 **TheGreenBow IPsec VPN Client**
Configuration Guide
**Linux StrongS/Wan,
FreeS/Wan or OpenS/Wan**

WebSite: <http://www.thegreenbow.com>

Contact: support@thegreenbow.com

Table of contents

1	Introduction	3
1.1	Goal of this document	3
1.2	VPN Network topology	3
1.3	Linux VPN Gateway	3
2	Linux system installation	4
3	Linux VPN configuration	4
3.1	Installation of your Certificate Authority	4
3.2	Generate a Certificate for the Gateway	4
3.3	Certificate creation for TheGreenbow VPN Client	4
3.4	Installation des certificats	4
3.5	Configuration of OpenSwan on the gateway	4
3.5.1	Configuration of ipsec.secrets file	4
3.5.2	Configuration of ipsec.conf file	4
3.5.3	Start IPsec service	4
4	TheGreenBow IPsec VPN Client configuration	4
4.1	VPN Client Phase 1 (IKE) Configuration	4
4.2	VPN Client Phase 2 (IPsec) Configuration	4
4.3	Open IPsec VPN tunnels	4
5	Tools in case of trouble	4
5.1	A good network analyser: ethereal	4
5.2	Netdiag.exe	4
6	VPN IPsec Troubleshooting	4
6.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA])	4
6.2	« INVALID COOKIE » error	4
6.3	« no keystate » error	4
6.4	« received remote ID other than expected » error	4
6.5	« NO PROPOSAL CHOSEN » error	4
6.6	« INVALID ID INFORMATION » error	4
6.7	I clicked on "Open tunnel", but nothing happens	4
6.8	The VPN tunnel is up but I can't ping !	4
7	Contacts	4

1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client with a Linux StrongS/Wan, FreeS/Wan or OpenS/Wan VPN router.



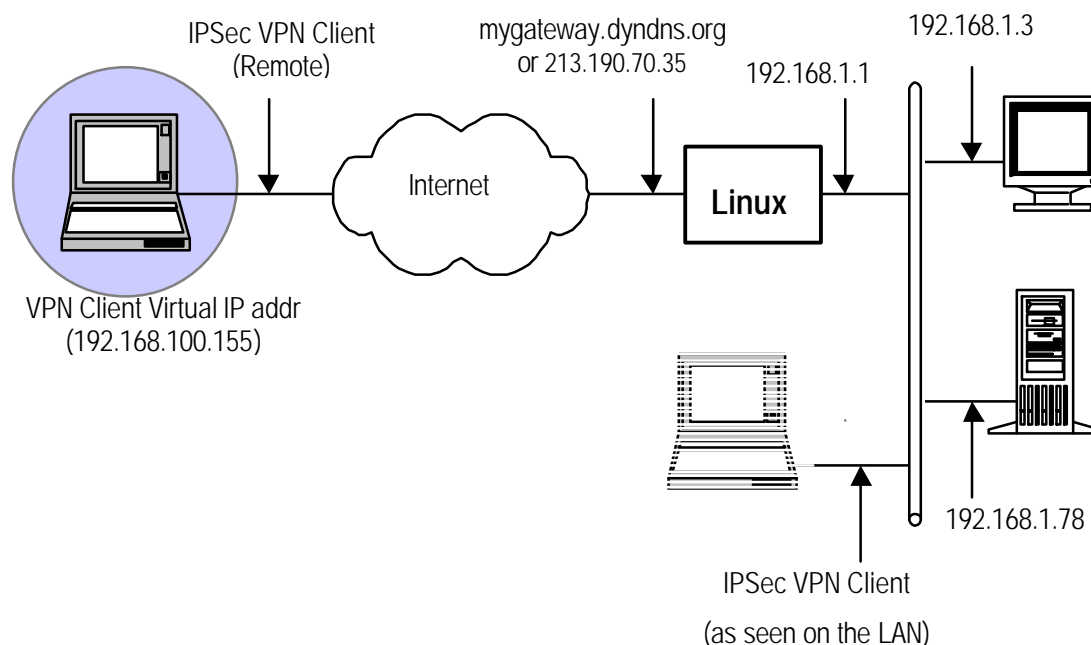
For more information about various version of Linux IPsec please refer to those websites:

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

This document has been written by CapLaser s.a. (www.caplaser.fr).

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client to the LAN behind the Linux gateway. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.



1.3 Linux VPN Gateway

Our tests and VPN configuration have been conducted with Linux Redhat 8. Linux Redhat 8 must be installed and updated with GRUB as a **boot loader**.

The RPMS of Linux StrongS/wan can be downloaded from <http://www.lamerzklan.de/~eldoc/strongswan>.

You'll need a RPM pack from the kernel compatible with your hardware. In this document, we've been using the RPM kernel-2.4.26-4.ipsec.i386.rpm and StrongS/wan commands: strongswan-userland-2.0.2-rh8.i386.rpm.

	Doc.Ref	tgvpn_ug_Linux_en
	Doc.version	2.0 – Feb.2005
	VPN version	2.5x

2 Linux system installation

Installation starts with the new kernel compiled with IPsec VPN using the following command « **rpm -ivh kernel-2.4.26-4.ipsec.i386.rpm** ».

Check that this kernel is the default kernel within the grub.conf file, which is not always the case. Modify grub.conf if necessary. To do so, replace the correct value in the field « default=x ».

Then, install the pack strongswan-userland-2.0.2-rh8.i386.rpm using the following command « **rpm -ivh strongswan-userland-2.0.2-rh8.i386.rpm** ».

Using command « **ntsysv** », check that IPsec daemon is selected to start when the machine boots. Then reboot the machine.

3 Linux VPN configuration

This section describes how to build an IPSec VPN configuration with your Linux VPN gateway. Documentation from NAT CARLSON website (<http://www.natecarlson.com/linux/ipsec-x509.php>) has been used to configure Certificates on the Linux VPN Gateway.

Linux StrongSwan being a fork project of FreeSwan and similar to OpenSwan project from upon this documentation is based.

3.1 Installation of your Certificate Authority

1) Open the file `/usr/share/ssl/openssl.cnf`. This contains default values for OpenSSL Certificate generation.

You'll need to change following options:

'**default_days** ': This is the duration, in days, during which your certificates will be valid, and the default value is 365 days, that is to say 1 year. A value of ' 3650 ' will give 10 years of validity to our certificates. Remember it can be revoked anytime.

'[**req_distinguished_name**] ': You don't really need to change the options below the `req_distinguished_name`; they are only default values (such as the place, the name of company, etc.) for the generation of certificates. It is easier to type them here than to change them for each certificate creation.

2) Create a file to store your CA. You can use something like `/var/sslca`; you may chose the name you want. Change the permissions of the folder into 700, so that people cannot reach the private keys, which they are not supposed to reach.

3) Publish script `/usr/share/ssl/misc/CA`, and set the line which indicates ' `DAYS="days 365"` ' with a very high number (this indicates how long the certificate of the authority of certificate is valid.) Make sure that this number is higher than the value of the step 1; or Windows can not accept your Certificates. Note that if this number is too high, it can cause problems.

4) Launch command '**CA -newca** ': answer questions using examples below with settings of your network.

Inputs are Red and **comments are Blue**.

Never use non non-alphanumeric characters (e.g. -,+,/,...)

```
nate@example:~/sslca$ /usr/share/ssl/misc/CA -newca
CA certificate filename (or enter to create)
(enter)
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:(enter password) That's the password you'll to
create other certificates.
Verifying password - Enter PEM pass phrase:(repeat 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(enter) Enter country code, FR for
France
State or Province Name (full name) [SomeState]: State(enter) Enter your
state/province, for example MidiPyrenees
Locality Name (eg, city) []:City(enter) Enter City name
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
ExampleCo(enter) Enter company name (or leave it blank)
Organizational Unit Name (eg, section) [):(enter) can be left blank
Common Name (eg, YOUR name) []:CA(enter) Enter the name of your Certificate
Authority
Email Address []:ca@example.com(enter)
nate@example:~/sslca$
```

Also let's create a crl file, which you will need on your gateway:

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

You will have to update this CRL file each time you revoke a certificate.

It is done; you now have your own Certificate Authority, which you can use to produce the Certificates. Now, you will have to produce of a certificate for each machine that will establish an IPSec connection. This includes the gateway, and each one of your VPN Client machine.

3.2 Generate a Certificate for the Gateway

The following section details how to create a certificate, and to convert it into the right format for Windows.

Once more, we'll use the CA script but this time it will be used to sign Certificates instead of creating a new "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:(enter password) Password to encrypt the new private
key of the certificate.
Verifying password- Enter PEM pass phrase:(repeat 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 ht 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(enter)
State or Province Name (full name) [SomeState]:State(enter)
Locality Name (eg, city) []:City(enter)
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ExampleCo(enter)
Organizational Unit Name (eg, section) [):(enter)
Common Name (eg, YOUR name) []:host.example.com(enter) This can be a
hostname, a real name, an email address, or pretty much anything.
```

	Doc.Ref	tgvpn_ug_Linux_en
	Doc.version	2.0 – Feb.2005
	VPN version	2.5x

Email Address [**]** **user@example.com(enter)** (optional)

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password [**]** **{enter}**

An optional company name [**]** **{enter}**

Request (and private key) is in newreq.pem

You've just generated a certificate request. This is equivalent to sending a request to Thawte or Verisign to get a Certificate you'd use in SSL. For your own need, you'll sign it with your own CA:

```
nate@example:~/sslca$ /usr/share/ssl/misc/CA -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter PEM pass phrase: (password you've entered while creating the 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(enter)

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

Then, just rename created files for easier use in future.

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

That all you need to do for the OpenSwan gateway - You will need these two files as well as the 'cacert.pem' file created in the file 'demoCA', and the 'crl.pem' file generated earlier, as explained further in upcoming sections.

3.3 Certificate creation for TheGreenbow VPN Client

The creation of the certificate of the VPN Client is made exactly same manner as for the gateway. However, use winhost.example.com, instead of host.example.com in the procedure in order to distinguish the certificates.

It is then necessary to convert this certificate with the P12 format recognized by 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

Install the files at their appropriate location (create the files of destination if the RPM did not do that for you):

```
$ 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/cacertpem /etc/ipsec.d/cacerts
$ cp /var/sslca/crl.pem /etc/ipsec.d/crls/crl.pem
```

Once the P12 Certificate for VPN Client is created, save it on a USB Stick memory (removable disk).

3.5 Configuration of OpenSwan on the gateway

For information, the machine used for tests is called fw2.caplaser.net and the certificates were created with this name. Adapt the following lines to your case.

3.5.1 Configuration of ipsec.secrets file

Add the following line to the `/etc/ipsec.secrets` file:

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

The password indicated here is the password used at the time of the creation of SSL Certificate.

Here the `ipsec.secrets` file resulting from the tests where the contents of the root certificate has been removed because it's too big.

```
: 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 the « } »
# Added line
: RSA fw2.caplaser.net.key "password"
```

3.5.2 Configuration of ipsec.conf file

Here the `ipsec.conf` file:

```
# /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,%v4:172.16.0.0/12,%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
```

3.5.3 Start IPsec service

Once configured, IPsec service can be started with the following command:

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

You can use "restart" instead of "start", because the RPM activates the IPsec service and the machine has been rebooted already. Therefore the IPsec service is already under operation with the default configuration.

The Linux StrongSwan logs can indicate configuration problems and are located in **/var/log/secure**

The field "net.ipv4.ip_forward" in the file "/etc/sysctl.conf" must be set to 1, then launch command:

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

Check that MASQUERADE is active for the outgoing traffic to the Internet. In case it is not active, then launch command:

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

You must replace "interface eth0" with your machine interface to the Internet (e.g. ppp0 for DSL). Look at documentation on routing and firewall for more information.

Other useful command lines:

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

4 TheGreenBow IPsec VPN Client configuration

Create the necessary certificates from the P12 file copied previously from the server and copy them in the folder of your choice (also look at <http://www.thegreenbow.fr/doc/greenbow-x509.pdf>).

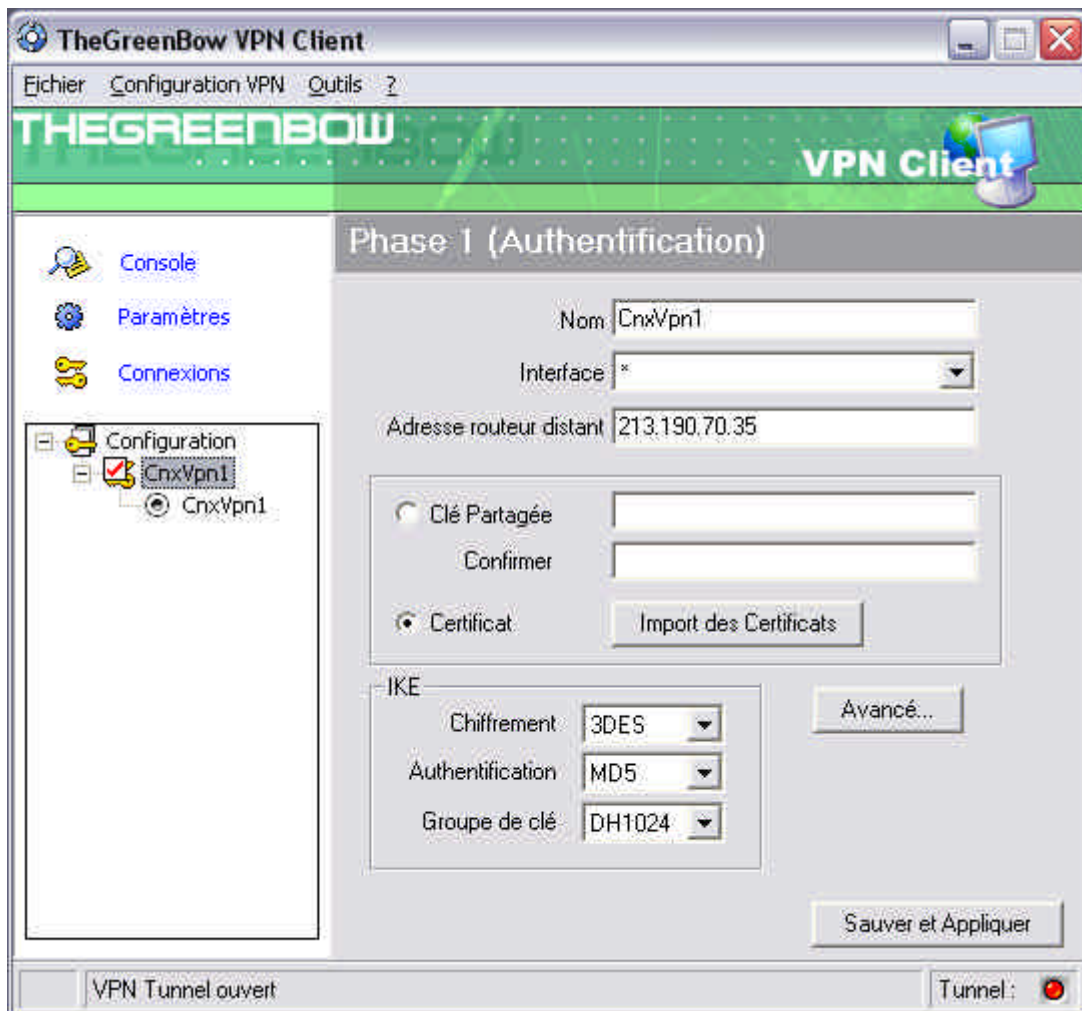


Launch TheGreenBow IPsec VPN Client with the icon on your Windows desktop and VPN client application icon should appear on the task bar



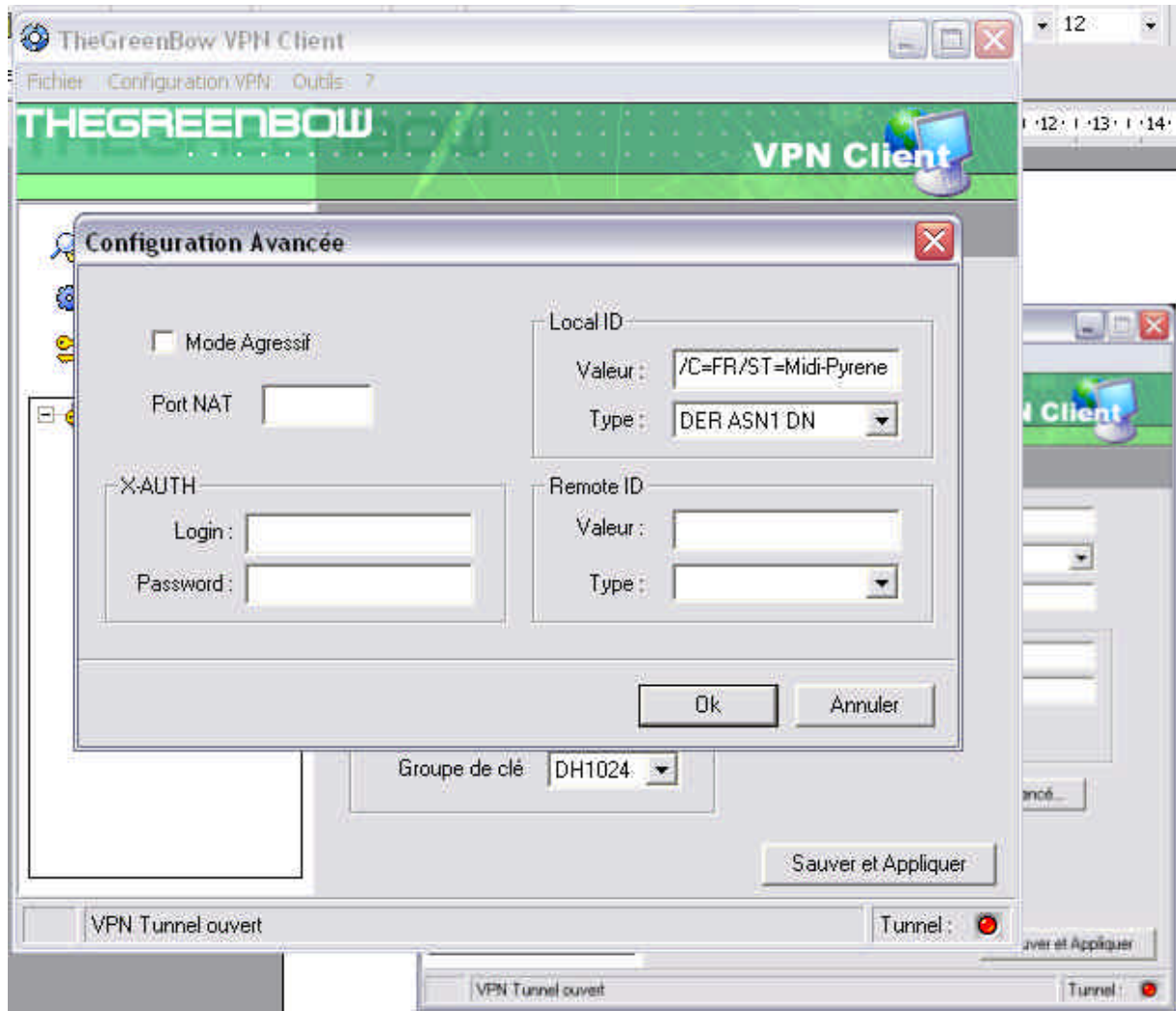
4.1 VPN Client Phase 1 (IKE) Configuration

You must create a new Phase 1 and modifying "Remote Gateway Address" with the Internet fixed IP address of your Linux gateway (i.e. 213.190.70.35).



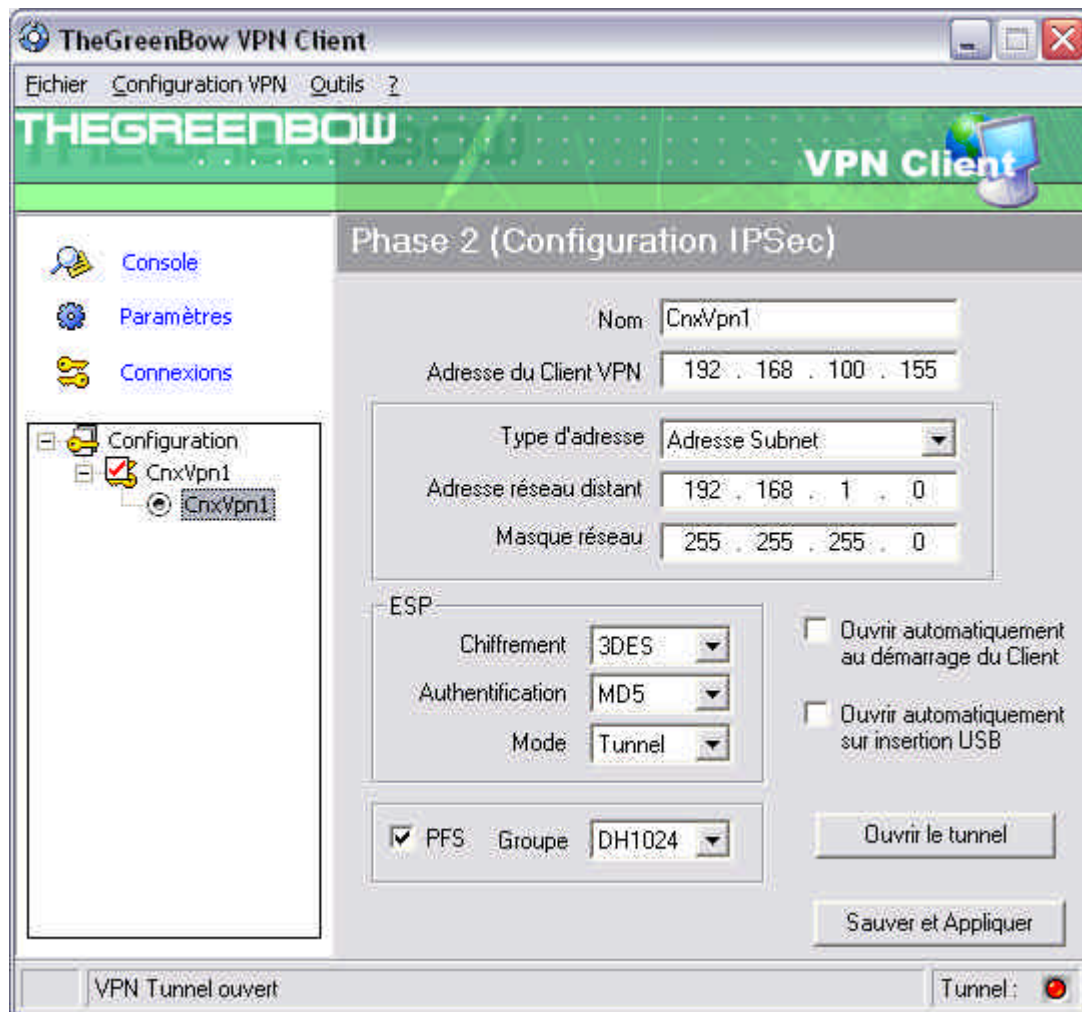
Phase 1 configuration

Select "**Certificate**" and import the certificates that you have just created with the "Certificate" tool as indicated in its documentation. Click on "**Advanced ...**" button and make a copy/paste of the value "DER ASN1 DN" created by the "Certificate" tool.



4.2 VPN Client Phase 2 (IPSec) Configuration

You must create a Phase 2 (Configuration IPSec) as following:



Phase 2 Configuration

4.3 Open IPSec VPN tunnels

Once both Linux router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

1. Click on "**Save & Apply**" to take into account all modifications we've made on your VPN Client configuration
2. Click on "**Open Tunnel**", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)
3. Select "**Connections**" to see opened VPN Tunnels
4. Select "**Console**" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Microsoft Windows 2000 Server.

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
2	0.153567	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
3	0.205363	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
4	0.257505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
5	0.300882	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
6	0.310186	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
7	0.313742	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
8	0.321913	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
9	0.323741	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
10	0.334980	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
11	0.691160	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
12	1.692568	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
13	1.693164	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)
14	2.693600	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
15	2.694026	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)

Frame 1 (142 bytes on wire, 142 bytes captured)
 Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff

5 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

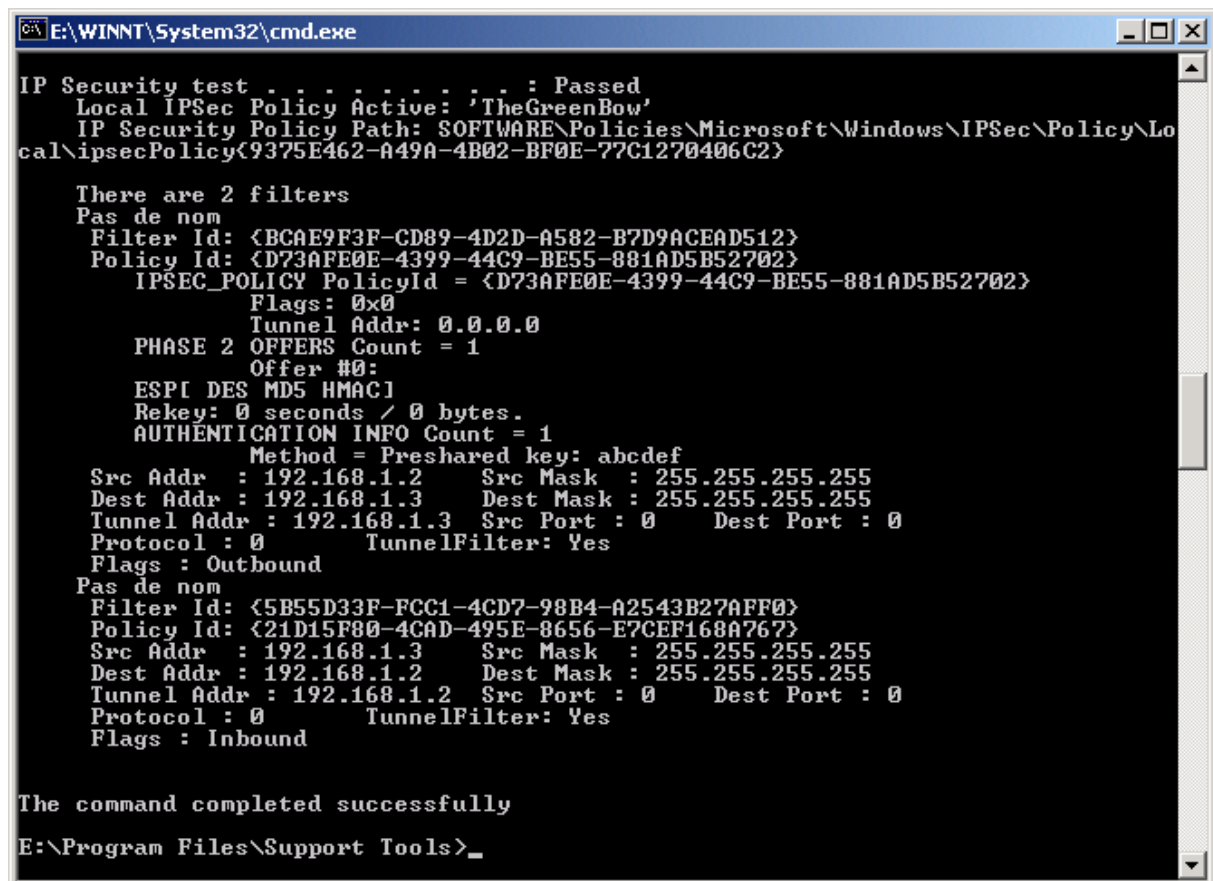
5.1 A good network analyser: ethereal

Ethereal is free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website <http://www.ethereal.com/>. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.

5.2 Netdiag.exe

Netdiag.exe can be found in Microsoft Windows 2000 Server Support Tools. Read Knowledge base article Q257225 for more details.

In a window CMD.EXE, type "select netdiag /test :ipsec /debug". Output will be:



```
E:\WINNT\System32\cmd.exe
IP Security test . . . . . : Passed
Local IPSec Policy Active: 'TheGreenBow'
IP Security Policy Path: SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local\ipsecPolicy{9375E462-A49A-4B02-BF0E-77C1270406C2}

There are 2 filters
Pas de nom
Filter Id: {BCAE9F3F-CD89-4D2D-A582-B7D9ACEAD512}
Policy Id: {D73AFE0E-4399-44C9-BE55-881AD5B52702}
IPSEC_POLICY PolicyId = {D73AFE0E-4399-44C9-BE55-881AD5B52702}
Flags: 0x0
Tunnel Addr: 0.0.0.0
PHASE 2 OFFERS Count = 1
Offer #0:
ESP{ DES MD5 HMAC}
Rekey: 0 seconds / 0 bytes.
AUTHENTICATION INFO Count = 1
Method = Preshared key: abcdef
Src Addr : 192.168.1.2   Src Mask : 255.255.255.255
Dest Addr : 192.168.1.3   Dest Mask : 255.255.255.255
Tunnel Addr : 192.168.1.3   Src Port : 0   Dest Port : 0
Protocol : 0   TunnelFilter: Yes
Flags : Outbound
Pas de nom
Filter Id: {5B55D33F-FCC1-4CD7-98B4-A2543B27AFF0}
Policy Id: {21D15F80-4CAD-495E-8656-E7CEF168A767}
Src Addr : 192.168.1.3   Src Mask : 255.255.255.255
Dest Addr : 192.168.1.2   Dest Mask : 255.255.255.255
Tunnel Addr : 192.168.1.2   Src Port : 0   Dest Port : 0
Protocol : 0   TunnelFilter: Yes
Flags : Inbound

The command completed successfully
E:\Program Files\Support Tools>_
```

6 VPN IPSec Troubleshooting

6.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

```
114920 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [SA][VID]
114920 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

6.2 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOK IE
115933 Default SEND Informational [NOTIFY] with INVALID_COOKIE error
```

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

6.3 « no keystate » error

```
115315 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [SA][VID]
115317 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [SA][VID]
115317 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [KEY][NONCE]
115319 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [KEY][NONCE ]
115319 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

6.4 « received remote ID other than expected » error

```
120348 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [SA][VID]
120349 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [SA][VID]
120349 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [KEY][NONCE]
120351 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [KEY][NONCE]
120351 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.

6.5 « NO PROPOSAL CHOSEN » error

```

115911 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [SA][VID]
115913 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [SA][VID]
115913 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [KEY][NONCE]
115915 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [KEY][NONCE]
115915 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915 Default (SA CNXVPN1 -CNXVPN1 -P2) SEND phase 2 Quick Mode
[SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational [HASH][DEL]
115915 Default CNXVPN1 -P1 deleted
    
```

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

```

115911 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [SA][VID]
115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error
    
```

6.6 « INVALID ID INFORMATION » error

```

122623 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1 -P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626 Default (SA CNXVPN1 -CNXVPN1 -P2) SEND phase 2 Quick Mode
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational [HASH][DEL]
122626 Default CNXVPN1 -P1 deleted
    
```

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type ("Subnet address" and "Single address"). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

6.7 I clicked on "Open tunnel", but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

6.8 The VPN tunnel is up but I can't ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- ? Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- ? Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- ? Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- ? Check your ISP support ESP

- ? If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
- ? Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
- ? You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- ? We recommend you to install ethereal (<http://www.ethereal.com>) on one of your target computer. You can check that your pings arrive inside the LAN.

	Doc.Ref	tgvpn_ug_Linux_en
	Doc.version	2.0 – Feb.2005
	VPN version	2.5x

7 Contacts

News and updates on TheGreenBow web site : <http://www.thegreenbow.com>

Technical support by email at support@thegreenbow.com

Sales contacts at +33 1 43 12 39 37 ou by email at info@thegreenbow.com