Cómo crear un tunel cifrado con OpenVPN para múltiples clientes con autenticación con usuario y password

Instalar y configurar openvpn

Instalar openvpn

```
apt-get install openvpn
```

Instalar openssl

Se necesita para generar los certificados

```
apt-get install openssl
```

Crear los certificados

En el servidor ejecutar

```
computer:/root# cd /usr/share/doc/openvpn/examples/easy-rsa/2.0
computer:/usr/share/doc/openvpn/examples/easy-rsa/2.0# . ./vars
computer:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./clean-all

computer:/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]:ES
State or Province Name (full name) [CA]:CS
Locality Name (eg, city) [SanFrancisco]:Castellon
Organization Name (eg, company) [Fort-Funston]:nombreInstitucion
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [Fort-
```

```
Funston CA]:grupovpn
Email Address [me@myhost.mydomain]:

computer:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-
key-server grupoopenvpn-server
Generating a 1024 bit RSA private key
..............................++++++
.....................................++++++
writing new private key to 'grupoopenvpn-server.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]:CS
Locality Name (eg, city) [SanFrancisco]:Castellon
Organization Name (eg, company) [Fort-Funston]:NombreInstitución
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname)
[grupoopenvpn-server]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/share/doc/openvpn/examples/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:'CS'
localityName          :PRINTABLE:'Castellon'
organizationName      :PRINTABLE:'NombreInstitución'
commonName            :PRINTABLE:'grupoopenvpn-server'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until May  2 11:55:26 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
```

```
computer:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....................................................+.......
+.................................+....+...........
+..............................
+.....................................................................
.................................
+.....................................................................
.....................+.......+.................
+.............................
+..................................
+.....................................+.
+.....................................................................
.........................
+.....................................................................
.....................................................................
.....................................
+.....................................................+++*+
+*++*
```

Copiar los certificados a `/etc/openvpn`

```
computer:/usr/share/doc/openvpn/examples/easy-rsa/2.0# cd keys

computer:/usr/share/doc/openvpn/examples/easy-rsa/2.0/keys# cp
dh1024.pem ca.crt grupoopenvpn-server.* /etc/openvpn/

computer:/usr/share/doc/openvpn/examples/easy-rsa/2.0/keys# cd
/etc/openvpn
```

Configuración y arranque del servidor autenticando con un script

Editar el fichero `/etc/openvpn/openvpn.conf` con el siguiente contenido:

```
tmp-dir /dev/shm
#tmp-dir /tmp
#auth-user-pass-verify /etc/openvpn/auth-ovpn-sql.sh via-env
#auth-user-pass-verify /etc/openvpn/auth-ovpn-sql.sh via-file
auth-user-pass-verify /etc/openvpn/autentica.py via-file
client-cert-not-required
script-security 2

local 10.90.74.33
port 1194
#proto tcp
proto udp
dev tun

dh /etc/openvpn/dh1024.pem
ca /etc/openvpn/ca.crt
```

```
cert /etc/openvpn/grupoopenvpn-server.crt
key /etc/openvpn/grupoopenvpn-server.key

server 192.168.12.0 255.255.255.0
ifconfig-pool-persist ipp2.txt
push "dhcp-option DNS 150.128.98.10"
#push "route 192.168.13.0 255.255.255.0"
client-to-client
keepalive 10 120
#comp-lzo
user nobody
group nogroup
persist-key
persist-tun
verb 5
#script-security 2

cipher BF-CBC
auth SHA1
tls-server

push "redirect-gateway def1"
```

local 10.90.74.33 Esta instrucción sirve para indicar la IP en la que atiende túneles. Si no se pone, atiende en cualquier interfaz. Puede ocurrir que no conteste con la IP esperadas.

server 192.168.12.0 255.255.255.0 es la red sobre la que se va a dar IP a los clientes. El servidor tendrá la 192.168.12.1. Esta IP no se tiene que asignar previamente al servidor.

Para añadir la ruta por defecto a través del tunel, http://openvpn.net/index.php/open-source/documentation/howto.html#redirect

this is a major gripe for me as well: the behaviour on how to start external programs changed quite drastically somewhere between rc7 and rc13 (I believe rc10 was the first version), especially on the Windows platform

http://readlist.com/lists/lists.sourceforge.net/openvpn-users/2/10247.html

hay que añadir `script-security 2` en debian lenny

scritp de autenticación en el servidor

Como se comenta en el man, en este sistema la seguridad y confidencialidad del sistema recae en el script de autenticación del usuario y password, con lo que hay que ser meticuloso con él.

El script debe tener los permisos adecuados de ejecución

En perl

```
#!/usr/bin/perl


# Código perl que comprueba el usuario y el password
```

```
exit(0);   # si la autenticación es correcta

#exit(1);  # si la autenticación no es correcta
```

En bash

```
#!/bin/bash

# Código shell que comprueba el usuario y el password

exit 0 # si la autenticación es correcta

#exit 1  # si la autenticación no es correcta
```

La comprobación del usuario y password se puede llevar a cabo consultando una base de datos, por ejemplo utilizando python

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
''' Autentica un usuario contra postgresql, el usuario y el
password se encuentran almacenados en un fichero que se pasa como
primer parámetro al script (es lo que hace la opción
auth-user-pass-verify /etc/openvpn/autentica.py via-file
del fichero de configuración de openvpn
'''

import sys, getopt, os, string, time
from sys import argv
import psycopg2
import hashlib


def usage():
    print "Utiliza: %s -h" % sys.argv[0]
    print """

    """
    return

def getSize(file):
    """ Obtiene el tamaño de un fichero, pasado como una cadena de
caracteres
    """
    sf=os.stat(file)
    return sf.st_size

def main():


sys.stderr.write('DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDD\n')
    nombre=argv[1]
```

```
    f=open(nombre,"r")

    nuser=f.readline()[:-1].strip()
    npass=hashlib.md5(f.readline()[:-1].strip()).hexdigest()
    f.close()

    #os.system('sleep 60')



    conn = psycopg2.connect("dbname='userapp' user='userapp' 
host='localhost' password='mipass'");
    cur = conn.cursor()
    cur.execute("""SELECT password FROM member where username=
%s""",(nuser,))

    # print nuser
    # print hashlib.md5(npass).hexdigest()
    rows = cur.fetchall()


    if rows:
      palm=rows[0][0]

      if npass==palm:
         print "access accepted"
         return 0
      else:
         print "access denied"
         return 1
    else:
      print "no"
      return 1

if __name__ == '__main__':


sys.stderr.write('DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDD\n')

    a=main()
    #print a
    exit(a)
```

Puesta en marcha del servidor

Para ver la salida del servidor y las conexiones de los clientes se puede ejecutar

```
openvpn /etc/openvpn/openvpn.conf
```

para ponerlo «en explotación» se puede utilizar el script de arranque

```
/etc/init.d/openvpn start
```

Abrir los puertos del cortafuegos

En el fichero `firewall` (o el que se utilice para definir as reglas del cortafuegos) añadir la siguiente regla:

```
iptables -A INPUT -p udp --dport 1194 -j ACCEPT
```

Configuración y arranque de clientes

En todos los casos hay que copiar el fichero `ca.crt` creado en el servidor, que es público, al cliente (en linux en `/etc/openvn/ca.crt`).

Mediante fichero de configuración en Linux

Editar el fichero `/etc/openvpn/openvpn.conf` con el siguiente contenido:

```
client
port 1194
#proto tcp
proto udp
dev tun

remote 150.128.97.59
#push "route 192.168.13.0 255.255.255.0"
#Debe ser push "route 192.168.13.0 255.255.255.0"
keepalive 10 120
#comp-lzo
script-security 2
user nobody
group nogroup
nobind persist-key
persist-tun
verb 3


cipher BF-CBC
auth SHA1


ca /etc/openvpn/ca.crt
#capath .
auth-user-pass
```

Puesta en marcha del cliente

Para ver la salida del servidor y las conexiones de los clientes se puede ejecutar

```
openvpn /etc/openvpn/openvpn.conf
```

para ponerlo «en explotación» se puede utilizar el script de arranque

```
/etc/init.d/openvpn start
```

Mediante el networkmanager en Linux

Instalar el paquete `network-manager-openvpn`.

Ir a `Conexiones VPN` → `Configurar VPN…`, seleccionar la pestaña `VPN` y pulsar el botón `Añadir`.

Seleccionar el tipo de conexión `OpenVPN` y pulsar `Crear`.

En la pestaña `VPN` poner los siguientes datos:

```
Nombre de la Conexión: openvpnClient

Pasarela: servidor.dominio
Tipo: Contraseña
Nombre de Usuario: mm
Contraseña:
Certificado CA: /etc/openvpn/ca.crt
```

La contraseña se puede dejar en blanco.

Pulsar el botón `Avanzado` y seleccionar la pestaña `Seguridad` y poner los siguientes datos:

```
Cifrado: BF-CBC
Autenticación HMAC: SHA-1
```

Ir a `Conexiones VPN` → `openvpnClient` (o el nombre que se le haya dado a la conexión).

Problemas

En algunas distribuciones de GNU/Linux se produce el error «The VPN connection “openvpn” failed because there were no valid VPN secrets», reiniciando el networkmanager parece que se soluciona (https://bugzilla.redhat.com/show_bug.cgi?id=497454#c4).

En http://www.matejunkie.com/how-to-fix-networkmanagers-openvpn-plugin-in-ubuntu-904/ comentan una posible solución

Windows

Instalar openvpn

Crear en `C:\\Archivos\ de\ programa\\OpenVPN\\config\\` un fichero con el siguiente contenido:

```
client
port 1194
#proto tcp
proto udp
dev tun

remote 150.128.97.59
#push "route 192.168.13.0 255.255.255.0"
```

```
keepalive 10 120
#comp-lzo
script-security 2
user nobody
group nogroup
nobind persist-key
persist-tun
verb 3


cipher BF-CBC
auth SHA1


ca C:\\Archivos\ de\ programa\\OpenVPN\\config\\ca.crt
#capath .
auth-user-pass
```

Copiar el certificado del servidor en `C:\\Archivos\ de\ programa\\OpenVPN\\config\\`

Activar el forwarding y firewall en el servidor

Instalar las siguientes reglas en el `firewall`

```
#!/bin/sh
IPTABLES=/sbin/iptables

  $IPTABLES -F -t nat

  $IPTABLES -t nat -A POSTROUTING -o eth0 -s 192.168.12.0/24 -j
MASQUERADE
  $IPTABLES -t nat -A POSTROUTING -s 192.168.12.0/24 -d 0.0.0.0/0
-j SNAT --to 10.228.152.37
```

Editar el fichero `/etc/sysctl.conf` y poner:

```
net.ipv4.ip_forward = 1
```

normalmente esta linea estará comentada, hay que descomentarla.

Esto hace que el forwarding se active al arrancar, si sólo queremos hacer una prueba se puede hacer:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Enlaces

- http://bobby-tables.com/python.html
- http://guifi.net/node/3278, cómo generar certificados para openVPN y túneles con esos certificados.

- http://www.guifi.net/node/12373, Tunels OpenVPN als CPEs amb RouterOS v3
- http://es.wikibooks.org/wiki/OpenVPN/Ejemplo_de_configuraci%C3%B3n_con_claves_asim%C3%A9tricas
- http://www.openvpn.net/index.php/open-source/documentation/howto.html
- http://openvpn.net/index.php/open-source/documentation/graphical-user-interface.html, frontends gráficos.
- http://techtots.blogspot.com/2010/01/configuring-openvpn-freeradius-mysql.html
- http://rafasec.blogspot.com/2008/03/freeradius-mysql_17.html
- http://www.roessner-net.com/?p=4
- http://www.wiggy.net/code/pyrad/

Tracedump:

```
newBaseSize: 12pt
newBaseSizeInPt: 12
```