Universidad Luterana Salvadoreña

Facultad Ciencias del Hombre y La Naturaleza

Licenciatura en Ciencias de La Computación

Cátedra:

Redes II

Tema:
OpenVPN con GNU/Linux.

INTEGRANTES		**CARNÊ**
APELLIDOS	**NOMBRES**	
Durán Hernández	Carlos Ernesto.	DH01132367
Guadrón Benavides	César Ismael.	GB02110071
Melchor Mármol	Wilmer.	MM02110152

Catedrático: Ing.Manuel Flores Villatoro.

San Salvador, 15 de noviembre de 2014

INDICE

TEMA PÁG

INDICE DE ILUSTRACIONES

INTRODUCCIÓN.

En el presente trabajo describimos cada una de las actividades, que como grupo hemos realizado en el proyecto de Redes II, el cual consiste en la instalación, configuración e implementación de un servidor VPN con GNU/Linux, en el que integra un conjunto de aplicaciones que proporcionan la capacidad de ejecutar GNU/Linux cómo un servidor VPN desde equipos remotos que tengan acceso a Internet.

También se explican los procedimientos que hacen funcionar el servidor VPN, así como los distintos servicios y protocolos que en su conjunto hacen funcionar un servicio VPN, creando un túnel para el encapsulamiento de protocolos y autenticación de usuarios, logrando mayor seguridad en la conexión.

En este documento se muestra el diagrama de red a utilizar así como también el diagrama de GANT en el que se contempla las actividades realizadas durante el proyecto, y también se muestran las herramientas tangibles e intangibles a utilizar, tales como Hardware y Software.

1 OBJETIVOS.

Objetivo General.

Instalar y configurar una Red Privada Virtual o VPN, con sistemas operativos GNU/Linux.

Objetivos Específicos.

- ✓ Instalar y configurar OpenVPN para la configuración de la Red Privada Virtual con GNU/Linux.
- ✓ Configurar una PC como servidor VPN con GNU/Linux para clientes Windows y Linux.
- ✓ Crear certificados para servidor OpenVPN y cliente OpenVPN.
- ✓ Crear usuarios para OpenVPN.
- ✓ Realizar la conexión entre cliente/servidor OpenVPN.

2 MARCO TEÓRICO.

2.1 Red privada virtual.

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.[1] Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

2.2 Características básicas de la seguridad.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación.

- Autentificación y autorización:

  ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

- Integridad:

  De que los datos enviados no han sido alterados.

- Confidencialidad/Privacidad:

  Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

- No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.
- Control de acceso: Se trata de asegurar que los participantes autenticados tiene acceso únicamente a los datos a los que están autorizados.
- Auditoria y registro de actividades: Se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.
- Calidad del servicio: Se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.

2.3 Requisitos básicos.

- Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- Cifrado de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos si son interceptados. Esta tarea se realiza con algoritmos de cifrado como DESo 3DES que sólo pueden ser leídos por el emisor y receptor.
- Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.
- Nuevo algoritmo de seguridad SEAL.

3 TIPOS DE VPN

3.1 VPN de acceso remoto.

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

3.2 VPN punto a punto.

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

Tunneling.

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo

una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

3.3 VPN over LAN.

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

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

4 IMPLEMENTACIONES.

El protocolo estándar de factores el IPSEC, pero también están PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

- Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Fortinet,SonicWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen (Junipe r Networks), Symantec, Nokia, U.S. Robotics,D-link, Mikrotik, etc.

- Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, GNU/Linux y los Unix en general. Por ejemplo productos de código abierto como Open SSH, Open VPN y Free S/ Wan.

En ambos casos se pueden utilizar soluciones de firewall ('cortafuegos' o 'barrera de fuego', en castellano), obteniendo un nivel de seguridad alto por la protección que brinda, en detrimento del rendimiento.

5 VENTAJAS Y DESVENTAJAS

5.1 Ventajas.

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.
  - Nos permiten reducir los costos de interconexión de redes geográficamente distantes.
  - Ofrecen seguridad de acceso para los usuarios que se conectan via WiFi.
  - Nos permiten crear una capa extra de seguridad dentro de una red corporativa para proteger recursos informáticos sensibles.
  - Nos permiten acceder a los recursos de la red a la cual nos conectamos. Puede ser la red de nuestra empresa o la red de nuestra casa.
  - Nos permiten acceder a sitios web con contenido específico para cada país.
  - Nos permiten sobrepasar las restricciones de acceso a internet.
  - Ofrecen la posibilidad de navegar de manera anónima.
  - Funcionan con cualquier programa o aplicación.

5.2 Desventajas.

- La velocidad de acceso es menor al de una conexión tradicional.
- Es necesario contar con ciertos conocimientos técnicos para implementar una conexión VPN.
- La conectividad no es muy estable, por lo que suele ser necesario conectarse nuevamente cada vez que se necesite.
- No todos los equipos de red son compatibles entre sí al utilizar las tecnologías VPN.
- Una brecha en la seguridad del equipo remoto puede poner en riesgo los recursos de la red a la cual nos conectamos.

6 TIPOS DE CONEXIÓN.

6.1 Conexión de acceso remoto.

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

6.2 Conexión VPN router a router.

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentifica ante el router que realiza la llamada y también sirve para la intranet.

6.3 Conexión VPN firewall a firewall.

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

7 DIAGRAMA DE RED VPN.

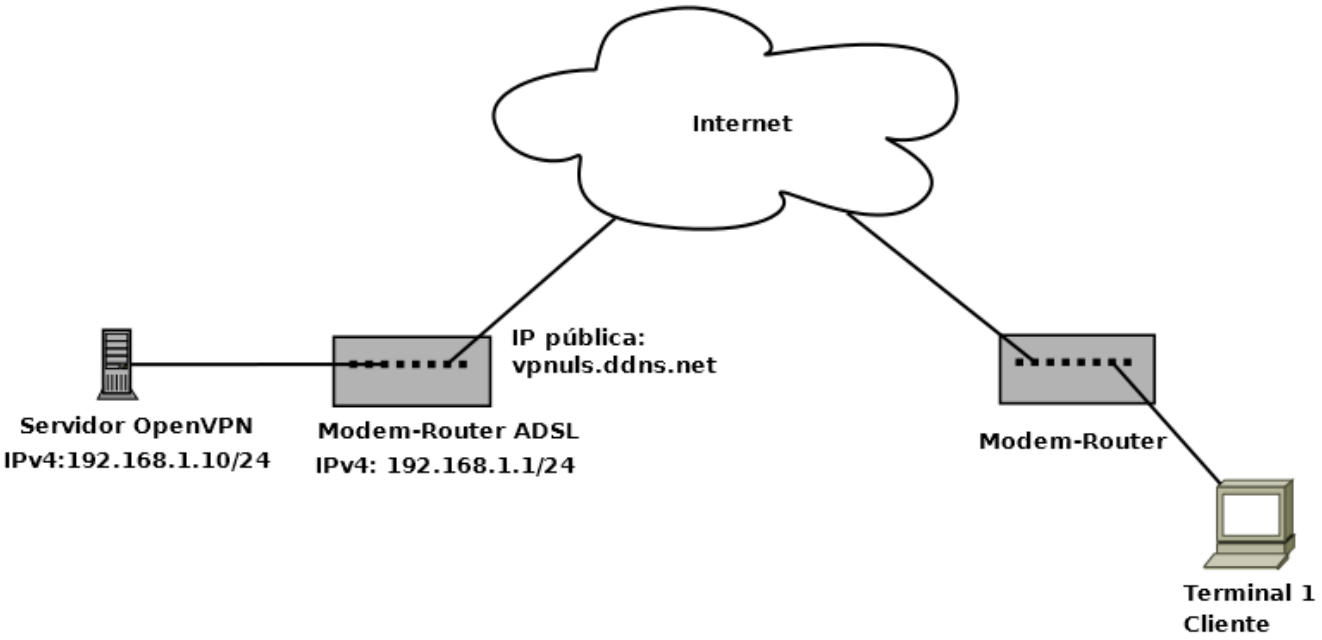


Ilustración 1 Diagrama de Red

8 HERRAMIENTAS DE TRABAJO.

- ✓ Sistema operativo GUN/Linux, como servidor VPN.
- ✓ Clientes (cualquier computadora que tenga acceso a internet).
- ✓ Modem Router ADSL.
- ✓ Tarjetas de red inalámbricas.
- ✓ Cables de red directos categoría 5e o superior.
- ✓ Crimpadora.

9 DESCRIPCIÓN DEL TRABAJO.

El proyecto de Redes II, consta de la configuración de un servidor VPN, con el cual se pretende acceder remotamente por medio de una red virtual al servidor que se ejecuta en un sistema GNU/Linux, que será ejecutado por los clientes que tengan acceso a Internet.

Con el Servidor VPN (Virtual Prívate Network), se puede acceder remotamente desde cualquier parte del mundo con solo tener acceso a Internet y con un nivel de seguridad y autenticación para acceder al servidor VPN.

El proyecto será realizado instalando el servidor VPN utilizando la versión del software libre Debian de GNU/Linux 7.6 wheezy estable, en la que se harán las configuraciones necesarias para el correcto funcionamiento así como también se configurara un Switch para el re direccionamiento y liberación de puertos.

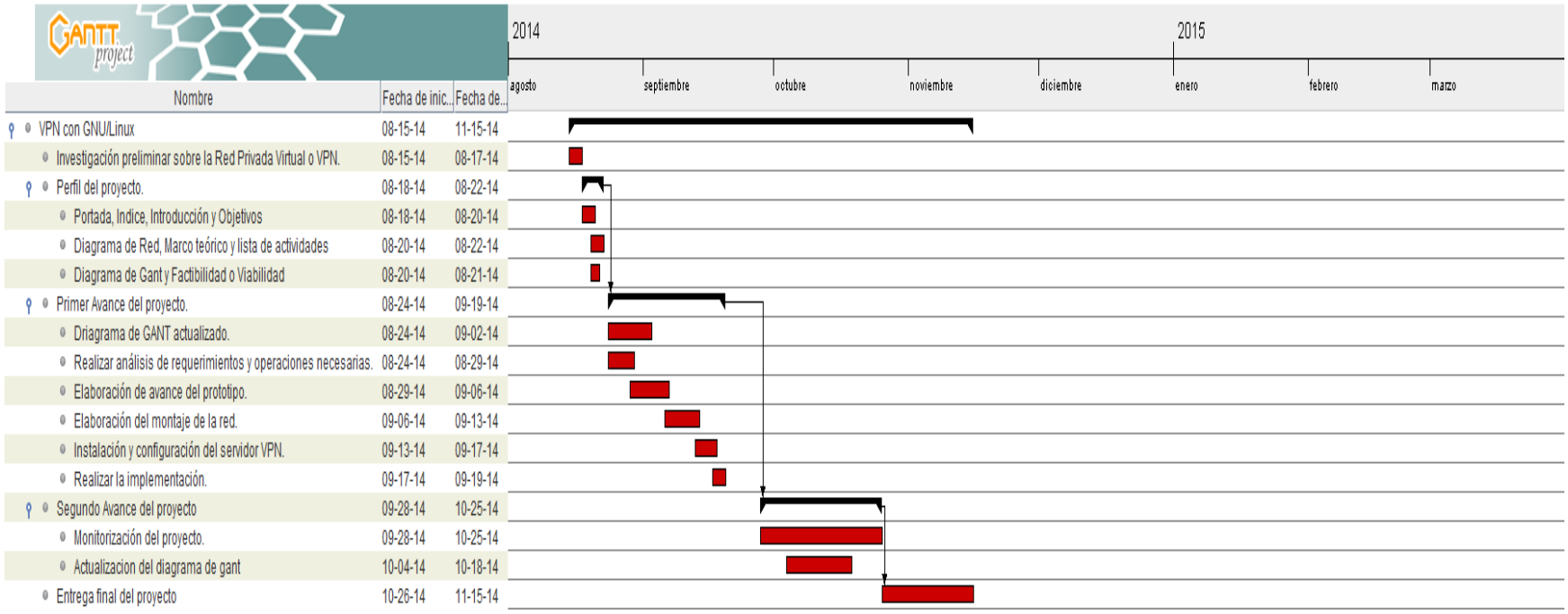
Pasos generales del proyecto:

- ✓ Instalación de sistema operativo GNU/Linux.
- ✓ Instalación y configuración del servidor OpenVPN con GNU/Linux.
- ✓ Configuración del Router para el correcto funcionamiento.
- ✓ Pruebas y monitoreo.

10 LISTA DE ACTIVIDADES.

- ✓ Investigación preliminar sobre la Red Privada Virtual (VPN) u OpenVPN.
- ✓ Elaboración de perfil de proyecto.
- ✓ Elaboración del primer avance del proyecto.
- ✓ Realizar análisis de requerimientos y operaciones necesarias.
- ✓ Elaboración de avance del prototipo.
- ✓ Realizar la implementación.
- ✓ Elaboración del montaje de la red.
- ✓ Instalación y configuración del servidor OpenVPN.
- ✓ Elaboración del segundo avance del prototipo.
- ✓ Monitorización del proyecto.
- ✓ Implementación y entrega final del proyecto.

11 DIAGRAMA DE GANTT.



Nombre	Fecha de inic...	Fecha de...
VPN con GNU/Linux	08-15-14	11-15-14
Investigación preliminar sobre la Red Privada Virtual o VPN.	08-15-14	08-17-14
Perfil del proyecto.	08-18-14	08-22-14
Portada, Indice, Introducción y Objetivos	08-18-14	08-20-14
Diagrama de Red, Marco teórico y lista de actividades	08-20-14	08-22-14
Diagrama de Gant y Factibilidad o Viabilidad	08-20-14	08-21-14
Primer Avance del proyecto.	08-24-14	09-19-14
Driagrama de GANT actualizado.	08-24-14	09-02-14
Realizar análisis de requerimientos y operaciones necesarias.	08-24-14	08-29-14
Elaboración de avance del prototipo.	08-29-14	09-06-14
Elaboración del montaje de la red.	09-06-14	09-13-14
Instalación y configuración del servidor VPN.	09-13-14	09-17-14
Realizar la implementación.	09-17-14	09-19-14
Segundo Avance del proyecto	09-28-14	10-25-14
Monitorización del proyecto.	09-28-14	10-25-14
Actualizacion del diagrama de gant	10-04-14	10-18-14
Entrega final del proyecto	10-26-14	11-15-14

Actividades Realizadas. Actividades Pendientes.

Ilustración 2 Diagrama de Gant.

12 FACTIBILIDAD DEL PROYECTO.

Analizaremos la disponibilidad de los recursos necesarios para llevar a cabo los objetivos y metas señalados. A raíz del tipo de proyecto que estamos presentando hemos determinado las siguientes factibilidades:

12.1 FACTIBILIDAD TÉCNICA.

Al hacer la investigación sobre las tecnologías existentes sobre Redes Privadas Virtuales o VPN, se hizo la recolección de la información sobre los componentes y equipos tecnológicos necesarios para llevar a cabo el proyecto de VPN con GNU/Linux.

De acuerdo con los componentes necesarios para la implementación del servidor VPN, se hizo la evaluación con respecto a dos enfoques (Hardware y software).

En cuanto al hardware, los componentes necesarios para la implementación del servidor VPN son los siguientes:

Servidor:
Procesador Pentium 4 de 2.0 GHZ o superior.
Tarjeta madre.
RAM 2GB o Más.
Disco Duro 320 o más.
Tarjeta de red integrada o PCI Ethernet 10/100 Mbps. O superior.
Monitor, Teclado y Mouse.

Clientes.

- Puerto para conexión de teclado
- Puerto para conexión de mouse
- Puerto de red Ethernet 10/100 Mbps
- Puerto para conexión de monitor
- Dos puertos USB 2.0.
- Tarjeta madre.
- Monitor.
- Teclado.
- Mouse.

Tomando en cuenta los requerimientos y habiendo evaluado el hardware con el que se dispone, es factible técnicamente la implementación del proyecto.

En cuanto al software:

Se pretende utilizar un sistema operativo GNU/Linux, como por ejemplo Debian o una distribución derivada de la misma ya sea Ubuntu o Linux min, etc.

Como resultado del estudio técnico realizado, se determinó que se cuenta con los requerimientos básicos en cuanto al hardware y software necesarios para la implementación del servidor VPN.

12.2 FACTIBILIDAD OPERATIVA.

Según el estudio de factibilidad operativa y el análisis realizado podemos determinar que se cuenta con los conocimientos necesarios y básicos para poder implementar el proyecto de VPN con GNU/Linux.

Además es necesario el apoyo de otros recursos como bibliográficos, digitales y la web, entre otros, para poder implementar el proyecto y así lograr determinar que la implementación es factible operativamente.

12.3 FACTIBILIDAD ECONÓMICA.

Según el estudio de factibilidad económica y el análisis realizado podemos determinar económicamente con los recursos con los que se cuenta y con los que se necesitan para poder desarrollar el proyecto de Redes Privadas Virtuales o VPN:

Recursos disponibles:

- ✓ Una computadora con sistema operativo GNU/Linux utilizado como servidor VPN.
- ✓ Dos computadoras que servirán como clientes con acceso a Internet.
- ✓ Servicio de Internet.

RECURSOS NECESARIOS DE ADQUIRIR		
RECURSOS	**COSTOS**	**CANTIDAD**
Cable UTP categoría 5e o superior	$ 0.50 yd	1
Conectores RJ45	$ 0.15	5
Crimpadora	$ 12	1
Switch Fast Ethernet	$ 20	1

13 CONCLUSIÓN.

En conclusión se muestra el proceso para desarrollar la implementación de un Servidor OpenVPN con GNU/Linux, que consiste en el uso de redes virtuales privadas a través de protocolos para hacer un túnel entre ellos y así hacer un acceso remoto a través de Internet.

Como grupo se llegó a la conclusión, que el perfil que se muestra contiene las generalidades básicas para la instalación y configuración de una VPN, así como también la utilización de la misma en el que se muestra los objetivos del proyecto, los cuales se cumplieron y se ponen en manifiesto en la culminación del mismo. El cual es de suma importancia porque en él se puede plasmar las ideas principales realizadas en el proyecto e identificar si el mismo es viable o factible y así desarrollar la configuración de OpenVPN en GNU/Linux.

.

14 BIBLIOGRAFÍA.

REFERENCIA 1.

Autor: Wikipedia.

Título: Red Privada Virtual.

URL: http://es.wikipedia.org/wiki/Red_privada_virtual

Fecha de Consulta: 20/08/2014.

REFERENCIA 2.

Autor: Web Adicto.

Título: ¿Qué es una Red Privada Virtual VPN? - Ventajas, Desventajas y Herramientas

URL:http://webadicto.net/post/Redes-Privadas-Virtuales-VPN-Ventajas-Desventajas-y-Herramientas

Fecha de Consulta: 22/08/2014.

REFERENCIA 3.

Título: **Configurar OpenVPN Roadwarrior en Debian 6 y Windows**

Fecha de creación: 23 de noviembre 2011

URL: http://www.tech-nico.com/blog/configurar-openvpn-roadwarrior-con-debian-6-y-windows/

Fecha de consulta: 10 de noviembre 2014