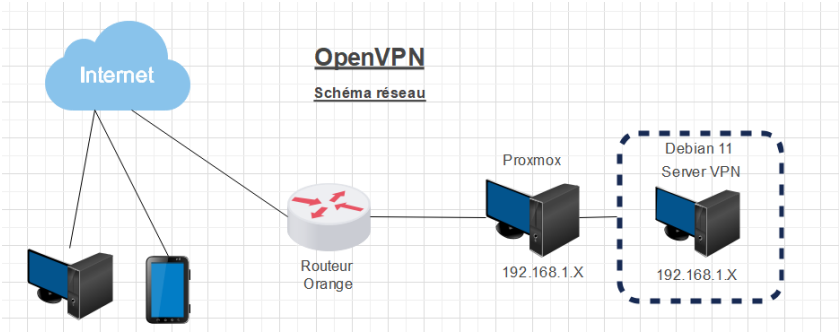
Configuration d'un VPN avec OpenVPN

Cette fiche de procédure contient les étapes essentiel pour la configuration d'un serveur VPN à travers Internet (cas concret)

Schéma réseau :



Dans mon cas mon serveur VPN se situe sur mon serveur Proxmox comme machine virtuelle.

Installation de OpenVPN & Configuration coté serveur :

Suivre ces étape en tant que **root**

```
apt install openvpn
```

Copier le fichier des outils fournis avec OpenVPN pour la création de clés

```
cp -r /usr/share/easy-rsa  /etc/openvpn
```

Copier et modifier le fichier vars afin de modifier les valeurs par défaut pour la génération des certificats

```
cp vars.example vars && nano vars
```

Dans ce fichier modifier les champs suivant en les décommentant

```
set_var EASYRSA_REQ_COUNTRY    "XX"
set_var EASYRSA_REQ_PROVINCE   "XX"
set_var EASYRSA_REQ_CITY       "XX"
set_var EASYRSA_REQ_ORG "XX"
set_var EASYRSA_REQ_EMAIL      "XX"
set_var EASYRSA_REQ_OU         "XX"
```

Mise en place de l'infrastructure du dossier pour les clés et certificats

Pour créer le dossier pour les clés & certificats

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

Génération du certificat du CA

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

Génération du certification du server vpn (signé par CA)

```
./easyrsa build-server-full serveur-xx nopass
```

Génération du certificat et clé privée du client (**avec un mot de passe**)

```
./easyrsa build-client-full (nom client)
```

Génération de la clé de chiffrement par Diffie-Hellman

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

Génération de la clé de chiffrement TLS

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

Configuration du fichier « server.conf » OpenVPN

Le fichier de configuration se trouve dans les exemples fournis

```
cp /usr/share/doc/openvpn/examples/samples-config-files/server.conf  /etc/openvpn/
```

Puis modifier le fichier server.conf

```
port 1194
proto udp
dev tun
ca /etc/openvpn/easy-rsa/pki/ca.crt
cert /etc/openvpn/easy-rsa/pki/issued/serv-vpn.crt
key /etc/openvpn/easy-rsa/pki/private/serv-vpn.key  # this file should be kept secret
dh /etc/openvpn/easy-rsa/pki/dh.pem
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt
push "route 192.168.X .X 255.255.255.0" # création d'une route vers le LAN sur le client
keepalive  10 120                # ping pour tester la connexion toutes les 10 sc, TTL 120
tls-crypt /etc/openvpn/easy-rsa/private/ta.key
cipher  AES-256-GCM
user nobody
group nogroup
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log         /var/log/openvpn/openvpn.log
verb 3
```

Activation du service OpenVPN

Pour lancer le service OpenVPN

```
systemctl enable openvpn@server.service  && systemctl start openvpn@server.service
```

La partie serveur est maintenant configuré.

Configuration des règles

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o ensX -j MASQUERADE
```

Configuration du routage des paquets IP

```
nano /etc/sysctl.conf
net.ipv4.ip_forward=1
sysctl -p
```

Activation d'une route sur le port 1194

Depuis ma box orange je vais renseigner sur le Nat/Pat mon server VPN

Activer	Application/Service	Port interne	Port externe	Protocole	Équipement	IP externe	
☑	Secure Web Server (HTTPS)	443	443	TCP	rerverse-proxy	Toutes	🗑
☑	Web Server (HTTP)	80	80	TCP	[redacted]	Toutes	🗑
☑	FTP Server	25565	25565	TCP		Toutes	🗑
☑	vpn	1194	1194	TCP/UDP	OpenVPN	Toutes	🗑

Ainsi de bien mettre l'adresse IPv4 en mode statique

Équipement	Adresse IP statique	Adresse MAC	
PC-336	[redacted]		🗑
rerverse-proxy			🗑
Équipement			🗑
portfolio			🗑
Équipement			🗑
Équipement			🗑
Équipement			🗑
OpenVPN	[redacted]	[redacted]	🗑

Configuration du client

Pour le client j'installe openvpn sur mon windows

https://openvpn.net/downloads/openvpn-connect-v3-windows.msi

Puis aller dans le répertoire suivant

C:\Program Files\OpenVPN\sample-config

Le fichier à modifier sera « client.ovpn »

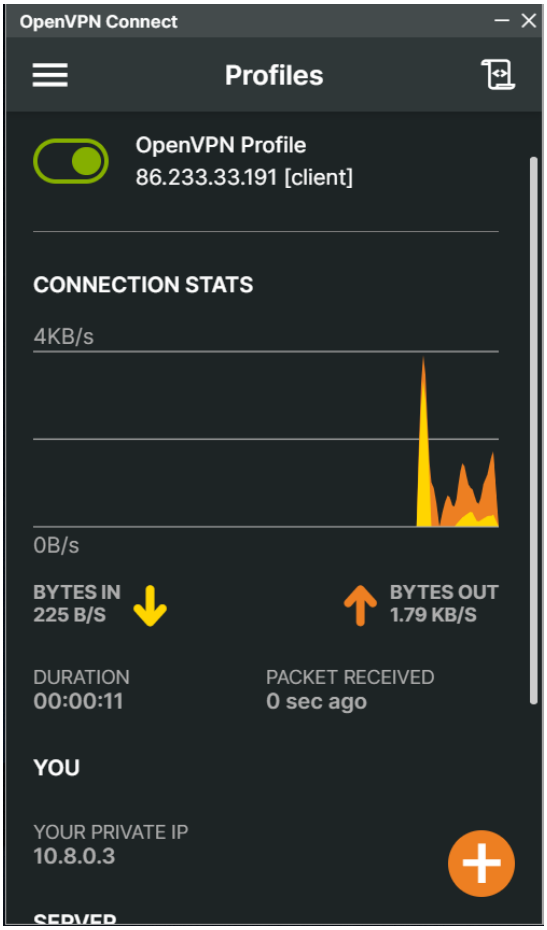
```
client
dev tun
proto udp
remote XX .XX.XX.XX 1194
resolv-retry infinite
nobind
persist-key
persist-tun
mute-replay-warnings
<ca>
## Mettre la clé CA##
</ca>
<cert>
##Mettre la clé publique du client##
</cert>
<key>
##Mettre la clé privée du client ##
</key>
<tls-crypt>
##Mettre la clé privée de chiffrement tls ##
</tls-crypt>
cipher AES-256-GCM
verb 3
```

Lancement du VPN entre client et serveur

Sur le serveur pour visualiser la connexion entre le client et le serveur tapez sur le serveur

```
tail -f /var/log/openvpn/openvpn.log
```

Une fois lancé exéctuer OpenVPN en tant que « Administrateur » et faire un clic droit sur « client.ovpn » et cliqué sur start OpenVPN :



Sur le serveur

```
root@OpenVPN:~# tail -f /var/log/openvpn/openvpn.log
2023-04-01 21:45:14 86.233.33.191:53394 peer info: IV_COMP_STUBv2=1
2023-04-01 21:45:14 86.233.33.191:53394 peer info: IV_TCPNL=1
2023-04-01 21:45:14 86.233.33.191:53394 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2023-04-01 21:45:14 86.233.33.191:53394 [emrys] Peer Connection Initiated with [AF_INET]86.233.33.191:53394
2023-04-01 21:45:14 emrys/86.233.33.191:53394 MULTI_sva: pool returned IPv4=10.8.0.2, IPv6=(Not enabled)
2023-04-01 21:45:14 emrys/86.233.33.191:53394 MULTI: Learn: 10.8.0.2 → emrys/86.233.33.191:53394
2023-04-01 21:45:14 emrys/86.233.33.191:53394 MULTI: primary virtual IP for emrys/86.233.33.191:53394: 10.8.0.2
2023-04-01 21:45:14 emrys/86.233.33.191:53394 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2023-04-01 21:45:14 emrys/86.233.33.191:53394 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2023-04-01 21:45:14 emrys/86.233.33.191:53394 SENT CONTROL [emrys]: 'PUSH_REPLY,route 192.168.1.1 255.255.255.0,route-
gateway 10.8.0.1,topology subnet,ping 10,ping-restart 120,ifconfig 10.8.0.2 255.255.255.0,peer-id 0,cipher AES-256-GCM
' (status=1)
```

La connexion est bien établie entre le client et le serveur.