

I have used OPENVPN here to set up between Ubuntu server and Windows 8.1 client.

There are some important steps to be performed while doing this set up.

- 1) Install and configure software on your server.
- 2) To copy files from your server
- 3) Set up a port forward on your router.

### **Overview of the Installation**

1. Installing and network settings on the server
2. Installation and Configuration of OpenVPN on the server
3. Creating the Keys and Certificates
4. Install and Configure OpenVPN Client

#### **Part 1:**

- 1) Install the OpenVPN and the bridge utilities onto the server:

```
sudo apt-get install openvpn bridge-utils
```

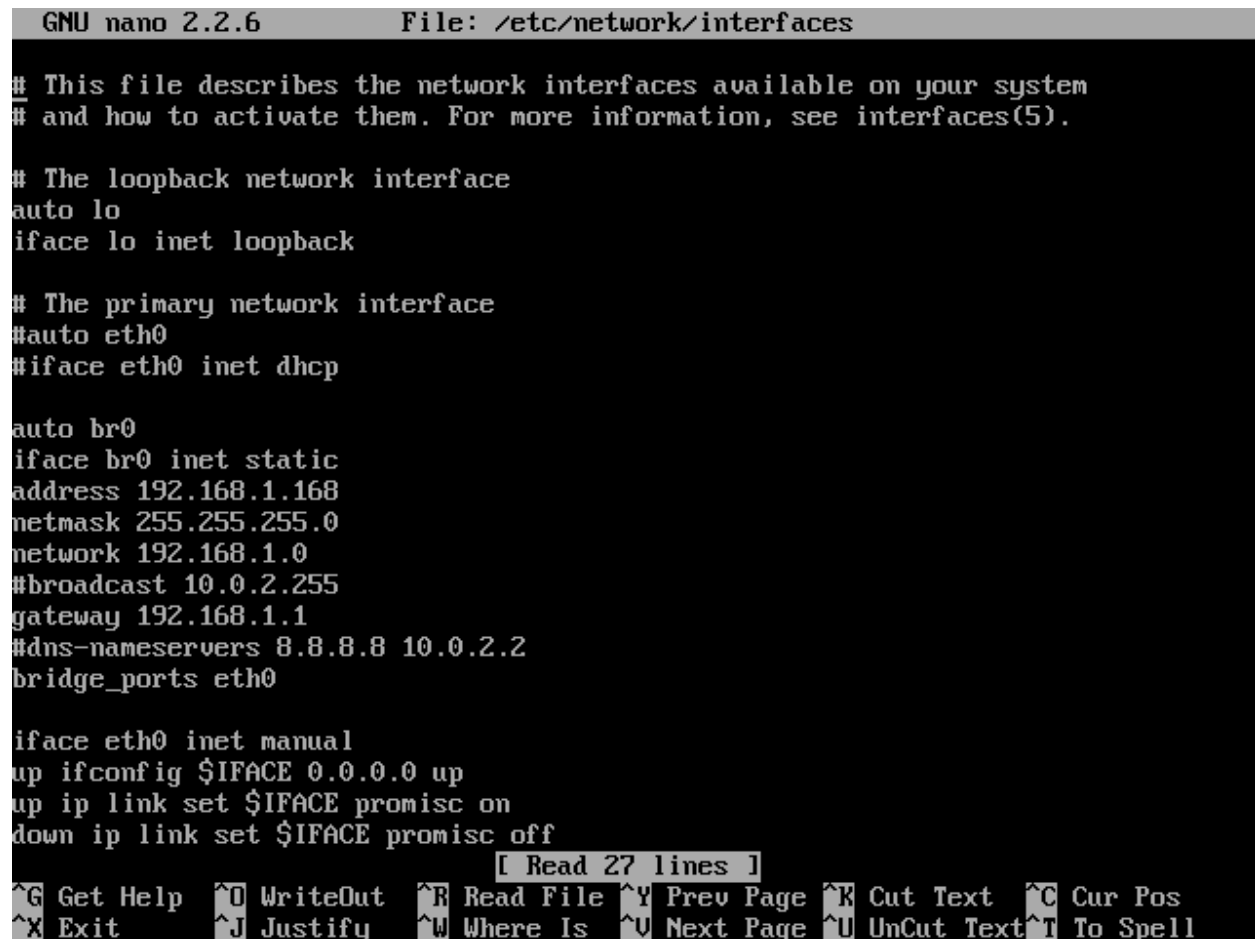
- 2) Change your network to use the new interface by modifying your /etc/network/interfaces file. Make sure you back it up first. The file should be changed to look something like this:

```
Sudo nano /etc/network/interfaces
```

```
# This file describes the network interfaces available on system
# and how to activate them.
# The loopback network interface
auto lo
iface lo inet loopback
```

```
# Set up the bridge interface for OpenVPN
auto br0
iface br0 inet static
address 192.168.1.168
netmask 255.255.255.0
gateway 192.168.1.1
bridge_ports eth0
```

```
iface eth0 inet manual
up ifconfig $IFACE 0.0.0.0 up
up ip link set $IFACE promisc on
down ip link set $IFACE promisc off
down ifconfig $IFACE down
```



```
GNU nano 2.2.6      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#auto eth0
#iface eth0 inet dhcp

auto br0
iface br0 inet static
address 192.168.1.168
netmask 255.255.255.0
network 192.168.1.0
#broadcast 10.0.2.255
gateway 192.168.1.1
#dns-nameservers 8.8.8.8 10.0.2.2
bridge_ports eth0

iface eth0 inet manual
up ifconfig $IFACE 0.0.0.0 up
up ip link set $IFACE promisc on
down ip link set $IFACE promisc off

[ Read 27 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

3) To allow your VPN client to browse the Internet, you will need to enable IPv4 forwarding.

```
sudo nano /etc/sysctl.conf
```

Uncomment the line that reads: net.ipv4.ip\_forward=1

4) You will need to open a port on your firewall to allow the VPN traffic get to the server. OpenVPN uses ports 1194 by default, so on your router, forward that port (as UDP) to your server running OpenVPN.

```
Sudo ufw disable
```

```
Sudo service iptables stop
```

5) Reboot your server and try pinging google.com

## Part-2

### Now, Create the Server Keys and Certificates:

Easy-RSA is a series of scripts which greatly simplifies this process. We will modify a text file then issue the commands to generate the keys.

1. Create an easy-rsa folder, copy the example files into it, and set the permissions:

Login as root:

```
sudo mkdir /etc/openvpn/easy-rsa/
```

```
sudo apt-get install openvpn easy-rsa
```

```
sudo cp -R /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

```
sudo chown -R $USER /etc/openvpn/easy-rsa/
```

2. Edit the text file so that it reflects your information:

```
sudo nano /etc/openvpn/easy-rsa/vars
```

3) Change these items (located at the end of the file) to personalize your certificate.

```
export KEY_COUNTRY="US"
```

```
export KEY_PROVINCE="TX"
```

```
export KEY_CITY="Edinburg"
```

```
export KEY_ORG="UTPA"
```

```
export KEY_EMAIL=dvuppala@broncs.utpa.edu
```

```
GNU nano 2.2.6      File: /etc/openvpn/easy-rsa/vars

export KEY_SIZE=2048

# 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="TX"
export KEY_CITY="Edinburg"
export KEY_ORG="UTPA"
export KEY_EMAIL="dvuppala@broncs.upta.edu"
export KEY_OU="MyOrganizationalUnit"

# X509 Subject Field
export KEY_NAME="EasyRSA"

# PKCS11 Smart Card
# export PKCS11_MODULE_PATH="/usr/lib/changeme.so"
# export PKCS11_PIN=1234

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^T To Spell
```

4) Generate the server keys and copy them to the correct locations.

```
cd /etc/openvpn/easy-rsa/
```

```
source vars
```

```
./clean-all
```

```
./build-dh
```

```
./pktool --initca
```

```
./pktool --server server
```

```
cd keys
```

```
openvpn --genkey --secret ta.key
```

```
sudo cp server.crt server.key ca.crt dh2048.pem ta.key /etc/openvpn/
```

### Part-3

#### Generate the Client Keys and Certificates

It's now time to generate the client keys. These are created on the server, not on the laptop.

1) Create the client key:

```
cd /etc/openvpn/easy-rsa/
```

```
source vars
```

```
./pktool client-name
```

2) Copy the Keys to the Client Machine (Laptop). Each client will need the following files from the following locations.

```
/etc/openvpn/ca.crt
```

```
/etc/openvpn/ta.key
```

```
/etc/openvpn/easy-rsa/keys/client-name.crt
```

```
/etc/openvpn/easy-rsa/keys/client-name.key
```

COPYing Files to LOCAL machine from virtual UBUNTU:

IN root:

```
Sudo mkdir /media/windows-share1/
```

```
Cd /etc/openvpn/
```

```
Sudo cp client-name.crt client-name.key /media/windows-share1/
```

```
Cd ..
```

```
Cd ..
```

Ls -l {lion}- check for Ca.crt ta.key

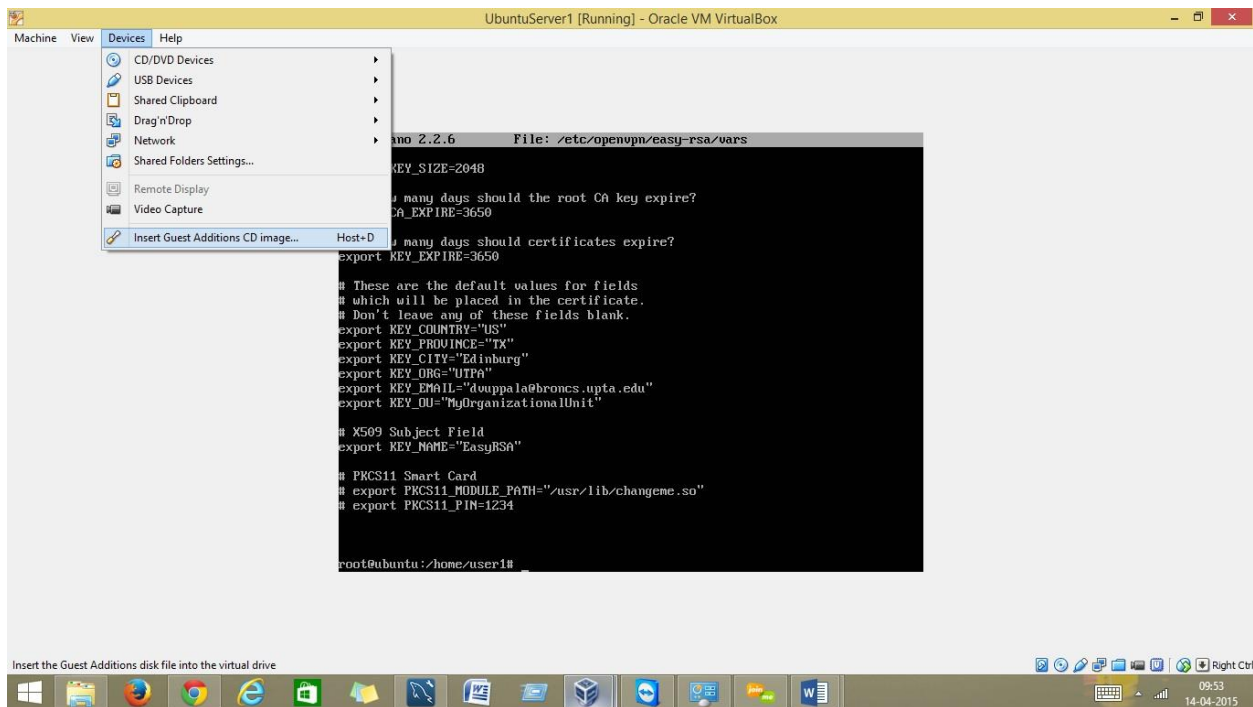
Make sure you are in keys folder now- cd /etc/openvpn/easy-rsa/keys/

Sudo cp ca.crt ta.key /media/windows-share1/

Cd /media/windows-share1/

Ls -l

On the top menu in virtual Ubuntu- DEVICE ➔ Install insert GUEST Additions  
There will be pop up, cancel it.



Now go for checking Virtual Box version—4.3.26

Download from---guesadditons on openvpn website-and save it in your downloads folder.

Now go to Machine settings on Virtual Ubuntu.

Click on STORAGE ➔ on right side , load the ISO guest additions file that is in downloads folder ➔ hit ok ➔ reboot the server.

Again Machine seetings on Ubuntu

Click on SHARED FOLDERS → click on right side to ADD plus sign → other (Browse) the sharedfolder1 by

Now get to file explorer → create one new folder in C drive under THIS

PC → Browse sharedfolder1 → ok → Auto Mount → OK

Reboot now.

Now configure- server config:

- 1) Copy the sample configuration file into the OpenVPN directory and open it in an editor.

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
```

```
sudo gzip -d /etc/openvpn/server.conf.gz
```

```
sudo nano /etc/openvpn/server.conf
```

- 2) Now customize it with tunnel settings.  
The below screen shot describes dev tun

```
GNU nano 2.2.6      File: /etc/openvpn/server.conf

# 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.

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```



```
GNU nano 2.2.6      File: /etc/openvpn/server.conf

# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 192.168.1.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```

The above screenshot describes the network address for the VPN server in server command.

```
GNU nano 2.2.6      File: /etc/openvpn/server.conf

# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
push "redirect-gateway def1"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

The above screenshot describes the push dhcp -options in the server command.

Now this successfully completes the sever configuration.

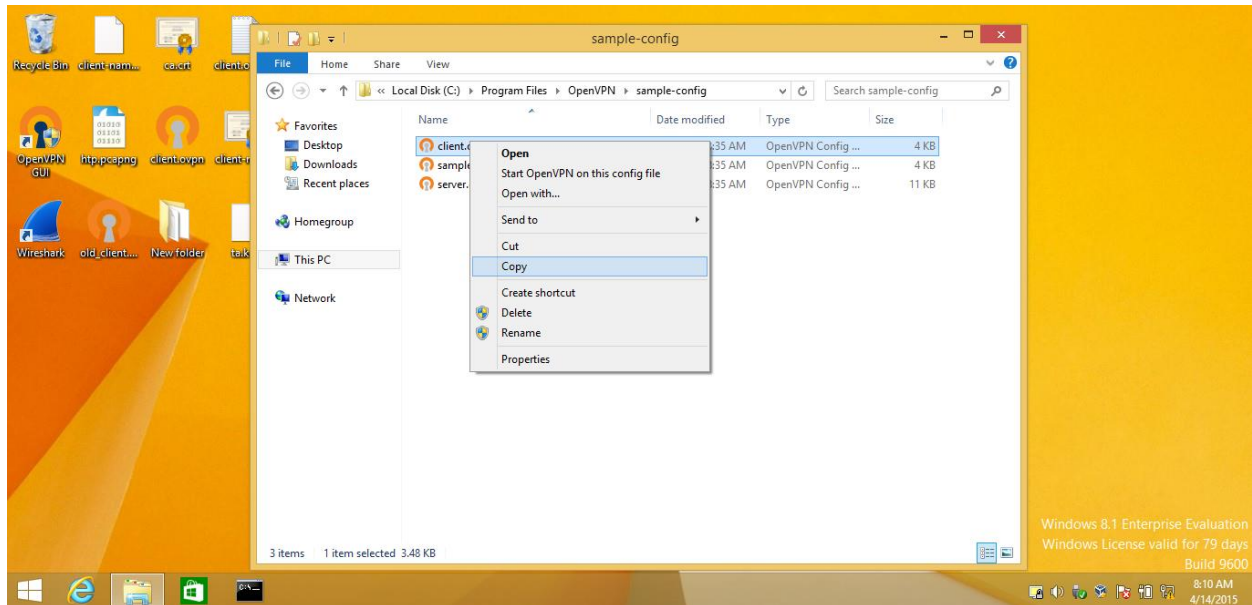
#### Part4:

Client configuration:

Download OpenVPN GUI from OpenVPN website.

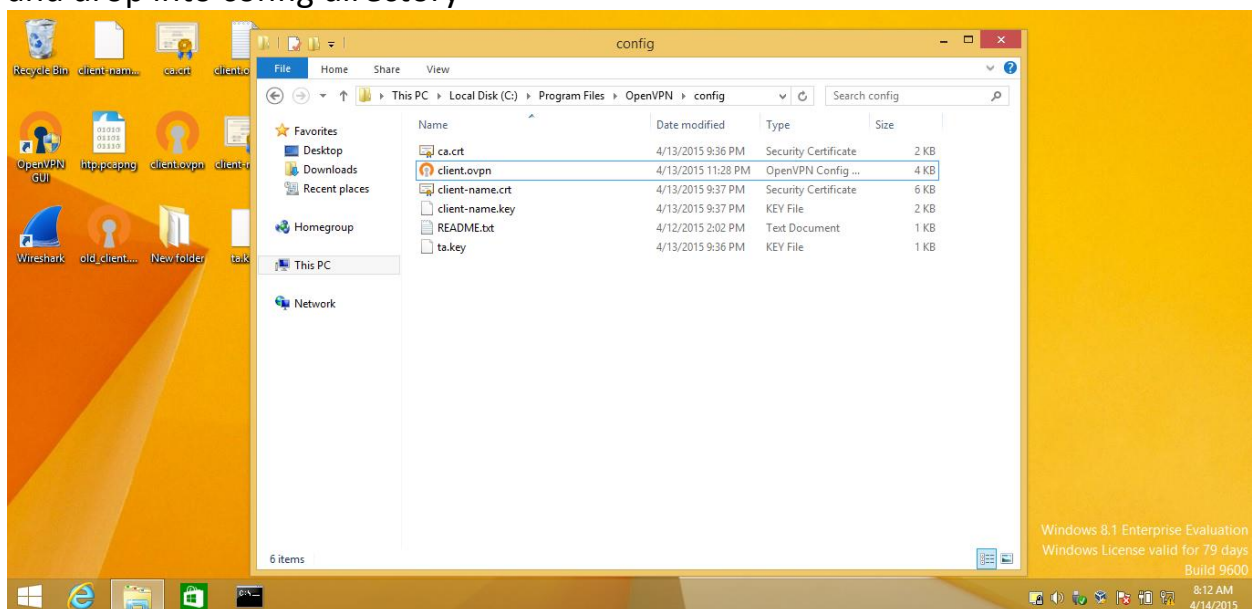
Go to program files> OpenVPN >sample-config files

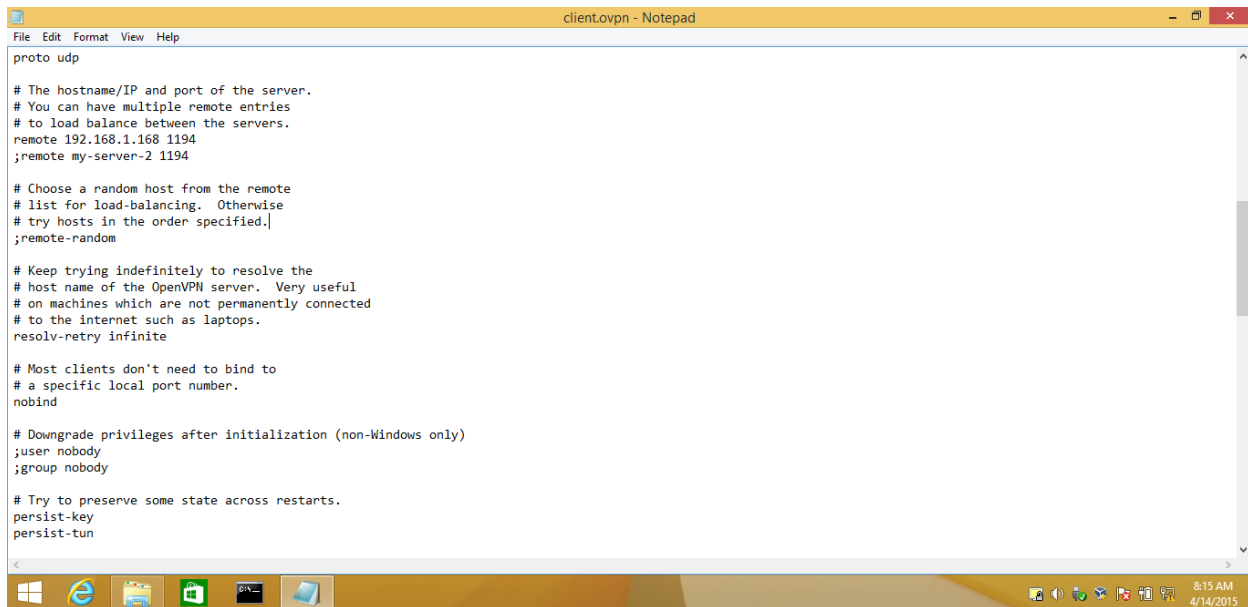
Copy the client.ovpn file.



Now paste this file in openVPN > config directory

Copy the four key files we obtained from the server to the desktop and then drag and drop into config directory





```
client.ovpn - Notepad
File Edit Format View Help
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.1.168 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing. Otherwise
# try hosts in the order specified.
;remote-random

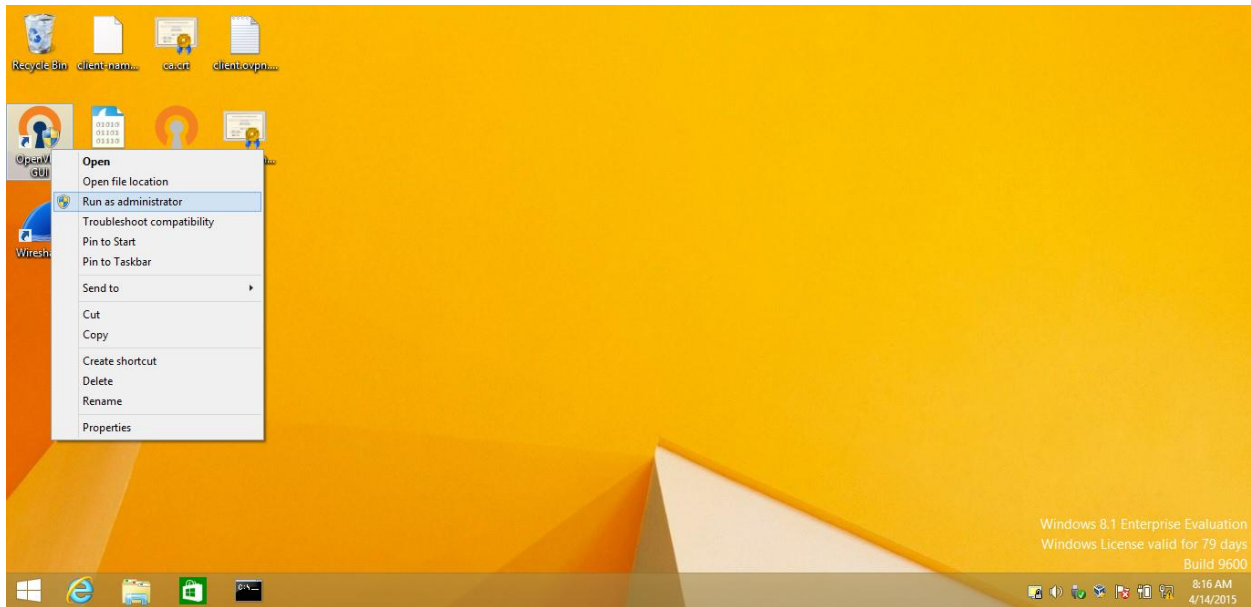
# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

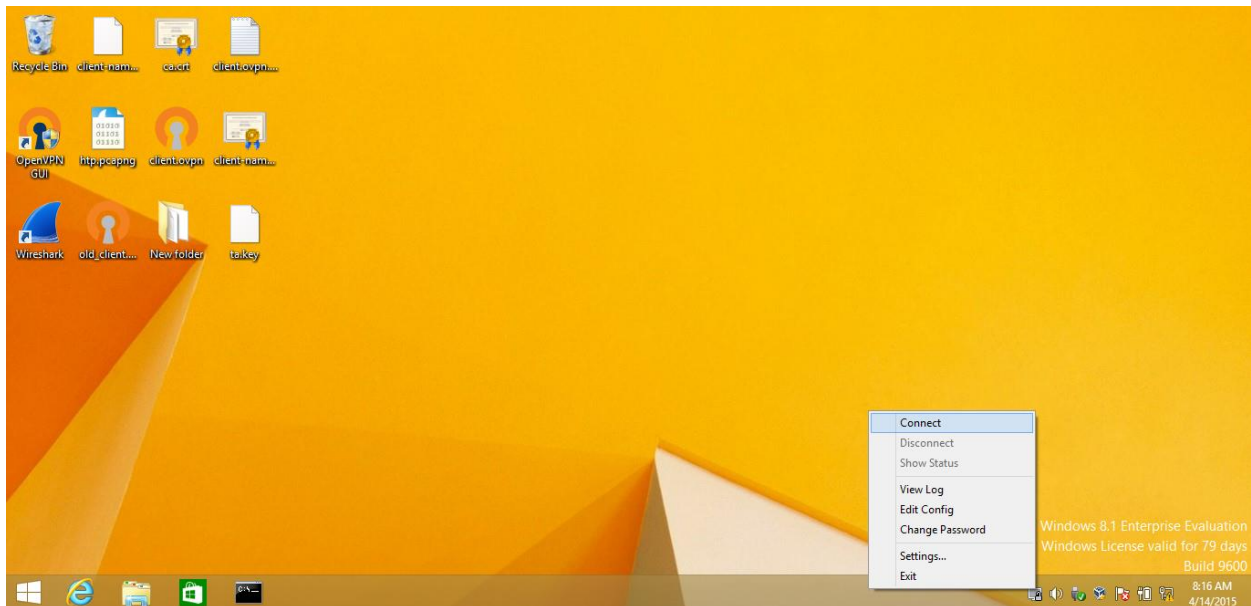
# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun
```

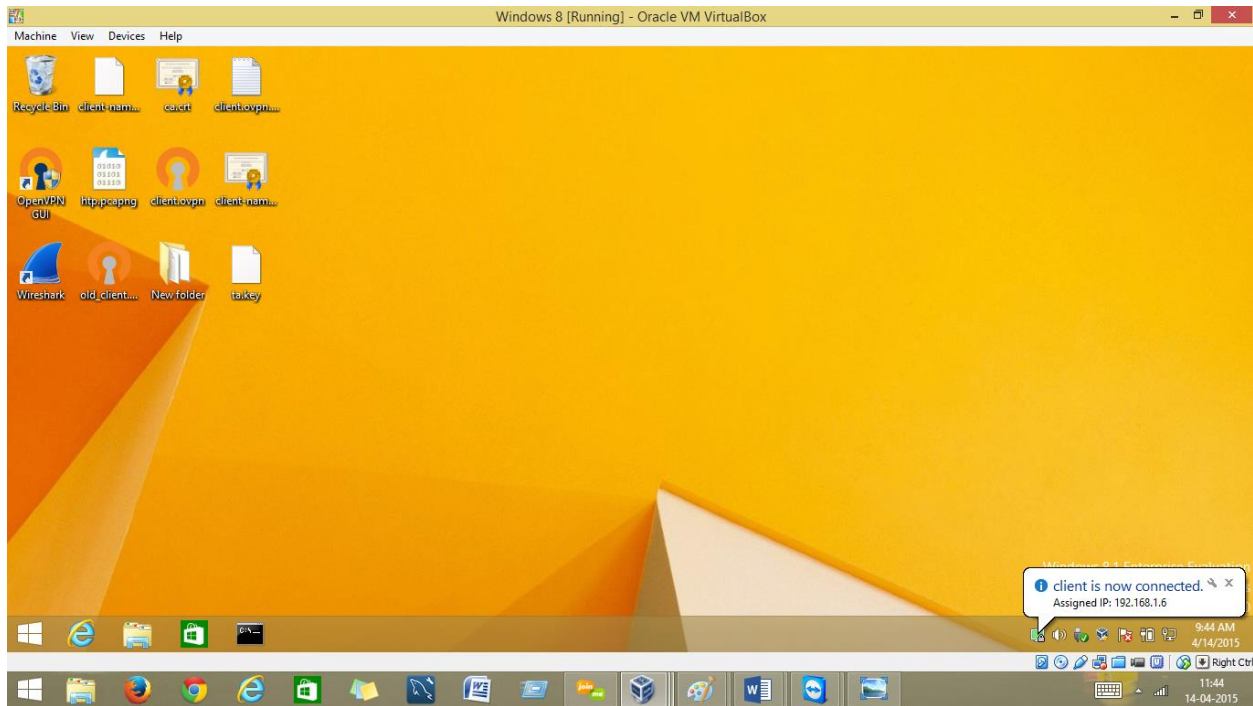
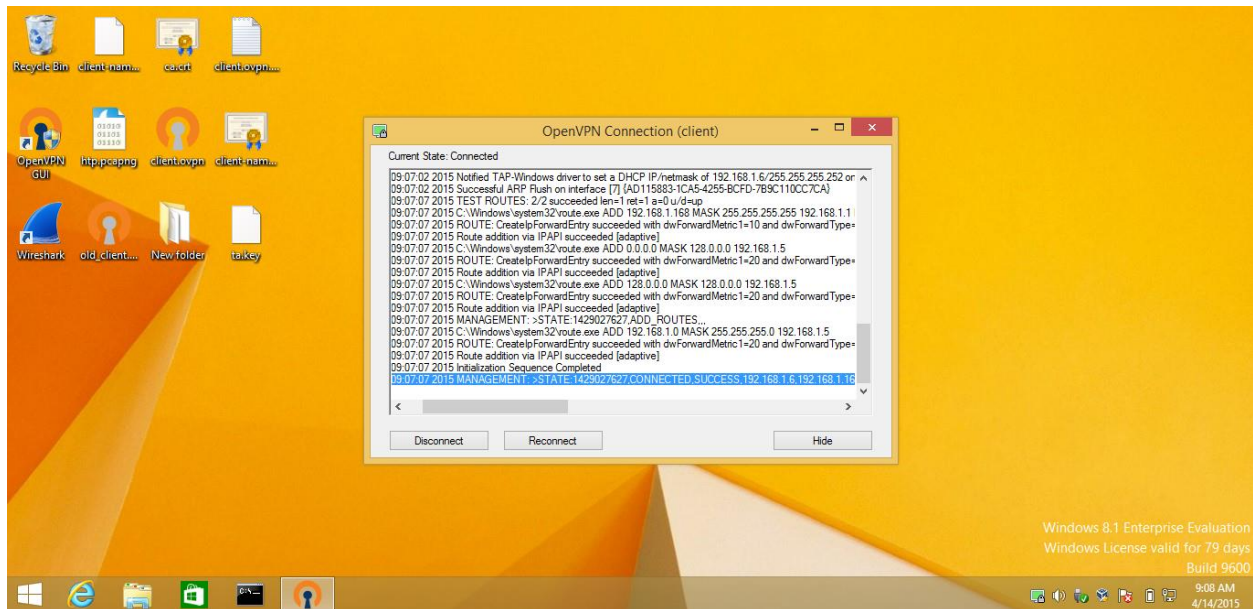
The above screenshot describes the client.ovpn file with remote command where we give vpn server ip address and port number 1194, since 1194 port is by default with openvpn.



Now, run the open vpn gui and run as administrator, then click on right bottom on the icon and right click to connect as below.



Once you click connect, it will show the OpenVPN status file log and it will connect to the server with the IP address.



OpenVPN Client is successfully completed.

**References:**

1. For OPENVPN setup on Ubuntu server  
<https://help.ubuntu.com/its/serverguide/openvpn.html>
2. <http://www.thegeekstuff.com/2013/09/openvpn-setup/>
3. For Linux commands: Linuxcommands.org
4. For Samba Instructions: <https://help.ubuntu.com/community/>
5. For VPN- [http://en.wikipedia.org/wiki/Virtual\\_private\\_network](http://en.wikipedia.org/wiki/Virtual_private_network)