 **TheGreenBow IPSec VPN Client**
Configuration Guide
SmoothWall
Corporate Server

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

Contact: support@thegreenbow.com

Table of contents

1	Introduction	0
1.1	Goal of this document	0
1.2	VPN Network topology	0
1.3	SmoothWall Corporate Server	0
2	SmoothWall Corporate Server VPN configuration	0
2.1	SmoothWall Preparing Certificates	0
2.2	SmoothWall Configuring SmoothTunnel IPsec Road Warrior connection	0
3	TheGreenBow IPsec VPN Client configuration	0
3.1	VPN Client Preparing Certificates	0
3.2	VPN Client Phase 1 (IKE) Configuration	0
3.3	VPN Client Phase 2 (IPsec) Configuration	0
3.4	Open IPsec VPN tunnels	0
4	VPN IPsec Troubleshooting	0
4.1	« PAYLOAD MALFORMED » error	0
4.2	« INVALID COOKIE » error	0
4.3	« no keystate » error	0
4.4	« received remote ID other than expected » error	0
4.5	« NO PROPOSAL CHOSEN » error	0
4.6	« INVALID ID INFORMATION » error	0
4.7	I clicked on "Open tunnel", but nothing happens	0
4.8	The VPN tunnel is up but I can't ping !	0
5	Contacts	0

1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client with a SmoothWall Corporate Server VPN gateway.

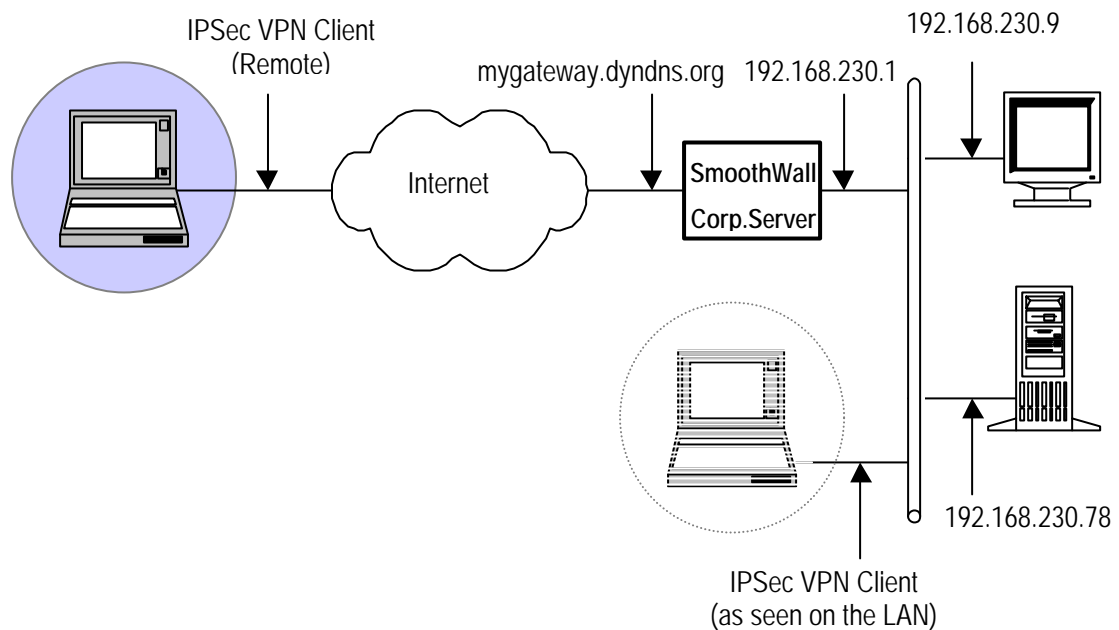
This VPN Configuration Guide has been written with the kind contribution of www.k4dot.com and SmoothWall Limited.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client to the LAN behind the SmoothWall Corporate Server 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.

A Road Warrior connection also needs to be configured. The following example makes use of these values:

- External IP of the SmoothTunnel: 192.168.72.236
- IP Subnet behind the SmoothTunnel: 192.168.230.0/255.255.255.0
- IP of the Road Warrior when connected: 192.168.230.3



1.3 SmoothWall Corporate Server

Our tests and VPN configurations have been conducted using SmoothWall Corporate Server 3 with the SmoothTunnel 3.1 module installed.

2 SmoothWall Corporate Server VPN configuration

This section describes how to build an IPSec VPN configuration with your SmoothWall Corporate Server VPN Gateway.

2.1 SmoothWall Preparing Certificates

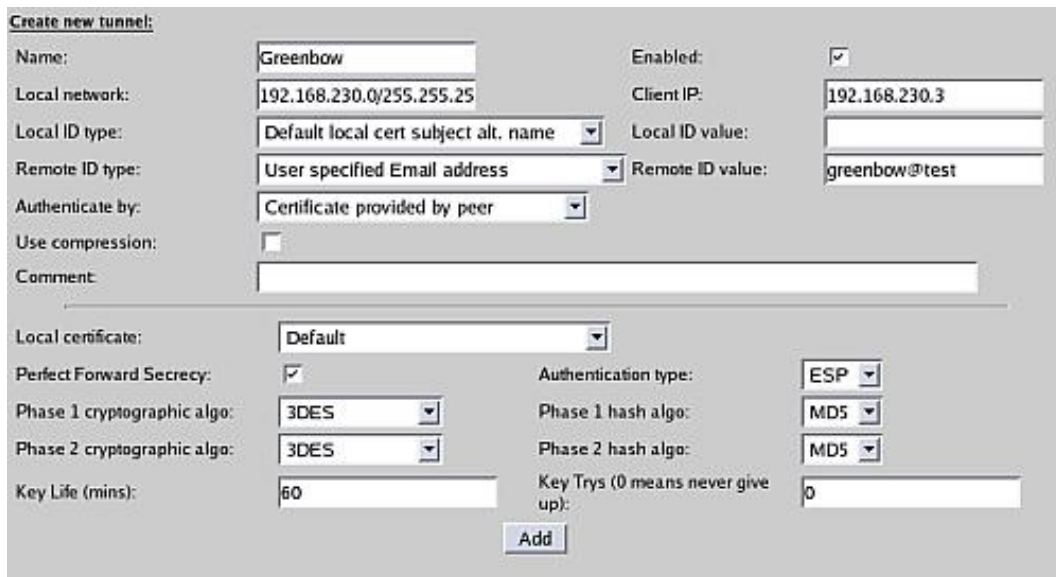
TheGreenBow IPSec VPN Client will need both the CA certificate and a certificate made especially for TheGreenBow VPN Client.

- ID type+value for the SmoothTunnel certificate: DNS: greenbow.test
- ID type+value for TheGreenBow certificate: EMAIL: greenbow@test

2.2 SmoothWall Configuring SmoothTunnel IPSec Road Warrior connection

A certificate for TheGreenBow VPN Client will have to be created. Once this is done, a VPN configuration for TheGreenBow VPN connection needs to be made.

Below is a screenshot of a configuration made with the values cited above.



The screenshot shows the 'Create new tunnel' configuration window. The fields are filled with the following values:

- Name: Greenbow
- Local network: 192.168.230.0/255.255.25
- Local ID type: Default local cert subject alt. name
- Remote ID type: User specified Email address
- Authenticate by: Certificate provided by peer
- Use compression:
- Comment: (empty)
- Local certificate: Default
- Perfect Forward Secrecy:
- Phase 1 cryptographic algo: 3DES
- Phase 2 cryptographic algo: 3DES
- Key Life (mins): 60
- Enabled:
- Client IP: 192.168.230.3
- Local ID value: (empty)
- Remote ID value: greenbow@test
- Authentication type: ESP
- Phase 1 hash algo: MD5
- Phase 2 hash algo: MD5
- Key Trys (0 means never give up): 0

An 'Add' button is located at the bottom center of the form.

This VPN configuration is the standard way of configuring an IPSec Road warrior. This VPN configuration can be used for SSH Sentinel, Safenet Softremote and TheGreenBow VPN Clients.

Note the Local and Remote ID type and value. The remote ID type and value is entered fully here – whereas the local ID type and value only has the type selected and nothing is entered in the Local ID value field. The value will be retrieved automatically from the certificate selected on the "global" page, so there is no need to enter the local ID value here.

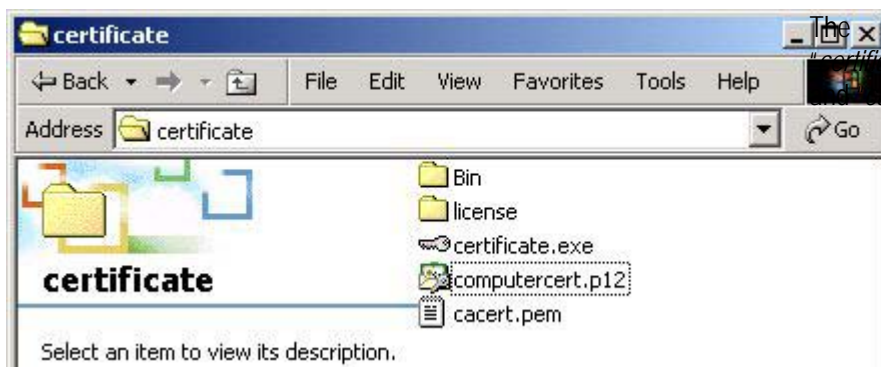
3 TheGreenBow IPSec VPN Client configuration

After installing TheGreenBow VPN client, the CA and the Certificate created for TheGreenBow VPN Client, will need to be retrieved from the SmoothTunnel. This is done in the normal way.

3.1 VPN Client Preparing Certificates

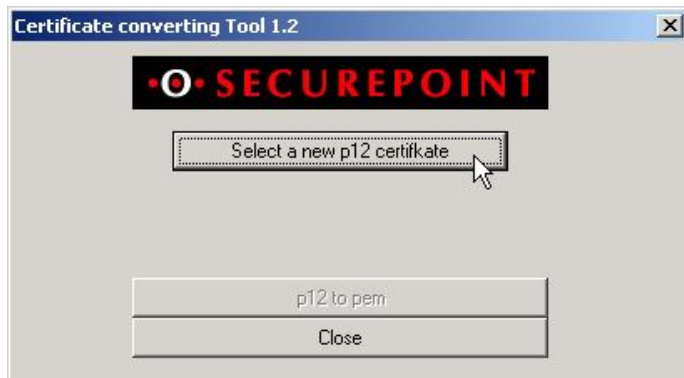
First, Export the CA as a PEM file and export **TheGreenBow Certificate** as a PKCS#12 file. In order for TheGreenBow VPN Client to be able to use the PKCS#12 Certificate, it needs to be converted into PEM format first. On TheGreenBow web site there is a program freely available that does just that – http://www.thegreenbow.com/vpn_tool.html. Download the utility and unpack it to a folder on your desktop. Once that is done, move the CA file called "cacert.pem" and the PKCS#12 file called "computercert.p12" to the same folder.

The contents of this folder should look somewhat like this:



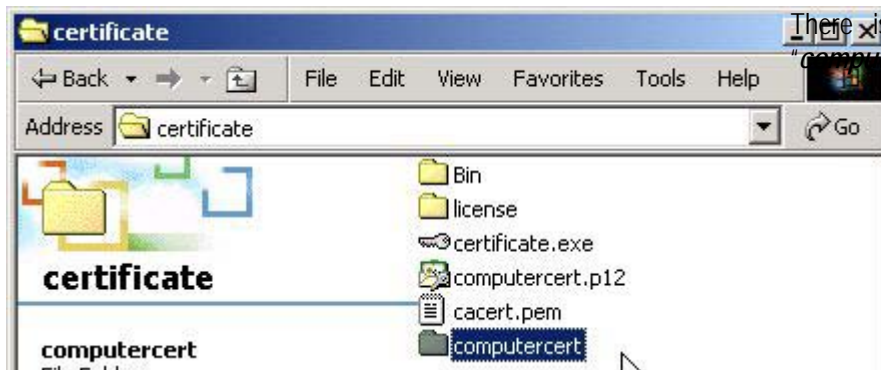
The important files here are "certificate.exe", "computercert.p12" and "cacert.pem"

Double click the "certificate.exe" and you should see this:



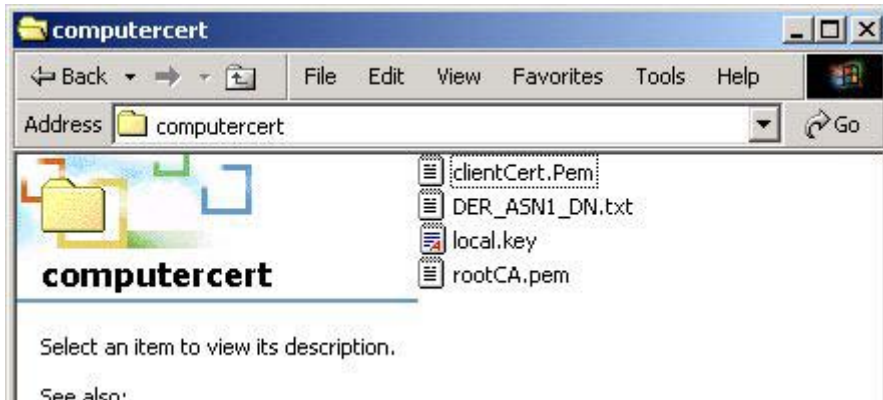
Click the "Select a new p12 certificate" and choose the "computercert.p12" file we exported from the SmoothTunnel. Enter the password for the P12 file when asked. A successful messages should appear. Then click the "Close" button.

After the Certificate converting tool has been run, the contents of the folder should now look like this:



There is now a new folder called "computercert".

Open the "computercert" folder and you will see this:

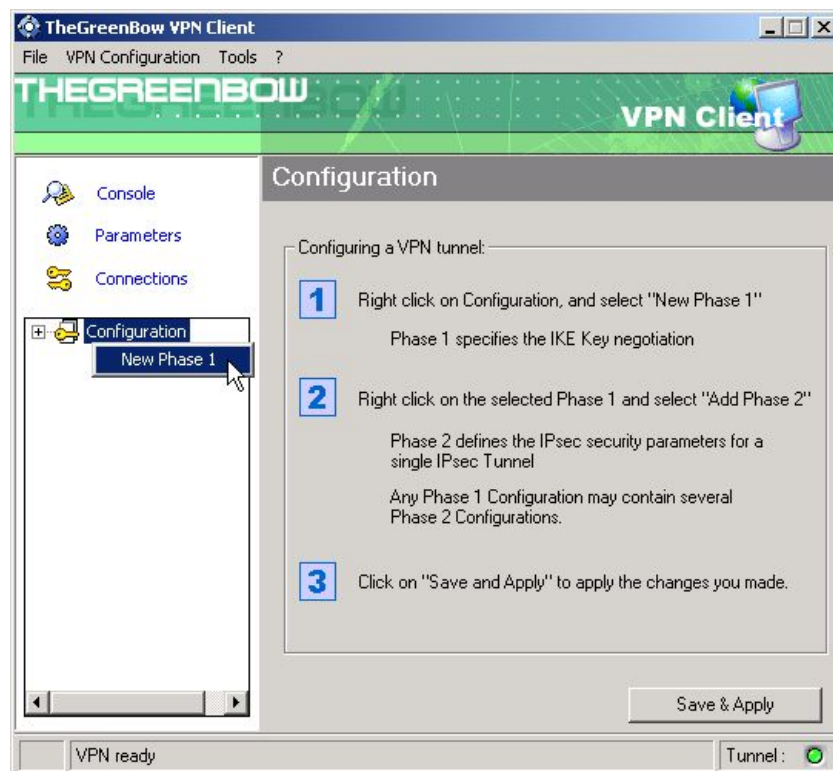


The two files you will need from this folder are the "clientCert.pem" and the "local.key" files. The "rootCA.pem" is not used. Use the "cacert.pem" exported from the SmoothTunnel.

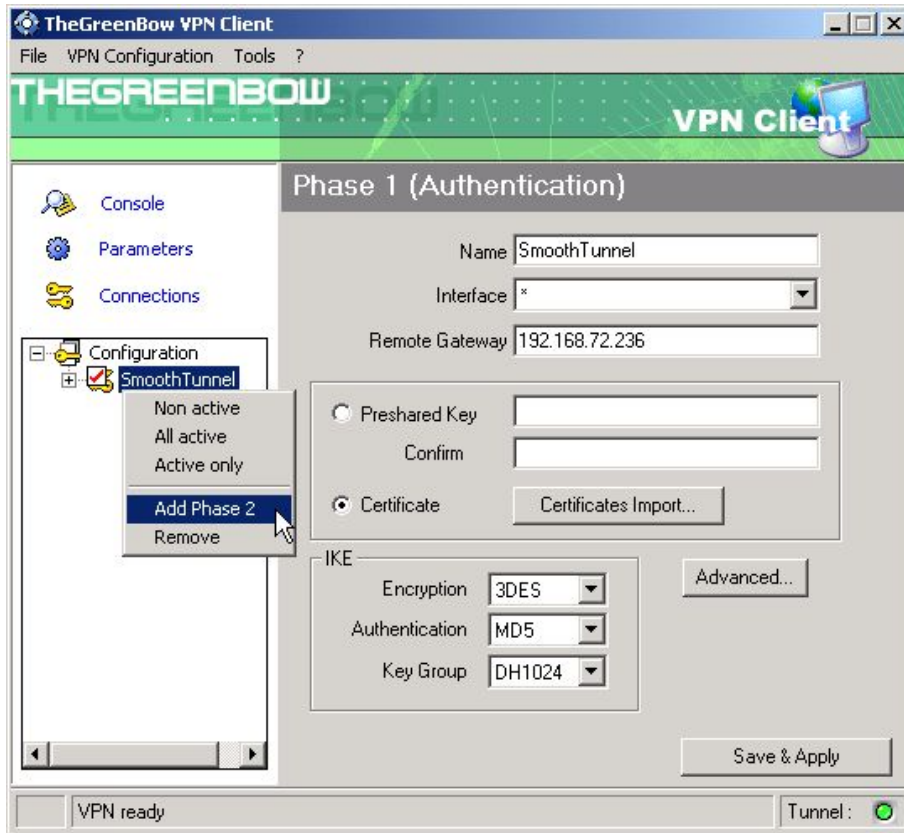
A good idea would be to rename these files using relevant names like "GreenbowAtTest.pem", "GreenbowAtTest.key" and "GreenbowAtTestCA.pem"

3.2 VPN Client Phase 1 (IKE) Configuration

Now lets start configuring the TheGreenbow IPsec VPN Client. Open up the TheGreenbow VPN Client and right click on the "configuration" to add a phase 1 configuration screen:



Once the new phase 1 configuration screen has been added, it has been renamed to "SmoothTunnel". Here is the configured screen:



Phase 1 configuration

This is a fairly easy screen to configure. The only real configuration lies in the certificate import:

- Enter the SmoothTunnel external IP address or host name in the "Remote Gateway" field.
- Select the "Certificate" radio button.
- Select the appropriate IKE encryption settings. This should match the phase 1 settings on the SmoothTunnel. Select the highest available keygroup.
- Before creating and configuring the Phase 2 screen, lets look at importing the certificates. Clicking the "Certificates Import" button, will give you this simple window:

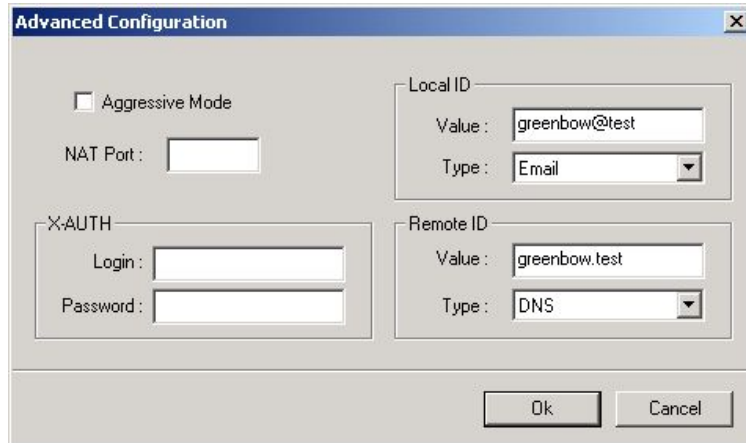


The root certificate is the "cacert.pem" or "GreenbowAtTestCA.pem" file.

The User certificate is the "clientCert.pem" or "GreenbowAtTest.pem" file.

The User Private Key is the "local.key" or "GreenbowAtTest.key" file.

Next, click the "advanced" button to set ID type and values:



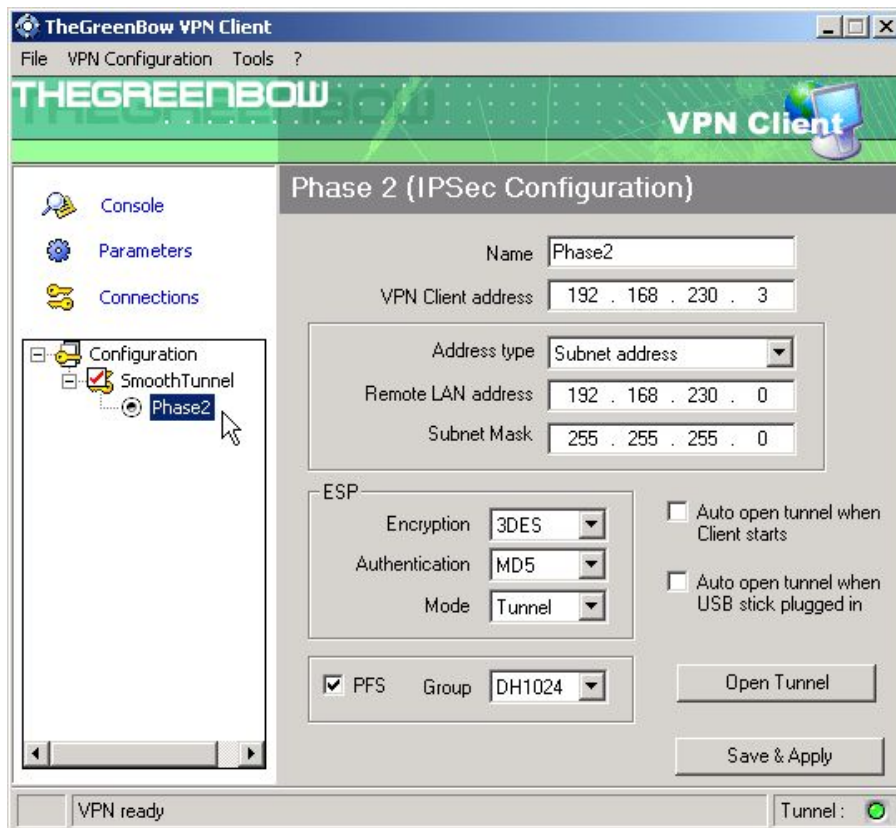
Local ID is filled in using the ID allocated to the *GreenbowAtTest* certificate. In this case, it was a type of email and the value of *greenbow@test*

Remote ID is filled using the corresponding values for the certificate used by the SmoothTunnel. In this case a DNS name, *greenbow.test*

3.3 VPN Client Phase 2 (IPSec) Configuration

Now lets add a Phase 2 to the **SmoothTunnel** connection. Right click on the **SmoothTunnel** entry in **TheGreenbow** VPN client and select "Add Phase 2".

Then select the "new phase 2" screen. The values that needs to be changed and entered are displayed here:



Phase 2 Configuration

Enter the IP address the VPN client is allocated when it connects to the **SmoothTunnel** in the *"VPN Client address"* field.


The next section is filled with the Remote network subnet information.

In the **ESP** section, select values that correspond to the Phase 2 settings in the **SmoothTunnel** configuration. **PFS** is "Perfect Forward Secrecy" and should be selected both here and on the **SmoothTunnel**.

3.4 Open IPsec VPN tunnels

Once both SmoothWall 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. Successful IPsec tunnel opening should look like this:



```
155824 Default IKE daemon is removing SAs...
155830 Default Reinitializing IKE daemon
155830 Default IKE daemon reinitialized
155842 Default (SA SmoothTunnel-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID]
155842 Default (SA SmoothTunnel-P1) RECV phase 1 Main Mode [SA] [VID]
155842 Default (SA SmoothTunnel-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
155842 Default (SA SmoothTunnel-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE] [CERT_REQ] [NAT_D] [NAT_D]
155842 Default (SA SmoothTunnel-P1) SEND phase 1 Main Mode [ID] [CERT] [SIG] [NOTIFY]
155842 Default (SA SmoothTunnel-P1) RECV phase 1 Main Mode [ID] [CERT] [SIG]
155842 Default phase 1 done: initiator id greenbow@test, responder id greenbow.test
155842 Default (SA SmoothTunnel-Phase2-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID] [NAT_OA]
155842 Default (SA SmoothTunnel-Phase2-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
155842 Default (SA SmoothTunnel-Phase2-P2) SEND phase 2 Quick Mode [HASH]
```

4 VPN IPSec Troubleshooting

4.1 « PAYLOAD MALFORMED » error

```

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.

4.2 « INVALID COOKIE » error

```

115933 Default message_rcv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
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.

4.3 « 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.

4.4 « 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_rcv_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.

4.5 « 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

```

4.6 « 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).

4.7 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).

4.8 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.

 THEGREENBOW	Doc.Ref	tgvpn_ug_SmoothWall_en
	Doc.version	2.0 – Feb.2005
	VPN version	2.5x

5 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