

# Túneles en el CiberEspacio

## Segunda parte

Allá por el numero 2 de TuxInfo, había publicado la primera parte de esta nota, donde hacia una gran introducción a lo que eran redes privadas virtuales.

En esta ocasión, mostraremos la configuración de otra tecnología para la implementación de VPN's, llamada OPENVPN.

Es un proyecto GNU, que también tiene un cliente en WINDOWS. Puede ser usada en la topología LAN to LAN, en el momento en que todo esta conectado, o también podría ser usada como Perfiles móviles, en este caso, usuarios con Desktops o Notebooks en Windows.

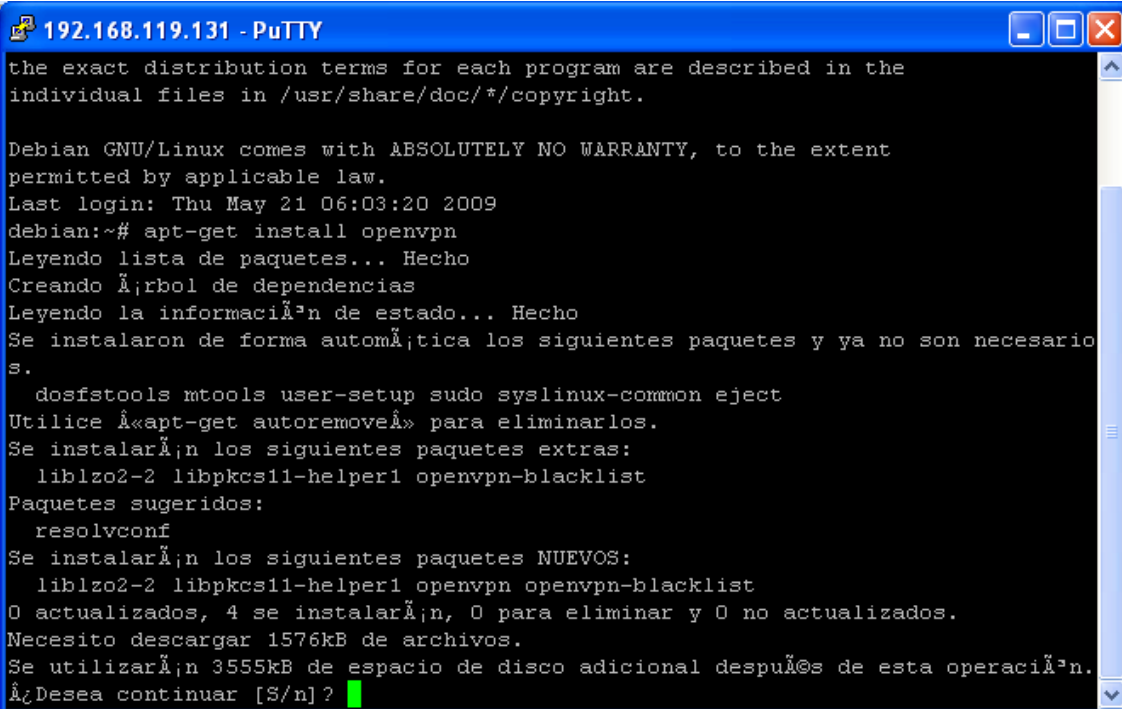
En esta nota, Abarcaremos esta topología.

En la tecnología pptp , el método de autenticación del Usuario , es de Usuario y Password. En esta tecnología, el método que se usa de autenticación, es de certificados digitales. El servidor genera un certificado , y también genera un certificado para los clientes. Luego, hay que alojar los certificados y las keys de los clientes, usando el programa openvpn-gui.

Servidor OPENVPN:

El servidor OPENVPN lo configuraremos en lo que para mi es la mejor distribución de Linux, o sea, debian.

Para ello, instalaremos el paquete, vía apt-get



```
192.168.119.131 - PuTTY
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 21 06:03:20 2009
debian:~# apt-get install openvpn
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalaron de forma automática los siguientes paquetes y ya no son necesario
s.
 dosfstools mtools user-setup sudo syslinux-common eject
Utilice «apt-get autoremove» para eliminarlos.
Se instalarán los siguientes paquetes extras:
 liblzo2-2 libpkcs11-helper1 openvpn-blacklist
Paquetes sugeridos:
 resolvconf
Se instalarán los siguientes paquetes NUEVOS:
 liblzo2-2 libpkcs11-helper1 openvpn openvpn-blacklist
0 actualizados, 4 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 1576kB de archivos.
Se utilizarán 3555kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? █
```

```
192.168.119.131 - PuTTY
¿Desea continuar [S/n]?
Des:1 http://debian.logiclinux.com lenny/main liblzo2-2 2.03-1 [61.5kB]
Des:2 http://debian.logiclinux.com lenny/main libpkcs11-helper1 1.05-1 [42.4kB]
Des:3 http://debian.logiclinux.com lenny/main openvpn-blacklist 0.3 [1068kB]
Des:4 http://debian.logiclinux.com lenny/main openvpn 2.1~rc11-1 [404kB]
Descargados 1576kB en 2min14s (11.7kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete liblzo2-2 previamente no seleccionado.
(Leyendo la base de datos ...
24512 ficheros y directorios instalados actualmente.)
Desempaquetando liblzo2-2 (de ../liblzo2-2_2.03-1_i386.deb) ...
Seleccionando el paquete libpkcs11-helper1 previamente no seleccionado.
Desempaquetando libpkcs11-helper1 (de ../libpkcs11-helper1_1.05-1_i386.deb) ...
Seleccionando el paquete openvpn-blacklist previamente no seleccionado.
Desempaquetando openvpn-blacklist (de ../openvpn-blacklist_0.3_all.deb) ...
Seleccionando el paquete openvpn previamente no seleccionado.
Desempaquetando openvpn (de ../openvpn_2.1~rc11-1_i386.deb) ...
Procesando disparadores para man-db ...
Configurando liblzo2-2 (2.03-1) ...
Configurando libpkcs11-helper1 (1.05-1) ...
Configurando openvpn-blacklist (0.3) ...
Configurando openvpn (2.1~rc11-1) ...
Restarting virtual private network daemon..
debian:~#
```

Una vez que hemos bajado e instalado el software, resta la configuración. Usaremos los scripts que nos provee el paquete para la correcta configuración.

```
debian:~# cp -a /usr/share/doc
doc/ doc-base/
debian:~# cp -a /usr/share/doc/openvpn/examples/easy-rsa/ /etc/openvpn/
debian:~# cd /etc/op
openoffice/ openvpn/ opt/
debian:~# cd /etc/open
openoffice/ openvpn/
debian:~# cd /etc/openvpn/easy-rsa/2.0/
debian:/etc/openvpn/easy-rsa/2.0# ls
build-ca      build-key-server Makefile      sign-req
build-dh      build-req      openssl-0.9.6.cnf.gz vars
build-inter   build-req-pass openssl.cnf    whichopensslcnf
build-key      clean-all     pkitool
build-key-pass inherit-inter  README.gz
build-key-pkcs12 list-crl      revoke-full
debian:/etc/openvpn/easy-rsa/2.0# ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/
2.0/keys
debian:/etc/openvpn/easy-rsa/2.0# ./clean-all
debian:/etc/openvpn/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]:ar
State or Province Name (full name) [CA]:BA
Locality Name (eg, city) [SanFrancisco]:BuenosAires
Organization Name (eg, company) [Fort-Funston]:Linuxin
Organizational Unit Name (eg, section) []:Nada
Common Name (eg, your name or your server's hostname) [Fort-Funston
CA]:VPNServe
Email Address [me@myhost.mydomain]:mguazzardo76@gmail.com
```

¿Que hemos hecho aca?.

```
debian:/etc/openvpn/easy-rsa/2.0# ./vars
Se setean las variables de ambiente.
```

```
debian:/etc/openvpn/easy-rsa/2.0# ./build-ca
Se generaran el certificado. Mas abajo generaremos la key del server.
```

```
debian:/etc/openvpn/easy-rsa/2.0# ./build-key-server vpnserver
```

```
Generating a 1024 bit RSA private key
```

```
.....++++++
```

```
.....++++++
```

```
writing new private key to 'vpnserver.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]:AR
State or Province Name (full name) [CA]:BA
Locality Name (eg, city) [SanFrancisco]:BuenosAires
Organization Name (eg, company) [Fort-Funston]:Linuxin
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [vpnserver]:
Email Address [me@myhost.mydomain]:mguazzardo76@gmail.com
```

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:tupass

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:'AR'
```

```
stateOrProvinceName :PRINTABLE:'BA'
```

```
localityName     :PRINTABLE:'BuenosAires'
```

```
organizationName :PRINTABLE:'Linuxin'
commonName       :PRINTABLE:'vpnsrver'
emailAddress      :IA5STRING:'mguazzardo76@gmail.com'
Certificate is to be certified until May 19 18:06:51 2019 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
```

Acá, se genera la key del server. Fijarse, que la key se llamara vpnsrver.key

Generaremos la key del cliente.

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

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cliente@algo.com
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:'AR'
stateOrProvinceName :PRINTABLE:'BA'
localityName      :PRINTABLE:'BuenosAires'
organizationName  :PRINTABLE:'Linuxin'
commonName        :PRINTABLE:'cliente'
emailAddress      :IA5STRING:'cliente@algo.com'
Certificate is to be certified until May 19 18:09:20 2019 GMT (3650 days)
Sign the certificate? [y/n]:y
```



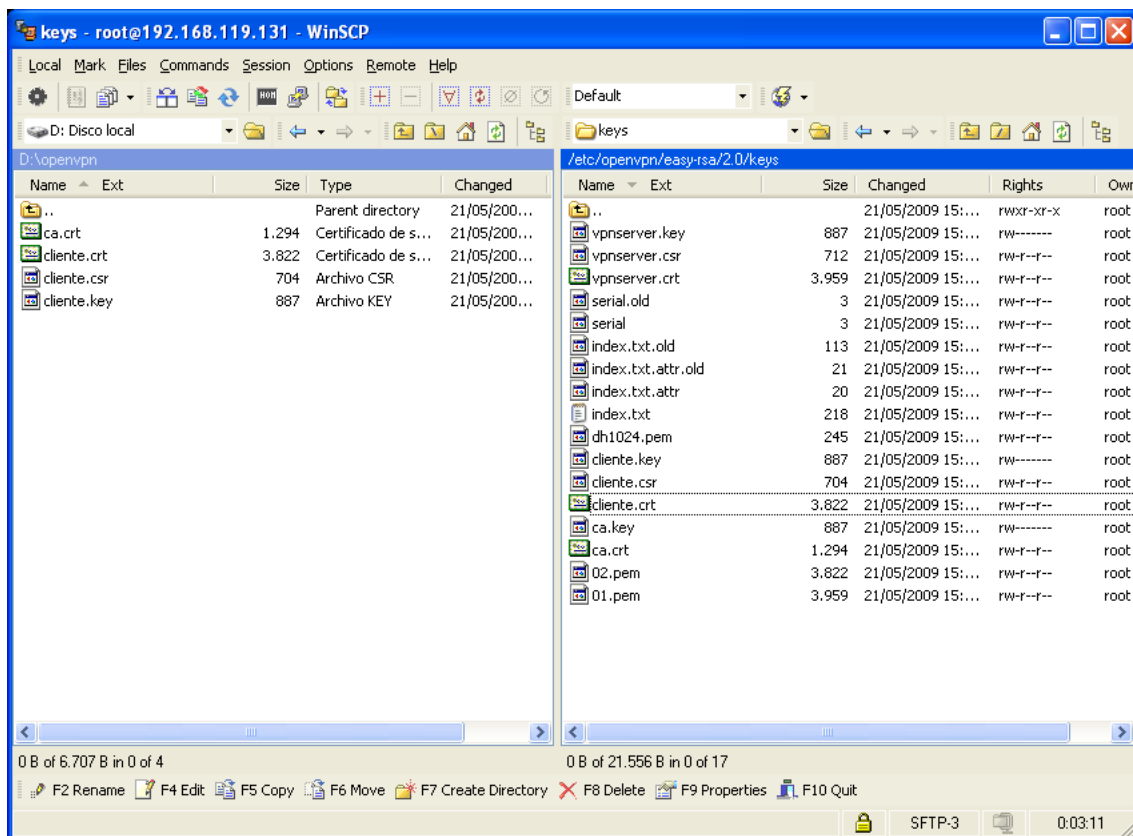
Vemos donde quedaron las keys, y los certs

```
debian:/etc/openssl/easy-rsa/2.0# ls keys
01.pem ca.crt cliente.crt cliente.key index.txt index.txt.attr.old serial
vpnsrvr.crt vpnsrvr.key
02.pem ca.key cliente.csr dh1024.pem index.txt.attr index.txt.old serial.old
vpnsrvr.csr
```

Ahora , copiamos la key y el cert del Server, a la carpeta /etc/openssl

```
debian:/etc/openssl/easy-rsa/2.0# cd keys
debian:/etc/openssl/easy-rsa/2.0/keys# cp ca.crt ca.key serial
serial serial.old
debian:/etc/openssl/easy-rsa/2.0/keys# cp ca.crt ca.key vpnsrvr.crt vpnsrvr.key
dh1024.pem /etc/openssl
```

Luego, copiar cliente

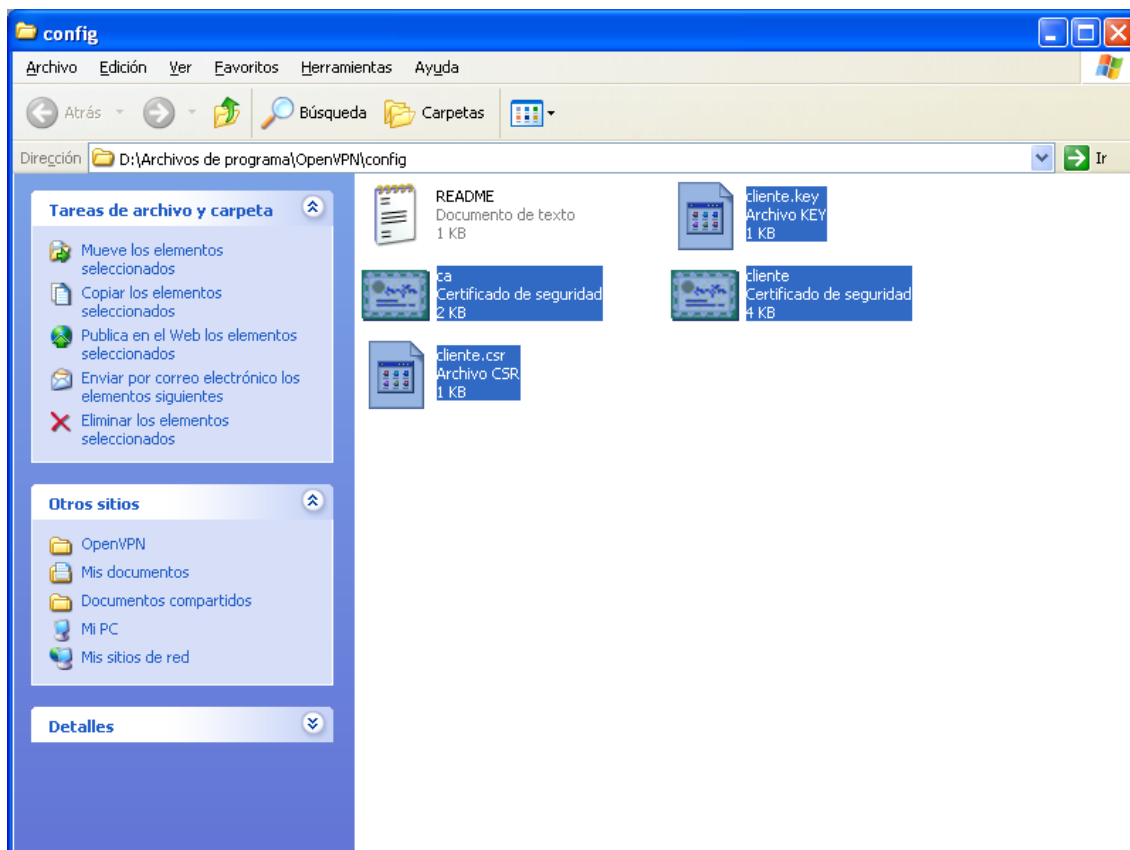


```
debian:/etc/openssl# /etc/init.d/openvpn start
Starting virtual private network daemon: server.
debian:/etc/openssl# ps -ef | grep openvpn
nobody 2161 1 0 14:25 ? 00:00:00 /usr/sbin/openvpn --writepid
/var/run/openvpn.server.pid --daemon ovpn-server --cd /etc/openssl --config
/etc/openssl/server.conf
```

Bajando el cliente pa win

<http://openvpn.se/download.html>

Luego, hay que ir al directorio de configuración



Fundamental, que el archivo de configuración del cliente, tenga lo siguiente:

```
tls-client
client
dev tun
proto udp
remote 192.168.119.131
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert cliente.crt
key cliente.key
comp-lzo
verb 4
```

Lo llamamos cliente.ovpn

Una vez que cargamos el archivo de configuración del cliente, en mi caso en la carpeta

D:\archivos de programa\openvpn\, podremos lanzar la vpn. Un error muy común, es que no encuentre los archivos crt o key, estos deberán estar en la misma carpeta, sino el programa no lo podrá leer.

Si algún error hubiera aparecido, por favor, fijarse en el directorio logs. Ahí mismo podrán encontrar la información de por que aparece el error.

Cualquier duda, mandenme un email a [mguazzardo76@gmail.com](mailto:mguazzardo76@gmail.com)

Saludos

Marcelo Guazzardo <http://mguazzardo.wordpress.com>