How To Setup a Site-to-Site VPN with Cisco Remote Gateway

26 April 2011

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=11892

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

Date	Description
26 April 2011	First release of this document

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Setup a Site-to-Site VPN with Cisco Remote Gateway).

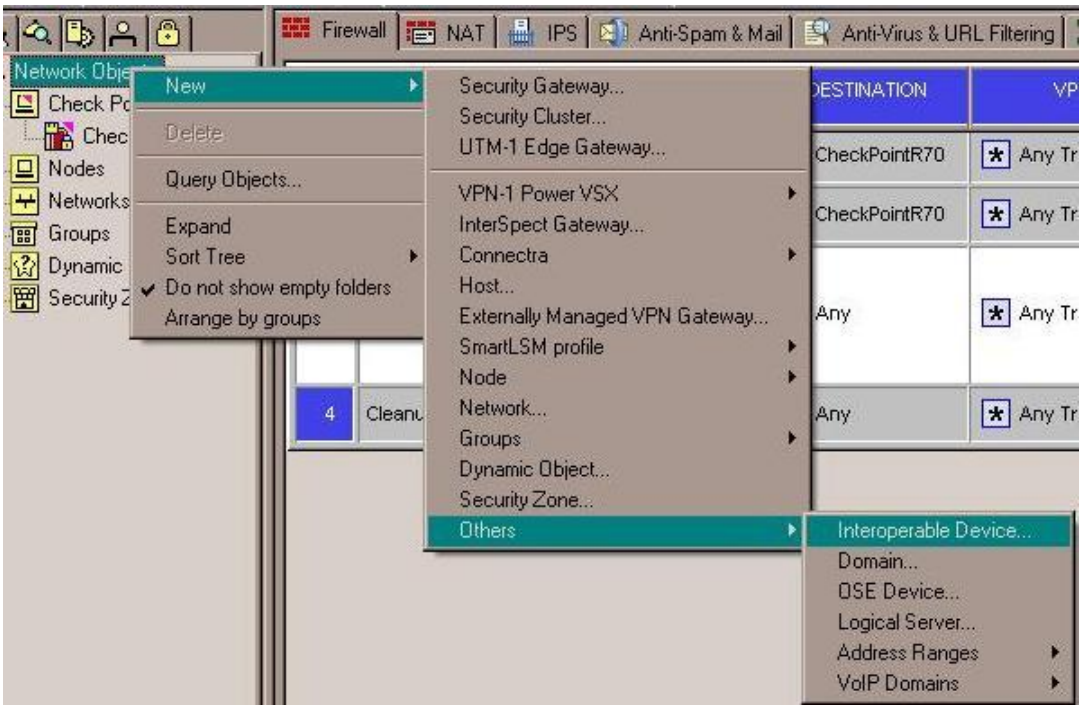
Contents

VPN Setup

Configuring the Cisco Gateway Object

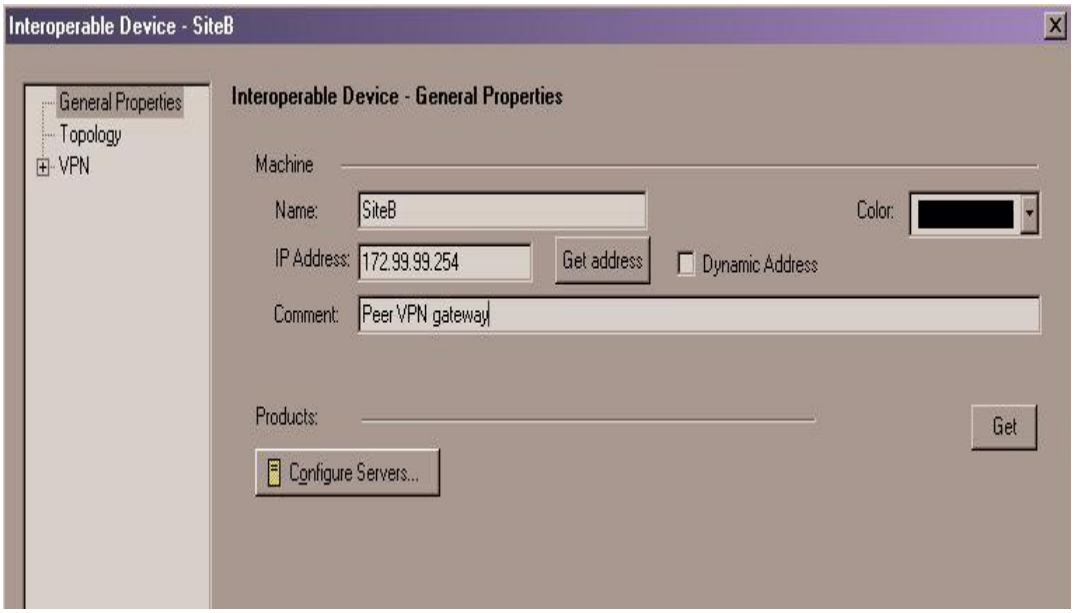
To create the Cisco Gateway Object:

1. Right click: **Network Objects** >**New** >**Others** >**Interoperable Device**



2. In the General Properties dialog box, enter a Name for the Gateway, IP address and description (optional).

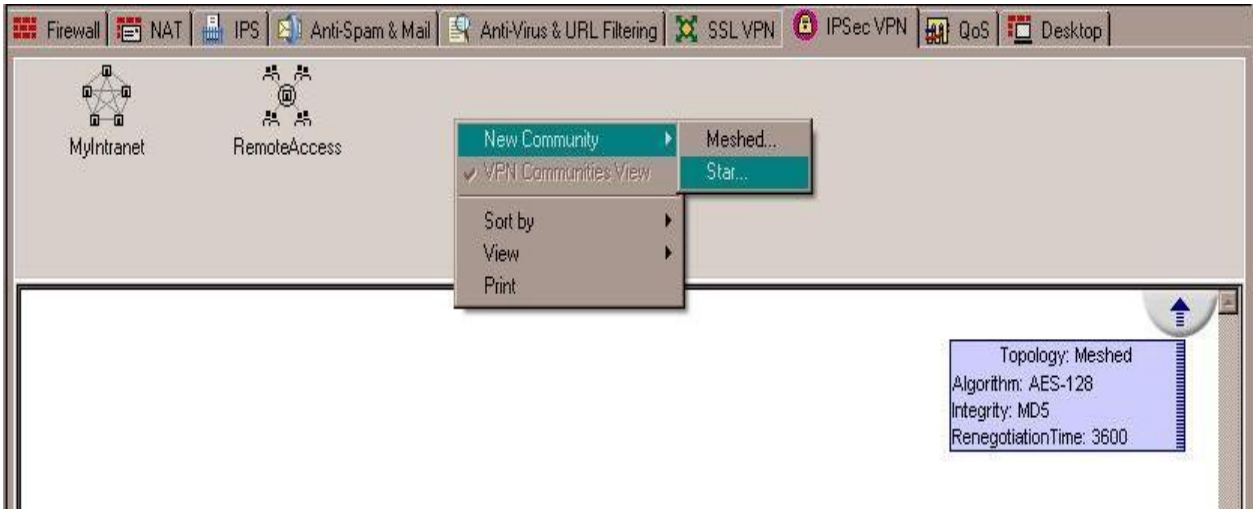
Note - Use the external routable IP address of the Cisco peer for the IP.



3. Click OK.

VPN Community Setup

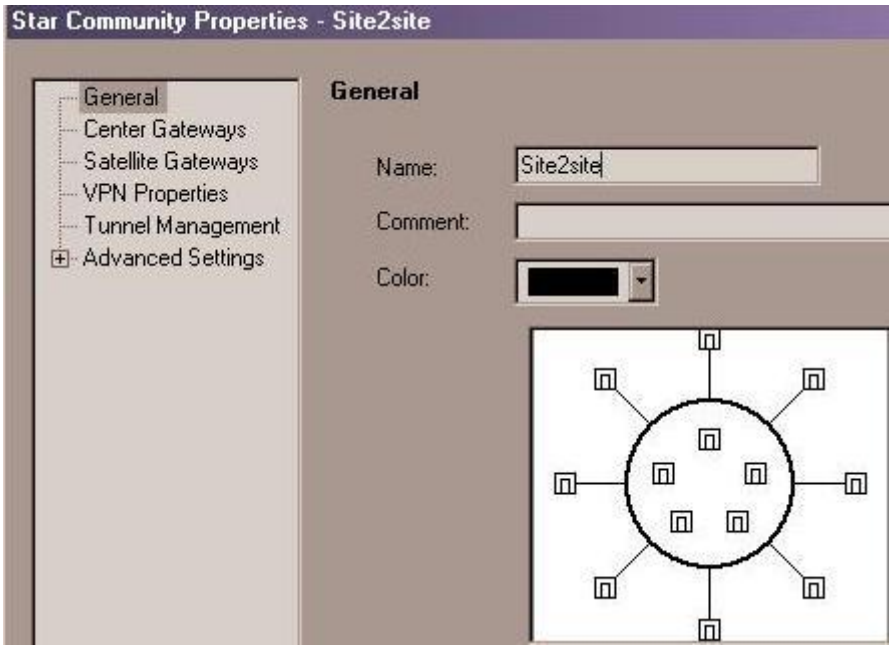
1. Select the **IPSec VPN** tab.
2. Right click in the open area on the top panel. Select **New Community**-->**Star**



VPN Community Configuration

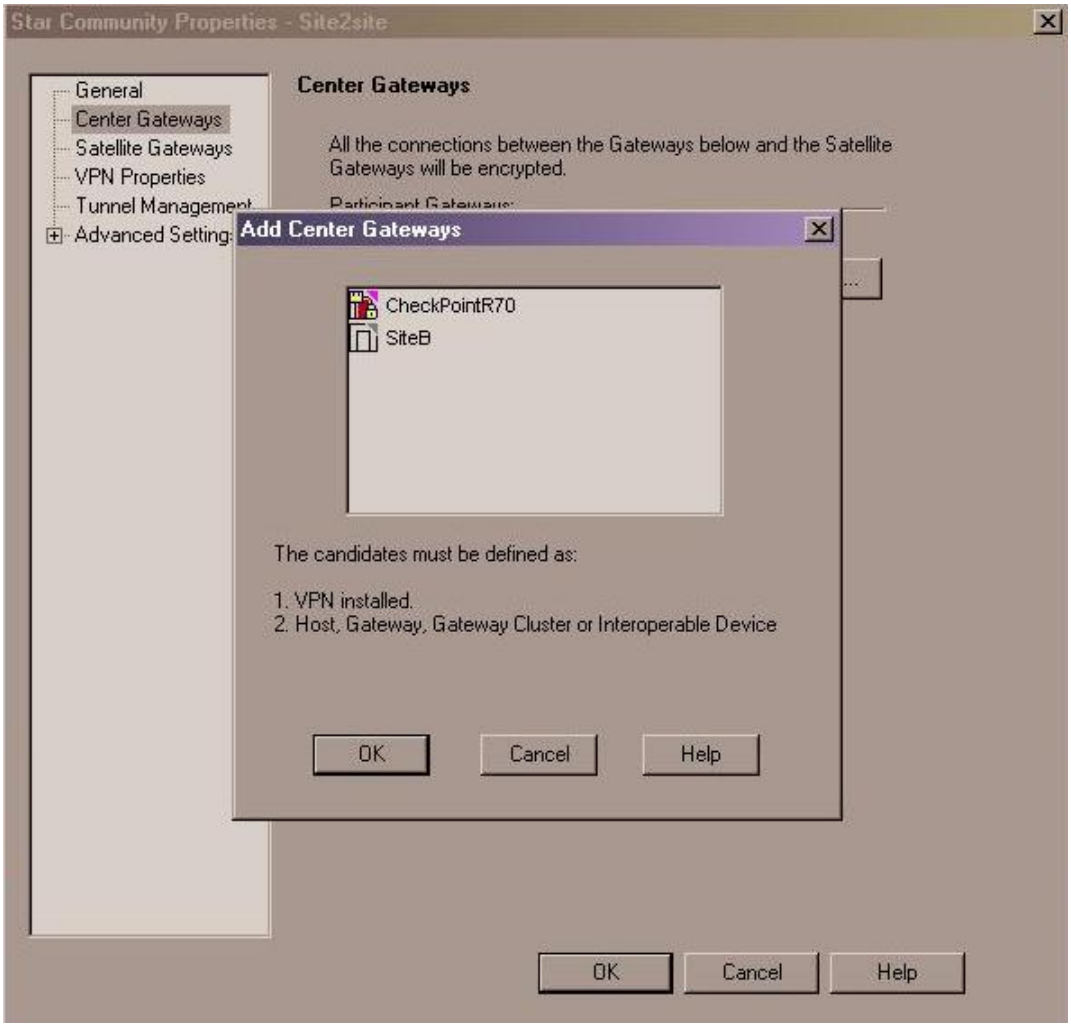
To configure the VPN:

1. Name the VPN Community.



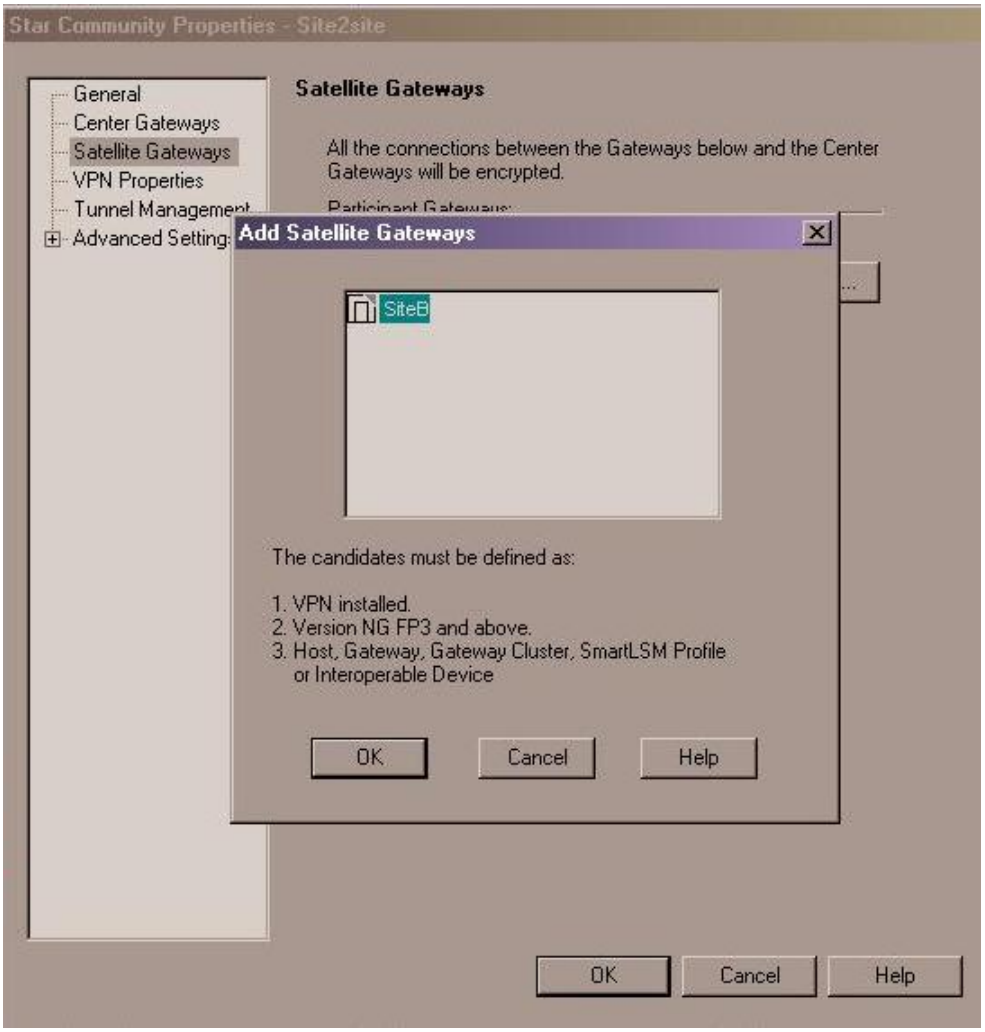
2. Click **Center Gateways**.
3. Click **Add.**
4. Select the local Check PointSecurity Gateway object.

5. Click **OK.**



6. Click **Satellite Gateways.**
7. Click **Add**
8. Select the previously named Cisco peer gateway object.

9. Click **OK**.



10. Click **VPN Properties**.

Note - You can change the Phase 1 and Phase 2 properties here. Note the values you select, because the peer will need to match these values.

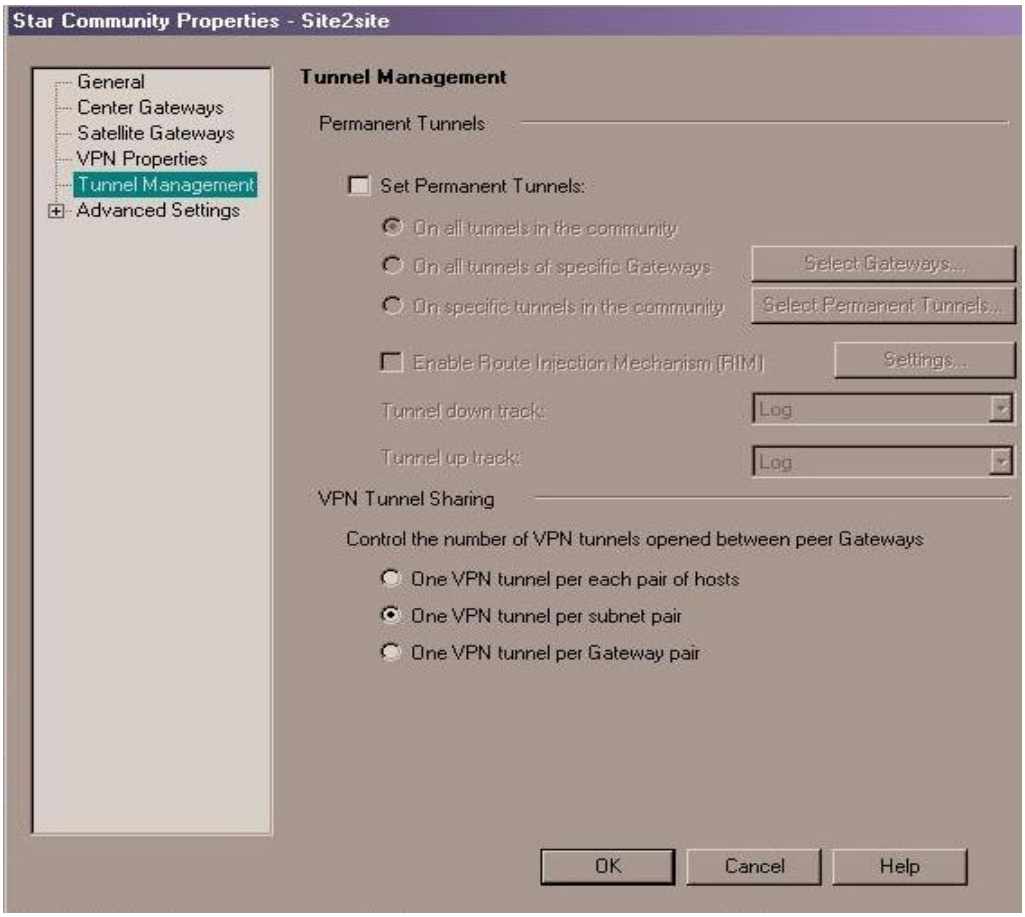
You can define the Tunnel setup in the Tunnel Management option. **One VPN tunnel per subnet pair** is the recommended tunnel sharing method. This shares your network on either side of the VPN, makes the phase 2 negotiation easier, and requires fewer tunnels to be built for the VPN.

You can restrict access on the VPN through your security rulebase.

Note - Permanent tunnels can only be done between Check Point gateways.

To Configure VPN Tunnel:

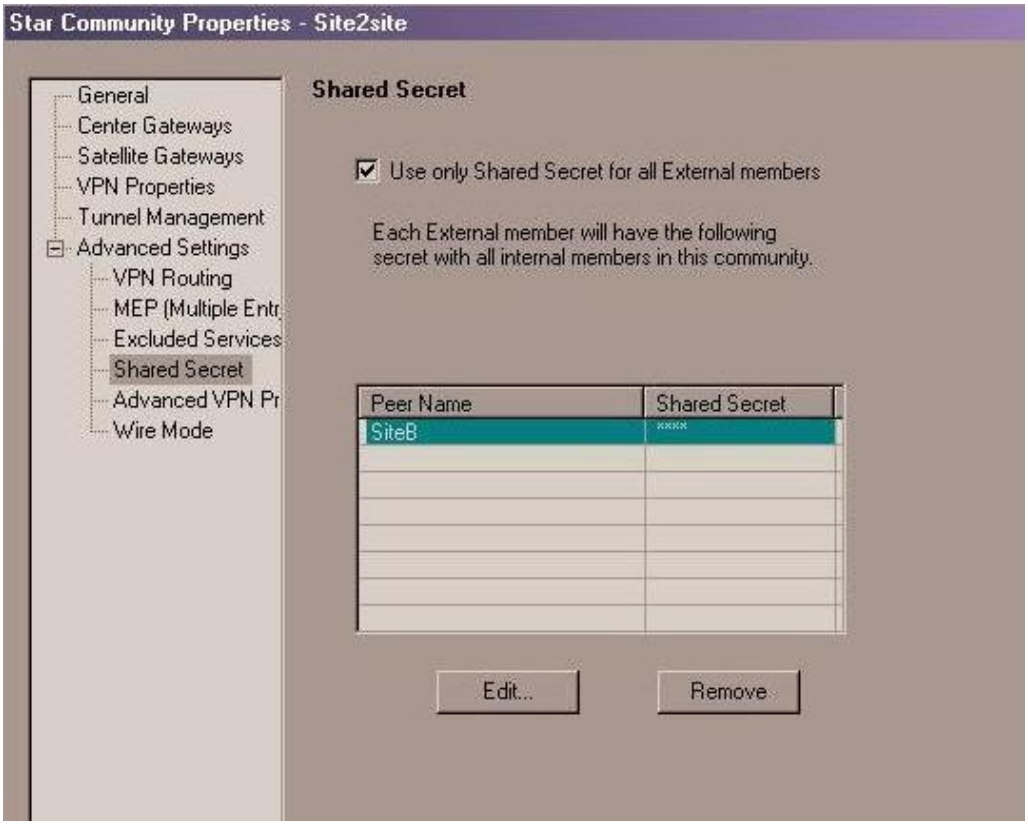
1. Click **Tunnel Management** to configure the tunnel.



To Configure the Shared Secrets:

1. Click **Advanced Settings**
2. Click **Shared Secret**
3. Select **Use only Shared Secret for all External members**
4. Select your peer gateway in the list
5. Click **Edit** to edit the shared secret.

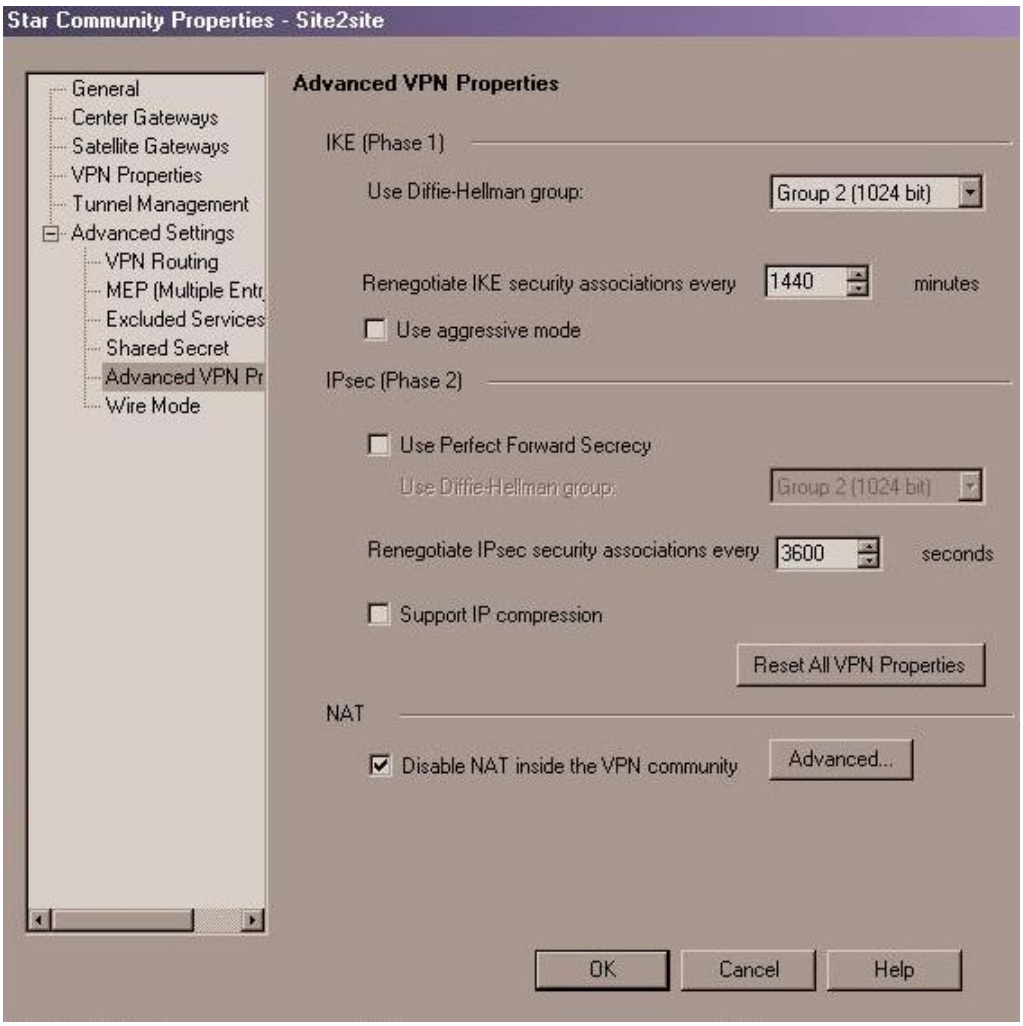
Note - Remember this secret because your peer will need it to set up the VPN on the other end.



To Modify Phase 1 and Phase 2 Advanced Settings

1. Click **Advanced VPN Properties**
   Keep note of these values.

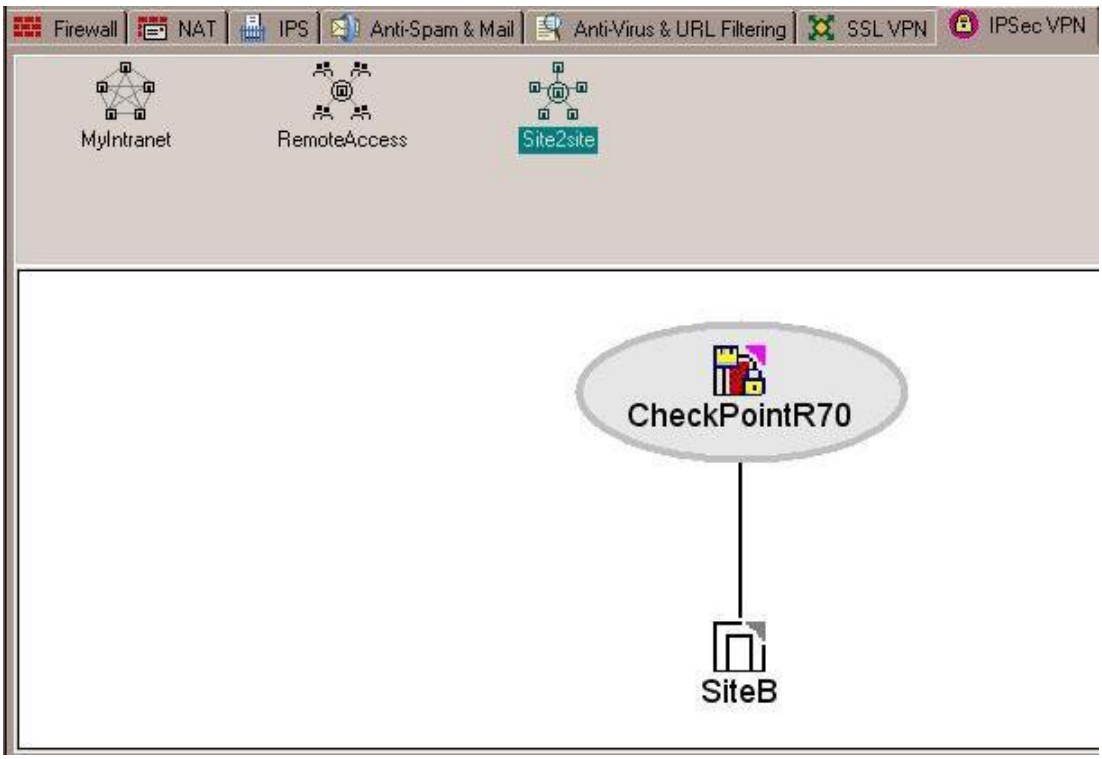
Note - It is recommended that you select **Disable NAT inside the VPN community** to access resources behind your peer gateway using their real IP addresses and vice versa.



2. Click **OK** to exit back to the SmartDashboard.

Note - You may see the following message: **At least one of the VPN Community members does not have the VPN domain defined. Are you sure you want to continue?**

3. Click **Yes** to view your defined VPN community



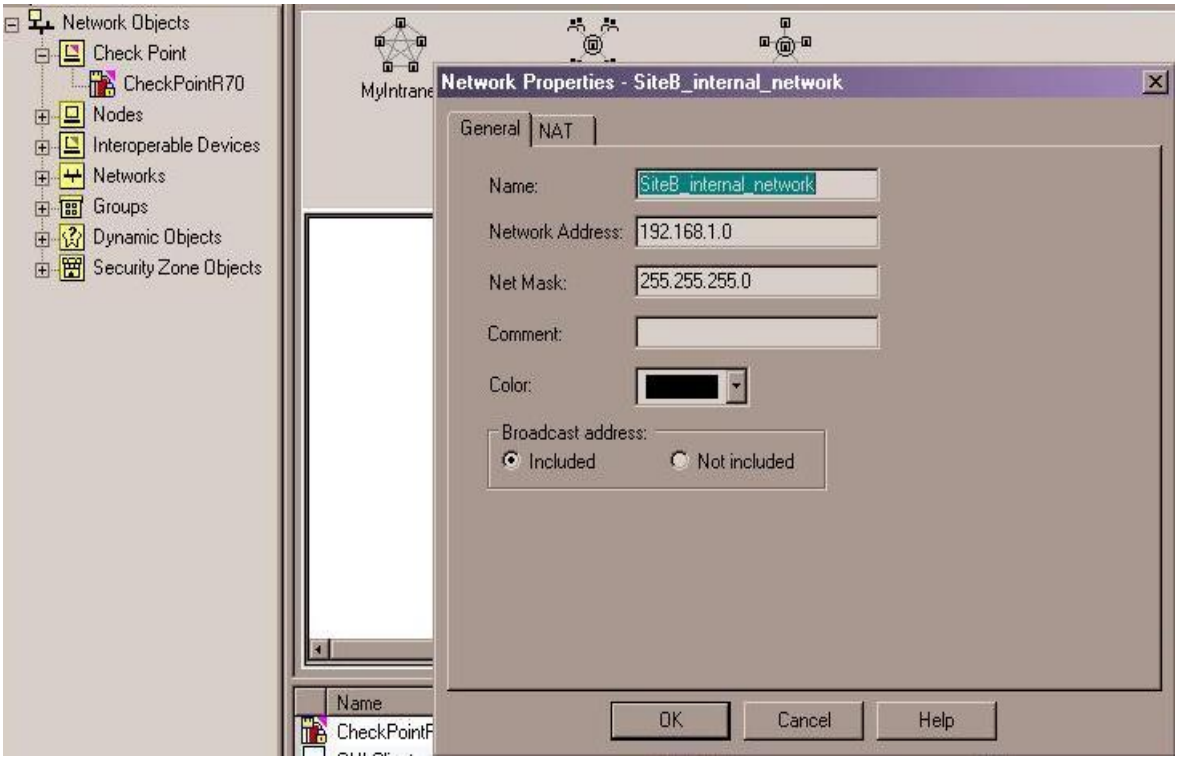
Defining the VPN Domain

Make sure you have Network Objects to represent the local networks and the Cisco peer networks that will be sharing with you.

To Define the VPN Domain:

1. Right-click **Networks**
2. Select **Network**

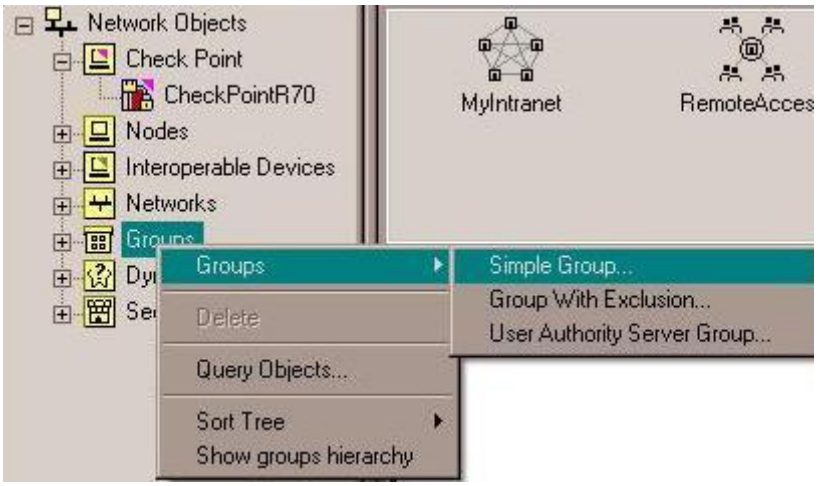
   In the Network Properties window, enter the properties of the Cisco peer internal network.



When many networks are shared on either end of the tunnel, it is recommended to create different groups to represent the domains on either side of the VPN tunnel.

To create a Group:

1. Right click **Groups**
2. Select **Groups**>**Simple Group**



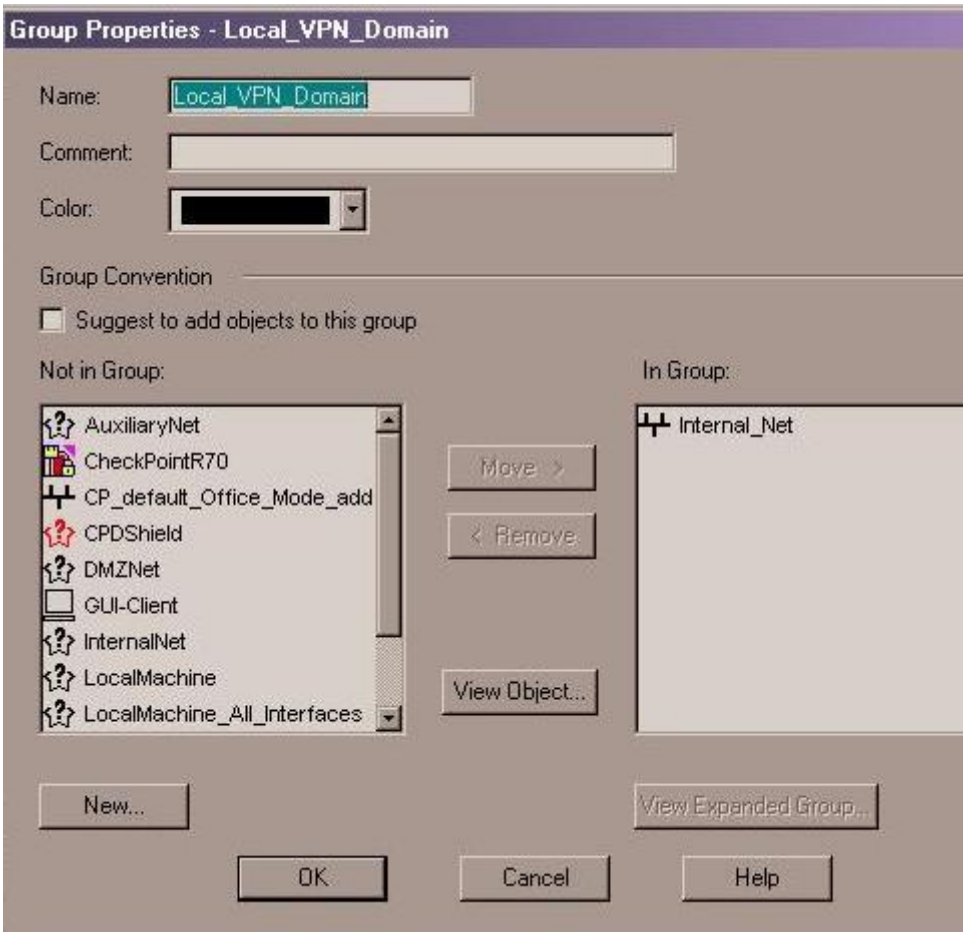
This example shows one shared network, and there is one object in the group. There is no limit to the number of networks that can be shared.

Important - Adding groups within a group can impact network performance. Make sure the group is "flat".

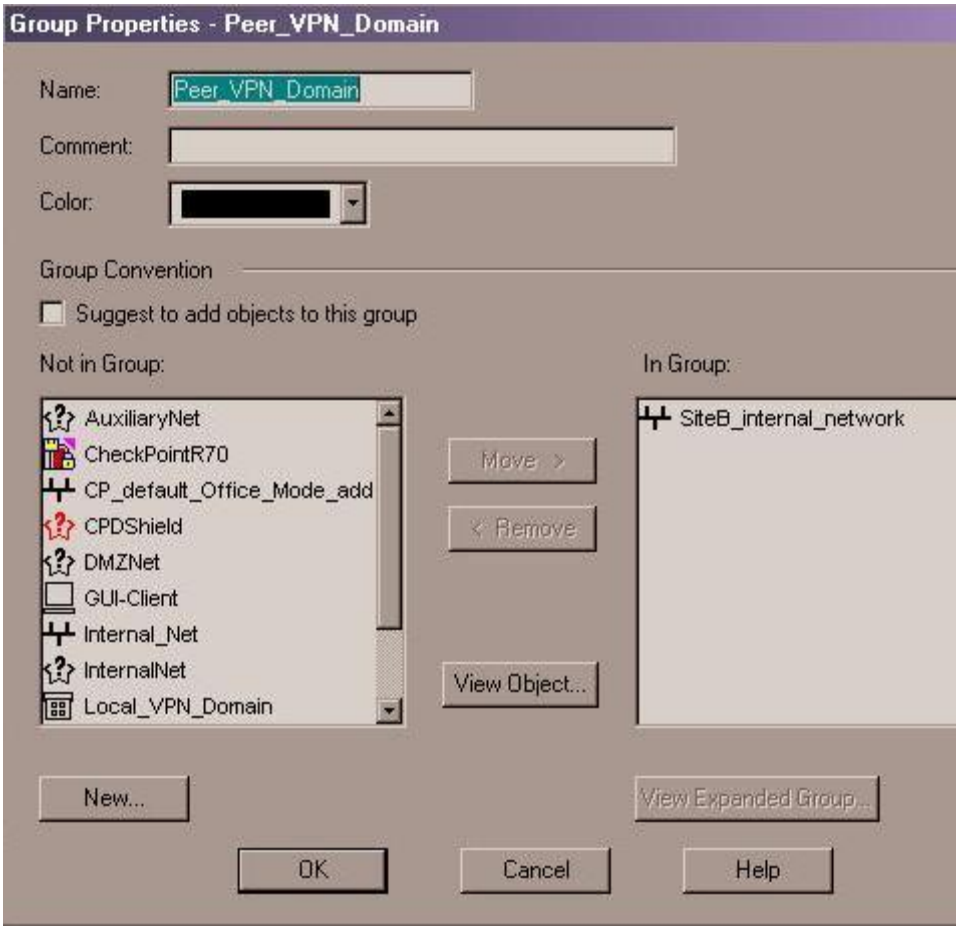
We recommend that the name of the group is relevant to the network setup, for example: "Local_VPN_Domain".

Add all local networks for the VPN, to create the group that represents the Cisco peer shared network.

3. Click **OK**



4. Adding a second group:

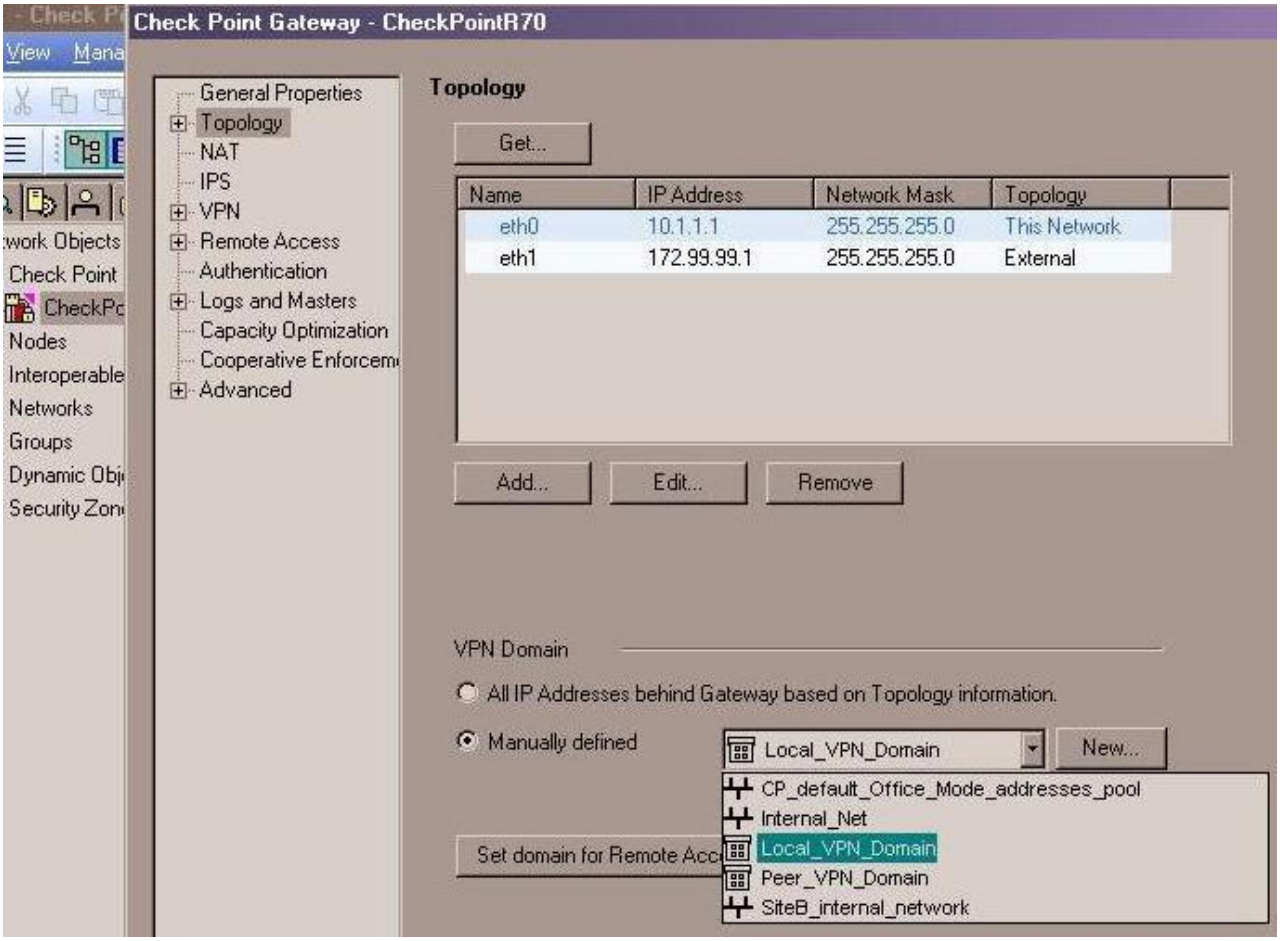


VPN Domain Configuration

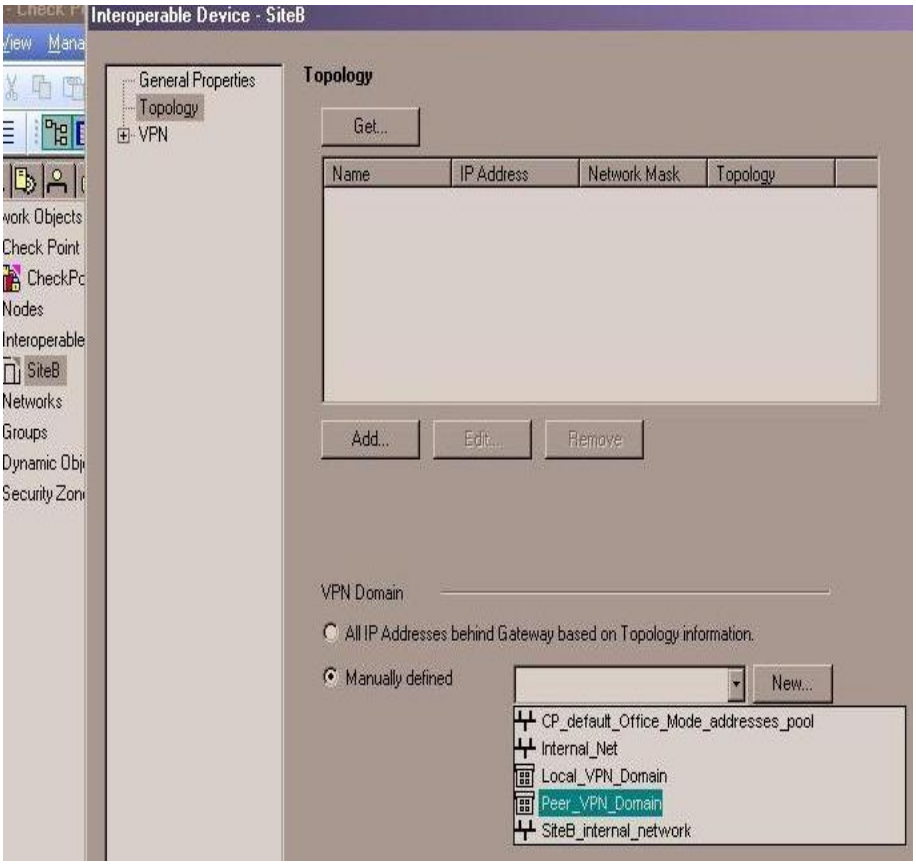
Setting the VPN domains for each gateway:

1. Open the Properties for your local Check Point gateway object.
2. Click **Topology i**n the **VPN Domain** area.
3. Select **Manually defined**

4. From the list, select <**local VPN domain group object**>.



5. Click **OK** and open the Properties for the Cisco gateway.
6. Select the group/network that represents the VPN domain.



7. Click **OK**

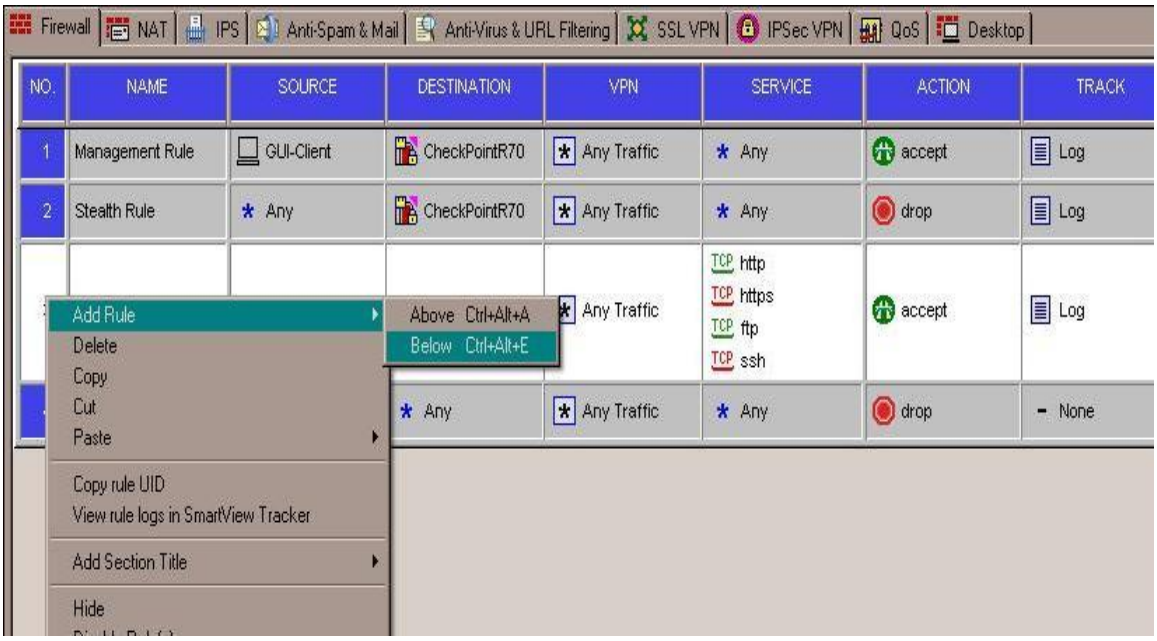
Rules for Traffic

After you setup the objects, the VPN, and the community, set up Rules to control flow of traffic to allow and restrict access to the VPN.

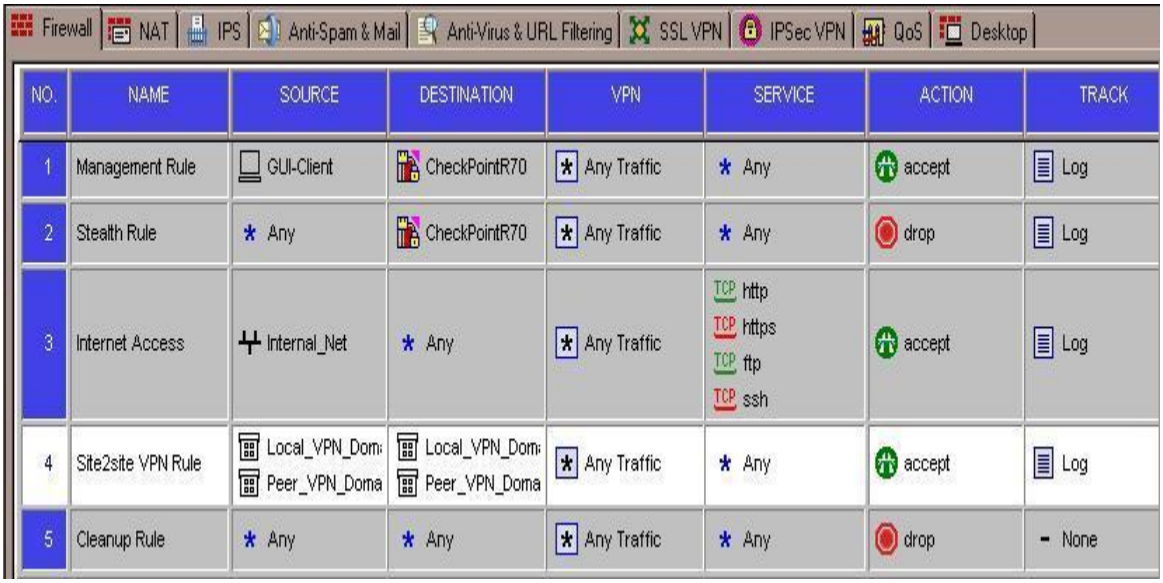
Setting a Rule

To setup a Rule:

1. Right click above the number in the rule column where you want the rule to be set.
2. Select **Add Rule**>**Below**



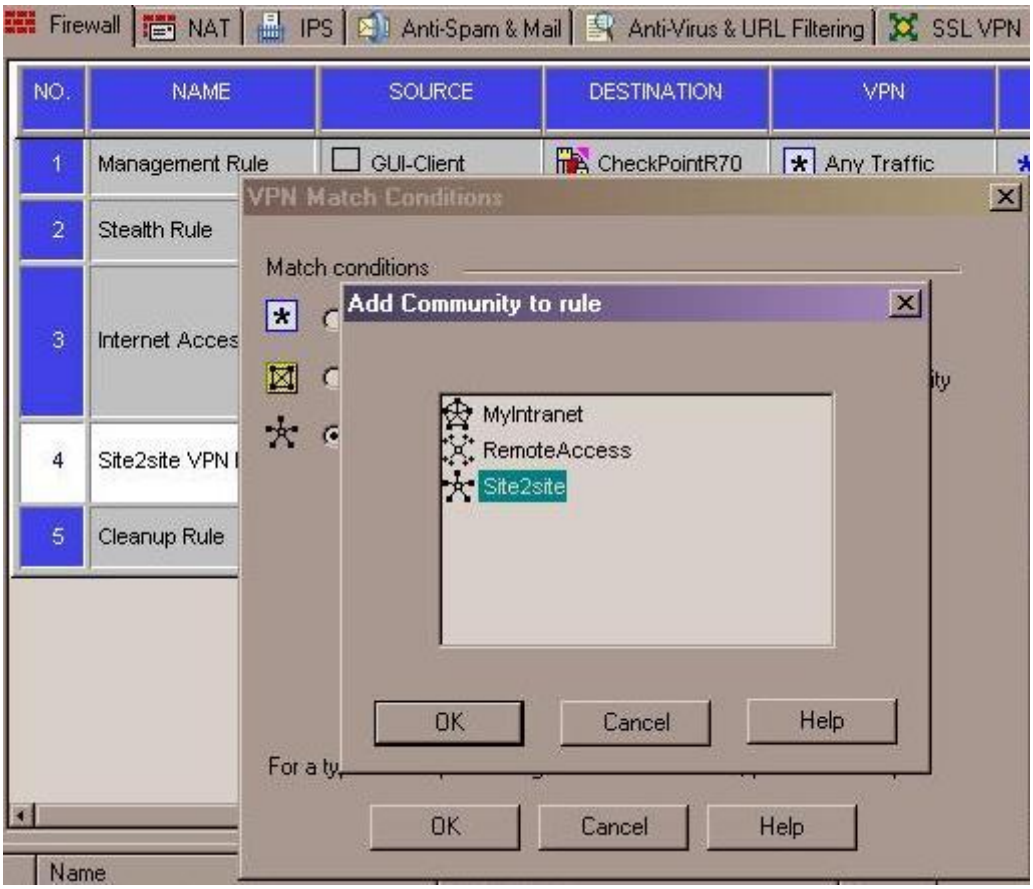
In the example below, the Rule allows any service across the tunnel in both directions.



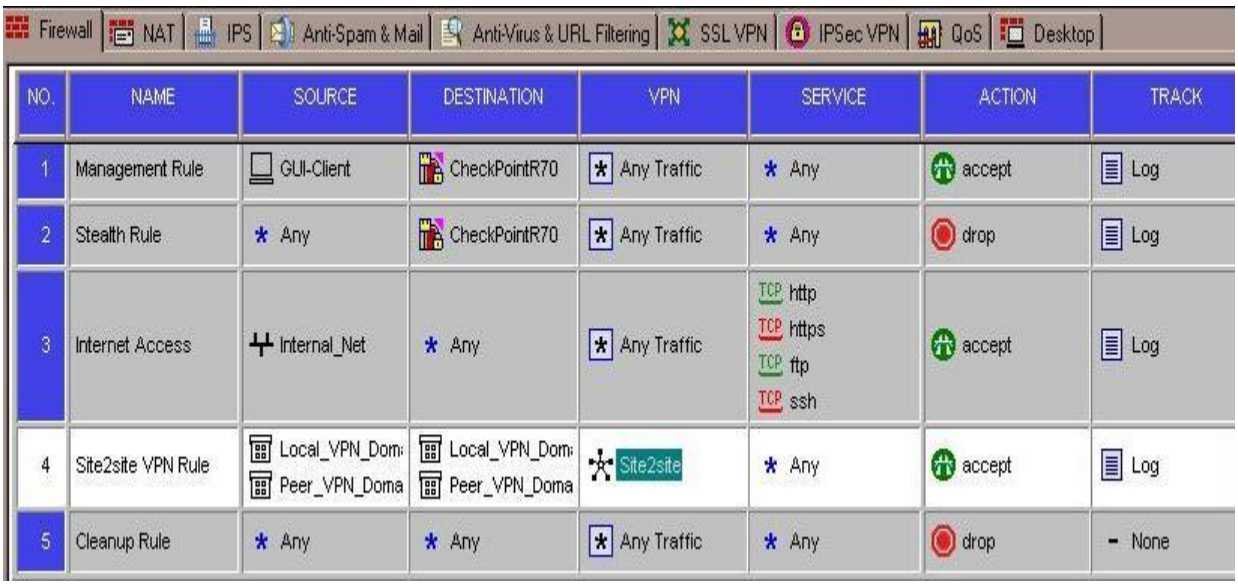
Setting VPN Community in the Rule

To set the VPN community in the VPN column of the Rule:

1. Right click the **Any Traffic** icon.
2. Select **Edit Cell.**
3. Select **Only connections encrypted in specific VPN Communities.**
4. Click **Add.**
5. Select the VPN community.
6. Click **OK.**
7. Click **OK** again.



The Rule appears in the VPN column.



Final Step

Install the policy to the local Check Point gateway. The VPN is setup!

After the Cisco remote side sets up their VPN to match, a secure communication with their site is established.