TheGreenBow IPSec VPN Client

Guide de Configuration

Linux StrongS/Wan, FreeS/Wan ou OpenS/Wan

WebSite: http://www.thegreenbow.com

Contact: support@thegreenbow.com

Table des matières

1 Introduction

1.1 But du document

Le but de ce document est de décrire comment configurer le Client IPSec VPN TheGreenBow avec un routeur VPN basé sur Linux StrongS/Wan, FreeS/Wan ou OpenS/Wan.

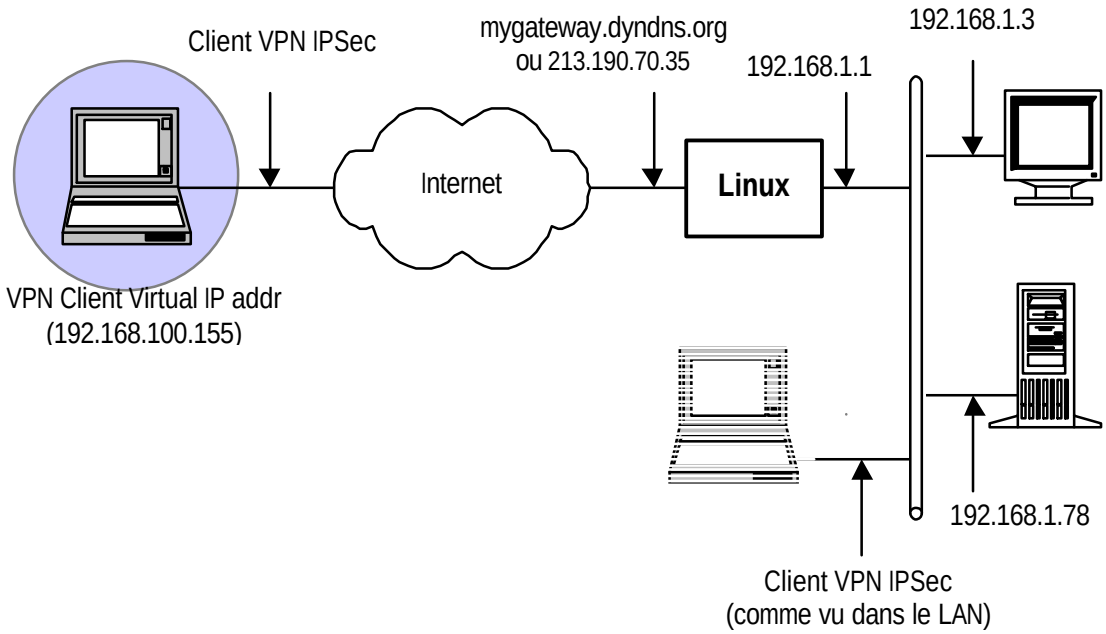
Pour plus d'information sur Linux IPSec, se référer aux sites web suivants:

- Linux StrongSwan Version V2.1.3 (http://www.strongswan.org/)
- Linux FreeSWan Version V1.9.9 oder V2.0.6 (http://www.freeswan.org/)
- Linux OpenSWan Version V2.1.2 (http://www.openswan.org/)
- Patches for X.509-Certifikate (http://www.strongsec.com/), AES-Patches, NAT Traversal, Notify-Delete

Ce document a été écrit avec le support de CapLaser s.a. (www.caplaser.fr).

1.2 Topologie réseau

Dans cet exemple, le Client VPN IPSec TheGreenBow doit se connecter au LAN derrière le routeur VPN Linux. Le Client VPN est connecté à Internet via une connexion Dial up ou un accès DSL du FAI. Le Client VPN aura une adresse IP virtuelle dans le réseau local distant. Toutes les adresses IP dans ce document sont données à titre d'exemple.



1.3 Configuration du système Linux

Les tests et les configurations VPN sont basés sur Linux Redhat 8. Linux Redhat 8 doit être installé avec GRUB comme boot loader.

Le RPMS de Linux Strong/Wan peuvent être téléchargés depuis http://www.lamerzklan.de/~eldoc/strongswan. Il faut un pack RPM compatible avec votre matériel. Dans ce document nous utiliserons le RPM kernel-2.4.26-4.ipsec.i386.rpm et les commandes StrongS/wan: strongswan-userland-2.0.2-rh8.i386.rpm.

2 Installation des RPMs

L'installation démarre avec le nouveau noyau compilé avec VPN IPSec en utilisant la commande **« rpm –ivh kernel-2.4.26-4.ipsec.i386.rpm »**.

Vérifier que le nouveau noyau est le noyau par défaut dans le fichier grub.conf. Modifier le fichier grub.conf si nécessaire. Pour se faire, remplacer la valeur correcte dans le champs « default=x ».

Puis installer le pack strongswan-userland-2.0.2-rh8.i386.rpm utiliser la commande **« rpm –ivh strongswan-userland-2.0.2-rh8.i386.rpm »**.

En utilisant la commande « **ntsysv** », vérifier que le démon IPSec est sélectionné pour démarrer quand la machine reboote. Puis rebooter la machine.

3 Configuration VPN IPsec du routeur Linux

Cette section décrit une configuration VPN IPSec avec votre routeur VPN Linux. La documentation du site web NAT CARLSON (http ://www.natecarlson.com/linux/ipsec-x509.php) a été utilisée pour configurer les Certificats sur le routeur VPN Linux.

Linux StrongSwan est une branche de FreeSwan similaire au projet OpenSwan sur lequel est basée cette documentation.

3.1 Installation du Certificate Authority

1) Ouvrir le fichier /usr/share/ssl/openssl.cnf. Il contient des valeurs par défaut pour la génération de Certificat OpenSSL.

Il faut changer les options suivantes:

'default_days ': C'est la durée, en jour, de validité de votre certificat. la valeur par défaut est 365 jours, soit un an. Une valeur de ' 3650 ' donne 10 ans de validité de vos certificats. Rappelez-vous qu'il peut être révoqué à tout moment.

'[req_distinguished_name] ': Vous n'avez pas besoin de changer les options dessous req_distinguished_name; Elles sont des valeurs par défaut (comme le nom de la société, etc.) pour la génération des certificats. Il est plus facile de les entrer ici plutôt de le changer pour chaque création de certificat.

2) Créer un fichier pour stocker votre CA. Vous pouvez utiliser le chemin suivant /var/sslca (vous pouvez choisir le nom que vous voulez). Changez les permissions du répertoire en 700, pour que les utilisateurs ne puissant pas atteindre les clés privées.

3) Publier le script /usr/share/ssl/misc/CA, et changer la ligne indiquant ' DAYS="days 365" ' avec un nombre très grand. Vérifier que ce nombre est plus grand que le nombre en étape 1) sinon Windows n'acceptera pas vos Certificats. Note: un nombre trop grand peut poser des problèmes.

4) Lancer la commande **'CA -newca '**: répondre aux questions en utilisant les exemples ci dessous pour configurer votre réseau.

Valeur en Rouge et **commentaires en Bleue.**

Ne jamais utiliser de caractère non-alphanumerique (e.g. -,+, /,...)

```
nate@example:~/sslca$ /usr/share/ssl/misc/CA -newca
CA certificate filename (or enter to create)
(entrer)
Making CA certificate ...
Using configuration from /usr/lib/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....+++++
..+++
.....+++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase: (entrer password) Password utilisé pour creer les
autres certificats.
Verifying password - Enter PEM pass phrase: (repeter password)
-----
```

```
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) [AU]:US(entrer) Entrer country code, FR pour
France
State or Province Name (full name) [SomeState]: State(entrer) Entrer pour
state/province, par exemple MidiPyrenees
Locality Name (eg, city) []:City(entrer) Entrer Ville
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
ExampleCo(entrer) Entrer nom société (ou laisser blanc)
Organizational Unit Name (eg, section) []:(entrer) laisser blanc
Common Name (eg, YOUR name) []:CA(entrer) Entrer le nom du Certificate
Authority
Email Address []:ca@example.com(entrer)
nate@example:~/sslca$
```

Aussi créer un fichier CRL:

```
nate@example:~/sslca$ openssl ca -gencrl -out crl.pem
```

Ce fichier CRL doit être mis à jour chaque fois que vous révoquez un certificat.

C'est fait; vous avez votre propre Certificate Authority, que vous pouvez utiliser pour créer les Certificats. Maintenant, vous devez créer un Certificat pour chaque machine qui doit établir une connexion IPSec. Ceci inclut le routeur VPN, et chaque Client VPN.

3.2 Création du Certificat pour le routeur VPN

La section suivante détaille comment créer un Certificat et comment le convertir au bon format.

Utiliser le script CA une fois de plus, mais cette fois il sera utilisé pour signer les Certificats au lieu de créer un nouveau "Certificate Authority".

```
nate@example:~/sslca$ /usr/share/ssl/misc/CA -newreq
Using configuration from /usr/lib/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....................................+++
.....................................+++
writing new private key to 'newreq.pem'
Enter PEM pass phrase: (entrer password) Password pour encrypter la
nouvelle clé privée du certificat.
Verifying password - Enter PEM pass phrase:(répeter password)
-----
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) [AU]:US(entrer)
State or Province Name (full name)[Some-State]:State(entrer)
Locality Name (eg, city) []:City(entrer)
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:ExampleCo(entrer)
Organizational Unit Name (eg, section) []:(entrer)
Common Name (eg, YOUR name) []:host.example.com(entrer) peut être le
```

```
hostname, nom reel, email adresse, ou n'importe quelle info.
Email Address []:user@example.com(entrer) (optionnel)

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:(entrer)
An optional company name []:(entrer)
Request (and private key) is in newreq.pem
```

Vous venez de générer un "certificate request". Ceci est équivalent à envoyer une requête à Thawte ou Verisign pour récupérer un Certificat à utiliser dans SSL. Pour vos propres besoins, vous le signerez avec votre propre CA.

```
nate@example:~/sslca$ /usr/share/ssl/misc/CA -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter PEM pass phrase: (password que vous avez entre en creant le CA)
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'State'
localityName :PRINTABLE:'City'
organizationName :PRINTABLE:'ExampleCo'
commonName :PRINTABLE:'host.example.com'
emailAddress :IA5STRING:'user@example.com'
Certificate is to be certified until Feb 13 16:28:40 2012 GMT (3650 days)
Sign the certificate? [y/n]:y(entrer)

1 out of 1 certificate requests certified, commit? [y/n]y(entrer)
Write out database with 1 new entries
Data Base Updated
Signed certificate is in newcert.pem
```

Puis, renommer les fichiers créés pour simplifier l'usage futur.

```
nate@example:~/sslca$ mv newcert.pem host.example.com.pem
nate@example:~/sslca$ mv newreq.pem host.example.com.key
```

Vous aurez besoin de ces 2 fichiers ainsi que le fichier 'cacert.pem' et le fichier 'crl.pem'.

3.3 Création du certificat pour le Client VPN TheGreenbow

La création du Certificat du Client VPN est faite de la même façon que celle du Routeur VPN. Cependant, utilisez winhost.example.com, plutôt que host.example.com dans la procédure pour distinguer les Certificats.

Il est alors nécessaire de convertir ce Certificat au format P12 reconnu par Windows.

```
$ openssl pkcs12 -export -in winhost.example.com.pem -inkey
winhost.example.com.key -certfile demoCA/cacert.pem -out
winhost.example.com.p12
```

3.4 Installation des certificats

Installer les fichiers dans leurs propres répertoires:

```
$ cp /var/sslca/host.example.com.key /etc/ipsec.d/private
$ cp /var/sslca/host.example.com.pem /etc/ipsec.d/certs
$ cp /var/sslca/winhost.example.com.key /etc/ipsec.d/private
$ cp /var/sslca/winhost.example.com.pem /etc/ipsec.d/certs
$ cp /var/sslca/demoCA/cacert.pem /etc/ipsec.d/cacerts
$ cp /var/sslca/crl.pem /etc/ipsec.d/crls/crl.pem
```

Une fois le Certificat P12 créé pour le Client VPN, sauver le sur un disque amovible USB (USB Memory Stick)

3.5 Configuration de OpenSwan sur le routeur VPN

Pour information, la machine utilisée pour les tests est appelée fw2.caplaser.net et les Certificats sont créés avec ce nom. Adapter les lignes à votre propre situation.

3.1.1 Configuration du fichier ipsec.secrets

Ajouter la ligne suivante au fichier **/etc/ipsec.secrets**:

```
: RSA host.example.com.key "password"
```

Le password indiqué ici est le password utilisé au moment de la création du Certificat SSL.

Le fichier **ipsec.secrets** ne contient pas le Certificat Racine car il est trop volumineux.

```
: RSA{
      # RSA 2192 bits   fw2.caplaser.net   Fri Sep 24 13:26 :26 2004
      # for signatures only, UNSAFE FOR ENCRYPTION
      # Quite some stuff already in there that must not be removed to
please the “ipsec verify” command that might not like it …
      }
# do not change the indenting of that «} »
# Added line
: RSA fw2.caplaser.net.key "password"
```

3.1.2 Configuration du fichier ipsec.conf

Le fichier **ipsec.conf** contient:

```
# /etc/ipsec.conf – strongSwan IPSec configuration file
# RCSID $Id : ipsec.conf.in,v 1.2 2004/03/15 21:03 :06 as Exp $

# This file :  /usr/share/doc/freeswan/ipsec.conf-sample
#
# Manual :     ipsec.conf.5
#
# Help :
# http://www.strongsec.com/freeswan/install.htm

version   2.0  # conforms to second version of ipsec.conf
specification

# basic configuration
config setup
```

```
      interfaces=%defaultroute
      nat_traversal=yes
      virtual_private=%v4:10.0.0.0/8,%v4:172.160.0.0/12,%v4:192.168.0.
0/16
      # Debug-logging controls:  « none » for (almost) none, « all »
for lots.
      Klipsdebug=none
      plutodebug=none
      # crlcheckinterval=600
      # strictcrlpolicy=yes

conn %default
      keyingtries=1
      compress=yes
      disablearrivalcheck=no
      authby=rsasig
      leftrsasigkey=%cert
      rightrsasigkey=%cert

# OE policy groups are disabled by default
conn block
      auto=ignore

conn clear
      auto=ignore

conn private
      auto=ignore

conn private-or-clear
      auto=ignore

conn clear-or-private
      auto=ignore

conn packetdefault
      auto=ignore

# Add connections here.

Conn roadwarrior-net
      leftsubnet=192.168.1.0/24
      also=roadwarrior

conn roadwarrior
      left=%defaultroute
      leftcert=fw2.caplaser.net.pem
      right=%any
      rightsubnet=vhost:%no,%priv
      auto=add
      pfs=yes
```

3.1.3 Démarrage du service IPSec

Une fois configuré, le service IPSec peut être démarré avec la commande suivante:

```
/etc/init.d/ipsec restart
```

Vous pouvez utiliser "**restart**" plutôt que "**start**", parce que le RPM active le service IPSec et la machine a déjà été redémarrée. En conséquence, le service IPSec est déjà opérationnel avec la configuration par défaut.

Les logs de StrongSwan sont situés dans **`/var/log/secure`**et ils permettent de pister les problèmes de configuration

Le champ "**net.ipv4.ip_forward**" dans le fichier "**/etc/sysctl.conf**" doit être positionné à 1, puis lancer la commande:

```
/etc/init.d/network restart
```

Vérifier que MASQUERADE est actif pour le trafic sortant sur Internet. S'il n'est pas actif, alors lancer la commande:

```
iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE
iptables-save > /etc/sysconfig/iptables
```

Vous devez remplacer "interface eth0" avec l'interface de votre machine (e.g. ppp0 pour DSL). Lire la documentation sur le routage et le firewall pour plus d'information.

Autres lignes de commandes:

```
mount /mnt/floppy
copy mon_certificat.p12 /mnt/floppy
umount /mnt/floppy
```

4 Configuration du Client VPN Ipsec TheGreenBow

Créer les Certificats nécessaires depuis le fichier P12 précédemment copié depuis le serveur et les copier dans les répertoires concernés (voir aussi http://www.thegreenbow.fr/doc/greenbow-x509.pdf).

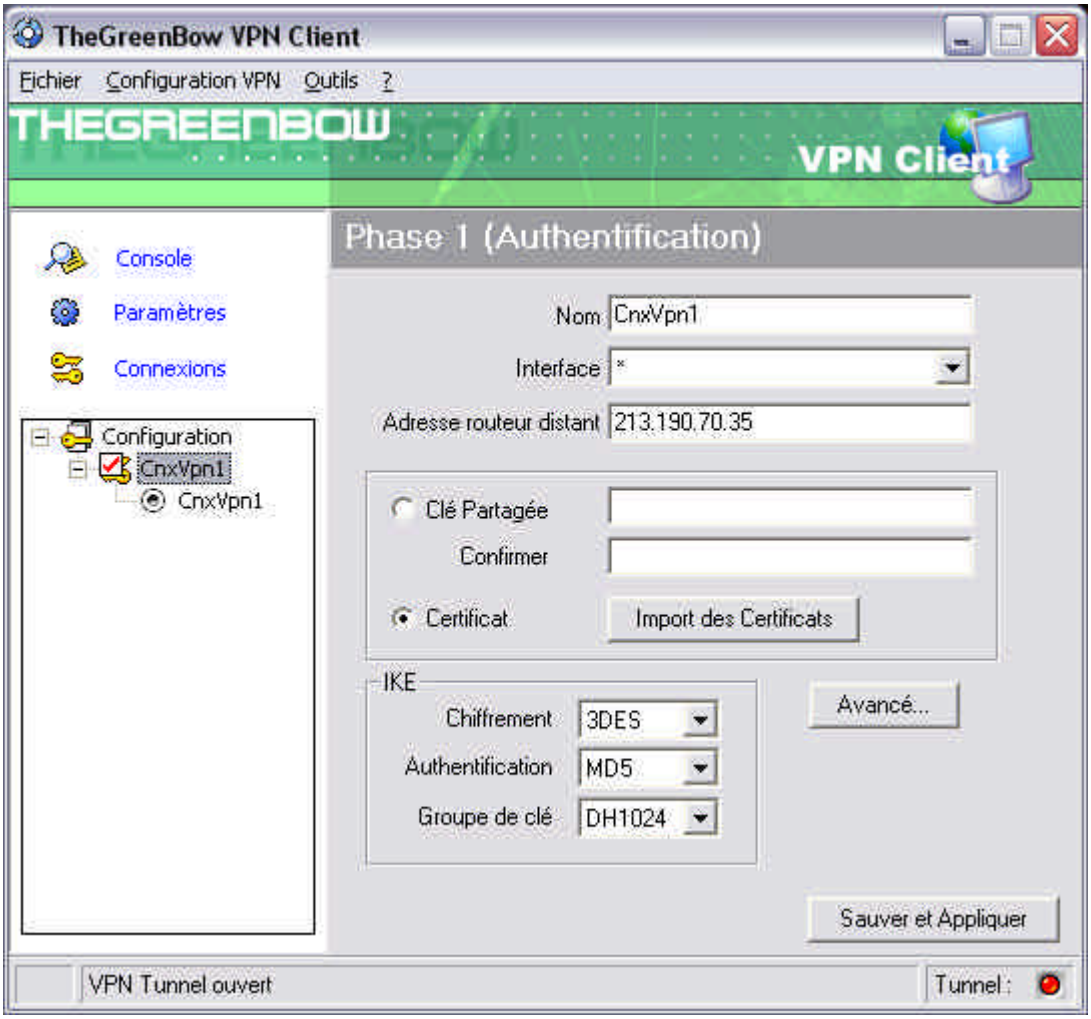
Lancer le Client VPN IPSec TheGreenBow avec l'icône sur le "Bureau" de Windows 

et l'icône de l'application Client VPN doit apparaître dans la barre de tache 

.

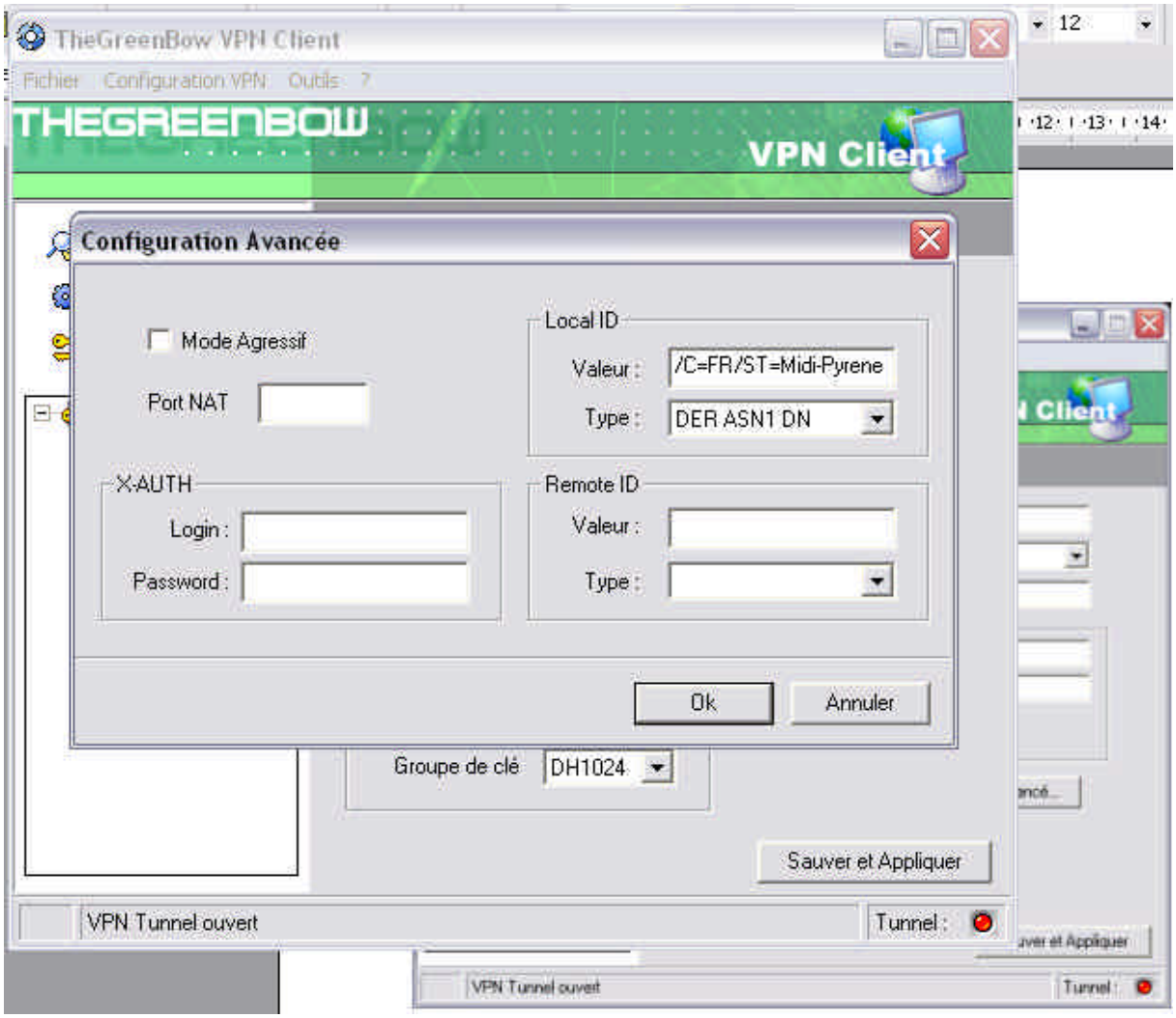
4.1 Configuration de la Phase 1 (IKE)

Vous devez créer une Phase 1 et modifier "**Adresse routeur distant**" avec l'adresse IP Internet de votre Routeur VPN Linux (i.e. 213.190.70.35).



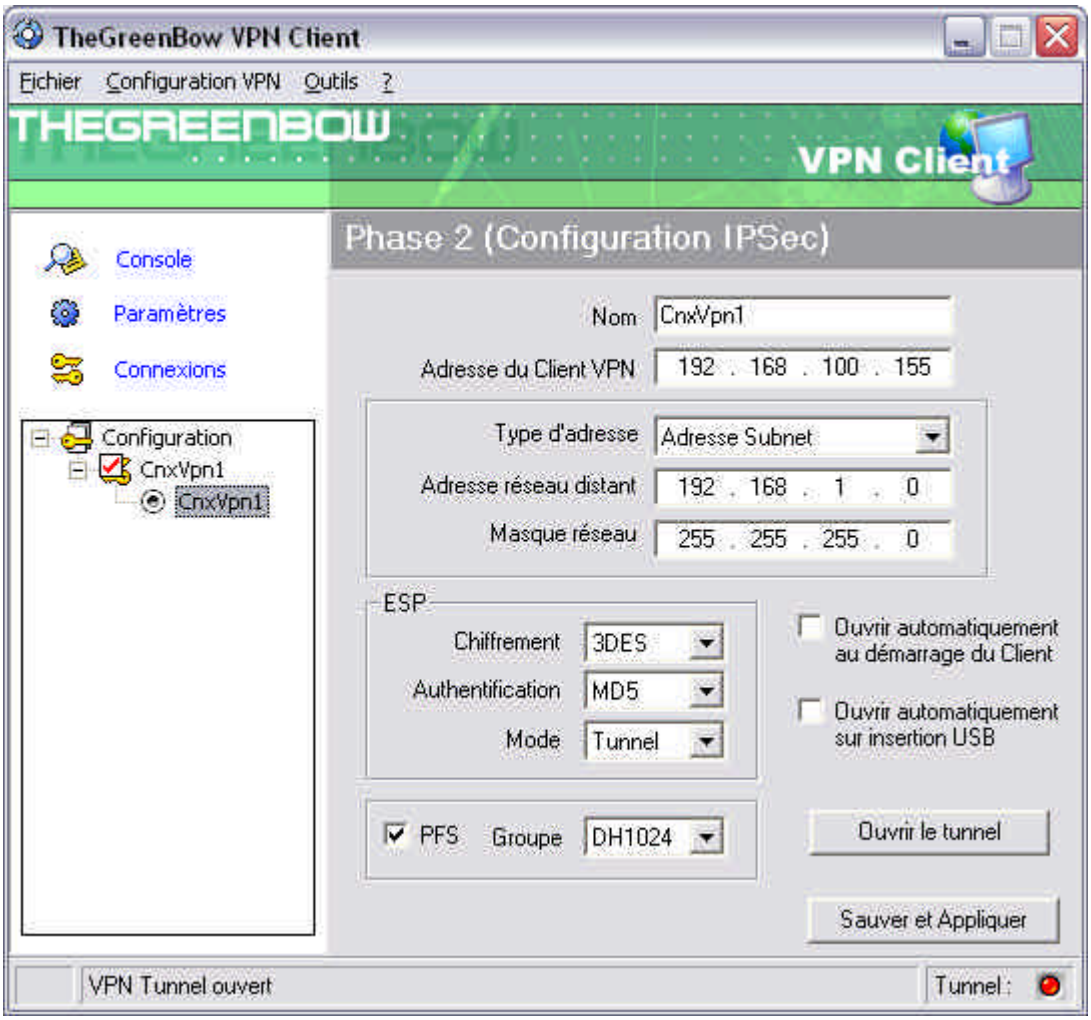
Configuration de la Phase 1

Selectionner "**Certificat**" et importer les certificats que vous avez crée. Cliquer sur "**Avancé …** " et remplir Local ID.



4.2 Configuration du Client VPN Phase 2 (IPSec)

Vous devez créer une Phase 2 (Configuration IPSec) comme suit:



Configuration de la Phase 2

4.3 Ouvrir des tunnels VPN IPSec

Lorsque le routeur VPN Linux et le Client VPN IPSec TheGreenBow ont été configurés, vous êtes prêt pour ouvrir des tunnels VPN. Mais avant tout, soyez certain d'avoir autorisé le trafic IPSec dans votre Firewall.

1. Cliquer sur "**Sauver et Appliquer**" pour prendre en compte les dernières modifications faites votre configuration VPN.

2. Cliquer sur "**Ouvrir le Tunnel**", ou générer du trafic qui ouvrir automatiquement un tunnel IPSec sécurisé (par exemple ping, IE browser).

3. Sélectionner "**Connections**" pour voir les Tunnels VPN

4. Sélectionner "**Console**" si vous voulez avoir accès aux traces VPN IPSec et ajuster les filtres d'affichage de messages IPSec.

5 VPN IPSec Troubleshooting

"J'ai le message XXXXX dans la console". Qu'est ce que cela veut dire ?

Nous rendons disponible pour téléchargement un guide plus complet des messages Console du Client VPN TheGreenBow avec explications et astuces pour résolutions.

Il contient en particulier les messages d'erreurs les plus fréquents et les raisons possibles:

- Message d'erreur « PAYLOAD MALFORMED »
- Message d'erreur « INVALID COOKIE »
- Message d'erreur « no keystate »
- Message d'erreur « received remote ID other than expected »
- Message d'erreur « NO PROPOSAL CHOSEN »
- Message d'erreur « INVALID ID INFORMATION »

Si ce document de troubleshootings VPN ne suffit pas, envoyez-nous tous les échanges avec les lignes RECV et SEND . Réglez les filtres de Log à "0" et cliquez sur "Save File" (i.e. "sauver fichier"). Vous trouverez le fichier de Log dans Program Files \Sistech \TheGreenBow \LogFiles.

6 Contacts

News et mises à jour sur le site web TheGreenBow: http://www.thegreenbow.com

Support Technique par e-mail au support@thegreenbow.com

Contact commercial au +33 1 43 12 39 37 ou par email à l'adresse sales@thegreenbow.com