IPsec VPN Guide

Opengear to Shrew Soft VPN Client

This is a guide on how to create an IPsec VPN tunnel from a local client running Shrew Soft VPN Client to an Opengear device.

In this document:

1. Network Configuration
2. Configuring the Opengear Side
3. Configuring the Shrew Soft Side
4. Example Using Dynamic DNS
5. Notes on Opengear IPsec VPN Configuration

Required files:

shrew_to_opengear.vpn (configuration for Shrew Soft VPN Client)

Background on how IPsec works:

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

The Shrew Soft VPN Client for Windows is a free IPsec Remote Access VPN Client for Windows 2000, XP, Vista and 7 operating systems (x86 and amd64 versions). It can be downloaded from:

http://www.shrew.net/download/vpn

Useful help resource:

http://www.shrew.net/static/help-2.1.x/vpnhelp.htm

If you are using Ubuntu the required packages can be downloaded via Synaptic Package Manager:

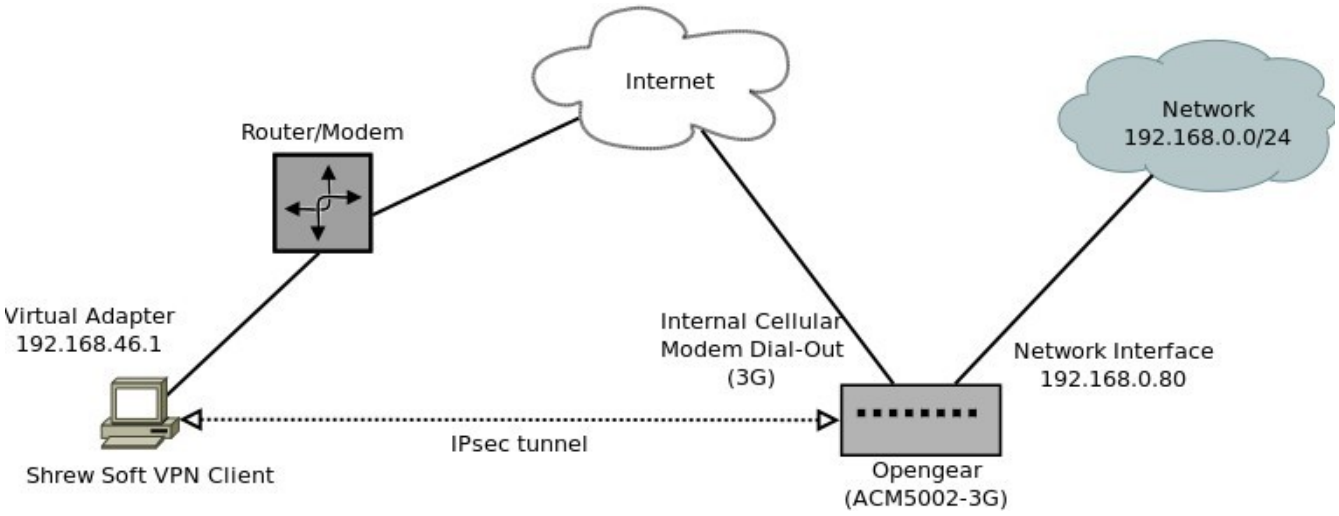
```
$ sudo apt-get install ike ike-qtgui
```

1. Network Configuration

In this guide the Opengear device is connected to the Internet via 3G. Instead of using the IP address assigned by the carrier, the Opengear device is configured to use dynamic DNS via dyndns. The address used is *opengeartest.dyndns.org* and is the *public address* of the Opengear device for the purposes of this guide.

In this example:

1. Opengear device ACM5002-3G
   Internal Cellular Modem: opengeartest.dyndns.org
   Network Interface: 192.168.0.80
2. Local workstation running Shrew Soft VPN Client
   Connected to Internet via router/modem (ADSL2+)
   Virtual Adapter: 192.168.46.1 (for the purposes of the VPN tunnel)



Scenario: you wish to establish a secure VPN to a remote site using an Opengear device with 3G. The IPsec VPN connection would allow you to manage any network hosts behind the Opengear eg:

- IP enabled PLC
- SCADA
- RDP

2. Configuring the Opengear Side

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:

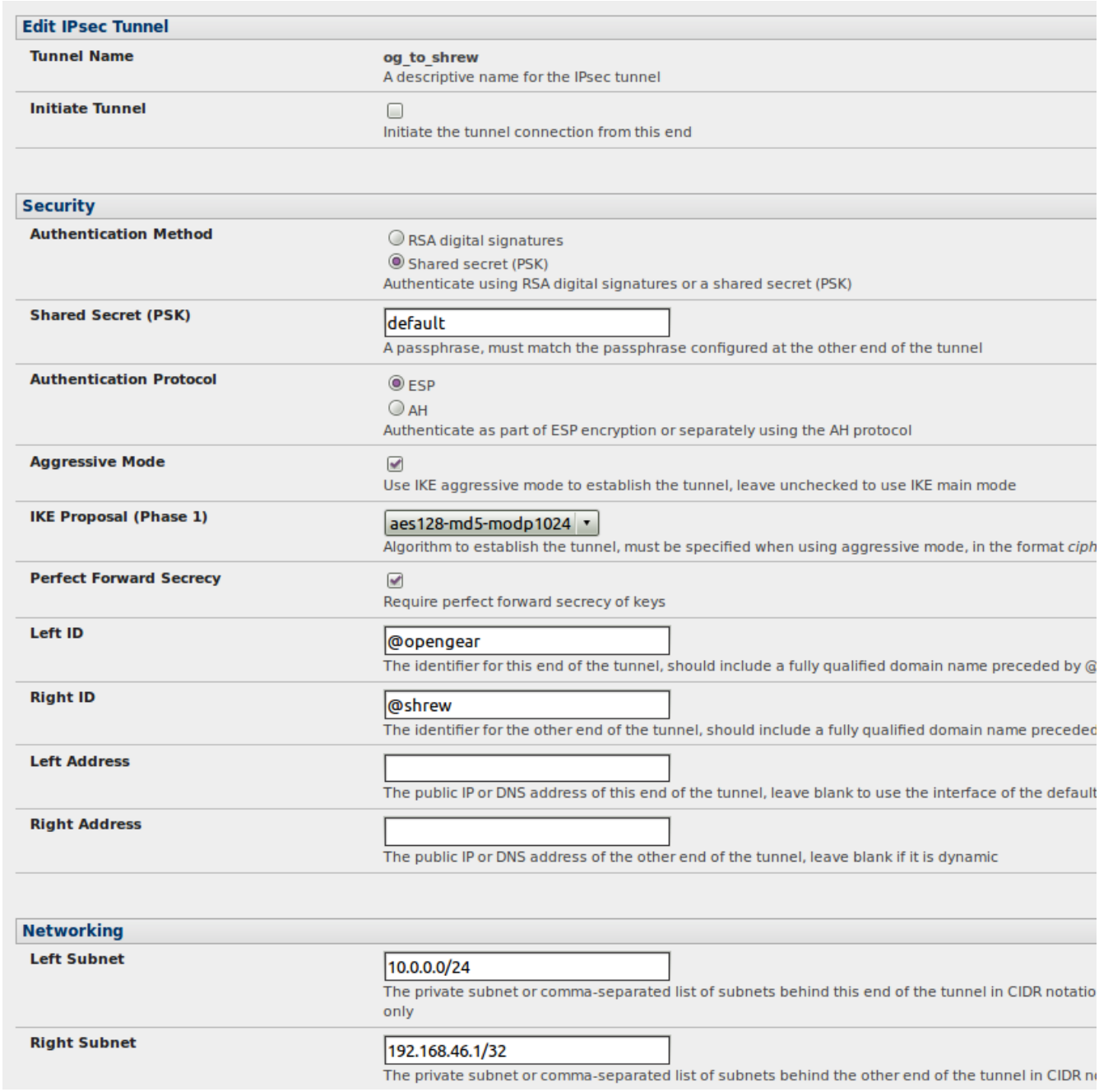
- The authentication method is Pre Shared Key (PSK)
- The Opengear device is an ACM5002-3G with private network address 192.168.0.80 using dynamic DNS opengeartest.dyndns.org
- The Shrew Soft VPN Client is on virtual address 192.168.46.1

Field	Opengear Device
Tunnel Name	og_to_shrew
Initiate Tunnel	No
Authentication Method	PSK
Shared Secret (PSK)	default
Authentication Protocol	ESP
Aggressive Mode	Yes
IKE Proposal	Select desired algorithm
Left ID	@opengear
Right ID	@shrew
Left Address	*leave blank*
Right Address	*leave blank*
Left Subnet	192.168.0.0/24
Right Subnet	192.168.46.1/32

Replace Left Subnet with the private network address of the Opengear device.

Replace Right Subnet with the private network address of the Shrew Soft VPN Client – this should be something other than your computer's LAN IP address and specific to the tunnel connection.

Screenshot of Opengear settings:



3. Configuring the Shrew Soft Side

1. Edit **shrew_to_opengear.vpn** with Notepad or similar

2. Search and replace opengear.public.address.here with the public IP address of the Opengear device.

> In this example the Internet IP of the Opengear is not static and a dynamic DNS provider is used – opengeartest.dyndns.org

3. Search and replace 192.168.14.0 / 255.255.255.0 with the private network address behind the Opengear

4. Open **Shrew Access Manager**, click **File** -> **Import** and choose **shrew_to_opengear.vpn**

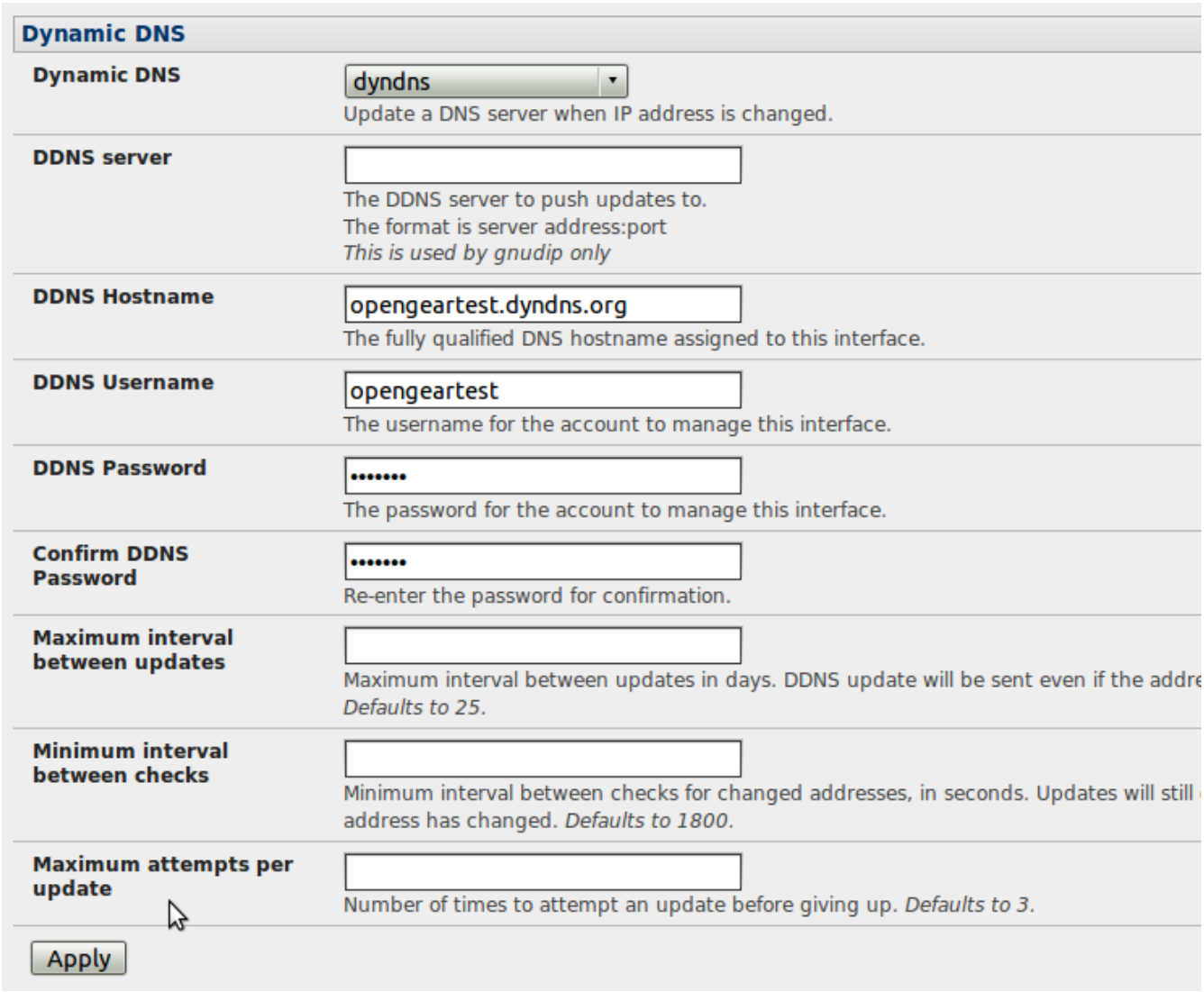
5. Click **Connect**. A new window will open up, click **Connect**.

6. Once the tunnel is working make sure you change the PSK passphrase at both ends to something secret (currently set to *default*).

"IPsec SA established tunnel mode" should be visible in the Syslog:

<84>Apr 5 23:01:56 pluto[7357]: "og_to_shrew"[1] 150.101.188.49 #2: STATE_QUICK_R2: IPsec SA established tunnel mode {ESP=>0x06c91a10 <0x9c53c62c xfrm=AES_256-HMAC_MD5 NATOA=none NATD=none DPD=none}

4. Example Using Dynamic DNS



5. 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