

Configuring Site-to-Site VPN between Safe@Office with DAIP and VPN-1 NG

November 2002

Copyright © 2002 SofaWare Technologies Inc, All Rights Reserved. Reproduction, adaptation, or translation with prior written permission is prohibited except as allowed under copyright laws.

Introduction

This document explains how to configure bi-directional VPN connections (Site-to-Site) between Safe@Office appliances with dynamic IPs (DAIP) and Check Point FW-1/VPN-1 NG FP2/FP3.

Figure 1 shows a sample implementation of this solution, in which a Safe@Office appliance is connected to a VPN-1 Site-to-Site VPN gateway.

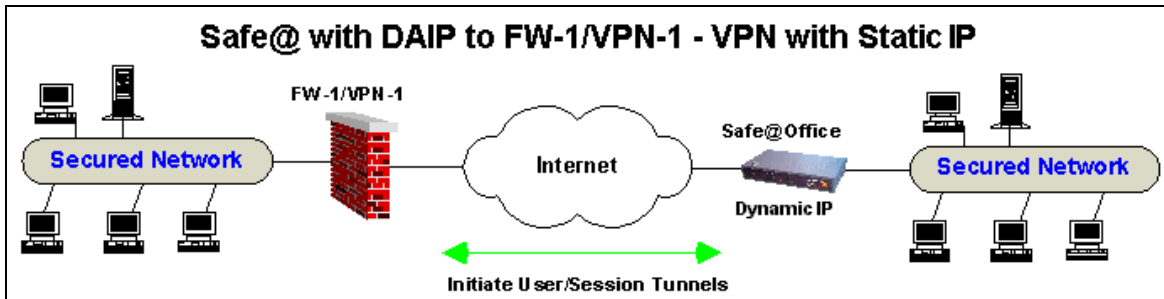


Figure 1: Safe@Office with DAIP to FW-1/VPN-1 (Site-to-Site VPN)

Note: This solution works in both FP2 and FP3. However, if you need to encrypt traffic from multiple networks behind the FW-1/VPN-1 NG to the Safe@ network, it is recommended that you use FP3. This is because when you initiate a VPN tunnel from the Safe@ network to one of the FW-1/VPN-1 NG FP3 networks, all the other FW-1/VPN-1 NG FP3 networks are automatically able to encrypt packets back to the Safe@ network. In FP2, you must initialize the tunnel from the Safe@ network to each one of the FW-1/VPN-1 NG FP2 networks separately.



Note: This VPN connectivity solution requires Safe@Office 3.0.17 or above.

To implement this solution, you must perform the following tasks in the order below:

1. “Configuring FW-1 NG FP2/FP3,” page 2
2. “Exporting the Safe@ Gateway Object’s Certificate,” page 22
3. “Configuring the Safe@Office Appliance,” page 23



About This Document

You should be familiar with the following before using this guide:

- Basic FW-1/VPN-1 use. For information, refer to the *Check Point VPN-1/FireWall-1 Administration Guide*.
- S-box use for your software configuration. For information, refer to the *SofaWare S-box Getting Started Guide*.



Note: The screens shown in this document appear in both VPN-1 NG FP2 and FP3. Where FP2 and FP3 screens differ, both are shown.



Note: This document explains how to configure a Site-to-Site VPN in Community mode. Traditional mode is also supported.

Contacting Technical Support

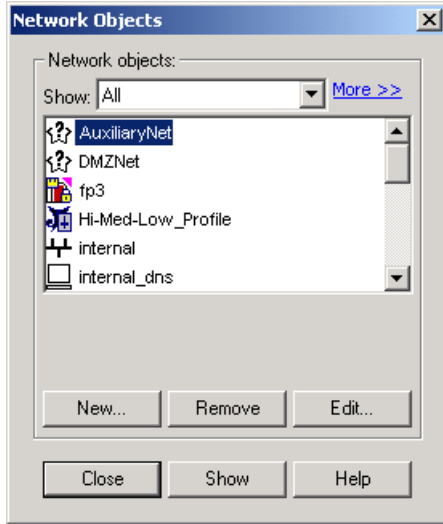
To contact technical support, send an email to: support@sofaware.com

Configuring FW-1 NG FP2/FP3

To configure VPN-1 NG FP2/FP3 for Site-to-Site VPN with DAIP

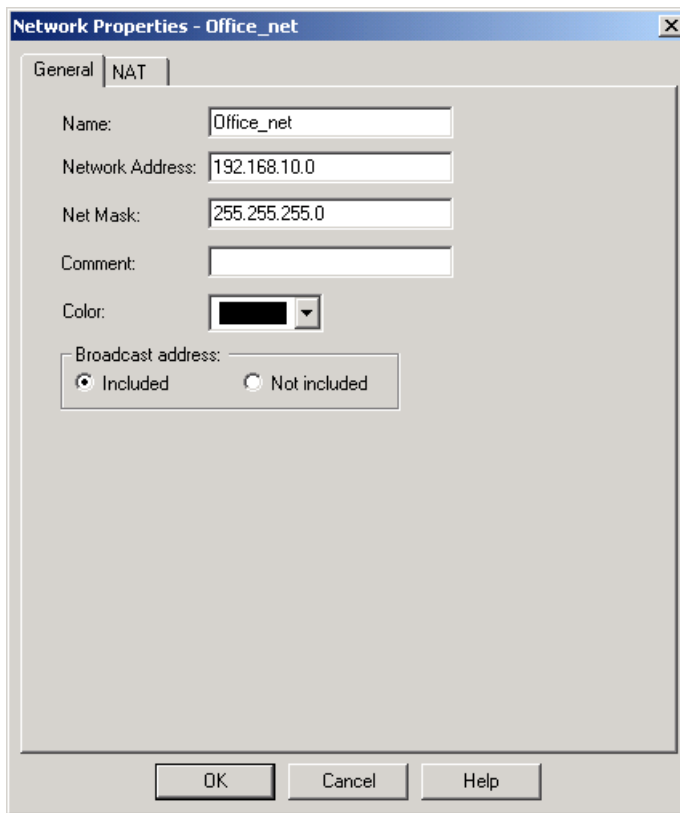
1. Open the Check Point SmartDashboard.
2. Create a Safe@ network network object by doing the following:
 - a. In the **Manage** menu, click **Network Objects**.

The **Network Objects** dialog box appears.



- b. Click **New...** and then **Network...**

The **Network Properties** dialog box appears with the **General** tab displayed.





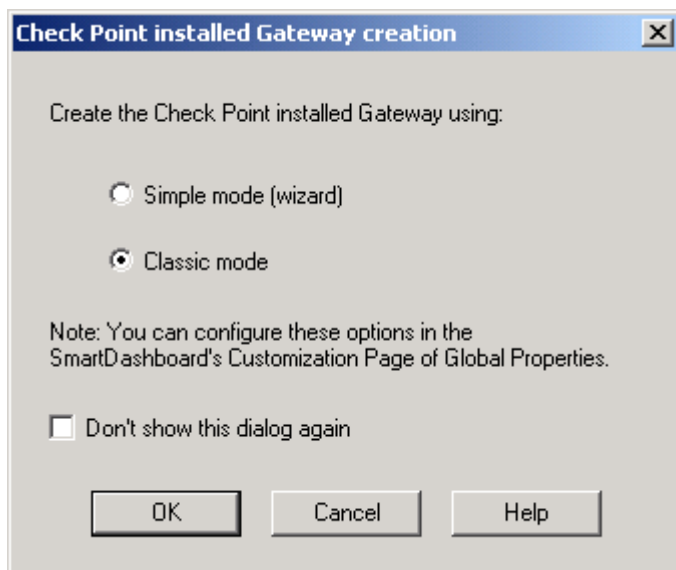
Note: The network address may differ depending on the Safe@ appliance's network range. In this example, 192.168.10.0/24 is used.

- c. In the **Name** field, type the network object name.
 - d. In the **Network Address** field, type the network object's IP address.
 - e. In the **Net Mask** field, type the network object's subnet mask.
 - f. Click **OK**.
3. Create a Safe@ gateway object in VPN-1 NG-FP2/3, by doing the following:
- a. In the **Manage** menu, click **Network Objects**.

The **Network Objects** dialog box appears.

- b. Click **New...**, **Check Point**, and then **Managed Gateway**.

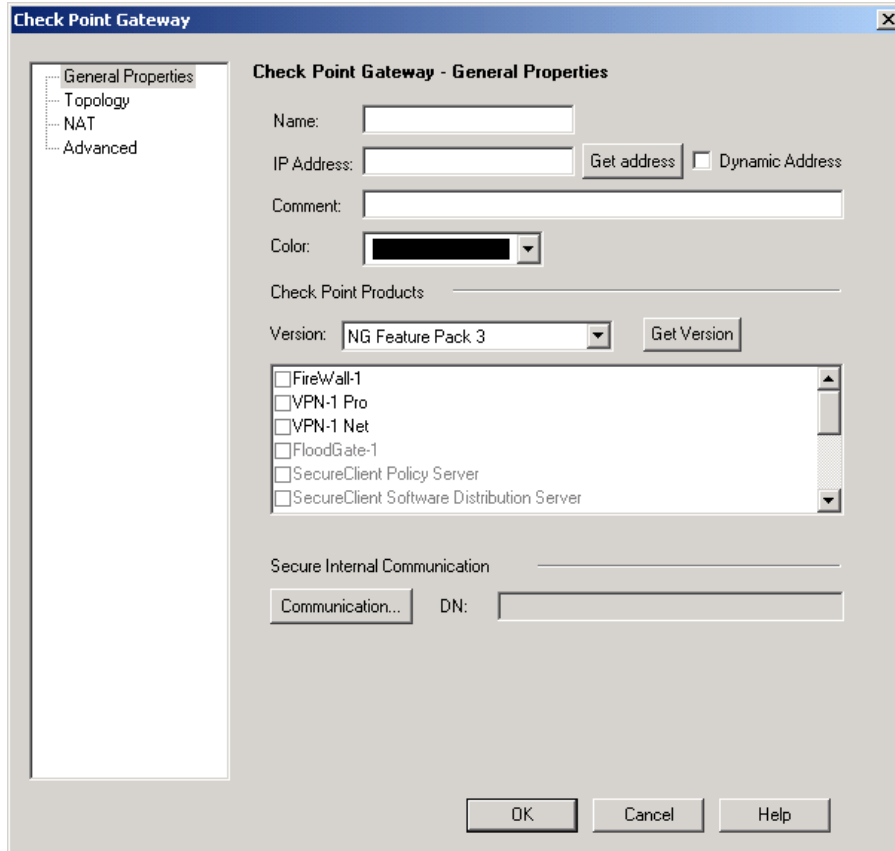
The **Check Point installed Gateway creation** dialog box appears.



- c. Select **Classic mode**.
- d. Click **OK**.

The **Check Point Gateway** dialog box opens with **General Properties** tab displayed.

4. Configuring Site-to-Site VPNs between Safe@Office with DAIP and VPN-1 NG



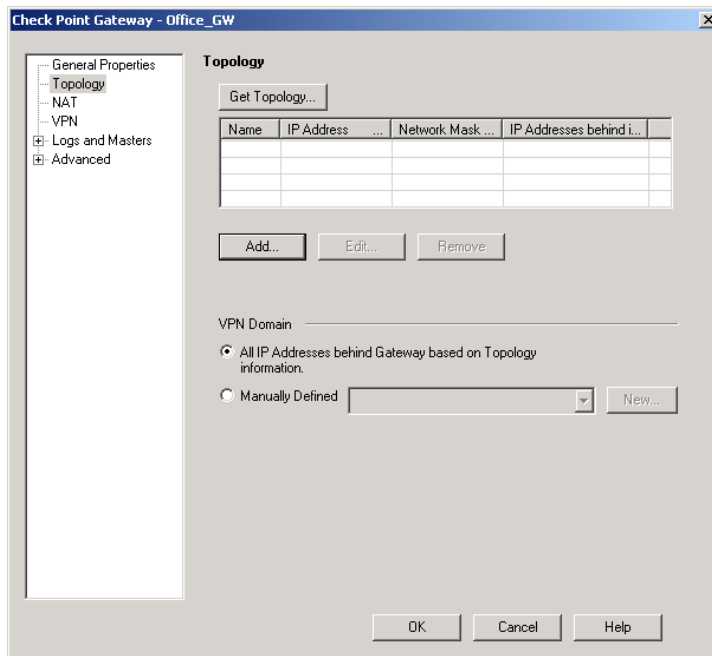
Do the following:

- 1) In the **Name** field, type the object's name.
 - 2) In the **Version** list, select **NG Feature Pack 2** or **NG Feature Pack 3**.
 - 3) In the **IP Address** area, select the **Dynamic Address** check box.
 - 4) In the **Check Point Products** list, verify that **FireWall-1** and **VPN-1 Pro** are selected.
- e. Click **Topology**.

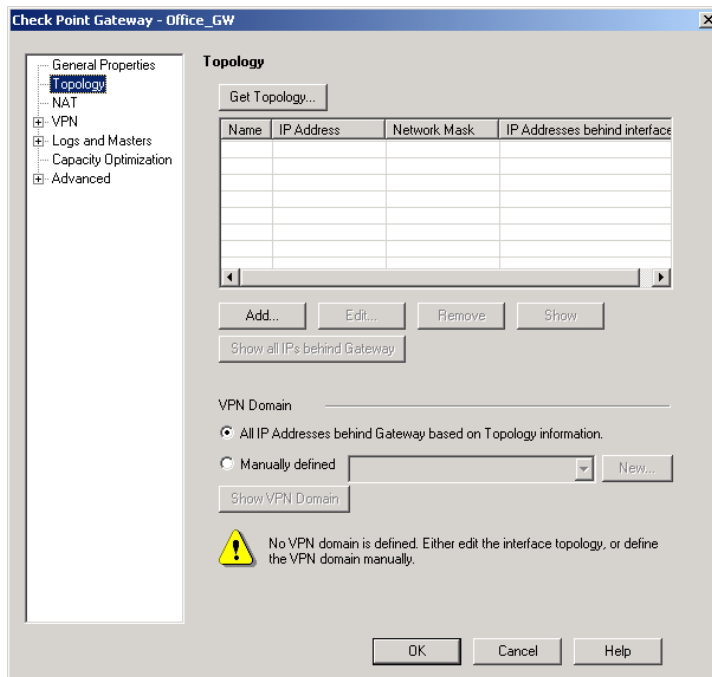
The **Topology** tab is displayed.



If you are using FP2, the screen appears as follows:



If you are using FP3, the screen appears as follows:





- f. Add both an internal and external Safe@ interface.

Do the following for each interface:

- 1) Click **Add....**

The **Interface Properties** dialog box appears with the **General** tab displayed.

The screenshot shows the 'Interface Properties' dialog box with the 'General' tab selected. The 'Name' field is set to 'Internal', the 'IP Address' field is set to '192.168.10.0', and the 'Net Mask' field is set to '255.255.255.0'. The 'Dynamic IP' checkbox is unchecked. A note at the bottom states: 'Note: the interface name must exactly match the name the operating system uses for this interface. See help for further information.' The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

- 2) In the **Name** field, type the interface's name.
- 3) If you are configuring the internal interface, type the interface's IP address, and subnet mask in the appropriate fields.



Note: The network address may differ depending on the Safe@ appliance's network range. In this example, 192.168.10.0/24 is used.

- 4) If you are configuring the external interface, select **Dynamic IP**.



The **IP Address** and **Net Mask** fields appear dimmed.

Interface Properties

General | Topology

Name: External

IP Address: [dimmed]

Net Mask: [dimmed]

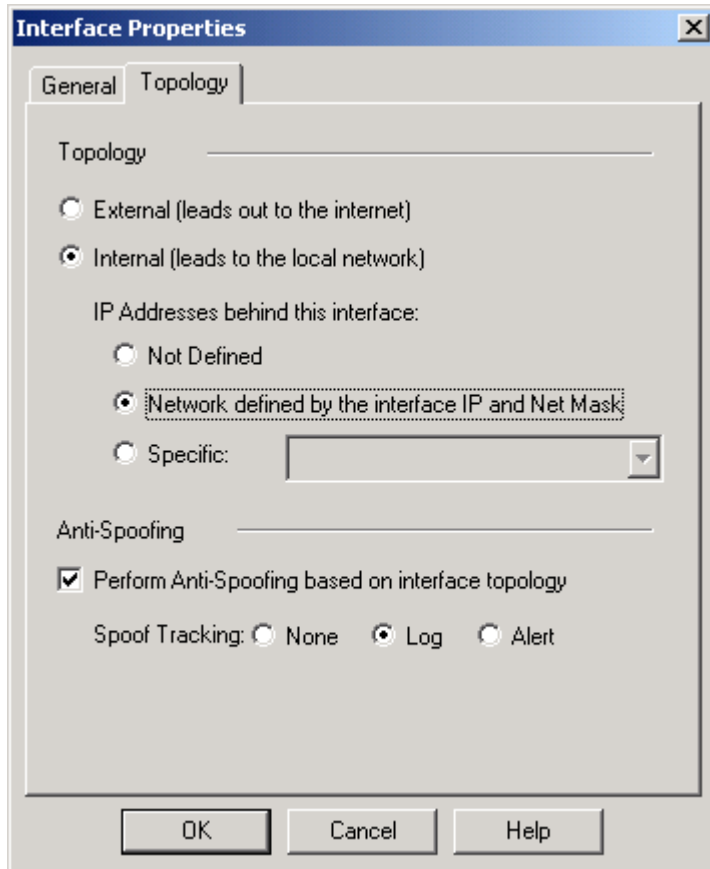
Dynamic IP

Note: the interface name must exactly match the name the operating system uses for this interface. See help for further information.

OK Cancel Help

5) Click on the **Topology** tab.

The **Topology** tab is displayed.



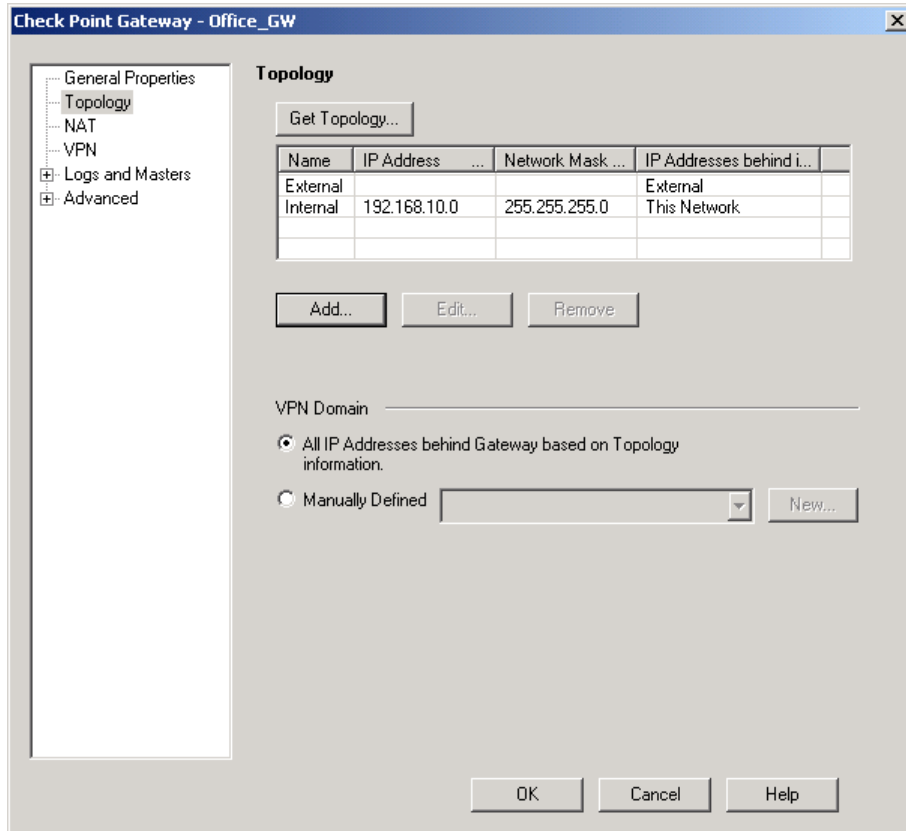
- 6) If you are configuring the external interface, select **External (leads out to the internet)** in the **Topology** area.
- 7) If you are configuring the internal interface, select **Internal (leads to the local network)** in the **Topology** area, and in the **IP address behind this interface** area select **Network defined by the interface IP and Net Mask**.
- 8) In the **Anti-Spoofing** area, select **Perform Anti-Spoofing based on interface topology**.



9) Click **OK**.

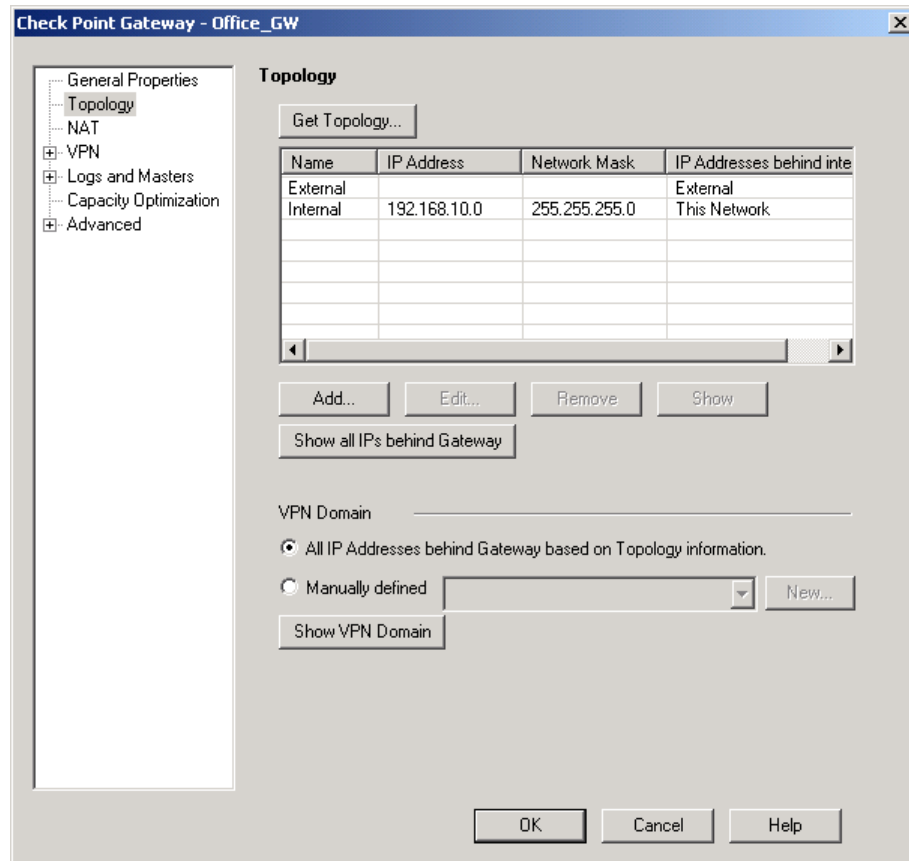
The **Topology** tab reappears.

If you are using FP2, the screen appears as follows:



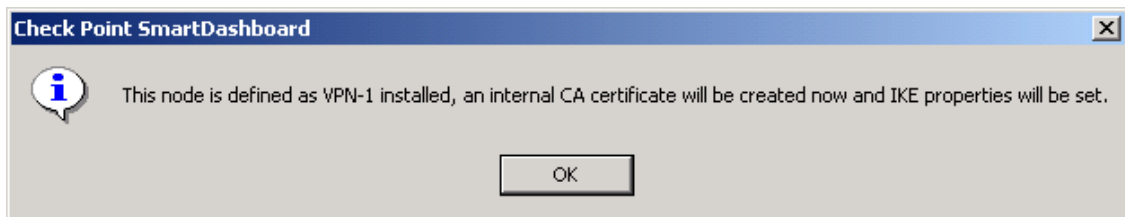


If you are using FP3, the screen appears as follows:



g. Click **OK**.

A confirmation message appears.



h. Click **OK**.

The Safe@ gateway object's internal CA certificate is created.

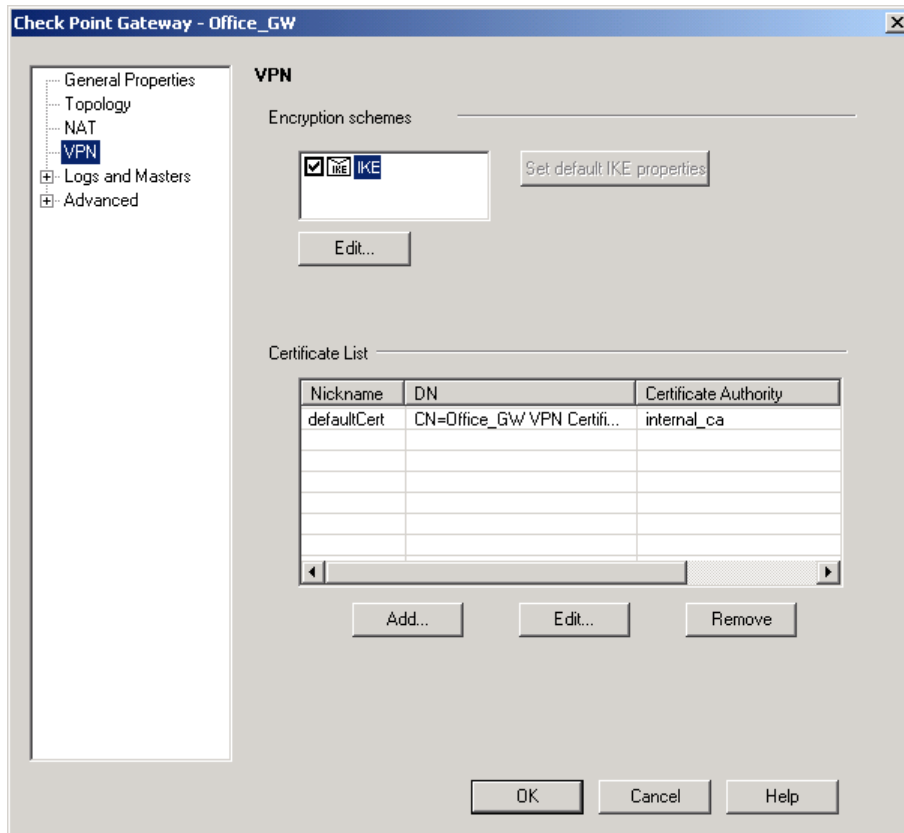
A success message appears.



- i. Click **OK**.

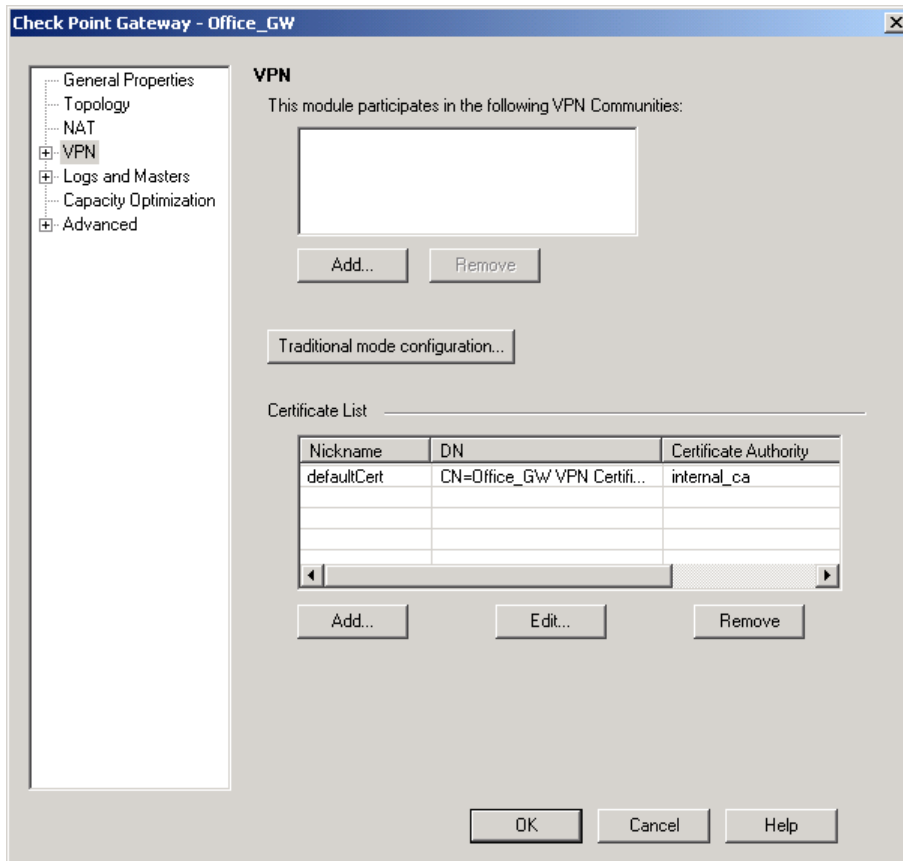
The certificate is added to the **Certificate List** in the **VPN** tab.

If you are using FP2, the screen appears as follows:





If you are using FP3, the screen appears as follows:



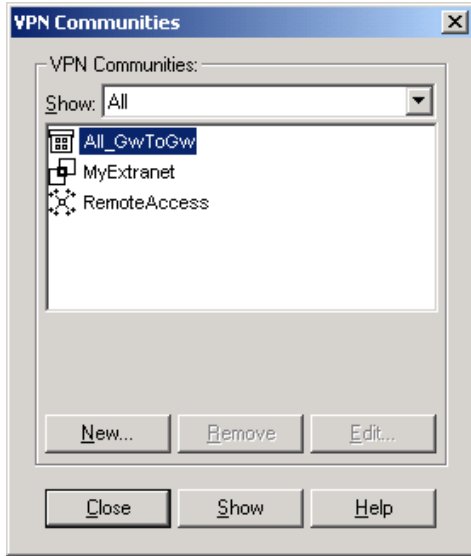
4. Configure a community by doing the following:



Note: You can configure either a Meshed or a Star community. In this document, a Star community is used.

a. In the **Manage** menu, click **VPN Communities**.

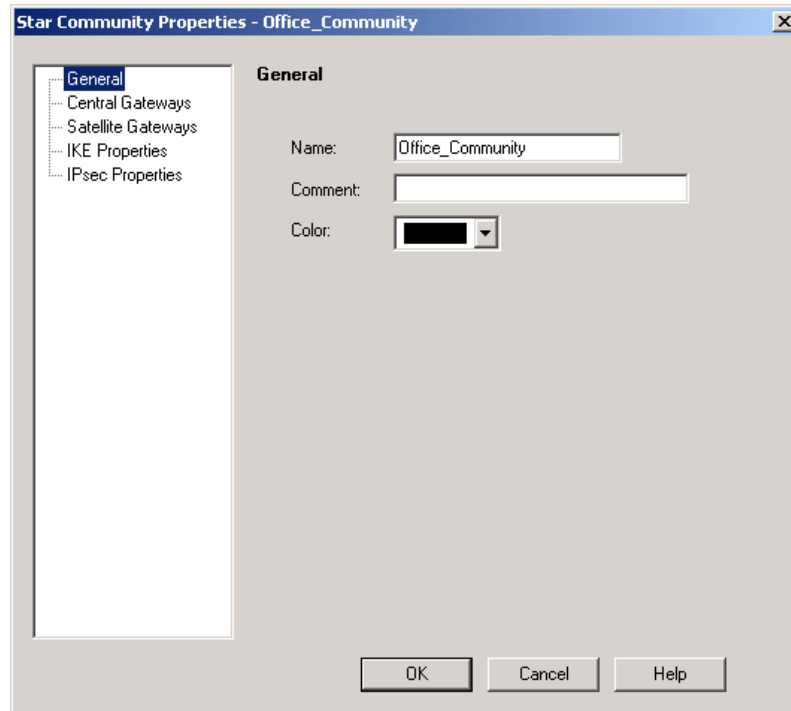
The **VPN Communities** dialog box appears.



b. Do one of the following:

- If you are using FP2, click **New...**, **Intranet...**, and then **Star...**

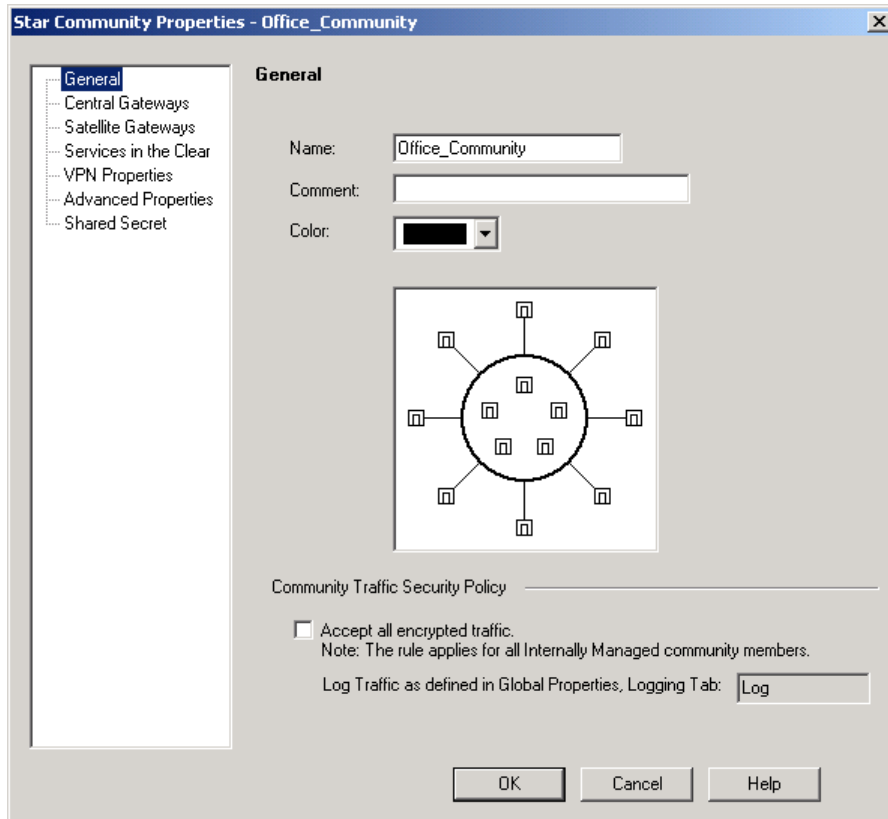
The **Star Communities Properties** dialog box appears with the **General** tab displayed.





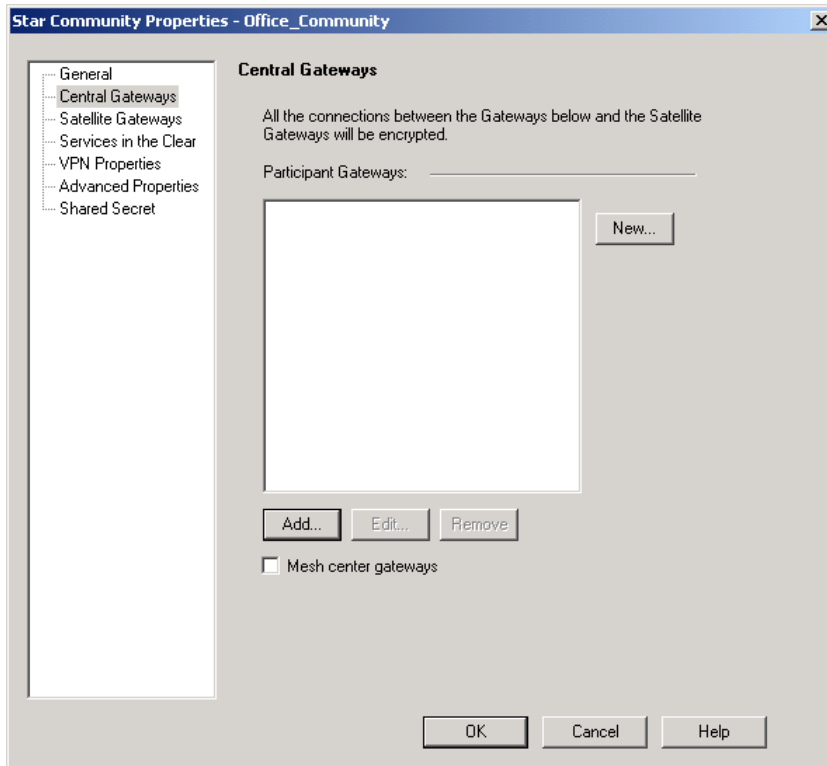
- If you are using FP3, click **New...**, **Site To Site...**, and then **Star...**

The **Star Communities Properties** dialog box appears with the **General** tab displayed.



- c. In the **Name** field, type the community's name.
- d. Click **Central Gateways**.

The **Central Gateways** tab is displayed.



e. Click **Add....**

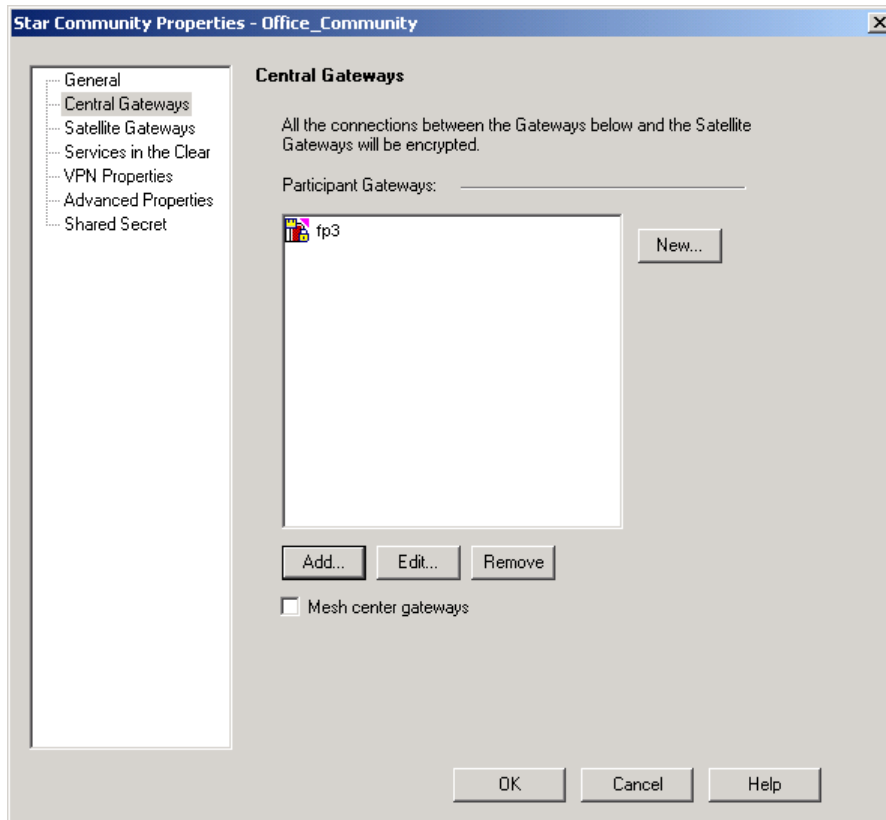
The **Add Central Gateways** dialog box appears.





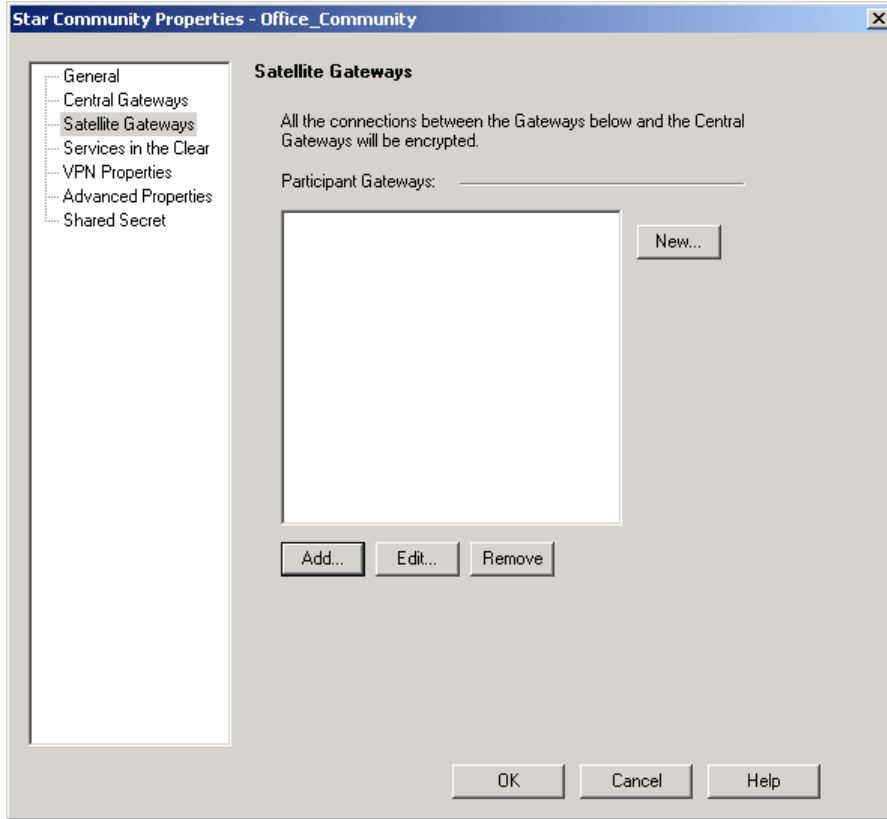
- f. Select the FW-1 gateway (fp3 in the example above).
- g. Click **OK**.

The **Central Gateways** tab reappears, with the FW-1 gateway listed in the **Participant Gateways** area.



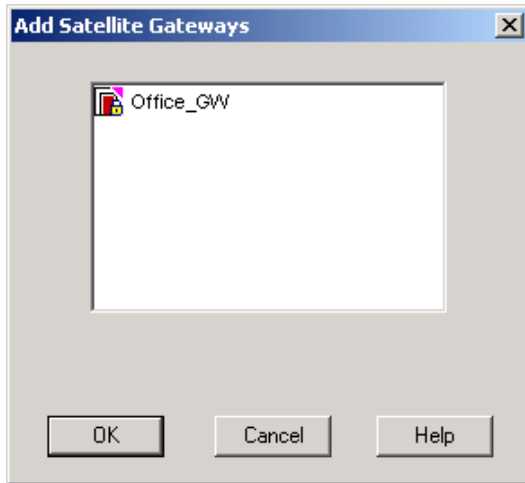
- h. Click **Satellite Gateways**.

The **Satellite Gateways** tab is displayed.



- i. Click **Add...**

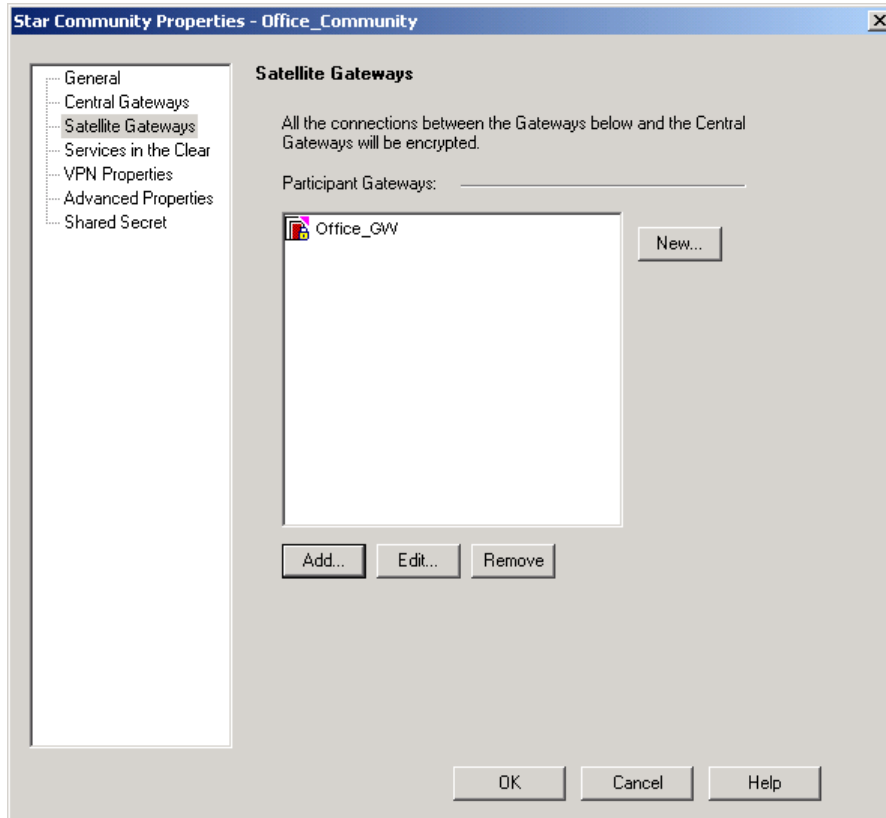
The **Add Satellite Gateways** dialog box appears.



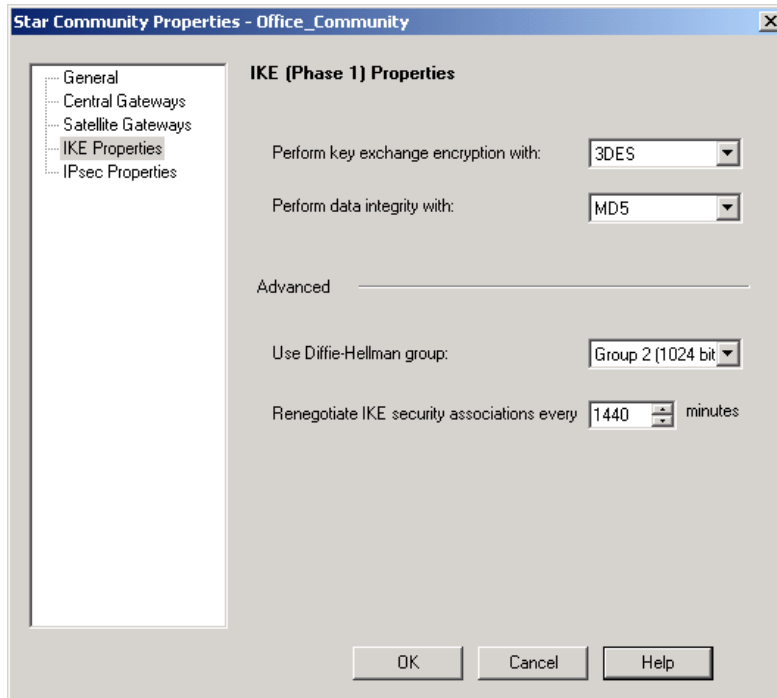


- j. Select the Safe@ gateway (Office_GW in the example above).
- k. Click **OK**.

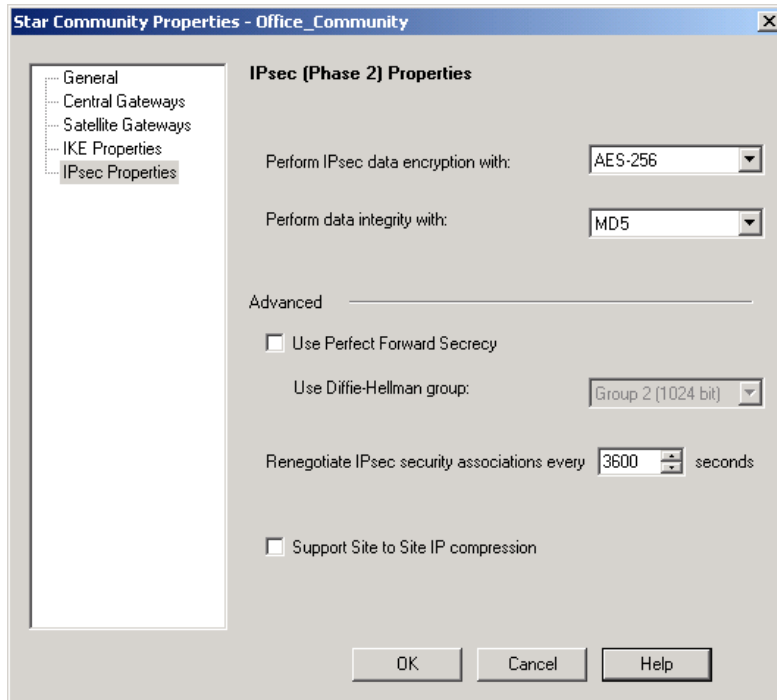
The **Satellite Gateways** tab reappears, with the Safe@ gateway listed in the **Participant Gateways** area.



- l. Set VPN properties as desired in the following screens:
 - If you are using FP2, click **IKE Properties** and **IPsec Properties**.
The **IKE (Phase 1) Properties** tab is displayed...



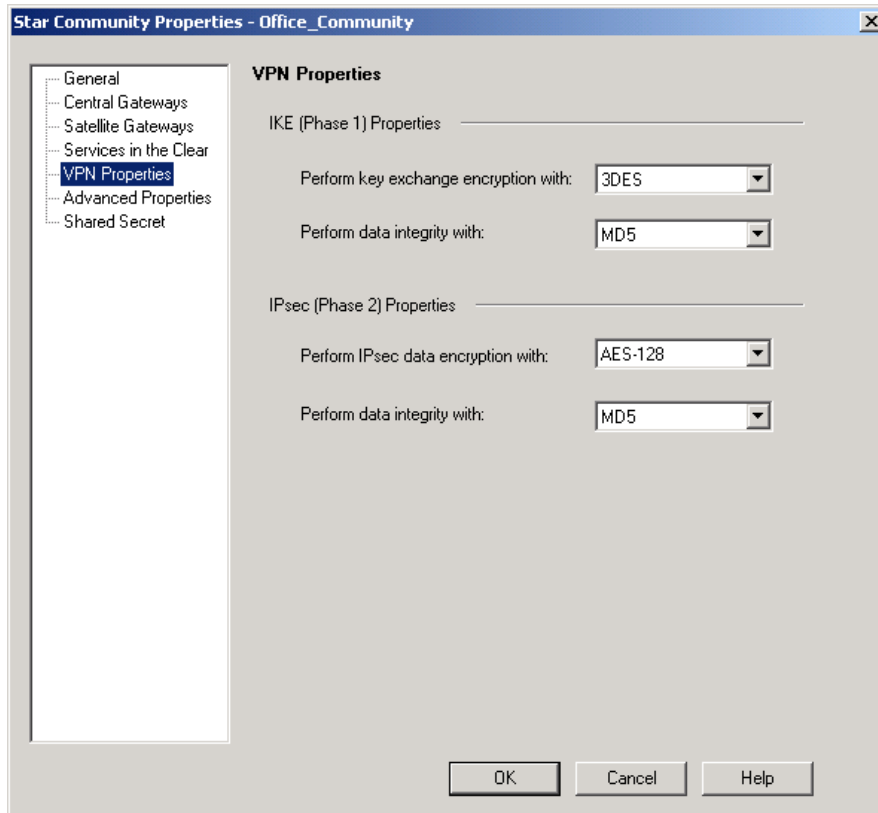
...and the **IPsec (Phase 2) Properties** tab is displayed.





- If you are using FP3, click **VPN Properties**.

The **VPN Properties** tab is displayed.



Note: In both FP2 and FP3, in Traditional mode, Phase 2 must be configured with SHA-1 and 3DES. For more information, refer to the *SofaWare VPN Configuration Guide*, page 34.

5. Create a topology user. Refer to the *SofaWare VPN Configuration Guide*, page 26.
6. Configure the rule base.



Note: The rule base shown below is only an example. Your rule base may look different depending on your network and needs.



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON
1	Office_net	internal	Office_Communit	TCP ftp	accept	Log	fp3
2	internal	Office_net	Office_Communit	TCP http	accept	Log	fp3
3	* Any	* Any	* Any	* Any	drop	Log	fp3

7. Compile the policy.

Exporting the Safe@ Gateway Object's Certificate

You must use the CertExport tool to export the Safe@ gateway object's certificate and create a *.p12 certificate file.



Important: You can only export the Safe@ gateway object's certificate *after* you have installed the policy.

Installing CertExport



Note: The CertExport tool is supported on the following platforms: win32, Solaris2, rs6000, linux22, and FreeBSD. Only win32 is supported on NG FP2.



Note: If FireWall-1 management and module are located on different machines (Distributed mode), the CertExport tool must be installed on the management server.



Note: The procedure is the same both for FP2 and FP3.

To install CertExport on win32

1. Create a directory named cert_export.
2. Surf to www.sofaware.com, and download the Cert_Export.zip file suitable for your operating system.
3. Unzip the file to the cert_export directory.



Creating a Certificate

To create a *.p12 certificate

1. Open a command prompt window, and change directory to the cert_export directory. The executable's name is vpn.exe.
2. Type `vpn export_p12 -obj <network object> -cert <certobj> -file <filename> -passwd <password>`, where:

- `<network object>` is the Safe@ gateway object name.
- `<certobj>` is the name of the certificate as it appears in Safe@ gateway object.

See the **Check Point Gateway** dialog box's **VPN** tab on page 12. The certificate's name appears in the **Certificate List** area. In this example, the certificate's name is defaultCert.

- `<filename>` is the name of the file to be created. It must be a *.p12 file.
- `<password>` is the password used to authenticate and load the *.p12 file.

For example: `cert_export export_p12 -obj Office_GW -cert defaultCert -file office_cert.p12 -passwd mypassword`



Important: The syntax is case-sensitive.

3. Press **ENTER**.

The Safe@ gateway object's certificate is exported and the *.p12 file is created in the **cert_export** directory.

Configuring the Safe@Office Appliance

To configure the Safe@Office appliance

1. Load the certificate to the Safe@Office appliance. For instructions, see the *SofaWare S-box Getting Started Guide*, "Installing a Certificate", page 111.
2. Create the VPN profile in Safe@ Office. For instructions, see the *SofaWare S-box Getting Started Guide*, "Adding and Editing VPN Sites using SofaWare Safe@Office", page 102.



While creating the VPN profile, make the following selections:

- a. In the **VPN Gateway Address** dialog box, select **Unrestricted Access**.
- b. In the **VPN Network Configuration** dialog box, select **Download Configuration**.
- c. In the **Shared Secret** dialog box, select **Use Certificate**.