

# Site to Site VPN in R80.x

Author: Danny Drake

## Table of Contents

SITE TO SITE VPN IN R80.X.....	1
INTRODUCTION.....	2
SITE TO SITE VPN SETTINGS.....	3
VPN WITH A THIRD PARTY .....	13
COMMON SKS FOR TROUBLESHOOTING S2S VPNS .....	16

## Introduction

This document is a tutorial for beginners. It provides step by step instructions and examples of setting up Site to Site VPN with Check Point R80.x products. It also includes an example of setting up a S2S VPN with a third-party Gateway (Fortinet).

Some experience with R80.x SmartConsole is assumed, as well as basic understanding of IPSec and principles of Site to Site VPNs.

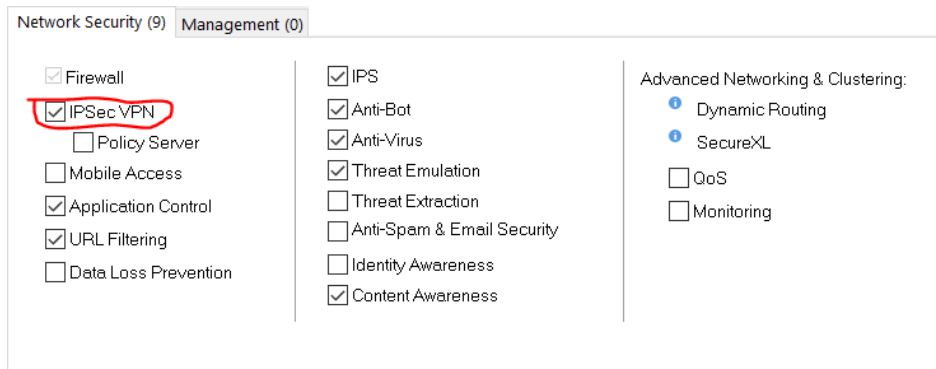
## Site to Site VPN Settings



1. First thing you want to do is create the network/host objects you'll need to use on both ends of the VPN tunnel. i.e.

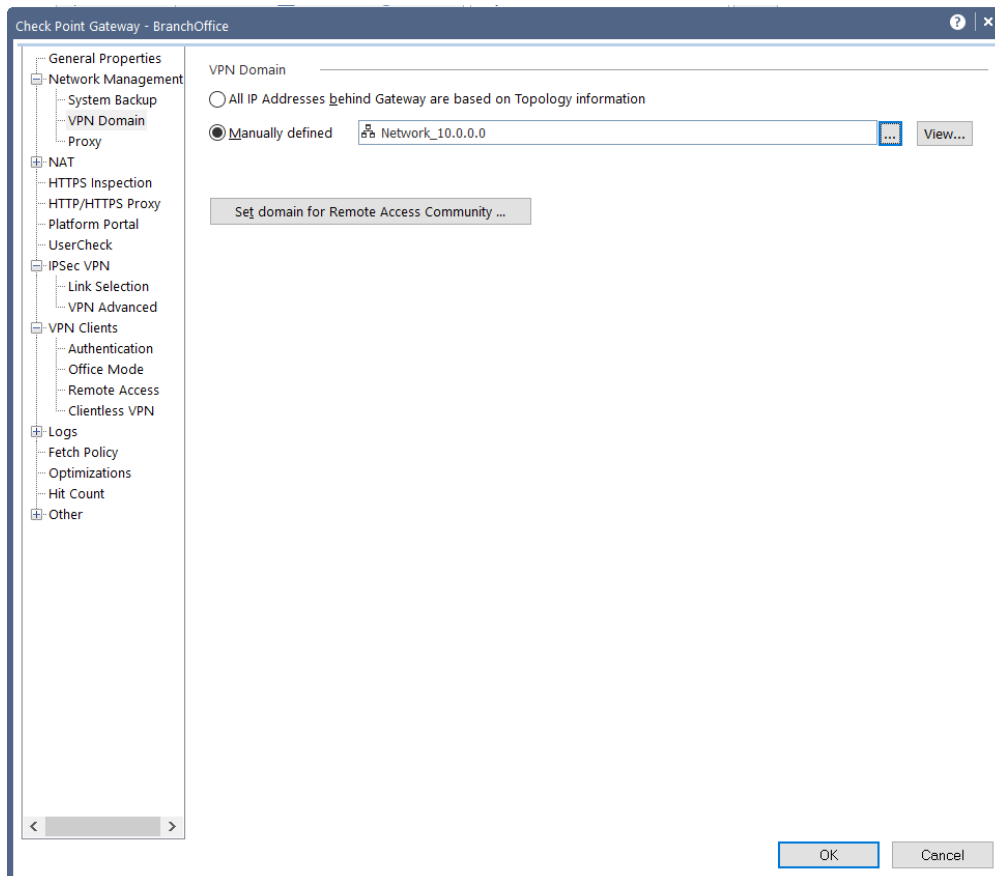
The screenshot shows the 'Network' configuration window for an object named 'Network\_10.0.0.0'. The window has a search icon, a help icon, and a close icon in the top right corner. Below the title bar, there is a tree view icon and the object name 'Network\_10.0.0.0' with a sub-label 'Enter Object Comment'. The main area is divided into a left sidebar and a right main panel. The sidebar has 'General' selected and 'NAT' below it. The main panel is titled 'IPv4' and contains the following fields: 'Network address' with the value '10.0.0.0', 'Net mask' with the value '255.255.255.0', and 'Broadcast address' with two radio buttons: 'Included' (selected) and 'Not included'. Below this is the 'IPv6' section with 'Network address' and 'Prefix' fields, both currently empty. At the bottom of the main panel is an 'Add Tag' button. At the bottom of the window are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Host' configuration window for an object named 'my pc'. The window has a search icon, a help icon, and a close icon in the top right corner. Below the title bar, there is a tree view icon and the object name 'my pc' with a sub-label 'Enter Object Comment'. The main area is divided into a left sidebar and a right main panel. The sidebar has 'General' selected, with 'Network Management', 'NAT', 'Advanced', and 'Servers' listed below. The main panel is titled 'Machine' and contains the following fields: 'IPv4 address' with the value '172.22.100' and a 'Resolve from name' button, and 'IPv6 address' with an empty field. At the bottom of the main panel is an 'Add Tag' button. At the bottom of the window are 'OK' and 'Cancel' buttons.

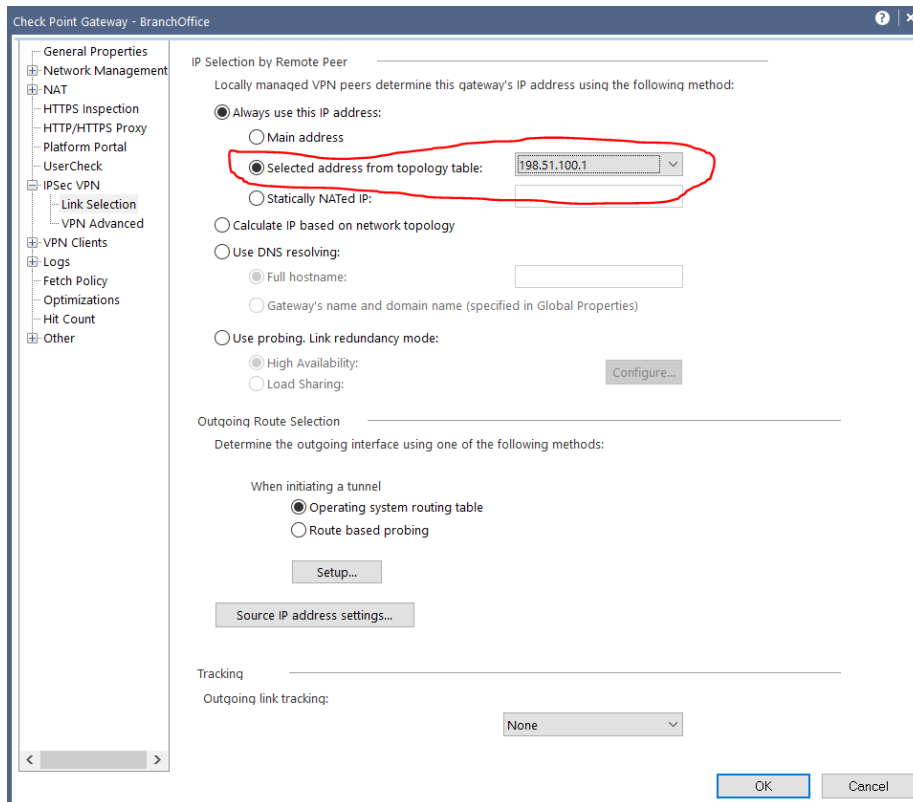
2. Then open the gateway object you are installing the VPN tunnel on and enable the IPSec VPN blade.



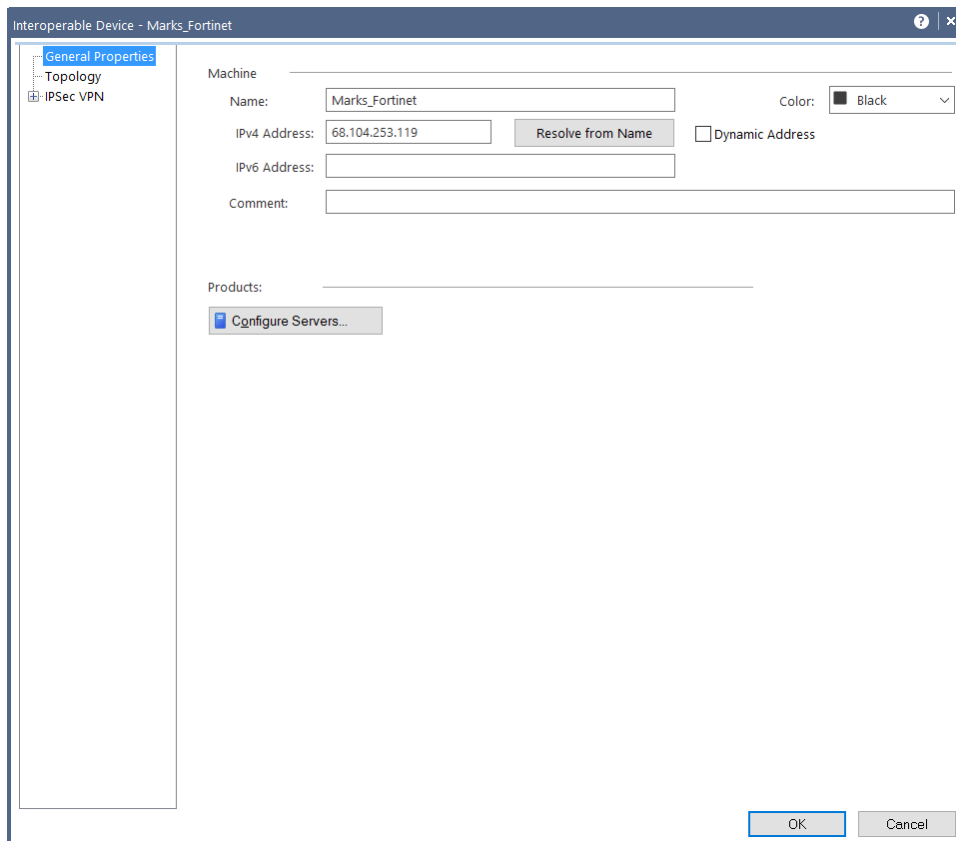
3. Select the   to open the Network Management options. Select VPN domain. Unless you want all interfaces to be part of the tunnel you need to manually define the VPN domain. Click the manually define radial and select the internal network you are coming from (created in step 1).

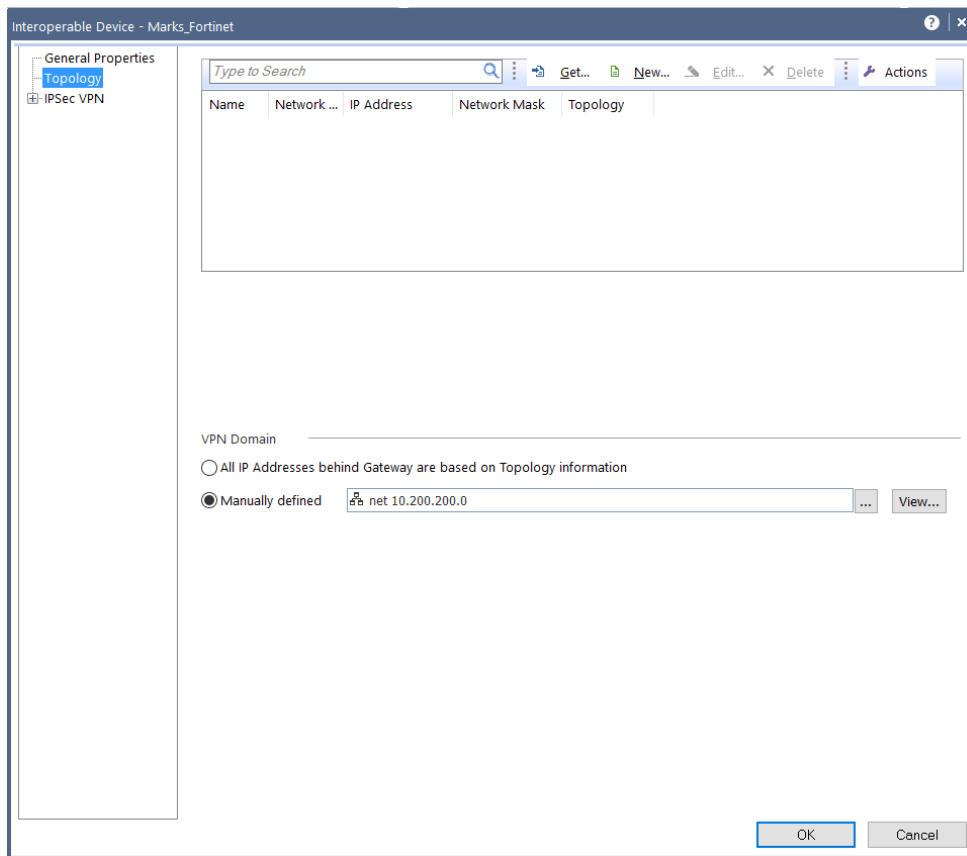


4. If your GWs external IP is different from the IP on the interface you are using for your tunnel you will need to select the link manually. Open the drop down under IPSec VPN and select Link Selection. Then select the Selected address from topology table radial and select the interface you want to use.

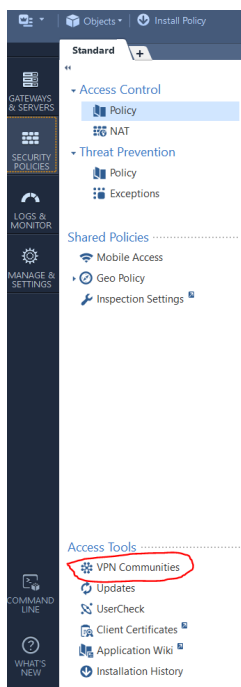


- For 3<sup>rd</sup> party GWs you will need to create it as an interoperable device, and select the link selection within the topology tab. Then click the manually defined radial and select the inside network on the other end of the tunnel.



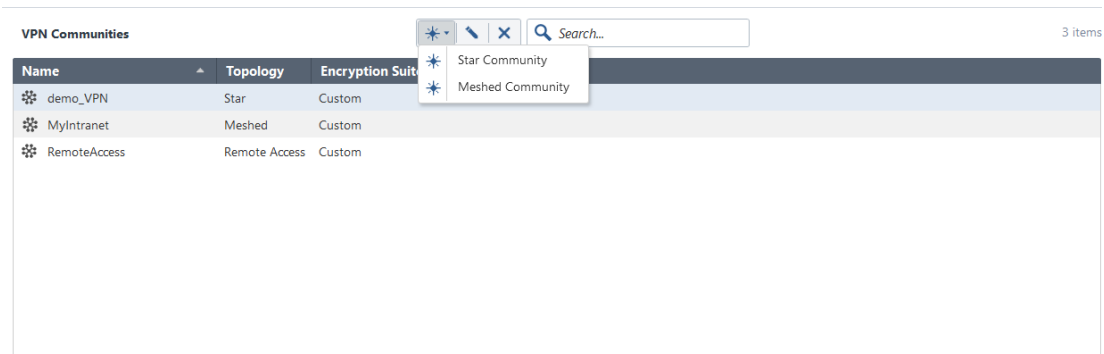


- Next you will need to create the VPN community. Click on the security policies tab on the left pane. The select VPN Community at the bottom left.

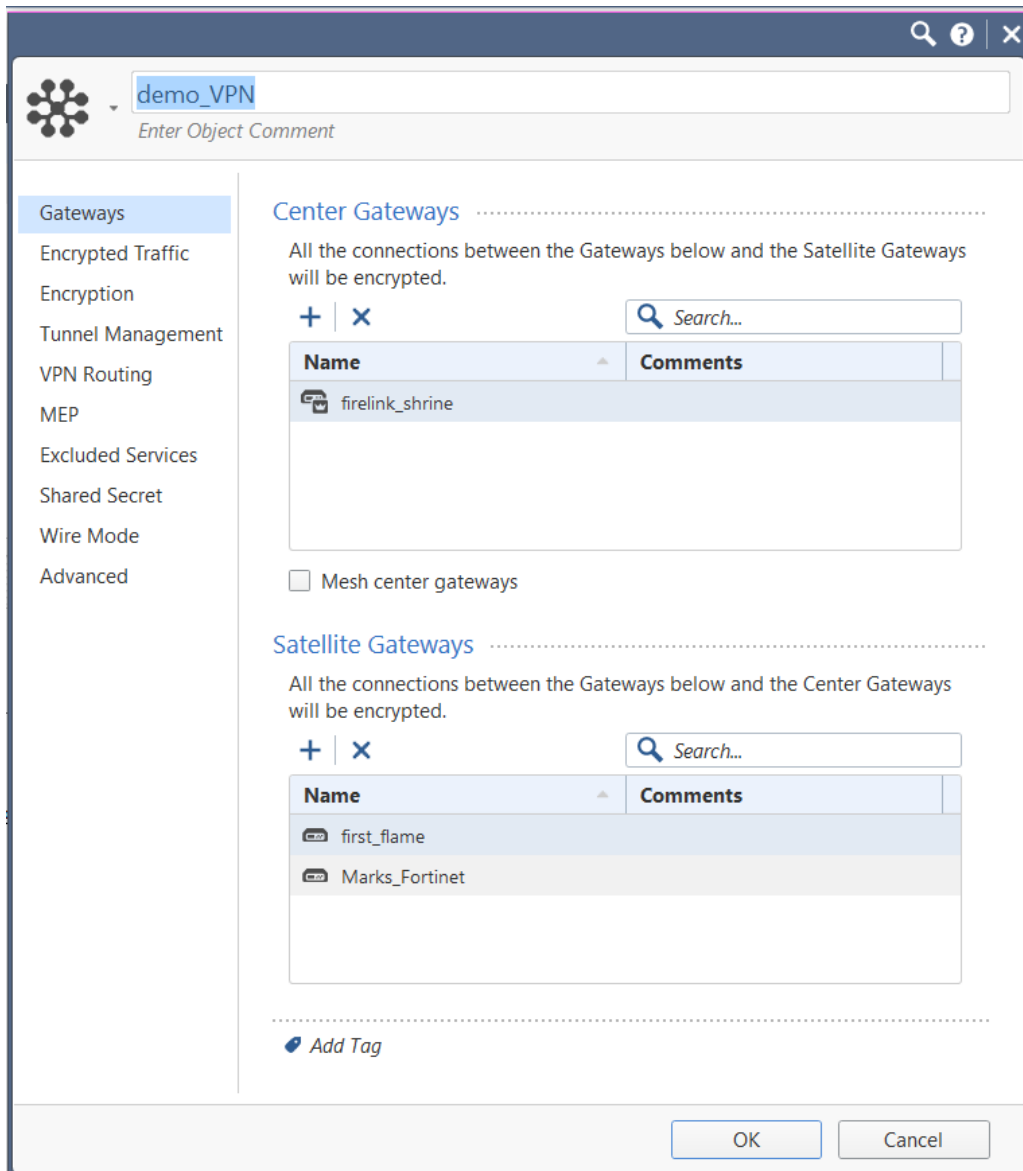


- There are two types of communities you could create; a Mesh community, consisting of multiple gateways all being able to connect VPN to each other; or a

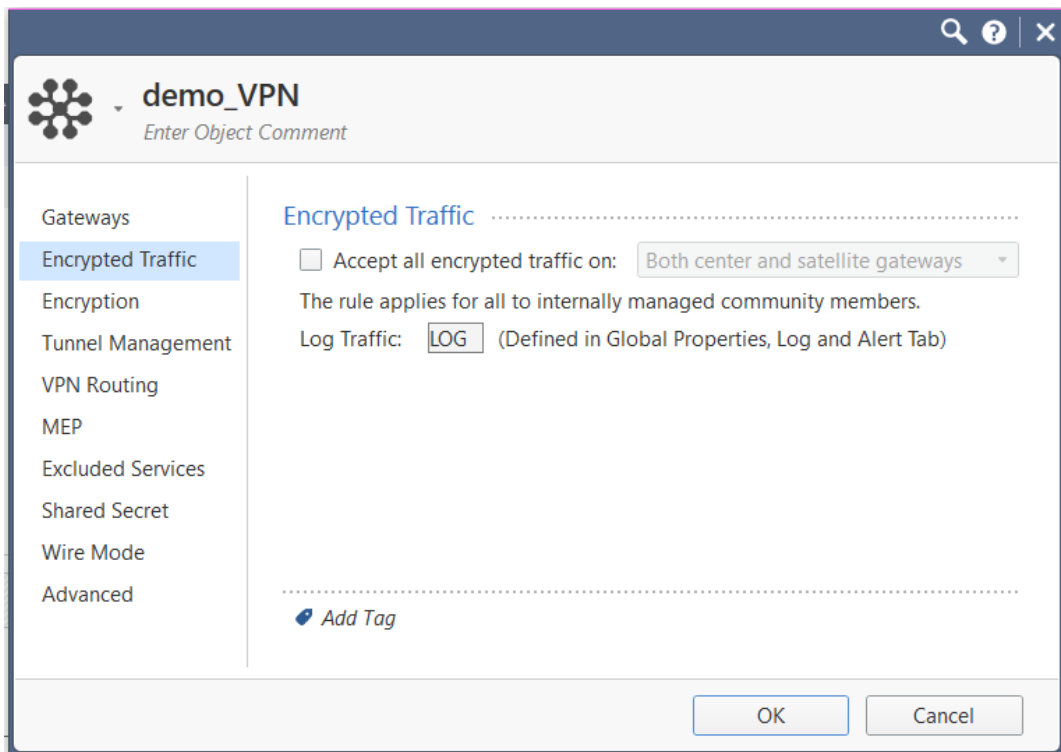
Star community, which is one central GW with remote GWs VPN back to it. Select new, and your choice of community.



8. Give it a name and select your participating GWs

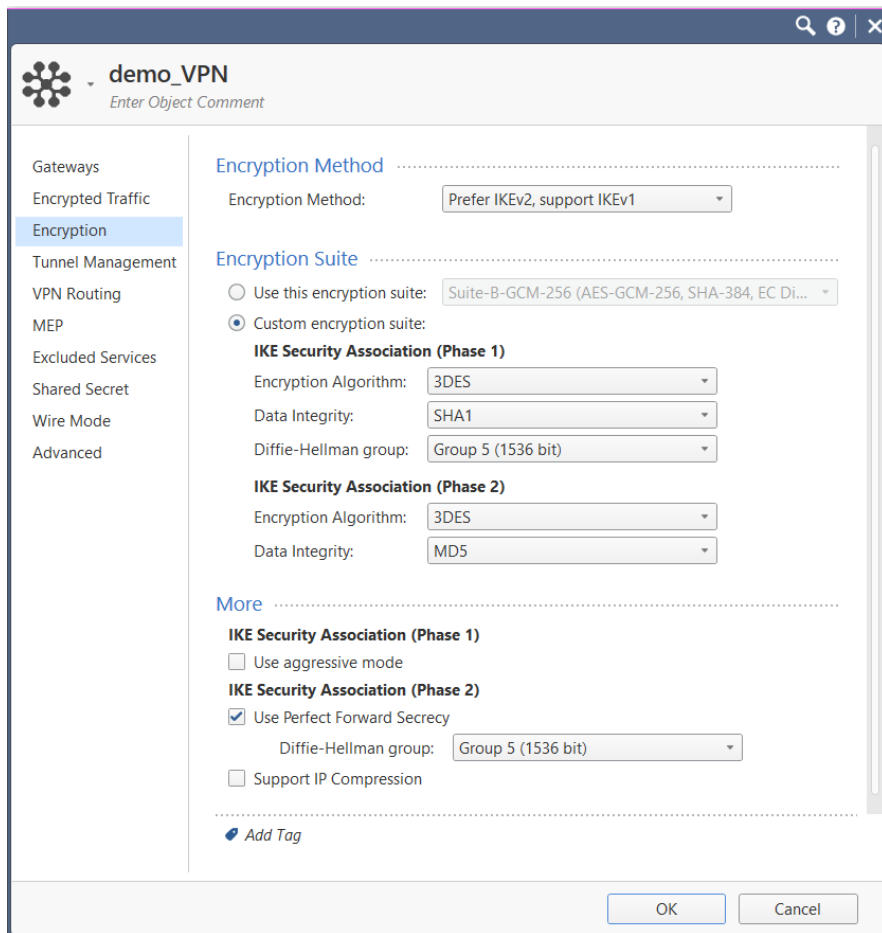


9. You can choose to accept all internal traffic if the participating GWs without the need for an access rule.

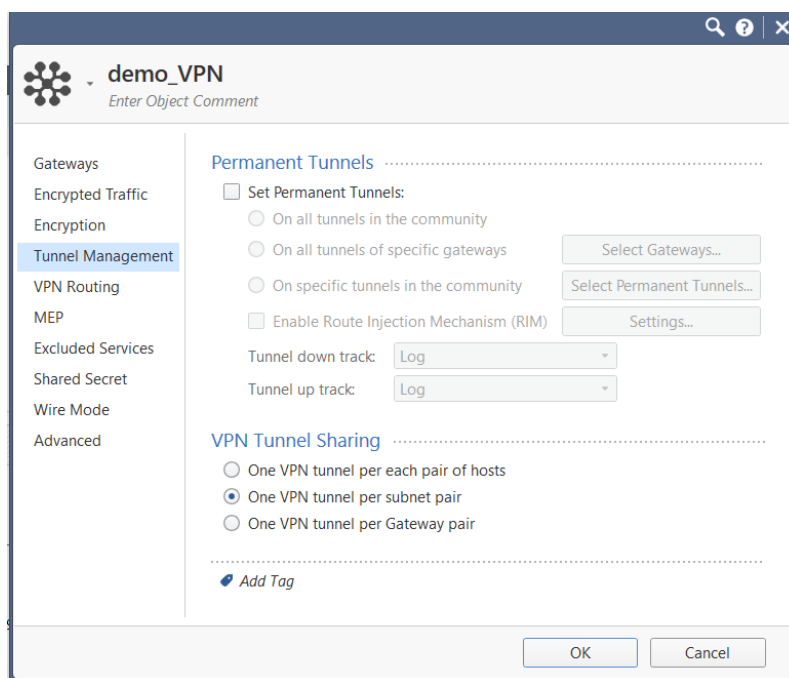


10. Next, choose the encryption method. This is where most of your troubleshooting with 3<sup>rd</sup> party GWs will take place. The Encryption methods must be identical on both ends. Use Aggressive mode if you are connecting to a 3<sup>rd</sup> party that does not support Main mode. Use Perfect Forward Secrecy for extreme security needs as it will affect performance.

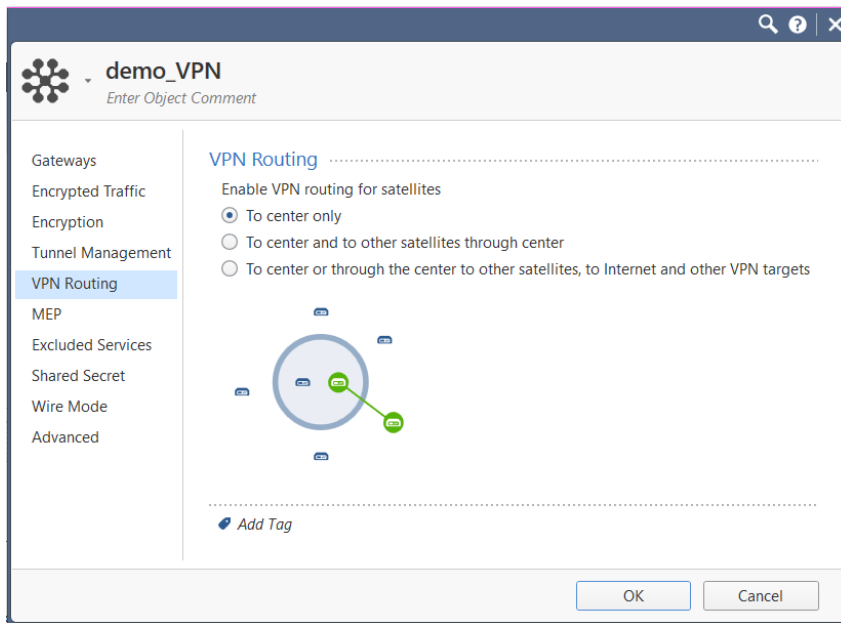




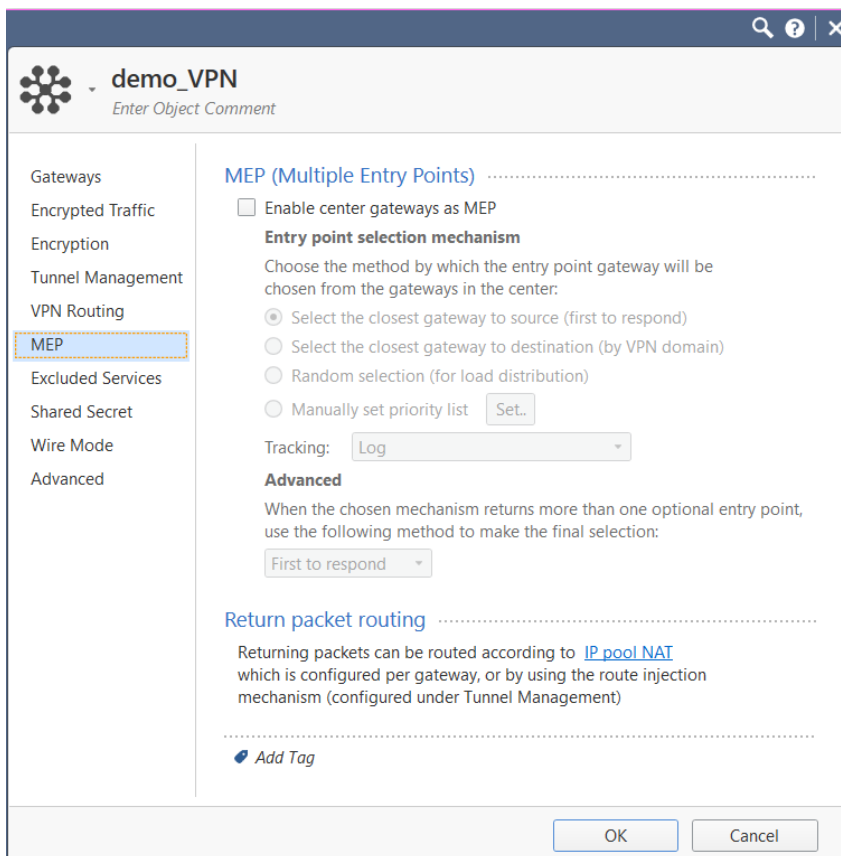
11. You can choose to create permanent tunnels if you wish.



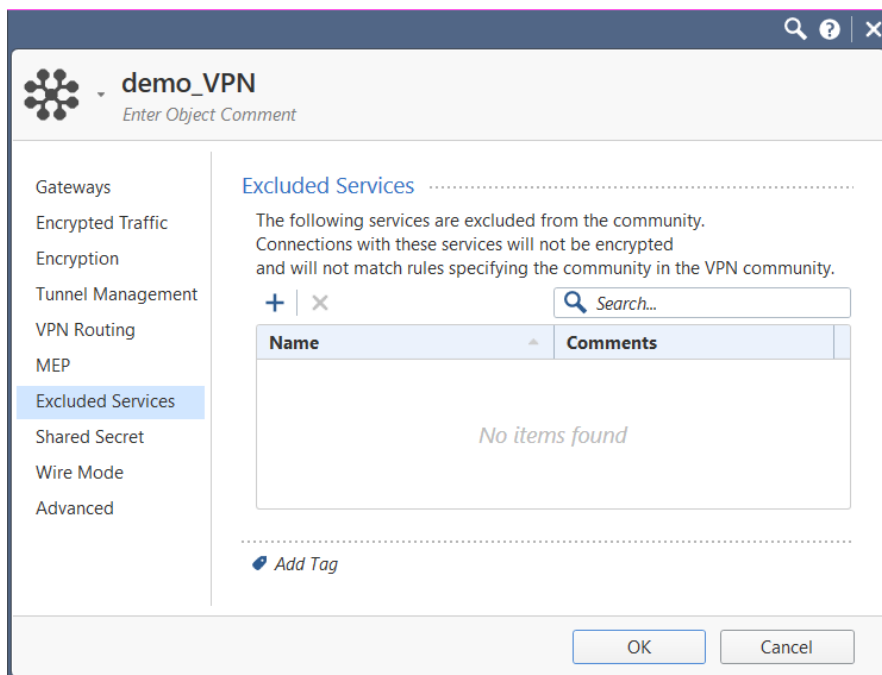
12. Decide how the tunnel routes. Whether the satellites can go through the center or just to it only.



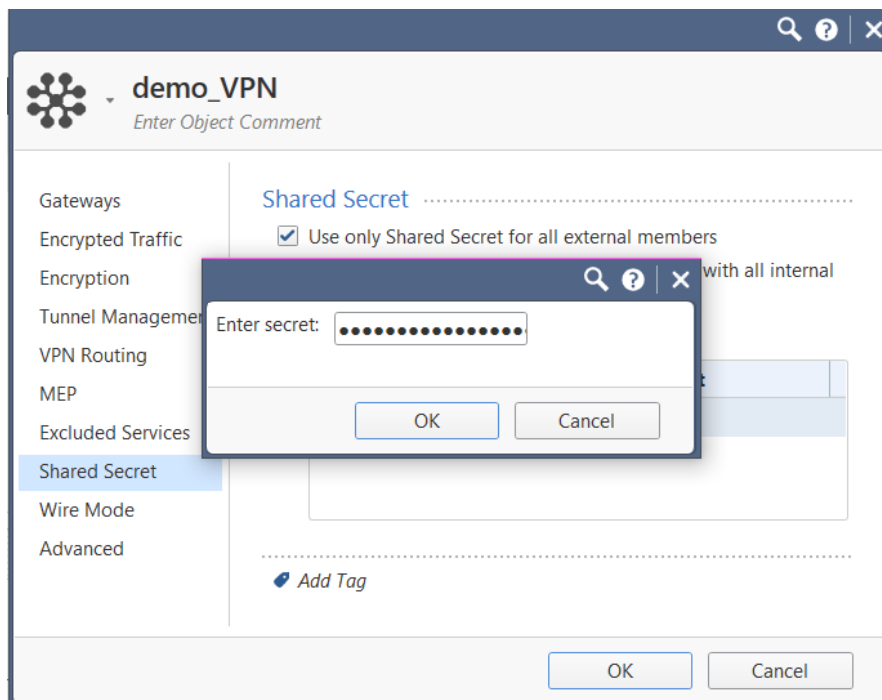
13. MEP (Multiple Entry Points) is used for load balancing if you are expecting heavy load on your tunnel.



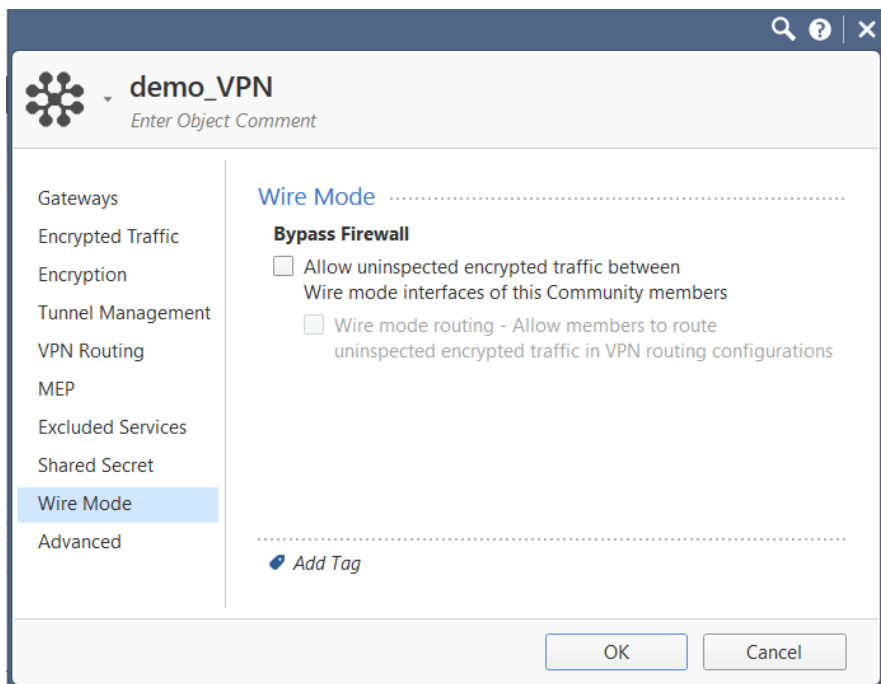
14. You can choose certain traffic that will not be encrypted over the tunnel to increase performance.



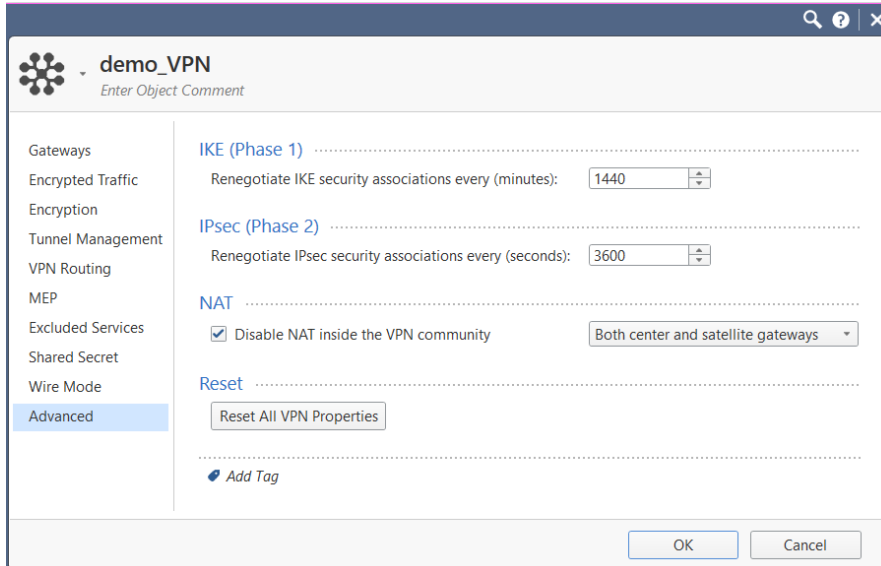
15. When connecting to a 3<sup>rd</sup> party you will need a Shared Secret. This password must be identical on both ends of the tunnel.



16. Wired mode simulates the GWs being connected together via wired connection, bypassing the GW completely.



17. In the advanced settings you can configure when IKE phase 1 and 2 are auto-renegotiated. You will also want to disable NAT here. NAT can cause issues accessing internal assets if you are connecting by IP.



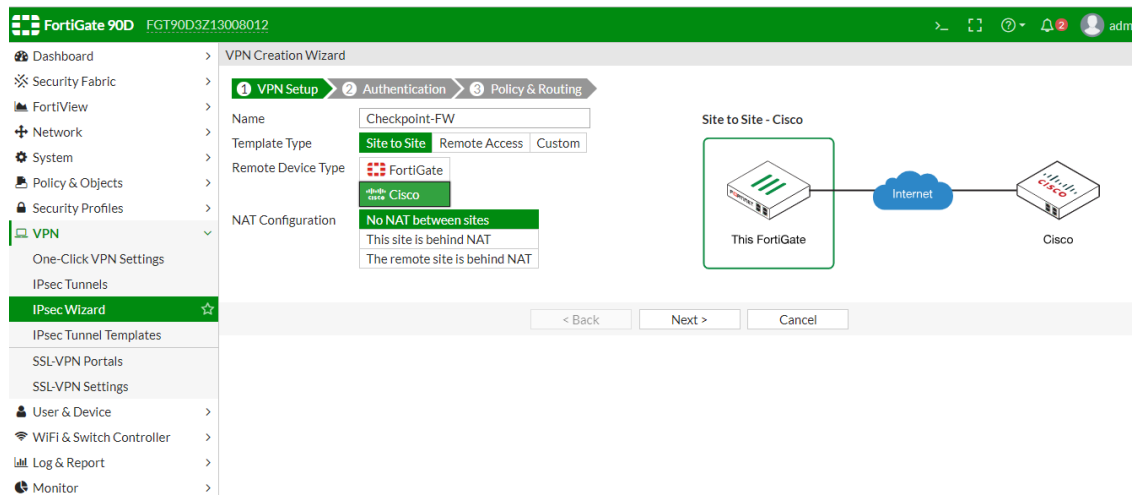
18. Next, you will create an Access Rule to allow the VPN traffic. You will add the network/host objects in the destination and source. Choose the VPN community you created, then allow and log the traffic.

VPN (4)						
4	vpn	<ul style="list-style-type: none"> <li>10.2.2.0</li> <li>my pc</li> <li>net 10.200.200.0</li> <li>192</li> </ul>	<ul style="list-style-type: none"> <li>10.2.2.0</li> <li>my pc</li> <li>net 10.200.200.0</li> <li>192</li> </ul>	demo_VPN	* Any	Accept

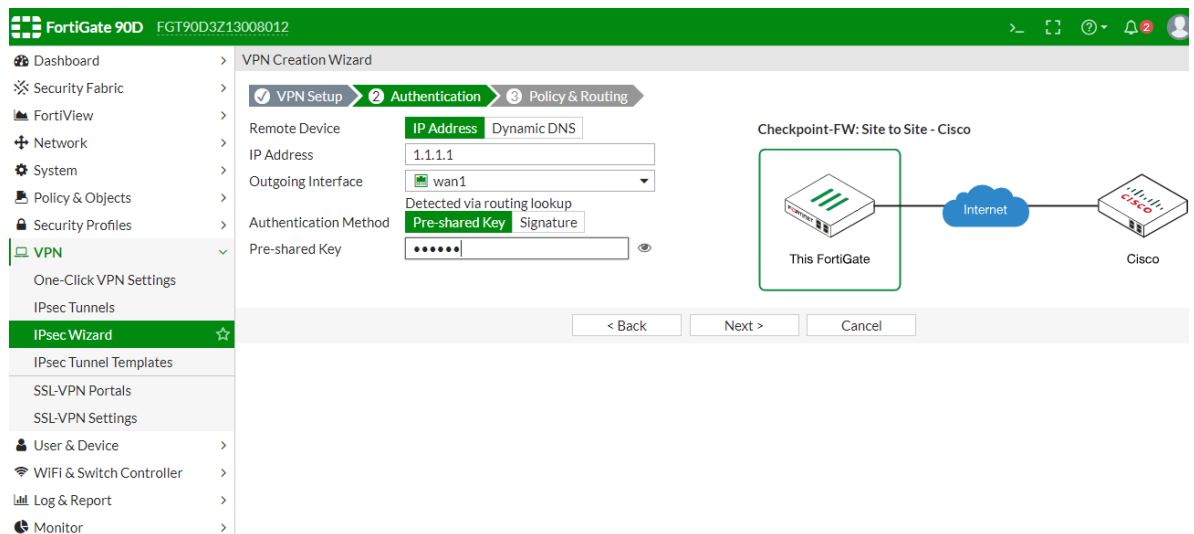
19. Publish and install policy on participating GWs

## VPN with a Third Party

1. An example of configuring on a Fortinet for the 3<sup>rd</sup> party. The IPsec wizard. Name, select type of VPN, and NAT configuration.



2. Configure IP, interface, and authentication methods.



3. Configure the source and destination subnets. Click **create**.

FortiGate 90D FGT90D3Z13008012

VPN Creation Wizard

VPN Setup Authentication Policy & Routing

Local Interface: internal

Local Subnets: 10.200.200.0/24

Remote Subnets: 172.2.2.0/24

Internet Access: None | Share WAN | Force to use remote WAN

Checkpoint-FW: Site to Site - Cisco

This FortiGate Internet Cisco

< Back Create Cancel

FortiGate 90D FGT90D3Z13008012

+ Create New Edit Delete Print Instructions

Tunnel	Interface Binding	Template	Status	Priority
Checkpoint	wan1	Site to Site - Cisco	Up	4

#### 4. Preconfigured templates

FortiGate 90D FGT90D3Z13008012

View

Template	Description
Dialup - FortiClient (Windows, Mac OS, Android)	On-demand tunnel for users using the FortiClient software.
Site to Site - FortiGate	Static tunnel between this FortiGate and a remote FortiGate.
Dialup - FortiGate	On-demand tunnel between two FortiGate devices.
Dialup - iOS (Native)	On-demand tunnel for iPhone/iPad users using the native iOS IPsec client.
Dialup - Android (Native L2TP/IPsec)	On-demand tunnel for Android users using the native L2TP/IPsec client.
Dialup - Windows (Native L2TP/IPsec)	On-demand tunnel for Windows users using the native L2TP/IPsec client.
Dialup - Cisco IPsec Client	On-demand tunnel for users using the Cisco IPsec client.
Site to Site - Cisco	Static tunnel between this FortiGate and a remote Cisco firewall.
Dialup - Cisco Firewall	On-demand tunnel between a FortiGate device and a Cisco Firewall.

#### 5. Configure the encryption method here.

**FortiGate 90D** FGT90D3Z13008012

- Dashboard > VPN Template Details
- Security Fabric >
- FortiView >
- Network >
- System >
- Policy & Objects >
- Security Profiles >
- VPN >
  - One-Click VPN Settings
  - IPsec Tunnels
  - IPsec Wizard
  - IPsec Tunnel Templates** ☆
  - SSL-VPN Portals
  - SSL-VPN Settings
- User & Device >
- WiFi & Switch Controller >
- Log & Report >
- Monitor >

Site to Site - Cisco

**Phase 1 Interface**

- Proposal: 3des-sha1 3des-md5
- Dead Peer Detection: on-demand
- DH Group: 5

**Remote Gateway Address**

- Allow this object in routing table: enable

**Local Address Group**

- Allow this object in routing table: enable

**Remote Address Group**

- Allow this object in routing table: enable

**Phase 2 Interface**

- DH Group: 5
- Perfect Forward Secrecy (PFS): enable
- Source Address Type: name
- Destination Address Type: name
- Proposal: 3des-md5

**Static Route**

## Common SKs for troubleshooting S2S VPNs

[sk34467](#) - Debugging Site-to-Site VPN

[sk60318](#) - How to Troubleshoot VPN Issues in Site to Site

[sk108600](#) - VPN Site-to-Site with 3rd party