



TheGreenBow IPsec VPN Client Configuration Guide

Opengear IPsec gateway (IM4200, IMG4000 & ACM5000)

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

Contact: support@thegreenbow.com

Configuration Guide written by:

Writer: support@opengear.com

Company: www.opengear.com

Table of contents

1	Introduction	3
1.1	Goal of this document	3
1.2	VPN Network topology	3
1.3	Opengear Restrictions	3
1.4	Opengear VPN gateway	3
1.5	Opengear VPN gateway product info.....	3
2	Opengear VPN configuration	4
2.1	Enable the Opengear VPN gateway	4
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.....	10
4.1	A good network analyser: Wireshark	10
5	VPN IPsec Troubleshooting	11
5.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA]).....	11
5.2	« INVALID COOKIE » error.....	11
5.3	« no keystate » error	11
5.4	« received remote ID other than expected » error.....	11
5.5	« NO PROPOSAL CHOSEN » error	12
5.6	« INVALID ID INFORMATION » error.....	12
5.7	I clicked on "Open tunnel", but nothing happens.....	12
5.8	The VPN tunnel is up but I can't ping !.....	12
6	Contacts.....	14

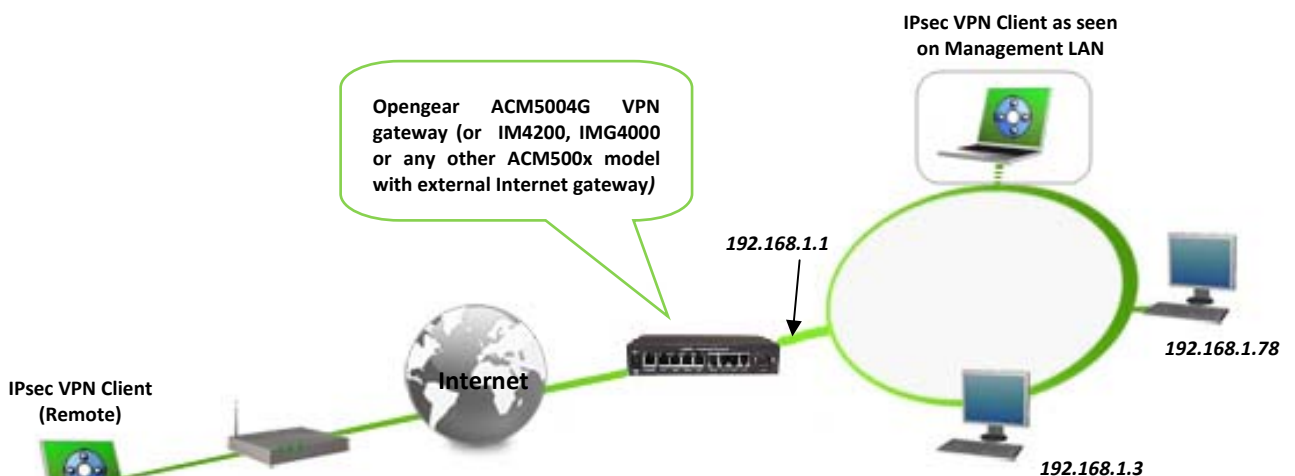
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure the GreenBow IPsec VPN Client software with an Opengear console server VPN gateway to establish VPN connections to remotely access the console server, attached serial devices and devices on its management LAN.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect the GreenBow IPsec VPN Client software to the Management LAN behind the Opengear VPN 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.



1.3 Opengear Restrictions

Opengear firmware version 2.8.1 or later is required to work with the TheGreenBow IPsec VPN client. This firmware can be downloaded from <http://www.opengear.com/download.html>.

1.4 Opengear VPN gateway

Our tests and VPN configuration have been conducted with Opengear firmware release 2.8.1.

1.5 Opengear VPN gateway product info

Opengear's ACM5000, IMG4000 and IM4200 Console Servers each include Openswan, a Linux IPsec implementation.

The Opengear IPsec VPN gateway function is available in the ACM5004G Console Server which connects directly to the wireless Internet. The Opengear IMG4216-25, IMG4004-5, IM4208-2/4216-2/4248-2 and ACM5002/5003/5004 model Console Servers can also serve as a VPN gateway when connected to the Internet through an appropriately configured Internet gateway. These products are referred to collectively in this document as the Opengear VPN gateway.

All product info, user guides and frequently asked questions for the products that provide the Opengear VPN gateway can be found on the Opengear website: www.opengear.com

Opengear Product page	www.opengear.com/products.html
Opengear User Guide	www.opengear.com/download/manual/
Opengear FAQ/Knowledge Base	www.opengear.com/faq.html

2 Opengear VPN configuration

The IMG4216-25, IMG4004-5, IM4208-2/4216-2/4248-2 and ACM5002/5003/5004(M/W) require an Internet gateway (such as DSL router) with port forwarding configured for port 500 UDP and protocol 50 (ESP). The ACM5004G is a cellular VPN end-point connected directly to the wireless Internet, and generally requires static (persistent) IP addresses.

TheGreenBow IPsec VPN client enables the remote administrator to connect to a remote Opengear VPN gateway over the Internet. Through this secure VPN connection the administrator can access the *console server* and attached serial consoles, and networked devices on the Management LAN.

Configuration of IPsec is quite complex so Opengear provides a simple GUI interface for basic set up as described below. However for more detailed information on configuring Openswan IPsec at the command line refer wiki.openswan.org, www.thegreenbow.com/doc/tgbvpn_cg_Linux_en.pdf or www.opengear.com/faq.html

This section describes how to build an IPsec VPN configuration with your Opengear VPN gateway.

2.1 Enable the Opengear VPN gateway

- Connect to the management console on your Opengear VPN gateway
- Select **IPsec VPN** on the **Serial & Networks** menu and click **Add** (or **Edit** to update an existing IPsec Tunnel)
- In **Tunnel Name** enter any descriptive name you wish to identify the IPsec Tunnel you are adding (such as *WestStOutlet-VPN*).
- The Opengear VPN gateway will already have been assigned a **System Name** when it was configured (eg *img4004-5*) using **Administration** in the **System** menu

System Name: img4004-5 Model: IMG4004-5 Firmware: 2.8.1
 Uptime: 0 days, 1 hours, 59 mins, 45 secs Current User: root

Serial & Network: IPsec VPN

Add IPsec Tunnel

Tunnel Name:
A descriptive name for the IPsec tunnel

Authentication Method:
 RSA digital signatures
 Shared secret (PSK)
Authenticate using RSA digital signatures or a shared secret (PSK)

Generate Keys: RSA digital signatures cannot be used until IPsec RSA keys have been generated.
Click [here](#) to generate keys.

Authentication Protocol:
 ESP
 AH
Authenticate as part of ESP encryption or separately using the AH protocol

Left ID:
The identifier for this end of the tunnel, should include a fully qualified domain name preceded by @, e.g. left@example.com

Right ID:
The identifier for the other end of the tunnel, should include a fully qualified domain name preceded by @, e.g. right@example.com

Left Address:
The public IP or DNS address of this end of the tunnel, leave blank to use the interface of the default route

Right Address:
The public IP or DNS address of the other end of the tunnel, leave blank if it is dynamic

Left Subnet:
The private subnet behind this end of the tunnel in CIDR notation, e.g. 192.168.123.0/24, leave blank to allow connections to this host only

Right Subnet:
The private subnet behind the other end of the tunnel in CIDR notation, e.g. 192.168.123.0/24, leave blank to connect to a single host

Initiate Tunnel:
Initiate the tunnel connection from this end

Descriptive name e.g. WestStOutlet-VPN89

Note: IPsec VPN connections are generally *peer to peer* connections (between gateways and gateways) rather than *client server* connections. So for convenience in the Opengear GUI in the Opengear VPN gateway is referred to as the Left or Local host/gateway, and TheGreenBow is the Remote or Right host/gateway

- Select *Shared secret (PSK)* as the **Authentication Method** to be used
- You will need to enter a passphrase (Pre Shared Key) and this same passphrase must be entered into TheGreenBow VPN Client software (such as 0123456789)

System Name: img4004-5 Model: IMG4004-5 Firmware: 2.8.1
 Uptime: 0 days, 2 hours, 4 mins, 30 secs Current User: root

Serial & Network: IPsec VPN

Add IPsec Tunnel

Tunnel Name:
A descriptive name for the IPsec tunnel

Authentication Method:
 RSA digital signatures
 Shared secret (PSK)
Authenticate using RSA digital signatures or a shared secret (PSK)

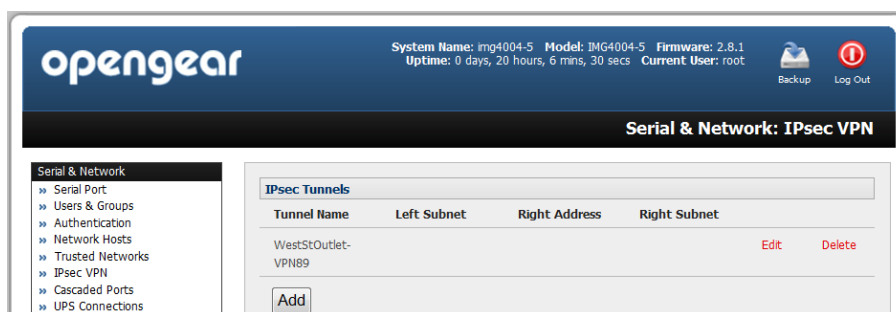
Shared Secret (PSK):
A passphrase, must match the passphrase configured at the other end of the tunnel

Shared secret e.g. 0123456789

- In **Authentication Protocol** select the authentication protocol to be used. Either authenticate as part of *ESP* (Encapsulating Security Payload) encryption or separately using the *AH* (Authentication Header) protocol. Leave at default (ESP)
- Leave the **Left ID** and **Right ID** fields blank

Doc.Ref	tgbvpn_ug-Opengear-en
Doc.version	0.9 – Nov 2009
VPN version	4.x

- Enter the public IP or DNS address of this Opengear VPN gateway (or if not an ACM5004G enter the address of the gateway device connecting it to the Internet) as the **Left Address**. You can leave this blank to use the interface of the default route
- In **Right Address** enter the public IP or DNS address of the remote end of the tunnel (only if the remote end has a static or dyndns address). Otherwise leave this blank
- If the Opengear VPN gateway is serving as a VPN gateway to a local subnet (e.g. the *console server* has a Management LAN configured) enter the private subnet details in **Left Subnet**. Use the CIDR notation (where the IP address number is followed by a slash and the number of 'one' bits in the binary notation of the netmask). For example 192.168.0.0/24 indicates an IP address where the first 24 bits are used as the network address. This is the same as 255.255.255.0. If the VPN access is only to the console server itself and to its attached serial console devices then leave **Left Subnet** blank
- If there is a VPN gateway at the remote end, enter the private subnet details in **Right Subnet**. Again use the CIDR notation and leave blank if there is only a remote host
- Select **Initiate Tunnel** if the tunnel connection is to be initiated from the Left console server end. This can only be initiated from the VPN gateway (Left) if the remote end was configured with a static (or dyndns) IP address
- Click **Apply** to save changes



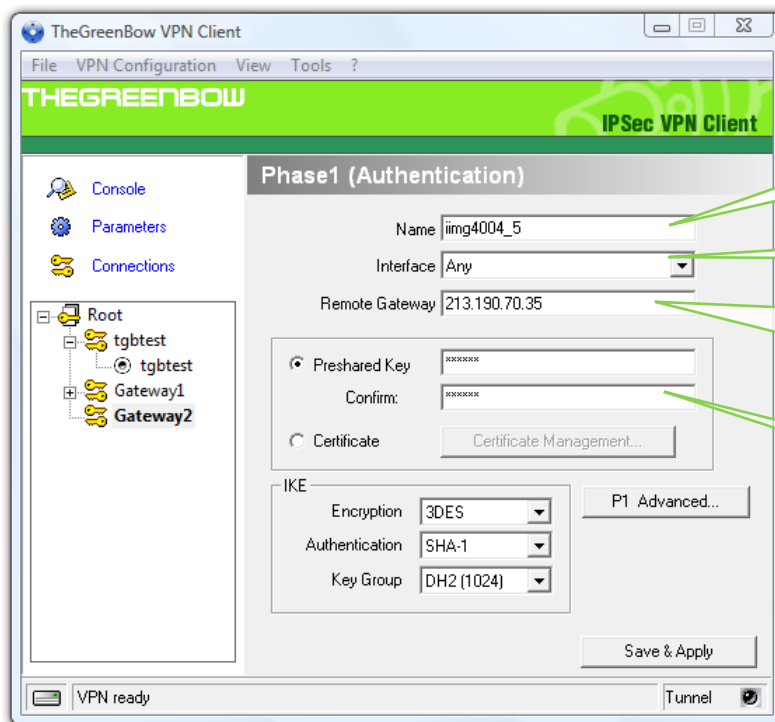
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Opengear VPN gateway via VPN connections. To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html.



Launch TheGreenBow IPSec VPN Client with the icon on your Windows desktop

3.1 VPN Client Phase 1 (IKE) Configuration



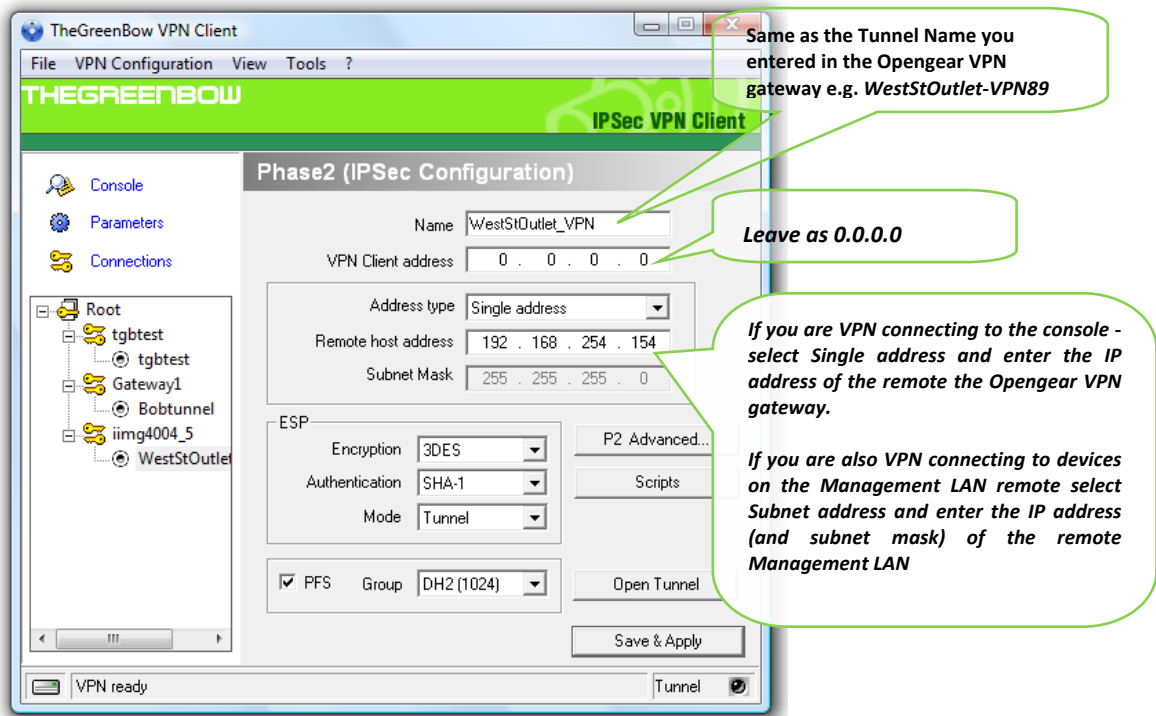
Phase 1 configuration

- To create Phase 1 (IKE) you will need to enter the remote Opengear VPN gateway's System Name (Name) and IP address or DNS name (Remote Gateway)
- Select use **Preshared Key** for User Authentication with the Opengear VPN gateway - entering the same keys that were configured on the remote Opengear VPN gateway
- Click **Save & Apply** to save the settings

The above configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Opengear User Manual or TheGreenBow IPSec VPN Client software User Guide for more details on configuring Certificates and other advanced options.

3.2 VPN Client Phase 2 (IPSec) Configuration

- To create a Phase2 right click the Phase 1 policy that was added in the left hand panel (e.g. the new gateway "img4005-5" added above) and click **Add Phase 2**
- Fill in the appropriate fields for the Phase 2 settings, shown in the following screenshot:

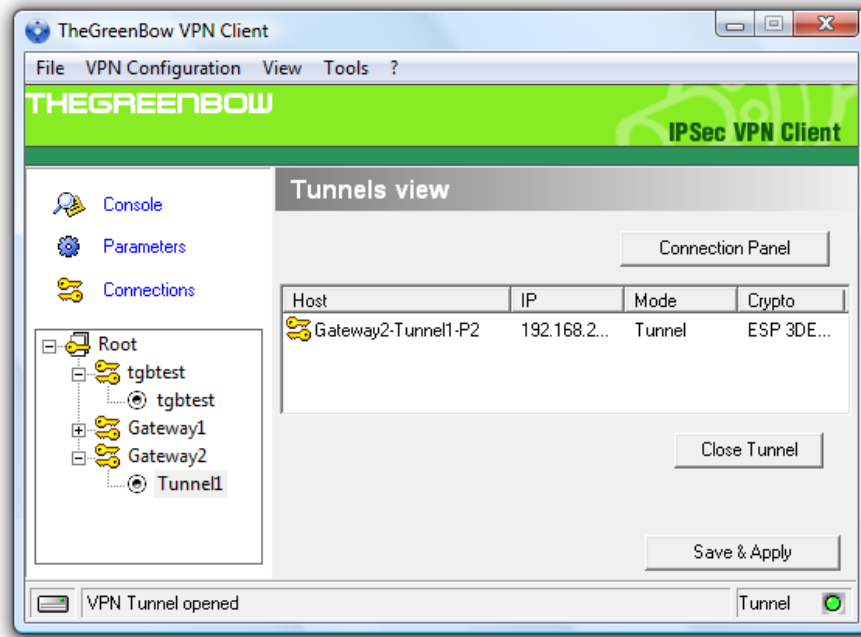


Phase 2 Configuration

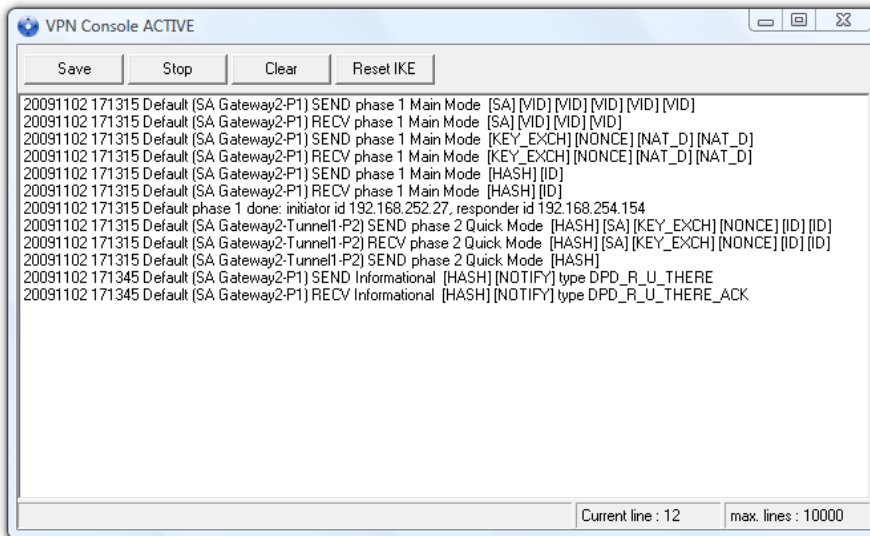
3.3 Open IPsec VPN tunnels

Once both Opengear VPN gateway and TheGreenBow IPsec VPN Client software have been configured you are ready to open VPN tunnels. First make sure you enable your firewall with IPsec traffic.

- Click on **"Save & Apply"** to take into account all modifications we've made on your VPN Client configuration
- Click on **"Open Tunnel"**, or generate traffic that will automatically open a secure IPsec VPN Tunnel (e.g. ping, IE browser)
- Select **"Connections"** to see opened VPN Tunnels



- 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 Opengear VPN gateway.

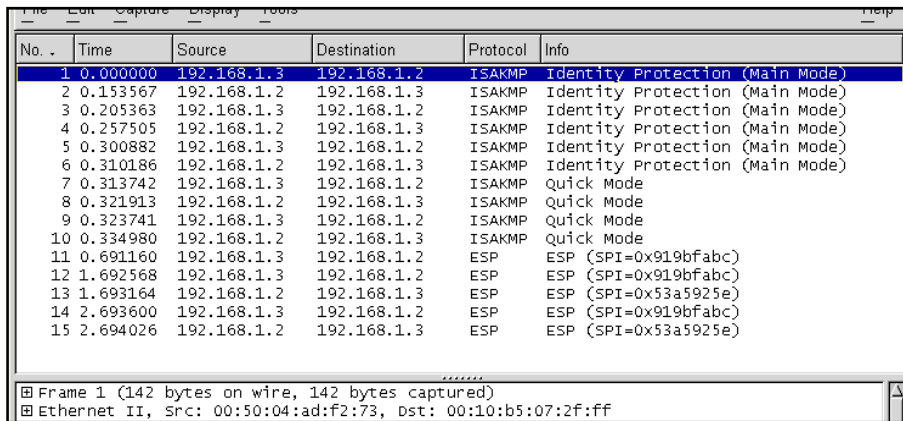


4 Tools in case of trouble

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

Doc.Ref	tgbvpn_ug-Opengear-en
Doc.version	0.9 – Nov 2009
VPN version	4.x

- 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.

	Doc.Ref	tgbvpn_ug-Opengear-en
	Doc.version	0.9 – Nov 2009
	VPN version	4.x

6 Contacts

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

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com