NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

➢ Introduction :

Tout au long de ce tutoriel nous allons voir comment installer un serveur VPN avec OpenVPN sous Debian Squeeze commençons tout d'abord à les définir et voir leurs fonctions.

Debian : est une distribution libre du système d'exploitation libre Linux, développée par plusieurs milliers de volontaires dans le monde entier, qui collaborent via Internet.
Debian Squeeze étant la version 6.

VPN : Un VPN (de l'anglais Virtual Private Network) est un Réseau Privé Virtuel. Il permet, lorsque vous êtes sur un site distant (à votre domicile par exemple) , d'avoir accès au réseau local de votre entreprise à travers une connexion internet sécurisée. Ainsi, vous avez accès aux ressources de votre réseau local (fichiers partagés, intranet, extranet...) comme si vous étiez sur votre lieu de travail.

OpenVPN : est un logiciel libre permettant de créer facilement une liaison VPN site à site.
OpenVPN permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance ou de certificats. Il fonctionne sur un mode client/serveur, ce qui implique son installation sur les 2 sites distants, l'un côté client, l'autre côté serveur.

Nous allons donc travailler sur l'environnement Debian Squeeze, nous allons suivre toutes les étapes de l'installation de cette distribution, puis l'installation d'OpenVPN ainsi que la création des certificats, pour en finir avec la configuration du serveur et la configuration de clients.

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Sommaire :

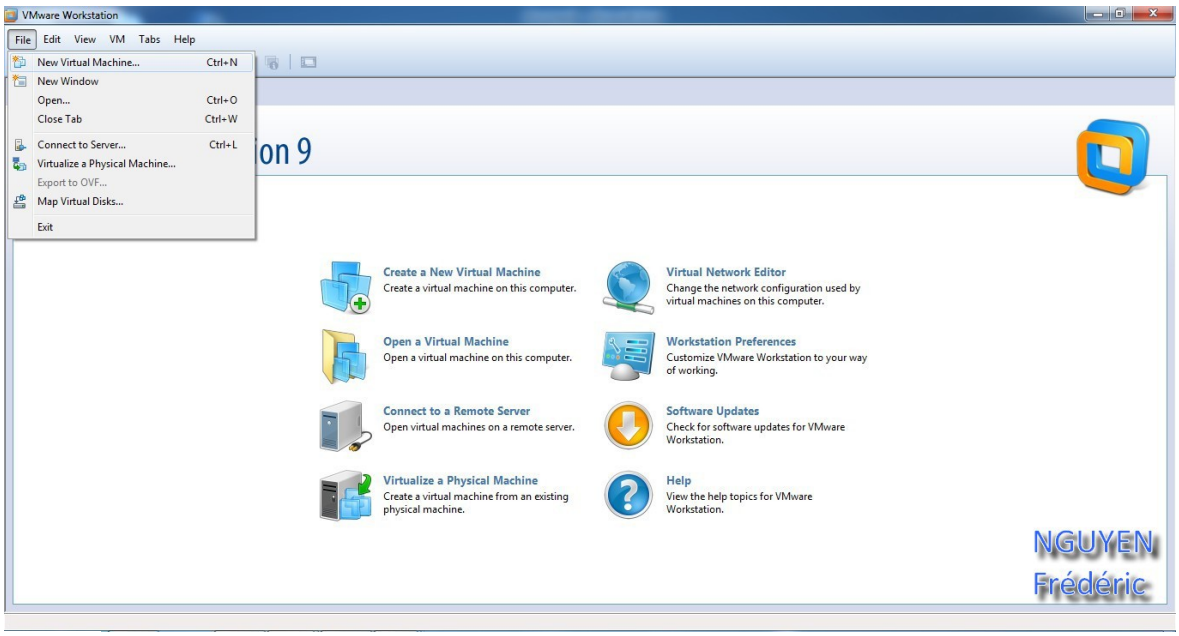
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

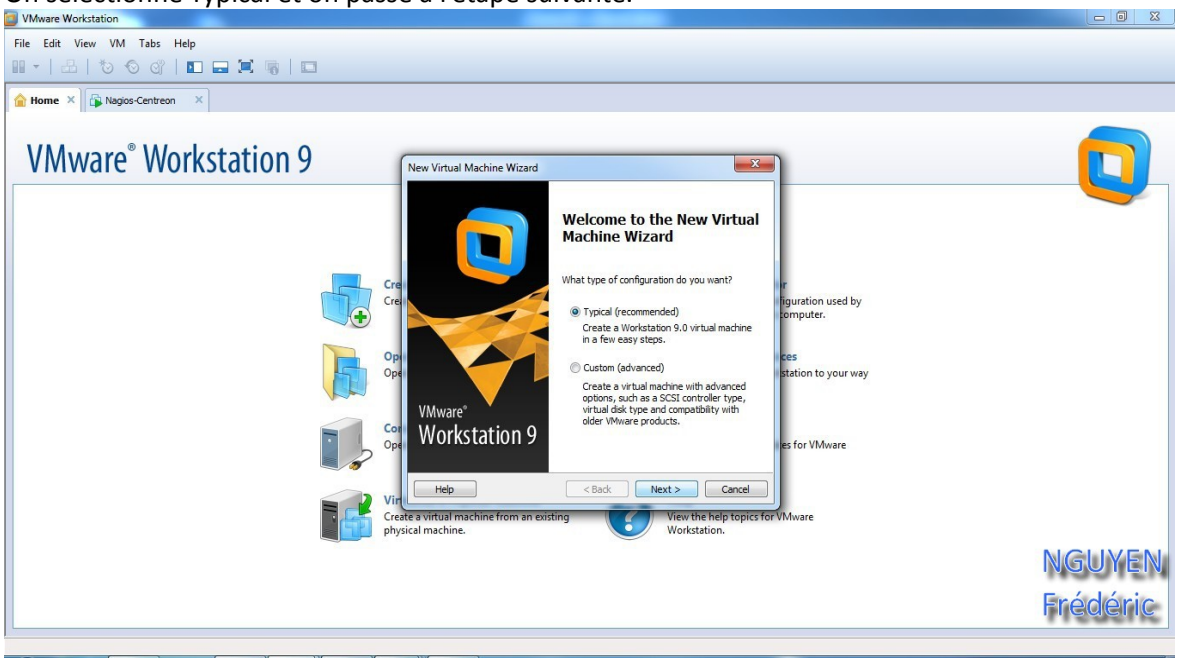
I) Installation de Debian Squeeze

Dans cette partie nous utiliserons Workstation, un outil de virtualisation de système d'exploitation, pour installer Debian sur une machine virtuel.

Dans le menu « File » on sélectionne « New Virtual Machine » pour créer une machine virtuel



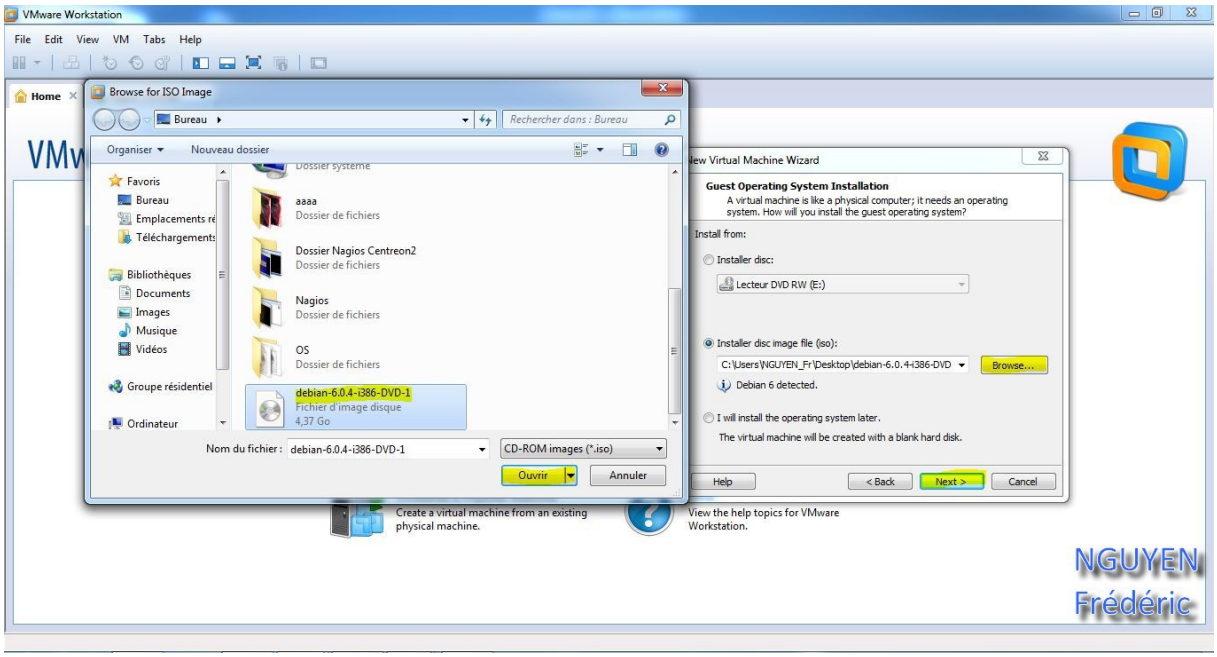
On sélectionne Typical et on passe à l'étape suivante.



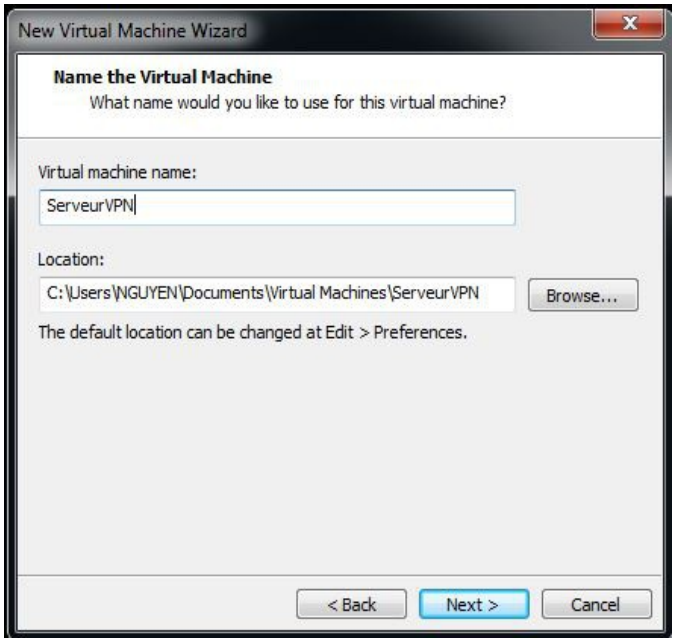
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Ont choisir l'option de l'iso, où est contenue Debian 6 et on passe à l'étape suivante.



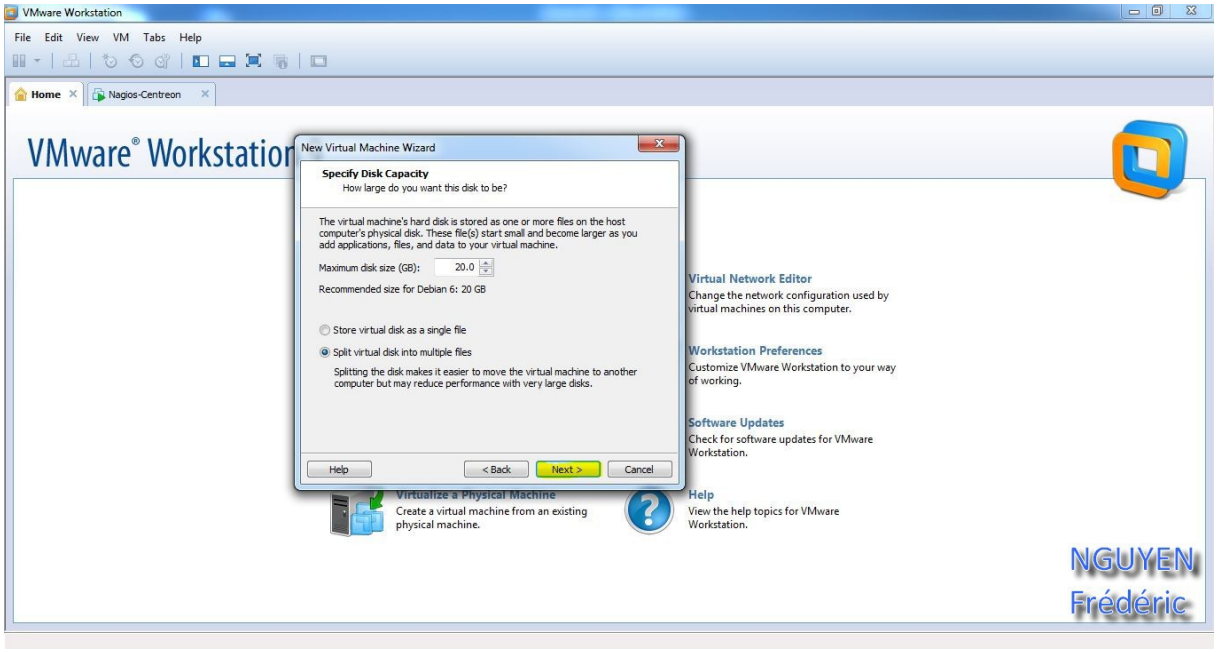
Dans cette étape ont choisis seulement le nom de la machine virtuel.



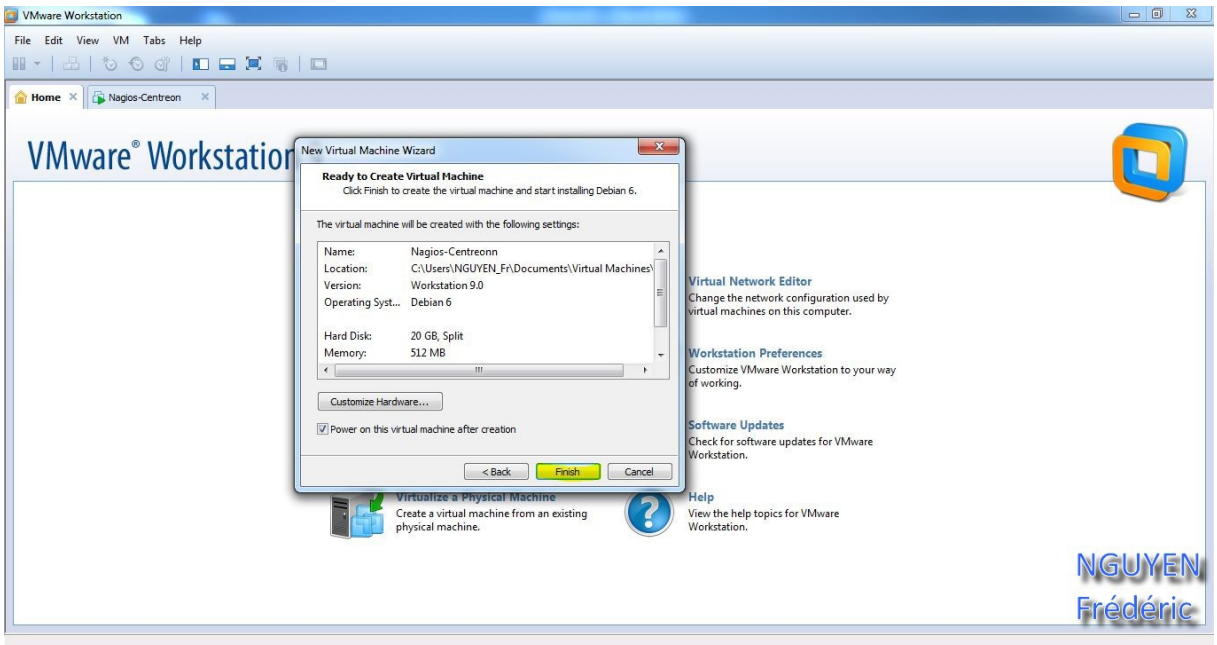
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On laisse par défaut et on passe à l'étape suivante.



Puis on termine en cliquant sur « Finish »

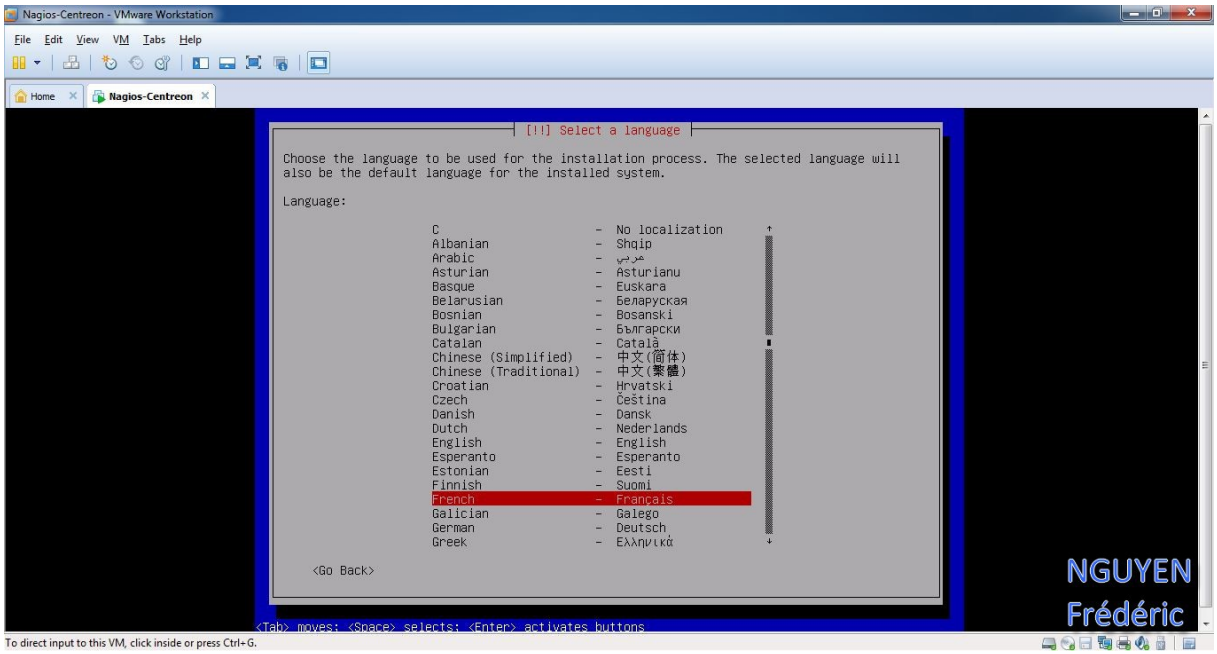


NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

C'est vraiment à partir de ce moment, qu'on va commencer à installer Debian.
On démarre la machine virtuelle et on sélectionne « Install ».

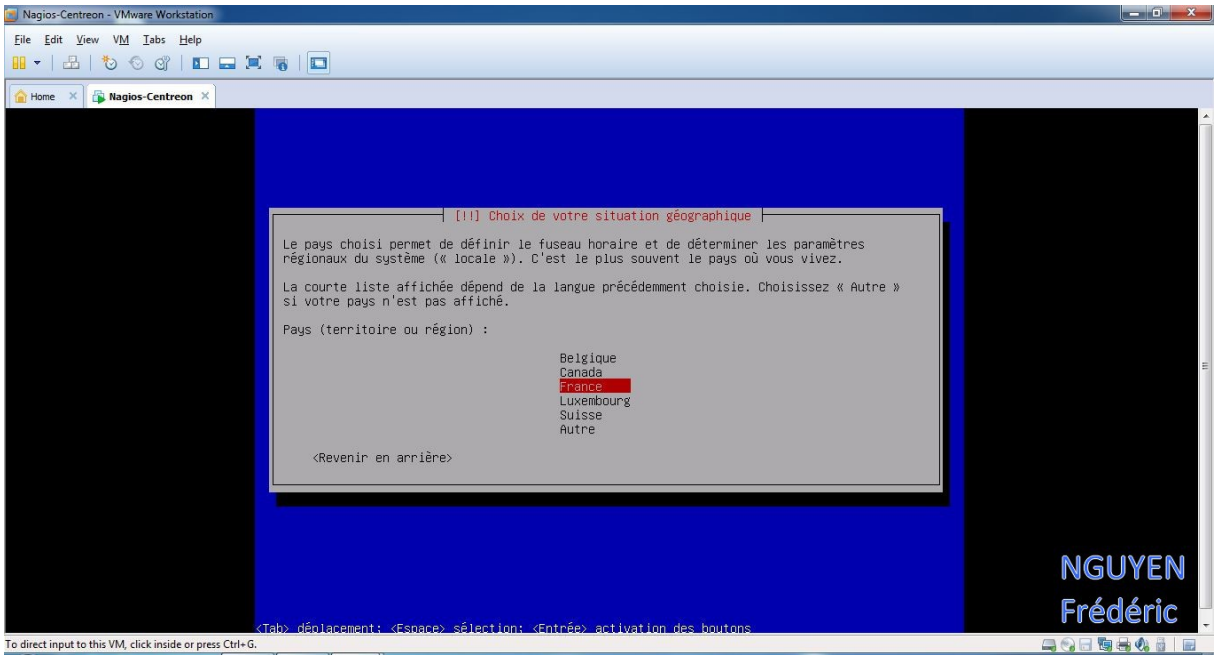
On choisit la langue désiré.



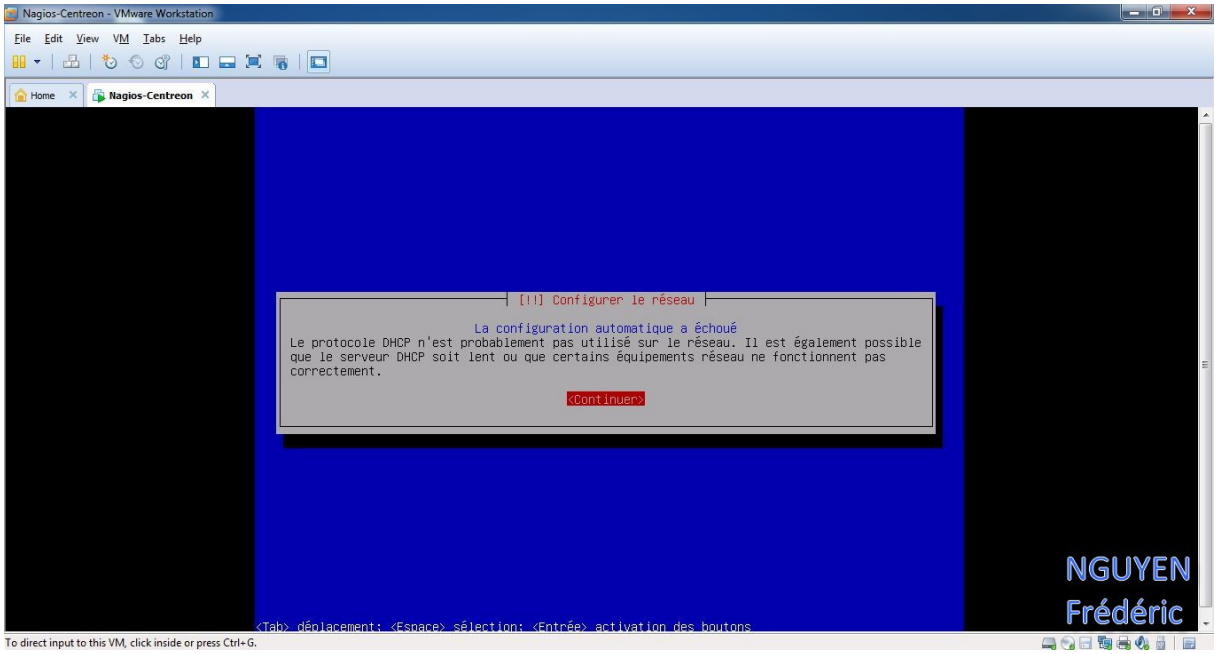
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On choisit notre situation géographique.



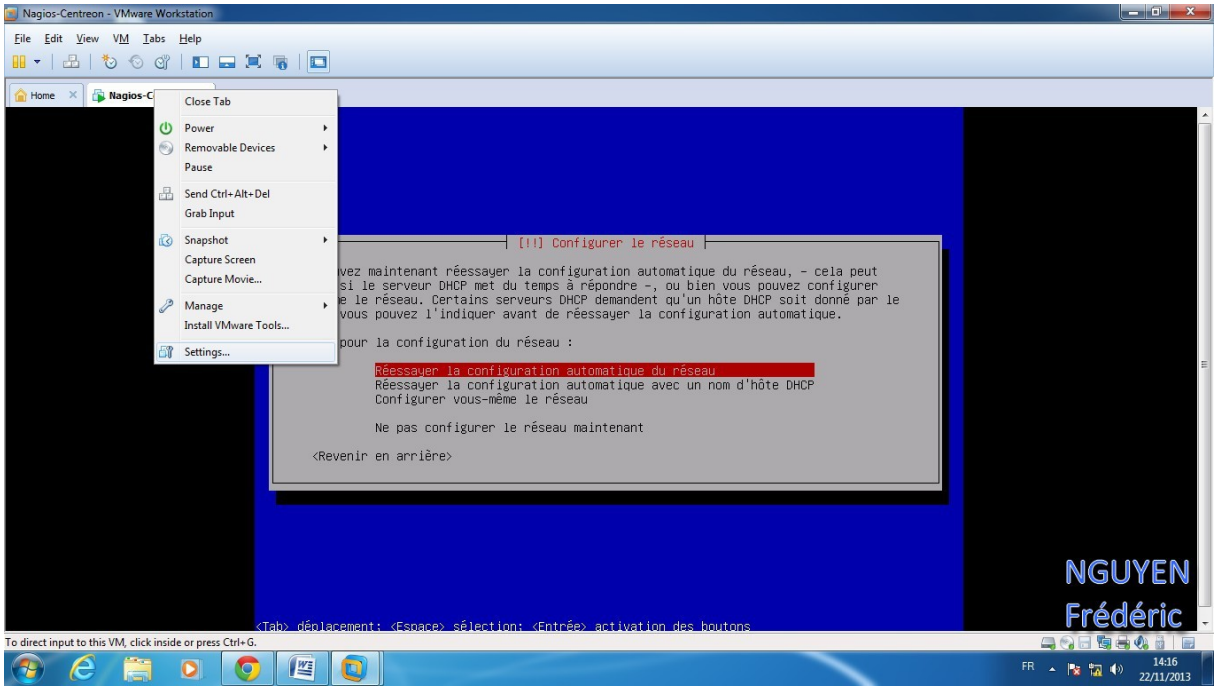
En passant à l'étape suivant, on rencontre un problème de réseau.



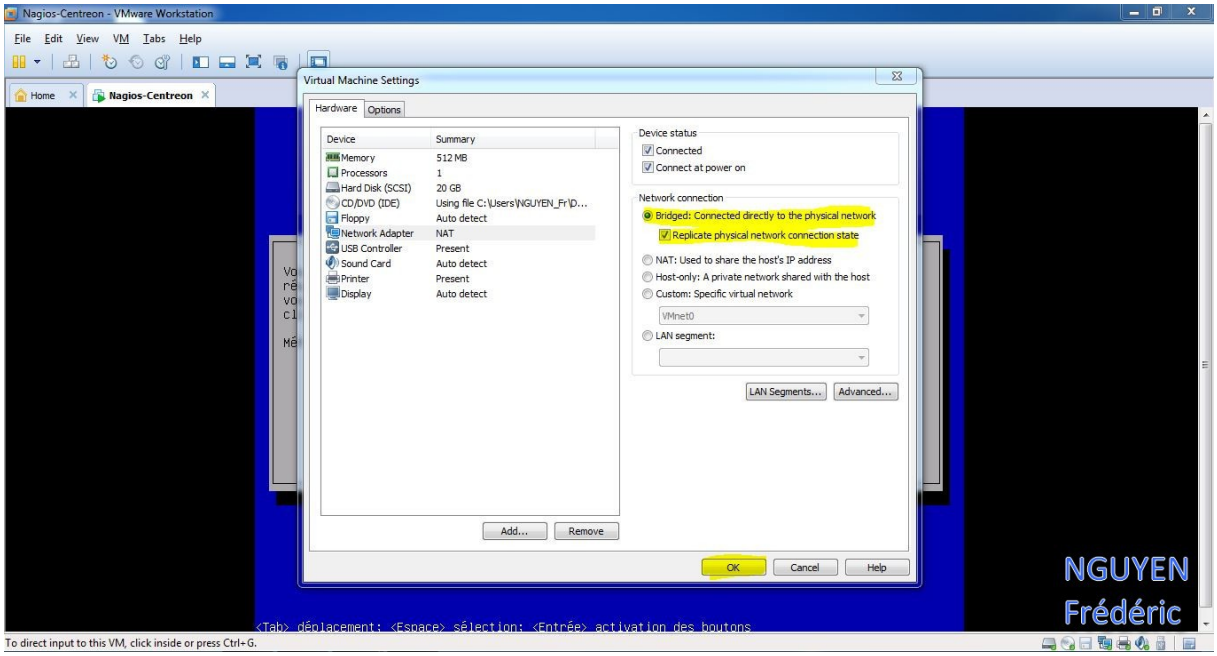
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Rien de très inquiétant on a seulement à branché notre carte réseau en « Bridged »
Pour cela « on clique-droit » et on sélectionne « Settings …»



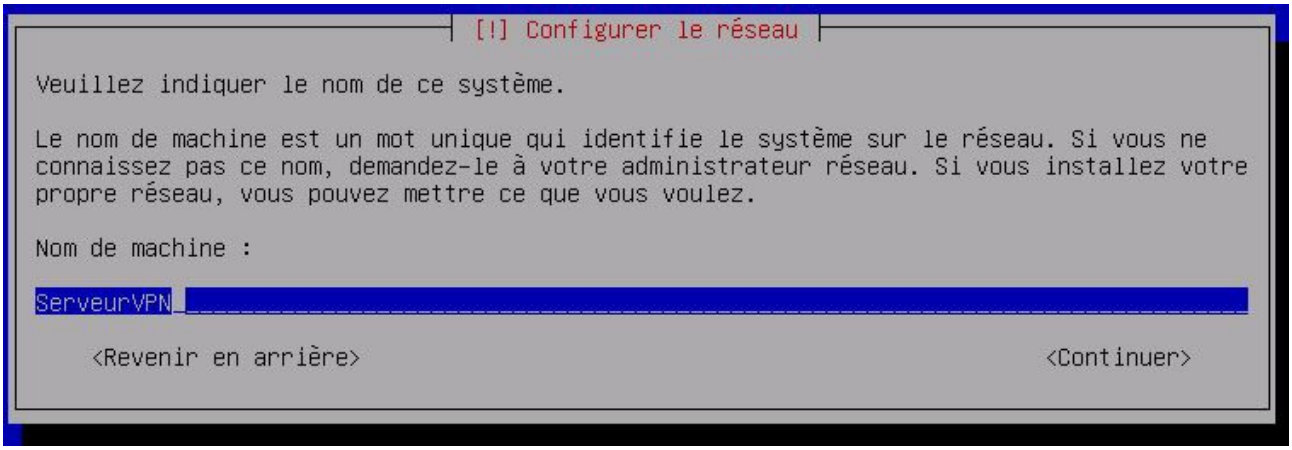
Puis on sélectionne en « Bridged » et là on aura plus de problème de connexion réseau .



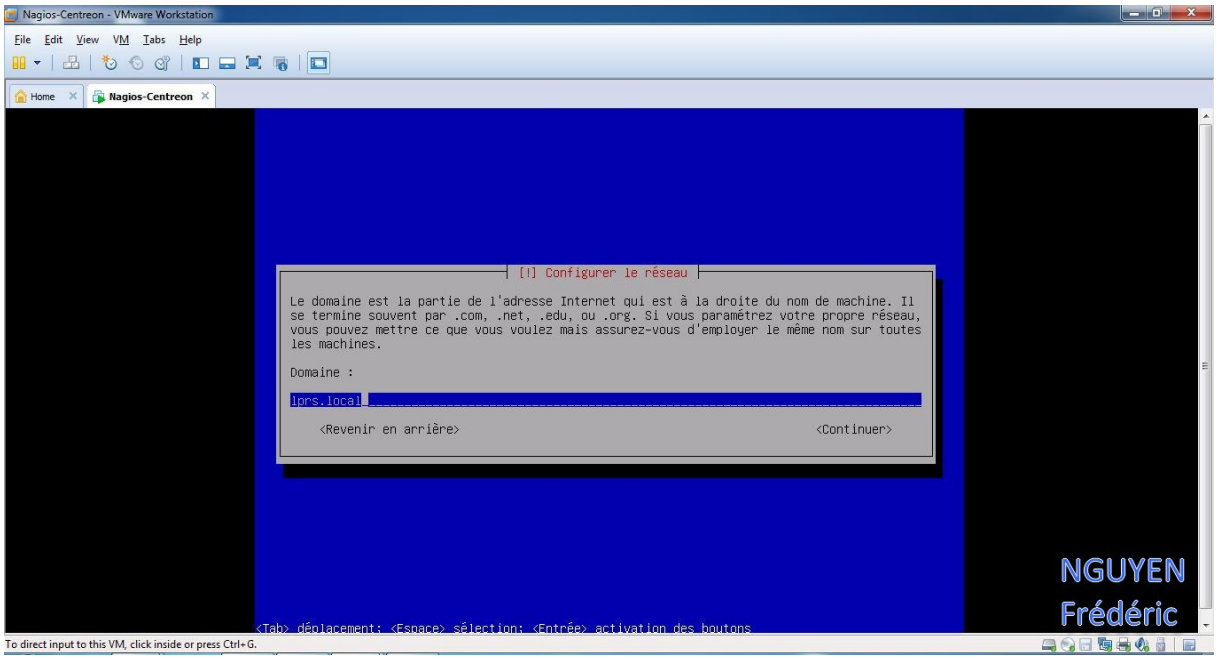
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Pour le nom de la machine on met « ServeurVPN ».



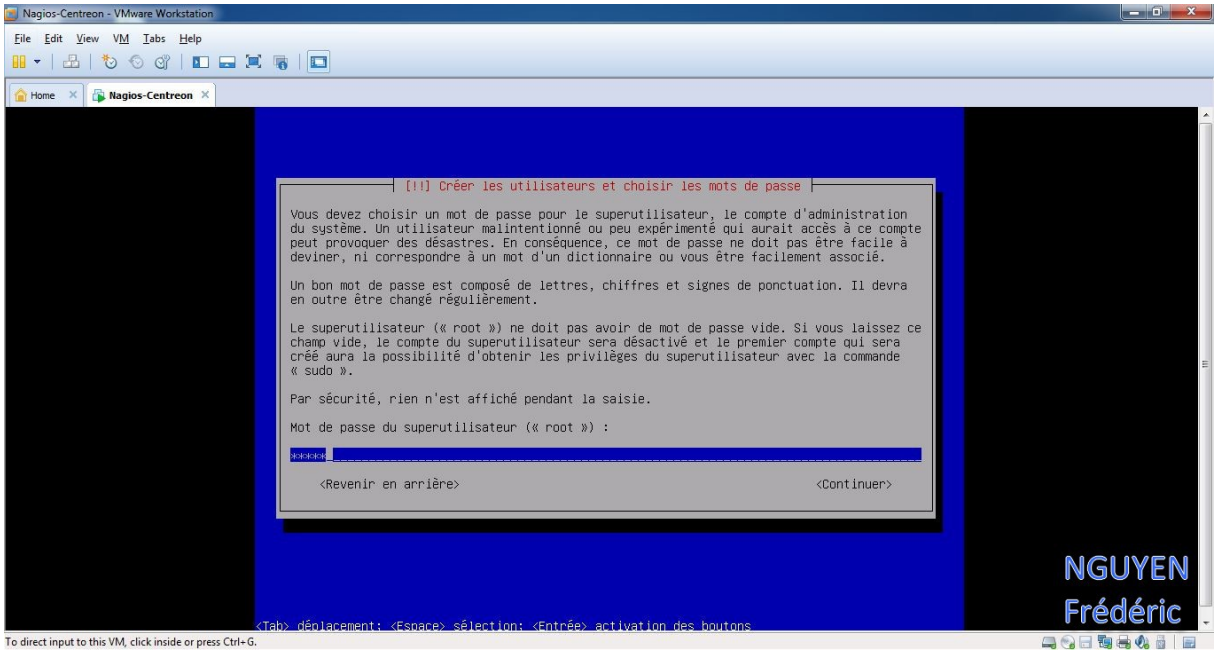
Pour le domaine on met « lprs.local »



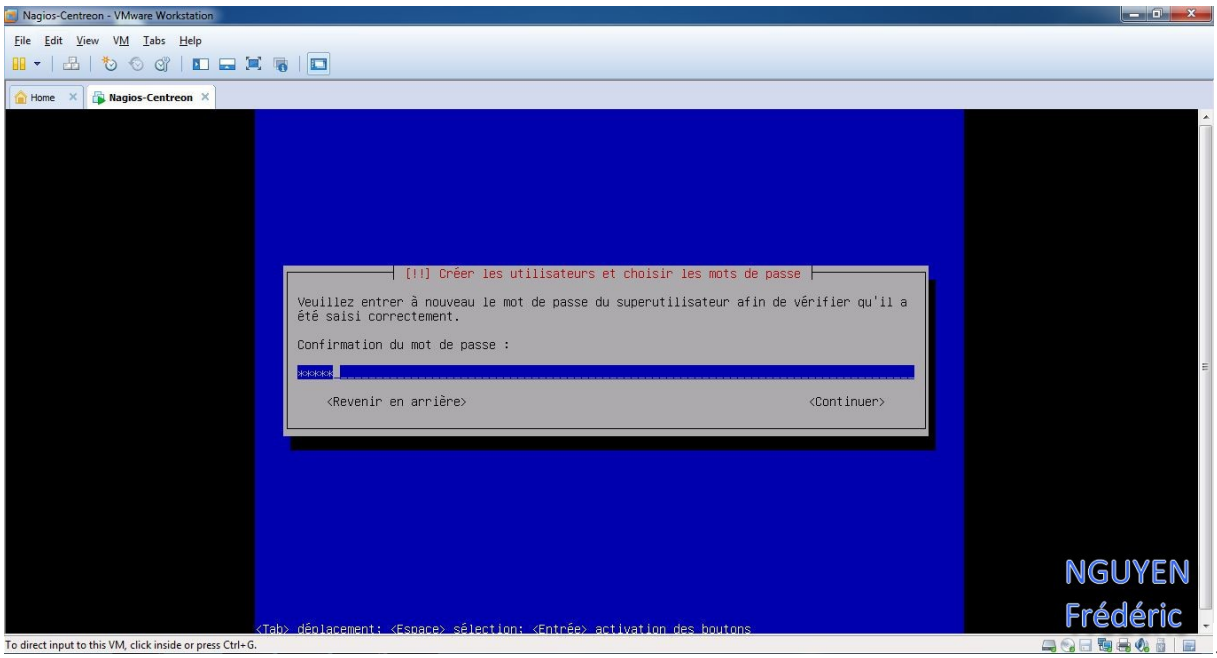
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On va définir un mot de passe pour le compte super-utilisateur, donc le compte « root », ainsi son mot de passe sera « admin »



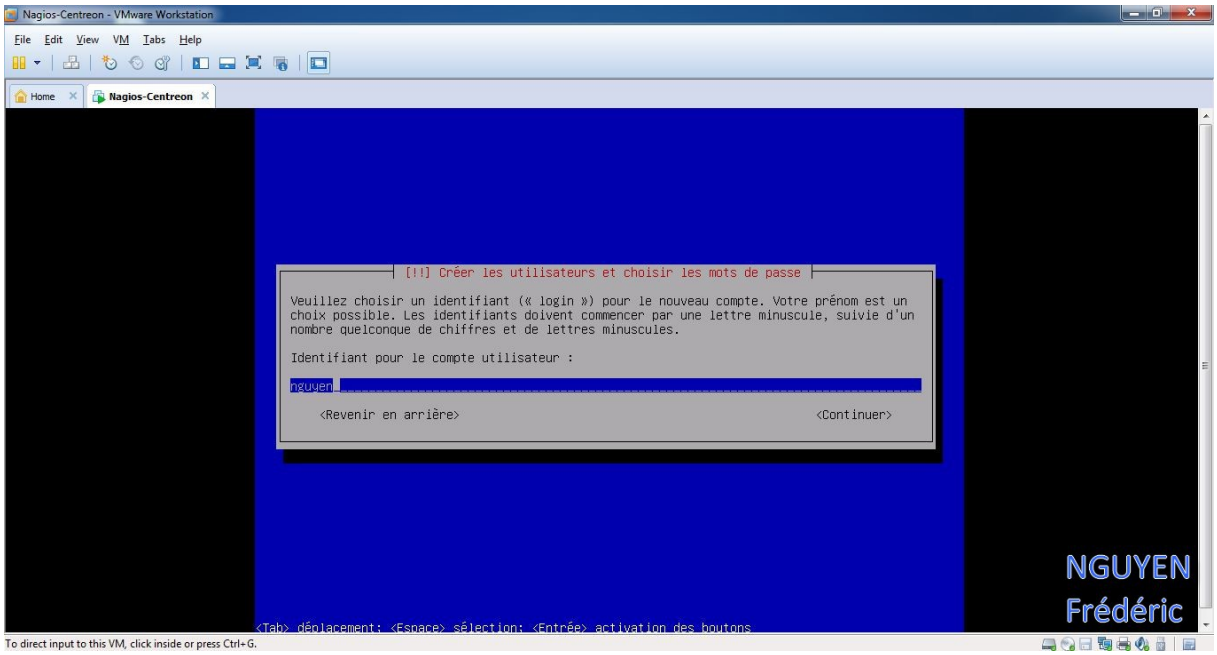
Puis on reconfirme le mot de passe saisi précédemment



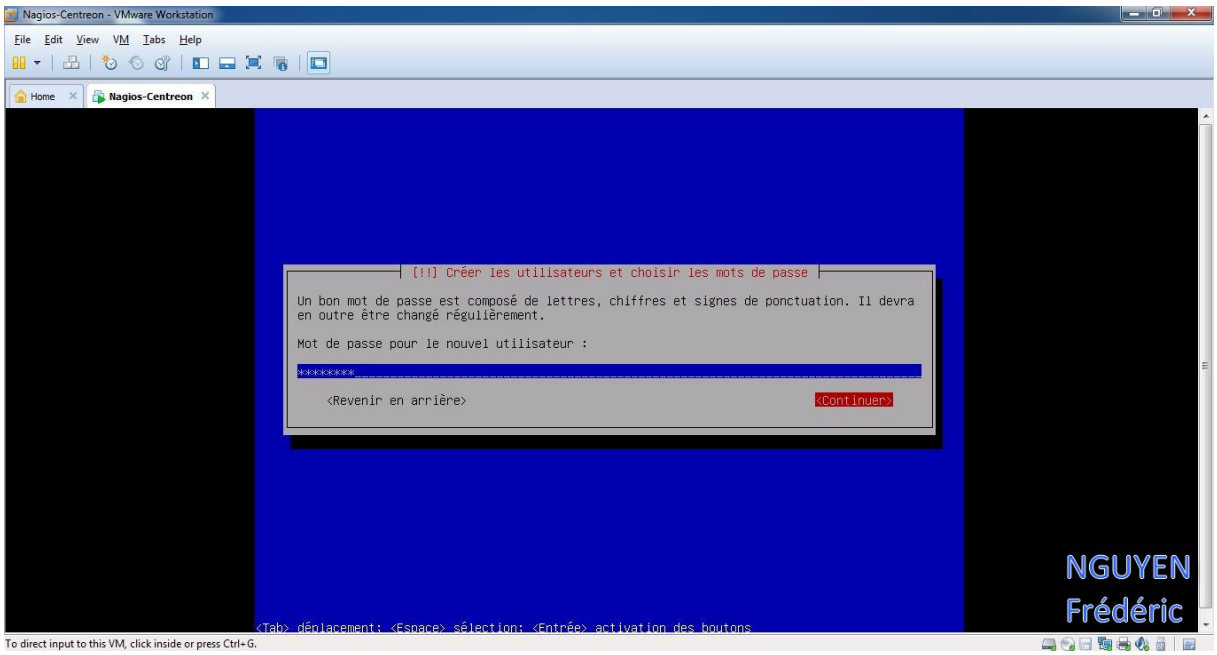
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On créer maintenant un nouveau compte, dans ce cas le nom du compte sera « nguyen » et le mot de passe « frederic ».
On saisit donc le nom du compte « nguyen » .



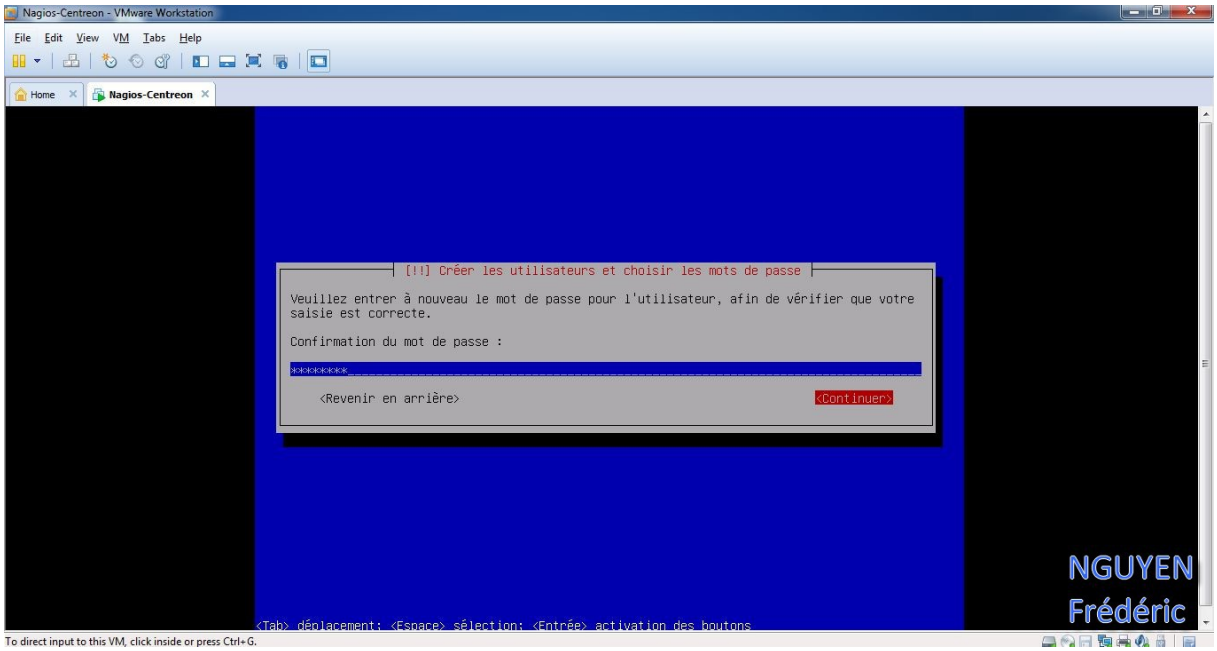
On définit le mot de passe « frederic ».



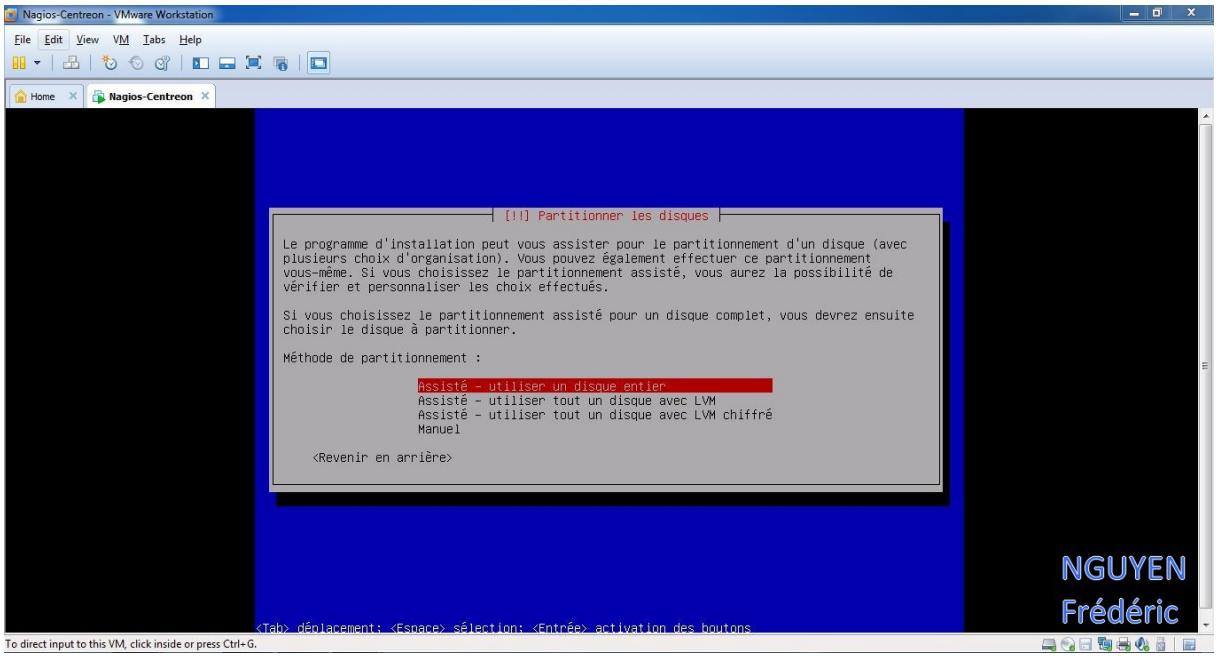
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On re-tape le mot de passe « frederic »



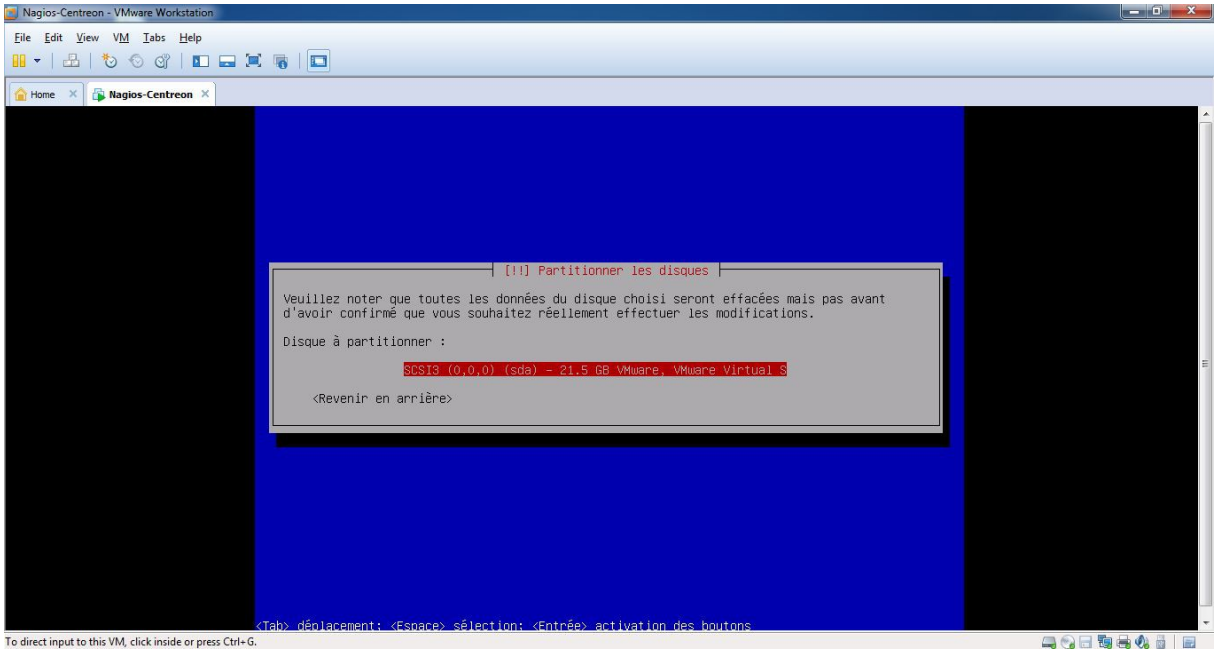
On sélectionne « Assisté – utiliser un disque entier ».



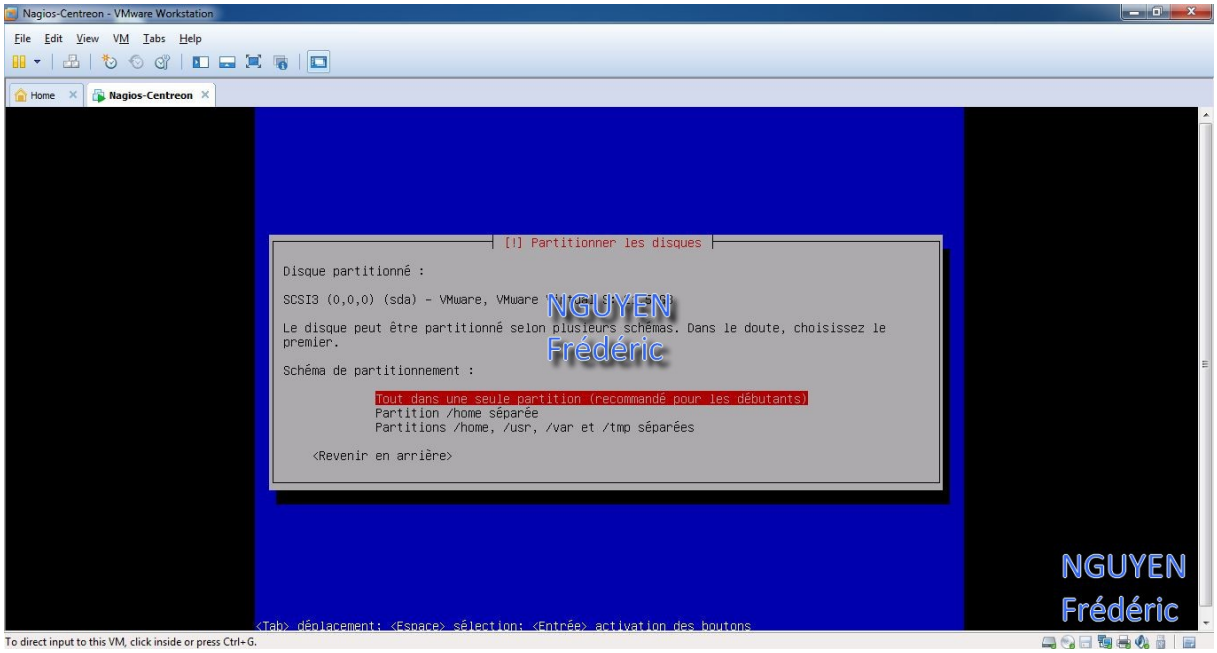
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On choisit le disque à partitionner.



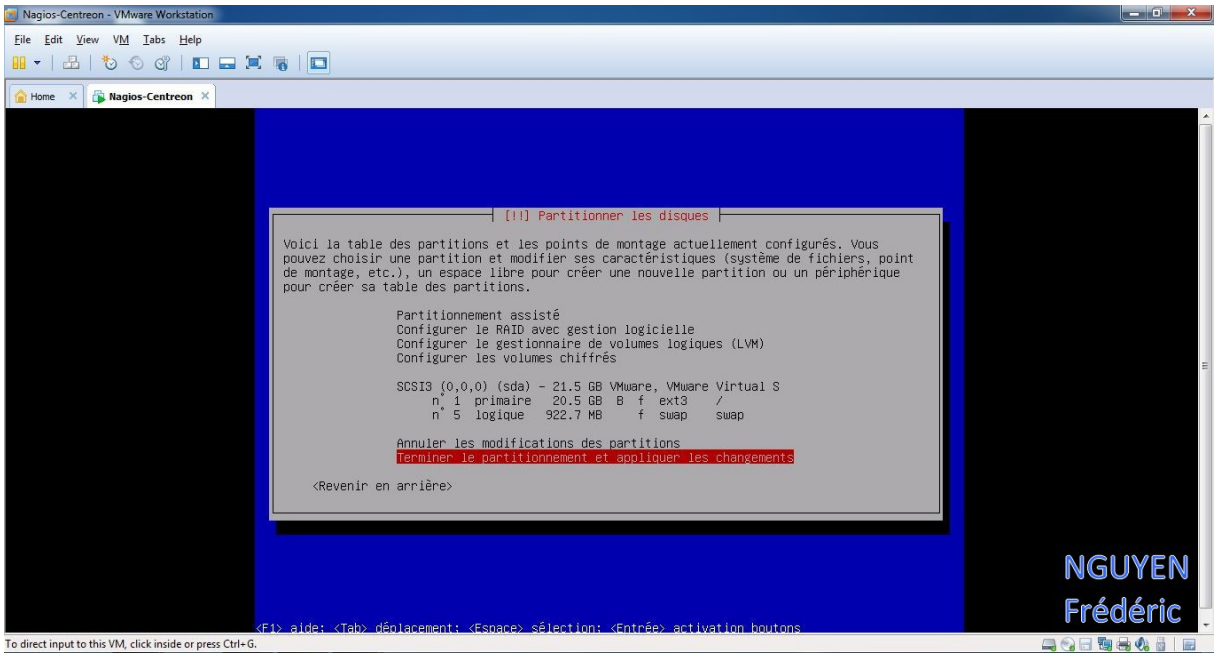
On choisit tout dans une seule partition.



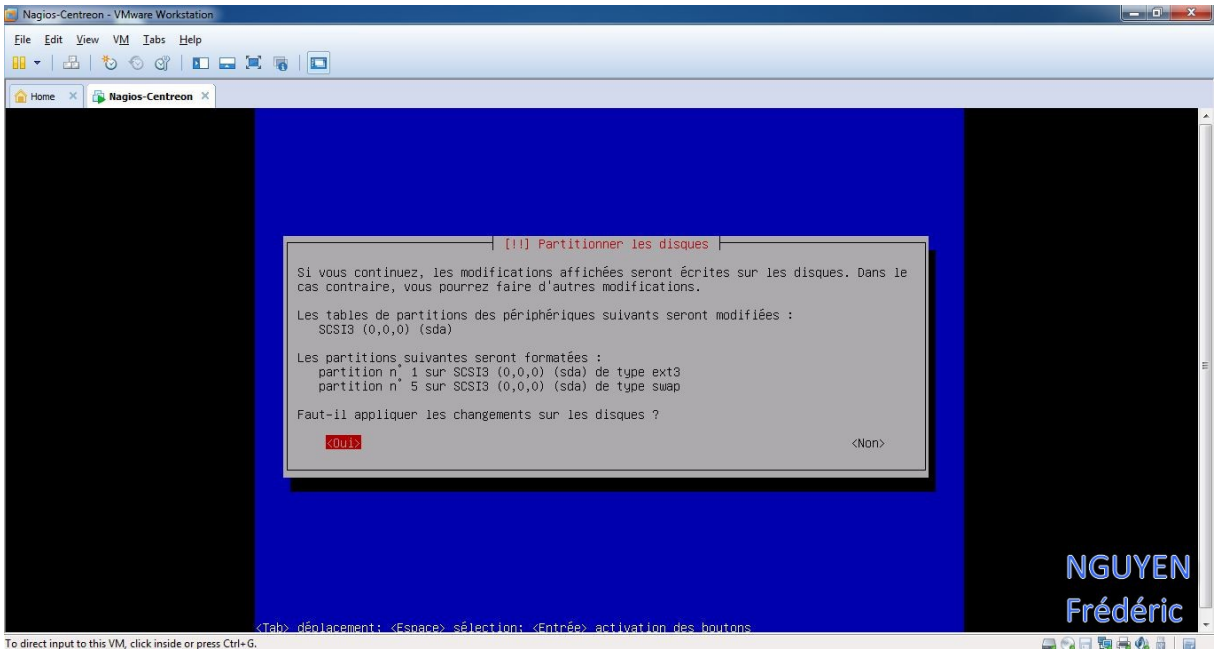
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On sélectionne « Terminer le partitionnement et appliquer les changements ».



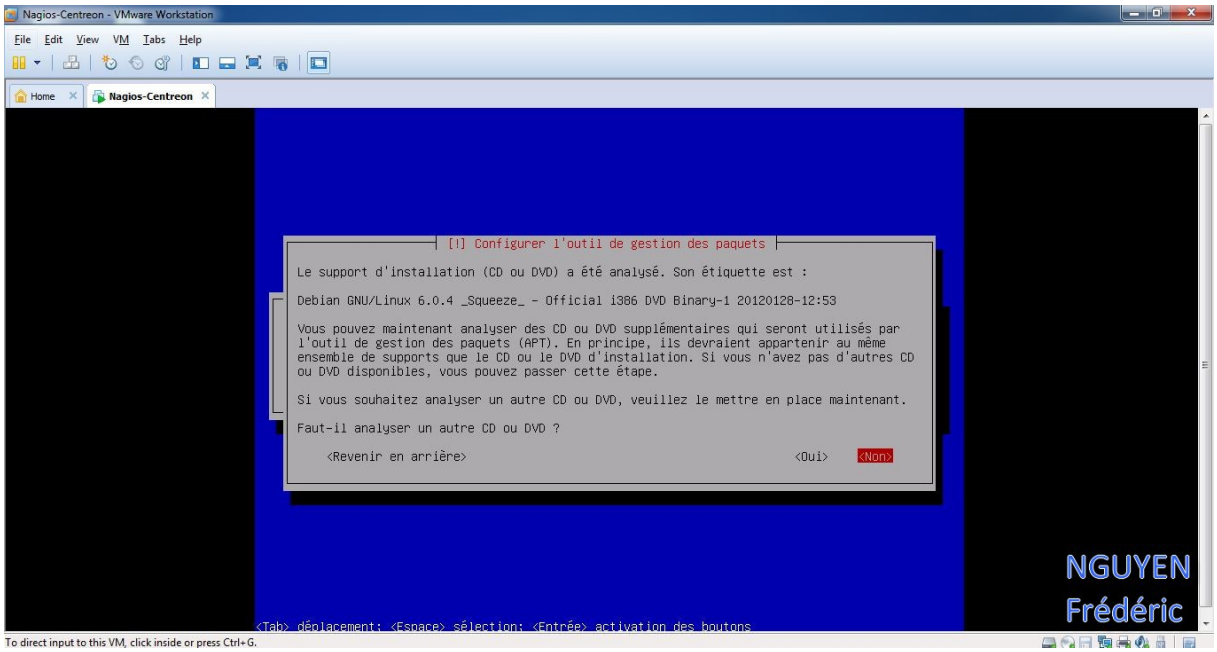
On sélectionne « Oui ».



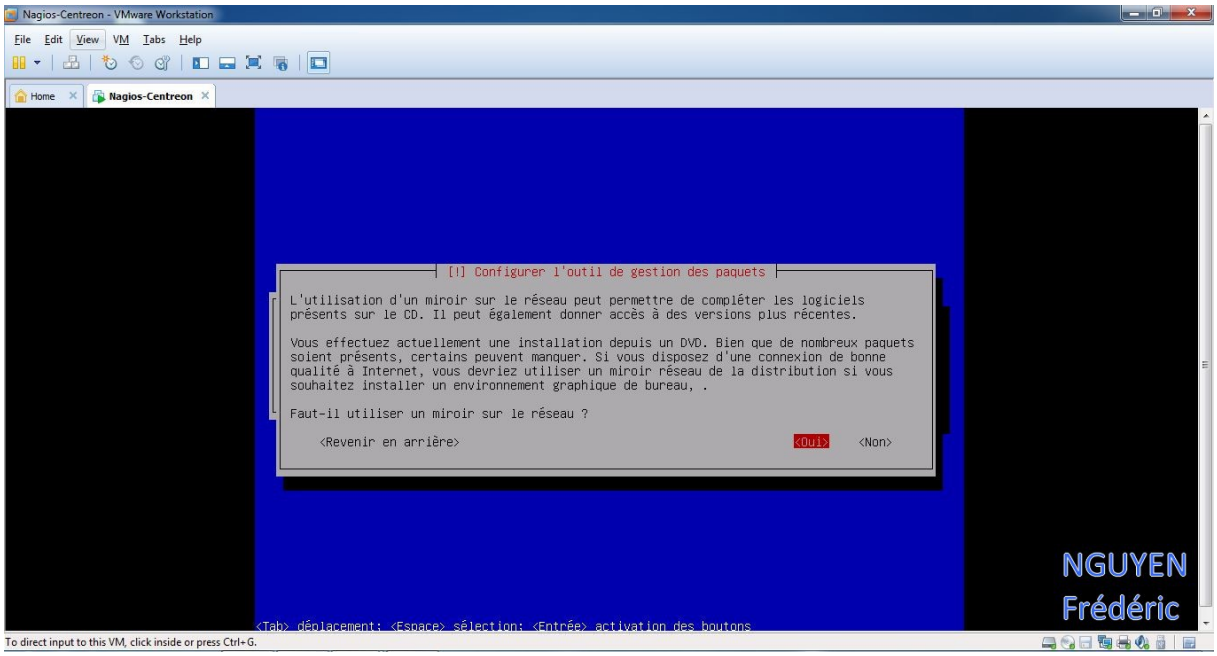
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On sélectionne « Non ».



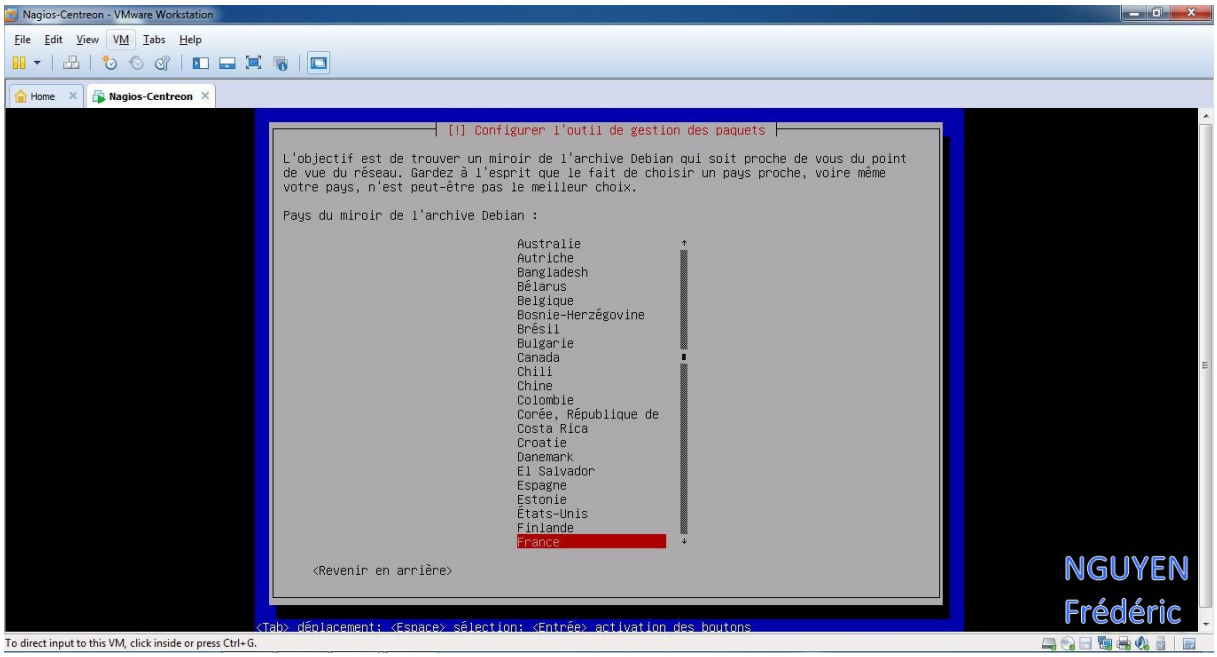
On sélectionne « Oui » pour pouvoir utiliser le miroir du réseau



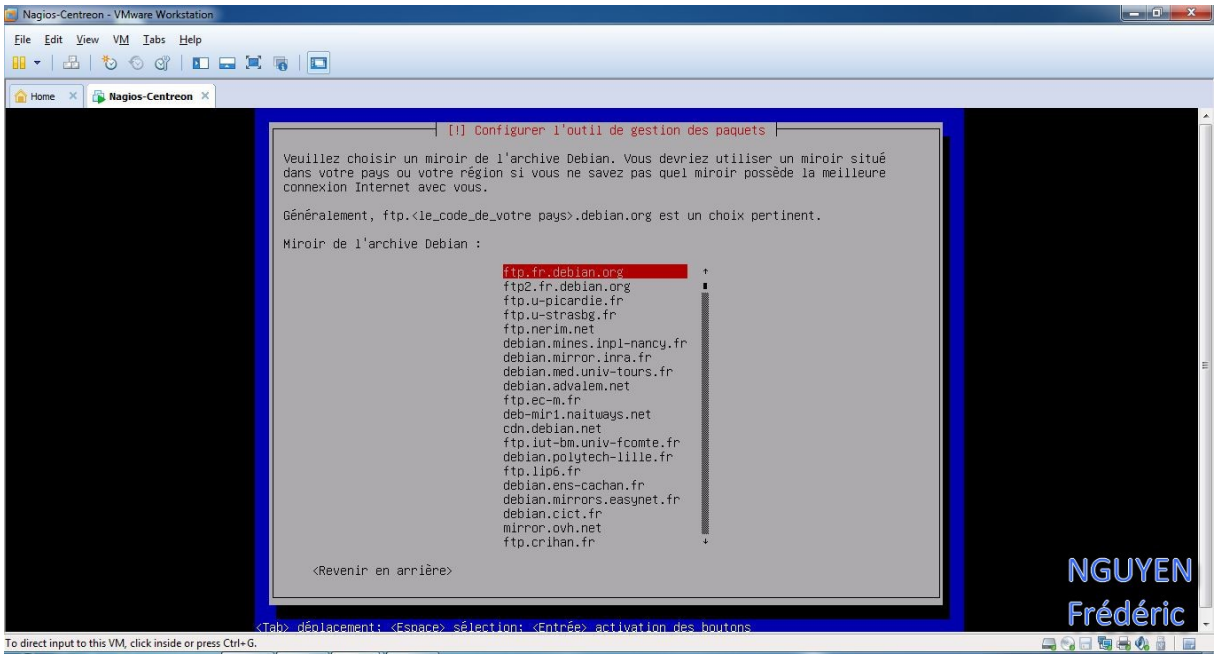
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On choisit « France ».



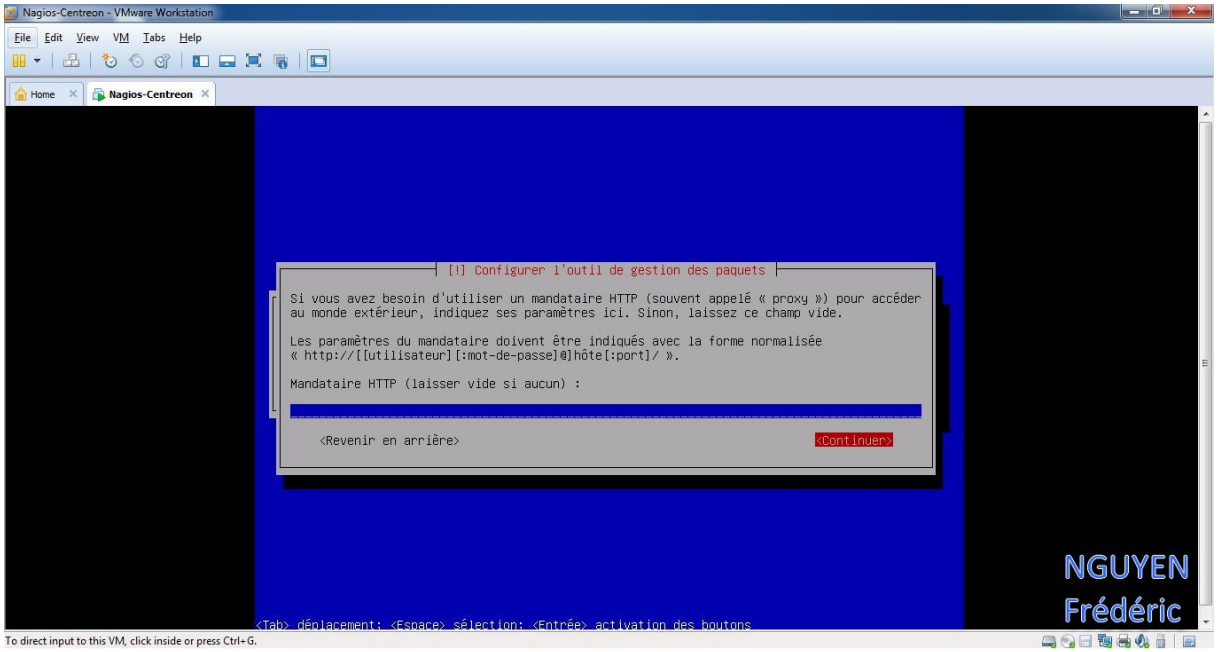
On choisit le premier miroir.



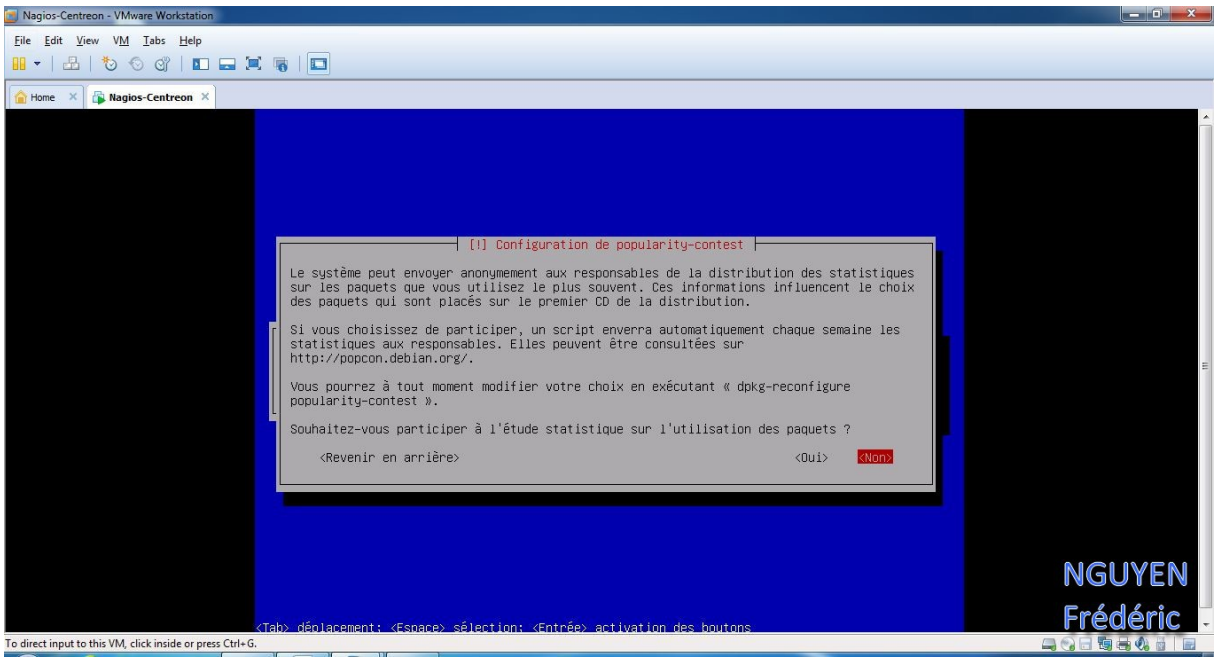
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On laisse vide et on passe à l'étape suivante en sélectionnant « Continuer »



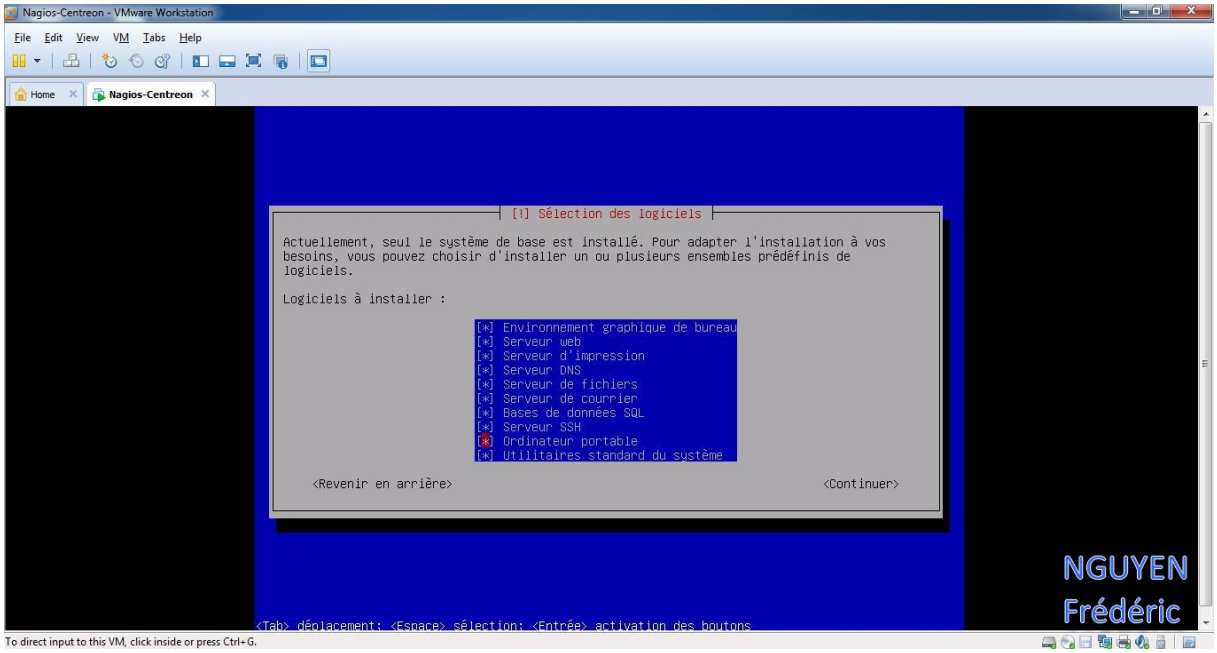
On sélectionne « Non ».



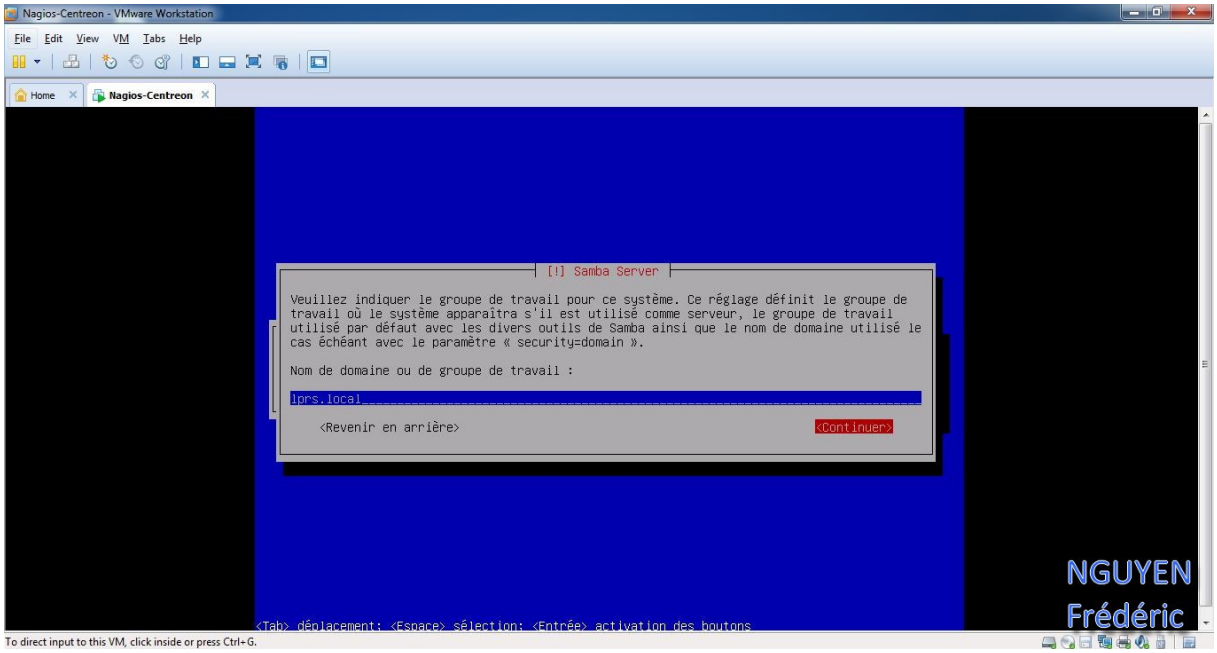
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Ont sélectionne les logiciels à installer et on passe à l'étape suivant en sélectionnant « Continuer »



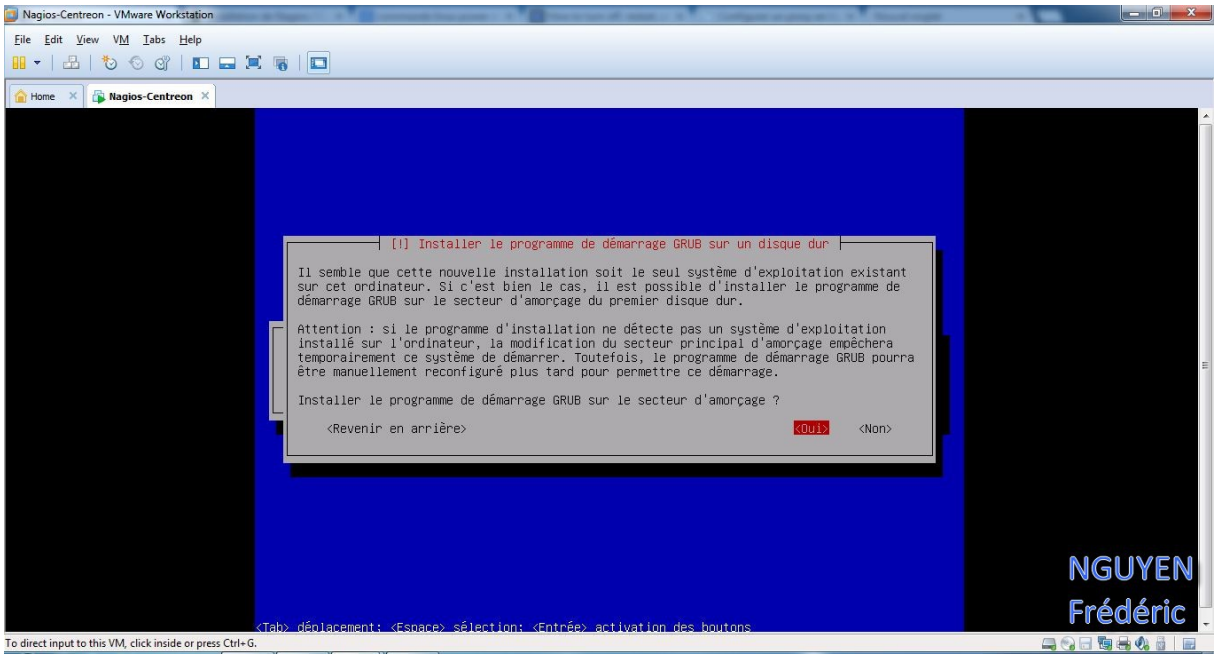
On met pour le nom de domaine « lprs.local »



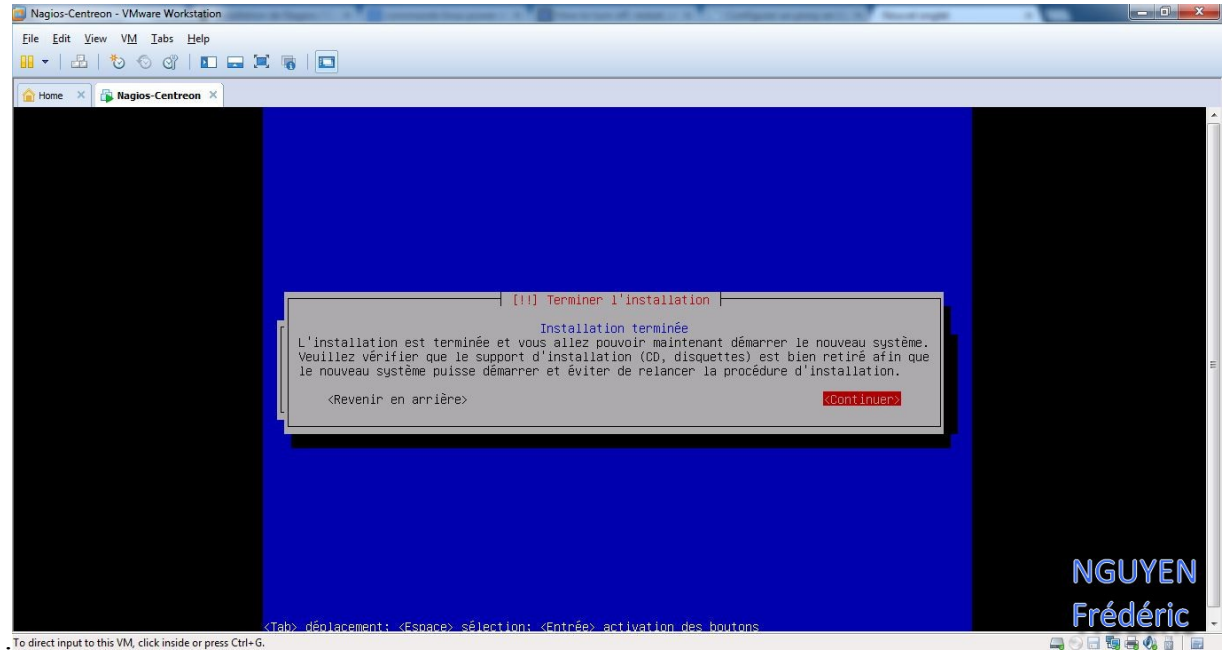
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

On installe le programme de démarrage GRUB sur le secteur d'amorçage en sélectionnant « Oui ».



On termine l'installation en sélectionnant « Continuer »



L'installation de Debian 6 est maintenant terminer.

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

II) Installation d'OpenVPN et Création de certificats

Dans cette partie nous allons d'abord commencé par installer OpenVPN puis créer les certificats.

A) Installation d'OpenVPN :

On démarre notre machine virtuelle et on se connecte en « root » avec le mot de passe « admin »

```
Starting kerneloops:
Starting mpt-status monitor: mpt-statusd.
Starting internet superserver: inetd.
Starting PostgreSQL 8.4 database server: mainsaned disabled; edit /etc/default/s
aned
SpamAssassin Mail Filter Daemon: disabled, see /etc/default/spamassassin
.
Starting Samba daemons: nmbd smbd.
Starting OpenBSD Secure Shell server: sshd.
Starting the Winbind daemon: winbind.
Starting MTA: exim4.

Debian GNU/Linux 6.0 ServeurVPN tty1

ServeurVPN login: root
Password:
Linux ServeurVPN 2.6.32-5-amd64 #1 SMP Mon Sep 23 22:14:43 UTC 2013 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@ServeurVPN:~# _
```

On va installer OpenVPN avec cette commande :

```
> apt-get install openvpn
```

Ce qui nous donne :

```
7 974 ko réceptionnés en 32s (248 ko/s)
Préconfiguration des paquets...
Sélection du paquet openssl-blacklist précédemment désélectionné.
(Lecture de la base de données... 129039 fichiers et répertoires déjà installés.
)
Dépaquetage de openssl-blacklist (à partir de .../openssl-blacklist_0.5-2_all.de
b) ...
Sélection du paquet liblzo2-2 précédemment désélectionné.
Dépaquetage de liblzo2-2 (à partir de .../liblzo2-2_2.03-2_amd64.deb) ...
Sélection du paquet libpkcs11-helper1 précédemment désélectionné.
Dépaquetage de libpkcs11-helper1 (à partir de .../libpkcs11-helper1_1.07-1_amd64
.deb) ...
Sélection du paquet openvpn-blacklist précédemment désélectionné.
Dépaquetage de openvpn-blacklist (à partir de .../openvpn-blacklist_0.4_all.deb)
 ...
Sélection du paquet openvpn précédemment désélectionné.
Dépaquetage de openvpn (à partir de .../openvpn_2.1.3-2+squeeze2_amd64.deb) ...
Traitement des actions différées (« triggers ») pour « man-db »...
Paramétrage de openssl-blacklist (0.5-2) ...
Paramétrage de liblzo2-2 (2.03-2) ...
Paramétrage de libpkcs11-helper1 (1.07-1) ...
Paramétrage de openvpn-blacklist (0.4) ...
Paramétrage de openvpn (2.1.3-2+squeeze2) ...
Restarting virtual private network daemon.:.
root@ServeurVPN:~# _
```

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Installation d'OpenSSL pour la sécurisation des données :

Généralement, OpenSSL est installé par défaut sur les machines et ne nécessite donc pas d'être réinstallé.

```
> apt-get install openssl
```

Ce qui nous donne :

```
root@ServeurVPN:~# apt-get install openssl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
openssl est déjà la plus récente version disponible.
openssl passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@ServeurVPN:~# _
```

Donc, dans notre cas OpennSSL était déjà installer.

B) Génération des certificats :

L'installation d'OpenVPN crée un dossier dans **/usr/share/doc/openvpn/easy-rsa/** contenant tous les scripts permettant de générer facilement tous les certificats et clés d'authentification nécessaire au fonctionnement d'OpenVPN.

Ces certificats permettront de procéder a l'échange d'une clé de session et permettront de vérifier l'identité des parties.Ils nécessitent bien sûr d'utiliser une autorité de certification(AC) , qui sera créée par nos soins.

La connexion entre le serveur et un client du VPN se passe de la façon suivante :

-Chaque entité du VPN (Serveur Inclus) doit disposer d'un certificat valide.

- A la connexion , le client vérifie le certificat du serveur grâce au certificat de l'AC.

-Le client soumet son certificat et si celui-ci est vérifié grace au certificat de l'AC et qu'il ne se trouve pas sur la liste de révocation , la connexion est mise en place.

Le paquet « easy-rsa » installé précédemment va faciliter la création des certificats requis ; il contient en effet un ensemble de scripts permettant de gérer ces certificats.

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

C) Le fichier de variables :

Avant toute chose, créez un dossier easy-rsa dans le répertoire d'OpenVPN et copier les scripts originaux dedans afin de centraliser applications et scripts :

```
> mkdir /etc/openvpn/easy-rsa/
```

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

On crée ensuite un dossier keys destiné à contenir les différents certificats et clés générés :

```
> mkdir /etc/openvpn/easy-rsa/keys/
```

A partir du dossier **/etc/openvpn/easy-rsa/**, il faut dans un premier temps éditer le fichier « vars » afin d'initialiser différentes variables servant à la génération des certificats :

Comme vous le verrez ci-après , renseigner ces différents champs facilitera la création des clés dans la suite des opérations.

Deux méthodes s'offre à nous pour configurer le fichier « vars »

- Première méthode :

```
> nano /etc/openvpn/easy-rsa/vars
```

On entre les informations personnelles comme suit :

```
Export KEY_DIR=$D/keys
Export KEY_COUNTRY=''FR''
Export KEY_PROVINCE=''FR''
Export KEY_CITY=''Dugny''
Export KEY_ORG=''serveurvpn'
Export KEY_EMAIL=''frederic_95140@hotmail.fr''
```

Ce qui nous donne :

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

- Deuxième méthode :

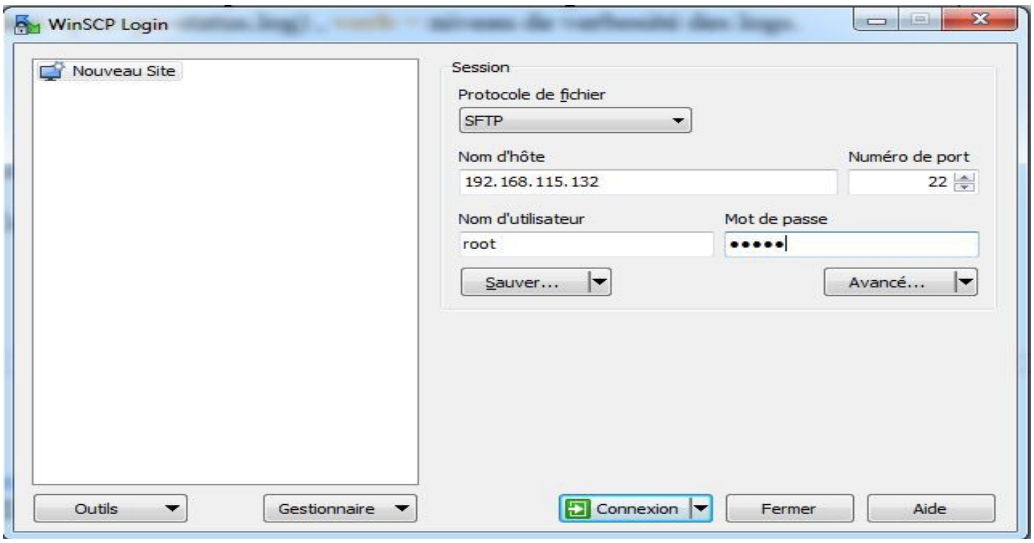
On télécharge et installe WinSCP.

WinSCP est un client SFTP graphique pour Windows. Il utilise SSH et est open source. Le protocole SCP est également supporté. Le but de ce programme est de permettre la copie sécurisée de fichiers entre un ordinateur local et un ordinateur distant.

On fait **ifconfig** pour voir notre adresse IP, dans notre cas notre adresse ip est : « 192.168.115.132 »

```
root@ServeurVPN:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:34:ad:37
          inet adr:192.168.115.132  Bcast:192.168.115.255  Masque:255.255.255.0
          adr inet6: fe80::20c:29ff:fe34:ad37/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6602 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3046 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:8334941 (7.9 MiB)  TX bytes:174271 (170.1 KiB)

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:165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:26317 (25.7 KiB)  TX bytes:26317 (25.7 KiB)
```

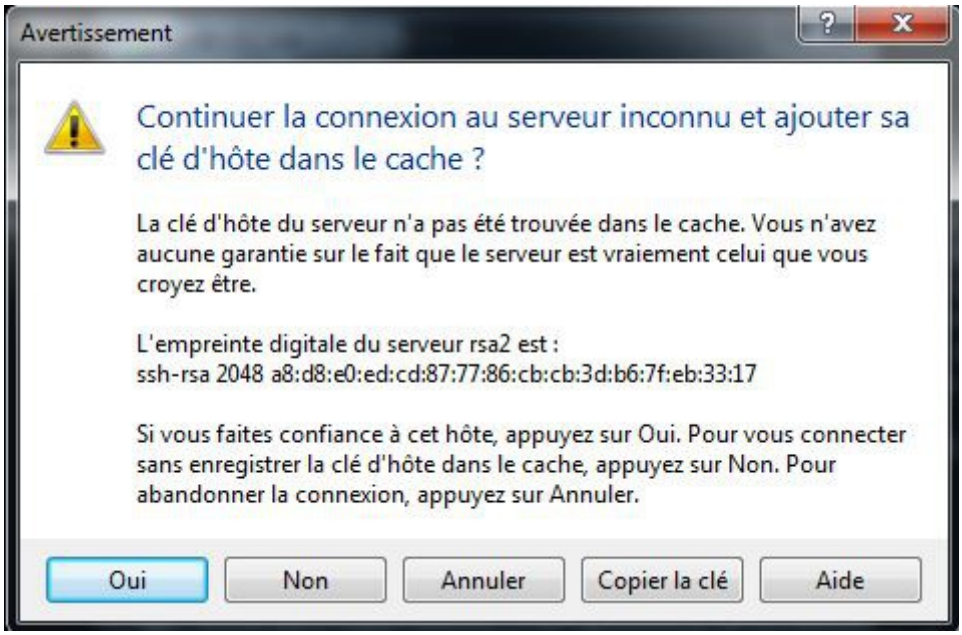
Puis on remplit les différents champs comme dans l'image :
- Protocole de fichier : **« SFTP »**
- Nom d'hôte : **« 192.168.115.132 »**
- Nom d'utilisateur : **« root »**
- Numéro de port : **« 22 »**
- Mot de passe : **« admin »**



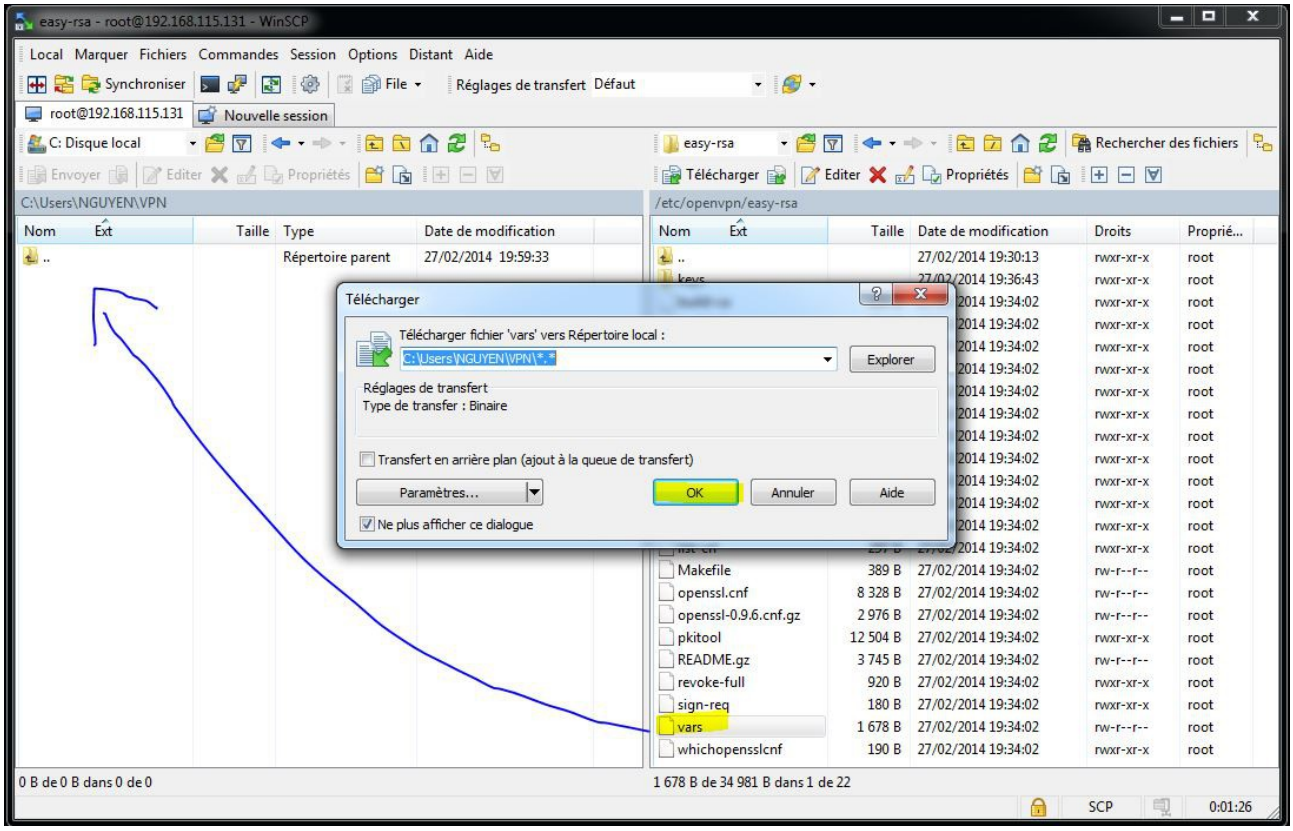
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Une fenêtre apparaît, on met « Oui »



On transfère depuis la machine, le fichier « vars » qui se situe dans le répertoire « /etc/openvpn/easy-rsa/» vers notre ordinateur avec WinSCP.



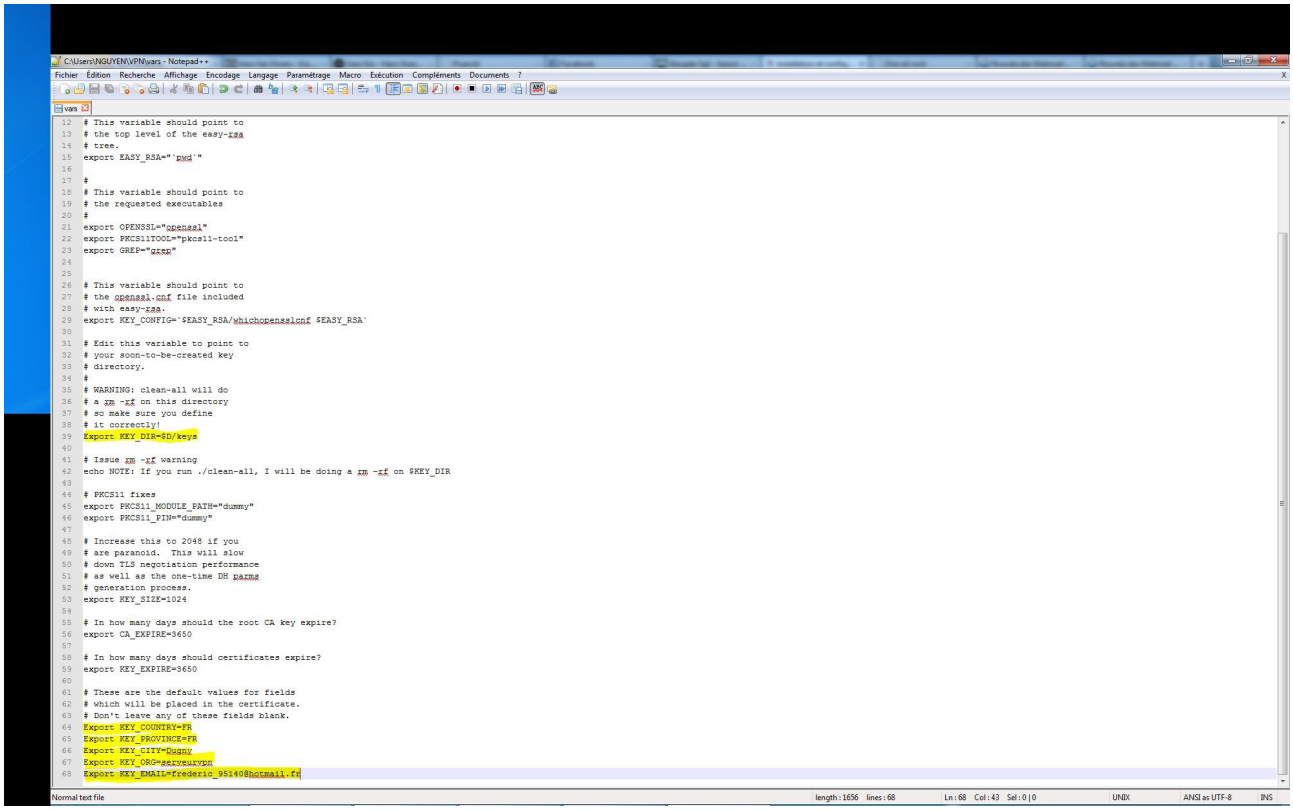
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Depuis notre ordinateur, on ouvre bloc note le fichier « vars », on modifie ces champs et on enregistre :

```
Export KEY_DIR=$D/keys
Export KEY_COUNTRY=''FR''
Export KEY_PROVINCE=''FR''
Export KEY_CITY=''Dugny''
Export KEY_ORG=''serveurvpn'
Export KEY_EMAIL=''frederic_95140@hotmail.fr''
```

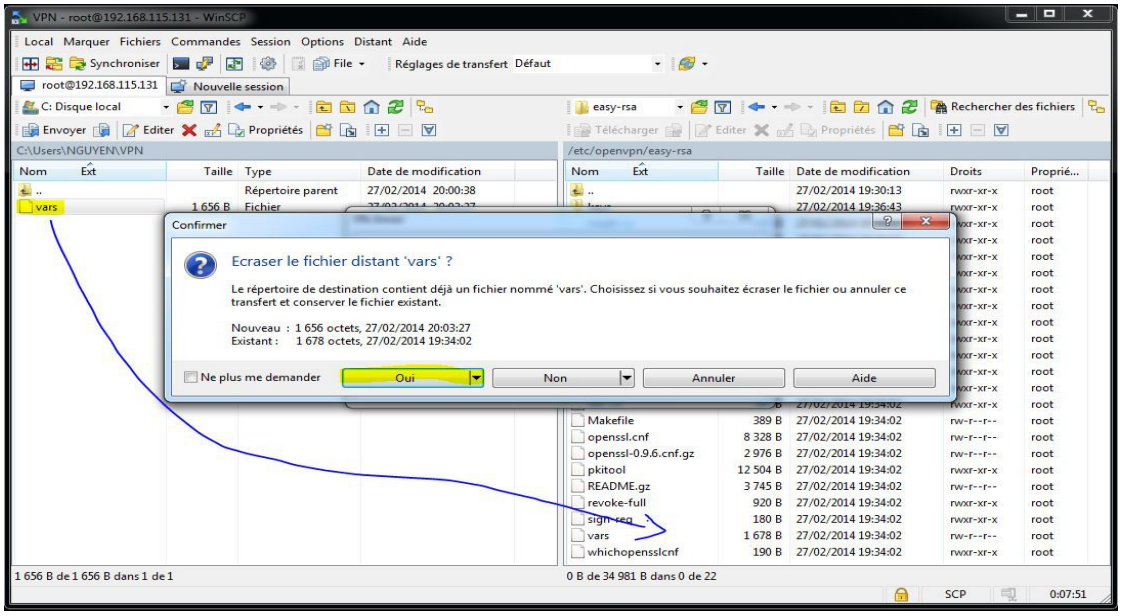
Ce qui nous donne :



NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Puis on transfère depuis WinSCP dans « /etc/openvpn/easy-rsa/ » et on met « Oui » pour l'écraser



On exécute enfin le script afin d'initialiser les variables :

```
> . ./vars
```

Ceci fait , on met à jour le fichier via la commande :

```
> source ./vars
```

Puis on exécute la commande :

```
> ./clean-all
```

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

D) L'autorité de certification :

On crée un certificat d'autorité de certification (fichiers « ca.crt » et « ca.key ») avec la commande :

```
> ./build-ca
```

il faut faire **[Entrée]** à toutes les questions.

Ce qui nous donne :

```
root@ServeurVPN:/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) [FR]:
State or Province Name (full name) [FR]:
Locality Name (eg, city) [Dugny]:
Organization Name (eg, company) [serveurvpn]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [serveurvpn CA]:
Name []:
Email Address [frederic_95140@hotmail.fr]:
root@ServeurVPN:/etc/openvpn/easy-rsa#
root@ServeurVPN:/etc/openvpn/easy-rsa# _
```

Tous les certificats et les clés créés sont stockés automatiquement dans le répertoire keys/ . Les fichier .key ne doivent pas être accessibles en lecture/écriture que par leur propriétaire respectif.

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

E) L'autorité du serveur :

La génération du certificat et de la clé du serveur VPN se fait simplement, par l'exécution du script build-key-server, toujours à partir du dossier **/etc/openvpn/easy-rsa** :

Différentes informations sont demandées pendant l'exécution de ce script :

« Commun-name » : Entrez le nom du serveur que vous avez pour lancer le script, pour notre cas c'est « ServerVPN »
« Sign the certificate ? » : tapez "yes"
« 1 out of 1 certificate requests certificated, commit » : tapez "yes"

Ce script conduit à la création des fichiers nom_choisi_du_serveur.crt et nom_choisi_du_serveur.key dans le dossier /etc/openvpn/easy-rsa/keys.

```
> ./build-key-server nom_choisi_du_serveur
```

Dans notre cas ça sera :

```
> ./build-key-server serveurvpn
```

Ce qui donne :

```
Name []:
Email Address [frederic_95140@hotmail.fr]:

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:'FR'
stateOrProvinceName   :PRINTABLE:'FR'
localityName          :PRINTABLE:'Dugny'
organizationName      :PRINTABLE:'serveurvpn'
commonName            :PRINTABLE:'serveurvpn'
emailAddress          :IA5STRING:'frederic_95140@hotmail.fr'
Certificate is to be certified until Feb 25 20:36:18 2024 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
```

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

F) Le certificat du client :

On crée les certificats du(des) client(s) avec :

```
> ./build-key nom_du_client1
```

Dans notre cas, le nom du client est « client1 » ce qui donne :

```
> ./build-key nom_du_client1
```

Pour le paramètre « Commun-name », saisissez le même nom que nom_du_client1 que vous avez utilisé dans la commande.

Répétez cette opération autant de fois que vous voulez pour générer plusieurs certificats et clés si vous avez plusieurs clients. N'oubliez pas cependant de changer de nom_du_client à chaque fois .

Ce script entraine la création des fichiers nom_du_client1.crt et nom_du_client1.key dans le dossier /etc/opnevpn/easy-rsa/keys.

Ce qui donne :

```
Name []:
Email Address [frederic_95140@hotmail.fr]:

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:'FR'
stateOrProvinceName   :PRINTABLE:'FR'
localityName          :PRINTABLE:'Dugny'
organizationName      :PRINTABLE:'serveurvpn'
commonName            :PRINTABLE:'client1'
emailAddress          :IA5STRING:'frederic_95140@hotmail.fr'
Certificate is to be certified until Feb 25 20:45:19 2024 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
```

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

III) Configuration du Serveur

Dans cette partie nous allons configurer le serveur.

Dans notre contexte le serveur VPN doit avoir comme adresse : « 192.168.3.254 »

Donc on va changer notre ip en fessant :

```
> nano /etc/network/interfaces
```

Et on mettra dans interfaces :

```
# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see
interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

#NetworkManager

auto eth0
iface eth0 inet dhcp
 address 192.168.3.251
 network 192.168.3.0
 netmask 255.255.255.0
broadcast 192.168.0.255
 gateway 192.168.0.254
```

Puis on fait un « reboot »

Le script de démarrage d'OpenVPN recherche les fichiers .conf se trouvant dans « /etc/openvpn/ ».

Nous allons donc créer un fichier de configuration dans ce répertoire :

```
> nano /etc/openvpn/server.conf
```

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Et on mettera dans server.conf :

```
     # Elements de base

port 1194
proto udp
dev tun
comp-lzo
persist-key
persist-tun
keepalive 10 120

server 24.0.0.0 255.255.255.0

#         Parametres ssl
ca easy-rsa/keys/ca.crt
cert easy-rsa/keys/servervpn.crt
key easy-rsa/keys/servervpn.key
dh easy-rsa/keys/dh1024.pem
#               Logs
status openvpn-status.log
verb 3
```

port = port d'écoute d'OpenVPN (ici 1194) , proto = Protocol utilisé (ici udp), dev tun = Tunnel IP , comp-lzo = active la compression des paquets , persist-key et persist-tun = rendent l'acces au cles et au périphérique tun persistant au redémarrage, keepalive = garder la connexion active meme si rien ne se passe, server = adresse du serveur dans le VPN , push "route"= serveur joignable via la connexion VPN ,push "redirect-gateway" = pour que le trafic passe entierement par le VPN , status = enregistre l'état courant du serveur(ici dans openvpn-status.log) , verb = niveau de verbosité des logs.

Voila, la configuration du côté serveur est terminée.

Pour démarrer le serveur, la commande est :

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

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

IV) Configuration des Clients

Dans cette partie voir comment configurer un client Linux et un client Windows pour ce connecter au VPN.

A) Client Linux :

Le client Linux nécessite la même installation que le serveur :

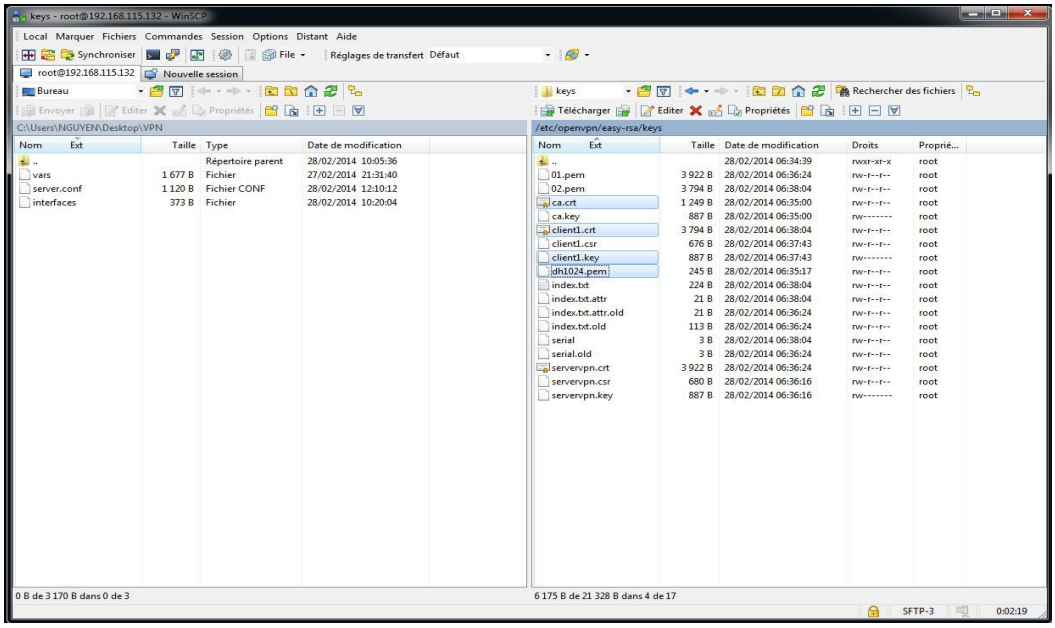
```
> apt-get install openvpn
```

Pour garder une certaine cohérence entre le serveur et les clients, j'utilise la même hiérarchie de dossiers sur les clients que sur le serveur. Ainsi, on crée un dossier « config » et un dossier « /easy-rsa/keys dans /etc/openvpn »

```
> mkdir /etc/openvpn/config && mkdir /etc/openvpn/easy-rsa && mkdir /etc/openvpn/easy-rsa/keys
```

Pour fonctionner, les clients ont besoin de 4 fichiers provenant du serveur :

1. ca.crt
2. nom_du_client1.crt
3. nom_du_client1.key
4. le fichier de configuration client.conf



NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Voici le contenu du fichier client.conf permettant de se connecter au serveur défini précédemment :

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.0.31 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nogroup

# Try to preserve some state across restarts.
persist-key
```

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

```
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca easy-rsa/keys/ca.crt
cert easy-rsa/keys/client1.crt
key easy-rsa/keys/client1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

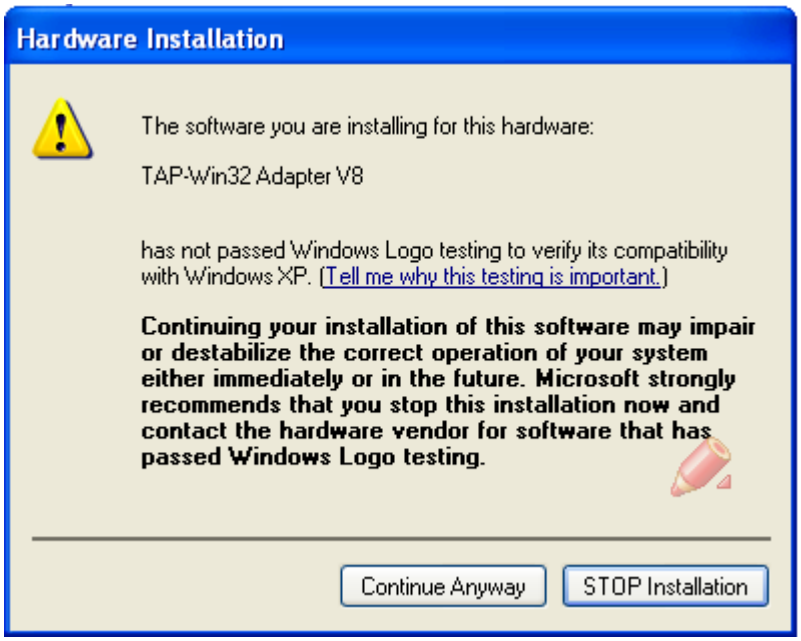
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

B) Client Windows :

Pour le client Windows, il est nécessaire d'installer une application spécifique, OpenVPN GUI for Windows, qui se trouve ici :
http://openvpn.se

Une fois téléchargée, lancer l'installation d'OpenVPN. Une fenêtre vous demandera si vous acceptez d'installer une nouvelle interface «TAP-Win32 Adapter V8». Acceptez.



L'installation finie, deux petits ordinateurs avec un globe font leur apparition dans la barre des tâches. Cela correspond à l'interface virtuelle nouvellement créée « TAP-Win32 Adapter V8 » permettant la connexion au VPN.

 ← Icône de l'interface TAP Win32 pour OpenVPN dans la barre des tâches de Windows.

Copiez les 4 fichiers suivants dans le dossier « C:\Program Files\OpenVPN\config **»** :

- 1. ca.crt
- 2. nom_du_client1.crt
- 3. nom_du_client1.key
- 4. client.conf

→ Il faut renommer le fichier client.conf en client.ovpn

NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

La configuration du fichier de configuration client.ovpn est la même que pour un client Linux, excepté pour les chemins de fichiers. Si les certificats et clés sont bien placés dans le dossier config, le contenu du fichier client.ovpn doit être :

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.0.31 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nogroup
```

NGUYEN
Frédéric
BTS SIO

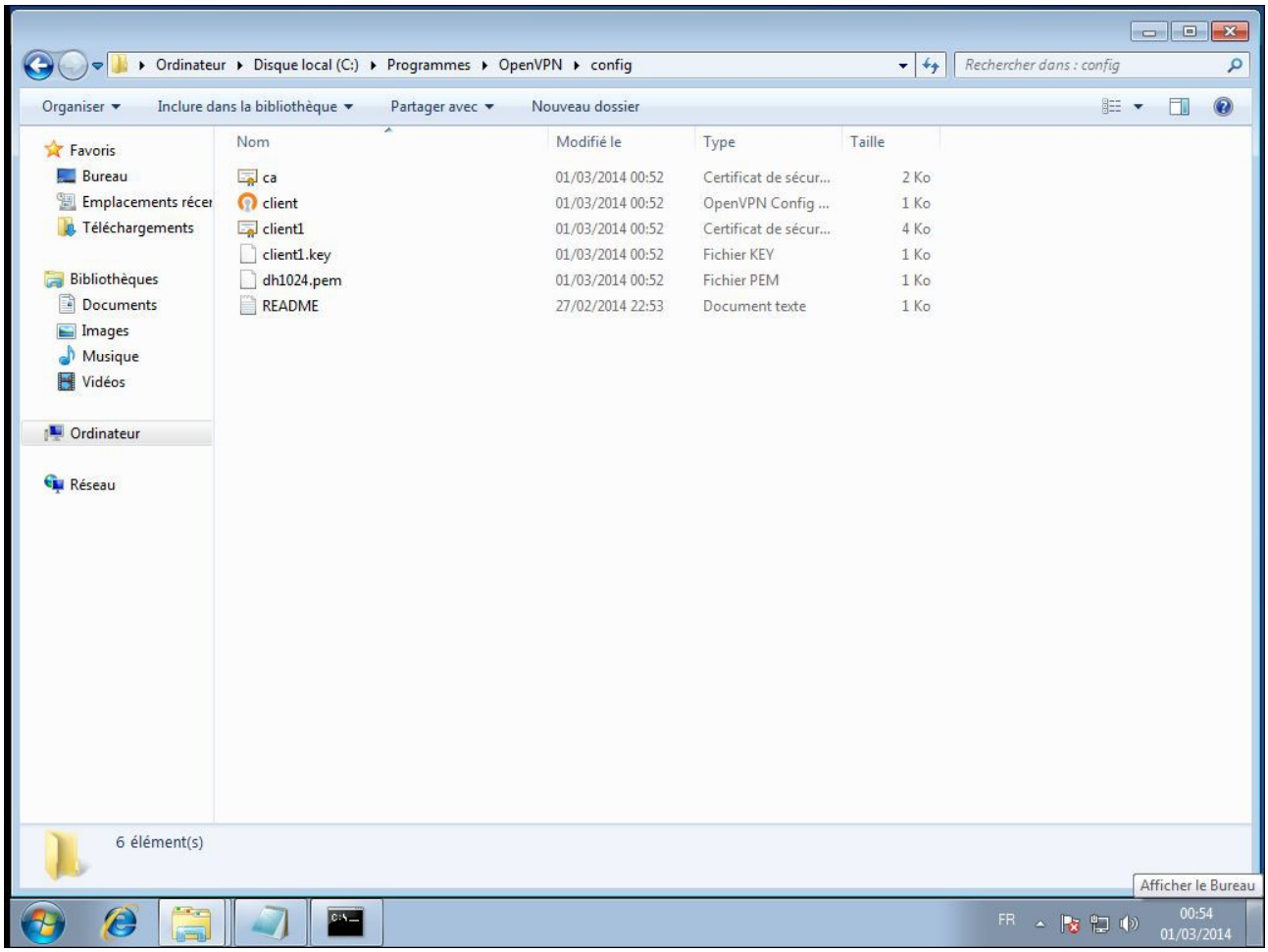
Installation d'un VPN avec OpenVPN sous Debian Squeeze

```
# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca easy-rsa/keys/ca.crt
cert easy-rsa/keys/client1.crt
key easy-rsa/keys/client1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

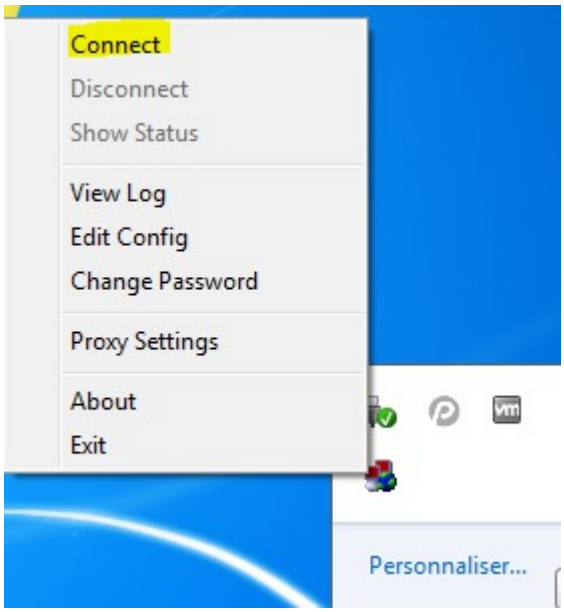
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Ce qui donne :



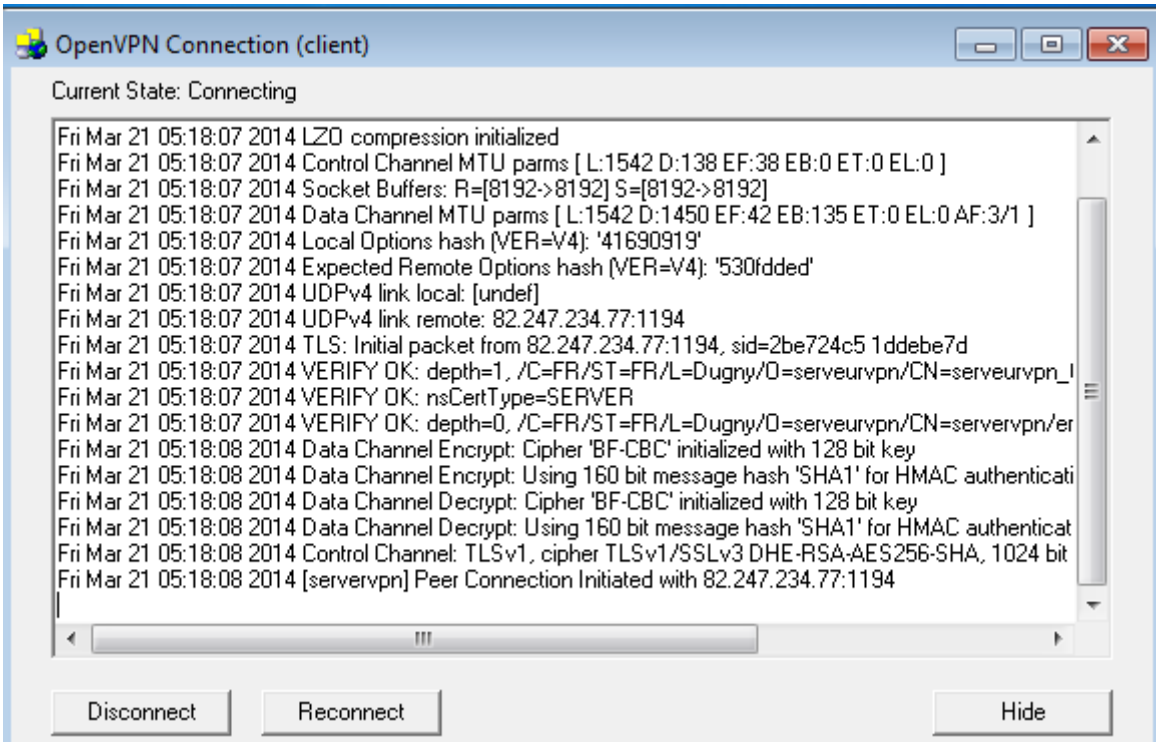
Pour se connecter au VPN, un clic droit sur l'icône d'interface « TAP-Win32 Adaptater V8 » et « connect »



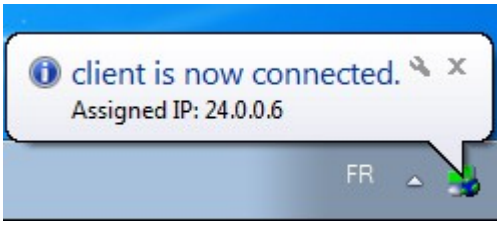
NGUYEN
Frédéric
BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Une fenêtre appârait alors :



Si la connexion au VPN est un succès, les écrans de l'icône de l'interface « TAP-Win32 Adaptater V8 » deviennent verts.



Le tutoriel est maintenant finis.