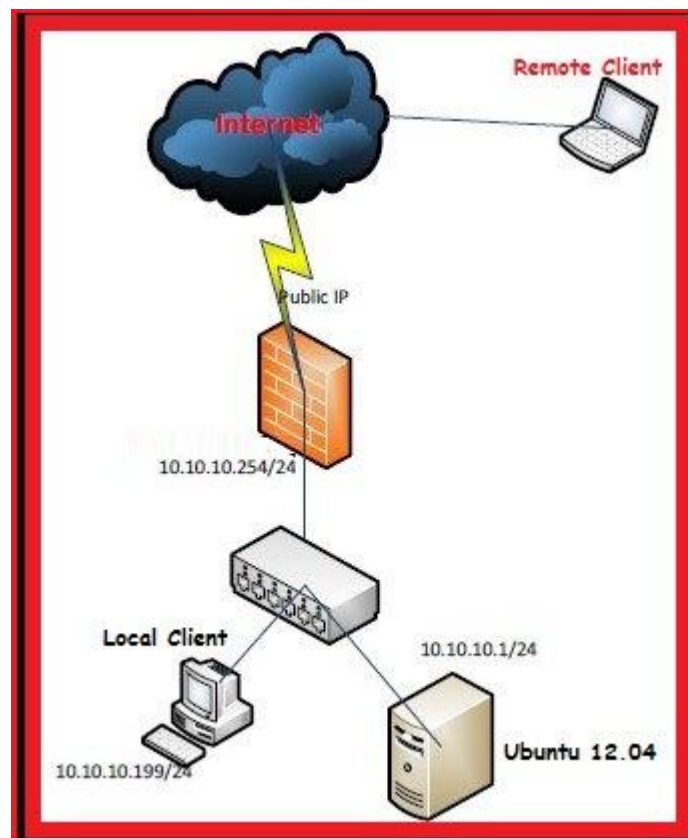


INSTALLATION D'UN SERVEUR OPENVPN & CONFIGURATION D'UN CLIENT

http://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel

<http://www.commentcamarche.net/contents/initiation/vpn.php3>

Le VPN permet a un utilisateur de se connecter avec une connexion Internet sur le réseau local de l'Entreprise via un tunnel sécurisé créé par le VPN.



I) Installation de l'OpenVPN

```
# apt-get install openvpn
```

II) Configuration de l'OpenVPN

II-A) Préparation de Clés et Certificats

Nous allons copier les scripts par défaut de « easy-rsa » dans « /etc/openvpn/easy-rsa ».

Ce sont des scripts qui vont nous aider à configurer les Certificats d'Autorité (CA : Certificate Authority), Certificats (Certificates) et générer les clés (Keys) pour le Serveurs et les Clients.

```
# cd /etc/openvpn/
```

```
# mkdir easy-rsa
```

```
# cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
```

On va éditer le fichier « /etc/openvpn/easy-rsa/vars »

```
# cd easy-rsa/
```

```
# emacs vars &
```

Nous allons modifier les paramètres d'informations qui seront alors pré-définis quand nous lancerons le script « build-ca »

```
export KEY_COUNTRY="FR"
```

```
export KEY_PROVINCE="IDF"
```

```
export KEY_CITY="Paris"
```

```
export KEY_ORG="OCI"
```

```
export KEY_EMAIL="sylvain@free.fr"
```

On va indiquer que nous allons utiliser le fichier « /etc/openvpn/easy-rsa/vars » comme fichier référant pour nos scripts.

```
# source vars
```

```
# ./clean-all
```

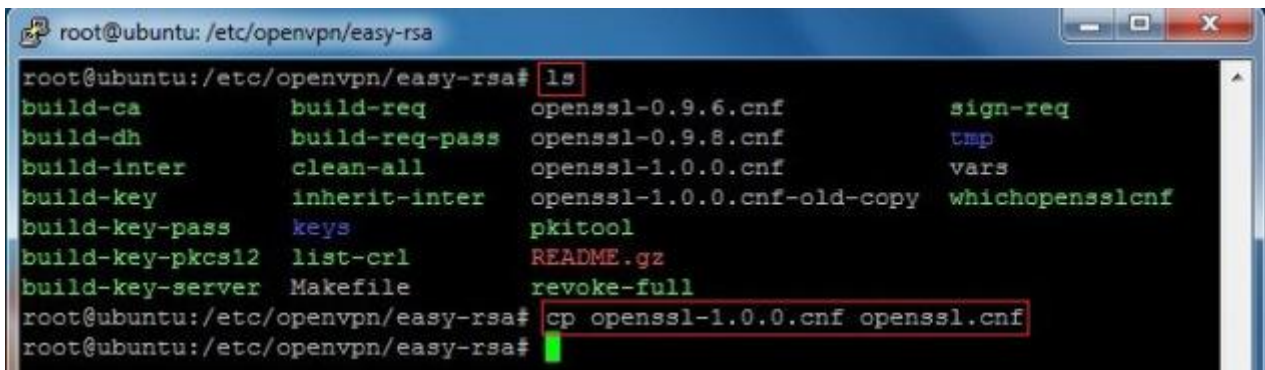
Le script de création de clés va utiliser le protocole SSL, pour cela nous allons lui en déclarer un.

Listez le répertoire « /etc/openvpn/easy-rsa/ » (Sachant qu'à l'étape précédente, nous nous étions mis dans le bon répertoire, si vous avez un doute, tapez la commande « pwd »).

Et ensuite copiez la dernière version du fichier de configuration « openssl-x.x.x.cnf » en « openssl.cnf ».

```
# ls
```

```
# cp openssl-1.0.0.cnf openssl.cnf
```



```
root@ubuntu: /etc/openvpn/easy-rsa# ls
build-ca          build-req          openssl-0.9.6.cnf    sign-req
build-dh          build-req-pass     openssl-0.9.8.cnf    tmp
build-inter       clean-all         openssl-1.0.0.cnf    vars
build-key         inherit-inter     openssl-1.0.0.cnf-old-copy  whichopensslcnf
build-key-pass    keys              pkitool
build-key-pkcs12  list-crl          README.gz
build-key-server  Makefile          revoke-full
root@ubuntu: /etc/openvpn/easy-rsa# cp openssl-1.0.0.cnf openssl.cnf
root@ubuntu: /etc/openvpn/easy-rsa#
```

II-A-1) Création du Certificat d'Autorité

```
# ./build-ca
```

Vous allez voir les paramètres que nous avons configuré dans le fichier « /etc/openvpn/easy-rsa/vars ».

Si les paramètres par-défaut sont bons, cliquez juste sur « Entrée » pour valider sinon modifier en direct et cliquez sur « Entrée ».

Dans le cas où vous avez vu une erreur, modifiez le fichier « /etc/openvpn/easy-rsa/vars » et relancer les commandes « source vars » et « ./clean-all ».

```
root@ubuntu: /etc/openvpn/easy-rsa
root@ubuntu:/etc/openvpn/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) [PK]:
State or Province Name (full name) [Punjab]:
Locality Name (eg, city) [Lahore]:
Organization Name (eg, company) [Tendo Pvt Ltd]:
Organizational Unit Name (eg, section) [changeme]:IT Dept.
Common Name (eg, your name or your server's hostname) [changeme]:Arbab
Name [changeme]:Arbab
Email Address [arbab.nazar@tendo.org]:
root@ubuntu:/etc/openvpn/easy-rsa#
```

II-A-2) Création de la Clé pour le Serveur

Nous allons générer une clé pour le Serveur Open VPN, ici notre serveur s'appelle « tendo »

./build-key-server tendo

Pareil, cliquez sur « Entrée » jusqu'à la question « Sign the certificate » et tapez « y » et « y » pour la question suivante (« Commit » = « Appliquer »).

```
root@ubuntu: /etc/openvpn/easy-rsa
root@ubuntu:/etc/openvpn/easy-rsa# ./build-key-server tendo
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'tendo.key'
-----
Country Name (2 letter code) [PK]:
State or Province Name (full name) [Punjab]:
Locality Name (eg, city) [Lahore]:
Organization Name (eg, company) [Tendo Pvt Ltd]:
Organizational Unit Name (eg, section) [changeme]:IT Dept
Common Name (eg, your name or your server's hostname) [tendo]:
Name [changeme]:Arbab
Email Address [arbab.nazar@tendo.org]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
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:'PK'
stateOrProvinceName  :PRINTABLE:'Punjab'
localityName         :PRINTABLE:'Lahore'
organizationName     :PRINTABLE:'Tendo Pvt Ltd'
organizationalUnitName:PRINTABLE:'IT Dept'
commonName           :PRINTABLE:'tendo'
name                 :PRINTABLE:'Arbab'
emailAddress         :IA5STRING:'arbab.nazar@tendo.org'
Certificate is to be certified until Dec  9 11:26:18 2022 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
root@ubuntu:/etc/openvpn/easy-rsa#
```

II-A-3) Création de la Clé Diffie-Hellman

Nous allons configurer l'échange de clés Diffie-Hellman

http://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

```
# ./build-dh
```

Nous allons copier les clés qui nous intéressent dans « /etc/openvpn »

```
# cd keys/
```

```
# cp ca.crt tendo.crt tendo.key dh1024.pem /etc/openvpn/
```

II-B) Configuration du Serveur (fichier « /etc/openvpn/server.conf »)

Nous allons prendre un template et le modifier.

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

```
# gzip -d /etc/openvpn/server.conf.gz
```

Editez le fichier « /etc/openvpn/server.conf ».

Voici un exemple de fichier « server.conf », juste modifier la ligne « push route » qui est votre réseau local.

```
port 1194
proto udp
dev tun
ca ca.crt
cert tendo.crt
key tendo.key # This file should be kept secret
dh dh1024.pem
```

```
#VPN subnet for OpenVPN to draw client addresses from.
server 172.16.10.0 255.255.255.0
ifconfig-pool-persist ipp.txt
```

```
#Push routes to the client to allow it to reach other
#private subnets behind the server.
push "route 10.10.10.0 255.255.255.0"
```

```
#If you want that all of your Internet traffic pass
#through the VPN server then enable this
push "redirect-gateway def1 bypass-dhcp"
```

```
# For name resolution, enable this
;push "dhcp-option DNS 10.10.10.254"
```

```
client-to-client
keepalive 10 120
comp-lzo
max-clients 10
persist-key
persist-tun
status openvpn-status.log
verb 3
mute 20
```

Démarrer le service « openvpn ».

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


II-C) Création des Clés pour le(s) Client(s)

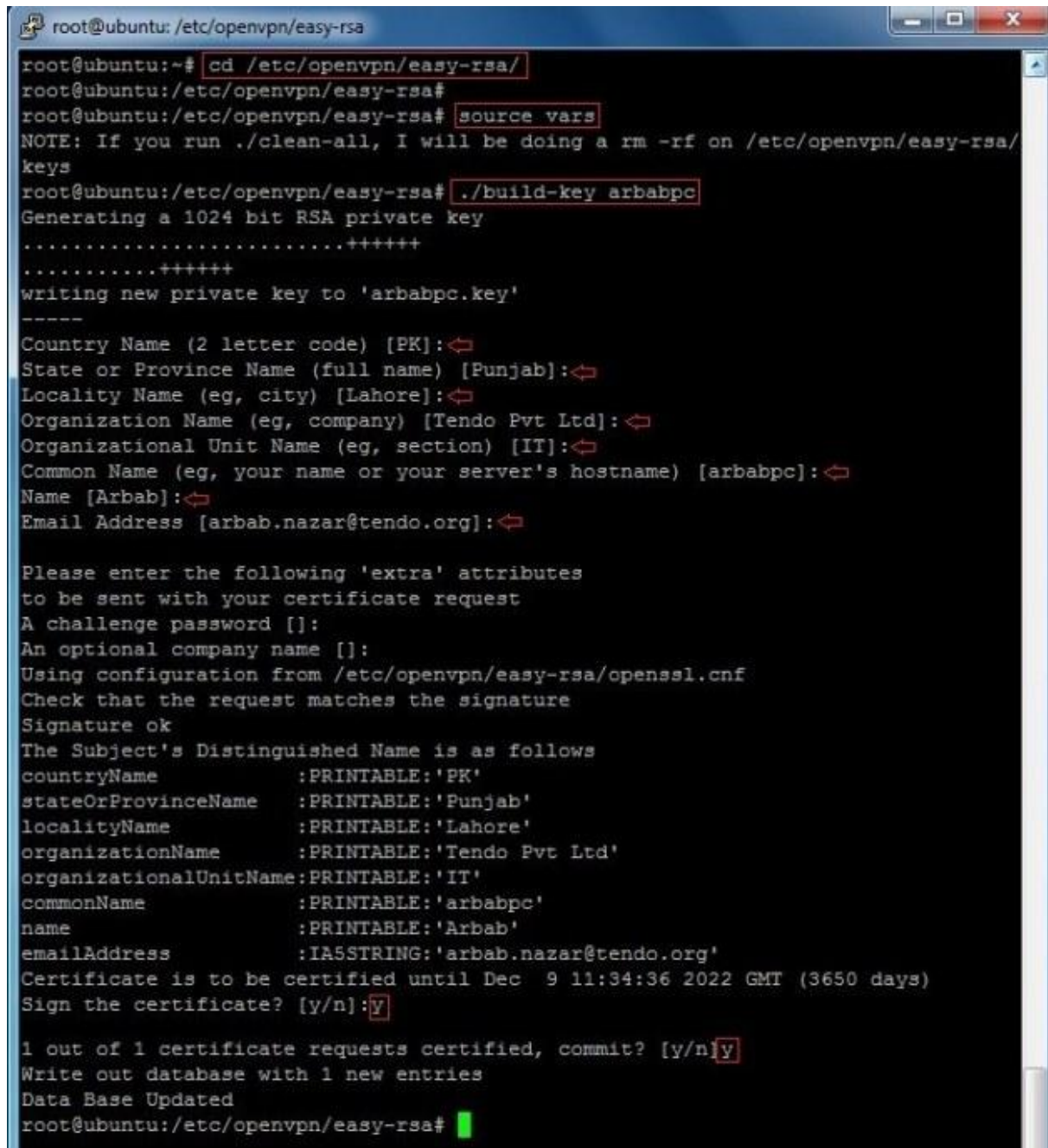
Ici nous allons créer une clé pour « arababpc ». C'est un nom qui n'a aucune relation avec le « hostname » du PC ni de relation avec le « login » de l'utilisateur.

Mais la logique serait de mettre comme nom, à la place de « arababpc », un « login » qui sera plus parlant.

```
# cd /etc/openvpn/easy-rsa/
```

```
# source vars
```

```
# ./build-key arababpc
```



```
root@ubuntu: /etc/openvpn/easy-rsa
root@ubuntu:~# cd /etc/openvpn/easy-rsa/
root@ubuntu:/etc/openvpn/easy-rsa#
root@ubuntu:/etc/openvpn/easy-rsa# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/
keys
root@ubuntu:/etc/openvpn/easy-rsa# ./build-key arababpc
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'arababpc.key'
-----
Country Name (2 letter code) [PK]:
State or Province Name (full name) [Punjab]:
Locality Name (eg, city) [Lahore]:
Organization Name (eg, company) [Tendo Pvt Ltd]:
Organizational Unit Name (eg, section) [IT]:
Common Name (eg, your name or your server's hostname) [arababpc]:
Name [Arbab]:
Email Address [arbab.nazar@tendo.org]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
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:'PK'
stateOrProvinceName  :PRINTABLE:'Punjab'
localityName         :PRINTABLE:'Lahore'
organizationName     :PRINTABLE:'Tendo Pvt Ltd'
organizationalUnitName:PRINTABLE:'IT'
commonName           :PRINTABLE:'arababpc'
name                 :PRINTABLE:'Arbab'
emailAddress         :IA5STRING:'arbab.nazar@tendo.org'
Certificate is to be certified until Dec  9 11:34:36 2022 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
root@ubuntu:/etc/openvpn/easy-rsa#
```

Cette opération est à faire pour chaque utilisateur.

Pour recréer, une clé pour un autre utilisateur, relancer les commandes qui suit :

```
# source vars
```

```
# ./build-key Julien
```

III) Routage entre le Réseau VPN et le Réseau Local

Afin que les clients VPN qui seront sur le réseau 172.16.0.0 / 24 puissent communiquer avec le réseau de local 10.10.10.0 / 24, en théorie, dans le fichier « /etc/openvpn/server.conf », la ligne « push "route 10.10.10.0 255.255.255.0" » devrait le faire. Faites un essai de connexion comme indiqué dans le chapitre suivant « IV) Clients VPN ».

Si vous n'arrivez pas faire de « ping » sur le réseau local, vous pouvez faire ce qui suit :

Méthode 1 : Modifier les fichiers de démarrage

Editez le fichier « **/etc/sysctl.conf** » et dé-commentez la ligne « **net.ipv4.ip_forward=1** ».
Puis éditez le fichier « **/etc/rc.local** » et rajouter les 2 lignes qui suivent, avant la dernière ligne « **exit 0** »
iptables -A FORWARD -j ACCEPT
iptables -t nat -A POSTROUTING -s 172.16.10.0/24 -o eth0 -j MASQUERADE

Méthode 2 : Script à charger au démarrage

```
# cd /etc/init.d/  
# touch route_vpn  
# chmod 755 route_vpn  
# emacs route_vpn &
```

Mettre les lignes suivantes :

```
#!/bin/bash  
echo 1 > /proc/sys/net/ipv4/ip_forward  
iptables -A FORWARD -j ACCEPT  
iptables -t nat -A POSTROUTING -s 172.16.10.0/24 -o eth0 -j MASQUERADE
```

```
#!/route_VPN  
# update-rc.d route_VPN defaults
```

IV) Clients VPN

III-A) Clients Ubuntu

Sur les postes clients, il faut installer « **openvpn** » et créer un fichier de profil de connexion avec l'extension « **.ovpn** » qui sera tout aussi compatible pour les clients Windows.

Il vous faut copier les fichiers « **tendo.crt** », « **arbabpc.crt** » et « **arbabpc.key** » qui sont sur le serveur dans « **/etc/openvpn/easy-rsa/keys** » sur le(s) poste(s) client(s) dans « **/etc/openvpn** » par-exemple.

```
# apt-get install openvpn
```

```
# cd /etc/openvpn  
# emacs client.ovpn
```

Mettez ce qui suit :

```
# Client  
client  
dev tun  
proto tcp-client  
remote 10.10.10.1 1194      # @ IP du Serveur + Port de connexion  
resolv-retry infinite  
cipher AES-256-CBC
```

```
# Cles et Certificats  
ca tendo.crt              # CA du Serveur  
cert arababpc.crt         # CA du client  
key arababpc.key          # Clé du client  
tls-auth ta.key 1
```

```
# Securite  
nobind  
persist-key  
persist-tun  
comp-lzo  
verb 3
```

Pour se connecter avec le VPN, il faut taper la commande suivante :
openvpn client.ovpn

IV-B) Clients Microsoft

Il y a 2 logiciels VPN Clients pour Windows « OpenVPN Client » et « Securepoint »

IV-B-1) « Open VPN Client »

Vous pourrez trouver le logiciel sur le lien suivant :

<http://openvpn.net/index.php/open-source/downloads.html>

Une fois le logiciel téléchargé puis installé. Il vous faut copier les fichiers « **tendo.crt** », « **arbabpc.crt** » et « **arbabpc.key** » sur dans le répertoire où vous avez installé « OpenVPN ».

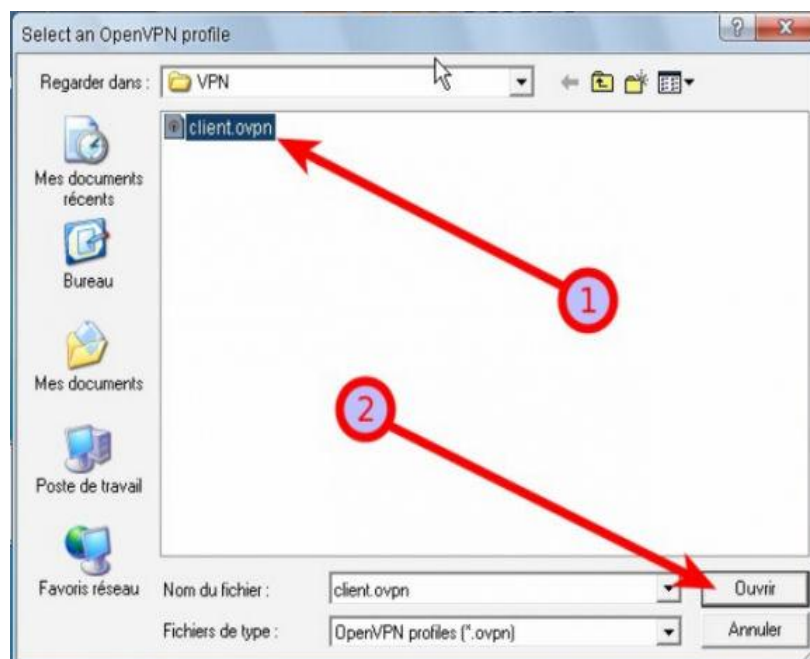
Ensuite, il suffit de cliquer sur le nouvel icône dans la barre des tâches. La fenêtre suivante devrait apparaître. Il faut alors cliquer sur le bouton « + » pour ajouter une nouvelle connexion VPN.



Ensuite on sélectionne l'option d'importation locale (1) et on clique sur Import (2)



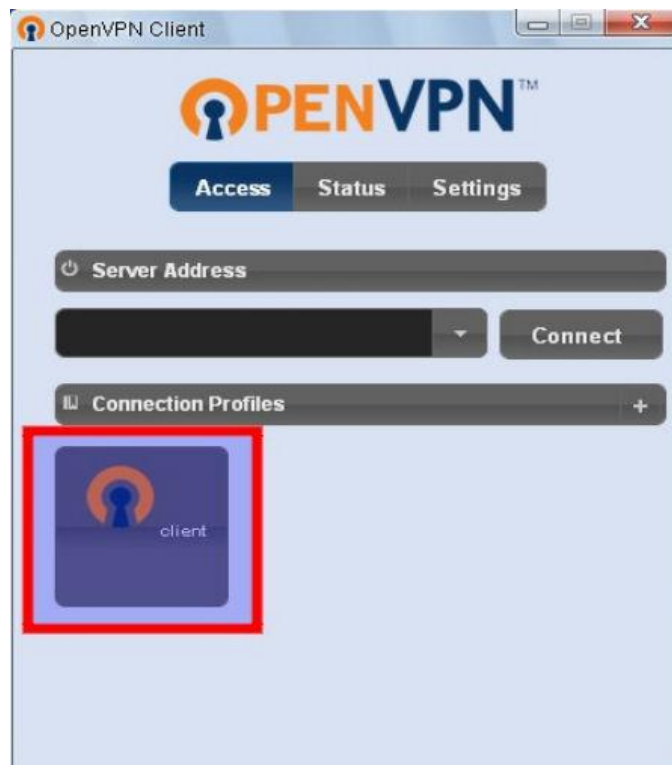
On sélectionne ensuite le fichier « client.ovpn » que vous avez récupéré du Serveur.



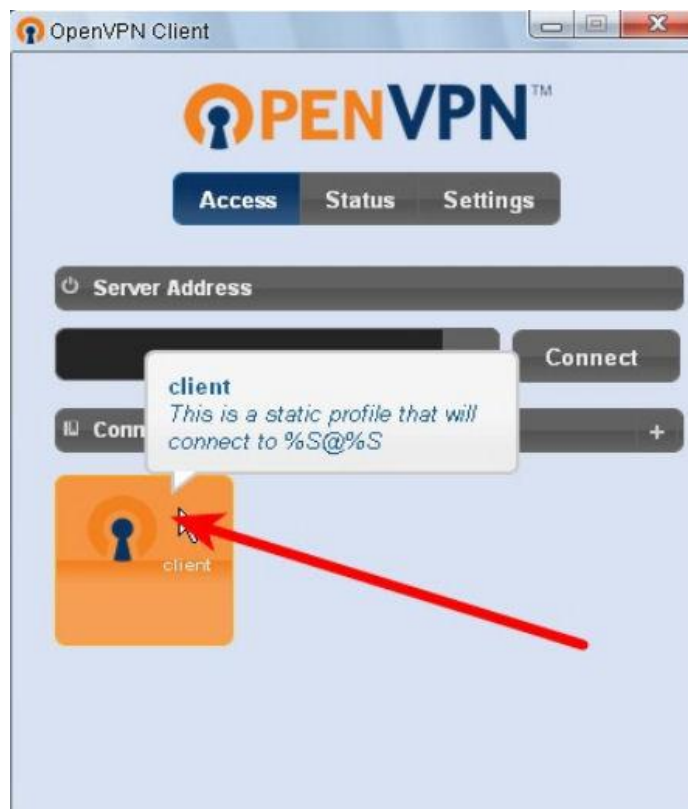
On sauvegarde la configuration



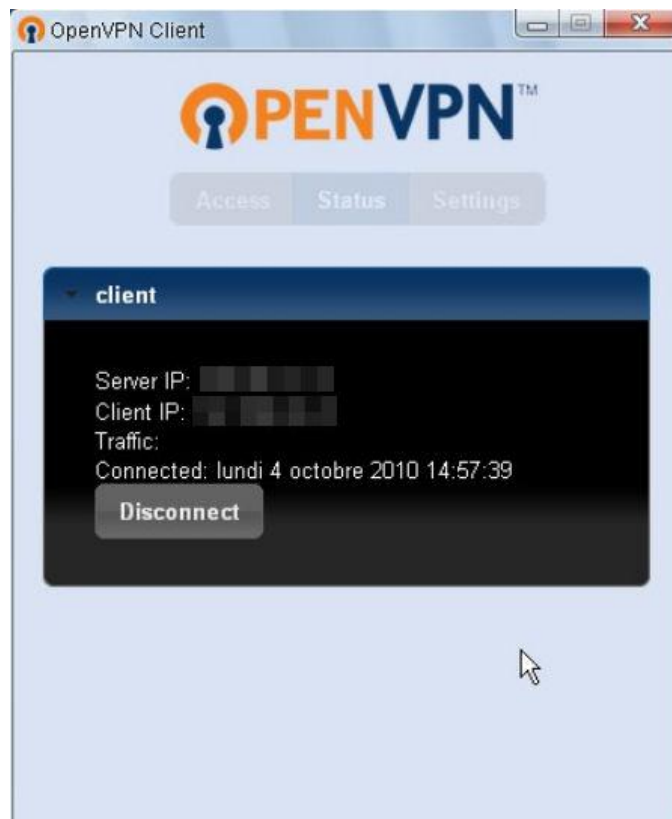
La nouvelle connexion VPN devrait apparaître dans la fenêtre principale



Lancez la connexion « client » que vous venez de configurer



Une fois la connexion établie, on a le message suivant :

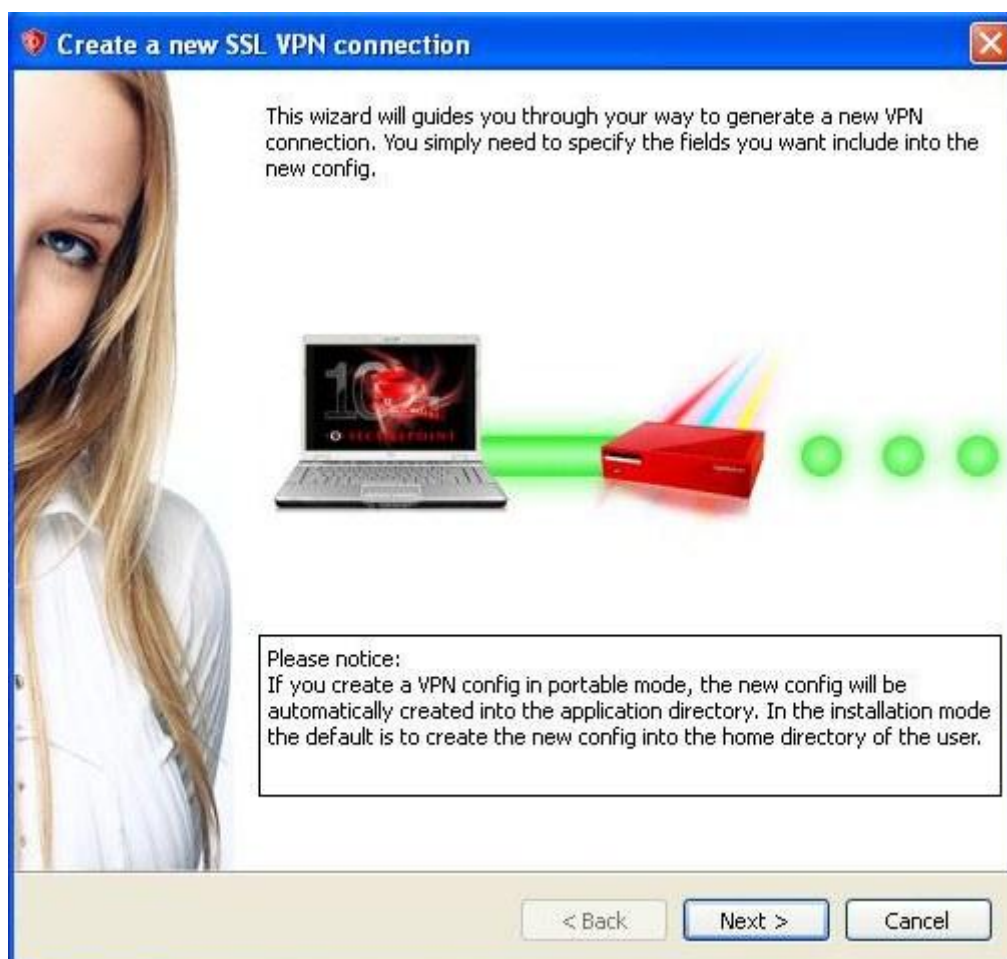
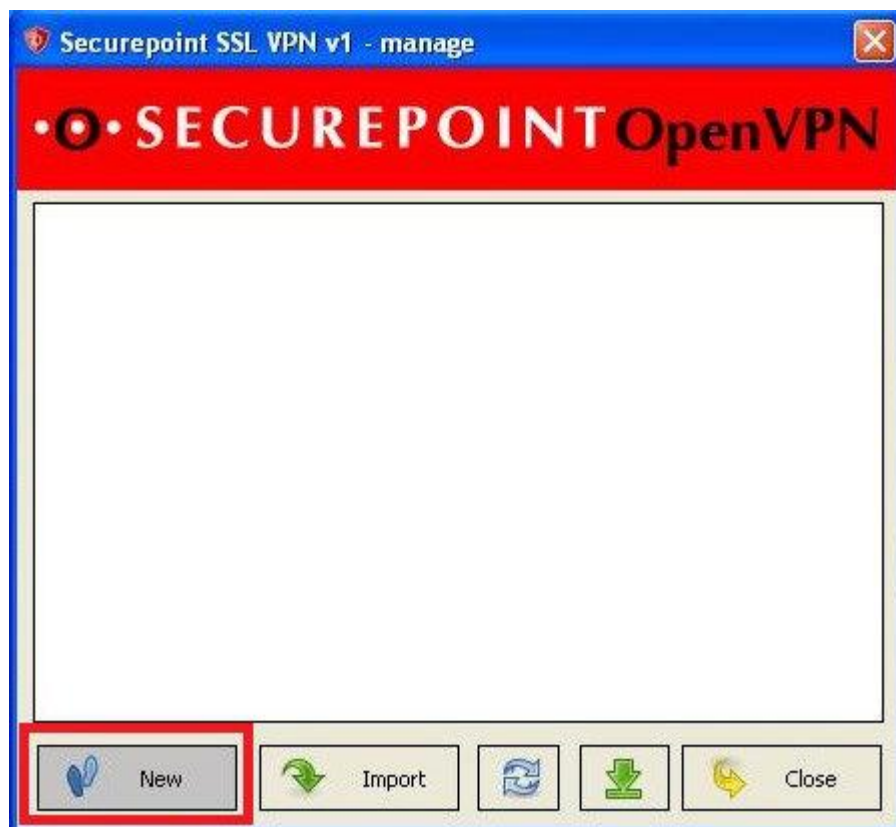


Pour se déconnecter du VPN, il suffit de cliquer sur le bouton « Disconnect »



IV-B-1) « Securepoint »

Vous pouvez utiliser « Securepoint » que vous trouverez sur le site suivant : <http://sourceforge.net/projects/securepoint/>



Create a new SSL VPN connection

General Settings
Specify the name of the config file which should create.

Please enter the name of the config.

Name:

< Back Next > Cancel

Create a new SSL VPN connection

Remote Settings
Specify the remote settings of the connection.

Please enter the IP and Port of the remote OpenVPN server.

IP: *ip address of your vpn server*

Port:

Protocol:

< Back Next > Cancel

Create a new SSL VPN connection

Certificates
Please specify the certificates for the connection.

Root CA:
 ...

Certificate:
 ...

Key:
 ...

Server certificate: ☐

< Back Next > Cancel

Create a new SSL VPN connection

Advanced Settings
Please specify the advanced settings.

Settings for Windows

MSSFIX: ☒ Route method:

Windows directory:

☒ Use default(c:\windows)

☐ Other

☒ Use environment

☐ Path use \\ instead of \

Verbosity: Auth user/pass: ☐ **Uncheck this**

Route delay: No bind: ☒

Mute: Float: ☒

Comp-LZO: ☒

< Back Next > Cancel

Create a new SSL VPN connection

Conclusion
Please check your defined settings.

Data of new config: OpenVPN

Remote IP: [REDACTED] Port: 1194

Protocol: UDP

CA: C:/Documents and Settings/Arbab/Desktop/client/ca.crt

Certificate: C:/Documents and Settings/Arbab/Desktop/client/arbapc.crt

Key: C:/Documents and Settings/Arbab/Desktop/client/arbapc.key

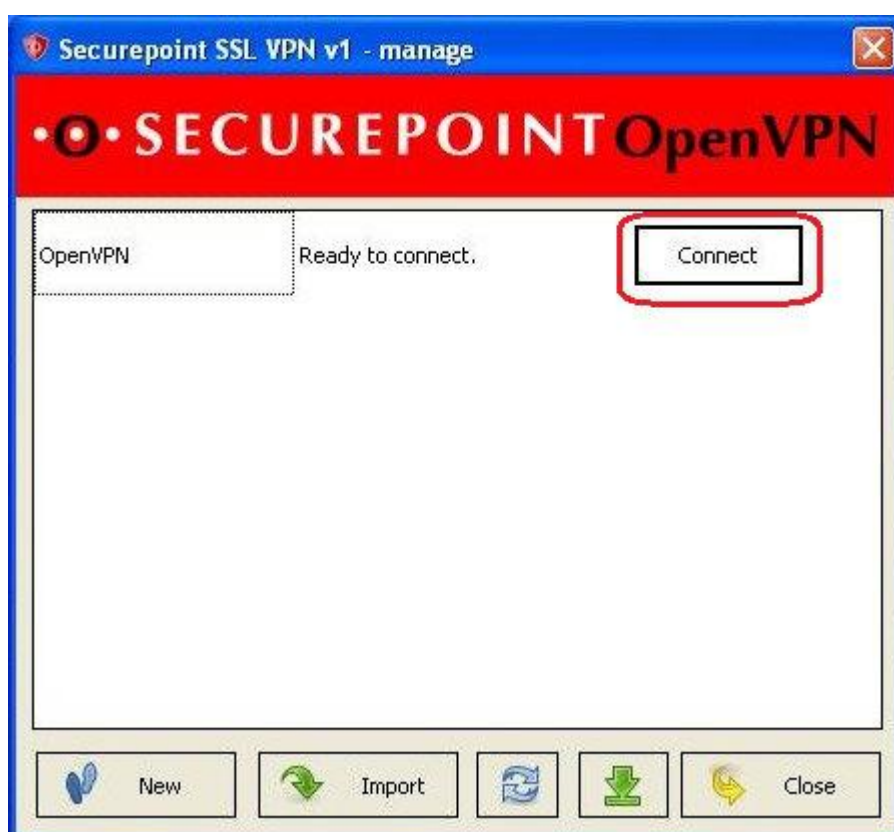
Certificate type: Normal

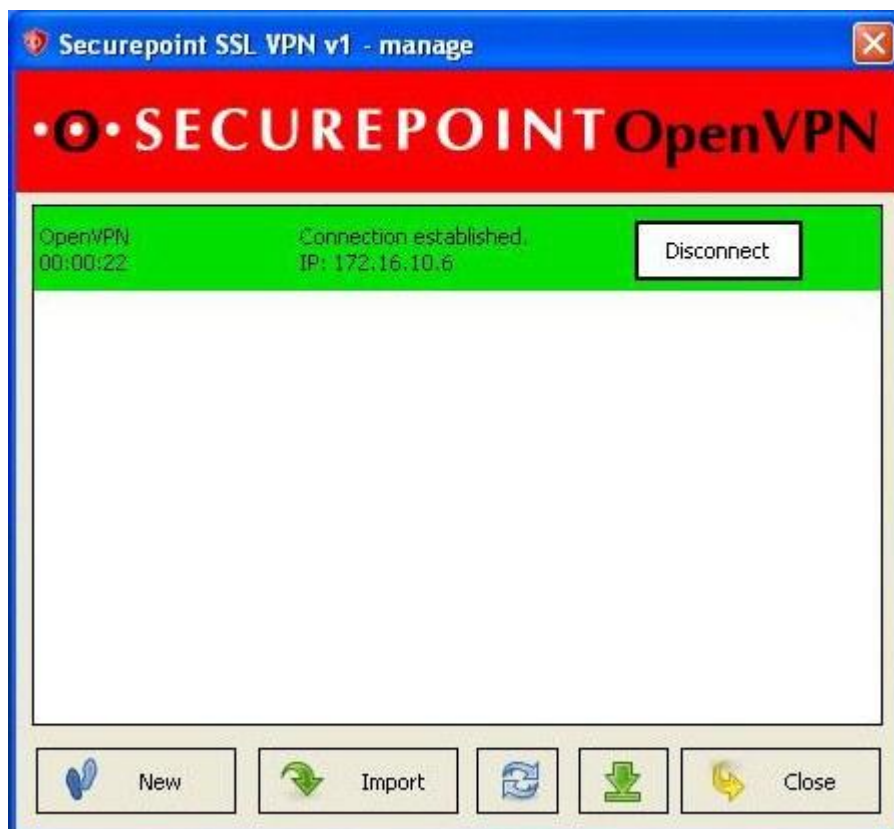
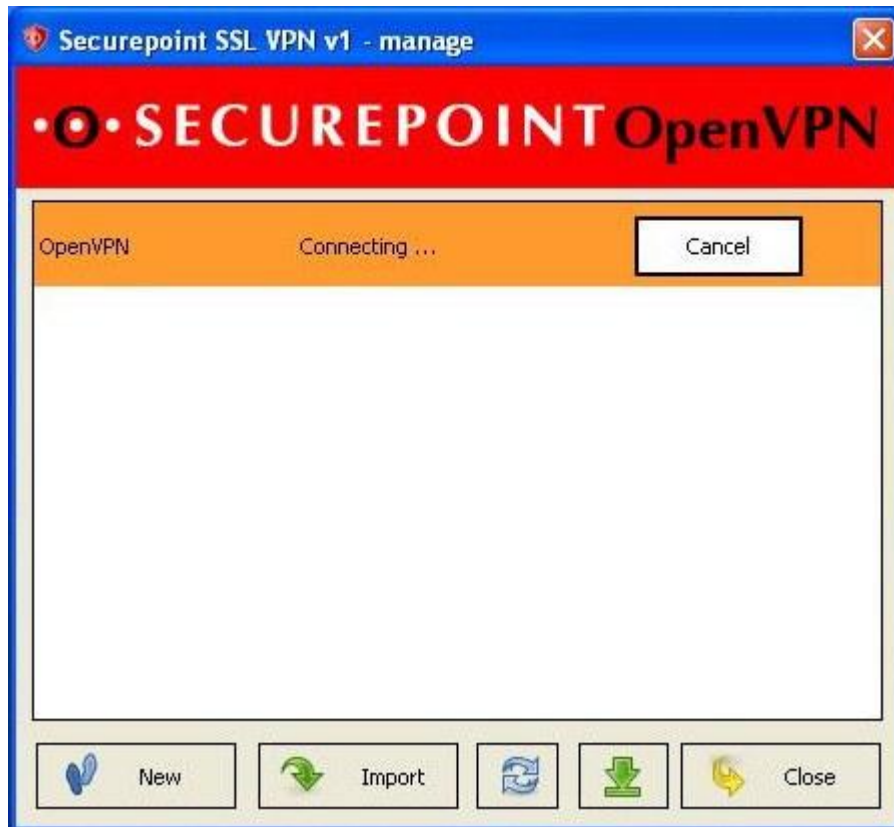
Advanced:

Windir:	default	Route method:	Exe
MSSFIX:	Yes	Float:	Yes
Verbosity:	3	Auth user/pass:	No
Route delay:	2	No bind:	Yes
Mute:	20	Comp-LZO:	Yes

MTU [1500], dev tun, persist key and persist tun will be added automatically.

< Back Finish Cancel





III-C) Tests une fois connecté

Nous allons vérifier la « Table de Routage ».

C:\> **netstat -r**

Vous aurez le réseau 10.10.10.0 / 24 et le réseau 172.16.0.0 / 24 qui apparaîtront.
Il ne reste plus qu'à essayer de joindre les machines du réseau local.