Table des matières

Côté serveur :

```
apt-get install openvpn
cp -R /usr/share/doc/openvpn/examples/easy-rsa/2.0/ /etc/openvpn/easy-rsa/
cd /etc/openvpn/easy-rsa/
vi vars
source ./vars
./clean-all
./build-ca
./build-key-server server
./build-key client1
openvpn –genkey –secret keys/ta.key
cd keys/ && cp ca.crt dh1024.pem server.crt server.key ta.key ../../
vi  /etc/openvpn/server.conf
```

/etc/openvpn/server.conf :

```
port 1194
proto udp
dev tap
topology subnet
ca ca.crt
cert devilschild.crt
key devilschild.key
dh dh1024.pem
server 172.16.1.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"
ifconfig-pool-persist ipp.txt
client-to-client
keepalive 10 120
tls-auth ta.key 0 # A pas diffuser
comp-lzo
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
verb 3
management 172.16.1.254 223 /root/ovpn.pass
```

iptables :

```
iptables -A OUTPUT -o tap0 -j ACCEPT
iptables -A INPUT -i tap0 -j ACCEPT
iptables -A FORWARD -i tap0 -j ACCEPT
```

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

Côté client :

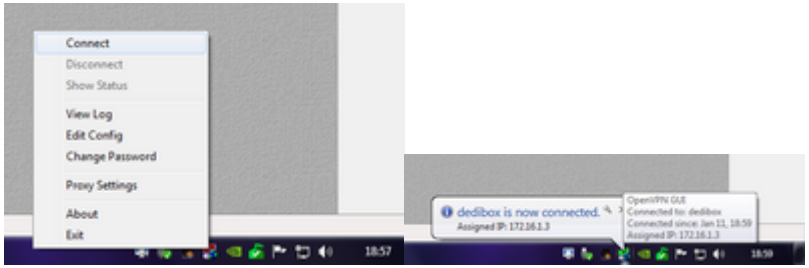
Récupérer le client : http://openvpn.se/download.html et l'installer

Copie des fichiers **ca.crt** et **clientX.crt** et **clientX.key** et **ta.key** sous **C:\Program Files (x86)\OpenVPN\config**

Créer le fichier de conf client **monserveurvpn.ovpn** en modifiant les paramètres ci-dessous :

```
dev tap
proto udp
remote X.X.X.X 1194
ca ca.crt
cert clientX.crt
key clientX.key
```

Lancer **OpenVPN GUI** :



Et maintenant tout le trafic passe par le VPN, si le firewall de votre serveur est correctement configuré.

Pour lancer automatiquement au boot :

```
"C:\Program Files (x86)\OpenVPN\bin\openvpn-gui-1.0.3.exe" --connect monserveurvpn.ovpn
```

From:
https://unix-bck.ndlp.info/ - **Where there is a shell, there is a way**

Permanent link:
https://unix-bck.ndlp.info/doku.php/informatique:nix:linux:linux_openvpn:openvpn

Last update: **2013/01/12 16:45**