para los servidores de tipo: correo, web, base de datos, etcétera, se debe considerar algunos aspectos importantes de cómo configurar la dirección IP estática a estos servicios que proporcionan seguridad, estos aspectos serán útiles para poder filtrar cualquier problema de tráfico de red o envío de spams.



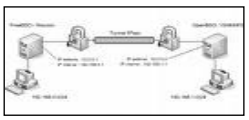
El direccionamiento IP dinámico se aplica en equipos de cómputo que cuenten con un proveedor de servicios de internet como por ejemplo infinitum, axtel, etcétera. Este tipo de servicios consiste en que al momento de conectarse a internet se le asigna una IP de manera automática, esto para indicar la dirección hacia los demás equipos que estén conectados y así evitar algún problema de duplicidad de IP's, para este tipo de direccionamientos ya no es necesario configurar de manera manual los parámetros de red.

También se debe considerar que los proveedores de servicios de internet venden el servicio de direccionamiento dinámico para que el usuario no tenga problemas de configuración al querer acceder a internet.

Una IP pública se utiliza generalmente para montar servidores de tipo internet, correo, base de datos, por consiguiente, es importante saber que las direcciones IP públicas tienen un costo adicional para que estos servicios que se requieren en instituciones educativas, empresas públicas y privadas, puedan funcionar.

A continuación se mencionan las características de la IP pública estática y la IP pública dinámica.

a) Una dirección IP pública estática no cambia y se utiliza principalmente para alojar páginas web o servicios en Internet.
b) Una dirección IP pública dinámica se elige de un conjunto de direcciones disponibles y cambia cada vez que uno se conecta a internet.



4.5.1 Selección de direcciones IP

Para este proyecto se asignaran las direcciones IP estáticas, esto con el fin de realizar la validación de la conexión remota mediante su propia clave privada o pública.

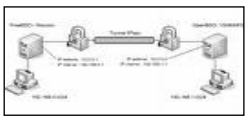
Para la toma de esta decisión, es necesario tener un control de acceso a los usuarios que tenga permisos de conexión remota a un servidor VPN, y así evitaremos problemas que otro usuario se conecta al mismo grupo de red virtual.

Se pueden ocupar ambas direcciones, tanto públicas como privadas, y para poder tener acceso a la conexión remota, se tiene que seleccionar el rango de IPs, o bien, una subred que abarque el número de servicios que tiene la conexión remota que se aplicará en el laboratorio de redes y seguridad.

4.6 Software VPN

Hay una gran variedad de software VPN que tiene la estructura de tipo cliente – servidor y tipo cliente, a continuación se mencionan algunas herramientas de VPN's que son:

- VPN WinGat
- Kerio VPN Client
- VPN Mobile
- IPsec VPN Client
- LogMeln Tamachi
- Security Kiss
- OpenVPN



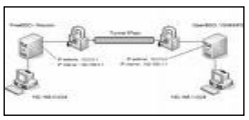
Estas herramientas se pueden instalar en diferentes plataformas de los sistemas operativos, debe tomarse en cuenta que cada herramienta tiene un proceso distinto para la instalación y la configuración, esto se debe a la diferencia de la arquitectura con la que cuenta cada sistema operativo en el equipo de cómputo.

4.6.1 Selección del software VPN

En este proyecto se seleccionó el software OpenVPN que es una herramienta completa de código abierto que se adapta a una amplia gama de configuraciones, incluyendo el acceso remoto, VPN sitio a sitio, la seguridad wifi y las soluciones de control remoto a escala empresarial. Una de las razones por la cual se utiliza OpenVPN es por las limitaciones que se encuentran en la herramienta IPSec que son:

- 1) Problemas de modificación al kernel.
- 2) Se implementan en los equipos de hardware
- 3) Su configuración es muy compleja
- 4) Conflicto con las direcciones IP dinámicas y estáticas.
- 5) Se requiere de muchos puertos y protocolos en el firewall
- 6) Problemas con la incompatibilidad en algunas aplicaciones VPN's.

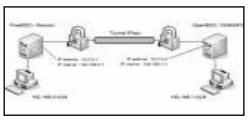
El protocolo SSL/TLS tiene un papel muy importante y es parte fundamental de la implementación de OpenVPN para mejorar los procesos de seguridad en las redes remotas con tecnología aceptada en todas las dependencias públicas y privadas.



Las características que tiene el protocolo SSL/TLS son parte del software OpenSSL que vienen instaladas en cualquier sistema moderno e implementan mecanismos de cifrado y autenticación basadas en certificados. Los certificados generalmente son emitidos por entidades de reconocida confiabilidad aunque también las puede emitir uno mismo y usarse la propia VPN.

Las características clave de la herramienta OpenVPN son:

a) Se basa en el desarrollo del driver TUN, este driver se utiliza para la simulación de interfaces de red, así como su manipulación en el espacio de usuario. En otras palabras, es el encargado de levantar el túnel así como también la encapsulación de paquetes a través del enlace virtual.
b) Las comunicaciones del enlace VPN son únicamente a través del puerto TCP o UDP, lo que permite integrar routers y firewalls.
c) La versión OpenVPN 2.0 funciona bajo el modelo cliente – servidor, permitiendo así la conexión de varios usuarios al servidor central que atienda continuamente peticiones en un solo puerto.
d) OpenVPN ofrece una interfaz de gestión que se puede utilizar para controlar de forma remota o administrar de manera centralizada un demonio OpenVPN. La interfaz de administración también puede ser utilizada para desarrollar una interfaz gráfica de usuario o una aplicación basada en web para una OpenVPN.
e) OpenVPN utiliza una fortaleza de la seguridad en modelos industriales diseñada para proteger contra los ataques pasivos y activos.
f) Proporciona la administración remota de la aplicación por medio de un socket que permanece establecido por la máquina.
g) La gran flexibilidad que tiene para ser utilizado junto con un lenguaje interpretado. Existen numerosos formatos de scripts, como bash, perl, ruby, etcétera que pueden ser utilizados para una gran variedad de propósitos.
h) El controlador TUN/TAP junto con la biblioteca OpenSSL son fundamentales para el funcionamiento de OpenVPN.



i) El controlador TUN emula un dispositivo que va de punto a punto mientras que el controlador TAP simula la interfaz de la red.

4.7 Protocolos VPN

Los protocolos VPN'S tienen una gran variedad de características de configuración e instalación, por eso es importante saber qué tipo de protocolos permite una mejor tecnología y seguridad en el software o hardware al momento de implementarse en el equipo de cómputo.

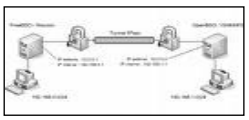
Los protocolos más conocidos son: IPSec, PPTP, SSL/TLS, L2TP, etcétera, estos protocolos indican los principales avances que han tenido las VPN's en el mercado tecnológico. Estos protocolos generan un túnel con la interfaz TUN, que generan el cifrado de datos para proteger la información de los usuarios que se conectan a distintos equipos de cómputo.

Cada protocolo tiene su propio proceso de instalación y configuración que depende también de los equipos de cómputo y del sistema operativo. Esto se basa en una arquitectura de soporte y las mejoras del desarrollo que tenga el kernel para los distintos sistemas operativos.

4.7.1 Selección del protocolo VPN

Se seleccionó el protocolo SSL/TLS que hoy en día es considerado como uno de los protocolos más fuertes y seguros, permitiendo tener una mejor seguridad en las redes remotas y el proceso de autenticación de los usuarios que estén registrados en el servidor VPN.

El protocolo SSL/TLS permite la autenticación mutua entre un cliente y el servidor; este protocolo está por encima de TCP/IP y por debajo de HTTP, LDAP, IMAP y otros protocolos de nivel de red. Este protocolo es origen de



Netscape que fue desarrollado para los navegadores web para proporcionar conexiones seguras y las transferencias de números de tarjetas bancarias.

4.8 Estructura de cliente – servidor

La estructura de este servidor VPN, está pensado para una red LAN y usuarios remotos, el principal cuestionamiento de este diseño, es como configurar el servidor VPN y los usuarios que pueden conectarse a los distintos sistemas operativos.

Esta estructura está pensada para tener acceso al servidor VPN, en forma remota y dentro de un laboratorio de cómputo o en una sala de conferencias.

A continuación se muestra una estructura de cómo está configurado el servidor y el usuario, para acceder al servidor de la escuela, empresa, corporativo, negocio, etcétera; esta estructura consiste en que el usuario tendrá que estar primero registrado en el servidor VPN, contar con una contraseña, una IP privada o pública, un método de cifrado que se va a utilizar para poder cifrar los datos en forma segura y tener una eficiencia de seguridad entre el usuario y el servidor; y una conexión segura ante todo tipo de amenazas y vulnerabilidades que existe en el Internet. Se muestra en la figura 4.9 la estructura de cliente - servidor.

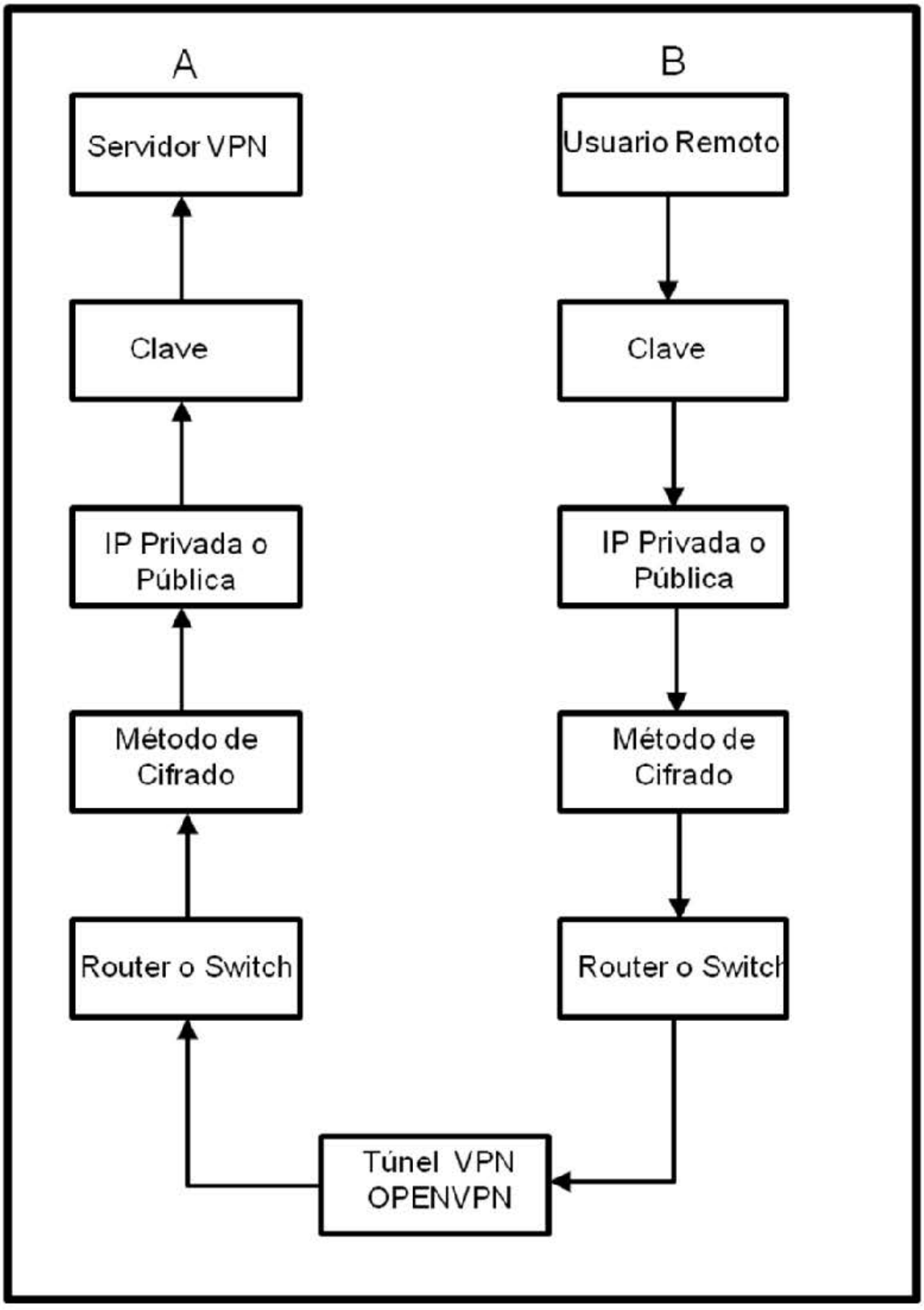
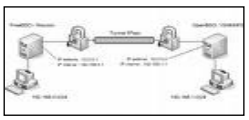


Figura 4.9 Estructura de una VPN de Cliente - Servidor



El planteamiento de esta estructura, consiste en configurar la interfaz del servidor VPN, con una dirección IP que tiene la interfaz eth0, esto indica que es una red insegura y la interfaz eth1, es la subred que se debe configurar desde el servidor VPN. Y también se establece una dirección IP Virtual que tendrá de interfaz a la TUN.

Ya que se configuró la interfaz que va a estar en comunicación con los usuarios remotos hacia el servidor VPN se tienen que configurar los parámetros que debe tener el servidor VPN y los usuarios remotos, en sus distintas versiones de los sistemas operativos.

En este modelo podemos ver que necesitamos algunos parámetros que se tiene que utilizar para llevar a cabo el desarrollo del proyecto de tesis, en la construcción del servidor VPN y los usuarios se tiene que tomar en cuenta el lugar en donde se implementara el servidor VPN, el tipo de red que existe y las propiedades de la IP. Conocer las características del equipo de red que se está utilizando en el Laboratorio.

También se puede observar en este modelo, que se aplicará la configuración para ambos sistemas operativos que son: Linux y Windows; para el servidor se utilizará Linux y los usuarios remotos pueden utilizar Windows y Linux. Se muestra en la siguiente figura 4.9, el modelo cliente - servidor.

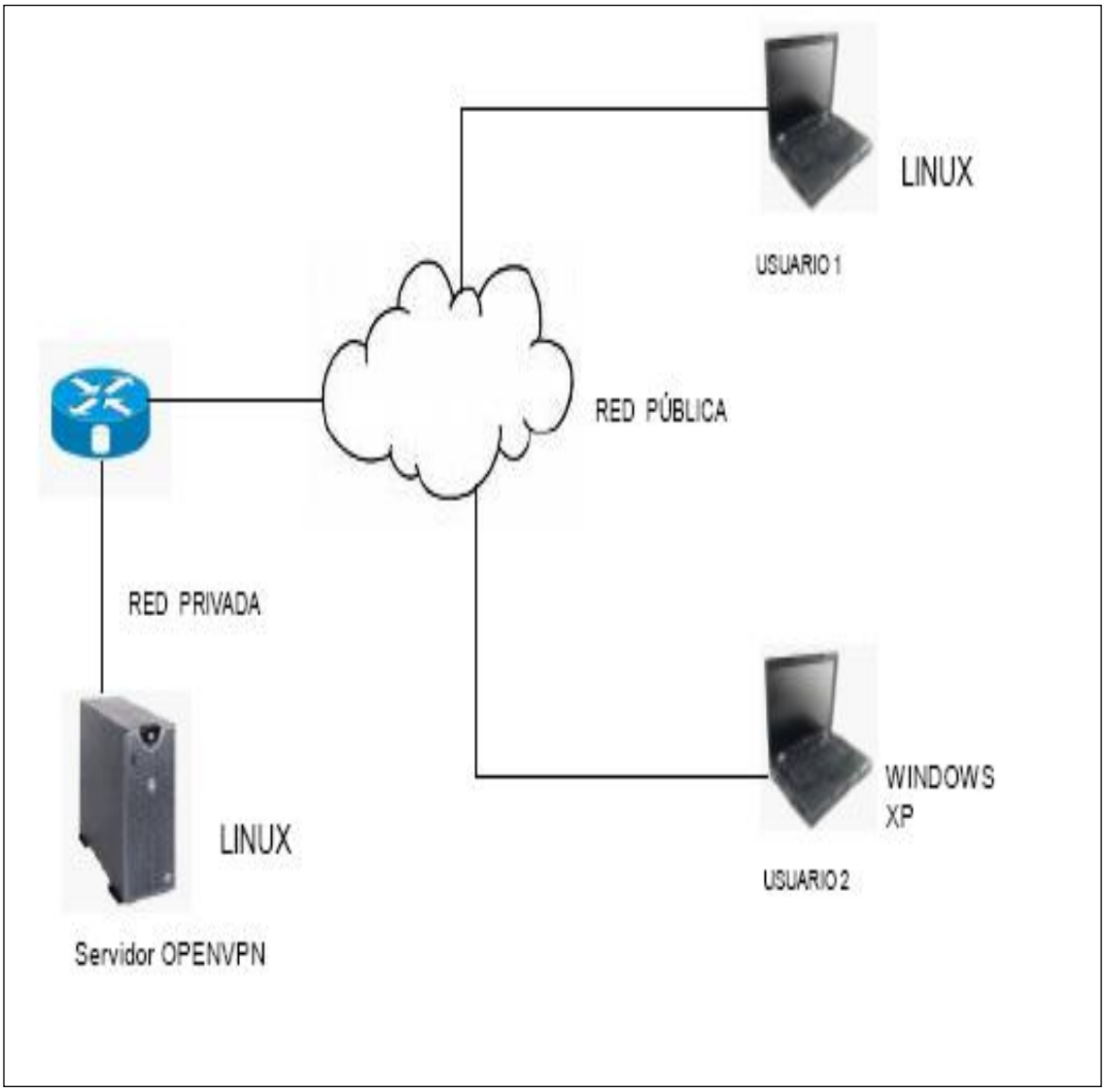
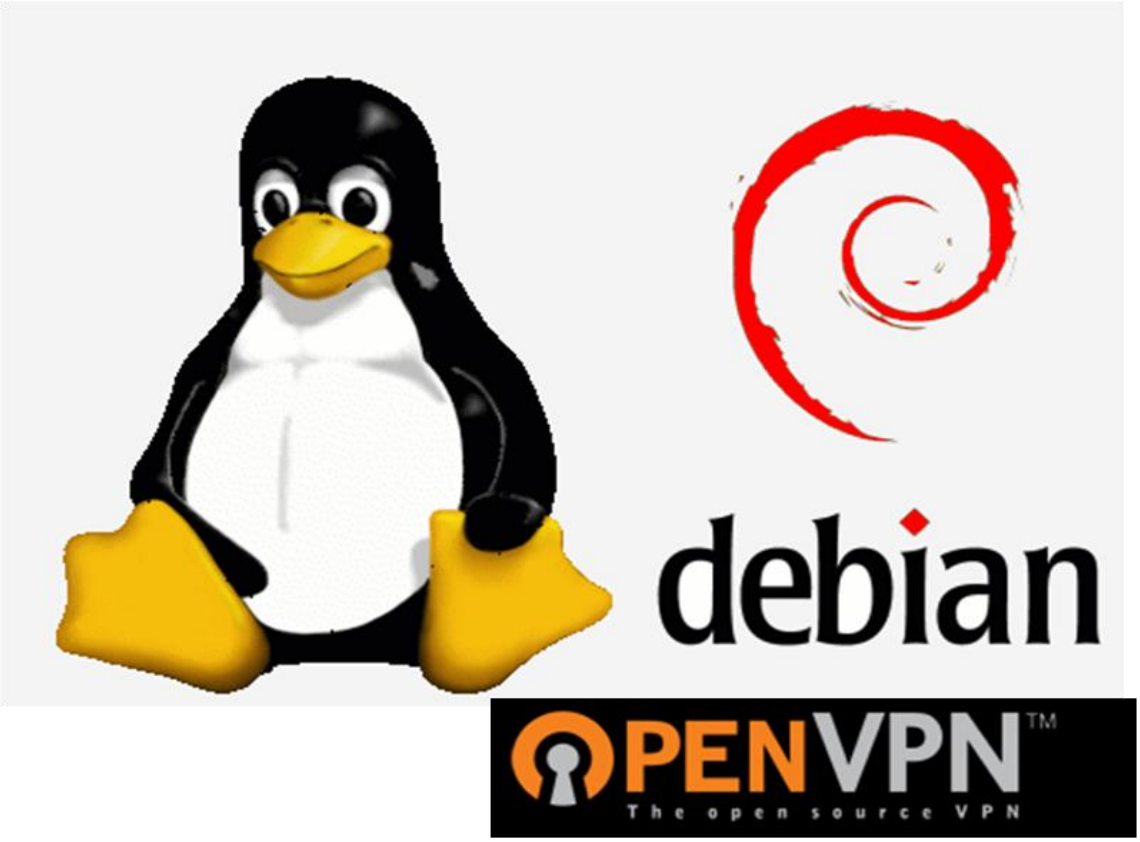


Figura 4.9 El modelo Cliente - Servidor

CAPÍTULO 5



IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

Nota: * Los datos mostrados en este capítulo fueron cambiados por motivos de seguridad

5.1 Instalación y configuración de la distribución de Debian

Antes de iniciar la instalación del Sistema Operativo se deben identificar los criterios de instalación, como se mencionó en el capítulo anterior, es necesario saber con qué requerimientos cuenta nuestro equipo para poder instalar el Sistema Operativo que sea de nuestro interés, que en este caso es la distribución Debian.

En este trabajo de tesis se escogió la distribución del sistema operativo Debian por ser uno de los Sistemas Operativos más estables y maduros ***"Debian sobrepasa a todas las otras distribuciones en lo bien integrados que están sus paquetes. Como todo el software lo empaqueta un grupo coherente, no sólo puede encontrar todos los paquetes en un mismo sitio sino que puede estar seguro de que se han eliminado todos los problemas al respecto de complejas dependencias. Aunque se cree que el formato deb tiene algunas ventajas sobre el rpm, es la integración entre paquetes lo que hace a Debian más robusto."***[7] *E*s por esto que en el laboratorio de redes y seguridad los equipos cuentan con dicho sistema instalado.

El Sistema Operativo Debian puede instalarse de tres maneras que son: por medio de imágenes del DVD, por medio del CDROM en modo consola y la tercera mediante la descarga del ISO por medio de la conexión a internet.

En este proyecto se eligió la instalación mediante un CDROM que permitió realizar la instalación básica del Sistema Operativo Debian y después de su instalación, mediante una conexión a internet se configuró el gestor de arranque para actualizar los archivos desde la página web de Debian.

[7] http://debianlinux.blogcindario.com/2007/09/00005-ventajas-de-debian.html, http://www.debian.org/index.es.html

El proceso de instalación en el modo gráfico es el siguiente:

1) Una vez insertado el disco de instalación lo primero que se configura es el idioma, para facilitar las instrucciones en el proceso de instalación se eligió el idioma español. (Figura 5.1)

Figura 5.1 Elección del idioma en la instalación

2) El siguiente paso es seleccionar el país de origen para poder seguir con la instalación. (Figura 5.2)

Figura 5.2 Elección del país

Ahora se seleccionará el idioma de teclado, que para este caso se seleccionó Latinoamericano, es importante tener la configuración de teclado porque algunos caracteres del español son desconocidos en otro idioma del teclado. (Figura 5.3)

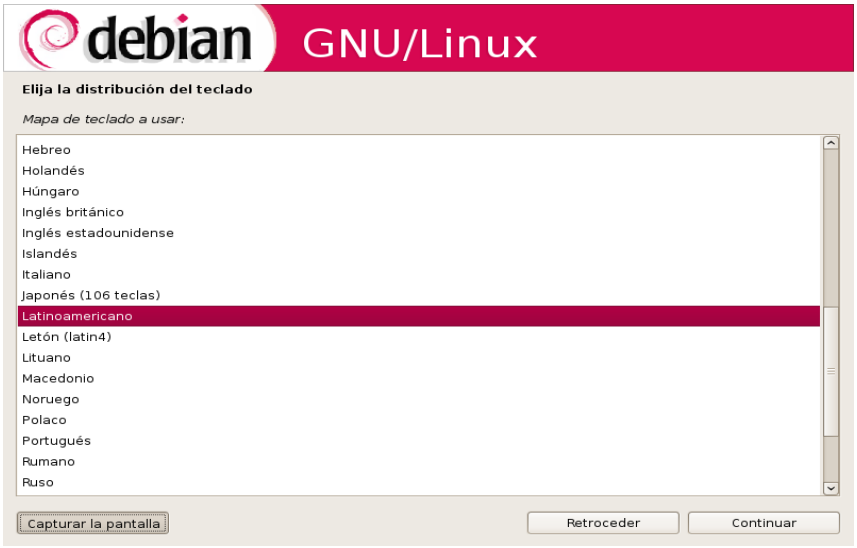


Figura 5.3 Selección del idioma del teclado

3) Es importante dejar bien definida la configuración de la red para poder instalar las actualizaciones del Sistema Operativo, así como las aplicaciones que requiera el sistema operativo. El usuario tendrá la libertad de elegir los programas que le sean de utilidad para fines laborales o empresariales según sea el caso.

Para seguir con la instalación se tiene que asignar el nombre del servidor o del equipo de cómputo, esto para poder establecer los parámetros del administrador (root) en este caso el servidor lleva el nombre de unamfi. (Figura 5.4)

Figura 5.4 Nombre del equipo

Ahora se tiene que configurar el nombre de dominio del servidor, esto va a permitir realizar la conexión a internet y obtener los permisos para descargar actualizaciones y configurar la dirección IP en forma estática. Como mención importante se debe tomar en cuenta, que si se tiene un equipo INFINITUM de Telmex, se asigna el nombre de dominio automáticamente, en este ejemplo el dominio es: gteway.2wire.net, el proveedor de servicios de internet proporcionará una IP de manera dinámica, por lo que ya no es necesario proporcionar una IP estática (Figura 5.5)

Figura 5.5 Asignación de nombre de dominio

El siguiente paso es dejar establecida la zona horaria en el Sistema Operativo Debian, es de suma importancia establecer estos parámetros para no tener problemas al recibir notificaciones de actualización de software. (Figura 5.6)

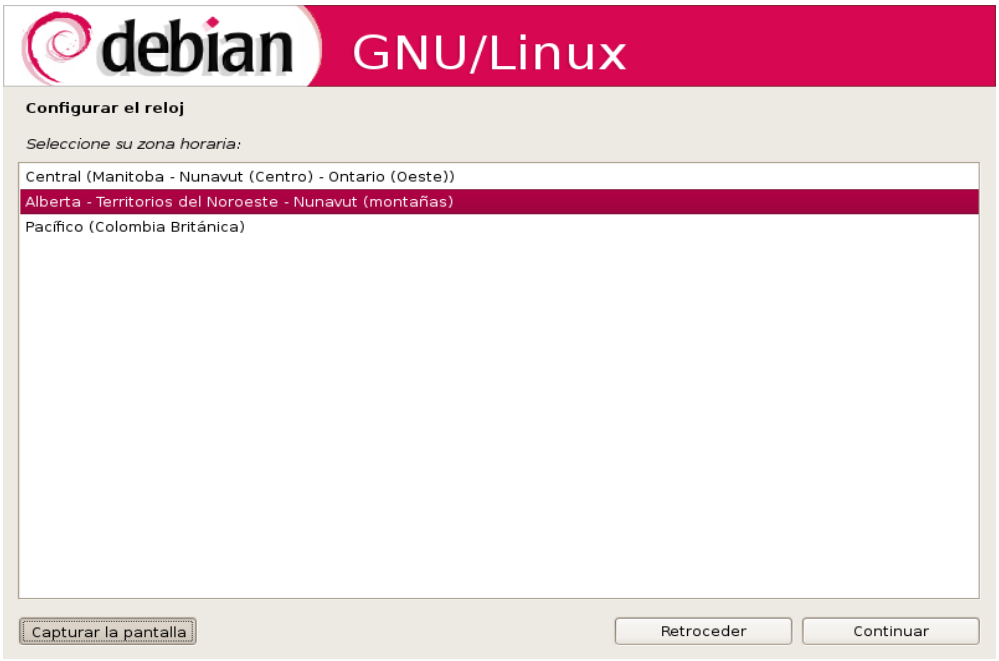


Figura 5.6 selección de zona horaria

4) En el siguiente apartado se muestran las particiones que tiene el disco duro que está instalado en el equipo, los parámetros se ven en una lista y se pueden observar de la siguiente manera:

   a) Particionar el disco duro.

   b) Utilizar todo el espacio del disco duro.

   c) Realizar las particiones avanzadas en el disco duro.

   Se puede identificar el tipo de disco duro, es decir, si es de tipo IDE o tipo Serial ATA, también se puede saber la marca del fabricante del disco duro y las unidades lógicas. (Figura 5.7)

Figura 5.7 Particionado de discos

En este caso se instalará el Sistema Operativo en todo el disco duro sin hacer ninguna partición. (Figura 5.8)

Figura 5.8 Instalación del Sistema Operativo en el Disco duro

Para continuar con el proceso de instalación se pregunta cuál es el proceso de particionado del disco duro, la forma de presentarlo se observa en la Figura 5.9

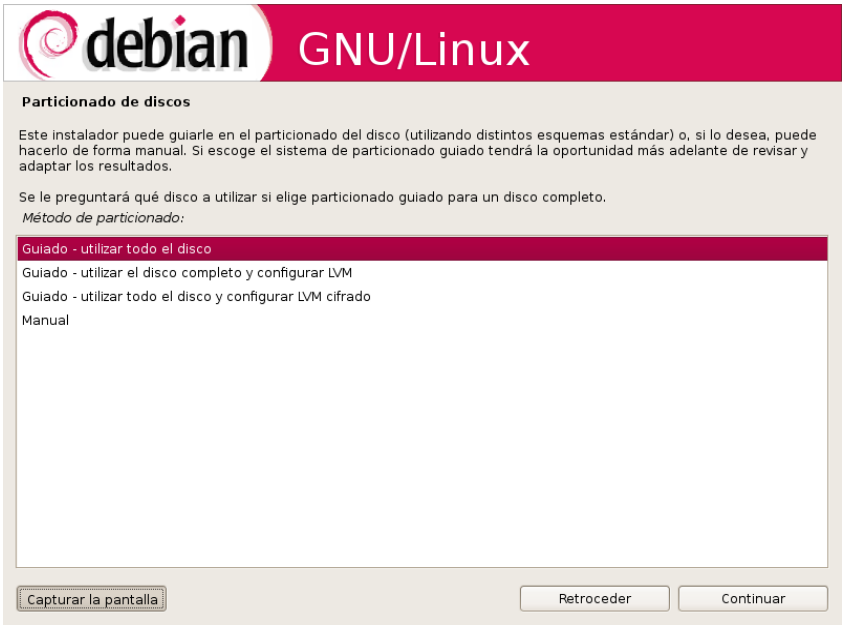


Figura 5.9 Particionado guiado del proceso de instalación

Ahora se tiene que insertar el nombre de superusuario (root) y la contraseña, en el momento en el que se inserte la contraseña para el superusuario se tiene que verificar que la contraseña sea alfanúmerica y no menor a 8 caracteres. (Figura 5.10)

Figura 5.10 Ingreso de la clave de superusuario

Una vez configurada la contraseña de superusuario, se tiene que crear una cuenta de usuario normal, es decir, aquel que no tenga derechos de administrador de la cuenta, en este ejemplo se creó al usuario con el nombre redunam. (Figura 5.11)

Figura 5.11 Creación de cuenta de usuario

5) Ahora se tiene que configurar la contraseña del usuario que va estar registrado en el sistema operativo, para que tenga permisos para entrar a ciertas aplicaciones que requiera el usuario en particular. (Figura 5.12)

Figura 5.12 Contraseña de la cuenta creada

6) En el siguiente paso se tiene que configurar el gestor de paquetes, ubicado en las direcciones de los Dominios que están registrados en México; los dos que se encuentran en el país son: ftp.mx.debian.org y mmc.geofisica.unam.mx, estas direcciones de Dominios permiten actualizar la paquetería de Debian y las herramientas que serán de utilidad para la aplicación a desarrollar. (Figura 5.13)

Figura 5.13 Configuración del gestor de paquetes

7) Una vez seleccionada la dirección del Dominio, se mostrará una lista de los programas que debe de instalar el usuario apegándose a las necesidades que se tengan (Figura 5.14)

Figura 5.14 Lista de programas a instalar

8) En la siguiente imagen se muestra la opción de instalar el servidor samba DHCP en el Sistema Operativo y así configurar los parámetros de IP, al permitir modificar el archivo smb.conf, la configuración WINS proveniente de DHCP se leerá desde /etc/samba/dhcp.conf. (Figura 5.15)

Figura 5.15 Instalación servidor Samba

9) Para configurar el servidor samba, se tendrá que indicar cuál será el grupo de trabajo que tendrá que aparecer cada que los clientes de red lo soliciten, en este trabajo se nombró al grupo de trabajo como redopenvpn. (Figura 5.16)

Figura 5.16 Instalación del paquete dhcp

10) Ya para terminar, se solicita la instalación del gestor de arranque, es importante mencionar que realizar el arranque del GRUB permitirá seleccionar el Sistema Operativo, mediante este proceso también se puede acceder al sistema cuando se tenga un conflicto al iniciar sesión o exista un cambio de contraseña del administrador o del usuario. (Figura 5.17)

Figura 5.17 Instalación del gestor de arranque

11) La última indicación que se muestra es el aviso de término de la instalación, después de este aviso es necesario reiniciar el Sistema Operativo. (Figura 5.18)

Figura 5.18 Instalación finalizada

5.2 Instalación de OPENVPN

La instalación del software OPENVPN permite la conexión por medio de un acceso remoto del cliente hacia el servidor VPN, de manera más detallada, la herramienta permite tener una conexión de una red local de manera segura y compartir los recursos de impresión, correo, archivos, etcétera.

La forma de instalar OPENVPN se hace mediante la ejecución de comandos en modo consola dentro del Sistema Operativo Debian, esto se explica a detalle de la siguiente manera:

1) Abriendo una terminal del Sistema Operativo, se ejecuta el comando apt-get install openvpn, en forma directa se instalan todos los directorios. En la figura 5.19 se muestra el comando de la instalación de OPENVPN.

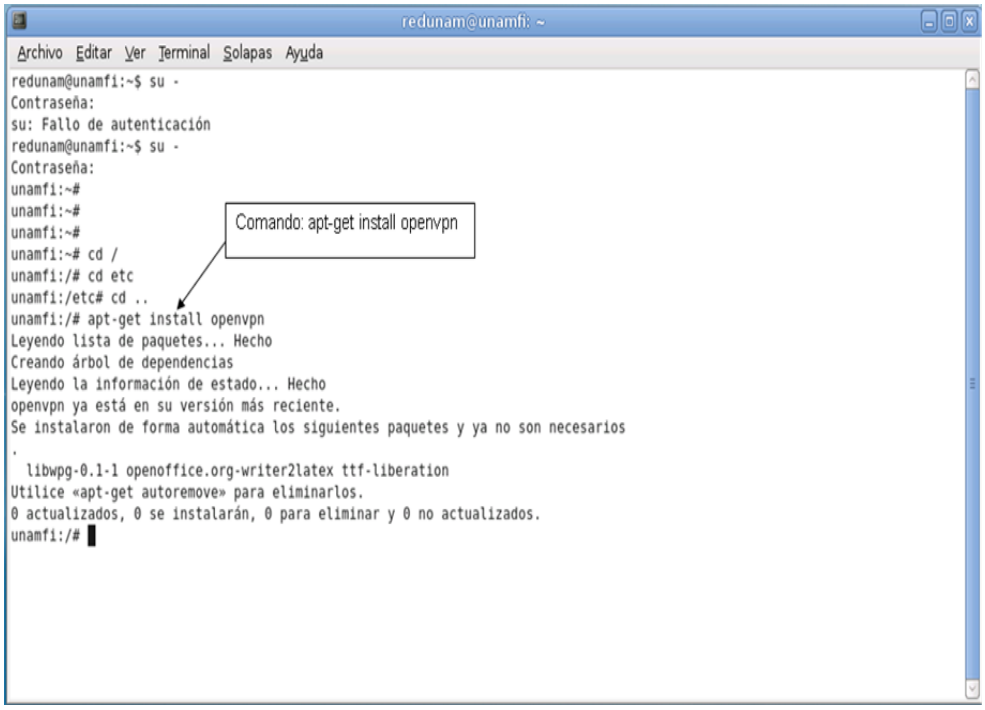


Figura 5.19 Instalación de OPENVPN en Linux.

2) Una vez terminada la instalación de OPENVPN en Linux, se ejecuta el comando apt - cache show openvpn que muestra la información del software que se instaló. (Figura 5.20)

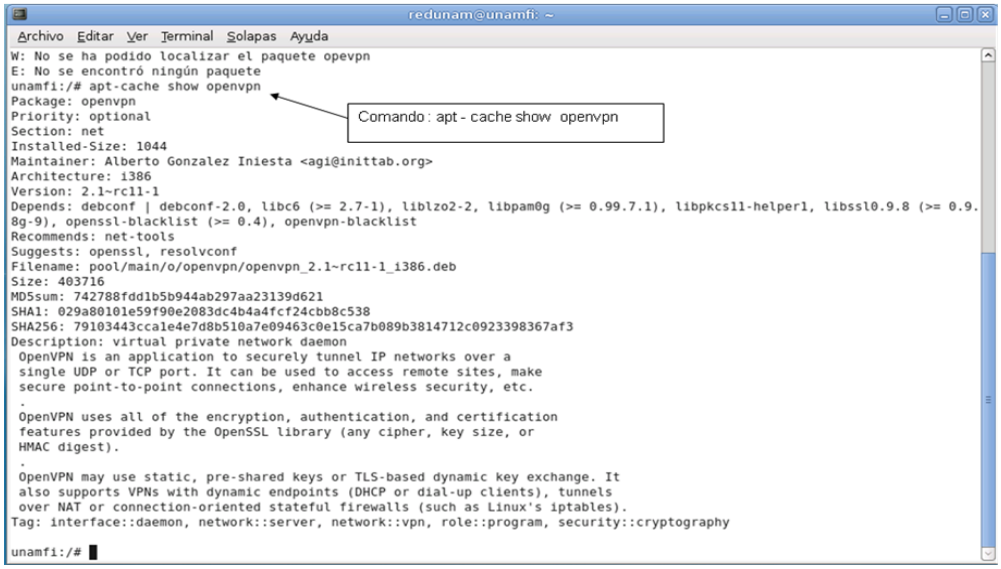


Figura 5.20 Información de la versión de OPENVPN.

3) Se pueden observar en forma de lista los archivos que tiene esta herramienta y que se encuentran en los distintos directorios del Sistema Operativo, con el comando dpkg –L openvpn. (Figura 5.21)

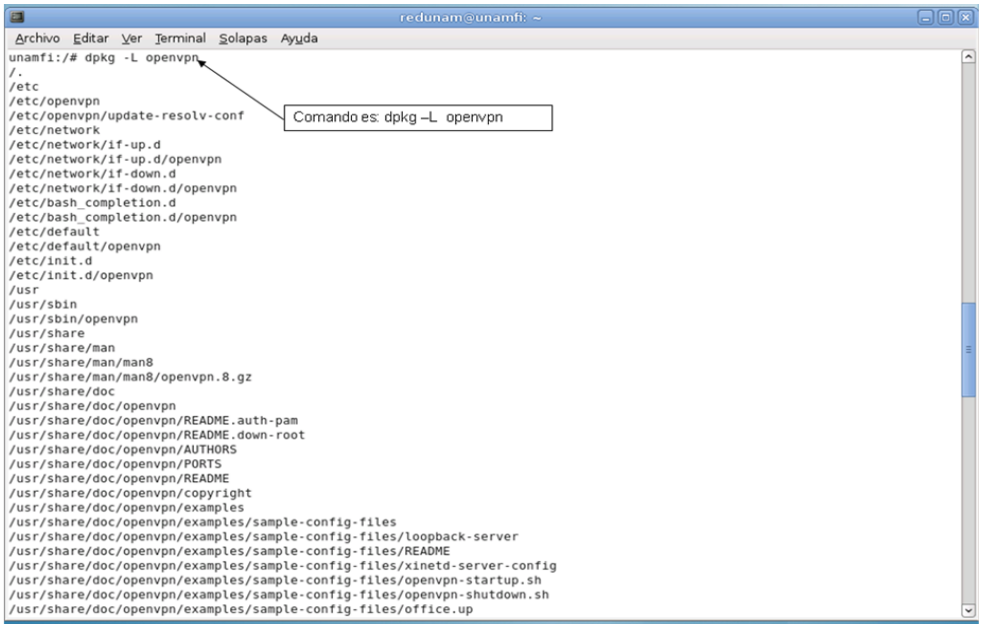


Figura 5.21 Contenido de archivos que tiene el software OPENVPN.

4) En la tabla 5.1 se muestra una visión general de los archivos instalados por el sistema de gestión de paquetes de Debian.

Tabla 5.1 Archivos de configuración instalados en el Sistema Operativo.

Archivo	Descripción
/etc/openvpn	Directorio que contiene los archivos de configuración
/etc/network/if-up.d/openvpn /etc/network/if-down.d /etc/network/if-down.d/openvpn	Se ejecuta un script start / stop openvpn cuando la red es activada / desactivada
/etc/init.d/openvpn	start / stop los scripts de los servicios de openvpn
/sbin/openvpn	Los archivos binarios de openvpn
/usr/share/doc/openvpn	Los archivos de la documentación de openvpn
/usr/share/man/man8/openvpn.8.gz	Manual de la página WEB de openvpn
/usr/share/doc/openvpn/examples/sample – config-files	Archivos de configuración de ejemplos openvpn
/usr/share/doc/openvpn/examples/simple - keys	Ejemplos de claves de openvpn
/usr/share/doc/openvpn/examples/easy-rsa	El archivo easy-rsa es la colección de secuencias de comandos útiles para crear los túneles
/usr/share/doc/openvpn/changelog.debian.gz /usr/share/doc/openvpn/changelog.gz	Muestra la versión histórica de openvpn
/usr/share/openvpn/verify-cn	Función de verificar-cn (revocación de mandato)
/usr/lib/openvpn/openvpn-auth-pam.so /usr/lib/openvpn/openvpn-down-root.so	Bibliotecas para la autenticación PAM y el modo chroot.

5.3 Configuración de los Parámetros de Red

Para empezar a configurar los parámetros de red se asignaron dos interfaces que fueron nombradas eth0 y eth1, estas interfaces son 2 tarjetas Ethernet que están colocadas en el equipo que funciona como servidor.

Estas tarjetas de red permiten que el mismo servidor en Linux configure un router para contar con un segmento de dirección IP y permitir la conexión de los clientes de manera local y mediante un acceso remoto. Se requiere de una IP fija para lograr la comunicación de un servidor con otro; o bien de un sitio con otro.

La IP fija requiere lo siguiente para proveer lo mencionado

1) Servicio de red (Ancho de Banda)
2) Modem/Router
3) Una interfaz de red

Hay que verificar que la IP sea configurada en el servidor OPENVPN con los parámetros asignados por el proveedor de servicios de internet y después es necesario asignar un segmento de red local para el área de trabajo.

Para la red local se utiliza una dirección IP privada con el siguiente segmento: 192.168.x.x/24, con la interfaz eth1.

Para la red remota se utiliza una dirección IP pública con el siguiente segmento: 132.248.xx.x o 200.38.133.97, con la interfaz eth0.

Como se mencionó, las direcciones mostradas en las siguientes imágenes son ficticias, esto por motivos de seguridad.

En la figura 5.22 se muestra que al insertar el comando ifconfig, se indica la dirección IP que contiene cada interfaz, en dicha figura se pone en recuadro la

interfaz eth0 cuya dirección IP es 132.254.xxx.xxx y la máscara de red es 255.255.255.0

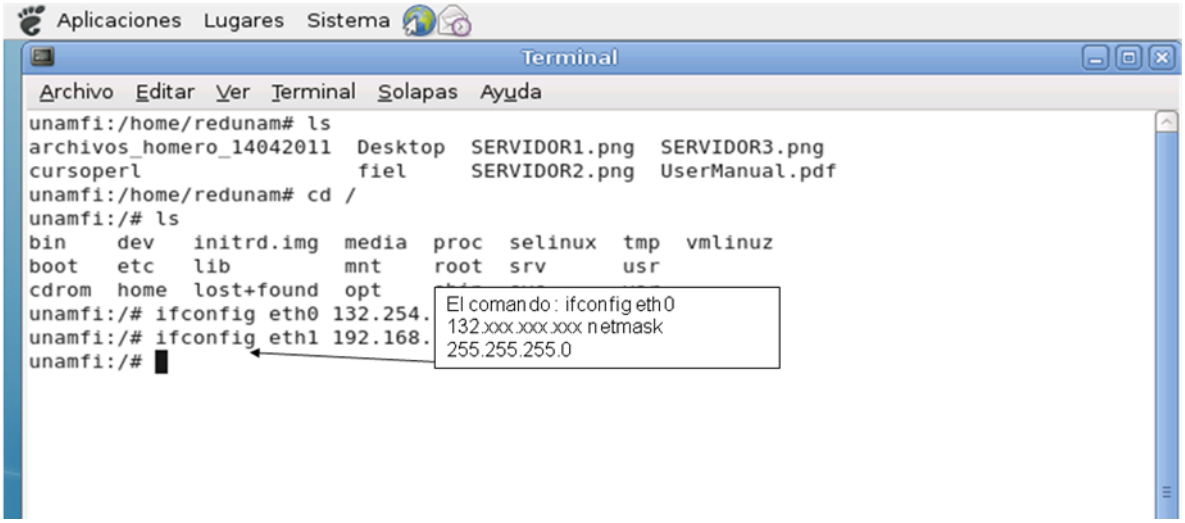


Figura 5.22 interfaces de red de eth0 y eth1.

En la figura 5.23, con el mismo comando ifconfig, se vuelven a mostrar las interfaces con sus respetivas direcciones IP´s.

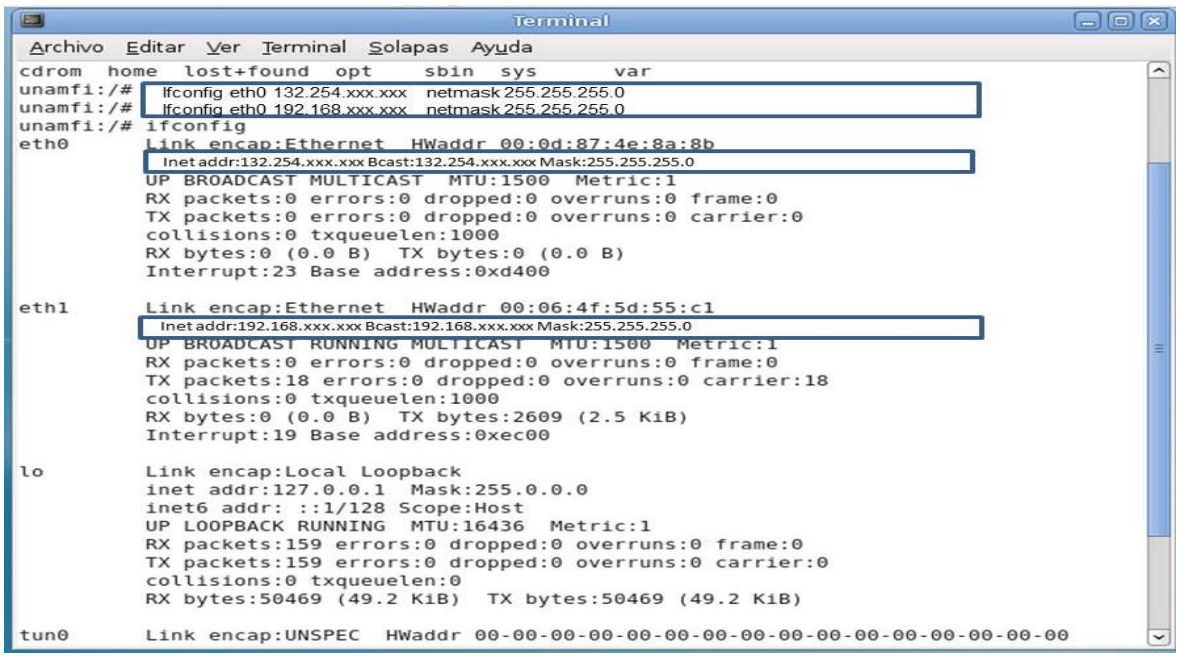


Figura 5.23 Interfaces de red con sus respectivas IP´s fijas y privadas

Los parámetros mostrados anteriormente son importantes en el servidor OPENVPN para que opere la comunicación a nivel interior y exterior, cuando existe una conexión remota, ambos requieren de IP´s fijas para tener entrada y salida de un sitio a otro, donde se podrán realizar transferencias de archivos o aplicaciones de manera segura y rápida.

Para poder acceder al archivo de configuración que es donde se ubican las interfaces de red, se emplea el siguiente comando: # nano /etc/sysctl.conf y una vez abierto este archivo, para que se puedan reactivar las reglas del firewall se edita de la siguiente manera:

1) Se activa el reenvío de paquetes para que el servidor y los clientes no tengan problemas de direcciones, en la figura 5.24 se indica el parámetro que se tiene que activar, el cual es: net.ipv4.ip_forward = 1

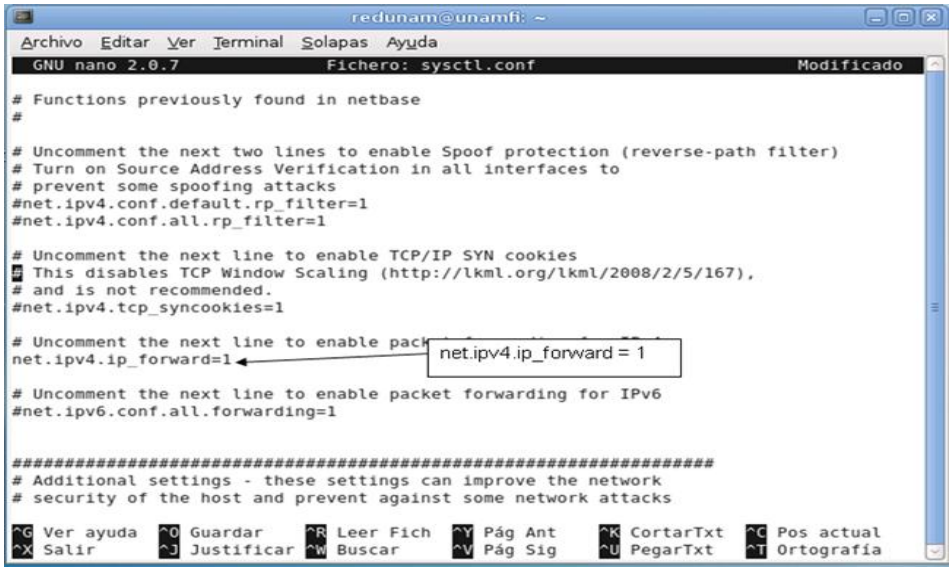


Figura 5.24 Configuración de sysctl.conf

2) Se instala el firewall en el servidor para activar algunos servicios y abrir algunos puertos de comunicación. La instalación del firewall se debe realizar como administrador root.

   El nombre del paquete se llama “arno-iptables-firewall”, este paquete se puede instalar en cualquier sistema operativo Linux; la instalación se

aplicará con el siguiente comando: $apt-get install arno-iptables-firewall (Figura 5.25)

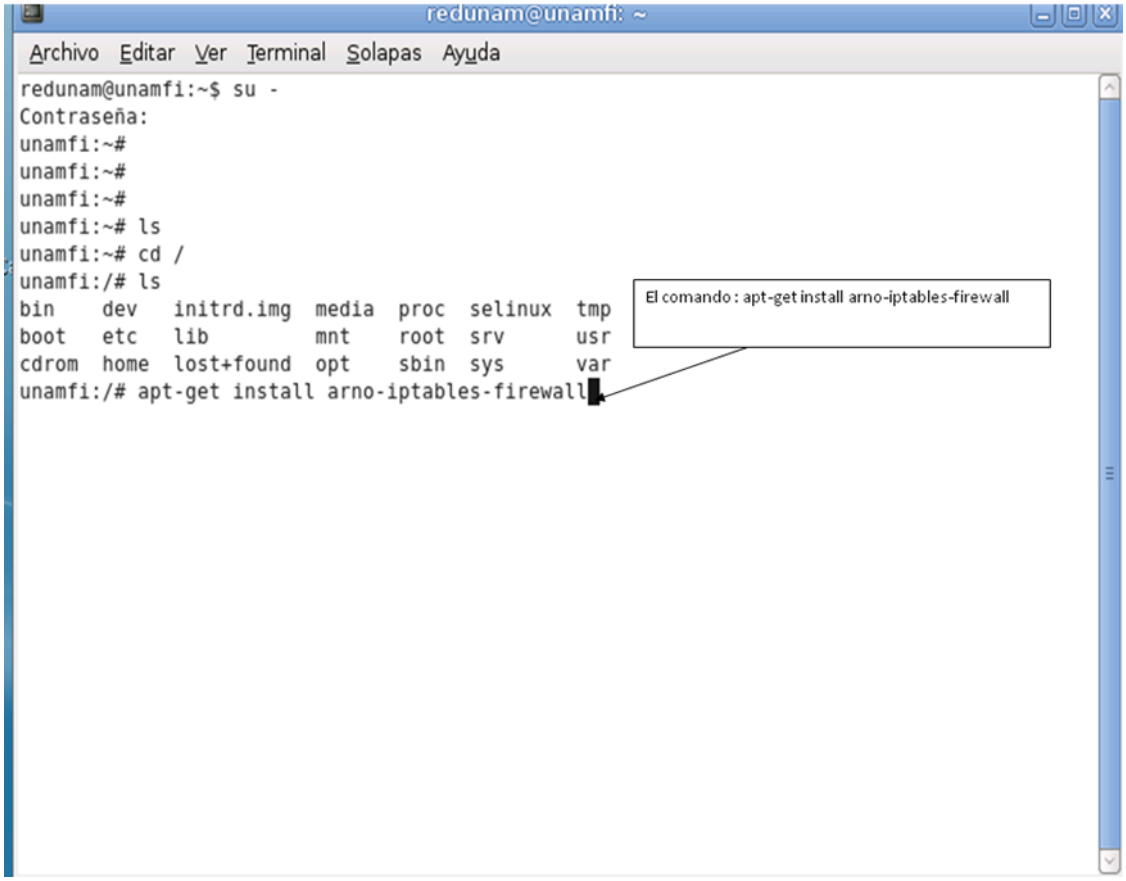


Figura 5.25 Comando para realizar la instalación del firewall

Mientras transcurre la instalación del firewall, aparece la siguiente ventana en la que se pregunta si se quiere configurar el paquete mediante debconf, después se asignan las interfaces de red eth0 y eth1.

Se asigna una como la interfaz externa y en este caso es eth0 y la interna será eth1 para activar la entrada y salida de datos del servidor OPENVPN a través de un modem/router. La figura 5.26 muestra la instalación en modo gráfico del firewall.

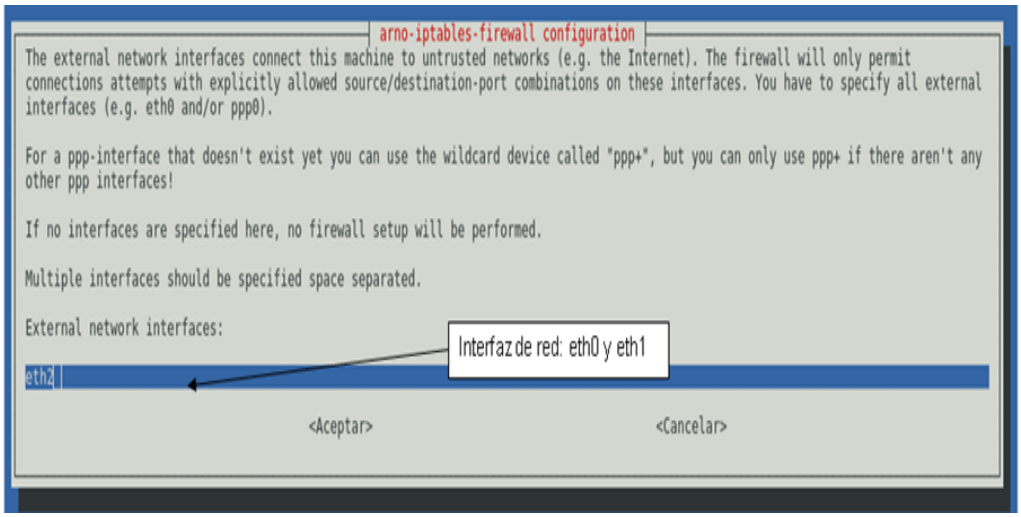


Figura 5.26 Configuración en modo gráfico

3) Ahora se especifica qué puertos se requieren tener abiertos en el firewall de seguridad que está instalado en el servidor OPENVPN. Los puertos que se necesitan son: TCP: 4661, FTP: 21 y SSH: 22, en la figura 5.27 se muestra la activación de los puertos.

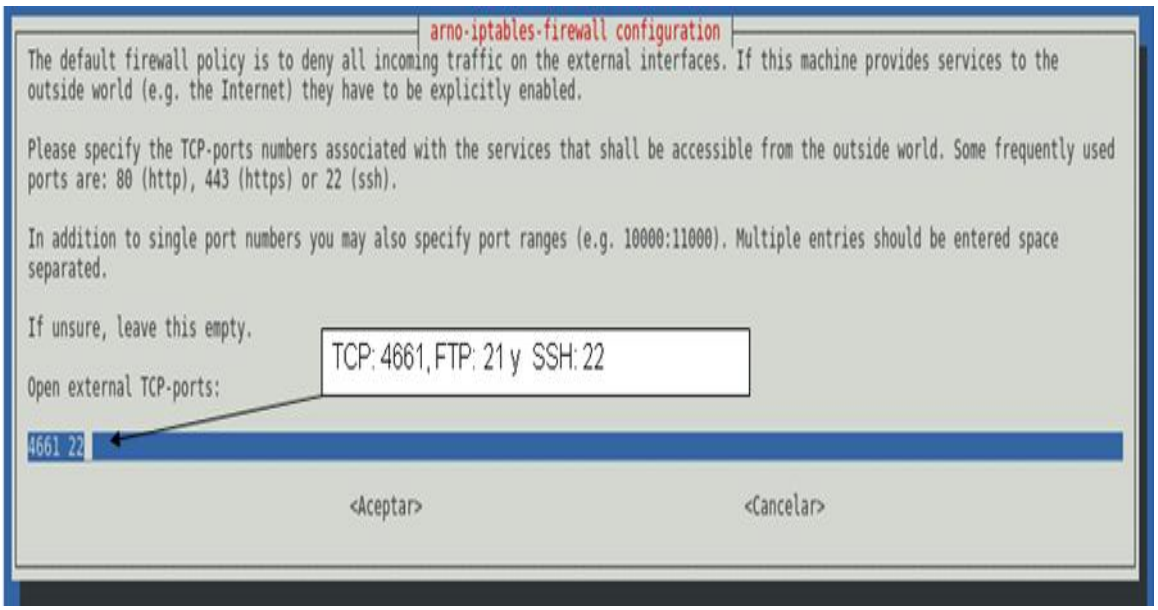


Figura 5.27 Puertos de activación de TCP

4) En la figura 5.28 se muestra que es necesario activar el puerto UDP para los usuarios que están en la red interna y externa, el puerto que se abre es el 4664.

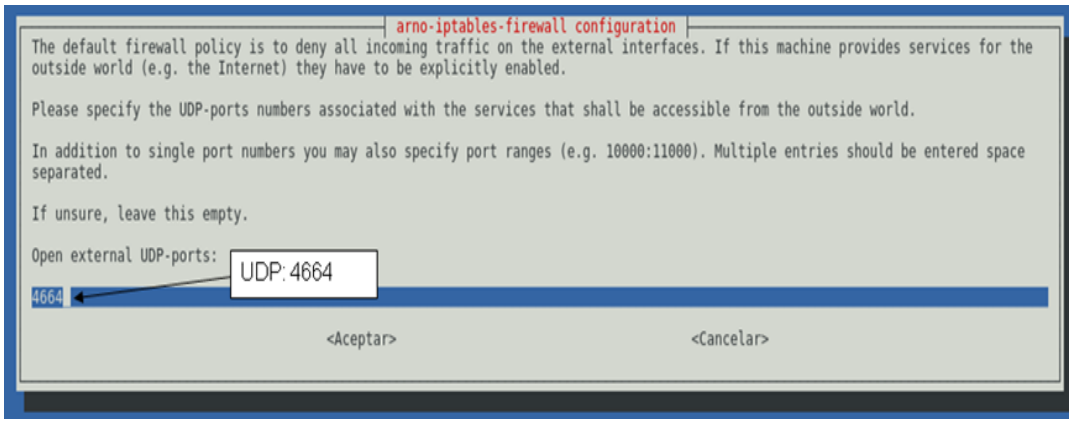


Figura 5.28 Activación del puerto UDP

5) Es necesario activar las interfaces de las tarjetas de red, para contar con un servicio de red local y una conexión remota por medio de la OPENVPN, la figura 5.29 indica el proceso de habilitar las interfaces necesarias.

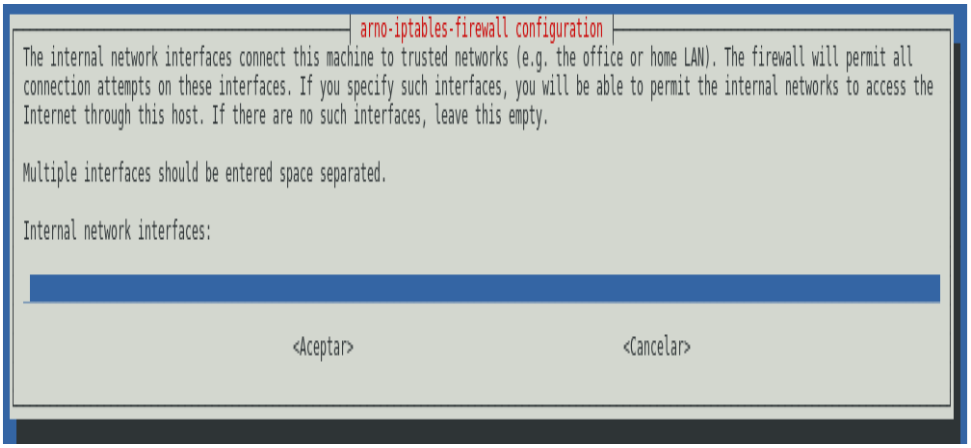


Figura 5.29 Interfaces de red activadas

6) En la figura 5.30 se muestra una indicación refiriéndose a la continuación automática de la instalación del paquete, o bien, si el usuario quiere hacer algunos cambios manualmente.

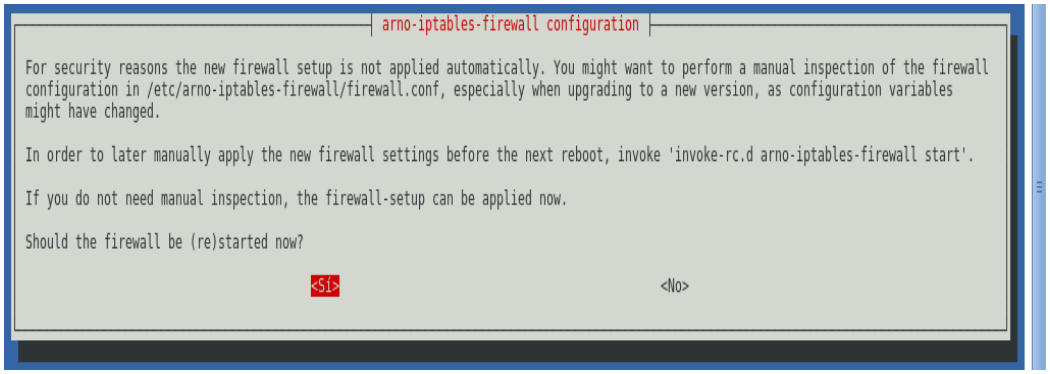


Figura 5.30 Continuación de la instalación

7) Si se dio clic en continuar con la instalación, el siguiente paso es deshabilitar el entorno gráfico que tiene el Sistema Operativo Debian, así como algunos demonios que tiene la parte gráfica del GNU y GNOME, cuando se instala un firewall en el Sistema Operativo se reafirma la seguridad que va a tener el servidor OPENVPN, en la figura 5.31 se muestra la desinstalación del entorno gráfico de Debian.

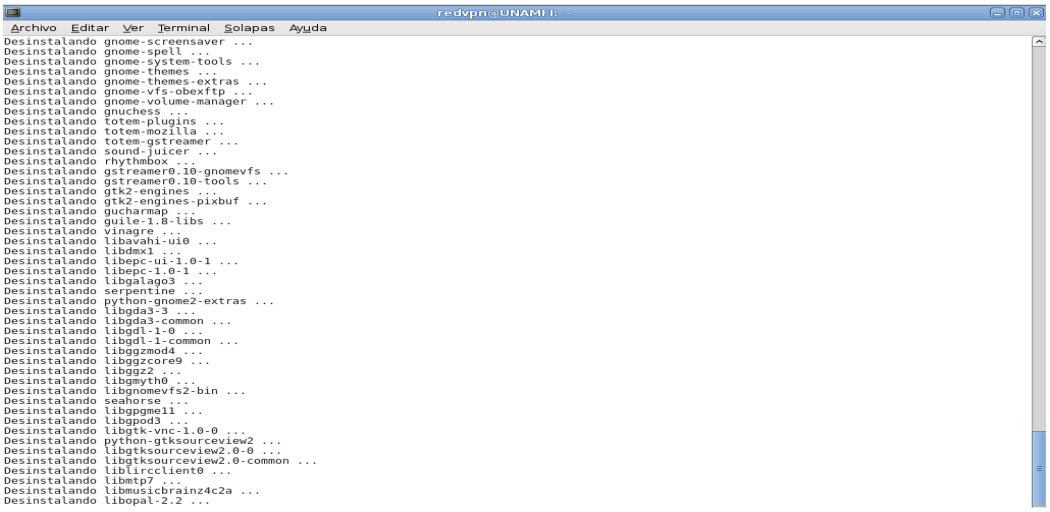


Figura 5.31 Proceso de la desinstalación en modo gráfico de Debian

8) Ya que se terminaron de desinstalar todos los programas que utilizan el entorno gráfico, ahora se instala los archivos repositorios que tiene el paquete arno-iptables-firewall para el servidor OPENVPN en Linux, en la figura 5.32 se muestran todos los archivos de configuración del nuevo firewall.

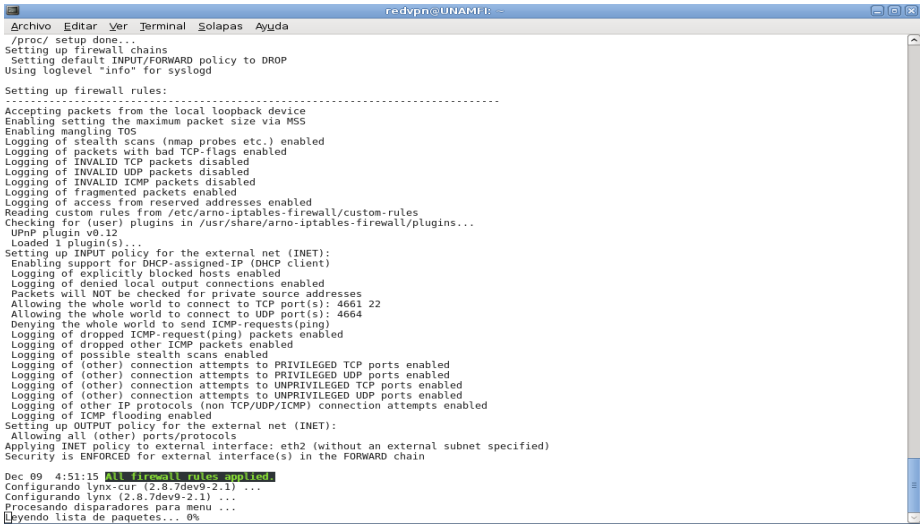


Figura 5.32 Nuevos archivos del firewall

9) Cuando ya terminó la instalación del firewall por completo, ahora hay que verificar su archivo de configuración, en la figura 5.33 se muestra el directorio con todos los archivos de configuración que tiene el arno-iptables-firewall.

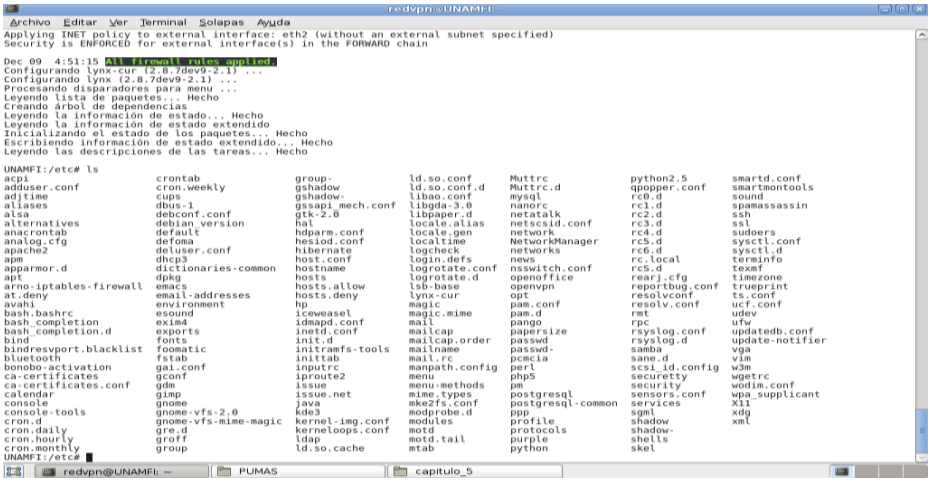


Figura 5.33 Directorio de arno-iptables-firewall

10) Se verifica el archivo de configuración del firewall que está dentro del directorio de arno-iptables-firewall, esto se hace para comprobar las reglas de iptables y algunos ejemplos de los servicios que se pueden restringir con la ayuda del firewall.

    Todo el proceso se realiza ejecutando el comando nano firewall.conf, y al acceder al editor de texto se aplicarán las reglas del firewall en dicho archivo.

    A continuación se muestran cuáles son los parámetros que hay que editar para que funcione el servidor OPENVPN:

    ext_if=”eth0”

    ext_if_dhcp_ip=0

    int_if=”eth1”

    internal_net=”132.xxx.xxx.xxx/24”

    nat=1

    trusted_if=”tun+”

    open_tcp=”22”

    open_udp=”1194”

Cuando ya se tiene configurado el firewall con todos los parámetros asignados, se inicia el servicio para que se activen los cambios que se han hecho.

Los comandos que permiten iniciar el servicio o detener el firewall son los siguientes:

$/etc/init.d/arno-iptables-firewall stop

$/etc/init.d/arno-iptables-firewall start

5.4 Configuración del servidor

Antes de realizar el proceso de configuración de los archivos que contiene el servidor OPENVPN, lo primero que se hace es instalar el paquete openssl con el siguiente comando :

UNAMFI:~# install openssl

Después se edita el archivo vars que se encuentra en /usr/share/doc/openvpn/examples/easy-rsa/ donde se definen las variables de easy-rsa, estas variables contienen los parámetros del servidor, modificando estas variables, los clientes tendrán los mismos datos a la hora de la conexión remota.

Siguiendo con el proceso, se limpian todos los registros anteriores que tenía el archivo ejecutable vars, para poder agregar los nuevos parámetros en el mismo archivo ejecutable. El comando a ejecutar es ./clean-all , en la figura 5.34 se muestra el registro de los parámetros del archivo vars.

```
UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ../vars
bash: ../vars: No existe el fichero o el directorio
UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# . ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on
/usr/share/doc/openvpn/examples/easy-rsa/2.0/keys
UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./clean-all
```

Figura 5.34 Archivo ejecutable vars y el comando de limpieza de registros

Ahora se crea el certificado de autenticación para el servidor y los clientes registrados en el servidor OPENVPN en Linux, ejecutándose UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-ca, todo esto para después asignar los nuevos parámetros que tendrá como datos importantes: nombre del país, estado o provincia, localidad, nombre de la organización o empresa, nombre del área o departamento de la empresa, nombre del dominio de trabajo o la dirección IP pública del servidor, y por

último la cuenta de correo electrónico. En la figura 5.35 se muestran los datos del certificado de autenticación que se asignaron.

```
UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-ca
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'ca.key'
-----

You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:mx
State or Province Name (full name) [CA]:mexico
Locality Name (eg, city) [SanFrancisco]:distrito federal
Organization Name (eg, company) [Fort-Funston]:UNAM
Organizational Unit Name (eg, section) []:INGENIERIA
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:UNAMFI
Email Address [me@myhost.mydomain]:jehteodorounam@yahoo.com.mx
UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0#
```

Figura 5.35 Certificado de autenticación

Para continuar con el proceso se genera el algoritmo Diffie-Hellman, en este paso se pregunta si se quiere firmar digitalmente con el certificado para el servidor y los clientes. En la figura 5.36, se muestra el comando para la instalación del algoritmo asimétrico de Diffie-Hellman en la cual lleva la instrucción UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-dh.

```
UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....+.....+.....+.....+.....
.....+.....+.....
+.....+.....
.....+.....
.....+.....+.....
.....+.....+.....+.....
.....+.....+....+.....
.....+...+.....+.....
.....+.....+.....+.....
.....+.....+.....+.....+...+.....+.....
....+.....+.....+.....
..+.....+.....+.....+.....
.+.....+.....+.....+.....
.....+.....+.....
.....+.....+.....
.....+.....+.....+.....
.....+.....+.....+.....+.....
```

Figura 5.36 Comando para la instalación del algoritmo Diffie-Hellman

Se genera el certificado y la clave para el servidor OPENVPN con el comando UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0#./build-key-server servidor (Figura 5.37).

```
UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-key-server servidor
Generating a 1024 bit RSA private key
.....++++++
...++++++
writing new private key to 'servidor.key'
-----
```

Figura 5.37 Comando para la configuración del certificado y la clave para servidor OPENVPN

Para realizar la copia de los archivos que están dentro del directorio keys, donde se identifican los certificados que fueron generados para el servidor y los clientes, se utiliza el siguiente comando: cp ca.* dh1024.pem server.crt server.key /etc/openvpn, en la figura 5.38 se muestra el comando.

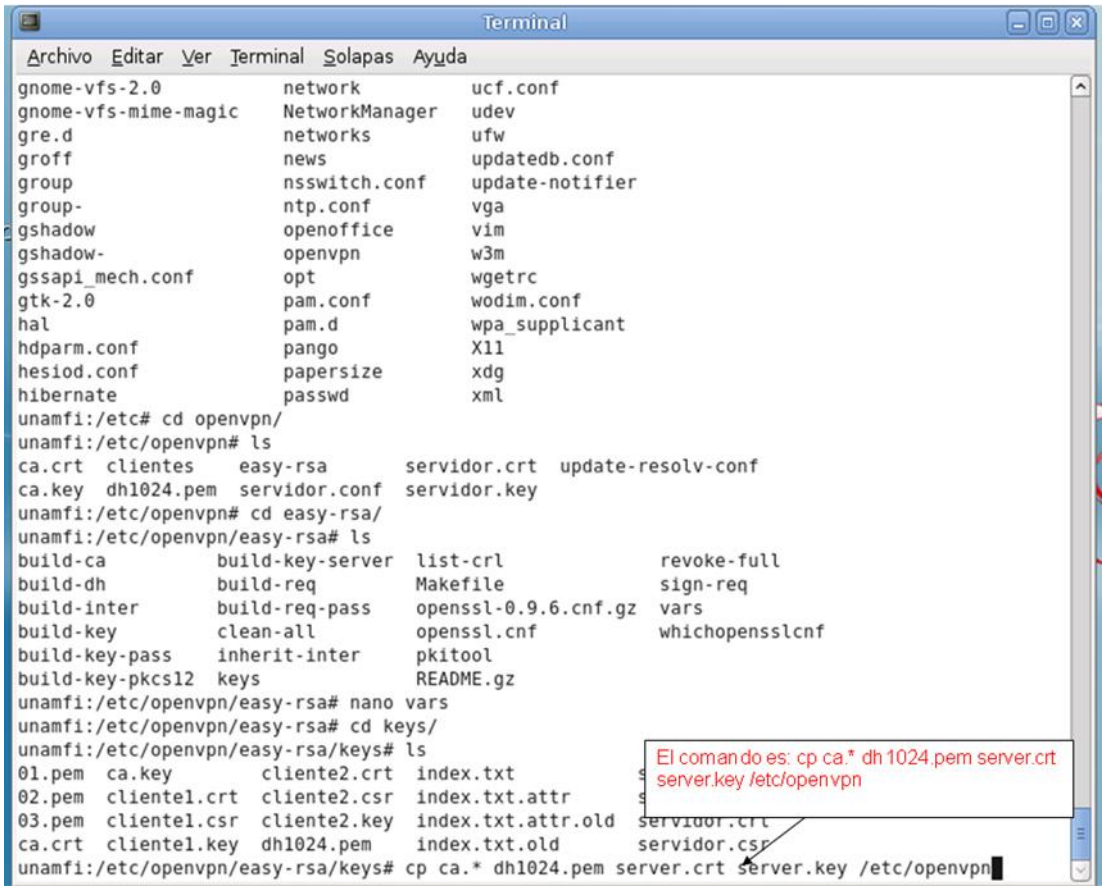


Figura 5.38 Copia de archivos del directorio keys

Ya teniendo estos archivos, se hace una copia de ellos en el directorio /etc/openvpn, esto se realiza de la siguiente manera:

UNAMFI:~# cp /usr/share/doc/openvpn/examples/easy-rsa/2.0/ /etc/openvpn/easy-rsa –R -v

En la figura 5.39 se indica el directorio donde están los archivos de configuración del servidor OPENVPN.

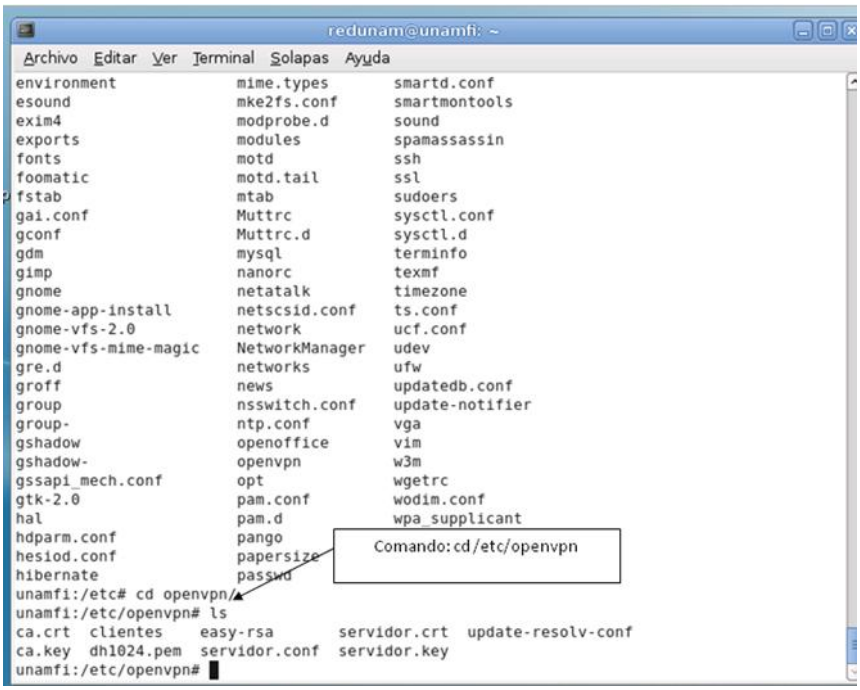


Figura 5.39 Archivos que están en el directorio /etc/openvpn para el servidor OPENVPN

Los archivos importantes que deben estar en el directorio /etc/openvpn para activar el servidor OPENVPN se encuentran en la Tabla 5.2.

Tabla 5.2 Archivos del directorio /etc/openvpn

Archivo	Descripción
ca.crt ca.key	Contiene el certificado de autenticación y clave. Sin esto no se podrán crear certificados para los clientes VPN.
dh1024.pem	Clave Diffie-Hellman, también es necesaria para los clientes.
server.crt server.key	Contiene el Certificado de autenticación para el servidor y la clave.

Se crea un archivo para el servidor OPENVPN con el nombre de servidor.conf, en donde se conjuntan todos los parámetros necesarios para que funcione el servidor OPENVPN, el comando para generar el archivo de configuración es: nano servidor.conf**,** este comando permitirá generar un archivo de texto para incluir las instrucciones del servidor OPENVPN, en la figura 5.40 se muestran las reglas de configuración.

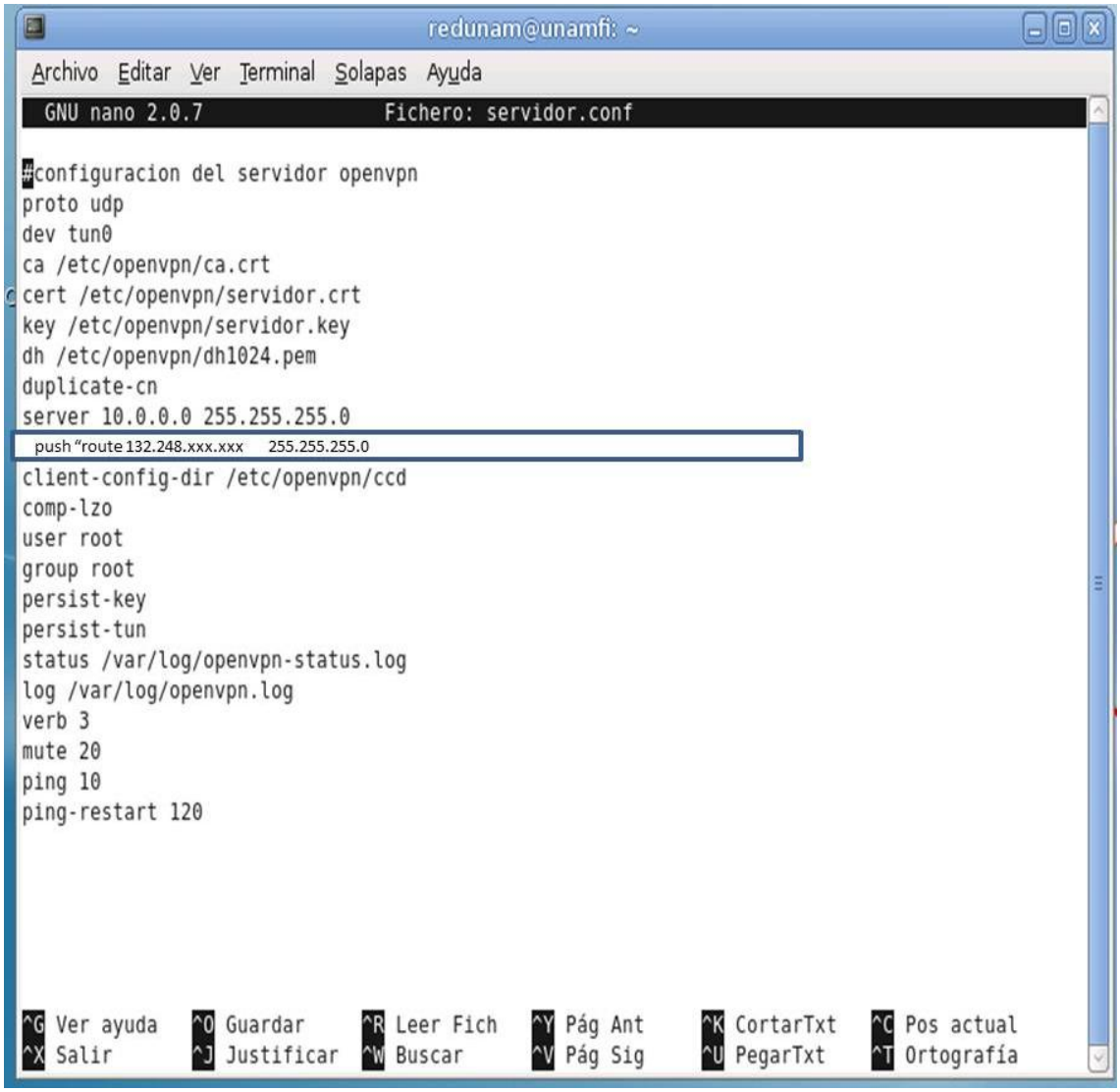


Figura 5.40 Reglas de configuración del servidor OPENVPN

A continuación se muestra la descripción detallada de cada parámetro que está configurado en el servidor OPENVPN (Tabla 5.3)

Tabla 5.3 parámetros del servidor OPENVPN

Parámetro	Descripción
proto udp	El servicio de OpenVPN utilizará protocolo UDP.
dev tun0	Interfaz virtual por la cual se crea el túnel.
ca /etc/openvpn/ca.crt	Especifica la ruta en donde se localiza el certificado de autenticación.
cert /etc/openvpn/servidor.crt	Especifica la ruta en donde se localiza el certificado de servidor.
key /etc/openvpn/servidor.key	Especifica la ruta en donde se localiza la clave de autenticación.
dh /etc/openvpn/dh1024.pem	Especifica la ruta que contiene el algoritmo Diffie Hellman.
server 10.0.0.0 255.255.255.0	Segmento de red VPN, la primera IP del segmento queda reservado para el servidor OpenVPN.
push “route 134.xxx.xxx.xxx 255.255.255.0”	Se configurá la IP fija del servidor OPENVPN
client-config-dir /etc/openvpn/ccd	Este parámetro manda llamar al archivo dentro de esta ruta para asignar IP Estáticas de la Red VPN.
comp-lzo	Comprimir dentro de la red virtual con lzo.
persist-key	Esta opción soluciona el problema por claves que persisten a través de los reajustes SIGUSR1.
persist-tun	Permite que no se cierre y se vuelvan a abrir los dispositivos TAP/TUN.
status /var/log/openvpn-status.log	Estado actual del servicio OpenVPN.
log /var/log/openvpn.log	Las bitácoras de los Logs del servicio OpenVPN.
ping 10	Ping cada 10 segundos al servidor OpenVPN.
ping-restart 120	Reinicia ping cada 120 segundos.

Finalmente, ya se puede hacer uso del servidor OPENVPN en Linux para utilizar el servicio de la red remota en cualquier lugar; con la condición de que cuente con permisos asignados por el administrador de la red, esto para hacer

uso de la red VPN dentro de una red interna como si estuviera trabajando desde su casa a la oficina.

Para iniciar el servidor OPENVPN y estar a la espera de las peticiones de conexión por los usuarios remotos, se utiliza el siguiente comando:

$openvpn --config/etc/openvpn/servidor.conf y el comando para la restauración es $ /etc/init.d/openvpn start

Con el comando ifconfig se presentan las direcciones IP de cada interfaz, así como la interfaz del túnel tun0 de OPENVPN que se configuró en Debian, se puede apreciar la dirección IP que se le asignó al túnel, la cual fue 10.0.0.1. La figura 5.41 muestra lo mencionado anteriormente.

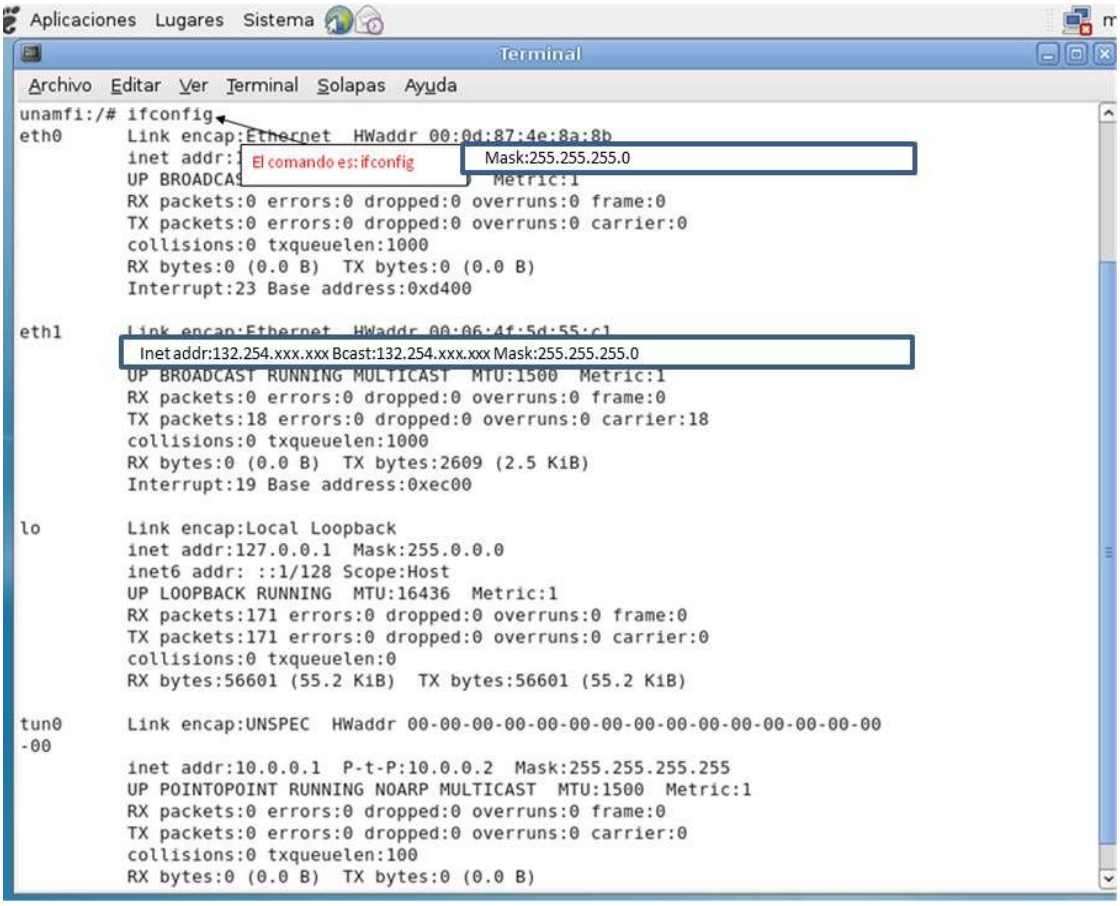


Figura 5.41 Interfaces de red y del túnel, con el comando ifconfig

5.5 Configuración de los clientes

Para poder agregar clientes en el servidor OPENVPN se crea el certificado y la clave por cada usuario que se conecte al servidor. Se recomienda poner en los certificados el nombre de la persona para tener mayor control de los usuarios conectados (Figura 5.42)

```
UNAMFI:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-key  cliente1
Generating a 1024 bit RSA private key
.....++++++
...++++++
writing new private key to 'cliente1.key'
-----
```

Figura 5.42 Creación de certificado y clave del usuario

Estos certificados se crean en el siguiente directorio /usr/share/doc/openvpn/examples/easy-rsa.

Ahora se tiene que verificar el directorio **keys**, donde se encuentran todos los usuarios que fueron creados desde el servidor OPENVPN, estos archivos permitirán a los usuarios tener acceso al servidor, en la figura 5.43 se muestra el nombre de cada usuario que se creó dentro del directorio **keys.**

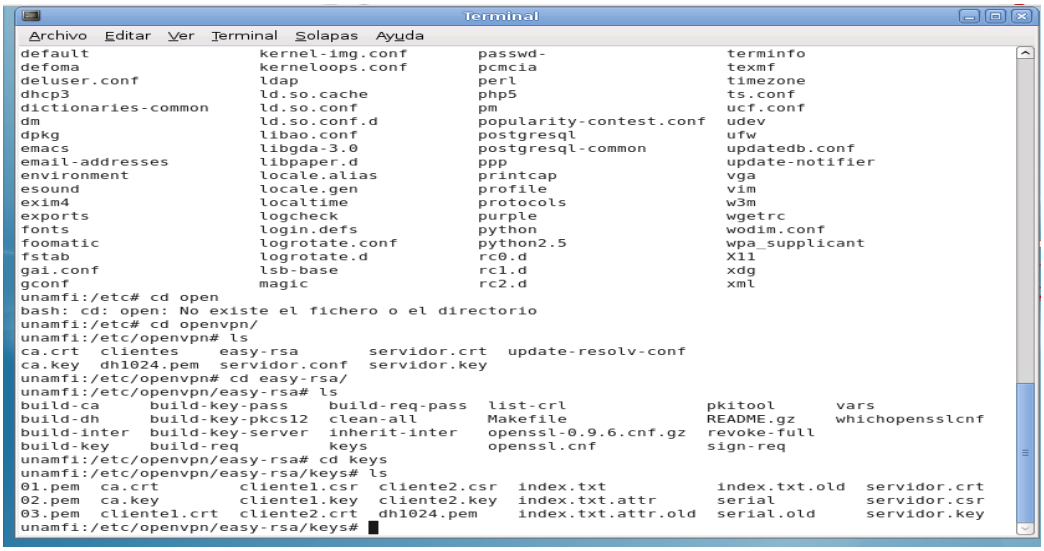


Figura 5.43 Directorio keys, donde los usuarios están creados

Los archivos importantes que deben estar en el directorio /etc/openvpn para activar el cliente1 OPENVPN son los que se muestran en la tabla 5.4

Tabla 5.4 Contenido del archivo cliente

Archivo	Descripción
ca.crt	Contiene el certificado de autenticación.
cliente1.crt cliente1.key	Contiene el Certificado de autenticación para el cliente1 y su clave.

Los archivos que se generaron para el cliente1 están en una carpeta con su respectivo nombre, En la figura 5.44 se muestran los archivos de configuración que tiene el cliente1 y cliente 2 en OPENVPN en Linux.

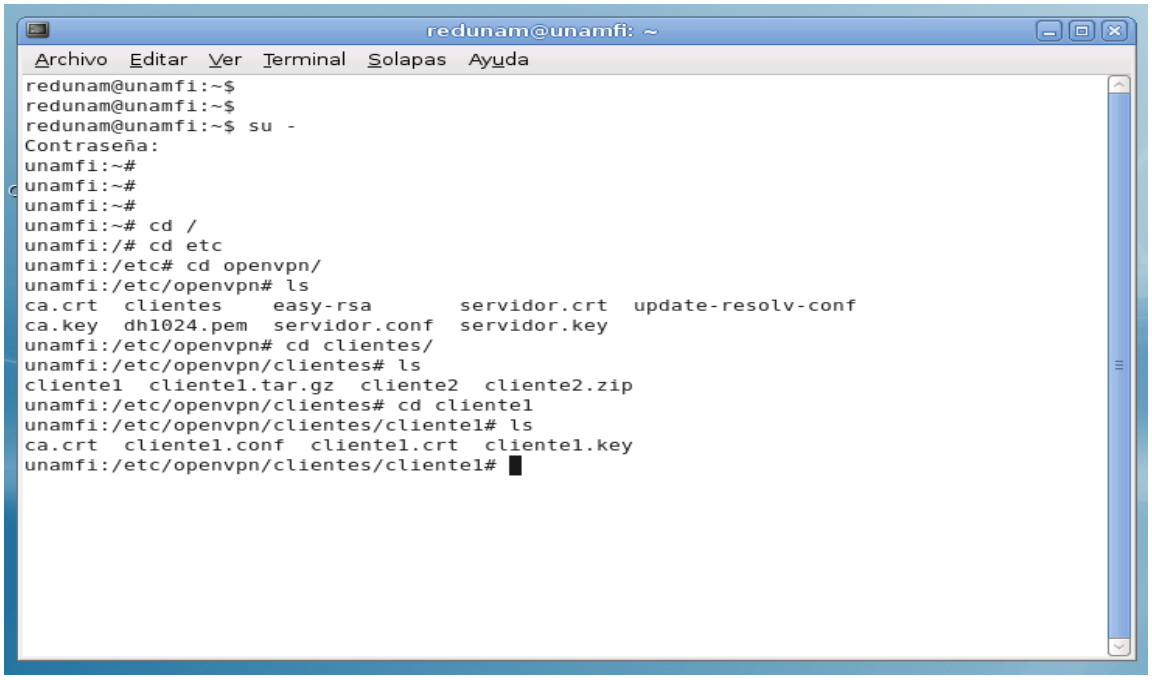


Figura 5.44, Archivos de configuración que tiene el cliente1 en Linux

Una vez generado el archivo de cada cliente, se transmite toda su información a un dispositivo USB o por algún medio de transferencia como Secure Shell o Filezilla, el directorio donde se encuentran dichos clientes se ubican en /etc/openvpn/easy-rsa/keys.

Se instala OPENVPN en la máquina cliente de Linux para poder activar el servicio empleando el comando $apt-get install openvpn.

Una vez instalado OPENVPN en la máquina cliente, se debe generar el archivo de configuración con todos los parámetros para tener conexión con el servidor OPENVPN. En la figura 5.45 se observa la configuración que tiene el cliente1.

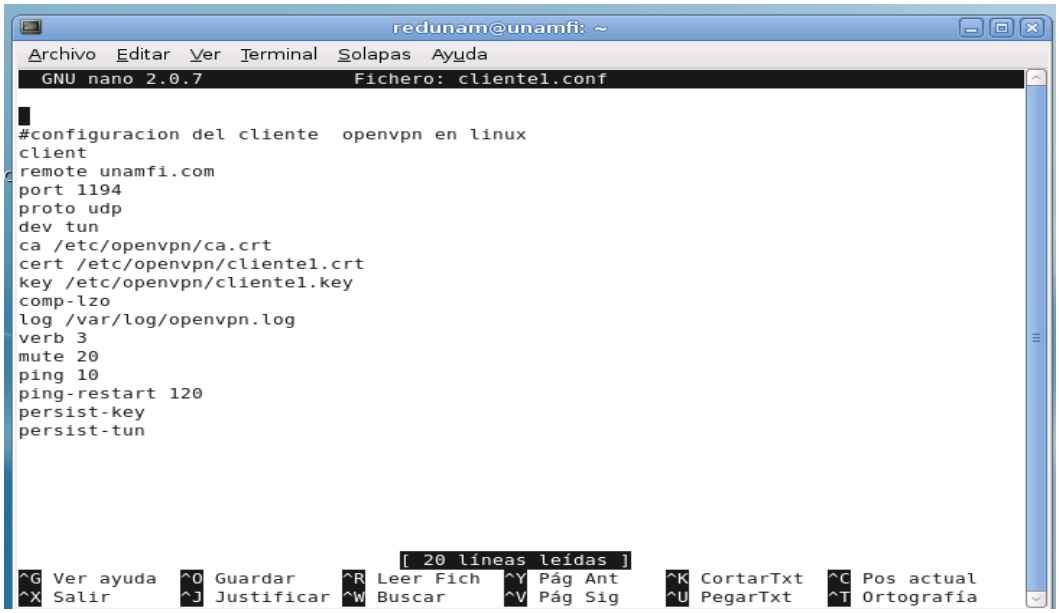


Figura 5.45 Configuración del cliente1

Se muestra la explicación de los parámetros que están asignados para los clientes y que tienen comunicación remota con el servidor OPENVPN. (Tabla 5.5)

Tabla 5.5 Parámetros del cliente1

Parámetro	Descripción
Client	Nombre del cliente de la red VPN.
remote unamfi.com	El nombre o IP del servidor OpenVPN, el cual controla los accesos a la misma.
Port 1194	Puerto del servicio OpenVPN en el servidor.
proto udp	Protocolo utilizado en red VPN
dev tun	Interfaz virtual con el cual se conecta a la red VPN.
ca /etc/openvpn/ca.crt	Especifica la ruta en donde se localiza el certificado de autenticación, este certificado es del servidor OpenVPN.
cert /etc/openvpn/cliente1.crt	Especifica la ruta en donde se localiza el certificado del cliente
key /etc/openvpn/cliente1.key	Especifica la ruta en donde se localiza la clave de autenticación del cliente.
comp-lzo	Comprimir dentro de la red virtual con lzo.
log /var/log/openvpn.log	Las bitácoras de los Logs del servicio OpenVPN.
ping 10	Ping cada 10 segundos al servidor OpenVPN.
ping-restart 120	Reinicia ping cada 120 segundos.
Persist-key	Esta opción soluciona el problema por claves que persisten a través de los reajustes.
persist-tun	Permite que no se cierre y se vuelvan a abrir los dispositivos TAP/TUN.

Finalmente ya se puede hacer uso del cliente OPENVPN en Linux, para utilizar el servicio de la red remota en cualquier lugar se tiene que iniciar el cliente OPENVPN con el comando:

$openvpn --config/etc/openvpn/cliente1.conf o con el otro comando para la restauración $ /etc/init.d/openvpn start

Es importante no olvidar que se debe comprobar que exista el servicio de OPENVPN, solo se tiene que verificar con el comando ifconfig de la interfaz del

túnel de OPENVPN en Linux, la forma como se ejecutaría el comando es de la siguiente manera: $ifconfig tun0.

Para poder agregar clientes que utilizan el Sistema Operativo Windows en el servidor OPENVPN, se instala la herramienta y a continuación se explica su procedimiento:

La primera ventana es la de bienvenida e informa la versión de dicho paquete, así como las versiones de Windows que soporta (Figura 5.46).

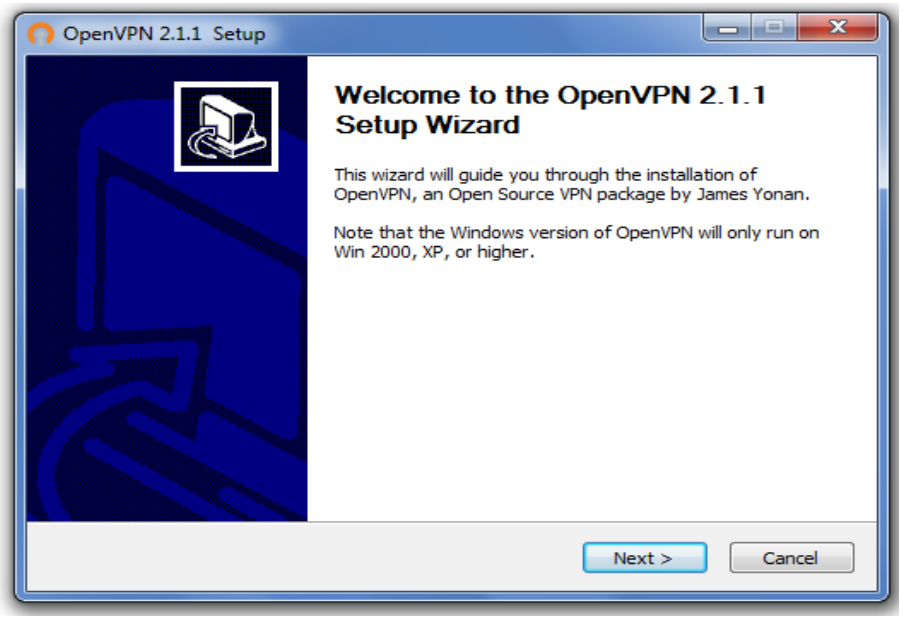


Figura 5.46 Pantalla de bienvenida de OpenVPN

En la siguiente ventana se muestra el acuerdo de la licencia que se tiene que aceptar para seguir con la instalación. (Figura 5.47)

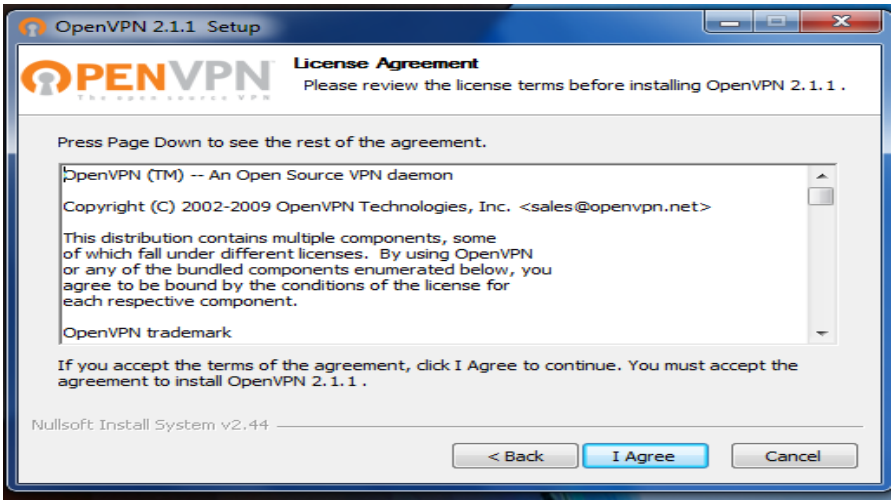


Figura 5.47 Acuerdo de Licencia

En la imagen 5.48 se seleccionan los componentes que se instalan en el Sistema, en este caso se selecciona todo para que no se tenga ningún problema al realizar las transferencias de información entre el cliente y el servidor.

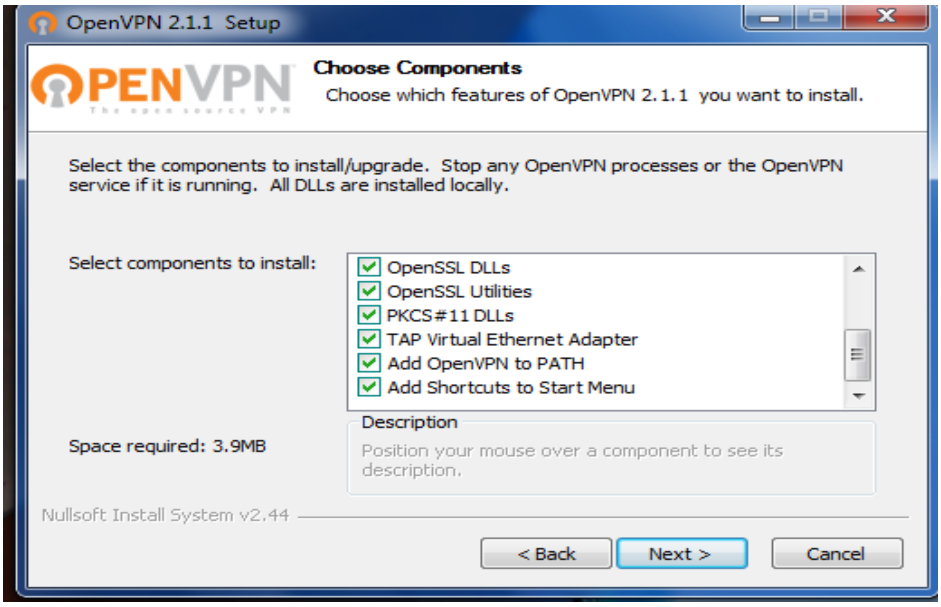


Figura 5.48 Acuerdo de Licencia

La ruta de ubicación donde se instala el programa es C:\ProgramFiles\OpenVPN. (Figura 5.49)

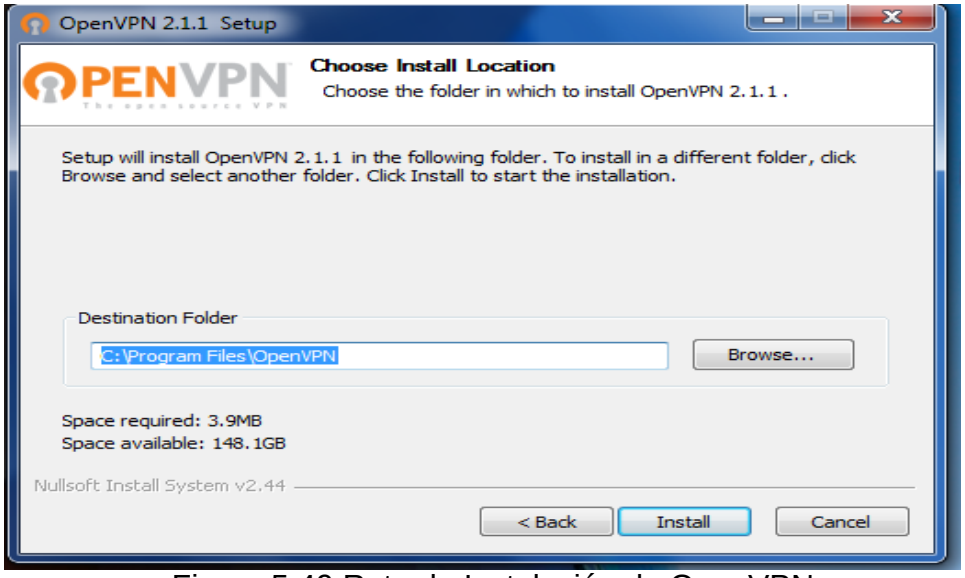


Figura 5.49 Ruta de Instalación de OpenVPN

Una vez aceptada la ruta de instalación se procede a seguir con el proceso como se muestra en la figura 5.50

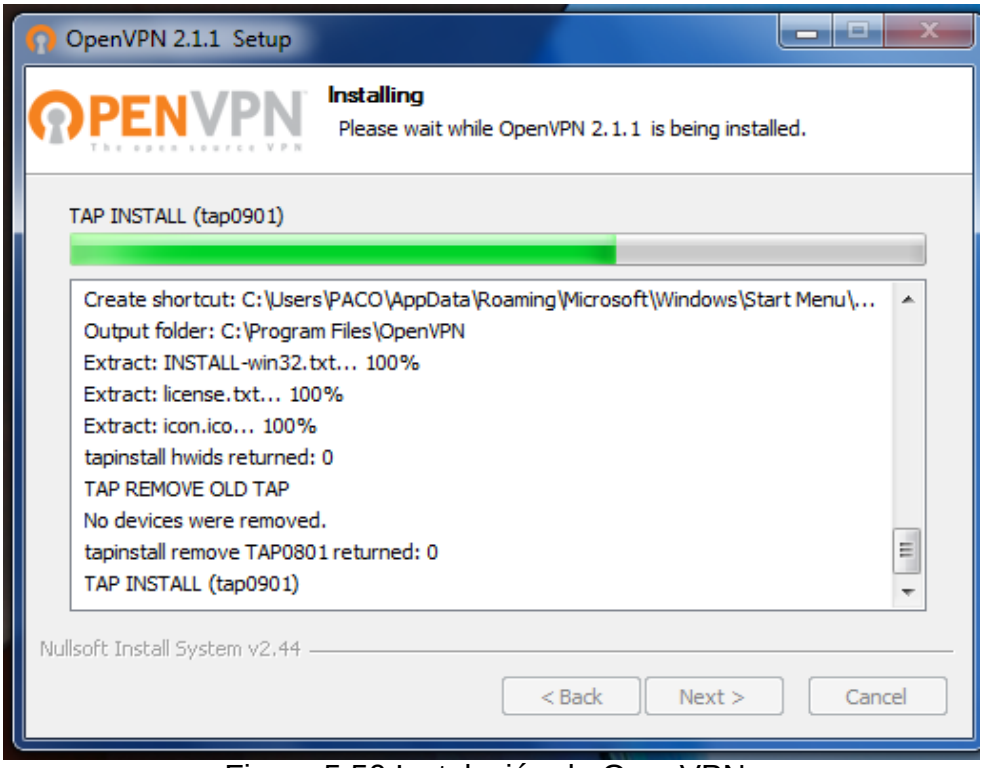


Figura 5.50 Instalación de OpenVPN

La instalación ha quedado concluida y la siguiente ventana muestra que el proceso ha finalizado. (Figura 5.51)

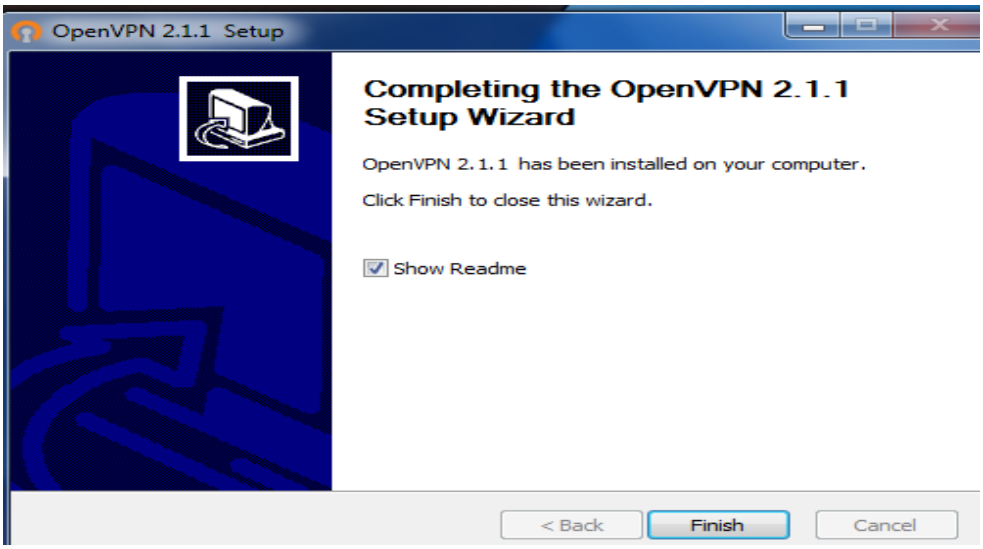


Figura 5.51 Instalación Finalizada

Una vez instalado el paquete de OpenVPN se abre una ventana de texto en donde se muestran algunas indicaciones el programa debe considerar para su correcto funcionamiento, para esto se configura la carpeta config, (Figura 5.52)

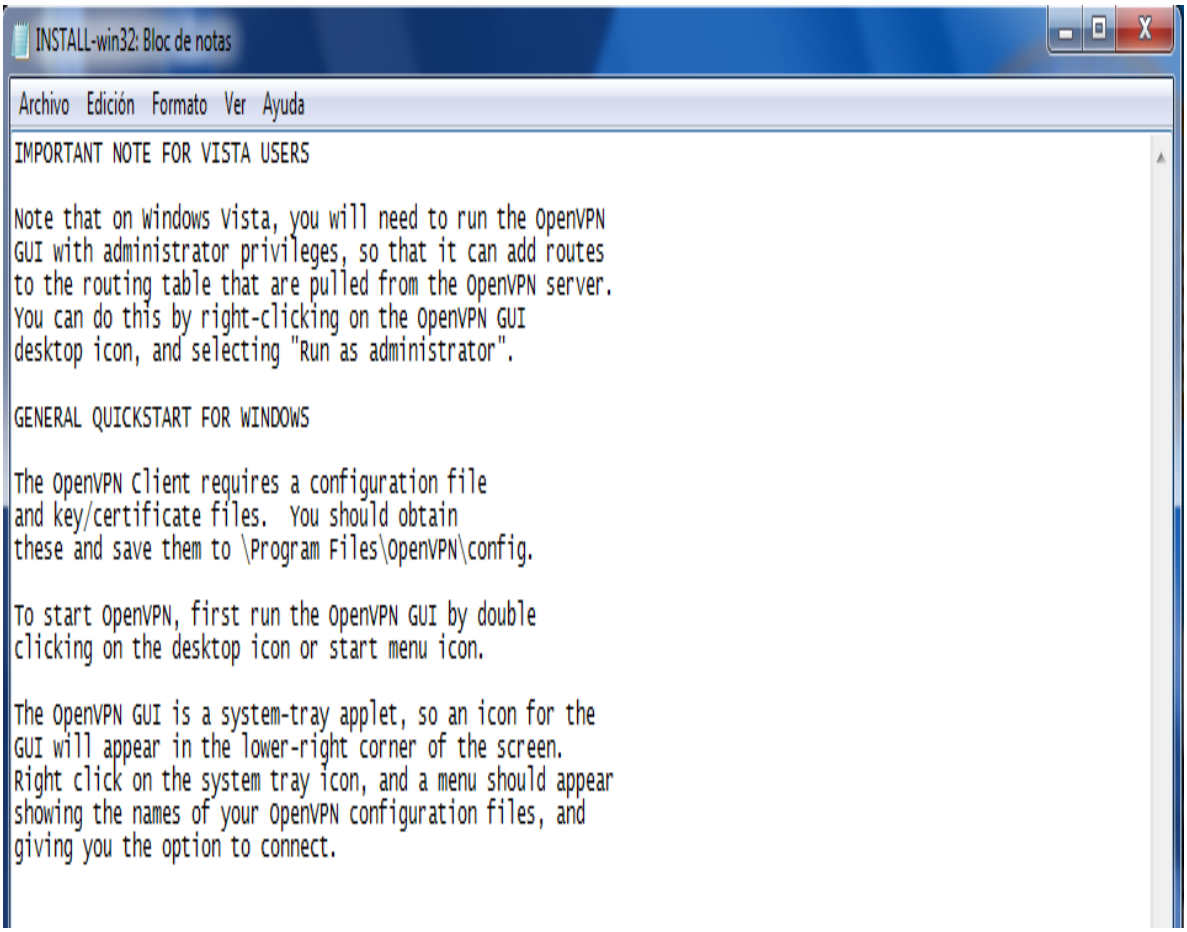


Figura 5.52 Indicaciones del programa OpenVPN.

Como se mencionó, se localiza la ruta de instalación de la herramienta OpenVPN la cual es: \Archivos de programa\OpenVPN\config (Figura 5.53)

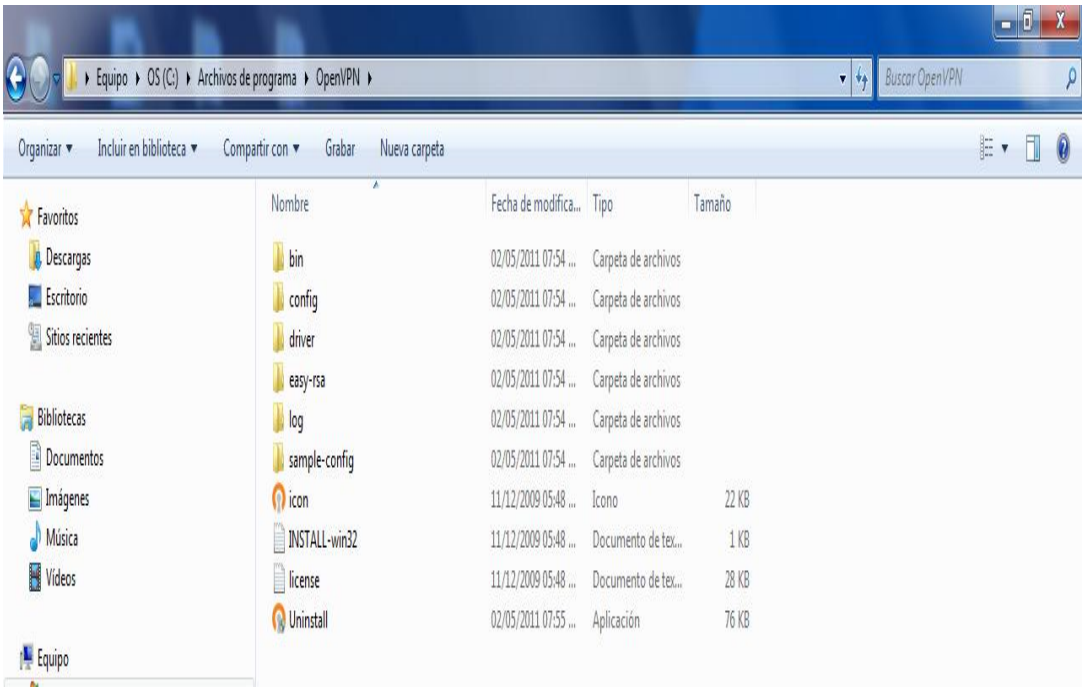


Figura 5.53 Ubicación de la herramienta OpenVPN

Desde la carpeta del cliente1, cuyos archivos fueron creados desde el servidor en Linux y posteriormente guardados en un dispositivo USB, serán copiados y depositados en la carpeta config del directorio de OpenVPN (Figura 5.54).

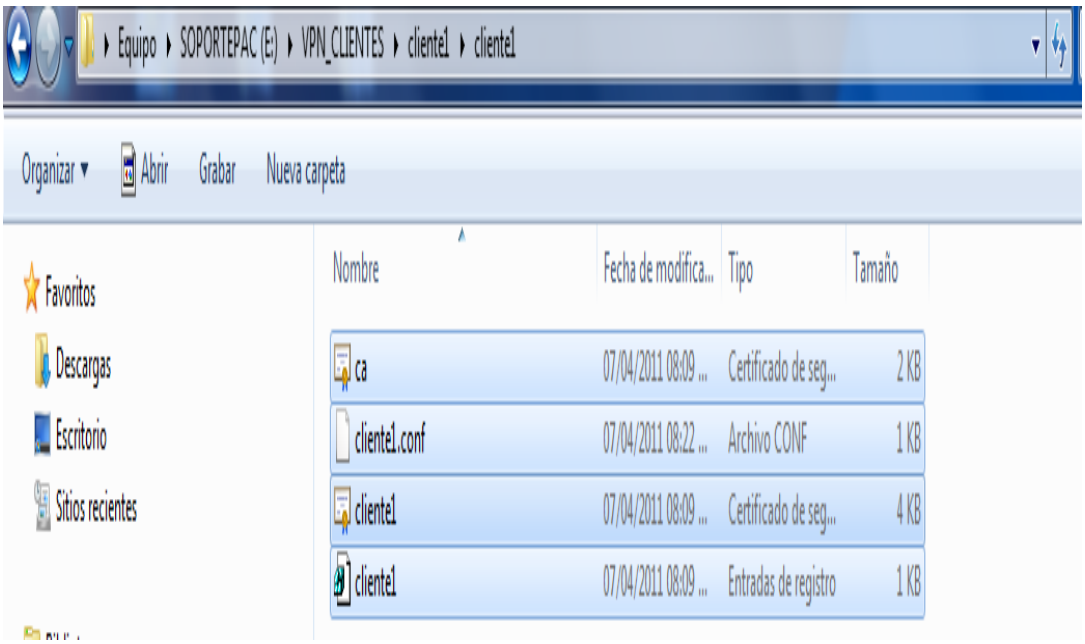


Figura 5.54 Archivos de la carpeta cliente1

En la Figura 5.55 se observa que los archivos que fueron copiados desde el dispositivo USB ya fueron colocados en la carpeta config.

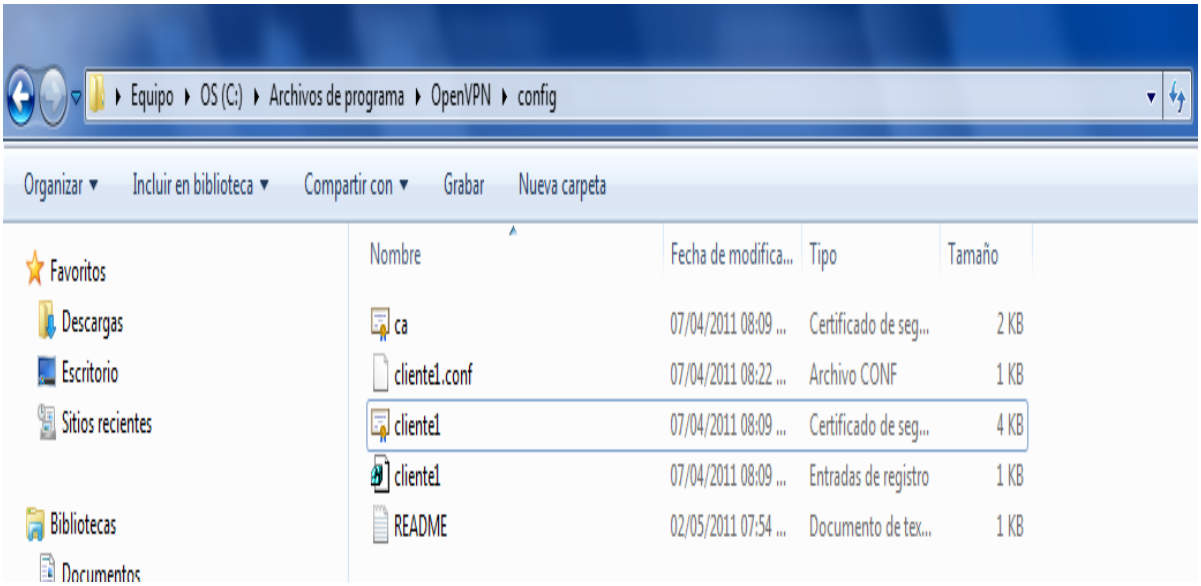


Figura 5.55 Archivos completos de la carpeta config

Por último, se puede ver el ícono de la herramienta OpenVPN, el cual se podrá utilizar confiablemente una vez realizadas las indicaciones anteriores (Figura 5.56)

Figura 5.56 Ícono de OpenVPN en Windows

5.6 Pruebas

Para comprobar la funcionalidad del proyecto, se realizaron las siguientes pruebas:

En lo que se refiere al Sistema Operativo Windows, una vez instalado OpenVPN en dicho sistema, se ve en la parte inferior derecha del escritorio de Windows el ícono de OpenVPN, al dar click derecho con el mouse, se observa el listado de opciones que tiene el programa Figura 5.57.

Figura 5.57 Opciones de OpenVPN en Windows

Al elegir conectar, se debe ingresar la contraseña del cliente (Figura 5.58).

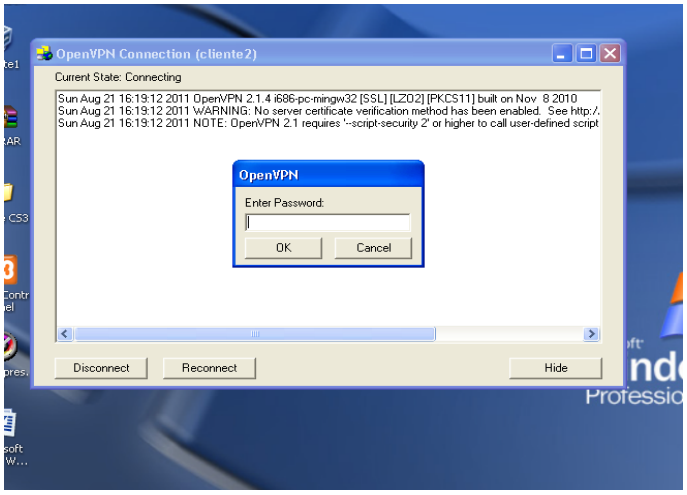


Figura 5.58 Solicitud de la contraseña de acceso a la red remota

Una vez ingresada la contraseña se hace la conexión remota de la VPN hacia la red interna de la organización, se verifican los datos y la configuración del cliente al servidor OpenVPN, si son correctos los datos es posible realizar cualquier actividad de manera segura por medio de la VPN que está enlazada a la red interna de la compañía o institución educativa. La figura 5.59 indica el proceso de autenticación y si el usuario está registrado por el servidor OpenVPN, si es así, el ícono que se muestra en la parte inferior del escritorio de Windows donde aparecen dos computadoras conectadas se pondrá de color verde.

Cuando se hace la conexión con el servidor, la configuración del túnel permite comunicarse con él, pues de cierta manera el túnel proporciona una dirección que sirve como enlace de máquina a máquina, esta dirección es por ejemplo 10.0.0.1 y da dos direcciones consecutivas.

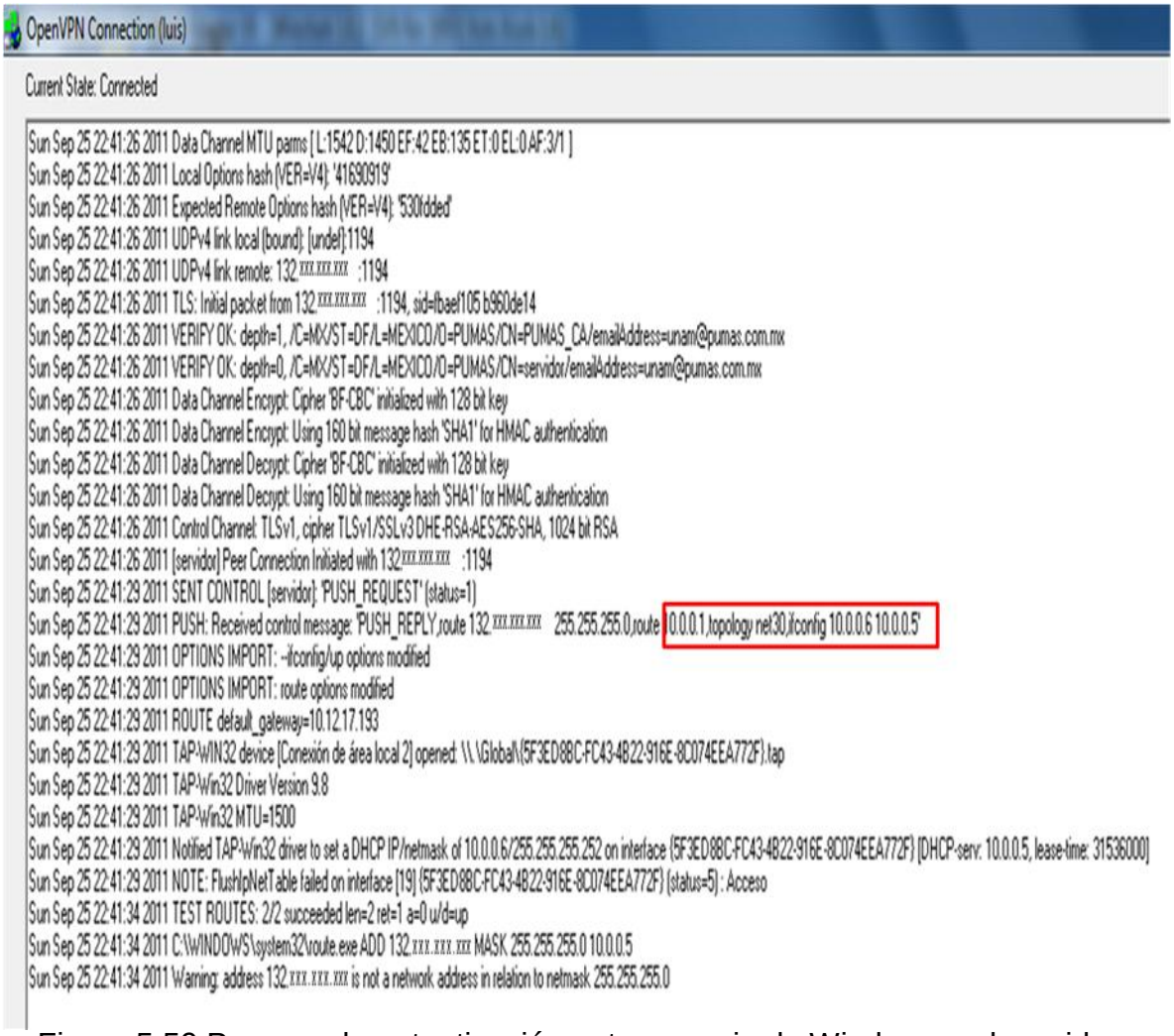


Figura 5.59 Proceso de autenticación entre usuario de Windows y el servidor OpenVPN

Para poder ver que ya se está dentro de la red VPN, se utilizó un servicio de identificación de IPs como www.myip.es, donde se muestra la dirección del nodo a la cual se está conectando (Figura 5.60).

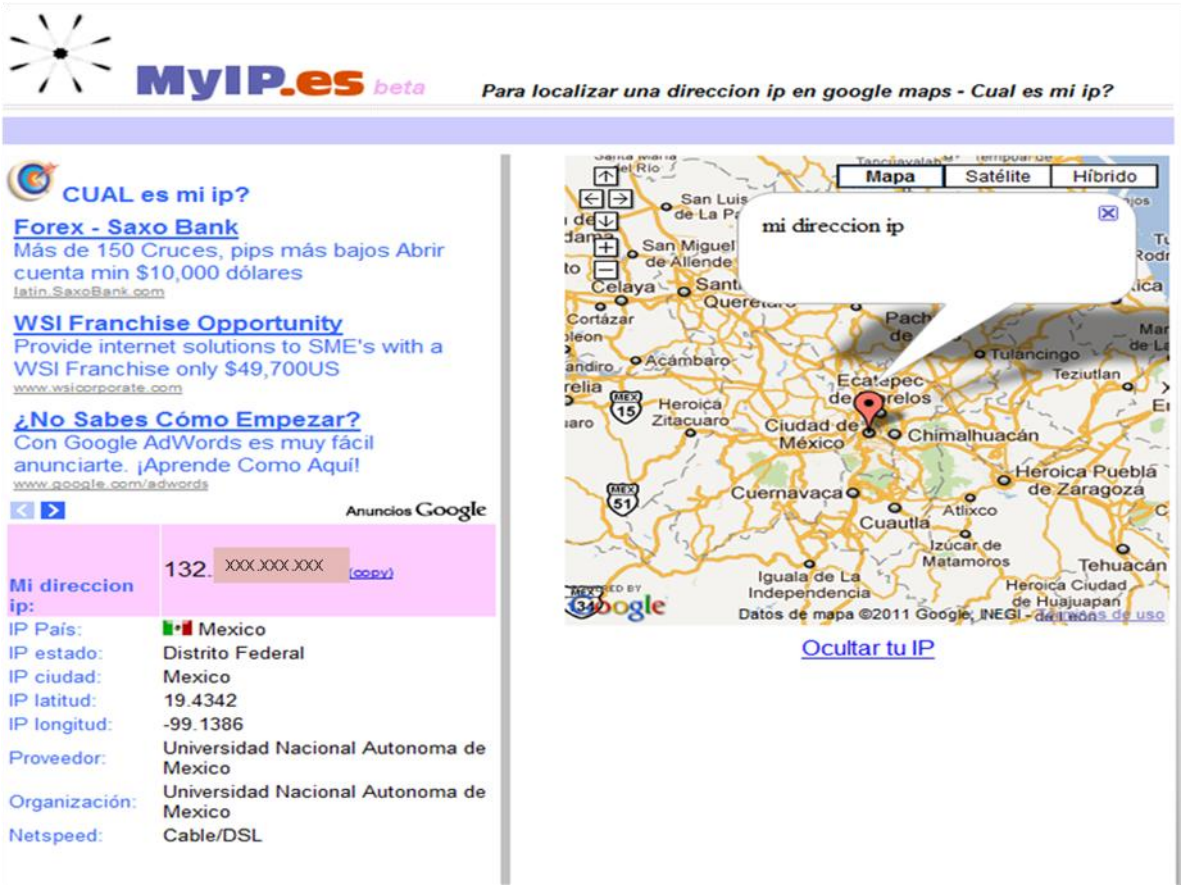


Figura 5.60 www.myip.es muestra la dirección del nodo a la cual se está conectando

Otra forma de comprobar la conectividad entre el cliente en Windows con el servidor, fue haciendo un ping a la dirección del servidor para ver la comunicación remota que había entre los dos equipos (Figura 5.61)

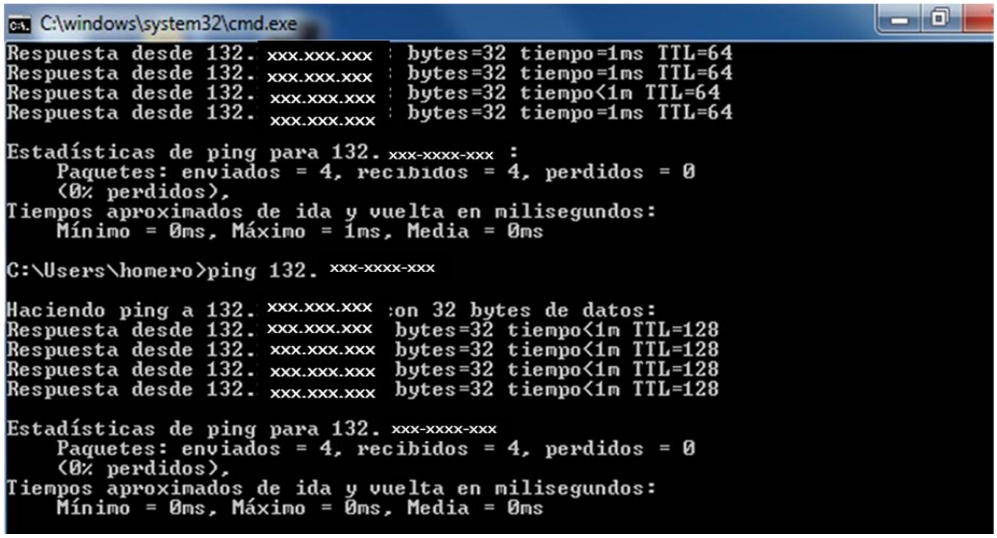


Figura 5.61 Verificación de la comunicación entre el cliente y el servidor OpenVPN

En lo que se refiere al cliente de Linux, se hace una prueba similar, haciendo un ping a la dirección del servidor como se muestra en la figura 5.62.

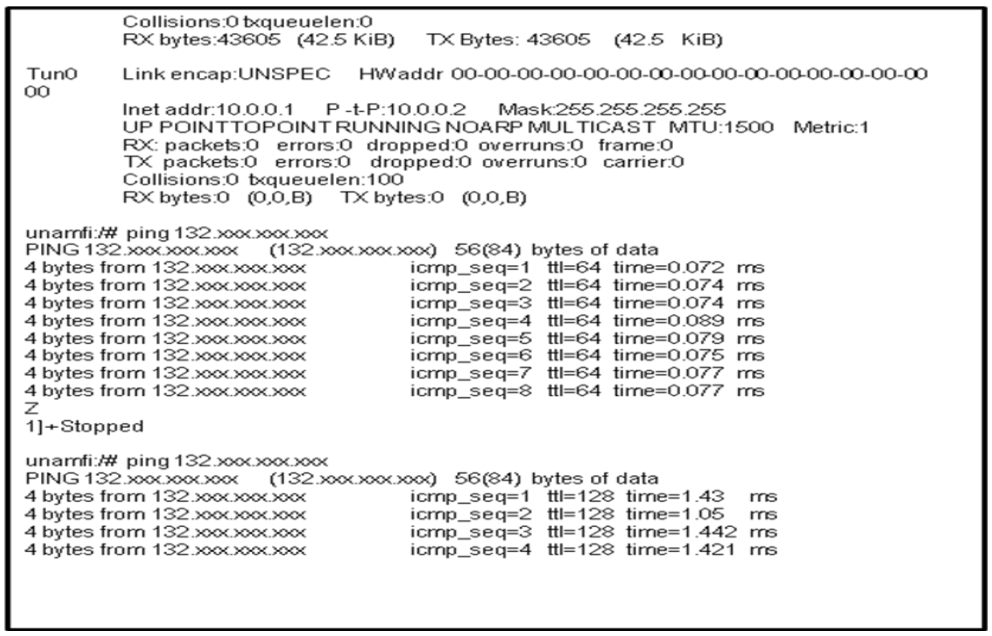
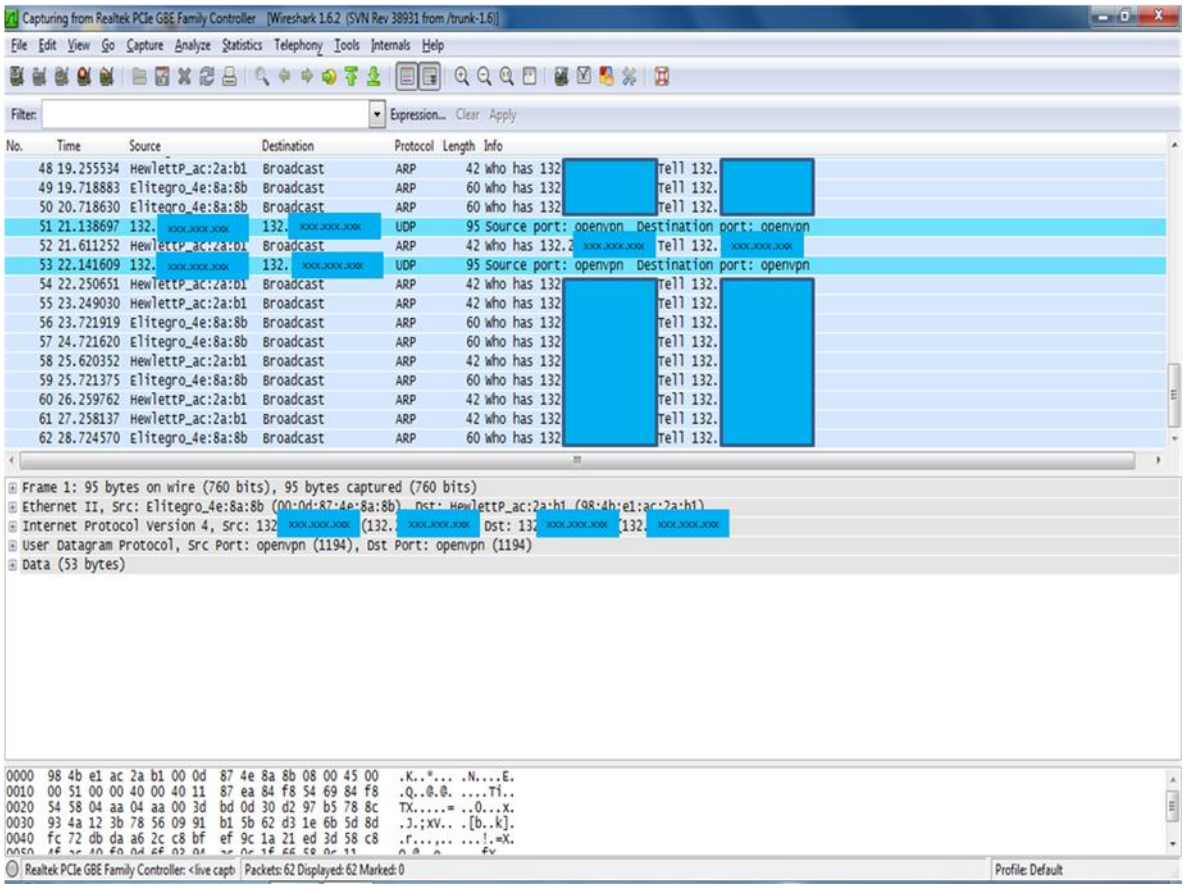


Figura 5.62 Verificación de la comunicación entre el cliente Linux y el servidor OpenVPN

Una vez verificado el funcionamiento del servidor, se activa el servicio de OpenVPN en Debian tecleando el comando cd /etc/init.d/openvpn start

Al tener comunicación con el servidor y una vez insertado el nombre de usuario y contraseña para acceder a éste, es posible acceder a los archivos compartidos por el servidor para ser empleados desde cualquier lugar. Cabe aclarar que para que el usuario acceda desde cualquier sitio, debe tener configurado todas las instrucciones mencionadas anteriormente, pues será por medio del túnel que se podrá autenticar.

Otro de los programas de apoyo que se utilizó fue el wireshark, este software funciona en las 2 plataformas sin ningún problema (Linux y Windows). En la figura 5.63 se muestra la captura de paquetes que se obtiene con el escaneo de red en el mismo entorno, en ella observa la dirección del servidor y la del equipo cliente.



5.63 Captura de paquetes en Wireshark

La función de OpenVPN es tener acceso a la red interna de una empresa en donde se quiere hacer uso de archivos que se van a consultar desde cualquier lugar, logrando así tener una herramienta útil en donde además de consultar archivos, es posible resguardarlos en otra computadora ajena a la empresa, estando previamente registrados los datos desde el servidor.

El servidor y los clientes que están en conexión con el servidor OpenVPN cuentan con un firewall para permitir la activación de los puertos y los accesos que tendrá cada usuario a los recursos, minimizando vulnerabilidades y amenazas.

La figura 5.64 muestra la conexión final que hubo entre el usuario y el servidor OpenVPN en Linux, esta comunicación se realizó de manera exitosa puesto que ambos equipos contaron con las configuraciones requeridas a lo largo de este capítulo.

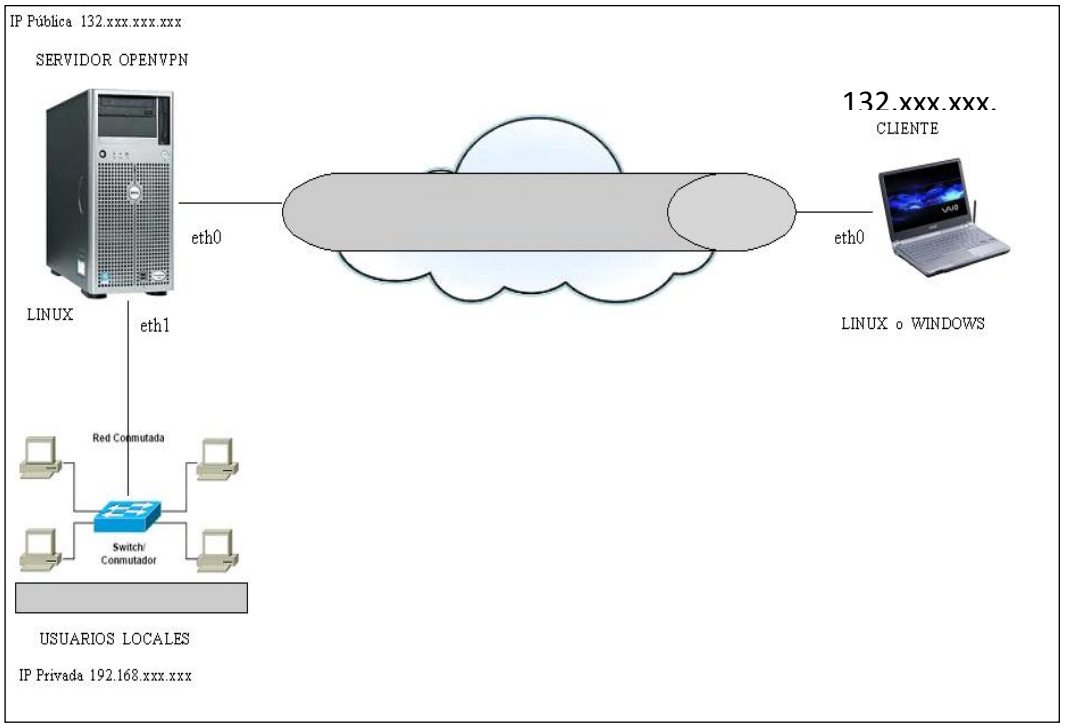


Figura 5.64 Conexión remota del usuario hacia el servidor OPENVPN

CONCLUSIONES

CONCLUSIONES

El proyecto de tesis se enfoca en la implementación de los mecanismos de seguridad de una VPN, en el cual dichos mecanismos tienen que permitir una conexión remota de manera segura y rápida, además de ofrecer seguridad para el usuario al momento de comunicarse con otro equipo.

Todo esto se logró con las indicaciones que se mostraron y las pruebas realizadas a lo largo de estos capítulos, logrando así una aportación importante en cuestión de seguridad, pues esto es una herramienta más que le permitirá al administrador de la red tener un mejor control de ella, específicamente al implementar y administrar una VPN, cifrando la información que es consultada y así ofrecerle al usuario integridad, confidencialidad y seguridad al momento de consultar algún archivo de dicha organización. Con estos mecanismos de seguridad implementados, se evitan o minimizan algunas vulnerabilidades que se pudieran presentar en el lugar.

Este proyecto tuvo éxito, ya que se pudieron hacer las conexiones que fueron planeadas al inicio de este trabajo, obteniendo una comunicación segura desde el servidor hacia los clientes y viceversa. Logrando así aumentar la movilidad y mejorar la productividad de los usuarios (alumnos /empleados).

Y todo esto se obtuvo usando técnicas de cifrado, un paquete llamado arno-iptables que incluía un firewall y por último un software llamado openvpn, que fue el que permitió enlazar 2 nodos que se encontraban en diferente área, conectándose de tal manera que pareciera que estaban en la misma LAN.

Otro de los procesos de seguridad realizado, fue el de habilitar pocos puertos, pues solo se habilitaron el de TCP, UDP, FTP, SSH y el puerto 1194, con eso se limita el acceso a otros sitios. La importancia de esto es que así se restringe el acceso a y desde cualquier otro puerto que pueda ocasionar alguna vulnerabilidad, ya que puede permitir el ingreso de algún código malicioso y como consecuencia se afecte al servidor.

Si bien el proyecto solo se realizó en el laboratorio, éste puede funcionar sin ningún problema en cualquier organización, solamente considerando una

mayor cantidad de clientes, llevando una configuración similar pero con base en las características y las peticiones de la organización, por ejemplo, se tendrían que habilitar otros puertos que utilice el cliente pero sin dejar vulnerable al servidor.

Es muy importante que se tome en cuenta el uso de una VPN, ya que se está ofreciendo integridad, confidencialidad y seguridad de los datos que transferimos a otro equipo, ese punto es muy importante para cualquier persona que quiere que su información esté segura e íntegra.

Por último, queremos mencionar que para una empresa u organización grande en donde se tenga que administrar a muchos clientes y de lugares muy lejanos, el uso de las VPN´s resultaría de gran ayuda por las ventajas mencionadas anteriormente y por el bajo costo que esto ocasionaría.

La implementación de VPN´s se están haciendo cada vez más frecuentes y quizás existan muchas herramientas de ayuda hoy en día, eso es bueno, pues cada vez se están preocupando muchos colegas por la protección de información de las personas, la importancia de contar con un proyecto como éste en el Laboratorio, además de ofrecer una herramienta más de seguridad en referencia a que el servidor esté protegido, es poder contar con una alternativa para compartir información, pues el profesor puede crear una carpeta compartida con los alumnos y que ellos consulten desde cualquier lugar sin ningún problema (previamente registrados en el servidor), ofreciéndoles seguridad, integridad, confidencialidad y rapidez al momento de transferir archivos. Otro punto importante de implementar el proyecto en el laboratorio es que el alumno se interese por proteger su información, que sepa cómo aplicar está herramienta, por si algún día se encuentra en un lugar que no cuente con medidas de seguridad el servidor, que pueda implementar dicho proyecto que además de ser de uso libre, logre consultar y trasferir archivos de manera segura desde cualquier punto donde se localice y que no se tengan que hacer muchos gastos en equipos de protección de red que ofrezcan lo mismo o menos que este proyecto.

CONCLUSIONES

En el ámbito profesional, la elaboración de éste trabajo deja una aportación importante ya que se le deja al laboratorio una herramienta más que pueda utilizar para su protección, así como que quede a la mano de los alumnos y que puedan consultarlo y servirles como base si es que necesitaran ayuda sobre algún tema de seguridad informática.

En el ámbito personal nos deja una satisfacción enorme poder realizar este trabajo, ya que nos involucramos más con los temas de seguridad informática, teniendo así un mayor conocimiento de lo que es una VPN y de las medidas de seguridad que deben existir en un servidor para que esté lo más protegido posible.

Trabajar con un compañero no es nada fácil ya que por los horarios de cada quien era muy difícil ajustar un horario para hacer las pruebas en el laboratorio, pero se logró hacer y queda claro que así será en futuras ocasiones cuando se deba trabajar en equipo, cada quien tendrá que poner de su parte para que el trabajo salga adelante.

APÉNDICE A

APÉNDICE A

ESTÁNDARES INTERNACIONALES

Redes inalámbricas (802.11)

Conocido también como WIFI, es una familia de estándares, especificaciones o protocolos de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y enlace de datos), especificando las normas de funcionamiento en una WLAN.

Se han desarrollado diversas especificaciones en esta familia debido a que han surgido nuevas necesidades para utilizar los medios más adecuados para lograr la implementación de una red inalámbrica en cualquier lugar.

1) 802.11a

El protocolo IEEE 802.11a se aprobó en el año de 1999. El estándar 802.11a , utiliza el mismo juego de los protocolos que tiene el estándar original 802.11, tiene una banda ancha de 5 Ghz y utiliza 52 subportadoras OFDM (Orthogonal Frequency – Division Multiplexing_ Frecuencia Ortogonal Multiplexando la División) con una velocidad máxima de 54 Mbit/s.

Utilizar la banda de 5 Ghz representa una ventaja del estándar 802.11a, dado que presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, porque restringe el uso de los equipos con este protocolo 802.11a; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como el estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

2) 802.11b

El estándar 802.11b es también un complemento del estándar 802.11; fue ratificado el mismo día que el estándar 802.11a en septiembre de 1999, con el fin de presentar mejoras y cambios al estándar 802.11.

Una WLAN (Wíreless Local Area Network _ Red de Área Local Inalámbrica) que constituye un sistema de comunicaciones de datos implementada como una extensión de una red local cableada dentro de un edificio o campus. Las redes WLAN combinan la conectividad hacia la red de datos con la movilidad del usuario. La IEEE 802.11b define dos componentes; una estación inalámbrica NIC (Network Interface Card _ Tarjeta de Red Inalámbrica), y un AP(Access Point - Punto de Acceso), el cual actúa como puente entre la estación inalámbrica y la red cableada.

3) 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo en el comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre del 2003. El 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de radares y satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU (Internacional Telecommunication Union - Unión de las Telecomunicaciones Internacionales) que fueron movidas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó que los convenientes para minimizar el impacto de abrir la banda de 5 Ghz, utilizada generalmente por sistemas militares.

4) 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación 802.11g. Que es la evolución del estándar 802..11b, éste utiliza la banda de 2.4 Ghz al igual que el estándar 802.11b, pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22 Mbit/s de velocidad real de trasferencia, similar a la del estándar 802.11a.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue el día 20 de junio del 2003. Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 Km con antenas parabólicas apropiadas.

5) 802.11n

En enero de 2004, IEEE anunció la formación de un grupo de trabajo 802.11 para desarrollar una nueva revisión del estándar 802.11n. La velocidad real de transmisión podría llegar a los 600 Mbps, y debería ser hasta 100 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input – Multiple Output _ Entrada Mu̶últiple – Salida Múltiple), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.

6) 802.11e

Las aplicaciones en tiempo real son ahora una realidad por las garantías QoS (Quality of Service -Calidad de Servicio) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC (Media Access Control Address - Dirección de Control

de Acceso al Medio) para soportar los servicios que requieren garantías de calidad de servicio. Para cumplir con su objetivo, IEEE 802.11e introduce un nuevo elemento llamado HCF(Hybrid Coordination Function - Función de Coordinación Hiíbrida) con dos tipos de acceso: EDCA (Enhanced Distributed Channel Access - Acceso al Canal Distribuido Enlazado) y HCCA (Controlled Access - Accesos Controlados)

7) 802.11 Super G

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz, alcanza una velocidad de transferencia de 108 Mbps. Esto es proporcionado por el chipset Atheros.

8) 802.11i

Está dirigido para combatir la vulnerabilidad actual en la seguridad de los protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Temporal Key Integrity Protocol - Protocolo de Claves Integrales, Seguras y Temporales) es también llamado hashing de las claves WPA2, WPE, WPA, incluyen mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricas y AES (Advanced Encryption Standard - Estándar de Cifrado Avanzado).

9) 802.11w

El estándar 802.11w está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envían la información del sistema en tramas desprotegidas, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas maliciosos. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red.

GLOSARIO

3DES	Estándar de Cifrado de Datos Triple (Triple Data Encryption Estándar). 3DES es un algoritmo de cifrado de clave simétrica implementado en 1990 y basado en DES, ya que al bloque de entrada de datos (64 bits) le son aplicadas tres iteraciones sucesivas de dicho algoritmo. 3DES parte de una clave inicial de 128 bits, la cual es dividida en dos claves diferentes de 64 bits.
A	
ACK	ACKNOWLEDGEMENT (ACK) (en español acuse de recibo), en comunicaciones entre computadoras, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.
AES	Estándar de Cifrado Avanzado (Advanced Encriyption Estándar). Es un algoritmo de cifrado de clave simétrica, adoptado como estándar en el año 1997 por el Instituto Nacional de Estándares y Tecnología, con base en una convocatoria pública lanzada a la comunidad científica internacional.
AH	Cabecera de Autenticación (Authentication Header). Proporciona autenticación e integridad de datos calculando un resumen sobre los paquetes a enviar, pero en cambio, no ofrece confidencialidad.
AMENAZA	Una amenaza es todo aquello que intenta o pretende destruir.
ANTENA	Dispositivo diseñado con el objetivo de emitir o recibir ondas electromagnéticas hacia el espacio libre.
C	
CHROOT	chroot en un sistema operativo Unix es una operación que cambia el directorio raíz, afectando solamente al proceso actual y a sus procesos hijos. "chroot" se refiere a la llamada de sistema chroot(2) o al programa ejecutable chroot(8).
D	
DEMONIO	Un demonio, daemon o dæmon (de sus siglas en inglés *Disk And Execution MONitor*), es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Este tipo de programas se ejecutan de forma continua (infinita), aunque se intente cerrar o matar el proceso, éste continuará en ejecución o se reiniciará automáticamente. Todo esto sin intervención de terceros y sin dependencia de consola alguna.

DHCP	DHCP (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de *host*) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.
DSA	Algoritmo de Firma Digital (Digital Signature Estándar). Sistema de firma digital adoptado como estándar por la organización de estándares de EEUU.
E	
ESP	Encapsulating Security Payload. Protocolo incluido dentro de IPv6 que realiza un cifrado de la información para garantizar la confidencialidad.
F	
FILEZILLA	FileZilla es un cliente FTP multiplataforma de código abierto y software libre, licenciado bajo la Licencia Pública General de GNU. Soporta los protocolos FTP, SFTP y FTP sobre SSL/TLS (FTPS).
FIREWALL	Dispositivo hardware o software que filtra tráfico a nivel de red y con base en unas determinadas reglas.
FTP	Protocolo de Transferencia de Ficheros (File Transfer Protocol). Protocolo perteneciente al nivel de aplicación y utilizado para transferir archivos entre diferentes equipos, ubicados éstos en redes basadas en TCP/IP. Por defecto, FTP emplea los puertos TCP 20 (Flujo de datos entre el cliente y el servidor) y 21 (transmisión de comandos de control).
G	
GUI	La interfaz gráfica de usuario, conocida también como GUI (del inglés *graphical user interface*) es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz. Su principal uso, consiste en proporcionar un entorno visual sencillo para permitir la comunicación con el sistema operativo de una máquina o computadora.

H	
HRU	El modelo de seguridad HRU (Harrison, Ruzzo, Ullman modelo) es un sistema operativo de nivel modelo de seguridad informática que se ocupa de la integridad de los derechos de acceso en el sistema. Es una extensión del modelo de Graham-Denning, en torno a la idea de que un conjunto finito de los procedimientos estén disponibles para editar los derechos de acceso de un sujeto *s* sobre un objeto *o.* Lleva el nombre de sus tres autores, Michael A. Harrison, Walter L. Ruzzo y Jeffrey D. Ullman.
HTTP	Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol). Protocolo del nivel de aplicación utilizado para la transacción de páginas o elementos web. Para ello, el cliente envía peticiones TCP al puerto 80 (por defecto) del servidor.
HUB	Concentrador elemental en una red Ethernet, que retransmite los datos que recibe de una estación a todas las démas estaciones que se encuentran conectadas en él.
I	
IDE	La interfaz ATA (Advanced Technology Attachment) o PATA, originalmente conocida como IDE (Integrated device Electronics), es un estándar de interfaz para la conexión de los dispositivos de almacenamiento masivo de datos y las unidades ópticas que utiliza el estándar derivado de ATA y el estándar ATAPI.
IEEE	Corresponde a las siglas de (Institute of Electrical and Electronics Engineers) en español Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en informática, ingenieros en biomédica, ingenieros en telecomunicación e ingenieros en Mecatrónica.
INFORMACIÓN	Se entiende por información a todo mensaje (conjunto de datos) que al receptor le interese, lo entienda o lo ignore antes de recibirlo.
INTEGRIDAD	Característica que asegura que la información enviada a través de un canal de comunicación inseguro no haya sido alterada durante su transcurso, es decir, el mensaje a transmitr ha de ser exactamente el mismo en el origen y en el destino.

INTERNET	Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen, funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.
INTRANET	Es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales. El término intranet se utiliza en oposición a Internet, una red entre organizaciones, haciendo referencia por contra a una red comprendida en el ámbito de una organización.
IP	Protocolo de Internet (Internet Protocol). Protocolo no orientado a conexión utilizado para la comunicación de datos a través de una red de paquetes conmutados.
IPSEC	Protocolo de seguridad de internet (Internet Protocol Security). Entorno de estándares abiertos basados en el protocolo IP, que ofrecen servicios de autenticación, cifrado e integridad de datos para asegurar las comunicaciones a través de dicho protocolo.
IPX	Intercambio de paquetes entre redes (Internetwork Packet Exchange). Protocolo de red no orientado a conexión, empleado para enviar y recibir informacion entre las distintas máquinas de una red Novell.
ISDN	Integrate Services Digital Network (Red Digital de Servicios Integrados). Red desarrollada por los operadores de telecomunicaciones con la intención de sustituir el sistema telefónico analógico por uno digital que permita integrar nuevos servicios (transmisión de voz, vídeo, datos).
K	
KERNEL	El núcleo o kernel (de la raíz germánica *Kern*) es un software que constituye la parte más importante del sistema operativo. Es el principal responsable de facilitar a los distintos programas, acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos a través de servicios de llamada al sistema.

L	
LOG	Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.
LZO	Lampel-Ziv-Oberhummer. Librería de comprensión de datos diseñada para comprimir y descomprimir en tiempo real.
O	
OUTSOURCING	Outsourcing es el proceso en el cual una firma identifica una porción de su proceso de negocio que podría ser desempeñada más eficientemente y/o más efectivamente por otra corporación, la cual es contratada para desarrollar esa porción de negocio. Esto libera a la primera organización para enfocarse en la parte o función central de su negocio.
P	
PAM	Módulo de Autenticación Enlazables (Pluggables Authentication Modules). Conjunto de módulos que se emplearán en el momento de validar el acceso a las diversas funciones y aplicaciones de un sistema operativo de tipo Unix.
PKI	Infraestructura de Clave Pública (Public Key Infraestructure). Conjunto de protocolos, servicios y estándares globales que soportan aplicaciones basadas en criptografía de clave pública. Ofrece registro, almacenamiento, selección y recuperación de claves, revocación de certificados digitales y evaluación de la confianza.
POLÍTICA	Una política representa el marco de referencia para la realización de las acciones que se deben emprender en una empresa en un periodo de tiempo. La política debe incluir tres cosas: “qué se debe hacer, cómo hacer para llegar a hacerlo y la medida empleada para evaluar lo que se ha hecho hecho”.
PPP	Protocolo de Punto a Punto (Point to Point Protocol). Protocolo que permite establecer una comunicación a nivel de enlace entre dos computadoras, a través de una línea síncrona o asíncrona.
PPTP	Protocolo de Túnel Punto a Punto (Point to Point Tunneling Protocol). Protocolo que permite la transferencia segura de datos desde el equipo remoto a una red corporativa, creando para ello una red privada virtual sobre una red física de datos TCP/IP. La conexión de control se realiza sobre el puerto 1723 (TCP).
PS	Comando del sistema operativo Unix. El comando ps muestra por pantalla un listado de los procesos que se están ejecutando en el sistema.

PSH	PSH es un bit que se encuentra en el campo del código en el protocolo TCP. Cuando PSH está activado indica que los datos de ese segmento y los datos que hayan sido almacenados anteriormente en el buffer del receptor deben ser transferidos a la aplicación receptora lo antes posible. A veces llegan varios segmentos que transportan datos y no tienen activado el bit PSH; el receptor almacenará esos datos pero no los entregará a la aplicación receptora hasta que reciba un segmento con el PSH activado. Con el bit a 1 está activado y a 0 desactivado.
Q	
QOS	QoS o Calidad de Servicio (*Quality of Service*, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.
R	
RJ45	RJ-45 (*registered jack 45*) es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). Es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho pines o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.
ROUTER	Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.
RSA	(Rivest, Shamir, Adleman). Algoritmo criptográfico asimétrico basado en una pareja de claves (pública y privada). Que pueden ser utilizadas al mismo tiempo tanto para cifrar una comunicación como para autenticar a sus participantes.
RTC	Red Telefónica Conmutada. Sistema de comunicación diseñado inicialmente para la transmisión de datos a tráves de un fax o un módem analógico.
S	
SA	Asociación de Seguridad (Security Association). Acuerdo unidireccional entre los participantes de una VPN, referido a los métodos y parámetros empleados en la estructura del túnel destinados éstos a garantizar la seguridad de los datos transmitidos.

SERIAL ATA	*Serial Advanced Technology Attachment* es una interfaz de transferencia de datos entre la placa base y algunos dispositivos de almacenamiento, como puede ser el disco duro, lectores y regrabadores de CD/DVD/BR, Unidades de Estado Sólido u otros dispositivos de altas prestaciones que están siendo todavía desarrollados. Serial ATA sustituye a la tradicional Parallel ATA o P-ATA. SATA proporciona mayores velocidades, mejor aprovechamiento cuando hay varias unidades, mayor longitud del cable de transmisión de datos y capacidad para conectar unidades al instante.
SLIP	El protocolo SLIP (Serial Line Internet Protocol) es un estándar de transmisión de datagramas IP para líneas serie, pero que ha quedado bastante obsoleto. Fue diseñado para trabajar a través de puerto serie y conexión de módem. SLIP se ha sustituido por el PPP (Point-to-Point Protocol) cuyo diseño es superior, tiene más y mejores características y no requiere de la configuración de su dirección IP antes de ser establecido. Sin embargo, con microcontroladores, se sigue utilizando el modo de encapsulación de SLIP para paquetes IP ya que usa cabeceras de tamaño reducido.
SOCKET	Un socket (enchufe), es un método para la comunicación entre un programa del cliente y un programa del servidor en una red. Un socket se define como el punto final en una conexión. Los sockets se crean y se utilizan con un sistema de peticiones o de *llamadas de función* a veces llamados interfaz de programación de aplicación de sockets (API, application programming interface).
SSH	Interfaz de Usuario Segura (Secure Shell). Protocolo que permite la autenticación y el intercambio de información a través de un canal seguro entre distintas máquinas de la red. Generalmente se emplea el puerto TCP 22 como puerto destino de la conexión.
SWITCH	Concentrador en una red Ethernet, que retransmite la información recibida sólo por el puerto al que se encuentra conectado el equipo al que va dirigida la información.
SYN	SYN es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión en el procedimiento de establecimiento de tres fases (3 way handshake). Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

T	
TUN	TUN o túnel es simplemente un enlace entre dos puntos a través de algún otro material. Una buena analogía es un túnel que pasa por debajo de una montaña. Ambos lados de la montaña están vinculados a través de un camino directo, en este caso la "montaña" es el Internet. Así que, esencialmente un túnel es un atajo directo a través de Internet.
U	
URL	Universal Resource Locator - Localizador de Recurso Uniforme. Sistema de direcciones que permiten identificar recursos dentro de internet (páginas web, servidores FTP, direcciones de correo).
V	
VPN	Red Privada Virtual (Virtual Private Network). Tecnología de red que permite una extensión de la red local sobre una red pública, como por ejemplo internet, con la peculiaridad de que la transmisión de datos se hace de manera privada, es decir, a tráves de unos elementos conocidos como túneles. Una VPN debe ser capaz de autenticar las comunicaciones, garantizar la integridad de la información transmitida y la confidencialidad de la misma.
W	
WINS	Servicio de nombres de internet de windows (Windows Internet Naming Service). Servidor de nombres para NetBIOS que mantiene una tabla de correspondecia entre las direcciones ethernet y los nombres de los ordenadores. Esto permite localizar rápidamente una computadora dentro de una red Windows.
WIRESHARK	Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

WPA	WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP. Los investigadores encontraron varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).
WPA2	WPA2 (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA, está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.
WPE	WEP, acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.
X	
XDSL	Se conoce como xDSL a la familia de tecnologías de acceso a Internet de banda ancha basadas en la digitalización del bucle de abonado telefónico (el par de cobre). La principal ventaja de xDSL frente a otras soluciones de banda ancha (cable módem, fibra óptica, etcétera) es precisamente la reutilización de infraestructuras ya desplegadas, por tanto más baratas al estar parcial o totalmente amortizadas y con gran extensión entre la población.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Capítulo 1

- GÓMEZ VEITES Álvaro, VELOSO ESPIÑEIRA Manuel. Redes de computadoras e internet. Madrid, Alfaomega, 2003.
- HERRERA PÉREZ, Enrique. Tecnologías y redes de transmisión de datos. México, Limusa, 2003.
- OLIFER, Natalia, OLIFER, Victor. Redes de Computadoras, MC Graw Hill, 2009.
- TANENBAUM, Andrew S. Redes de Computadoras. México, Pearson Educación, 2003.

Capítulo 2

- AREITIO Javier. Seguridad de la información, redes, informática y sistemas de información. Madrid, Paraninfo CENGAGE Learning, 2008.
- LÓPEZ BARRIENTOS, Jaquelina, QUEZADA REYES, Cintia. Apuntes de Seguridad Informática. México, Facultad de Ingeniería UNAM, 2005.

Capítulo 3 y 4

- ALONSO, Javier. Redes Privadas Virtuales. Madrid, Alfaomega, Primera edición, 2009.
- FEILNER Markus. Open VPN: Building And Operating Virtual Private Networks, Packt Publishing, 2006.
- LÓPEZ BARRIENTOS, Jaquelina, QUEZADA REYES, Cintia. Apuntes de Seguridad Informática. México, Facultad de Ingeniería UNAM, 2005.
- M. SURHONE Lambert. OpenVPN Virtual Private Network, Pre-shared Key, NetBSD, FreeBSD, OpenBSD, Linux, Solaris and Transport Layer Security,.Betascript, 2010.

REFERENCIAS ELECTRÓNICAS (Última revisión: 01/11/11 22:00 Hrs.)

Capítulo 1

- Topología Híbrida
  http://www.angelfire.com/cantina/alegre0/otrastopologias.htm
- Topología Malla
  http://abelperaza.tripod.com/malla.htm
- Conceptos Básicos de Redes
  http://www.monografias.com/trabajos30/conceptos-redes/conceptos-redes.shtml
- Modelo OSI
  http://www.arqhys.com/construccion/datos-capas.html
- Control de acceso al medio
  http://es.wikipedia.org/wiki/Control_de_Acceso_al_Medio
- Cable de Fibra Óptica
  http://es.wikipedia.org/wiki/Cable_de_fibra_%C3%B3ptica

Capítulo 2

- Ejemplo de Configuración con claves asimétricas en OpenVPN
  http://es.wikibooks.org/wiki/OpenVPN/Ejemplo_de_configuraci%C3%B3n_con_claves_asim%C3%A9tricas
- Diffie-Hellman
  http://es.wikipedia.org/wiki/Diffie-Hellman
- Algoritmos Simétricos
  http://en.wikipedia.org/wiki/Symmetric_encryption

Capítulo 3 y 4

- Definición de VPN
  http://www.ekontsulta.net/test/wiki/index.php/VPN

- Introducción a las Redes Privadas
  http://www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html
- Diccionario de comando de Linux
  http://infomatica.wordpress.com/comandos-linux/
- OpenVPN
  http://es.wikipedia.org/wiki/OpenVPN
- Foro de OpenVPN
  http://forum.pfsense.org/index.php/topic,29893.msg155139.html
- Sistema Operativo Debian
  http://debianlinux.blogcindario.com/2007/09/00005-ventajas-de-debian.html
- Virtual Private Network
  http://www.bellera.cat/josep/pfsense/openvpn_cs.html
- Configuración de un servidor VPN en Linux
  http://www.alcancelibre.org/staticpages/index.php/openvpn-clientes-win-linux-shorewall-P2
- OpenVPN en Windows
  http://www.redeszone.net/redes/openvpn-conectate-a-cualquier-red-de-forma-segura-mediante-openvpn-manual-para-gnulinux-y-windows-7-32bits-y-64bits-clienteservidor-ssltls/
- Tunel VPN
  http://www.tecnodelinglesalcastellano.com/2011/03/que-es-un-tunel-vpn-y-como-configurar.html
- Requerimientos de una VPN
  http://www.ekontsulta.net/test/wiki/index.php/VPN
- RFC 2246
  http://www.ietf.org/rfc/rfc2246.txt
- Firewalls de última generación Físicos
  http://www.sonicwall.com/mx/UTM_Firewall_VPN.html
- Netfilter para iptables
  http://www.netfilter.org/
- Openssl
  http://www.openssl.org/