UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACION

CÁTEDRA:

REDES II

TRABAJO DE INVESTIGACIÓN:

"Configuración de una red privada virtual con openvpn en el sistema operativo Debian Wheezy 7.0 "

PRESENTADO POR:

N°	APELLIDOS	NOMBRES	CARNET	Participación
01	Alejo	William Orlando	a01121151	100%
02	López Rivas	Ana Miriam	lr01121476	100%
03	Alfaro Velis	Ramón	av02110304	100%

CATEDRÁTICO:

Ing. Manuel Flores Villatoro

LUGAR Y FECHA:

San Salvador, 31 de Agosto de 2013

Índice de contenido

Índice de ilustraciones

INTRODUCCIÓN

En este trabajo aprenderemos como crear y configurar una VPN utilizando las herramientas de tecnologías libres como OPENVPN, y su uso aplicando estándares de calidad.

Una Red Privada Virtual (VPN) es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.

Con todo lo investigado y aplicado en nuestro proyecto estaremos listos y aptos para la instalación y configuración de herramientas de comunicación y conexiones remotas seguras como son las VPN que facilitan la conectividad de una red privada sobre una red pública.

Usaremos certificados de autenticación y seguridad para establecer una conexión entre el servidor VPN y los clientes, como un recurso útil del canal de comunicación.

OBJETIVOS

GENERAL

- Configurar e implementar una Red Privada Virtual en una red pública con un servidor Openvpn, para conocer casos de uso práctico de conexiones seguras y su implementación en una organización.

ESPECÍFICOS

- Instalar y configurar Openvpn en debian Wheezy 7.0

- Configurar el servicio para el funcionamiento de una VPN en una dirección IP pública.

- Configurar una VPN para establecer conexiones seguras entre 3 computadores.

MARCO TEÓRICO

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 una red 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. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, encriptación 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.

La conexión VPN a través de Internet es técnicamente una unión de wide area network (WAN) entre los sitios pero al usuario le parece como si fuera un enlace privado— de allí la designación "virtual private network".

CARACTERÍSTICAS BÁSICAS DE LA SEGURIDAD

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad de toda la comunicación:

Autenticación 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. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

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.
- *Auditoría 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.

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 DES O 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.

TIPOS DE VPN

Básicamente existen tres arquitecturas de conexión VPN:

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 (modem) y líneas telefónicas).

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.

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.

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 (Wi-Fi).

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.

IMPLEMENTACIONES

El protocolo estándar de facto es 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 de software tenemos a los productosde Fortinet, SonicWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen, (Juniper 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 de Unix en general. Por ejemplo productos de código abierto,como OpenSSH, OpenVPN y FreeS/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.

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.

TIPOS DE CONEXIÓN

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computador 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 autentica al servidor de acceso remoto, y el servidor se autentica ante el cliente.

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 autentica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

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 autentica ante el que responde y éste a su vez se autentica ante el llamante.

INFORMACIÓN SOBRE LA CONSTRUCCIÓN DEL PROYECTO

Artefactos utilizados

Tres equipos
Un router
Un Acces Point
Cable UTP categoría 5

Interface utilizada

TUN: El controlador TUN emula un dispositivo punto a punto, es utilizado para crear túneles virtuales operando con el protocolo IP. Encapsula todos los paquetes que se transporten a través de él como datagramas TCP o UDP.

Puertos y protocolos utilizados

Puerto por defecto en Server para el OpenVPN es 1194, puedes ser modificado por cualquier otro puerto que esté disponible

El protocolo que utilizamos para nuestra configuración fue TCP para la interfaz TUN para VPN tipo enrutada.

INSTALACIÓN Y CONFIGURACIÓN DE OPENVPN PARA VPN

En Debian/Ubuntu es posible instalar OpenVPN desde los repositorios oficiales:

1.- Primero debemos instalar en la terminal como usuario root:

apt-get install openvpn

apt-get install openssl

2.- Luego de la instalación se deben copiar los scripts de configuración de ejemplo al directorio /etc/openvpn:

cd /usr/share/doc/openvpn/examples/easy-rsa

cp -a 2.0/ /etc/openvpn/easy-rsa

cd /etc/openvpn/easy-rsa

Estos scripts permiten la creación automática de una autoridad certificante (CA) autofirmada, lo cual simplifica mucho la instalación. Ya que OpenVPN está basado en SSL, se utiliza openssl para la autenticación mutua de clientes y servidores. La CA se utiliza para expedir certificados para el servidor de VPN y los clientes.

Antes de comenzar a crear la CA y los certificados se deben configurar algunas variables de entorno.

3.- Es necesario establecer unos parámetros en el CA (Certificado de Autoridad) de nuestra VPN para eso usaremos:

nano vars

```
  GNU nano 2.2.6                    Fichero: vars

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="SV"
export KEY_PROVINCE="CA"
export KEY_CITY="Victoria"
export KEY_ORG="Uls"
export KEY_EMAIL="williamalejo@gmail.com"
export KEY_EMAIL=williamalejo@gmail.com
export KEY_CN=changeme
export KEY_NAME=changeme
export KEY_OU=changeme
export PKCS11_MODULE_PATH=changeme
export PKCS11_PIN=1234
```

Ilustración 1: Configuración de nano vars

Se deben configurar correctamente los parámetros KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, y KEY_EMAIL.

Luego de configurar el archivo vars es posible generar el certificado y clave para la Autoridad Certificante (CA):

4.- Ahora se creara el Certificado de Autoridad para posteriormente crear los certificados y claves privadas para nuestro servidor VPN:

. ./vars

./clean-all

./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) [SV]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [Victoria]:
Organization Name (eg, company) [Uls]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:
Name [changeme]:
Email Address [williamalejo@gmail.com]:
```

Ilustración 2: Creación de certificados de autoridad

El script build-ca crea el certificado de la CA utilizando los parámetros configurados en vars. Verificar que los parámetros entre corchetes estén correctos, modificar en caso contrario. Luego es posible generar el certificado y clave para el servidor de VPN:

5.- Ahora se creará el certificado y la clave para servidor

./build-key-server server

```
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'SV'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'Victoria'
organizationName      :PRINTABLE:'Uls'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'williamalejo@gmail.com'
Certificate is to be certified until Nov 18 09:25:32 2023 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Ilustración 3: Creación de cetificado y lleve de seguridad para servidor

El CN (Common Name) debe ser "server", responder 'y' dos veces para firmar y commit del certificado.

6.- Generaremos los certificados para los clientes (es importante que los certificados de los clientes y del servidor estén firmados por la misma CA)

./build-key Usuario1

./build-key Usuario2

./build-key Usuario3

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:usuario3
An optional company name []: Usuario 3
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'SV'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'Victoria'
organizationName      :PRINTABLE:'Uls'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'usuario3'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'usuario3@gmail.com'
Certificate is to be certified until Oct 16 18:58:53 2023 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]
```

Ilustración 4: Creación de certificado y llave de seguridad para los clientes

7.- Finalmente se deben generar los parámetros Diffie-Hellman:

./build-dh

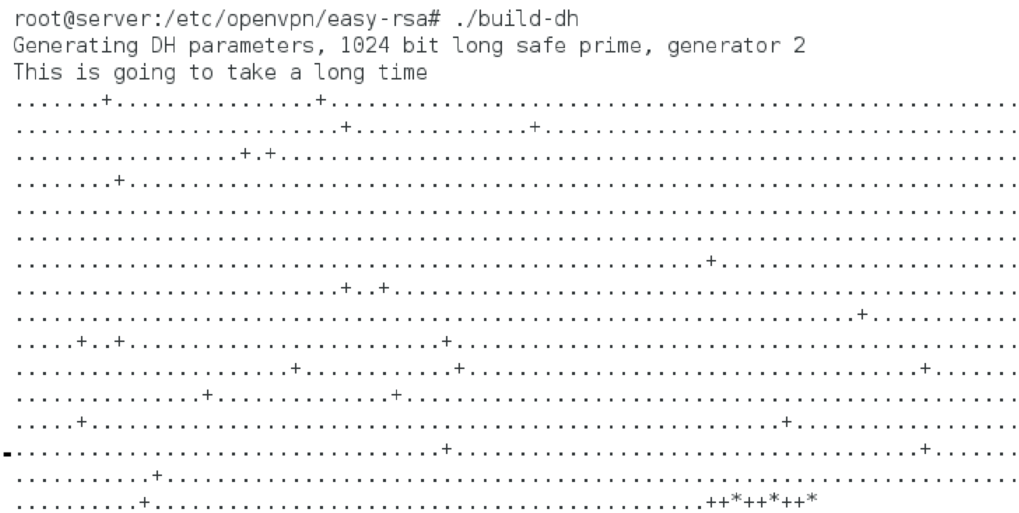

Ilustración 5: Generación de la base de datos

ARCHIVOS DE CONFIGURACIÓN PARA EL SERVIDOR Y LOS CLIENTES

Luego de construir nuestra PKI (Public Key Infrastructure), es decir nuestra infraestructura de autenticación y encriptación mediante clave pública, se deben copiar los archivos de configuración de ejemplo al directorio /etc/openvpn:

cp -a /usr/share/doc/openvpn/examples/sample-config-files/ /etc/openvpn/

- ***CONFIGURACIÓN DEL SERVIDOR.***

1.- Se descomprime el archivo de configuración del servidor

cd /etc/openvpn/sample-config-files/ gunzip server.conf.gz

2.- Editar el archivo de configuración del servidor:

nano server.conf

```
proto tcp
;proto udp

;dev tap
dev tun

easy-rsa/keys/ca ca.crt
easy-rsa/keys/cert server.crt
easy-rsa/keys/key server.key

easy-rsa/keys/dh dh1024.pem

server 10.8.0.0 255.255.255.0
```

Ilustración 1: Comprobación del funcionamiento de la vpn

De esta forma el servidor dará acceso a la red 10.8.0.0/24 y tomará la dirección IP 10.8.0.1 (los clientes tendrán una IP en el rango 10.8.0.2 a 10.8.0.254).

3.- Por último debemos copiar el archivo de configuración al directorio /etc/openvpn:

cp server.conf ../

cd /etc/openvpn

4.- Probando la configuración del servidor VPN:

root@server:/etc/openvpn# openvpn server.conf

```
root@server:/etc/openvpn# openvpn server.conf
Tue Oct  8 23:18:28 2013 OpenVPN 2.2.1 i486-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [eurephia] [MH] [PF_INET6] [IPv6 payload 20110424-2 (2.2
RC2)] built on Jun  6 2013
Tue Oct  8 23:18:28 2013 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts or executables
Tue Oct  8 23:18:28 2013 Diffie-Hellman initialized with 1024 bit key
Tue Oct  8 23:18:28 2013 TLS-Auth MTU parms [ L:1544 D:140 EF:40 EB:0 ET:0 EL:0 ]
Tue Oct  8 23:18:28 2013 Socket Buffers: R=[87380->131072] S=[16384->131072]
Tue Oct  8 23:18:28 2013 ROUTE default_gateway=192.168.2.1
Tue Oct  8 23:18:28 2013 TUN/TAP device tun0 opened
Tue Oct  8 23:18:28 2013 TUN/TAP TX queue length set to 100
Tue Oct  8 23:18:28 2013 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Tue Oct  8 23:18:28 2013 /sbin/ifconfig tun0 10.8.0.1 pointopoint 10.8.0.2 mtu 1500
Tue Oct  8 23:18:28 2013 /sbin/route add -net 10.8.0.0 netmask 255.255.255.0 gw 10.8.0.2
Tue Oct  8 23:18:28 2013 Data Channel MTU parms [ L:1544 D:1450 EF:44 EB:135 ET:0 EL:0 AF:3/1 ]
Tue Oct  8 23:18:28 2013 Listening for incoming TCP connection on [undef]
Tue Oct  8 23:18:28 2013 TCPv4_SERVER link local (bound): [undef]
Tue Oct  8 23:18:28 2013 TCPv4_SERVER link remote: [undef]
Tue Oct  8 23:18:28 2013 MULTI: multi_init called, r=256 v=256
Tue Oct  8 23:18:28 2013 IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
Tue Oct  8 23:18:28 2013 IFCONFIG POOL LIST
Tue Oct  8 23:18:28 2013 MULTI: TCP INIT maxclients=1024 maxevents=1028
Tue Oct  8 23:18:28 2013 Initialization Sequence Completed
```

Ilustración 2: Prueba de la configuración del servidor vpn

5. Inciar el Servidor Openvpn

root@server:/etc/openvpn# /etc/init.d/openvpn start

```
Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
          RX packets:51 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4240 (4.1 KiB)  TX bytes:4240 (4.1 KiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:880 (880.0 B)

wlan0     Link encap:Ethernet  HWaddr 00:1f:e1:4d:08:54
          inet addr:192.168.43.108  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:e1ff:fe4d:854/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10780 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12536 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9194304 (8.7 MiB)  TX bytes:1803133 (1.7 MiB)

root@server:/home/william#
```

Ilustración 3: Puesta en función de la vpn

- ***CONFIGURACIÓN DE LOS CLIENTES***

1. Debemos tener instalado Openvpn
2. Copiamos los certificados que generamos en el servidor, tanto los de usuarios como los de autoridad.
3. Estaríamos listos para conectarse al servidor VPN.
4. Luego reiniciamos el servicio.

   /etc/init.d/openvpn restart

ESCENARIO DE PRUEBAS

Al construir una VPN, lo que se desea es tener la posibilidad de acceder a una red local (protegida detrás de un firewall/gateway) desde Internet (o desde cualquier otra red insegura). El objetivo es que un cliente ubicado físicamente fuera de la red local (y posiblemente a kilómetros de distancia) parezca conectado de forma local. El servidor de VPN es el que posibilita la "extensión" y es quien provee una conexión segura entre el cliente y la red local a través de SSL (al utilizar certificados se obtiene autenticación mutua y confidencialidad).

El siguiente escenario presenta la configuración que tendrían los equipos informáticos que establecerán conexiones.

Usaremos 3 equipos informáticos, el equipo A hará la función de servidor VPN, los equipos B y C serán los usuarios 1 y 2, y usaremos el Internet para poder acceder a la red privada.

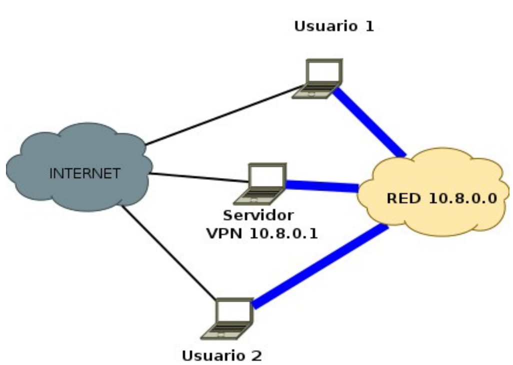

Ilustración 4: Escenario planteado

BUENAS PRÁCTICAS

- Conocer la operatividad y funcionalidad de una VPN.
- Saber donde colocar cada una de las IP y su uso.
- Conocer los protocolos a utilizar para la configuración del servidor VPN.
- Utilizar el protocolo TCP en vez del protocolo UDP, ya que este último da problemas a la hora de transmitir paquetes.

CONCLUSIONES

Después de haber investigado sobre como configurar una VPN podemos concluir que:

- Hay muchas herramientas basadas en software libre que nos facilitan la configuración de una vpn segura, entre estas se destaca OPENVPN que servirá para nuestro proyecto.

- Comprender la lógica de operatividad de una vpn ha sido uno de los aprendizajes más significativos que hemos obtenido, ya que nos ha permitido identificar su funcionamiento.

- Una vpn puede configurarse en distintas plataformas, nuestro equipo hará configuraciones y pruebas en los sistemas operativos Debian y Windows.

RECOMENDACIONES

Después de haber implementado este proyecto hacemos las siguientes recomendaciones:

- Proporcionar bibliografía relacionada con los proyectos de cátedra.

- Es importante realizar configuraciones y pruebas en maquinas virtuales antes de llevarlas a maquinas reales.

- Realizar talleres cortos se uso de comandos relacionados con los proyectos.

- Es importante un involucramiento constante por parte de los integrantes de los grupos en los proyectos.

REFERENCIAS BIBLIOGRÁFICAS

Academia Networking de Cisco Systems (CCNA3 y CCNA4)
Autores: Cysco Sistems, Inc.
Editorial: Cysco Press
Año de edición: 2006
ISBN: 84-205-4079-x

Url's consultadas entre las fechas 2 al 6 de agosto de 2013.

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

http://www.cisco.com/web/LA/soluciones/la/vpn/index.html

http://www.monkeedev.co.uk/blog/2009/03/06/setting-up-openvpn-in-debianubuntu/

http://ubanov.wordpress.com/2010/10/07/configurar_openvpn_debian_ubuntu/

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

http://linuxito.com.ar/121-instalación-y-configuracion-de-openvpn.html

http://www.monografias.com