




THEGREENBOW

 TheGreenBow IPSec VPN Client  
Configuration Guide  
Linksys WRVS4400N

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

Contact: [support@thegreenbow.com](mailto:support@thegreenbow.com)

Configuration Guide written by:

Writer: Humberto Garcia

Company: [www.hgr-it.com](http://www.hgr-it.com)

## Table of contents

1	Introduction .....	3
1.1	Goal of this document .....	3
1.2	VPN Network topology .....	3
1.3	Linksys WRVS4400N Restrictions .....	3
1.4	Linksys WRVS4400N VPN Gateway .....	3
1.5	Linksys WRVS4400N VPN Gateway product info.....	4
2	Linksys WRVS4400N VPN configuration .....	5
2.1	IPSEC VPN.....	5
2.2	Under Advanced settings.....	6
3	TheGreenBow IPsec VPN Client configuration .....	7
3.1	VPN Client Phase 1 (IKE) Configuration.....	7
3.2	VPN Client Phase 2 (IPsec) Configuration .....	8
3.3	Open IPsec VPN tunnels.....	9
4	Tools in case of trouble.....	11
4.1	A good network analyser: Wireshark .....	11
5	VPN IPsec Troubleshooting .....	12
5.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) .....	12
5.2	« INVALID COOKIE » error.....	12
5.3	« no keystate » error .....	12
5.4	« received remote ID other than expected » error.....	12
5.5	« NO PROPOSAL CHOSEN » error .....	13
5.6	« INVALID ID INFORMATION » error .....	13
5.7	I clicked on “Open tunnel”, but nothing happens.....	13
5.8	The VPN tunnel is up but I can't ping !.....	13
6	Contacts.....	15

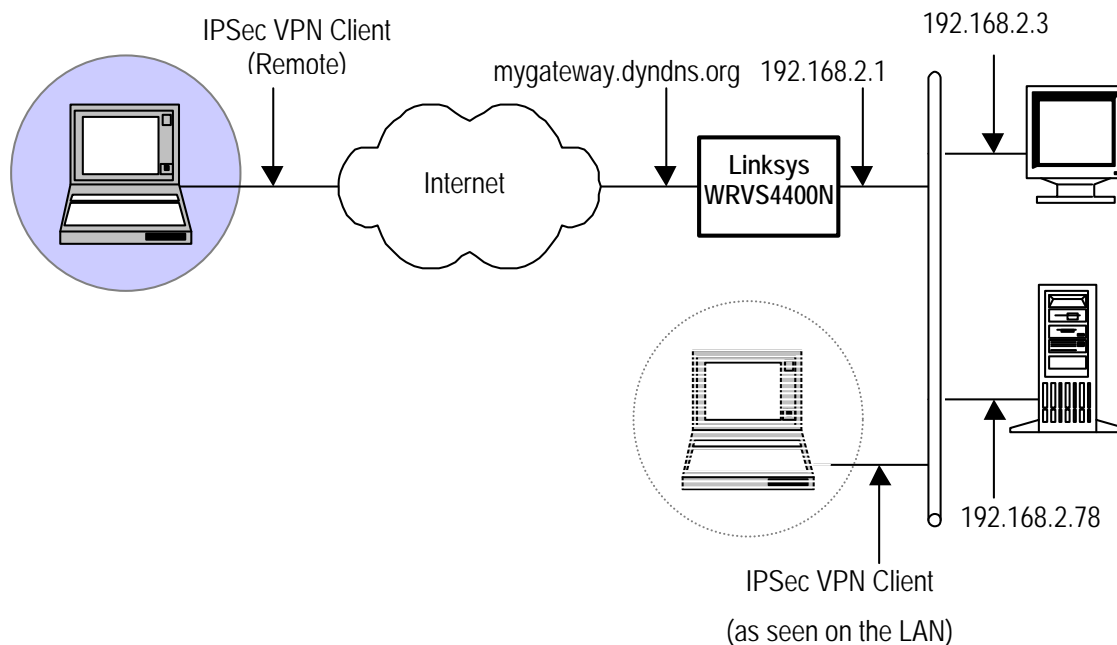
## 1 Introduction

### 1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client with a Linksys WRVS4400N 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 Linksys WRVS4400N 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.



### 1.3 Linksys WRVS4400N Restrictions

Depending on the firmware version, Linksys WRVS4400N can not create the VPN tunnel with TheGreenBow. I was trying to use latest firmware (1.01.03) and did not work, then flashed device with version 1.00.16 and everything was ok.

### 1.4 Linksys WRVS4400N VPN Gateway

Our tests and VPN configuration have been conducted with Linksys WRVS4400N firmware release V1.00.16.

## 1.5 Linksys WRVS4400N VPN Gateway product info

It is critical that users find all necessary information about Linksys WRVS4400N VPN Gateway. All product info, User Guide and knowledge base for the Linksys WRVS4400N VPN Gateway can be found on the Linksys WRVS4400N website: [www.linksys.com](http://www.linksys.com)

<a href="#">Linksys WRVS4400N Product page</a>	<a href="http://www.linksys.com/servlet/Satellite?c=L_Product_C2&amp;childpagename=US%2FLayout&amp;cid=1158193143712&amp;pagename=Linksys%2FCommon%2FVisitorWrapper&amp;id=4371287090B15">http://www.linksys.com/servlet/Satellite?c=L_Product_C2&amp;childpagename=US%2FLayout&amp;cid=1158193143712&amp;pagename=Linksys%2FCommon%2FVisitorWrapper&amp;id=4371287090B15</a>
<a href="#">Linksys WRVS4400N User Guide</a>	Same page.
<a href="#">Linksys WRVS4400N FAQ/Knowledge Base</a>	Same page.

## 2 Linksys WRVS4400N VPN configuration

This section describes how to build an IPsec VPN configuration with your Linksys WRVS4400N VPN router. Once connected to your Linksys WRVS4400N VPN gateway, you must select the "VPN" tab.

### 2.1 IPSEC VPN

Select Tunnel Entry:

IPsec VPN Tunnel:  Enable  Disable

Tunnel Name:

#### Local Security Group:

Local Security Group Type:

IP Address:  .  .  .

Subnet Mask:  .  .  .

#### Remote Security Group

Remote Security Group Type:

IP Address:  .  .  .

#### Remote Security Gateway

Remote Security Gateway Type:

This Gateway accepts requests from any IP address

#### Key Management

Key Exchange Method:

Encryption:

Authentication:

PFS:

Pre-Shared Key:

Key Life Time:  Sec.

#### Advanced

NetBIOS Broadcast

Connect	Disconnect	View Log	Advanced Settings
---------	------------	----------	-------------------

## 2.2 Under Advanced settings

### HGRVPN

**Phase 1:**

Operation mode:

Local Identity:  Local IP address

Name:

Remote Identity:  Remote IP address

Name:

Encryption:

Authentication:

Group:

Key Life Time:  Sec.

**Phase 2:**

Encryption: 3DES

Authentication: SHA1

PFS: Enable

Group:

Key Life Time:  Sec.

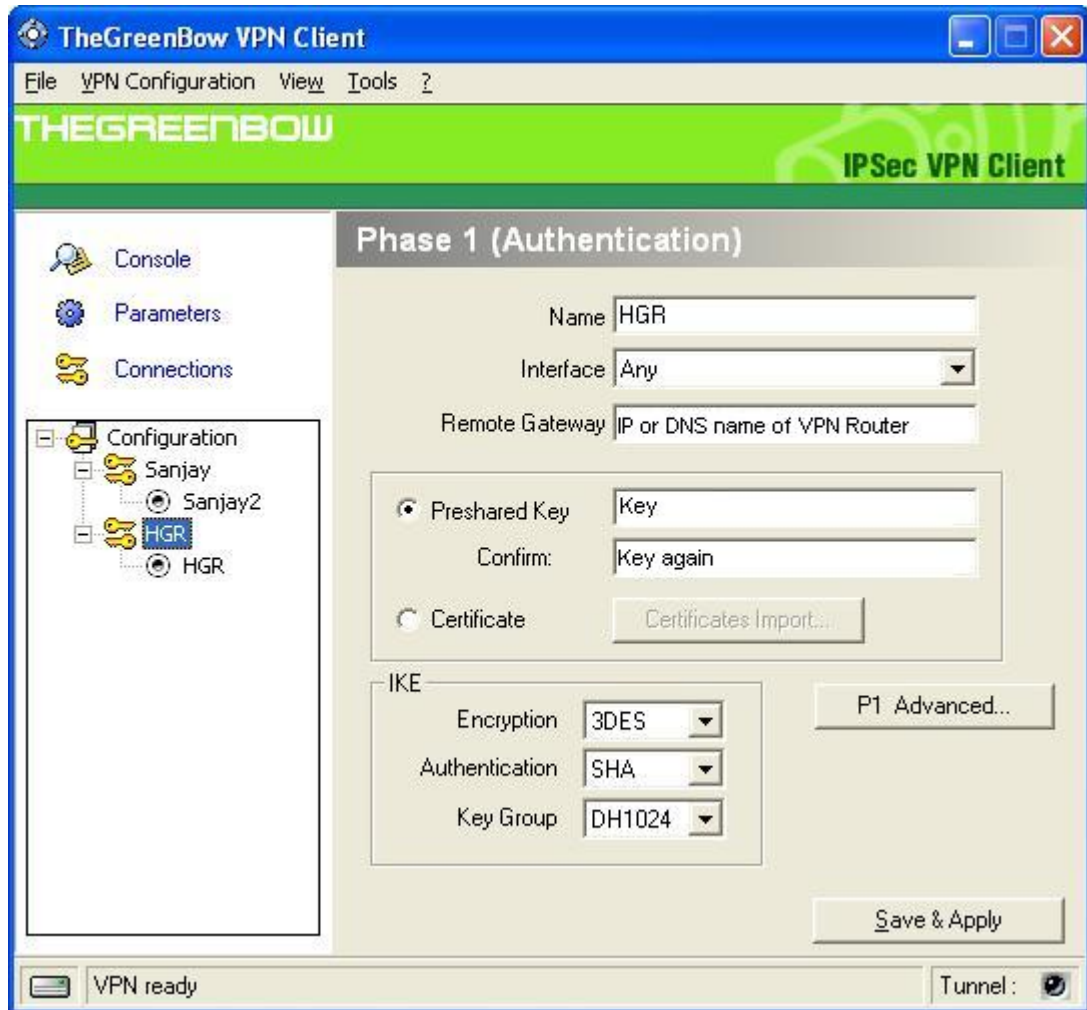
Click Save on this screen and in the main one and test the connection!!!

### 3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a Linksys WRVS4400N VPN router.

To download the latest release of TheGreenBow IPsec VPN Client software, please go to [http://www.thegreenbow.com/vpn\\_down.html](http://www.thegreenbow.com/vpn_down.html).

#### 3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 configuration

You may use Preshared key with the Linksys WRVS4400N router. This configuration is one example of can be accomplished in term of User Authentication. You may want to refer to either the Linksys WRVS4400N router user guide or TheGreenBow IPsec VPN Client User Guide for more details on User Authentication options.

P1 Advanced settings:

**Phase1 Advanced**

**Advanced features**

Config Mode      Redund.GW

Aggressive Mode      NAT-T

**X-Auth**

X-Auth Popup      Login

Hybrid Mode      Password

**Local and Remote ID**

Choose the type of ID:      Set the value for the ID:

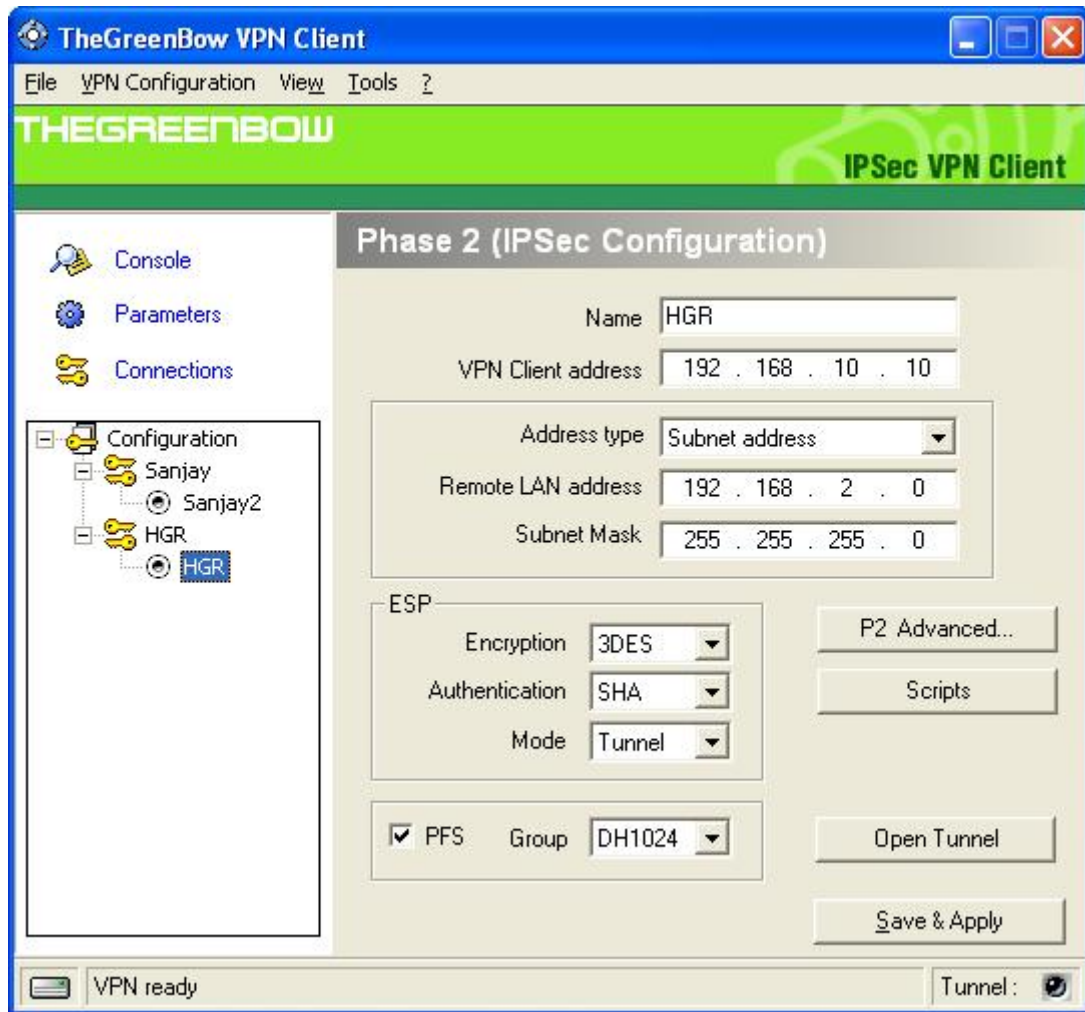
Local ID      

Remote ID      

### 3.2 VPN Client Phase 2 (IPSec) Configuration





Phase 2 Configuration

### 3.3 Open IPSec VPN tunnels

Once both Linksys WRVS4400N router and TheGreenBow IPSec VPN Client software 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 Linksys WRVS4400N VPN router.

Doc.Ref	tgvpn_ug_WRVS4400N_en
Doc.version	1.0 – Aug 2008
VPN version	4.x

```
20080627 142523 Default IKE daemon reinitialized
20080627 142526 Default (SA HGR-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID]
20080627 142526 Default (SA HGR-P1) RECV phase 1 Main Mode [SA] [VID] [VID] [VID]
20080627 142526 Default (SA HGR-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20080627 142526 Default (SA HGR-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20080627 142526 Default (SA HGR-P1) SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
20080627 142526 Default (SA HGR-P1) RECV phase 1 Main Mode [HASH] [ID]
20080627 142526 Default phase 1 done: initiator id 192.168.10.10, responder id home.com
20080627 142526 Default (SA HGR-HGR-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080627 142526 Default (SA HGR-HGR-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080627 142526 Default (SA HGR-HGR-P2) SEND phase 2 Quick Mode [HASH]
```

## 4 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.

### 4.1 A good network analyser: Wireshark

Wireshark is a 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.wireshark.org>. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (<http://www.wireshark.org/docs/>).

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 VPN IPSec Troubleshooting

### 5.1 « 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.

### 5.2 « 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.

### 5.3 « 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.

### 5.4 « 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.

## 5.5 « 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

```

## 5.6 « 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).

## 5.7 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).

## 5.8 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 Wireshark 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 Wireshark (<http://www.wireshark.org>) on one of your target computer. You can check that your pings arrive inside the LAN.

## 6 Contacts

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

Technical support by email at [support@thegreenbow.com](mailto:support@thegreenbow.com)

Sales contacts by email at [sales@thegreenbow.com](mailto:sales@thegreenbow.com)