Opengear to Fortigate IPSec Guide

Opengear to Fortigate v4.0,build0185,091020 (MR1 Patch 1)

This is a guide on how to create an IPsec VPN tunnel from an Opengear device to a Fortigate firewall.

In this document:

Background on how IPsec works:

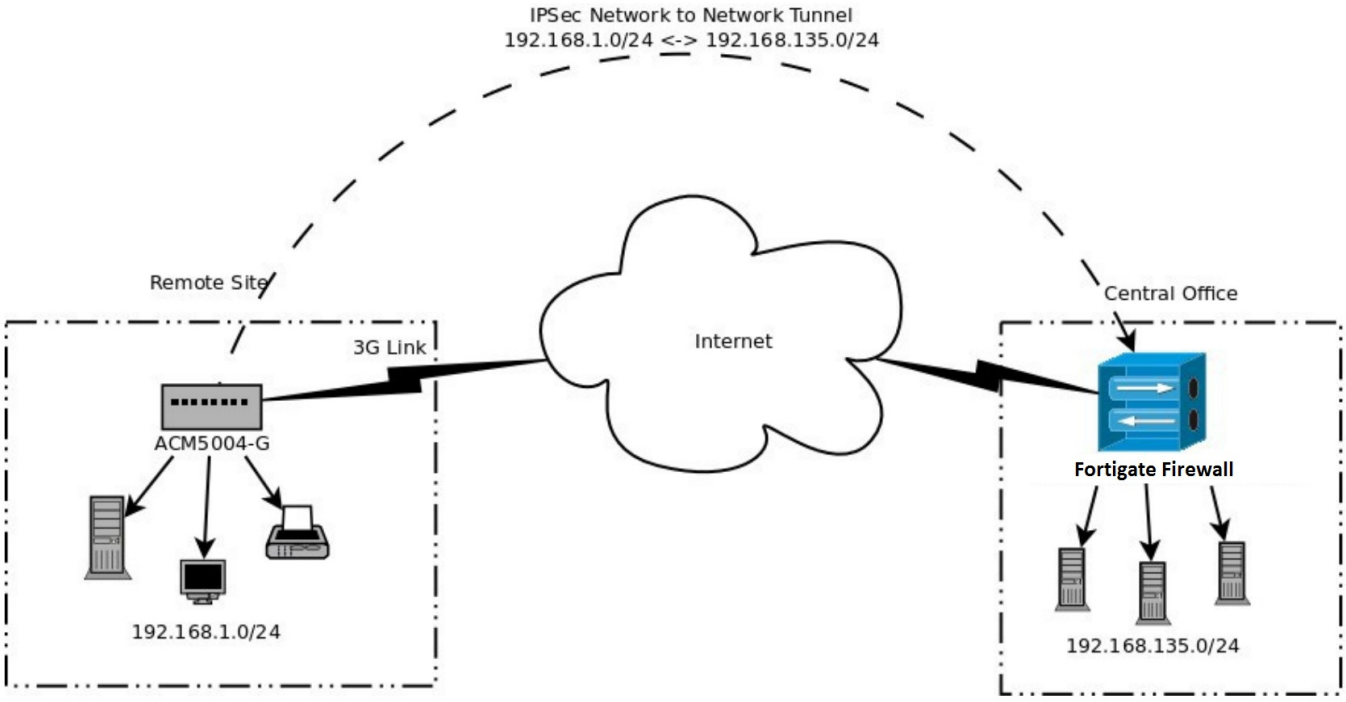
http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6

1. Network Configuration

Some Opengear console servers come equipped with a built-in cellular modem, which can be used as the console server's primary or secondary link to the Internet.

Many low-end cellular plans do not provide publicly accessible IP addresses so the console server is not IP accessible from other sites over the Internet. One way to allow such connectivity is to use a VPN. The Opengear ACM and IM products support IPSec VPNs. Regardless of how the Opengear console server connects to the internet, an IPSec VPN can provide a way to maintain a secure connection to the remote console server and, if it exists, the private network it resides in.

The following diagram illustrates a typical setup for this solution (showing an Opengear ACM5004-G as an example):



The ACM5004-G at the remote site has its Ethernet address set to be on the 192.168.1.0/24 subnet. It can either act as a gateway for that network, or simply be a member of the network. It is configured to initiate the IPSec connection.
Please note that if the ACM is not the gateway, you must add a route to the router responsible for the network to forward traffic for the central office (192.168.135.0/24) via the ACM

2. Fortigate Configuration

2.1 Fortigate Auto Key (IKE) Phase 1

The following configuration excerpts give the required configuration settings for a Fortigate to accept IPSec connections from the Opengear.

Field	Fortigate Auto Key (IKE) Phase 1
Name	fortigate_to_opengear
Remote Gateway	Dialup User
Local Interface	Choose appropriate listening interface
Mode	Aggressive
Authentication Method	Preshared Key
Pre-shared Key	mypresharedkey
Peer Options	Accept this peer ID ogremotesite
Enable Ipsec Interface Mode	Un-checked
P1 Proposal	
Encryption	3DES
Authentication	SHA1
DH Group	2
Keylife	28800
Local ID	Leave Blank
XAUTH	Disable
NAT Traversal	Checked
Keepalive Frequency	300
Dead Peer Detection	Checked

2.2 Fortigate Auto Key (IKE) Phase 2

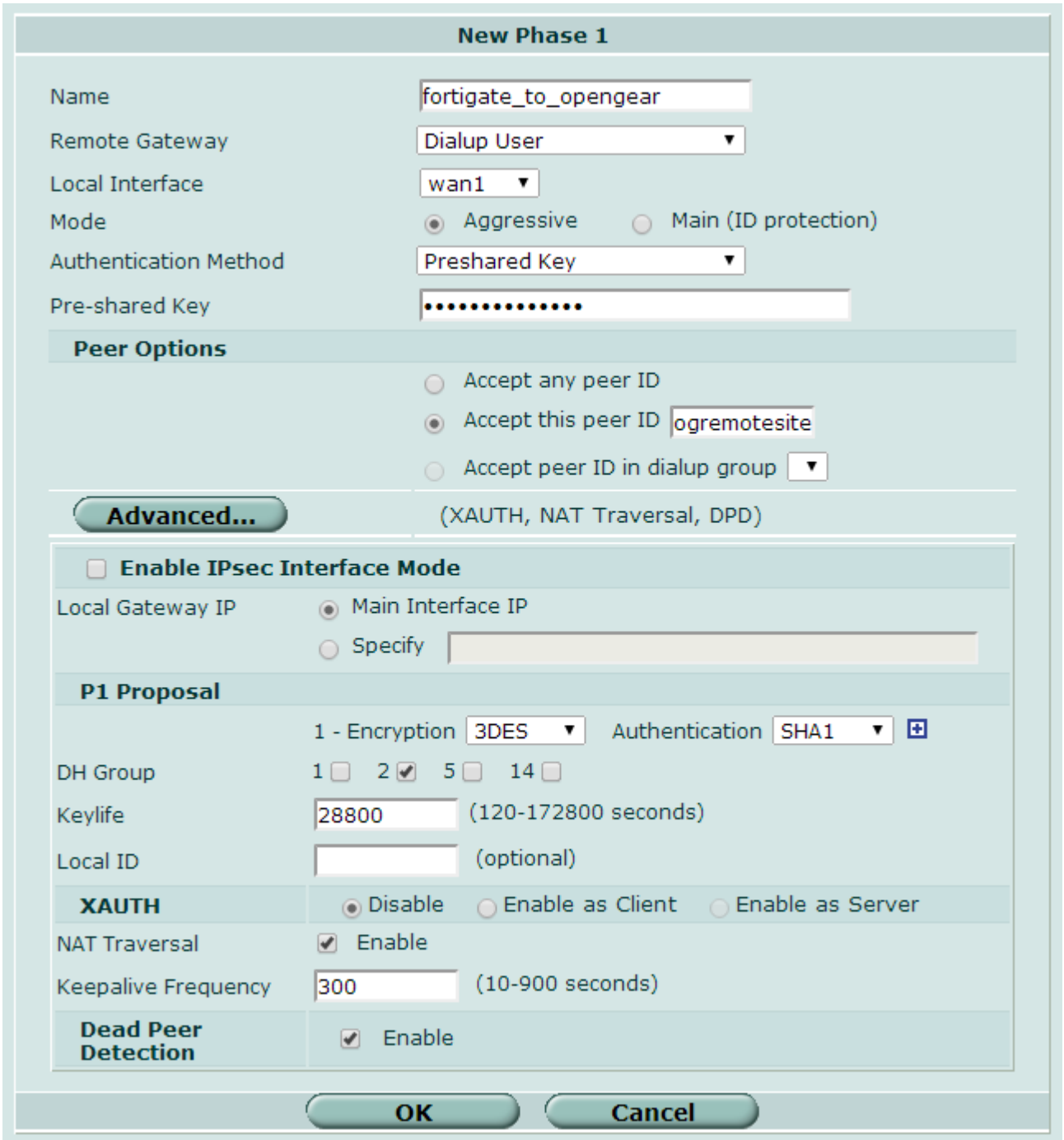
Field	Fortigate Auto Key (IKE) Phase 2
Name	fortigate_to_opengear2
Phase 1	fortigate_to_opengear
P2 Proposal	
Encryption	3DES
Authentication	SHA1
Enable replay detection	yes (checked)
Enable perfect forward secrecy(PFS)	yes (checked)
DH Group	2
Keylife	Seconds 3600
AutoKey Keep Alive	yes (checked)
DHCP-IPsec	no (un-checked)
Quick Mode Selector	
Source Address	192.168.135.0/24
Source port	0
Destination address	192.168.1.0/24
Destination port	0
Protocol	0

NOTE!: *Source address* MUST match the Right Subnet set on the Opengear device. *Destination address* MUST match the Left Subnet set on the Opengear device. The Fortigate uses those addresses to match the phase 2 proposal and if they do not match you will fail to complete phase 2 negotiations.

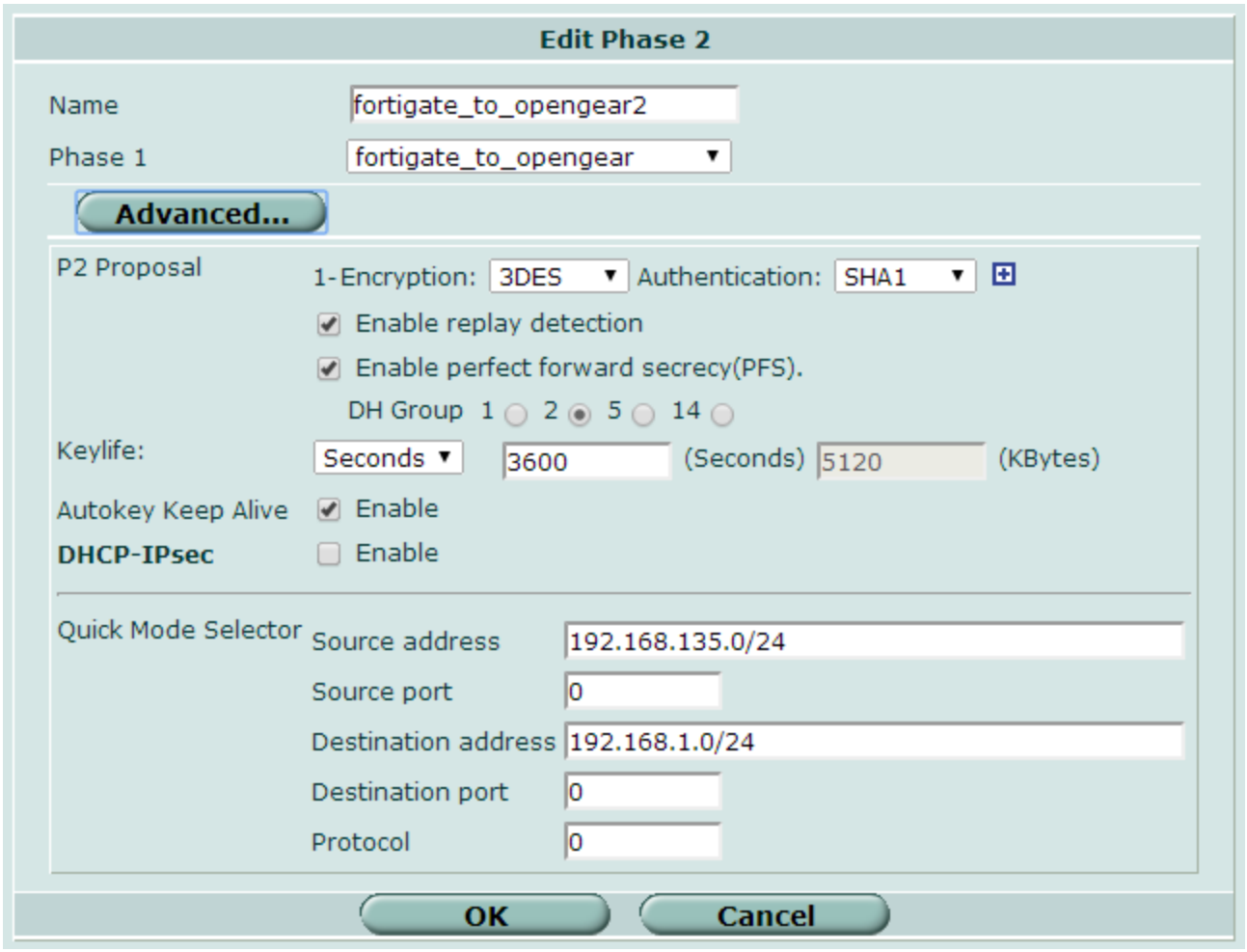
2.3 Fortigate Firewall Policy Configuration

Field	Fortigate Firewall Policy
Source Interface/Zone	Set to the internal interface to be allowed access to the remote Opengear network
Source Address	Set to the internal network to be allowed access to the remote Opengear network
Destination Interface/Zone	Set to the public facing interface
Destination Address	Set to same as the Opengear Left Subnet
Schedule	always or appropriate schedule
Service	ANY
Action	IPSEC
VPN Tunnel	fortigate_to_opengear
Allow Inbound	yes (checked)
Allow outbound	yes (checked)
Inbound NAT	no (un-checked)
Outbound NAT	no (un-checked)
Protection Profile	Unset or set to your needs
Traffic Shaping	Unset or set to your needs
Reverse Direction Traffic Shaping	Unset or set to your needs
Per-IP Traffic Shaping	Unset or set to your needs
Log Allowed Traffic	Unset or set to your needs

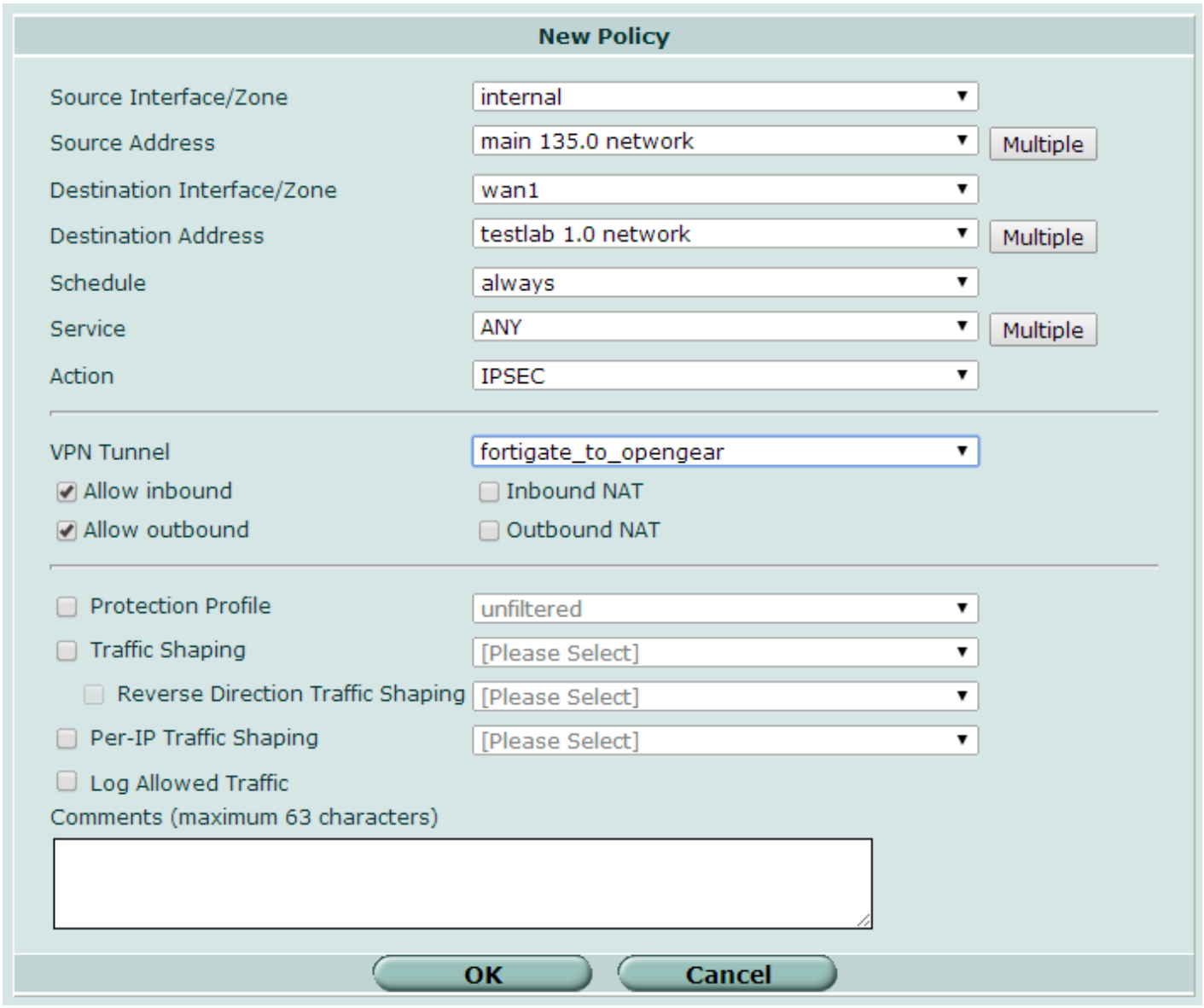
Screenshot of Fortigate Phase 1 settings:



Screenshot of Fortigate Phase 2 settings:



Screenshot of Fortigate Firewall settings:



3. Configuring the Opengear Side

For these examples, the Opengear must be able to route to the Fortigate device. It doesn't matter if the tunnel connection to the Fortigate device is made via the Opengear's network interface or via an always-up cell modem connection. However, on the Opengear, forwarding needs to be setup between the VPN interface and the interface which is on the **Left Subnet** (the Left Subnet from the Opengear's perspective is the Opengear remote site's private network – 192.168.1.0/24 in the examples used so far).

Configuration and Forwarding Examples:

- **Scenario 1**. The Opengear is connecting to the Fortigate device via an always-up cell modem connection. The Network interface of the Opengear is on the left subnet. Forwarding needs to be enabled between the VPN interface and the Network interface.

- **Scenario 2**. The Opengear is connecting to the Fortigate device via the Network interface. The Management LAN interface of the Opengear is on the left subnet. Forwarding needs to be enabled between the VPN interface and the Management LAN interface.

Also note that other devices on the left subnet need to add the tunneling Opengear device as the route to the right subnet located at the Fortigate end of the tunnel. This would already be the case if the Opengear device is the left subnet's default gateway.

To configure the Opengear device:

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. Note that custom options need to be added.

   In this example:

   - The Fortigate is on a private subnet 192.168.135.0/24
   - The Opengear is on a private subnet 192.168.1.0/24 and has an address of 192.168.1.20 on that subnet.

Field	Opengear Device
Tunnel Name	opengear_to_fortigate
Initiate Tunnel	yes (checked)
Authentication Method	Shared Secret (PSK)
Shared Secret (PSK)	*Enter your pre-shared-secret - this should be the same as what you set in the Fortigate Phase 1 Pre-shared Key.*
Authentication Protocol	ESP
Aggressive Mode	yes (checked)
IKE Proposal (Phase 1)	3des-sha-modp 1024
Perfect Forward Secrecy	yes (checked)
Left ID	@ogremotesite
Right ID	*leave blank*
Left Address	*leave blank*
Right Address	WAN address of the Fortinet
Left Subnet	192.168.1.0/24
Right Subnet	192.168.135.0/24
Custom Options	
leftsourceip	192.168.1.20 *(Adjust this to the address the Opengear device has on the left subnet)*
ikelifetime	8h
salifetime	1h
forceencaps	yes
dpddelay	60
dpdtimeout	120
dpdaction	restart

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

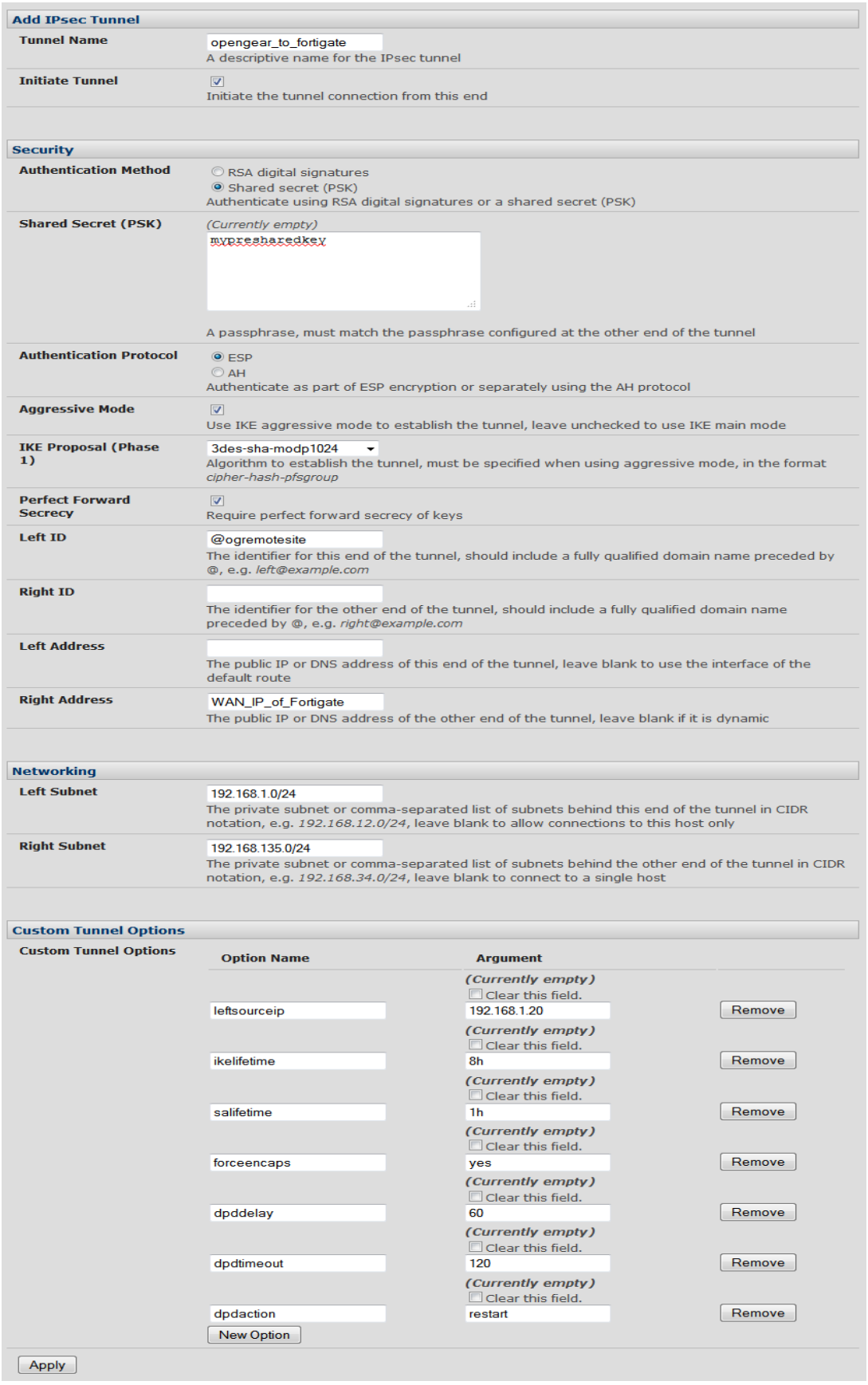
Replace *Right Subnet* with the private network address of the Fortinet device.

Make sure you click “Apply” once you have entered all the required details.

Custom options are used to aid debugging and inter-operability with the Fortinet device.

- The *leftsourceip=x.x.x.x* option sets the source IP for traffic originating on the Opengear which will traverse the tunnel. This allows tunnel testing using the *ping* comand locally on the Opengear.
- The *ikelifetime=8h* option sets the lifetime for the Phase 1 Security Associations (ISAKMP SA) to 8 hours. This corresponds to the *lifetime 28800* entries on the Fortigate configurations.
- The *salifetime=1h* option sets the lifetime for Phase 2 Security Associations (IPSec SA) to 1 hour.
- The *forceencaps=yes* option instructs the IPSec implementation on the Opengear to UDP encapsulate the IPSec traffic. This helps with firewall traversal issues.
- The *dpddelay=60* option is part of the Dead Peer Detection (DPD) functionality. It sets the delay (in seconds) between DPD keepalives that are sent to the remote end.
- The *dpdtimeout=120* option is also part of the DPD functionality. It sets the length of time (in seconds) the connection can be idle without hearing either a keepalive poll from the remote end or an acknowledgement from the remote end to a keepalive sent from this end. After this period has elapsed with no response and no traffic the peer is declared dead.
- The *dpdaction=restart* option determines the action to be performed when the DPD enabled peer is declared dead, the restart option means the the SA will immediately be renegotiated.

Screenshot of Opengear settings:



4. Checking if the Tunnel is Up

“IPsec SA established tunnel mode” should be visible in the Syslog on the Opengear:

```
<84>Jun  5 20:50:15 pluto[9997]: "opengear_to_fortigate/1x1" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP/NAT=>0x36f27b4f <0x2bc2cd9c xfrm=3DES_0-HMAC_SHA1 NATOA=none NATD=x.x.x.x:4500 DPD=enabled}
```

NOTE: x.x.x.x will be the WAN address of the Fortigate device.

5. Debugging

Debugging on Fortigate

To enable debug logging on the console do

FG200A # diagnose debug console

To enable debugging output

FG200A # diagnose debug enable

Phase1 debugging isn’t too useful. IKE/Phase2 debugging is where the problem almost always is. Turn on full debugging logs there.

FG200A # diagnose debug application ike -1

Debugging on Opengear

- ipsec setup --restart / --stop
  - Stops or restarts the vpn connections
- ipsec auto --status
  - Shows you the current status of the tunnel, and shows what openswan thinks the routed networks are