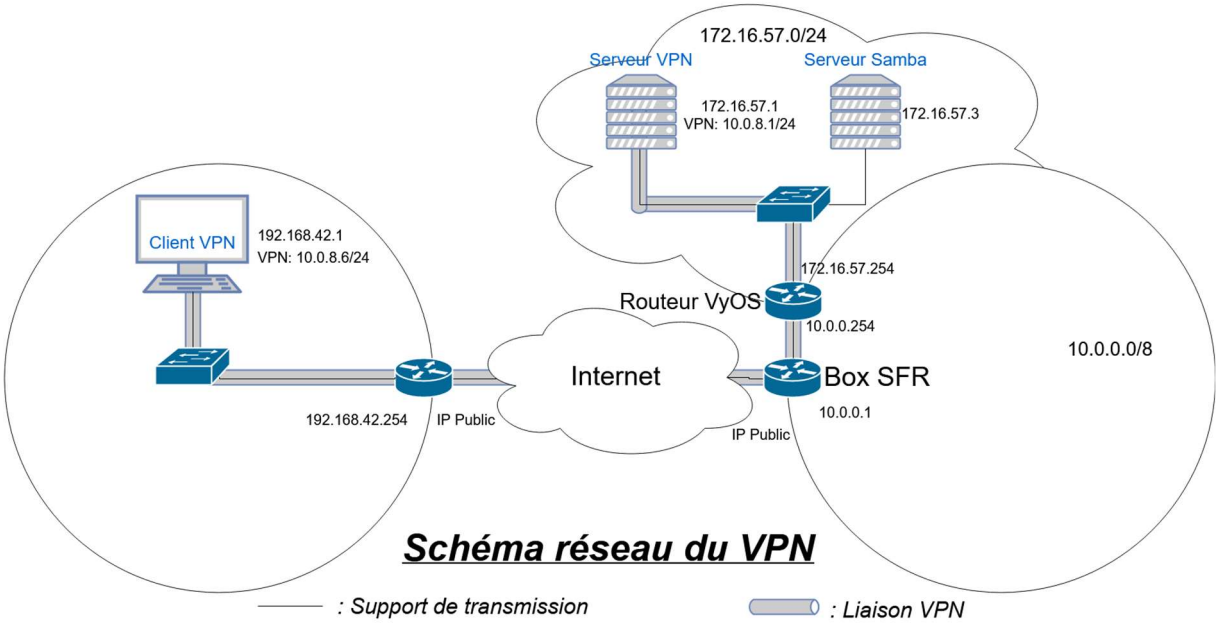
Procédure d'installation serveur VPN

Sommaire

1. Configuration requise

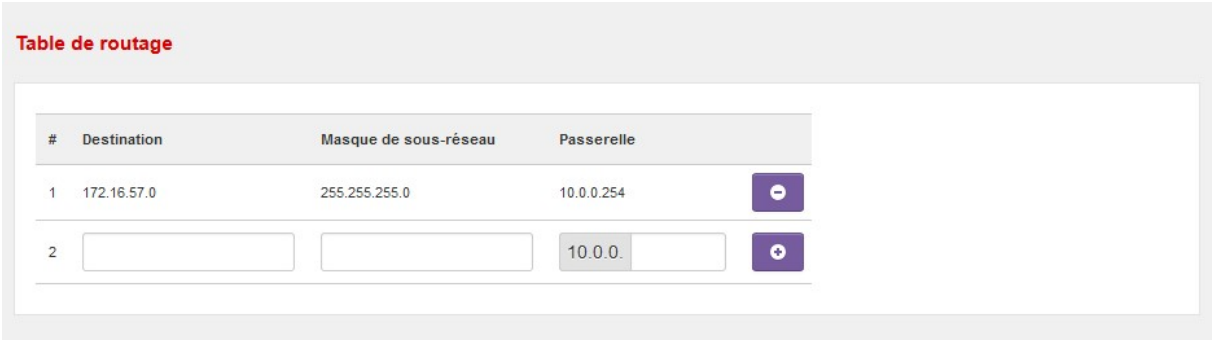
Un réseau similaire à ce schéma :



2. Configuration des routeurs

a. Configuration du routeur Principal(BOX)

Nous pouvons créer une route pour aller sur le réseau en 172.16.57.0/24.



Permet depuis mon réseau de pourvoir me connecter en SSH (Pas obligatoire).

Il faut obligatoirement rediriger le port d'écoute, vers le serveur OpenVPN.

J'ai mis le protocole UDP, mais on peut mettre les deux ce que j'ai fait mais je n'ai pas mis à jour le screen. @10.0.0.254 est le routeur Vyos.

b. Installation du routeur Virtuelle(VyOS)

Pour pouvoir avoir un VPN, fonctionnel sans conflit d'adresses IP, nous allons devoir utiliser un routeur, pour avoir une plage d'adresses différentes pour notre VPN en 172.16.57.0/24 et les machines qui sont sur le réseau en 10.0.8.0/24.

Pour cela, nous devons installer le routeur sur une machine virtuelle. L'identifiant et le mot de passe est vyOS.

Le clavier étant en qwerty, on peut le passer en azerty.

```
sudo loadkeys fr
```

Pour installer notre routeur, même si celui-ci peut être utiliser en live CD. Il faut exécuter cette commande :

```
install image
```

Il nous ait demandé si l'on veut bien continuer, pour cela presser juste la touche « Entrer ».

Pour ce qui est du partitionnement, pour mon cas je le mets en auto, mais il est possible de le faire manuellement.

Il nous demande si l'on veut bien l'installer sur le disque « sda », ce qui est mon cas donc je valide.

Après ce sont les questions poser pour chaque formatage, si l'on est conscient que toutes les données vont être effacer, saisir la taille de notre disque, le nom de l'image.

Nous pouvons si on le veut changer le mot de passe du compte « vyos ».

Une fois fait, notre routeur est installé.

c. Configuration du routeur Virtuelle(VyOS)

La configuration du clavier étant de base en qwerty, nous allons la passer en azerty.

```
sudo dpkg-reconfigure keyboard-configuration
```

Pour le français, sélectionner Generic 105-Key (Intl) PC puis Other, France, et enfin No compose key.

Si cela ne marche pas, utiliser cette commande.

```
sudo loadkeys fr
```

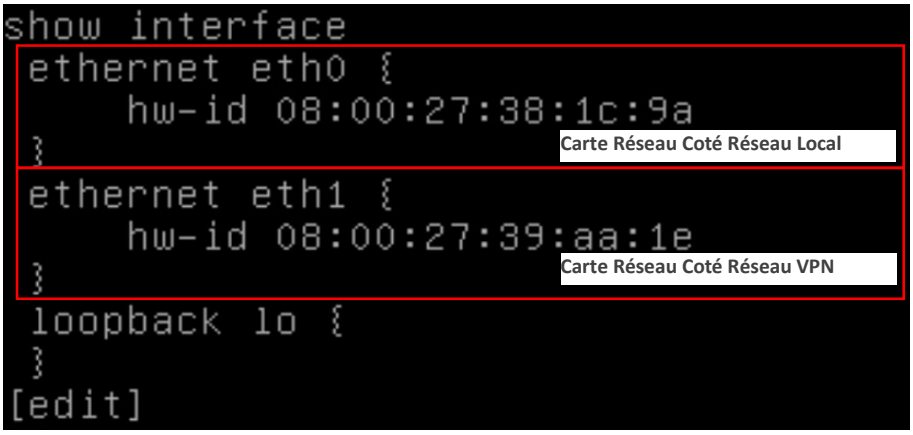
Nous allons activer le SSH, pour une prise à distance du routeur grâce à putty.

```
configure
set serivce ssh
commit
save
exit
```

Maintenant pour pouvoir se connecter en ssh, nous devons configurer les interfaces.

```
show interfaces
```

Voici le genre d'informations que nous recevons en retour.



Maintenant, que nous avons identifié les cartes réseaux, nous allons leurs attribuer une adresse et une description pour mieux les identifier.

```
configure
set interfaces ethernet eth0 address 10.0.0.254/8
set interface ethernet eth0 description WAN
save
set interfaces ethernet eth1 address 172.16.57.254/24
set interface ethernet eth1 description VPN
save
commit
```

Une fois fait, nous avons nos interfaces fonctionnelles. Mais nous n'avons pas accès à internet sur le réseau 172.16.57.0/24 pour cela, nous allons configurer le routeur de sorte que le réseau VPN ait accès au réseau WAN.

```
set nat source rule 10 description NAT-LAN-TO-WAN
set nat source rule 10 outbound-interface eth0
set nat source rule 10 source address 172.16.57.0/24
set nat source rule 10 translation address masquerade
set protocols static route 0.0.0.0/0 next-hop 10.0.0.1 distance 1
set protocols static route 10.0.8.0/24 next-hop 172.16.57.1 distance 2
```

Nous allons faire une redirection du port 1194, qui est le port utilisé pour le VPN vers l'adresse du serveur en 172.16.57.1.

```
set nat destination rule 100 description 'Port Forward: VPN to 176.16.57.1'
set nat destination rule 100 destination port 1194
set nat destination rule 100 inbound-interface eth0
set nat destination rule 100 protocol tcp
set nat destination rule 100 translation address 172.16.57.1
commit
save
exit
```

La configuration du routeur est finie, il n'y a plus besoin d'y toucher.

3. Installation des paquets

Pour mettre en place notre VPN, il faut installer certains paquets.

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

Attention, la suite des commandes linux doit être effectuée sur le serveur VPN et non le routeur.

4. Configuration du serveur OpenVPN

a. Générer le certificat et la clé de l'Autorité de Certification maître

Pour créer le certificat et la clé d'autorité de certification, nous devons faire une copie des fichiers de génération, pour cela il faut exécuter ces commandes.

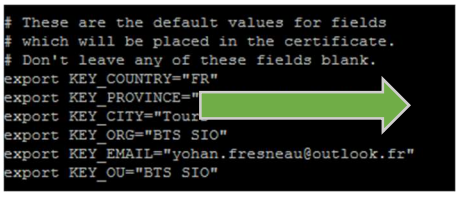
```
mkdir /home/administrateur/openvpn/
cp -r /usr/share/easy-rsa/* /home/administrateur/openvpn/
```

Une fois cela fait, nous devons modifier un fichier du nom « vars », pour créer notre certificat.

```
cd /home/administrateur/openvpn/
nano vars
```

En fin de fichier, nous avons quelques lignes comme voici.

```
# 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="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"
```



Cette modification n'est pas nécessaire, elle permet juste lors de la création des certificats, de ne pas saisir les informations.

Si le fichier « openssl.cnf » n'existe pas, il faut le renommer.

```
mv openssl-1.0.0.cnf openssl.cnf
```

Cette commande doit être effectuée, uniquement si le fichier « openssl.cnf » n'existe pas.

Maintenant que la modification a été effectuée, nous allons initialiser les variables.

```
. ./vars
```

Le « point/espace/point » n'est pas une erreur de saisir.

Nous devons effacer, tous les certificats existants.

```
./clean-all
```

Il est recommandé d'effacer le dossier « /home/administarteur/openvpn/key/ », en cas de certificats déjà existants.

Nous allons donc créer notre certificat et la clé de l'Autorité de Certification Maitre

```
./build-ca
```

Aucune information n'a besoin d'être saisie, sauf pour « Common Name » doit être le nom de la machine.

Maintenant, nous allons créer un certificat et une clé pour le serveur.

```
./build-key-server debian
```

Attention, l'argument « debian » doit être mis en fonction du hostname de votre machine.

Pendant la génération du certificat et de la clé, il nous faut mettre dans le champ « Common Name », le nom hostname de la machine. Il nous ait demandé de saisir un mot de passe(Obligatoire) et un nom d'entreprise(Facultatif).

```
Certificate is to be certified until Jun 29 11:58:03 2027 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Ne pas oublier de saisir « y » et de valider, deux fois sans quoi le certificat et la clé ne sera pas créer.

a. Création des certificats et des clés clients

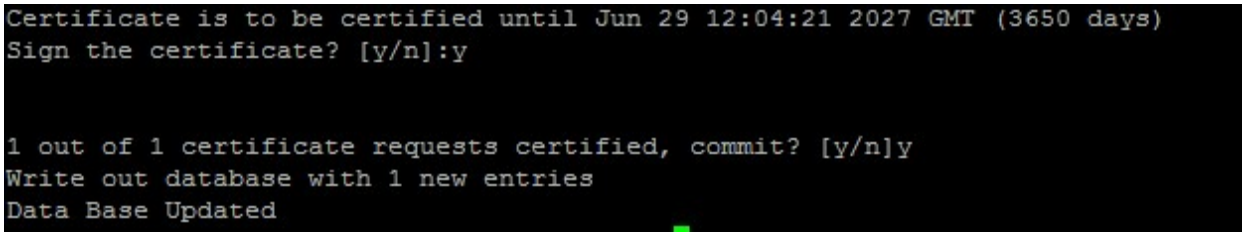
Pour créer des clés et des certificats et clients, c'est exactement la même méthode à utiliser, la commande est juste un peu différente.

```
./build-key utilisateur1
```

Attention, l'argument « utilisateur1 » doit être remplacer par le nom de l'utilisateur et doit être unique.

Il nous ait demander, de saisir des informations comme l'étape juste avant, il faut juste saisir dans « Commun Name » le nom de l'utilisateur. Pour mon cas le nom de la clé et du certificat son identique au nom de mon utilisateur.

Tout comme l'étape précédente, il nous ait demandé de saisir un mot de passe(Obligatoire) et un nom d'entreprise(Facultatif).



Ne pas oublier de saisir « y » et de valider, deux fois sans quoi le certificat et la clé ne sera pas créer.

Pour mon cas, ayant 3 utilisateurs en tous, je dois répéter l'opération encore 2 fois.

b. Les paramètres Diffie Hellman doivent être générés pour le serveur OpenVPN

Nous devons générer les paramètres pour le serveur OpenVPN.

```
./Build-dh
```

La génération peut prendre un peu de temps.

Voici le contenu et l'explication du dossier « /home/administrateur/openvpn/keys/ ».

Nom de fichier	Utilisation	Utilité	Secret
ca.crt	Serveur et tous les clients	Certificat racine CA	Non
dh2048.pem	Serveur seulement	Paramètres Diffie Hellman	Non
server.crt	Serveur seulement	Certificat serveur	Non
server.key	Serveur seulement	Clé serveur	Oui
utilisateur1.crt	Utilisateur 1 seulement	Certificat Utilisateur 1	Non
utilisateur1.key	Utilisateur 1 seulement	Clé Utilisateur 1	Oui
utilisateur2.crt	Utilisateur 2 seulement	Certificat Utilisateur 2	Non
utilisateur2.key	Utilisateur 2 seulement	Clé Utilisateur 2	Oui
utilisateur3.crt	Utilisateur 3 seulement	Certificat Utilisateur 3	Non
utilisateur3.key	Utilisateur 3 seulement	Clé Utilisateur 3	Oui

Peut varier selon le nom donner au clé et certificat créer.

Une fois la génération terminée, nous devons copier les fichiers suivant dans le dossier d'OpenVPN.

```
cp keys/dh2048.pem keys/ca.crt keys/debian.crt keys/debian.key /etc/openvpn/
```

c. Configuration du VPN coté serveurs

Pour la configuration des clients et du serveur, nous avons besoin de « gunzipper » un fichier.

```
cd /usr/share/doc/openvpn/examples/sample-config-files
gunzip server.conf.gz
```

Une fois cela fait, nous devons copier les fichiers extraits dans le dossier de configuration VPN.

```
cp server.conf /etc/openvpn/server.conf
```

Une fois le fichier copier, nous devons l'éditer.

```
cd /etc/openvpn/

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

```
port 1194
proto tcp
dev tun
ca ca.crt
cert debian.crt
key debian.key
dh dh2048.pem
server 10.0.8.0 255.255.255.0
#tls-auth ta.key
client-to-client
push "route 10.0.8.0 255.255.255.0"
push "route 172.16.57.0 255.255.255.0"
push "redirect-gateway def1 bypass-dhcp"
```

Configuration du fichier de config

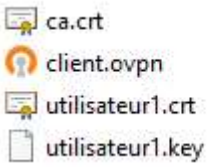
d. Configuration du VPN côté client

Pour ce qui est du côté client, il faut aller sur le site de OpenVPN et télécharger le client de OpenVPN qui se nomme « OpenVPN GUI ».

Nous devons copier le fichier « client.ovpn » qui se trouve dans le dossier « C:\Program Files\OpenVPN\sample-config ».

Puis le copier dans ce dossier « C:\Users\yohan\OpenVPN\config\ », qui est le dossier de configuration utilisateur, pour chaque utilisateur.

Une fois fait, nous devons copier les clés et certificat généré, pour ma part j'ai utilisé un serveur samba, dans le dossier « C:\Users\yohan\OpenVPN\config\ » au même emplacement que le fichier de configuration VPN client.

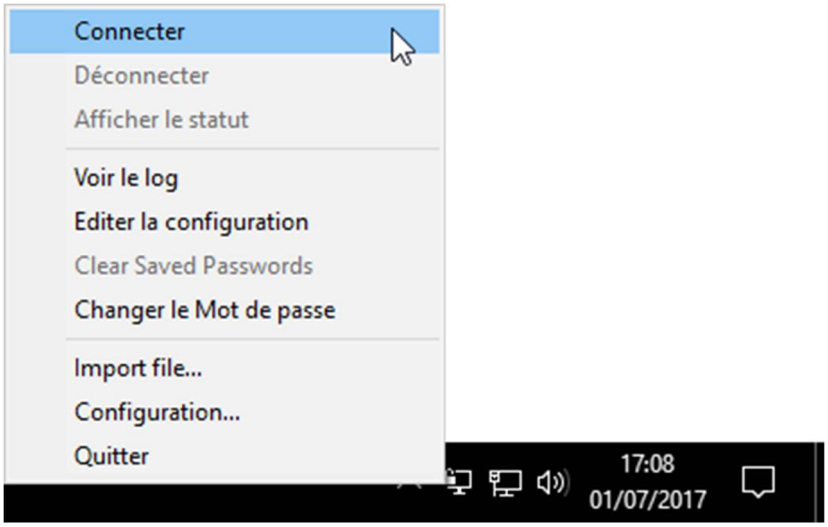


Pour établir la connexion, il faut modifier ces lignes dans le fichier de configuration.

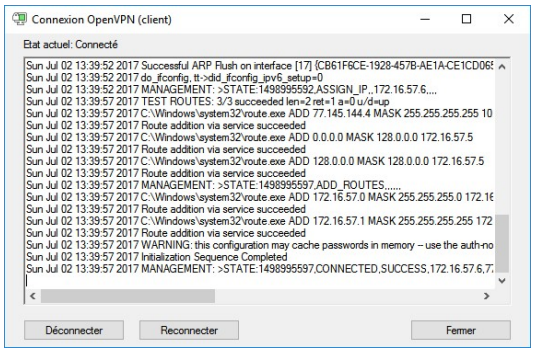
```
remote 77.145.144.4 1194
cert utilisateur1.crt
key utilisateur1.key
#tls-auth ta.key 1
```

5. Connexion au VPN

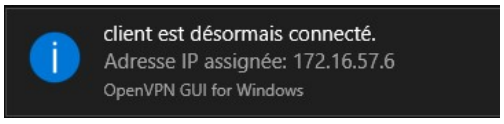
Pour se connecter au VPN, il faut fait clic droit sur l'icône « OpenVPN Gui » dans la barre des tâches, puis cliquez sur « connecter ».



Une fenêtre de log va apparaitre, avec les informations du client et de la connexion.



Une fois connecter, un message va apparaitre et nous informer de notre adresse IP, dans le réseau VPN en 10.0.8.0/24.



Cette icône  signifie que l'on est connecté. Si cette icône  apparait le client essai de joindre le serveur VPN. Celui-là  signifie que l'on n'est pas connecté.

6. Conclusion

Si on peut ping le serveur et les autres clients, cela veut dire que le VPN, est fonctionnel. Si ce n'est pas le cas vérifier que les passerelles sont bien les bonnes et que la table de routage des deux routeurs et le NAT sont bien configurés.