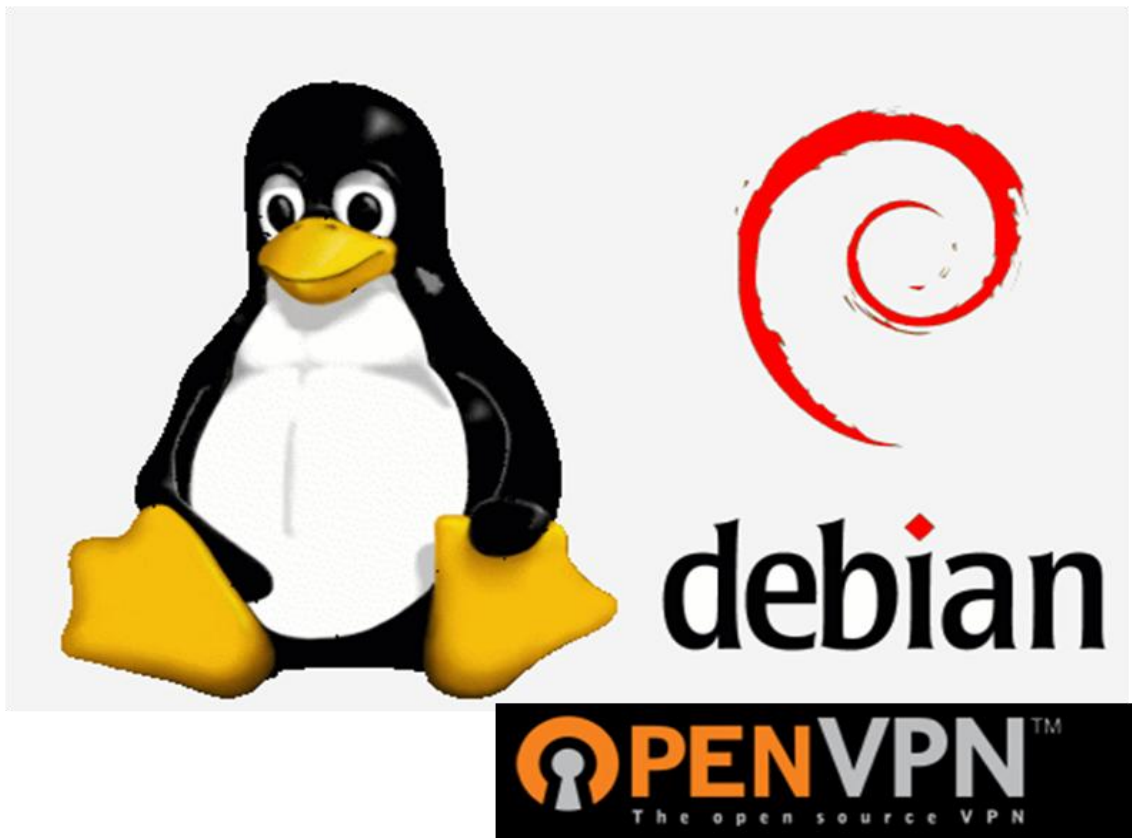


CAPÍTULO 5



IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

5.1 Instalación y configuración de la distribución de Debian

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

En este trabajo de tesis se escogió la distribución del sistema operativo Debian por ser uno de los Sistemas Operativos más estables y maduros ***“Debian sobrepasa a todas las otras distribuciones en lo bien integrados que están sus paquetes. Como todo el software lo empaqueta un grupo coherente, no sólo puede encontrar todos los paquetes en un mismo sitio sino que puede estar seguro de que se han eliminado todos los problemas al respecto de complejas dependencias. Aunque se cree que el formato deb tiene algunas ventajas sobre el rpm, es la integración entre paquetes lo que hace a Debian más robusto.”***¹ Es por esto que en el laboratorio de redes y seguridad los equipos cuentan con dicho sistema instalado.

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

En este proyecto se eligió la instalación mediante un CDROM que permitió realizar la instalación básica del Sistema Operativo Debian y después de su

1

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

instalación, mediante una conexión a internet se configuró el gestor de arranque para actualizar los archivos desde la página web de Debian.

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

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

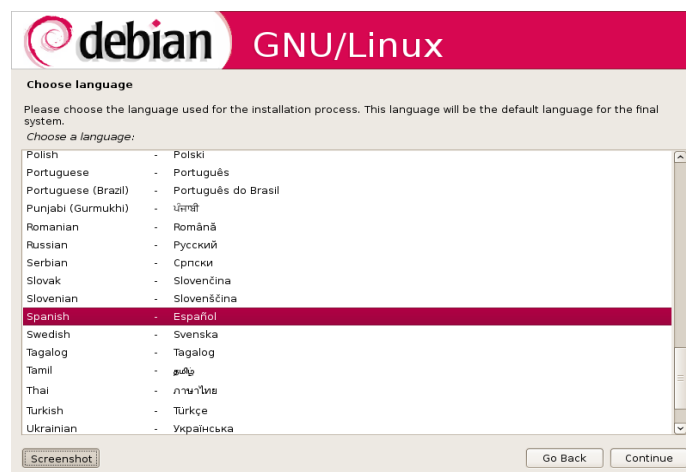


Figura 5.1 Elección del idioma en la instalación

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



Figura 5.2 Elección del país

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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



Figura 5.3 Selección del idioma del teclado

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN



Figura 5.4 Nombre del equipo

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



Figura 5.5 Asignación de nombre de dominio

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

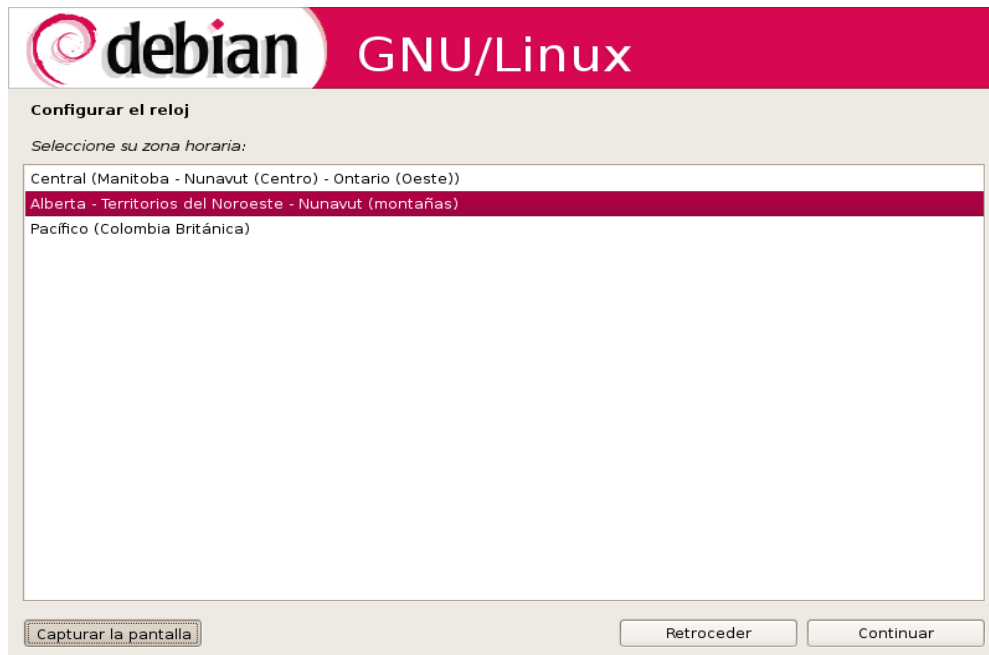


Figura 5.6 selección de zona horaria

- 4) En el siguiente apartado se muestran las particiones que tiene el disco duro que está instalado en el equipo, los parámetros se ven en una lista y se pueden observar de la siguiente manera:
 - a) Particionar el disco duro.
 - b) Utilizar todo el espacio del disco duro.
 - c) Realizar las particiones avanzadas en el disco duro.

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN



Figura 5.7 Particionado de discos

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



Figura 5.8 Instalación del Sistema Operativo en el Disco duro

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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



Figura 5.9 Particionado guiado del proceso de instalación

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



Figura 5.10 Ingreso de la clave de superusuario

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

Figura 5.11 Creación de cuenta de usuario

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

Figura 5.12 Contraseña de la cuenta creada

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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



Figura 5.13 Configuración del gestor de paquetes

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



Figura 5.14 Lista de programas a instalar

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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



Figura 5.15 Instalación servidor Samba

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



Figura 5.16 Instalación del paquete dhcp

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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



Figura 5.17 Instalación del gestor de arranque

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



Figura 5.18 Instalación finalizada

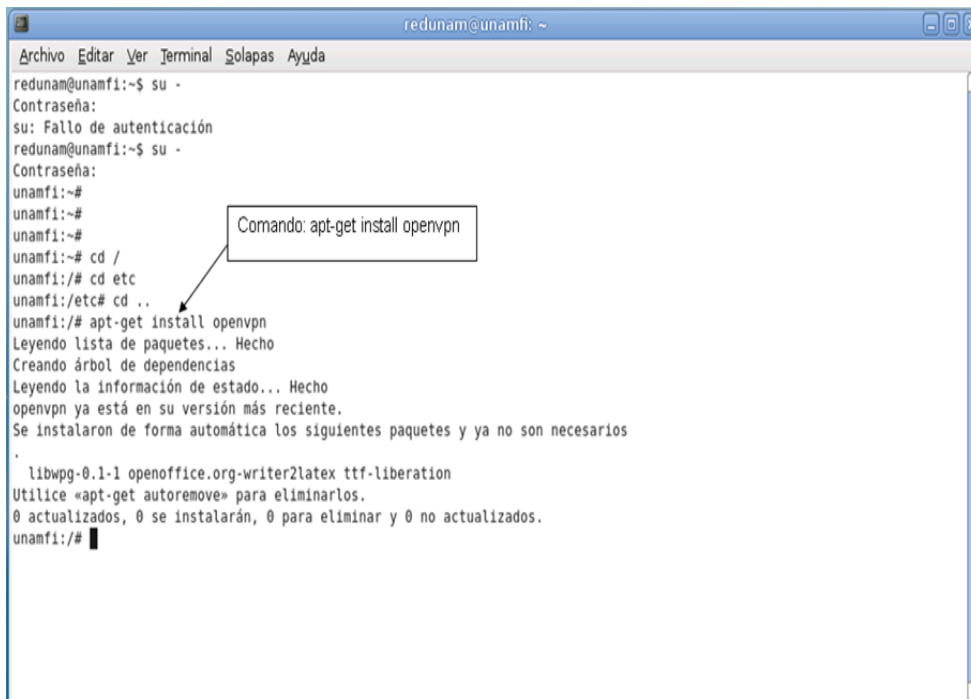
CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

5.2 Instalación de OPENVPN

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

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

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



```

redunam@unamfi: ~
Archivo Editar Ver Terminal Solapas Ayuda
redunam@unamfi:~$ su -
Contraseña:
su: Fallo de autenticación
redunam@unamfi:~$ su -
Contraseña:
unamfi:~#
unamfi:~#
unamfi:~#
unamfi:~# cd /
unamfi:~# cd etc
unamfi:~# cd ..
unamfi:~# apt-get install openvpn
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openvpn ya está en su versión más reciente.
Se instalaron de forma automática los siguientes paquetes y ya no son necesarios
.
 libwpg-0.1-1 openoffice.org-writer2latex ttf-liberation
Utilice «apt-get autoremove» para eliminarlos.
0 actualizados, 0 se instalarán, 0 para eliminar y 0 no actualizados.
unamfi:~#
  
```

Figura 5.19 Instalación de OPENVPN en Linux.

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

```

redunam@unamfi: ~
Archivo Editar Ver Terminal Solapas Ayuda
W: No se ha podido localizar el paquete opevpn
E: No se encontró ningún paquete
unamfi:~# apt-cache show openvpn
Package: openvpn
Priority: optional
Section: net
Installed-Size: 1044
Maintainer: Alberto Gonzalez Iniesta <agi@inittab.org>
Architecture: i386
Version: 2.1-rc11-1
Depends: debconf | debconf-2.0, libc6 (>= 2.7-1), liblzo2-2, libpam0g (>= 0.99.7.1), libpks11-helper1, libssl0.9.8 (>= 0.9.8g-9), openssl-blacklist (>= 0.4), openvpn-blacklist
Recommends: net-tools
Suggests: openssl, resolvconf
Filename: pool/main/o/openvpn/openvpn_2.1-rc11-1_i386.deb
Size: 403716
MD5sum: 742788fdd1b5b944ab297aa23139d621
SHA1: 029a80101e59f90e2083dc4b4a4fcf24cbb8c538
SHA256: 79103443ccale4e7d8b510a7e09463c0e15ca7b089b3814712c0923398367af3
Description: virtual private network daemon
 OpenVPN is an application to securely tunnel IP networks over a
 single UDP or TCP port. It can be used to access remote sites, make
 secure point-to-point connections, enhance wireless security, etc.
 .
 OpenVPN uses all of the encryption, authentication, and certification
 features provided by the OpenSSL library (any cipher, key size, or
 HMAC digest).
 .
 OpenVPN may use static, pre-shared keys or TLS-based dynamic key exchange. It
 also supports VPNs with dynamic endpoints (DHCP or dial-up clients), tunnels
 over NAT or connection-oriented stateful firewalls (such as Linux's iptables).
 Tag: interface::daemon, network::server, network::vpn, role::program, security::cryptography

unamfi:~#

```

Figura 5.20 Información de la versión de OPENVPN.

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

```

redunam@unamfi: ~
Archivo Editar Ver Terminal Solapas Ayuda
unamfi:~# dpkg -L openvpn
./
/etc
/etc/openvpn
/etc/openvpn/update-resolv-conf
/etc/network
/etc/network/if-up.d
/etc/network/if-up.d/openvpn
/etc/network/if-down.d
/etc/network/if-down.d/openvpn
/etc/bash_completion.d
/etc/bash_completion.d/openvpn
/etc/default
/etc/default/openvpn
/etc/init.d
/etc/init.d/openvpn
/usr
/usr/sbin
/usr/sbin/openvpn
/usr/share
/usr/share/man
/usr/share/man/man8
/usr/share/man/man8/openvpn.8.gz
/usr/share/doc
/usr/share/doc/openvpn
/usr/share/doc/openvpn/README.auth-pam
/usr/share/doc/openvpn/README.down-pam
/usr/share/doc/openvpn/AUTHORS
/usr/share/doc/openvpn/PORTS
/usr/share/doc/openvpn/README
/usr/share/doc/openvpn/copyright
/usr/share/doc/openvpn/examples
/usr/share/doc/openvpn/examples/sample-config-files
/usr/share/doc/openvpn/examples/sample-config-files/loopback-server
/usr/share/doc/openvpn/examples/sample-config-files/README
/usr/share/doc/openvpn/examples/sample-config-files/xinetd-server-config
/usr/share/doc/openvpn/examples/sample-config-files/openvpn-startup.sh
/usr/share/doc/openvpn/examples/sample-config-files/openvpn-shutdown.sh
/usr/share/doc/openvpn/examples/sample-config-files/office.up

```

Figura 5.21 Contenido de archivos que tiene el software OPENVPN.

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

Tabla 5.1 Archivos de configuración instalados en el Sistema Operativo.

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

5.3 Configuración de los Parámetros de Red

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

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

La IP fija requiere lo siguiente para proveer lo mencionado

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

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

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

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

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

```

unamfi:/home/redunam# ls
archivos_homero_14042011 Desktop SERVIDOR1.png SERVIDOR3.png
cursoper1 fiel SERVIDOR2.png UserManual.pdf
unamfi:/home/redunam# cd /
unamfi:/# ls
bin dev initrd.img media proc selinux tmp vmlinuz
boot etc lib mnt root srv usr
cdrom home lost+found opt
unamfi:/# ifconfig eth0 132.254.
unamfi:/# ifconfig eth1 192.168.
unamfi:/#
  
```

El comando: ifconfig eth0 132.xxx.xxx.xxx netmask 255.255.255.0

Figura 5.22 interfaces de red de eth0 y eth1.

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

```

cdrom home lost+found opt sbin sys var
unamfi:/# ifconfig eth0 132.254.xxx.xxx netmask 255.255.255.0
unamfi:/# ifconfig eth1 192.168.xxx.xxx netmask 255.255.255.0
unamfi:/# ifconfig
eth0
  Link encap:Ethernet HWaddr 00:0d:87:4e:8a:8b
  Inet addr:132.254.xxx.xxx Bcast:132.254.xxx.xxx Mask:255.255.255.0
  UP BROADCAST MULTICAST MTU:1500 Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
  Interrupt:23 Base address:0xd400

eth1
  Link encap:Ethernet HWaddr 00:06:4f:5d:55:c1
  Inet addr:192.168.xxx.xxx Bcast:192.168.xxx.xxx Mask:255.255.255.0
  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:18 errors:0 dropped:0 overruns:0 carrier:18
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B) TX bytes:2609 (2.5 KiB)
  Interrupt:19 Base address:0xec00

lo
  Link encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:16436 Metric:1
  RX packets:159 errors:0 dropped:0 overruns:0 frame:0
  TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:50469 (49.2 KiB) TX bytes:50469 (49.2 KiB)

tun0
  Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
  
```

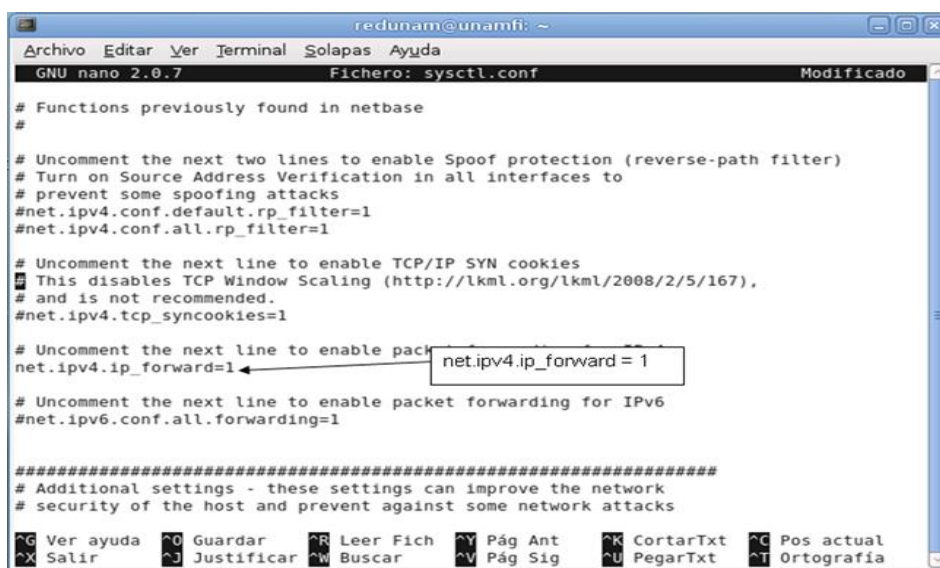
Figura 5.23 Interfaces de red con sus respectivas IP's fijas y privadas

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

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

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



```

redunam@unamfi: ~
GNU nano 2.0.7          Fichero: sysctl.conf          Modificado

# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# This disables TCP Window Scaling (http://lkml.org/lkml/2008/2/5/167),
# and is not recommended.
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward = 1

# Uncomment the next line to enable packet forwarding for IPv6
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks

^G Ver ayuda  ^O Guardar  ^R Leer Fich ^Y Pág Ant  ^K CortarTxt ^C Pos actual
^X Salir      ^J Justificar ^W Buscar   ^V Pág Sig  ^U PegarTxt  ^T Ortografía
  
```

Figura 5.24 Configuración de sysctl.conf

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

```

redunam@unamfi: ~
Archivo Editar Ver Terminal Solapas Ayuda
redunam@unamfi:~$ su -
Contraseña:
unamfi:~#
unamfi:~#
unamfi:~#
unamfi:~# ls
unamfi:~# cd /
unamfi:/# ls
bin    dev    initrd.img  media  proc  selinux  tmp
boot  etc    lib         mnt    root  srv      usr
cdrom  home  lost+found  opt    sbin  sys      var
unamfi:/# apt-get install arno-iptables-firewall
    
```

El comando: apt-get install arno-iptables-firewall

Figura 5.25 Comando para realizar la instalación del firewall

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

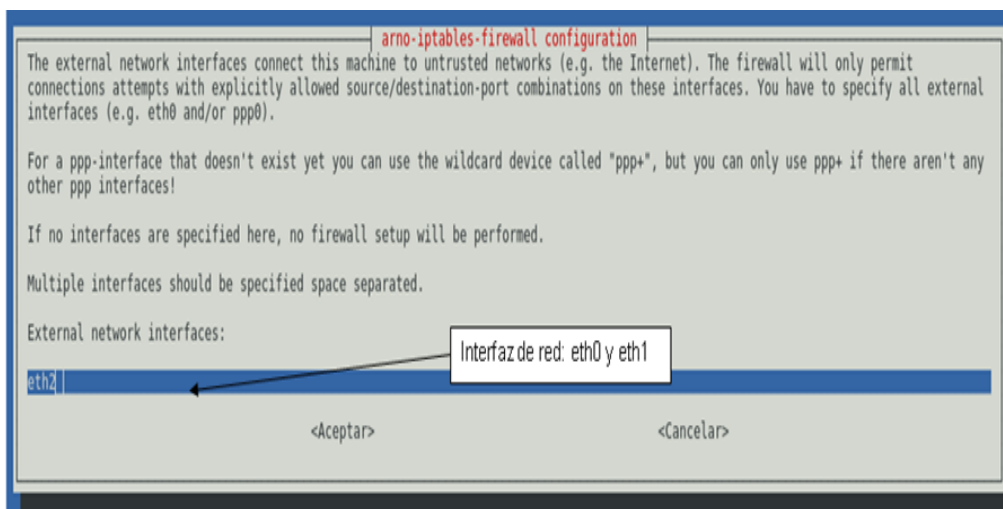


Figura 5.26 Configuración en modo gráfico

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

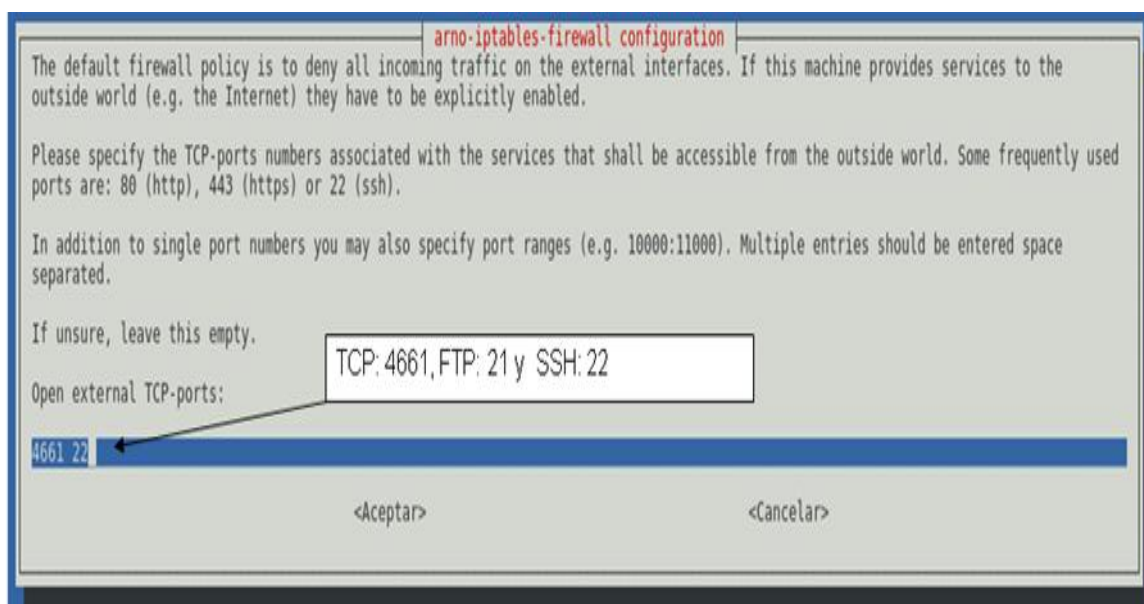


Figura 5.27 Puertos de activación de TCP

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

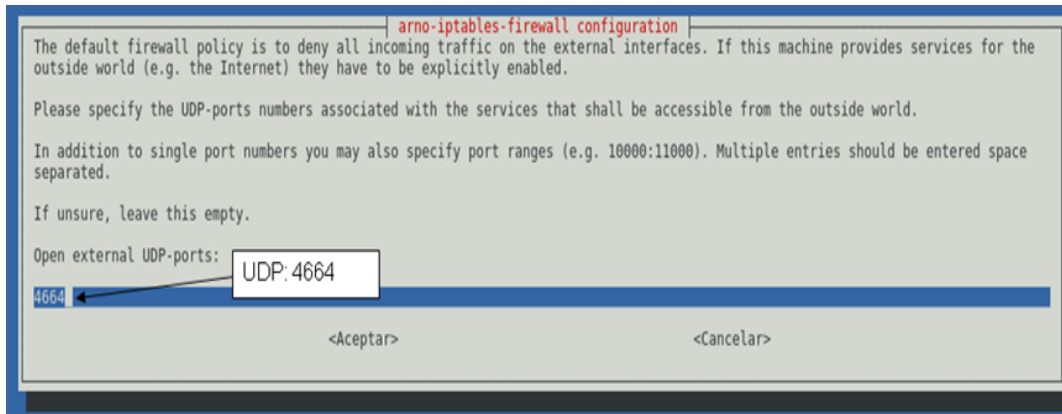


Figura 5.28 Activación del puerto UDP

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

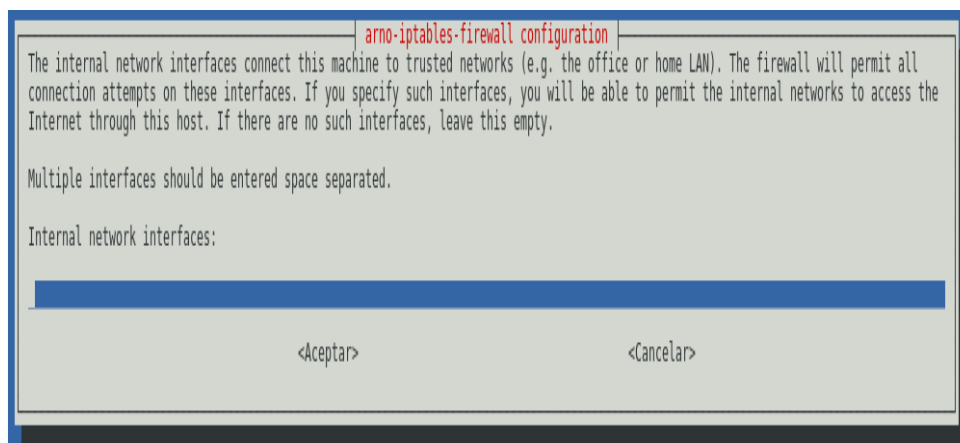


Figura 5.29 Interfaces de red activadas

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

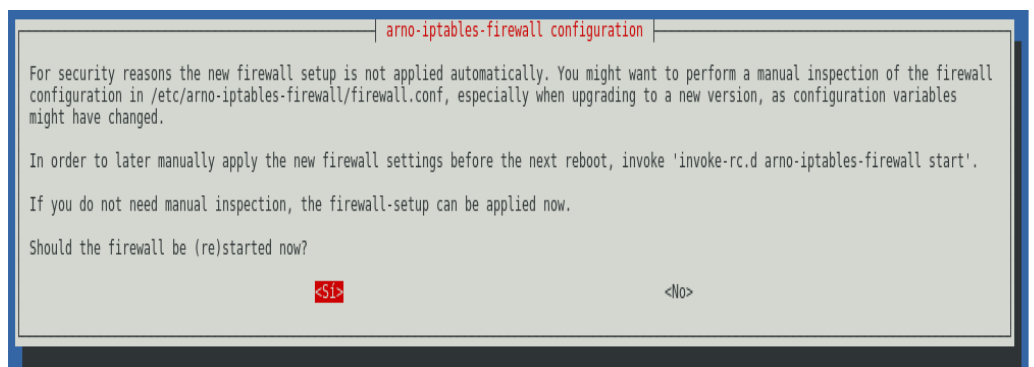


Figura 5.30 Continuación de la instalación

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

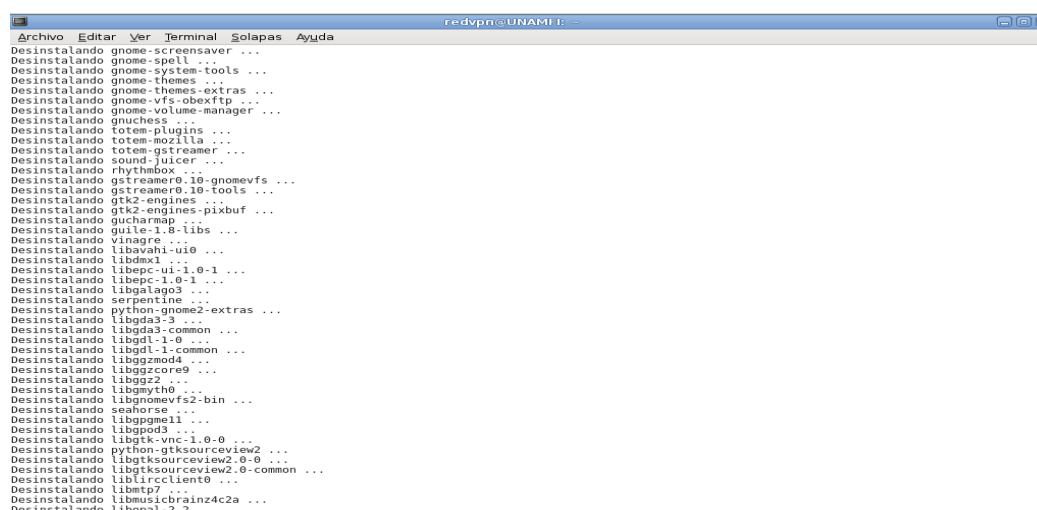


Figura 5.31 Proceso de la desinstalación en modo gráfico de Debian

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

```

redvpn@UNAMI: ~
~/proc/ setup done...
Setting up firewall chains
Setting default INPUT/FORWARD policy to DROP
Using loglevel 'info' for syslogd

Setting up firewall rules:
-----
Accepting packets from the local loopback device
Enabling setting the maximum packet size via MSS
Enabling mangling TOS
Logging of stealth scans (mmap probes etc.) enabled
Logging of packets with bad TCP-flags enabled
Logging of INVALID TCP packets disabled
Logging of INVALID UDP packets disabled
Logging of INVALID ICMP packets disabled
Logging of fragmented packets enabled
Logging of access from reserved addresses enabled
Reading custom rules from /etc/arno-iptables-firewall/custom-rules
Checking for (user) plugins in /usr/share/arno-iptables-firewall/plugins...
  UFW plugin v0.12
  Loaded 1 plugin(s)...
Setting up INPUT policy for the external net (INET):
  Enabling support for DHCP-assigned-IP (DHCP client)
  Logging of explicitly blocked hosts enabled
  Logging of denied local output connections enabled
  Packets will NOT be checked for private source addresses
  Allowing the whole world to connect to TCP port(s): 4661 22
  Allowing the whole world to connect to UDP port(s): 4664
  Denying the whole world to send ICMP-requests(ping)
  Logging of dropped ICMP-request(ping) packets enabled
  Logging of dropped other ICMP packets enabled
  Logging of possible stealth scans enabled
  Logging of (other) connection attempts to PRIVILEGED TCP ports enabled
  Logging of (other) connection attempts to PRIVILEGED UDP ports enabled
  Logging of (other) connection attempts to UNPRIVILEGED TCP ports enabled
  Logging of (other) connection attempts to UNPRIVILEGED UDP ports enabled
  Logging of other IP protocols (non TCP/UDP/ICMP) connection attempts enabled
  Logging of ICMP flooding enabled
Setting up OUTPUT policy for the external net (INET):
  Allowing all (other) ports/protocols
Applying INET policy to external interface: eth2 (without an external subnet specified)
Security is ENFORCED for external interface(s) in the FORWARD chain

Dec 09 4:51:15 UNAMI: firewall.rules.applied
Configurando lynx-cur (2.8.7dev9-2.1) ...
Configurando lynx (2.8.7dev9-2.1) ...
Procesando disparadores para menu ...
Leyendo lista de paquetes... 0%
Leyendo lista de paquetes... 0%
  
```

Figura 5.32 Nuevos archivos del firewall

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

```

redvpn@UNAMI: ~
~/proc/ setup done...
Setting up firewall chains
Setting default INPUT/FORWARD policy to DROP
Using loglevel 'info' for syslogd

Setting up firewall rules:
-----
Accepting packets from the local loopback device
Enabling setting the maximum packet size via MSS
Enabling mangling TOS
Logging of stealth scans (mmap probes etc.) enabled
Logging of packets with bad TCP-flags enabled
Logging of INVALID TCP packets disabled
Logging of INVALID UDP packets disabled
Logging of INVALID ICMP packets disabled
Logging of fragmented packets enabled
Logging of access from reserved addresses enabled
Reading custom rules from /etc/arno-iptables-firewall/custom-rules
Checking for (user) plugins in /usr/share/arno-iptables-firewall/plugins...
  UFW plugin v0.12
  Loaded 1 plugin(s)...
Setting up INPUT policy for the external net (INET):
  Enabling support for DHCP-assigned-IP (DHCP client)
  Logging of explicitly blocked hosts enabled
  Logging of denied local output connections enabled
  Packets will NOT be checked for private source addresses
  Allowing the whole world to connect to TCP port(s): 4661 22
  Allowing the whole world to connect to UDP port(s): 4664
  Denying the whole world to send ICMP-requests(ping)
  Logging of dropped ICMP-request(ping) packets enabled
  Logging of dropped other ICMP packets enabled
  Logging of possible stealth scans enabled
  Logging of (other) connection attempts to PRIVILEGED TCP ports enabled
  Logging of (other) connection attempts to PRIVILEGED UDP ports enabled
  Logging of (other) connection attempts to UNPRIVILEGED TCP ports enabled
  Logging of (other) connection attempts to UNPRIVILEGED UDP ports enabled
  Logging of other IP protocols (non TCP/UDP/ICMP) connection attempts enabled
  Logging of ICMP flooding enabled
Setting up OUTPUT policy for the external net (INET):
  Allowing all (other) ports/protocols
Applying INET policy to external interface: eth2 (without an external subnet specified)
Security is ENFORCED for external interface(s) in the FORWARD chain

Dec 09 4:51:15 UNAMI: firewall.rules.applied
Configurando lynx-cur (2.8.7dev9-2.1) ...
Configurando lynx (2.8.7dev9-2.1) ...
Procesando disparadores para menu ...
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Leyendo la información de estado extendido
Inicializando el estado de los paquetes... Hecho
Escribiendo la información de estado extendido... Hecho
Leyendo las descripciones de las tareas... Hecho

UNAMI:/etc# ls
acpi                cron.weekly        group-              ld.so.conf          muttrc              python2.5          smartd.conf
adduser.conf        cron.weekly        gshadow             ld.so.conf.d        muttrc.d            python2.5.conf    smartmontools
adjtime             cups                gsasl               libao.conf          nano                rc0.d              sound
aliases             cups                gsasl.mech.conf    libgda-3.0          nanorc              rc1.d              spamassassin
alsa                debconf.conf       gtk-2.0            libpaper.d          netataik            rc2.d              ssh
alternatives        debian.version     hal                locale.alias        netcsid.conf       rc3.d              ssl
anacrontab          default            hdparm.conf        locale.gen          network             rc4.d              sudoers
analog.cfg          defoma             hibernation        localtime           NetworkManager     rc5.d              sysctl.conf
apache2             dhcp3              hibernate          logcheck            news                rc6.d              sysctl.d
apparmor.d          dictionaries-common hosts                logrotate.conf     news                rc.local           terminfo
apt                 dpkg               hosts.allow         logrotate.d         nsswitch.conf       rc5.d             toxef
arno-iptables-firewall email-addresses     hosts.deny          lsb-base            openoffice          reportbug.conf    timezone
at.deny             environment        iceweasel          lynx-cur            openvpn             resolvconf        ts.conf
avahi               esound             idmappd.conf       magic               pam.conf            resolv.conf       ucf.conf
bash.bashrc        exim4              inetd.conf          magic.mime          pango               rat                udev
bash_completion    exim4              inetd.conf          mailcap             pango               rpc                ufw
bash_completion.d  exports            inittab            mailcap.order       paperize            rsyslog.conf     updatedb.conf
bind               fonts              inittab            mailcap.order       passwd              rsyslog.d         update-notifier
bluetooth          foomatic           inittab            mailname            pcscia              sane.d            vim
bonobo-activation gal.conf           inittab            manpath.conf        perl                scsi_id.conf     w3m
ca-certificates    gconf              iproute2           menu                php                 security          wgetrc
ca-certificates.conf gdm                issue.net          menu-methods        pm                  security          wodim.conf
calendar           gimp               issue.net          mime-types          postgreSQL          sensors.conf      wpa_supplicant
console            gnome               java               mke2fs.conf        postgresql-common  services         x11
console-tools      gnome-vfs-2.0      kde3               modprobe.d          profile             shadow            xdg
cron.d              gnome-vfs-mime-magic kernel-img.conf    modules            protocols           shadow            xml
cron.daily         gre.d              kernel-loops.conf modprobe            protocols           shadow            xdg
cron.hourly        groff              ldap               motd.tail           purple              shells
cron.monthly       group              ld.so.cache        mtab                python              skel
UNAMI:/etc#
  
```

Figura 5.33 Directorio de arno-iptables-firewall

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

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

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

```
ext_if="eth0"
```

```
ext_if_dhcp_ip=0
```

```
int_if="eth1"
```

```
internal_net="132.xxx.xxx.xxx/24"
```

```
nat=1
```

```
trusted_if="tun+"
```

```
open_tcp="22"
```

```
open_udp="1194"
```

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

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

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

5.4 Configuración del servidor

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

```
UNAMFI:~# install openssl
```

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

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

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

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

```

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

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

```

Figura 5.35 Certificado de autenticación

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

```

Terminal
Archivo Editar Ver Terminal Solapas Ayuda
gnome-vfs-2.0      network      ucf.conf
gnome-vfs-mime-magic NetworkManager udev
gre.d             networks     ufw
groff            news         updatedb.conf
group            nsswitch.conf update-notifier
group-          ntp.conf     vga
gshadow          openoffice   vim
gshadow-        openvpn      w3m
gssapi_mech.conf opt          wgetrc
gtk-2.0          pam.conf     wodim.conf
hal              pam.d        wpa_supplicant
hdparm.conf      pango        X11
hesiod.conf      papersize    xdg
hibernate        passwd       xml
unamfi:/etc# cd openvpn/
unamfi:/etc/openvpn# ls
ca.crt  clientes  easy-rsa  servidor.crt  update-resolv-conf
ca.key  dh1024.pem servidor.conf servidor.key
unamfi:/etc/openvpn# cd easy-rsa/
unamfi:/etc/openvpn/easy-rsa# ls
build-ca          build-key-server  list-crl          revoke-full
build-dh          build-req         Makefile          sign-req
build-inter      build-req-pass    openssl-0.9.6.cnf.gz vars
build-key        clean-all        openssl.cnf       whichopensslcnf
build-key-pass   inherit-inter     pkitsol
build-key-pkcs12 keys              README.gz
unamfi:/etc/openvpn/easy-rsa# nano vars
unamfi:/etc/openvpn/easy-rsa# cd keys/
unamfi:/etc/openvpn/easy-rsa/keys# ls
01.pem  ca.key      cliente2.crt  index.txt
02.pem  client1.crt cliente2.csr  index.txt.attr
03.pem  client1.csr cliente2.key  index.txt.attr.old
ca.crt  client1.key dh1024.pem   index.txt.old
server.crt server.csr
unamfi:/etc/openvpn/easy-rsa/keys# cp ca.* dh1024.pem server.crt server.key /etc/openvpn
    
```

Figura 5.38 Copia de archivos del directorio keys

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

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

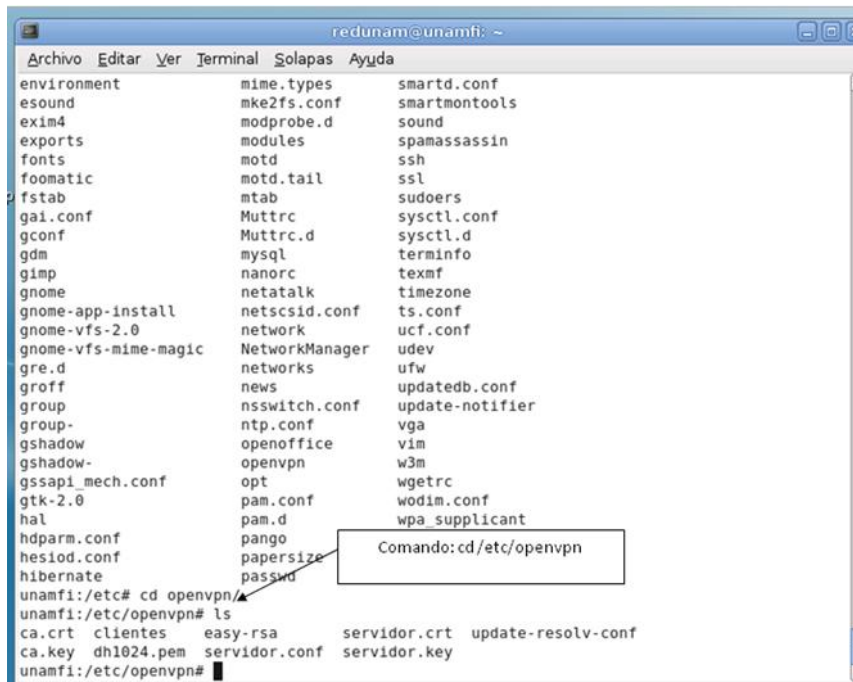


Figura 5.39 Archivos que están en el directorio /etc/openvpn para el servidor OPENVPN

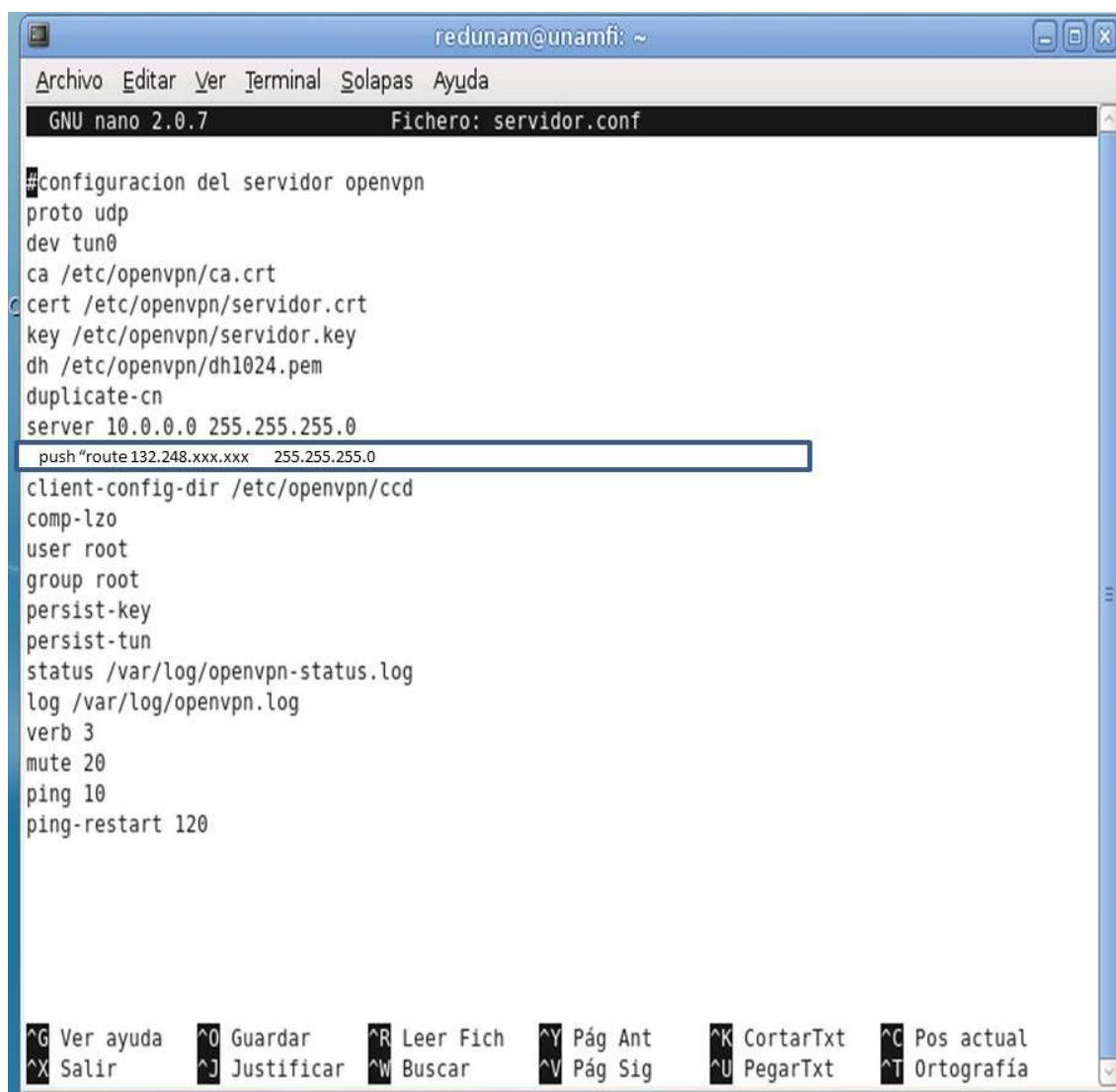
Los archivos importantes que deben estar en el directorio /etc/openvpn para activar el servidor OPENVPN se encuentran en la Tabla 5.2.

Tabla 5.2 Archivos del directorio /etc/openvpn

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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



```

redunam@unamfi: ~
Archivo Editar Ver Terminal Solapas Ayuda
GNU nano 2.0.7 Fichero: servidor.conf
#configuracion del servidor openvpn
proto udp
dev tun0
ca /etc/openvpn/ca.crt
cert /etc/openvpn/servidor.crt
key /etc/openvpn/servidor.key
dh /etc/openvpn/dh1024.pem
duplicate-cn
server 10.0.0.0 255.255.255.0
push route 132.248.xxx.xxx 255.255.255.0
client-config-dir /etc/openvpn/ccd
comp-lzo
user root
group root
persist-key
persist-tun
status /var/log/openvpn-status.log
log /var/log/openvpn.log
verb 3
mute 20
ping 10
ping-restart 120

^G Ver ayuda  ^O Guardar    ^R Leer Fich  ^Y Pág Ant    ^K CortarTxt  ^C Pos actual
^X Salir      ^J Justificar ^W Buscar     ^V Pág Sig    ^U PegarTxt   ^T Ortografía
  
```

Figura 5.40 Reglas de configuración del servidor OPENVPN

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

Tabla 5.3 parámetros del servidor OPENVPN

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

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

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

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

```

unamfi:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0d:87:4e:8a:8b
          inet addr:192.168.1.100  Bcast:192.168.1.1  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:23 Base address:0xd400

eth1      Link encap:Ethernet  HWaddr 00:06:4f:5d:55:c1
          inet addr:132.254.1.100  Bcast:132.254.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:18
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2609 (2.5 KiB)
          Interrupt:19 Base address:0xec00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:171 errors:0 dropped:0 overruns:0 frame:0
          TX packets:171 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56601 (55.2 KiB)  TX bytes:56601 (55.2 KiB)

tun0     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.0.0.1  P-t-P:10.0.0.2  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:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
  
```

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

5.5 Configuración de los clientes

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

```

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

```

Figura 5.42 Creación de certificado y clave del usuario

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

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

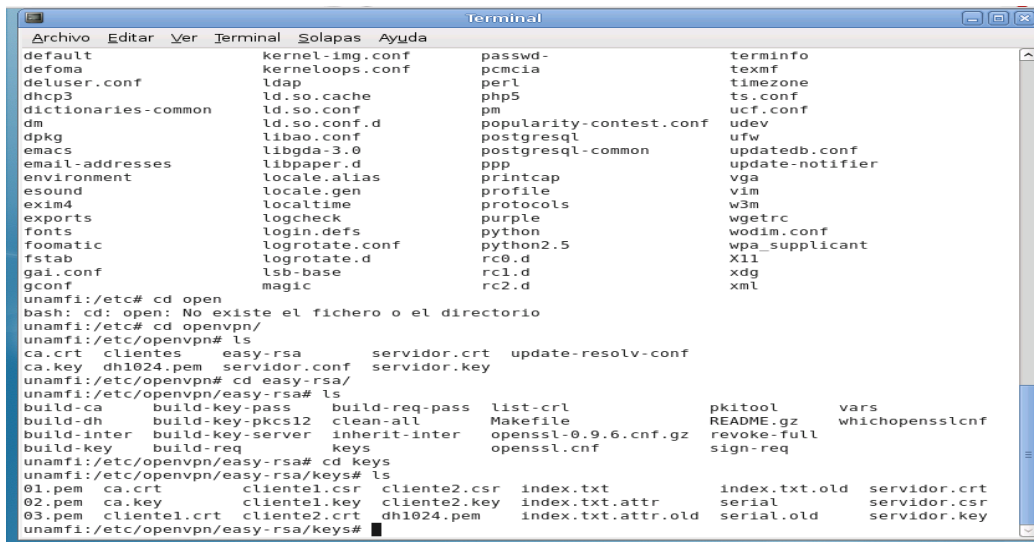


Figura 5.43 Directorio keys, donde los usuarios están creados

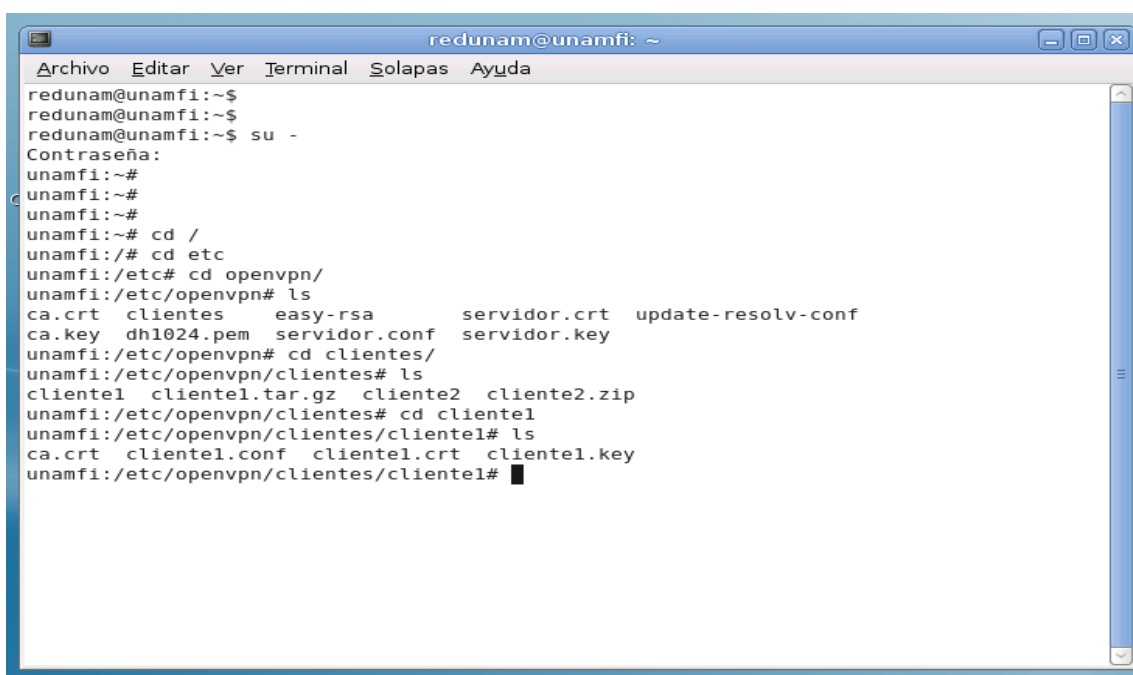
CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

Tabla 5.4 Contenido del archivo cliente

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

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



```

redunam@unamfi:~$
redunam@unamfi:~$
redunam@unamfi:~$ su -
Contraseña:
unamfi:~#
unamfi:~#
unamfi:~#
unamfi:~# cd /
unamfi:/# cd etc
unamfi:/etc# cd openvpn/
unamfi:/etc/openvpn# ls
ca.crt  clientes  easy-rsa      servidor.crt  update-resolv-conf
ca.key  dh1024.pem  servidor.conf  servidor.key
unamfi:/etc/openvpn# cd clientes/
unamfi:/etc/openvpn/clientes# ls
cliente1  cliente1.tar.gz  cliente2  cliente2.zip
unamfi:/etc/openvpn/clientes# cd cliente1
unamfi:/etc/openvpn/clientes/cliente1# ls
ca.crt  cliente1.conf  cliente1.crt  cliente1.key
unamfi:/etc/openvpn/clientes/cliente1#
    
```

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

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

```

#configuracion del cliente openvpn en linux
client
remote unamfi.com
port 1194
proto udp
dev tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/cliente1.crt
key /etc/openvpn/cliente1.key
comp-lzo
log /var/log/openvpn.log
verb 3
mute 20
ping 10
ping-restart 120
persist-key
persist-tun

```

Figura 5.45 Configuración del cliente1

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

Tabla 5.5 Parámetros del cliente1

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

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

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

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

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



Figura 5.46 Pantalla de bienvenida de OpenVPN

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

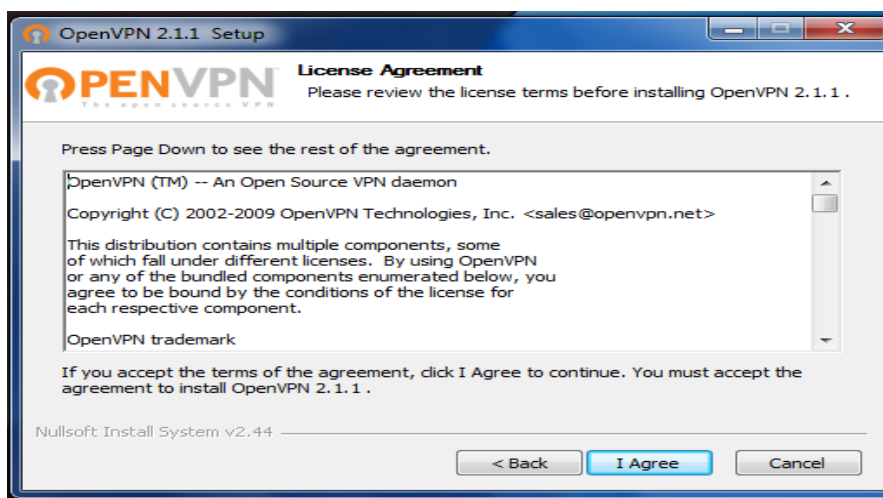


Figura 5.47 Acuerdo de Licencia

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

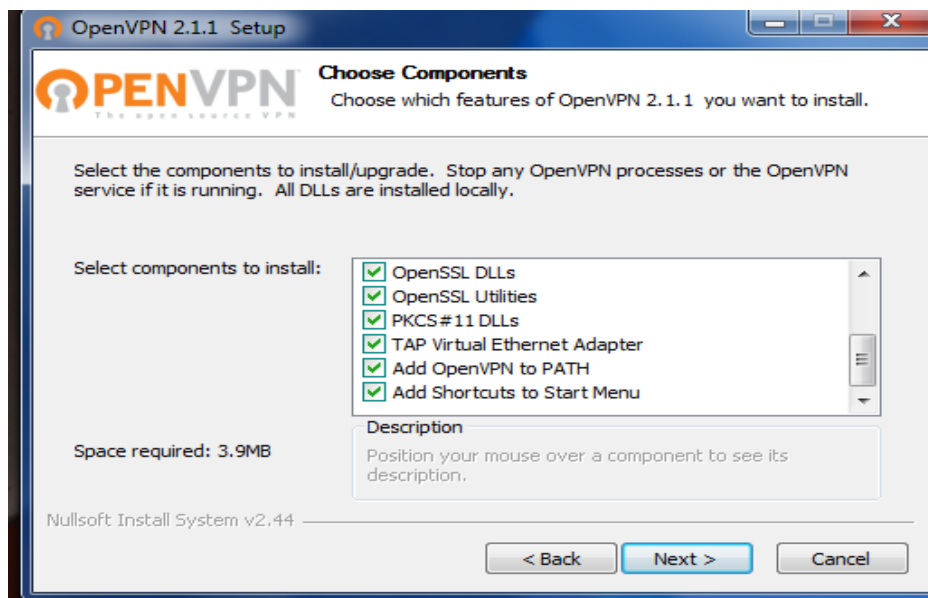


Figura 5.48 Acuerdo de Licencia

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

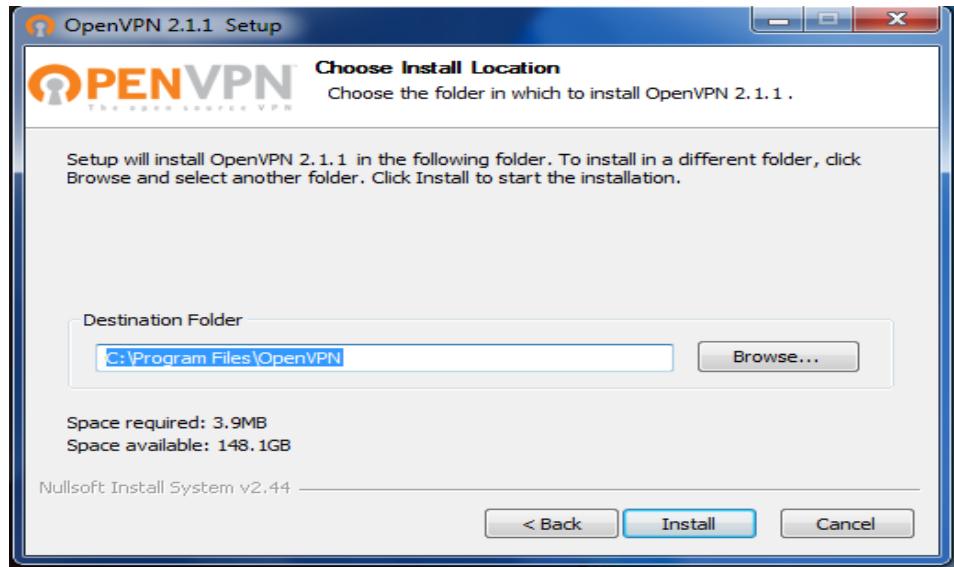


Figura 5.49 Ruta de Instalación de OpenVPN

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

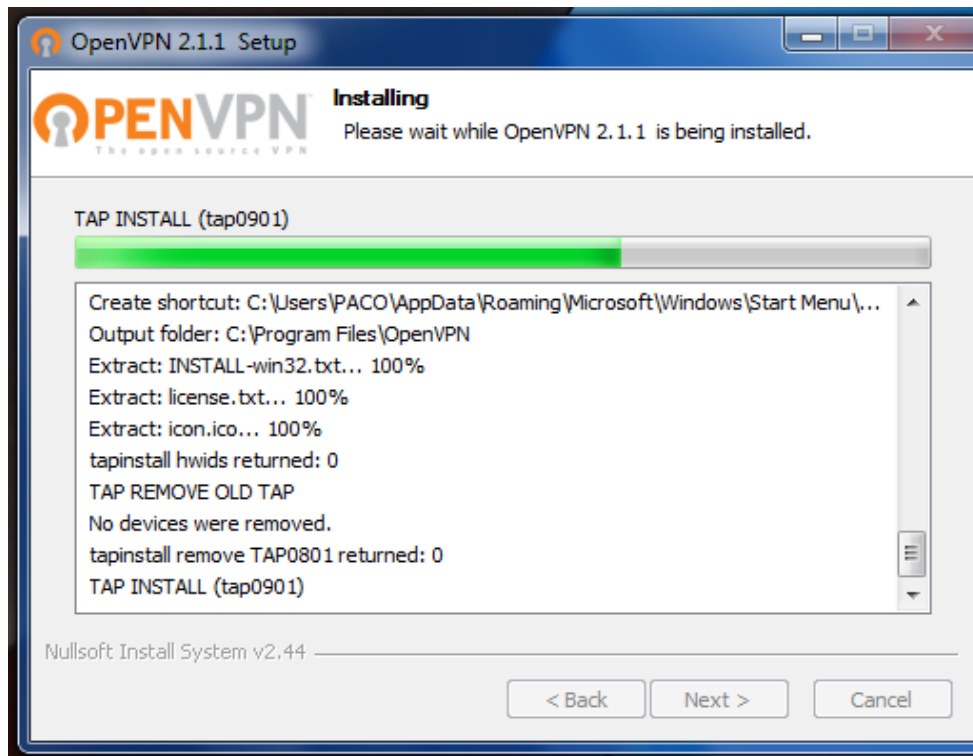


Figura 5.50 Instalación de OpenVPN

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

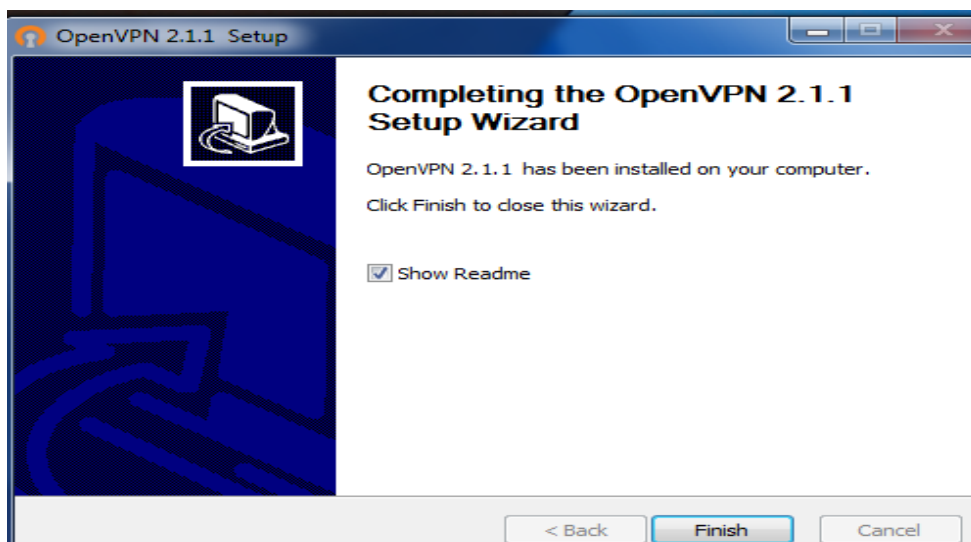


Figura 5.51 Instalación Finalizada

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

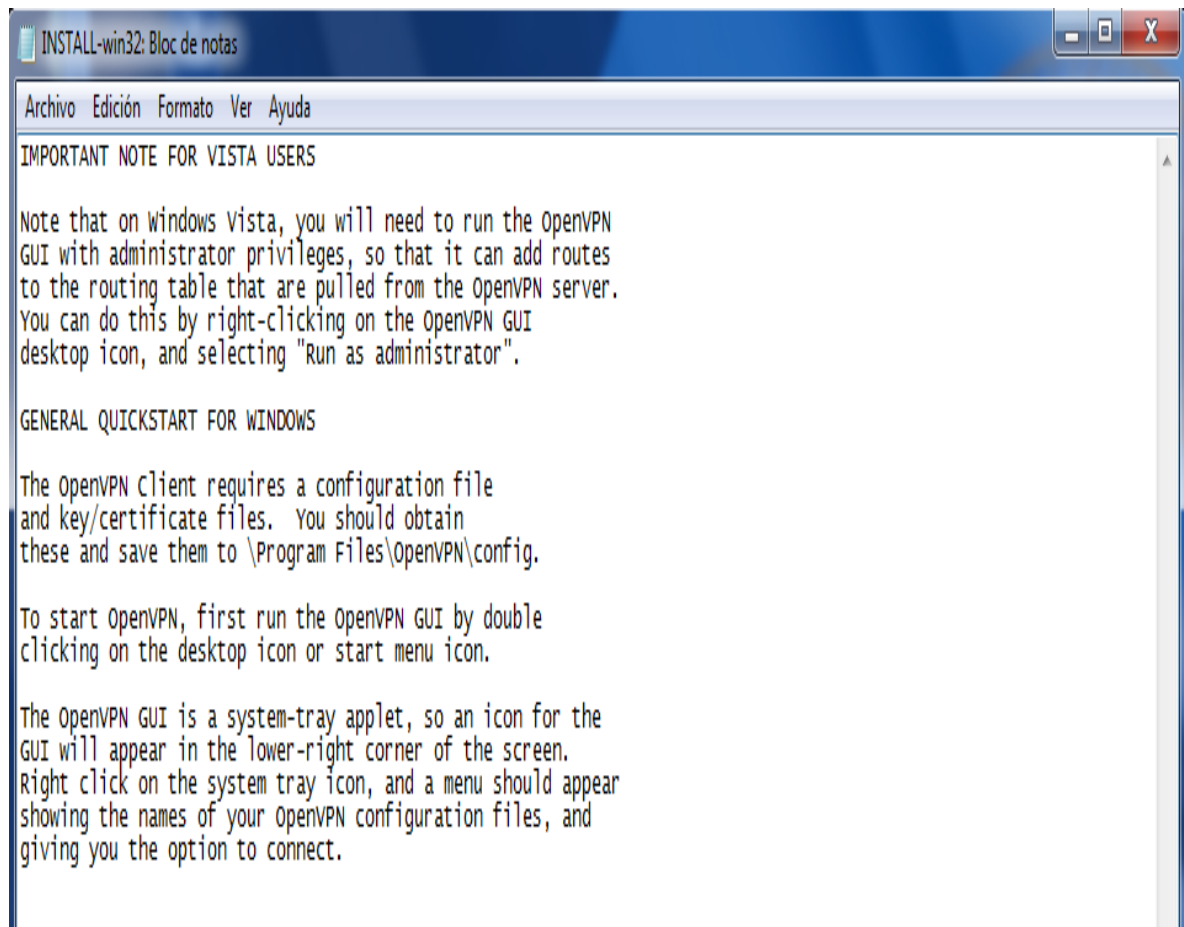


Figura 5.52 Indicaciones del programa OpenVPN.

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

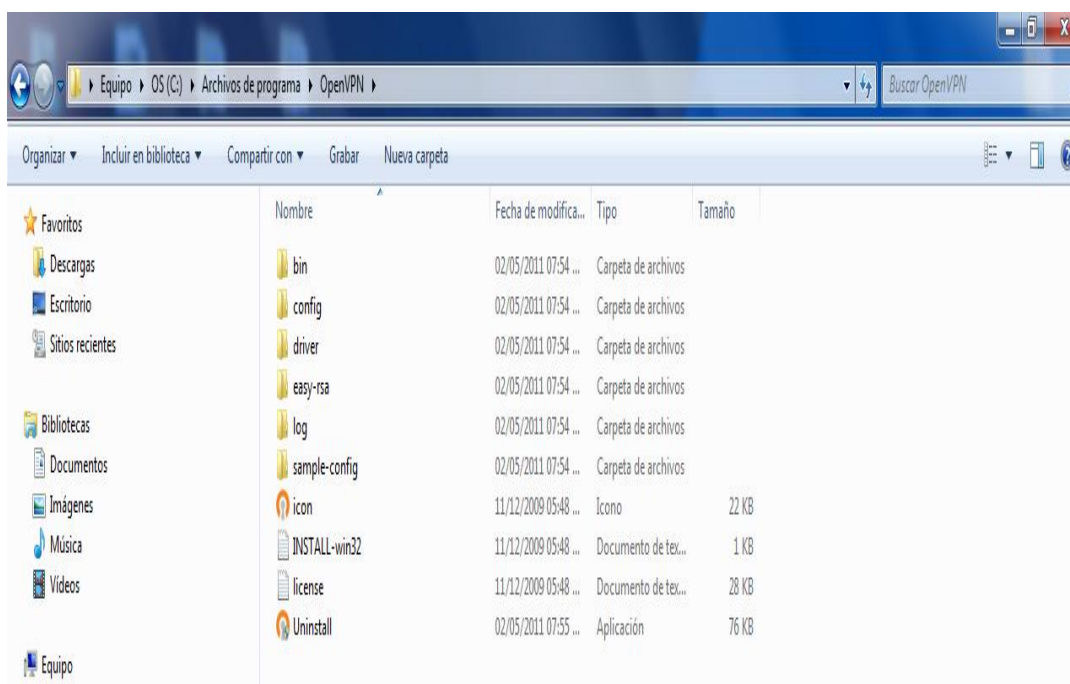


Figura 5.53 Ubicación de la herramienta OpenVPN

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

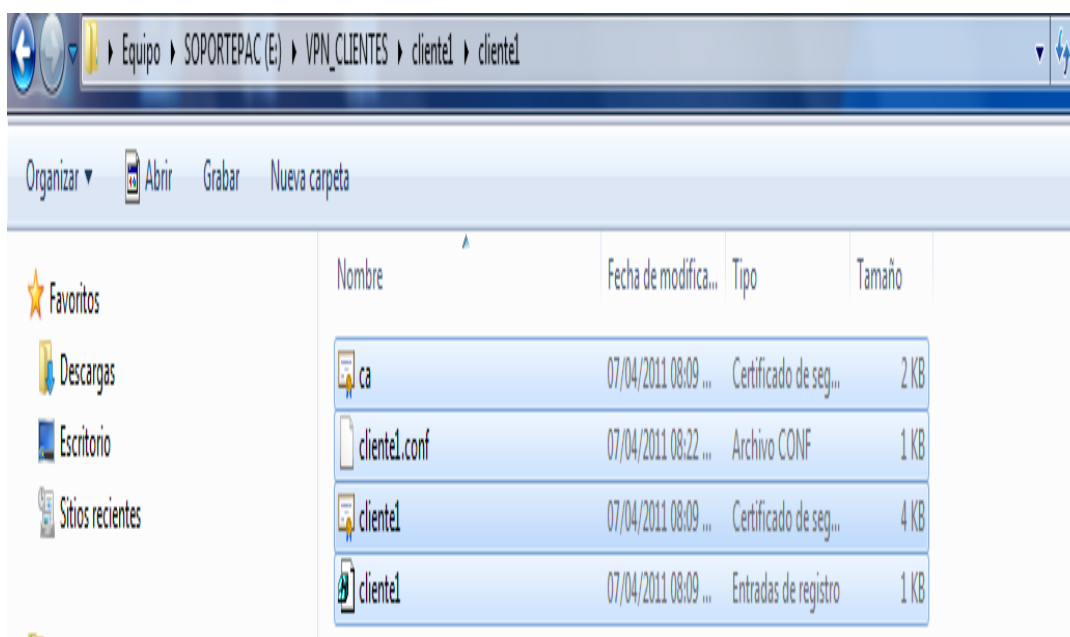


Figura 5.54 Archivos de la carpeta cliente1

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

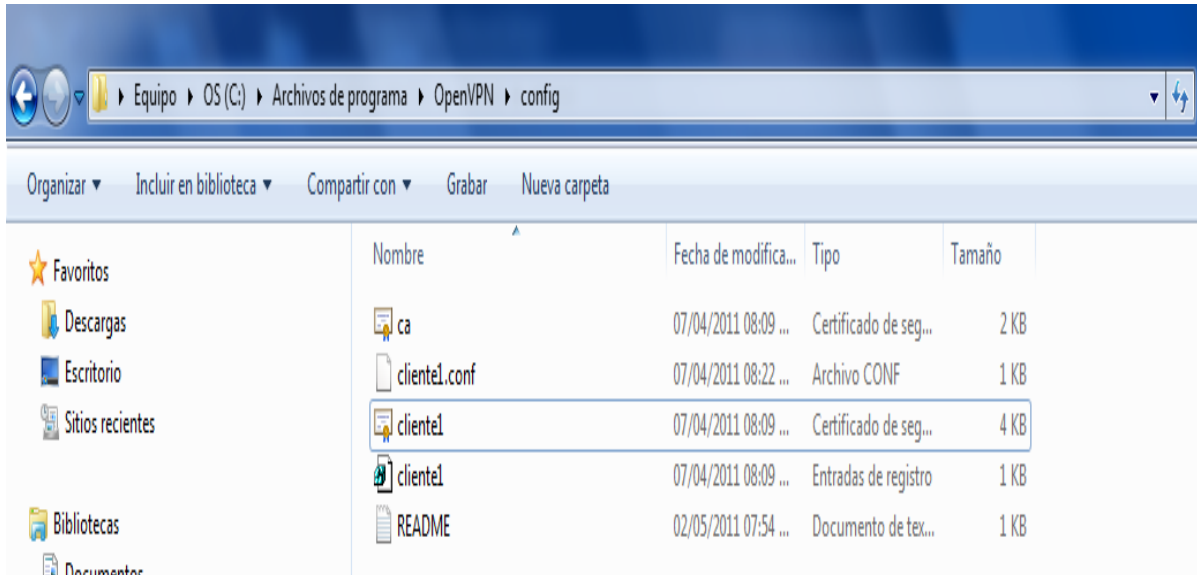


Figura 5.55 Archivos completos de la carpeta config

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



Figura 5.56 Ícono de OpenVPN en Windows

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

5.6 Pruebas

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

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



Figura 5.57 Opciones de OpenVPN en Windows

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

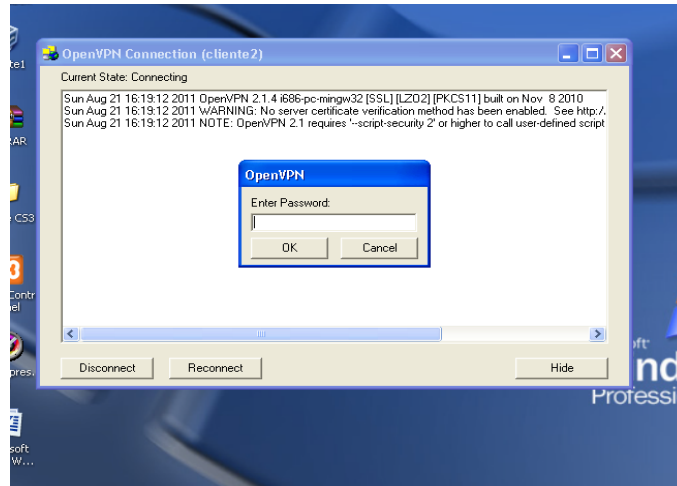


Figura 5.58 Solicitud de la contraseña de acceso a la red remota

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

```

OpenVPN Connection (luis)
Current State: Connected

Sun Sep 25 22:41:26 2011 Data Channel MTU parms [ L:1542 O:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1 ]
Sun Sep 25 22:41:26 2011 Local Options hash (VER=V4): 41690919
Sun Sep 25 22:41:26 2011 Expected Remote Options hash (VER=V4): 530fdded
Sun Sep 25 22:41:26 2011 UDPv4 link local (bound): [undef]:1194
Sun Sep 25 22:41:26 2011 UDPv4 link remote: 132.xxx.xxx.xxx :1194
Sun Sep 25 22:41:26 2011 TLS: Initial packet from 132.xxx.xxx.xxx :1194, sid=fbaf105b960de14
Sun Sep 25 22:41:26 2011 VERIFY OK: depth=1, /C=MX/ST=DF/L=MEXICO/O=PUMAS/CN=PUMAS_CA/emailAddress=unam@pumas.com.mx
Sun Sep 25 22:41:26 2011 VERIFY OK: depth=0, /C=MX/ST=DF/L=MEXICO/O=PUMAS/CN=servidor/emailAddress=unam@pumas.com.mx
Sun Sep 25 22:41:26 2011 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sun Sep 25 22:41:26 2011 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Sun Sep 25 22:41:26 2011 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sun Sep 25 22:41:26 2011 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Sun Sep 25 22:41:26 2011 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Sun Sep 25 22:41:26 2011 [servidor] Peer Connection Initiated with 132.xxx.xxx.xxx :1194
Sun Sep 25 22:41:29 2011 SENT CONTROL [servidor]: 'PUSH_REQUEST' (status=1)
Sun Sep 25 22:41:29 2011 PUSH: Received control message: 'PUSH_REPLY,route 132.xxx.xxx.xxx 255.255.255.0,route 10.0.0.1,topology net30,jcconfig 10.0.6.10.0.0.5'
Sun Sep 25 22:41:29 2011 OPTIONS IMPORT: --iconfig/up options modified
Sun Sep 25 22:41:29 2011 OPTIONS IMPORT: route options modified
Sun Sep 25 22:41:29 2011 ROUTE default_gateway=10.12.17.193
Sun Sep 25 22:41:29 2011 TAP-WIN32 device (Conexión de área local 2) opened: \\.\Global\{5F3ED88C-FC43-4B22-916E-8C074EEA772F}.tap
Sun Sep 25 22:41:29 2011 TAP-Win32 Driver Version 9.8
Sun Sep 25 22:41:29 2011 TAP-Win32 MTU=1500
Sun Sep 25 22:41:29 2011 Notified TAP-Win32 driver to set a DHCP IP/netmask of 10.0.0.6/255.255.252 on interface {5F3ED88C-FC43-4B22-916E-8C074EEA772F} [DHCP-serv: 10.0.0.5, lease-time: 31536000]
Sun Sep 25 22:41:29 2011 NOTE: FlushIpNetTable failed on interface [19] {5F3ED88C-FC43-4B22-916E-8C074EEA772F} (status=5): Acceso
Sun Sep 25 22:41:34 2011 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 w/d=up
Sun Sep 25 22:41:34 2011 C:\WINDOWS\system32\route.exe ADD 132.xxx.xxx.xxx MASK 255.255.255.0 10.0.0.5
Sun Sep 25 22:41:34 2011 Warning: address 132.xxx.xxx.xxx is not a network address in relation to netmask 255.255.255.0
    
```

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

The screenshot shows the MyIP.es website interface. On the left, there are several advertisements and a table of IP details. On the right, a Google Map shows the location of the IP address in Mexico.

Mi direccion ip:	132.XXX.XXX.XXX (copy)
IP País:	Mexico
IP estado:	Distrito Federal
IP ciudad:	Mexico
IP latitud:	19.4342
IP longitudud:	-99.1386
Proveedor:	Universidad Nacional Autonoma de Mexico
Organización:	Universidad Nacional Autonoma de Mexico
Netspeed:	Cable/DSL

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

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

```

ca. C:\windows\system32\cmd.exe
Respuesta desde 132. xxx.xxx.xxx : bytes=32 tiempo=1ms TTL=64
Respuesta desde 132. xxx.xxx.xxx : bytes=32 tiempo=1ms TTL=64
Respuesta desde 132. xxx.xxx.xxx : bytes=32 tiempo<1m TTL=64
Respuesta desde 132. xxx.xxx.xxx : bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 132. xxx-xxxx-xxx :
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\homero>ping 132. xxx-xxxx-xxx

Haciendo ping a 132. xxx.xxx.xxx :on 32 bytes de datos:
Respuesta desde 132. xxx.xxx.xxx bytes=32 tiempo<1m TTL=128
Respuesta desde 132. xxx.xxx.xxx bytes=32 tiempo<1m TTL=128
Respuesta desde 132. xxx.xxx.xxx bytes=32 tiempo<1m TTL=128
Respuesta desde 132. xxx.xxx.xxx bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 132. xxx-xxxx-xxx
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
    
```

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

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

```

Collisions:0 bqueuelen:0
RX bytes:43605 (42.5 KiB) TX Bytes: 43605 (42.5 KiB)

Tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
00
Inet addr:10.0.0.1 P-t-P:10.0.0.2 Mask:255.255.255.255
UP POINTTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX: packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
Collisions:0 bqueuelen:100
RX bytes:0 (0,0,B) TX bytes:0 (0,0,B)

unamfi:## ping 132.xxx.xxx.xxx
PING 132.xxx.xxx.xxx (132.xxx.xxx.xxx) 56(84) bytes of data
4 bytes from 132.xxx.xxx.xxx icmp_seq=1 ttl=64 time=0.072 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=2 ttl=64 time=0.074 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=3 ttl=64 time=0.074 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=4 ttl=64 time=0.089 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=5 ttl=64 time=0.079 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=6 ttl=64 time=0.075 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=7 ttl=64 time=0.077 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=8 ttl=64 time=0.077 rrs
Z
1)+Stopped

unamfi:## ping 132.xxx.xxx.xxx
PING 132.xxx.xxx.xxx (132.xxx.xxx.xxx) 56(84) bytes of data
4 bytes from 132.xxx.xxx.xxx icmp_seq=1 ttl=128 time=1.43 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=2 ttl=128 time=1.05 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=3 ttl=128 time=1.442 rrs
4 bytes from 132.xxx.xxx.xxx icmp_seq=4 ttl=128 time=1.421 rrs
    
```

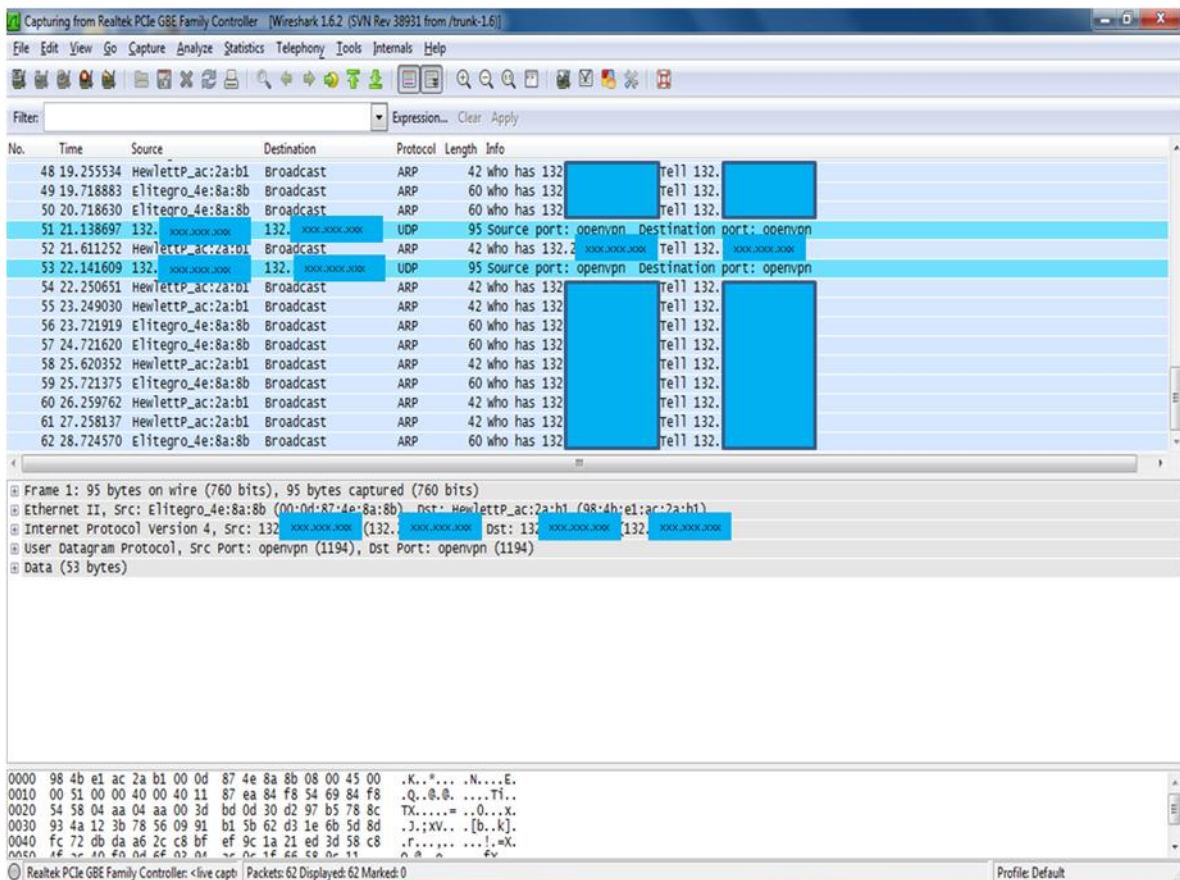
Figura 5.62 Verificación de la comunicación entre el cliente Linux y el servidor OpenVPN

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

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

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



5.63 Captura de paquetes en Wireshark

CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS DE UNA VPN

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

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

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

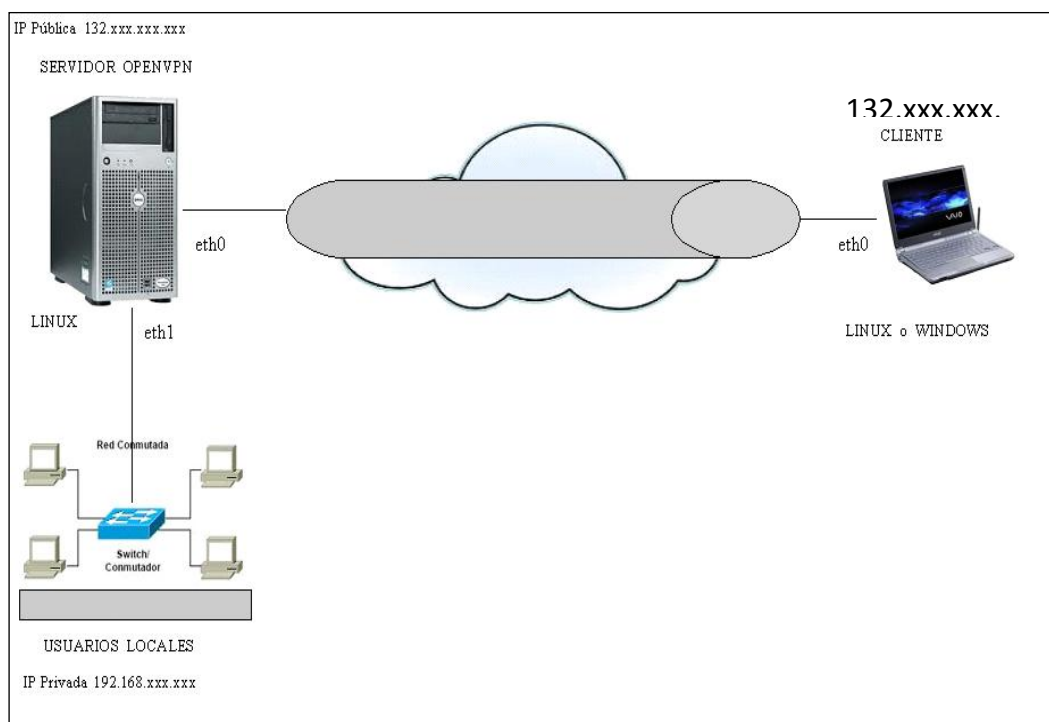


Figura 5.64 Conexión remota del usuario hacia el servidor OPENVPN

