

Livrable d'installation d'OPENVPN sous Linux

Présentés par : **Abdelaziz KARROUM**

Aymane MOSSADAQ

Encadré par : **Prof. Mehdi MOUKHAFI**

Plan de travail :

I)- Pourquoi le choix d'installation d'openvpn à partir d'un script ?

1)-Les avantages de script

2)-Les inconvénients de script

II)-Les étapes d'installation de OPENVPN sous Linux :

1)- Installation d'Openvpn à partir d'un script

2)-Donner la permission d'exécution de openvpn-install.sh en mode root

3)-Exécuter openvpn-install.sh

4)-Recharger la configuration d'openvpn pour prendre en compte vos modifications

5)-Vérification de l'état d'openvpn

6)-Activation de Firewall

7)-Déplacement de fichier client

8)-Installation de network-manager

9)-la plage de vpn est :

10) -L'activation de VPN

III)-Démonstration par WireShark :

1)-Définition de Wireshark :

2)-Avant l'activation d'openvpn :

3)-Après l'activation d'openvpn :

I)-Pourquoi le choix d'installation d'openvpn à partir d'un script ?

- Nous avons choisi le script parce que nous avons rencontré des problèmes lors de la création des certificats au niveau d'easy-rsa, après plusieurs tentatives de création manuelle.

1)-Les avantages de script :

Les scripts simplifient la création d'outils personnalisés pour administrer les logiciels et vous permettent d'accomplir rapidement des tâches courantes, ce qui vous permet d'effectuer des tâches volumineuses plus facilement et de manière plus cohérente.

2)-Les inconvénients de script :

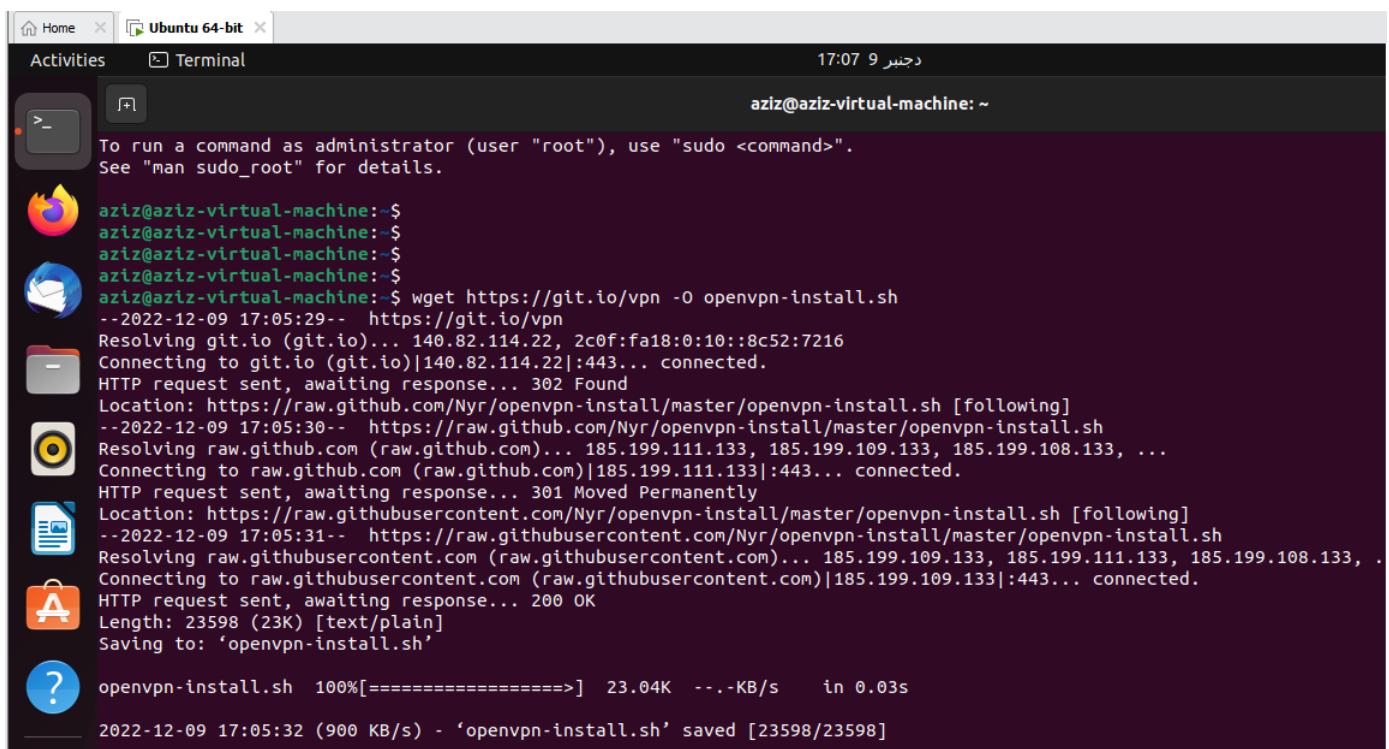
- ❖ Il nécessite de tout développer.
- ❖ Il impose de nombreuses modifications lors d'une modification au niveau de la source, du contenu ou de la destination.
- ❖ Il est facteur d'un grand nombre de bugs et de régressions à chaque modification.
- ❖ Il nécessite l'utilisation d'un planificateur de tâches externe.
- ❖ Il nécessite de tout documenter, au risque de se perdre dans le code produit.

II)-Les étapes d'installation de OPENVPN sous Linux :

1)- Installation de Openvpn à partir d'un script :

➤ wget <https://git.io/vpn> -O openvpn-install.sh

- ❖ **Wget** : est un outil informatique créé par le projet GNU. il est gratuit pour le téléchargement non interactif de fichiers à partir de différents serveurs Web. Il prend en charge les protocoles http https et ftp.
- ❖ **L'utilisation de -O** n'est pas destinée à signifier simplement utiliser le nom de fichier au lieu de celui de l'URL ; plutôt c'est analogue à la redirection du shell.
- ❖ **L'extension .sh** : est un fichier de commande de langage de script qui contient un programme informatique à exécuter par le shell dans linux.



```
aziz@aziz-virtual-machine: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

aziz@aziz-virtual-machine:~$
aziz@aziz-virtual-machine:~$
aziz@aziz-virtual-machine:~$
aziz@aziz-virtual-machine:~$ wget https://git.io/vpn -O openvpn-install.sh
--2022-12-09 17:05:29-- https://git.io/vpn
Resolving git.io (git.io)... 140.82.114.22, 2c0f:fa18:0:10::8c52:7216
Connecting to git.io (git.io)[140.82.114.22]:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh [following]
--2022-12-09 17:05:30-- https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.109.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)[185.199.111.133]:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh [following]
--2022-12-09 17:05:31-- https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)[185.199.109.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23598 (23K) [text/plain]
Saving to: 'openvpn-install.sh'

openvpn-install.sh 100%[=====] 23.04K --.-KB/s in 0.03s

2022-12-09 17:05:32 (900 KB/s) - 'openvpn-install.sh' saved [23598/23598]
```

N.B : On peut utiliser `wget` pour télécharger d'autre fichier à partir d'un autre site. Par exemple vous pouvez obtenir la dernière version de WordPress en utilisant `wget` comme suit : `wget https://wordpress.org/latest.zip`

2)-Donner la permission d'exécution de `openvpn-install.sh` en mode root :

➤ `sudo chmod +x openvpn-install.sh`

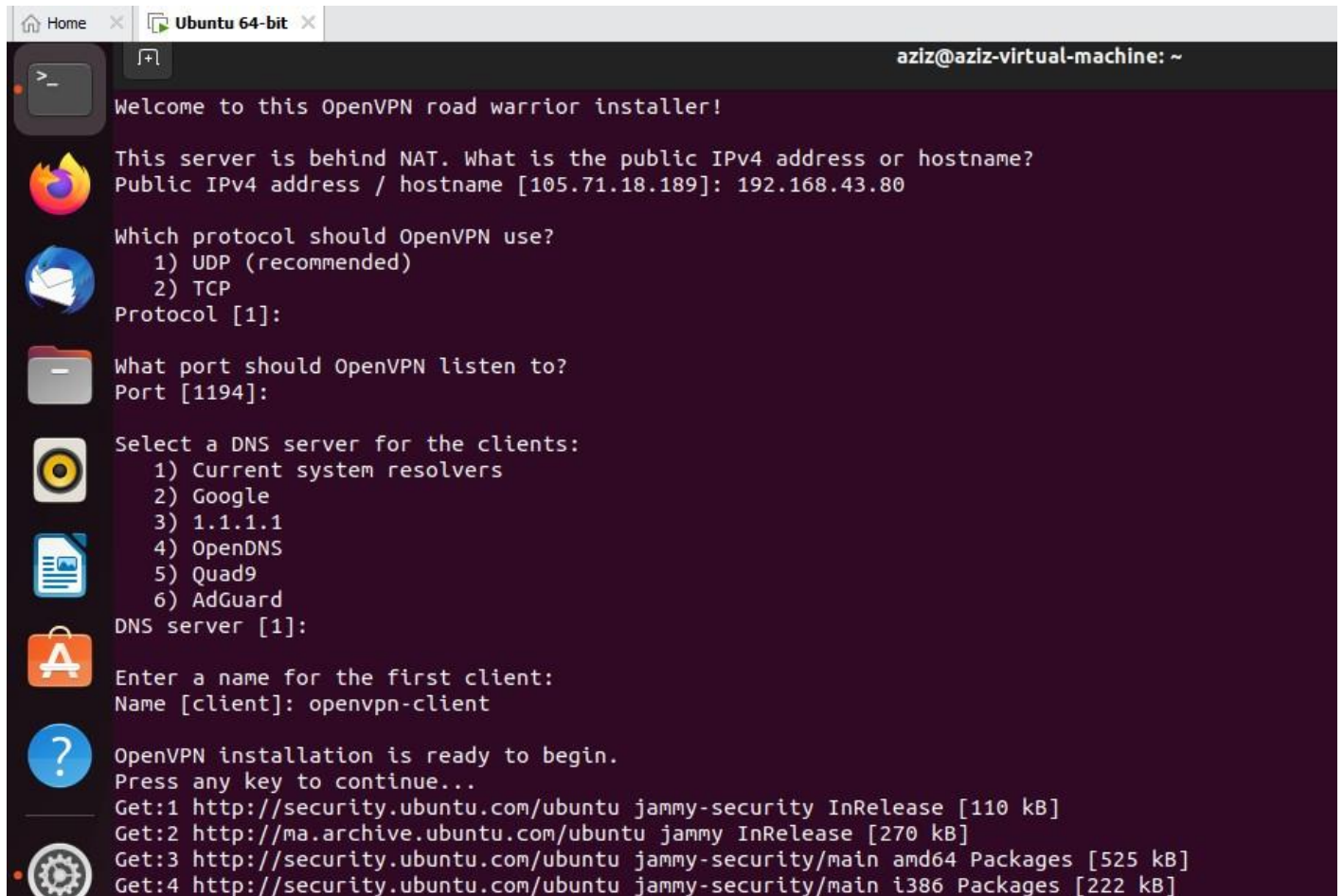
```
aziz@aziz-virtual-machine:~$  
aziz@aziz-virtual-machine:~$  
aziz@aziz-virtual-machine:~$  
aziz@aziz-virtual-machine:~$ sudo chmod +x openvpn-install.sh  
[sudo] password for aziz:  
aziz@aziz-virtual-machine:~$
```

3)-Exécuter `openvpn-install.sh` :

➤ `sudo ./openvpn-install.sh`

```
aziz@aziz-virtual-machine:~$  
aziz@aziz-virtual-machine:~$  
aziz@aziz-virtual-machine:~$ sudo ./openvpn-install.sh
```





```
Home x Ubuntu 64-bit x aziz@aziz-virtual-machine: ~
Welcome to this OpenVPN road warrior installer!

This server is behind NAT. What is the public IPv4 address or hostname?
Public IPv4 address / hostname [105.71.18.189]: 192.168.43.80

Which protocol should OpenVPN use?
1) UDP (recommended)
2) TCP
Protocol [1]:

What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
1) Current system resolvers
2) Google
3) 1.1.1.1
4) OpenDNS
5) Quad9
6) AdGuard
DNS server [1]:

Enter a name for the first client:
Name [client]: openvpn-client

OpenVPN installation is ready to begin.
Press any key to continue...
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:2 http://ma.archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [525 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [222 kB]
```

- Après avoir exécuté le script, nous trouvons la liste des informations comme vous pouvez le voir ci-dessus :
- ❖ Entrez votre adresse privé (IP) pour le service exemple : **192.168.43.80**
- ❖ Choisissez le protocole convenable pour vous **(UDP/TCP)**.
- ❖ Laissez le port **[1194]** qui est choisi par défaut ; mais il y a plusieurs ports utiliser par le vpn.
- ❖ Sélectionner le serveur DNS convenable pour le client **«1) Current system resolvers »**.
- ❖ Entrez le nom de client comme par exemple : **«openvpn-client»**.
- ❖ Et après cette configuration vous allez voir l'installation de openvpn.

- Puis le téléchargement **des certificats** qui sont des fichiers permettant de contenir la clé publique ainsi que d'autres informations à l'aide de **openssl**. Le certificat ajoute une notion de confiance à un référent, générateur du certificat racine, l'Autorité de Certification (**ca.crt**) et **ca.key** comporte la clé de ca.crt.
- Le fichier **easy-rsa** est un utilitaire pour gérer le **ICP**.
- OpenVPN se base sur une infrastructure de clés publiques (**ICP**, **PKI** en anglais).

[illegible]

4)-Recharger la configuration d'openvpn pour prendre en compte vos modifications :

- `sudo systemctl restart openvpn`

```

aziz@aziz-virtual-machine: ~
The client configuration is available in: /root/openvpn-client.ovpn
New clients can be added by running this script again.
aziz@aziz-virtual-machine:~$
aziz@aziz-virtual-machine:~$
aziz@aziz-virtual-machine:~$ sudo systemctl restart openvpn
[sudo] password for aziz:

```

5)-Vérification de l'état d'openvpn :

- `sudo systemctl status openvpn`


```

aziz@aziz-virtual-machine:~$ sudo systemctl status openvpn
● openvpn.service - OpenVPN service
   Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
   Active: active (exited) since Fri 2022-12-09 17:52:18 +01; 19s ago
     Process: 9506 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 9506 (code=exited, status=0/SUCCESS)
       CPU: 4ms

17:52:18 09 دجنبر aziz-virtual-machine systemd[1]: Starting OpenVPN service...
17:52:18 09 دجنبر aziz-virtual-machine systemd[1]: Finished OpenVPN service.
aziz@aziz-virtual-machine:~$

```

6)-Activation de Firewall :

- sudo ufw enable
- sudo ufw status

```

aziz@aziz-virtual-machine: ~
aziz@aziz-virtual-machine:~$ sudo ufw enable
Firewall is active and enabled on system startup
aziz@aziz-virtual-machine:~$ sudo ufw status
Status: active

```

→Ajouter le port 1194 et le protocole upd qu'on a choisi précédemment (voir l'étape 3) dans ufw :

- sudo ufw allow 1194/udp

```

aziz@aziz-virtual-machine:~$ sudo ufw allow 1194/udp
Rule added
Rule added (v6)
aziz@aziz-virtual-machine:~$ sudo ufw status
Status: active

To Action From
--
1194/udp ALLOW Anywhere
1194/udp (v6) ALLOW Anywhere (v6)

```

→Il faut installer net-tools :

- sudo apt install net-tools

```

aymane@aymane-HP-ProBook-645-G1:~$ sudo apt install net-tools
[sudo] Mot de passe de aymane :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
 net-tools
0 mis à jour, 1 nouvellement installés, 0 à enlever et 251 non mis à jour.

```

```

Il est nécessaire de prendre 204 ko dans les archives.
Après cette opération, 819 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools a
md64 1.60+git20181103.0eebece-1ubuntu5 [204 kB]
204 ko réceptionnés en 25s (8,191 o/s)
Sélection du paquet net-tools précédemment désélectionné.
(Lecture de la base de données... 170764 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../net-tools_1.60+git20181103.0eebece-1ubuntu5_am
d64.deb ...
Dépaquetage de net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Paramétrage de net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...

```

→ Pour utiliser la commande :

➤ `sudo netstat -anp | grep openvpn`

```

aymane@aymane-HP-ProBook-645-G1:~$ sudo netstat -anp | grep openvpn
udp        0      0 192.168.43.19:1194    0.0.0.0:*
10080/openvpn
unix 3      [ ]          STREAM     CONNECTED   74920      10080/openvpn
aymane@aymane-HP-ProBook-645-G1:~$

```

- ❖ **net-stat** est une ligne de commande affichant des informations sur la connexion réseau.
- ❖ **anp** : all numeric program.
- ❖ **grep** : afficher le contenu de fichier voulu.

7)-Déplacement de fichier client :

→ Prendre le client (openvpn-client.ovpn) que vous avez créé et mettez-le dans le même dossier où il y a openvpn-install.sh :

➤ `sudo cp openvpn-client.ovpn /home/aziz/`

```

aziz@aziz-virtual-machine:~$
aziz@aziz-virtual-machine:~$ sudo su
root@aziz-virtual-machine:/home/aziz# ls -l
total 60
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Desktop
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Documents
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Downloads
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Music
-rwxrwxr-x 1 aziz aziz 23598 17:05 9  openvpn-install.sh
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Pictures
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Public
drwx----- 3 aziz aziz 4096 16:55 9  snap
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Templates
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Videos

```

```

root@aziz-virtual-machine:/home/aziz# cd /
root@aziz-virtual-machine:/# ls
bin  cdrom  etc  lib  lib64  lost+found  mnt  proc  run  snap  swapfile  tmp  var
boot  dev  home  lib32  libx32  media  opt  root  sbin  srv  sys  usr
root@aziz-virtual-machine:/# cd root
root@aziz-virtual-machine:~# ls -l
total 12
-rw-r--r-- 1 root root 5003 17:41 9  openvpn-client.ovpn
drwx----- 5 root root 4096 16:54 9  snap
root@aziz-virtual-machine:~# cp openvpn-client.ovpn /home/aziz/
root@aziz-virtual-machine:~# exit
exit

```

```

aziz@aziz-virtual-machine: ~
aziz@aziz-virtual-machine:~$ ls -l
total 68
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Desktop
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Documents
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Downloads
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Music
-rw-r--r-- 1 root root 5003 18:00 9  openvpn-client.ovpn
-rwxrwxr-x 1 aziz aziz 23598 17:05 9  openvpn-install.sh
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Pictures
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Public
drwx----- 3 aziz aziz 4096 16:55 9  snap
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Templates
drwxr-xr-x 2 aziz aziz 4096 16:55 9  Videos
aziz@aziz-virtual-machine:~$

```

8)-Installation de network-manager :

➤ `sudo apt install -y network-manager-openvpn`

```

aymane@aymane-HP-ProBook-645-G1:~$ sudo apt install -y network-manager-openvpn
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
network-manager-openvpn est déjà la version la plus récente (1.8.18-1).
network-manager-openvpn passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 251 non mis à jour.
aymane@aymane-HP-ProBook-645-G1:~$
aymane@aymane-HP-ProBook-645-G1:~$
aymane@aymane-HP-ProBook-645-G1:~$

```

9)-la plage de vpn est :

on tape la commande (*ip a* ou bien *ifconfig*)

```

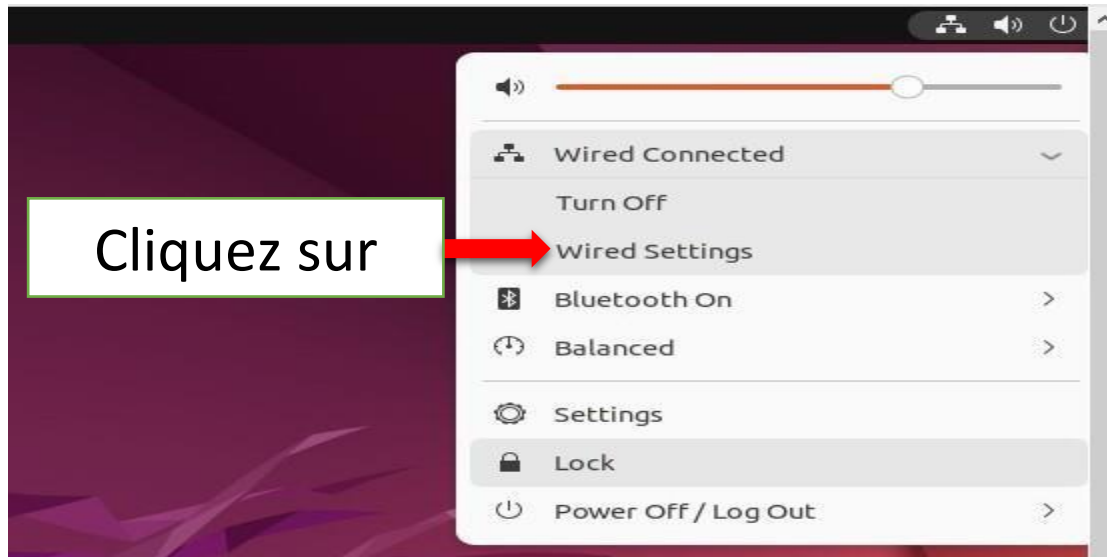
aziz@aziz-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:1b:0c:cc brd ff:ff:ff:ff:ff:ff
    altnamename enp2s1
    inet 192.168.17.128/24 brd 192.168.17.255 scope global dynamic noprefixroute ens33
        valid_lft 1646sec preferred_lft 1646sec
    inet6 fe80::5668:a210:90d5:5fed/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

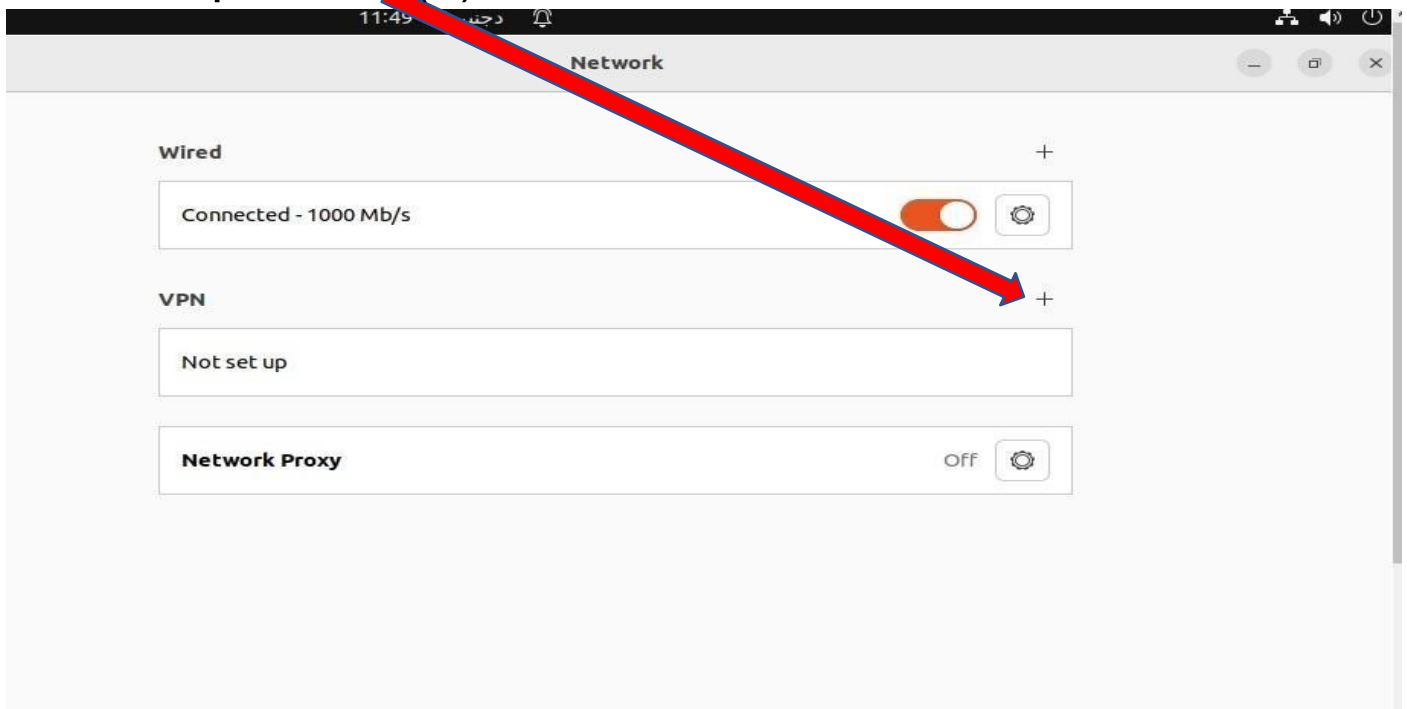
```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 512
link/none
inet 10.8.0.1/24 scope global tun0
    valid_lft forever preferred_lft forever
inet6 fe80::2bda:2feb:c14a:2eb5/64 scope link stable-privacy
    valid_lft forever preferred_lft forever
```

↳ c'est l'interface virtuelle de vpn qui a été créé par défaut lors d'installation d'openvpn.

9) -L'activation de VPN :



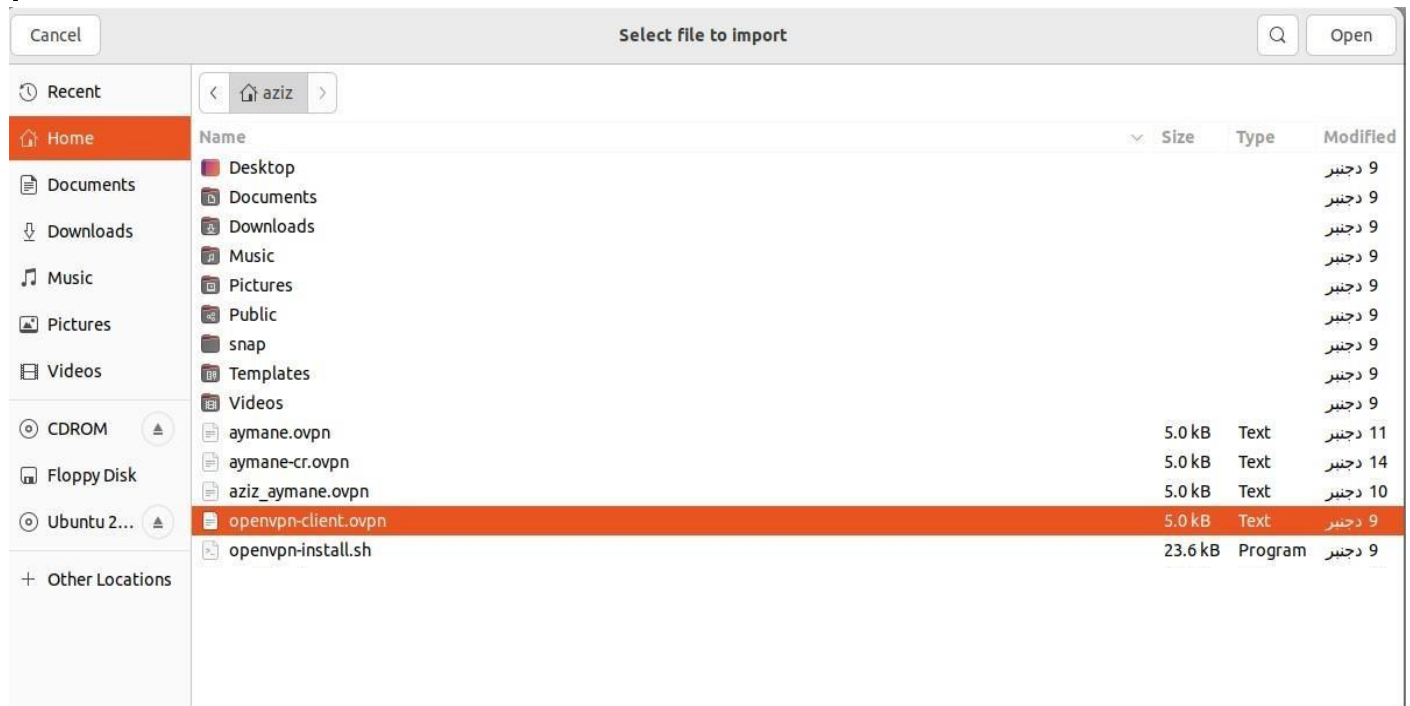
-Puis cliquez sur (+)



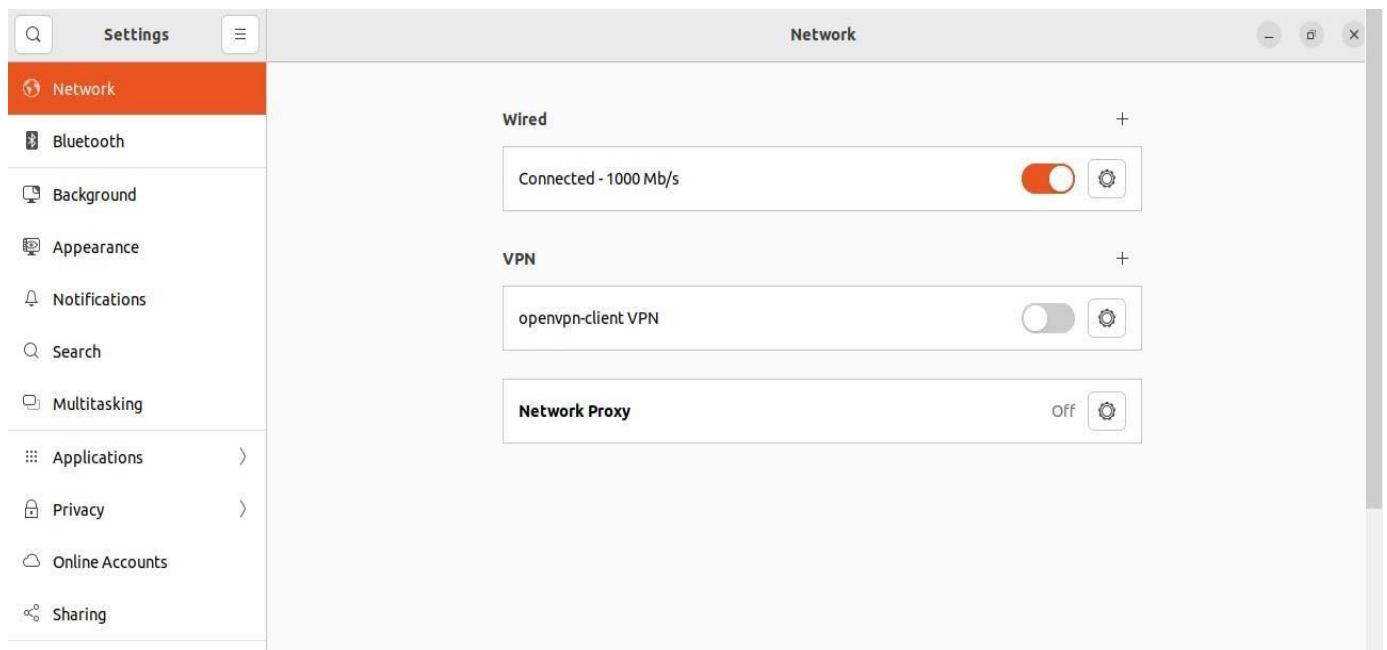
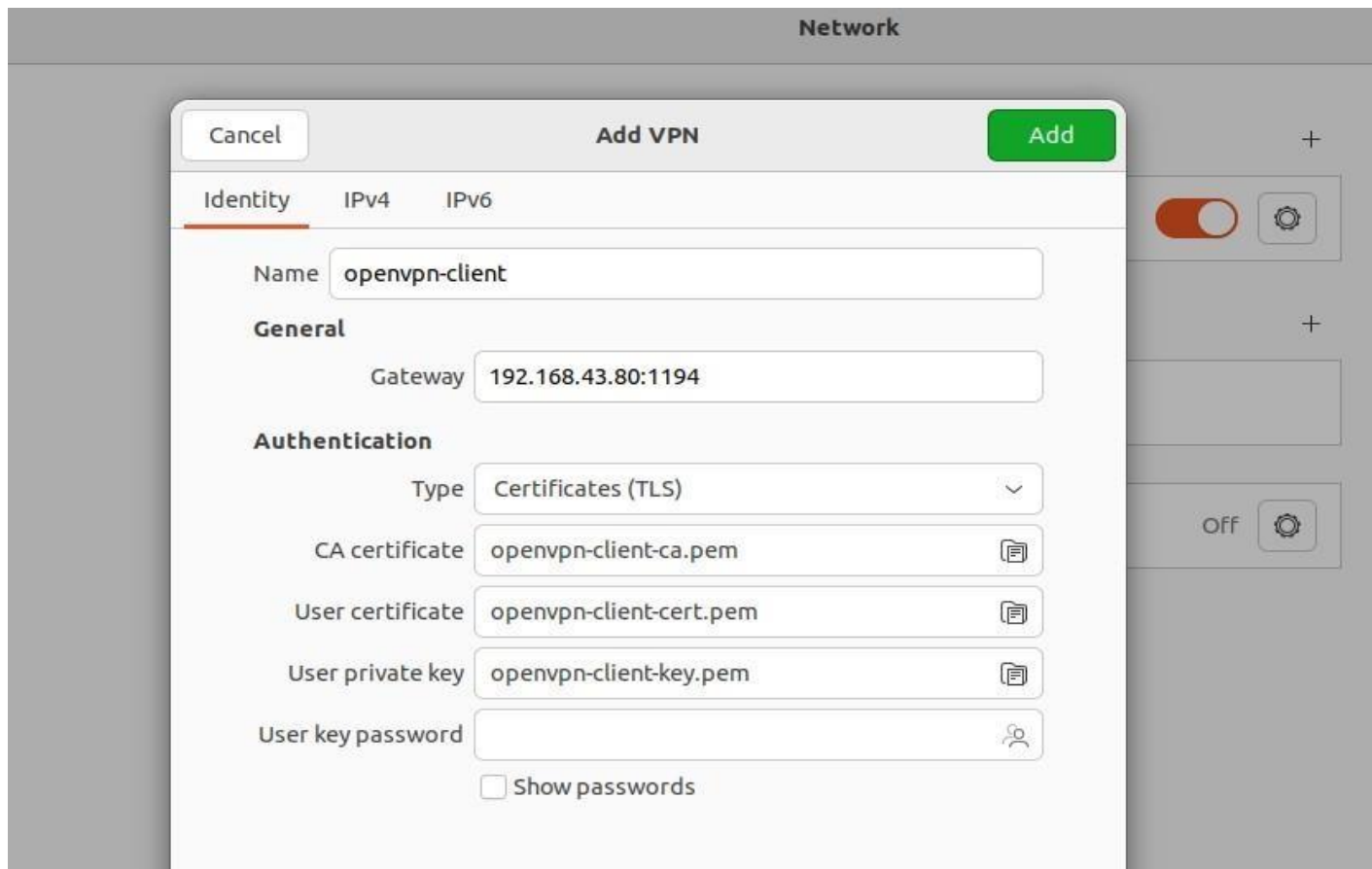
-puis cliquez sur



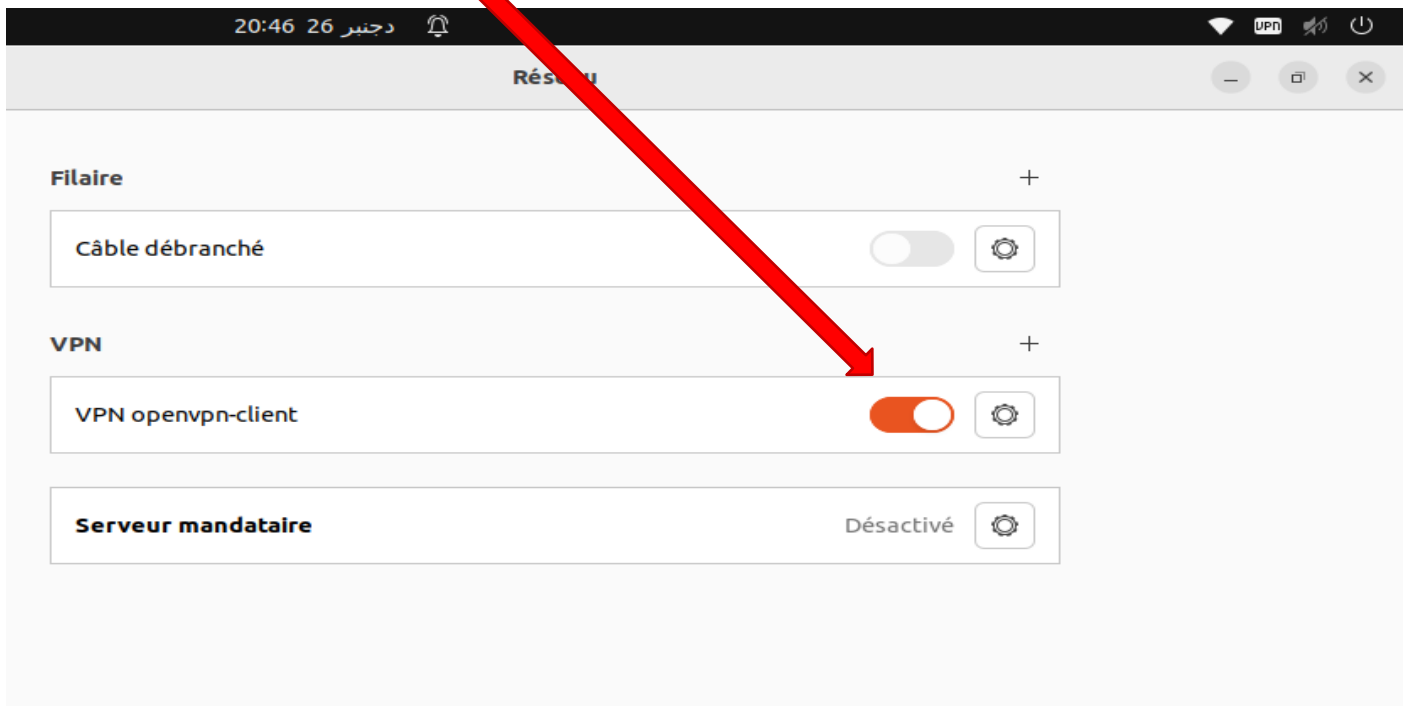
-Et choisissez le client que vous avez créé précédemment :



-Et puis vous cliquez sur ajouter (Add).



Puis activez le VPN

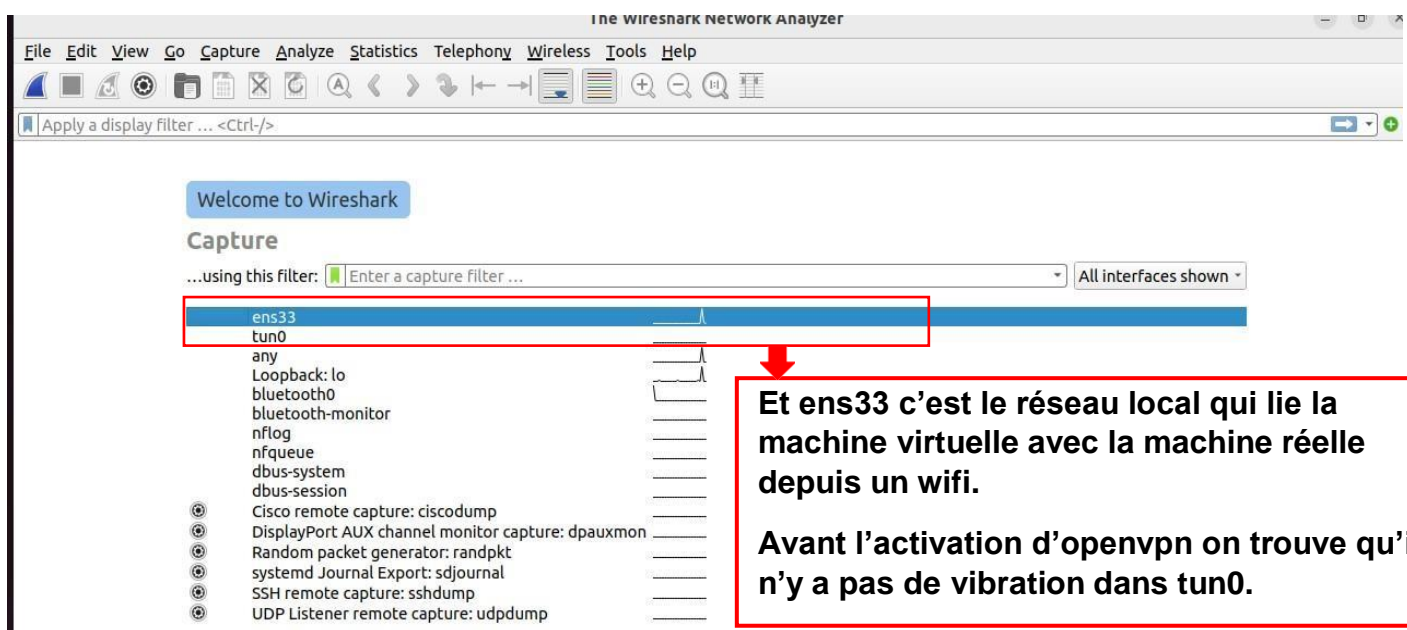


III)-Démonstration par WireShark :

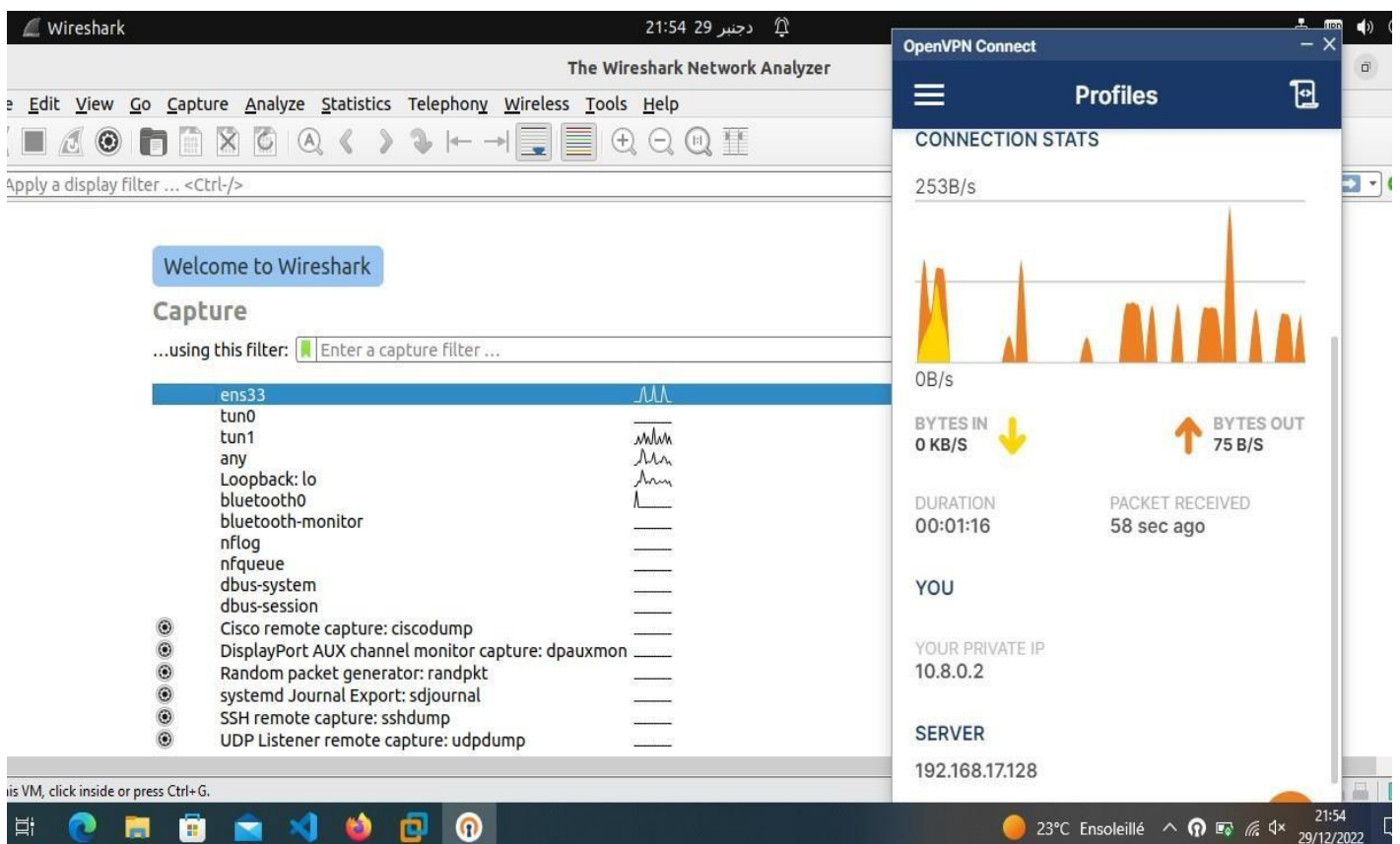
1)-Définition de Wireshark :

Wireshark est un **analyseur de paquets** libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles et l'éducation.

2)-Avant l'activation d'openvpn :



3)-Après l'activation d'openvpn :



-Après nous avons activé le client openvpn sur la machine windows (machine réelle) ; et nous avons fait un ping vers le client depuis notre serveur openvpn dans ubuntu (machine virtuelle), on voit que le tun1 a été ajouter dans notre liste de wireshark et nous voyons qu'il y a une variation sur la vibration de tun client (tun1) et sur eth0 (ens33). Alors on conclue qu'il y a une connexion entre le client el le serveur.

-Et après on accède eth0(ens33) pour voir les échanges des informations (client/server) d'openvpn entre les deux machines comme vous voyez sur le schéma au-dessous :

The screenshot displays two windows. The left window is Wireshark, showing a packet capture on the 'ens33' interface. The packet list shows multiple OpenVPN messages. The packet details pane for frame 623 shows the structure of an OpenVPN packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and OpenVPN Protocol. The packet bytes pane shows the raw data, with a red box highlighting the encrypted payload, which is represented by 'x' characters. The right window is OpenVPN Connect, showing the 'Profiles' section. It displays the connection status, including the duration (00:00:47), bytes in/out (84 B/S), and the IP addresses of the client (10.8.0.2) and the server (192.168.17.128). The VPN protocol is listed as UDPv4.

No.	Source	Destination	Protocol	Length	Info
1412	192.168.17.128	192.168.17.1	OpenVPN	126	MessageType
1415	192.168.17.1	192.168.17.128	OpenVPN	126	MessageType
1416	192.168.17.128	192.168.17.1	OpenVPN	126	MessageType
1420	192.168.17.1	192.168.17.128	OpenVPN	126	MessageType
1421	192.168.17.128	192.168.17.1	OpenVPN	126	MessageType
1441	192.168.17.1	192.168.17.128	OpenVPN	126	MessageType
1442	192.168.17.128	192.168.17.1	OpenVPN	126	MessageType
1447	192.168.17.1	192.168.17.128	OpenVPN	126	MessageType
1448	192.168.17.128	192.168.17.1	OpenVPN	126	MessageType
1451	192.168.17.1	192.168.17.128	OpenVPN	126	MessageType
1452	192.168.17.128	192.168.17.1	OpenVPN	126	MessageType

Frame 623: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface ens33
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_1b:0c:cc (00:0c:29:1b:0c:cc)
Internet Protocol Version 4, Src: 192.168.17.1, Dst: 192.168.17.128
User Datagram Protocol, Src Port: 63422, Dst Port: 1194
OpenVPN Protocol

0000 00 0c 29 1b 0c cc 00 50 56 c0 00 08 08 00 45 00) P V E .
0010 00 78 c6 fc 00 00 80 11 cf a6 c0 a8 11 01 c0 a8 - x
0020 11 80 f7 be 04 aa 00 64 6c e8 48 00 00 01 00 00 d l . H

OpenVPN Connect Profiles

OB/s

BYTES IN 84 B/S

BYTES OUT 84 B/S

DURATION 00:00:47

PACKET RECEIVED 0 sec ago

YOU

YOUR PRIVATE IP 10.8.0.2

SERVER 192.168.17.128

SERVER PUBLIC IP 192.168.17.128

PORT 1194

VPN PROTOCOL UDPv4

La partie des données cryptées

-Pour plus d'information vous pouvez accéder à ces pdf :

- [OpenVPN Access Server System Administrator Guide](#)
- [VPN-Tunneling \(greyc.fr\)](#)