

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

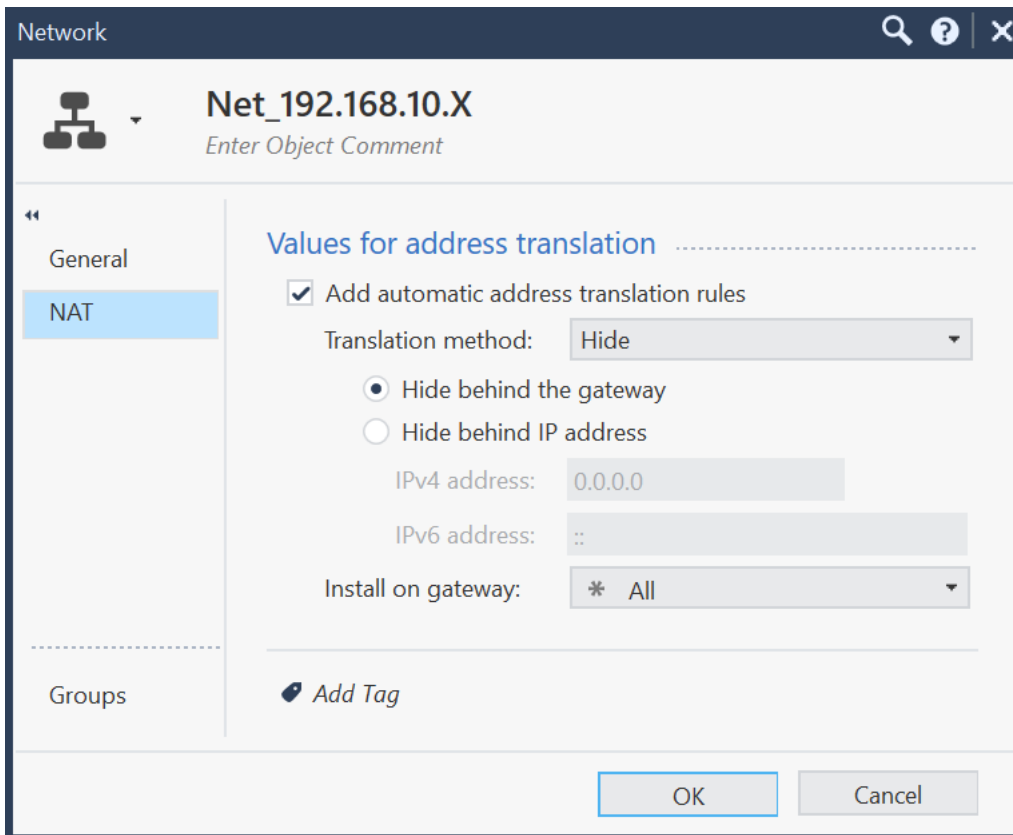
Mark Bennett

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.



Network

Net_192.168.10.X
Enter Object Comment

General

NAT

Groups

Values for address translation

Add automatic address translation rules

Translation method: Hide

Hide behind the gateway
 Hide behind IP address

IPv4 address: 0.0.0.0

IPv6 address: ::

Install on gateway: * All

Add Tag

OK Cancel

Gateway Cluster Properties - GW-Cluster ? x

- General Properties
- Cluster Members
- ClusterXL and VRRP
- Network Management
- NAT
 - HTTPS Inspection
 - HTTP/HTTPS Proxy
- ICAP Server
 - Platform Portal
 - Mail Transfer Agent
- IPSec VPN
- VPN Clients
- Logs
 - Fetch Policy
 - Optimizations
 - Hit Count
- Other

Machine

Name: Color: Black v

IPv4 Address: Resolve from Name

IPv6 Address:

Comment:

Platform

Hardware: 5000 Appliances v Version: R80.40 v OS: Gaia v Get

Network Security (3)

Access Control:

Firewall

IPSec VPN

Policy Server

Mobile Access

Application Control

URL Filtering

Identity Awareness

Content Awareness

Threat Prevention (0)

Advanced Networking & Clustering:

Dynamic Routing

SecureXL

QoS


ClusterXL

Monitoring

Other:

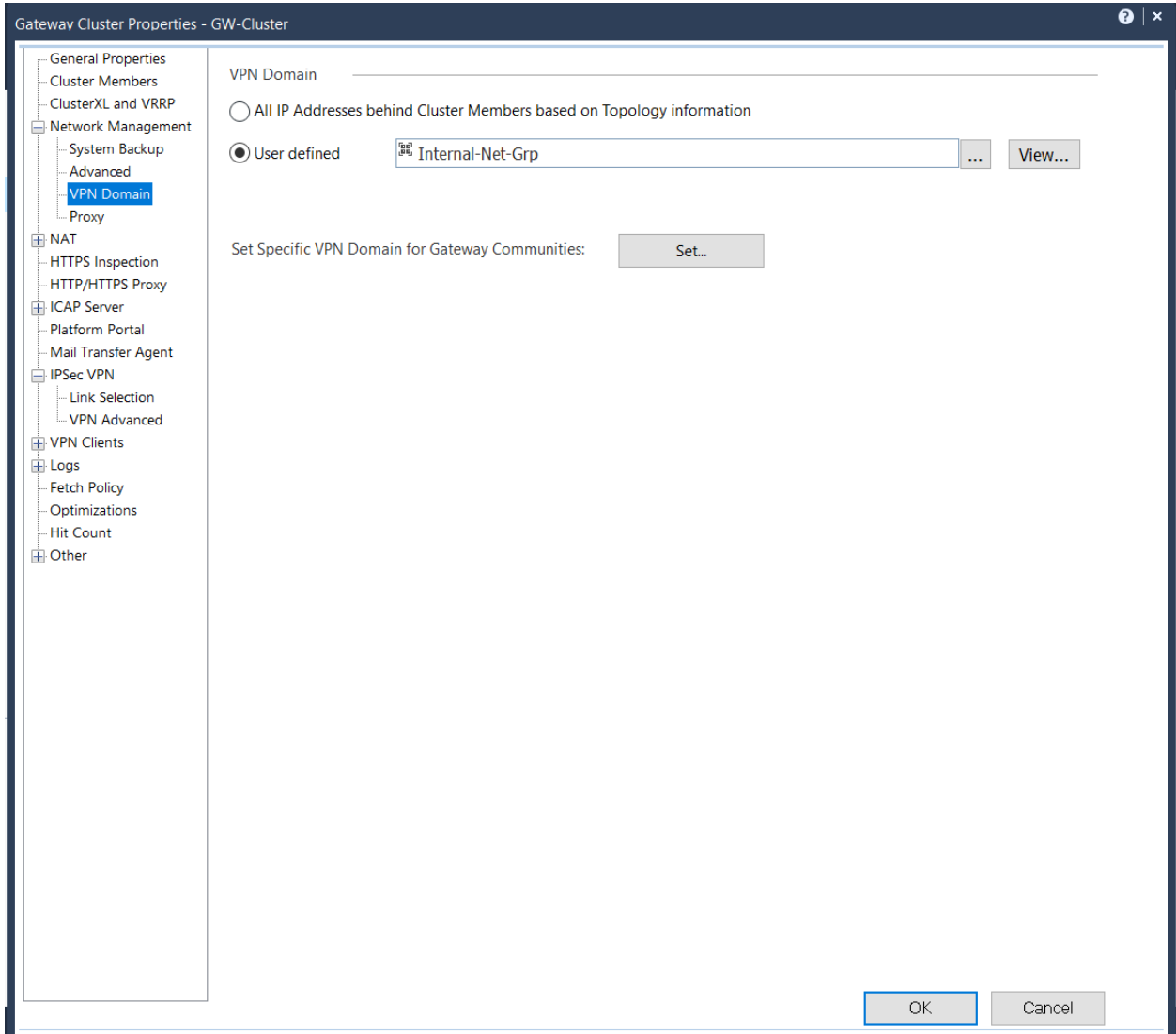
Data Loss Prevention

Anti-Spam & Email Security

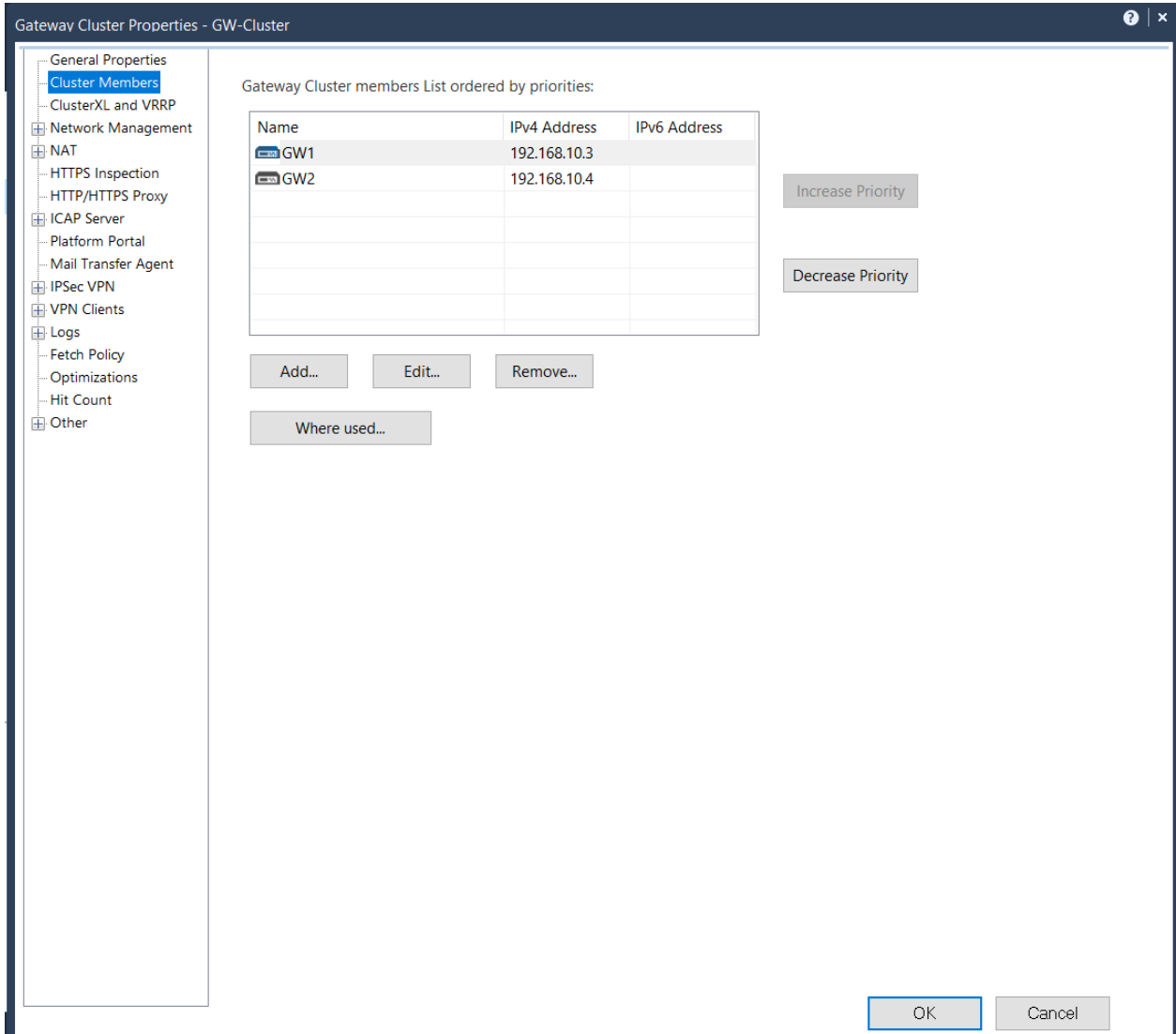
 **Firewall**

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

OK
Cancel



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



Gateway Cluster Properties - GW-Cluster

General Properties
Cluster Members
ClusterXL and VRRP
Network Management
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
ICAP Server
Platform Portal
Mail Transfer Agent
IPSec VPN
VPN Clients
Logs
Fetch Policy
Optimizations
Hit Count
Other

Gateway Cluster members List ordered by priorities:

Name	IPv4 Address	IPv6 Address
GW1	192.168.10.3	
GW2	192.168.10.4	

Increase Priority

Decrease Priority

Add... Edit... Remove...

Where used...


OK Cancel

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 VPN Tunnel

Type:  VPN-Tunnel

Enable:

Comment:

VPN Tunnel

VPN Tunnel ID:

Peer:

VPN Tunnel Type

Numbered
 Unnumbered

Local Address:

Remote Address:

Physical device:

Add Destination Route ✕

Destination:

Subnet mask:

Next Hop Type:

Normal: Accept and forward packets.

Reject: Drop packets, and send *unreachable* messages.

Black Hole: Drop packets, but don't send *unreachable* messages.

Rank:

Local Scope:

Comment:

Add Gateway

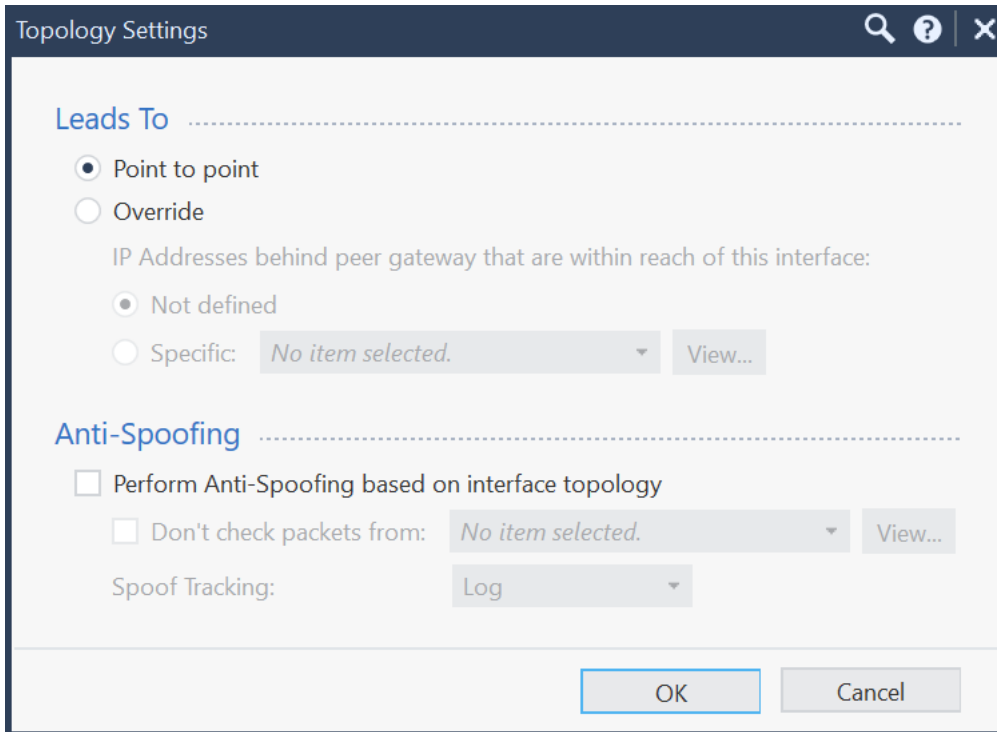
Ping:

Gateway	Priority ▲	Monitored Addresses
vpnt1	None	None

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

IPv4 Static Routes

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	



Topology Settings

Leads To

Point to point
 Override

IP Addresses behind peer gateway that are within reach of this interface:

Not defined
 Specific: *No item selected.* View...

Anti-Spoofing

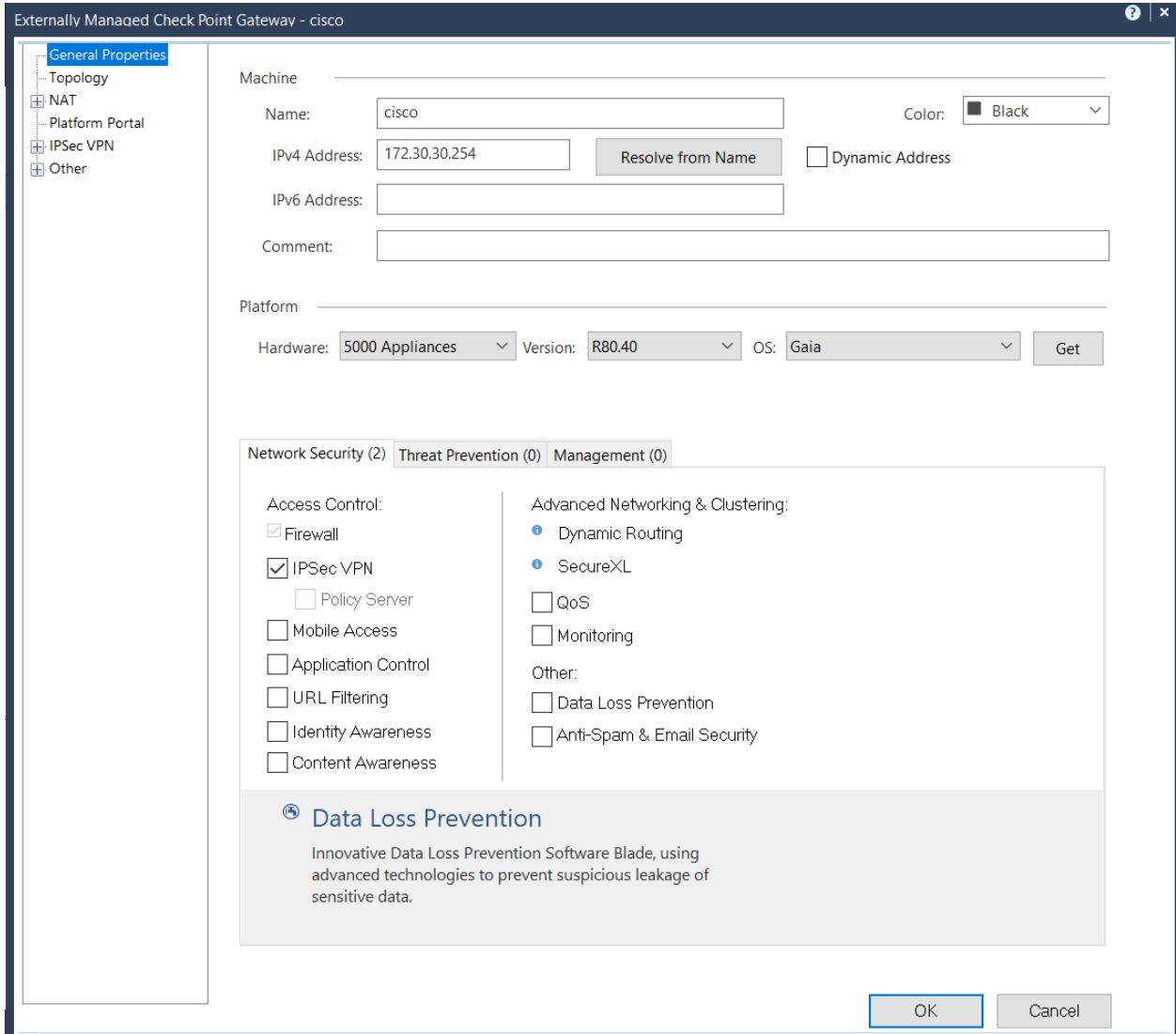
Perform Anti-Spoofing based on interface topology

Don't check packets from: *No item selected.* View...

Spoof Tracking: *Log*

OK Cancel

Set the interface topology this way in SmartConsole



Externally Managed Check Point Gateway - cisco

General Properties

- Topology
- NAT
- Platform Portal
- IPSec VPN
- Other

Machine

Name: Color:

IPv4 Address: Dynamic Address

IPv6 Address:

Comment:

Platform

Hardware: Version: OS:

Network Security (2) Threat Prevention (0) Management (0)

Access Control:

- Firewall
- IPSec VPN
 - Policy Server
- Mobile Access
- Application Control
- URL Filtering
- Identity Awareness
- Content Awareness

Advanced Networking & Clustering:

- Dynamic Routing
- SecureXL
- QoS
- Monitoring

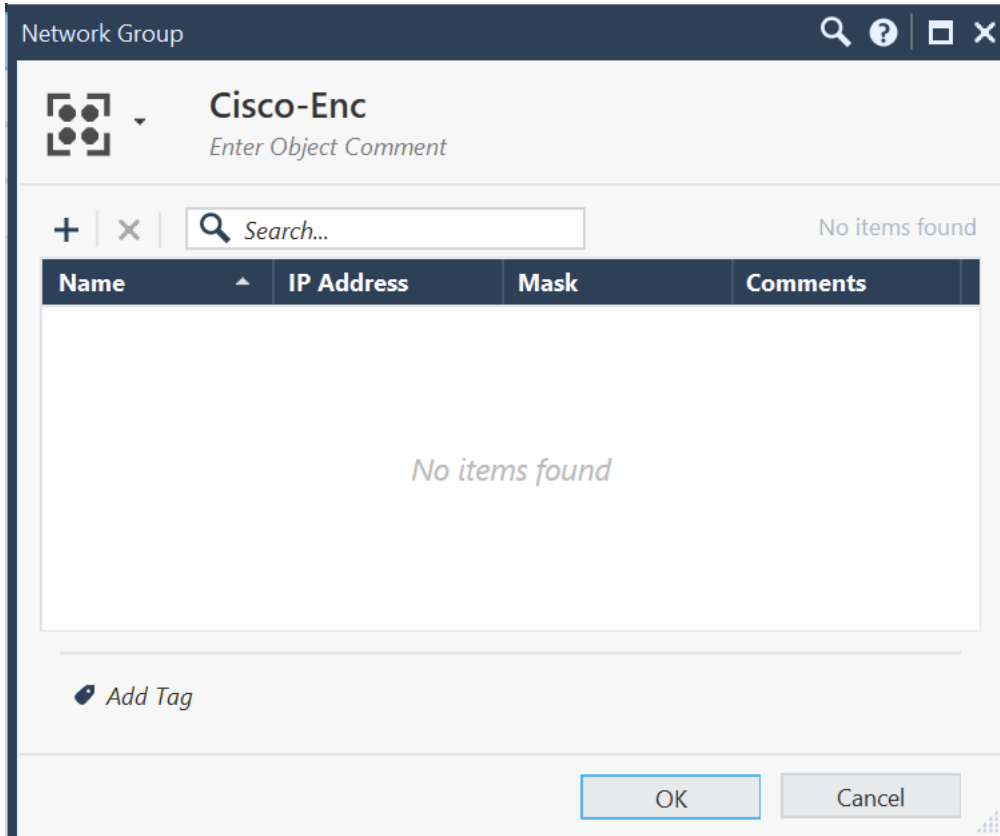
Other:

- Data Loss Prevention
- Anti-Spam & Email Security

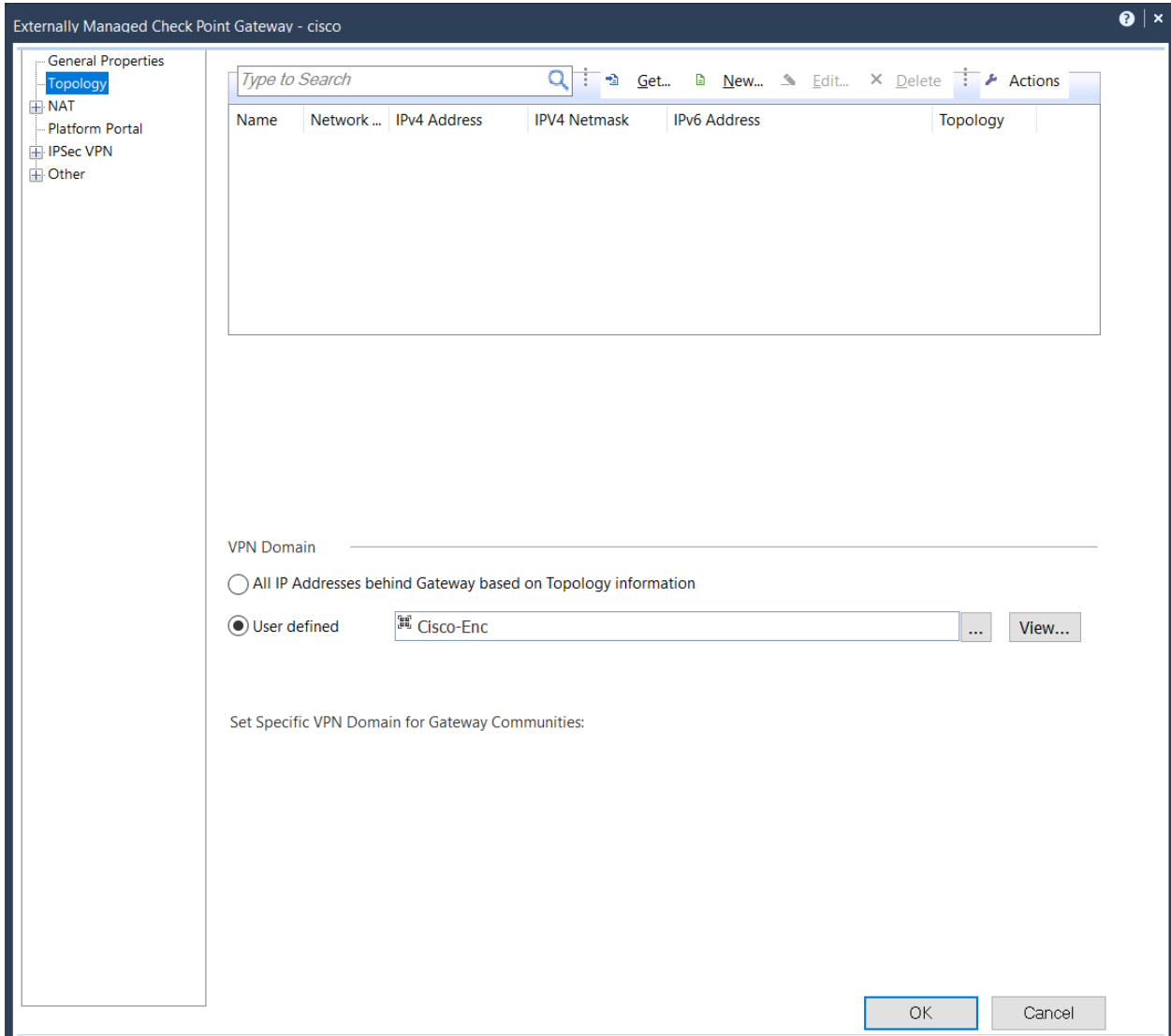
Data Loss Prevention

Innovative Data Loss Prevention Software Blade, using advanced technologies to prevent suspicious leakage of sensitive data.

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.

Star Community
🔍 ? ✕

My-Center

Enter Object Comment

«

- Gateways
- Encrypted Traffic
- Encryption
- Tunnel Management
- VPN Routing
- MEP
- Excluded Services
- Shared Secret
- Wire Mode
- Advanced

Center Gateways

All the connections between the Gateways below and the Satellite Gateways will be encrypted.

+ ✕ 🔍 Search... 1 item

Gateway	Gateway Comments	VPN Domain
📡 cisco		📡 Cisco-Enc

Mesh center gateways

Satellite Gateways

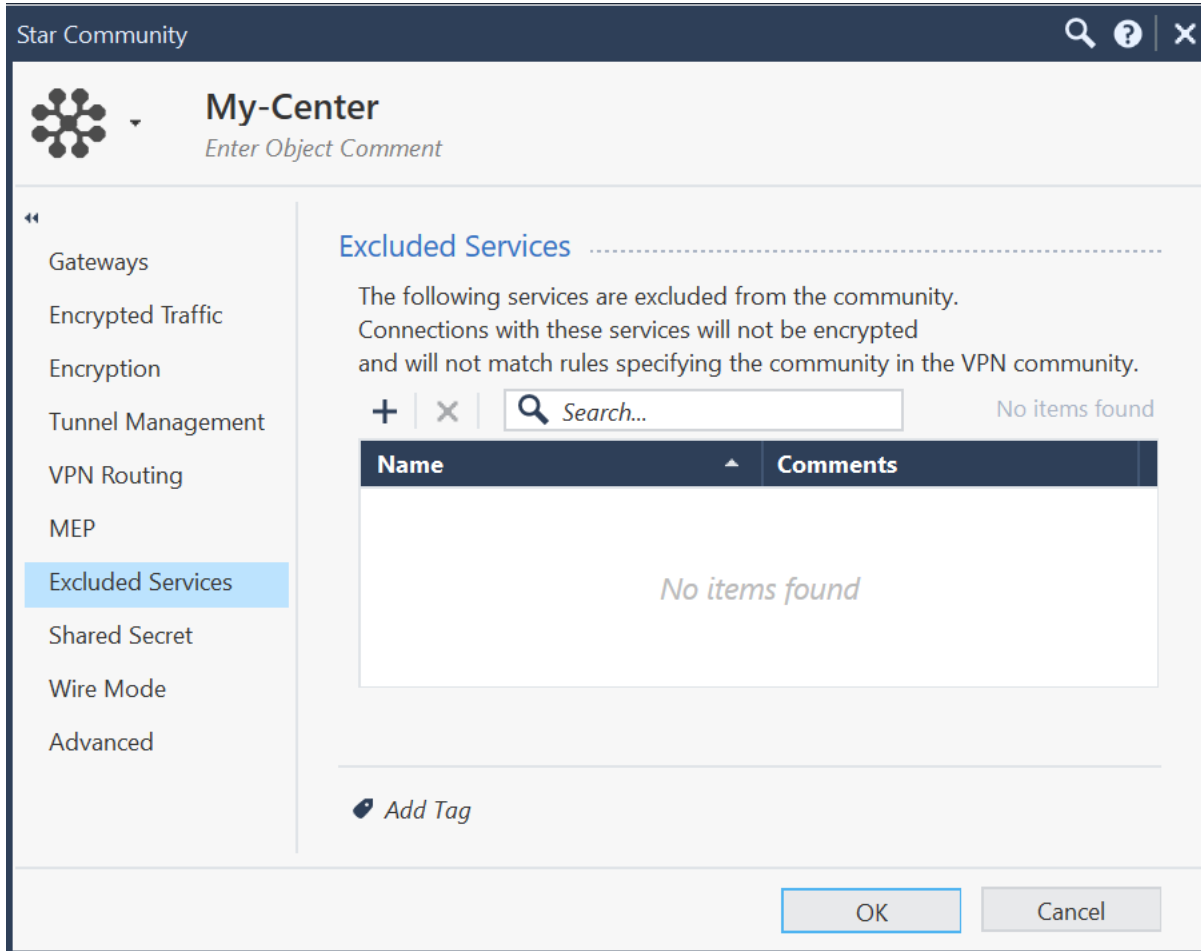
All the connections between the Gateways below and the Center Gateways will be encrypted.

+ ✕ 🔍 Search... 1 item

Gateway	Gateway Comments	VPN Domain
📡 GW-Cluster		👤 Net_192.168.10.X

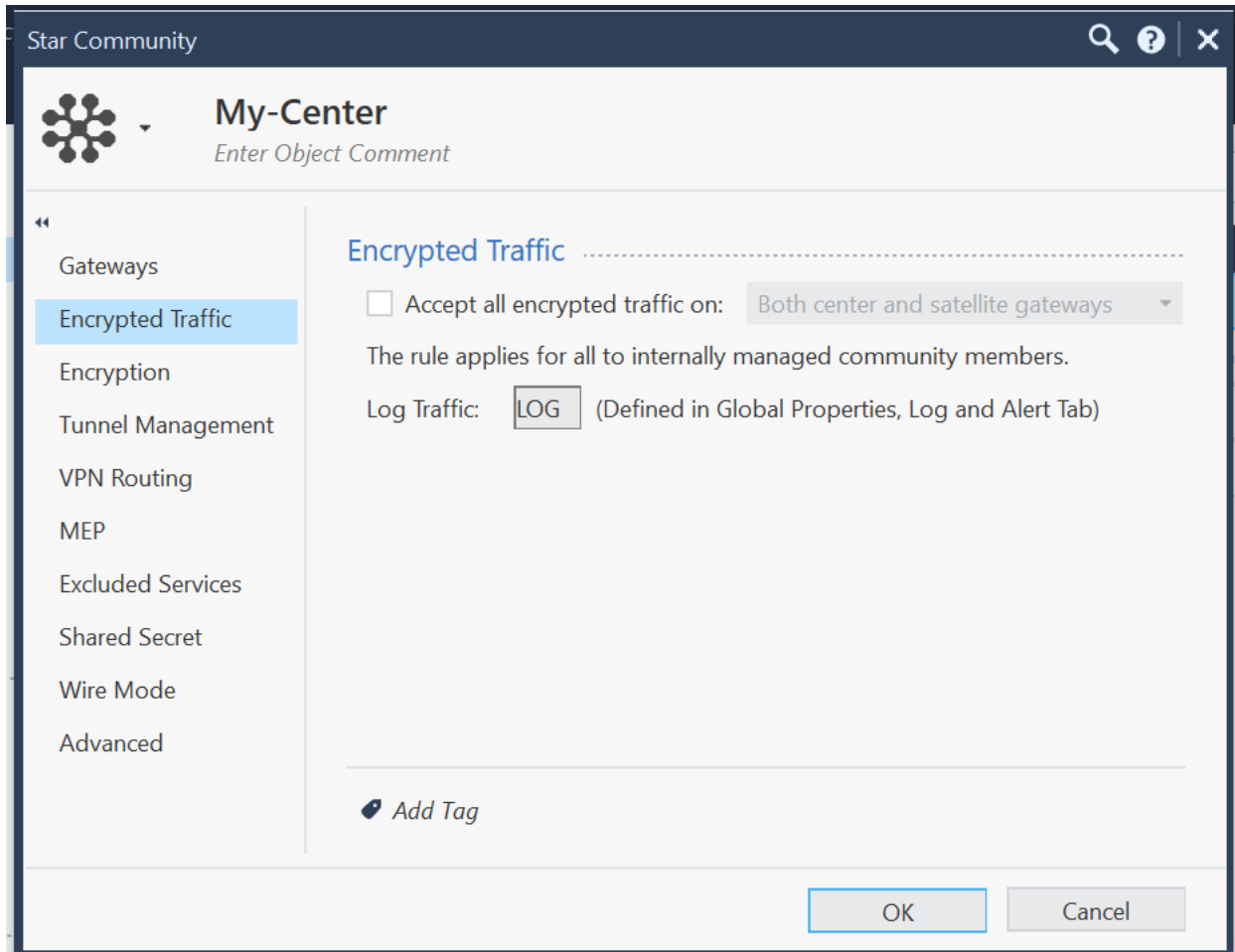
🏷️ Add Tag

OK
Cancel



The screenshot shows a configuration window titled "Star Community" with a "My-Center" header and the instruction "Enter Object Comment". A left-hand navigation menu lists various settings: Gateways, Encrypted Traffic, Encryption, Tunnel Management, VPN Routing, MEP, Excluded Services (highlighted), Shared Secret, Wire Mode, and Advanced. The main content area is titled "Excluded Services" and contains the following text: "The following services are excluded from the community. Connections with these services will not be encrypted and will not match rules specifying the community in the VPN community." Below this text is a search bar with a plus icon, a close icon, and a search input field containing "Search...". To the right of the search bar, it says "No items found". Below the search bar is a table with two columns: "Name" and "Comments". The table is currently empty, displaying "No items found" in the center. At the bottom left of the main area is an "Add Tag" button with a tag icon. At the bottom right of the window are "OK" and "Cancel" buttons.

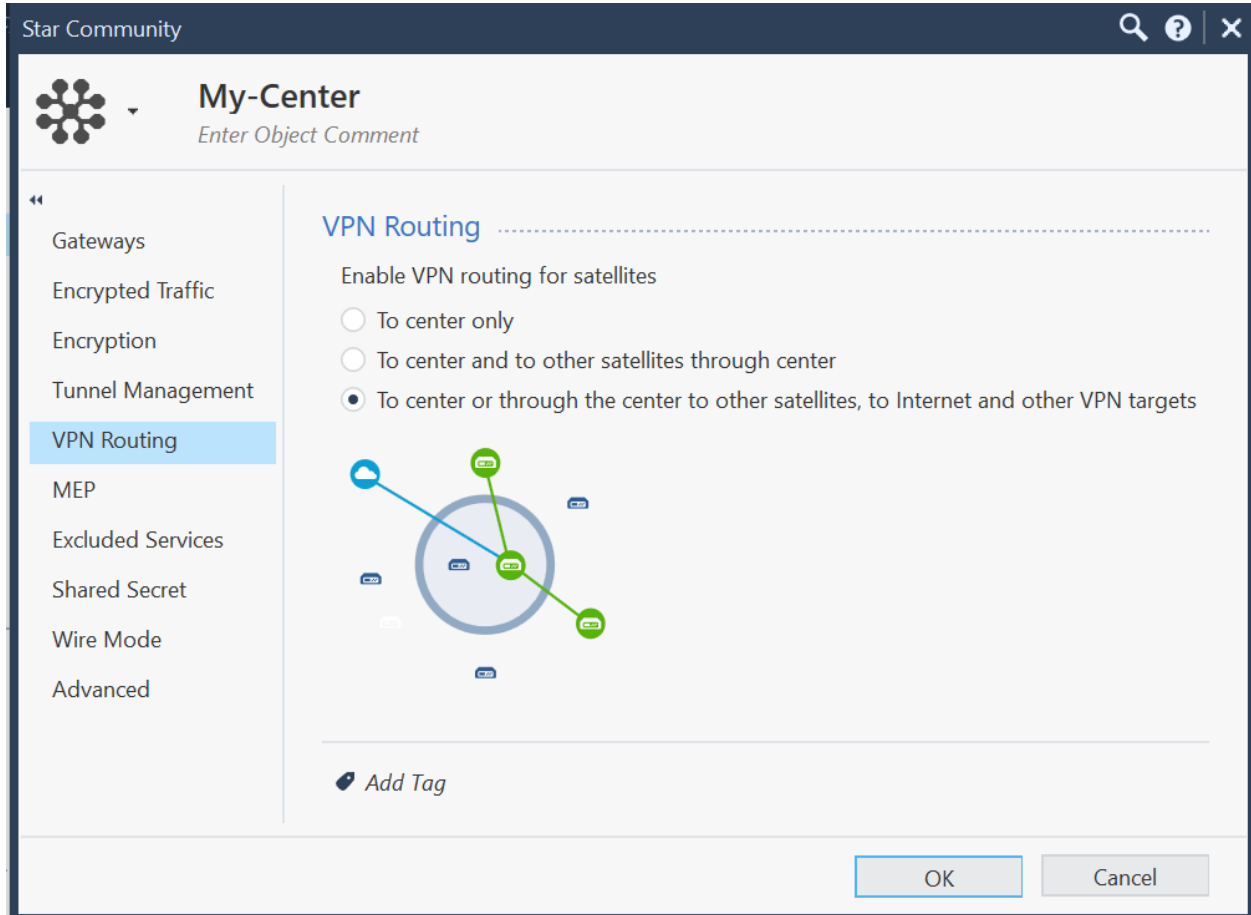
Now Let's define the community we are using.



The screenshot shows a configuration window titled "Star Community" with a search icon, help icon, and close icon in the top right. The main header is "My-Center" with a sub-header "Enter Object Comment". A left sidebar contains a list of menu items: Gateways, Encrypted Traffic (highlighted), Encryption, Tunnel Management, VPN Routing, MEP, Excluded Services, Shared Secret, Wire Mode, and Advanced. The main content area is titled "Encrypted Traffic" and contains the following settings:

- Accept all encrypted traffic on: **Both center and satellite gateways** (dropdown menu)
- The rule applies for all to internally managed community members.
- Log Traffic: **LOG** (Defined in Global Properties, Log and Alert Tab)

At the bottom left of the main content area, there is an "Add Tag" button with a tag icon. At the bottom right, there are "OK" and "Cancel" buttons.

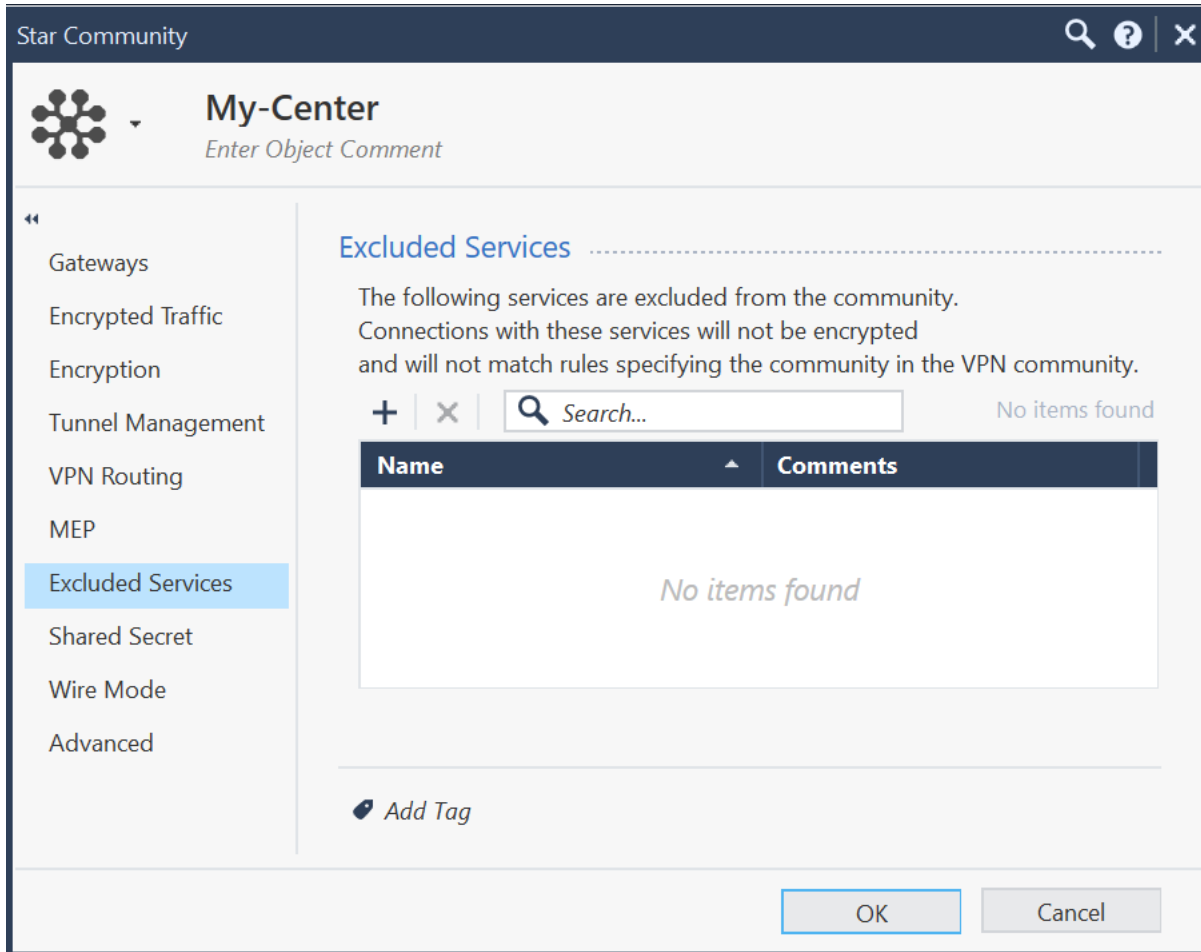


The screenshot shows the 'My-Center' configuration window in the Star Community interface. The window title is 'Star Community' and the main title is 'My-Center' with a subtitle 'Enter Object Comment'. A left-hand navigation menu lists various settings: Gateways, Encrypted Traffic, Encryption, Tunnel Management, VPN Routing (highlighted), MEP, Excluded Services, Shared Secret, Wire Mode, and Advanced. The main content area is titled 'VPN Routing' and contains the following options:

- Enable VPN routing for satellites
 - To center only
 - To center and to other satellites through center
 - To center or through the center to other satellites, to Internet and other VPN targets

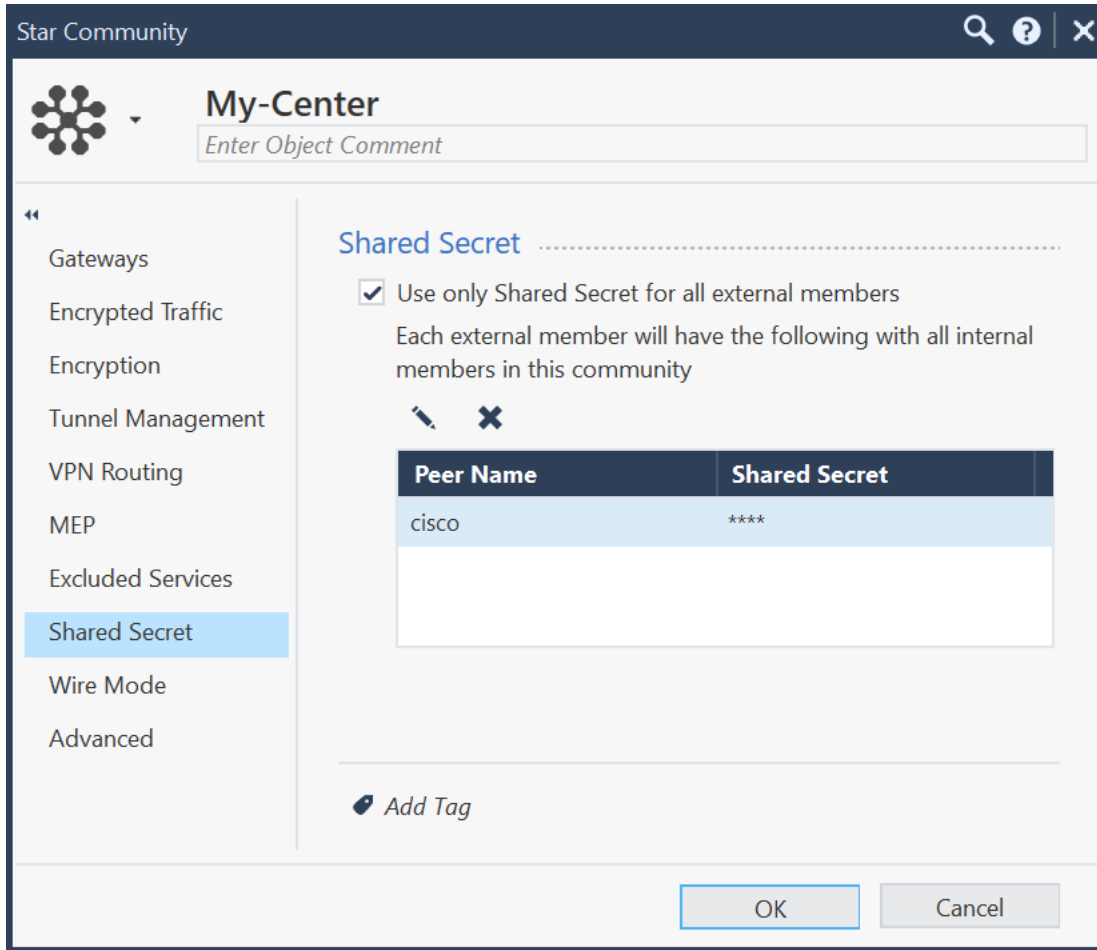
Below the radio buttons is a network diagram showing a central hub (a large blue circle) connected to several satellite nodes (smaller green circles). A blue line connects the central hub to a cloud icon representing the Internet. Below the diagram is an 'Add Tag' button. At the bottom right of the window are 'OK' and 'Cancel' buttons.

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.



The screenshot shows a window titled "Star Community" with a search icon, help icon, and close icon in the top right. The main content area is titled "My-Center" with a sub-header "Enter Object Comment". A left-hand navigation menu lists several options: Gateways, Encrypted Traffic, Encryption, Tunnel Management, VPN Routing, MEP, Excluded Services (highlighted in blue), Shared Secret, Wire Mode, and Advanced. The main area is titled "Excluded Services" and contains the following text: "The following services are excluded from the community. Connections with these services will not be encrypted and will not match rules specifying the community in the VPN community." Below this text is a search bar with a magnifying glass icon and the text "Search...". To the right of the search bar, it says "No items found". Below the search bar is a table with two columns: "Name" and "Comments". The table is currently empty, and the text "No items found" is centered in the table area. At the bottom left of the main area, there is a button labeled "Add Tag" with a tag icon. At the bottom right of the window, there are two buttons: "OK" and "Cancel".

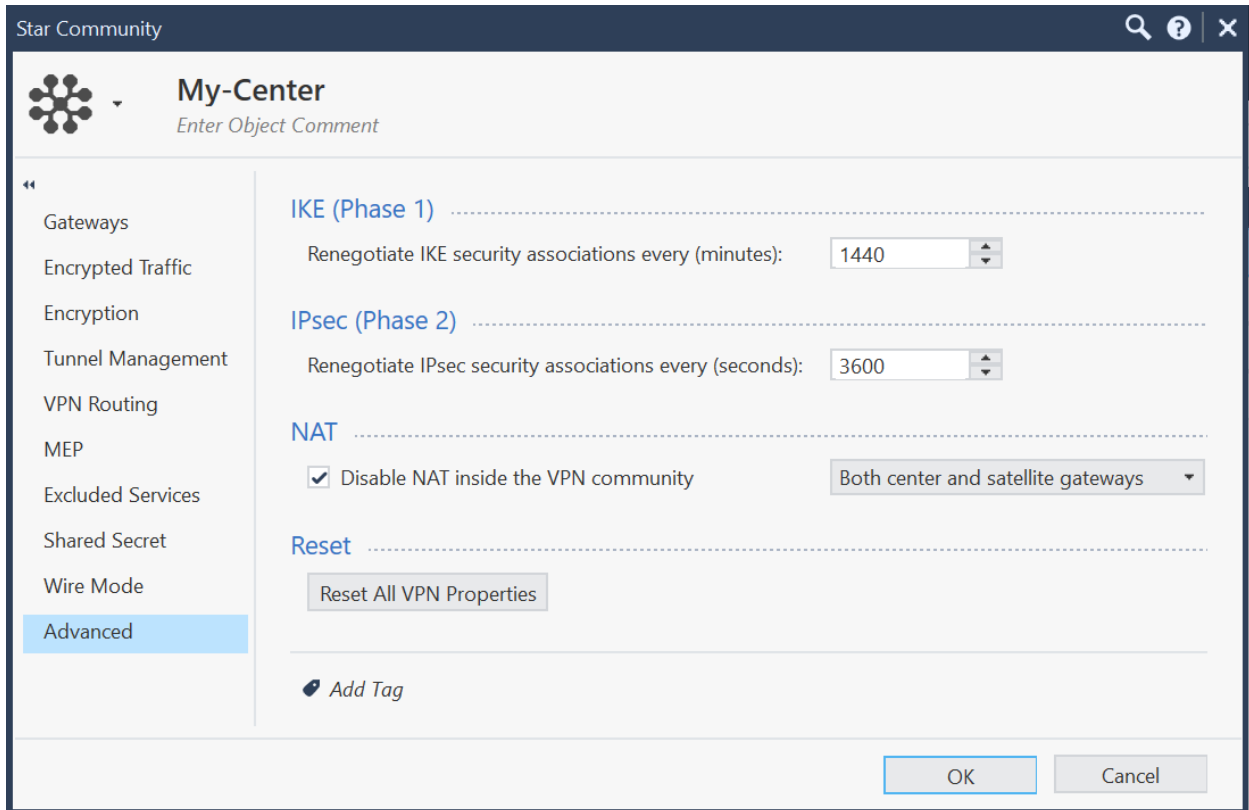
Exclude any services necessary



The screenshot shows the 'Star Community' interface with the 'My-Center' tab selected. The left sidebar contains a navigation menu with the following items: Gateways, Encrypted Traffic, Encryption, Tunnel Management, VPN Routing, MEP, Excluded Services, Shared Secret (highlighted), Wire Mode, and Advanced. The main content area is titled 'Shared Secret' and includes a checkbox labeled 'Use only Shared Secret for all external members' which is checked. Below this, a text description states: 'Each external member will have the following with all internal members in this community'. There are edit and delete icons above a table. The table has two columns: 'Peer Name' and 'Shared Secret'. The first row contains 'cisco' and '****'. Below the table is an 'Add Tag' button. At the bottom right of the window are 'OK' and 'Cancel' buttons.

Peer Name	Shared Secret
cisco	****

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.