IPsec VPN Guide

Opengear to Snapgear

This is a guide on how to create an IPsec VPN tunnel between an Opengear device and a Snapgear device. The Opengear device is using 3G to connect to the Internet and the Snapgear is using ADSL2+. The example presented in this guide uses PSK authentication.

In this document:

1. Configuring the Snapgear
2. Configuring the Opengear
3. Notes on Opengear IPsec VPN Configuration

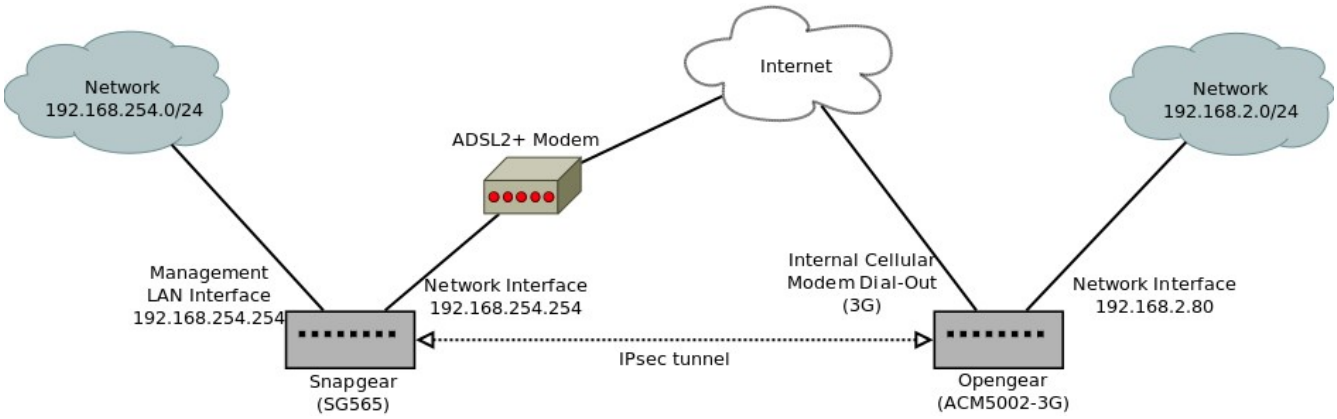
Background on how IPsec works:

http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6

Scenario: creating an IPsec VPN tunnel between two secure networks over an insecure network (such as the Internet).

- Snapgear device (SG565) to manage a local network
- Opengear device (ACM5002-3G) to manage a remote network

The IPsec VPN tunnel is to be created between these two gateways. Network hosts behind the Opengear would be able to securely communicate with the network hosts behind the Snapgear.



1. Configuring the Snapgear

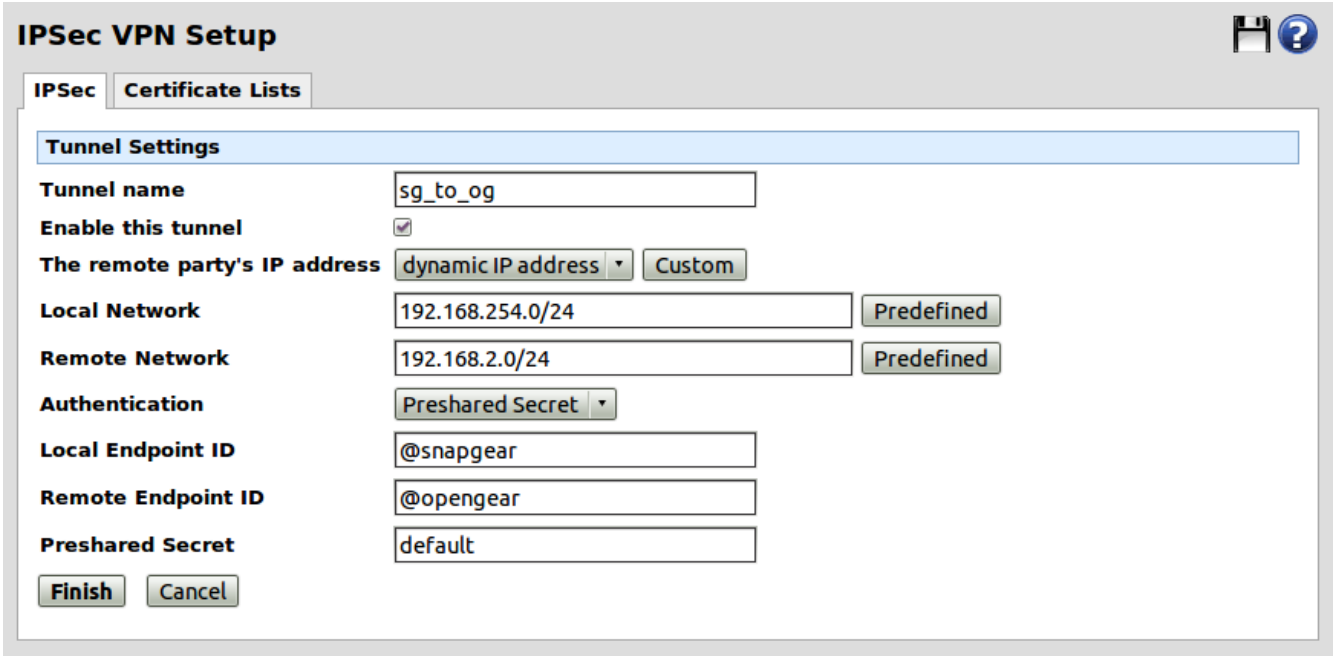
In this example the Snapgear is connecting to the Internet via an ADSL2+ modem and is the gateway for the local network 192.168.254.0/24. The Opengear is connecting to the Internet via an internal cellular (3G) modem and is the gateway for the remote network 192.168.2.0/24.

1. In the Web UI for the Snapgear go to **VPN** → **IPsec**. From here you can enter the below details using **Quick Setup** or **Advanced**.

2. **Quick Setup**:

Field	SG565
Tunnel Name	sg_to_og
Enable this tunnel	No
The remote party's IP address	[click on Predefined to select dynamic IP address]
Local Network	192.168.254.0/24
Remote Network	192.168.2.0/24
Authentication	Preshared Secret
Local Endpoint ID	@snapgear
Remote Endpoint ID	@opengear
Preshared Secret	default

Replace Local Network with the private network address behind the Snapgear and Remote Network with the private network address behind the Opengear.

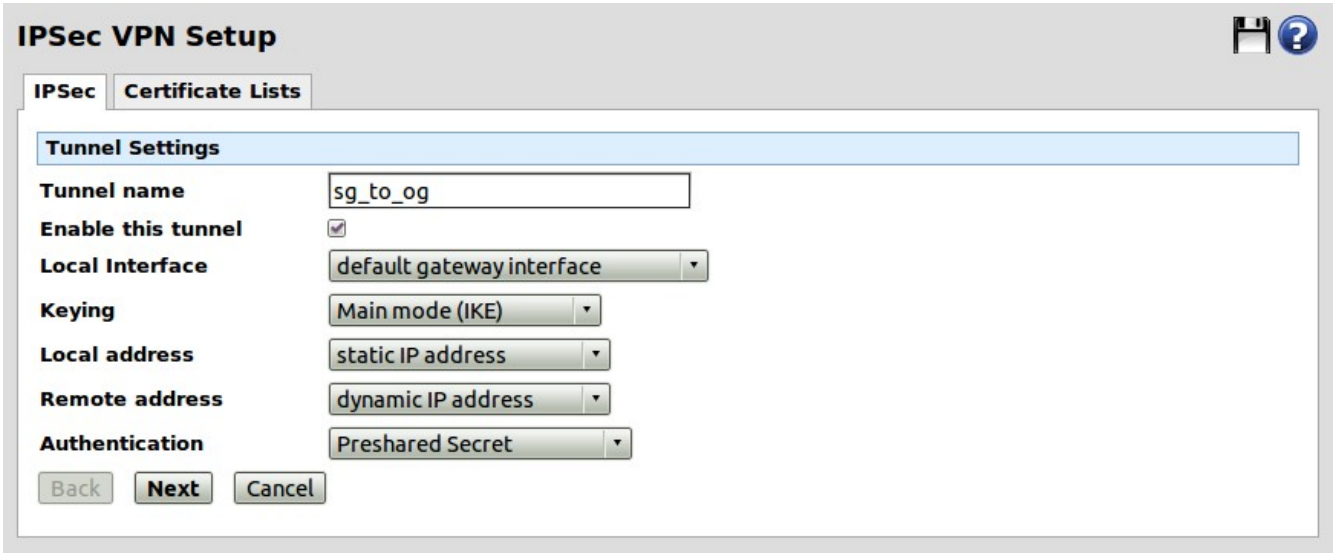


Click **Finish**

You will need to enter **Advanced** mode in order to change the **Keying** to '**Main mode (IKE)**'.

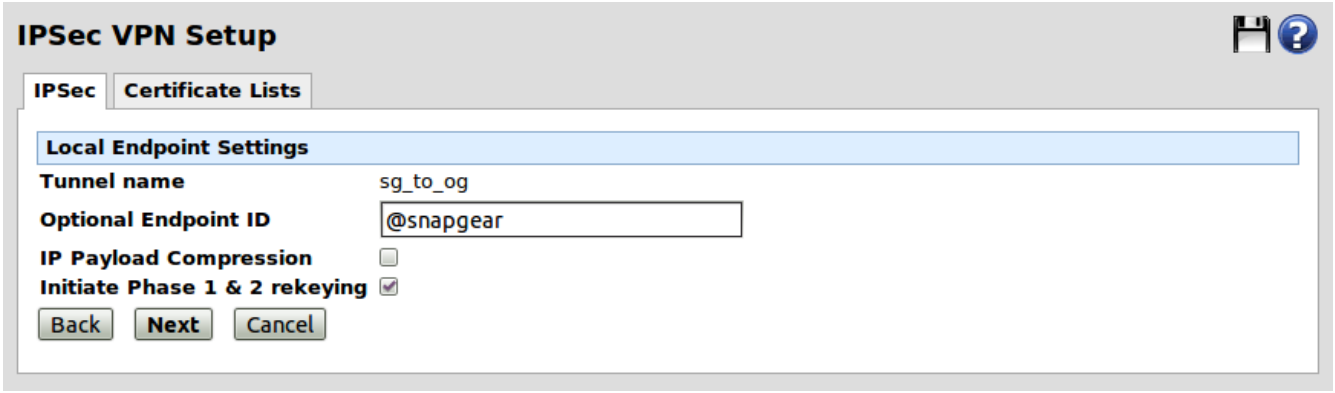
3. **Advanced**

Enter the following:



Click **Next**

Enter local ID:

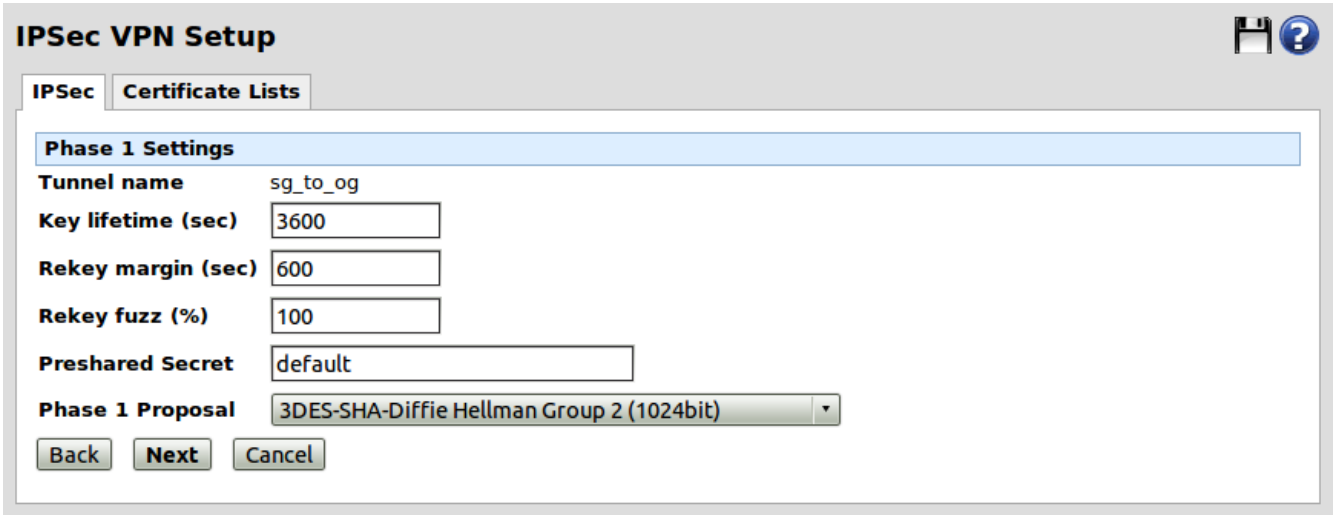


Click **Next**

Enter remote ID:

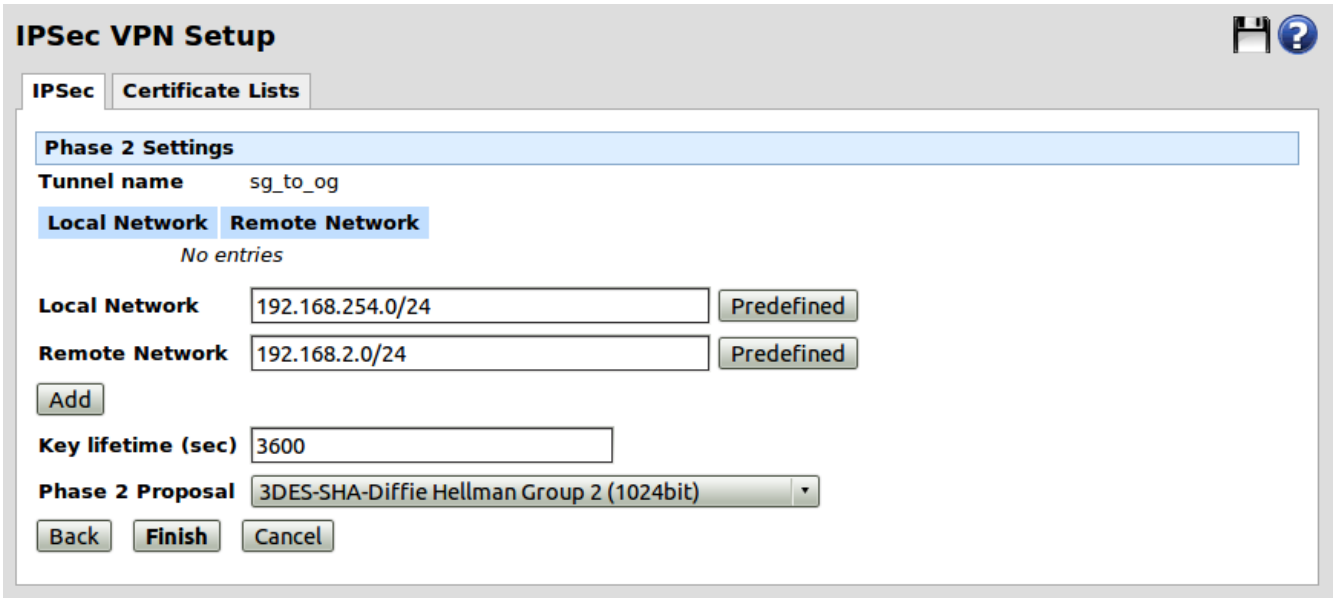
Click **Next**

Enter Preshared Secret

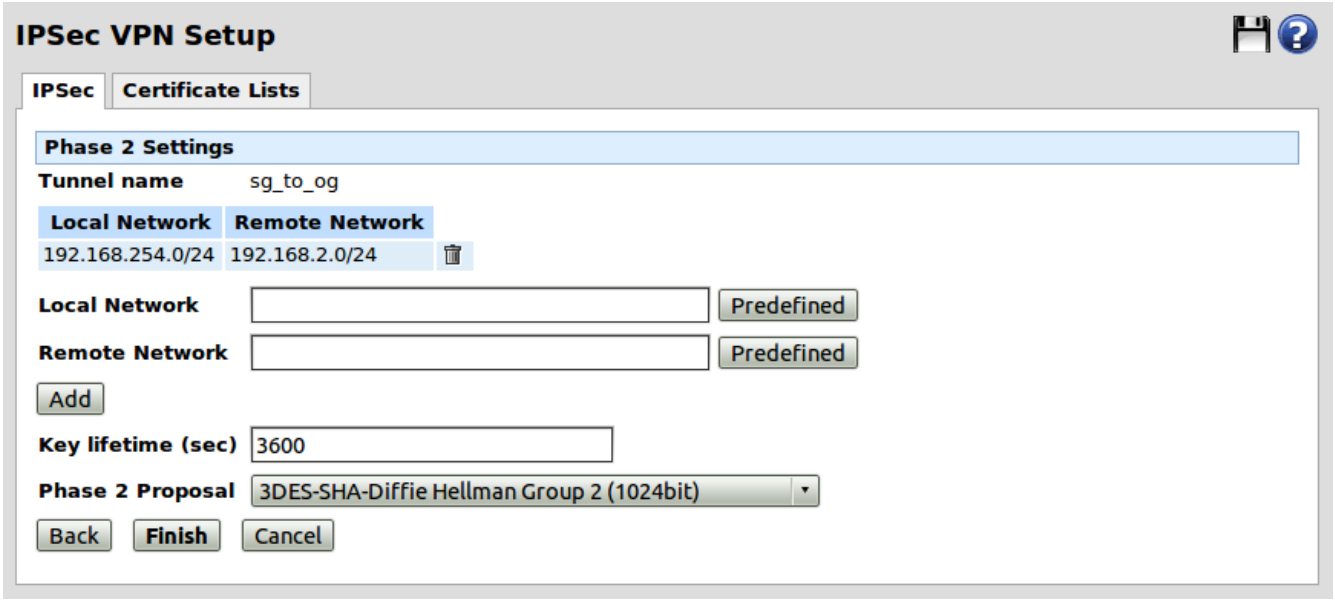


Click **Next**

Enter the local subnet and the remote subnet addresses (ie the private network addresses behind the Snapgear and Opengear respectively):

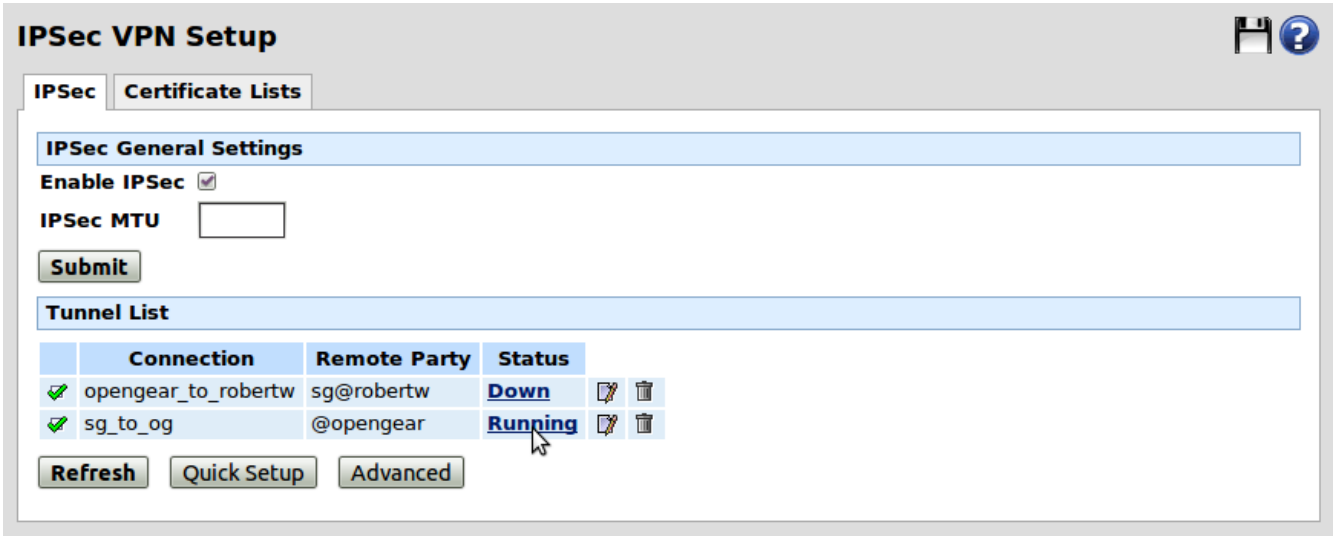


Click **Add**

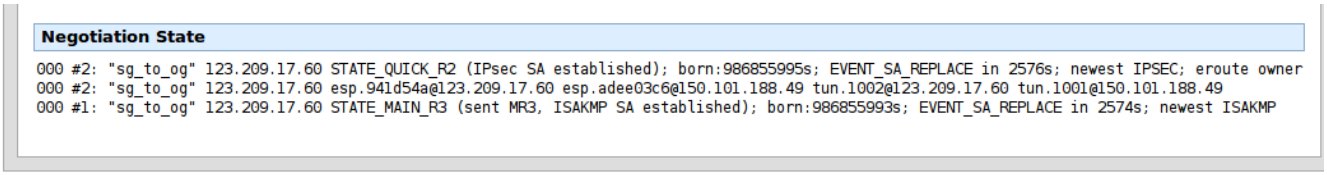


Click **Finish**

Once the tunnel is up and running (ie configured on the Opengear side as well) you can observe the following on the main IPSec VPN Setup page:



Click on **Running** for the newly created tunnel. Scrolling down to the bottom to Negotiation State you should see “IPsec SA established” once the tunnel is up and running.



2. Configuring the Opengear

1. Go to the Web UI, from the navigation menu under **Serial & Network** select **IPsec VPN**, click **Add**

2. Enter the details as listed in the table, there is a screenshot on the following page

In this example:

- The authentication method is Pre Shared Key (PSK)
- The Opengear device is an ACM5002-3G with private network address 192.168.2.80
- The Snapgear device is an SG565 with private network address 192.168.254.254

Field	Opengear Device
Tunnel Name	og_to_sg
Initiate Tunnel	Yes
Authentication Method	PSK
Shared Secret (PSK)	default
Authentication Protocol	ESP
Aggressive Mode	No
IKE Proposal	Negotiable
Perfect Forward Secrecy	No
Left ID	@opengear
Right ID	@snapgear
Left Address	*leave blank*
Right Address	*public.address.of.snapgear*
Left Subnet	192.168.2.0/24
Right Subnet	192.168.254.0/24

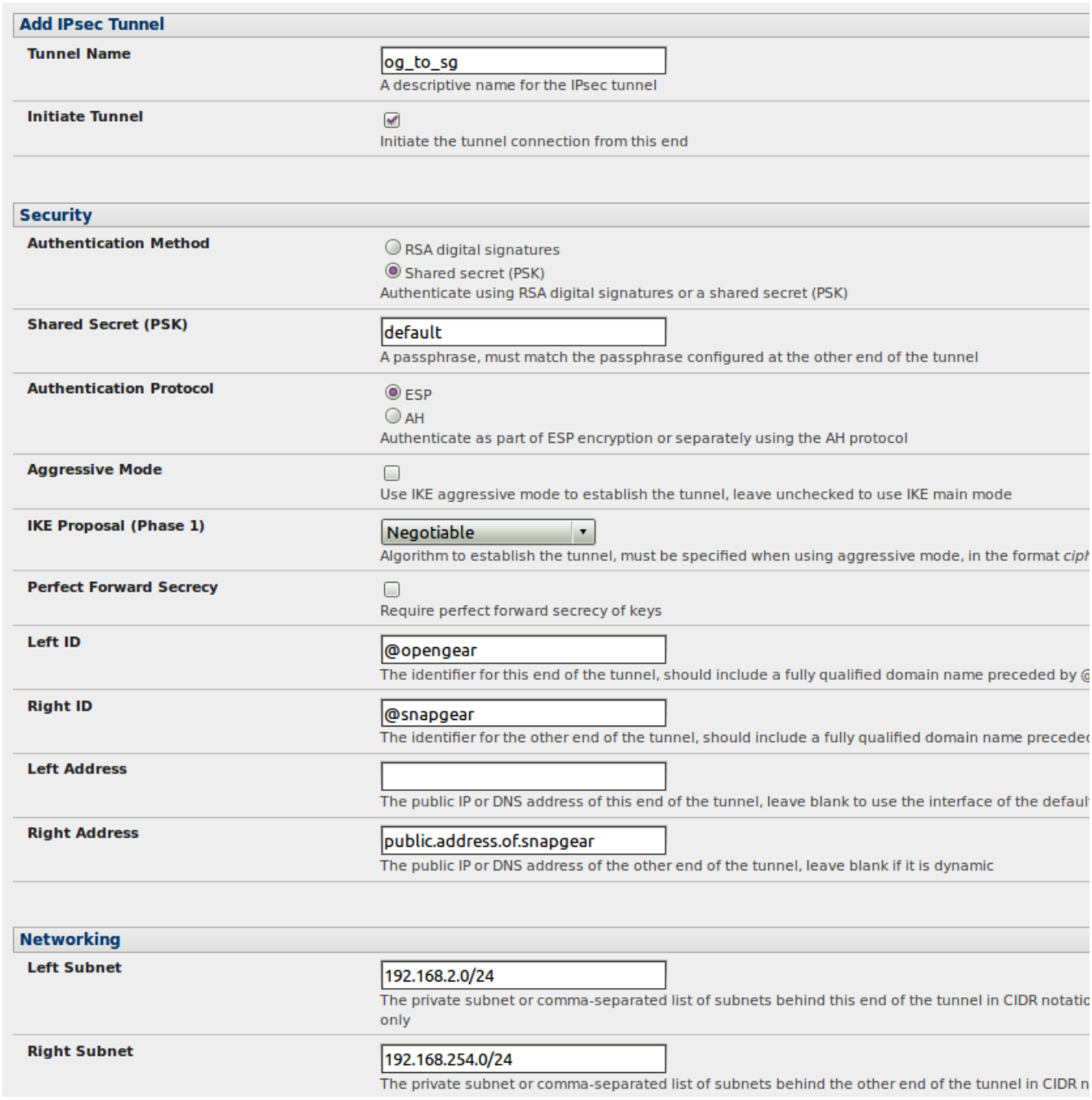
Replace Left Subnet with the private network address behind the Opengear device and Right Subnet with private network address behind the Snapgear device.

Replace public.address.of.snapgear with the public address of the Snapgear – eg IP address assigned by your Internet Service Provider. You may also use a DNS address.

After hitting **Apply** and once the tunnel is up and running "IPsec SA established tunnel mode" should be visible in the Syslog:

<84>Apr 10 18:55:14 pluto[27059]: "og_to_sg" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP=>0x41f3e508 <0xe3aea7bb xfrm=AES_128-HMAC_SHA1 NATOA=none NATD=none DPD=none}

ACM5002-3G IPsec VPN Configuration



3. Notes on Opengear IPsec VPN Configuration

- Only on: ACM500x, IM42xx, IMG4xxx and KCS
- Establishes a VPN connection between console servers at remote sites and a VPN gateway (e.g.: CISCO router) on central office network. Remote console server can be accessed with CMS6000 on central network.
- Uses Openswan to configure a VPN allowing multiple access to console servers
- 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.
- Enter a **Left ID** and **Right ID**. This is the identifier that the Local host/gateway and remote host/gateway use for IPsec negotiation and authentication. Each ID must include an '@' and can include a fully qualified domain name preceded by '@' (e.g. *left@example.com*)
- 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