



Asignatura:

Sistemas Operativos III

Tema:

HOWTO Y VIDEO (SERVIDOR VPN)

Participante:

Santiago M. Duval Contreras

Matricula:

2015-3246

Facilitador:

José Doñe

Fecha:

5/4/2020

HOW-TO? | Instalar un Servidor VPN en ClearOS

HOW-TO? | Instalar un Servidor VPN en ClearOS

En este documento veremos los pasos requerido para habilitar un servidor de OpenVPN en ClearOS - Oracle VirtualBox.

Link a demostración audiovisual: <https://youtu.be/AE2n6cQ28xs>


Requerimientos del OS:

Tener instalado el programa VirtualBox y tener el OS de ClearOS instalado con los requisitos de hardware virtuales que sean requeridos. Selinux tiene que estar desactivado. Todas las maquinas tienen que estar dentro de una misma red interna.

Paso 1 – Instalar el servicio de OpenVPN.

Con el comando **yum install epel-release openvpn** descargamos e instalamos el servicio de VPN y las ultima lista de repositorios en el Servidor de ClearOS.

```
[root@samba4 ~]# yum install epel-release openvpn
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink
 * base: linorg.usp.br
 * epel: mirror.vcu.edu
 * extras: mirror.arizona.edu
 * updates: mirror.facom.ufms.br
base                                     | 3.6 kB  00:00:00
extras                                 | 2.9 kB  00:00:00
updates                                | 2.9 kB  00:00:00
Package epel-release-7-12.noarch already installed and latest version
Package openvpn-2.4.8-1.el7.x86_64 already installed and latest version
Nothing to do
[root@samba4 ~]# _
```



Paso 2 – Descargar easy-rsa.

```
[root@samba4 ~]# wget https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
--2020-04-02 09:15:24-- https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
Resolving github.com (github.com)... 140.82.113.4
Connecting to github.com (github.com):140.82.113.4:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3 [following]
--2020-04-02 09:15:24-- https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3
Resolving codeload.github.com (codeload.github.com)... 140.82.112.10
Connecting to codeload.github.com (codeload.github.com):140.82.112.10:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: '2.3.3.tar.gz'

[ <=> ] 27,506 158KB/s in 0.2s

2020-04-02 09:15:33 (158 KB/s) - '2.3.3.tar.gz' saved [27506]
```

Paso 3 – Descomprimir el archivo 2.3.3.tar.gz

Descomprimiremos el archivo de easy-rsa utilizando el comando **tar xvf 2.3.3.gz**

```
easy-rsa-old-2.3.3/easy-rsa/2.0/revoke-full
easy-rsa-old-2.3.3/easy-rsa/2.0/sign-req
easy-rsa-old-2.3.3/easy-rsa/2.0/vars
easy-rsa-old-2.3.3/easy-rsa/2.0/whichopensslcnf
easy-rsa-old-2.3.3/easy-rsa/Windows/
easy-rsa-old-2.3.3/easy-rsa/Windows/README.txt
easy-rsa-old-2.3.3/easy-rsa/Windows/build-ca-pass.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/build-ca.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/build-dh.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/build-key-pass.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/build-key-pkcs12.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/build-key-server-pass.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/build-key-server.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/build-key.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/clean-all.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/index.txt.start
easy-rsa-old-2.3.3/easy-rsa/Windows/init-config.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/revoke-full.bat
easy-rsa-old-2.3.3/easy-rsa/Windows/serial.start
easy-rsa-old-2.3.3/easy-rsa/Windows/vars.bat.sample
[root@samba4 ~]# ls
2.3.3.tar.gz      centos_7.sh  easy-rsa-old-2.3.3  jansson      thinclient_drives
anaconda-ks.cfg   centos_8.sh  firewall_script.sh  samba-4.10.4.tar.gz
[root@samba4 ~]#
```

Paso 4 – Crear el directorio easy-rsa en el directorio /etc/openvpn/

Paso 5 – Usar el comando cd para movernos al directorio de los archivos de configuración.

```
[root@samba4 openvpn]# cd /usr/share/doc/openvpn-2.4.8/sample/sample-config-files/
[root@samba4 sample-config-files]# ls
client.conf      office.up      roadwarrior-server.conf  tls-office.conf
firewall.sh      openvpn-shutdown.sh  server.conf              xinetd-client-config
home.up          openvpn-startup.sh  static-home.conf         xinetd-server-config
loopback-client  README          static-office.conf
loopback-server  roadwarrior-client.conf  tls-home.conf
```

Paso 6 – copiamos el archivo server.conf al folder de openvpn

Utilizando el comando **cp server.conf /etc/openvpn/server/** moveremos este archivo al directorio de openvpn

Paso 7 – Editamos el archivo server.conf

Utilizando el comando **nano /etc/openvpn/server/server.conf** y realizaremos lo siguiente:

cambiar el path de las siguientes líneas:

```
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh2048.pem
```

verificamos la línea:

```
server "server ip" 255.255.255.0
```

Quitar los ; y sustituir los datos de estas líneas:

```
push "redirect-gateway def1"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
```

Comentar la siguiente línea:

```
#tls-auth ta.key 0
```

Descomentar estas líneas:

```
user nobody
group nobody
```

Paso 8 – Creamos el directorio keys dentro del directorio de easy-rsa.

Utilizamos el comando **mkdir /etc/openvpn/easy-rsa/keys** para crear este directorio.

Paso 9 – Copiamos el contenido de los archivos rsa al directorio de openvpn.

Nos movemos al directorio donde descargamos los archivos de easy-rsa y con el comando **cp easy-rsa-old-2.3.3/easy-rsa/2.0/* /etc/openvpn/easy-rsa/** para mover todos los archivos que tengamos dentro del directorio de rsa a la carpeta de openvpn.

Paso 10 – Cambiar el nombre del archivo de openssl.

Utilizando el comando **nano /etc/openvpn/easy-rsa/openssl-1.0.0.cnf** abrimos el archivo hacemos una edición mínima y lo guardamos como **openssl.cnf**.

```
[root@samba4 easy-rsa]#
[root@samba4 easy-rsa]# ls
build-ca      build-key-pass  build-req-pass  list-crl        openssl.cnf  vars
build-dh      build-key-pkcs12 clean-all       openssl-0.9.6.cnf pktool       whichopensslcnf
build-inter   build-key-server inherit-inter    openssl-0.9.8.cnf revoke-full
build-key     build-req       keys            openssl-1.0.0.cnf sign-req
[root@samba4 easy-rsa]#
```

Paso 11 – Dentro del directorio de easy-rsa, ejecutamos el comando source ./vars y posteriormente ./clean all

```
[root@samba4 easy-rsa]# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
[root@samba4 easy-rsa]# ./clean-all
[root@samba4 easy-rsa]#
```

Paso 12 – Editar el archivo vars que se encuentra dentro del directorio easyrsa.

Utilizando el comando nano vars editamos los siguientes parametros de acuerdo a nuestras necesidades:

```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="DR"
export KEY_PROVINCE="SD"
export KEY_CITY="SantoDomingo"
export KEY_ORG="COSSERVER"
#export KEY_EMAIL="me@myhost.mydomain"
#export KEY_EMAIL=mail@host.domain
export KEY_CN="COSSERVER"
export KEY_NAME="cent-s-001"
export KEY_OU=COSSERVER
#export PKCS11_MODULE_PATH=changeme
#export PKCS11_PIN=1234
```

Paso 12 – Ejecutamos el comando ./build-ca para crear el ca.key

```
[root@samba4 easy-rsa]# ./build-ca
Generating a 4096 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) [DR]:
State or Province Name (full name) [SD]:
Locality Name (eg, city) [SantoDomingo]:
Organization Name (eg, company) [COSSERVER]:
Organizational Unit Name (eg, section) [COSSERVER]:
Common Name (eg, your name or your server's hostname) [COSSERVER]:
Name [cent-s-001]:
Email Address [mail@host.domain]:
```

HOW-TO? | Instalar un Servidor VPN en ClearOS

Paso 13 – Ejecutamos el comando `./build-key server` para crear la llave del servidor.

```

[root@samba4 easy-rsa]# ./build-key-server server
Generating a 4096 bit RSA private key
.....++
.....+
+
writing new private key to '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) [DR]:
State or Province Name (full name) [SD]:
Locality Name (eg, city) [SantoDomingo]:
Organization Name (eg, company) [COSSERVER]:
Organizational Unit Name (eg, section) [COSSERVER]:
Common Name (eg, your name or your server's hostname) [server]:
Name [cent-s-001]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:3246
An optional company name []:ITLA

```

Paso 14 – Ejecutamos el comando ./build-dh

```
[root@samba4 easy-rsa]# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time

..+.....+
.....+
.....+
.....+.
.....+
.....+.
.....++
.....+
.....+.
.....+
.....++++*
```


Paso 14 – Mover las llaves que acabamos de crear al directorio de openvpn.

Utilizando el comando `cp dh2048.pem ca.crt server.crt server.key /etc/openvpn` para mover estos archivos a la path que habíamos colocado en el paso 7.

Paso 15 – Editar el archivo sysctl.conf.

Utilizando el comando `nano /etc/sysctl.conf` y añadimos la siguiente línea `net.ipv4.ip_forward=1`

Paso 16 – Ejecutamos el comando sysctl –system

```
[root@samba4 openvpn]# sysctl --system
* Applying /usr/lib/sysctl.d/00-system.conf ...
* Applying /usr/lib/sysctl.d/10-default-yama-scope.conf ...
kernel.yama.ptrace_scope = 0
* Applying /usr/lib/sysctl.d/50-default.conf ...
kernel.sysrq = 16
kernel.core_uses_pid = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.promote_secondaries = 1
net.ipv4.conf.all.promote_secondaries = 1
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /etc/sysctl.d/99-sysctl.conf ...
net.ipv4.ip_forward = 1
* Applying /etc/sysctl.conf ...
net.ipv4.ip_forward = 1
[root@samba4 openvpn]#
```

Paso 17 – Nos movemos al directorio /etc/openvpn/easy-rsa.

Paso 18 – Ejecutar el comando ./build-key client para construir la llave del cliente.

```
[root@samba4 easy-rsa]# ./build-key client
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to 'client.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,
```

HOW-TO? | Instalar un Servidor VPN en ClearOS

Paso 20 – Utilizar el comando cd para desplazarse al directorio keys.

Paso 21 – Copiar las llaves de usuario al directorio de FTP.

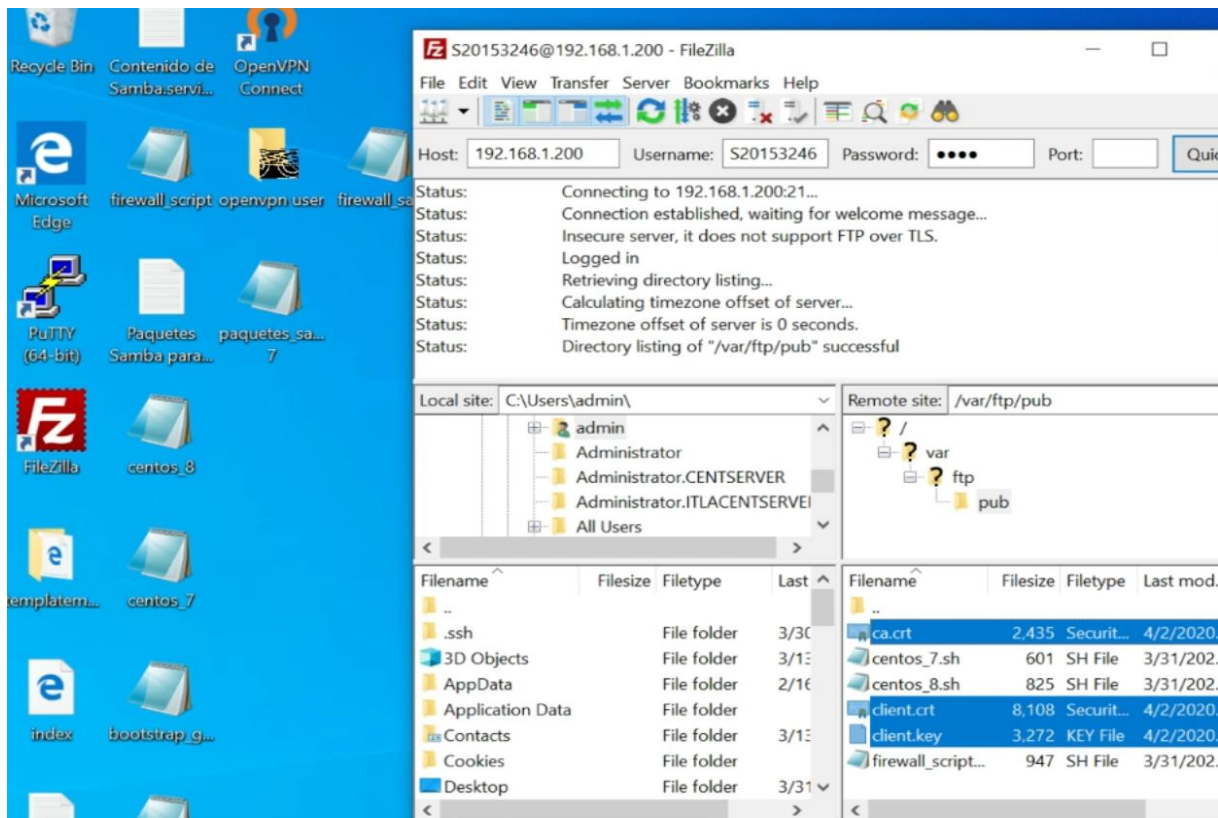
Utilizamos el comando `cp ca.crt client.crt client.key /var/ftp/pub/` para después moverlos a la maquina cliente.

Paso 22 – Iniciar el servicio de openvpn.

Utilizamos el comando `systemctl start openvpn-server@server` y `systemctl enable openvpn-server@server` para usar iniciar el servicio de openvpn y habilitar el inicio onboot.

```
openvpn-server@server.service - OpenVPN service for server
Loaded: loaded (/usr/lib/systemd/system/openvpn-server@server.service; disabled; vendor preset: disabled)
Active: active (running) since Thu 2020-04-02 14:51:32 EDT; 4s ago
Docs: man:openvpn(8)
      https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
      https://community.openvpn.net/openvpn/wiki/HOWTO
Main PID: 2350 (openvpn)
Status: "Initialization Sequence Completed"
CGroup: /system.slice/system-openvpn\x2dservice.slice/openvpn-server@server.service
        └─2350 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-versi...
```

Paso 23 – Transferimos los certificados de cliente utilizando el cliente FTP.



HOW-TO? | Instalar un Servidor VPN en ClearOS

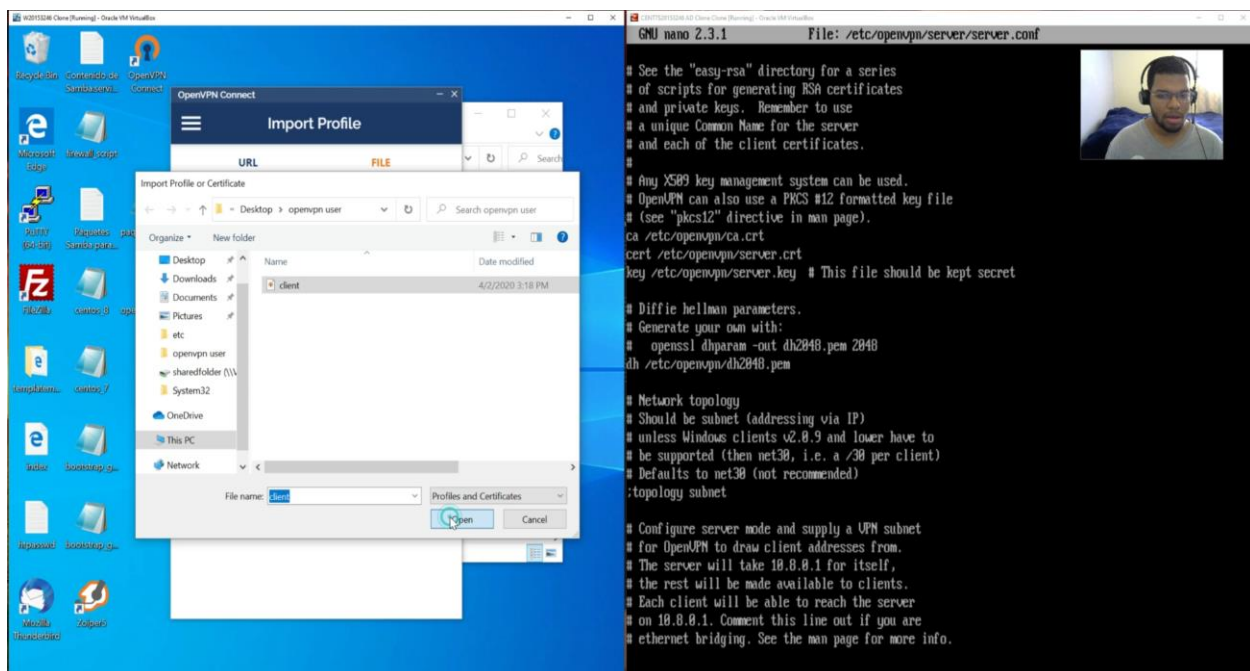
Paso 24 – Crearemos el archivo del cliente .ovpn

Creamos un nuevo documento de texto e introducimos los siguientes datos, cuando hayamos terminado de crear el documento lo guardamos con la extensión .ovpn

```
*New Text Document - Notepad
File Edit Format View Help
client
dev tun
proto udp
remote 192.168.1.200 1194
resolv-retry infinite
nobind
mute-replay-warnings
ca ca.crt
cert client.crt
key client.key
ns-cert-type server
comp-lzo
verb 3
mute 20
explicit-exit-notify 2
auth-user-pass |
```

Paso 25 – Cargar el archivo en el programa OpenVPN Connect.

Podemos descargar este programa desde la página web de openvpn, una vez instalado le daremos a la opción de importar archivo ovpn, procedemos entonces a cargar el archivo que acabamos de crear.



HOW-TO? | Instalar un Servidor VPN en ClearOS

Paso 26 – Introducir el usuario que habíamos creado anteriormente.

Procedemos a introducir el usuario y password que habíamos seleccionado al momento de crear la llave de usuario y debería de conectarse automáticamente a nuestro servidor de OpenVPN sin ningún inconveniente.

