

# TheGreenBow IPsec VPN Client

## Configuration Guide

### Barracuda NG Firewall

Written by: **TheGreenBow TechSupport Team**  
Company: **[www.thegreenbow.com](http://www.thegreenbow.com)**

Website: **[www.thegreenbow.com](http://www.thegreenbow.com)**  
Contact: **[support@thegreenbow.com](mailto:support@thegreenbow.com)**

## Table of Contents

1	Introduction.....	3
1.1	Goal of this document.....	3
1.2	VPN Network topology .....	3
1.3	Barracuda NG Firewall Restrictions .....	3
1.4	Barracuda NG Firewall VPN Gateway .....	3
1.5	Barracuda NG Firewall VPN Gateway product info .....	3
2	Barracuda NG Firewall VPN configuration.....	4
2.1	Configure the Client Network and Gateway .....	4
2.2	Create a Barracuda VPN CA Template .....	4
2.3	Add a Personal License .....	5
2.4	Step 4. Add Firewall Rules.....	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.....	8
4	Tools in case of trouble.....	9
4.1	A good network analyser: Wireshark.....	9
5	VPN IPsec Troubleshooting.....	10
5.1	“PAYLOAD MALFORMED” error (wrong Phase 1 [SA]) .....	10
5.2	“INVALID COOKIE” error .....	10
5.3	“no keystate” error .....	10
5.4	“received remote ID other than expected” error .....	10
5.5	“NO PROPOSAL CHOSEN” error .....	11
5.6	“INVALID ID INFORMATION” error .....	11
5.7	I clicked on “Open tunnel”, but nothing happens. ....	11
5.8	The VPN tunnel is up but I can’t ping ! .....	12
6	Contacts .....	13

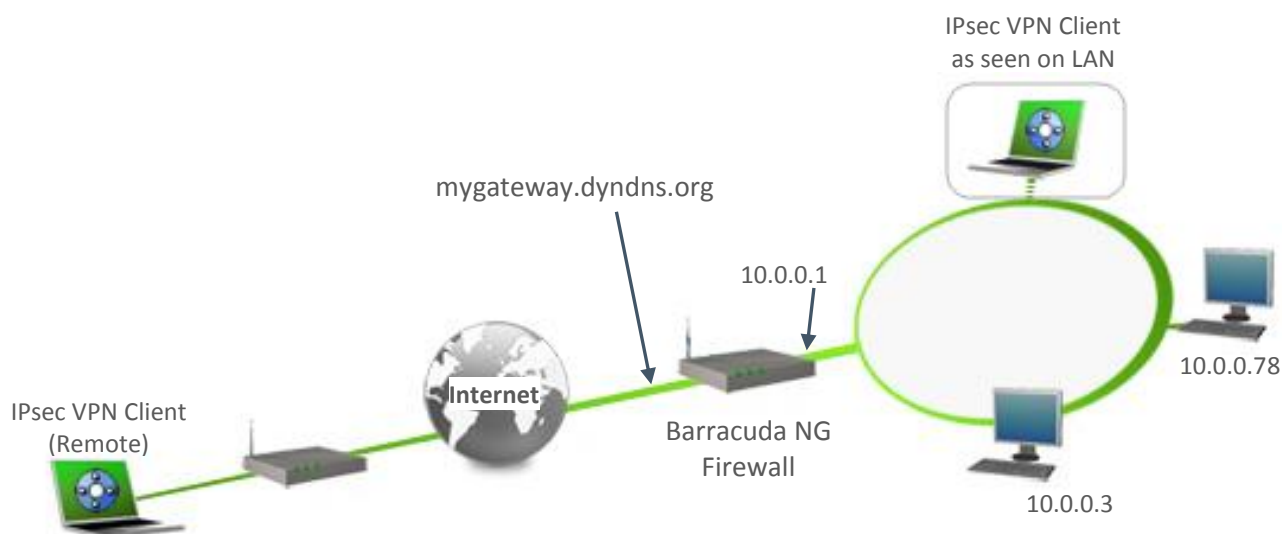
## 1 Introduction

### 1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a Barracuda NG Firewall VPN router to establish VPN connections for remote access to corporate network.

### 1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client software to the LAN behind the Barracuda NG Firewall 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 Barracuda NG Firewall Restrictions

No known restrictions.

### 1.4 Barracuda NG Firewall VPN Gateway

Our tests and VPN configuration have been conducted with Barracuda NG Firewall firmware release 5.4.

### 1.5 Barracuda NG Firewall VPN Gateway product info

It is critical that users find all necessary information about Barracuda NG Firewall VPN Gateway. All product info, User Guide and knowledge base for the Barracuda NG Firewall VPN Gateway can be found on the Barracuda NG Firewall website: <https://www.barracuda.com/products/ngfirewall>

Barracuda NG Firewall Product page  
Barracuda NG Firewall User Guide

<https://www.barracuda.com/products/ngfirewall>  
[https://www.barracuda.com/assets/docs/Introduction\\_Presentations/Barracuda\\_NGF\\_Product\\_Overview\\_US.pdf](https://www.barracuda.com/assets/docs/Introduction_Presentations/Barracuda_NGF_Product_Overview_US.pdf)  
<https://www.barracuda.com/products/ngfirewall/faq>

Barracuda NG Firewall FAQ/Knowledge Base

## 2 Barracuda NG Firewall VPN configuration

This section describes how to build an IPsec VPN configuration with your Barracuda NG Firewall VPN router. Once connected to your Barracuda NG Firewall VPN gateway,

### 2.1 Configure the Client Network and Gateway

- Open the **VPN Settings** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN Service > VPN Settings**).
- Click **Lock**.
- Verify that the default server certificate and key are valid.
- Right-click the **Settings** table and select **Edit Server Settings**.
- Verify that the **Default Server Certificate** and **Default Key** are both valid (green).
- Close the **Server Settings** window.
- Configure the client network.
- Click the **Client Networks** tab.
- Right-click the table and select **New Client Network**.
- In the **Client Network** window, configure the following settings:

Setting	Description
<b>Name</b>	<i>Client to Site VPN Network</i>
<b>Network Address</b>	192.168.6.0
<b>Network Mask</b>	24
<b>Gateway</b>	192.168.6.1
<b>Type</b>	Specifies the type of network that is used for VPN clients: routed (Static Route) – A separate subnet. A static route on the Barracuda NG Firewall routes traffic between the VPN client subnet and the local network. local (proxy ARP) – A subnet of a local network. For example, Local network: 10.0.0.0/24, Local segment 10.0.0.128/28. You must also specify the IP range for the network: <b>IP Range Base</b> – The first IP address in the IP range for the VPN client subnet (e.g., 10.0.0.128). <b>IP Range Mask</b> – The subnet mask of the VPN client subnet (e.g. 28).

- Click **OK**.
- Click **Send Changes** and then click **Activate**.

### 2.2 Create a Barracuda VPN CA Template

- Open the **Client to Site** page (**Config > Full Config > Box > Virtual Server > your virtual server > Assigned Services > VPN Service > Client to Site**).
- Click **Lock**.
- Click the **Barracuda VPN CA** tab and then click the **Templates** tab under it.
- Right-click the table and select **New Template**.
- In the **Barracuda Templates** window, configure the following settings:

Setting	Description
Name	<i>VPNTemplate</i>
DNS	(Optional) The IP address of the DNS server.
WINS	(Optional) The IP address of the WINS server.
Network Routes	<i>10.0.0.0/24</i>
Accepted Ciphers	The encryption algorithms that the VPN server will offer. Recommended settings: <ul style="list-style-type: none"><li>• <i>AES</i> for licensed systems.</li><li>• <i>DES</i> for export restricted systems.</li></ul>

- Click **OK** to save the template.
- Click **Send Changes** and then click **Activate**.

## 2.3 Add a Personal License

- Open the **Client to Site** page (**Config > Full Config > Box > Virtual Server > your virtual server > Assigned Services > VPN Service > Client to Site**).
- Click **Lock**.
- Click the **Barracuda VPN CA** tab and then click the **Pool Licenses** tab under it.
- In the upper table, select your **VPN Pool Licenses**.
- Right-click the lower table and select **New personal license**.
- Select an index number for the new license and then click **OK**.
- In the **Personal License** window, configure the license.
- In the **Used by** field, enter the name of the user (e.g., *Test User*).
- In the **IP Address & Networking** section, specify these settings:
  - **Network** – The client network.
  - **Template** – *VPNTemplate*
  - **ENA** – Active ENA (Exclusive Network Access) prevents access to networks the client is not directly connected to.



VPN connections with enabled ENA setting, can only be established with VPN clients running the Barracuda Personal Firewall.

- In the **Password and Peer Restriction** section, click **Change Server Password** to set a server password.
- From the the **Active Certificate** tab:
  - Select the server certificate from the **Certificate** list (e.g., *ServerCertificate*).
  - Verify that the **Certificate** and **User Key** are listed as *Valid*.
- Click **Export to File** to export the license file. This file will be distributed to clients to authenticate when connecting to the VPN (e.g., *personal\_license1.lic*).  
You can choose to enter a password to protect the file.

**Personal License**

**Change Personal License**

License is disabled

License: barracudavpn-99-1

Used by: testuser

Stat. Name:

**IP Address & Networking**

Assigned IP: Dynamic Address

Network: VPNClientNetwc Nr. dyn

Template: VPNTemplate Parameters...

ENA: No Split Tunnel ON

**Password and Peer Restriction**

Scheme: local

User ID:

VPN-Type: Personal + SSL

Change Server Password...

ACL: Addr/Mask

Add Delete

Enable VPN Client NAC

Active Certificate | Obsolete Certificate Usage: Only allow active key

License Type: File

Certificate: Valid

User Key: Valid (FXQLZZ) Bits: 512

Server Key: ServerCert

Edit Certificate.. Export to Clipboard...

Create New Key... Export to File...

Import Key... Export Issuer Cert...

Copy To Obsolete Certificate Mgmt...

OK Cancel

- Click **OK** to save the personal license.
- Click **Send Changes** and then click **Activate**. In the **Status** column next to the new personal license, a green check mark indicates that the license file can now be used on a client to connect to the VPN.

## 2.4 Add Firewall Rules

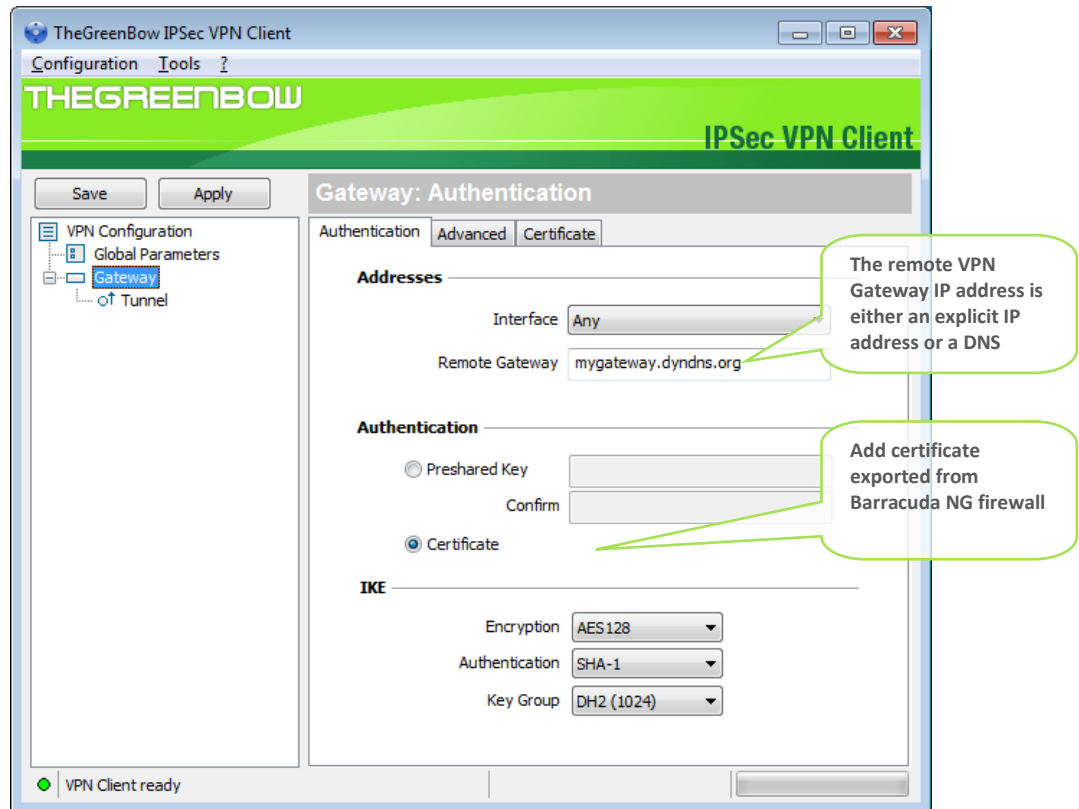
Add two forwarding firewall rules to connect your client-to-site VPN to your network.

## 3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a Barracuda NG Firewall VPN router via VPN connections.

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

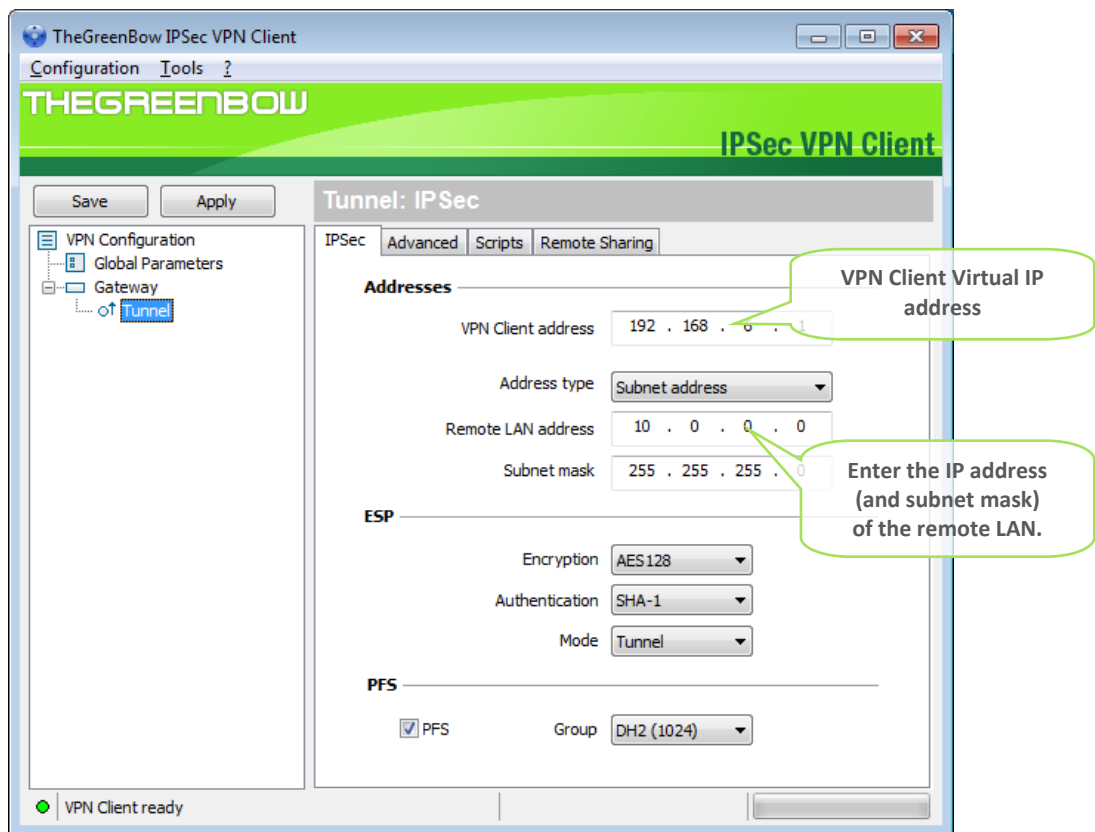
### 3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 configuration

You may use either Preshared key, Certificates, USB Tokens, X-Auth combined with RADIUS Server for User Authentication with the Barracuda NG Firewall router. This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Barracuda NG Firewall router user guide or TheGreenBow IPsec VPN Client software User Guide for more details on User Authentication options.

## 3.2 VPN Client Phase 2 (IPsec) Configuration



Phase 2 Configuration

## 3.3 Open IPsec VPN tunnels

Once both Barracuda NG Firewall 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 Barracuda NG Firewall VPN router.

```
20110215 141513 Default phase 1 done: initiator id /C=fr/ST=idf/L=paris/O=bloodzonard/OU=seri
20110215 141513 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) RECV phase 2 Quick Mode [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode [HASH]
20110215 141524 Default (SA gateway1-P1) RECV Informational [HASH] [NOTIFY] type DPD_R_
20110215 141524 Default (SA gateway1-P1) SEND Informational [HASH] [NOTIFY] type DPD_R_
20110215 141534 Default (SA gateway1-P1) SEND Informational [HASH] [DELETE]
20110215 141534 Default <gateway1-tunnel1-P2> deleted
20110215 141534 Default (SA gateway1-P1) SEND Informational [HASH] [DELETE]
```

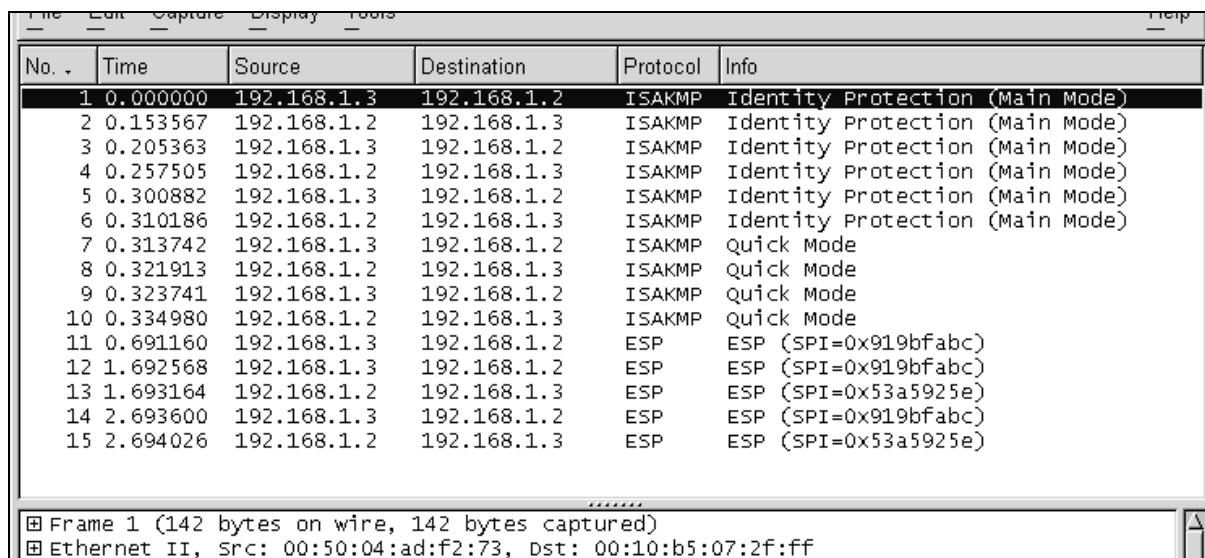


## 4 Tools in case of trouble

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 [www.wireshark.org](http://www.wireshark.org). It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation ([www.wireshark.org/docs/](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 ([www.wireshark.org](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: [www.thegreenbow.com](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)

# **Secure, Strong, Simple**

TheGreenBow Security Software