TheGreenBow IPSec VPN Client

Configuration Guide

Netopia 3346

WebSite: http://www.thegreenbow.com

Contact: support@thegreenbow.com

Table of contents

1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Netopia 3346 VPN router.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Netopia 3346 VPN router. 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.
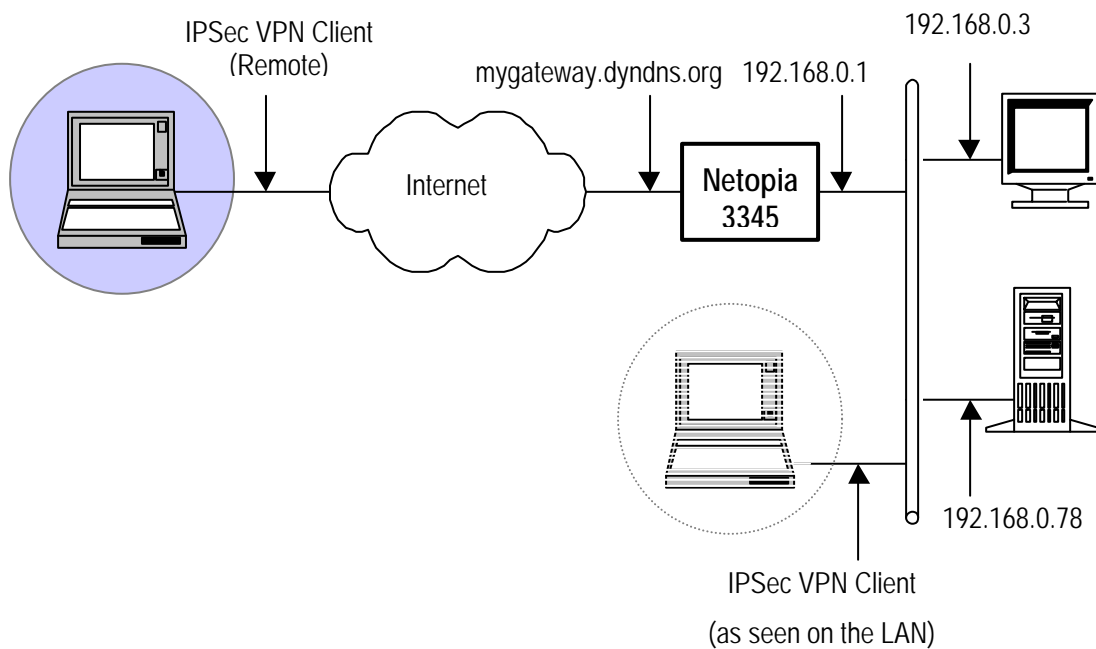
2 Netopia 3346 VPN Configuration

2.1 Netopia 3346 Configuration interface

Netopia VPN configuration can be achieved by a telnet connexion. Read Netopia 3346 documentation for more information.

```
                        Netopia 3346 v8.3.1r0


                     WAN Configuration...

                     System Configuration...

                     Utilities & Diagnostics...

                     Statistics & Logs...

                     Quick Menus...

                     Quick View...




     Return/Enter for WAN Line configuration.
     You always start from this main screen.
```
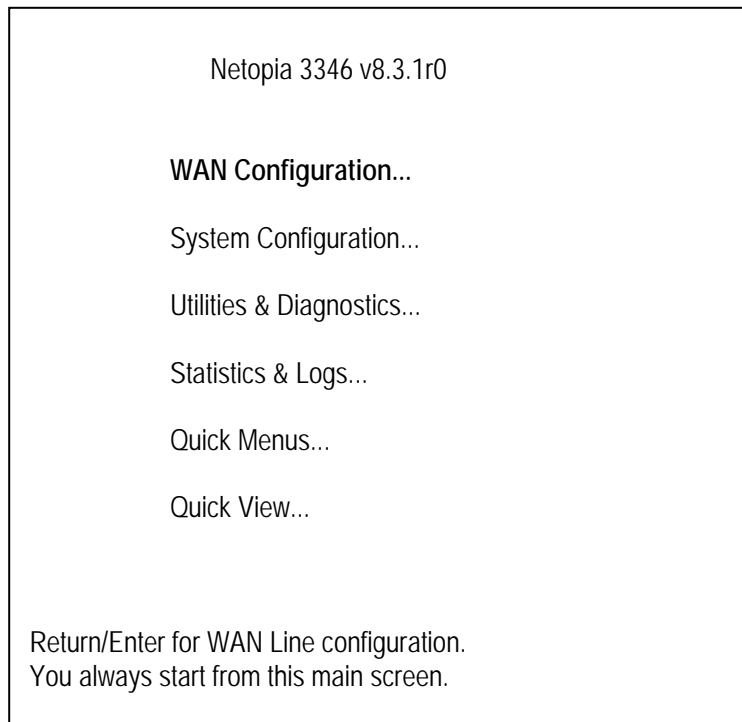
Select "**WAN configuration** " and press ENTER.

```
                        WAN Configuration

              WAN (Wide Area Network) Setup...
              ATM Circuits Configuration...

              Display/Change Connection Profile...
              Add Connection Profile...
              Delete Connection Profile...


              ATMP/PPTP Default Profile...
              IKE Phase 1 Configuration...

              Advanced Connection Options...
```
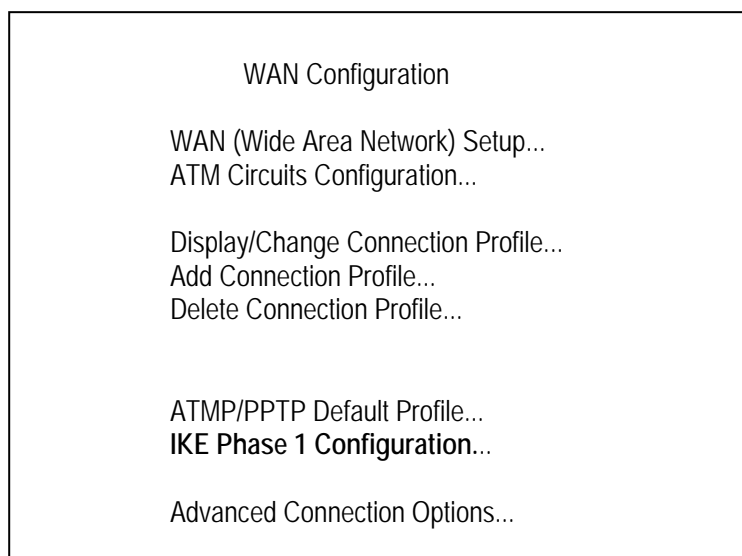
Select "**IKE Phase1 Configuration**" and press ENTER.

2.2 Netopia 3346 IKE Phase 1 configuration

```
            IKE Phase 1 Configuration


        Display/Change IKE Phase 1 Profile...
        Add IKE Phase 1 Profile...
        Delete IKE Phase 1 Profile...
```
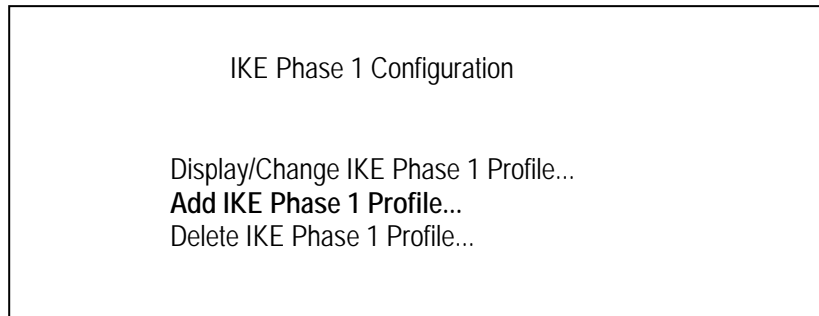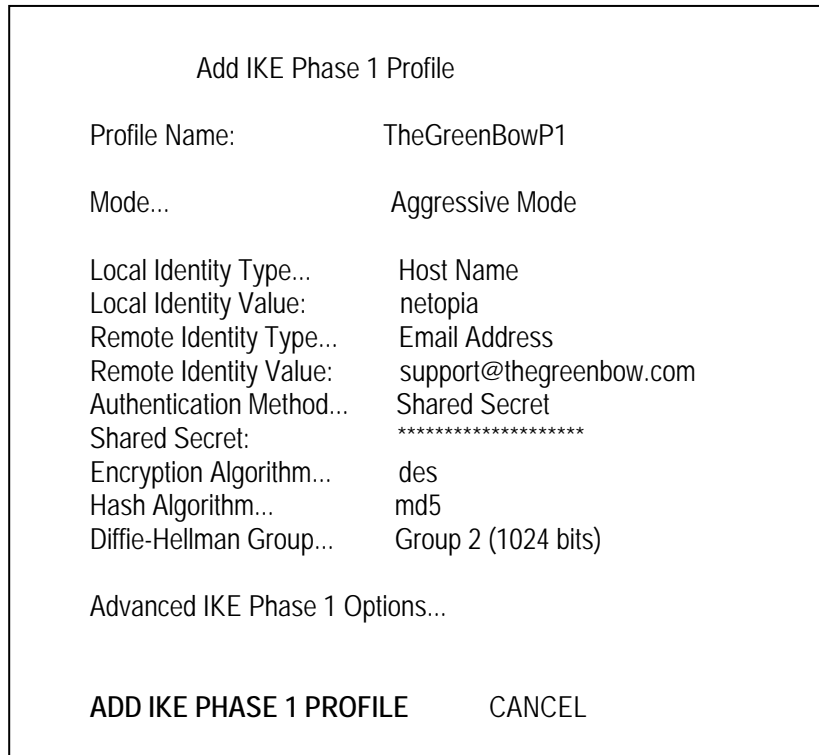
Select "**Add IKE Phase 1 Profile**" and press ENTER.

We create a IKE Phase 1 called TheGreenBowP1. These settings will be used in the VPN client's Phase 1 configuration.

```
            Add IKE Phase 1 Profile

    Profile Name:            TheGreenBowP1

    Mode...                   Aggressive Mode

    Local Identity Type...    Host Name
    Local Identity Value:     netopia
    Remote Identity Type...   Email Address
    Remote Identity Value:    support@thegreenbow.com
    Authentication Method...  Shared Secret
    Shared Secret:            *******************
    Encryption Algorithm...   des
    Hash Algorithm...         md5
    Diffie-Hellman Group...   Group 2 (1024 bits)

    Advanced IKE Phase 1 Options...


    ADD IKE PHASE 1 PROFILE       CANCEL
```

Once phase 1 finished, select "**ADD IKE PHASE 1 PROFILE**" and press ENTER.

2.3 Netopia 3346 Connection profile

You are back to "WAN configuration" screen.

```
                    WAN Configuration

            WAN (Wide Area Network) Setup...
            ATM Circuits Configuration...

            Display/Change Connection Profile...
            Add Connection Profile...
            Delete Connection Profile...


            ATMP/PPTP Default Profile...
            IKE Phase 1 Configuration...

            Advanced Connection Options...
```

Select "**Add Connection Profile**" and press ENTER.

```
                    Add Connection Profile

        Profile Name:           TheGreenBow
        Profile Enabled:        Yes

        Encapsulation Type...       IPsec


        Encapsulation Options...


        IP Profile Parameters...



        Interface Group...          Any Port



        COMMIT              CANCEL
```

Choose a name for this connection profile and press ENTER.

Select IPSec as "**Encapsulation Type**".

Select "**Encapsulation Options**" and press ENTER.

In this screen, you make reference to Phase 1 previously created. In "**Encapsulation**", select "**ESP**".

```
                          IPsec Tunnel Options


        Key Management...              IKE
        IKE Phase 1 Profile...         TheGreenBowP1

        Encapsulation...               ESP




        ESP Encryption Transform...    DES
        ESP Authentication Transform...   HMAC-MD5-96




        Advanced IPsec Options...

           COMMIT               CANCEL
```

Select "**Advanced IPsec Options**" and press ENTER.

```
                        Advanced IPsec Options


        SA Lifetime seconds:          28800
        SA Lifetime Kbytes:           0

        Perfect Forward Secrecy:        No

        Dead Peer Detection:            No







        Return/Enter accepts * Tab toggles * ESC cancels.
```

Press **ENTER** once done.

```
                    Add Connection Profile

        Profile Name:           TheGreenBow
        Profile Enabled:        Yes

        Encapsulation Type...       IPsec


        Encapsulation Options...


        IP Profile Parameters...



        Interface Group...          Any Port



        COMMIT                  CANCEL


    Configure a new Conn. Profile. Finished?  COMMIT or CANCEL to exit.
```

Select "**IP Profile Parameters**" and press ENTER.

```
                    IP Profile Parameters

        Remote Tunnel Endpoint:        0.0.0.0
        Add Network...



        Address Translation Enabled:      No



        Stateful Inspection Enabled:      No


        Filter Set...              Basic Firewall
        Remove Filter Set

        Advanced IP Profile Options...

            COMMIT                CANCEL
```

Select "**Add Network**" and press ENTER.

```
                Display/Change Network Configuration


        Remote Member Format...        Host Address
        Remote Member Address:         0.0.0.0

        Local Member Format...         Subnet
        Local Member Address:          192.168.1.0
        Local Member Mask:             255.255.255.0




           COMMIT                CANCEL

        Return/Enter to select <among/between> ...
```

These settings are Phase 2 IDs.

Save changes once finished.

3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

In the "**Interface**" field, you can select a star ("*****"), if the client host receive a dynamic IP Address from an ISP for example.

"**Remote Address**" field value is the Netopia router public IP address or DNS address.
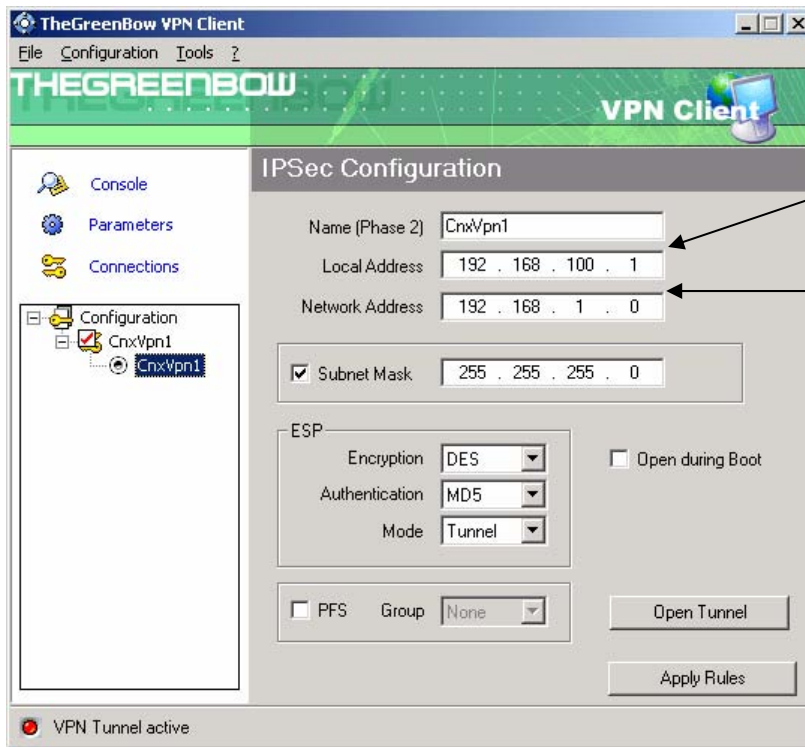
By clicking in "**Advanced**" button, you can setup Phase 1 IDs and Aggressive Mode.
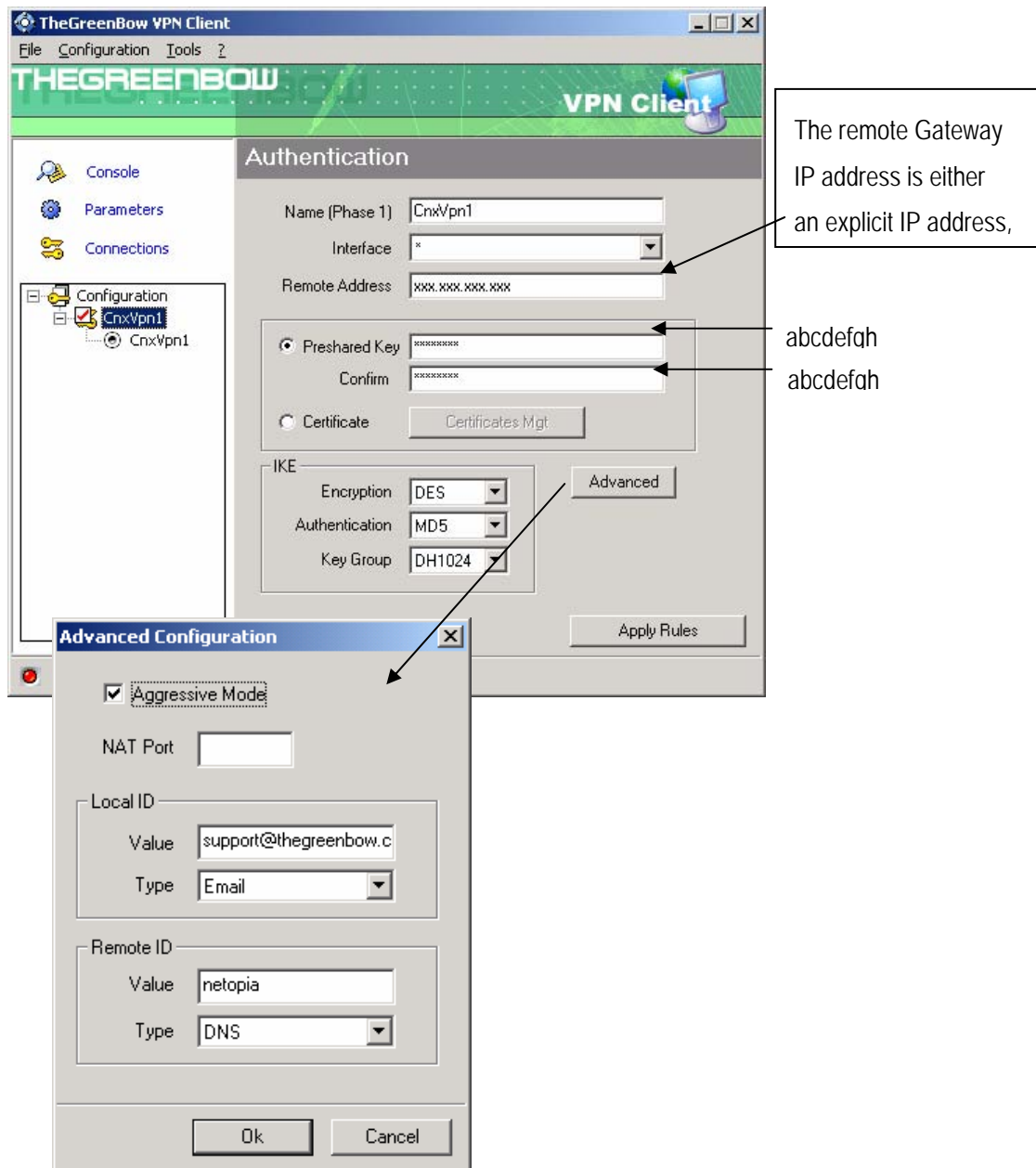
3.2 TheGreenBow VPN Client Phase 2 (IPSec) Configuration

In this window, you define IPSec Policy.

"**Local Address** " is the virtual IP address of the client inside the LAN. This address must not belong to the remote LAN.

You may define a static virtual IP address here.

Do NOT specify an IP address belonging to the remote LAN's subnet !!

Enter the IP address

(and subnet mask)

Phase2 Configuration

3.3 Open the IPSec VPN tunnels

Once both Netgear FVL328 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.

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_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 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
```

If you have an « no keystate » error, 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_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 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.

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