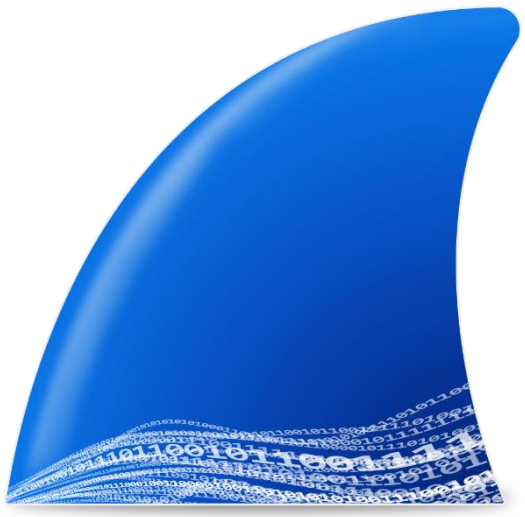
# Installation & Configuration d'un Serveur/Client OpenVPN

M.LEGRAND

# Table des matières

# Introduction :

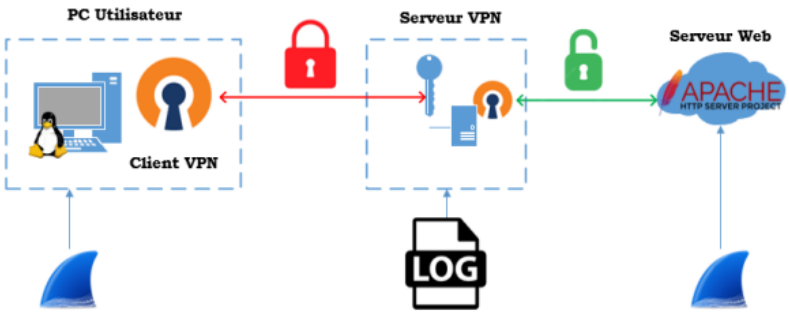
OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel. Son développement a commencé le 13 mai 2001 grâce à James Yonan.

## Qu'est ce qu'est le VPN ?

Un VPN fonctionne en établissant un tunnel chiffré entre le dispositif de l'utilisateur (le client VPN) et un serveur VPN. Ce tunnel sert à encapsuler et à chiffrer les données échangées entre l'utilisateur et le serveur, assurant ainsi leur confidentialité et leur intégrité. Une fois que le client VPN envoie les données au serveur VPN, ce dernier les déchiffre et les transmet au serveur de destination, dans ce cas, un serveur web. De manière symétrique, les données envoyées depuis le serveur web sont reçues par le serveur VPN, qui les chiffre avant de les renvoyer au client VPN. Ce dernier déchiffre les données avant de les traiter. Ce processus garantit que les informations sensibles restent sécurisées même lorsqu'elles traversent des segments de réseau non sécurisés.

## Contexte :

L'objectif de ce TP est de vous familiariser avec les principes de base des VPN, les protocoles de sécurisation comme IPSec et OpenVPN, et les meilleures pratiques pour la configuration et la gestion de la sécurité dans les communications réseau. Cette expérience pratique aidera les étudiants à comprendre comment les VPN contribuent à renforcer la sécurité des données et à maintenir la confidentialité des informations transmises sur Internet.



# Configuration du serveur OpenVPN

## Installation et configuration d'OpenVPN

On va commencer à mettre tous les paquets de Debian à jour et mettre la plus haute version de debian avec les commandes :

```
root@SRVVPN:~# apt update && apt upgrade
```

Ensuite, on va installer le service OpenVPN :

```
root@SRVVPN:~# apt install openvpn
```

```
0 mis à jour, 7 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 2 499 ko dans les archives.
Après cette opération, 7 628 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libccid amd64 1.5.2-1 [367 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 pcscd amd64 1.9.9-2 [89,7 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 easy-rsa all 3.1.0-1 [54,8 kB]
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 libpkcs11-helper1 amd64 1.29.0-1 [51,2 kB]
Réception de :5 http://deb.debian.org/debian bookworm/main amd64 opensc-pkcs11 amd64 0.23.0-0.3+deb12u1 [914 kB]
Réception de :6 http://deb.debian.org/debian bookworm/main amd64 opensc amd64 0.23.0-0.3+deb12u1 [371 kB]
Réception de :7 http://deb.debian.org/debian bookworm/main amd64 openvpn amd64 2.6.3-1+deb12u2 [651 kB]
2 499 ko réceptionnés en 0s (9 300 ko/s)
Préconfiguration des paquets...
Sélection du paquet libccid précédemment désélectionné.
(Lecture de la base de données... 174267 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../0-libccid_1.5.2-1_amd64.deb ...
Dépaquetage de libccid (1.5.2-1) ...
Sélection du paquet pcscd précédemment désélectionné.
Préparation du dépaquetage de .../1-pcscd_1.9.9-2_amd64.deb ...
Dépaquetage de pcscd (1.9.9-2) ...
Sélection du paquet easy-rsa précédemment désélectionné.
Préparation du dépaquetage de .../2-easy-rsa_3.1.0-1_all.deb ...
Dépaquetage de easy-rsa (3.1.0-1) ...
Sélection du paquet libpkcs11-helper1:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../3-libpkcs11-helper1_1.29.0-1_amd64.deb ...
Dépaquetage de libpkcs11-helper1:amd64 (1.29.0-1) ...
Sélection du paquet opensc-pkcs11:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../4-opensc-pkcs11_0.23.0-0.3+deb12u1_amd64.deb ...
Dépaquetage de opensc-pkcs11:amd64 (0.23.0-0.3+deb12u1) ...
Sélection du paquet opensc précédemment désélectionné.
Préparation du dépaquetage de .../5-opensc_0.23.0-0.3+deb12u1_amd64.deb ...
Dépaquetage de opensc (0.23.0-0.3+deb12u1) ...
Sélection du paquet openvpn précédemment désélectionné.
Préparation du dépaquetage de .../6-openvpn_2.6.3-1+deb12u2_amd64.deb ...
Dépaquetage de openvpn (2.6.3-1+deb12u2) ...
Paramétrage de libccid (1.5.2-1) ...
Paramétrage de pcscd (1.9.9-2) ...
Progression : [ 59%] [#########################################################################################.....................................................................]
```

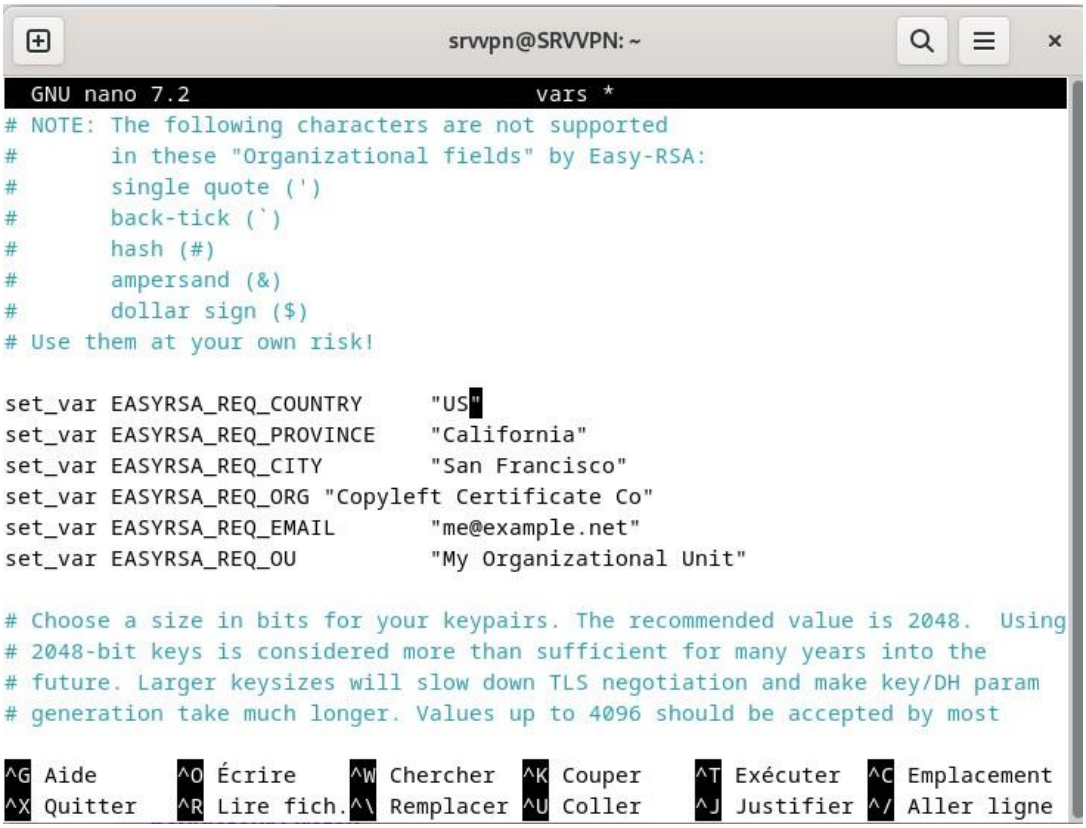
On va copier le répertoire easy-rsa qui permet de générer les certificats :

```
root@SRVVPN:~# cp -pr /usr/share/easy-rsa /etc/openvpn/server/ && cd /etc/openvpn/server/easy-rsa
```

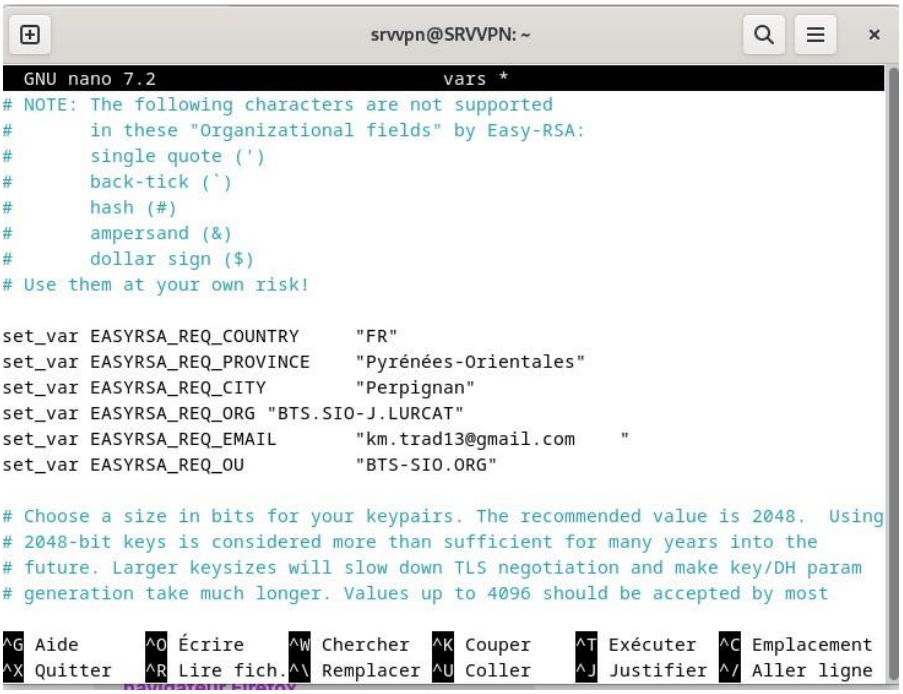
On va renommer et éditer le fichier vars :

```
root@SRVVPN:~# cp vars.example vars && nano vars
```

On va rechercher cette partie dans le fichier « vars » :




Puis on décommente et modifie selon nos informations :



On va maintenant crée l'autorité de certification :

```
root@SRVVPN: ~# ./easyrsa init-pki
```

```
root@SRVVPN: ~# ./easyrsa build-ca
```

```
* Notice:
Using Easy-RSA configuration from: /etc/openvpn/server/easy-rsa/vars

* WARNING:

  Move your vars file to your PKI folder, where it is safe!

* Notice:
Using SSL: openssl OpenSSL 3.0.11 19 Sep 2023 (Library: OpenSSL 3.0.11 19 Sep 2023)

Using configuration from /etc/openvpn/server/easy-rsa/pki/49d4f726/temp.5cd822a9
.....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.........+.+.........+.+......+...+..+...+..........+..+.+.....+...++++++++++++++++++++++++++++++++++++
++++++++++++*.....+....+.........+...+.........+................+......+...+.+..+...+.....+..........+.........+..+...+....+..+....++++++++++++++++++++++++++++++++++++++++++++
++++++
........+.....+...+......+.+......+...+..+....+...+...+.....+...+................+....+..+...+.......+...+......+..+..........++++++++++++++++++++++++++++++++++++++++++++
+*....+.....+.......+...+..+......+......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.......+...+......+......+....+...........+......+..............
.......................+.....+......+....+...+.........+......+.+..+.+..+...+.+................+...+................+..+......+....+.........+......+......+..+......+.+........
..+..+...+.................+.....+.+.....+...+.........+.+......+.........+..+...+.+.........+.........+......+.........................+...++++++++++++++++++++++++++++++++
++++++++++++++
-----
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.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:FR

* Notice:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/server/easy-rsa/pki/ca.crt
```

**Common Name : Mettre FR ou laisser par défaut**

On génère désormais le certificat du serveur :

```
root@SRVVPN:~#./easyrsa build-server-full server
```

Puis le certificat du client :

```
root@SRVVPN:~#./easyrsa build-client-full client
```

Ensuite, générer le fichier dh.pem :

*Ce fichier va être utilisé pour la première connexion en chiffrement symétrique.*

```
root@SRVVPN:~#./easyrsa gen-dh
```

*Tout dépend de votre machine mais, l'opération peut-être plus au moins de temps.*

On génère le fichier clé :

```
root@SRVVPN:~# openvpn –genkey tls-auth ta.key
```

On renomme le fichier dh.pem :

```
root@SRVVPN:~# mv /etc/openvpn/dh.pem /etc/openvpn/dh2048.pem
```

## Test de la configuration

On tape : `root@SRVVPN:~# systemctl status openvpn.service`

```
root@SRVVPN:~# systemctl status openvpn.service
● openvpn.service - OpenVPN service
     Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; preset: enabled)
     Active: active (exited) since Tue 2024-05-14 19:08:28 CEST; 1h 50min ago
    Process: 919 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 919 (code=exited, status=0/SUCCESS)
        CPU: 2ms

mai 14 19:08:28 SRVVPN systemd[1]: Starting openvpn.service - OpenVPN service...
mai 14 19:08:28 SRVVPN systemd[1]: Finished openvpn.service - OpenVPN service.
root@SRVVPN:~#
```

On redémarre openvpn :

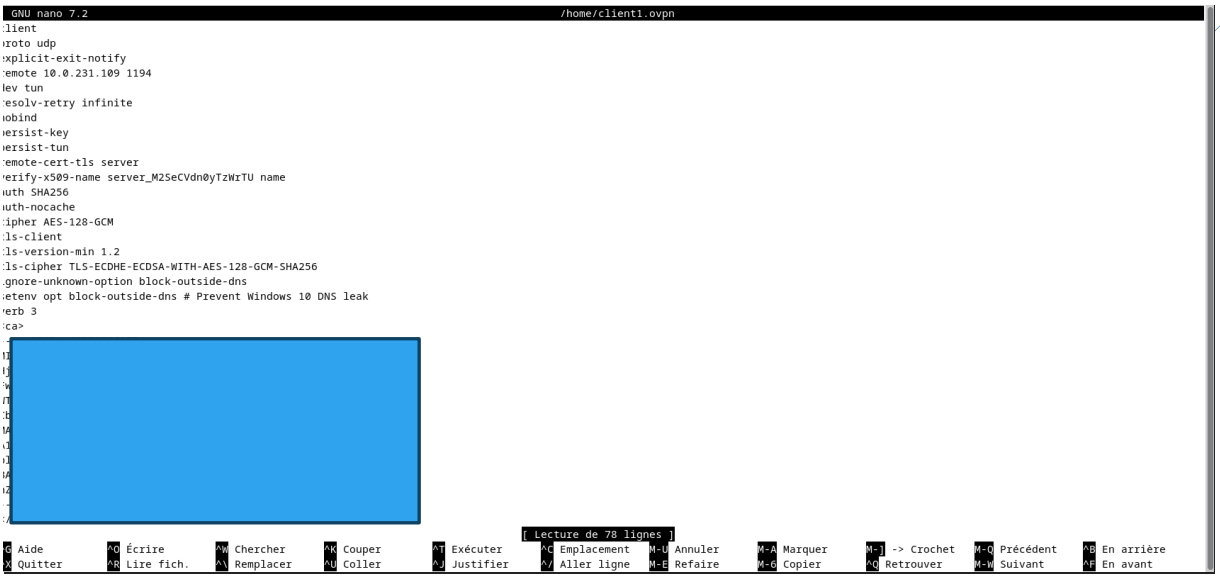
```
root@SRVVPN:~# systemctl restart openvpn.service
```

On va copier le dossier client1.ovpn :

```
root@SRVVPN:~# cp client1.ovpn /home
```

Puis :

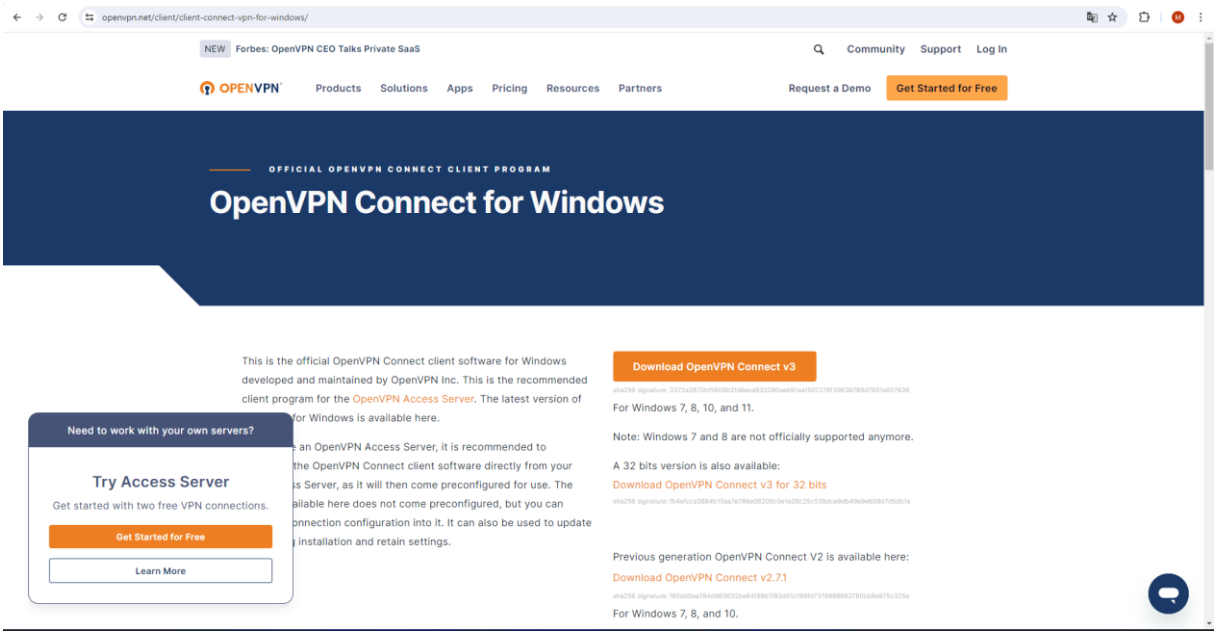
```
root@SRVVPN:~# nano /home/client1.ovpn
```



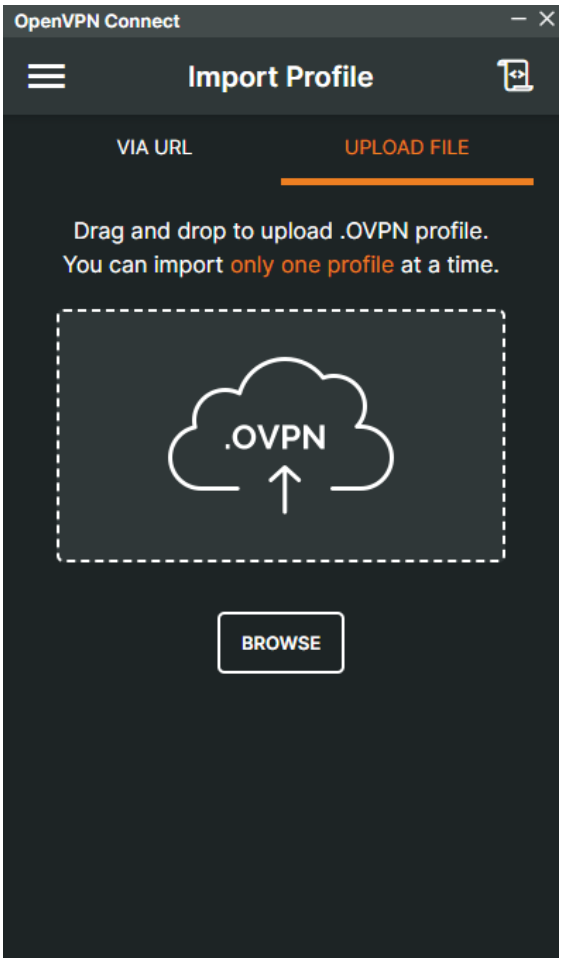

On copie l’entité du fichier et on le collera plus tard.

# Installation OpenVpn sur client Windows :

Ouvrir Edge et taper https://openvpn.net/client/client-connect-vpn-for-windows/ :

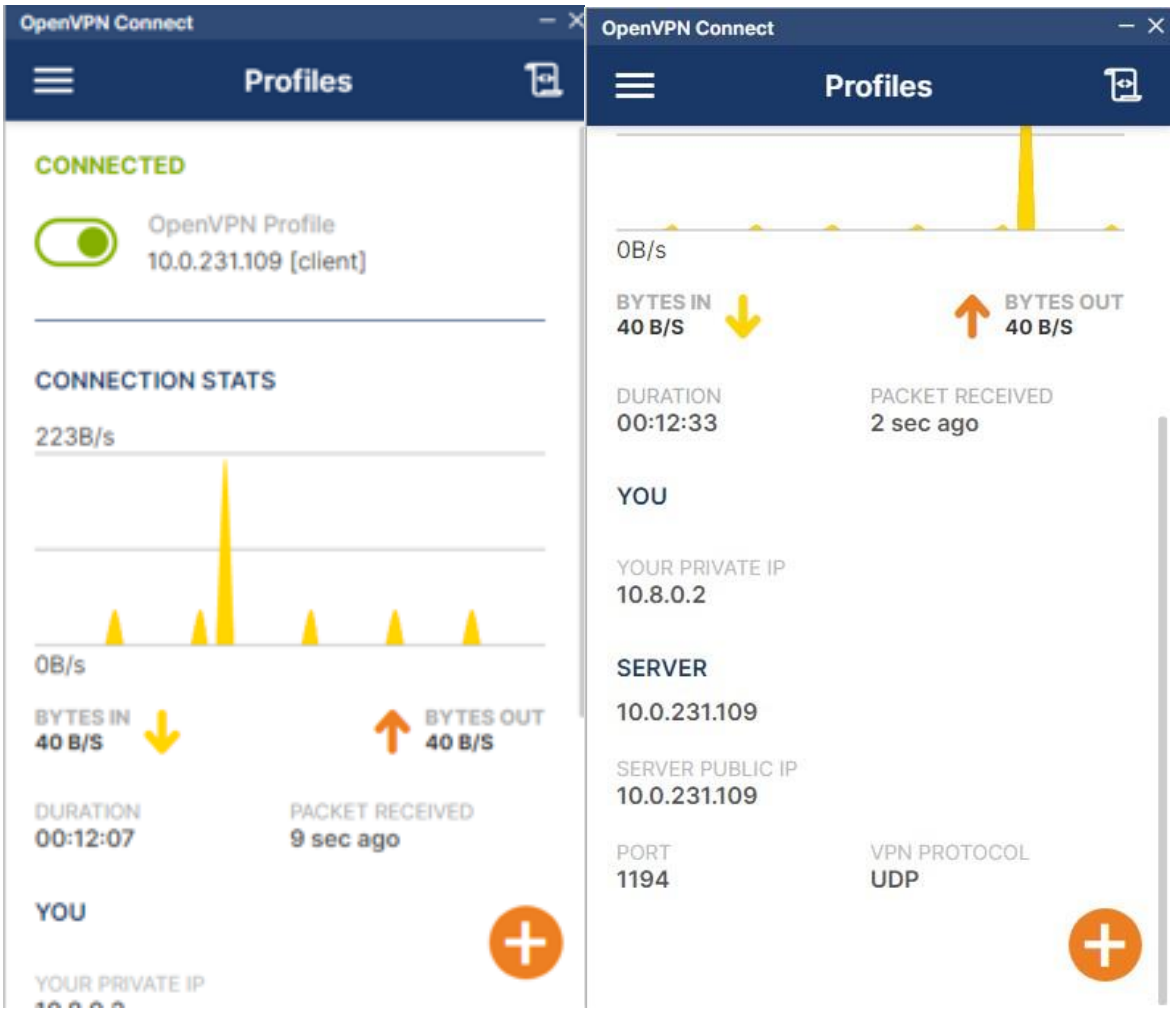


Ouvrer OpenVPN :




On va créer le fichier client1.ovpn dans bloc-notes et on colle ce qu'on a copié précédemment sur le serveur, enregistrer sous le fichier en « nomdufichier.ovpn » puis glisser le dans « upload file »

Et vous voilà connecter ! :



# Configuration du serveur Web Apache

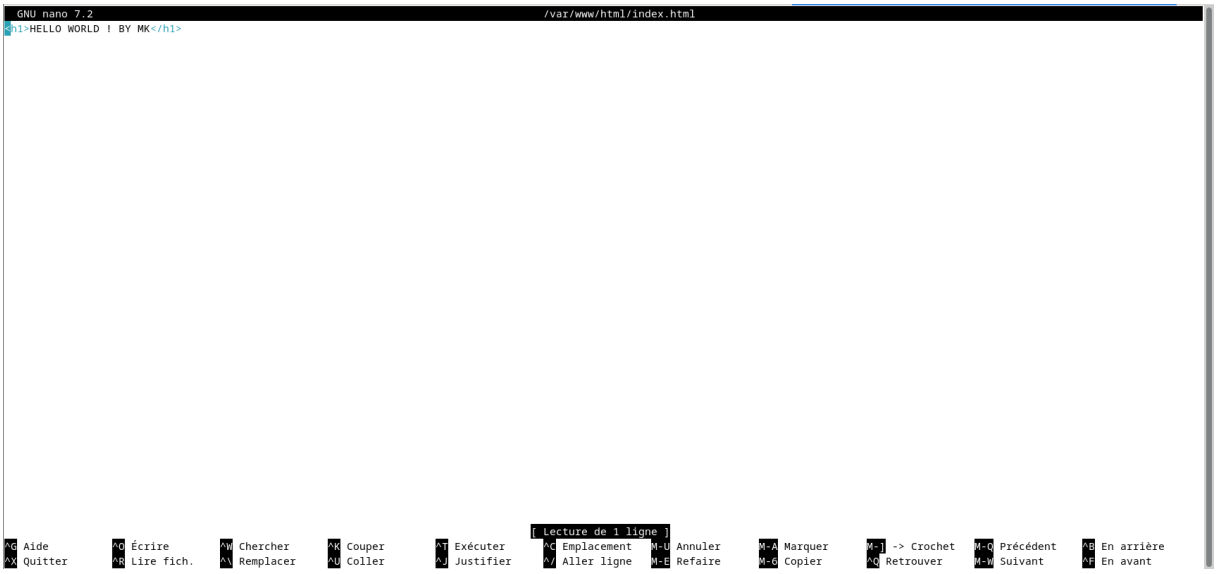
Pour installer apache :

```
root@SRVWEB : ~# apt install apache2
```

Pour activer la sécurisation https/tls d'apache :

```
root@SRVWEB : ~# a2enmod ssl && a2ensite
```

Puis modifier le fichier « index.html » situer dans /var/www/html :

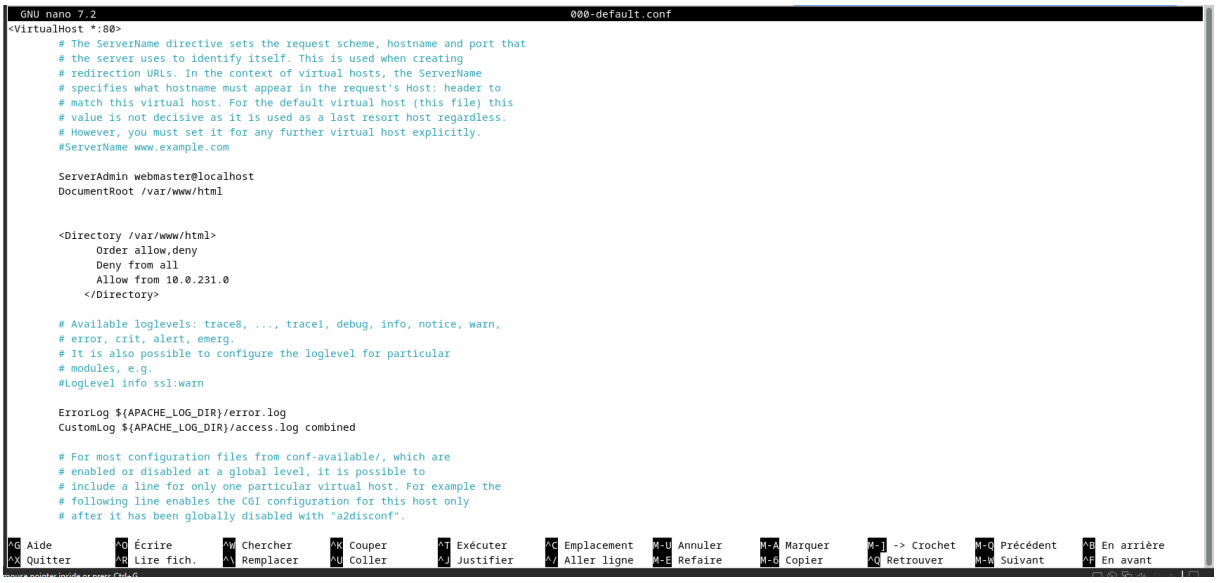


Pour les restrictions d'accès par adresse IP :

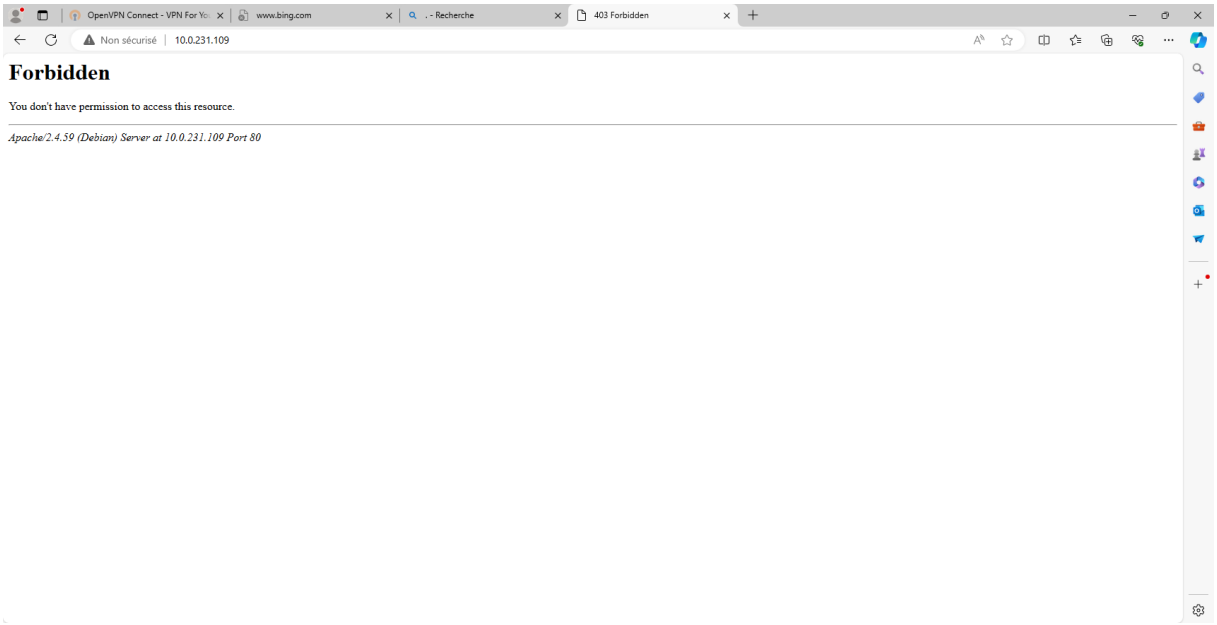
```
root@SRVWEB:~#nano /etc/apache2/sites-available/000-default.conf
```

**Insérer cela :**

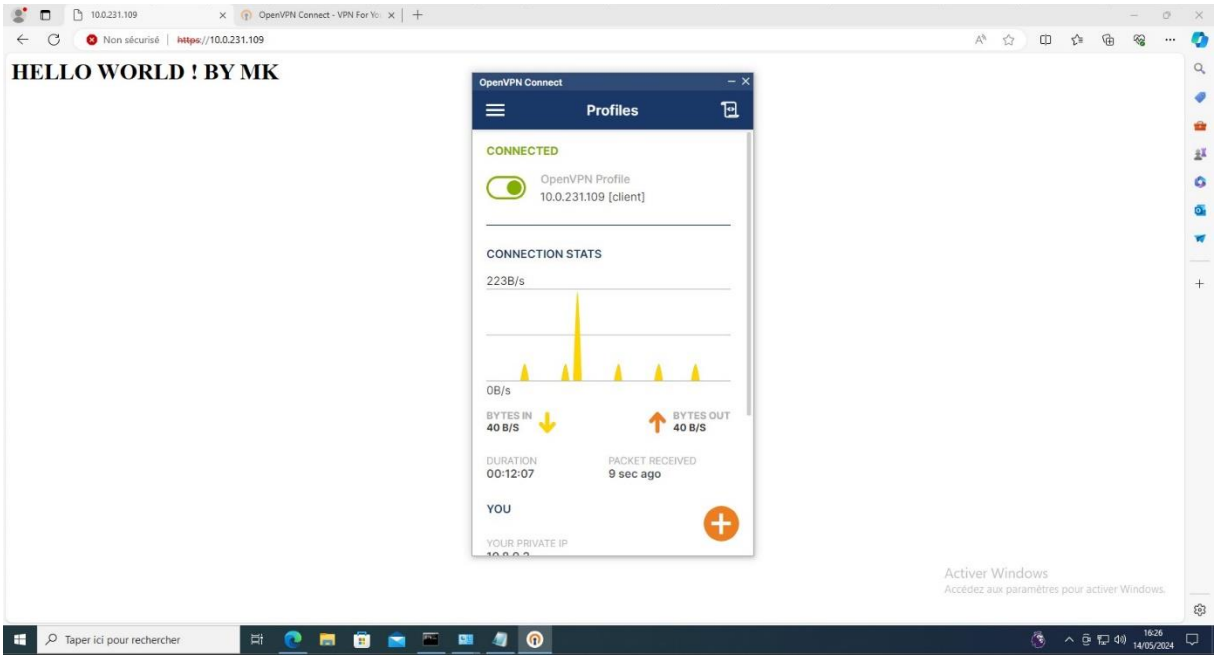
```
<Directory /var/www/html>
        Order allow,deny
        Deny from all
        Allow from 10.0.231.109
    </Directory>
```

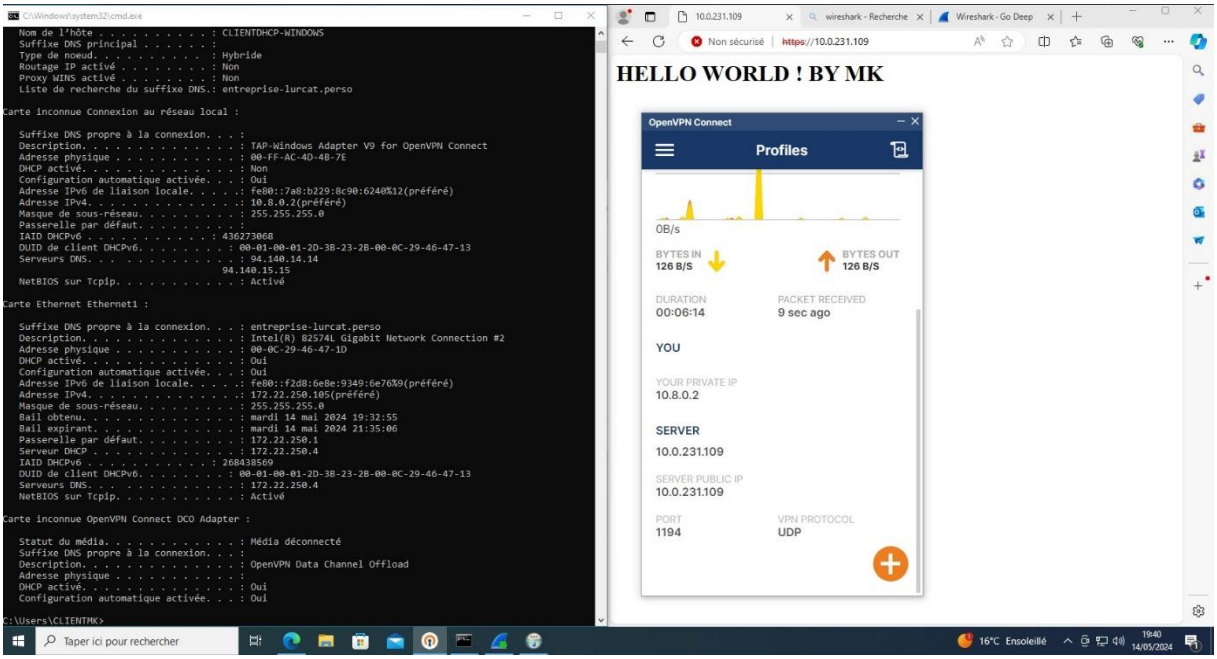



Ce qui nous donnera ceci :



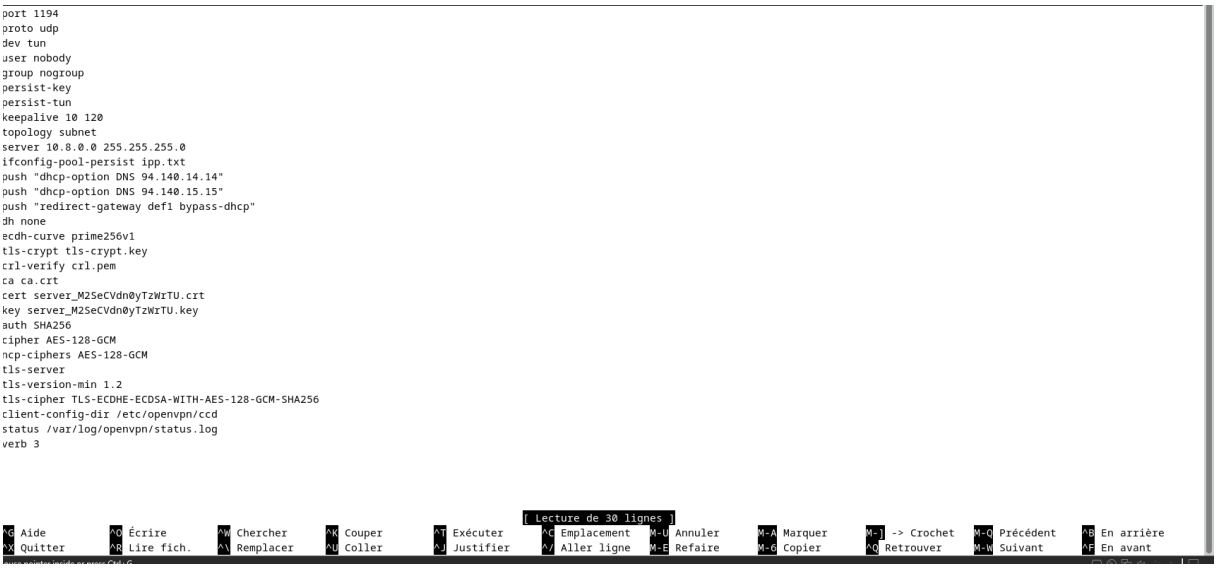
Désormais on a accès que par https depuis les clients VPN :



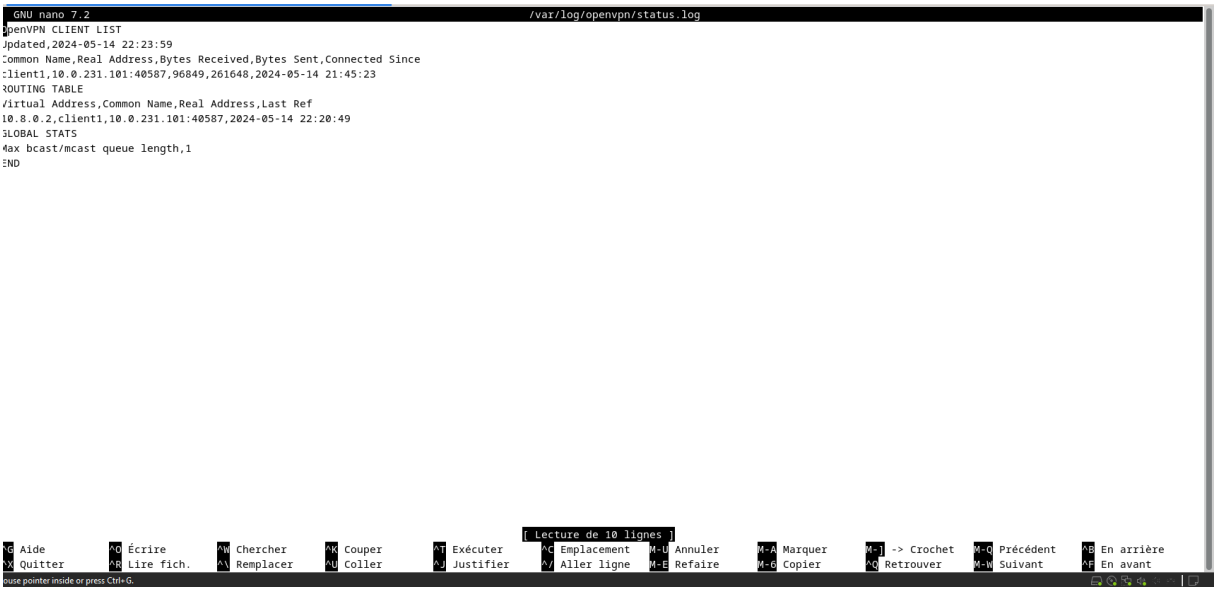



# Collecte et analyse des Logs sur le serveur OpenVPN :

Accès au fichier « server.conf » qui correspond aux meilleures pratiques de sécurité et aux exigences du système.




## Accès aux fichiers de log OpenVPN :



Status OpenVpn.Service :

```
:oot@SRVVPN:/var/log/openvpn# systemctl status openvpn.service
• openvpn.service - OpenVPN service
     Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; preset: enabled)
     Active: active (exited) since Tue 2024-05-14 21:01:11 CEST; 1h 24min ago
    Process: 4372 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 4372 (code=exited, status=0/SUCCESS)
        CPU: 2ms

ıai 14 21:01:10 SRVVPN systemd[1]: Stopping openvpn.service - OpenVPN service...
ıai 14 21:01:11 SRVVPN systemd[1]: Starting openvpn.service - OpenVPN service...
ıai 14 21:01:11 SRVVPN systemd[1]: Finished openvpn.service - OpenVPN service.
```

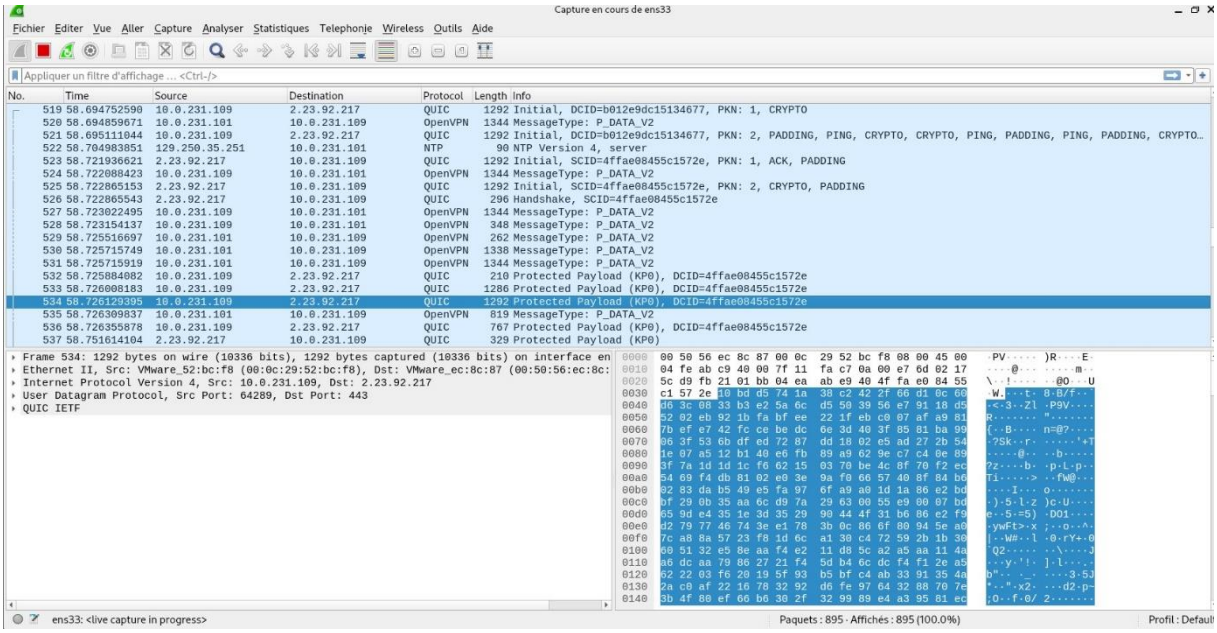
Pour voir le journal d'openvpn (Utile en cas d'erreur !) :

```
root@SRVVPN:~#journalctl -xeu openvpn.service
```

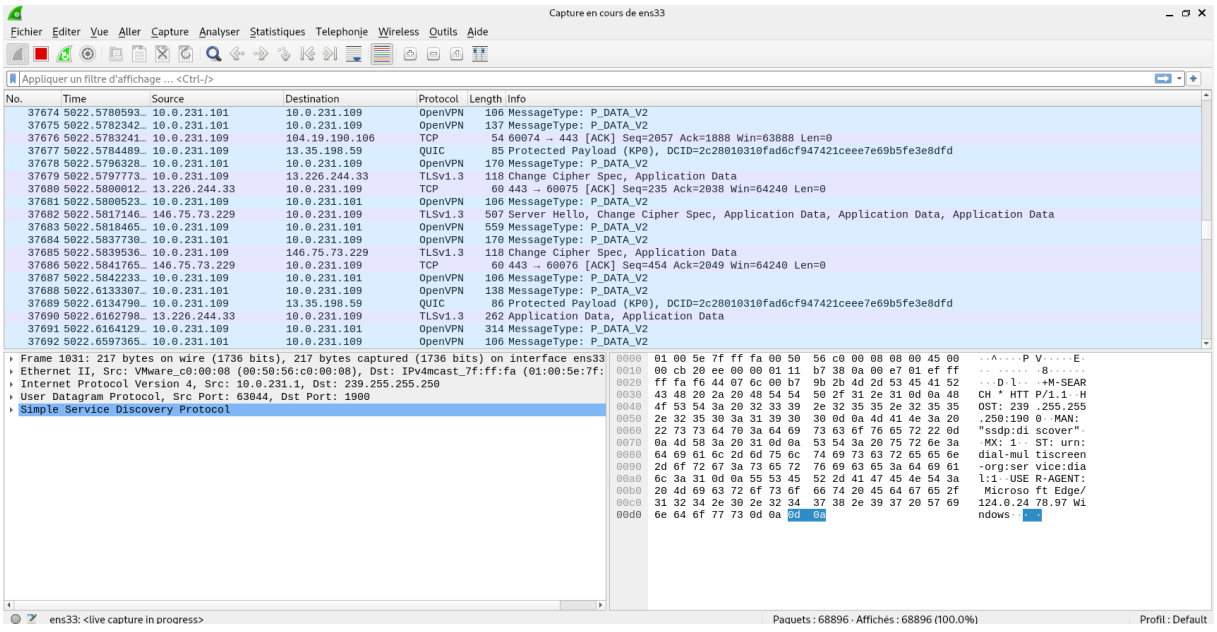
```
 L'unité (unit) openvpn.service a commencé à démarrer.
ai 14 19:08:28 SRVVPN systemd[1]: Finished openvpn.service - OpenVPN service.
 Subject: L'unité (unit) openvpn.service a terminé son démarrage
 Defined-By: systemd
 Support: https://www.debian.org/support

 L'unité (unit) openvpn.service a terminé son démarrage, avec le résultat done.
ai 14 21:01:10 SRVVPN systemd[1]: openvpn.service: Deactivated successfully.
 Subject: Unit succeeded
 Defined-By: systemd
 Support: https://www.debian.org/support

 The unit openvpn.service has successfully entered the 'dead' state.
ai 14 21:01:10 SRVVPN systemd[1]: Stopped openvpn.service - OpenVPN service.
 Subject: L'unité (unit) openvpn.service a terminé son arrêt
 Defined-By: systemd
 Support: https://www.debian.org/support

 L'unité (unit) openvpn.service a terminé son arrêt.
ai 14 21:01:10 SRVVPN systemd[1]: Stopping openvpn.service - OpenVPN service...
 Subject: L'unité (unit) openvpn.service a commencé à s'arrêter
 Defined-By: systemd
 Support: https://www.debian.org/support

 L'unité (unit) openvpn.service a commencé à s'arrêter.
ai 14 21:01:11 SRVVPN systemd[1]: Starting openvpn.service - OpenVPN service...
 Subject: L'unité (unit) openvpn.service a commencé à démarrer
 Defined-By: systemd
 Support: https://www.debian.org/support

 L'unité (unit) openvpn.service a commencé à démarrer.
ai 14 21:01:11 SRVVPN systemd[1]: Finished openvpn.service - OpenVPN service.
 Subject: L'unité (unit) openvpn.service a terminé son démarrage
 Defined-By: systemd
 Support: https://www.debian.org/support

 L'unité (unit) openvpn.service a terminé son démarrage, avec le résultat done.
```

WireShark :

Depuis client Windows :




Depuis Serveur :



## Conclusion :

J'en tire de ce TP qui est très intéressant pour une entreprise d'adopter la technologie VPN, il sécurise les échanges envers les différents services. Grâce au chiffrement, personne ne peut avoir accès aux informations qui sont envoyées sur Internet.  C'est un gage de sécurité qui permet d'éviter, par exemple, des attaques par déni de service sur le réseau de l'entreprise. De plus, le VPN permet de chiffrer la connexion internet des collaborateurs, ce qui permet de se protéger contre l'attaque de l'homme au milieu. Cette attaque est très fréquente lorsque l'on se connecte depuis des réseaux publics, il est donc indispensable pour vous et vos collaborateurs d'utiliser un VPN lors de déplacements.

## Annexe :

| Port Number | Protocol |
|---|---|
| 20, 21 | File Transfer Protocol (FTP) |
| 22 | Secure Shell (SSH) |
| 23 | Telnet Protocol |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 53 | Domain Name System (DNS) |
| 67, 68 | Dynamic Host Configuration Protocol (DHCP) |
| 80 | HyperText Transfer Protocol (HTTP) |
| 110 | Post Office Protocol (POP3) |
| 137 | NetBIOS Name Service |
| 143 | Internet Message Access Protocol (IMAP4) |
| 443 | Secure HTTP (HTTPS) |
| 445 | Microsoft-DS (Active Directory) |

| | |
|---|---|
| 7000 | fileserver |
| 7001 | Cache Manager callback service |
| 7002 | ptserver |
| 7003 | vlserver (VLDB) |
| 7004 | kaserver |
| 7005 | volserver (volume management) |
| 7007 | bosserver |
| 7008 | upserver |
| 7009 | AFS/NFS Translator |
| 7020 | AFS backup coordinator |
| 7021 | AFS backup buserver |
| 7025-7032 | AFS backup tape controllers |
| 7101 | xstat |
| 2106 | fs monitor port |
| next available port | pts, kas, fs, klog, etc. |