CONFIGURATION DE OPENVPN AVEC CLIENT FEDORA ET CLIENT WINDOWS

Distribution : Fedora 14

Noyau GNU/Linux :2.6.35

Version document : 1

Auteur : Le Cabellec Anthony

12 Décembre 2010

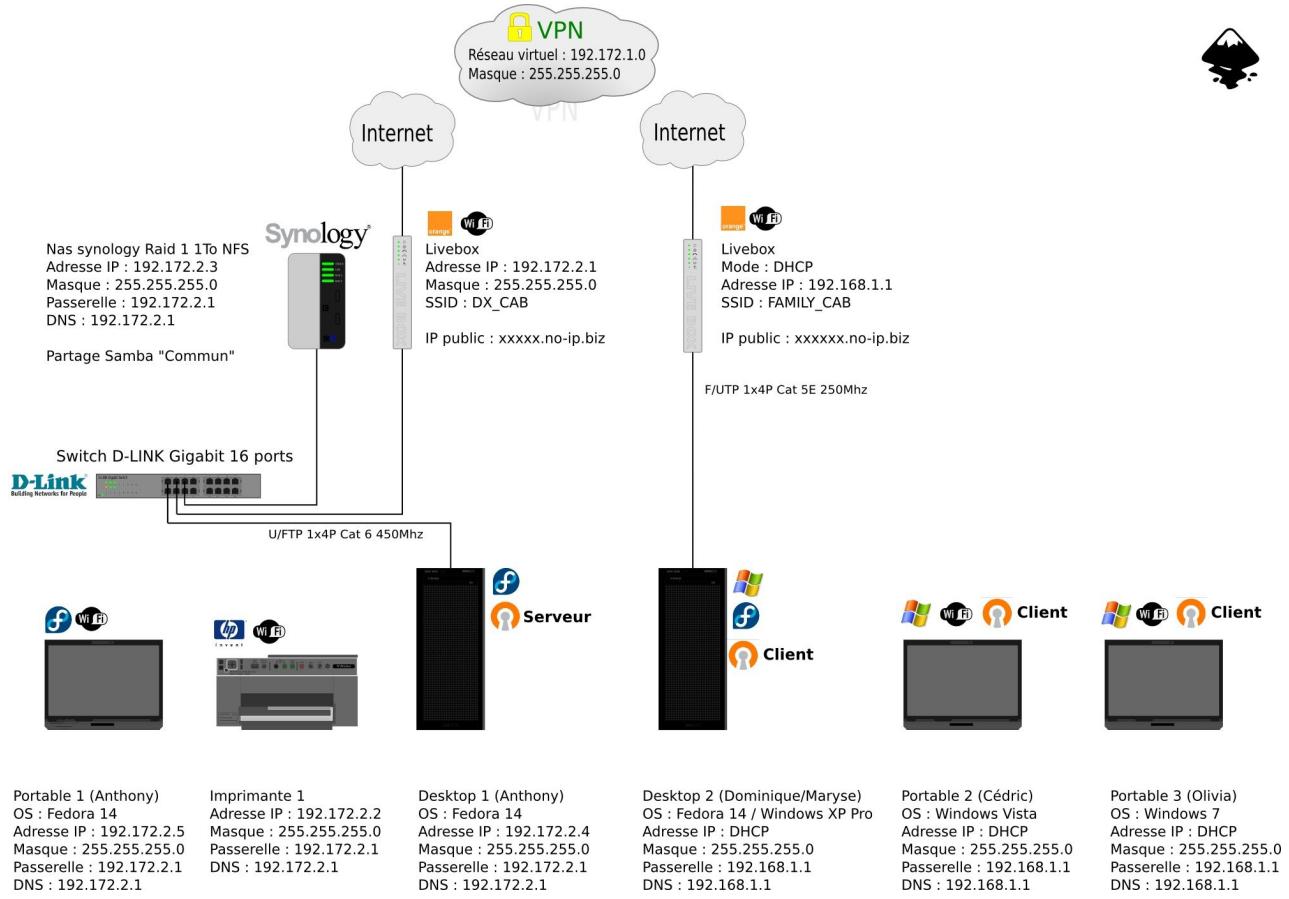
Table des matières

1 – Présentation

Voici un petit tutoriel qui va vous permettre de connecter différents clients sur un réseau distant. Et cela de manière transparente et sécurisé. La configuration peu être très différentes suivant l'architecture de votre réseau. Je me suis basé sur mon architecture qui ressemble beaucoup à celle de n'importe quel particulier équipé d'un modem triplay.

Le but sera de pouvoir avoir accès à mon disque dur réseau (NAS). Ainsi ma famille aura accès aux données depuis n'importe quelle connexion internet. Pratique non ! Ils pourront ainsi y stocker leur données (Car le NAS est configurer en Raid1).

Architecture de mon réseau :



Le principe de fonctionnement d'OpenVPN sera de créer un réseau virtuel intermédiaire. Ce réseau sera complètement sécurisé car il sera encapsulé dans une connexion cryptée et sécurisée.

Non allons donc devoir créer ce réseau virtuel. Le serveur OpenVPN sera le desktop 1 (Sachez que de nombreux modem/routeur offre directement le VPN, seulement pour continuer de bénéficier la téléphonie et la tv par ADSL ils ne nous laisse pas le choix que d'utilisé les box FAI)

Notre réseau virtuel sera en 192.172.1.0 255.255.255.0

2 – Installation d'OpenVPN

Connectons-nous en root :

```
[anthony@Tony-Desktop ~]$ su -
Mot de passe :
[root@Tony-Desktop ~]#
```

```
[root@Tony-Desktop ~]# yum install openvpn openssl

.........
```

Installons le paquet « Openvpn » :

3 – Création des certificats de sécurités SSL

Nous allons tout d'abord créer les répertoires qui contiendront les certificats et copier le répertoire contenant les scripts OpenVPN:

```
[root@Tony-Desktop ~]# mkdir /etc/openvpn/easy-rsa/
[root@Tony-Desktop ~]# cp /usr/share/openvpn/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
[root@Tony-Desktop ~]# mkdir /etc/openvpn/easy-rsa/keys
```

Créons le fichier index.txt qui listera les certificats et leurs statuts :

```
[root@Tony-Desktop ~]# touch /etc/openvpn/easy-rsa/keys/index.txt
[root@Tony-Desktop ~]# echo 01 >/etc/openvpn/easy-rsa/keys/serial
```

Nous allons ensuite éditer le fichier contenant les variables des scripts. Pour cela nous allons utiliser l'éditeur Vi :

```
[root@Tony-Desktop ~]# vi /etc/openvpn/easy-rsa/vars
```

Et nous renseignons correctement les champs suivant :

```
# 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="FR"
export KEY_PROVINCE="44"
export KEY_CITY="NANTES"
export KEY_ORG="CAB"
export KEY_EMAIL="anthony.lecabellec@gmail.com"
```

A noter qu'il est également possible de configurer la durée de validité des clés. (Variable KEY_EXPIRE) par défaut à 3650 soit 10 années.

On se place dans le répertoire et on initialise les variables :

```
[root@Tony-Desktop ~]# cd /etc/openvpn/easy-rsa/
[root@Tony-Desktop ~]# . ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
```

On supprime les clés existantes (Normalement il n'y en a aucune) :

```
[root@Tony-Desktop ~]# ./clean-all
```

Remarque : cette la commande ./clean-all ne devra être effectuée qu'un seul fois.

Générons maintenant le certificat d’autorité de certification (Appeler Master CA) :

```
[root@Tony-Desktop easy-rsa]# ./build-ca
Generating a 1024 bit RSA private key
..................++++++
...++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:
State or Province Name (full name) [44]:
Locality Name (eg, city) [NANTES]:
Organization Name (eg, company) [CAB]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [VPNSRV]:
Name []:VPNSRV
Email Address [anthony.lecabellec@gmail.com]:
```

Ne pas oublier d'indiqué le Common Name qui est le nom du serveur VPN.

Générons la clé et le certificat pour le serveur :

```
[root@Tony-Desktop easy-rsa]# ./build-key-server VPNSRV
Generating a 1024 bit RSA private key
.........++++++
..............................++++++
writing new private key to 'SRVVPN.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:
State or Province Name (full name) [44]:
Locality Name (eg, city) [NANTES]:
Organization Name (eg, company) [CAB]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [VPNSRV]:
Name []:VPNSRV
Email Address [anthony.lecabellec@gmail.com]:

.............

Certificate is to be certified until Nov 20 20:02:36 2020 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
```

Générons la clé et le certificat pour le client PORTABLE2:

```
[root@Tony-Desktop easy-rsa]# ./build-key PORTABLE2
Generating a 1024 bit RSA private key
.................++++++
.....................++++++
writing new private key to 'PORTABLE2.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:
State or Province Name (full name) [44]:29
Locality Name (eg, city) [NANTES]:ARZANO
Organization Name (eg, company) [CAB]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [VPNSRV]:PORTABLE2
Name []:Portable_2
Email Address [anthony.lecabellec@gmail.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:lecabellec
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'FR'
stateOrProvinceName   :PRINTABLE:'29'
localityName          :PRINTABLE:'ARZANO'
organizationName      :PRINTABLE:'CAB'
commonName            :PRINTABLE:'PORTABLE2'
name                  :T61STRING:'Portable_2'
emailAddress          :IA5STRING:'anthony.lecabellec@gmail.com'
Certificate is to be certified until Nov 20 20:06:57 2020 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
```

Remarque : Le Common Name devra impérativement être différents des autres clients et du serveur.

Génération des paramètres de Diffie-Hellman :

```
[root@Tony-Desktop easy-rsa]# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
........+.....................+.............+.....................................................
+.....................................................................
+.....................................................................+.........+.....................
+.........................+.....................................................+.............+...................+.....++*++*++*
[root@Tony-Desktop easy-rsa]#
```

Nous générons une clé ta.key afin d'évité un attaque par interception de clé :

```
[root@Tony-Desktop easy-rsa]# openvpn - -genkey – -secret keys/ta.key
```

4 – Configuration du serveur

```
[root@Tony-Desktop easy-rsa]# cp /usr/share/doc/openvpn-2.1.1/sample-config-
files/server.conf /etc/openvpn/
[root@Tony-Desktop openvpn]# vi serveur.conf
```

```
#Configuration serveur
#Port par défaut 1194 (ne pas oublier d'ouvrir ce port sur votre par-feu
port 1194
#protocole ou transitera le tunnel udp suffisant car il encapsulera du tcp crypté
proto udp
#mode routed
dev tun
#chemin des fichiers de sécurité
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/VPNSRV.crt
key /etc/openvpn/easy-rsa/keys/VPNSRV.key
dh /etc/openvpn/easy-rsa/keys/dh1024.pem
tls-auth /etc/openvpn/easy-rsa/keys/ta.key
#adresse du réseau virtuel
Server 192.172.1.0 255.255.255.0
#passerelle par defaut ici notre serveur
push "route 192.172.2.0 255.255.255.0"
keepalive 10 120
#type de cryptage
cipher AES-128-CBC
 #compression de données
comp-lzo
#nombre de client sumultanées
max-clients 10
#user et groupe du processus
user nobody
group nobody
#rendre la connexion persistante
persist-key
persist-tun
#Niveau de verbosité
verb 5
```

5 - Configuration client :

Le portable2 fonctionne sous Windows XP ainsi il faudra installer la version client pour Windows que vous trouverez sur le site officiel d'openVPN :

http://openvpn.net/download.html

Sous un client Linux il faudra simplement installer OpenVPN car OpenVPN fait aussi bien serveur que client. La ligne client ou serveur dans le fichier de configuration détermine s'il fonctionnera en mode serveur ou client,

Une fois la version Windows installée, vous allez copier les clés et certificats ci-dessous dans le répertoire config :

ca.crt
ta.key
PORTABLE2.crt
PORTABLE2.key

Et ensuite nous allons créer le fichier de configuration client.ovpn avec le bloc note.

A noter que celui-ci est installer sur Windows XP d'où l'extension .ovpn du fichier de configuration. Sous linux cela sera client.conf.

```
#Configurtion client
#Mode client
client
# mode routed
dev tun
#Le protocole
proto udp
#Adresse du serveur IP ou DNS
remote xxxxxx.no-ip.biz 1194
#Permet la recherche constante du serveur
resolv-retry infinite
nobind
user nobody
group nobody
persist-key
persist-tun
mute-replay-warnings
#Les différents clés et certificats
ca ca.crt
cert PORTABLE2.crt
key PORTABLE2.key
tls-auth ta.key
#Type de cryptage
cipher AES-128-CBC
#Compression
comp-lzo
#Verbosité
verb 3
```

6 – Configuration du parfeu

Coté client vous ne devriez rien avoir à faire. Coté serveur par contre quelques règles sont à ajouter,

OpenVPN utilise le port UDP 1194 par défaut. Il faudra donc ajouter une règle au parfeu du serveur via iptables pour ouvrir le port :

```
[root@Tony-Desktop easy-rsa]# iptables -t filter -A INPUT -m state --state NEW -m udp -p udp --dport 1194 -j ACCEPT
```

Afin que les clients puisse accéder au disque dur réseau il va falloir activé IP forward sur le serveur :

```
[root@Tony-Desktop easy-rsa]#echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
```

Puis autorisé le forward au niveau du parfeu :

```
[root@Tony-Desktop easy-rsa]# iptables -I INPUT -i tun0 -j ACCEPT
[root@Tony-Desktop easy-rsa]# iptables -I FORWARD -i tun0 -j ACCEPT
[root@Tony-Desktop easy-rsa]# iptables -I FORWARD -o tun0 -j ACCEPT
[root@Tony-Desktop easy-rsa]# iptables -I OUTPUT -o tun0 -j ACCEPT
```

7 – Configuration du modem

Coté client rien à faire. Coté serveur il faudra configurer le NAT. En ouvrant le port 1194 en udp et en redirigeant les paquets sur le serveur (Ici en 192.172.2.4)

Il faudrait également ajouter une route sur le modem qui fait office de de passerelle. Seulement sur la Livebox je n'ai pas trouvé comment réaliser.
Ci-dessous la commande à réaliser sur le modem :

```
[root@Tony-Desktop easy-rsa]#route add -net 192.172.1.0 netmask 255.255.255.0 gw
192.172.2.4
```

Étant donner que j'ai pas encore trouver la réponse à cette question. Nous allons allons ajouter la route sur le NAS.

8 – Configuration du NAS

Comme je n'ai pas encore trouver comment ajouter une route à la livebox nous allons l'ajouter sur le NAS. Pour cela j'ai utilisé une connexion ssh :

```
[root@Tony-Desktop easy-rsa]#route add -net 192.172.1.0 netmask 255.255.255.0 gw
192.172.2.4
```

9 – Test

Coté serveur :

Lancement du serveur via la commande openvpn :

```
[root@Tony-Desktop openvpn]#openvpn  serveur.conf

.....

Sun Dec 12 19:00:57 2010 us=245542 UDPv4 link remote: [undef]
Sun Dec 12 19:00:57 2010 us=245558 MULTI: multi_init called, r=256 v=256
Sun Dec 12 19:00:57 2010 us=245590 IFCONFIG POOL: base=192.172.1.4 size=62
Sun Dec 12 19:00:57 2010 us=245615 Initialization Sequence Completed
```

Pour lancer OpenVPN au démarrage de l'ordinateur :

```
[root@Tony-Desktop easy-rsa]#chkconfig openvpn start
```

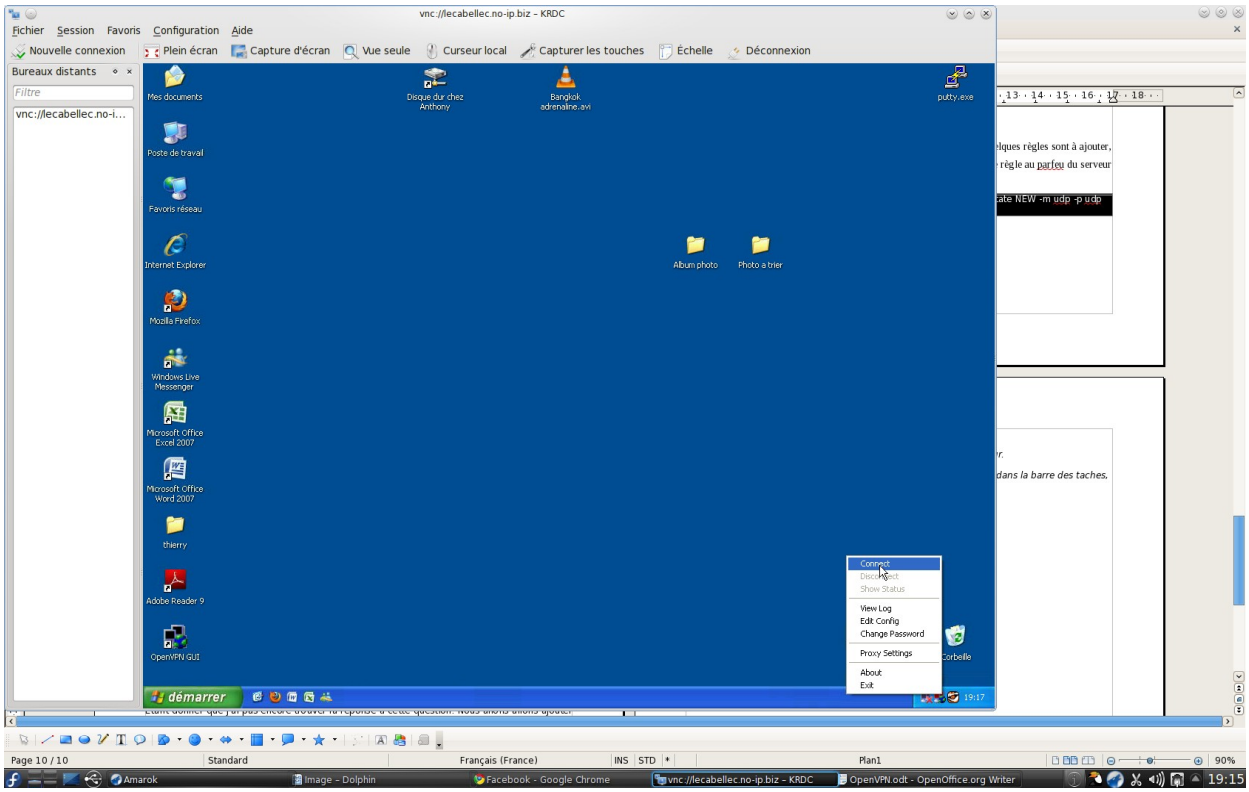
Via la commande ifconfig vous devriez voir une nouvelle interface « tun0 » :

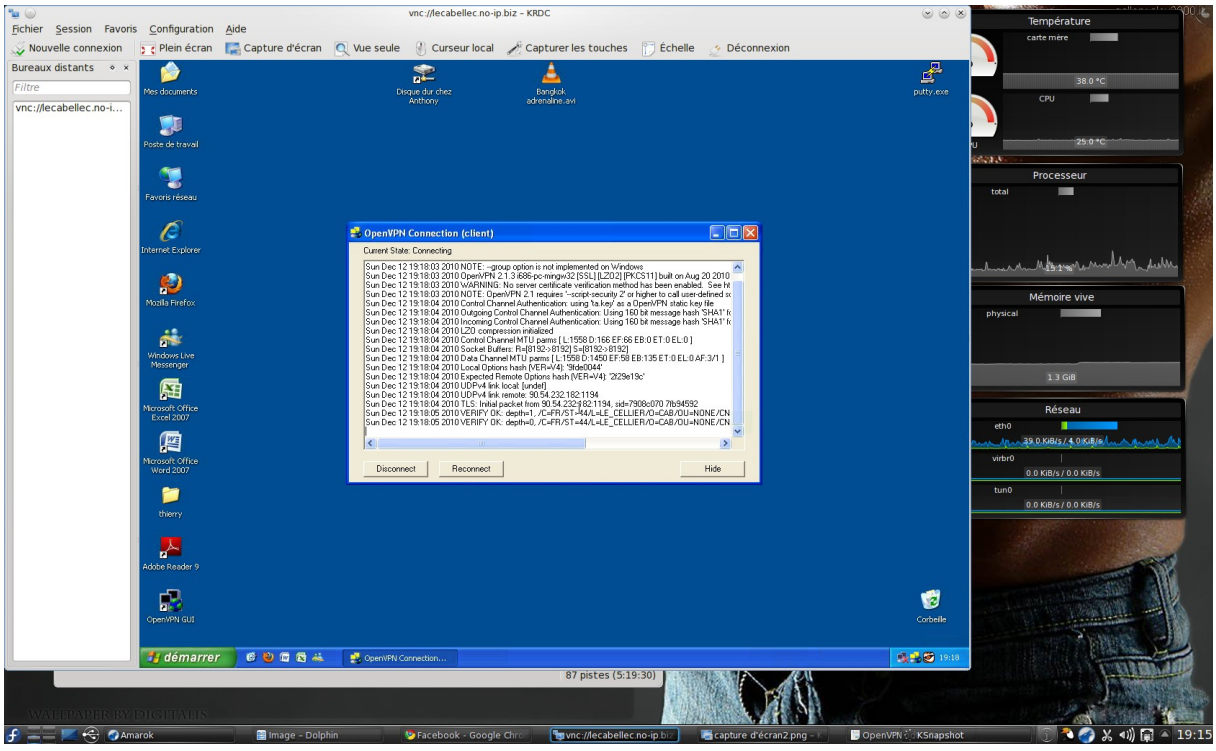
```
[root@Tony-Desktop openvpn]# ifconfig
eth0      Link encap:Ethernet  HWaddr 90:E6:BA:2D:12:B4
          inet adr:192.172.2.4  Bcast:192.172.2.255  Masque:255.255.255.0
          adr inet6: fe80::92e6:baff:fe2d:12b4/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2266403 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2356459 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:3176390160 (2.9 GiB)  TX bytes:1707425101 (1.5 GiB)
          Interruption:48 Adresse de base:0x6000

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:364 errors:0 dropped:0 overruns:0 frame:0
          TX packets:364 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:105706 (103.2 KiB)  TX bytes:105706 (103.2 KiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet adr:192.172.1.1  P-t-P:192.172.1.2  Masque:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Coté client :

Sous un client Linux la manipulation est identique que coté serveur.

Sous Windows par contre il faudra lancer « OpenVPN GUI ». Un icône apparaitra dans la barre des taches,
Un clique gauche vous affichera un menu. Cliquer sur connect.





Maintenant vous êtes connecté sur le réseau virtuel. Pour accéder au disque dur réseau NAS il suffit tout simplement d'ajouter un lecteur réseau

Ici un lecteur réseau pointant sur \\192.172.2.3\Commun

Enjoy ...