



# TheGreenBow IPsec VPN Client Configuration Guide

## Opengear IPsec gateway (IM4200, IMG4000 & ACM5000)

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

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

Configuration Guide written by:

Writer: [support@opengear.com](mailto:support@opengear.com)

Company: [www.opengear.com](http://www.opengear.com)

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

## 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

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

# 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

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

## 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.

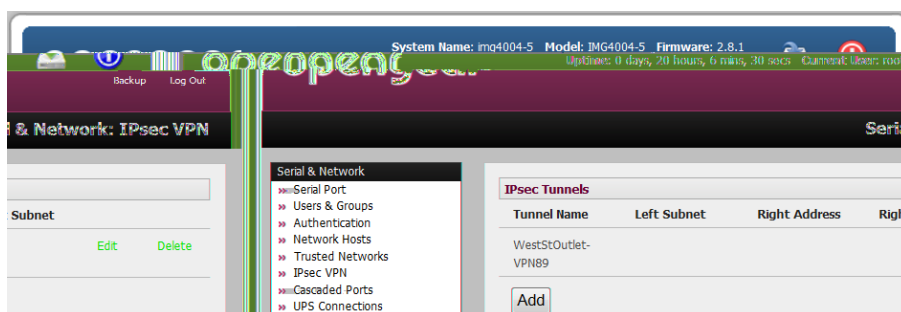
TheGreenBow IPsec VPN client enables the remote administrator to connect to a remote Opengear VPN gateway over the Internet. Through this secure VPN connection the administrator can access the *console server* and attached serial consoles, and networked devices on the Management LAN.

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 [Op 1 Op >](#)

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

	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



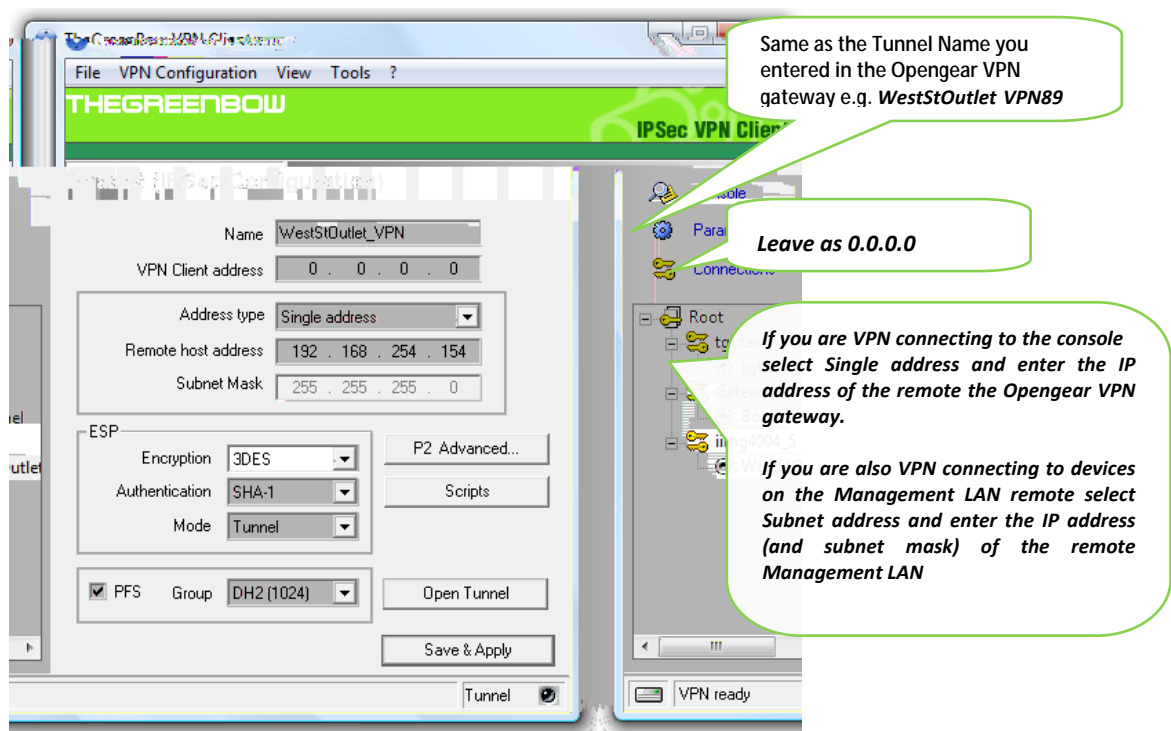
L

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

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

### 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

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

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

## 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	0.253505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
5	0.263505	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
6	0.263505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
7	0.263505	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
8	0.263505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
9	0.263505	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
10	0.263505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
11	0.263505	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
12	0.263505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
13	0.263505	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
14	0.263505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
15	0.263505	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
16	0.263505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
17	0.263505	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
18	0.263505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
19	0.263505	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
20	0.263505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)

42 bytes captured on interface eth0, 42 bytes on wire (capture length 42 bytes) on interface eth0, 42 bytes on wire (capture length 42 bytes) on interface eth0

Frame 1 (42 bytes on wire) captured on interface eth0 (0:10:b5:c0:2f:ff) from 192.168.1.3 to 192.168.1.2 on interface eth0 (0:10:b5:c0:2f:ff)

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

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

## 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

```

---

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

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