# Open VPN

## Les options principales d'Open VPN

- - remote : hôte sur lequel on va se connecter

--local : Hôte sur lequel on est

--dev précisez l'interface virtuelle utilisé (tun)

--port : port d'écoute utilisé (par défaut 1194)

--verb : mode verbeux (log) (à utiliser le 5)

–ifconfig : adressage virtuel (exemple –ifconfig 10.0.0.1 10.0.0.2

--push – route : les deux permettent l'ajout de route à distance sur le client

--server : désigner le serveur SSL / désigner le serveur qui distribue l'adressage virtuel

–client : désigne le client SSL / le client recevant l'adressage

-dh –ca –cert –key : permets d'indiquer le chemin où se trouve les fichiers de chiffrement

–genkey : crée une clé symétrique

--secret : indique le chemin de la clé symétrique

Création d'un certificat :

Premièrement nous allons créer les dossiers

```
mkdir apps/openvpn/keys
mkdir apps/openvpn/log
mkdir apps/openvpn/conffiles
mkdir apps/easy-rsa
```

Ensuite nous allons copier le répertoire *usr*/share/easy-rsa dans *apps*/easy-rsa

Nous allons ensuite modifier le fichier *apps/*easy-rsa/vars

*export KEY_DIR=/apps/openvpn/keys
*export KEY_COUNTRY= « FR »
*export KEY_PROVINCE= « IDF »
*export KEY_CITY= «Montmorency »
*export KEY_ORG= « booktic »
*export KEY_EMAIL= »me@booktic.com »

Ensuite nous allons appliquer les variables crées au préalable grace a la commande source vars

Nous nous mettons donc dans le dossier /*apps*/easy-rsa et exécutant sources vars

Puis nous utiliserons le script ./build-ca
Ensuite ./build -key server « SRVVPN »
Et ./build-key « SRVVPNCLI »

Puis nous allons créer la clé de chiffrement grace a la comande ./build-dh

Nous créons le fichier de configuration du serveur VPN, nous metterons ce fichier dans /*apps/*openvpn/confflies

Dans celui-ci nous mettons

```
proto udp
dev tun

ca /apps/openvpn/keys/ca.crt
cert /apps/openvpn/keys/booktic.crt
key /apps/openvpn/keys/booktic.key
dh /apps/openvpn/keys/dh2048.pem

server 192.168.1.0 255.255.255.0
push "route 172.17.2.0 255.255.255.0"
push "dhcp-option DNS 172.17.2.3"

client-to-client
keepalive 10 120
persist-key
persist-tun

#tls-auth ta.key 0

cipher AES-128-CBC

comp-lzo

max-clients 100
```

```
status openvpn-status.log
log /apps/openvpn/log/openvpn.log
log-append /apps/openvpn/openvpn.log
verb 5
```

Pour lancer le serveur VPN nous faisaons la commande suivante :
openvpn /*apps*/openvpn/conffiles/vpn.conf

Le serveur est maintenant actif.

Nous allons maintenant configurer le serevur,

Grâce a WinSCP on récupère les certificats que nous avons créer sur le sur le serveurs dans /*apps*/openvpn/keys et les transférons au meme endroit sur le client

Nous enregistrons un fichier de configuration pour le client, dans /apps/openvpn/conffiles :

```
client
dev tun
proto udp
remote 172.16.1.112 1194

resolv-retry infinite
nobind

ca /apps/openvpn/keys/ca.crt
cert /apps/openvpn/keys/client1.crt
key /apps/openvpn/keys/client1.key

persist-key
persist-tun

mute-replay-warnings

#tls-auth ta.key 0

cipher AES-128-CBC

comp-lzo

verb 5
```

Pour lancer le client il faut faire comme sur le serveur : openvpn /apps/openvpn/conffiles/vpncli.conf

Creéation des certificats sur DEBIAN 9

REMPLACE TOUTES LES COMMANDES BUILD

Configuration du SSL

1- *etc/*sslopenssl.cnf
Dans ce fichier il y a normalement « dir = /denoCA »
Nous le remplacons par « dir = *apps*apps/easy-rsa »
Sauvegardez

2- Creez dans *apps/*easy-rsa
un repertoire newcerts
créez avec touch deux fichiers vides
index.txt
serial

3- Ecrivez dans le fichier « serial »
« echo « 01 »>serial »

*Créez les certificats
*Créez l'autorité = build-ca
C'est a dire openssl req -new -modes -x509
-keyout CANicolas.key -out CANicolas.crt

* openssl req -modes -new keyout SRVvpn.key -out SRVvpn.csr

* openssl ca -cert CANicolas.crt
-keyfile CANicolas.key
- in SRVvpn.csr
- out SRVvpn.crt