IURRETA INSTITUTUA
Goi-mailako Lanbide-Heziketako Berariazko Institutua

EUSKO JAURLARITZA
GOBIERNO VASCO
HEZKUNTZA UNIBERTSITATE ETA IKERKETA SAILA
DEPARTAMENTO DE EDUCACIÓN, UNIVERSIDADES E INVESTIGACIÓN

OpenVPN

Túneles Cifrados Hacia la Escuela

Versión: 1.0.1

Alfredo Barrainkua Zallo

Diciembre del 2009

Índice

1. Introducción

Cada día es más habitual que los usuarios accedan a las redes de las empresas en modo remoto, desde lugares ajenos a la propia empresa. Los **Road Warriors**, trabajadores que han de utilizar continuamente la carretera, acceden a la red de la empresa desde redes cliente, desde hoteles o desde otro tipo de lugares, con la intención de rellenar peticiones, consultar precios, descargar catálogos, etc...

Este acceso debe de ser lo más cómodo posible. Tiene que simularse en el mayor grado posible el contexto de la propia red. Lógicamente, esta situación tiene que equilibrarse con el nivel de seguridad que requiere la empresa.

La tecnología que permite lograrlo es **VPN**. Por medio de VPN la información se transporta cifrada. Solo los ordenadores de la empresa (normalmente portátiles) pueden acceder, y además los usuarios tienen que autenticarse. A estas VPN se les suele llamar "**tunnel**", porque la información solo va de una parte del túnel a la otra, y desde fuera no se puede ver.

Para hacer VPNs hay diferentes manera. Lo que aquí se trata se basa en la tecnología **SSL/TLS** para cifrar la información. El producto en sí es **OpenVPN.** Hay que recordar que las VPNs desarrolladas con esta tecnología son del nivel de aplicación.

Para conectar el dispositivo **/dev/tun** de la computadora A con el dispositivo **/dev/tun** de la computadora B **OpenVPN** utiliza el siguiente mecanismo: crea una conexión cifrada **UDP** (TCP) por medio de Internet y reenvía el tráfico entre las máquinas A y B. Debido al diseño “erpizia” de las interfazs **TUN** y **TAP** es posible instaurar este enlace mediante un programa que está en espacio de usuario. Así, **OpenVPN** se convierte en un diablo portable entre plataformas, al estilo de **SSH**, y no un módulo específico de un sistema usuario, como **IPSec**.

En nuestro sistema se utilizará **GNU/Debian Linux 4.0** (Etch) y **OpenVPN** como servidor, y como clientes Windows, Mac OSX y Ubuntu. Los clientes Windows habrán de ser Win2000, WinXP, WinVista o Win7.

2. TUN / TAP

El dispositivo TUN es un enlace virtual IP de punto a punto. Por otra parte, el dispositivo TAP es un dispositivo ethernet virtual. No se pueden confundir. En las dos terminaciones de conexión se tendrá que utilizar uno u otro. Por tanto, no se puede poner en los dos extremos de la conexión **-dev-tun** y **-dev-tap**. Se deberá utilizar uno o el otro.

2.1. ¿Qué es bridging?

Con esta técnica se crea una LAN ethernet de área extensa, funcionando en una subred. Para más información práctica, consultar Ethernet Bridging Mini-HOWTO.

2.2. ¿Qué diferencia hay entre bridging y routing?

Bridging y routing son dos métodos para unir sistemas mediante VPN.

2.2.1. Ventajas del bridging

- Los mensajes broadcast se transmiten a toda la VPN. Así se posibilita que el software que necesita LAN broadcast funcione correctamente (que Windows NETBIOS comparta ficheros, búsquedas de red,....).
- No hay que configurar el encaminamiento.
- Funciona con cualquier protocolo de Ethernet: Ipv4, Ipv6, Netware IPX, AppleTalk,....
- Es muy fácil de configurar para los Road Warriors.

2.2.2. Desventajas del bridging

- No es tan eficiente como el routing y no es tan escalable.

2.2.3. Ventajas del routing

- Eficiencia y escalabilidad.
- Permite mejor afinación del MTU, y por lo tanto, más eficiencia.

2.2.4. Desventajas del routing

- Los clientes deberán utilizar un servidor WINS para que funcionen las búsquedas entre redes, por ejemplo utilizando Samba.
- Hay que poner los caminos necesarios para unir todas las redes.
- El software dependiente del broadcast no verá las máquinas del otro extremo de la red VPN.
- Por lo general, solo funcionará con IPv4, y en algunas ocasiones con IPv6, si se aceptan los drivers de los dispositivos TUN de ambos extremos.

2.2.5. Diferencias a nivel de configuración

Cuando un cliente se conecta por medio de un bridge a una red remota, se le asigna una dirección IP, y por tanto, es capaz de conectarse a máquinas remotas como si estuviese conectado en local. La configuración de bridging necesita una herramienta especial del sistema operativo para conseguir un puerto físico y un dispositivo TAP. En Linux, esa herramienta es **brtcl**. En Windows XP, hay que seleccionar el dispositivo TAP-Win32 y la tarjeta ethernet en **Control Panel -> Network Connections**, y haciendo clic con el botón de la derecha, seleccionar **Bridge Connections**.

Cuando un cliente se conecta por medio de routing, utiliza su propia subred, y el encaminamiento se da tanto en el cliente como en el servidor. Así, los paquetes cruzan la VPN. El cliente no tiene porque ser una máquina, puede ser una red de varias máquinas.

El bridging y el routing, funcionalmente son muy parecidos. La principal diferencia es que las VPN con routing no abre mensajes IP broadcast y las VPN con bridging si.

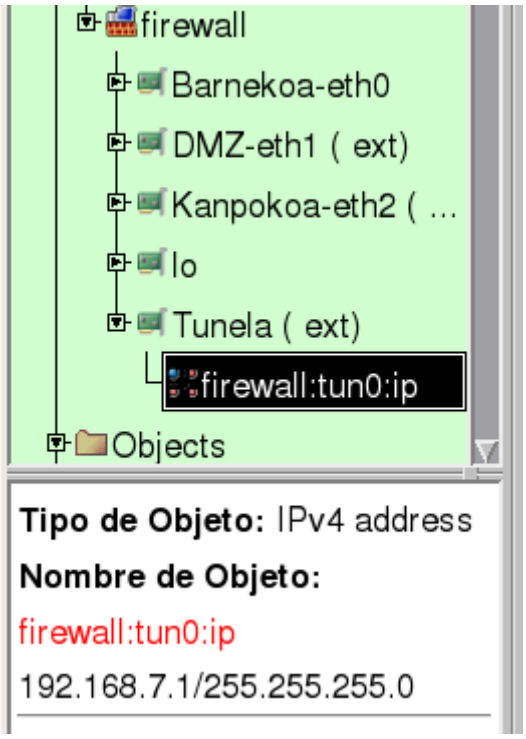
Cuando se hace bridging, hay que utilizar **-dev tap** en ambos extremos de la conexión. Con routing, se puede utilizar tanto **-dev tap** como **-dev tun**, pero ha de ser igual en ambos extremos. **-dev tun** es algo más eficiente en el caso del routing.

3. Configurando el Cortafuegos

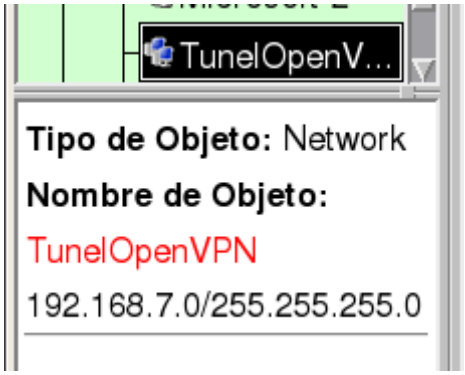
Para permitir las comunicaciones entre la red VPN y la red de la escuela, habrá que cambiar la configuración de **FWBuilder**. Vamos a realizarlo en FWBuilder 2.0.9 y 2.1.19.

La red de la VPN es **192.168.7.0/24**. A esta red hay que dejarle acceder por medio de la interfaz pública. Esto hay que realizarlo en la ficha de dicha interfaz (FWB 2.0.9). Posteriormente habrá que permitir la conexión desde esta red a las redes internas y a la DMZ para los protocolos que necesitemos.

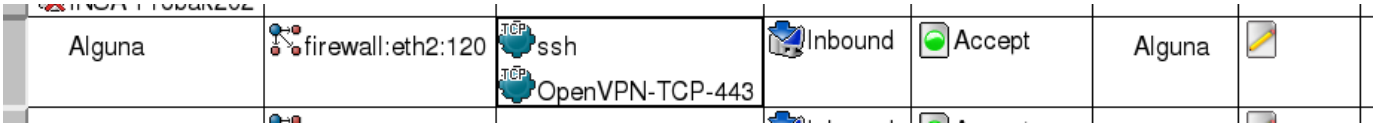
Vamos a definir la interfaz, la red, las reglas, etc en FWBuilder 2.0.9.



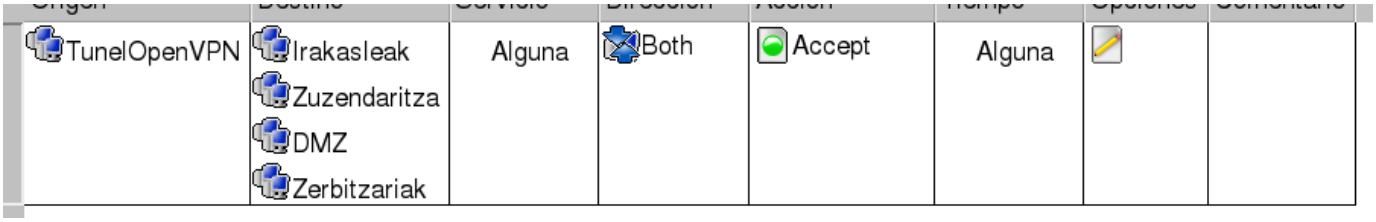
Interfaz del cortafuegos definido.



Hemos definido la red 192.168.7.0/24.

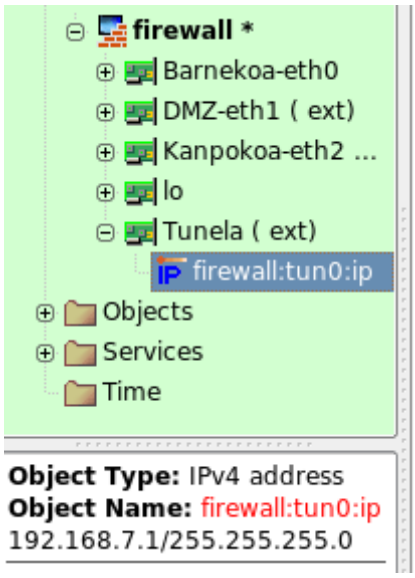


Acceso desde el exterior a la IP correspondiente del cortafuegos para openvpn y ssh (estaba de antes) En la interfase externa.

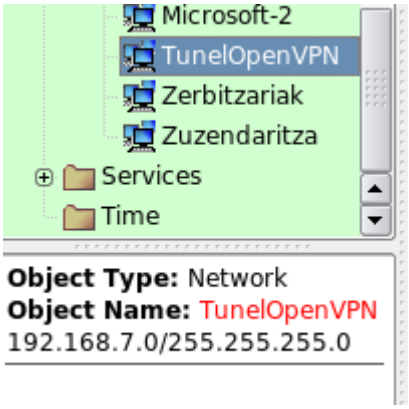


Permisos de conexión desde la interfase del túnel

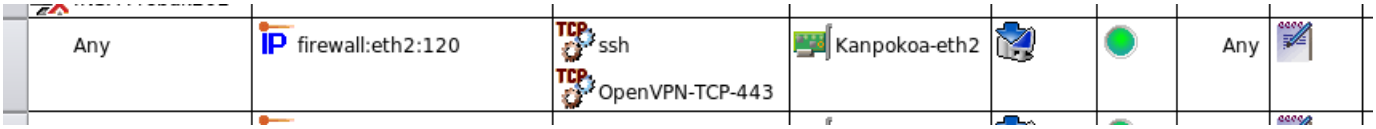
Vamos a realizar lo mismo con la versión 2.2.19 de FWBuilder. En esta versión del programa no se crean las pestañas correspondientes a las interfases. Se incluyen en la pestaña de políticas, pero en la misma, se hace alusión de a qué interfase corresponde la política.



Interfaz del cortafuegos.



La red del túnel definida.



Los permisos de conexión desde el exterior definidos.

Las políticas de comunicación del tunes definidas.

Se puede hilar más fino. Esto es un ejemplo y la seguridad es cuestión de cada administrador. También hay otras formas de hacerlo. Por ejemplo, sin crear el interfase del túnel. En este caso, las políticas no corresponderían al interfaz, sino serían globales.

4. El Servidor

El servidor será un sistema **GNU/Linux Debian 4.0 (Etch)**. Los usuarios necesitaran un certificado y tendrán que autenticarse con nombre y contraseña.

Para el canal VPN se utilizará una interfaz **TUN.** Si no hay que funcionar en modo bridge, ni se utiliza un servidor DHCP para asignar direcciones IP, ni hacen falta mensajes broadcast, es mejor utilizar la interfaz TUN. A día de hoy, hasta los sistemas Windows utilizan el servicio **DNS** para buscar servidores y servicios, por lo que no son tan necesarios los mensajes broadcast. El encaminamiento entre la red de las conexiones OpenVPN y la red interna de la escuela se realizará en el cortafuegos.

4.1. Instalando el servidor

Para utilizar OpenVPN y crear los certificados, hay que instalar los siguientes paquetes:

```
aptitude install vtun openssl liblzo2-2 openvpn
```

4.2. Creando el certificado del servidor

En el anexo A se crea una autoridad certificadora, y con ella se creará el certificado del servidor. El certificado será para el cortafuegos y lo llamaremos **fw-cert.pem**.

```
cd /etc/zertifikatuak
openssl req -new -days 1095 -keyout fw-key.pem -out fw-req.pem
```

Habrán de seleccionarse las opciones por defecto. En el campo "**Common Name**" se introducirá "**suhesia.iurreta-institutua.net**". Después habrá que introducir la dirección de correo electrónico, "**sare-admin@iurreta-institutua.net**".

Se firmará la petición del certificado mediante nuestra autoridad certificadora. Se solicitará la frase de paso de la clave privada. Nos pedirá la clave de la autoridad certificadora. Introducirla.

```
openssl ca -policy policy_anything -out fw-cert.pem -in fw-req.pem
```

Ahora, deberemos quitarle la contraseña a la clave privada. Así, no se requerirá de ella cada vez que haya que utilizarla. Nos pedirá la contraseña que hemos introducido al crear la solicitud de certificado. introducirla.

```
openssl rsa -out fw-priv.pem -in fw-key.pem
```

Ahora copiaremos al lugar correspondiente el certificado del cortafuegos y la clave privada. También el certificado de la autoridad certificadora.

```
cp /etc/zertifikatuak/fw-cert.pem /etc/openvpn/fw-cert.pem
cp /etc/zertifikatuak/fw-priv.pem /etc/openvpn/fw-priv.pem
cp /etc/zertifikatuak/iurretaCA/ca-cert.pem /etc/openvpn/ca-cert.pem
```

Si se crean los certificados en otro ordenador, habrá que copiarlos de otra forma.

Cambiamos los permisos del fichero de la clave privada del cortafuegos:

```
chmod 600 /etc/openvpn/fw-priv.pem
```

También es necesario crear los parametros DH (Diffie-Hellman). El fichero se creará donde estén las claves **OpenVPN**.

```
cd /etc/openvpn
openssl dhparam -out dh1024.pem 1024
```

4.3. Configurando el servidor

El fichero de configuración será **/etc/openvpn/openvpn.conf**. Este será el contenido:

```
# ¿Servidor TCP o UDP? Usaremos TCP/443 (HTTPS) por ser altamente im,probable que esté filtrado
ese puerto
proto tcp
;proto udp

# ¿En qué dirección hay que aceptar las conexiones?
local 212.142.138.120

# ¿Qué puerto utilizará OpenVPN? HTTPS
port 443

# El tipo de interfaz que utiliza. Será TUN.
# Así, se puede hacer el encaminamiento entre redes
dev tun
;tun-mtu 1500

# Los certificados. El de la autoridad y el cortafueggos y la clave privada
ca /etc/openvpn/ca-cert.pem
cert /etc/openvpn/fw-cert.pem
key /etc/openvpn/fw-priv.pem

# Los parámetros Diffie-hellman
dh /etc/openvpn/dh1024.pem

# Es el servidor y utilizará la red 192.168.7.0/24
# para conectarse.
# El servidor utilizara la dirección 192.168.7.1
server 192.168.7.0 255.255.255.0

# A los clientes siempre se les asignará la misma dirección
# En el fichero ipp.txt se anotará la dirección de cada cliente
ifconfig-pool-persist /var/run/ipp.txt

# Información del encaminamiento para los clientes
# Los clientes deberán cambiar sus tablas de encaminamiento
push "route 10.22.0.0 255.255.255.0"
push "route 10.22.2.0 255.255.255.0"
push "route 10.22.3.0 255.255.255.0"
push "route 172.31.249.0 255.255.255.240"

# Opciones DHCP para los clientes
push "dhcp-option DNS 10.22.0.7"
```

```
push "dhcp-option DNS 10.22.2.7"
push "dhcp-option DNS 10.22.3.7"
push "dhcp-option WINS 10.22.0.7"
push "dhcp-option WINS 10.22.2.7"
push "dhcp-option WINS 10.22.3.7"
push "dhcp-option DOMAIN iurreta-institutua.net"

# Para aceptar diferentes conexiones para cada cliente con el mismo certificado
duplicate-cn

# Para saber si el otro extremo de la conexión sigue activo, cada 10
# segundos se envía una especie de "ping". Si en 120 segundos
# no se recibe respuesta, el otro extremo está "muerto"
keepalive 10 120

# Tipo de cifrado
cipher AES-256-CBC
auth SHA1

# Activar compresión
comp-lzo

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute
status /var/run/openvpn-status.log

# Fichero de registro. Si no se indica nada, se utilizará "syslog"
# Si se utiliza "log", al reiniciar se reescribirá el fichero
# Si se utiliza "log-append", al reiniciar se le añadirá al fichero
# No utilizar ambas opciones
;log         /var/log/openvpn.log
log-append  /var/log/openvpn.log

# Nivel de registro
# 0 → 9
verb 3

# Para renegociar con los clientes las claves después de este tiempo
reneg-sec 28800

# Es necesario usuario y contraseña
plugin /usr/lib/openvpn/openvpn-auth-pam.so login
# El usuario root no accede mediante OpenVPN
#plugin /usr/lib/openvpn/openvpn-down-root.so login ???
```

4.4. Creando los usuarios OpenVPN

Como se ha comentado, los usuarios deberán tener su propio certificado, y deberán introducir su nombre de usuario y contraseña. Para ello, el servidor **OpenVPN,** nuestro cortafuegos, tendrá que comprobar los nombres de usuario y las contraseñas. Para ello se pueden utilizar tanto los usuarios locales, o existenten en un servicio de directorio como OpenLDAP o ActiveDirectory. Veremos con los usuarios locales, por ser más sencillo.

Para crear en el cortafuegos el usuario del ejemplo **alfredobz** ejecutaremos el siguiente comando:

```
useradd -m -k /etc/skel -s /bin/bash alfredobz
```

```
passwd alfredobz
```

Listo! Ahora hay que reiniciar **OpenVPN:**

```
/etc/init.d/openvpn restart
```

Y el servidor ya está en marcha y preparado para aceptar conexiones..

5. Creando los Certificados de los Usuarios

El proceso será el mismo que el utilizado para crear los certificados para el servidor. Crearemos el certificado para el usuario **alfredobz**:

```
cd /etc/zertifikatuak
openssl req -new -days 1095 -keyout alfredobz-key.pem -out alfredobz-req.pem
openssl ca -policy policy_anything -out alfredobz-cert.pem -in alfredobz-req.pem
openssl rsa -out alfredobz-priv.pem -in alfredobz-key.pem
```

Se seleccionarán las opciones por defecto. Después habrá que introducir el nombre del usuario en el campo "**Common Name**" que será "**Alfredo Barrainkua**". La dirección de correo será "**alfredobz@iurreta-institutua.net**".

Se ha creado la clave privada y la petición de certificado. Luego, la autoridad certificadora ha firmado el certificado. Para ello nos pedirá la contraseña de la autoridad certificadora. Al final, se le quita la contraseña a la clave privada, para no tener que introducirla continuamente cada ver que se utiliza. Para realizarlo nos pedirá la contraseña introducida al crear la solicitud del certificado.

Si creamos el certificado en una máquina distinta al cortafuegos, deberemos copiarlo en el directorio **/usr/lib/ssl/misc** del cirtafuegos. En caso contrario ya se encuentra en dicho directorio. Los permisos deberán ser 644. He aquí cómo hacerlo.

```
cp alfredobz-cert.pem /usr/lib/ssl/misc/
chmod 644  /usr/lib/ssl/misc/ alfredobz-cert.pem
```

La clave privada tiene que estar en el ordenador remoto, como se verá en el siguiente capítulo.

TRUCO: Guaaau! Sería un gran avance si tuviésemos un script **sor-ovpn-erab.sh** en el directorio **/root/bin**:

```
# sor-ovpn-erab.sh
# Alfredo Barrainkua 2009, GPL Lizentziapean
# OpenVPN erabiltzaileak sortzeko eskripta

if [ $# -lt 1 ]; then

        echo -n "Erabilpena: $0 erabiltzailea"
        echo
        exit 1
fi

        echo
```

```
        echo "Erabiltzailea sortzen ::: Erabiltzailearen pasahitza behar duzu sartu"
        useradd -m -k /etc/skel -s /bin/null $1
        passwd $1

        cd /usr/lib/ssl/misc

        echo
        echo "Zertifikatu eskabidea sortzen ::: Erabiltzailearen pasahitza eta datuak behar
dituzu sartu"
        openssl req -new -days 1095 -keyout $1-key.pem -out $1-req.pem

        echo
        echo "Zertifikatu eskabidea sinatzen ::: Zertifikatu agintearen pasahitza behar duzu
sartu"
        openssl ca -policy policy_anything -out $1-cert.pem -in $1-req.pem

        echo
        echo "Gako pribatuaren pasahitza kentzen ::: Erabiltzailearen pasahitza behar duzu
sartu"
        openssl rsa -out $1-priv.pem -in $1-key.pem


        cp $1-cert.pem /etc/openvpn/

        cd /root/bin

        exit 0
```

6. Clientes

Se instalará **OpenVPN** en los sistemas más comunes, Windows, Linux y OSX.

6.1. Mac OSX

Para los sistemas MAC OSX se utilizará la aplicación **TunnelBlick**. Se puede descargar de la siguiente dirección:

http://tunnelblick.googlecode.com/files/Tunnelblick_3.0b10.dmg

Instalar y adelante!

Necesitamos un dato del certificado del servidor. Para ver el certificado hacemos:

```
openssl x509 -noout -text -in fw-cert.pem
```

En la salida obtenida hay una línea tal como esta:

Subject: E=EH, ST=Bizkaia, L=Iurreta, OU=Sarea, CN=suhesia.iurreta-institutua.net/emailAddress=sare-admin@iurreta-institutua.net

La necesitaremos para configurar el cliente.

Ahora hay que configurar el cliente. Cada usuario deberá de tener el fichero de configuración **~/Library/openvpn/openvpn.conf**. El contenido será algo así:

```
# Cliente
client

# Tipo de interfaz
dev tun

# Tipo de conexión
proto tcp

# Dirección del servidor y puerto
remote 212.142.138.120 443

# TLS del servidor. Saldrá del certificado del servidor (fw-cert.pem).
# Para ontener la información del certificado hacemos
# openssl x509 -noout -text -in fw-cert.pem
# Sustituir los espacios dentro de un campo con el caracter "_"
# Separar los campos con el caracter "/". Poner al principio tambien!!!
# Todo en una sola línea.
```

```
tls-remote "/C=EH/ST=Bizkaia/L=Iurreta/O=Iurreta_Institutua/OU=Sarea/CN=suhesia.iurreta-
institutua.net/emailAddress=sare-admin@iurreta-institutua.net"

# Intentar siempre resolver el nombre del servidor
resolv-retry infinite

# No utilizar un puerto especial
nobind

# Dejar los privilegios después del inicio. Para máquinas no Windows
user nobody
group nobody

# Entre reinicios, mantener algunas cosas
persist-key
persist-tun

# Parametros SSL/TLS
ca ~/Library/openvpn/ca-cert.pem
cert ~/Library/openvpn/alfredobz-cert.pem
key ~/Library/openvpn/alfredobz-priv.pem

# Utilizar usuario y contraseña
auth-user-pass

# Metodo de cifrado
cipher AES-256-CBC
auth SHA1

# Compresión
comp-lzo

# Fichero de registro
log-append   /var/log/openvpn.log

# Nivel de registro
verb 3

# Renegociación
reneg-sec 0

# Para poder utilizar escripts externos (Linux)
#script-security 2

# Al iniciar y al apagar, utilizar el siguiente script (Solo Linux)
#up /etc/openvpn/update-resolv-conf
#down /etc/openvpn/update-resolv-conf
```

Si se quiere editar el fichero de configuración:

```
sudo /Applications/TextEdit.app/Contents/MacOS/TextEdit ~/Library/openvpn/openvpn.conf
```

Se pondrán en el mismo directorio el fichero **ca-cert.pem** que tiene el certificado de la autoridad certificadora, el certificado del usuario y la clave privada. Los permisos de este último fichero serán 600.

Haciendo clic en el icono de arranque de **TunnelBlick,** seleccionar "**Set Nameserver**".

Ya está todo hecho, como si estuviesemos en la red de la escuela.

6.2. Windows

Para los clientes Windows hay una interfaz gráfica. El paquete que tiene esa interfaz contiene también el programa OpenVPN, pero puede dar problemas. Por lo tanto, se recomienda descargar la aplicación y la interfaz gráfica y luego instalarlas. **EN ESTE ORDEN!**

Utilizaremos estas direcciones para descargar los programas:

http://openvpn.net/release/openvpn-2.0.9-install.exe

http://openvpn.se/files/install_packages/openvpn-2.0.9-gui-1.0.3-install.exe

Luego, y como es típico en Windows, se ejecuta y se instalará todo.

Necesitamos un dato del certificado del servidor. Para ver el certificado hacemos:

```
openssl x509 -noout -text -in fw-cert.pem
```

En la salida obtenida hay una línea tal como esta:

Subject: E=EH, ST=Bizkaia, L=Iurreta, OU=Sarea, CN=suhesia.iurreta-institutua.net/emailAddress=sare-admin@iurreta-institutua.net

La necesitaremos para configurar el cliente.

La configuración se llevará a cabo en el fichero **c:\Archivos de Programa\openvpn\config\openvpn.ovpn**. El contenido será el siguiente:

```
# Cliente
client

# Tipo de interfaz
dev tun

# Tipo de conexión
proto tcp

# Dirección del servidor y puerto
remote 212.142.138.120 443

# TLS del servidor. Saldrá del certificado del servidor (fw-cert.pem).
# Para ontener la información del certificado hacemos
# openssl x509 -noout -text -in fw-cert.pem
# Sustituir los espacios dentro de un campo con el caracter "_"
# Separar los campos con el caracter "/". Poner al principio tambien!!!
# Todo en una sola línea.
tls-remote "/C=EH/ST=Bizkaia/L=Iurreta/O=Iurreta_Institutua/OU=Sarea/CN=suhesia.iurreta-
institutua.net/emailAddress=sare-admin@iurreta-institutua.net"

# Intentar siempre resolver el nombre del servidor
resolv-retry infinite

# No utilizar un puerto especial
nobind

# Dejar los privilegios después del inicio. Para máquinas no Windows
#user nobody
#group nobody

# Entre reinicios, mantener algunas cosas
```

```
persist-key
persist-tun

# Parametros SSL/TLS
ca C:\Archivos de Programa\openvpn\config\ca-cert.pem
cert C:\Archivos de Programa\openvpn\config\alfredobz-cert.pem
key C:\Archivos de Programa\openvpn\config\alfredobz-priv.pem

# Utilizar usuario y contraseña
auth-user-pass

# Método de cifrado
cipher AES-256-CBC
auth SHA1

# Compresión
comp-lzo

# Fichero de registro (No Windows)
#log-append  /var/log/openvpn.log

# Nivel de registro
verb 3

# Renegociación
reneg-sec 0
```

Se pondrán en el mismo directorio el fichero **ca-cert.pem** que tiene el certificado de la autoridad certificadora, el certificado del usuario y la clave privada. Los permisos de este fichero deberán de ser 600.

Después, hay que hacer clic en el icono OpenVPN y seleccionar “Conectar”.

6.3. Ubuntu Linux

La instalación del cliente es como la del servidor:

```
aptitude install vtun openssl liblzo2-2 openvpn
```

Necesitamos un dato del certificado del servidor. Para ver el certificado hacemos:

```
openssl x509 -noout -text -in fw-cert.pem
```

En la salida obtenida hay una línea tal como esta:

Subject: E=EH, ST=Bizkaia, L=Iurreta, OU=Sarea, CN=suhesia.iurreta-institutua.net/emailAddress=sare-admin@iurreta-institutua.net

La necesitaremos para configurar el cliente.

El fichero de configuración será **/etc/openvpn/openvpn.conf**. Su contenido es muy parecido al de los ficheros de configuración de Windows y MacOS, pero con una peculiaridad: las dos últimas líneas. Cuando se pone en marcha y se para OpenVPN se ejecutara el script que se indica. El objetivo es cambiar los servidores DNS.

```
# Cliente
client
```

```
# Tipo de interfaz
dev tun

# Tipo de conexión
proto udp

# Dirección del servidor y puerto
remote 212.142.138.120 443

# TLS del servidor. Saldrá del certificado del servidor (fw-cert.pem).
# Para ontener la información del certificado hacemos
# openssl x509 -noout -text -in fw-cert.pem
# Sustituir los espacios dentro de un campo con el caracter "_"
# Separar los campos con el caracter "/". Poner al principio tambien!!!
# Todo en una sola línea.
tls-remote "/C=EH/ST=Bizkaia/L=Iurreta/O=Iurreta_Institutua/OU=Sarea/CN=fsuhesia.iurreta-
institutua.net/emailAddress=sare-admin@iurreta-institutua.net"

# Intentar siempre resolver el nombre del servidor
resolv-retry infinite

# No utilizar un puerto especial
nobind

# Dejar los privilegios después del inicio. Para máquinas no Windows
user nobody
# Para Ubuntu/Debian, el grupo es nogroup
;group nobody
group nogroup

# Entre reinicios, mantener algunas cosas
persist-key
persist-tun

# Parametros SSL/TLS
ca /etc/openvpn/ca-cert.pem
cert /etc/openvpn/alfredobz-cert.pem
key /etc/openvpn/alfredobz-priv.pem

# Utilizar usuario y contraseñaErabiltzaile eta pasahitza erabili
auth-user-pass

# Método de cifrado
cipher AES-256-CBC
auth SHA1

# Compresión
comp-lzo

# Fichero de registro
log-append   /var/log/openvpn.log

# Nivel de registro
verb 3

# Renegociación
reneg-sec 0

# Para poder utilizar escripts externos (Linux)
script-security 2

# Al iniciar y al apagar, utilizar el siguiente script (Solo Linux)
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

En un directorio se pondrán el fichero **ca-cert.pem** que contiene el certificado de la autoridad certificadora, el certificado del usuario y la clave privada. Los permisos de este fichero deberán ser 600.

Ahora tendremos que reiniciar OpenVPN:

```
/etc/init.d/openvpn restart
```

Se introducirá el nombre de usuario y la contraseña y en marcha. Acceso a la escuela.

7. Por hacer

- Conectar dos redes. Para escuelas con dos edificios.
- Utilizar OpenLDAP como back-end para la autenticación de los usuarios

8. Autor

Alfredo Barrainkua Zallo, Responsable de IKT de Iurreta Institutua

Críticas, mejoras, propuestas de cambio y/o preguntas esta dirección:

alfredobz@iurreta-institutua.net

9. Anexo A. Creando la Autoridad Certificadora

Para validar los certificados, necesitamos de una autoridad certificadora. La autoridad certificadora será **iurretaCA**. Vamos a crear la autoridad, para un plazo de tres años. El certificado de la autoridad será auto-firmado. Es decir, nos auto-certificamos.

En el fichero de configuración **/etc/ssl/openssl.cnf**, realizaremos los siguientes cambios:

en la sección **[CA_default]**:

```
dir = ./demoCA                                  -> iurretaCA
default_days = 365                              -> 1095
```

en la sección **[req_distinguished_name]**:

```
countryName_default = AU                        -> EH
stateOrProvinveName_default = Some State        -> Bizkaia
O.organizationName_default = Internet ... Ltd -> Iurreta GLHB Institutua
organizationalUnitName_default = Sarea
```

Añadir la siguiente línea en la misma sección:

```
localityName_default = Iurreta
```

Vamos a crear la estructura de directorios que pide el fichero de configuración **/etc/ssl/openssl.cnf**, en el directorio que deseemos. Por ejemplo, en el directorio **/etc/zertifikatuak**.

```
mkdir /etc/zertifikatuak
chmod 700 /etc/zertifikatuak
cd /etc/zertifikatuak
mkdir -p iurretaCA/certs
mkdir -p iurretaCA/crl
mkdir -p iurretaCA/newcerts
mkdir -p iurretaCA/private
echo 00 > iurretaCA/serial
touch iurretaCA/index.txt
```

Vamos a crear el certificado de la autoridad certificadora. Solo debemos introducir algunas cosas como la contraseña. El resto de datos los coge por defecto del fichero de configuración.

CUIDADO! Como está establecido en el fichero de configuración, la frase de paso tendrá una longitud máxima de 20 caracteres. Por ejemplo: **Toki ona da eskola**.

```
openssl req -new -keyout iurretaCA/private/ca-key.pem -out iurretaCA/certs/ca-req.pem
```

Donde aparecen las opciones por defecto, pulsar RETURN. Luego nos pedirá el nombre del responsable "**Common Name**", e introducimos "**Sare Admninistraria**". Luego nos pide su correo electrónico. Introducimos "**sare-admin@iurreta-institutua.net**".

Ahora firmaremos la solicitud.

```
openssl ca -days 1095 -batch -selfsign -extensions v3_ca -keyfile iurretaCA/private/ca-key.pem -out iurretaCA/newca.pem -in iurretaCA/certs/ca-req.pem
```

Ahora le damos el formato x509 al certificado.

```
openssl x509 -days 1095 -signkey iurretaCA/private/ca-key.pem -out iurretaCA/ca-cert.pem -in iurretaCA/newca.pem
```

Listo. Ya estamos preparados para crear certificados para nuestra escuela.