Generación de una nueva cuenta VPN

Dentro de srv-firewall (A.K.A. gorgoroth o firewall) nos introducimos en la carpeta de los ficheros de conf de OpenVPN.

$ cd /etc/openvpn/easy-rsa/2.0

Ejecutamos el script de generación de claves para el usuario:

```
$ source ./vars
$ ./build-key USUARIO*
```

* El usuario consiste en el primer caracter del identificador nombre seguido del apellido, (eje. Mikel Blanco ⇒ mblanco)

nos hará una serie de cuestiones que procederemos a contestar con lógica:

```
gorgoroth:/etc/openvpn/easy-rsa/2.0# ./build-key mblanco
Generating a 1024 bit RSA private key
.....................................++++++
.........................++++++
writing new private key to 'mblanco.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]:ES
State or Province Name (full name) [CA]:Bi
Locality Name (eg, city) [SanFrancisco]:Bilbao
Organization Name (eg, company) [Fort-Funston]:Merkatu
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [mblanco]:
Email Address [me@myhost.mydomain]:mblanco@merkatu.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ES'
stateOrProvinceName   :PRINTABLE:'Bi'
localityName          :PRINTABLE:'Bilbao'
```

```
organizationName      :PRINTABLE:'Merkatu'
commonName            :PRINTABLE:'mblanco'
emailAddress          :IA5STRING:'mblanco@merkatu.com'
Certificate is to be certified until May  1 14:07:36 2020 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

los certificados ya se han generado y se encuentra en la carpeta keys:

```
$ cd /etc/openvpn/easy-rsa/2.0/keys
```

Dentro de este directorio se habrán generado 3 ficheros:

```
usuario.crt usuario.csr y usuario.key
```

Copiamos los ficheros a algún servidor al que tengamos acceso vía SAMBA para poder recogerlos luego.

```
scp -p usuario.crt nombre_servidor:/path/a/la/carpeta/
scp -p usuario.key nombre_servidor:/path/a/la/carpeta/

(Ej.: scp -p mblanco.crt srv-datos:/merkatu/sat/vpn/)
```

Es momento de generar el directorio de configuración para la máquina cliente. Para ello es necesario crear un directorio con los siguientes archivos:

```
ca.crt usuario.crt usuario.key enrutado.bat y client.ovpn
```

el fichero client.ovpn debe contener algo así:

```
client
dev tun
proto udp
remote bilbao.merkatu.com 1194
resolv-retry infinite
nobind
#Las dos siguientes opciones no van en windows
user nobody
group nobody
persist-key
persist-tun
ca ca.crt
cert usuario.crt
key usuario.key
comp-lzo
verb 4
mute 20
route-method exe
```

```
up enrutado.bat
```

el enrutado.bat deberia tener esta información:

```
route -p add 10.12.13.0 MASK 255.255.255.0 10.12.14.5
```

Nos vamos a la maquina del cliente vpn e instalamos el software:

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

Instalamos el software en la maquina cliente y metemos los ficheros de conf generados en la carpeta:

```
c://Archivos de programa/Openvpn/config
```

Cruzamos los dedos, esperamos a la alineación correcta de los planetas, apretamos el condensador de fluzo y rearrancamos el cliente VPN. Debería poder conectarse.

Eliminación de una cuenta VPN

Dentro de srv-firewall (A.K.A. gorgoroth o firewall) nos introducimos en la carpeta de los ficheros de conf de OpenVPN.

$ cd /etc/openvpn/easy-rsa/2.0

Ejecutamos el script de eliminación de usuario:

```
source ./vars
./revoke-full USUARIO
```

Esto devolverá un mensaje tal que:

```
Using configuration from /root/openvpn/20/openvpn/tmp/easy-rsa/openssl.cnf
DEBUG[load_index]: unique_subject = "yes"
Revoking Certificate 04.
Data Base Updated
Using configuration from /root/openvpn/20/openvpn/tmp/easy-rsa/openssl.cnf
DEBUG[load_index]: unique_subject = "yes"
client2.crt: /C=KG/ST=NA/O=OpenVPN-
TEST/CN=client2/emailAddress=me@myhost.mydomain
error 23 at 0 depth lookup:certificate revoked
```

La última línea nos informa de un error avisando de que el certificado ha sido revocado. Ya hemos terminado.

Instalación y uso de una cuenta VPN

Windows

Descargamos e instalamos la última versión del OpenVpn GUI (Grafical User Interface).

¡¡¡ATENCION!!!! En el caso de Windows Vista/7 la instalación debe hacerse como Administrador, y debemos comentar la línea del enrutado.bat para que no se ejecute. Una vez instalado hay que ejecutarlo también como administrador.

OpenVPN puede correr como daemon, como servicio o desde la línea de comandos, pero también es posible controlar OpenVPN por medio de un front-end grafico o interfaz gráfico de usuario, conocido también como GUI por sus siglas en inglés.

- En primer lugar descargamos la última versión para Windows de OpenVPN disponible aqui.
- Instalamos el programa (esta vez no he hecho capturas de la instalación, pero ya sabéis, siguiente, siguiente, siguiente...)
- Una vez instalado vamos a la ruta donde hemos hecho la instalación, por defecto C:/Archivos de Programa/OpenVPN y entramos en la carpeta “config” dentro de esta carpeta tenemos que introducir los ficheros que vengan en la carpeta config adjunta, sustituyendo los certificados por los de la persona que corresponda y modificando las siguientes líneas del client.ovpn:

```
client
dev tun
proto udp
remote bilbao.merkatu.com 1194
resolv-retry infinite
nobind
#Las dos siguientes opciones no van en windows
user nobody
group nobody
script-security 2 system
persist-key
persist-tun
ca ca.crt
cert usuario.crt
key usuario.key
comp-lzo
verb 4
mute 20
route-method exe
up enrutado.bat
```

- Nota: en caso de querer crear más de una conexión VPN podemos crear carpetas dentro de la carpeta config, cada una de ellas tendrá el nombre de la VPN a la que se conecta y contendrá los certificados necesarios y su correspondiente archivo .ovpn.
- Ejecutamos la aplicación OpenVPN y vemos que se añade un pequeño icono al lado del reloj.
- Hacemos clic derecho en el icono mostrado, nos aparece el nombre de la conexión que hemos configurado antes y si damos clic a Conectar se iniciara la conexión con el servidor VPN

configurado.
- Una vez la conexión es satisfactoria el icono de antes cambia a color verde.

Mac

Hemos utilizado la versión 3.2.6 de Tunnelblick. El programa está disponible aquí.

El archivo de configuración y los certificados son los mismos que se han utilizado para configurar la conexión con el OpenVPN.

Lo que me ha estado dando problemas han sido las DNS. No tuve problemas en abrir la conexión pero no tenía otra forma de acceder al servidor que indicando su dirección IP. El problema es que tenía metidas en la configuración de la tarjeta de red las de Euskaltel (212.55.8.132 y 133) y claro ... No encontraba ningún servidor con nombre srv-web. La solución, dejar sin definir los servidores de nombre.

Una vez conectado, para abrir la unidad de red:

Menu → Ir → Conectarse al Servidor

La dirección al servidor, en el caso de nombre_proyecto sería la siguiente smb:*srv-web/nombre_proyecto/. Utilizamos el protocolo smb (samba) para comunicarnos con Windows.*

From:
https://wiki.merkatu.info/ - **Wiki de merkatu**

Permanent link:
https://wiki.merkatu.info/montaje_vpn?rev=1341822011

Last update: **2017/03/27 17:43**