How to Create a Unnumbered VTI Tunnel -all traffic through VTI

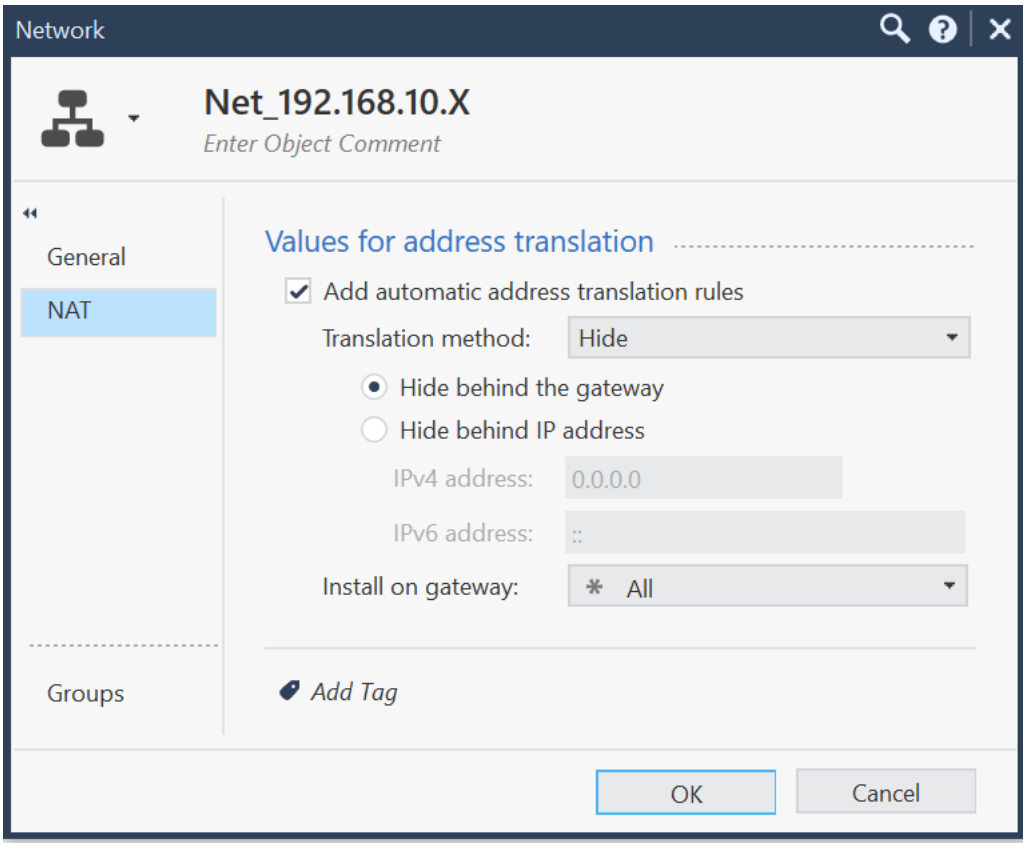
Mark Bennett

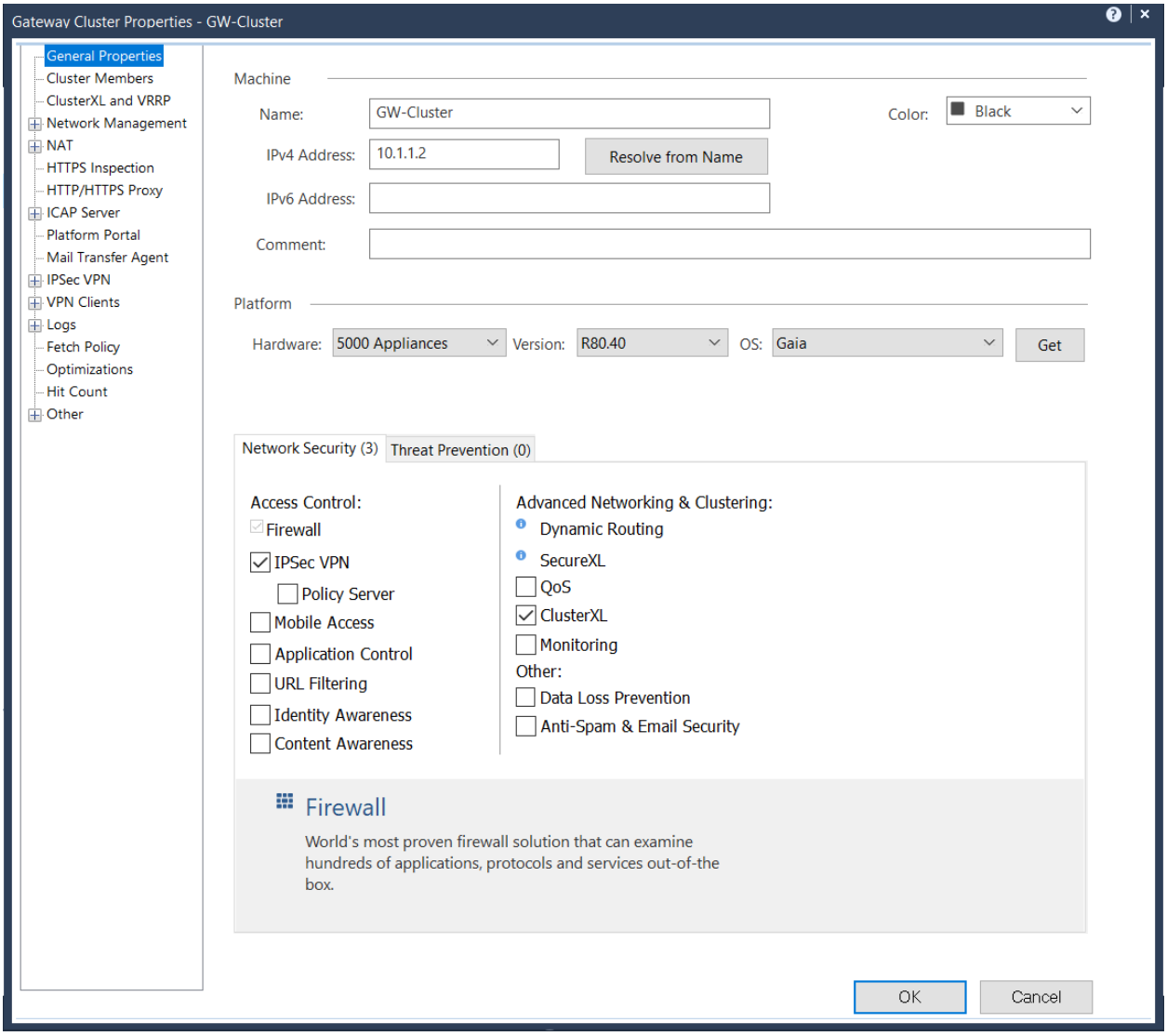
SE SLED Arizona Region

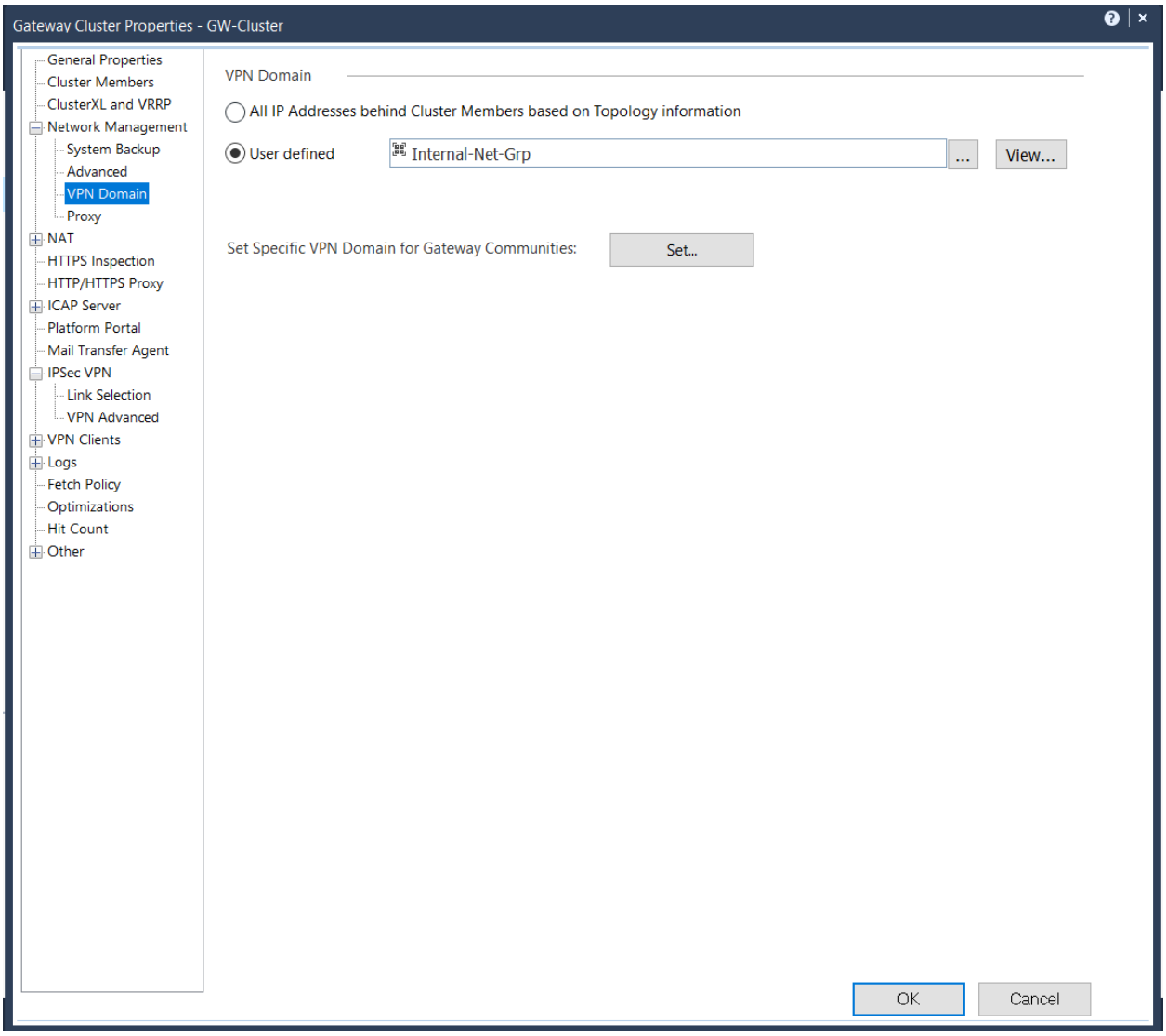
Sept 20, 2021

By following this simple procedure you will be able to get an unnumbered VTI tunnel working in a few minutes to any 3rd part IPSEC device. This document assumes a basic working knowledge of Check Point and VPN tunnels

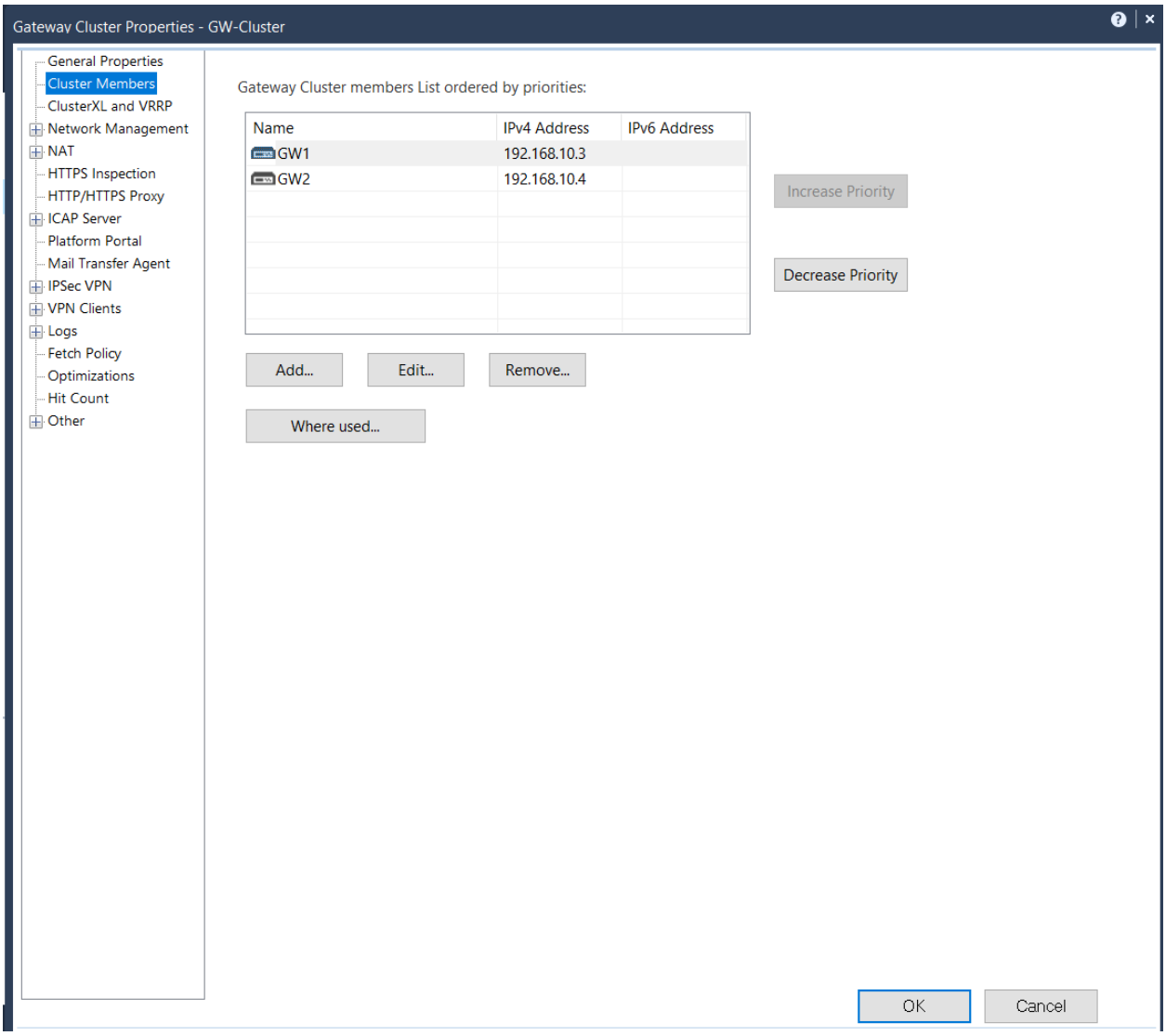
First let us define our local “VPN domain” (aka. Encryption Domain) (Networks or Networks that can be used through a tunnel) if you have more than one network create them and put them in a group.







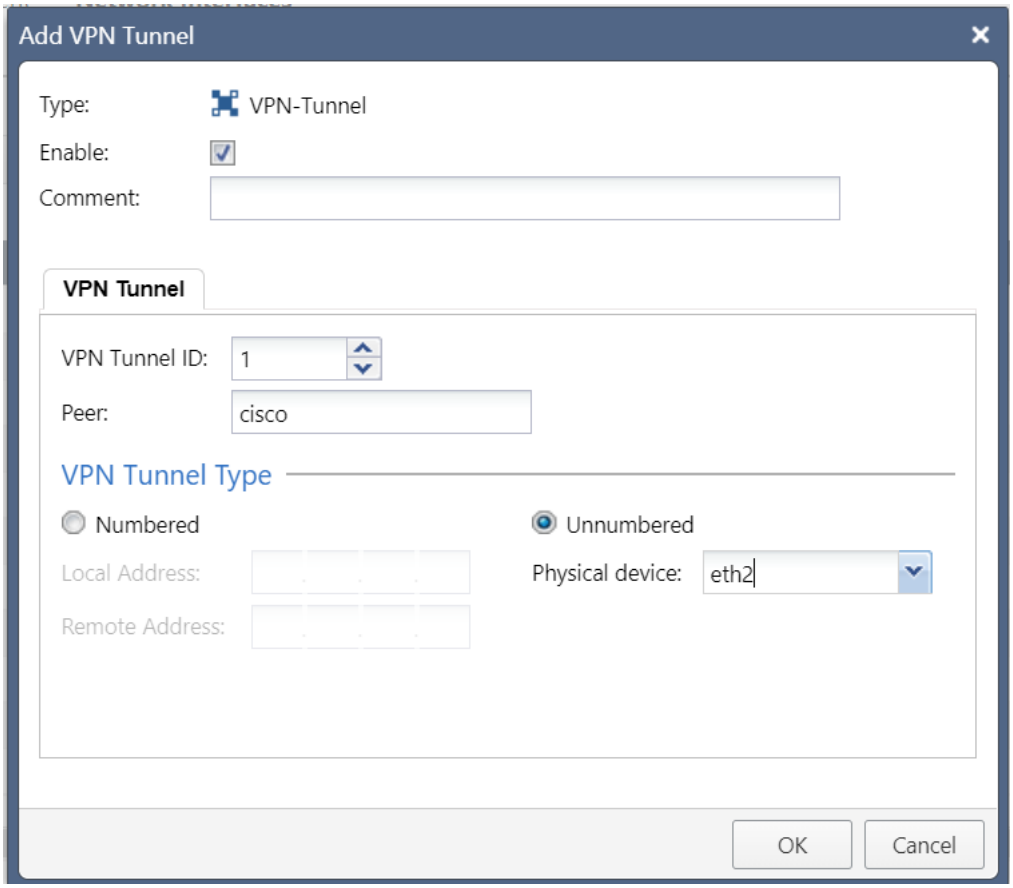
Now Define the VPN (Encryption) domain by adding the object or group you created at the beginning of the document

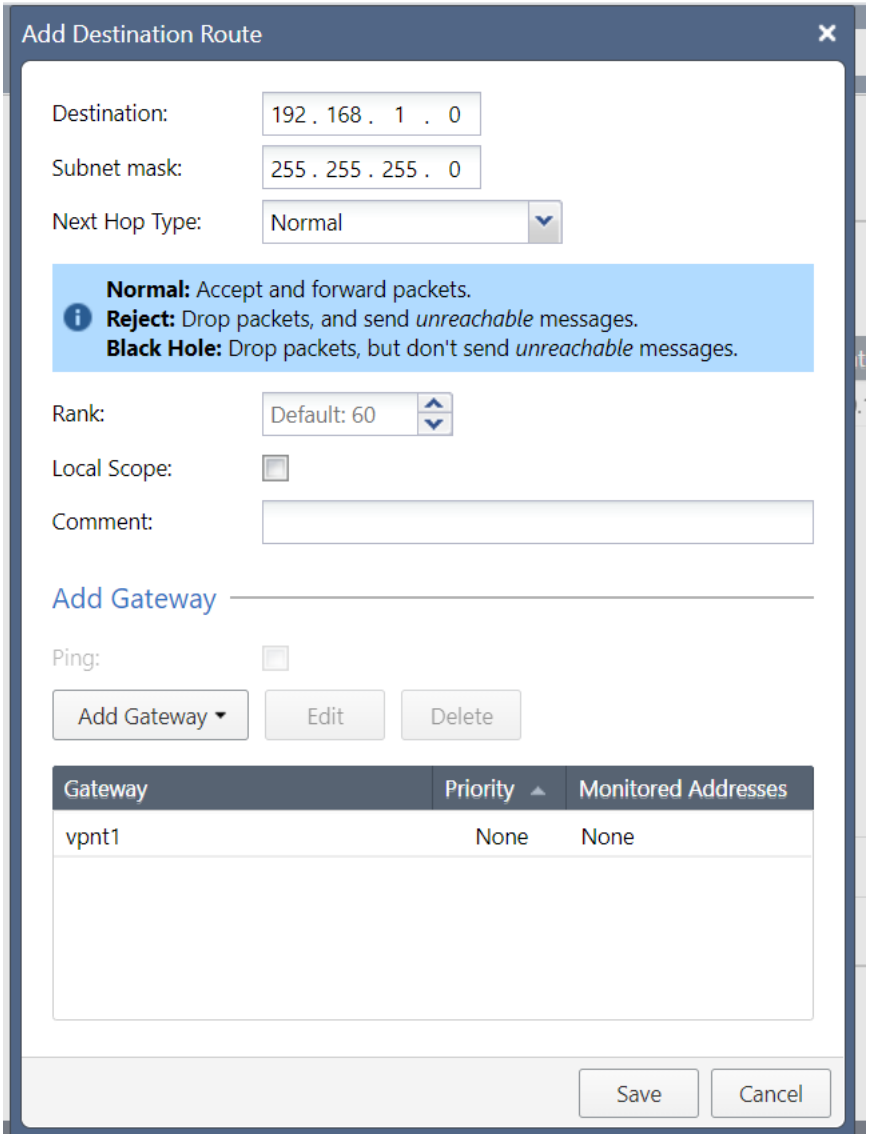


This is currently a cluster. Note the IP addresses you will have to adjust for your own IP network.

Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status
Mgmt	Ethernet	192.168.100.3	255.255.255.0	-	-	No Link
Sync	Ethernet	10.50.50.1	255.255.255.252	-	-	Up
eth1	Ethernet	10.1.1.3	255.255.255.0	-	-	Up
eth2	Ethernet	192.168.10.3	255.255.255.0	-	-	Up
eth3	Ethernet	172.16.1.3	255.255.255.0	-	-	Up
eth4	Ethernet	-	-	-	-	Down
eth5	Ethernet	-	-	-	-	Down
eth6	Ethernet	-	-	-	-	Down
eth7	Ethernet	-	-	-	-	Down
eth8	Ethernet	-	-	-	-	Down
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up
vpnt1	VPN-Tunnel	-	-	-	-	Up

Notice the example GAIA settings for the interfaces and the vpnt1 VPN-Tunnel interface you must create.



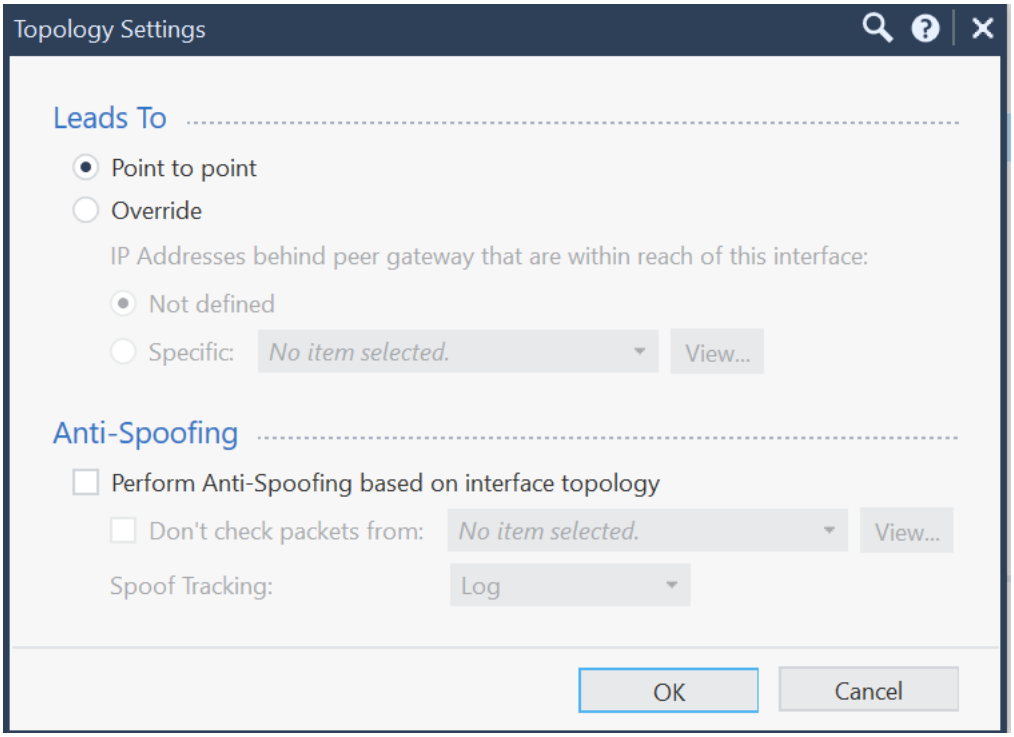


Add a route for the peer network (destination) to go through the vpnt1 interface in GAIA

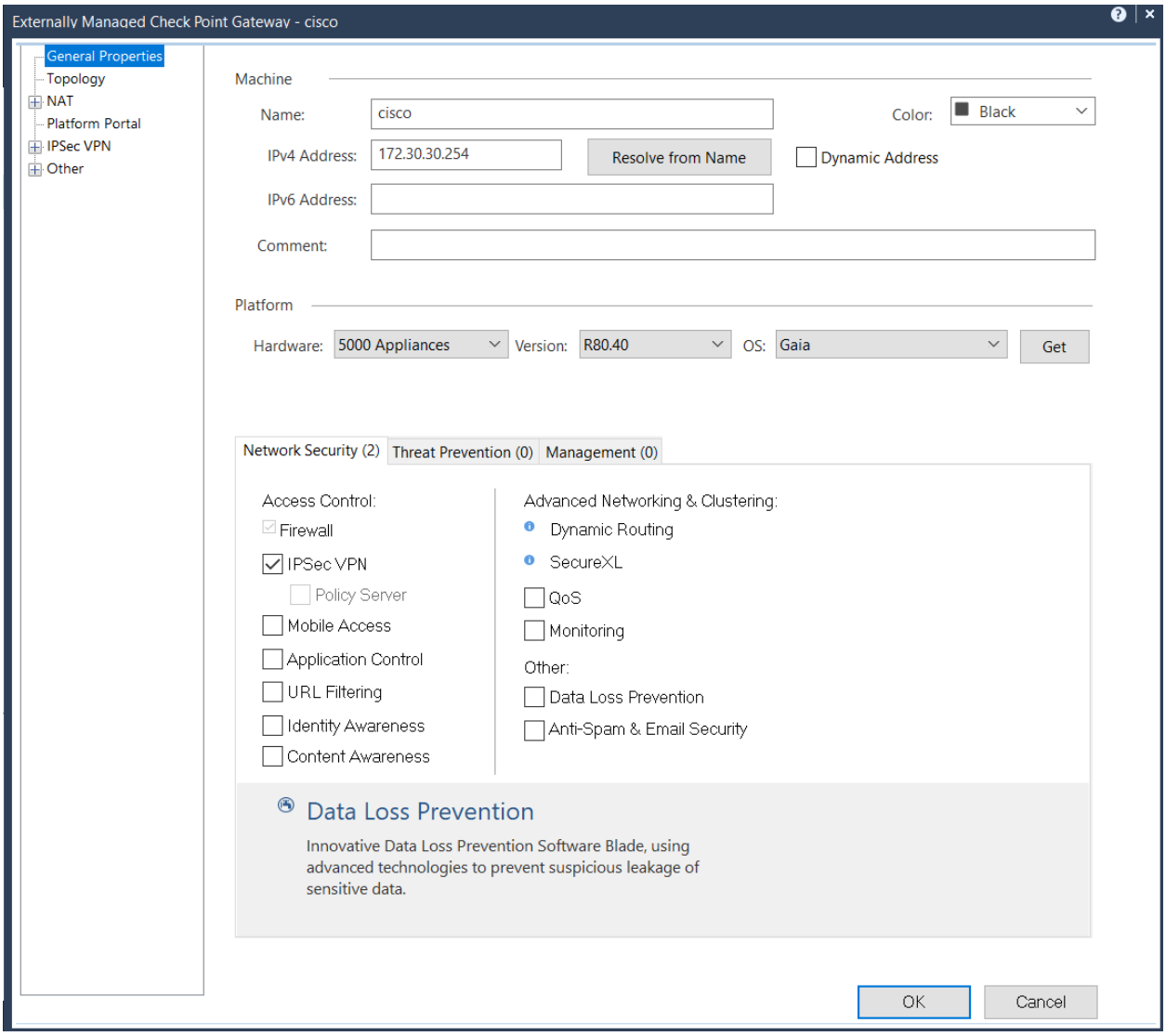
IPv4 Static Routes

Add | Edit | Delete

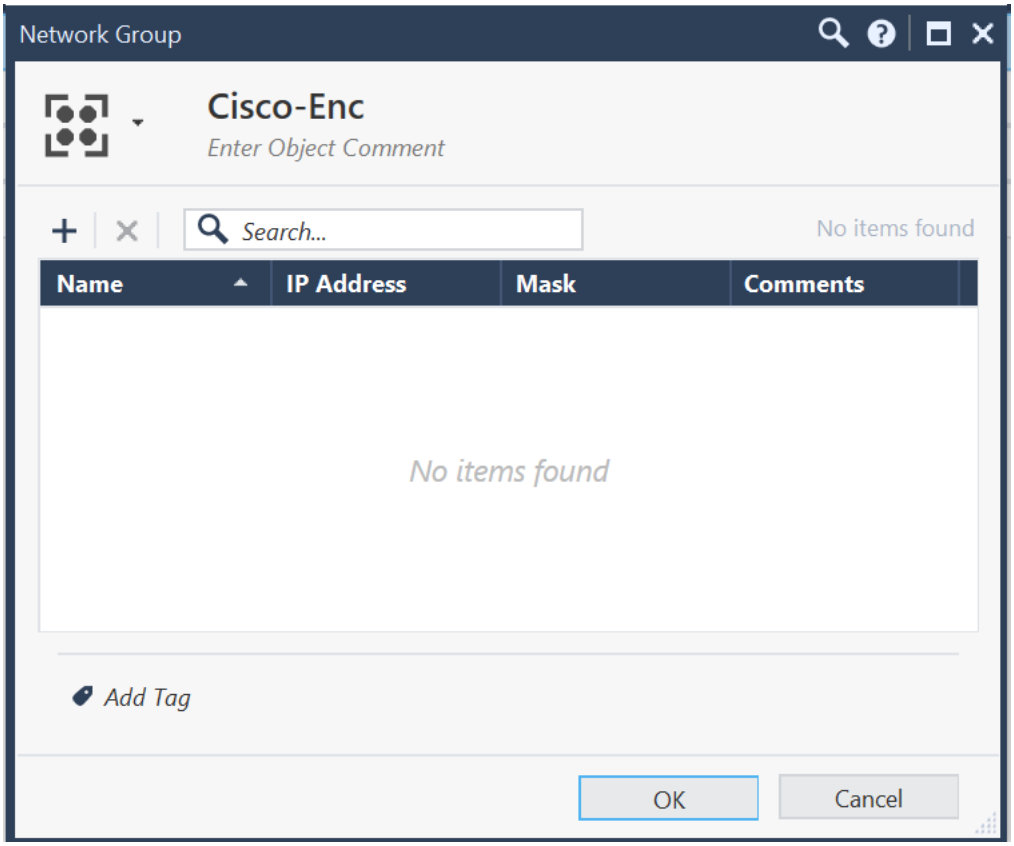
Destination Address	Next Hop Type	Rank	Local Scope	Gateways (Priority)	Monitored Protocols	Ping	Comment
Default	Normal	60	N/A	10.1.1.1 (None)	None	No	
192.168.1.0/24	Normal	60	Off	vpnt1 (None)	None	No	



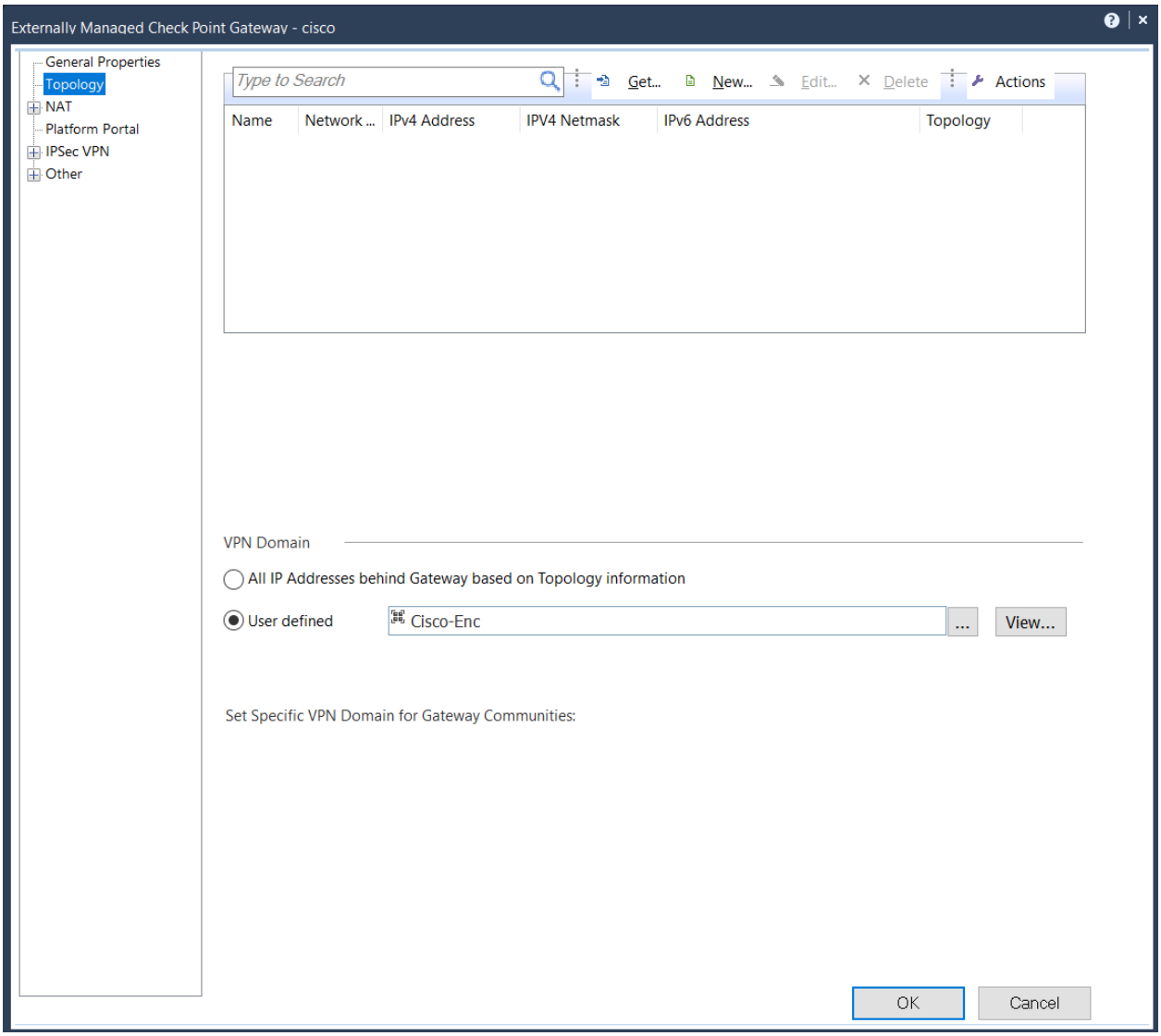
Set the interface topology this way in SmartConsole



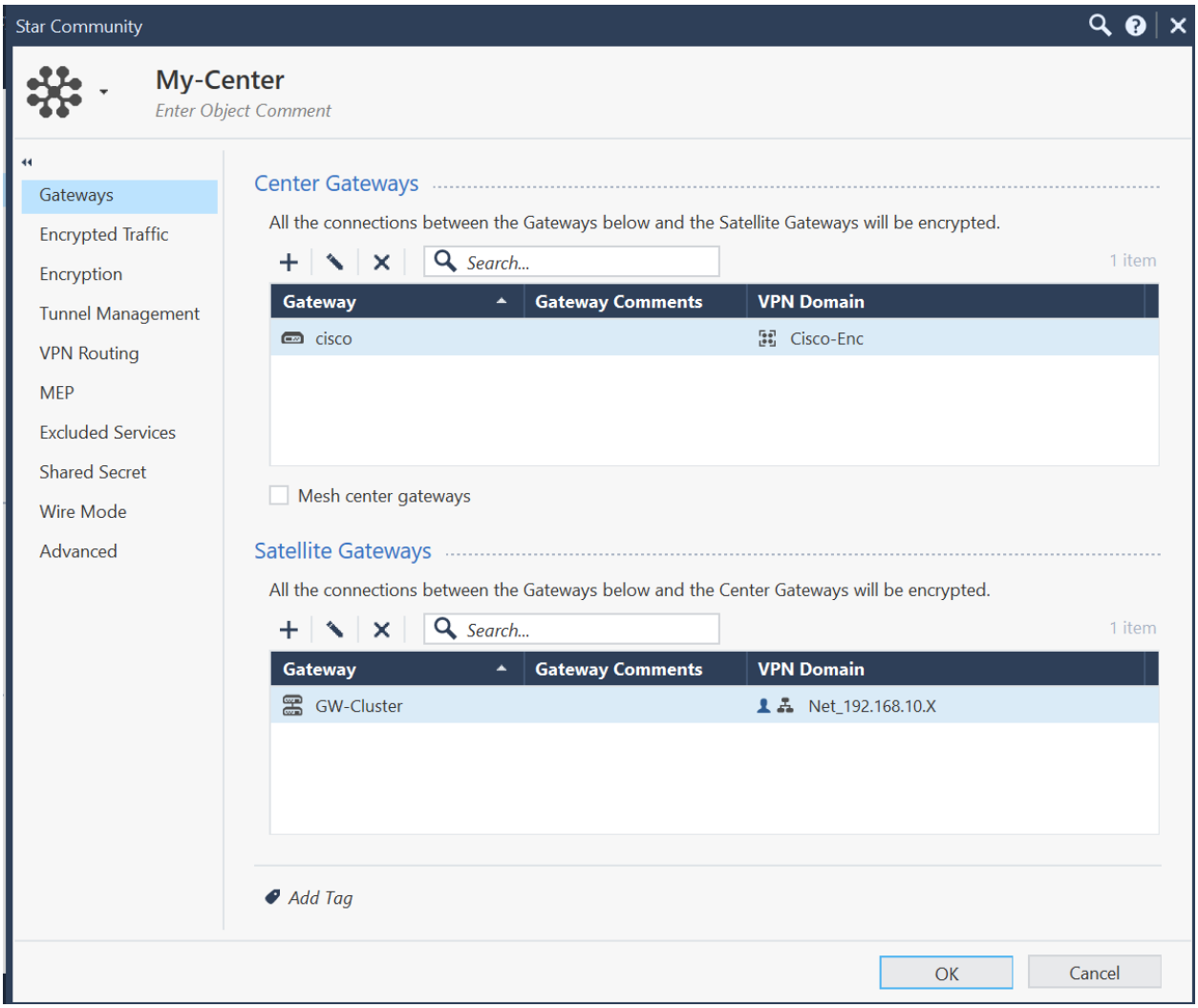
Now let's define the peer information

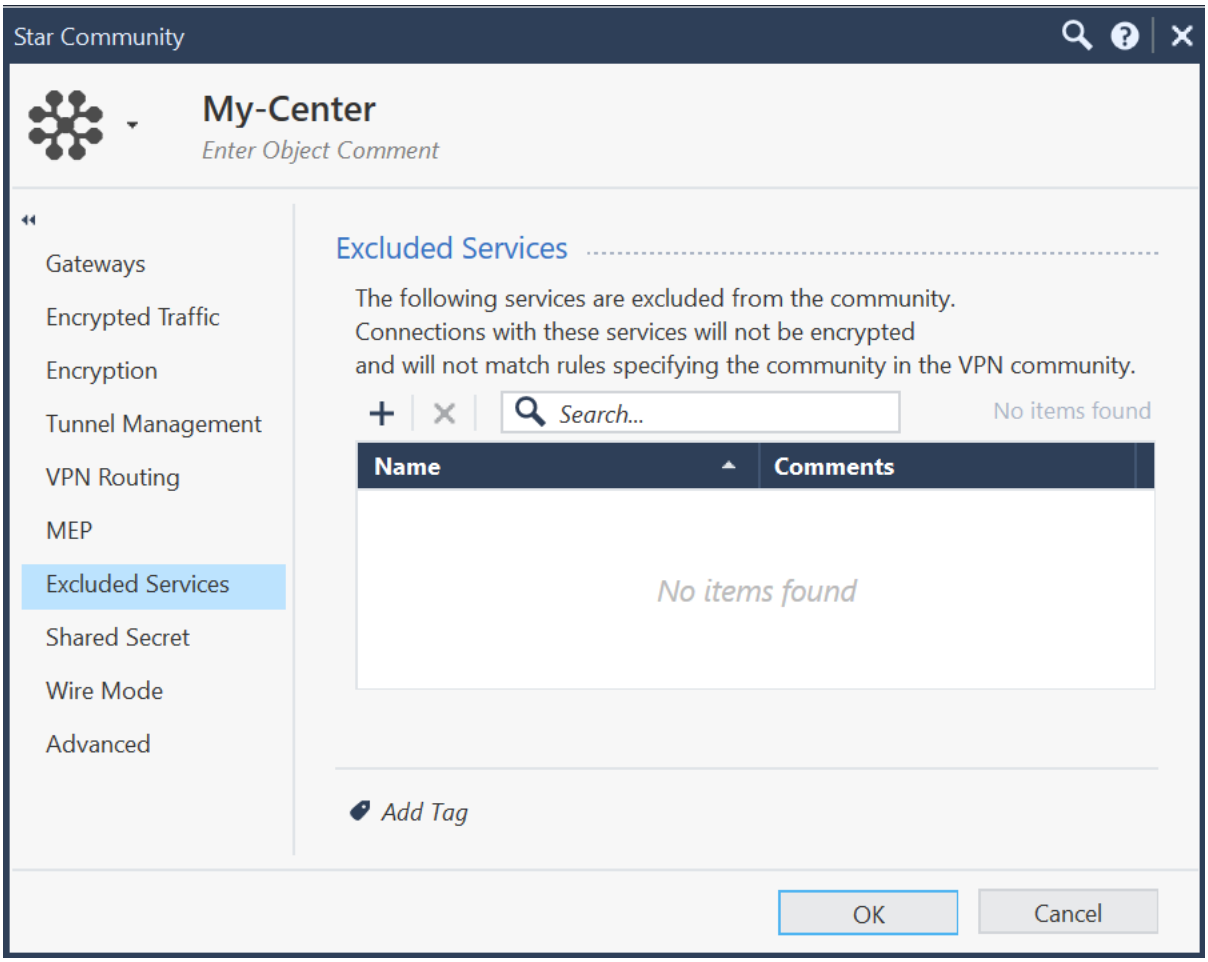


Create a Blank Group with nothing in it to use for the VPN domain.

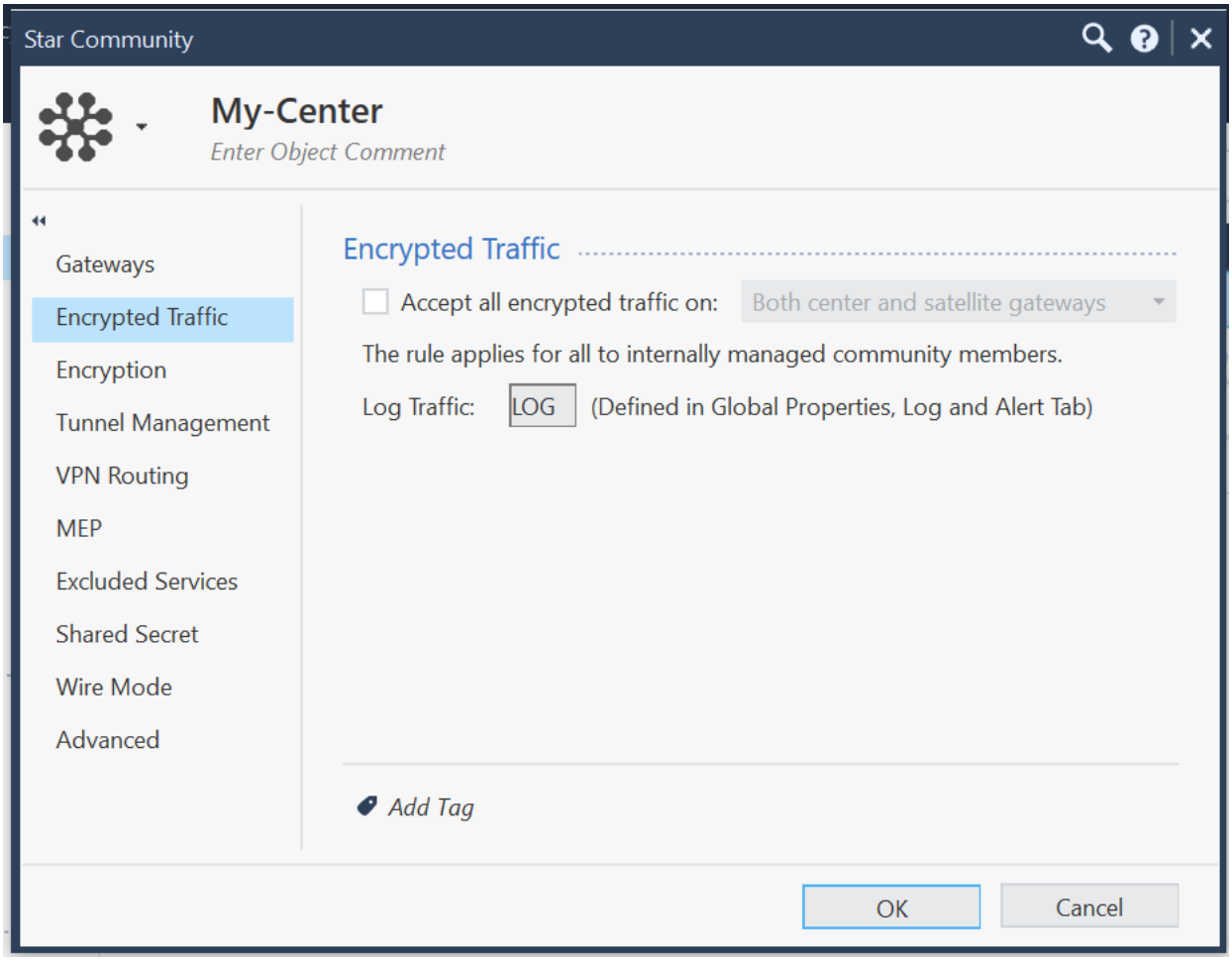


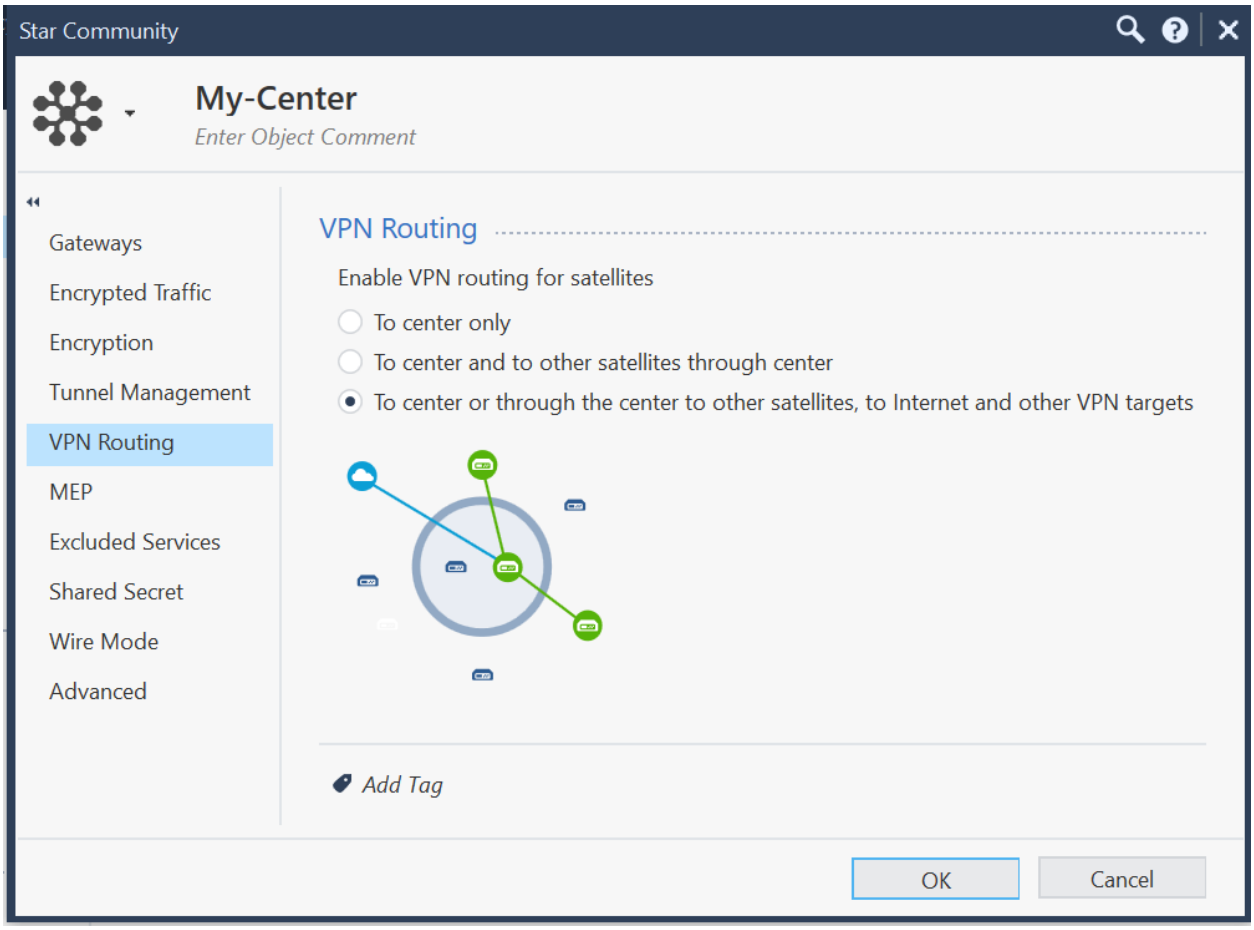
Add that group as the VPN domain.



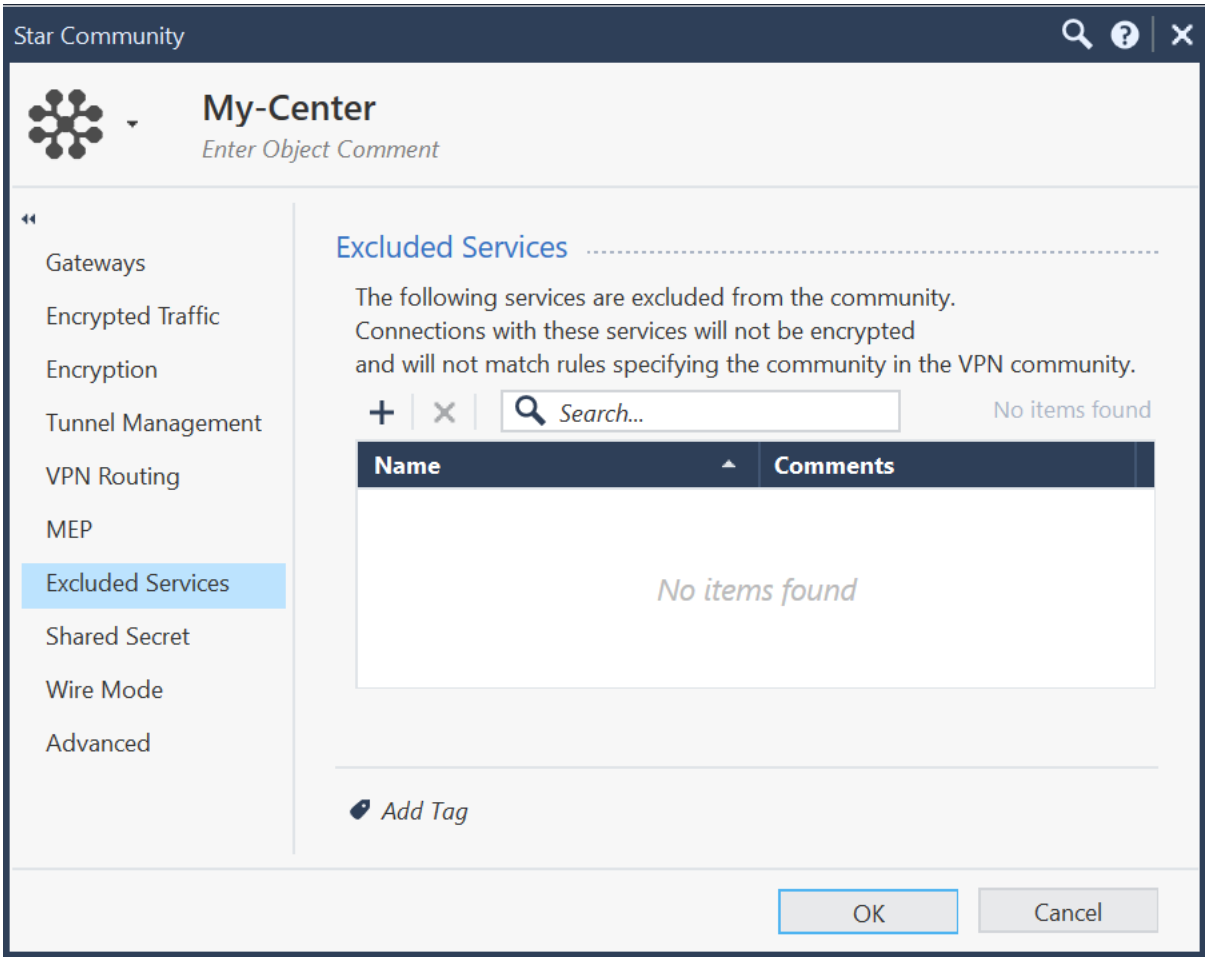


Now Let's define the community we are using.

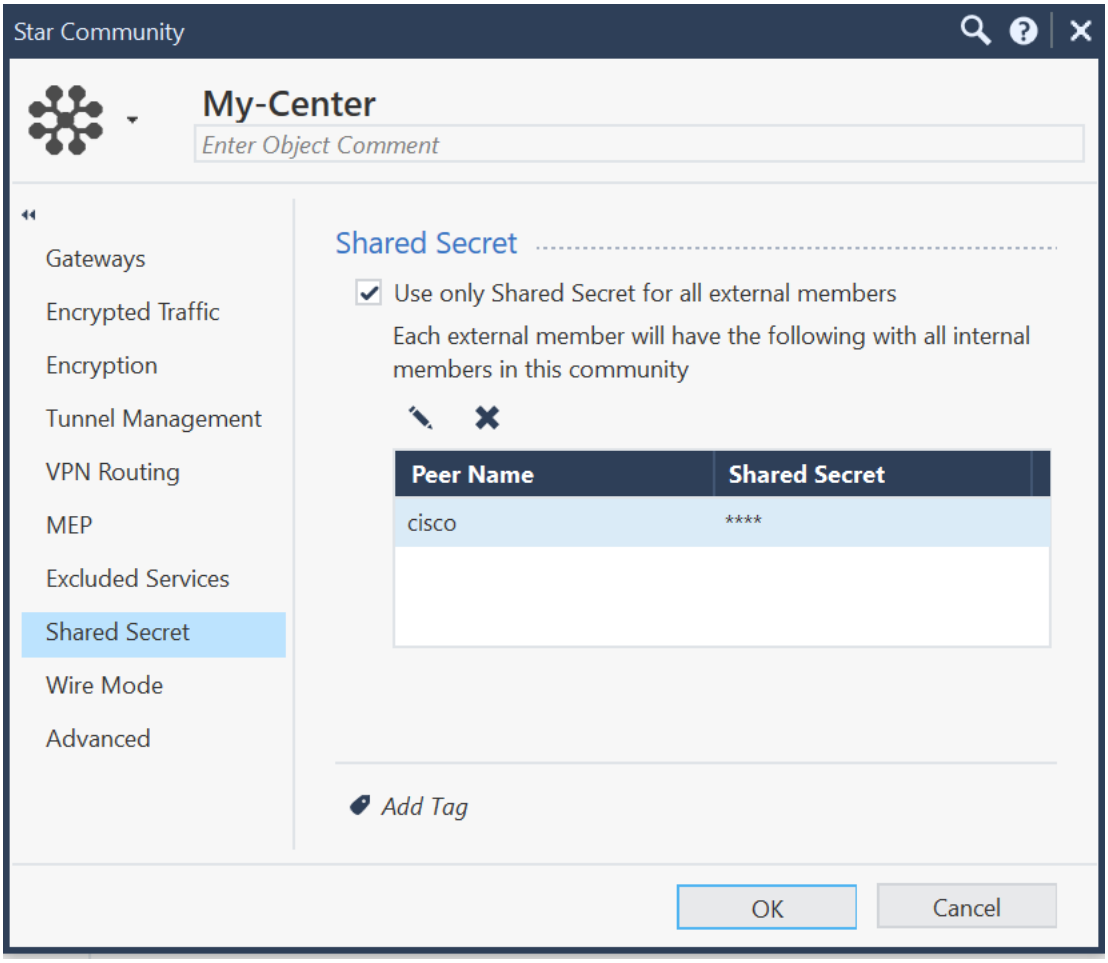




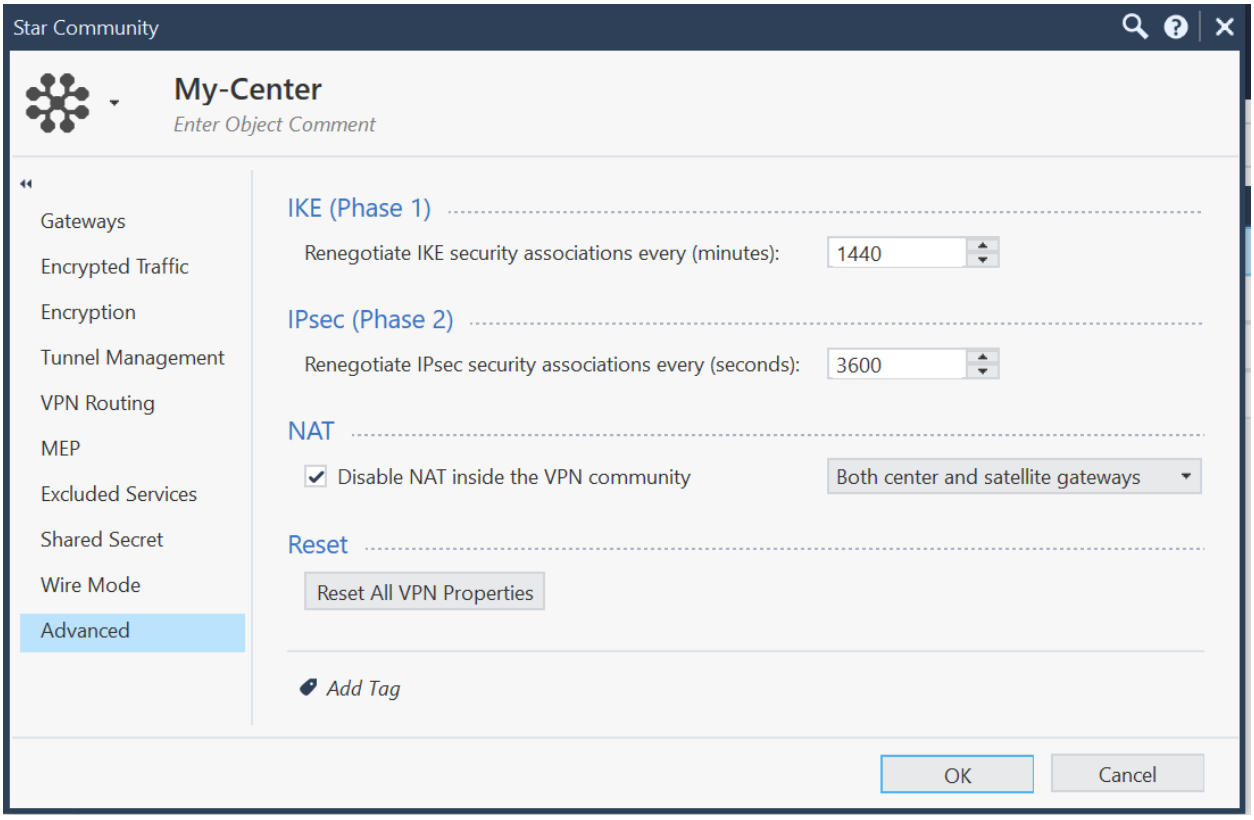
Set VPN routing for To Center or through the center to other satellites, to internet and other VPN targets (this can be used if you want to also go to internet which will be shown how in another document I will write) or pick to center only.



Exclude any services necessary



Set your shared secret decided upon by you and peer



Set negotiation and check “Disable NAT inside the VPN community”

Test your traffic and tunnel will come up and traffic will flow.