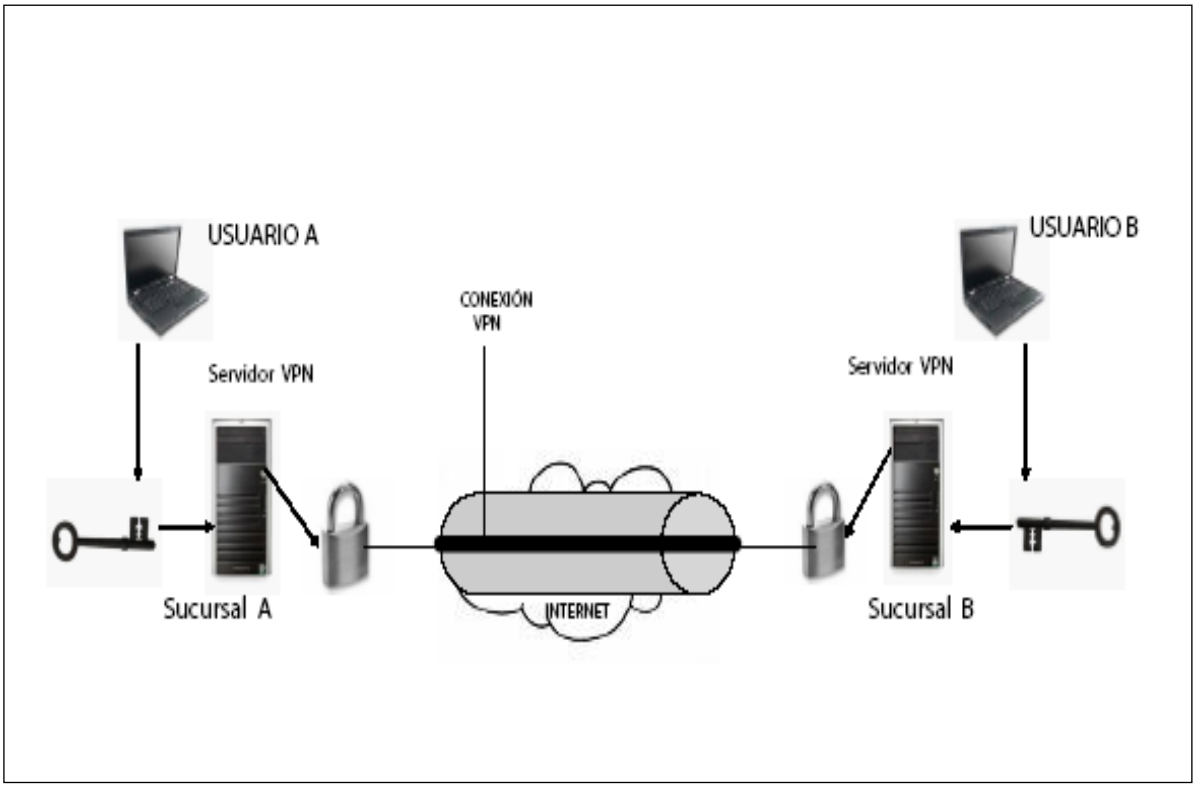
CAPÍTULO 4



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

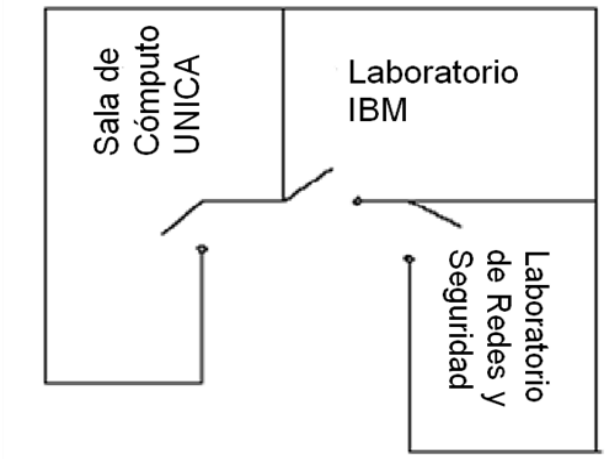


Figura 4.3 Ubicación del Laboratorio de Redes y Seguridad

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

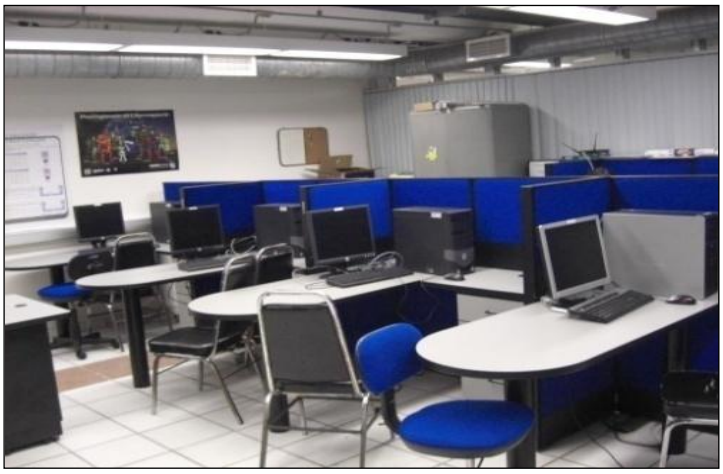


Figura 4.4 Equipo de cómputo

4.2 Metodología

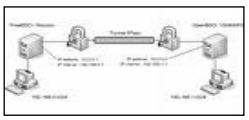
El siguiente paso para el diseño de una VPN, es la selección de la metodología. Es indispensable considerar que las metodologías se pueden clasificar en dos tipos:

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



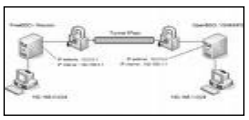
hacerlo. El modelo de la matriz de acceso se encarga de especificar quién eres y qué tienes permitido hacer.

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."**[1] 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

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

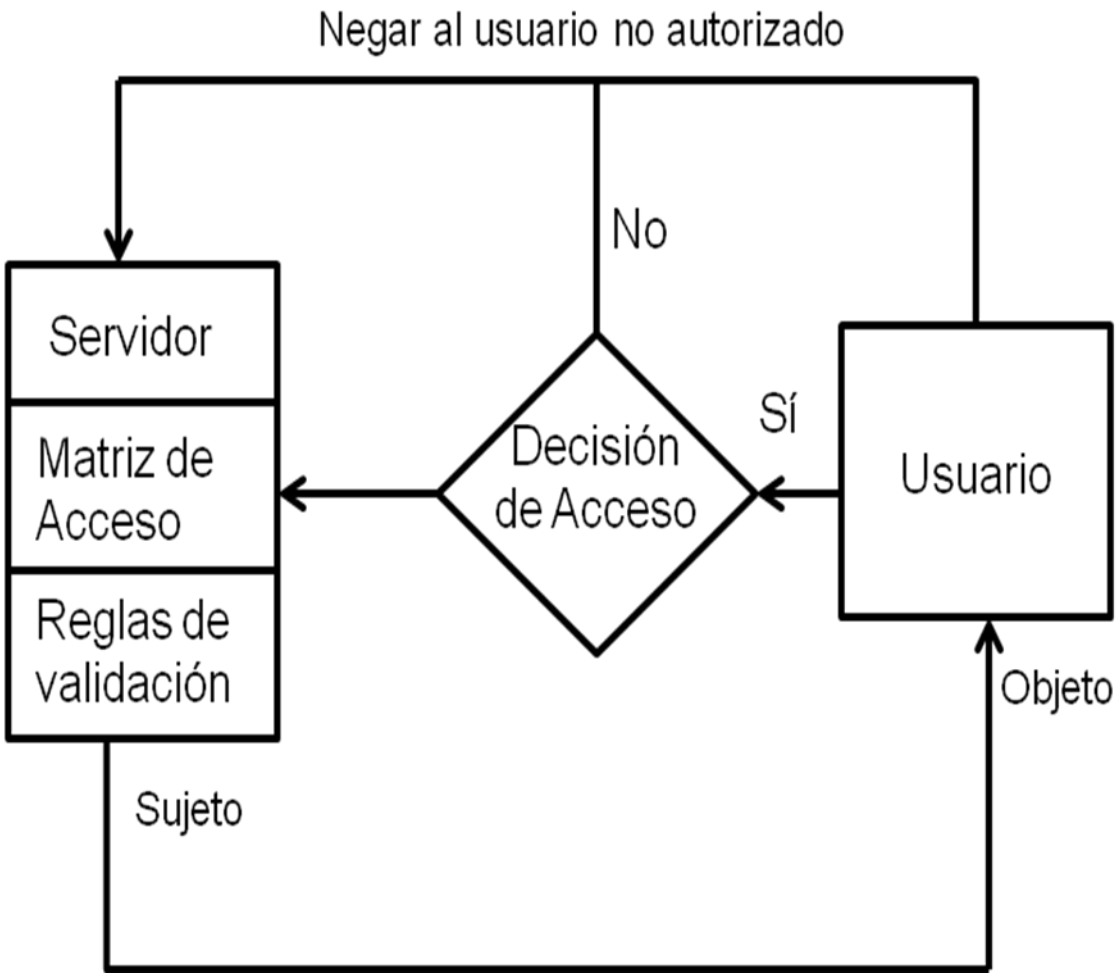
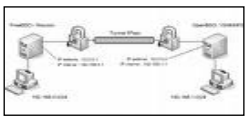


Figura 4.7 Modelo HRU

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.

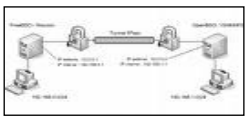
4.3 Selección del hardware

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.

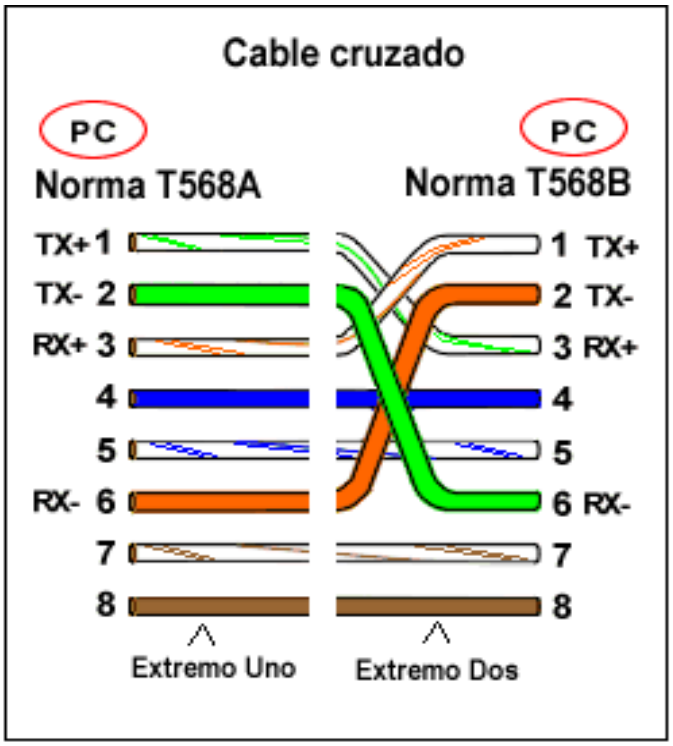


Figura 4.8 Configuración de colores de un cable cruzado

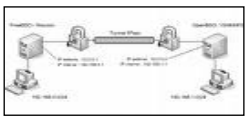
4.4 Sistema Operativo

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.

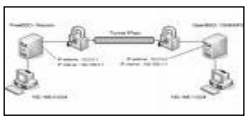
Algunos ejemplos de sistemas operativos son:

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

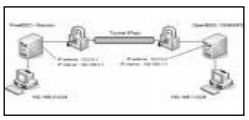
- AIX
- AMIX
- GNU / Hurd
- HP-UX
- Irix
- Minix
- System V
- Solaris
- UnixWare

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.

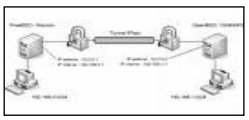
El sistema operativo está formado por una organización voluntaria con documentos fundadores.

- 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:

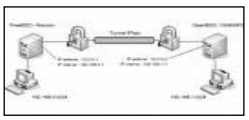
Un procesador: 700 MHz x86, una memoria RAM de 384 MB, un Disco Duro de 8GB, una tarjeta gráfica que soporte una gran resolución, un lector de CD-ROM, tarjeta de sonido y conexión a internet.

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.



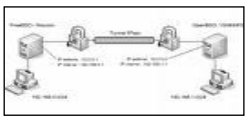
El direccionamiento IP dinámico se aplica en equipos de cómputo que cuenten con un proveedor de servicios de internet como por ejemplo infinitum, axtel, etcétera. Este tipo de servicios consiste en que al momento de conectarse a internet se le asigna una IP de manera automática, esto para indicar la 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.

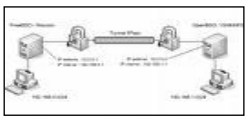
Para la toma de esta decisión, es necesario tener un control de acceso a los usuarios que tenga permisos de conexión remota a un servidor VPN, y así evitaremos problemas que otro usuario se conecta al mismo grupo de red virtual.

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



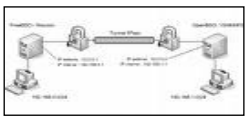
Estas herramientas se pueden instalar en diferentes plataformas de los sistemas operativos, debe tomarse en cuenta que cada herramienta tiene un proceso distinto para la instalación y la configuración, esto se debe a la diferencia de la arquitectura con la que cuenta cada sistema operativo en el equipo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

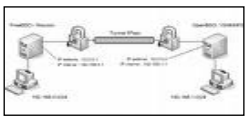
El protocolo SSL/TLS tiene un papel muy importante y es parte fundamental de la implementación de OpenVPN para mejorar los procesos de seguridad en las redes remotas con tecnología aceptada en todas las dependencias públicas y privadas.



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.

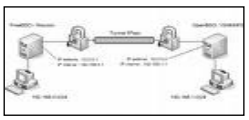
Los protocolos más conocidos son: IPSec, PPTP, SSL/TLS, L2TP, etcétera, estos protocolos indican los principales avances que han tenido las VPN's en el mercado tecnológico. Estos protocolos generan un túnel con la interfaz TUN, que generan el cifrado de datos para proteger la información de los usuarios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

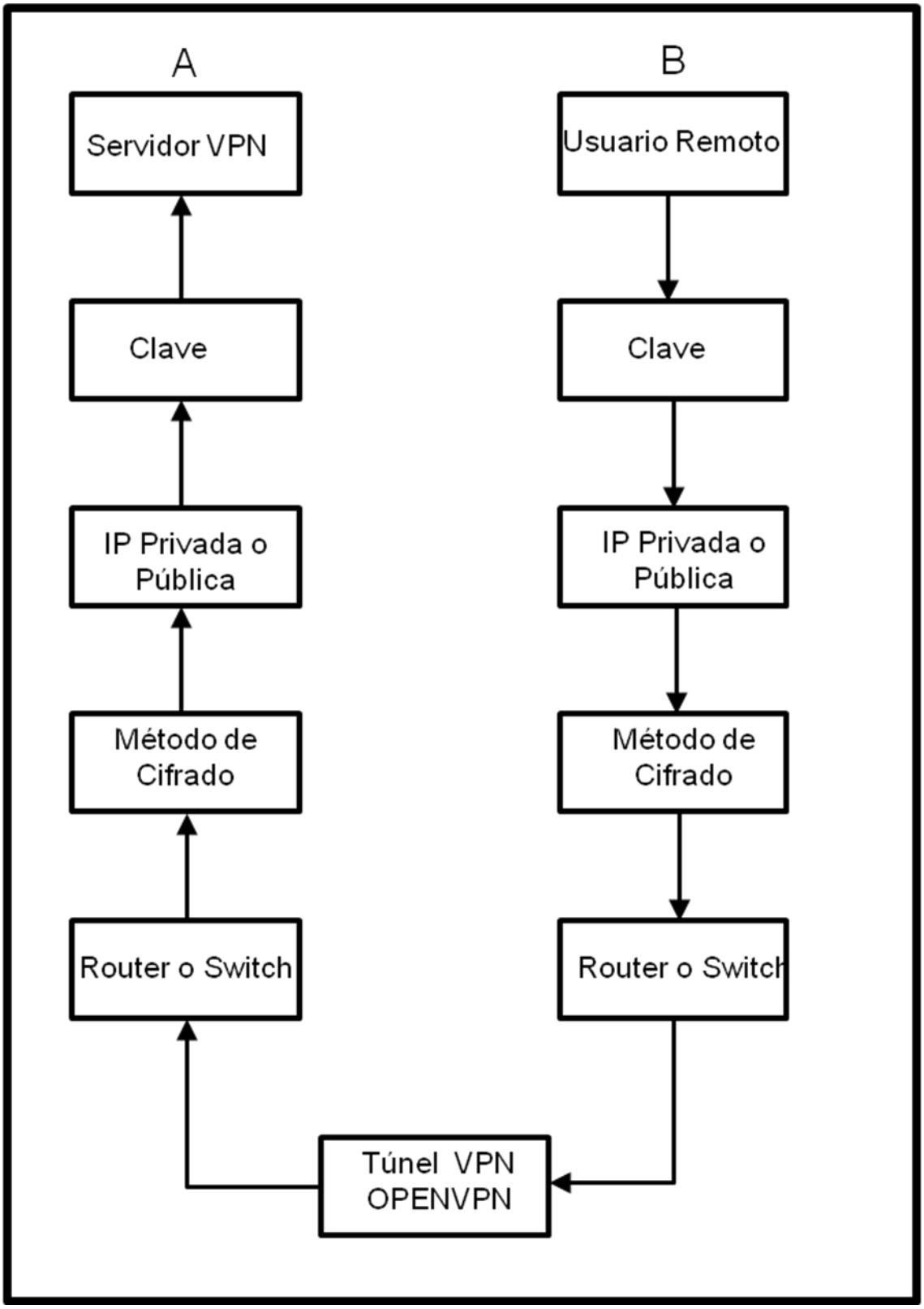
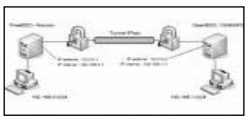


Figura 4.9 Estructura de una VPN de Cliente - Servidor



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.

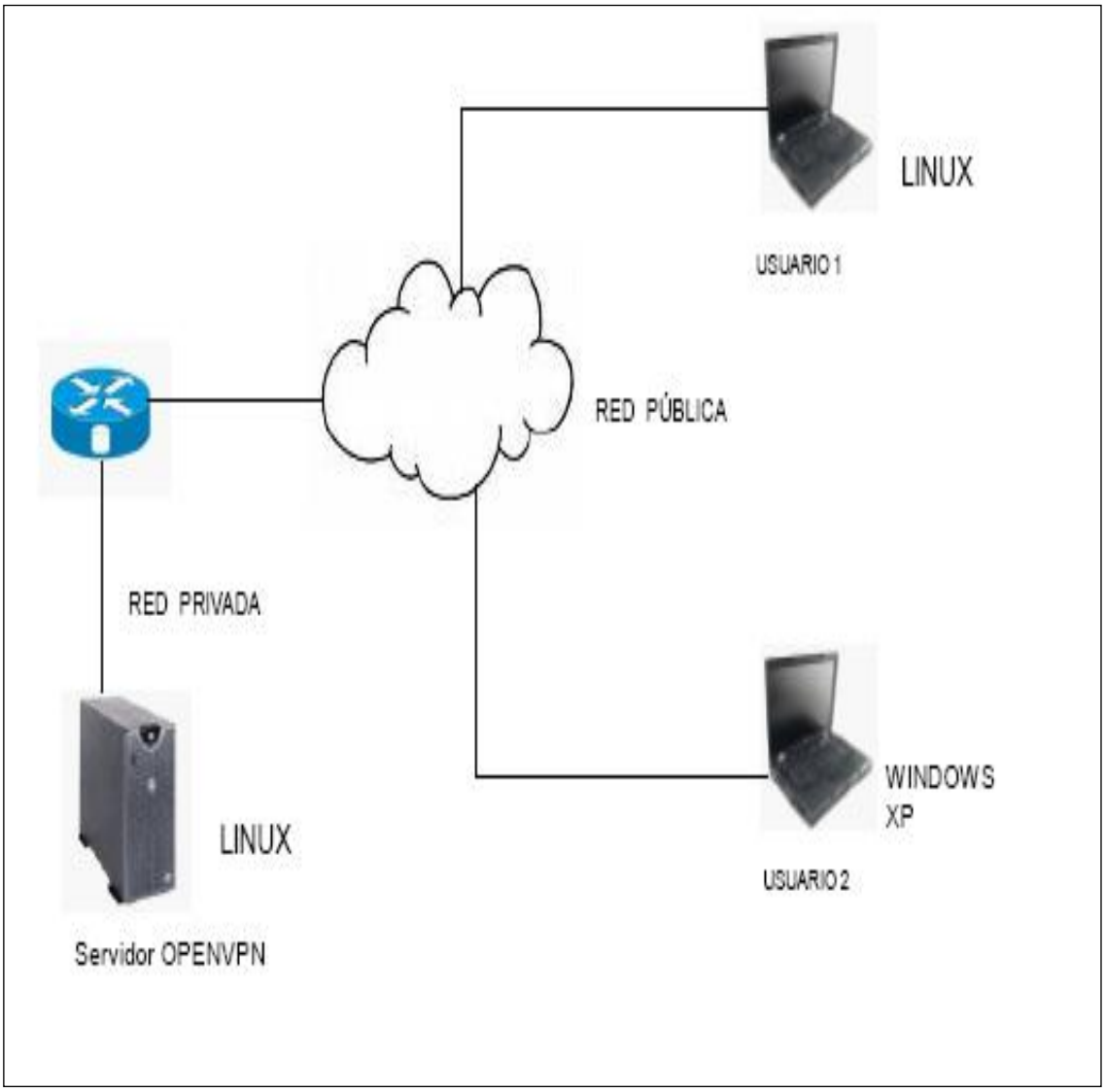


Figura 4.9 El modelo Cliente - Servidor