

Overview

This document describes how to configure Check Point VPN-1/FireWall-1 to implement the scenarios described in the VPN Consortium's interoperability specification (<http://www.vpnc.org/interopProfiles.html>).

In This Document

<i>Network Configuration</i>	<i>page 1</i>
<i>Scenario 1 Configuration</i>	<i>page 2</i>
<i>Scenario 2 Configuration</i>	<i>page 18</i>

Network Configuration

Network Configuration Overview

FIGURE 1 shows the network configuration for both scenarios.

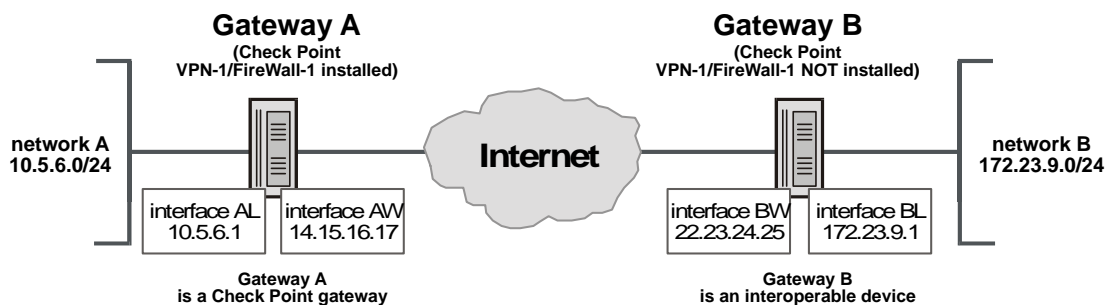


FIGURE 1 Scenario 1 Network Configuration

In VPN-1/FireWall-1, there are two methods by which a VPN can be configured:

- **simplified method** — VPN communities

A VPN community is a group of gateways that encrypt all communications among themselves, according to parameters defined for the VPN community as a whole. There is no need to define encryption rules in the Security Policy Rule Base — membership in the community implies encryption.

- **traditional method**

Using the traditional method, the administrator defines the encryption parameters for each gateway and the encryption rules in the Security Policy Rule Base.

This document describes how to configure the scenarios using the simplified configuration method.



Note - The step-by-step instructions in the following sections assume the reader has a working knowledge of Check Point VPN-1/FireWall-1, and only the parameters directly related to the scenarios are described in detail.

Scenario 1 Configuration

Scenario 1 Configuration Overview

TABLE 1 summarizes each of the phase 1 and phase 2 parameters in this scenario and specifies how they are set.

TABLE 1 Scenario 1 — Phase 1 and Phase 2 parameters

parameter	defined in...
phase 1	
Main mode	default
Triple DES	Select 3DES under Perform key exchange encryption with under IKE (Phase 1) Properties in the VPN Community's VPN Properties page (FIGURE 23 on page 14).
SHA-1	Select SHA-1 under Perform data integrity with under IKE (Phase 1) Properties in the VPN Community's VPN Properties page (FIGURE 23 on page 14).
MODP group 2	Select Group 2 (1024 bit) in Use Diffie-Hellman group under IKE (Phase 1) in the VPN Community's Advanced VPN Properties page (FIGURE 24 on page 15).
pre-shared secret	<ul style="list-style-type: none"> ▪ Enable for the VPN Community by checking Use only Shared Secret for all External members in the VPN Community's Shared Secret page (FIGURE 25 on page 16). ▪ Define a pre-shared secret for Gateway B in the Shared Secret page (FIGURE 26 on page 16).
SA lifetime	Specify a value for Renegotiate IKE security associations every ... minutes under IKE (Phase 1) in the VPN Community's Advanced VPN Properties page (FIGURE 24 on page 15).
phase 2	
Triple DES	Select 3DES under Perform IPSec data encryption with under IKE (Phase 2) Properties in the VPN Community's VPN Properties page (FIGURE 23 on page 14).
SHA-1	Select SHA-1 under Perform data integrity with under IKE (Phase 2) Properties in the VPN Community's VPN Properties page (FIGURE 23 on page 14).
ESP tunnel mode	default; cannot be changed
MODP group 2	Select Group 2 (1024 bit) in Use Diffie-Hellman group under IKE (Phase 2) in the VPN Community's Advanced VPN Properties page (FIGURE 24 on page 15).

TABLE 1 Scenario 1 — Phase 1 and Phase 2 parameters (continued)

parameter	defined in...
Perfect Forward Secrecy	Check Use Perfect Forward Secrecy under IKE (Phase 2) in the VPN Community's Advanced VPN Properties page (FIGURE 24 on page 15).
SA lifetime	Specify a value for Renegotiate IKE security associations every ... seconds under IKE (Phase 2) in the VPN Community's Advanced VPN Properties page (FIGURE 24 on page 15).
between 10.5.6.0/24 and 172.23.9.0/24	In the Topology page of the gateway's Properties window (for example, FIGURE 8 on page 7), select All IP addresses behind gateway based on topology .

Configuration Step-By-Step

To implement this scenario, you will perform the following:

- create a new policy
- define a VPN Community
- define Gateway A and add it to the VPN Community
- define Gateway B and add it to the VPN Community
- define the VPN Community's encryption and authentication parameters
- save and install the policy

In This Section

<i>Create a New Policy</i>	<i>page 3</i>
<i>Define a VPN Community</i>	<i>page 4</i>
<i>Define Gateway A</i>	<i>page 5</i>
<i>Define Gateway B</i>	<i>page 10</i>
<i>Define the VPN Community Parameters</i>	<i>page 13</i>
<i>Save and Install the Policy</i>	<i>page 16</i>
<i>Define Routing</i>	<i>page 17</i>

Create a New Policy

- 1** Choose **File-->New** from the menu to create a new Policy.

2 In the **New Policy Package** window (FIGURE 2):

- Enter a name for the Policy.
- Check **Security and Address Translation**.

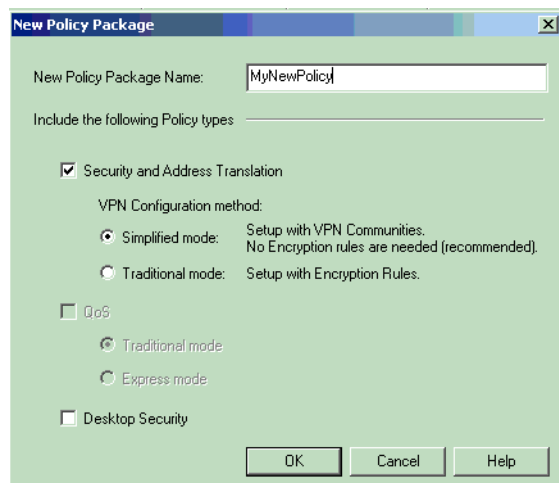


FIGURE 2 New Policy Package window

Define a VPN Community

3 Click the **VPN Manager** tab (FIGURE 3).



FIGURE 3 Policy tabs

- 4 Right click in the upper pane (below the tabs) and select **New Community --> Meshed**.

In the **General** page of the VPN Community's **Properties** window (FIGURE 4), specify the name of the VPN Community.

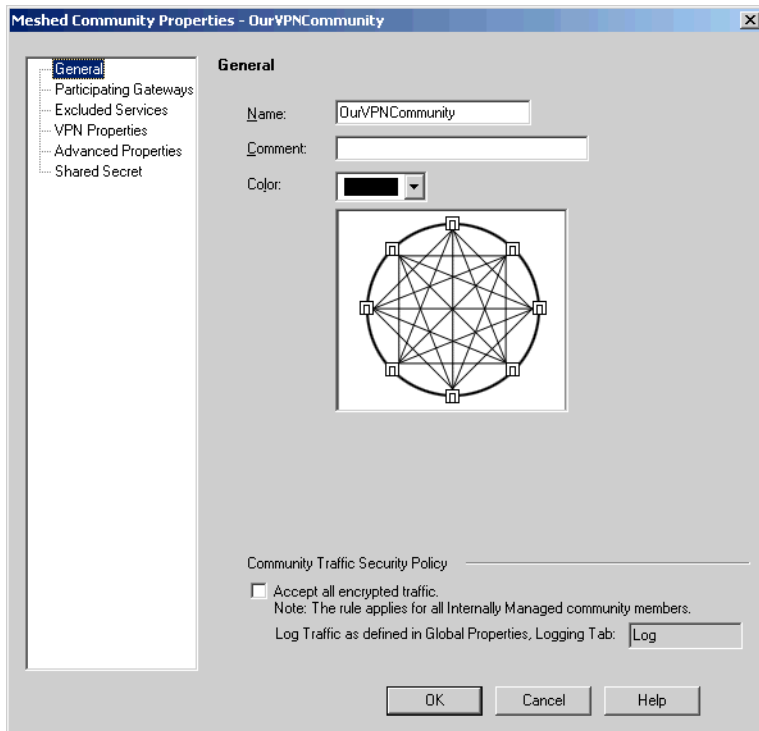


FIGURE 4 General page of VPN Community's Properties window

Define Gateway A

Gateway A — General Properties

- 5 In the object tray at the left of the screen (FIGURE 5), right-click **Check Point** and select **New Check Point --> Gateway**.

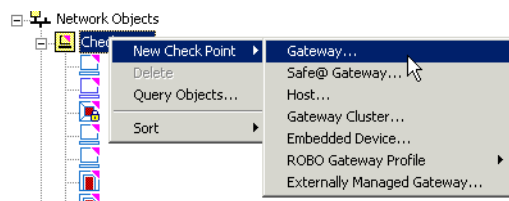


FIGURE 5 Defining a new gateway from the tray

6 Select **Classic Mode** (FIGURE 6).

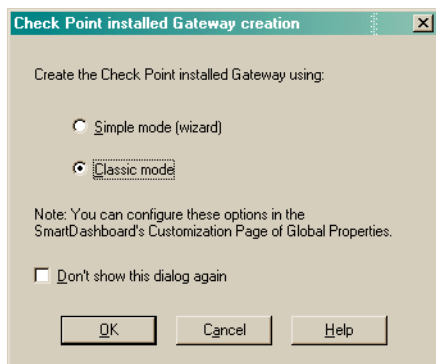


FIGURE 6 Gateway Creation Mode window

7 Define Gateway A as shown below (FIGURE 7).

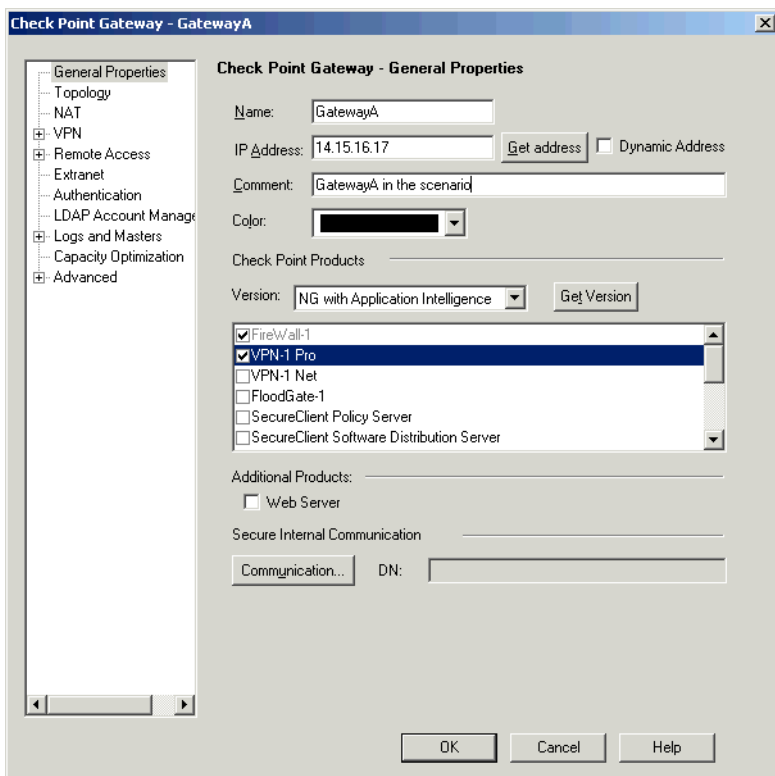


FIGURE 7 Gateway A General Properties

Gateway A — Topology

8 Open the **Topology** page (FIGURE 8).

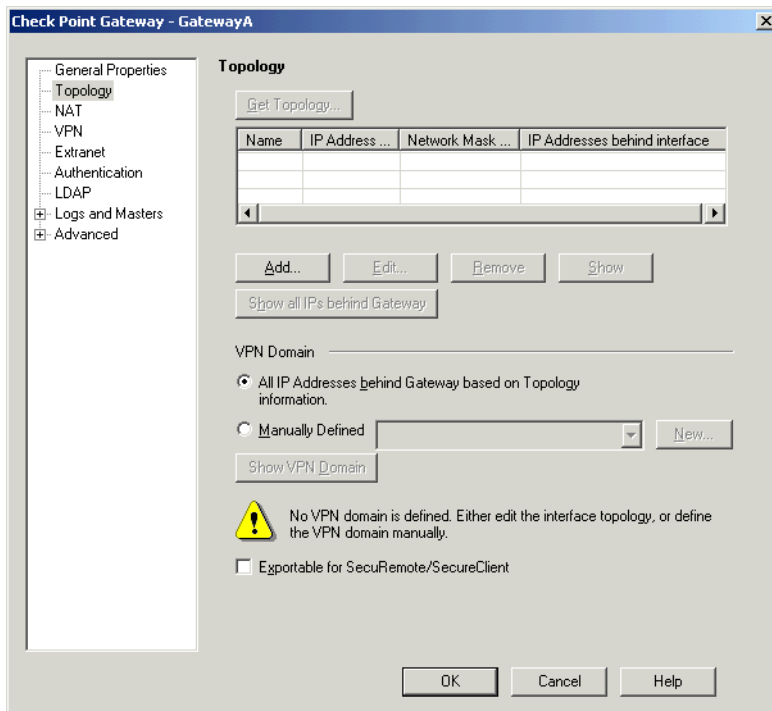


FIGURE 8 Gateway A Topology page

9 Under **VPN Domain**, select **All IP addresses behind gateway based on topology information**.

10 Click **Add** to define the interfaces.

11 Define interface AL as shown below (FIGURE 9).

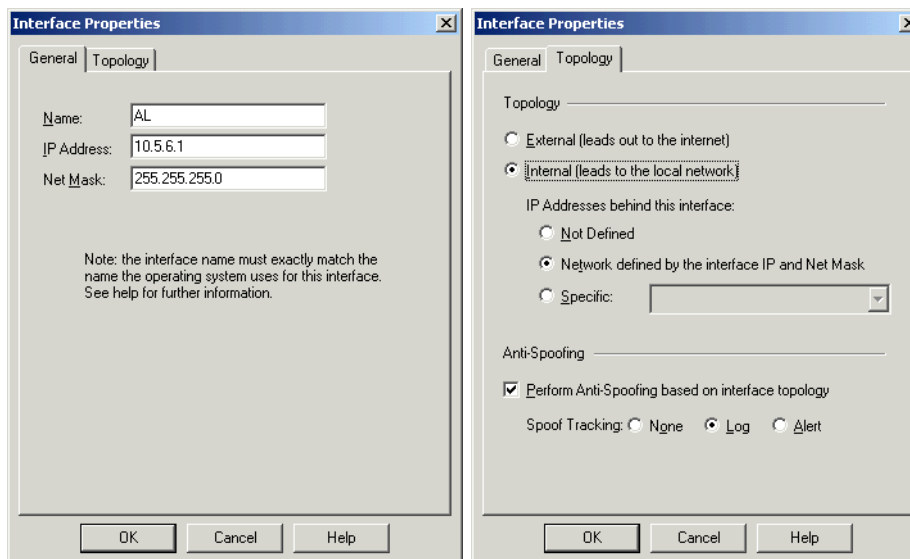


FIGURE 9 Gateway A Interface AL Properties

12 Define interface AW as shown below (FIGURE 10).

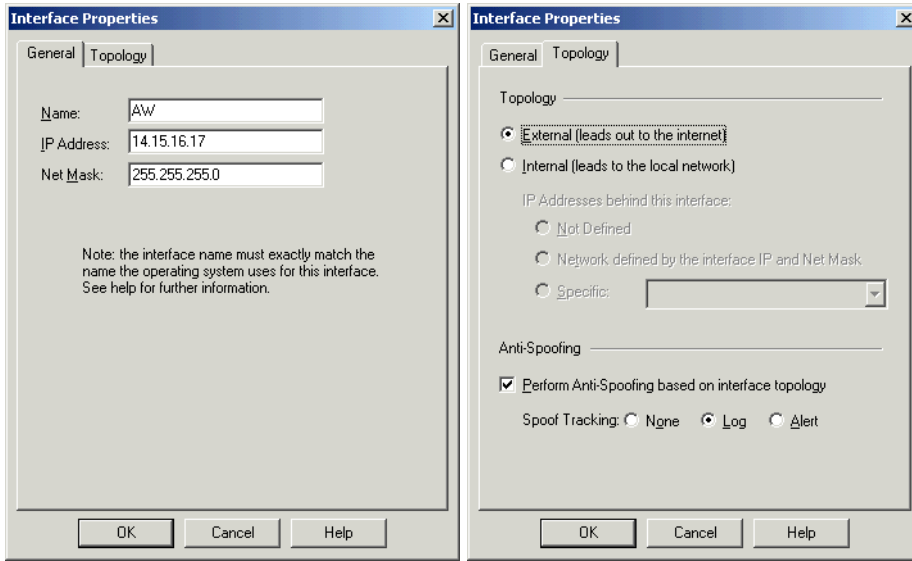


FIGURE 10 Gateway A Interface AW Properties

Gateway A's topology is shown in FIGURE 11.

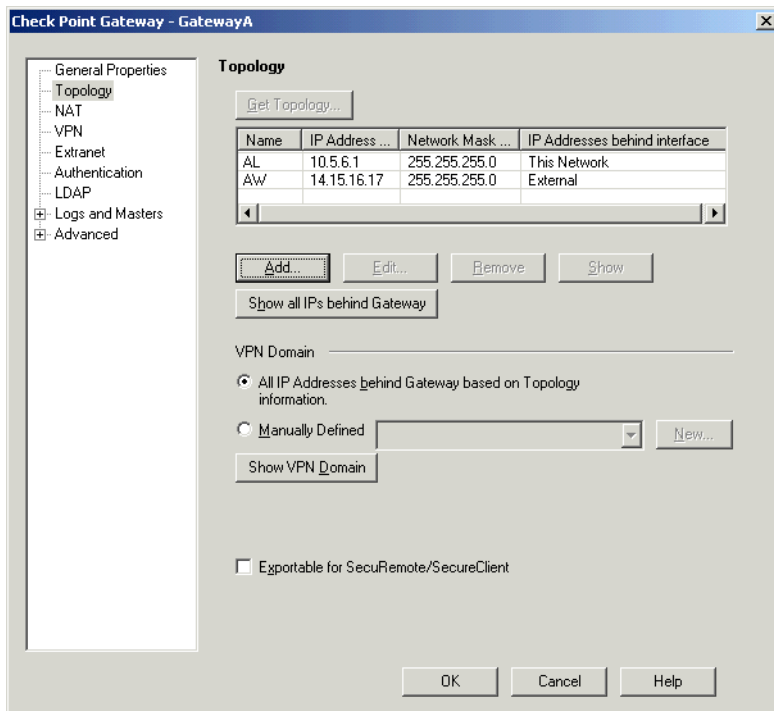


FIGURE 11 Gateway A Topology

Gateway A — VPN

13 Open the **VPN** page (FIGURE 12) and click **Add** (under **VPN**).

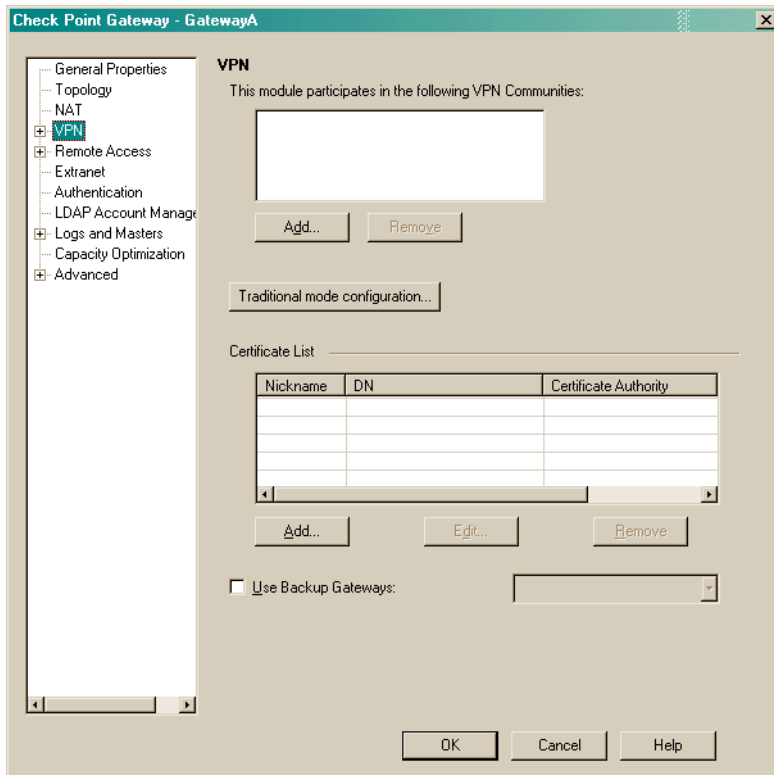


FIGURE 12 Gateway A VPN page

In the **Add This Gateway to Community** window (FIGURE 13), select the VPN Community you defined earlier (FIGURE 4 on page 5) and click **OK**.

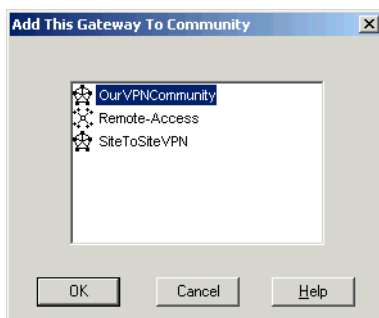


FIGURE 13 Add This Gateway to Community

Define Gateway B

Gateway B — General Properties

14 In the object tray at the left of the screen (FIGURE 14):

- Right-click Network Objects.
- Select **New --> Interoperable Devices**.

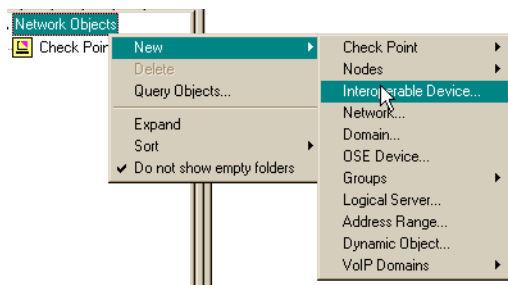


FIGURE 14 Defining an interoperable device from the object tray

15 Define Gateway B as shown below (FIGURE 15).

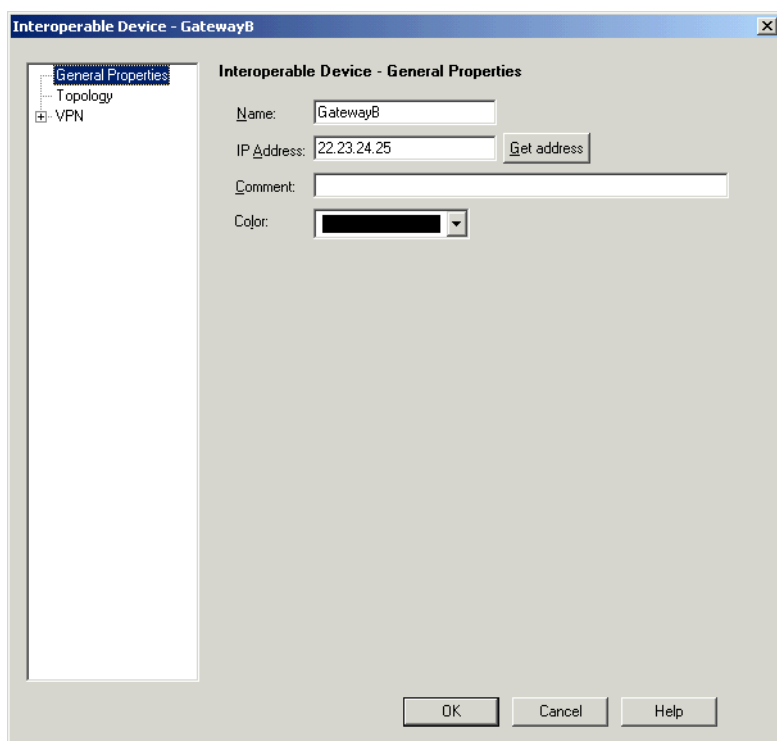


FIGURE 15 Gateway B General Properties

16 Open the **Topology** page (FIGURE 16).

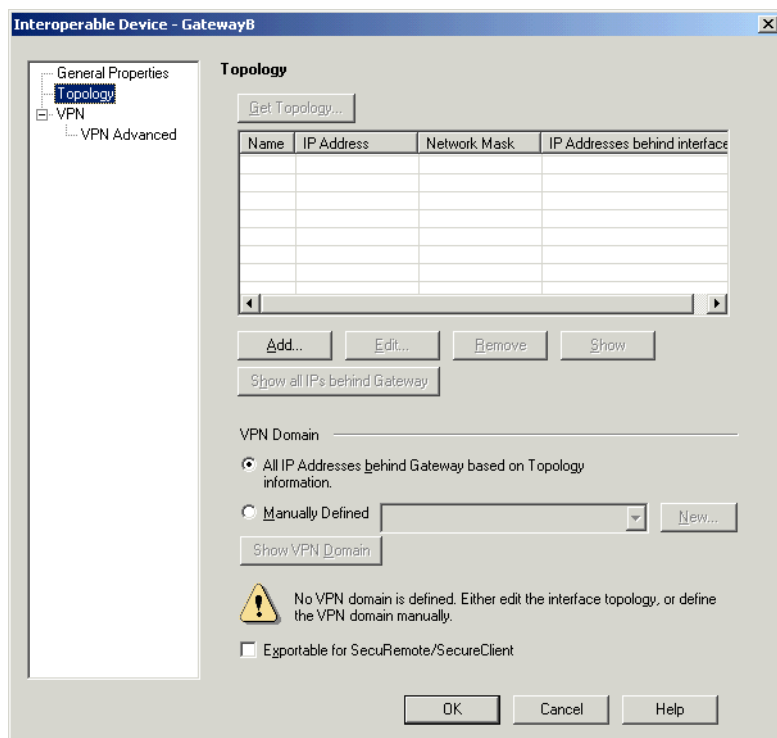


FIGURE 16 Gateway B Topology page

17 Under **VPN Domain**, select **All IP addresses behind gateway based on topology information**.

18 Click **Add** to define the interfaces.

19 Define interface BW as shown below (FIGURE 17).

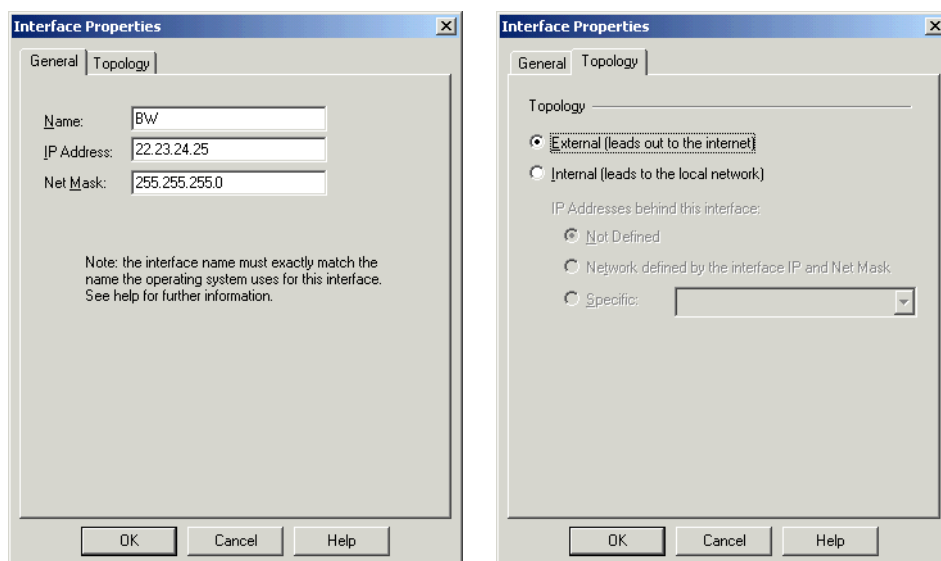


FIGURE 17 Gateway B Interface BW Properties

20 Define interface BL as shown below (FIGURE 18).

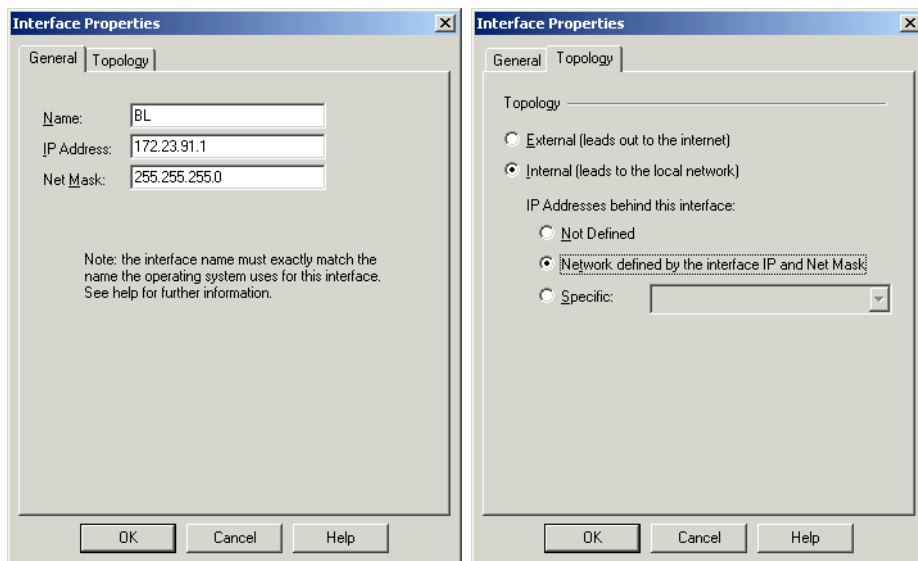


FIGURE 18 Gateway B Interface BL Properties

Gateway B — VPN

21 Open the **VPN** page (FIGURE 19) and click **Add** (under **VPN**).

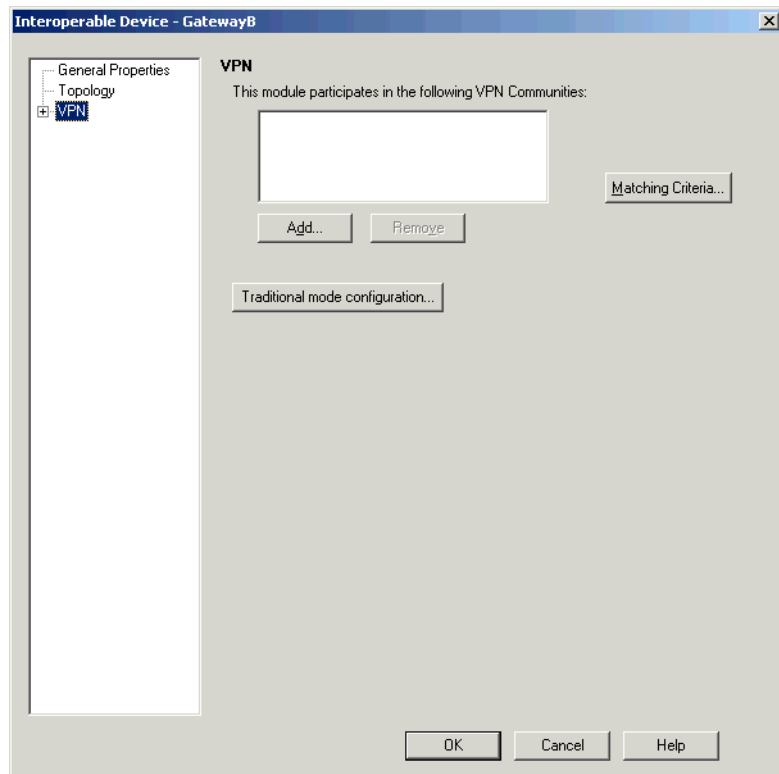


FIGURE 19 Gateway B VPN page

22 In the **Add This Gateway to Community** window (FIGURE 13), select the VPN Community you defined earlier (FIGURE 4 on page 5) and click **OK**.

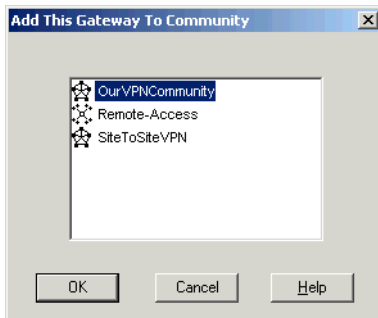


FIGURE 20 Add This Gateway to Community
Define the VPN Community Parameters

23 Double-click on the VPN Community's icon (FIGURE 21).

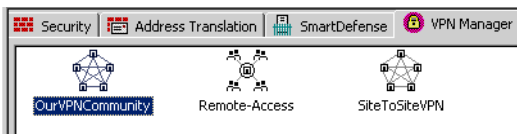


FIGURE 21 VPN Communities

In the **Participating Gateways** page (FIGURE 22), you can see both GatewayA and GatewayB.

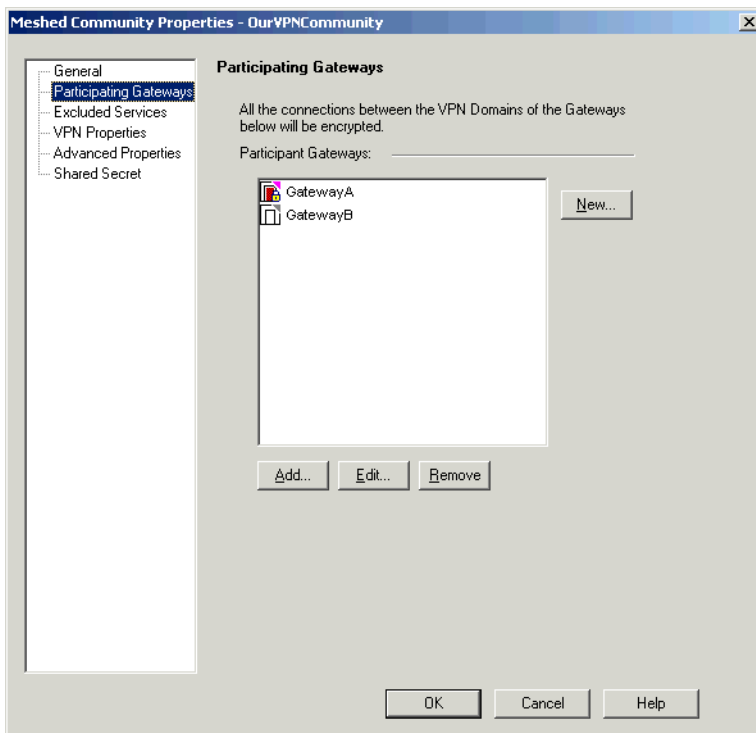


FIGURE 22 Participating Gateways page

24 In the **VPN Properties** page (FIGURE 23), set the IKE (Phase 1) and IPsec (Phase 2) properties (see TABLE 1 on page 2).

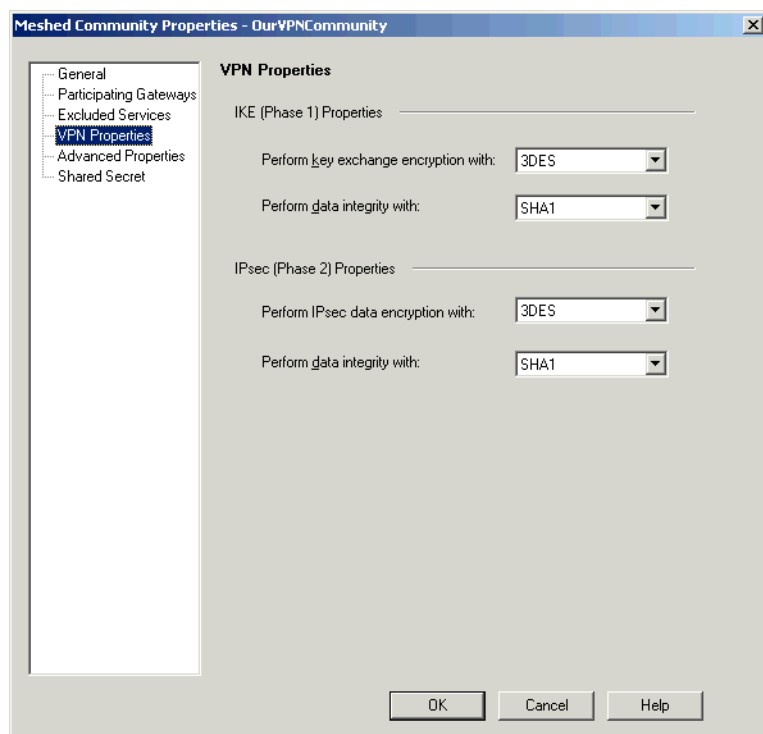


FIGURE 23 VPN Properties page

25 In the **Advanced Properties** page (FIGURE 24), set additional IKE (Phase 1) and IPsec (Phase 2) properties (see TABLE 1 on page 2).

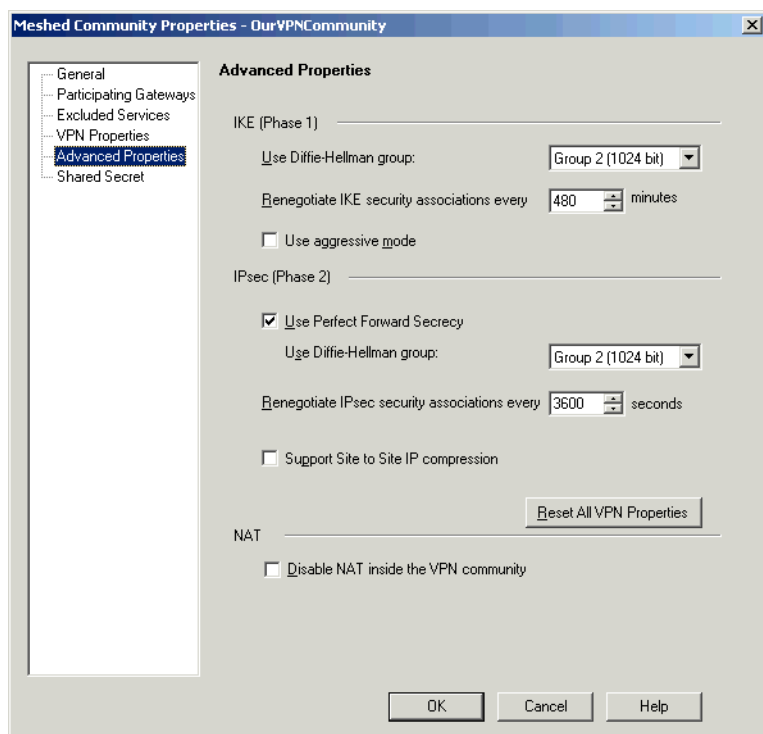


FIGURE 24 Advanced Properties page

26 In the **Shared Secret** page (FIGURE 25), check **Use only shared secrets for all external members**.

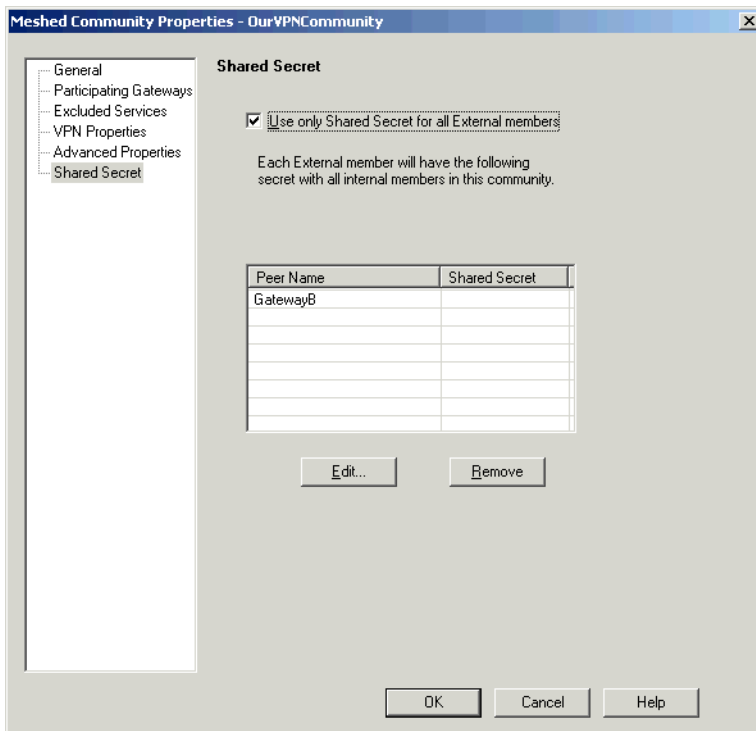


FIGURE 25 Shared Secret page



Note - Shared secrets can be used only when one of the gateways is not managed by Check Point.

27 Select Gateway B under **Peer Name** and click **Edit**.

28 Enter the pre-shared secret (“hr5xb84l6aa9r6”) and click **Set**.

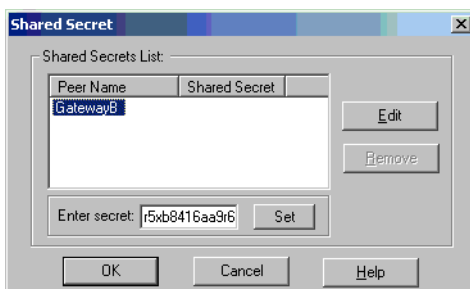


FIGURE 26 Shared Secret window

Save and Install the Policy

29 Define a security policy that will allow the required encrypted communication. (FIGURE 27)

Add a rule using **Rules -->Add rule -->top**

30 Edit the rule:

VPN: **Edit cell...** and select **Only connections encrypted in any Site-to-Site VPN Community**

- 31** Service: Specify the allowed services that are to be encrypted (eg: **Authenticated** Group, and **icmp-proto**)
- 32** Action: Change to **Accept**
- 33** Track: Change to **Log**
- 34** Add a final rule to drop any other communication **Rules -->Add Rule -->Bottom**
- 35** Save the Policy **File -->Save**

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	* Any	All_GwToGw	Authenticated icmp-proto	accept	Log
2	* Any	* Any	* Any Traffic	* Any	drop	- None

FIGURE 27 The Security Policy

- 36** Save the Policy.
- 37** Install the Policy on Gateway A.

Define Routing

- 38** In the Operating System, define Gateway A's default gateway.

Configuration Complete

All communications between Gateway A and Gateway B will be encrypted.
The configuration for scenario 1 is now complete.

Scenario 2 Configuration

Scenario 2 Configuration Overview

Scenario 2 is identical to scenario 1, except that identification is performed using signatures authenticated by PKIX certificates.

TABLE 2 summarizes each of the phase 1 and phase 2 parameters in this scenario and specifies how they are set.

TABLE 2 Scenario 2 — Phase 1 and Phase 2 parameters

parameter	defined in...
phase 1	
Main mode	default
Triple DES	Select 3DES under Perform key exchange encryption with under IKE (Phase 1) Properties in the VPN Community's VPN Properties page (FIGURE 52 on page 34).
SHA-1	Select SHA-1 under Perform data integrity with under IKE (Phase 1) Properties in the VPN Community's VPN Properties page (FIGURE 52 on page 34).
MODP group 2	Select Group 2 (1024 bit) in Use Diffie-Hellman group under IKE (Phase 1) in the VPN Community's Advanced VPN Properties page (FIGURE 53 on page 35).
PKIX certificate	Create for each gateway in the VPN page of its Properties window (for example, FIGURE 41 on page 27).
SA lifetime	Specify a value for Renegotiate IKE security associations every ... minutes under IKE (Phase 1) in the VPN Community's Advanced VPN Properties page (FIGURE 53 on page 35).
phase 2	
Triple DES	Select 3DES under Perform IPSec data encryption with under IKE (Phase 2) Properties in the VPN Community's VPN Properties page (FIGURE 52 on page 34).
SHA-1	Select SHA-1 under Perform data integrity with under IKE (Phase 2) Properties in the VPN Community's VPN Properties page (FIGURE 52 on page 34).
ESP tunnel mode	default; cannot be changed
MODP group 2	Select Group 2 (1024 bit) in Use Diffie-Hellman group under IKE (Phase 2) in the VPN Community's Advanced VPN Properties page (FIGURE 53 on page 35).
Perfect Forward Secrecy	Check Use Perfect Forward Secrecy under IKE (Phase 2) in the VPN Community's Advanced VPN Properties page (FIGURE 53 on page 35).
SA lifetime	Specify a value for Renegotiate IKE security associations every ... seconds under IKE (Phase 2) in the VPN Community's Advanced VPN Properties page (FIGURE 53 on page 35).
selectors for all IP protocols, all ports	In the Topology page of the gateway's Properties window (for example, FIGURE 40 on page 26), select All IP addresses behind gateway based on topology .
between 10.5.6.0/24 and 172.23.9.0/24	Select 3DES under Perform IPSec data encryption with under IKE (Phase 2) Properties in the VPN Community's VPN Properties page (FIGURE 52 on page 34).

Configuration Step-By-Step

To implement this scenario, you will perform the following:

- create a new policy
- define a Certificate Authority for both Gateway A and Gateway B
- define a VPN Community
- define Gateway A, generate its certificate and add the gateway to the VPN Community
- define Gateway B, generate its certificate and add the gateway to the VPN Community
- define the VPN Community's encryption and authentication parameters
- save and install the policy

In This Section

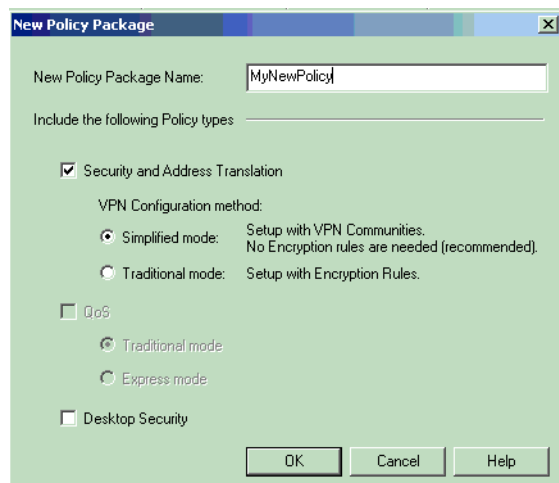
<i>Create a New Policy</i>	<i>page 19</i>
<i>Define a VPN Community</i>	<i>page 20</i>
<i>Define a Certificate Authority</i>	<i>page 21</i>
<i>Get the Certificate Authority's Own Certificate</i>	<i>page 22</i>
<i>Define Gateway A</i>	<i>page 23</i>
<i>Adding the Gateway's Certificate</i>	<i>page 27</i>
<i>Define Gateway B</i>	<i>page 29</i>
<i>Define the VPN Community Parameters</i>	<i>page 33</i>
<i>Advanced Properties page</i>	<i>page 35</i>
<i>Define Routing</i>	<i>page 36</i>

Create a New Policy

- 1** Choose **File-->New** from the menu to create a new Policy.

2 In the **New Policy Package** window (FIGURE 28):

- Enter a name for the Policy.
- Check **Security and Address Translation**.

**FIGURE 28** New Policy Package window

Define a VPN Community

3 Click the **VPN Manager** tab (FIGURE 29).**FIGURE 29** Policy tabs

- 4 Right click in the upper pane (below the tabs) and select **New Community --> Meshed**.

In the **General** page of the VPN Community's **Properties** window (FIGURE 30), specify the name of the VPN Community.

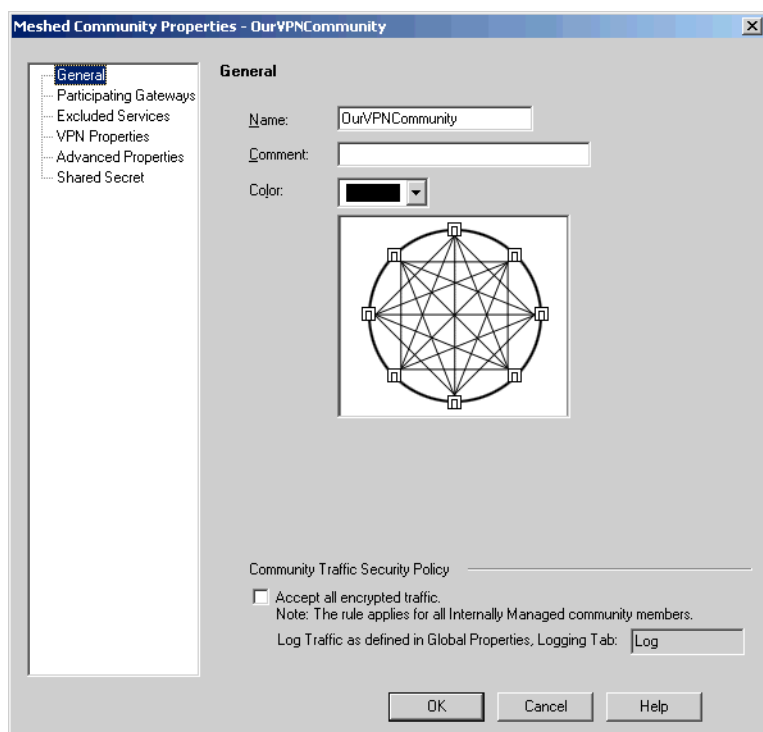


FIGURE 30 General page of VPN Community's Properties window

Define a Certificate Authority

- 5 From the menu, choose **Manage-->Servers and OPSEC Applications**.

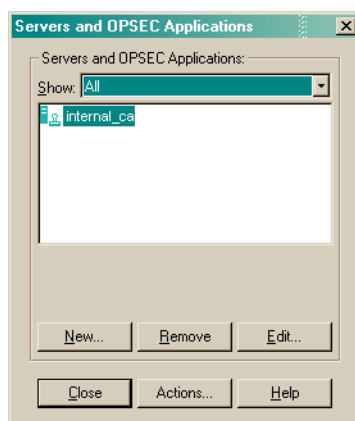


FIGURE 31 Servers and OPSEC Applications window

- 6 In the **Servers and OPSEC Applications** window (FIGURE 31), click **New** and choose **Certificate Authority** from the menu (FIGURE 32).

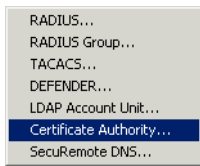


FIGURE 32 New Certificate Authority

- 7 In the **Certificate Authority Properties** window (FIGURE 33), specify a name and select **OPSEC PKI** under **Certificate Authority**.

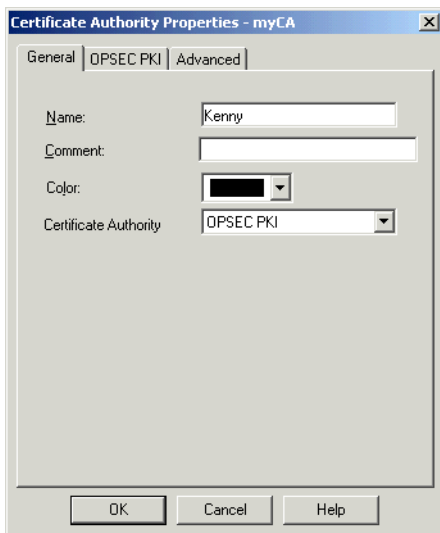


FIGURE 33 Certificate Authority Properties window — General tab

Get the Certificate Authority's Own Certificate

- 8 You must now get and save the Certificate Authority's own certificate from the Certificate Authority. Follow the procedure defined by the Certificate Authority for this step.

- 9 In the **OPSEC PKI** tab (FIGURE 34), click **Get** and browse to the certificate you saved in the previous step.

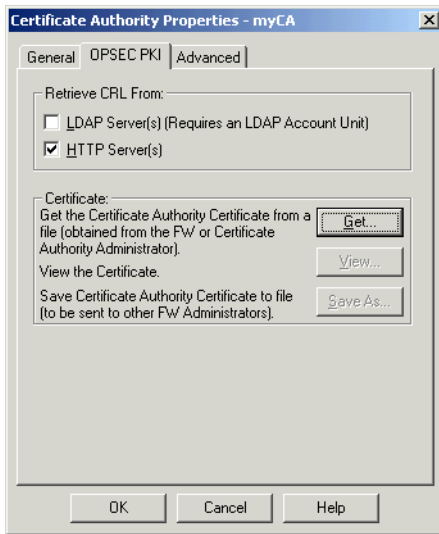


FIGURE 34 Certificate Authority Properties window — OPSEC PKI tab

Define Gateway A

Gateway A — General Properties

- 10 In the object tray at the left of the screen (FIGURE 35), right-click **Check Point** and select **New Check Point --> Gateway**.

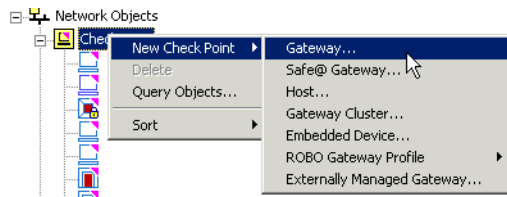
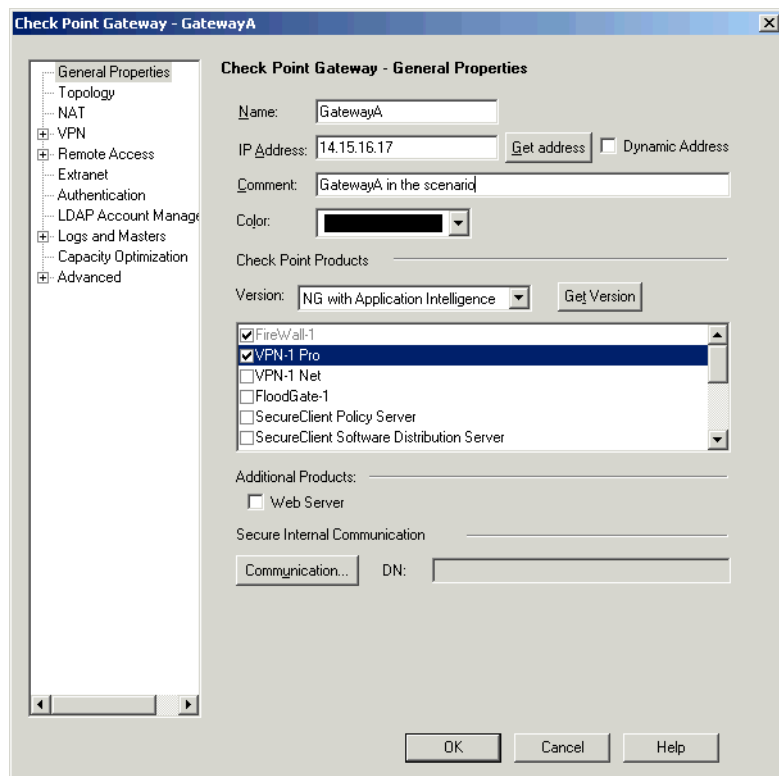


FIGURE 35 Defining a new gateway from the tray

11 Define Gateway A as shown below (FIGURE 36).**FIGURE 36** Gateway A General Properties

Gateway A — Topology

12 Open the **Topology** page (FIGURE 37).

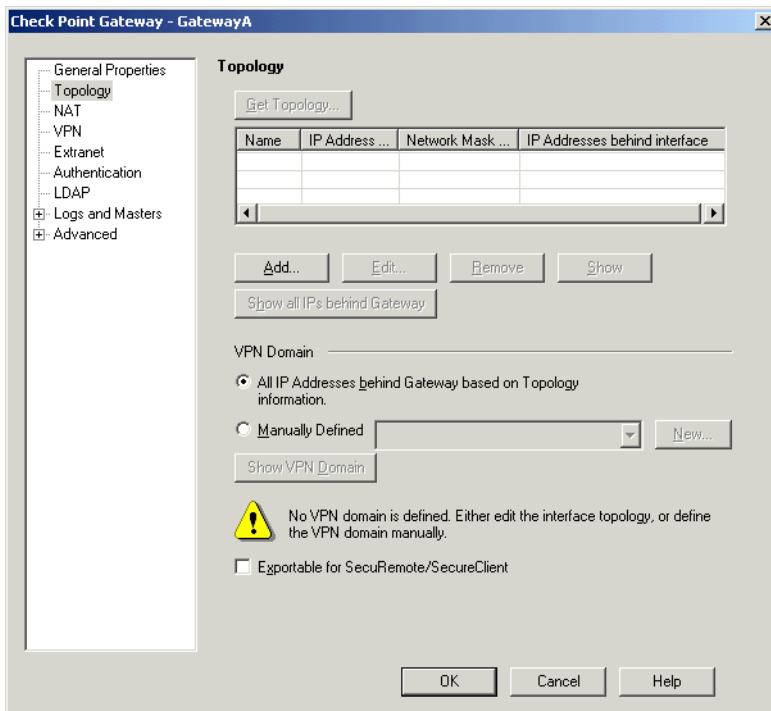


FIGURE 37 Gateway A Topology page

13 Under **VPN Domain**, select **All IP addresses behind gateway based on topology information**.

14 Click **Add** to define the interfaces.

15 Define interface AL as shown below (FIGURE 38).

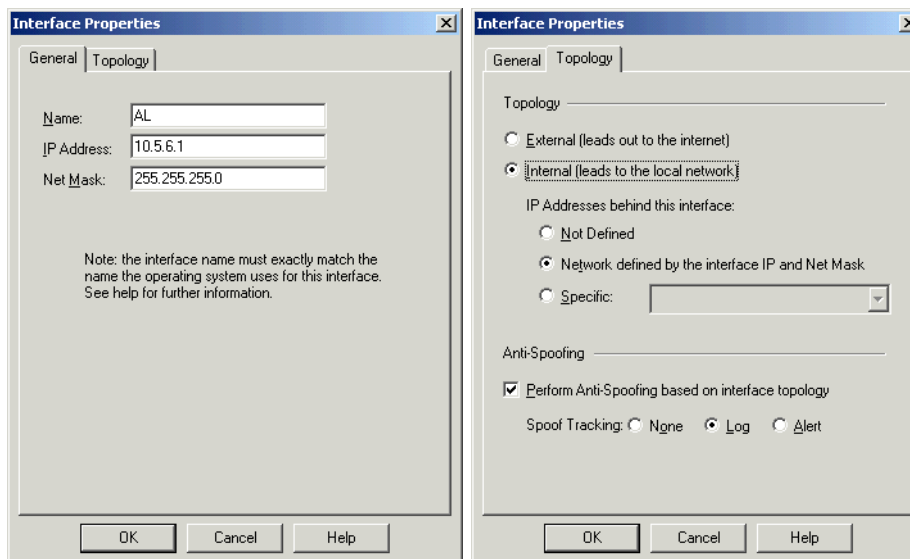


FIGURE 38 Gateway A Interface AL Properties

16 Define interface AW as shown below (FIGURE 39).

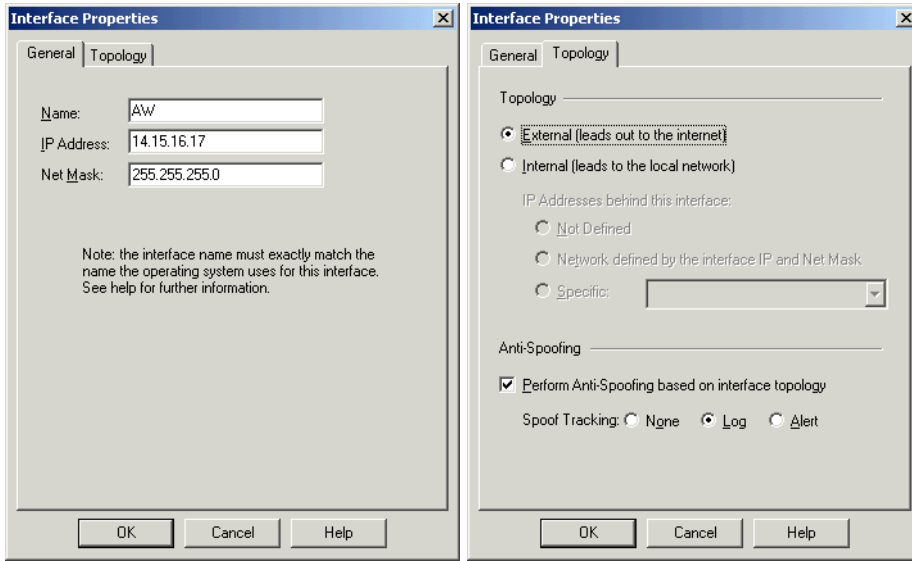


FIGURE 39 Gateway A Interface AW Properties

Gateway A's topology is shown in FIGURE 40.

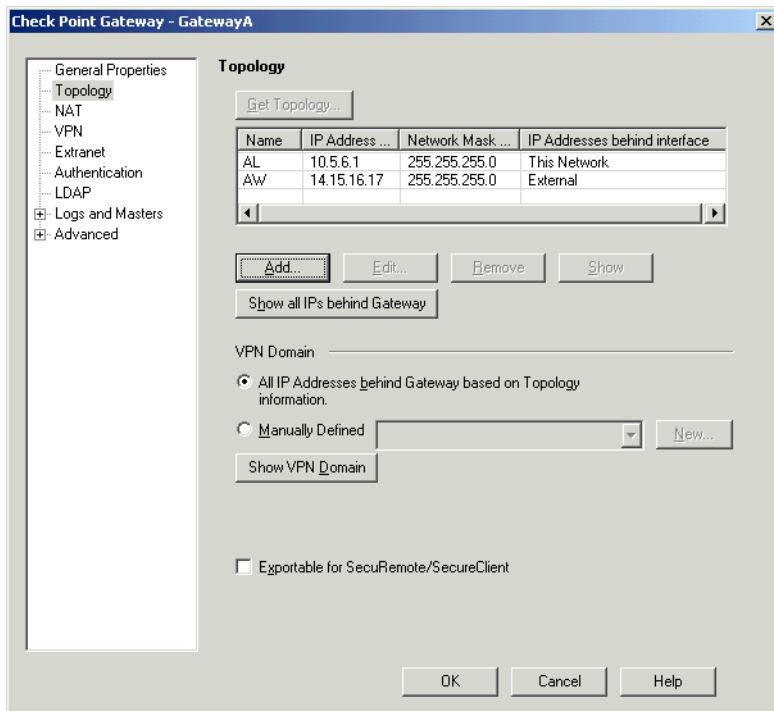


FIGURE 40 Gateway A Topology

Gateway A — VPN

17 Open the **VPN** page (FIGURE 41) and click **Add** (under **VPN**).

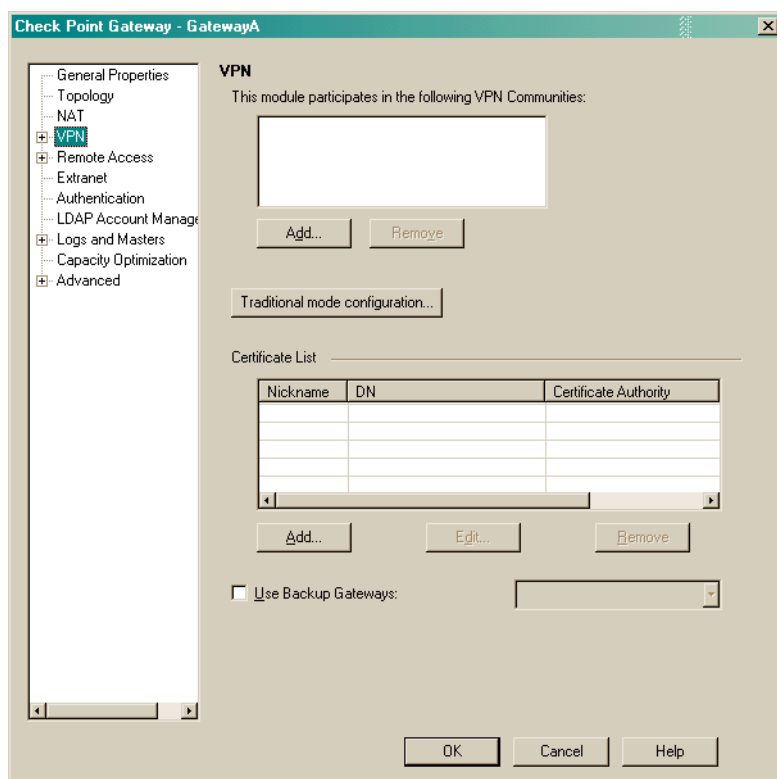


FIGURE 41 Gateway A VPN page

18 In the **Add This Gateway to Community** window (FIGURE 42), select the VPN Community you defined earlier (FIGURE 30 on page 21) and click **OK**.

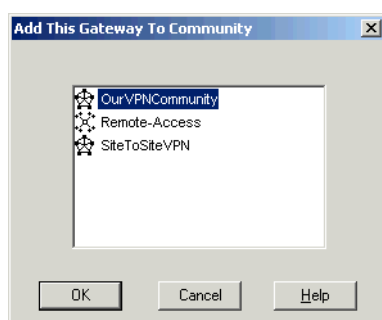


FIGURE 42 Add This Gateway to Community

Adding the Gateway's Certificate

19 In the **VPN** page of Gateway A's **Properties** window (FIGURE 41), click **Add** (under **Certificates**) to open the **Certificate Properties** window (FIGURE 43).

Adding a gateway's certificate consists of the following:

- Generating a certificate request, that is, a request for the Certificate Authority to issue a certificate for this gateway (step 22 on page 28).
- Submitting the certificate request to the Certificate Authority (step 23 on page 28).

- Getting the certificate from the Certificate Authority (after it has been issued) and saving it to a file (step 24 on page 28).
- Adding the certificate to the gateway (step 25 on page 29).

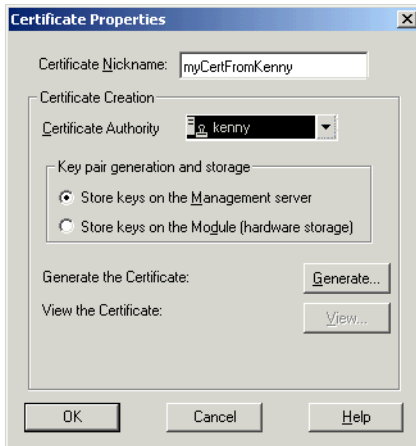


FIGURE 43 Certificate Properties window

- 20** Specify a nickname for the certificate.
- 21** Select a Certificate Authority.



Note - The Certificate Authority "kenny" was defined earlier (see "Define a Certificate Authority" on page 21).

- 22** Click **Generate**.

A certificate request will be created for submission to the Certificate Authority.

- 23** Submit the certificate request to the Certificate Authority.

The details of how to do this depend on the Certificate Authority.

- 24** Get the certificate from the Certificate Authority and save it in a file.

The details of how to do this depend on the Certificate Authority.

- 25** Add the certificate to the gateway by clicking **Get** in the **Certificate Properties** window (FIGURE 44) and browsing to the file you saved in the previous step.

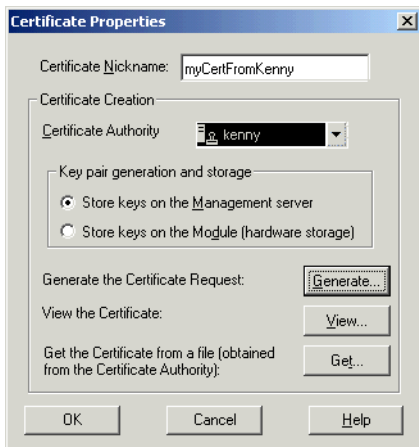


FIGURE 44 Certificate Properties window after certificate request was generated

Define Gateway B

Gateway B — General Properties

- 26** In the object tray at the left of the screen (FIGURE 14), right-click **Interoperable Devices** and select **New Interoperable Device**.

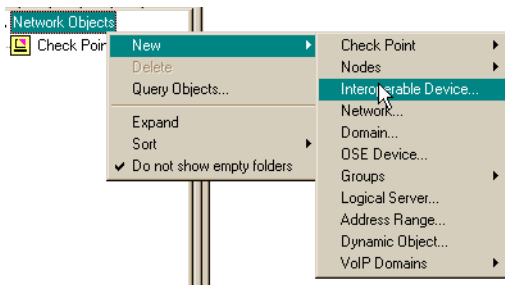
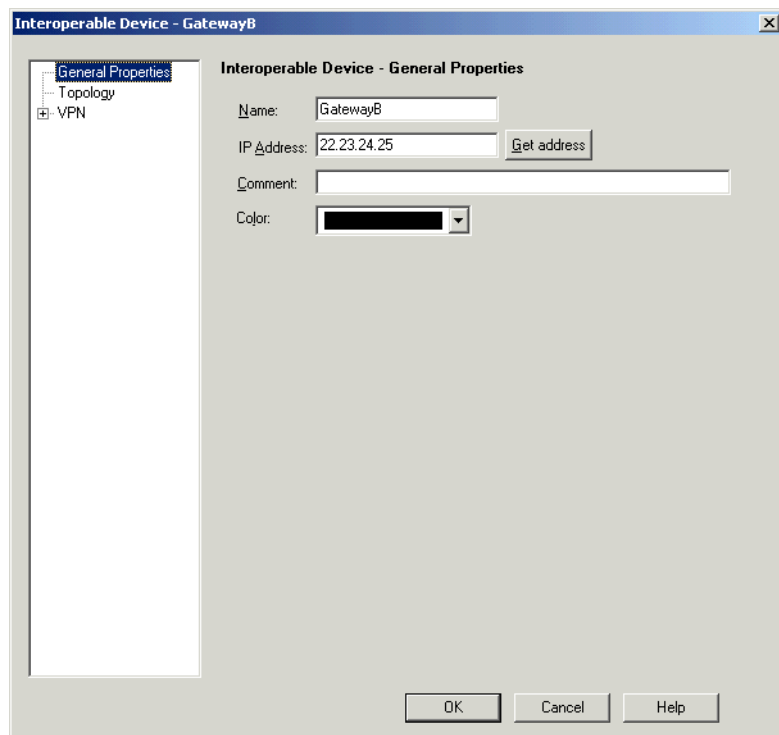


FIGURE 45 Defining an interoperable device from the object tray

27 Define Gateway B (FIGURE 46).**FIGURE 46** Gateway B General Properties

28 Open the **Topology** page (FIGURE 47).

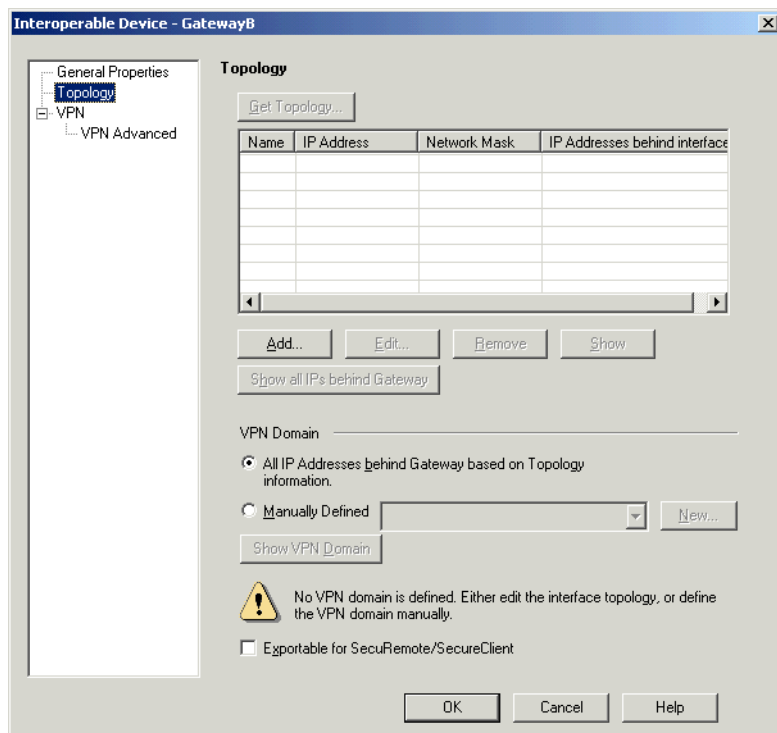


FIGURE 47 Gateway B Topology page

29 Under **VPN Domain**, select **All IP addresses behind gateway based on topology information**.

30 Click **Add** to define the interfaces.

31 Define interface BW as shown below (FIGURE 48).

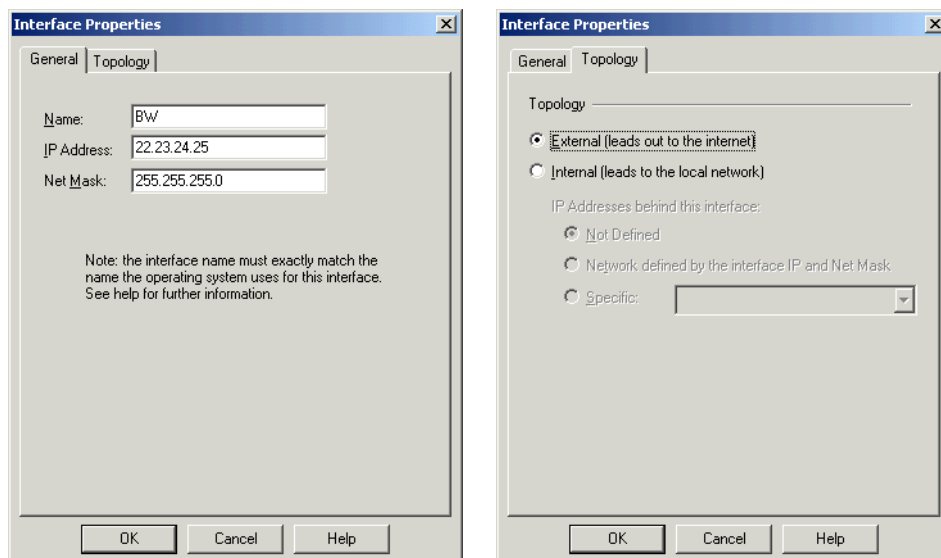
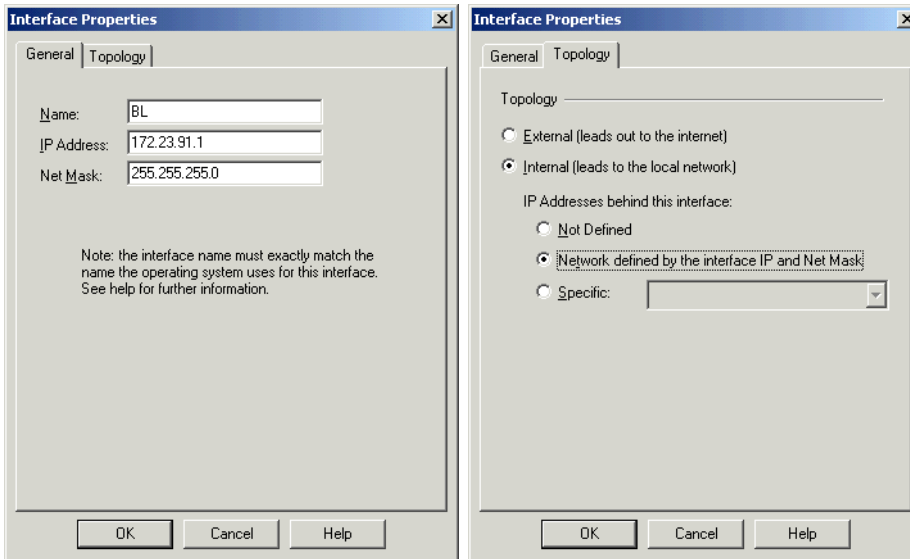


FIGURE 48 Gateway B Interface BW Properties

32 Define interface BL as shown below (FIGURE 49).**FIGURE 49** Gateway B Interface BL Properties

Gateway B — VPN

33 Generate a certificate for Gateway B in the same way you generated a certificate for Gateway A (see step 19 on page 27 through step 26 on page 29).

Define the VPN Community Parameters

34 Double-click on the VPN Community's icon (FIGURE 50).

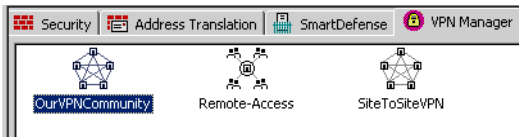


FIGURE 50 VPN Communities

In the **Participating Gateways** page (FIGURE 51), you can see both GatewayA and GatewayB.

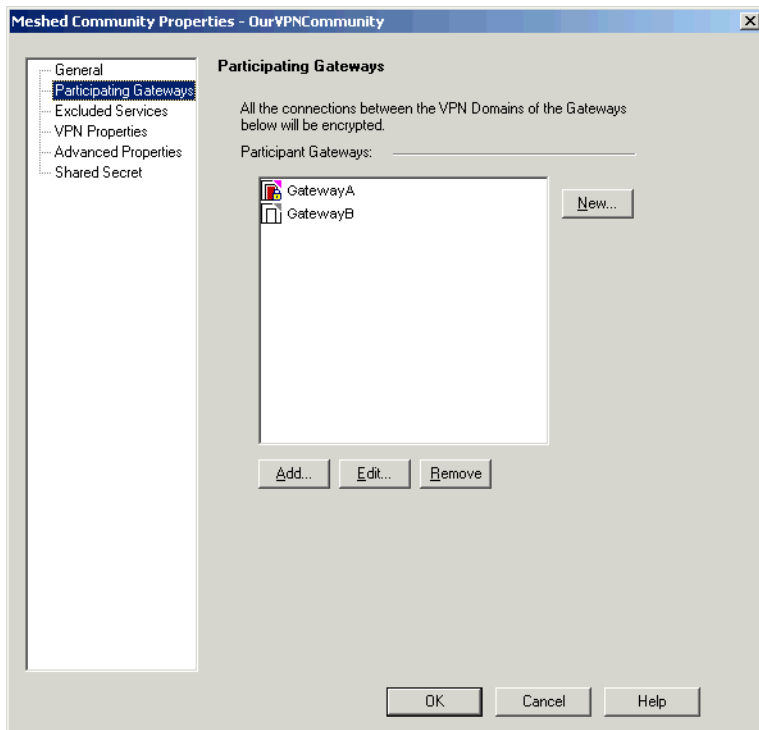


FIGURE 51 Participating Gateways page

35 In the **VPN Properties** page (FIGURE 52), set the IKE (Phase 1) and IPsec (Phase 2) properties (see TABLE 1 on page 2).

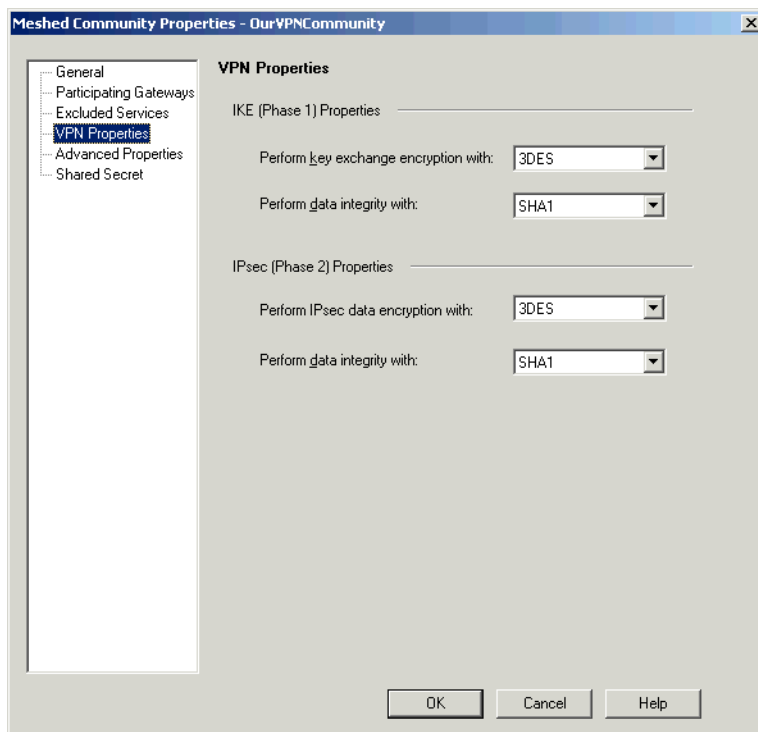


FIGURE 52 VPN Properties page

36 In the **Advanced Properties** page (FIGURE 53), set additional IKE (Phase 1) and IPsec (Phase 2) properties (see TABLE 1 on page 2).

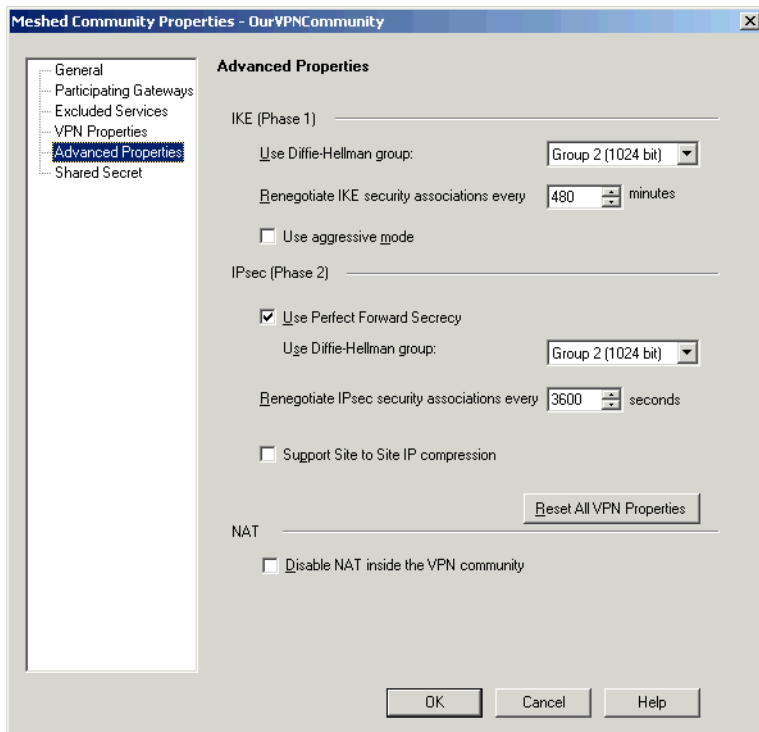


FIGURE 53 Advanced Properties page

37 Define a security policy that will allow the required encrypted communication. (Figure 53)

Add a rule using **Rules -->Add rule -->top**

38 Edit the rule:

VPN: **Edit cell...** and select **Only connections encrypted in any Site-to-Site VPN Community**

39 Service: Specify the allowed services that are to be encrypted (eg: **Authenticated** Group, and **icmp-proto**)

40 Action: Change to **Accept**

41 Track: Change to **Log**

42 Add a final rule to drop any other communication **Rules -->Add Rule -->Bottom**

43 Save the Policy **File -->Save**

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	* Any	All_GwToGw	Authenticated icmp-proto	accept	Log
2	* Any	* Any	* Any Traffic	* Any	drop	- None

FIGURE 54 The Security Policy

44 Install the Policy on Gateway A.

Define Routing

45 In the Operating System, define Gateway A's default gateway.

Configuration Complete

All communications between Network A and Network B will now be encrypted by Gateway A and Gateway B.
The configuration for scenario 2 is now complete.