UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

LICENCIATURA EN CIENCIAS DE LA COMPUTACION

CATEDRATICO:

MANUEL VILLATORO

MATERIA:

REDES II

PROYECTO

VPN CON GNU/LINUX

PRESENTADO POR:

INTEGRANTES

APELLIDO	NOMBRE	CARNET	NOTA
FLORES TORRES	HENRY EDENILSON	FT02110600	
ALVARADO FUNES	ROBERTO VLADIMIR	AF02110290	

FECHA DE ENTREGA:

SABADO 15 NOVIEMBRE DE 2014

Índice de contenido

INTRODUCCION

En el presente trabajo se manifiesta la descripción de la configuración de un VPN con GNU/Linux el cual consiste en la extensión de una red local segura, que es diferenciada de la red pública por su seguridad y alto nivel de confianza. Les detallamos los tipos de VPN que existen, las ventajas y los tipos de implementaciones que posee esta red.

La red VPN es muy segura al usarla porque permite una confianza en la red local, de manera que tiene beneficios a la hora de implementarla y como en este caso lo haremos con GNU/Linux la red permite que la computadora envié y reciba datos dinámica mente sobre redes compartidas o publicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada esto se realiza el estableciendo una conexión de tanto la computadora cliente como el servidor teniendo en cuanta la nube de internet y el envió de paquetes cifrados.

Algo muy importante de esta red VPN es que se utiliza tecnología de túnel la cual permite que la transmisión de datos y paquetes sea de manera favorable, ya que este en la red usa un proceso de encapsulación y posteriormente pasa a un estado de que los datos son encriptados para no ser vistos por otros usuarios en la red pública.

Esta tecnología es muy útil para establecer redes que se extienden en áreas geográficas extensas, por ejemplo en diferentes ciudades o en otro sector donde se monta la red. Con la configuración del VPN se muestran muchas ventajas entre ellas están la seguridad y la accesibilidad a datos que estén en otro sector de la red, y esta información viaja en paquetes encriptados en la red para quien intercepte estos paquetes no tenga acceso.

En la configuración se presentar los tipos de implementaciones en la cual hay varios que se pueden ejecutar en el proyecto, veremos la viabilidad del proyecto y los costos estimados en la realización.

OBJETIVOS

OBJETIVO GENERAL.

- Presentar la configuración y como se implementa un VPN con GNU/Linux.

OBJETIVOS ESPECIFICOS.

- Mostrar las ventajas en la implementación de un VPN con GNU/Linux.
- Detallar los tipos de VPN y los diferentes protocolos que se pueden implementar.

MARCO TEORICO

¿QUE ES UNA VPN?

(Virtual Private Network) es una extensión de una red local y privada que utiliza como medio de enlace una red publica. A demás es posible utilizar otras infraestructuras como WAN tales como Frame Relay, ATM, etc.

Este método permite enlazar dos o más redes simulando una única red privada permitiendo así la comunicación entre computadoras como si fueran punto a punto. También un usuario remoto se puede conectar a una LAN utilizando una conexión VPN, y de esta manera utilizar aplicaciones, enviar datos, etc. de manera segura.

Las redes privadas virtuales utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, esto es importante a la hora de diferenciar Redes Privadas Virtuales y Redes Privadas, ya que esta ultima utiliza líneas telefónicas dedicadas para formar la red. Una de las principales de una VPN es la seguridad, los paquetes viajan a través de infraestructuras públicas (Internet) en forma encriptado y a través del túnel de manera que sea prácticamente ilegible para quien intercepte estos paquetes. Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas entre las cuales podemos mencionar ciudades, países y continentes.

VENTAJAS DE UNA VPN:

1. Seguridad: provee encriptación y encapsulamiento de datos de manera que hace que estos viajen codificados y a través de un túnel.
2. Costo: ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.
3. Mejor Administración: cada usuario que se conecta puede tener un número de IP dinámicamente si así se requiere.
4. Facilidad: para los usuarios con poca experiencia para conectarse a grandes redes corporativas transfiriendo sus datos de forma segura.

TIPOS DE VPN:

Las formas en que deben implementar las VPNs pueden ser basadas en HARDWARE o a través de SOFTWARE, pero lo más importante es el protocolo que se utiliza para la implementación.

Las VPNs basada en HARDWARE utilizan básicamente equipo dedicados como por ejemplo los router, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del microprocesador para brindar otros servicios, en concreto podemos decir: los equipos dedicados son los de fácil implementación y buen rendimiento, solo que las desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son PROPIEDADES.

EXISTEN DIFERENTES TECNOLOGIAS PARA ARMAR VPNs

- DLSW: Data Link Switching (SNA over IP).
- IPX: for Novell Netware over IP.
- GRE: Generic Routing Encapsulation.
- ATMP: Ascend Tunnel Management Protocol.
- IPSEC: Internet Protocol Security Tunnel Mode.
- PPTP:Point to Point Tunneling Protocol.
- L2TP: Layer To Tunneling Protocol.

Entre los más usados y con mejor rendimiento estarían IPSEC y PPTP, aunque a este último se le conocen fallas de seguridad.

• IPSEC (Internet Protocol Secure)

Es un protocolo de seguridad creado para establecer comunicaciones que proporcionen confidencialidad e integridad de los paquetes que se transmiten a través de internet. Ipsec tiene dos métodos para brindar seguridad, EOS (Encapsulating Security Payload) o HA (Authentication Header).

La diferencia entre ESP y AH es que el primero cifra los paquetes con algoritmos de cifrado definidos y los auntentica.
AH la firma digitalmente los paquetes asegurándose la identidad del emisor y receptor, el Ipsec tiene dos tipos de funcionamiento. Uno es el modo transporte en el cual la encriptación se produjo de extremo a extremo por lo que todas las maquinas de la red deben soportar Ipsec, y el otro es el modo túnel, en el cual la encriptación se produce solo entre routers de cada red. Esta ultima forma seria la más ordenada de organizar una red VPN basada en Ipsec.

• PPTP (Point to Point Tunneling Protocol):

Este es uno de los protocolos mas populares y fue originalmente diseñado para permitir el transporte (de modo encapsulado) de protocolos diferentes al TCP/IP a través de internet. Esto fue desarrollado por el foro PPTP (el cual está formado por tres empresas: Ascend Communications, Microsoft Corporation y robotics que ahora es conocida como 3 Com)hp
.
básicamente PPTP lo que hace es encapsular los paquetes del protocolo punto a punto PPP (Point to Point Protocol) que a su vez ya vienen encriptados en un paso previo para poder enviarlo a través de la red.
El proceso de encriptado es gestionado por PPP y luego es recibido por PPTP, este ultimo hace una conexión TCP llamada conexión TCP llamada conexión de control para crear el túnel y una versión modificada de la encapsulación de Enrutamiento Genérico (GRE, Generic Routing Encapsulation) para enviar los datos en formato de diagramas IP, que serian paquetes PPP encapsulados desde el cliente al servidor y viceversa.

El proceso de autenticación de PPTP utiliza los mismos métodos que usa PPP al momento de establecer una conexión. El método de encriptación que utiliza PPTP es el Microsoft Point to Point Encryption , MPPE, y solo es posible su utilización cuando se emplea CHAP (o MS-CHAP en los NT) como medio de autentificación.
MPPE trabaja con claves de incriptacion de 40 a 128 bits, la clave de 40 bits es la que cumple con todos los estándares, en cambio la de 128 bist está diseñada para su uso en Norte America. Cliente y servidor deben de emplear la misma codificación, si un servidor requiere de más seguridad de la que soporta el cliente, entonces el servidor rechaza la conexión.

HAY VARIAS POSIBILIDADES DE CONEXIÓN VPN.

Esto es definido según los requerimientos de la organización, por eso es aconsejable hacer un buen relevamiento a fin de obtener datos como por ejemplo si lo que se quiere enlazar son dos o más redes, o si solo se conectaran usuarios remotos.

A. CLIENTE A SERVIDOR (Client to Server)

Un usuario remoto que solo necesita servicios o aplicaciones que corren en el mismo servidor VPN.

B. DE CLIENTE A RED INTERNA (Client to LAN).

Un usuario remoto que utiliza servicios o aplicaciones que se encuentran en uno o más equipos dentro de la red interna.

C. DE RED INTERNA A RED INTERNA.

Esta forma supone la posibilidad de unir dos intranets a través de dos enrutadores, el servidor VPN en una de las intranets y el cliente VPN en la otra. Aquí entran en juego el mantenimiento de tablas de ruteo y enmascaramiento.

REQUERIMIENTOS PARA EL ARMADO DE UN VPN.

Para el correcto armado de un VPN, es necesario cumplir con una serie de elementos y conceptos que a continuación se detallan:

- Tener conexión a internet: ya sea por dirección IP dedicada, ASDL o dial-up.
- Servidor VPN: básicamente es una computadora conectada a internet esperando por conexiones de usuarios VPN y si estos cumplen con el proceso de autentificación, el servidor aceptara la conexión y dará acceso a los recursos de la red interna.
- Cliente VPN: este puede ser un usuario remoto o un enrutador de otra LAN.
- Asegurarse que la VPN sea capaz de:
    1. Encapsular los datos.
    2. Autentificar usuarios.
    3. Encriptar los datos.
    4. Asignar direcciones IP

¿QUE ES OPENVPN?

OpenVPN es un programa muy flexible para crear redes privadas virtuales (VPN). La idea es crear una red privada, sobre una red pública (Internet). Para asegurar que la red es privada se utiliza conexiones encriptadas, y los paquetes de red reales, se encapsulan en otros que van por Internet.

Vamos a configurar OpenVPN del modo RoadWarrior con PKI (Public Key Infraestructure) Un claro ejemplo para explicar el modo RoadWarrior: Son 1 o mas clientes que se conectan (autenticándose) de manera remota desde una PC hacia nuestro "linux OpenVPN Server", y utilizando internet como medio de acceso para ingresar de manera segura a los recursos de la empresa, como serian, un servidor de aplicaciones, mail, recursos compartidos, etc.

Nota: roadWarriod significa (Modo guerrero de la carretera

Primero debemos saber cual es nuestro ip en esa pc, lo podemos saber poniendo el comando ifconfig

DESCRIPCION DEL PROYECTO

en el presente documento se establecerá una conexión de un cliente remoto a una red local por medio del VPN para hacer un envió de información en forma protegida de manera que no pueda ser leída si alguien intersecta el paquete. Esta es una de las formas como una persona puede conectarse de manera segura en cualquier parte del mundo siempre que disponga de un acceso a Internet en pocas palabras pueda obtener una IP publica.

En el mundo actual es importante poder estar comunicado pero mas aun poder tener a la mano los datos, aplicaciones u otros programas que se encuentren en el servidor donde se realiza la conexión.

Con el VPN se puede tener acceso seguro a tus datos personales que posees en la empresa sin necesidad de estar cerca y lo mas importante de forma que nadie mas pueda optar ver la información.

El proyecto se elaborara con el objetivo de establecer conexiones entre clientes y redes locales conocidas también como intranet utilizando el VPN y el PPTP para elaborar la configuración de dichas maquinas que se establecerán como servidor y clientes.

GUIA DE INSTALACION DEL VPN

La configuración Road to Warrior (Host to LAN mediante túnel) permitirá que múltiples dispositivos u ordenadores se puedan conectar simultáneamente a nuestra red VPN y compartir recursos e informaciones con la red a que se conectan. Por lo tanto en este caso tenemos varios clientes que se pueden conectar de forma independiente al servidor VPN.

INSTALACIÓN DEL SERVIDOR

La instalación del servidor la vamos a realizar en un sistema operativo Debian Wheezy. La totalidad del procedimiento descrito tiene que funcionar en cualquier distribución que derive de Debian como

pueden ser Ubuntu, Crunchbang, Linux Mint, Kubuntu, etc.

Para instalar el servidor OpenVPN lo primero que tenemos que hacer es abrir una terminal. Dentro de la terminal teclean el siguiente comando:

sudo apt-get install openvpn openssl

CREAR UNA AUTORIDAD DE CERTIFICACIÓN

OpenVPN es un protocolo de VPN basado SSL/TLS mediante certificado y clave RSA creadas mediante openssl. Por lo tanto el nivel de seguridad proporcionado por OpenVPN es muy elevado. Al ser un protocolo que funciona bajo certificados y claves necesitaremos crear una autoridad de certificación para a posteriori generar los certificados.

La principal función de una autoridad de certificación es la de emitir y revocar certificados digitales para terceros. Para quien necesite más información puede consultar el siguiente enlace.

Crear el certificado raíz ca para firmar y revocar los certificados de los clientes

Para poder emitir y revocar la claves necesitamos crear nuestra propia autoridad certificadora y disponer de nuestro certificado raíz ca.ctr y de nuestra clave ca.key para poder crear y firmar las claves de los clientes y del servidor.

Para realizar este paso, y el resto de pasos, ejecutoriaremos los scripts que OpenVPN trae incorporados de serie. Para ello tenemos que crear una carpeta con nombre easy-rsa dentro de la ubicación /etc/openvpn.

Para ello abrimos una terminal y tecleamos el siguiente comando:

cd /etc/openvpn

mkdir easy-rsa

Seguidamente tenemos que copiar los scripts de configuración de OpenVPN, que se hallan en la ubicación /usr/share/doc/openvpn/examples/easy-rsa/2.0/, dentro de la carpeta easy-rsa que acabamos de crear. Para ello en la terminal tecleamos el siguiente comando:

cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* easy-rsa

Para ejecutar los scripts que acabamos de copiar o de obtener, tenemos que ir a la ubicación donde los guardamos. Para ello ingresamos el siguiente comando en la terminal:

cd /etc/openvpn/easy-rsa

Antes de ejecutar los scripts editaremos el fichero vars para modificar una serie de parámetros. Para modificar el fichero vars se tiene que introducir el siguiente comando en la terminal:

nano vars

Tamaño de las claves una vez abierto el editor de texto tenemos que localizar y modificar la siguiente línea:

export_KEY_SIZE=1024

Una vez encontrada la sustituyen por la siguiente linea o el parámetro de tu conveniencia:
export_KEY_SIZE=2048

dentro del archivo nano Vars tendremos que modificar ciertos parámetros por defecto por nuestros datos reales. En mi caso los datos a rellenar podrían ser:

export KEY_COUNTRY=”ES” “Poner las 2 iniciales de tu país”
export KEY_PROVINCE=”CA” “Poner las 2 iniciales de tu provincia”
export KEY_CITY=”s*******a” “Poner el nombre de tu ciudad”
export KEY_ORG=”geekland” “Poner el nombre de la organización”
export KEY_EMAIL=”xxxxxxx@gmail.com” “Usar vuestra dirección de email”
export KEY_EMAIL=xxxxxxx@gmail.com “Usar vuestra dirección de email”
export KEY_CN= wheezy “Usar el nombre del host del servidor”
export KEY_NAME=vpnkey “Designa el nombre de la entidad certificadora que se creará”
export KEY_OI=IT “Departamento de la empresa”
guardamos y cerramos el archivo.
Exportar variables del fichero editado:
source ./vars

Eliminaremos las claves existentes tecleamos el comando:
/clean-all

se utilizarán para poder intercambiar las claves ente cliente y servidor de forma segura:
/build-dh

vamos a crear el certificado y la clave privada de nuestra propia autoridad certificadora:
/build-ca

WhezzyVPN para poder crear el certificado y clave de nuestro servidor:
/build-key-server whezzyVPN

clienteVPN para poder crear el certificado y clave de nuestro cliente:
/build-key clientevpn

FORTIFICAR LA SEGURIDAD DEL SERVIDOR OPENVPN CON TLS-AUTH
openvpn --genkey --secret ta.key

UBICACIÓN DE LAS CLAVES GENERADAS:

/etc/openvpn/easy-rsa/keys.

Archivo	Deripción	Ucación	SECRETO
dh2048.pem	Parámetros Diffie Hellman	Servidor (/etc/openvpn)	Sí
ca.crt	Certificado raíz de la entidad certificadora	Servidor (/etc/openvpn) y cliente	No
ca.key	Clave de la entidad certificadora	Servidor (/etc/openvpn)	Sí
whezzyVPN.key	Clave del servidor VPN	Servidor (/etc/openvpn)	Sí
whezzyVPN.crt	Certificado del servidor VPN	Servidor (/etc/openvpn) y cliente	No
whezzyVPN.csr	Archivo de petición de certificado	Servidor (/etc/openvpn)	No
usuariovpn.key	Clave privada del cliente VPN	Cliente	Sí
usuariovpn.crt	Certificado del cliente VPN	Cliente	No
usuariovpn.csr	Archivo de petición de certificado	Servidor (/etc/openvpn)	No
ta.key	Clave para la Autentificación TLS	Servidor (/etc/openvpn) y cliente	Sí

Para reiniciar nuestro servidor teclear el siguiente comando:

/etc/init.d/openvpn restart

CONFIGURAR EL SERVIDOR OPENVPN

Los ficheros de ejemplo que podemos usar para ver la totalidad de opciones que tenemos disponibles se hallan comprimidos en la siguiente ubicación:

/usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz

Para consultarlos teclear el siguiente comando para acceder a la ubicación de este archivo:

cd /usr/share/doc/openvpn/examples/sample-config-files

Seguidamente copiamos el archivo comprimido que dispone de los archivos de muestra de configuración en la ubicación /etc/openvpn. Para ello tecleamos el siguiente comando:

cp -a /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/

Seguidamente accedemos a la ubicación donde hemos copiado el archivo comprimido que contiene los archivos de configuración:

cd /etc/openvpn

Para descomprimir el archivo que contiene los archivos de configuración tecleamos:

gunzip server.conf.gz

Una vez descomprimido el archivo ya podemos consultar los ejemplos de configuración tanto del cliente como del servidor y tecleamos el comando.

nano server.conf

Parámetro	Descripción
dev tun	Dispositivo virtual en el cual se creara el túnel.
proto udp	Protocolo de la conexión VPN. También podríamos usar el tcp.
port 1194	Puerto de escucha del servicio. El puerto de escucha se puede modificar.
ca ca.crt	Certificado de la autoridad certificadora que creamos.
cert whezzyVPN.crt	Certificado del servidor que hemos creado.
key whezzyVPN.key	Clave privada del servidor que hemos creado.
dh dh2048.pem	Carga de los parámetro de Diffie Hellman.
Server 10.8.0.0 255.255.255.0	Indicamos que a los clientes del VPN se les asignará IP del tipo 10.8.0.0/24
ifconfig-pool-persist ipp.txt	Se crea un fichero ipp.txt en el que se registran las IP de los clientes que se conectan al servidor VPN.
push “route 192.168.1.0 255.255.255.0”	Con esta línea hacemos que los paquetes que tengan como destino la red 192.168.1.0 viajen por la interfaz del túnel (tun0). De esta forma el cliente VPN se podrá comunicar con cualquier máquina de la red 192.168.1.0.
keepalive 10 120	El servidor VPN enviará un ping cada 10 segundos y como máximo esperará 120 segundos para que el cliente de una contestación.
tls-aut ta.key 0	Activación de la autentificación TLS en el servidor.
comp-lzo	Activar compresión LZO para la transmisión de datos.
max-clients 10	Número máximo de clientes que se pueden conectar de forma simultánea. El valor se puede modificar según las necesidades.
user nobody	Para limitar los privilegios del demonio de VPN hacemos que funcione con el usuario nobody.
group nogroup	Para limitar los privilegios del demonio de VPN hacemos que funcione con el grupo nogroup.
push “redirect-gateway def1”	Para que la totalidad de tráfico vaya a través de nuestro VPN
push “dhcp-option DNS 10.8.0.1”	Estamos definiendo que las peticiones DNS de los clientes se hagan a través del servidor VPN ubicado en 10.8.0.1
cipher AES-256-CBC	Por defecto el algoritmo de cifrado de OpenVPN es Blowfish con un tamaño de clave de 128 bits. Quien crea que no es suficiente puede añadir esta línea para cambiar el algoritmo de cifrado a AES con un clave de cifrado de 256 bits. Para ver todos los algoritmos de cifrado disponibles teclear openvpn –show-ciphers en la terminal.
Persist-key	En caso que el servidor OpenVPN se caiga las claves no tendrán que ser analizadas de nuevo.
persist-tun	El dispositivo tun0 no tendrá que ser reabierto ni cerrado en el caso que tengamos que reiniciar el servidor.
status openvpn-status-log	Log donde se guardará información respecto al túnel creado.

plugin /usr/lib/openvpn/openvpn-auth-pam.so /etc/pam.d/login Activación del script encargado de realizar la autenticación del usuario y del cliente. (Ver el apartado "Autentificación del cliente mediante usuario y password")

verb 3 Grado de detalle del estado del túnel en los logs.

CONFIGURAR EL CLIENTE OPENVPN

Una vez configurado el servidor ahora pasaremos a configurar el cliente. Para ello dentro de la ubicación /etc/openvpn tecleamos el siguiente comando:

¬ nano client.conf

Se abrirá el fichero de configuración en el que podrán ver un ejemplo de configuración para un cliente estándar. Aseguramos que el fichero de configuración estándar tenga los parámetros que se muestran en la tabla de este apartado. En caso de no tenerlos habrá que añadirlos manualmente, en el caso de que los parámetros estén comentados habrá que descomentarlos y en el caso que no existan se deberán añadir y/o modificar.

Parámetro Descripción

dev tun Dispositivo virtual en el cual se creara el túnel.

proto udp Protocolo de transmisión de paquetes del servidor VPN. Se puede usar TCP.

remote geekland.sytes.net 1194 Dirección IP pública/Host DNS dinámico y puerto de escucha del servidor VPN. El puerto 1194 se puede cambiar. Si lo cambiamos deberemos adaptar el resto de configuraciones al nuevo puerto

resolv-retry infinite El cliente intentará de forma indefinida resolver la dirección o nombre de host indicado por la directiva remote (geeekland.sytes.net).

nobind A los clientes se les asignará puertos dinámicos (no privilegiados) cuando haya retorno de paquetes del servidor al cliente.

user nobody Para limitar los privilegios de los clientes que se conectan al VPN les asignamos el usuario nobody. (no necesario para windows)

group nogroup Para limitar los privilegios de los clientes que se conectan al VPN les asignamos el grupo nogroup. (no necesario para windows)

persist-key En caso que el servidor OpenVPN sea reiniciado no se tendrán que volver a leer las claves.

persist-tun El dispositivo tun0 no tendrá que ser reabierto ni cerrado en el caso que tengamos que reiniciar el cliente Vpn.

ca ca.crt Certificado de la autoridad certificadora que creamos

cert usuariovpn.crt Certificado del cliente

key usuariovpn.key Clave privada del cliente

ns-cert-type server Para prevenir ataques man in the middle. Con esta frase hacemos que los clientes solo puedan aceptar un certificado de servidor del tipo servidor "nsCertType=server". En este campo podríamos aplicar otras alternativas similares como por ejemplo "remote-cert-tls server".

tls-auth ta.key 1 Activación de la identificación TLS en el cliente.

cipher AES-256-CBC Por defecto el algoritmo de cifrado de OpenVPN es Blowfish con un tamaño de clave de 128 bits. Quien crea que no es suficiente puede añadir esta línea para cambiar el algoritmo de cifrado a AES con un clave de cifrado de 256 bits. Para ver todos los algoritmos de

cifrado disponibles teclear openvpn –show-ciphers en la terminal.

auth-user-pass Para indicar que el cliente tiene que introducir un nombre de usuario y un password.

auth-nocache Para evitar que los password queden almacenados en la memoria cache de los clientes.

comp-lzo Activar compresión LZO para la transmisión de datos.

verb 3 Grado de detalle del estado del túnel

Para añadir un usuario, como por ejemplo el usuariovpn2, tienen que teclear el siguiente comando en la terminal:

¬ useradd usuariovpn2 -M -s /bin/false

Una vez creado el usuario tenemos que definir un password del usuariovpn2. Para ello tecleamos el siguiente comando en la terminal:

¬ passwd usuariovpn2

Una vez introducido el comando nos pedirá que introduzcamos la clave de usuario y después nos pedirá confirmación.

En el caso que a posteriori se precise eliminar el usuariovpn2 tan solo tienen que introducir el siguiente comando en la terminal:

deluser usuariovpn2

CONFIGURAR IPTABLES PARA EL ENRUTAMIENTO DE PETICIONES

Para ello lo primero que tenemos que hacer es habilitar el IP forwarding. Para habilitar el IP Forwading de forma permanente tecleamos el siguiente comando en la terminal:

nano /etc/sysctl.conf

Se abrirá el editor de textos y seguidamente tendremos que localizar la siguiente linea:

#net.ipv4.ip_forward=1

Una vez localizada tan solo hay que descomentarla de forma que quede de la siguiente forma:

net.ipv4.ip_forward=1

Guardamos los cambios y cerramos el archivo.

Una vez habilitado el Ipforwarding tenemos que permitir el tráfico por nuestro túnel VPN, y además tenemos que hacer que los clientes VPN puedan acceder a redes externas públicas y otras subredes dentro de la red VPN. Para poder conseguir esto en la terminal escriben el siguiente comando:

nano /etc/rc.local

Una vez se abra el editor de textos tienen que escribir las siguientes reglas en nuestro firewall

iptables -A FORWARD -i eth0 -o tun0 -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A FORWARD -s 10.8.0.0/24 -o eth0 -j ACCEPT

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

SEGURIDAD QUE NOS APORTARÁ EL SERVIDOR OPENVPN

Si se configura el servidor Openvpn, tal y como se detalla en el post, se obtendrá un nivel de seguridad muy elevado y resultará prácticamente invulnerable frente a ataques.

La seguridad que aportará el servidor OpenVPN que acabamos de configurar estará compuesta por 3 capas:

Capa 1 “Identificación TLS”: Con la identificación TLS estamos introduciendo una firma digital HMAC a los paquetes antes de empezar la identificación reciproca entre cliente y servidor. Si no se pasa el test de la firma HMAC, no se llegará ni a iniciar el proceso de autentifican entre cliente y servidor.

Capa 2 “SSL/TLS”: Mediante las herramientas de seguridad proporcionadas SSL/TLS se realiza el proceso de identificación bidireccional entre el cliente y el servidor OpenVPN mediante claves criptográficas.

Capa 3 “Cifrado”: Dispone de varios tipos de cifrado disponibles en la transmisión de datos entre el cliente y el servidor. Además podemos aplicar medidas para los privilegios del demonio de OpenVPN sean los mínimos para poder realizar la función que tiene que realizar.

Todas estas características, más las que se detallan en el post, hacen que OpenVPN sea una opción muy válida para la transmisión segura de datos sensibles. Por esto motivo OpenVPN es el protocolo que utilizan muchas organizaciones en el mundo empresarial. Además OpenVPN es una solución multiplataforma y dentro de lo que cabe no es difícil de configurar si lo comparamos con por ejemplo Ipsec.

Cabe decir que actualmente no se conocen vulnerabilidades importantes en este tipo de servidor VPN. Es posible que se descubran vulnerabilidades pero si vamos aplicando las actualizaciones de seguridad no deberíamos tener problema alguno en lo que a seguridad se refiere.

La instalación del cliente OpenVPN en GNU/Linux

Guarda muchas similitudes con la de la parte servidor, de hecho el paquete que instalaremos será exactamente el mismo.

Este artículo está basado en Debian Wheezy como sistema operativo cliente, pero salvo por la instalación de OpenVPN debería ser igual en otras distribuciones.

Requisitos previos

Disponer de un servidor OpenVPN correctamente configurado al que conectarnos (cosa bastante

evidente).

Los certificados necesarios para la conexión SSL/TLS:

Clave pública de la CA: Sobrebits_CA.crt.

Clave pública de usuario: Nombredeusuario.crt.

Clave privada de usuario: Nombredeusuario.key.

Los certificados los ubicaremos igual que en el anterior tutorial:

$ sudo mv Sobrebits_CA.crt /etc/ssl/certs/

$ sudo mv Nombredeusuario.crt /etc/ssl/certs/

$ sudo mv Nombredeusuario.key /etc/ssl/private/

Instalación y configuración del cliente OpenVPN

Instalamos OpenVPN con el gestor de paquetes de nuestra distribución. Como esta guía está hecha con Debian vamos a tirar de apt-get:

$sudo apt-get install openvpn

Como se dijo en el artículo de la parte servidor el comportamiento de OpenVPN por defecto es el de cargar todos los archivos *.conf de su directorio /etc/openvpn al ejecutarse el servicio. Puesto que este no es el comportamiento que quiero voy a editar el archivo de configuración de OpenVPN para que la conexión sólo se establezca cuando se le solicite.

$sudo nano /etc/default/openvpn

Y descomentamos la línea:

AUTOSTART="none"

Lo siguiente que haremos es copiar el archivo de configuración de cliente de ejemplo que podemos encontrar en el directorio de documentación del programa al directorio de trabajo del mismo.

$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/

Y lo editamos:

$ sudo nano /etc/openvpn/client.conf

Aquí básicamente deberemos configurar tres cosas: la dirección de nuestro servidor OpenVPN, la ruta hacia los certificados anteriormente citados y forzar que todo el tráfico se envíe a través de la VPN:

Dirección del servidor y puerto

remote tmblck.sytes.net 1194

Ruta de los certificados

ca /etc/ssl/certs/Sobrebits_CA.crt

cert /etc/ssl/certs/Nombredeusuario.crt

key /etc/ssl/private/Nombredeusuario.key

Redirigimos todo el tráfico a través de la VPN

redirect-gateway def1

Lo que debería acabar dándonos esta línea:

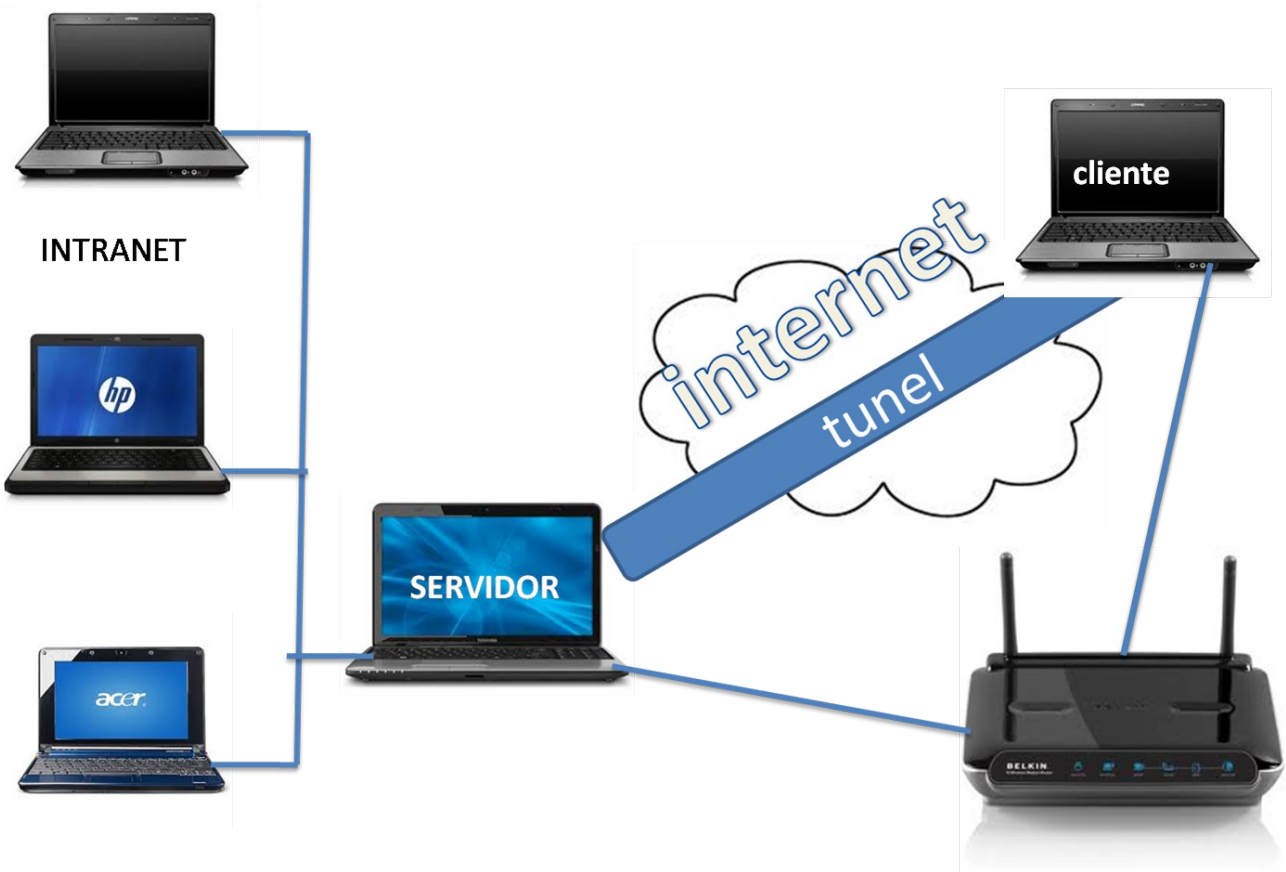
Initialization Sequence Completed

En el momento en el que esto pase ya estaremos navegando a través de la VPN. Para comprobarlo podemos dirigirnos a uno de esos cientos de sitios web donde nos dicen nuestra IP pública o bien:

traceroute www.google.es

Que debería mostrarnos la ruta de nuestro paquete por la red a la que nos hemos conectado.

DIAGRAMA DE RED DEL PROYECTO VPN



Lista de actividades

1-) Recopilación de información necesaria para instalar y configurar un VPN.

2-) Redactar y presentar el perfil del proyecto VPN.

3-) Instalación de debían en la computadora.

4-) Instalación del openvpn, que nos servira para hacer las conexiones, identificaciones, encapsulamiento y asignara las ip a los clientes.

5-) Configuración de la computadora que utilizaremos como servidor VPN.

6-) Configuración de las computadoras que se utilizaran como clientes que tendran el servicio VPN.

7-) Pruebas hacia el openvpn.

8-) Corrección de errores del proyecto.

DIAGRAMA DE GANTT

ACTIVIDADES	AGOSTO				SEPTIEMBRE				OCTUBRE			
SEMANAS	1ra	2da	3ra	4ta	1ra	2da	3ra	4ta	1ra	2da	3ra	4ta
Recopilación de información necesaria para instalar y configurar un VPN												
Redactar y presentar el perfil del proyecto RPN												
Instalación de debían en la computadora												
Instalación del openvpn, que nos servira para hacer las conexiones, identificaciones, encapsulamiento y asignara las ip a los clientes.												
Configuración de la computadora que utilizaremos como servidor VPN.												
Configuración de las computadoras que se utilizaran como clientes que tendra el servicio VPN												
Pruebas hacia el openvpn												
Corrección de errores del proyecto												

VIABILIDAD DEL PROYECTO.

El proyecto de elaborar una conexión de cliente servidor utilizando un VPN es de suma importancia para las empresas que necesitan tener la información de su empresa o aplicaciones o progrmas que necesitan para trabajar este proceso se puede llevar a cabo si consideramos que la tecnologia que se utiliza esta al alcance de nuestras manos por ello las empresas se favorecen de este mecanismo de enviar datos o información de forma segura a otras partes del mundo. Y sus requerimientos no son tan altos ya que solo se necesita tener los conocimientos adecuados para poder llevar a cabo este tipo de procesos.

Ademas se puede contratar a personas para que realicen esta tarea de configurar un VPN que favorezca a la empresa en su funcionamiento en el traspaso de la información.

Tomando en cuenta que los gastos serian mínimos al momento de elaborar un proyecto de este tipo y que una persona con conocimientos intermedios en computación puede llevar a cabo contando con el equipo adecuado.

VIABILIDAD TÉCNICA Y ECONÓMICA.

Presupuesto:

CANTIDAD	DESCRIPCION	COSTO
3	computadoras	$450.00
1	Servidor VPN	$150.00
1	Acceso a internet (mensual)	$50.00
2	Servicios profesionales	$600.00
	total	$1,250.00

Computadora.
Mouse.
Teclado.
Tarjeta de red.
Módems.
Software (Debían whezy)
Cables directos

CONCLUCION

En este proyecto se realizara con la finalidad de implementar un VPN con GNU/Linux- el cual al final nos presentara, una serie de beneficios tanto a los usuarios de la red como también a los paquetes transmitidos, de esta manera con este proyecto se establecerá la comunicación entere maquinas no importando el lugar donde estén, es decir no necesaria mente deberá estar cerca de la red sino que se puede lograr tenerla virtud de administrar un equipo desde un sito lejano. Teniendo en cuenta los diferentes tipos de VPN existentes o las formas de implementarse en la red se desarrollara en el trabajo con un objetivo poder conocer más de las tecnologías usadas en este tipo de proyectos.

Se realizara la configuración siguiendo diferentes pasos, para mostrar las diferentes fases con las que consta un VPN y su implementación en GNU/Linux pues el desarrollo nos mostrara las ventajas de la elaboración de la red, teniendo en cuenta los protocolos destinados a la realización. Una configuración de este tipo es un poco compleja por la desventaja que es un proyecto nuevo para nosotros y la meta es llevarlo a cavo de la mejor manera.

- Se mostraron los pasos de instalación y configuración del openvpn así como también todos sus ficheros y archivos de verificación.

- Se da a conocer lo que es la tecnología de túnel la cual es una forma segura de que viajen los paquetes de nuestro servidor a nuestros clientes.

- Presentamos la descripción de las diferentes claves y certificados creados mediante los pasos de instalación del trabajo.

- Montaje del cliente con las especificaciones de que debería tener nuestro servidor y los archivos necesarios para conectar de forma correcta nuestro cliente.

BIBLIOGRAFIA.

Openvpn, modo guerrero de la carretera (road warrior)
http://rodrigoaguilera.net/openvpn-modo-guerrero-la-carretera-road-warrior

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

Configurar OpenVPN en debian 5/Ubuntu 10.4 y Mac OS/X
http://ubanov.wordpress.com/2010/10/07/configurar_openvpn_debian_ubuntu/

GLOSARIO

- ISP: se refiere a las siglas en Inglés para Internet Services Provider. Su traducción al español nos permite comprender de manera rápida y sencilla de qué se trata un ISP; un Proveedor de Servicios o acceso de Internet. A los ISP también se los llama IAP, que también corresponde a siglas en Inglés, en este caso para Internet Access Providers, que traducido al español, se entiende como Proveedores de Acceso a Internet.
- VPN: 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 sobre una red pública o no controlada como Internet.
- OPENVPN: OpenVPN es una solución de conectividad basada en software libre: SSL VPN Virtual Private Network, OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi y soporta una amplia configuración
- ROADWARRIOR: modo guerrero de la carretera.
-