Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

How to install and configure OpenVPN in Ubuntu 22.04

(It is extra help: please don't complain about anything in this document instead try to find a solution 😊)

Step 1: install openvpn

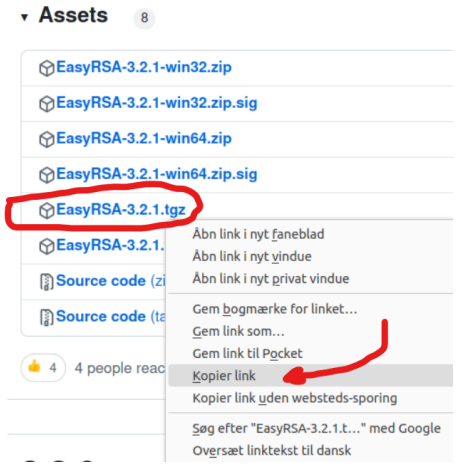
```
sudo apt update
sudo apt install openvpn
```
(the newer versions of Ubuntu have it already installed)

```
homayoon@homayoon-VirtualBox:~$ sudo apt install openvpn
[sudo] adgangskode for homayoon:
Indlæser pakkelisterne... Færdig
Opbygger afhængighedstræ... Færdig
Læser tilstandsoplysninger... Færdig
openvpn er allerede den nyeste version (2.5.9-0ubuntu0.22.04.3).
openvpn sat til manuelt installeret.
0 opgraderes, 0 nyinstalleres, 0 afinstalleres og 17 opgraderes ikke.
```

OpenVPN uses certificates to encrypt traffic between the server and clients.
To issue certificates, we will set up our own certificate authority (CA).
To build our CA public key infrastructure (PKI), **we will need EasyRSA**.

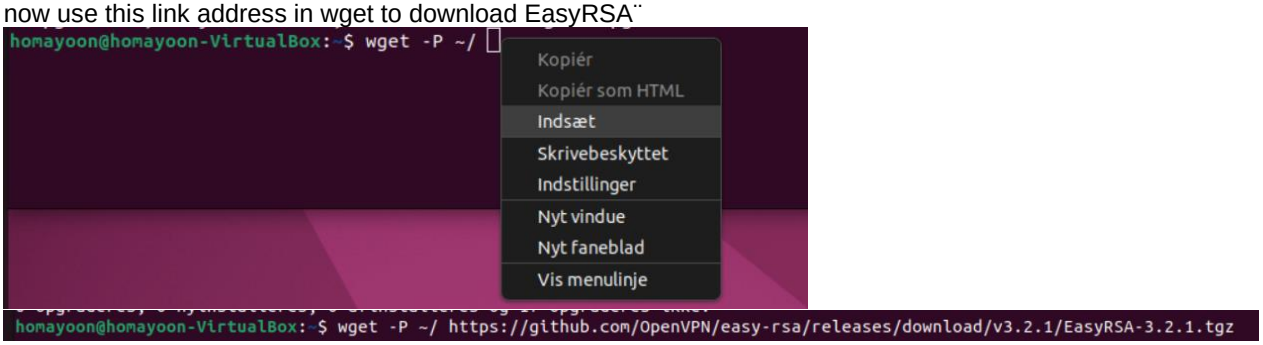
Open Firefox browser in your Ubuntu and Get EasyRSA link from the following Github repository:
https://github.com/OpenVPN/easy-rsa/releases

Right click on EasyRSA-3.2.1.tgz and copy the link address *(By this time the version would be something else, therefor you should change the v3.2.1 to the one you have downloaded)*



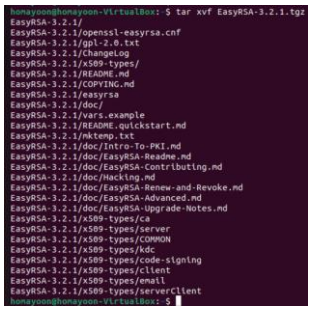
Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

now use this link address in wget to download EasyRSA¨



wget -P ~/ https://github.com/OpenVPN/easy-rsa/releases/download/v3.2.1/EasyRSA-3.2.1.tgz

```
cd ~
tar xvf EasyRSA-3.2.1.tgz (use the version you have downloaded e.g EasyRSA-unix-v3.0.8.tgz)
```



Step 2 – Configuring the EasyRSA variables and Building the CA

```
cd ~/EasyRSA-3.2.1/
cp vars.example vars
```

Open this new file using nano editor

```
nano vars
```

Change the Country name city org and other variables to your own location, address, email etc.

Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

~/EasyRSA-3.0.4/vars

```
~/EasyRSA-3.0.4/vars
. . .

set_var EASYRSA_REQ_COUNTRY    "US"
set_var EASYRSA_REQ_PROVINCE   "NewYork"
set_var EASYRSA_REQ_CITY       "New York City"
set_var EASYRSA_REQ_ORG        "DigitalOcean"
set_var EASYRSA_REQ_EMAIL      "admin@example.com"
set_var EASYRSA_REQ_OU         "Community"
```

From above to the following

```
set_var EASYRSA_REQ_COUNTRY     "DK"
set_var EASYRSA_REQ_PROVINCE    "Zealand"
set_var EASYRSA_REQ_CITY        "Roskilde"
set_var EASYRSA_REQ_ORG         "SmartiICT"
set_var EASYRSA_REQ_EMAIL       "mofa@zealand.dk"
set_var EASYRSA_REQ_OU          "Computer Science"

# Choose a size in bits for your keypairs. The recomm
```

Save the file by **Pressing control (Ctrl + o)** on your keyboard and O
Accept the filename by **Pressing Enter**.
Exit the file by **Pressing (Ctrl + x)**

Now initialize the Public Key Infrastructure (PKI) by the following command

```
./easyrsa init-pki
```

```
homayoon@homayoon-VirtualBox:~/EasyRSA-v3.0.6$ ./easyrsa init-pki

Note: using Easy-RSA configuration from: ./vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /home/homayoon/EasyRSA-v3.0.6/pki

homayoon@homayoon-VirtualBox:~/EasyRSA-v3.0.6$
```

Now create the ca certificate (ca.crt) and the ca private key (ca.key)

```
./easyrsa build-ca nopass
```

You can chage [Easy-RSA CA] to something else (I have changed it to Smartict). If you press Enter then it will use the default name which is [Easy-RSA CA]. (look the following image)

Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

```
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:smartict

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/homayoon/EasyRSA-v3.0.6/pki/ca.crt

homayoon@homayoon-VirtualBox:~/EasyRSA-v3.0.6$
```

Now we are ready to sign certificate requests

Step 3 – creating the server certificate, private key, and Encryption files

```
./easyrsa gen-req server nopass
```

This time do not change the default name [server] just press Enter

```
-----
Common Name (eg: your user, host, or server name) [server]:

Keypair and certificate request completed. Your files are:
req: /home/homayoon/EasyRSA-v3.0.6/pki/reqs/server.req
key: /home/homayoon/EasyRSA-v3.0.6/pki/private/server.key

homayoon@homayoon-VirtualBox:~/EasyRSA-v3.0.6$
```

The above command will create a private key and a request file for the server, you can find them in the pki folder.
Now we will move them to /etc/openvpn/ folder using the following command

```
sudo cp ~/EasyRSA-3.2.1/pki/private/server.key /etc/openvpn/
```

now sign the request

```
./easyrsa sign-req server server
```

```
homayoon@homayoon-VirtualBox:~/EasyRSA-v3.0.6$ ./easyrsa sign-req server server

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1  11 Sep 2018


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 1080 days:

subject=
    commonName                = server


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /home/homayoon/EasyRSA-v3.0.6/pki/safessl-easyrsa.cnf
```

Now copy the **ca.crt** and **server.crt** certificates to /etc/openvpn

(**ca.crt** is inside `~/EasyRSA-3.2.1/pki/` and **server.crt** is inside `~/EasyRSA-3.2.1/pki/issued` folder)

```
sudo cp ~/EasyRSA-3.2.1/pki/ca.crt /etc/openvpn/
sudo cp ~/EasyRSA-3.2.1/pki/issued/server.crt /etc/openvpn/
```

Navigate to `EasyRSA-3.2.1` it by using the following command

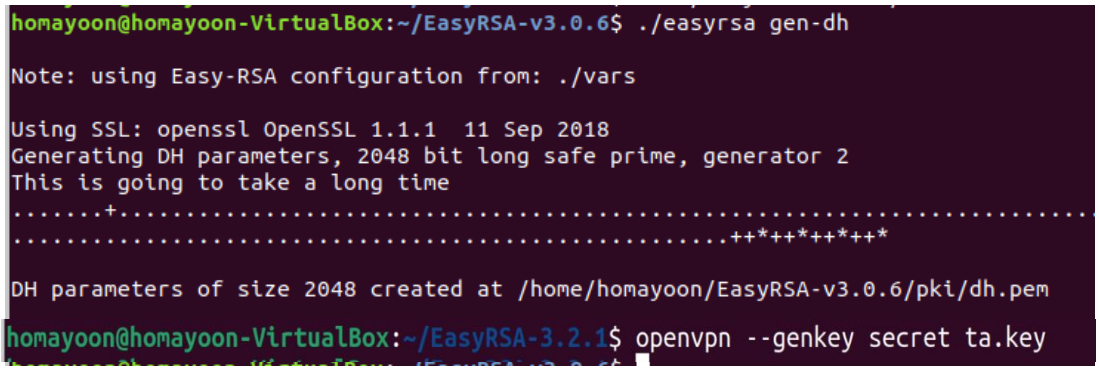
```
cd ~/EasyRSA-3.2.1/
```

Type the following command to generate Diffie-Hellman key

```
./easyrsa gen-dh
```

Now generate an HMAC signature (you know what it is and why …)

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



Copy these two files to /etc/openvpn/ directory

```
sudo cp ~/EasyRSA-3.2.1/ta.key /etc/openvpn/
sudo cp ~/EasyRSA-3.2.1/pki/dh.pem /etc/openvpn/
```

We are finished generateing CA and Server keys, certificates and HMAC of them. Now we are ready to create client key pairs.

Step 4 - Generating client key pair

Create a directory to store the client certificates

```
mkdir -p ~/client-configs/keys
chmod -R 700 ~/client-configs
cd ~/EasyRSA-3.2.1/
./easyrsa gen-req client1 nopass
```

Press Enter to accept the common name

```
-----
Common Name (eg: your user, host, or server name) [client1]:

Keypair and certificate request completed. Your files are:
req: /home/homayoon/EasyRSA-v3.0.6/pki/reqs/client1.req
key: /home/homayoon/EasyRSA-v3.0.6/pki/private/client1.key

homayoon@homayoon-VirtualBox:~/EasyRSA-v3.0.6$
```

Copy the client1.key to /client/configs/keys/

```
cp pki/private/client1.key ~/client-configs/keys/
```

Now sign the cient1 request as you did for the server this time the request type is client

```
./easyrsa sign-req client client1
```

When propted for confirmation type yes

```
homayoon@homayoon-VirtualBox:~/EasyRSA-v3.0.6$ ./easyrsa sign-req client client1

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1  11 Sep 2018


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 1080 days:

subject=
    commonName                = client1


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /home/homayoon/EasyRSA-v3.0.6/pki/safessl-easyrsa.cnf
Can't load /home/homayoon/EasyRSA-v3.0.6/pki/.rnd into RNG
140412188115392:error:2406F079:random number generator:RAND_load_file:Cannot oper
yRSA-v3.0.6/pki/.rnd
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'client1'
Certificate is to be certified until Feb 26 15:08:09 2023 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /home/homayoon/EasyRSA-v3.0.6/pki/issued/client1.crt

homayoon@homayoon-VirtualBox:~/EasyRSA-v3.0.6$
```

This will create **client1.crt** client certificate

Now copy the client client1.crt, ta.key and ca.crt to /client-configs/keys/ directory

```
cp ~/EasyRSA-3.2.1/pki/issued/client1.crt ~/client-configs/keys/
```

```
cp ~/EasyRSA-3.2.1/ta.key ~/client-configs/keys/
sudo cp /etc/openvpn/ca.crt ~/client-configs/keys/
```

Now we are finished with creating the CA, Server and Client Keys and Certificates.

It's time to configure our OpenVPN server.

The steps 5 to 10 are simple steps. Therefore, you should not expect details.

[*Step 9: where you generate **client1.ovpn**: copy the client1.ovpn to desktop by using the **cp** command then send it to yourself by email. then open your email in your windows and save the file on your windows.*]

Step 5 – Configuring the OpenVPN Service

Start by copying a sample OpenVPN configuration file into the configuration directory and then extract it in order to use it as a basis for your setup:

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

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

Open the server configuration file in your preferred text editor:

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

Now Edit the following:

```
tls-auth ta.key 0 (uncomment if commented remove ;)
cipher AES-256-CBC (uncomment if commented remove ;)
```
bellow this add
```
auth SHA256
```

change dh dh2048.pem to
```
dh dh.pem
```

```
user nobody (uncomment if commented remove ;)
group nogroup (uncomment if commented remove ;)
```

Save and close ctrl + O and ctrl + x

Step 6: Server networking configuration

modify the /etc/sysctl.conf file for IP forwarding
```
sudo nano /etc/sysctl.conf
net.ipv4.ip_forward=1 (uncomment if commented remove #)
```

Save and close ctrl + O and ctrl + x

Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

Now type:
```
sudo sysctl -p
```

You should get the following output
```
net.ipv4.ip_forward = 1
```

Now type the following to find your network interface
```
ip route | grep default
```
mine is **enp0s3** yours could be different (You will use this in rules.before)

```
homayoon@homayoon-VirtualBox:~$ ip route | grep default
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
```

Now you can add firewall rules to before.rules
```
sudo nano /etc/ufw/before.rules
```

add the lines in Orange color:
```
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#
*nat
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 10.8.0.0/8 -o enp0s3 -j MASQUERADE
COMMIT
# Don't delete these required lines, otherwise there will be errors
*filter
. . .
```

Save and close the file

Now allow forwarded packets by opening ufw and changing “DROP” to “ACCEPT” on line DEFAULT_FORWARD_POLICY="DROP"

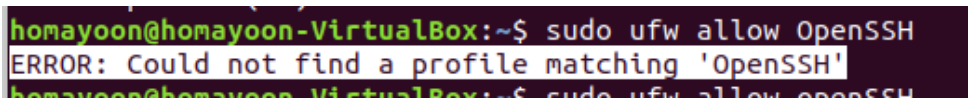
```
sudo nano /etc/default/ufw

DEFAULT_FORWARD_POLICY="ACCEPT"
```
Save and close the file

Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

Now run the following commands

```
sudo ufw allow 1194/udp
sudo ufw allow OpenSSH
```

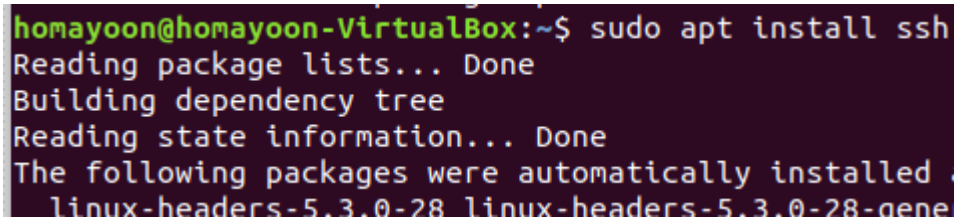
If you get the following Error:



Then download and install OpenSSH by using the following command

```
sudo apt install ssh
```

```
sudo ufw allow OpenSSH
```



Now run the following commands

```
sudo ufw disable
sudo ufw enable
sudo systemctl start openvpn@server
sudo systemctl status openvpn@server
```

```
homayoon@homayoon-VirtualBox:~$ sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
homayoon@homayoon-VirtualBox:~$ sudo ufw disable
Firewall stopped and disabled on system startup
homayoon@homayoon-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
homayoon@homayoon-VirtualBox:~$ sudo systemctl start openvpn@server
homayoon@homayoon-VirtualBox:~$ sudo systemctl status openvpn@server
● openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/lib/systemd/system/openvpn@.service; indirect; vendor preset: enabled)
   Active: active (running) since Tue 2020-03-17 15:01:21 CET; 26s ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Main PID: 20656 (openvpn)
   Status: "Initialization Sequence Completed"
    Tasks: 1 (limit: 4666)
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─20656 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/server.status

Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: Could not determine IPv4/IPv6 protoco
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: Socket Buffers: R=[212992->212992] S=
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: UDPv4 link local (bound): [AF_INET][u
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: UDPv4 link remote: [AF_UNSPEC]
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: GID set to nogroup
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: UID set to nobody
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: MULTI: multi_init called, r=256 v=256
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: IFCONFIG POOL: base=10.8.0.4 size=62,
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: IFCONFIG POOL LIST
Mar 17 15:01:21 homayoon-VirtualBox ovpn-server[20656]: Initialization Sequence Completed
lines 1-22/22 (END)
```

Check that the openvpn tun0 interface is available

```
ip addr show tun0
```

```
homayoon@homayoon-VirtualBox:~$ ip addr show tun0
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
 UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::6758:a440:e88:ab3f/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

Now enable it so it starts automatically when you start/restart the computer:

```
sudo systemctl enable openvpn@server
```

```
homayoon@homayoon-VirtualBox:~$ sudo systemctl enable openvpn@server
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn@server.service → /lib/system
d/system/openvpn@.service.
homayoon@homayoon-VirtualBox:~$
```

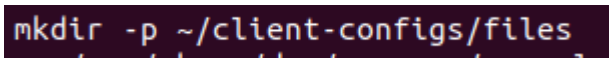
Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

Client configuration

Now open your Terminal and do the following steps

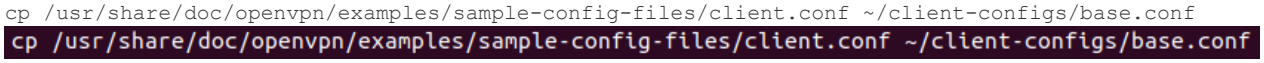
Step 1: Create files directory. This directory will hold your client configuration files e.g client1.ovpn

```
mkdir -p ~/client-configs/files
```



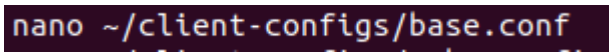
Step 2: Copy the sample client config file to ~/client-configs/ folder and give it a new name “base.conf”

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf
```



Step 3: open this base.conf file by using nano

```
nano ~/client-configs/base.conf
```



Step 4: Now make the following changes to base.conf file.

Find this line: `remote remote-my-server-1 1194`

```
remote remote-my-server-1 1194
```

Find the protocol it should be udp

```
proto udp
```

put a “#” sign before the following 4 lines

```
#ca ca.crt
#cert client.crt
#key client.key

#tls-auth ta.key 1
```

Find this line and make sure it looks as follows. If the second line does not exist, just type it in (insert it).

```
cipher AES-256-CBC
auth SHA256
```

Add the following line as well.

```
key-direction 1
```

save and close the file

Step 5: Create a make_config.sh script file

```
nano ~/client-configs/make_config.sh
```

Add the following lines to make_config.sh file then save and close the file.

```
#!/bin/bash

# First argument: Client identifier

KEY_DIR=~/client-configs/keys
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf

cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${KEY_DIR}/${1}.key \
    <(echo -e '</key>\n<tls-auth>') \
    ${KEY_DIR}/ta.key \
    <(echo -e '</tls-auth>') \
    > ${OUTPUT_DIR}/${1}.ovpn
```

Step 6: Make the file executable

```
chmod 700 ~/client-configs/make_config.sh
```

Step 7: Now create the file configuration file, which will be used on the client. In your case in your Windwos 10.

```
cd ~/client-configs
sudo ./make_config.sh client1
```

If you get an error on step 7 saying "*/make_config.sh: line 8: /root/client-configs/files/client1.ovpn: No such file or directory* " then do this :

sudo chown -R user.user ~/client-configs

(Where user.user is your username e.g in my case it will be **sudo chown -R homayoon.homayoon ~/client-configs)**

then run step 7 without sudo :

./make_config.sh client1

This will create a **client1.ovpn** file in the files folder under client_configs folder.

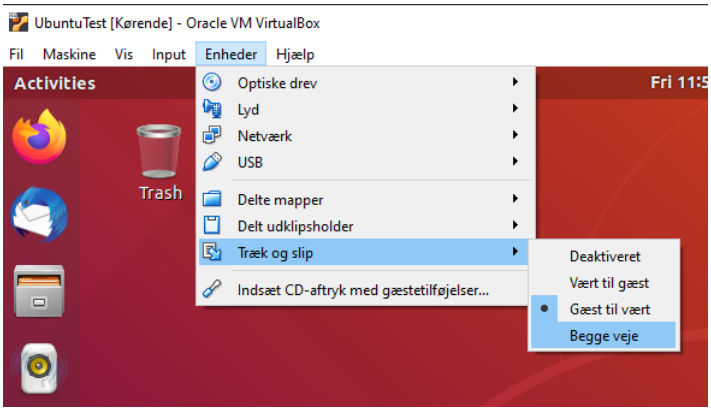
Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

Step 8: Now it's time to move this **client1.ovpn** to your Windows 10.

Copy client1.ovpn to the Desktop

```
cp ~/client-configs/files/client1.ovpn ~/Desktop/client1.ovpn
```

Now drag and drop it to your Windows desktop. For this to work you must enable drag and drop as shown in the following image.

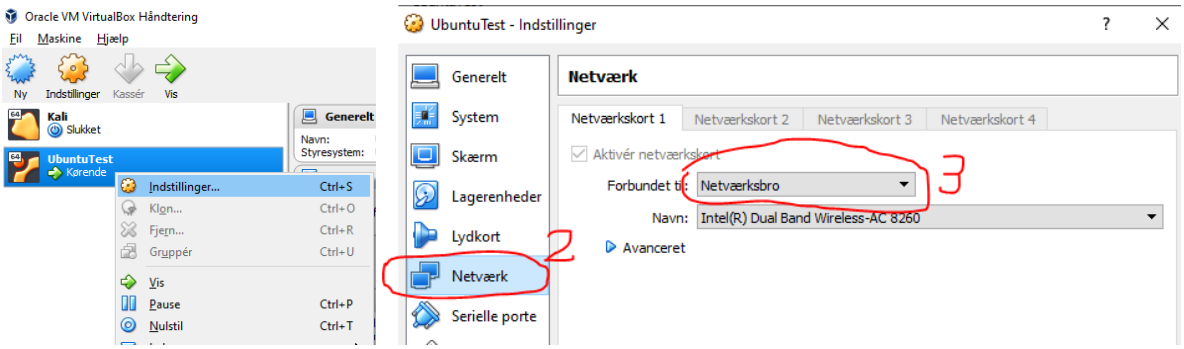


If drag and drop does not work for your then, open your browser, login to e.g Gmail or Hotmail or … and send this file as attachment to yourself. then in Windows open your mail program and save the client1.ovpn on your windows.

Change your VirtualBox network from NAT to Bridge

First of all make sure that your VirtualBox network is set to "Bridge network" in Danish it will be "Netværksbro" If not please change it.

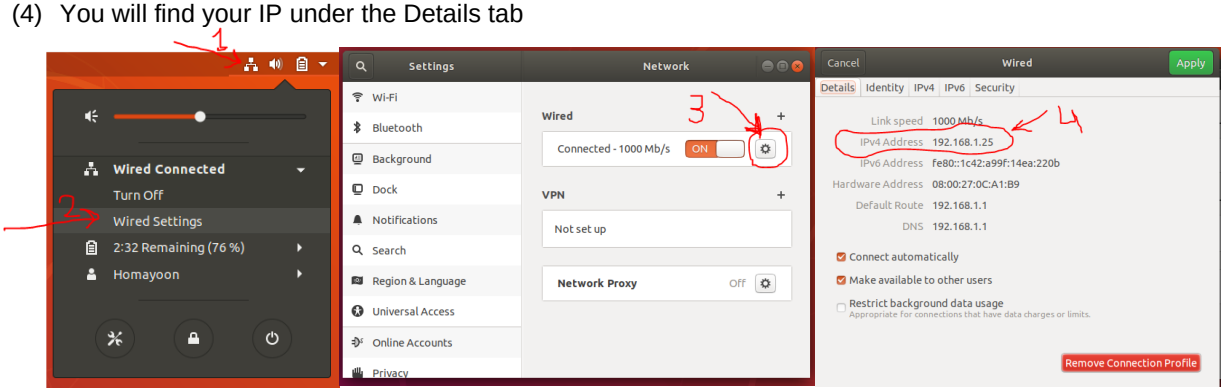
1) Right click on your Ubuntu/openvpnserver and choose settings/indstillinger
2) Click on network/Netværk and then choose Bridge/Netværksbro from the dropdown menu
3) Restart your ubuntu



Author: Homayoon Fayez
Associate Professor
Zealnd, Academy of Technologies and Business

Find the **openvpnserver** IP address by:

(1) clicking the network icon on the upper right corner of your ubuntu desktop.
(2) Click on Wired Settings
(3) Click on config icon wheel
(4) You will find your IP under the Details tab

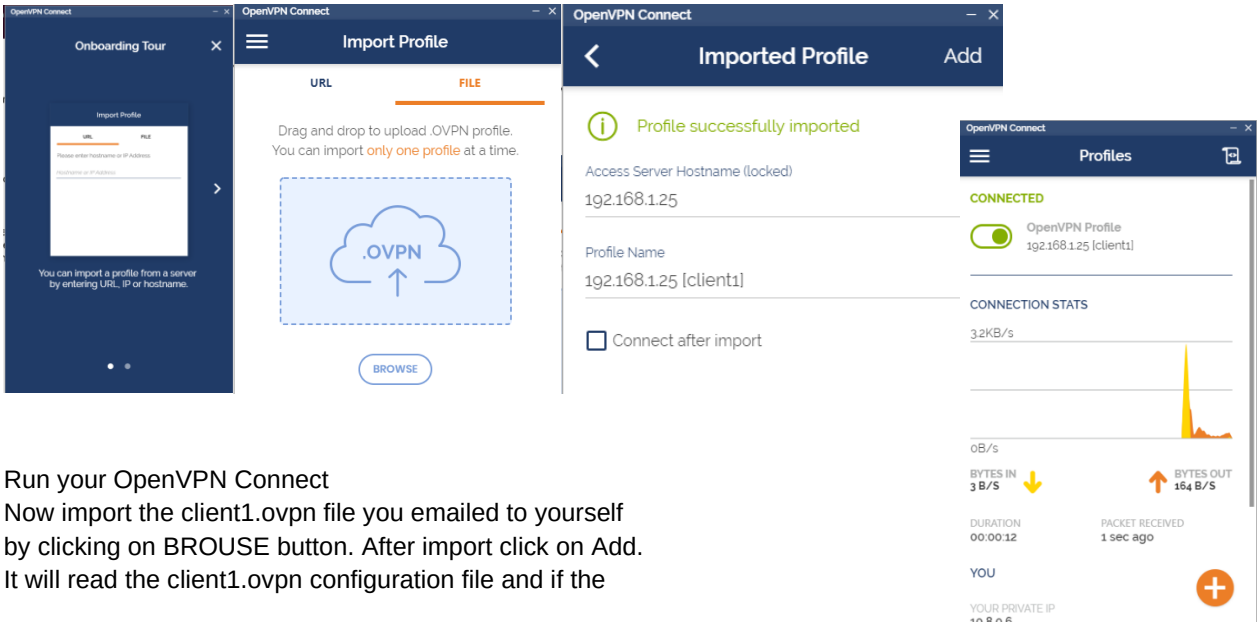


In my case the IP address is `192.168.1.25` Now it should look like this

Now open the client1.ovpn file inside your Windows and change `remote-my-server-1` to the IP address of your ubuntu(openvpnserver)

Installing OpenVPN Client

Download and Install OpenVPN connect for windows from https://openvpn.net/client-connect-vpn-for-windows/ `(Thanks to Alex)`



Run your OpenVPN Connect
Now import the client1.ovpn file you emailed to yourself by clicking on BROUSE button. After import click on Add. It will read the client1.ovpn configuration file and if the

configuration is right i.e. the server IP address, protocols
and all other configuration in client1.ovpn file and the server
configuration in your ubuntu then it will connect.

If, on the server, you run the status command again it will show the communication with the windows client.