Servidor VPN

Por: John A. Pérez B. ~ 20186748

Este tutorial es un extracto del siguiente video:

https://youtu.be/zPJIlk6ja8M

Configuración

Primero instalamos el repositorio **epel-release**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
login as: root
root@192.168.1.12's password:
Last login: Tue Nov 12 17:08:20 2019
[root@voip ~]# yum install -y epel-release
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
epel/x86_64/metalink
 * base: ftp.unicamp.br
 * epel: mirror.atl.genesisadaptive.com
 * extras: centos.ufes.br
 * updates: centos.ufes.br
```

6:10 PM
11/12/2019

Right Ctrl

6:10 PM

Luego instalamos el paquete **openvpn**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
[root@voip ~]# yum install -y openvpn
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.brisanet.com.br
 * epel: mirror.atl.genesisadaptive.com
 * extras: centos.brisanet.com.br
 * updates: centos.brisanet.com.br
Resolving Dependencies
--> Running transaction check
---> Package openvpn.x86_64 0:2.4.7-1.el7 will be installed
--> Processing Dependency: libpkcs11-helper.so.1()(64bit) for package: openvpn-2.4.7-1.el7.x86_64
--> Running transaction check
---> Package pkcs11-helper.x86_64 0:1.11-3.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package              Arch            Version              Repository      Size
================================================================================
Installing:
 openvpn              x86_64          2.4.7-1.el7          epel           522 k
Installing for dependencies:
 pkcs11-helper        x86_64          1.11-3.el7           epel            56 k

Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 577 k
Installed size: 1.3 M
Downloading packages:
(2/2): pkcs11-helper-1.11-3.el7.x86_64.rpm      0% [          ] 0.0 B/s |    0 B --:--:-- ETA
```

6:11 PM
11/12/2019

Right Ctrl

6:11 PM

Luego instalamos el paquete **easy-rsa** utilizando en siguiente enlace:

https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
[root@voip ~]# wget -O /tmp/easyrsa https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
--2019-11-12 17:11:33--  https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
Resolving github.com (github.com)... 140.82.113.3
Connecting to github.com (github.com)|140.82.113.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3 [following]
--2019-11-12 17:11:33--  https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3
Resolving codeload.github.com (codeload.github.com)... 140.82.113.10
Connecting to codeload.github.com (codeload.github.com)|140.82.113.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: '/tmp/easyrsa'

    [ <=>                                   ] 27,506      --.-K/s   in 0.1s

2019-11-12 17:11:34 (266 KB/s) - '/tmp/easyrsa' saved [27506]

[root@voip ~]#
```

6:11 PM
11/12/2019

Right Ctrl

6:11 PM

Luego desempaquetamos el paquete, y copiamos los archivos de configuración del servidor dentro del directorio **/etc/openvpn**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
[root@voip ~]# wget -O /tmp/easyrsa https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
--2019-11-12 17:11:33--  https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
Resolving github.com (github.com)... 140.82.113.3
Connecting to github.com (github.com)|140.82.113.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3 [following]
--2019-11-12 17:11:33--  https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3
Resolving codeload.github.com (codeload.github.com)... 140.82.113.10
Connecting to codeload.github.com (codeload.github.com)|140.82.113.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: '/tmp/easyrsa'

    [ <=>

2019-11-12 17:11:34 (266 KB/s) - '/tmp/easyrsa' saved [27506]

[root@voip ~]# tar xzf /tmp/easyrsa
[root@voip ~]# cp /usr/share/doc/openvpn-2.4.7/sample/sample-config-files/server.conf /etc/openvpn/
```

] 27,506 --.-K/s in 0.1s

6:12 PM
11/12/2019

Right Ctrl

6:12 PM

En el archivo de configuración hacemos los siguientes cambios.
Primero, asignamos el puerto de nuestro servidor

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
[root@voip ~]# wget -O /tmp/easyrsa https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
--2019-11-12 17:11:33--  https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
Resolving github.com (github.com)... 140.82.113.3
Connecting to github.com (github.com)|140.82.113.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3 [following]
--2019-11-12 17:11:33--  https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3
Resolving codeload.github.com (codeload.github.com)... 140.82.113.10
Connecting to codeload.github.com (codeload.github.com)|140.82.113.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: '/tmp/easyrsa'

    [ <=>                                                          ] 27,506      --.-K/s   in 0.1s

2019-11-12 17:11:34 (266 KB/s) - '/tmp/easyrsa' saved [27506]

[root@voip ~]# tar xzf /tmp/easyrsa
[root@voip ~]# cp /usr/share/doc/openvpn-2.4.7/sample/sample-config-files/server.conf /etc/openvpn/
[root@voip ~]# vim /etc/openvpn/server.conf
```

6:12 PM
11/12/2019

Right Ctrl

6:12 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
#########################################
# Sample OpenVPN 2.0 config file for    #
# multi-client server.                  #
#                                       #
# This file is for the server side      #
# of a many-clients <-> one-server      #
# OpenVPN configuration.                #
#                                       #
# OpenVPN also supports                 #
# single-machine <-> single-machine     #
# configurations (See the Examples page #
# on the web site for more info).       #
#                                       #
# This config should work on Windows    #
# or Linux/BSD systems.  Remember on    #
# Windows to quote pathnames and use    #
# double backslashes, e.g.:             #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
#                                       #
# Comments are preceded with '#' or ';' #
#########################################

# Which local IP address should OpenVPN
# listen on? (optional)
local 192.168.1.12

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun
-- INSERT --                                                    32,10         Top
```

6:13 PM
11/12/2019

Right Ctrl

6:13 PM

Luego comentamos el uso del archivo **ta.key**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

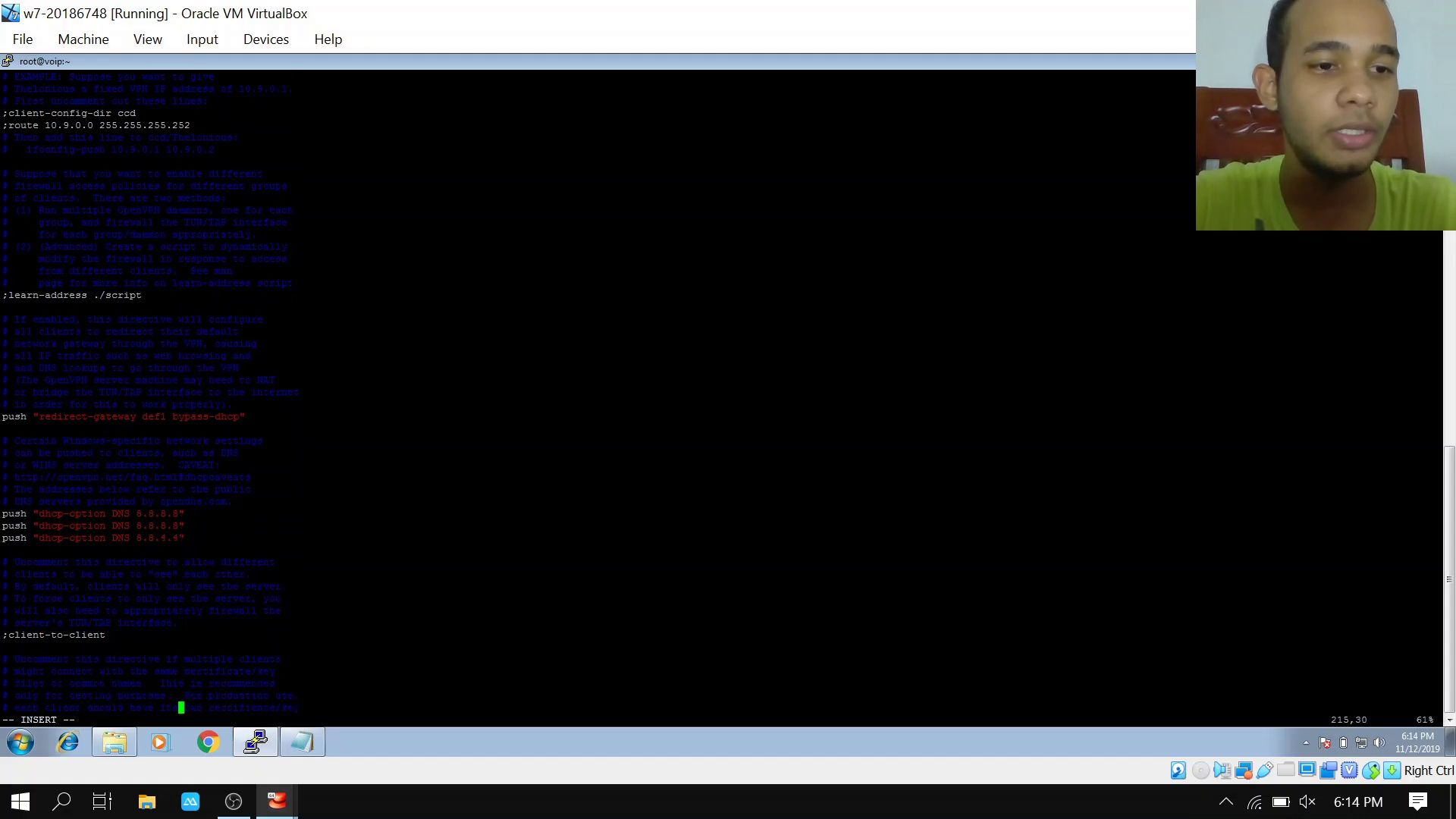
```
# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names.  This is recommended
# only for testing purposes.  For production use,
# each client should have its own certificate/key
# pair.
#
# IF YOU HAVE NOT GENERATED INDIVIDUAL
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",
# UNCOMMENT THIS LINE OUT.
;duplicate-cn

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the ncp-cipher option in the manpage
cipher AES-256-CBC

# Enable compression on the VPN link and push the
# option to the client (v2.4+ only, for earlier
# versions see below)
;compress lz4-v2
;push "compress lz4-v2"

# For compression compatible with older clients use comp-lzo
# If you enable it here, you must also
# enable it in the client config file.
;comp-lzo
-- INSERT --                                                    244,1         80%
```

6:14 PM
11/12/2019

Right Ctrl

6:14 PM

Descomentamos los DNS, y establecemos los que utilizaremos con el servidor vpn


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@voip:~
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
;learn-address ./script
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
;client-to-client
-- INSERT --
215,30 61%
6:14 PM
11/12/2019
Right Ctrl
6:14 PM

Descomentamos el usuario y el grupo como nobody

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
# option to the client (v2.4+ only, for earlier
# versions see below)
;compress lz4-v2
;push "compress lz4-v2"

# For compression compatible with older clients use comp-lzo
# If you enable it here, you must also
# enable it in the client config file.
;comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
user nobody
group nobody

# 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 openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
;log         openvpn.log
;log-append  openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3
```

-- INSERT -- 275,1 96%

6:14 PM
11/12/2019

Right Ctrl

6:14 PM

creamos el directorio **/easy-rsa/keys**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
[root@voip ~]# wget -O /tmp/easyrsa https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
--2019-11-12 17:11:33--  https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
Resolving github.com (github.com)... 140.82.113.3
Connecting to github.com (github.com)|140.82.113.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3 [following]
--2019-11-12 17:11:33--  https://codeload.github.com/OpenVPN/easy-rsa-old/tar.gz/2.3.3
Resolving codeload.github.com (codeload.github.com)... 140.82.113.10
Connecting to codeload.github.com (codeload.github.com)|140.82.113.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: '/tmp/easyrsa'

    [ <=>                                                                   ] 27,506      --.-K/s   in 0.1s

2019-11-12 17:11:34 (266 KB/s) - '/tmp/easyrsa' saved [27506]

[root@voip ~]# tar xzf /tmp/easyrsa
[root@voip ~]# cp /usr/share/doc/openvpn-2.4.7/sample/sample-config-files/server.conf /etc/openvpn/
[root@voip ~]# vim /etc/openvpn/server.conf
[root@voip ~]# mkdir -p /etc/openvpn/easy-rsa/keys
[root@voip ~]#
```

6:15 PM
11/12/2019

Right Ctrl

6:15 PM

Copiamos los archivos del paquete rsa que habíamos descargados dentro de este nuevo directorio

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
[root@voip ~]# cp easy-rsa-old-2.3.3/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
```

6:18 PM
11/12/2019

Right Ctrl

6:18 PM

En la parte final del archivo vars personalizamos las opciones con nuestra información

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
[root@voip ~]# vim /etc/openvpn/easy-rsa/vars
```

6:18 PM
11/12/2019

Right Ctrl

6:18 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
# This variable should point to
# the openssl.cnf file included
# with easy-rsa.
export KEY_CONFIG=`$EASY_RSA/whichopensslcnf $EASY_RSA`

# Edit this variable to point to
# your soon-to-be-created key
# directory.
#
# WARNING: clean-all will do
# a rm -rf on this directory
# so make sure you define
# it correctly!
export KEY_DIR="$EASY_RSA/keys"

# Issue rm -rf warning
echo NOTE: If you run ./clean-all, I will be doing a rm -rf on $KEY_DIR

# PKCS11 fixes
export PKCS11_MODULE_PATH="dummy"
export PKCS11_PIN="dummy"

# Increase this if you
# are paranoid.  This will slow
# down TLS negotiation performance
# as well as the one-time DH parms
# generation process.
export DH_KEY_SIZE=2048

# Private key size
export KEY_SIZE=4096

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650

# 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="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_EMAIL=mail@host.domain
export KEY_CN=changeme
export KEY_NAME=changeme
export KEY_OU=changeme
export PKCS11_MODULE_PATH=changeme
"/etc/openvpn/easy-rsa/vars" 77L, 1877C                                   76,1          95%
```

6:18 PM
11/12/2019

Right Ctrl

6:18 PM

Luego renombramos el archivo **openssl-1.0.0.cnf** como **openssl.cnf**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:~

```
[root@voip ~]# vim /etc/openvpn/easy-rsa/vars
[root@voip ~]# cp /etc/openvpn/easy-rsa/openssl-1.0.0.cnf /etc/openvpn/easy-rsa/openssl.cnf
```

6:20 PM
11/12/2019

Right Ctrl

6:20 PM

Generamos las variables con **./vars**, luego con **./clean-all** limpiamos las variables anteriores, y finalmente ejecutamos **./build-ca**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa

```
[root@voip easy-rsa]# ls
build-ca  build-inter  build-key-pass    build-key-server  build-req-pass  inherit-inter  list-crl          openssl-0.9.8.cnf  openssl.cnf  revoke-full  vars
build-dh  build-key    build-key-pkcs12  build-req         clean-all       keys           openssl-0.9.6.cnf  openssl-1.0.0.cnf  pkitool      sign-req     whichopensslcnf
[root@voip easy-rsa]# source .
./  ../
[root@voip easy-rsa]# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
[root@voip easy-rsa]#
```

6:21 PM
11/12/2019

Right Ctrl

6:21 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa

```
[root@voip easy-rsa]# ls
build-ca  build-inter  build-key-pass    build-key-server  build-req-pass  inherit-inter  list-crl          openssl-0.9.8.cnf  openssl.cnf  revoke-full  vars
build-dh  build-key    build-key-pkcs12  build-req         clean-all       keys           openssl-0.9.6.cnf  openssl-1.0.0.cnf  pkitool      sign-req     whichopensslcnf
[root@voip easy-rsa]# source .
./  ../
[root@voip easy-rsa]# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
[root@voip easy-rsa]# ./clean-all
```

6:21 PM
11/12/2019

Right Ctrl

6:21 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa

```
[root@voip easy-rsa]# ls
build-ca  build-inter  build-key-pass    build-key-server  build-req-pass  inherit-inter  list-crl          openssl-0.9.8.cnf  openssl.cnf  revoke-full  vars
build-dh  build-key    build-key-pkcs12  build-req         clean-all       keys           openssl-0.9.6.cnf  openssl-1.0.0.cnf  pkitool      sign-req     whichopensslcnf
[root@voip easy-rsa]# source .
./  ../
[root@voip easy-rsa]# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
[root@voip easy-rsa]# ./clean-all
[root@voip 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) [DO]:
State or Province Name (full name) [SD]:
Locality Name (eg, city) [SantoDomingo]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [CENTOS]:
Common Name (eg, your name or your server's hostname) [CENTOS]:
Name [SV-DC-001]:
Email Address [me@myhost.mydomain]:
[root@voip easy-rsa]#
```

6:21 PM
11/12/2019

Right Ctrl

6:21 PM

Ahora generamos las llaves del servidor con **./build-key-server server**, y como habíamos colocado la información en el archivo vars, simplemente damos enter

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa

```
[root@voip easy-rsa]# ls
build-ca  build-inter  build-key-pass    build-key-server  build-req-pass  inherit-inter  list-crl          openssl-0.9.8.cnf  openssl.cnf  revoke-full  vars
build-dh  build-key    build-key-pkcs12  build-req         clean-all       keys           openssl-0.9.6.cnf  openssl-1.0.0.cnf  pkitool      sign-req     whichopensslcnf
[root@voip easy-rsa]# source .
./  ../
[root@voip easy-rsa]# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
[root@voip easy-rsa]# ./clean-all
[root@voip 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) [DO]:
State or Province Name (full name) [SD]:
Locality Name (eg, city) [SantoDomingo]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [CENTOS]:
Common Name (eg, your name or your server's hostname) [CENTOS]:
Name [SV-DC-001]:
Email Address [me@myhost.mydomain]:
[root@voip easy-rsa]# ./build-key-server server
```

6:21 PM
11/12/2019

Right Ctrl

6:21 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa

```
Locality Name (eg, city) [SantoDomingo]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [CENTOS]:
Common Name (eg, your name or your server's hostname) [CENTOS]:
Name [SV-DC-001]:
Email Address [me@myhost.mydomain]:
[root@voip 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) [DO]:
State or Province Name (full name) [SD]:
Locality Name (eg, city) [SantoDomingo]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [CENTOS]:
Common Name (eg, your name or your server's hostname) [server]:
Name [SV-DC-001]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:CENTOS
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DO'
stateOrProvinceName   :PRINTABLE:'SD'
localityName          :PRINTABLE:'SantoDomingo'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'CENTOS'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'SV-DC-001'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Nov  9 22:22:11 2029 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
[root@voip easy-rsa]#
```

6:22 PM
11/12/2019

Right Ctrl

6:22 PM

Para generar los parámetros ejecutamos el comando **./build-dh**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa

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

6:24 PM
11/12/2019

Right Ctrl

6:24 PM

Copiamos las llaves y certificados del servidor dentro del directorio **/openvpn**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa/keys

```
[root@voip keys]# ls
01.pem  ca.crt  ca.key  dh2048.pem  index.txt  index.txt.attr  index.txt.old  serial  serial.old  server.crt  server.csr  server.key
[root@voip keys]# cp dh2048.pem ca.crt server.crt server.key  /etc/openvpn/
[root@voip keys]#
```

6:25 PM
11/12/2019

Right Ctrl

6:25 PM

Para comprobar que nuestro servidor se ha configurado correctamente iniciamos el servicio con **systemctl start openvpn@server** y comprobamos su estado con **systemctl status openvpn@server**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa/keys

```
[root@voip keys]# systemctl start openvpn@server
[root@voip keys]# systemctl enable openvpn@server
Created symlink from /etc/systemd/system/multi-user.target.wants/openvpn@server.service to /usr/lib/systemd/system/openvpn@.service.
[root@voip keys]# systemctl status openvpn@server
● openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Application On server
   Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-11-12 17:28:18 EST; 10s ago
 Main PID: 2732 (openvpn)
   Status: "Initialization Sequence Completed"
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─2732 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf

Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 Could not determine IPv4/IPv6 protocol. Using AF_INET
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 Socket Buffers: R=[212992->212992] S=[212992->212992]
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 UDPv4 link local (bound): [AF_INET]192.168.1.12:1194
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 UDPv4 link remote: [AF_UNSPEC]
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 GID set to nobody
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 UID set to nobody
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 MULTI: multi_init called, r=256 v=256
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 IFCONFIG POOL LIST
Nov 12 17:28:18 voip openvpn[2732]: Tue Nov 12 17:28:18 2019 Initialization Sequence Completed
[root@voip keys]#
```

6:28 PM
11/12/2019

Right Ctrl

6:28 PM

Configurando el cliente

Para generar las llaves del cliente ejecutamos **./build-keys [nombre del cliente]**, dentro del directorio **/keys**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa

```
[root@voip keys]# cd ..
[root@voip easy-rsa]# ls
build-ca  build-inter  build-key-pass    build-key-server  build-req-pass  inherit-inter  list-crl          openssl-0.9.8.cnf  openssl.cnf  revoke-full  vars
build-dh  build-key    build-key-pkcs12  build-req         clean-all       keys           openssl-0.9.6.cnf  openssl-1.0.0.cnf  pkitool      sign-req     whichopensslcnf
[root@voip 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,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DO]:
State or Province Name (full name) [SD]:
Locality Name (eg, city) [SantoDomingo]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [CENTOS]:
Common Name (eg, your name or your server's hostname) [client]:
Name [SV-DC-001]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:CENTOS
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DO'
stateOrProvinceName   :PRINTABLE:'SD'
localityName          :PRINTABLE:'SantoDomingo'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'CENTOS'
commonName            :PRINTABLE:'client'
name                  :PRINTABLE:'SV-DC-001'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Nov  9 22:29:12 2029 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
[root@voip easy-rsa]#
```

6:29 PM
11/12/2019

Right Ctrl

6:29 PM

Copiamos las llaves en un directorio al que tengamos acceso de forma remota para enviarlas al cliente

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/openvpn/easy-rsa/keys

```
[root@voip keys]# ls
01.pem  02.pem  ca.crt  ca.key  client.crt  client.csr  client.key  dh2048.pem  index.txt  index.txt.attr  index.txt.attr.old  index.txt.old  serial  serial.old  server.crt  server.csr  server.key
[root@voip keys]# mkdir /etc/client/
[root@voip keys]# cp /etc/client/ client.crt client.key ca.crt
cp: target 'ca.crt' is not a directory
[root@voip keys]# cp client.crt client.key ca.crt /etc/client/
[root@voip keys]#
```

6:30 PM
11/12/2019

Right Ctrl

6:30 PM

Luego asignamos los permisos correspondientes a dichos archivos de tal forma que se podrán visualizar al enviarlos al cliente

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@voip:/etc/client

```
[root@voip keys]# cd /etc/client/
[root@voip client]# ls
ca.crt  client.crt  client.key
[root@voip client]# ll
total 16
-rw-r--r--. 1 root root 2427 Nov 12 17:30 ca.crt
-rw-r--r--. 1 root root 8101 Nov 12 17:30 client.crt
-rw-------. 1 root root 3272 Nov 12 17:30 client.key
[root@voip client]# chmod 766
chmod: missing operand after ‘766’
Try 'chmod --help' for more information.
[root@voip client]# chmod 766 *
[root@voip client]# ll
total 16
-rwxrw-rw-. 1 root root 2427 Nov 12 17:30 ca.crt
-rwxrw-rw-. 1 root root 8101 Nov 12 17:30 client.crt
-rwxrw-rw-. 1 root root 3272 Nov 12 17:30 client.key
[root@voip client]#
```

6:30 PM
11/12/2019

Right Ctrl

6:30 PM

Transferimos las llaves al cliente

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@192.168.1.12 - FileZilla

File Edit View Transfer Server Bookmarks Help

Host: 192.168.1.12 Username: root Password: •••••••• Port: Quickconnect

Status: File transfer successful, transferred 2,427 bytes in 1 second
Status: Logged in
Status: Starting download of /etc/client/client.key
Status: Starting download of /etc/client/client.crt
Status: File transfer successful, transferred 3,272 bytes in 1 second
Status: File transfer successful, transferred 8,101 bytes in 1 second

Local site: C:\Users\client\Desktop\VPN\

- client
  - AppData
  - Application Data
  - Contacts
  - Cookies
  - Desktop
    - VPN
  - Documents
  - Downloads
  - Favorites

Remote site: /etc/client

- /
  - etc
    - client
  - root

Filename	Filesize	Filetype	Last modified
..			
ca.crt	2,427	Security Certifi...	11/12/2019 6:34:43...
client.crt	8,101	Security Certifi...	11/12/2019 6:34:43...
client.key	3,272	KEY File	11/12/2019 6:34:43...
client.txt	236	Text Document	11/11/2019 6:05:05...
easy-rsa.txt	77	Text Document	11/11/2019 4:55:12...

5 files. Total size: 14,113 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
ca.crt	2,427	Security Ce...	11/12/2019 1:3...	-rwxrw-rw-	0 0
client.crt	8,101	Security Ce...	11/12/2019 1:3...	-rwxrw-rw-	0 0
client.key	3,272	KEY File	11/12/2019 1:3...	-rwxrw-rw-	0 0

Selected 3 files. Total size: 13,800 bytes

Server/Local file	Direction	Remote file	Size	Priority	Status

Queued files | Failed transfers | Successful transfers (3)

Transfers finished
All files have been successfully transferred

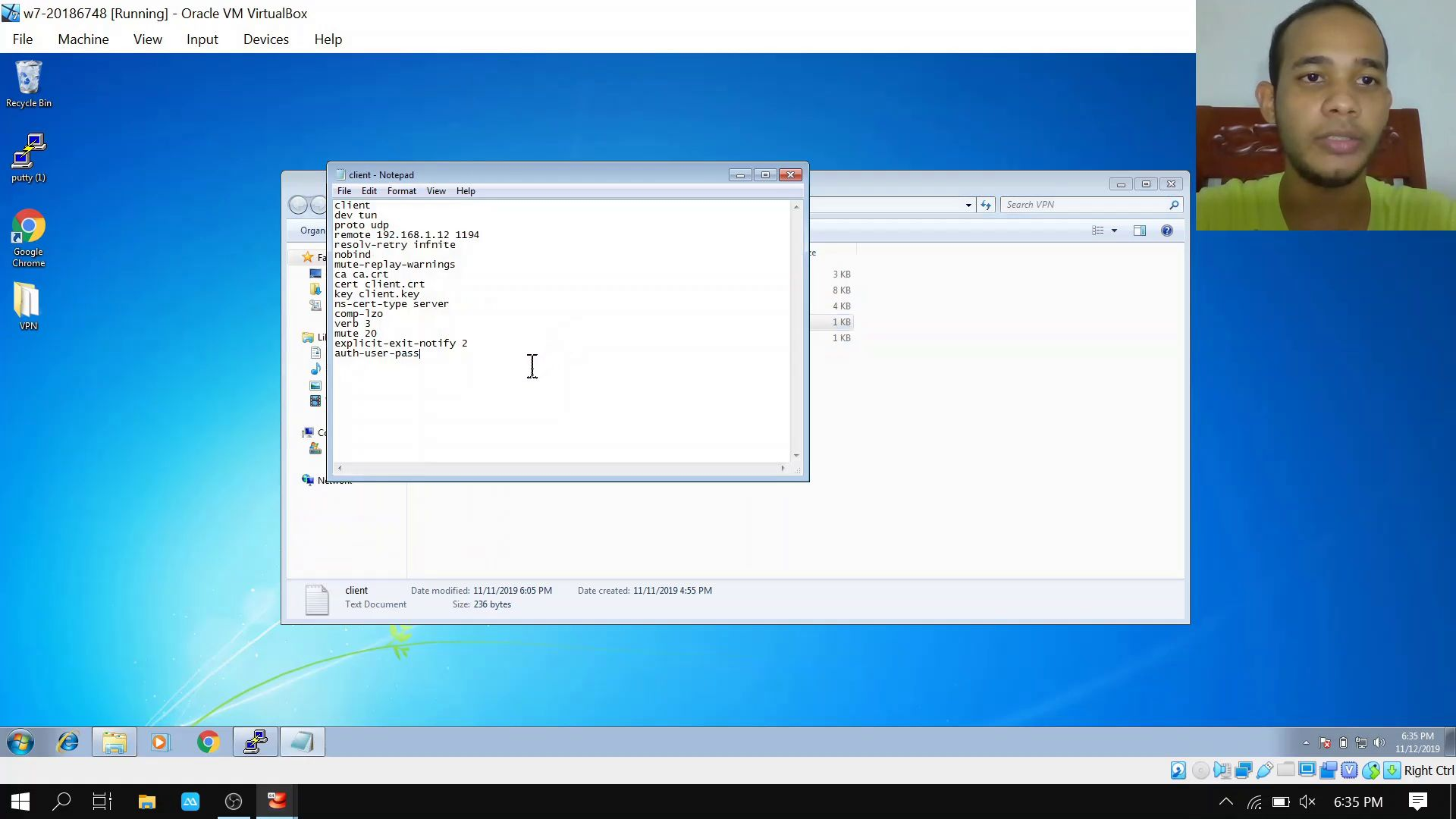
Queue: empty

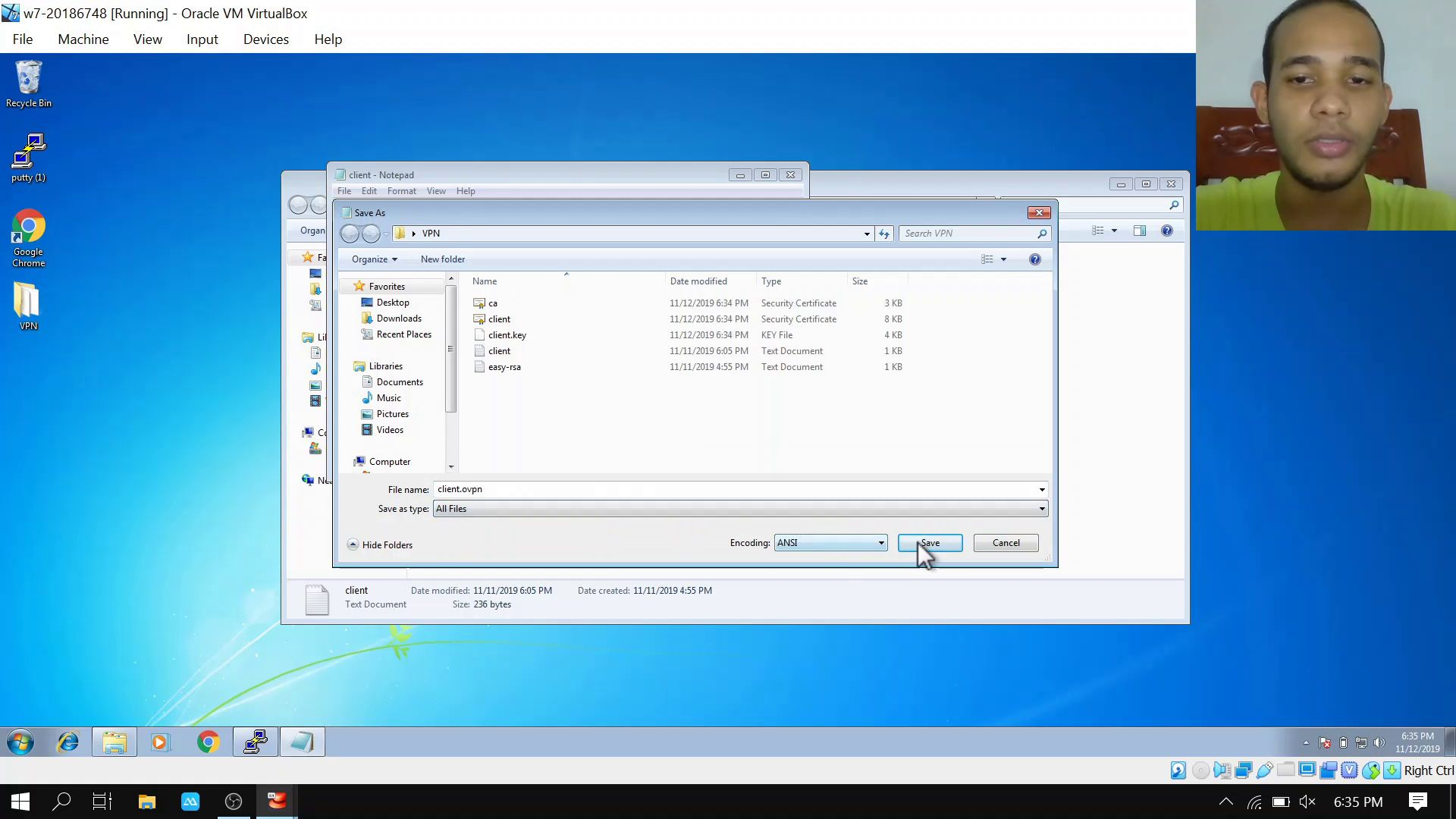
6:34 PM
11/12/2019

Right Ctrl

6:34 PM

Generamos un archivo con la información relacionada al cliente, la dirección del servidor y la ruta de las llaves del cliente dentro del sistema. Luego guardamos el archivo con una extensión **.ovpn**


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
putty (1)
Google Chrome
VPN
client - Notepad
File Edit Format View Help
client
dev tun
proto udp
remote 192.168.1.12 1194
resolv-retry infnite
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
Search VPN
client
Text Document
Date modified: 11/11/2019 6:05 PM
Date created: 11/11/2019 4:55 PM
Size: 236 bytes
6:35 PM
11/12/2019
Right Ctrl
6:35 PM


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
putty (1)
Google Chrome
VPN
client - Notepad
File Edit Format View Help
Save As
VPN
Search VPN
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Name
Date modified
Type
Size
ca 11/12/2019 6:34 PM Security Certificate 3 KB
client 11/12/2019 6:34 PM Security Certificate 8 KB
client.key 11/12/2019 6:34 PM KEY File 4 KB
client 11/11/2019 6:05 PM Text Document 1 KB
easy-rsa 11/11/2019 4:55 PM Text Document 1 KB
File name: client.ovpn
Save as type: All Files
Hide Folders
Encoding: ANSI
Save
Cancel
client
Text Document
Date modified: 11/11/2019 6:05 PM
Date created: 11/11/2019 4:55 PM
Size: 236 bytes
6:35 PM
11/12/2019
Right Ctrl
6:35 PM

Luego descargamos **openvpn connect** desde la página oficial de openvpn

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OpenVPN Client Connect For Wi

openvpn.net/client-connect-vpn-for-windows/

Grow your consulting business with OpenVPN: JOIN ACCESS SERVER'S RESELLER PROGRAM

OPENVPN

BUSINESS VPN CONSUMER VPN SUPPORT COMMUNITY GET OPENVPN

OFFICIAL OPENVPN CONNECT CLIENT PROGRAM

OpenVPN Connect for Windows

This is the official OpenVPN Connect client software for Windows workstation platforms developed and maintained by OpenVPN Inc. This is the recommended client program for the OpenVPN Access Server to enable VPN for Windows. The latest version of OpenVPN for Windows is available on our website.

If you have an OpenVPN Access Server, it is recommended to download the OpenVPN Connect client software directly from your own Access Server, as it will then come pre configured for use for VPN for Windows. The version available here contains no configuration to make a connection, although it can be used to update an existing installation and retain settings.

DOWNLOAD OPENVPN CONNECT V3 (BETA)

sha256 signature: a2a57b74f02edf953fdc4ae5308a4fe6fcee99166de970c43b9b8bc4c9ea7da1

For Windows 7, 8, 8.1, and 10.

A 32bits version is also available:
Download OpenVPN Connect v3 (beta) for 32 bits

sha256 signature: a56ed62407046bf808d7c1f79d3909d5e99ef8fb2ea55be08bb303cc3f8d3b7f

Alternatively, you can obtain the current stable OpenVPN Connect V2 here: Download OpenVPN Connect v2.7.1

sha256 signature: b38551b22c894f960387108bff6e20bbe478c847318c702f9cce1c0f0ae77939

For Windows 7, 8, 8.1, and 10.

Waiting for www.google.com...

6:37 PM
11/12/2019

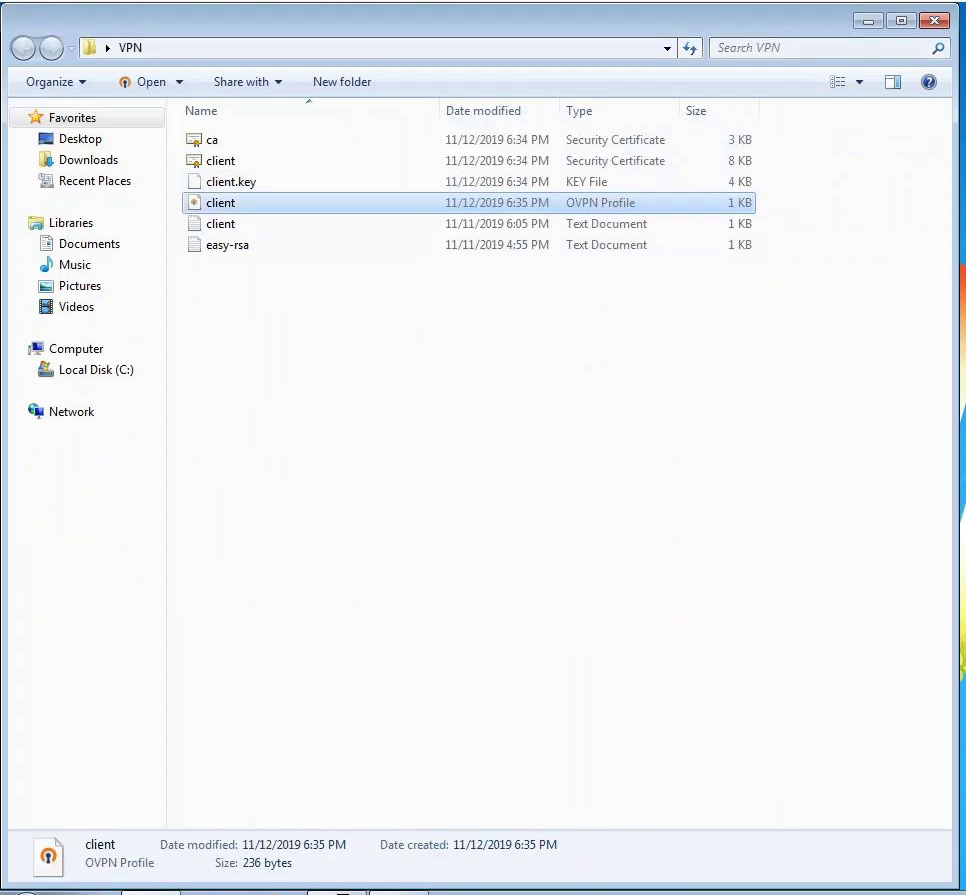
Right Ctrl

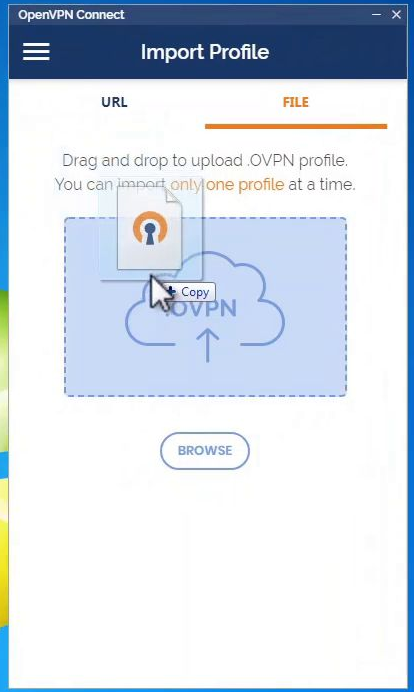
6:37 PM

Colocamos el archivo **.ovpn** en la aplicación de openvpn donde colocamos las credenciales del cliente, y luego seleccionamos la opción conectar después de importar

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help





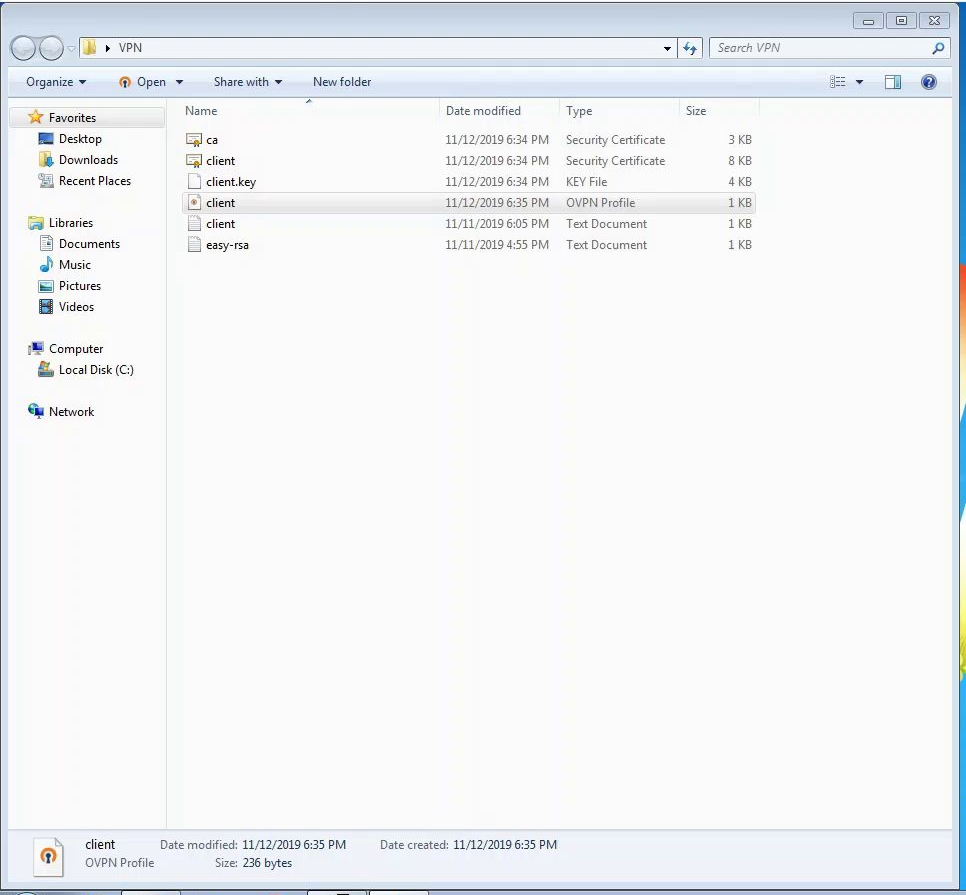
6:37 PM
11/12/2019

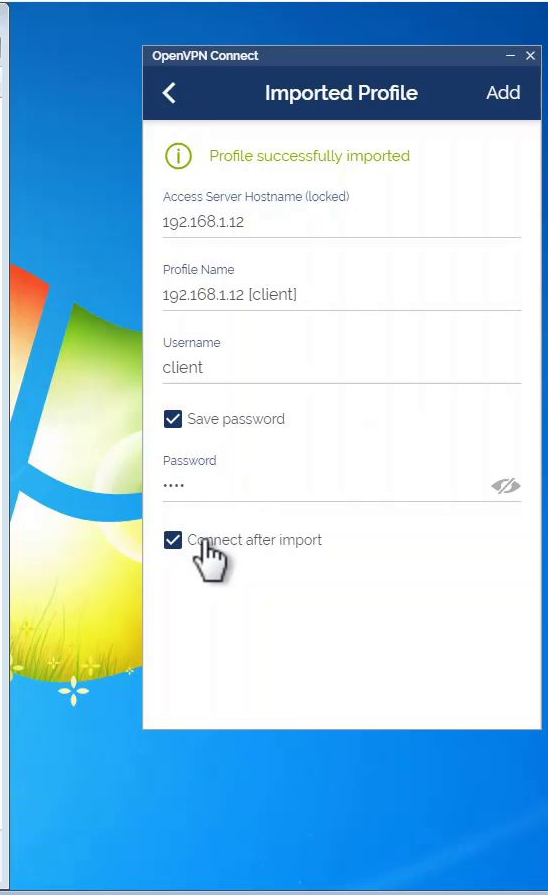
Right Ctrl

6:37 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help





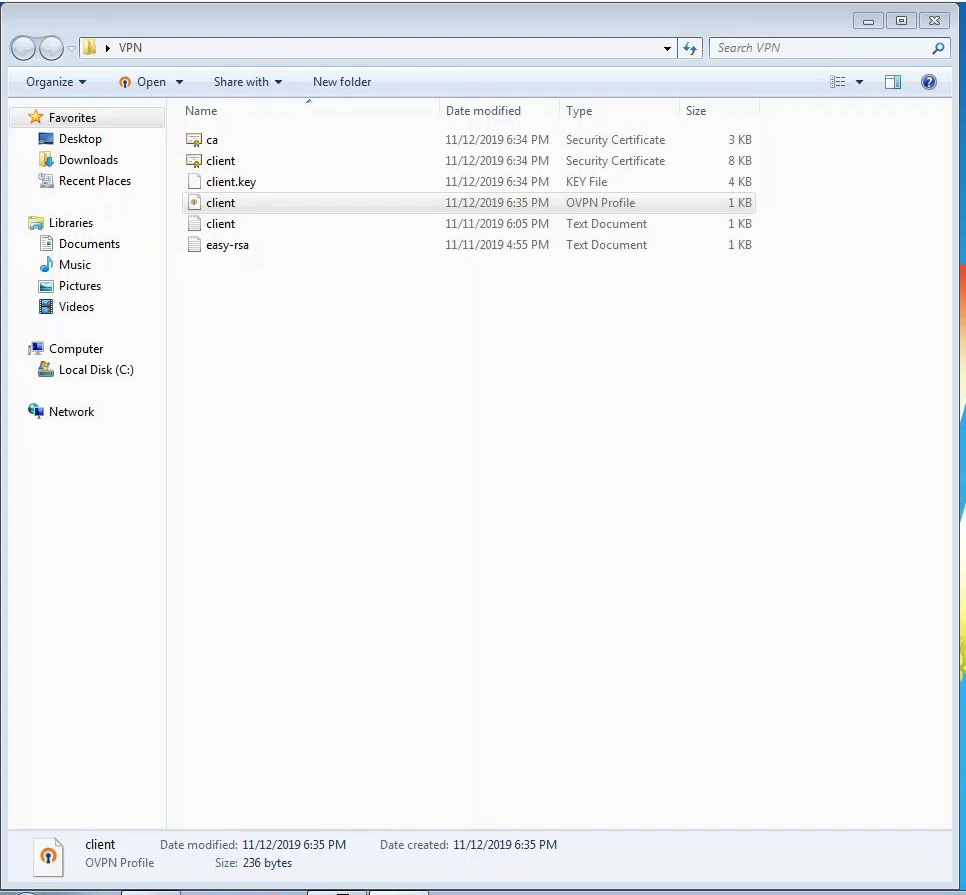
6:37 PM
11/12/2019

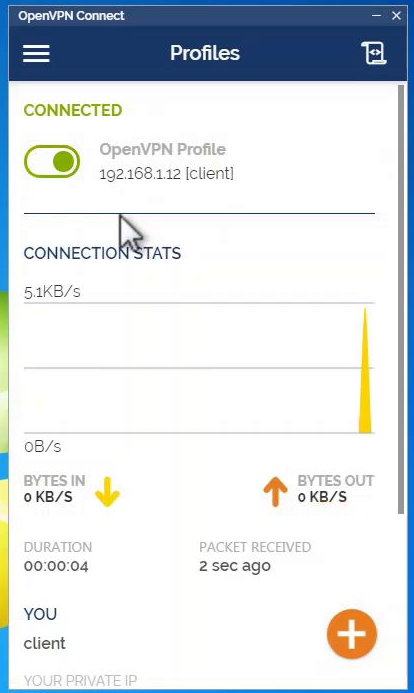
Right Ctrl

6:37 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



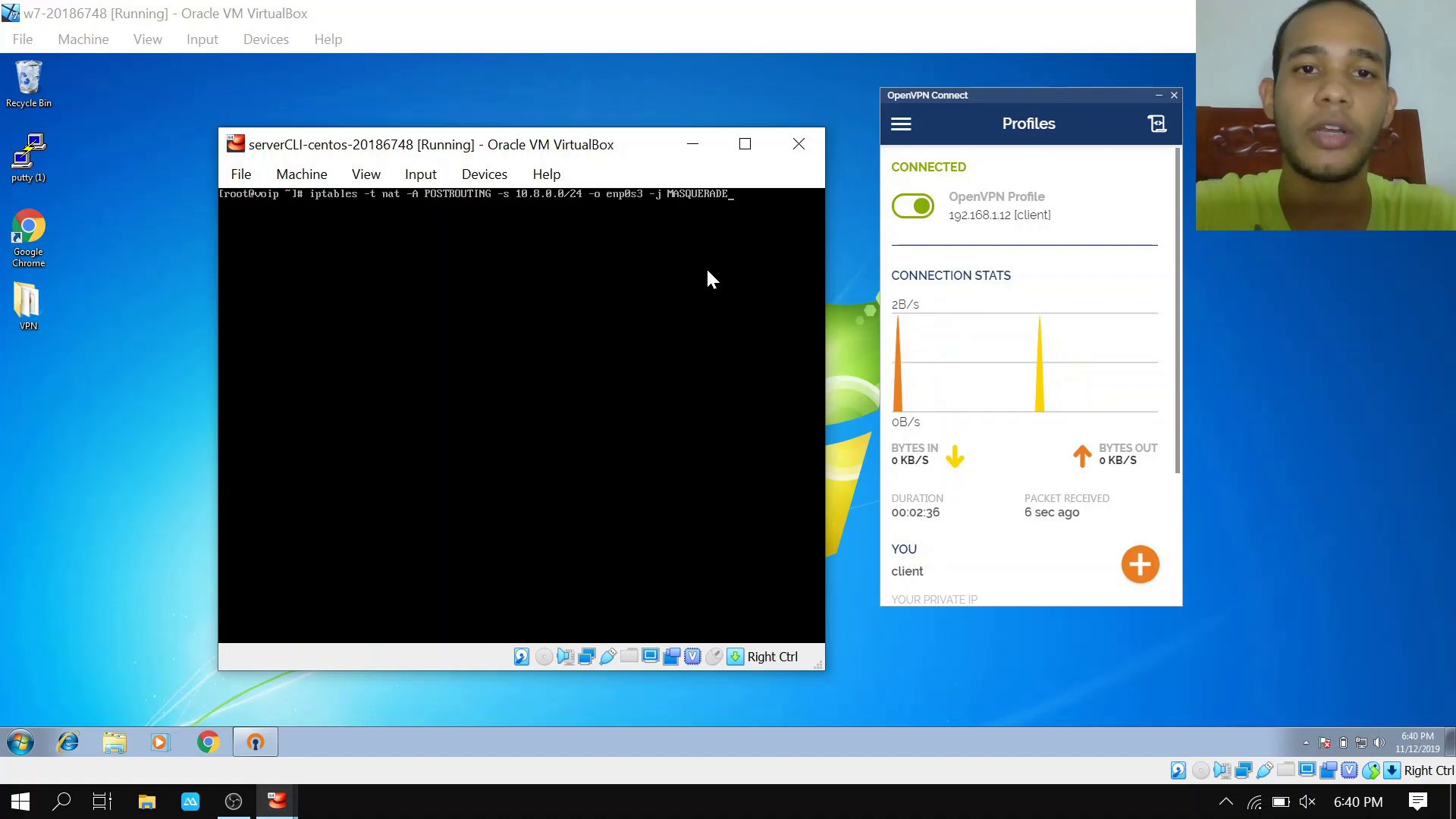


6:37 PM
11/12/2019

Right Ctrl

6:37 PM

Para enviar todo el tráfico de la red vpn al internet creamos una nueva regla con las iptables con salida a la interfaz de internet, colocando como parámetro la subred que utiliza openvpn


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
putty (1)
Google Chrome
VPN
serverCLI-centos-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@voip ~]# iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o enp0s3 -j MASQUERADE
Right Ctrl
OpenVPN Connect
Profiles
CONNECTED
OpenVPN Profile
192.168.1.12 [client]
CONNECTION STATS
2B/s
0B/s
BYTES IN
0 KB/S
BYTES OUT
0 KB/S
DURATION
00:02:36
PACKET RECEIVED
6 sec ago
YOU
client
YOUR PRIVATE IP
6:40 PM
11/12/2019
Right Ctrl
6:40 PM