Configuring Check Point Security Gateway with VPN

Version 1.0

Dokument Name: Configuring Check Point Security Gateway with VPN

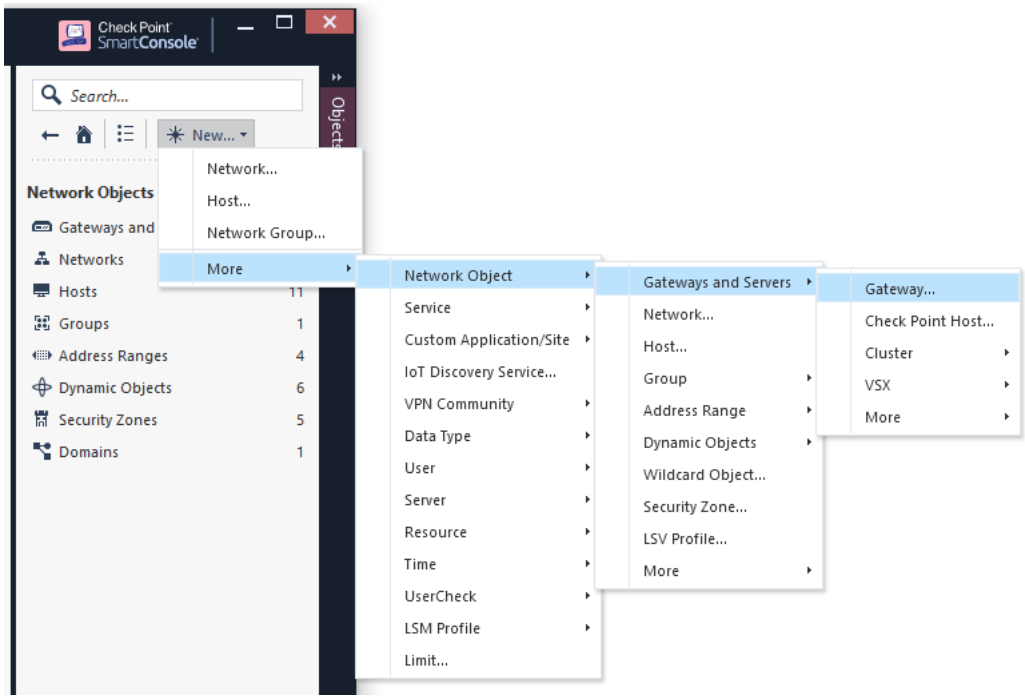
Dokumentenkontrolle

Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
1.0	10.07.2024				

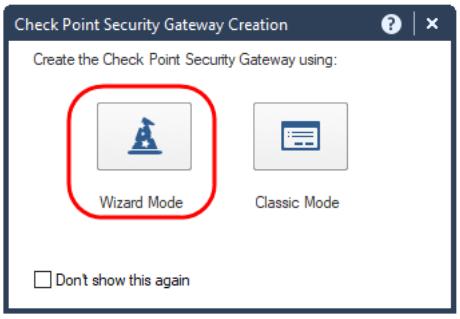
NetWyl Informatik GmbH
Täschmattstrasse 19
6015 Luzern
info@netwyl-informatik.ch
Phone: +41 41 520 73 90

Note: If you have a fresh installed Check Point Gateway that is also defined as Security Management server and should be used as a VPN Gateway, start from step 6.
In most cases this Gateway has the icon and is named "gw-".
To create Check Point Security Gateway:

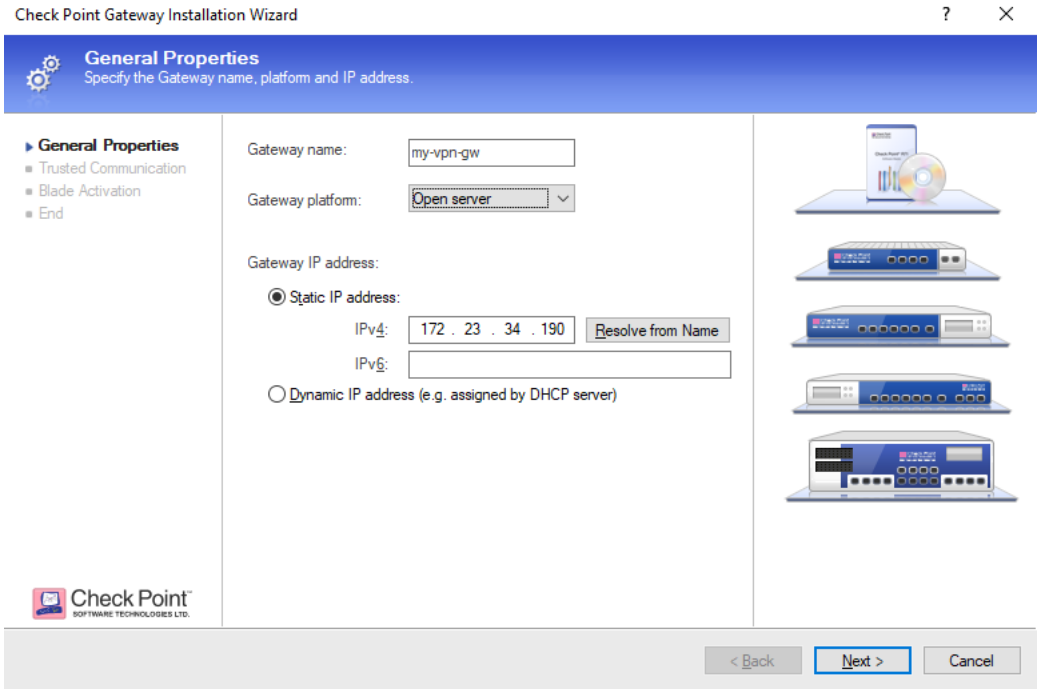
1. Click * New, go to More ->Network Object -> Gateways and Servers -> Gateway:



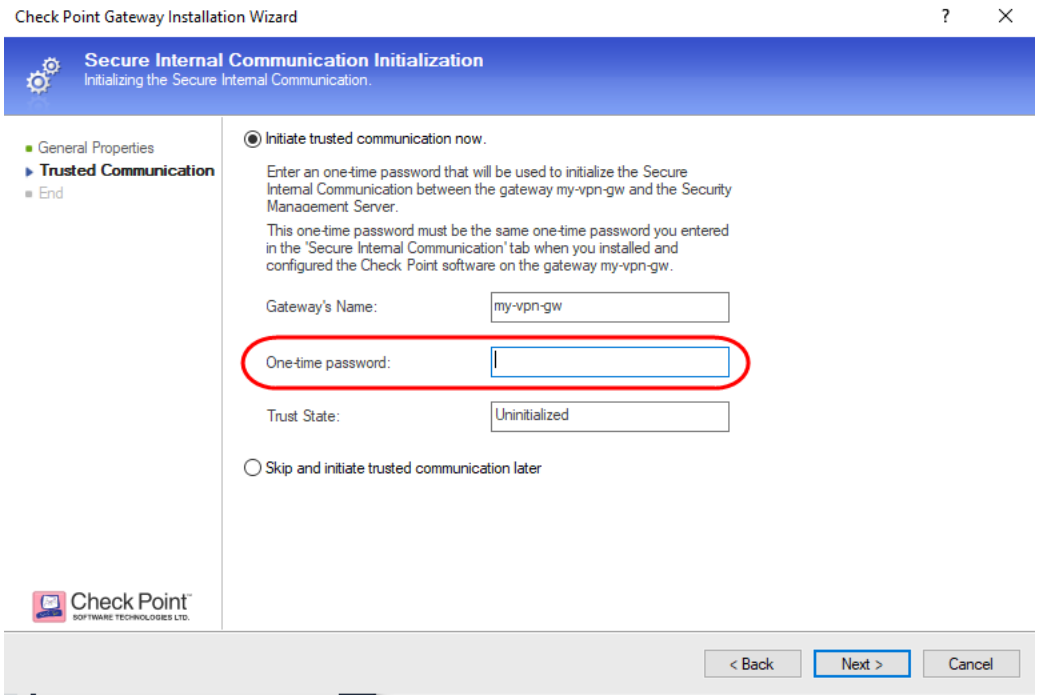
2. Click Wizard Mode



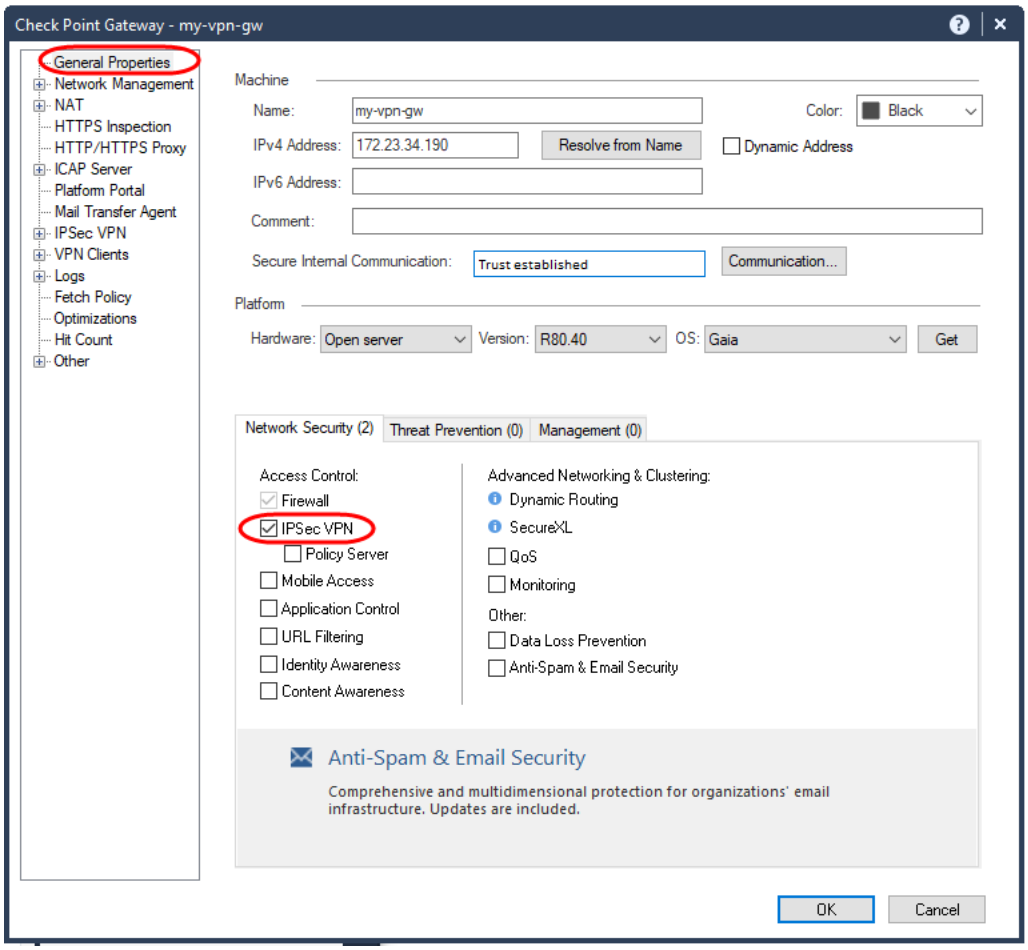
3. Enter
4. Gateway name
5. Gateway platform
6. IP address



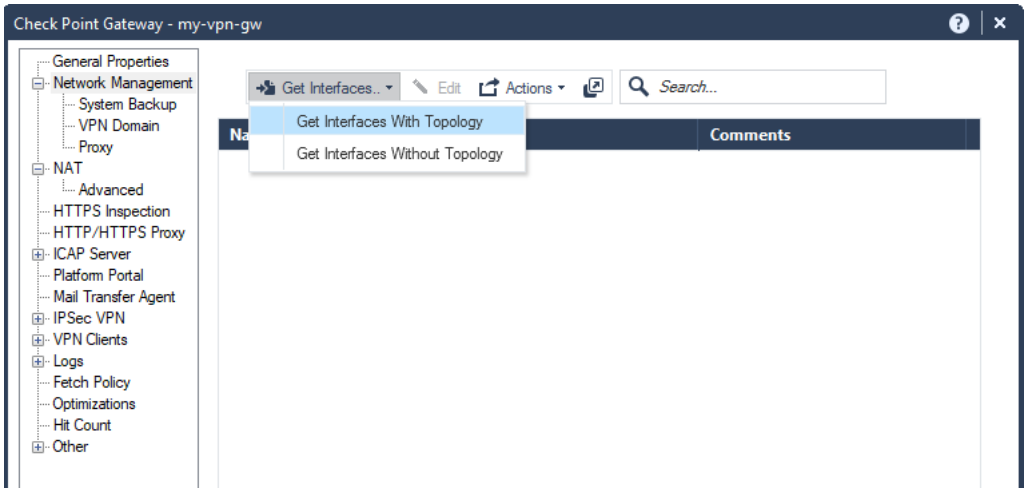
7. Click Next and enter the one-time password as defined on Check Point Security Gateway during installation.



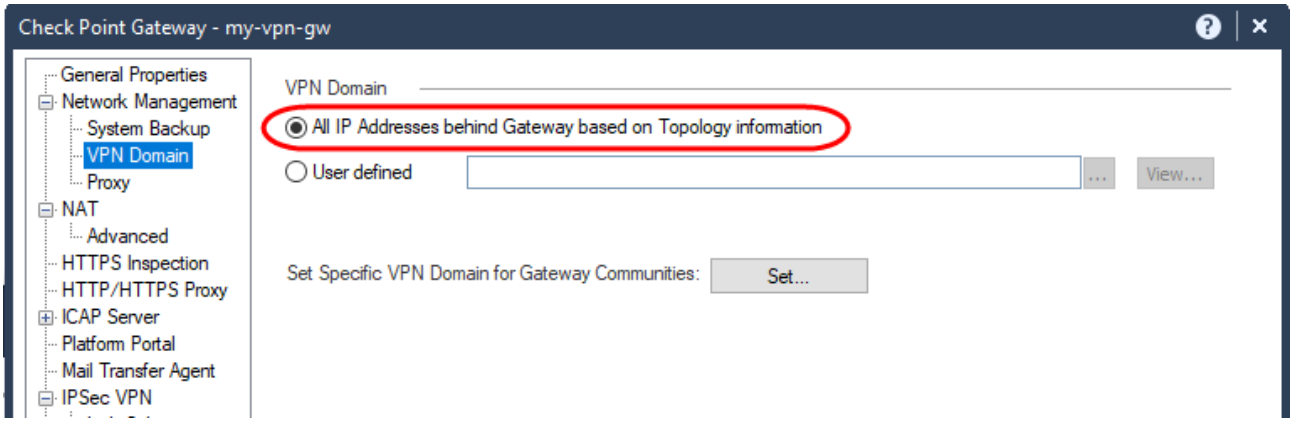
8. Click Next after trusted communication established, then click Finish.
9. In the General Properties window of your Security Gateway, make sure the 'IPSec VPN' checkbox is selected.



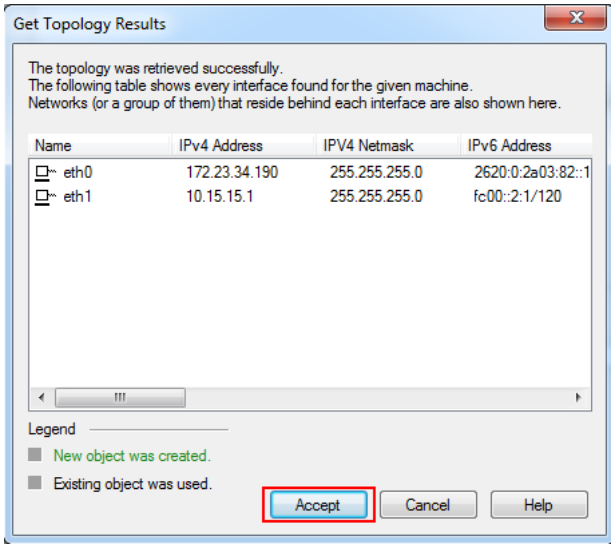
10. Define VPN encryption domain for your Gateway. Make sure that you have at least one internal and one external interfaces.



VPN encryption domain will be defined to all networks behind internal interface.



11. Click Accept

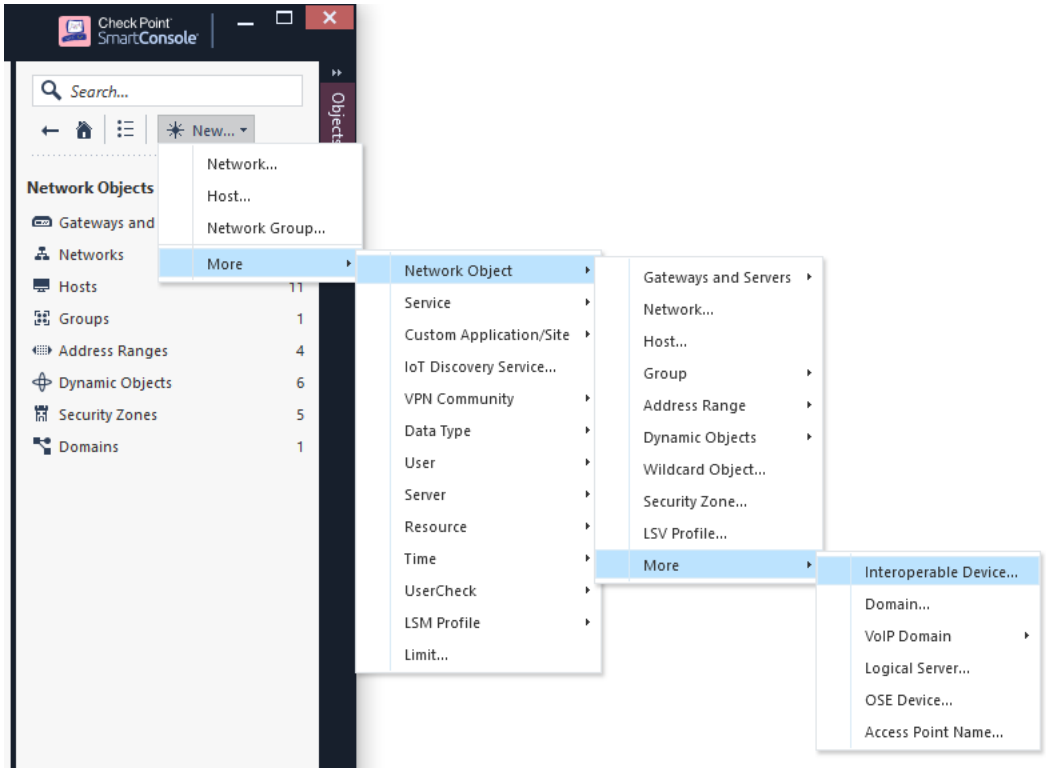


12. Click OK and close the Gateway dialog

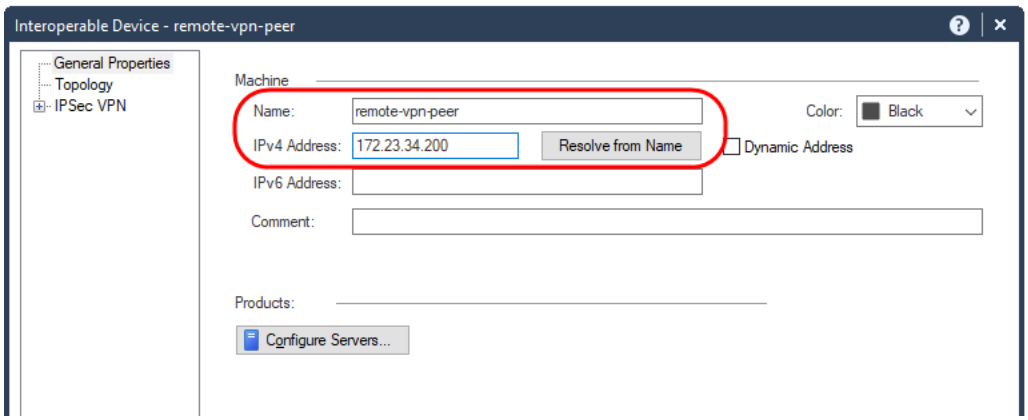
Configuring the Interoperable Device and VPN community

Create an object to represent the peer gateway.

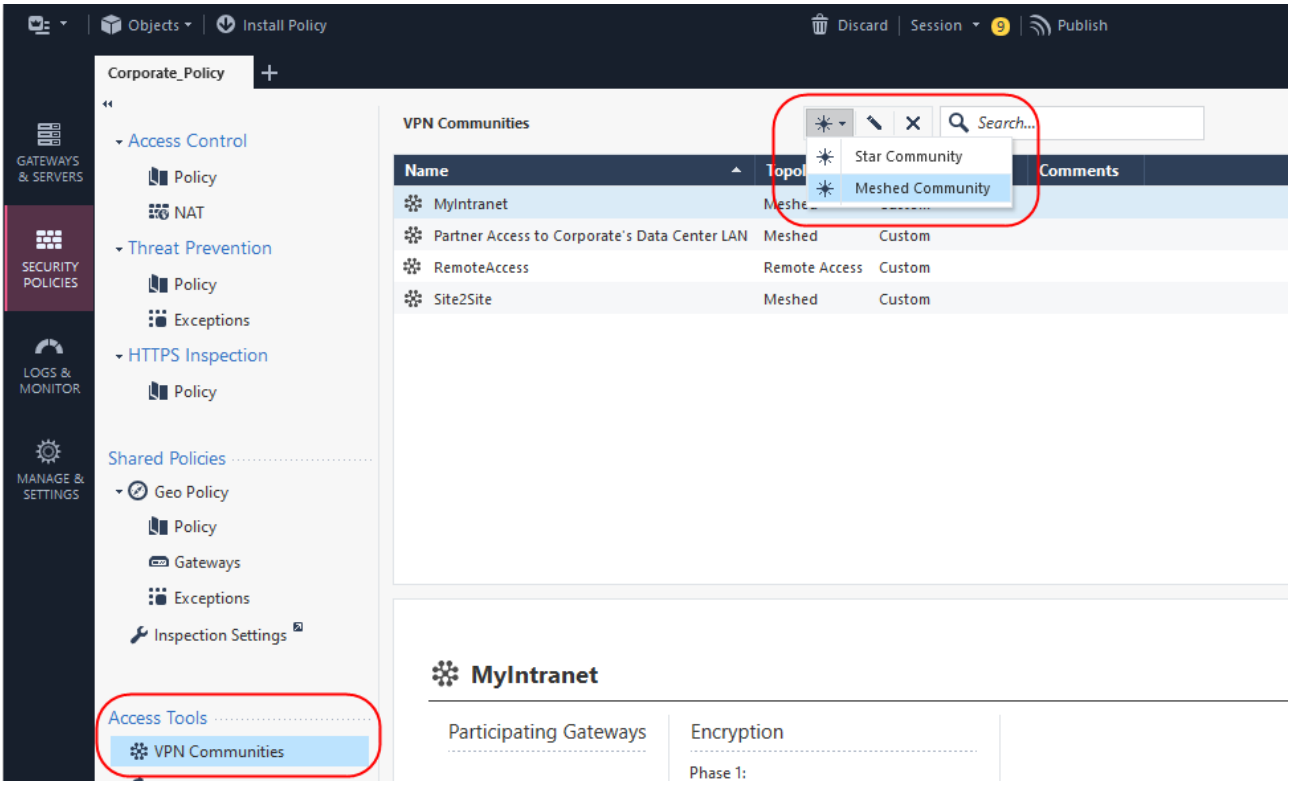
13. In New, go to Network Objects -> More -> Interoperable Device



14. Give the gateway a name, IP address, and (optional) description in the properties dialog window that is displayed and click OK.

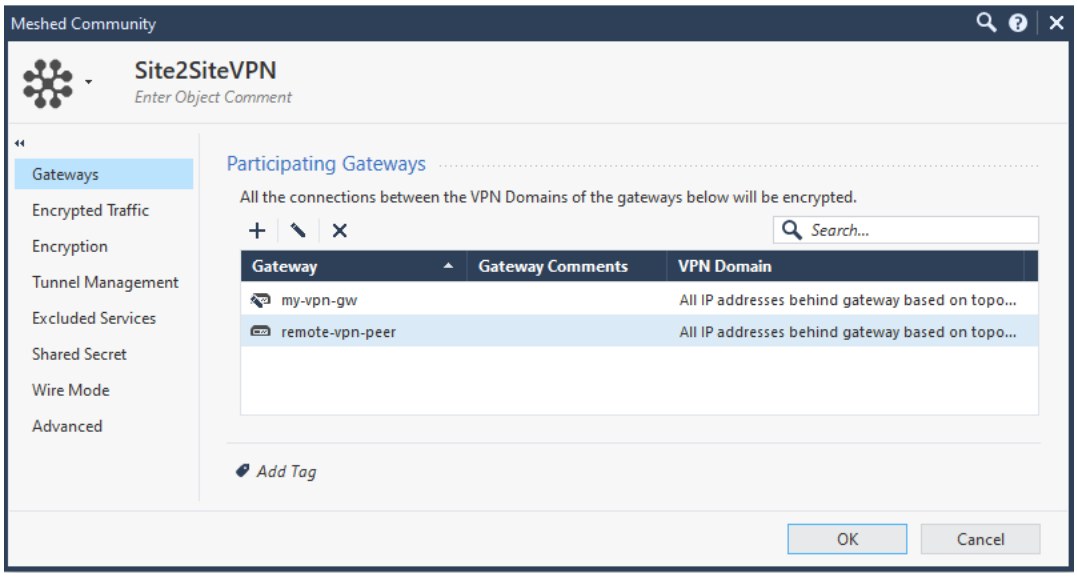


15. In Access Tools, go to VPN Communities. Click * on the top panel and select Meshed Community.

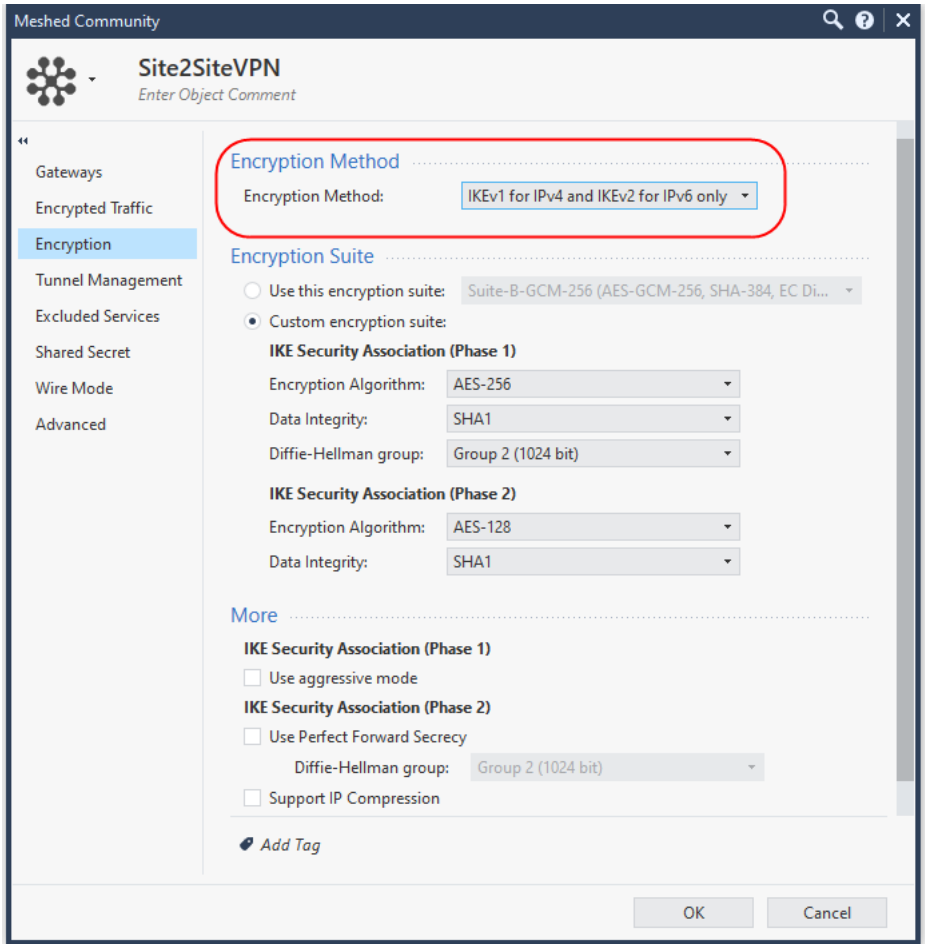


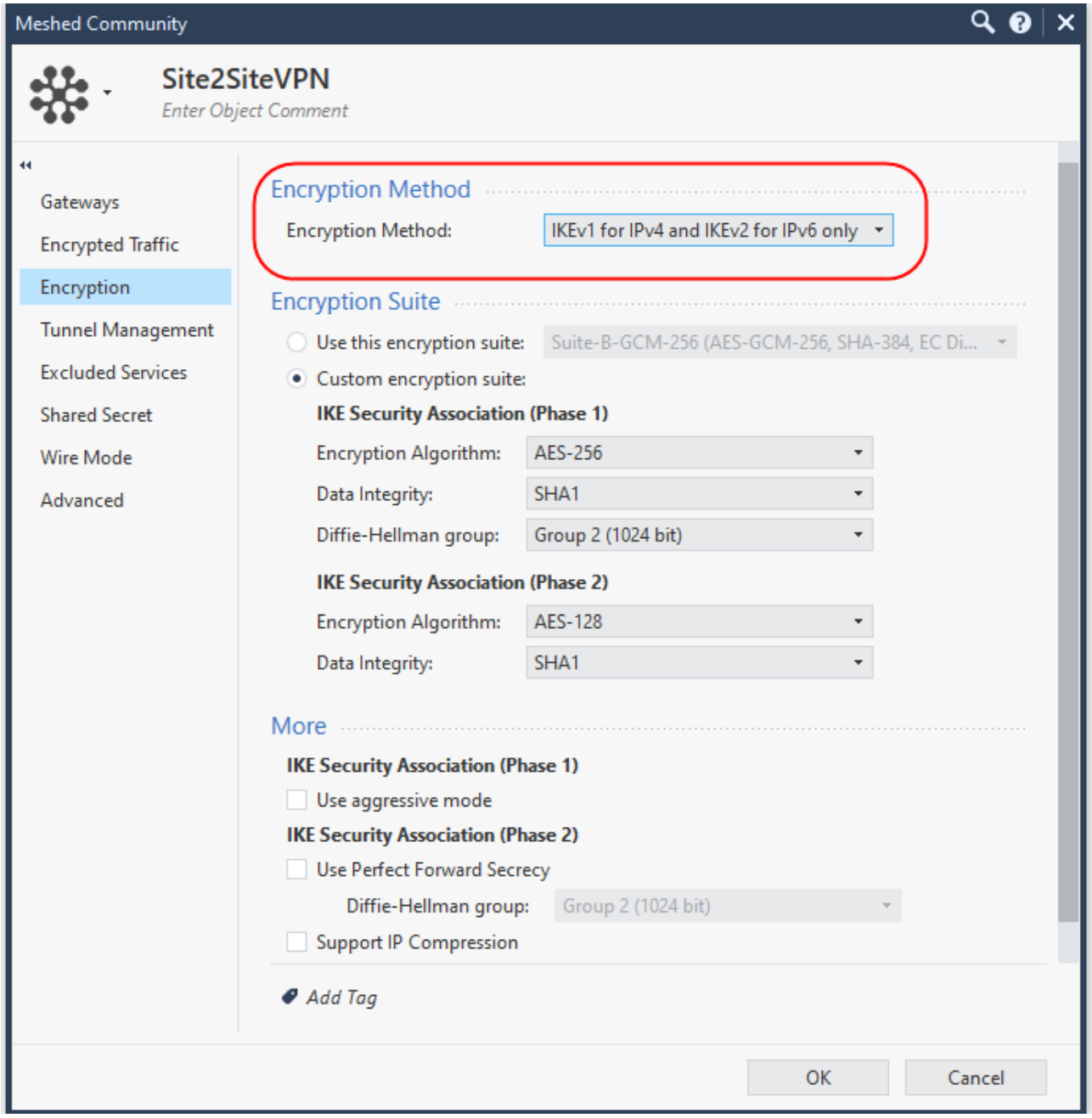
16. A Meshed Community Properties dialog pops up.
    In the General menu, enter your VPN community name

    In the Participating Gateways menu click: Add, select your both gateways objects, and click OK.



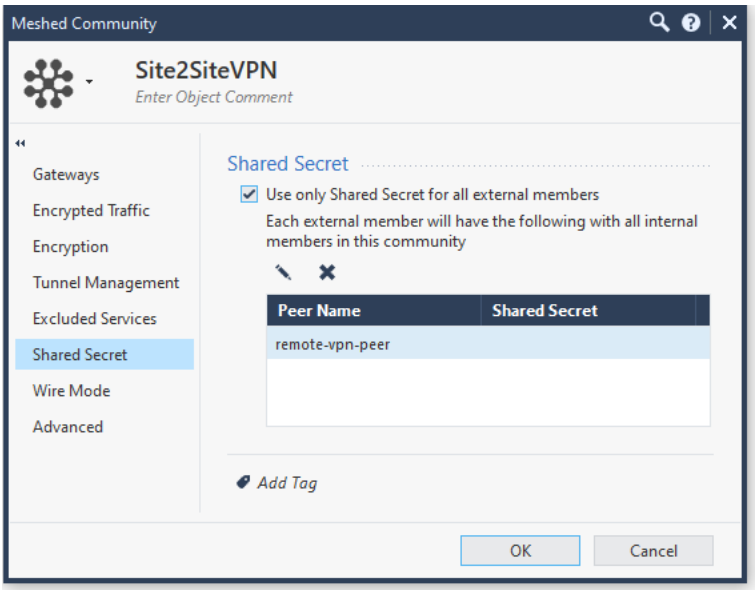
17. In the Encryption menu, you can change the Phase 1 and Phase 2 properties.
    You can also define which IKE version should be used. For IKEv1 leave the default, for IKEv2 select IKEv2 only.


Meshed Community
Site2SiteVPN
Enter Object Comment
Gateways
Encrypted Traffic
Encryption
Tunnel Management
Excluded Services
Shared Secret
Wire Mode
Advanced
Encryption Method
Encryption Method:
IKEv1 for IPv4 and IKEv2 for IPv6 only
Encryption Suite
Use this encryption suite:
Suite-B-GCM-256 (AES-GCM-256, SHA-384, EC Di...
Custom encryption suite:
IKE Security Association (Phase 1)
Encryption Algorithm:
AES-256
Data Integrity:
SHA1
Diffie-Hellman group:
Group 2 (1024 bit)
IKE Security Association (Phase 2)
Encryption Algorithm:
AES-128
Data Integrity:
SHA1
More
IKE Security Association (Phase 1)
Use aggressive mode
IKE Security Association (Phase 2)
Use Perfect Forward Secrecy
Diffie-Hellman group:
Group 2 (1024 bit)
Support IP Compression
Add Tag
OK
Cancel

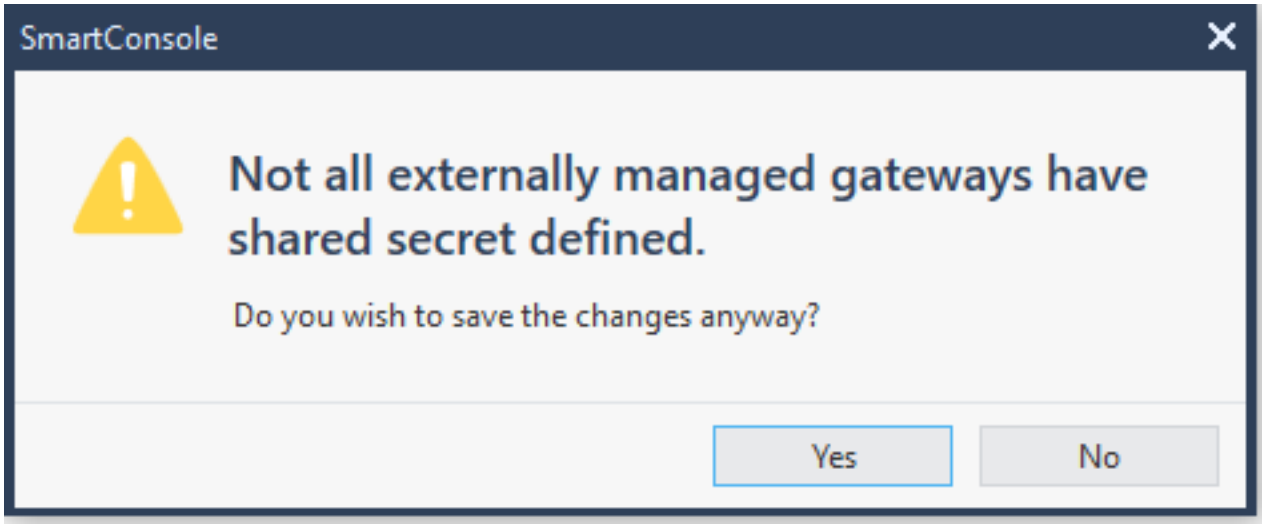


Note: Make a note of the values you select in order to set the peer to match them

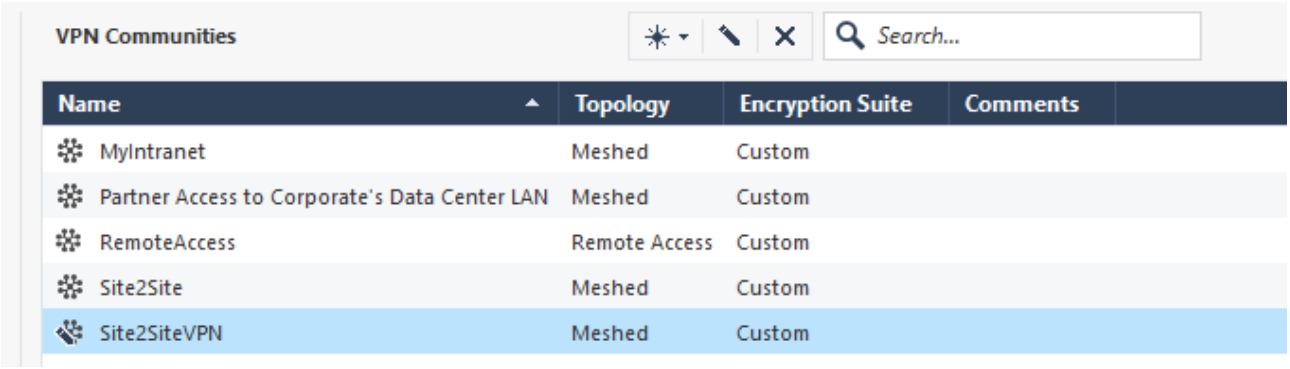
18. In the Tunnel Management menu you can define how to setup the tunnel.Note: The recommended tunnel sharing method is one VPN tunnel per subnet pair (default). This shares your network on either side of the VPN and makes the Phase 2 negotiation smooth. It also requires fewer tunnels to be built for the VPN.
    If you need to restrict access over the VPN, you can do that later through your security Rule Base.
19. For preshered authentication, expand the Advanced Settings menu and select: Shared Secret.
    Select the 'Use only Shared Secret for all External members' checkbox.
    Select your peer gateway from the entries in the list below and click Edit to edit the shared secret.Note: remember this secret, as your peer will need it to set up the VPN on the other end.



20. Expand the Advanced Settings menu and select: Advanced VPN Properties. Here, you can modify the more advanced settings regarding Phase 1 and 2.Note: Keep note of the values used. It is also a good idea to select:
    Disable NAT inside the VPN community so you can access resources behind your peer gateway using their real IP addresses, and vice versa.
21. Click OK on the VPN community properties dialog to exit back to the SmartDashboard. You may see the following message:



22. We are about to address the VPN domain setup in the next section, so click Yes to continue.
    Now you can see your VPN community defined:

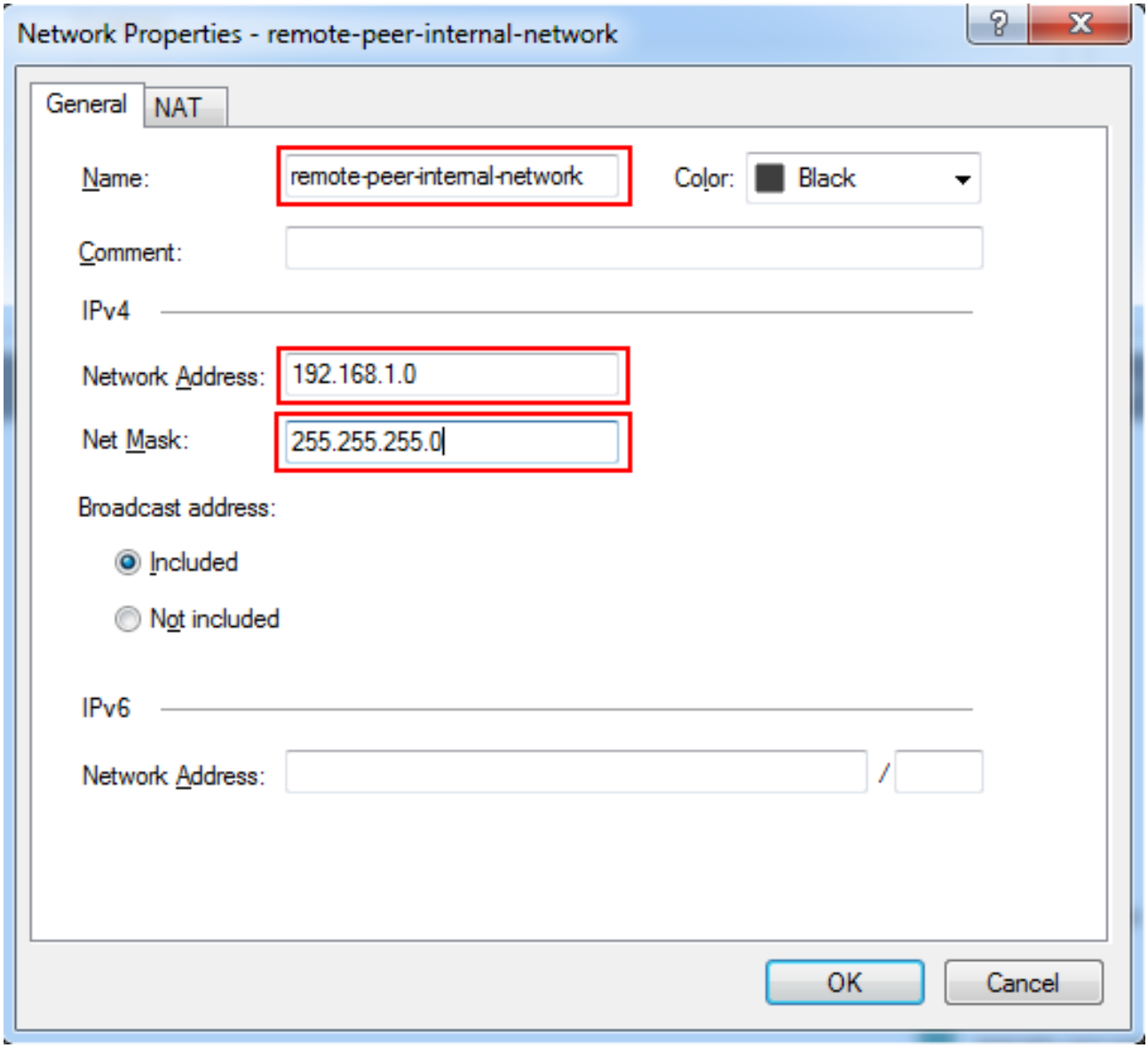


Defining VPN encryption domain for Interoperable Device

You now need to define your VPN encryption domains.
If you have not already done so, create network objects to represent your local networks and the peer networks they will be sharing with you.

To define VPN encryption domains:

23. From the Network Objects menu, right click on Networks and select Network to define a new network. In the following image, we are creating a network to represent our peer's internal network that they will be sharing with Check Point VPN gateway:

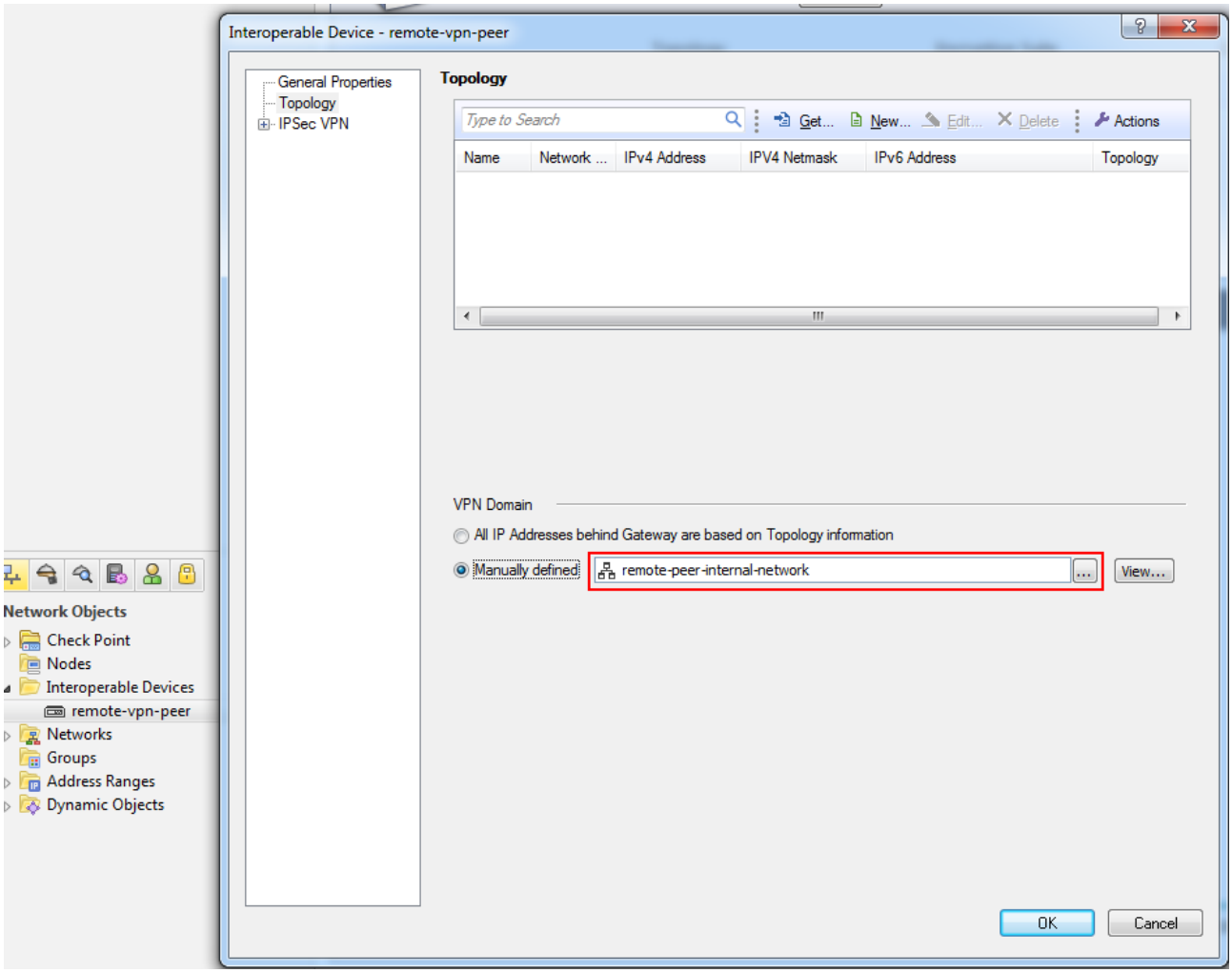


24. If you or your peer is sharing more than one network over the tunnel, create groups to represent each side's VPN domain. From the Network Objects menu, right click on Groups, select Groups and then Simple Group...In this example, only one network is shared, so the group will have only one object included, but you can put as many networks in this group as you want to share.

Note: it is important not to add groups within a group as this can impact performance. Make sure the group is "flat".

Give your group a meaningful name such as: Local_VPN_Domain.
Click OK once you have added all of your local networks and then repeat the procedure to create a group to represent your peer's shared networks.

25. Open the properties for the peer gateway and select the group/network that represents its VPN domain:



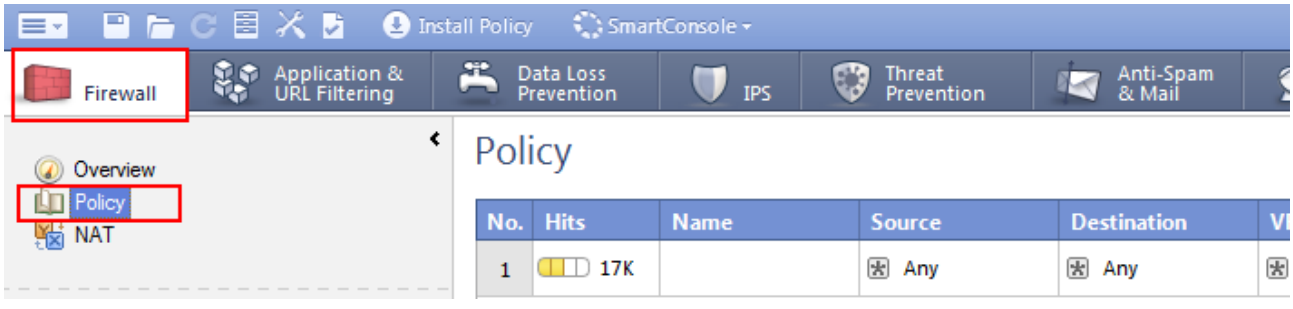
26. Click OK to complete the peer gateway configuration.

Creating a rule for the traffic

Now, you have both objects set up for VPN and you have defined your community. All that is left is to create a rule for the traffic.
Here is where you should restrict access if it is required.

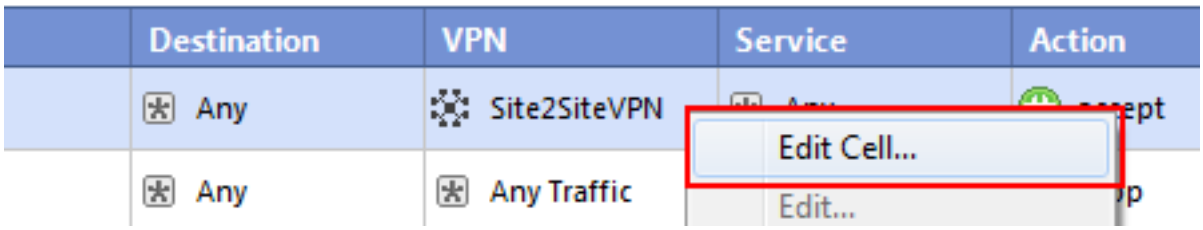
To create a rule for the traffic:

27. To allow VPN traffic, you should add the relevant rules to your Firewall Rule Base. Navigate Rule Base, Firewall -> Policy
28.

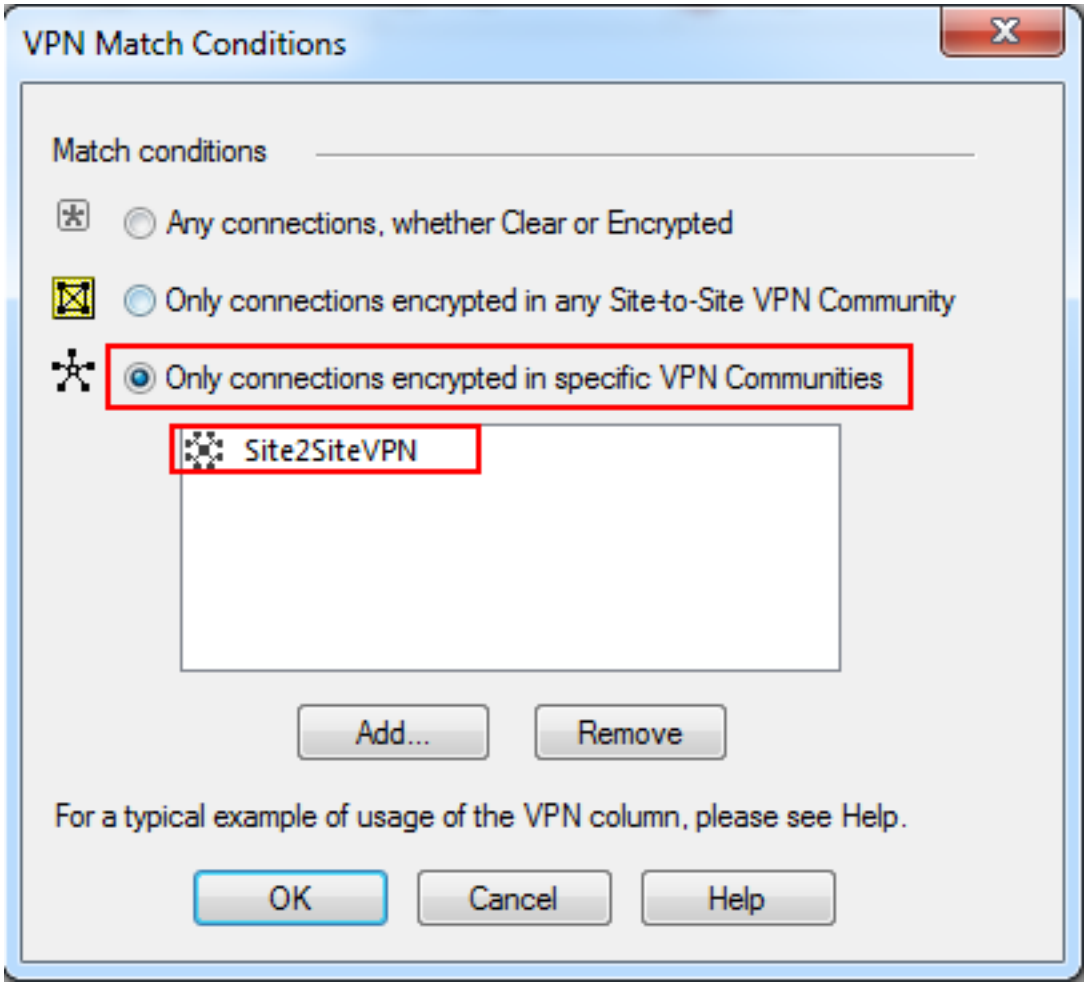


28. Decide where in your rule base you need to add your VPN access rule and right click the number on the rule just above where you want it and select: Add Rule -> Below.

29. You should explicitly set the VPN community in the VPN column on your rule, you have created before.
In the VPN column, right-click the Any Traffic icon and select: Edit Cell....



Select the: Only connections encrypted in specific VPN Communities option button and click Add.
Select the VPN community created in the above steps and click OK and then OK again.



30. In this example, we are allowing any service/any host across the tunnel in both directions. Your rule should now show the VPN community in the VPN column:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	17K	Site2Site VPN rule	Any	Any	Site2SiteVPN	Any	accept	Log	Policy Targets	Any
2	0		Any	Any	Any Traffic	Any	drop	None	Policy Targets	Any

Completing the procedure

31. Install the policy to your local Check Point gateway.
32. Once the remote side has setup their VPN to match, verify that you have secure communication with their site.

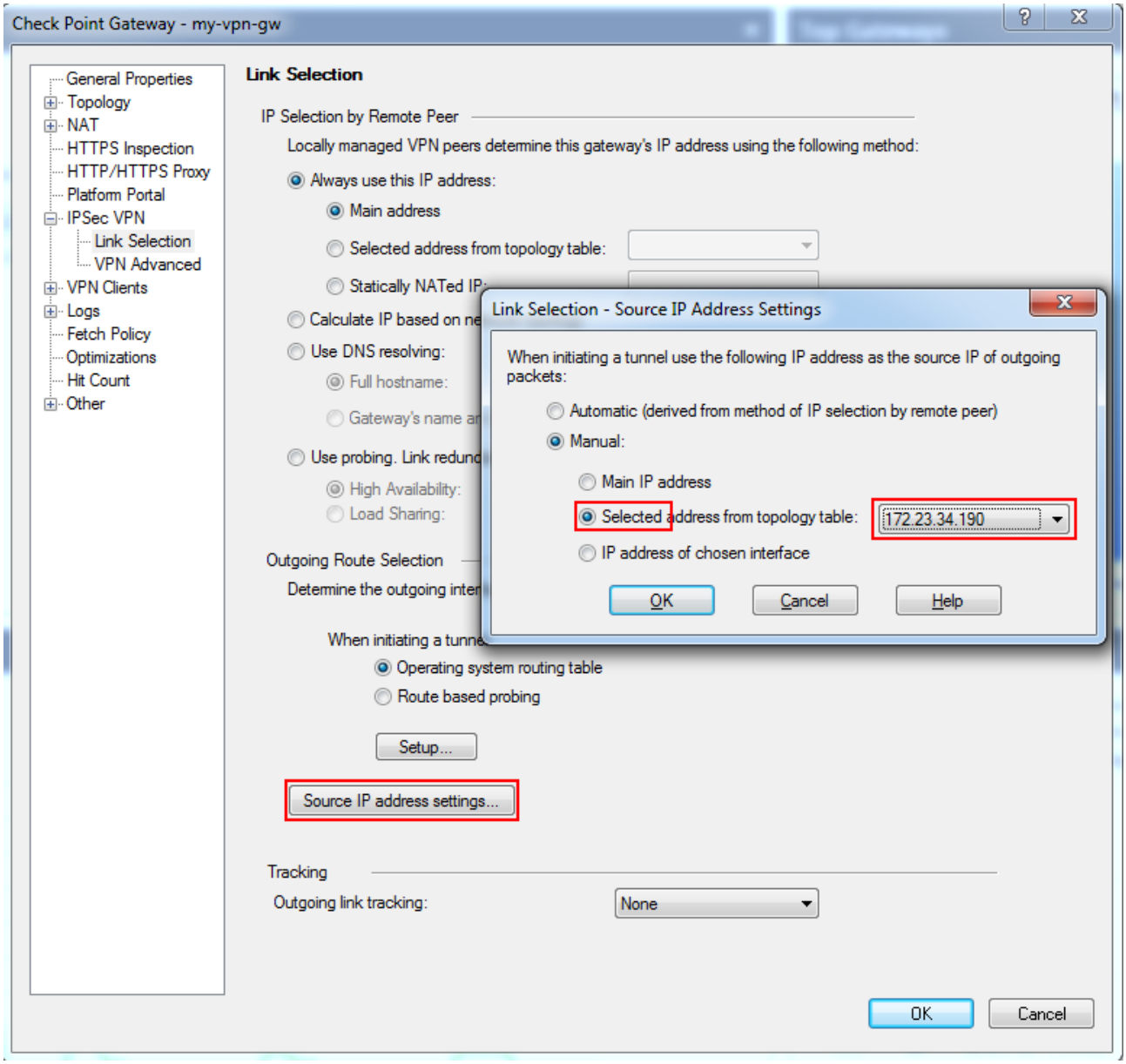
Troubleshooting

1. Problem: Traffic is dropped by 3rd party gateway and main IP configuration was defined to internal IP address for Check Point Gateway.

Generally, it is recommended to define main gateway IP address with external IP (in Check Point Gateway – General Properties). In some cases, for example: StandAlone gateway, administrator wants to define main IP address as internal IP in order to allow managing from internal network.

In this case, VPN link selection should be changed.

Open Check Point gateway properties dialog, select IPSec VPN -> Link Selection and click Source IP address settings...
In opened dialog, select Selected address from topology table and select relevant external IP address, used by remote peer



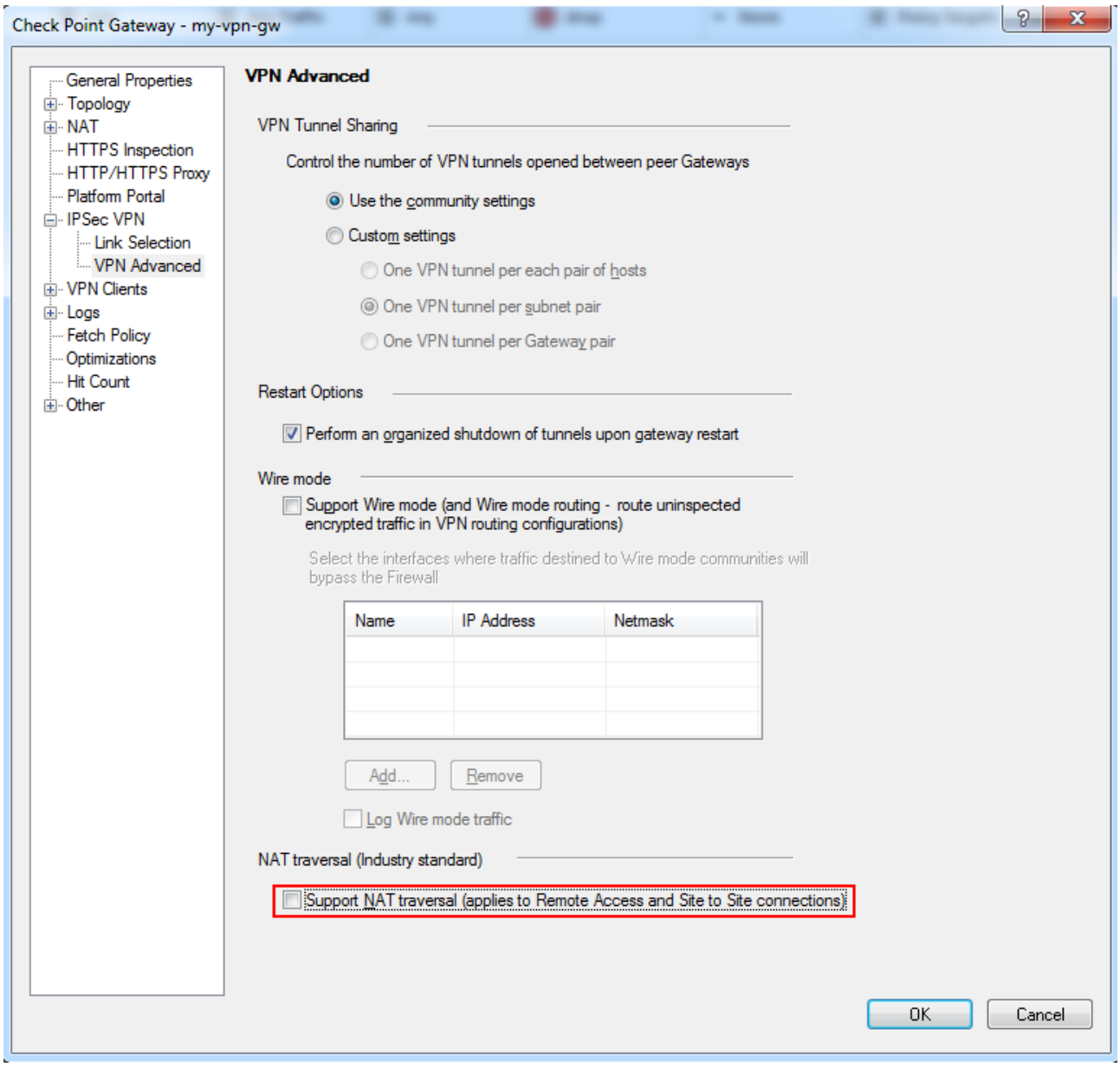
2. Problem: IKE keys were created successfully, but there is no IPsec traffic (relevant for IKEv2 only).

In some cases, remote peer chooses NAT-T encapsulation but Check Point gateway sends traffic without this encapsulation. As a result, a remote peer drops the IPsec traffic since it expecting NAT-T.

There are two workarounds available to resolve this problem:

33. If IKEv2 is required by remote peer, NAT-T should be disabled.

To do so, open Check Point gateway properties dialog, select IPSec VPN -> VPN Advanced and clear 'Support NAT traversal (applies to Remote Access and Site to Site connections)' checkbox:


Check Point Gateway - my-vpn-gw
General Properties
Topology
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Platform Portal
IPSec VPN
Link Selection
VPN Advanced
VPN Clients
Logs
Fetch Policy
Optimizations
Hit Count
Other
VPN Advanced
VPN Tunnel Sharing
Control the number of VPN tunnels opened between peer Gateways
Use the community settings
Custom settings
One VPN tunnel per each pair of hosts
One VPN tunnel per subnet pair
One VPN tunnel per Gateway pair
Restart Options
Perform an organized shutdown of tunnels upon gateway restart
Wire mode
Support Wire mode (and Wire mode routing - route uninspected encrypted traffic in VPN routing configurations)
Select the interfaces where traffic destined to Wire mode communities will bypass the Firewall
Name
IP Address
Netmask
Add...
Remove
Log Wire mode traffic
NAT traversal (Industry standard)
Support NAT traversal (applies to Remote Access and Site to Site connections)
OK
Cancel