Description

L'objectif est de mettre en place un serveur OpenVPN afin que lorsque j'utilise mon ordinateur en déplacement mon traffic Internet ne passe pas en clair sur la connexion où je suis afin d'éviter les vols de mots de passes ou tout autre soucis technique ou de censure.

Pour cela j'installe le serveur OpenVPN sur un serveur qui est disponible sur Internet (dans mon cas chez OVH) puis je configure mon ordinateur pour se connecter là bas et que ma passerelle par defaut (“default gateway”) pointe vers le serveur VPN.

OpenVPN

Ce logiciel est libre et permet de faire des connexions encryptées entre client-to-client ou client-to-server; la différence principale étant de pouvoir avoir plusieurs connexions ou non. L'authentification peut se faire d'une manière simple avec un nom d'utilisateur/mot de passe (fortement déconseillé) ou bien via un échange de certificats (PKI Authentification) qui est la meilleur solution.

La documentation du site est très bien faite :
http://openvpn.net/index.php/open-source/documentation/howto.html

Mise en place du serveur

J'installe le serveur sur une Debian/Squeeze, l'installation est simple :

```
apt-get install openvpn
```

Une fois le package installé il y'a 3 endroits importants :

- /etc/default/openvpn (contient la liste des fichier pour le démarrage)
- /etc/openvpn/ (contient la configuration de OpenVPN)
- /usr/share/doc/openvpn (contient des exemples et les scripts utiles au démarrage)

Au besoin ne pas hésiter à lire le READMBE spécial Debian

```
zless /usr/share/doc/openvpn/README.Debian.gz
```

Création du fichier de configuration du serveur :

```
cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz
/etc/openvpn/.
gzip -d /etc/openvpn/server.conf.gz
```

Création des certificats utilient au fonctionnement du serveur et à l'authentification des clients; dans mon cas je mets cela dans “/srv/syst/sbin/” :

```
cp -rv /usr/share/doc/openvpn/examples/easy-rsa/2.0 /srv/syst/sbin/easy-rsa
cd /srv/syst/sbin/easy-rsa
```

Il faut ensuite configurer le fichier “vars”, enfin ce n'est pas obligatoire mais ça simplifie beaucoup les choses.

```
export KEY_COUNTRY="BE"
export KEY_PROVINCE="HAINAUT"
export KEY_CITY="MONS"
export KEY_ORG="LoLiGrUB ASBL"
export KEY_EMAIL="equipe.technique@xxx.xx"
```

Exécuter les différentes commandes indiquées dans le HOWTO :

- . ./vars
- ./clean-all
- ./build-ca
- ./build-key-server server
- ./build-dh

Les certificats du serveur sont OK.

Maintenant créons un certificat pour le client :

- ./build-key frbayart1

Quelques configurations supplémentaires pour que tout soit bien trié :

- ln -s /srv/syst/sbin/easy-rsa/keys /srv/syst/vpn-keys
- mkdir /var/log/openvpn

Maintenant il faut éditer le fichier de configuration du serveur qui est dans /etc/openvpn/ nommé “server_443-TCP.conf”

```
local 1.2.3.4
port 443
proto tcp
dev tun
ca /srv/syst/vpn-keys/ca.crt
cert /srv/syst/vpn-keys/server.crt
dh /srv/syst/vpn-keys/dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt
push "redirect-gateway def1 bypass-dhcp"
keepalive 10 120
comp-lzo
max-clients 10
user nobody
group nogroup
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log         /var/log/openvpn/openvpn.log
verb 3
```

```
mute 20
```

Les 3 points importants sont :

- utiliser des chemins absolus pour éviter que les fichiers soient dans /etc/openvpn
- push “redirect-gateway def1 bypass-dhcp” afin que le traffic soit envoyé entièrement via le VPN
- server 10.8.0.0 255.255.255.0 qui indique les adresses IPs utilisées

Maintenant en éditant le fichier /etc/default/openvpn j'ajoute la ligne suivante

```
AUTOSTART="server_443-TCP"
```