TheGreenBow IPSec VPN Client

Configuration Guide

Vigor 2910

Table of contents

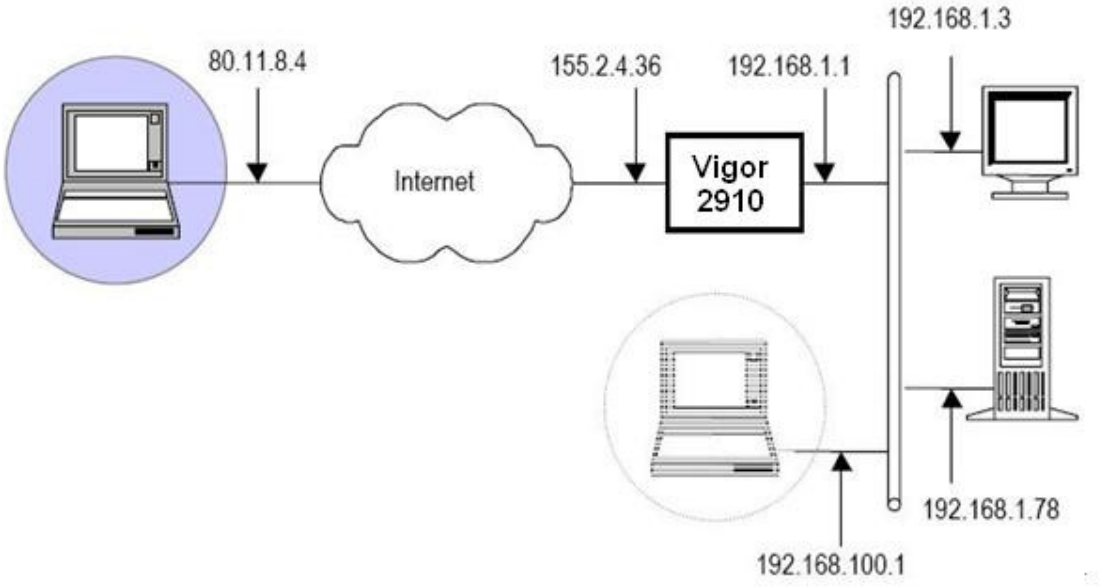
1 Introduction

1.1 Goal of this document

This VPN configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Vigor 2910 router.

1.2 Network topology

In our example, we will connect TheGreenBow VPN client to the LAN behind the Vigor 2910 Router. The VPN Client is connected to the Internet by a dialup/DSL connection from an ISP. The client will have a virtual IP address in the remote LAN. All the addresses in this document are given for example purpose.



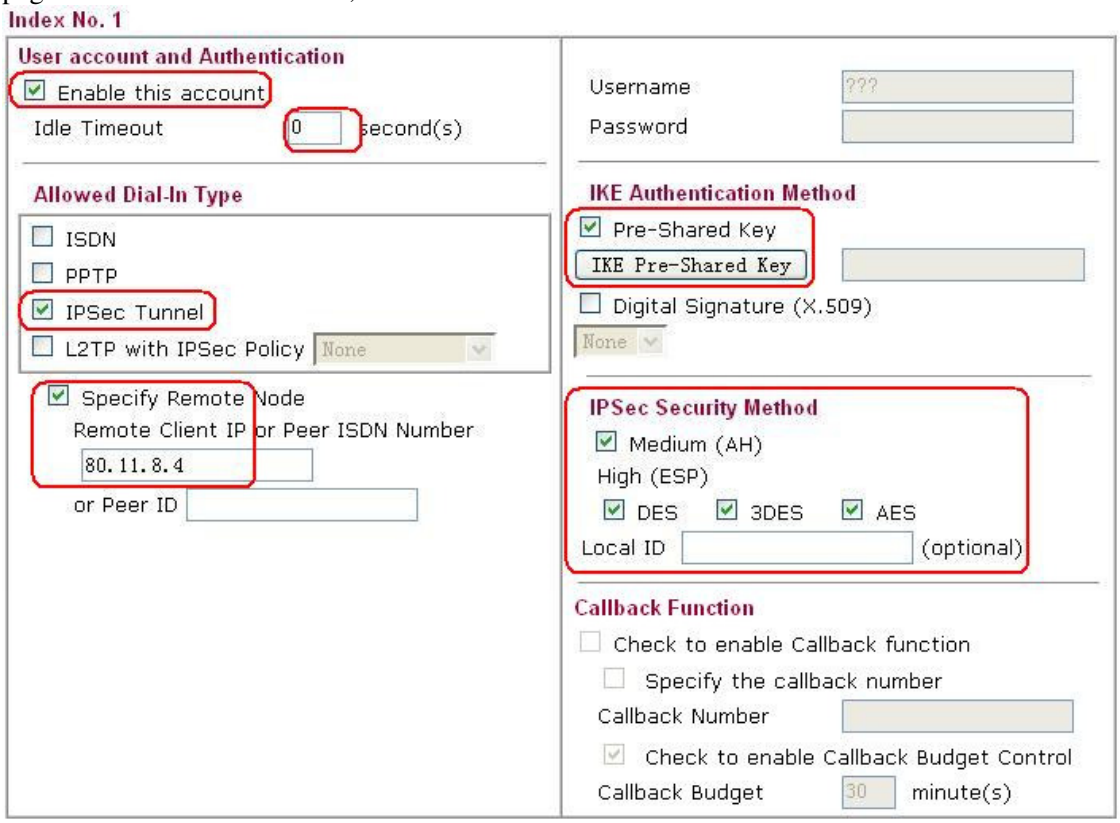
2 IPSec Main Mode Configuration

2.1 Vigor 2910 Configuration

This section describes how to build an IPSec VPN configuration(**Main mode**) with your Vigor 2910 VPN router. Refer to http://www.draytek.com/support/index.php for more information.

Vigor VPN configuration can be achieved with a web browser, so once connected to your VPN gateway, use the following setup links to configure the VPN.
VPN and Remote Access Setup

1. Click on **Remote Dial-in User** link. Then click one index number to open an individual setup page for a dial-in user account, as shown below.



a. Check the item **Enable this account** to activate the individual dial-in user account.
b. Enter a number for **Idle Timeout**. Set it to 0 means no idle timeout.
c. Make sure **IPSec Tunnel** is selected.
d. Enable **Specify Remote Node** and type the IP address of the VPN client.
e. Afterward, you should fill a Pre-Shared Key for this specific node. Press the **IKE Pre-Shared Key** button and enter the key in the pop-up window.

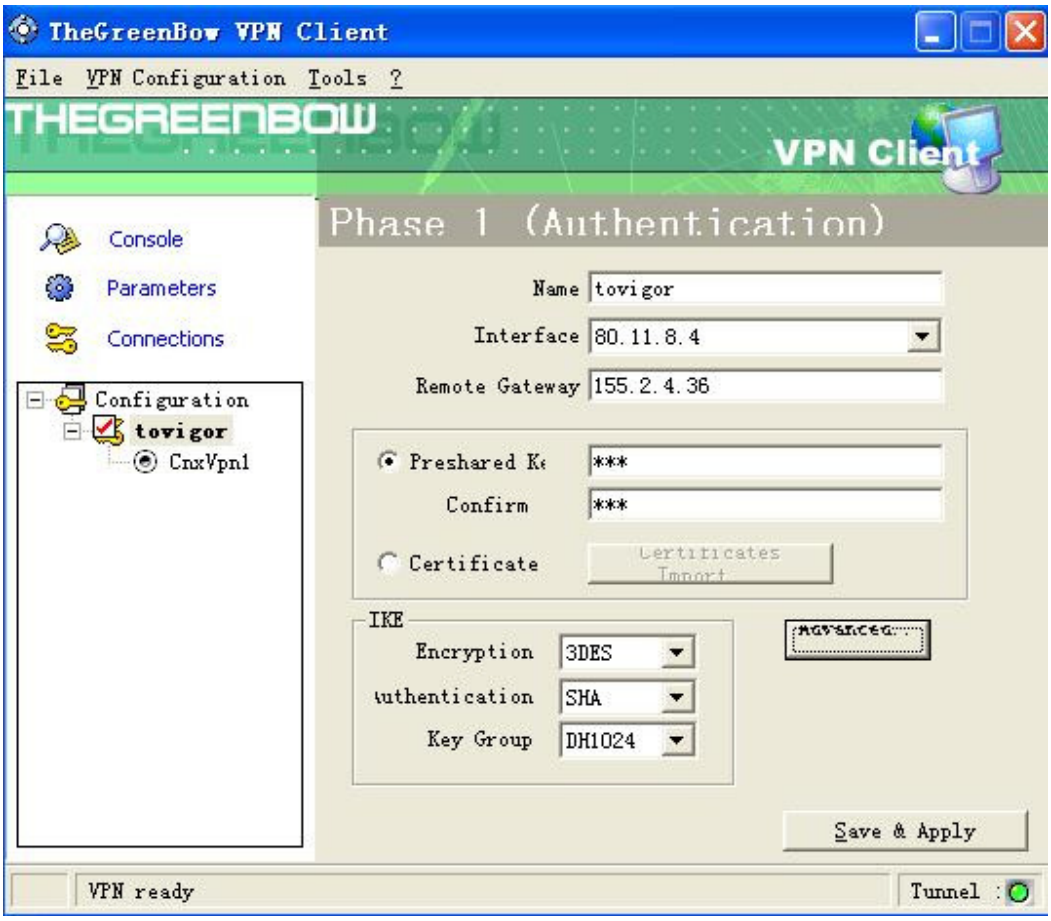
f. Select appropriate encryption algorithms in the **IPSec Security Method** field. This setup is for phase 2. **Note:** By default Vigor accepts all the attributes proposed by the VPN client.

Note: If you Enable **Specify Remote Node** in step d, this profile is specified to one fixed remote user. If you want to create a profile which can be applied to many users, especially those who use dynamic IP addresses, don't check this box. In this case, you can't enter the Pre-Shared key as the way described in step e. You must setup the Pre-shared key in
VPN and Remote Access Setup > IPSec General Setup

2.2 TheGreenBow IPSec VPN Client Configuration

2.2.1 VPN Client Phase 1(IKE) Configuration

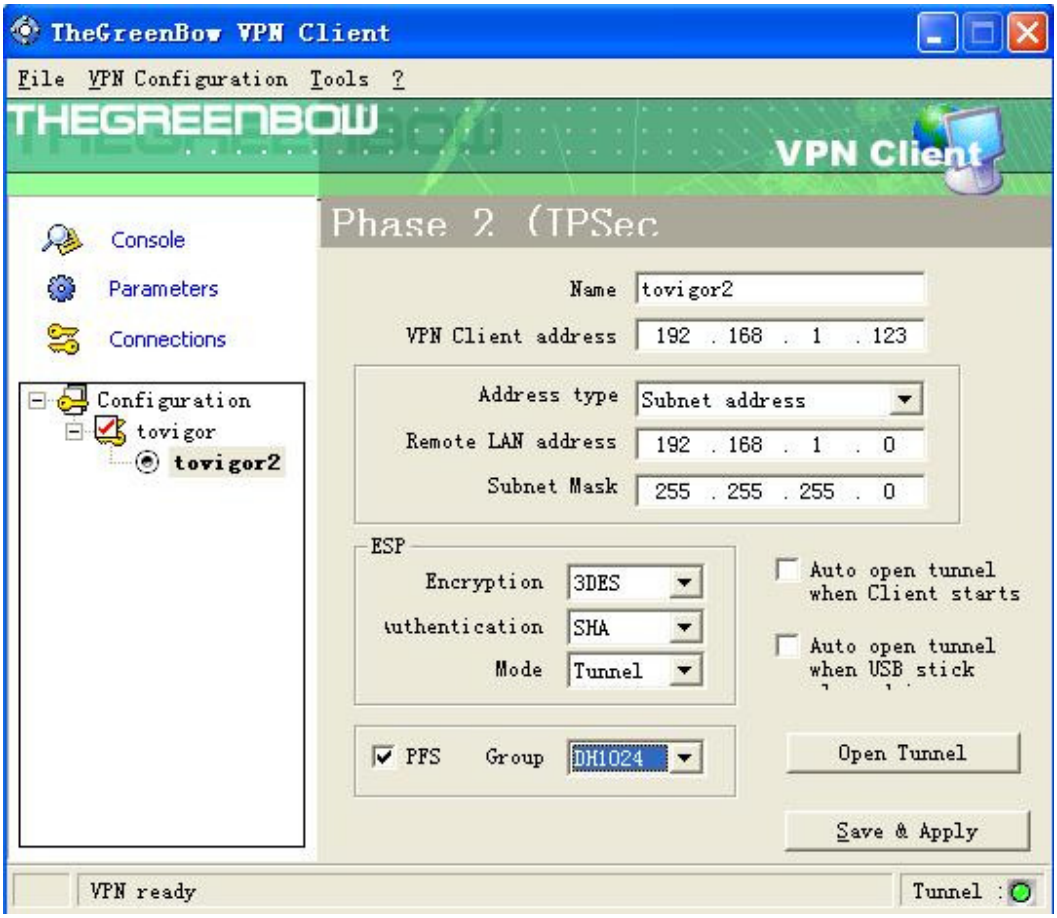
a. In the "**Interface**" field, you can select a star ("*"), if the VPN Client host receives a dynamic IP Address from an ISP for example.
b. "**Remote Gateway**" field value is the Vigor 2910 router public IP address or DNS address.
c. "**Preshared Key**" field value must be identical with the pre-shared key set in Vigor 2910 router.
d. In the "**IKE**" field, Vigor router supports the following parameters.
Encryption: DES/3DES
Authentication: MD5/SHA
Key Group: DH768/DH1024



Phase 1 configuration

2.2.2 VPN Client Phase 2(IPSec) Configuration

a. In the "**VPN Client address**" field, you may define a static virtual IP address here. You can type any IP address here, even 0.0.0.0. It does not prevent you from establishing a VPN tunnel.
b. Select Subnet address as "**Address type**", and enter the IP address (and subnet mask) of the remote LAN.
c. In the "**IKE**" field, Vigor router supports the following parameters.
Encryption: DES/3DES/AES128
Authentication: MD5/SHA
Mode: Tunnel
PFS Group: DH768/DH1024



Phase 2 configuration

2.2.3 Open the IPSec VPN tunnels

Once both Vigor 2910 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 "**Apply Rules**" 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.

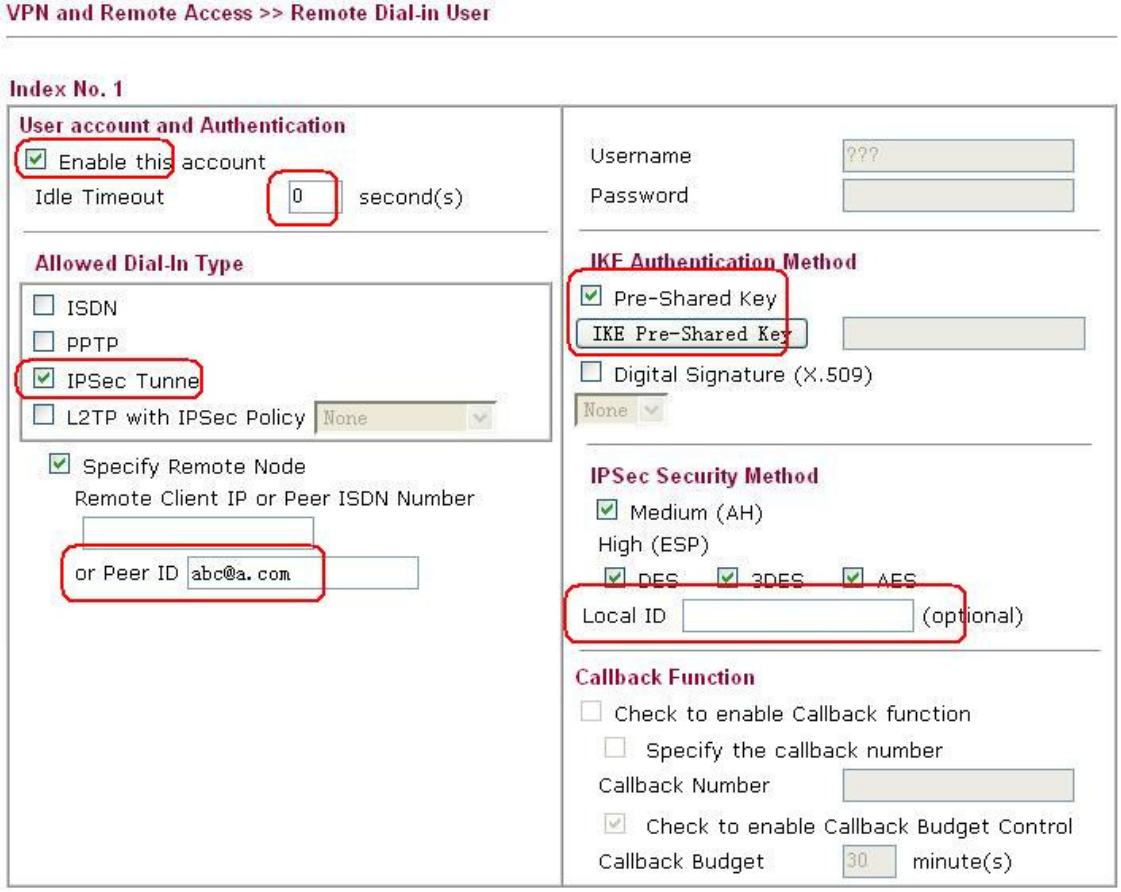
3 IPSec Aggressive Mode Configuration

3.1 Vigor 2910 Configuration

This section describes how to build an IPSec VPN configuration(**Aggressive mode**) with your Vigor 2910 VPN router. Refer to http://www.draytek.com/support/index.php for more information.

Vigor VPN configuration can be achieved with a web browser, so once connected to your VPN gateway, use the following setup links to configure the VPN.
Advanced Setup > VPN and Remote Access Setup

1. Click on **Remote User Profile Setup (Teleworker)** link. Then click one index number to open an individual setup page for a dial-in user account, as shown below.



a. Check the item **Enable this account** to activate the individual dial-in user account.
b. Enter a number for **Idle Timeout**. Set it to 0 means no idle timeout.
c. Make sure **IPSec Tunnel** is selected.
d. Enable **Specify Remote Node** and type the **Peer ID** of the VPN client. The corresponding value set in TheGreenBow is **Local ID**.
e. Afterward, you should fill a Pre-Shared Key for this specific node. Press the **IKE Pre-Shared Key** button and enter the key in the pop-up window.

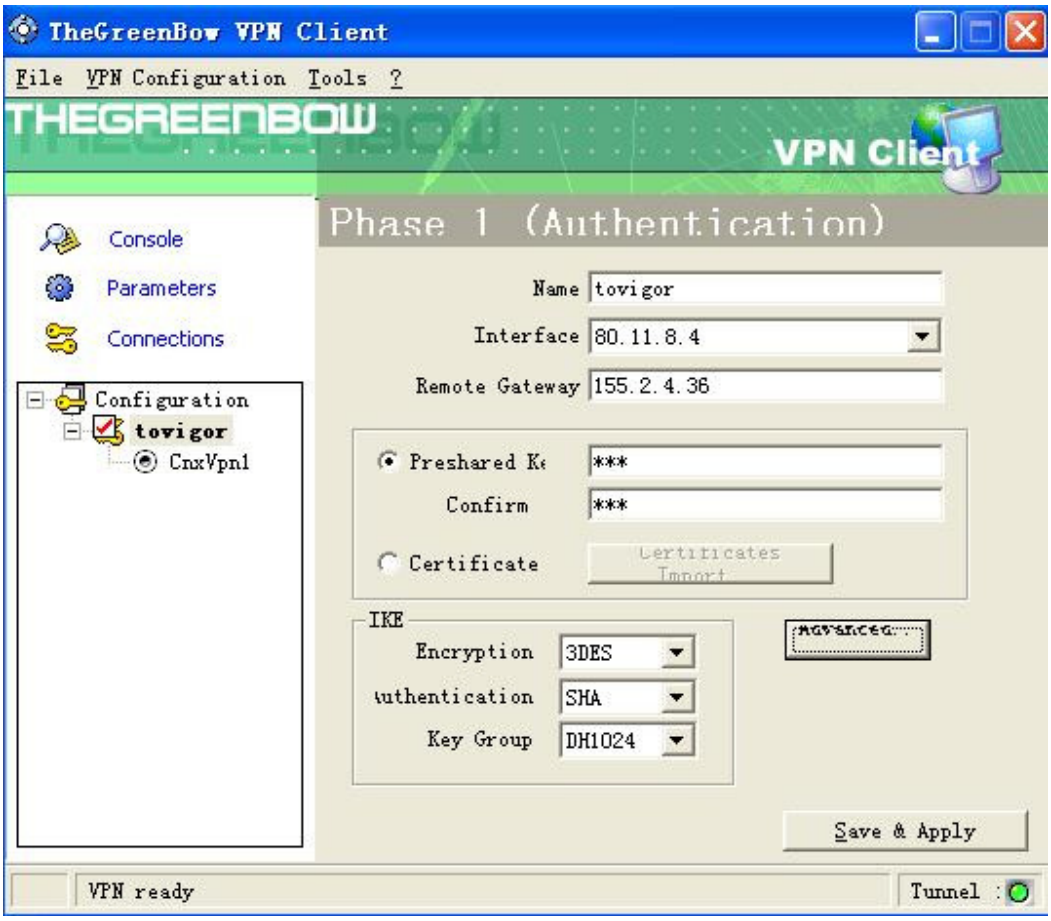
f. Select appropriate encryption algorithms in the **IPSec Security Method** field. This setup is for phase 2. **Note:** By default Vigor accepts all the attributes proposed by the VPN client.

Note: The **Local ID** field is optional. If it is enabled, you must setup the **Remote ID** in TheGreenBow.

3.2 TheGreenBow IPSec VPN Client Configuration

3.2.1 VPN Client Phase 1(IKE) Configuration

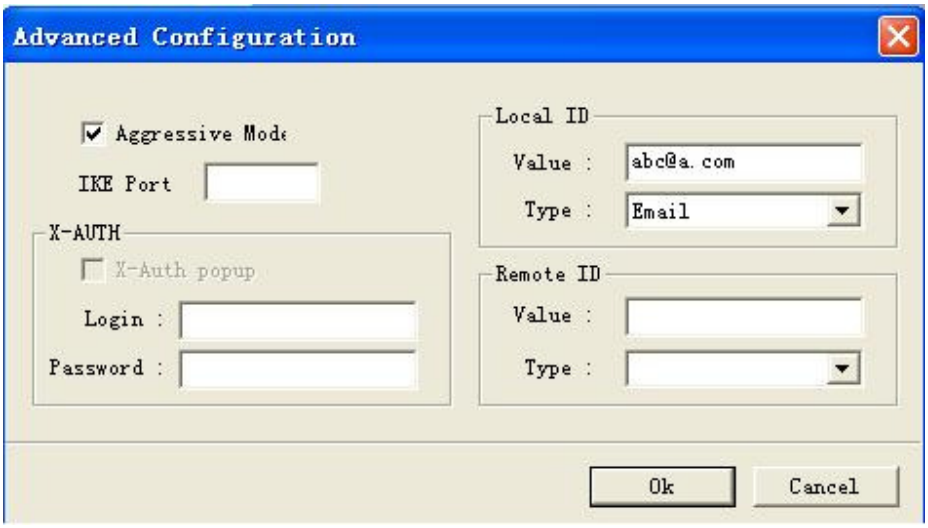
a. In the "**Interface**" field, you can select a star ("*"), if the VPN Client host receives a dynamic IP Address from an ISP for example.
b. "**Remote Gateway**" field value is the Vigor 2910 router public IP address or DNS address.
c. "**Preshared Key**" field value must be identical with the pre-shared key set in Vigor 2910 router.
d. In the "**IKE**" field, Vigor router supports the following parameters.
Encryption: DES/3DES
Authentication: MD5/SHA
Key Group: DH768/DH1024



Phase 1 configuration

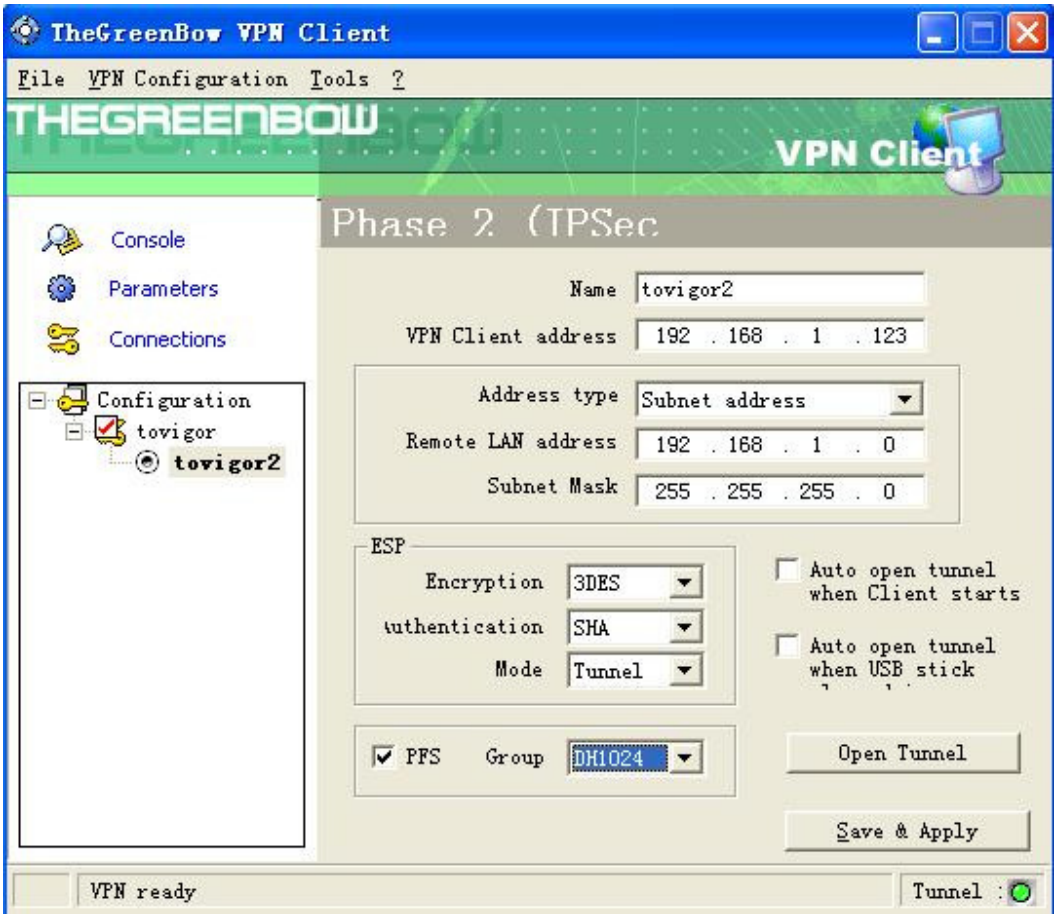
e. Click the **Advance** button. In the pop-up window please enable **Aggressive Mode**. Then you must setup the **Local ID** field. The **Value** must be identical with the one set in Vigor 2910 router(step d). Vigor only support DNS and Email types.

Note: If you setup the **Local ID** field in Vigor 2910 router, the **Remote ID** field in TheGreenBow must be configured also.


Advanced Configuration
Aggressive Mode
IKE Port
X-AUTH
X-Auth popup
Login :
Password :
Local ID
Value :
abc@a.com
Type :
Email
Remote ID
Value :
Type :
Ok
Cancel

3.2.2 VPN Client Phase 2(IPSec) Configuration

a. In the "**VPN Client address**" field, you may define a static virtual IP address here. You can type any IP address here, even 0.0.0.0. It does not prevent you from establishing a VPN tunnel.
b. Select Subnet address as "**Address type**", and enter the IP address (and subnet mask) of the remote LAN.
c. In the "**IKE**" field, Vigor router supports the following parameters.
Encryption: DES/3DES/AES128
Authentication: MD5/SHA
Mode: Tunnel
PFS Group: DH768/DH1024



Phase 2 configuration

3.2.3 Open the IPSec VPN tunnels

Once both Vigor 2910 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 "**Apply Rules**" 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.

4 VPN IPSec Troubleshooting

4.1 « PAYLOAD MALFORMED » error

```
114920 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [SA][VID]
114920 Default (SA BEFVP41-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_recv: 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 BEFVP41-P1) SEND phase 1 Main Mode [SA][VID]
115317 Default (SA BEFVP41-P1) RECV phase 1 Main Mode [SA][VID]
115317 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [KEY][NONCE]
115319 Default (SA BEFVP41-P1) RECV phase 1 Main Mode [KEY][NONCE]
115319 Default (SA BEFVP41-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 BEFVP41-P1) SEND phase 1 Main Mode [SA][VID]
120349 Default (SA BEFVP41-P1) RECV phase 1 Main Mode [SA][VID]
120349 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [KEY][NONCE]
120351 Default (SA BEFVP41-P1) RECV phase 1 Main Mode [KEY][NONCE]
120351 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default (SA BEFVP41-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.

4.5 « NO PROPOSAL CHOSEN » error

115911 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [SA][VID]
115913 Default (SA BEFVP41-P1) RECV phase 1 Main Mode [SA][VID]
115913 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [KEY][NONCE]
115915 Default (SA BEFVP41-P1) RECV phase 1 Main Mode [KEY][NONCE]
115915 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default (SA BEFVP41-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 BEFVP41-BEFVP41-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 BEFVP41-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 BEFVP41-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 BEFVP41-P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA BEFVP41-P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA BEFVP41-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA BEFVP41-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA BEFVP41-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 BEFVP41-BEFVP41-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 BEFVP41-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.