Installation d'Open VPN

par

Date de publication :

Dernière mise à jour :

I - Rappel théorique
II - Exemple de cas pratique
III - OpenVPN
Présentation
III-B - Installation
III-B-1 - Installation du serveur
Installation d'OpenVPN
Installation d'OpenSSL
Génération des certificats
Décompression du fichier de configuration d'OpenSSL
Edition du fichier vars
Generation du certificat racine
Generation du certificat du serveur
Génération d'un certificat client
Generation de Diffie-Hellman
Résumé des fichiers générés
Création du fichier de configuration
Lancement du serveur
III-B-2 - Installation du client sous linux
Lancement du client
III-B-3 - Installation du client sous windows
Installation
Configuration
Connection
III-B-4 - Installation du client sous Mac OS X

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

I - Rappel théorique

Au tout début, un ordinateur était isolé, il était dans une pièce tout seul, ne servant qu'a faire de longs calculs.

Mais bien vite il fut nécessaire de permettre à des groupes d'ordinateurs situés dans un même batiment de communiquer. Ce fut la naissance des **LAN** (ou réseaux locaux).

A cette époque, les communications étaient simples et ne possèdaient aucune notion de sécurité. Les communications ne sortant pas du bâtiment, la seule notion de sécurité était le garde à l'entrée ;-).

Parallèlement, une nouvelle forme de réseau se développait. Celui-ci permettait à des ordinateurs des quatres coins du monde de dialoguer ensemble **Internet**

Encore une fois, la sécurité des communications ne fut pas une priorité car les informations qui y circulait n'étaient ni confidentielles ni commerciales. Le but premier d'Internet fut de permettre au universités et laboratoires d'échanger leur informations.

Mais de part le succès et la mise à disposition du grand public d'Internet, des organismes de ventes, des banques voir même des gouvernements ont fournit des services en ligne. Il fut donc nécessaire de penser à la sécurité et confidentialité des communications.

C'est ainsi que naquit le protocole **SSL** (maintenant renommé en **TLS**), qui permettait d'ajouter une couche de sécurité sur des protocoles déjà existant sans devoir modifier radicalement les applications les utilisant. Elle va s'insérer dans la pile TCP/IP afin de chiffrer/déchiffrer les paquets entre la couche Application et la couche TCP.

Mais bientot, avec l'accroissement des sociétés, la notion de LAN ne suffisait plus (une société pouvant avoir une filliale dans plusieurs villes ou pays), et Internet n'étant pas assez sécurisé il reste un manque.

Par exemple, dans le cas d'un employé qui doit télétravailler, il serait intéressant de lui donner accès au même outil que s'il était physiquement dans l'entreprise. Et il serait impensable de penser à gérer les accès d'un intranet en l'étendant à Internet.

C'est dans de tels cas que la notion de **VPN** montre tout son intêret. En effet, un VPN est un Virtual Private Network, un réseau privé virtuelle. Il offre les mêmes avantages qu'un LAN, en permettant à des clients situés n'importe où dans le monde d'y être connecté, le tout en passant par un canal de communication sécurisé.

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

II - Exemple de cas pratique

Je vais tenter de vous expliquer l'utilité d'un VPN par un cas vécu.

Voulant administrer la base de donnée Mysql d'un serveur dédié, j'utilisait PhpMyAdmin, un très bon outil mais un peu lourd pour une utilisation intensive.

Or, il existe des outils tels que Mysql Administrator développé spécifiquement pour la gestion de *MySql*. Seul soucis, j'aurai été forcé d'ouvrir Mysql sur le réseau, et par conséquent sur Internet.

Même si cela est possible, cela peut s'avérer dangereux pour le serveur Mysql (attaque DoS, brut force, ...). Et cela m'ennuyait d'ouvrir une faille de sécurité simplement pour l'administration de MySql.

J'ai donc décidé d'installer un serveur Vpn (et plus particulièrement OpenVPN), j'avais ainsi un réseau virtuel, invisible de l'éxtérieur, dans lequel je pouvais ouvrir MySql et ainsi utiliser mon outil d'administration de manière transparente.

Cela n'est bien sur pas l'unique solution possible pour résoudre ce genre de problème, une autre possibilité aurait été d'utiliser un tunnel SSH.

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

III - OpenVPN

Présentation

OpenVpn est sans doute la référence Open Source dans le domaine du VPN. Cette solution ne se base pas sur les standards VPN tel que IPSec mais sur une surcouche de SSL. Il n'est donc pas compatible avec les solutions hardwares qu'offre certains routeur/modem et nécéssite l'installation d'un client logiciel.

Heureusement, ce client est disponible pour la plupart des systèmes d'exploitation (Windows, Mac OS X, Linux, BSD). Il existe même un portage pour les PocketPC.

III-B - Installation

III-B-1 - Installation du serveur

La première étape est de configurer un serveur OpenVPN, et dans notre cas sur un Linux Debian Sarge.

Ce serveur aura la responsabilité d'authentifier les utilisateurs, leur fournir une adresse ip dans le réseau virtuel ainsi qu'éventuellement fournir les différentes informations de routages dans certains cas complexes.

En ce qui concerne la sécurité, la communication est chiffrée à l'aide de openSSL, cela implique donc la nécessité de plusieurs certificats :

- Un certificat racine, qui sera utilisé pour signer à la fois le certificat du serveur et les certificats des clients
- Un certificat serveur, qui servira à chiffrer la communication
- Un ou plusieurs certificats client, optionnels, qui serviront à authentifier les utilisateurs

Les deux premiers certificats sont obligatoires, mais les certificats client uniquement dans le cas l'authenfication par certificat est utilisée. Un autre possibilité existe, basée sur un couple utilisateur/mot de passe.

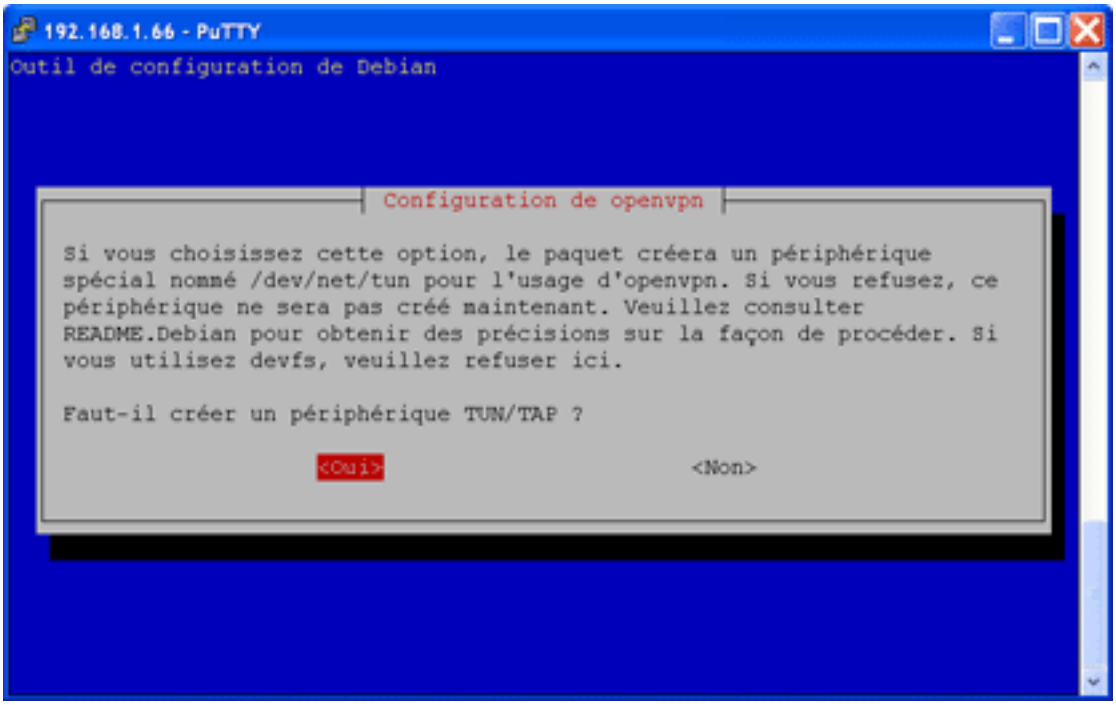
Installation d'OpenVPN

```
aptitude install openvpn
```

Cette commande va lancer le téléchargement des packages OpenVPN sur les repos Debian et la procédure d'installation. Durant celle-ci 2 questions seront posées :

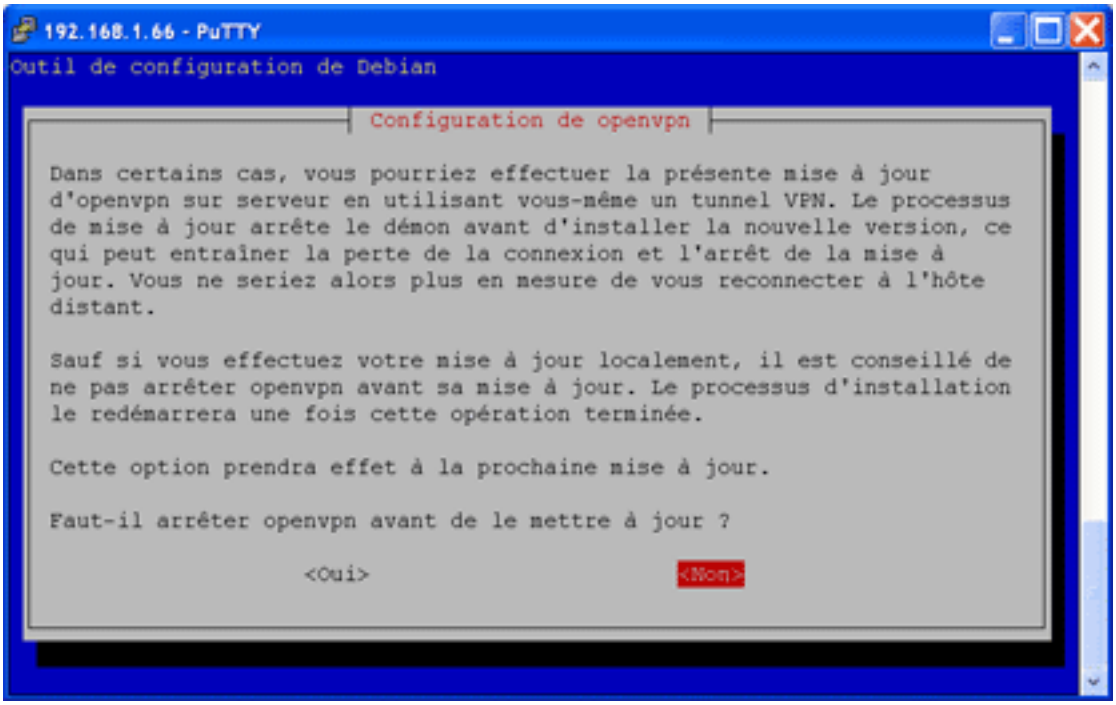
- Faut-il créer une interface tun/tap ? Répondre **Oui**

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.



Installation d'OpenVPN

- Faut-il arrêter OpenVPN avant de le mettre à jour ? **Non**



Installation d'OpenVPN

Sous Debian Etch, l'installation est identique, mis à part qu'aucune question n'est posée.

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

Installation d'OpenSSL

L'installation d'OpenSSL se fait via la commande :

```
aptitude install openssl
```

Génération des certificats

OpenVPN fourni des outils sous formes de scripts shell, qui aident à la génération des différents certificats.

```
cd /usr/share/doc/openvpn/examples/easy-rsa/
```

Décompression du fichier de configuration d'OpenSSL

Tout d'abord, il est nécessaire de décompresser le fichier de configuration d'OpenSSL :

```
gunzip openssl.cnf.gz
```

Edition du fichier vars

Le fichier vars contient divers variables qui seront utilisées dans les scripts. Il est intéressant de prédéfinir certaines d'entres elles afin de ne plus devoir les modifiées durant l'éxécution des scripts, et risquer de faire une faute de frappe.

En effet, ces informations seront communes au différents certificats, et si elles ne l'étaient pas, il y aurait un problème lors de l'authentification voir même durant la génération des certificats.

Je vous conseille d'éditer celles-ci :

```
# 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=BE
export KEY_PROVINCE=Luxembourg
export KEY_CITY=Houffalize
export KEY_ORG="Developpez.com"
export KEY_EMAIL="hikage@hikage.be"
```

Lancer ensuite

```
. ./vars
./clean-all
```

La première ligne va charger les variables du fichier vars précédemment editeurs.

La deuxième va créer les répertoires ou seront stockés les certificats, et dans le cas où ils existent déjà, effacer leur contenu.

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

*L'éxécution de **. ./vars** est importante avant chaque génération de certificats, et doit être obligatoirement éxécuté.*

Generation du certificat racine

```
build-ca
```

Lors de l'exécution de ce script, divers informations vous seront demandées, mais les valeurs par défaut sont celles qui ont été définies dans le fichiers **vars**. Seul le "Common Name" doit etre modifié, par exemple en "vpn-ca".

Il en résulte dans le répertoire *keys* :

- un fichier ca.crt (le certificat root)
- un fichier ca.key (la clé privée correspondante)

Generation du certificat du serveur

```
build-key-server vpn-server
```

Encore une fois, seul le common-name doit etre modifié (exemple : 'vpn-server')

Un mot de passe peut être spécifié, mais n'est pas nécessaire. Par contre, le certificat doit être signé lorsqu'il vous le sera demandé.

```
./build-key-server vpn-server
Generating a 1024 bit RSA private key
..............++++++
.............................++++++
writing new private key to 'vpn-server.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) [BE]:
State or Province Name (full name) [Luxembourg]:
Locality Name (eg, city) [Houffalize]:
Organization Name (eg, company) [Developpez.com]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:vpn-server
Email Address [hikage@hikage.be]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/share/doc/openvpn/examples/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'BE'
stateOrProvinceName   :PRINTABLE:'Luxembourg'
```


Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

```
localityName          :PRINTABLE:'Houffalize'
organizationName      :PRINTABLE:'Developpez.com'
commonName            :PRINTABLE:'vpn-server'
emailAddress          :IA5STRING:'hikage@hikage.be'
Certificate is to be certified until Jun 10 13:57:39 2017 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
```

Il en résulte dans le répertoire keys :

- vpn-server.crt (le certificat serveur)
- vpn-server.key (sa clé privée)
-

Génération d'un certificat client

```
./build-key nomDuClient
```

La génération du certificat client est identique à celle du certificat serveur et il résulte dans le répertoire keys :

- nomDuClient.crt (le certificat client)
- nomDuClient.key (sa clé privée)

```
debian:/usr/share/doc/openvpn/examples/easy-rsa# ./build-key hikage
Generating a 1024 bit RSA private key
.++++++
.......++++++
writing new private key to 'hikage.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) [BE]:
State or Province Name (full name) [Luxembourg]:
Locality Name (eg, city) [Houffalize]:
Organization Name (eg, company) [Developpez.com]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:hikage
Email Address [hikage@hikage.be]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/share/doc/openvpn/examples/easy-rsa/openssl.cnf
```


Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

```
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'BE'
stateOrProvinceName   :PRINTABLE:'Luxembourg'
localityName          :PRINTABLE:'Houffalize'
organizationName      :PRINTABLE:'Developpez.com'
commonName            :PRINTABLE:'hikage'
emailAddress          :IA5STRING:'hikage@hikage.be'
Certificate is to be certified until Jun 10 13:59:28 2017 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
```

Generation de Diffie-Hellman

```
./build-dh
```

La clé **Diffie-Hellman** est utilisée pour permettre à deux client de s'envoyer une clé privée sans risque que celle-ci soit interceptée.

Résumé des fichiers générés

keys/ca.key	Clé privé du certificat racine
keys/ca.crt	Certificat racine
keys/vpn-server.key	Clé privée du certificat serveur
keys/vpn-server.crt	Certificat du serveur
keys/nomDuClient.key	Clé privée de certificat du client NomDuClient
keys/nomDuClient.crt	Certificat du client nomDuClient
keys/dh1024.pem	Clé DH

Création du fichier de configuration

Lors du démarrage du serveur, OpenVPN ira chercher ses fichiers de configuration dans le répertoire **/etc/openvpn**, un fichier **vpn-server.conf** sera créé dans celui-ci.

Les fichiers ca.key, ca.crt, vpn-server.key, vpn-server.crt et dh.key doivent y être copiés aussi.

```
cp /usr/share/doc/openvpn/examples/easy-rsa/keys/ca.key /etc/openvpn
cp /usr/share/doc/openvpn/examples/easy-rsa/keys/ca.crt /etc/openvpn
cp /usr/share/doc/openvpn/examples/easy-rsa/keys/vpn-server.key /etc/openvpn
cp /usr/share/doc/openvpn/examples/easy-rsa/keys/vpn-server.crt /etc/openvpn
cp /usr/share/doc/openvpn/examples/easy-rsa/keys/dh1024.pem /etc/openvpn
```

Voici un exemple de fichier de configuration

```
port 1194
proto udp
```


Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

```
dev tun

ca ca.crt
cert vpn-server.crt
key vpn-server.key
dh dh1024.pem

server 10.250.250.0 255.255.255.0
ifconfig-pool-persist persist-ip.txt


client-to-client

keepalive 10 120

# comp-lzo

user nobody
group nobody

status vpn-server.log
log openvpn.log

verb 3

mute 20
```

Détaillons ce fichier de configuration :

Ligne	Description
port 1194	spécifie le port sur lequel ecoute OpenVPN, 1194 est le port attribué officiellement à OpenVPN
proto udp	spécifie le mode de communication, *udp* ou *tcp*. UDP est plus performant.
dev tun	spécifie le type d'interface à utiliser, soit *tap* soit *tun*, dans notre type de configuration utilisé le tun
ca ca.crt	spécifie le chemin vers le certificat racine, celui qui a ete généré.
cert vpn-server.crt	Spécifie le chemin vers le certificat du serveur
key vpn-server.key	Spécifie le chemin vers la clé privée associé au certificat serveur
dh dh1024.pem	Spécifie le chemin de la clé Diffie Helman
server 10.250.250.1 255.255.255.0	Spécifie le sous réseau qui sera utilisé dans le VPN, le serveur aura la premiere IP de celui-ci (ici : 10.250.250.1)
ifconfig-pool-persist persist-ip.txt	spécifie un fichier dans lequel sera stocké les couples "utilisateur" => ip. Cela permettra au utilisateurs de garder la même adresse ip dans le VPN à chaque connection.
client-to-client	permet au client de se voir entre eux
keepalive 10 120	specifie a OpenVPN de faire un "ping" toutes les 10 secondes vers les clients, et si un de ceux ci ne réponds pas dans les 120 secondes, il est considéré comme déconnecté.

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

user nobody	Spécifie le nom de l'utilisateur sous lequel OpenVpn sera exécuté
group nobody	Spécifie le nom de l'utilisateur sous lequel OpenVpn sera exécuté
status vpn-server.log	spécifie un fichier dans lequel le status du serveur sera visible
log /var/log/openvpn.log	spécifie un fichier de log pour OpenVPN
verb 3	spécifie le niveau d'information pour le fichier de log.
mute 20	permet de ne garder qu'une seule ligne sur 20 si ces 20 ligne sont identiques.

comp lzo *permet d'activer la compression du flux, en effet le chiffrement des données augmente sensiblement la taille des données échangés, et le fait de compresser permet de limiter cette augmentation.*

Mais pour pouvoir utilser la compression lzo, il faut que le module soit installer sur le système, et cela est faisable via ***aptitude install liblzo1***

Lancement du serveur

Le lancement du serveur se fait via la commande **/etc/init.d/openvpn start**

III-B-2 - Installation du client sous linux

L'installation du client sous linux ne diffère pas en réalité de l'installation du serveur.

L'exécutable OpenVPN est à la fois le serveur et le client en un seul et même exécutable, la différence se fait via le fichier de configuration.

Il est nécessaire de récupérer le certificat racine (ca.crt) ainsi que le certificat et la clé propre au client.

Fichier de configuration du client

```
client

proto udp
dev tun
remote vpn.developpez.com 1194

ca ca.crt
cert nomDuClient.crt
key nomDuClient.key



persist-key
persist-tun



keepalive 10 120

# comp-lzo

user nobody
```


Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

Fichier de configuration du client
```
group nobody

status vpn-server.log
log /var/log/openvpn.log

verb 3

mute 20
```

Comme on peut le voir, le fichier est fort semblable à celui du serveur, hormis :

Ligne de configuration	Description
client	Spécifie le mode client et non serveur
cert client.crt	Pointe vers le certificat du client
key client.key	Pointe vers la clé privée du client
remote vpn.developpez.com 1194	Specifie le nom ou l'ip publique (et non celle dans le vpn) du serveur VPN, ainsi que le port d'écoute de celui-ci

Lancement du client

Le lancement du client se fait aussi via la commande **/etc/init.d/openvpn start**

III-B-3 - Installation du client sous windows

S'il est possible d'utiliser le client Win32 fournit directement par OpenVPN, il existe un outil graphique plus pratique sous Windows : OpenVPN-GUI.

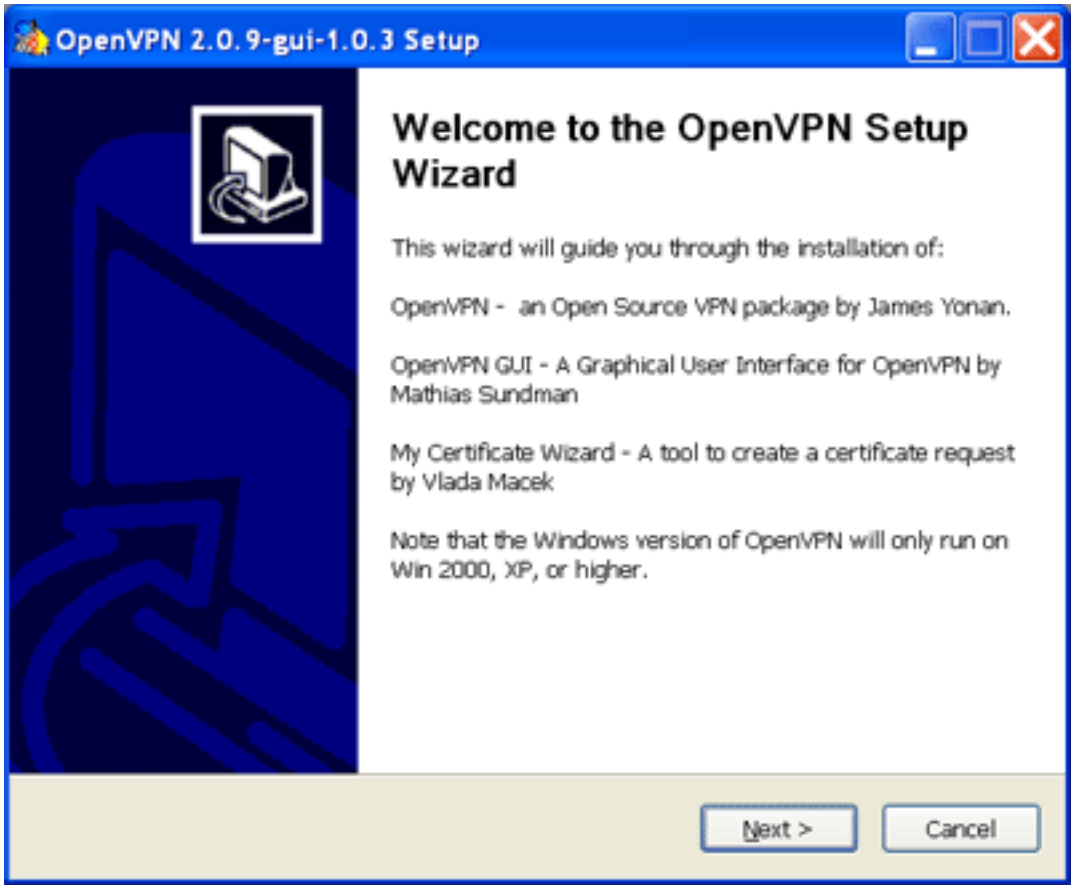
Il est disponible ici : **http://openvpn.se/**

N'ayant pas de Windows Vista, je n'ai pas pu réaliser de test sous ce dernier. Sous Windows XP l'installation ne pose aucun problème.

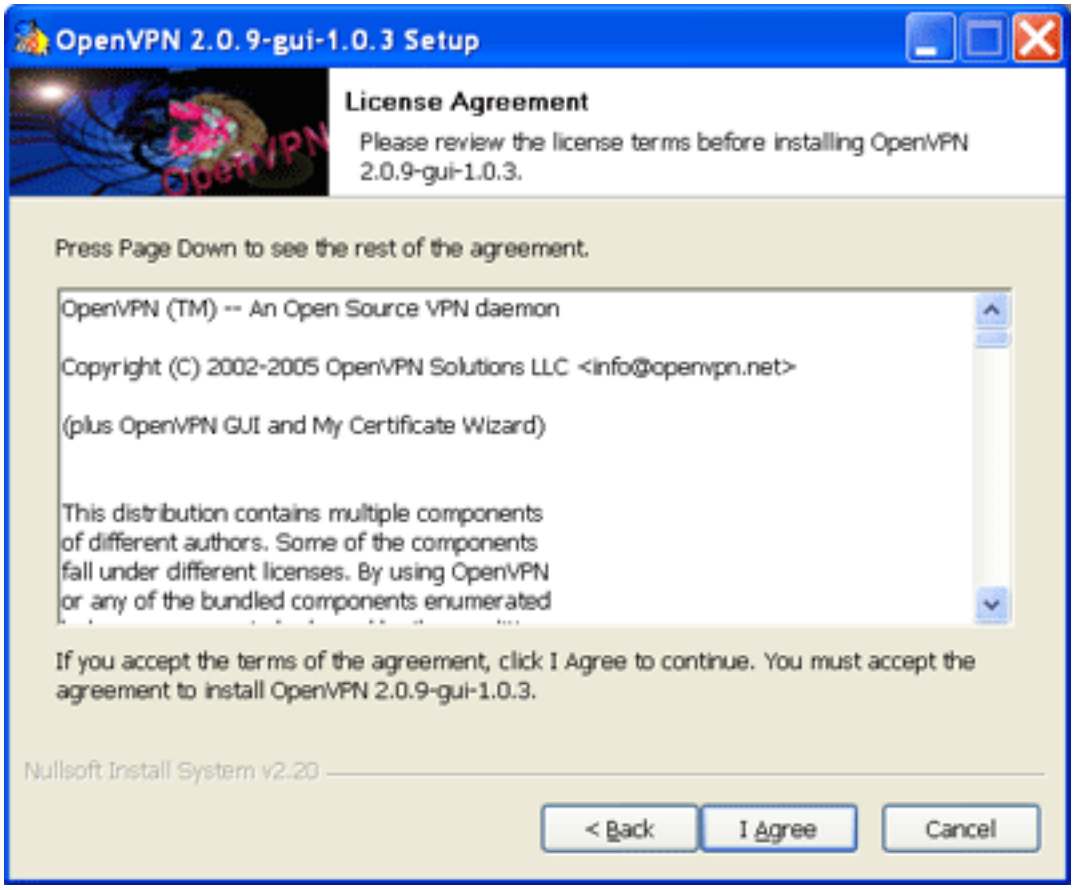
Installation

Il suffit de lancer le programme d'installation et de suivre les étapes :

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

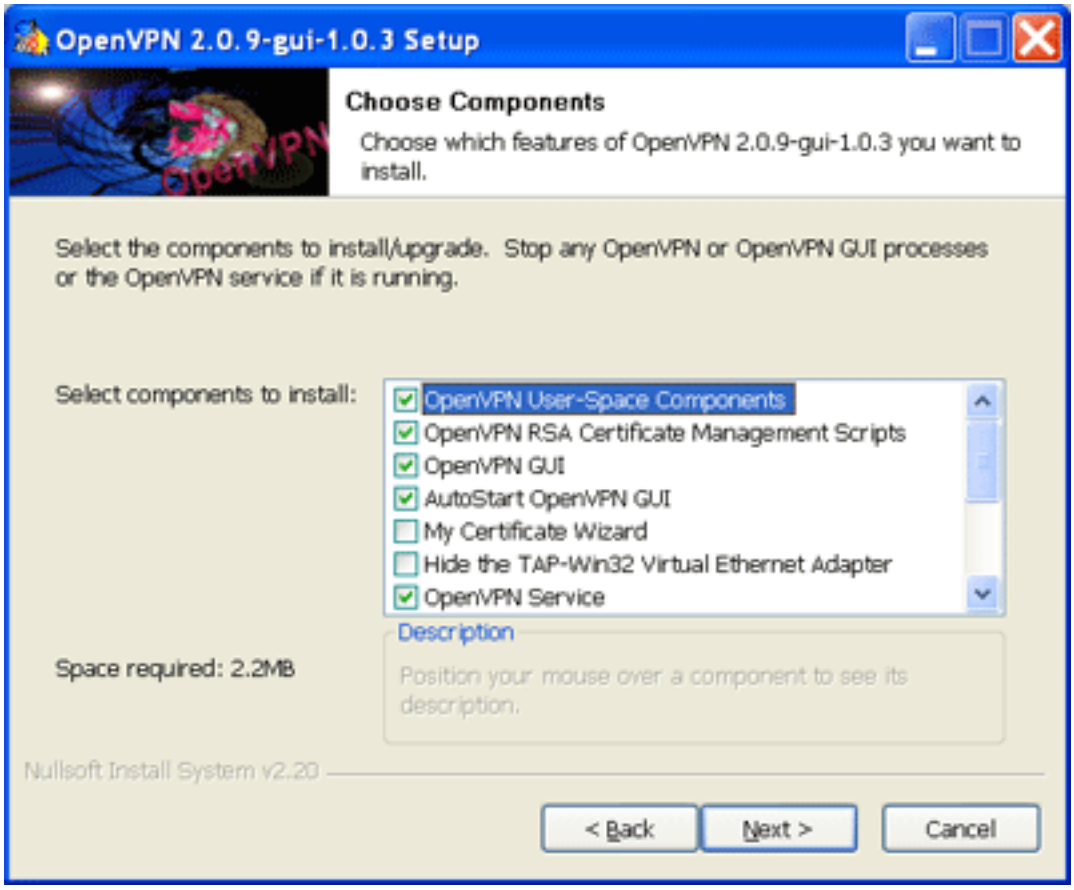


Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

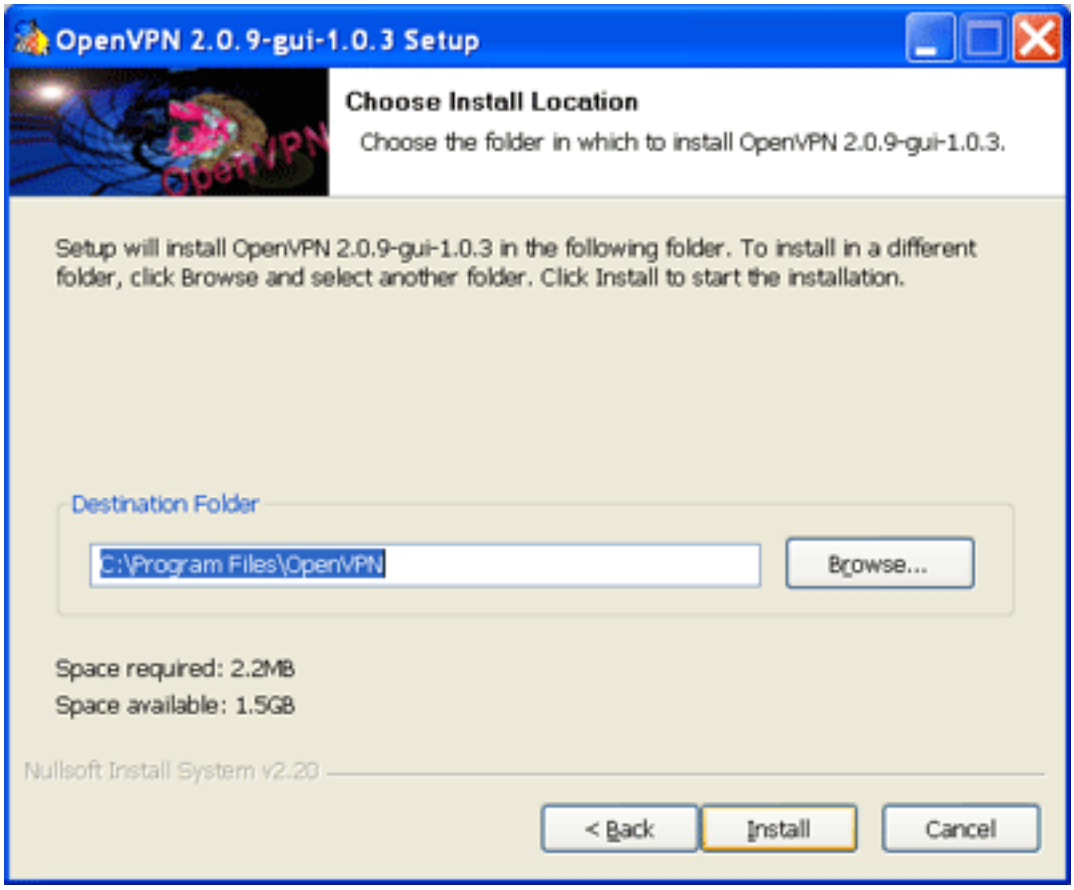


Laissez les valeurs par défaut lors du choix des options :

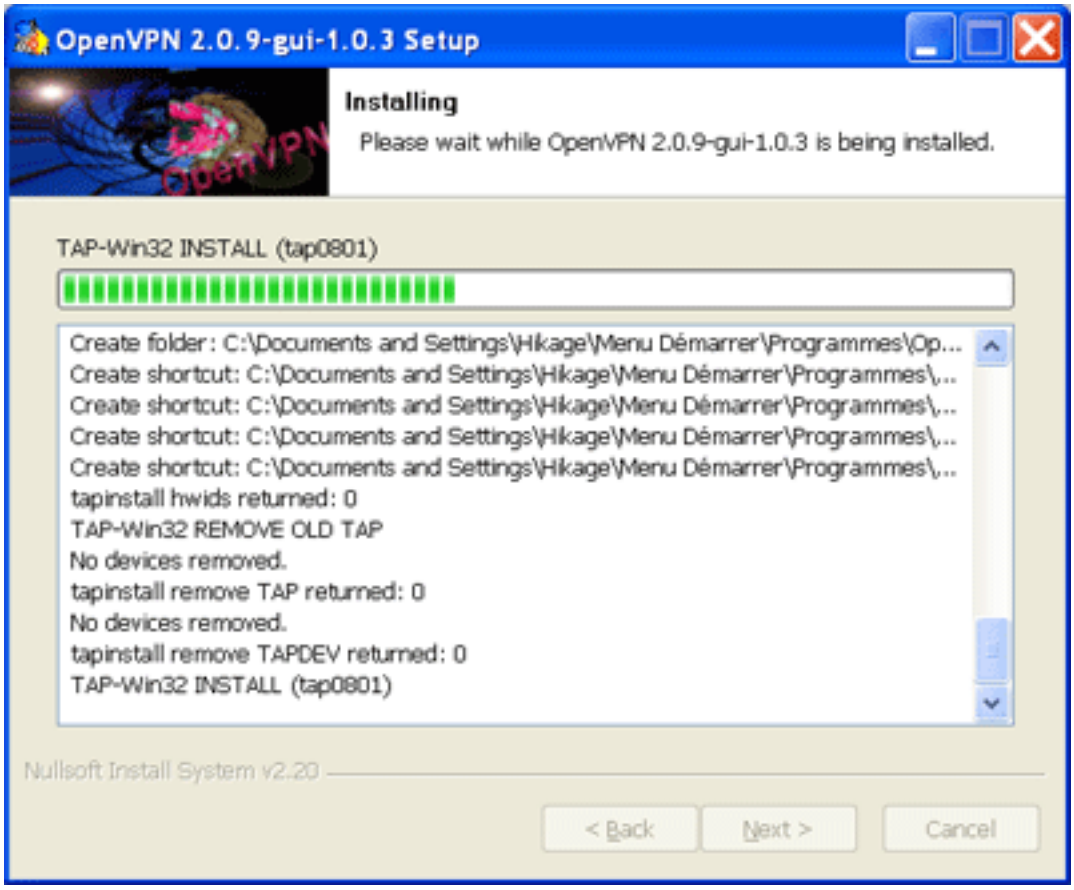
Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.



Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

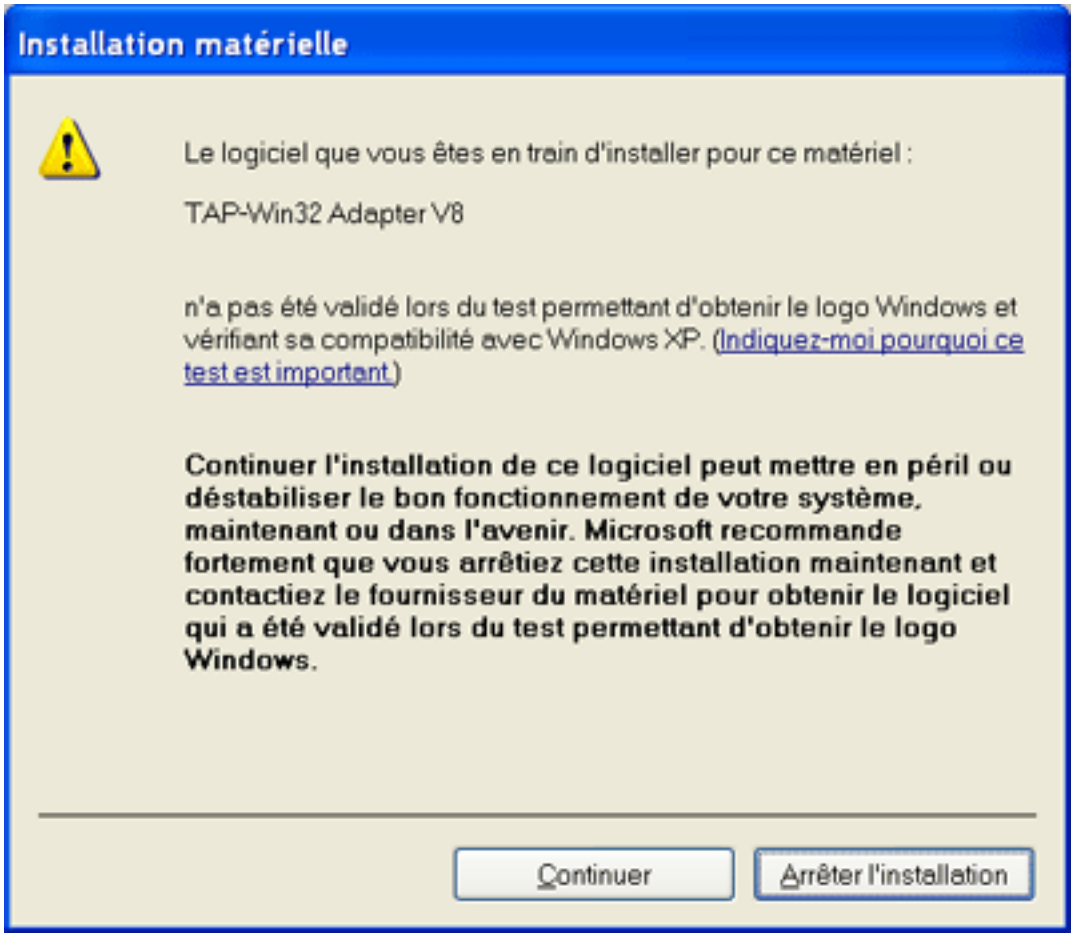


Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

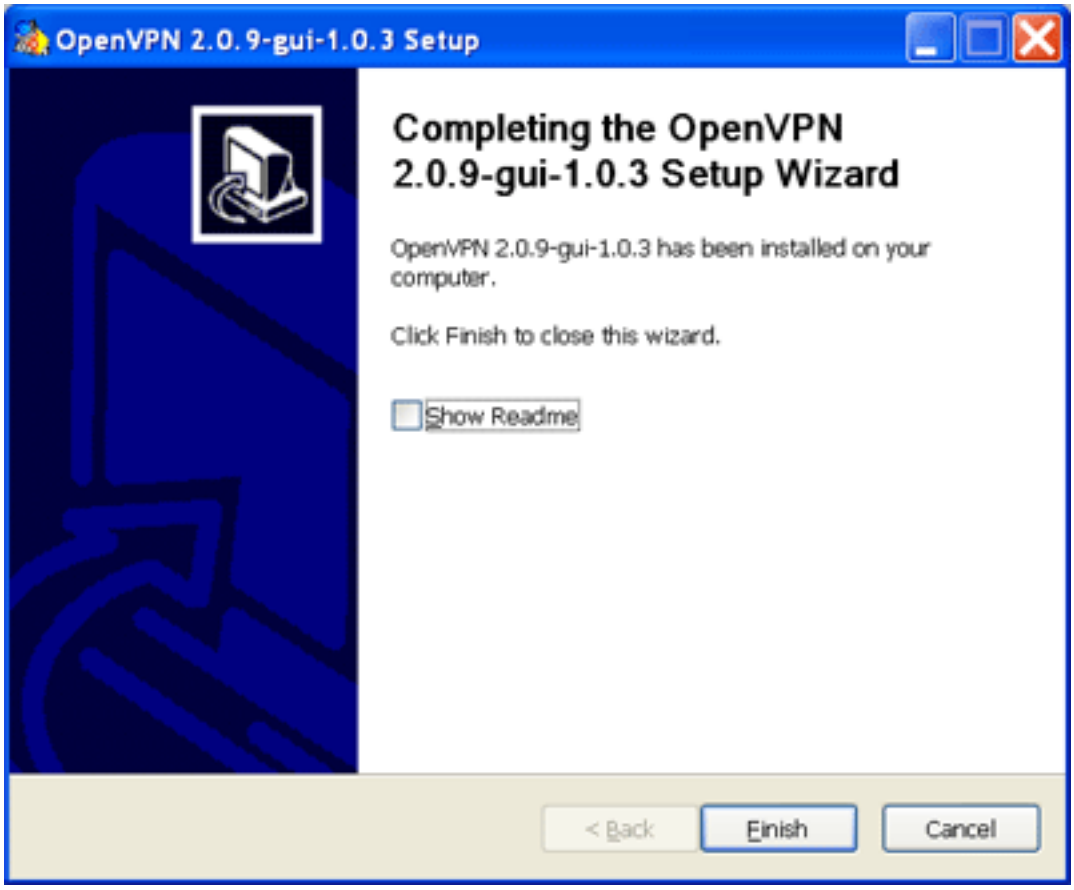


Un message d'avertissement sera affiché lors de l'installation du pilotes de la carte réseau virtuelle nécessaire à OpenVPN du au fait qu'elle n'est pas officiellement reconnue comme compatible, mais elle ne pose aucun problème sous windows XP.

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.



Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.



Si tout va bien, une icone devrait apparaitre dans la barre des taches :



Configuration

Tout comme sous linux, il sera nécessaire de récupérer le certificat racine (**ca.crt**), la clé du client (**nomDuClient.key**), le certificat du client (**nomDuClient.crt**) ainsi qu'un fichier de configuration.

Le fichier de configuration est identique à celui du client Linux, à quelques différences près :

- **user** et **group** ne sont pas possible sous windows, et doivent etre retiré
- **log** n'est pas pris en compte par OpenVPN gui, qui possède sont propre fichier de log
- L'extention du fichier doit etre **.ovpn**

En pratique le fichier de configuration ressemble à ceci :

Fichier de configuration du client Windows

```
client

proto udp
```


Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

Fichier de configuration du client Windows

```
dev tun
remote 192.168.25.128 1194

ca ca.crt
cert nomDuClient.crt
key nomDuClient.key



persist-key
persist-tun



keepalive 10 120

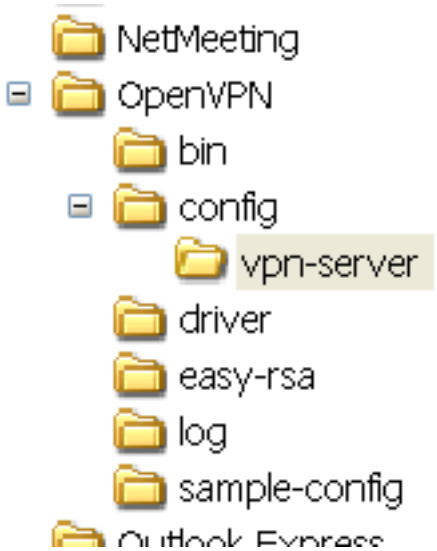
# comp-lzo


verb 3

mute 20
```

Les fichiers de configuration ainsi que les clés sont à placer dans le répertoire OPENVPN_DIR/config, ou OPENVPN_DIR est le répertoire choisi lors de l'installation.

Même si il est tout à fait possible de mettre tout directement dans ce répertoire, je conseille de créer un sous répertoire par connection. En effet, il est tout à fait possible d'etre connecté à plusieurs serveur OpenVPN en même temps, et pour ne pas confondre les fichiers de configuration et les clées de chaque connection, il est plus clair de créer un sous répertoire par connection :

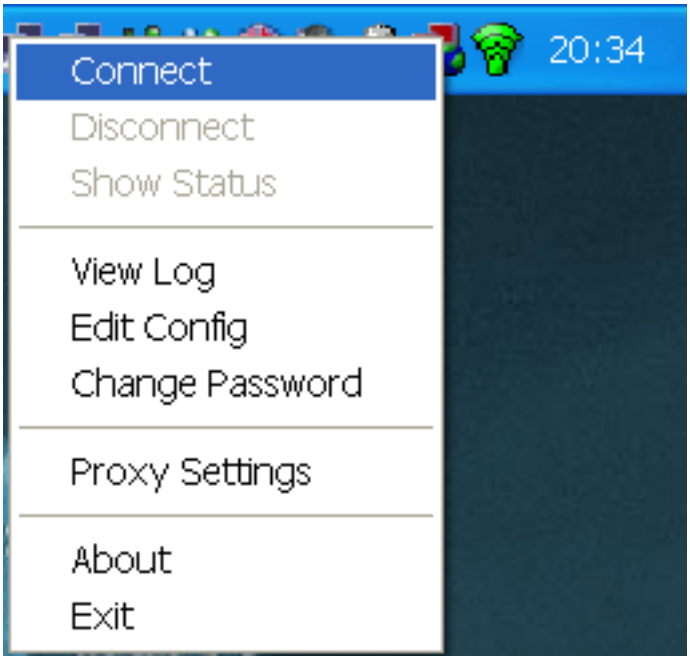


Répertoire de configuration

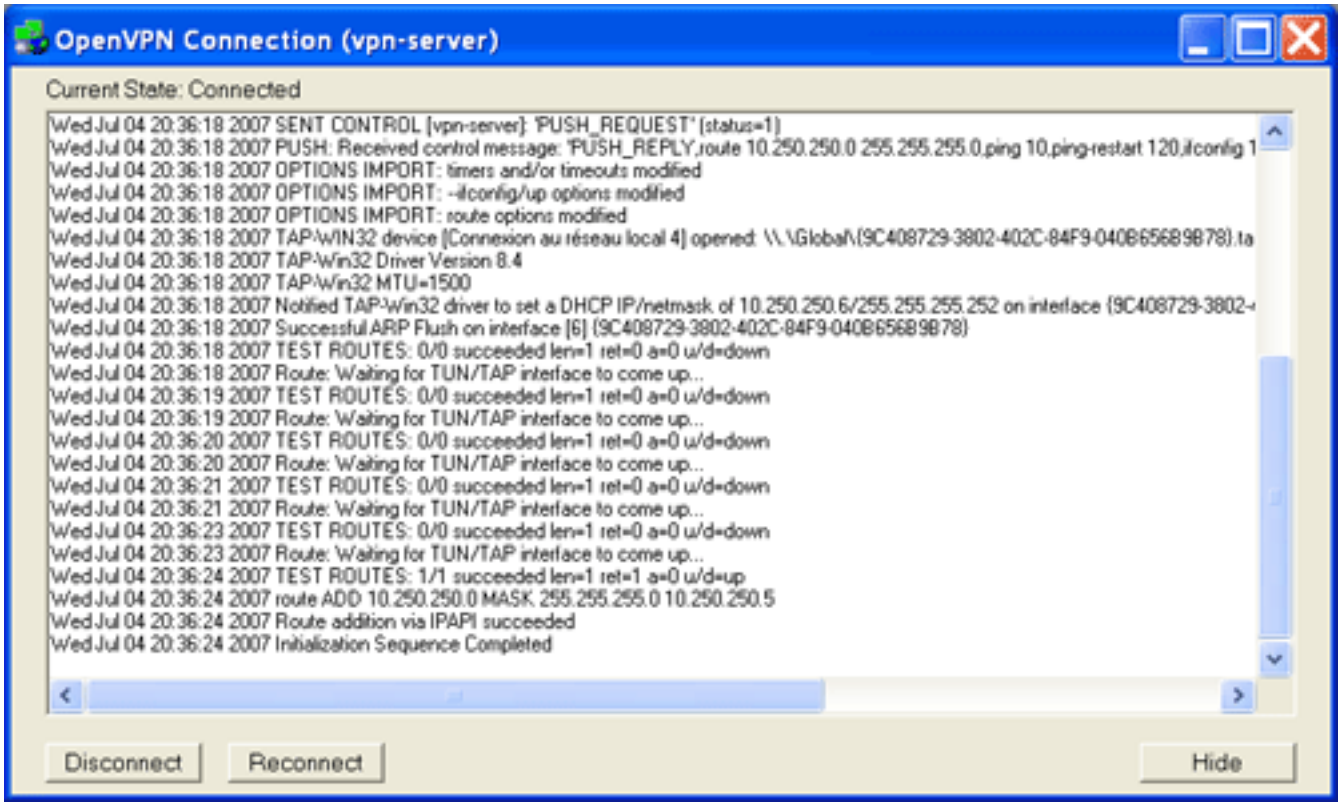
Connection

Dès que le fichier de configuration est placé dans le répertoire, un menu apparait lors d'un click droit sur l'icone de OpenVPN-Gui :

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.



Et miracle, si tout est bien fait, voici ce qui se passe lorsque l'on sélectionne "Connect" :



III-B-4 - Installation du client sous Mac OS X

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.

Ce document est issu de http://www.developpez.com et reste la propriété exclusive de son auteur. La copie, modification et/ou distribution par quelque moyen que ce soit est soumise à l'obtention préalable de l'autorisation de l'auteur.