Description

L'objectif est de mettre en place un serveur OpenVPN afin que lorsque j'utilise mon ordinateur en déplacement mon trafic 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 pour 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 README 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 utiles 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"
```

Reste à lancer le serveur VPN

```
/etc/init.d/openvpn start
```

N.B. : pour une installation sur Ubuntu plutôt que Debian, commencer par “sudo su” pour exécuter tout en tant que “root”. Il faut aussi créer les répertoires “/srv/syst/sbin/” qui n'existent pas.

Mise en place du client

Pour le client j'utilise un ordinateur sous Ubuntu. Pour installer le client aller dans Synaptic et choisir le paquet “openvpn”.

La logique de configuration du client est la même que le serveur à savoir :

- /etc/default/openvpn (contient la liste des fichier pour le démarrage)
- /etc/openvpn/ (contient la configuration de OpenVPN)

Il faut récupérer les certificats depuis le serveur, là c'est l'opération délicate afin de vous assurer que tout est sécurisé durant cette copie. Seul 3 fichiers sont utiles pour le client, dans mon cas le certificat que j'ai généré ce nomme frbayart1 du coup voici les fichiers que j'ai téléchargés :

```
ca.crt
frbayart1.crt
frbayart1.key
```

Ensuite j'ai créé mon fichier de configuration dans /etc/openvpn que j'ai nommé monvpn.conf (par exemple sudo gedit /etc/openvpn/monvpn.conf) :

```
client
dev tun
proto tcp
remote 1.2.3.4 443
resolv-retry infinite
nobind
user nobody
group nobody
persist-key
persist-tun
```

```
ca /home/francois/vpn/ca.crt
cert /home/francois/vpn/frbayart1.crt
key /home/francois/vpn/frbayart1.key
comp-lzo
verb 3
```

Au passage le groupe nobody n'existant pas sur mon linux je le crée (sudo addgroup nobody).

J'édite (sudo gedit) /etc/default/openvpn pour ajouter la ligne :

```
AUTOSTART="monvpn"
```

Puis je lance le tout :

```
/etc/init.d/openvpn start
```

Vous pouvez vérifier avec la commande ifconfig et ouvrir une page du navigateur sur http://whatismyipaddress.com/fr/mon-ip pour constater que l'IP est celle du serveur openvpn !

Pour arrêter :

```
/etc/init.d/openvpn stop
```

Partage de la connexion sur le serveur

Afin que le serveur autorise la partage de la connexion Internet qu'il utilise il faut ajouter une petite règle dans “iptables”

```
iptables -A POSTROUTING -t nat -s 10.0.0.0/8 ! -d 10.0.0.0/8 -o eth0 -j
MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Avec un traceroute ou mtr nous pouvons vérifier que nous passons bien par le serveur VPN et non via la connexion où nous sommes.

From:
https://www.loligrub.be/wiki/ - **LoLiGrUB**

Permanent link:
https://www.loligrub.be/wiki/documentation:openvpn?rev=1314560067

Last update: **2014/12/27 08:13**