Site to Site VPN in R80.x

Author: Danny Drake

Table of Contents

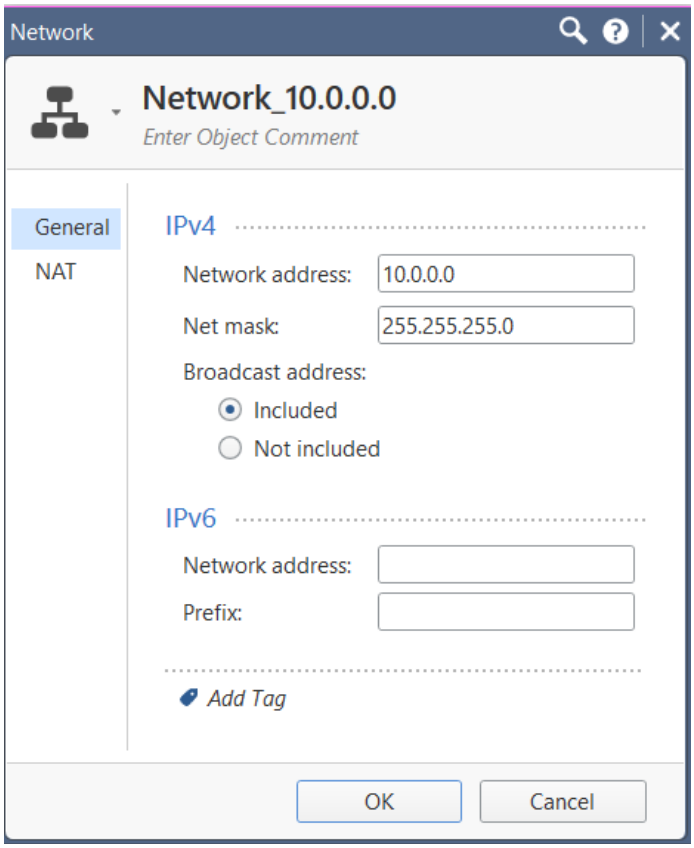
Introduction

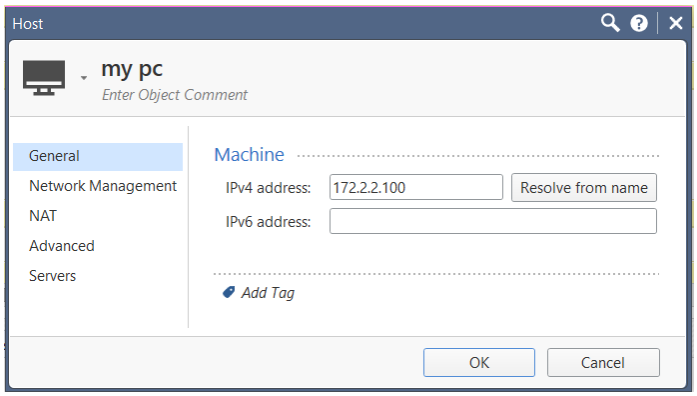
This document is a tutorial for beginners. It provides step by step instructions and examples of setting up Site to Site VPN with Check Point R80.x products. It also includes an example of setting up a S2S VPN with a third-party Gateway (Fortinet).

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

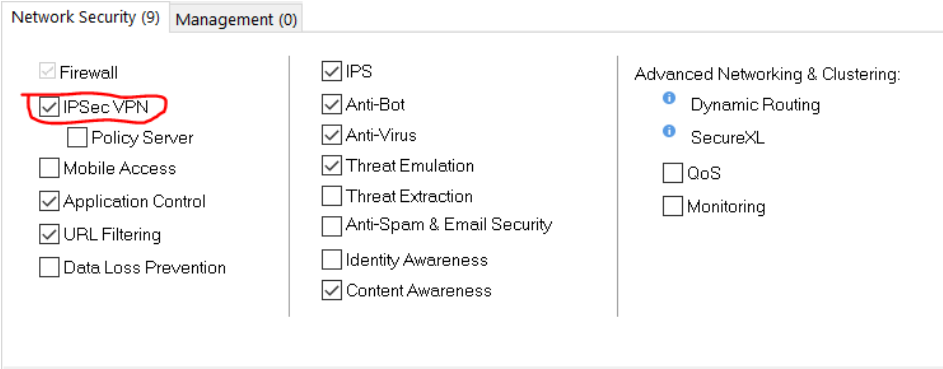
Site to Site VPN Settings

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.

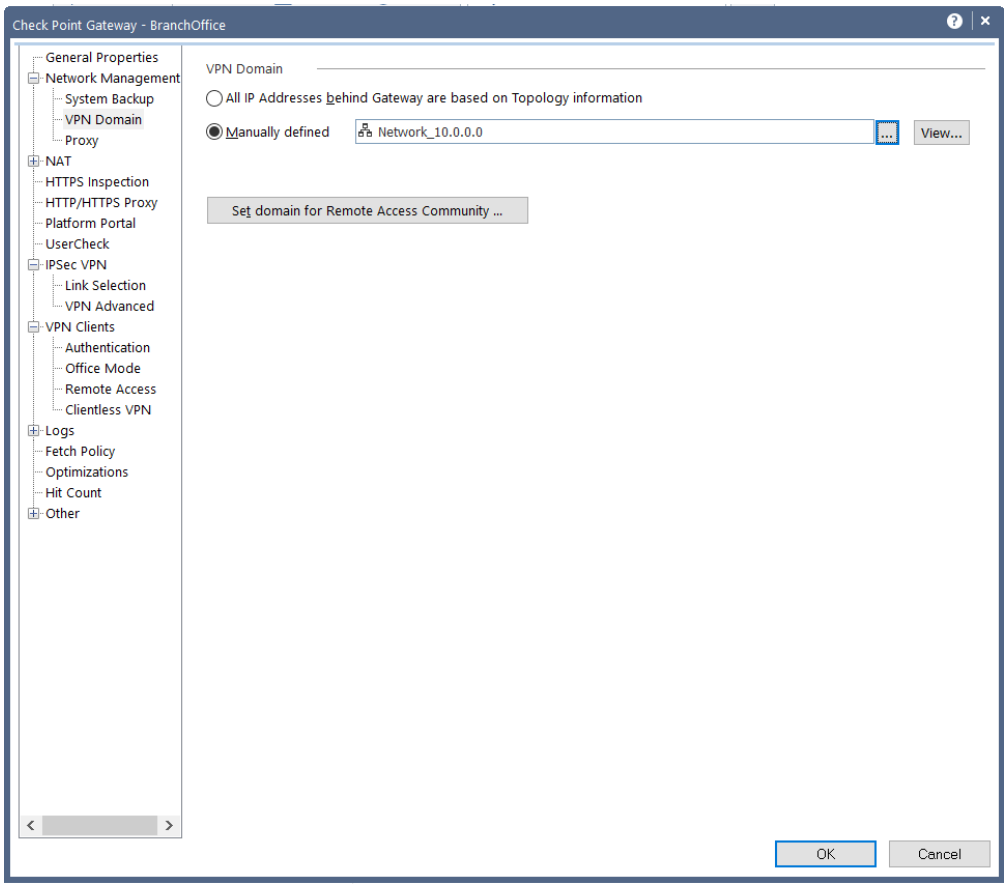




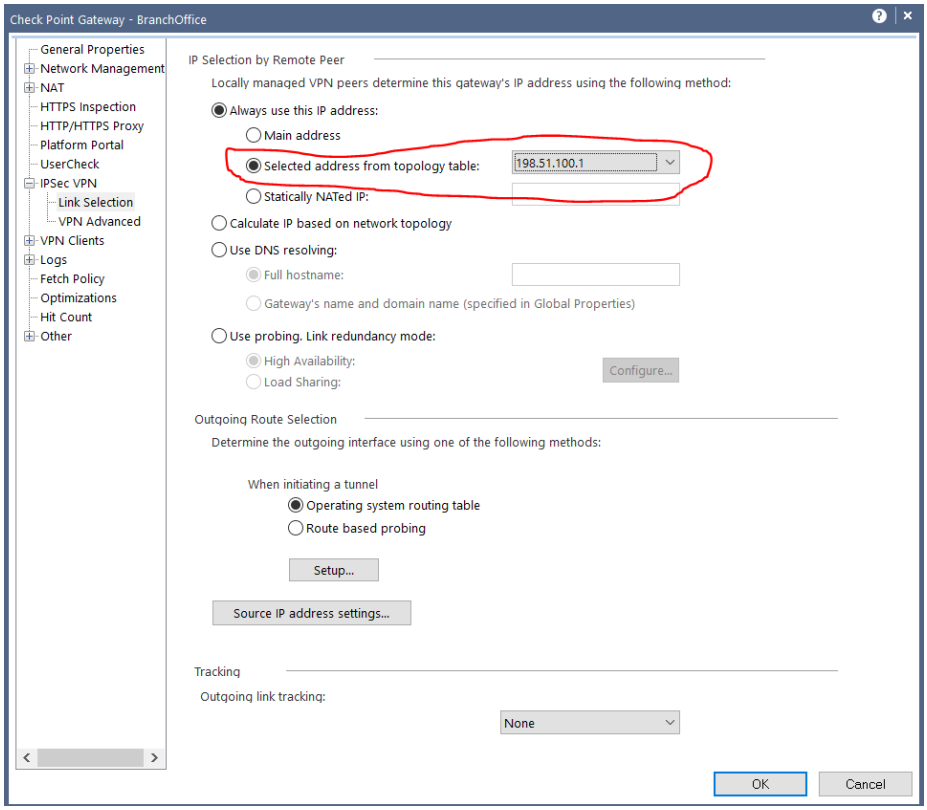
2. Then open the gateway object you are installing the VPN tunnel on and enable the IPSec VPN blade.



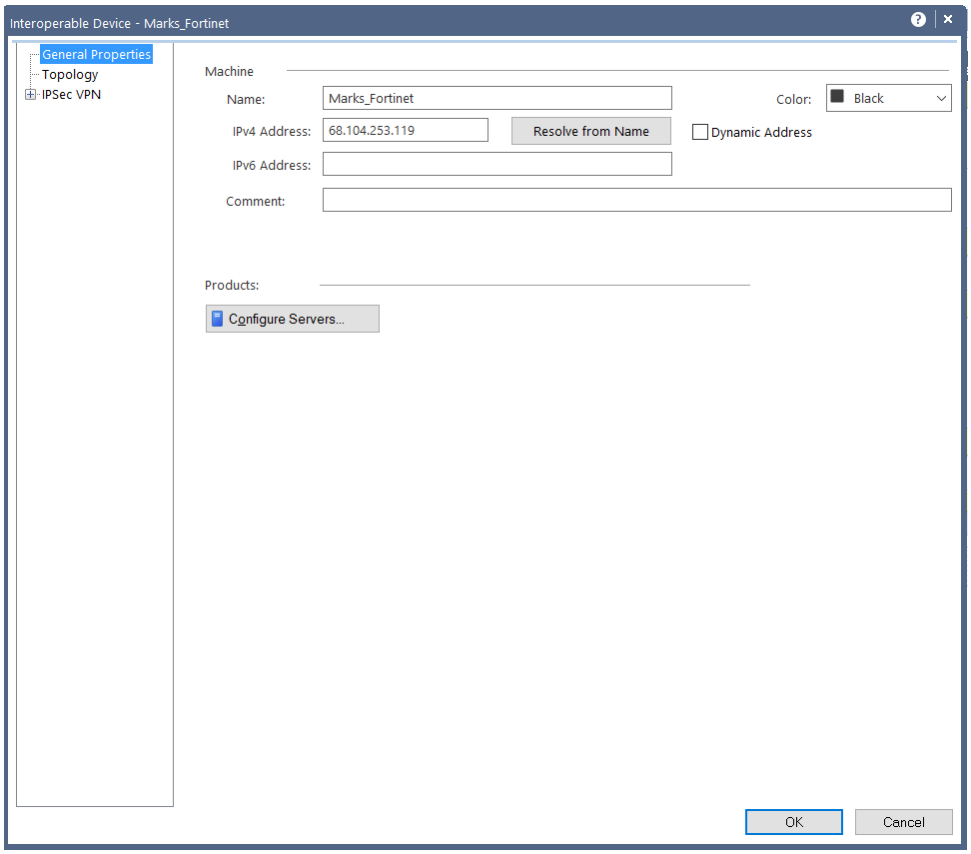
3. Select the to open the Network Management options. Select VPN domain. Unless you want all interfaces to be part of the tunnel you need to manually define the VPN domain. Click the manually define radial and select the internal network you are coming from (created in step 1).

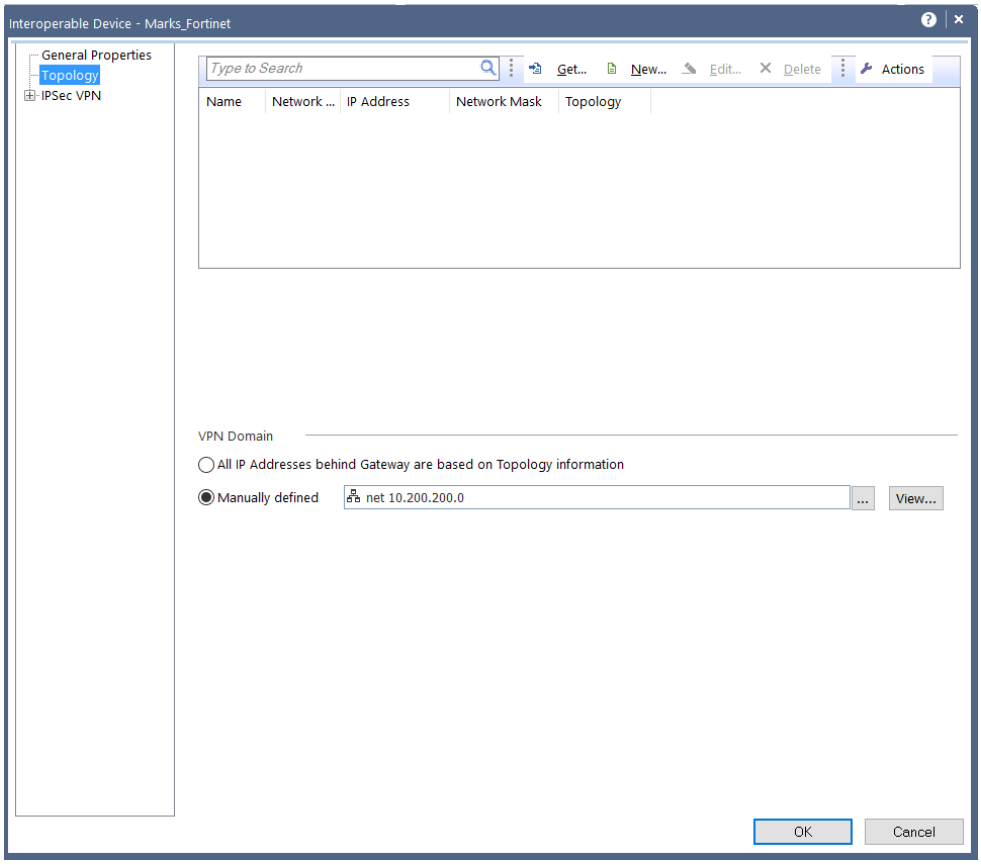


4. If your GWs external IP is different from the IP on the interface you are using for your tunnel you will need to select the link manually. Open the drop down under IPSec VPN and select Link Selection. Then select the Selected address from topology table radial and select the interface you want to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

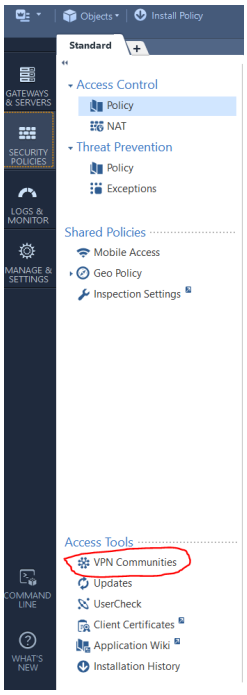


5. For 3rd party GWs you will need to create it as an interoperable device, and select the link selection within the topology tab. The click the manually defined radial and select the inside network on the other end of the tunnel.



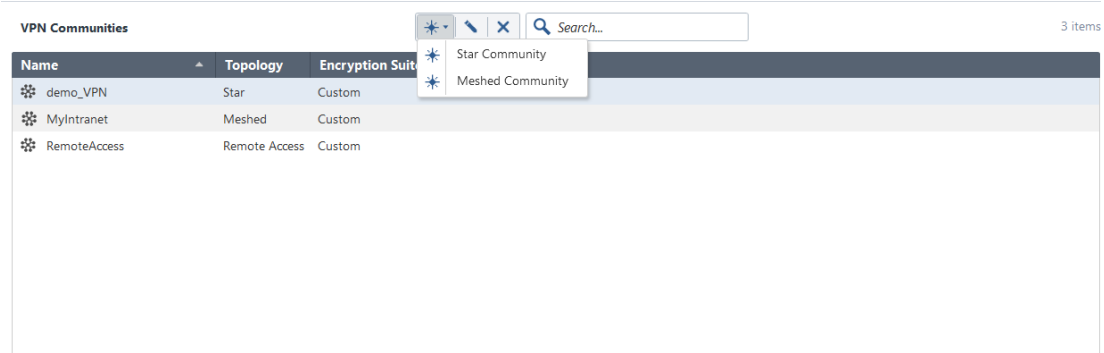


6. Next you will need to create the VPN community. Click on the security policies tab on the left pane. The select VPN Community at the bottom left.

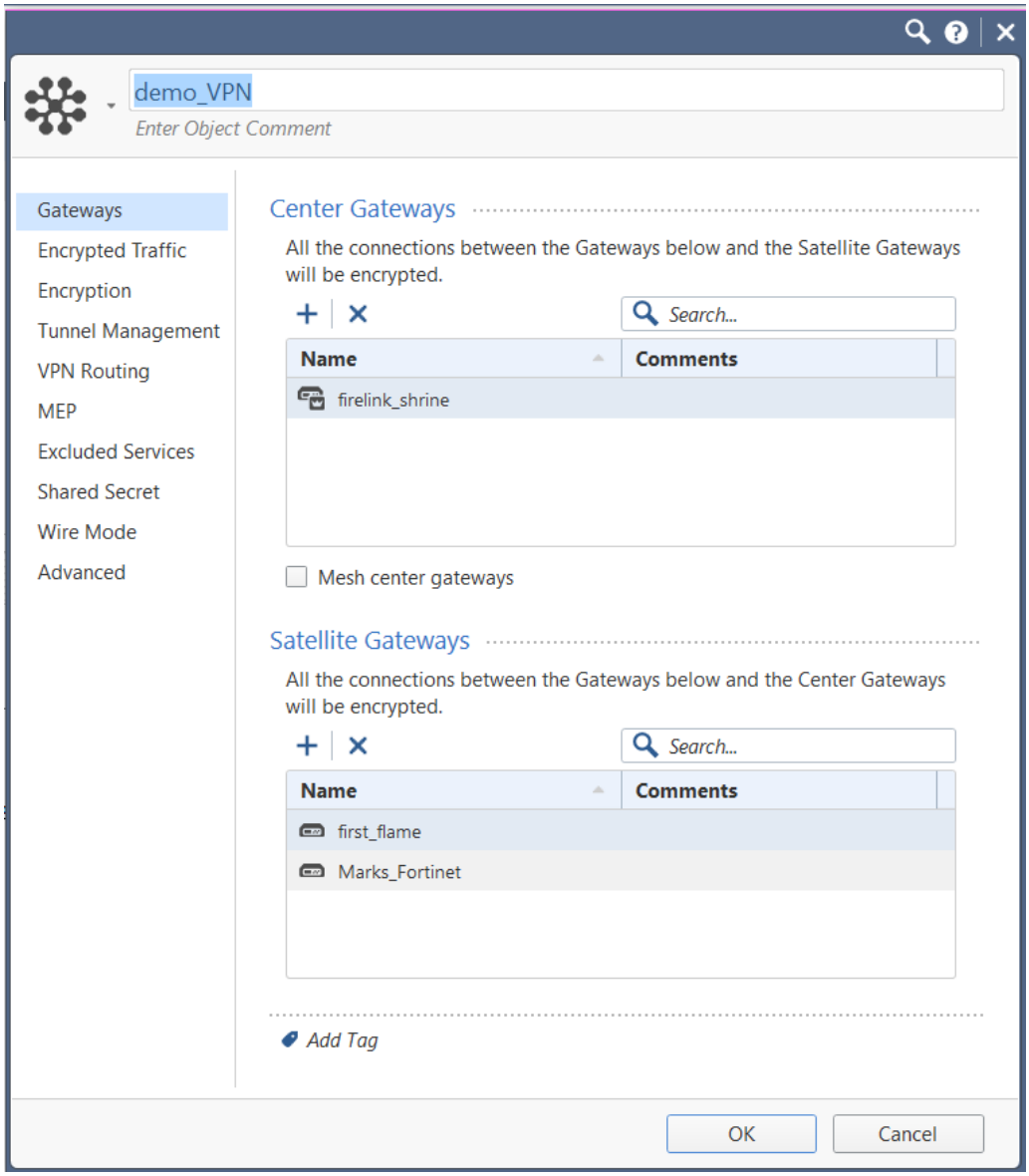


7. There are two types of communities you could create; a Mesh community, consisting of multiple gateways all being able to connect VPN to each other; or a

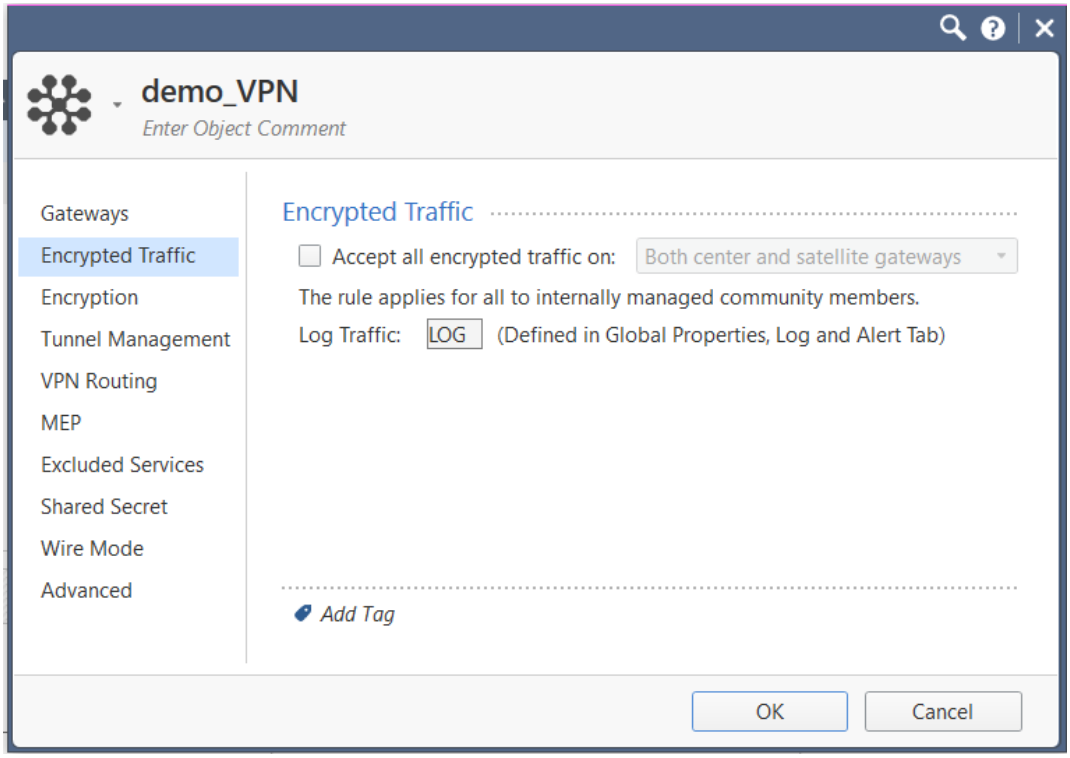
Star community, which is one central GW with remote GWs VPN back to it. Select new, and your choice of community.



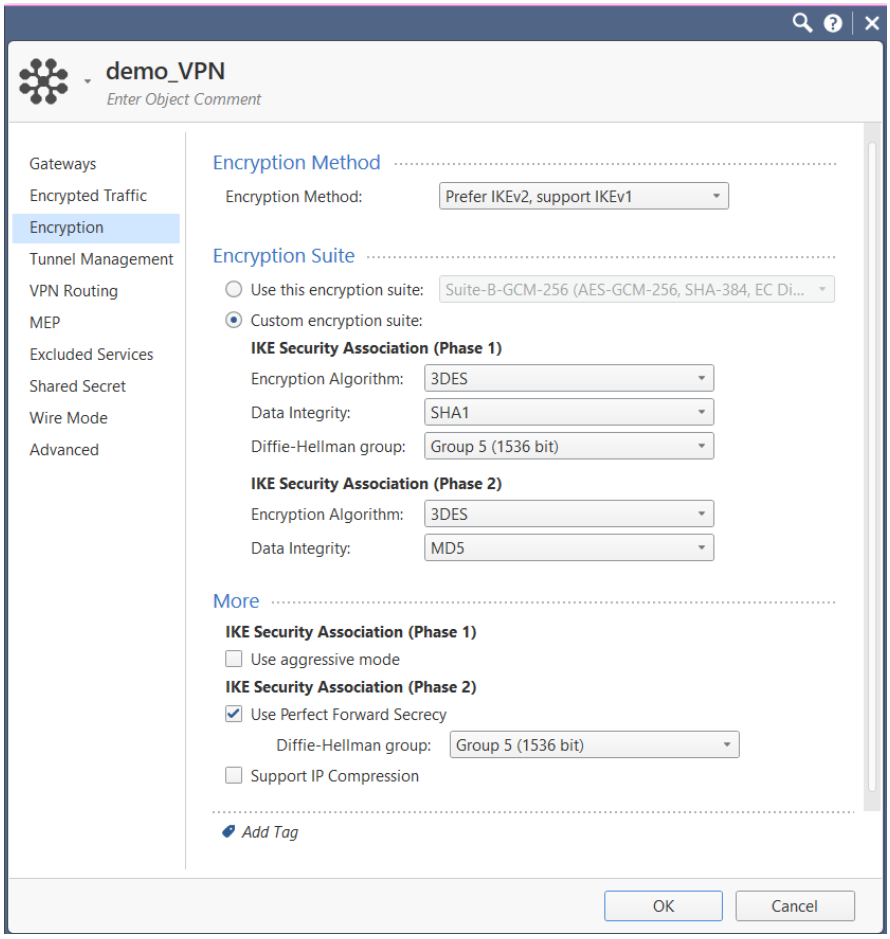
8. Give it a name and select your participating GWs



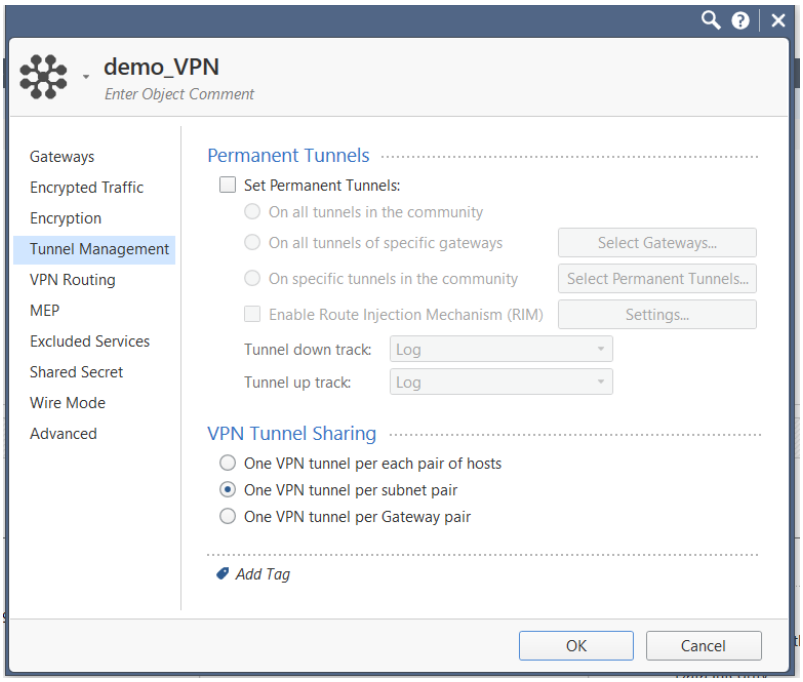
9. You can choose to accept all internal traffic if the participating GWs without the need for an access rule.



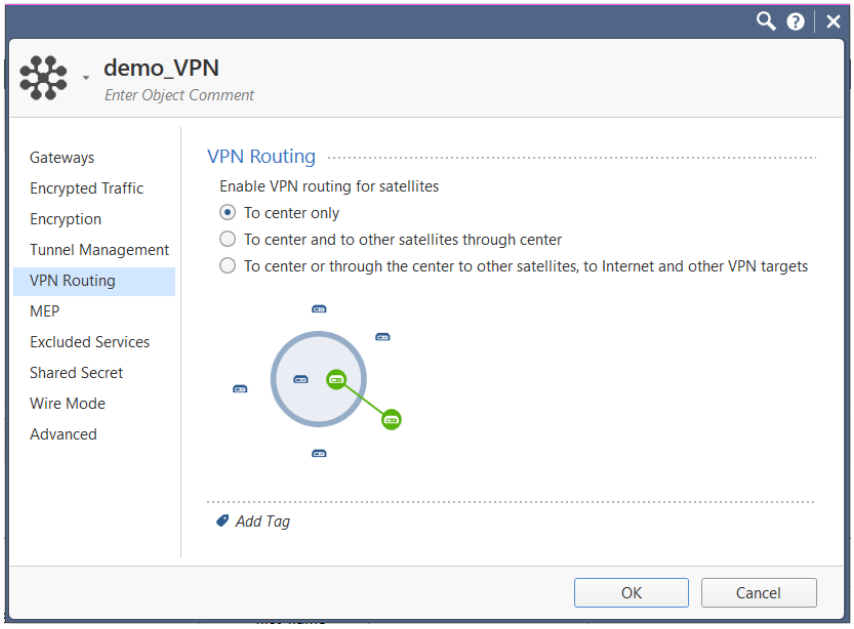
10. Next, choose the encryption method. This is where most of your troubleshooting with 3rd party GWs will take place. The Encryption methods must be identical on both ends. Use Aggressive mode if you are connecting to a 3rd party that does not support Main mode. Use Perfect Forward Secrecy for extreme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



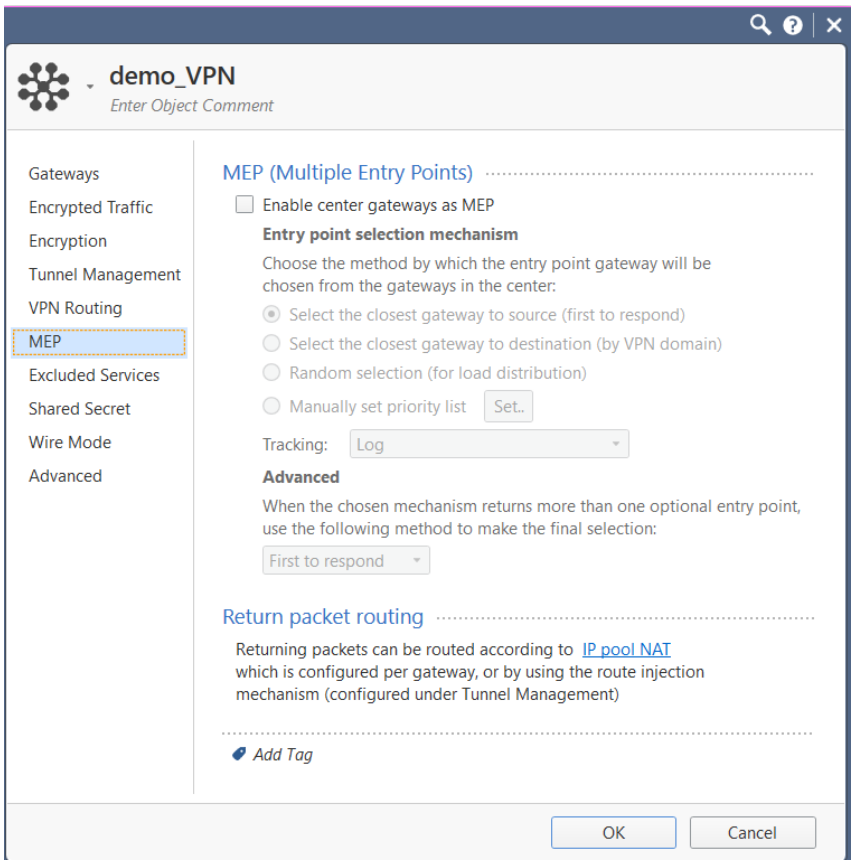
11. You can choose to create permanent tunnels if you wish.



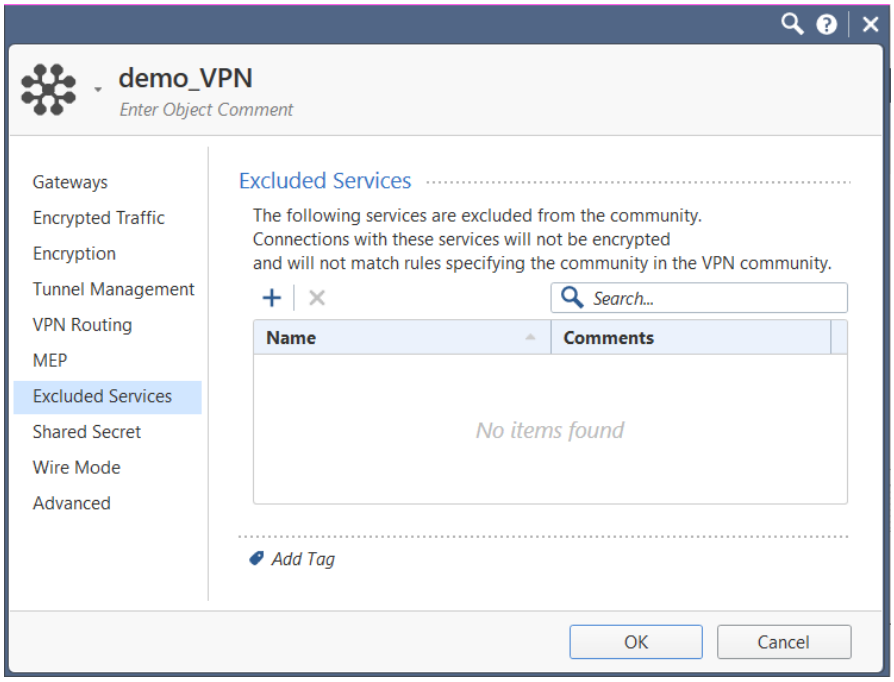
12. Decide how the tunnel routes. Whether the satellites can go through the center or just to it only.



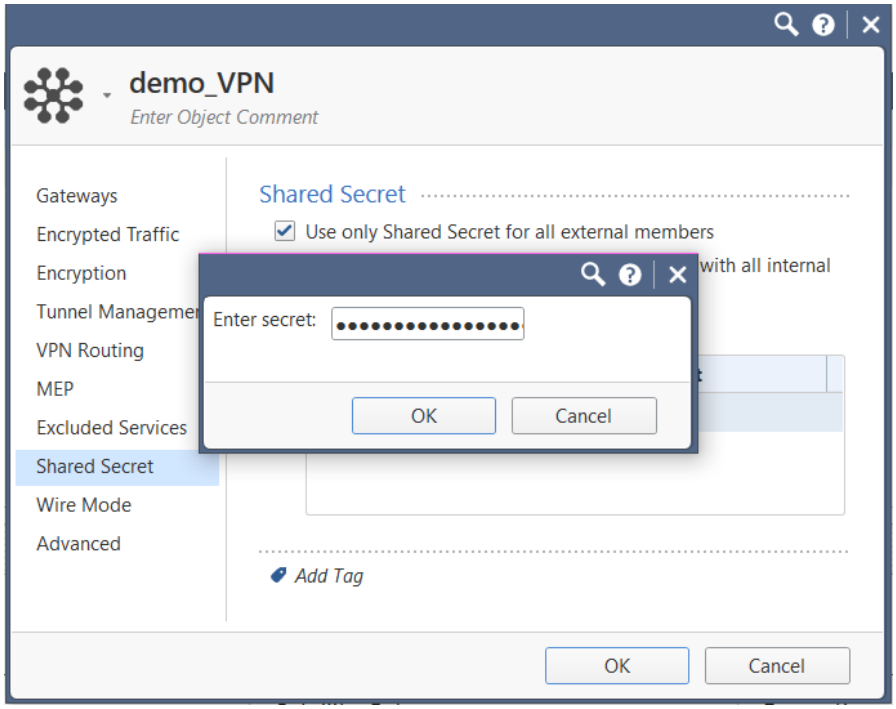
13. MEP (Multiple Entry Points) is used for load balancing if you are expecting heavy load on your tunnel.



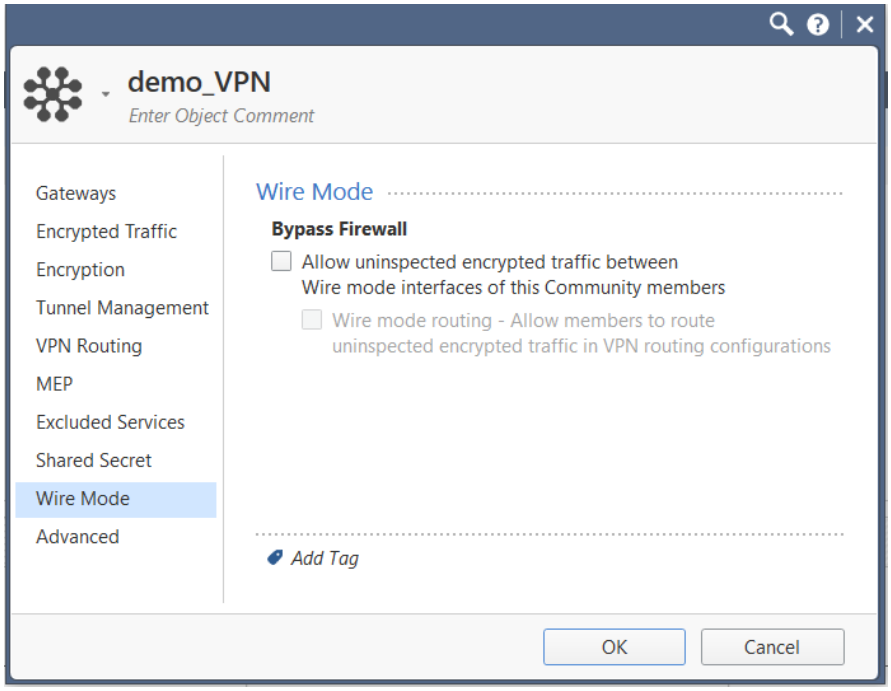
14. You can choose certain traffic that will not be encrypted over the tunnel to increase performance.



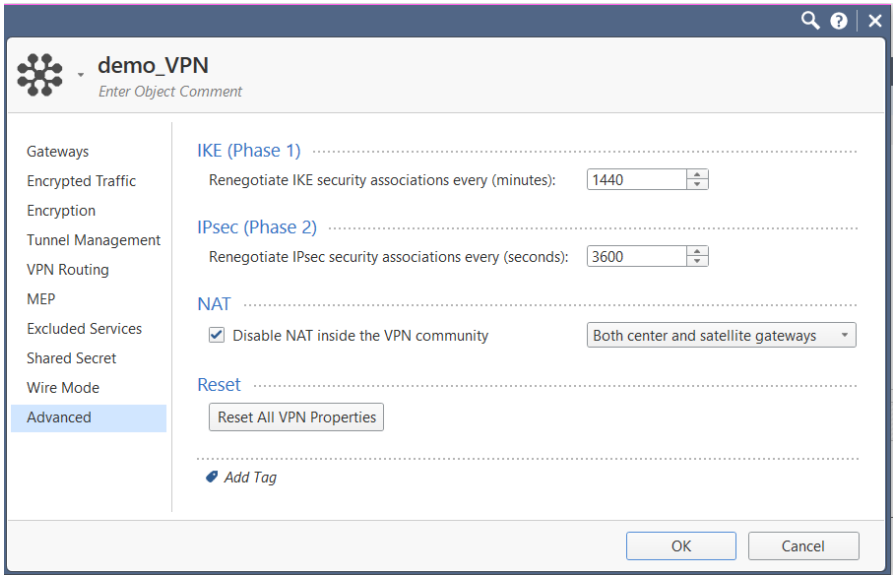
15. When connecting to a 3rd party you will need a Shared Secret. This password must be identical on both ends of the tunnel.



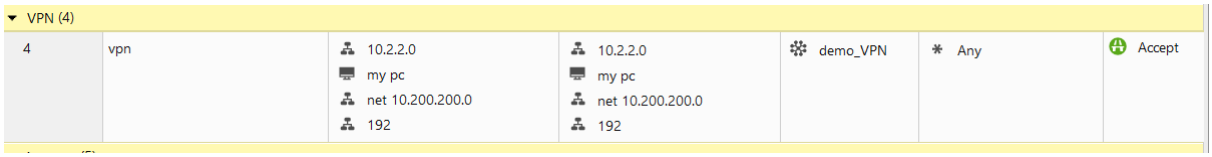
16. Wired mode simulates the GWs being connected together via wired connection, bypassing the GW completely.



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.



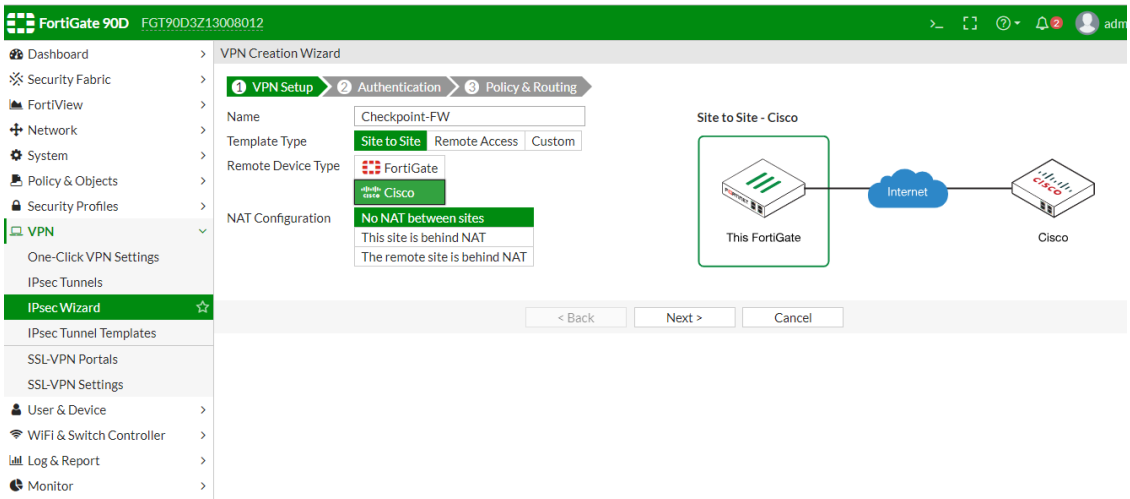
18. Next, you will create an Access Rule to allow the VPN traffic. You will add the network/host objects in the destination and source. Choose the VPN community you created, then allow and log the traffic.



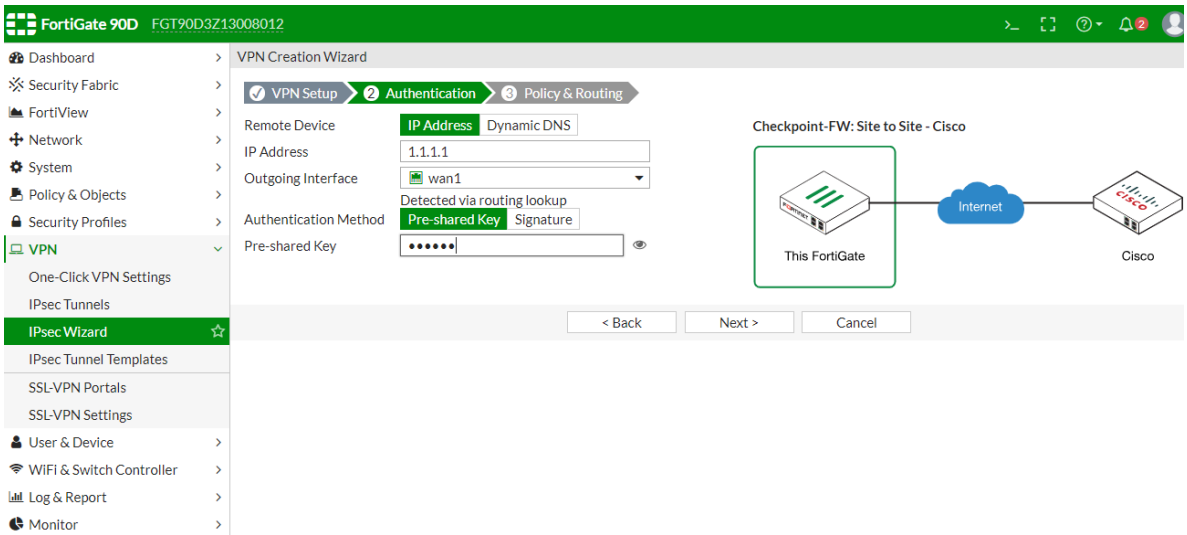
19. Publish and install policy on participating GWs

VPN with a Third Party

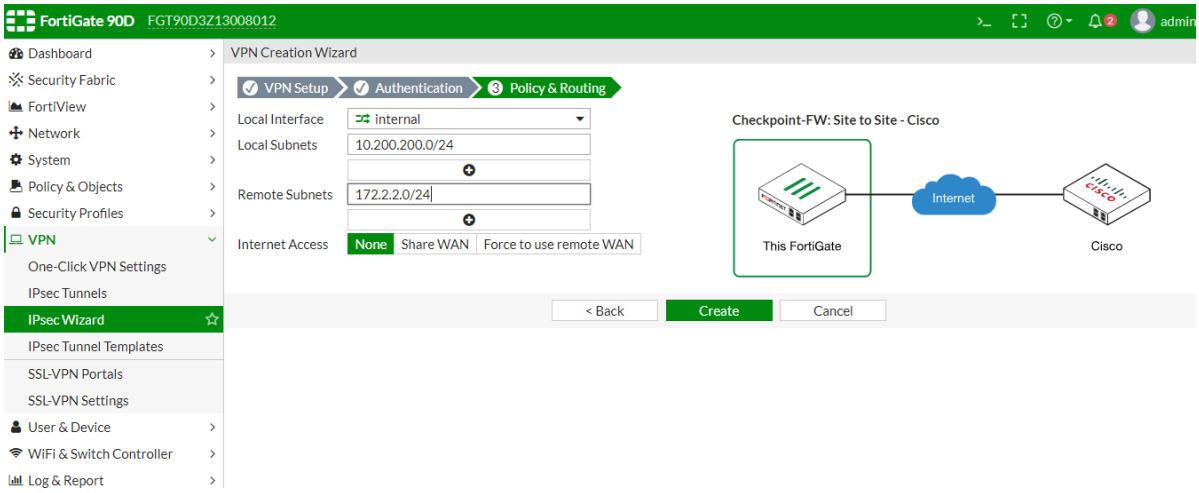
1. An example of configuring on a Fortinet for the 3rd party. The IPSec wizard. Name, select type of VPN, and NAT configuration.

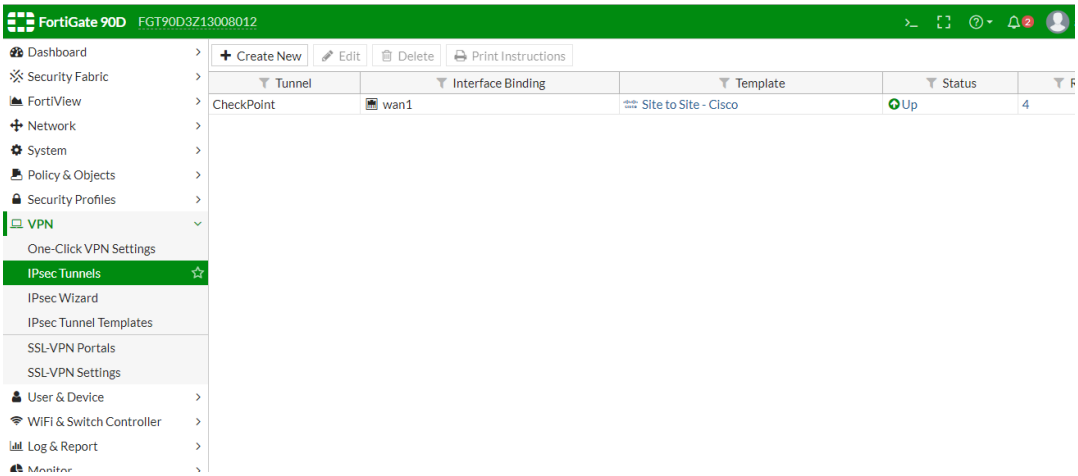


2. Configure IP, interface, and authentication methods.

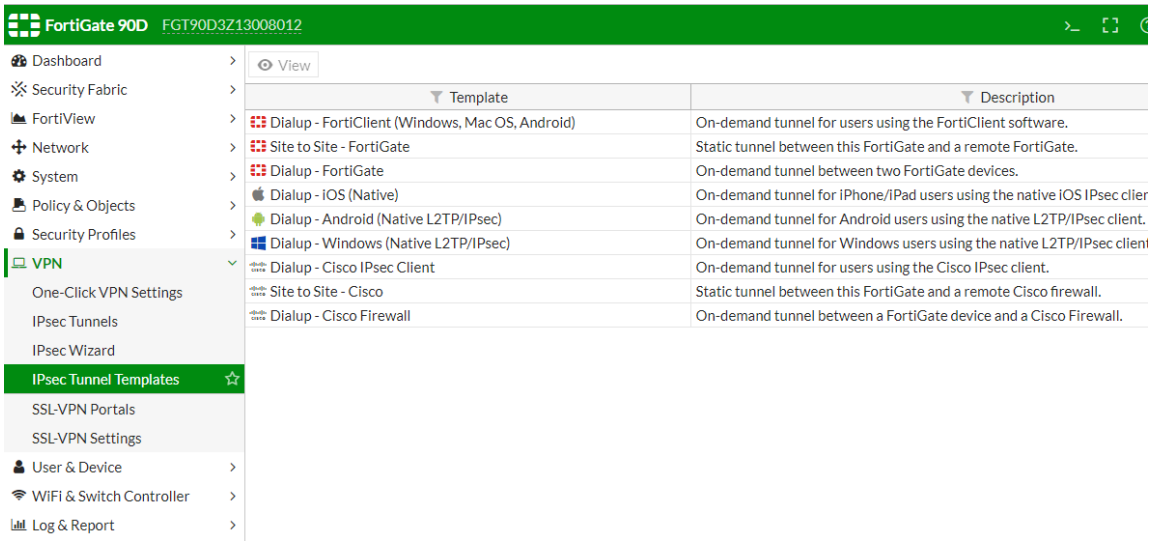


3. Configure the source and destination subnets. Click **create**.

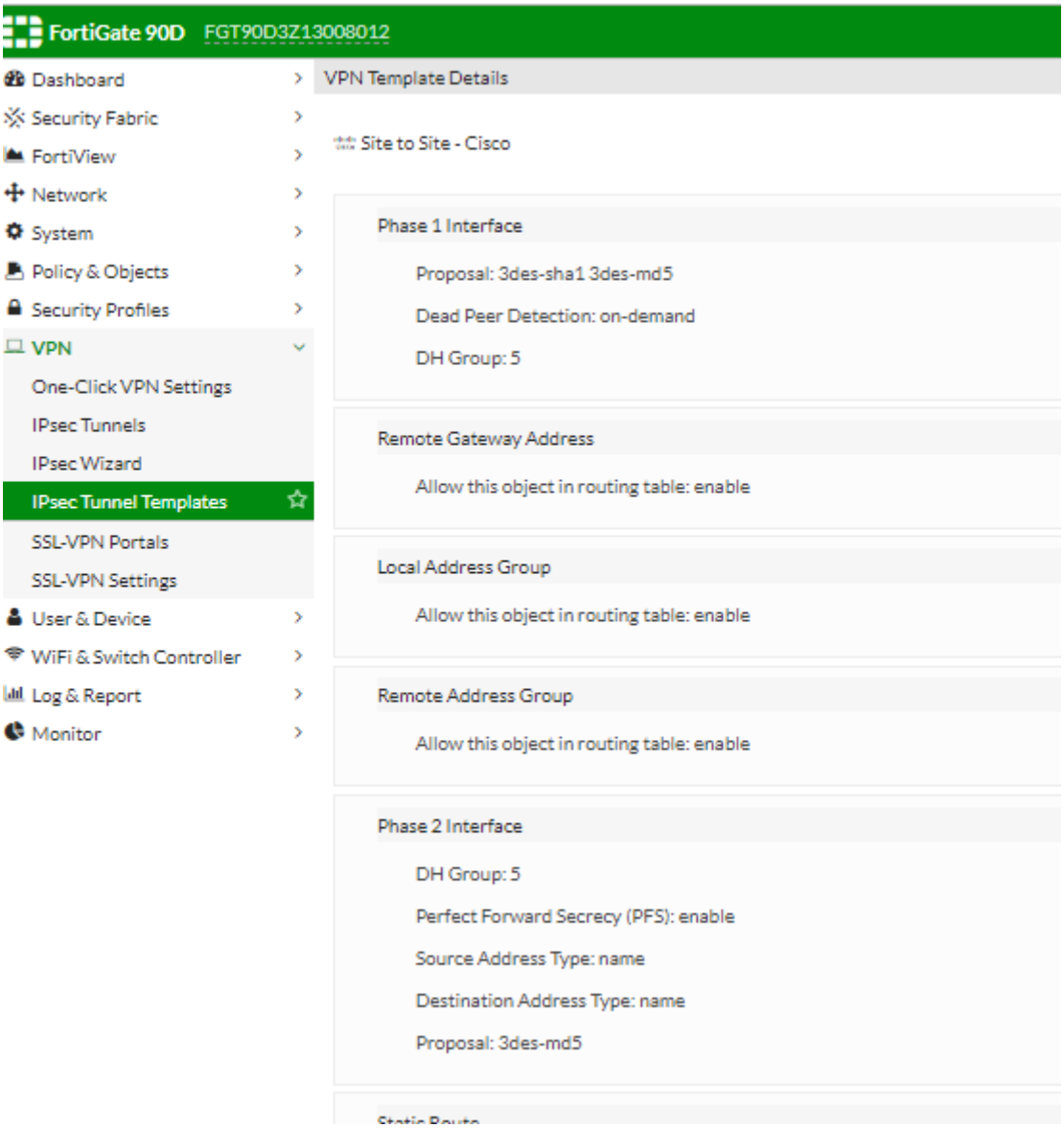




4. Preconfigured templates



5. Configure the encryption method here.


FortiGate 90D
FGT90D3Z13008012
Dashboard
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
VPN Template Details
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

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

