AudioCodes

Multi-Service Business Gateway (MSBG)

Configuration Note

AudioCodes MSBG Site-to-Site VPN

With

Check Point Firewall

AudioCodes
Connecting Networks

Table of Contents

1 Components Information 7

1.1 Introduction 7
1.2 Check Point 8
1.3 AudioCodes MSBG 8

2 Check Point Setup Notes 9

2.1 Check Point Configuration 9
2.2 Special Instructions for Check Point Configuration 27
2.3 Other Comments 27

3 MSBG Setup Notes 29

3.1 Configuring AudioCodes MSBG 29

4 Troubleshooting 41

4.1 Online Monitor 41
4.2 Configuring AudioCodes MSBG for Syslog Server 43

Reader's Notes

Disclaimer

This MSBG Configuration Note is designed to be a general guide reflecting AudioCodes in configuring our system. These notes cannot anticipate every configuration possibility, given the inherent variations in hardware and software products. Therefore, if you experience a problem not detailed in this document, please notify AudioCodes' Technical Support at support@audiocodes.com, and if appropriate, we will include it in our next document revision. AudioCodes Ltd. accept no responsibility for errors or omissions contained herein.

This document is subject to change without notice.

Date Published: March-22-2009

Version Information

Version	Date of Modification	Details of Modification
01	March 2009	Initial version by AudioCodes

Overview

This document describes the configuration required to setup Check Point Firewall and AudioCodes' MSBG active IPSec tunnel.

Targeted Audience

This document is intended for Engineers or Business Partners who are installing AudioCodes MSBG in a Check Point environment.

Reader's Notes

1 Components Information

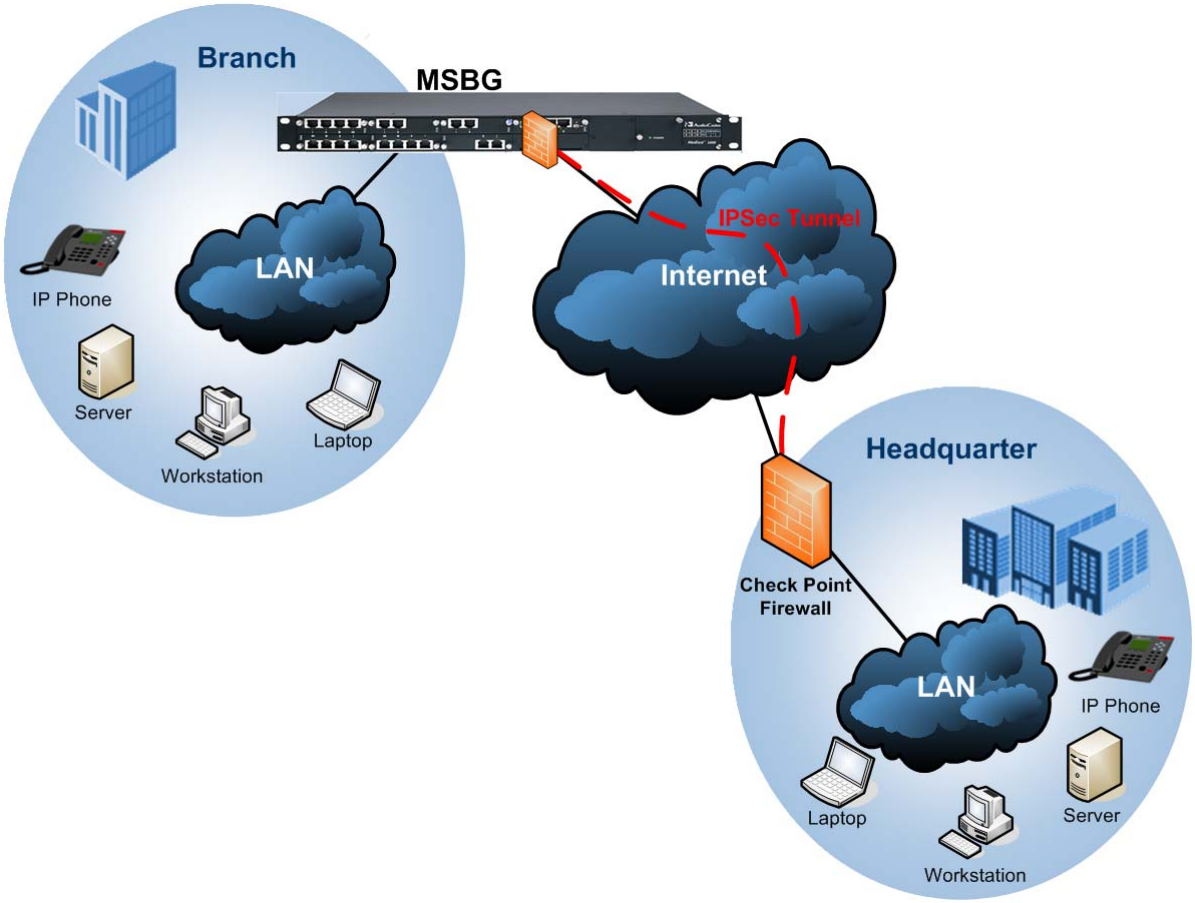
1.1 Introduction

This configuration note provides step-by-step procedures on how companies can create a secure VPN connection between a headquarters office and one of its branch offices using the Check Point Firewall product. This solution includes all the branch required services, routing and Firewall connectivity.

AudioCodes Multiservice Business Gateway (MSBG) provides multiple services included in a single device such as firewall, access router, LAN switch, Session Border Control (SBC), and a Voice-over-IP (VoIP) media gateway. AudioCodes MSBG provides enterprises, on one hand, with Local Area Network (LAN) connectivity that includes switching and telephony capabilities such as VoIP, digital and analog telephony connectivity. On the other hand, the MSBG also provides Wide Area Network (WAN) connectivity, where it is implemented as the main branch office router that includes a superior Firewall solution with Quality of Service (QoS) and Virtual Private Network (VPN) support.

This document focuses on the VPN settings and not on all other aspects that are involved in setting up the MSBG (such as WAN interface, routing issues, NAT etc.).

Figure 1-1: Example Layout of an Interoperability Test Environment



1.2 Check Point

Vendor	Check Point
Model	Firewall
Software Version	R65 HFA2
Additional Notes	None

1.3 AudioCodes MSBG

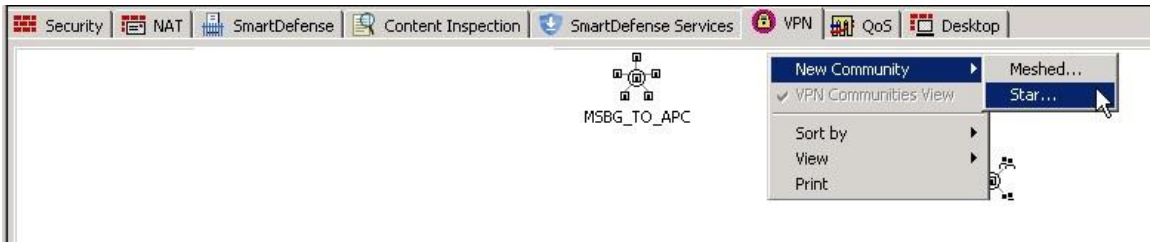
MSBG Vendor	AudioCodes
Model	MSBG
Software Version	4.9.2.5.50AL.028.
Additional Notes	

2 Check Point Setup Notes

2.1 Check Point Configuration

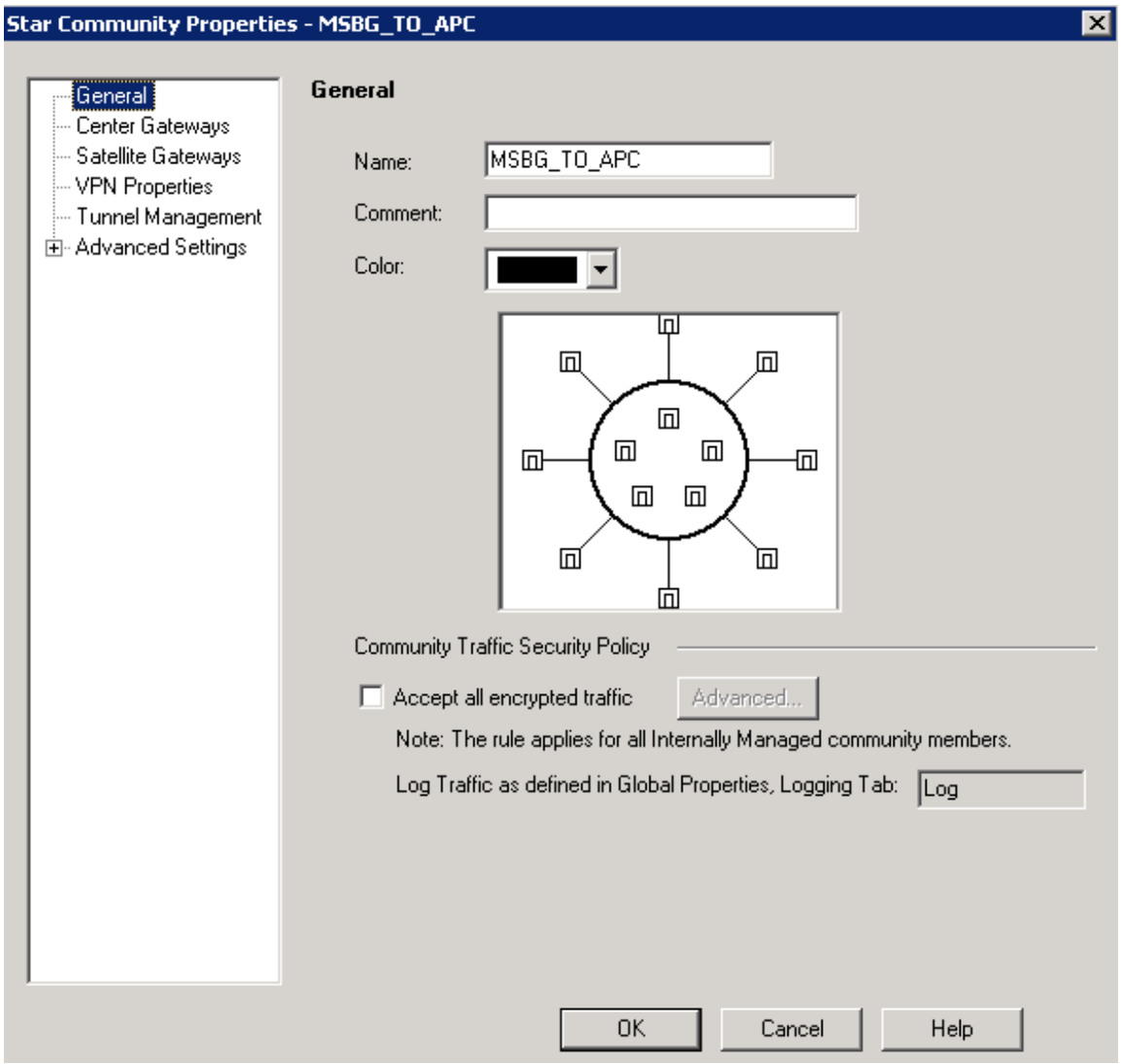
Step 1: Create a New Community

- From the 'VPN' menu, right-click and then select 'New Community' and 'Star'.



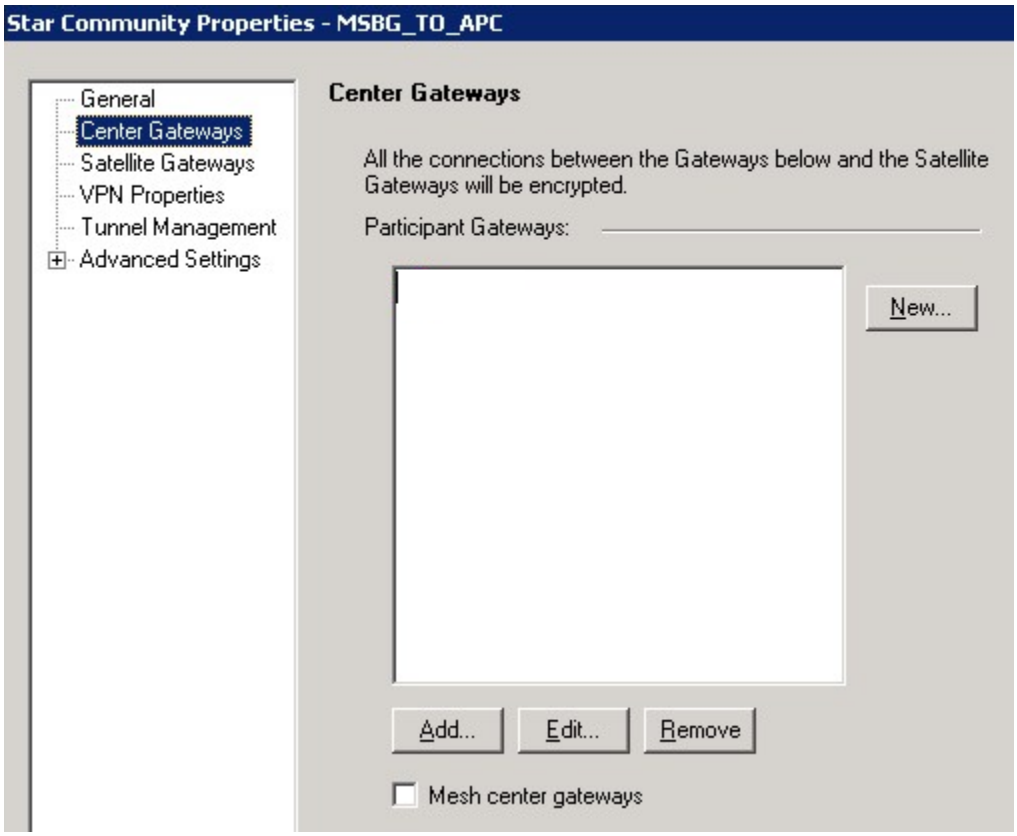
Step 2: Create a New Community – General

- Provide a **name** and **Comment** for this 'Star Community' (e.g. MSBG_TO_APC).

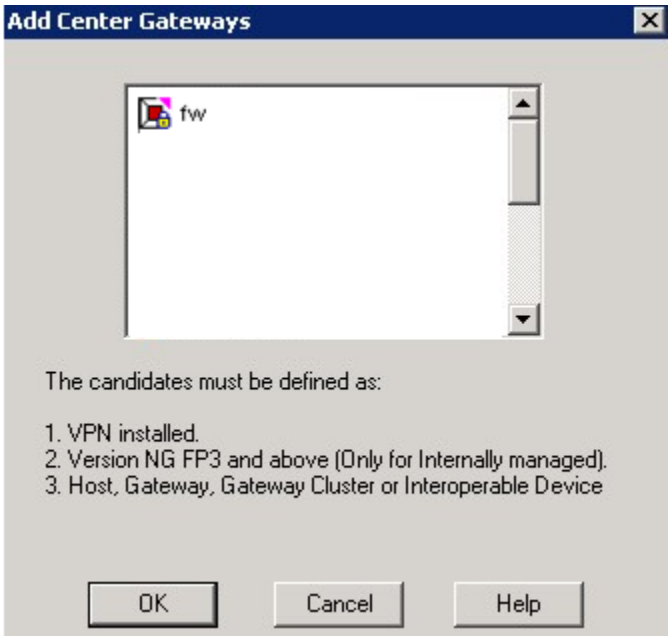


Step 3: Create New Community – Center Gateways

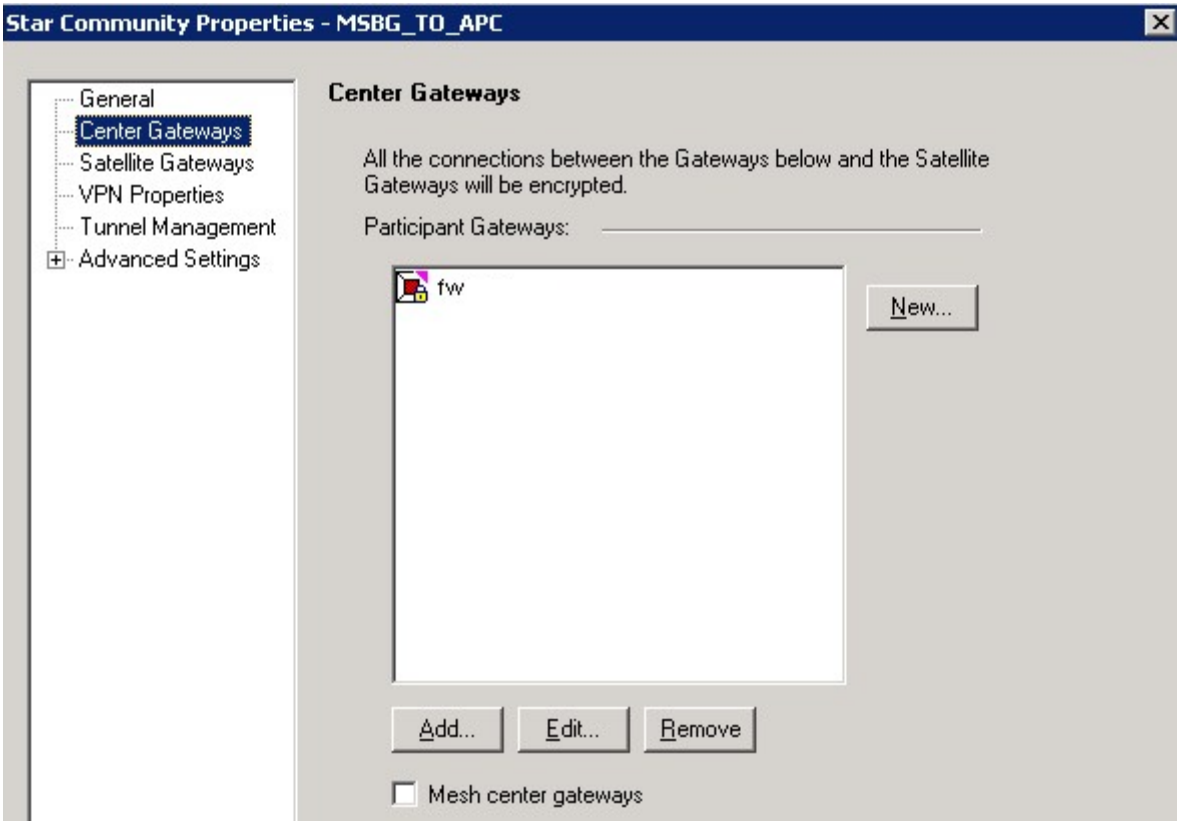
- In 'Center Gateways', click **Add**.



Step 4: Create a New Community – Add Center Gateway

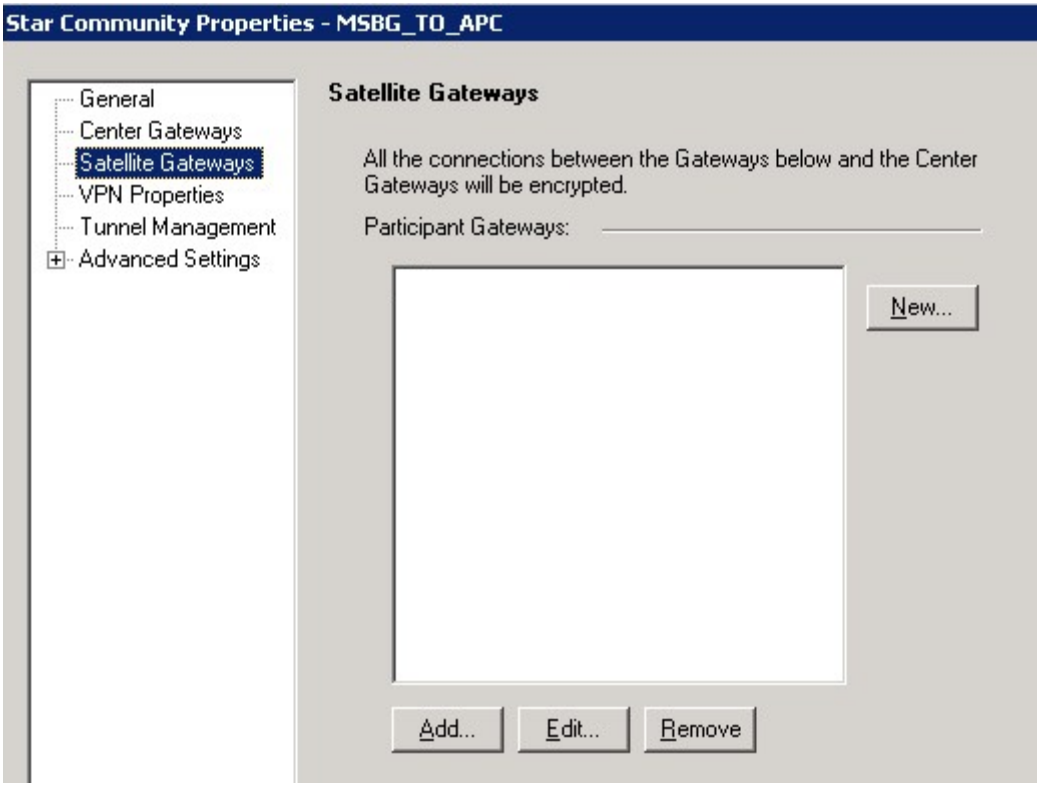


- Select your object from the list (e.g. fw-sys) and then click **OK**.

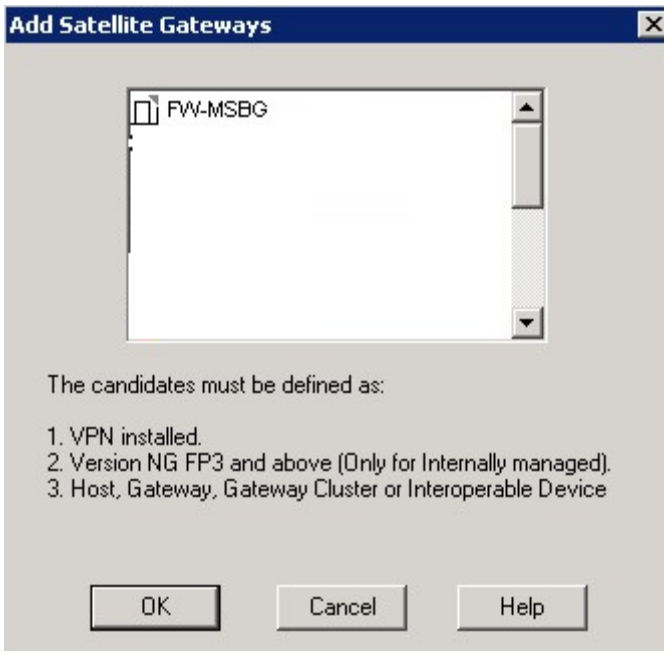


Step 5: Create a New Community - Satellite Gateways

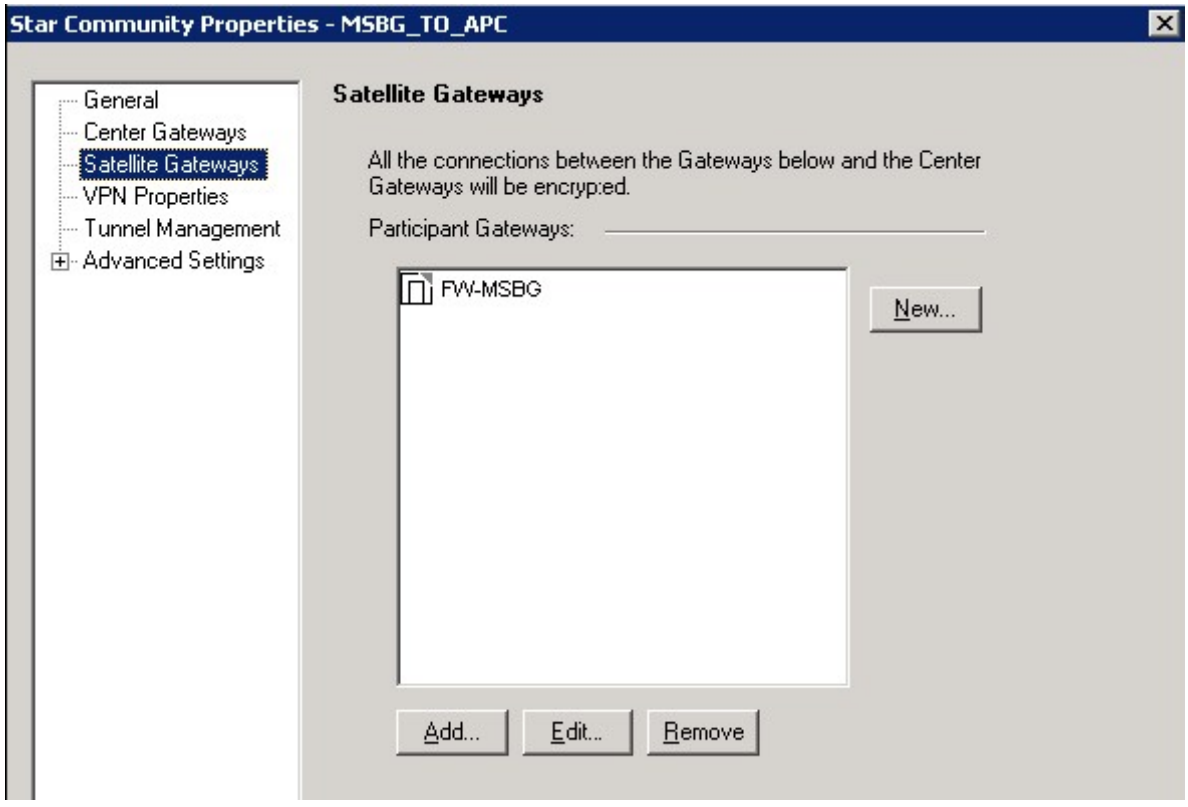
- Click **Add**.



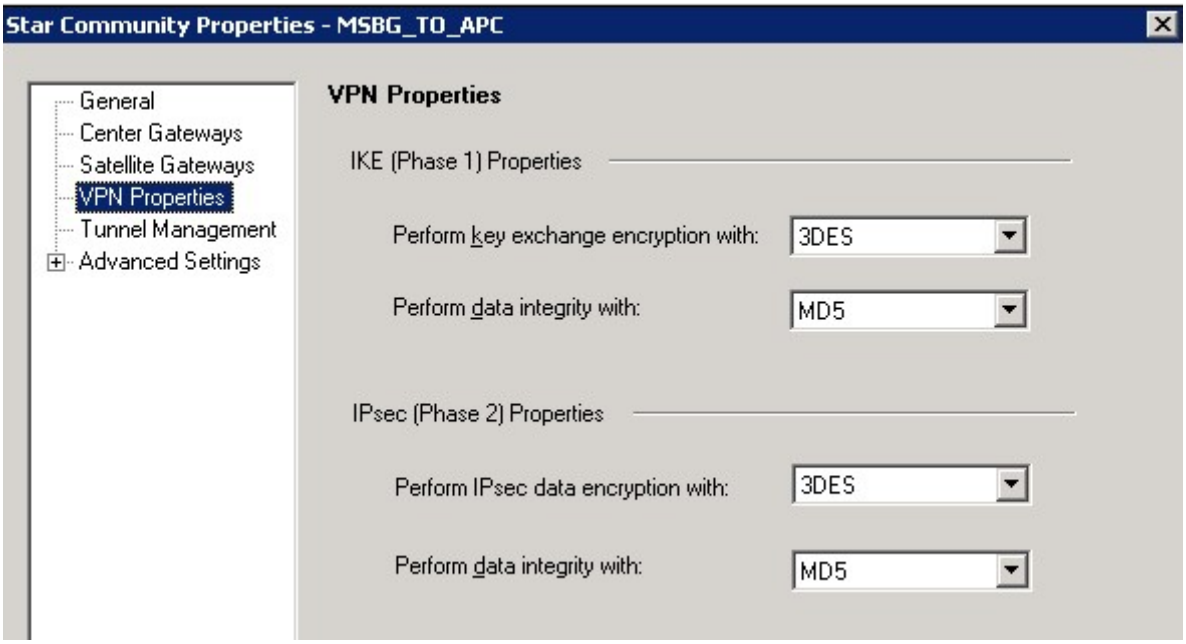
Step 6: Create New Community – Add Satellite Gateways



- Select your object from the list (e.g. FW-MSBG) and then click **OK**.



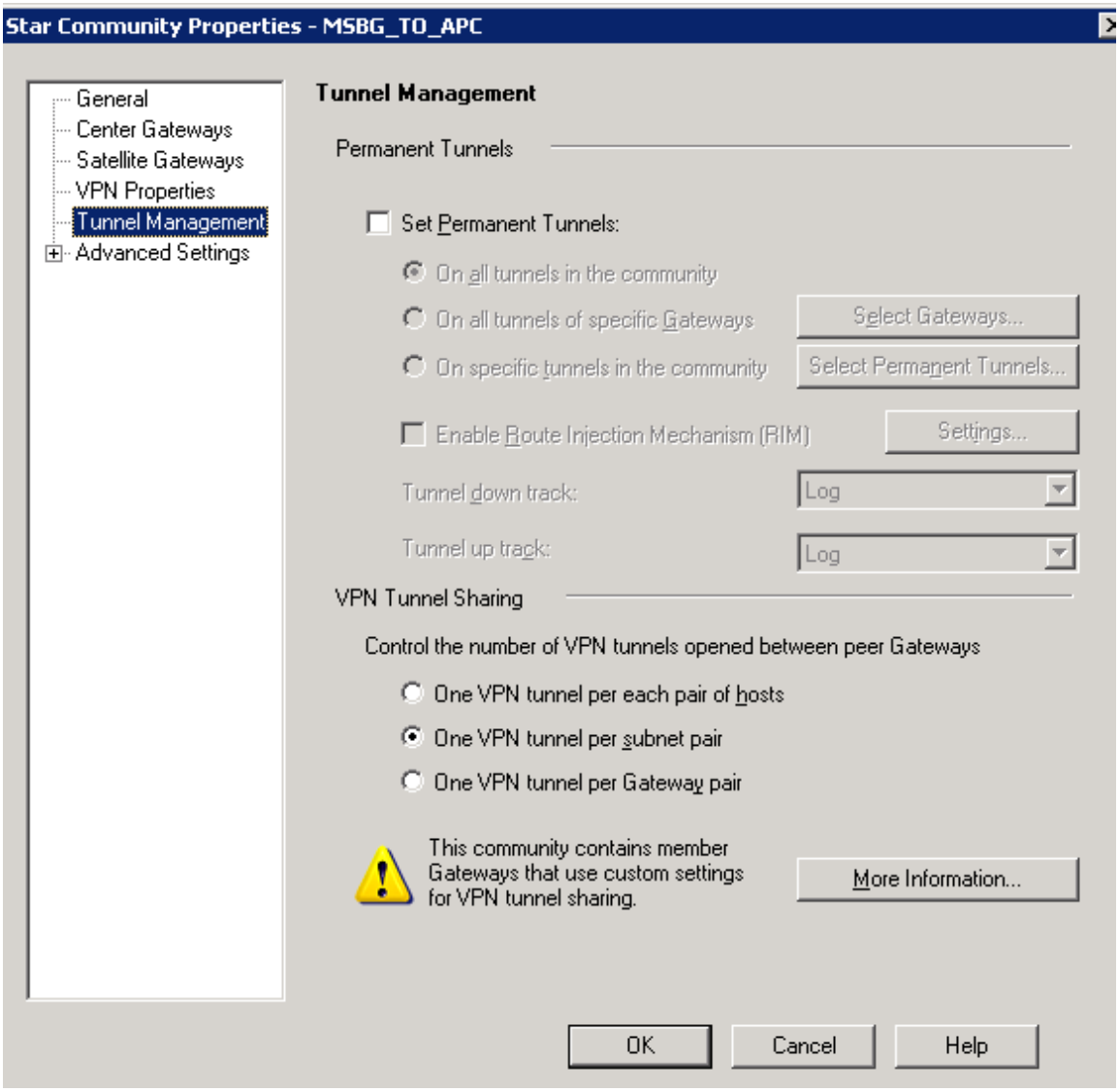
Step 7: Create a New Community - VPN Properties



- From the 'Perform key exchange encryption' drop-down list, select '3DES'.
- From the 'Perform data integrity' drop-down list, select 'MD5'.
- From the 'Perform IPsec data encryption with' drop-down list, select '3DES'.
- From the 'Perform data integrity with' drop-down list, select 'MD5'.

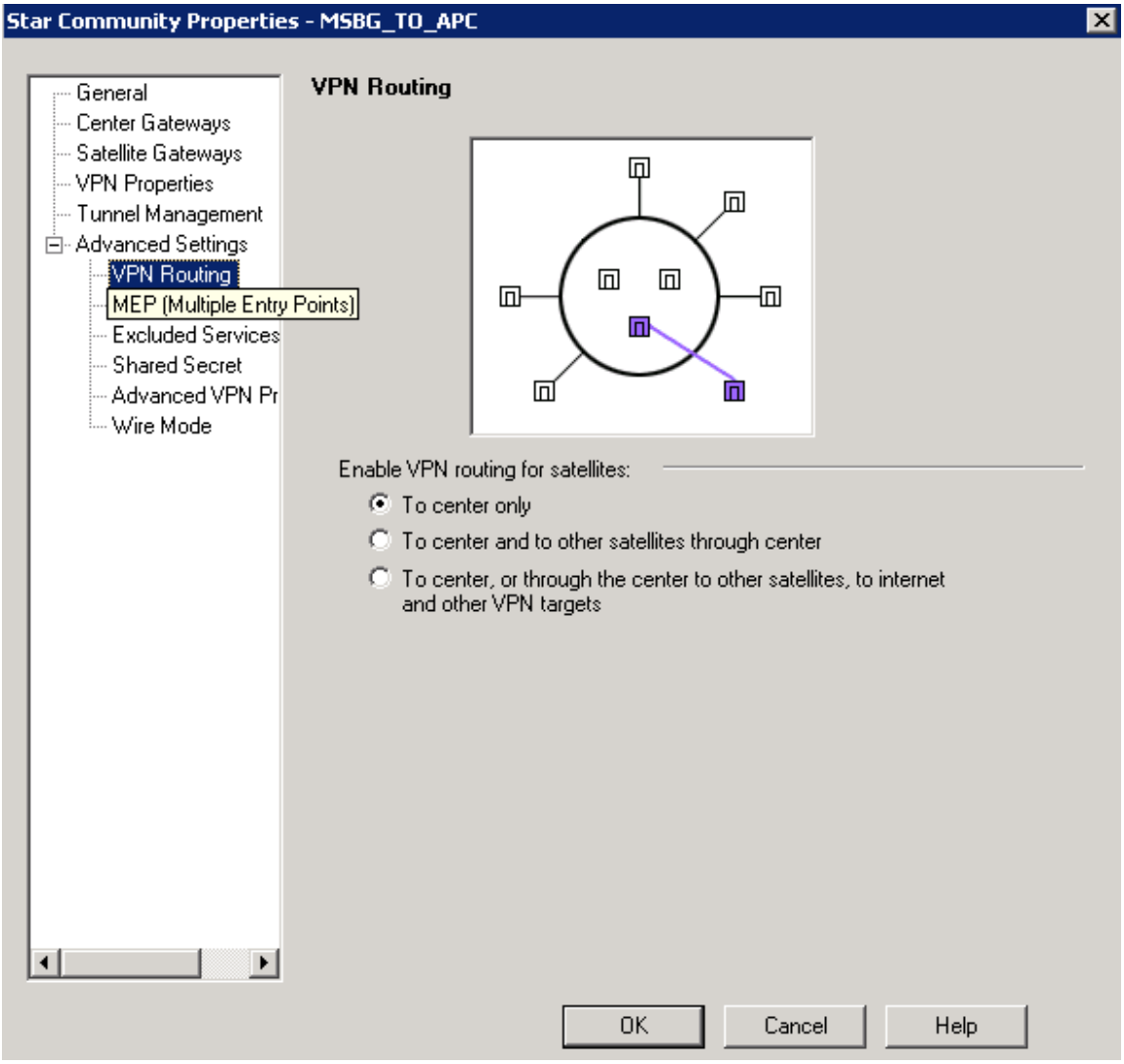
Step 8: Create a New Community – Tunnel Management

- Select the 'One VPN tunnel per subnet pair' option.



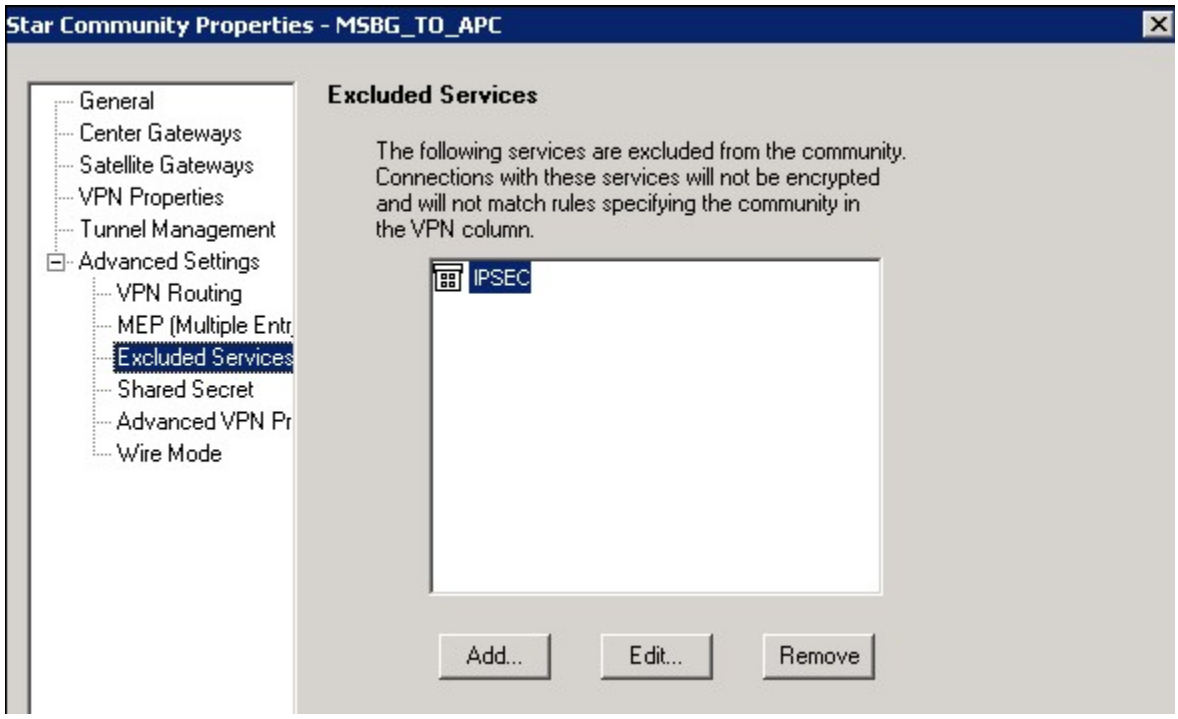
Step 9: Create a New Community – VPN Routing

- Select the 'To center only' option.



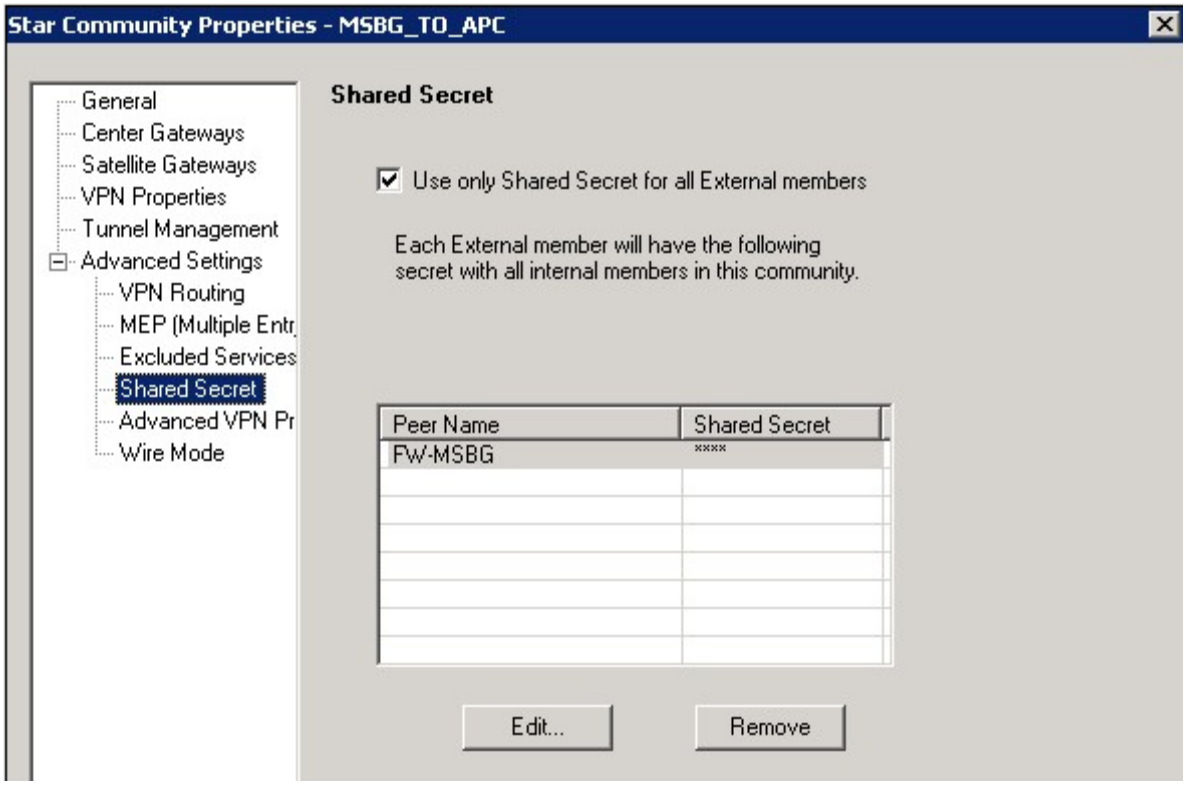
Step 10: Create a New Community – Excluded Services

- Click **Add** and then add IPsec.



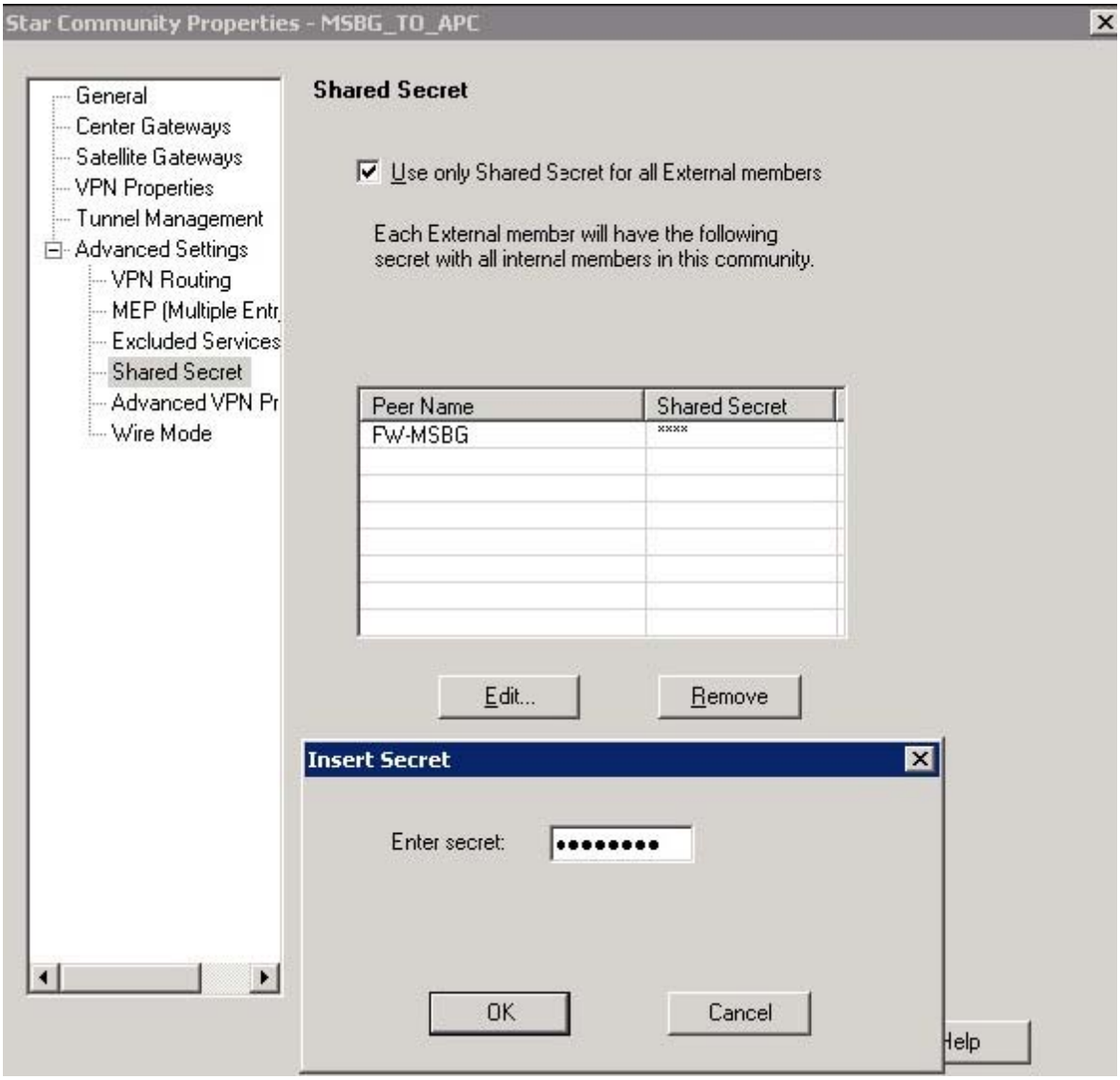
Step 11: Create a New Community – Shared Secret

- Select the 'Use only Shared Secret for all External members' check box.



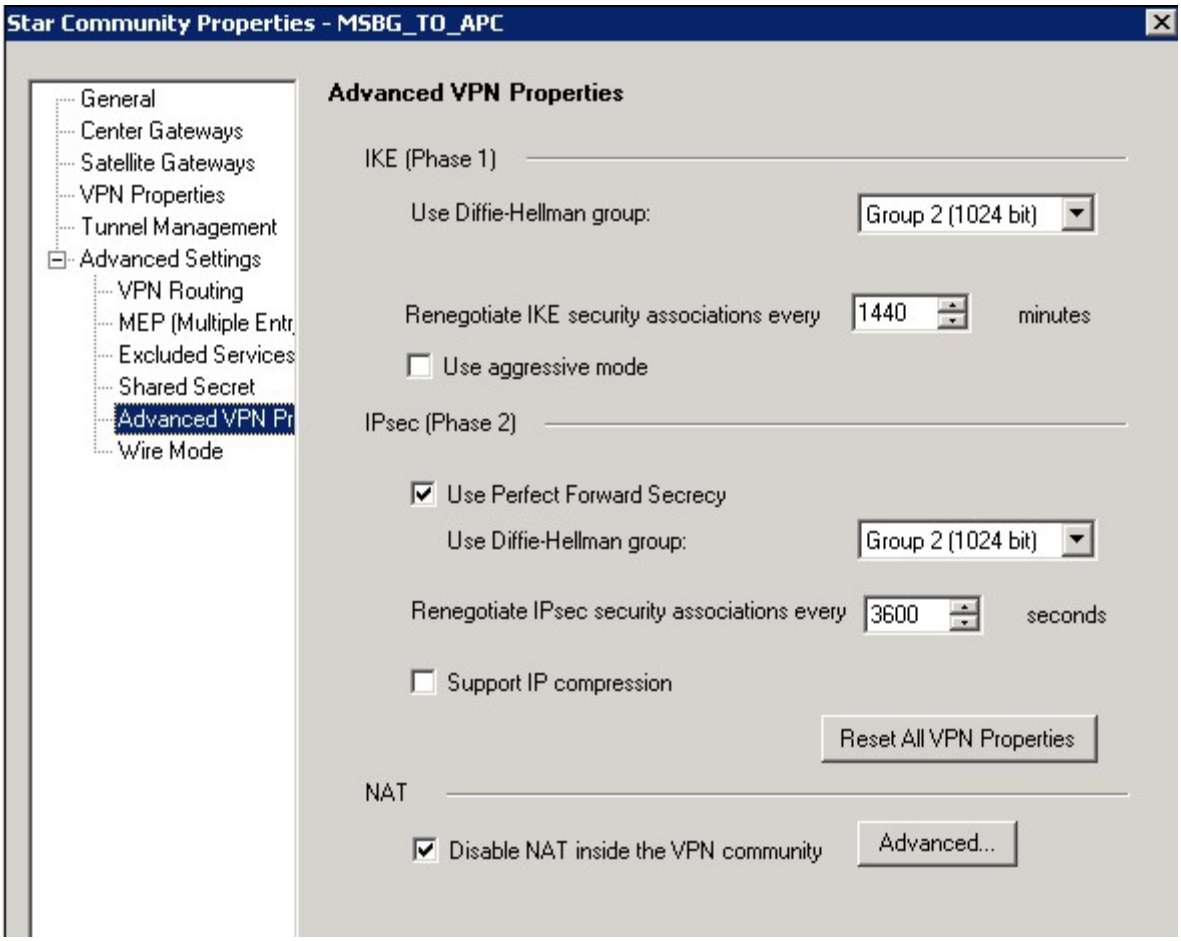
Step 12: Create a New Community – Insert Secret

- In the 'Shared Secret', click **Edit**.
- Enter the secret (e.g. 'secret').



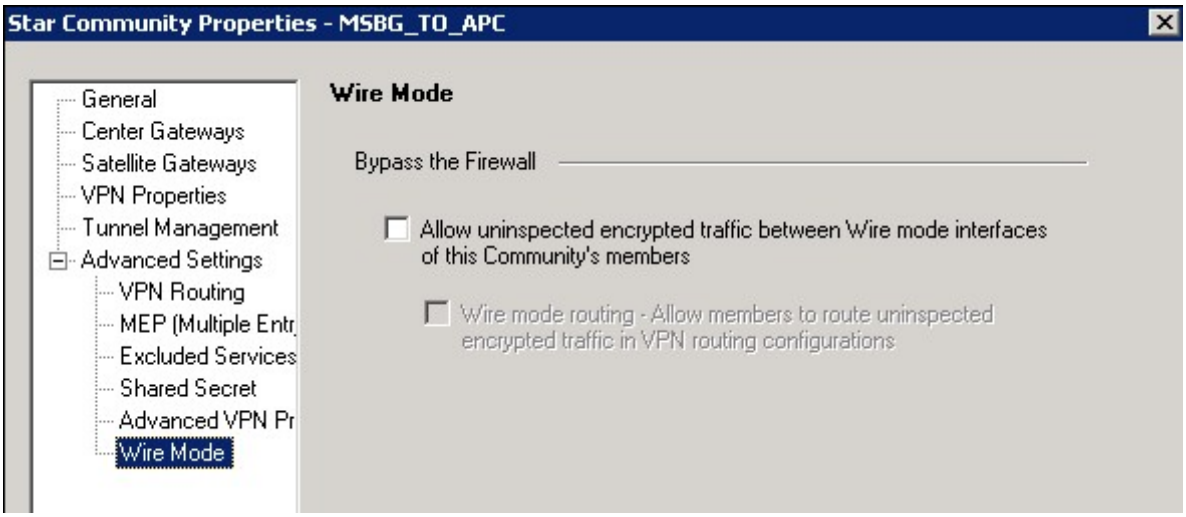
Step 13: Create a New Community – Advance VPN Properties

- Fill as below.



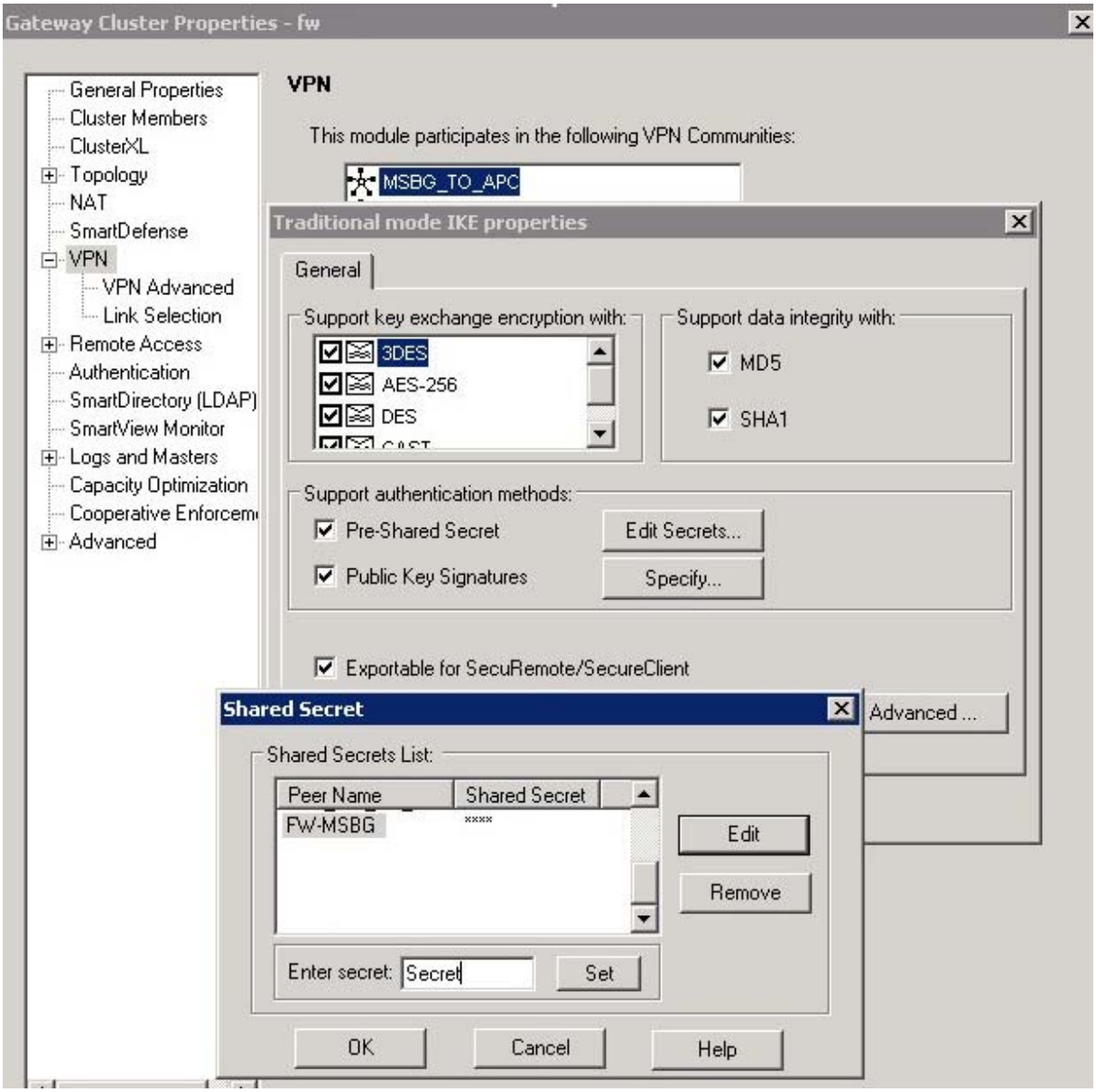
Step 14: Create a New Community – Shared Secret

- Ensure that 'Allow uninspected encrypted traffic between Wire mode interfaces of this Communities members' is unchecked.



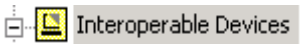
Step 15: Add Secret Password

1. In the VPN, open the 'Traditional mode IKE properties' dialog box.
2. Click **Edit Secrets**.
3. In the "Shared Secret List" select your created 'Peer Name' and in the 'Enter secret:' area, enter the password. (e.g. Secret).



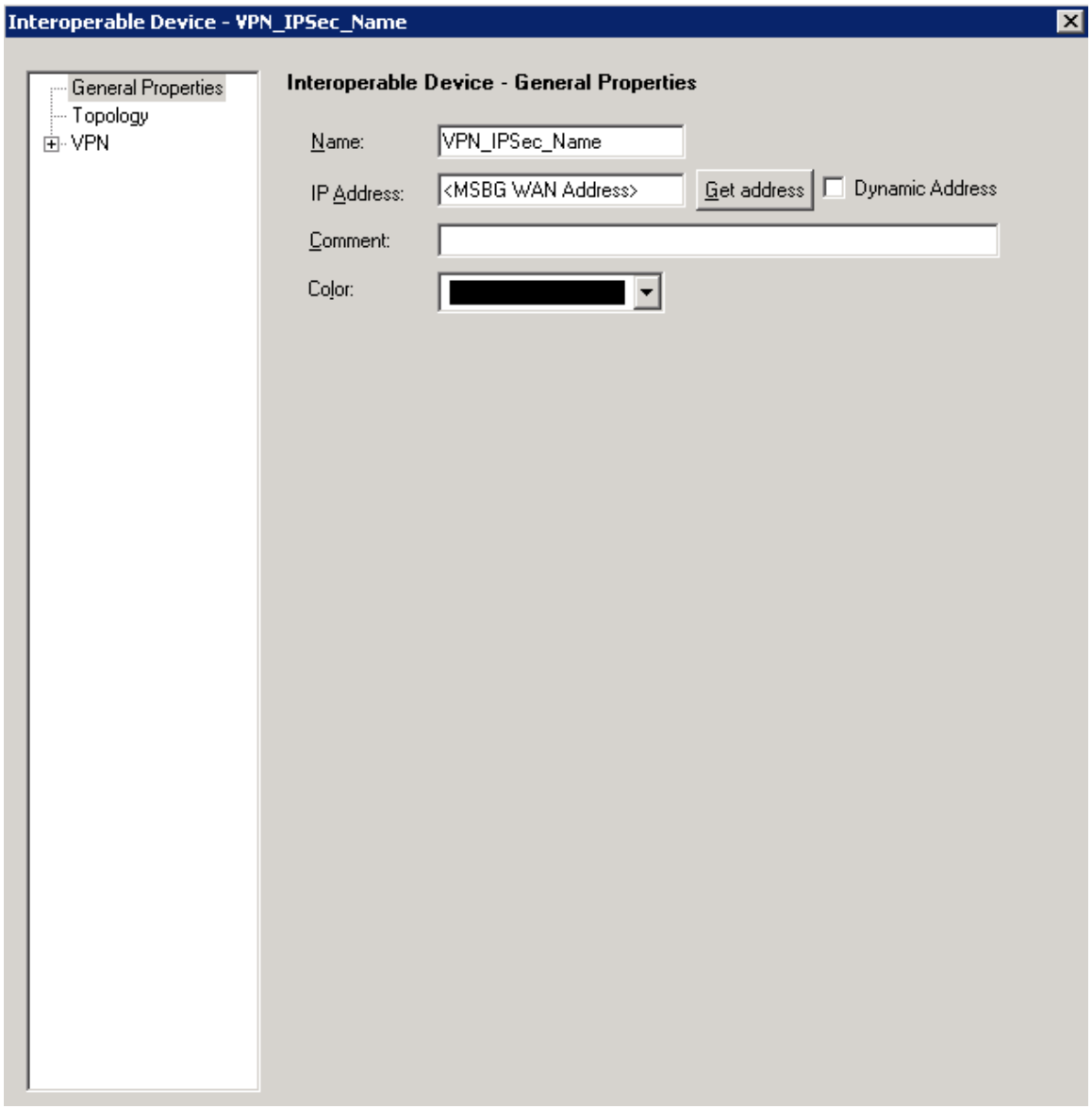
Step 16: Interoperable Device – Setup

- Right-click the 'Interoperable Devices', and select 'NEW Interoperable device'.



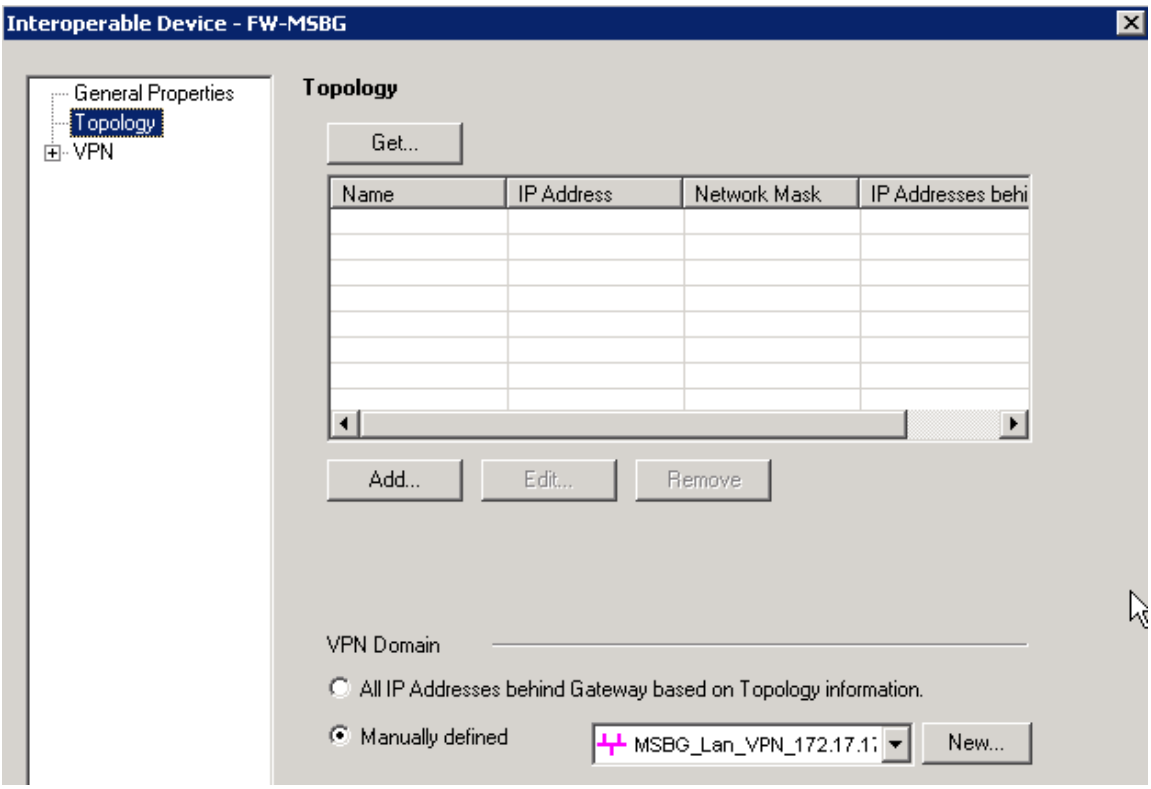
Step 17: Interoperable Device – General Properties

- **Name:** Clearly name.
- **IP Address:** MSBG WAN IP address.



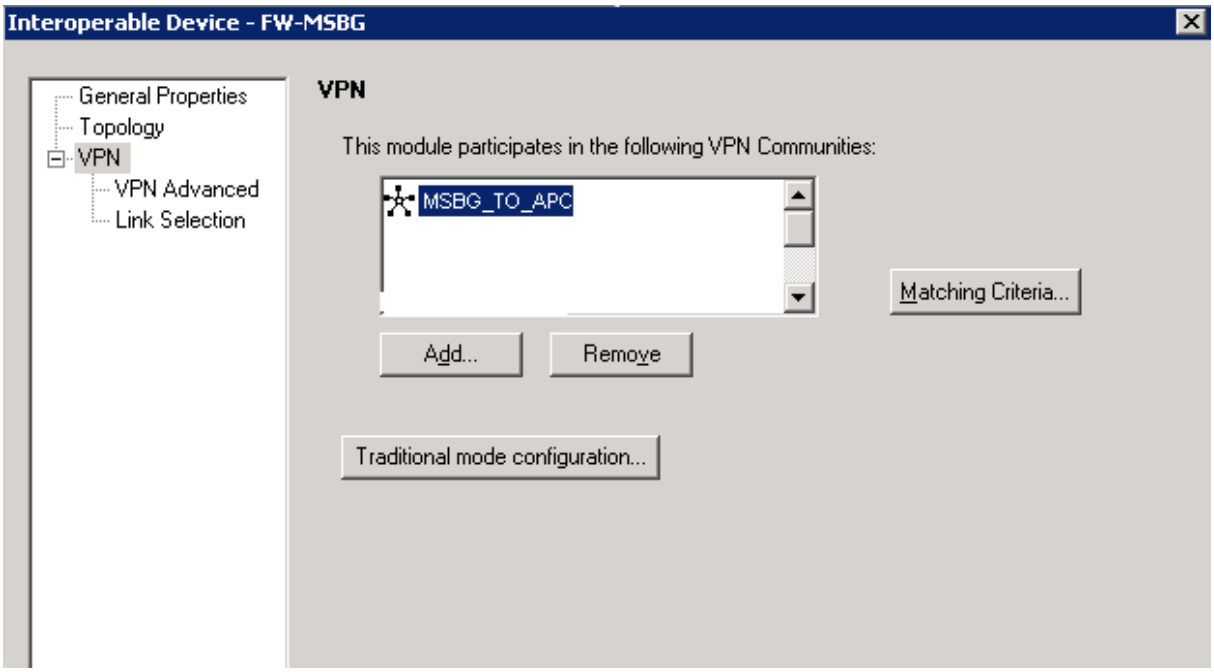
Step 18: Interoperable Device – Topology

- In the VPN Domain, select the 'Manually defined' option, and then from the drop-down list, select 'MSBG LAN'.



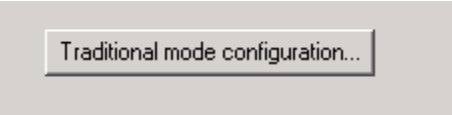
Step 19: Interoperable Device – VPN

- Select the Community that you created before (e.g. MSBG_TO_APC).



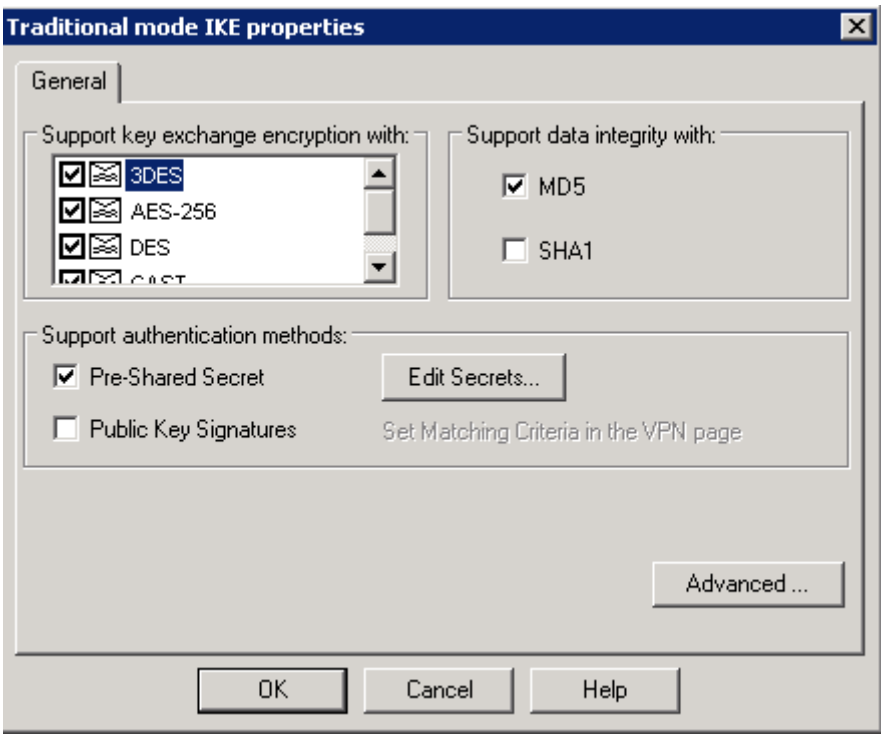
Step 20: Interoperable Device – VPN (Cont...)

- Click **Traditional mode configuration**.



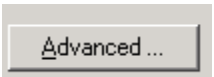
Step 21: Interoperable Device – VPN (Cont...)

- Clear the 'SHA1' check box.
- Select the 'Pre-Share Secret' check box.



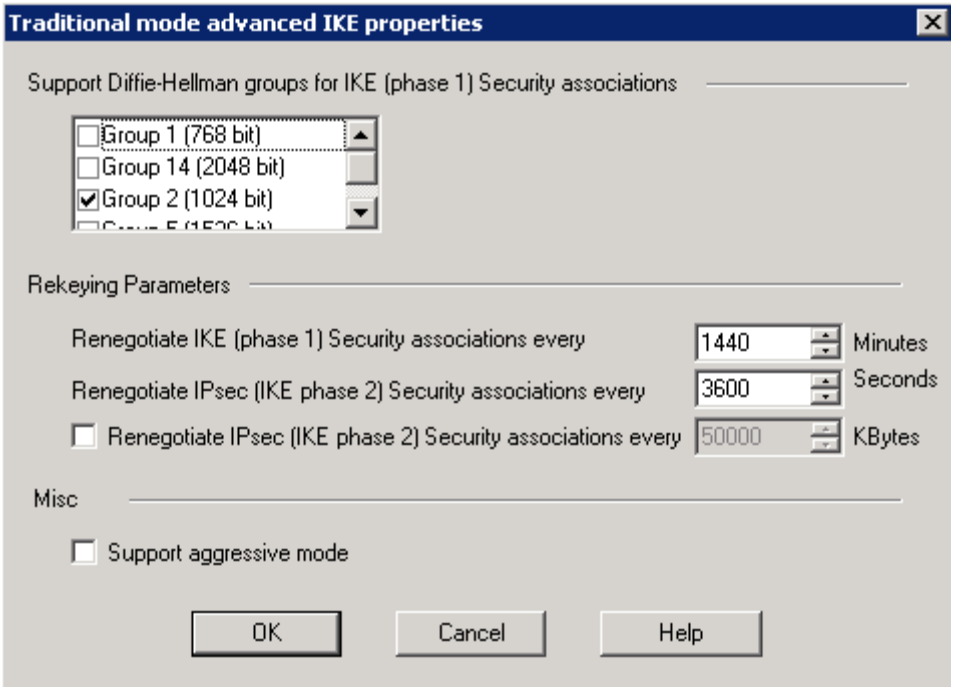
Step 22: Interoperable Device – VPN (Cont...)

- Click **Advanced**.



Step 23: Interoperable Device – VPN (Cont...)

- In 'Support Diffie-Hellman groups for IKE…' , select 'Group 2 (1024 bit)'.



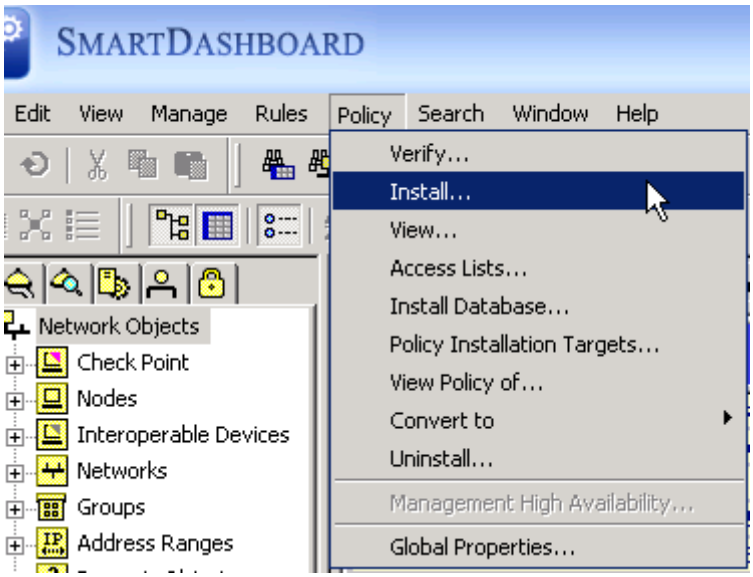
Step 24: Add New Rule – Connection between the VPN LAN to the Local LAN.

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION
2	Lan_192.168.15.0 MSBG_Lan_VPN_172.17.170.0	MSBG_Lan_VPN_172.17.170.0 Lan_192.168.15.0	MSBG_TO_APC	Any	accept

For creating a connection between the LANs, add a rule like in the above example.

Step 25: Install the New Configuration

- Go to 'Policy' >> 'Install', and install the configuration to the relevant Devices.



2.2 Special Instructions for Check Point Configuration

None.

2.3 Other Comments

None.

Reader's Notes

3 MSBG Setup Notes

This section describes the configuration of the AudioCodes' MSBG required for integration with the Check Point Firewall System.

3.1 Configuring AudioCodes MSBG

This section provides step-by-step procedures for configuring the AudioCodes' MSBG using the Web interface. Ensure that you configure the MSBG according to the configuration settings displayed in the screenshots provided in this section.

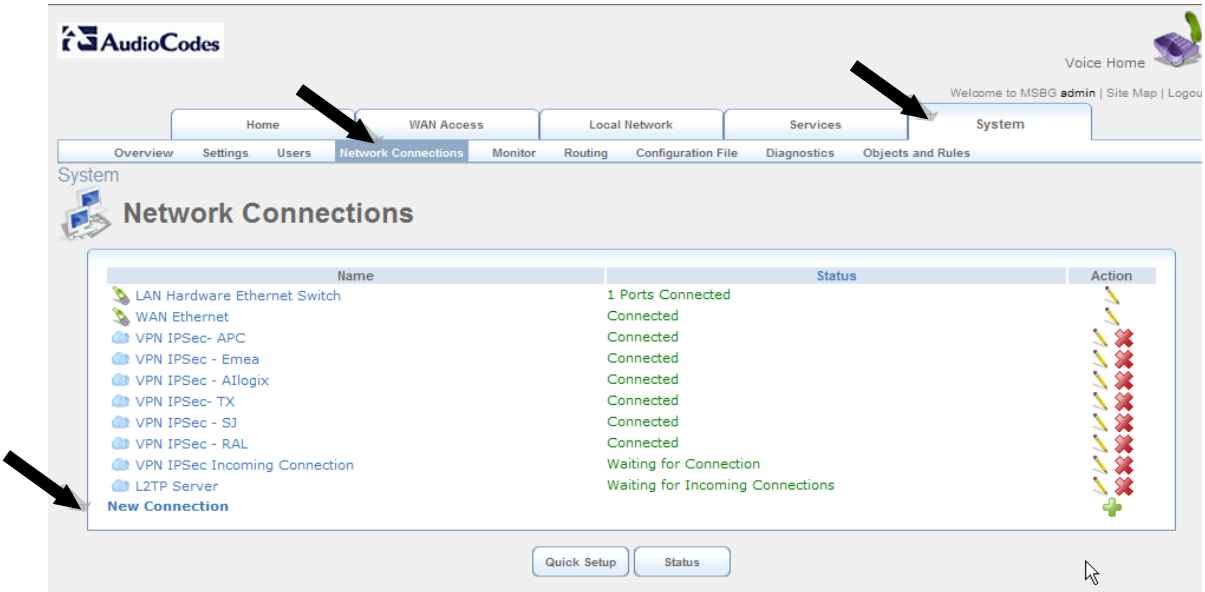
The procedures below describe how to setup a VPN between the AudioCodes MSBG and the Check Point Firewall.

Note the following Web interface guidelines:

- When making configuration changes for each procedure, ensure that you click the **Submit** button to save your changes; unless otherwise instructed.
- Some of the changes may require a gateway reset for these changes to take effect. Therefore, (and to save time), reset the gateway only after you complete all of the gateway configurations.
- For switching to the Data Web management, select 'Data Home', as shown below:

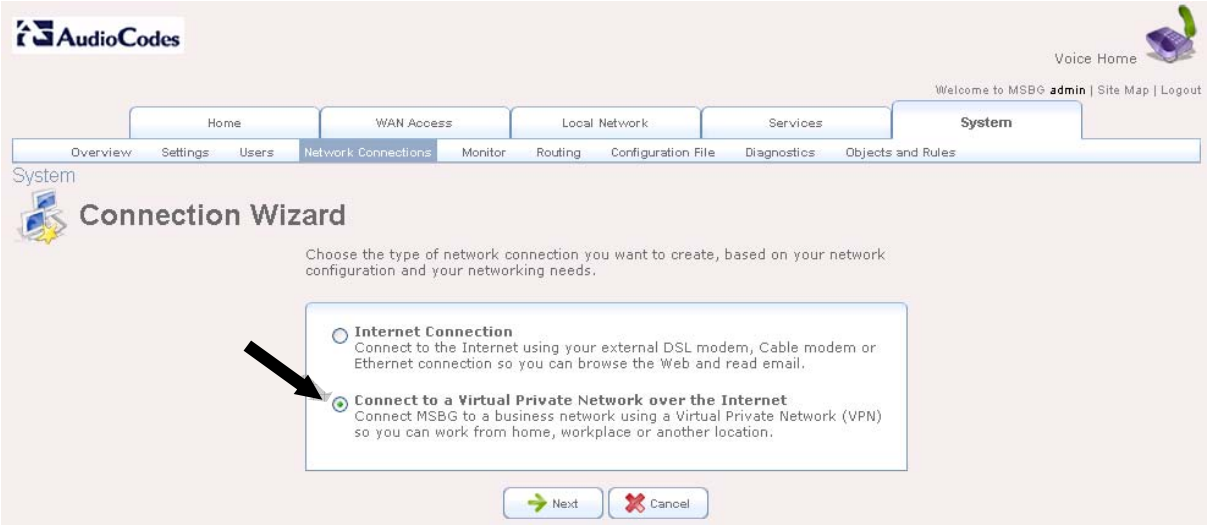
Step 1: Trunk Setting Setup

- Open the 'Network Connections' page (**System** > **Network Connections**).



- Click the **New Connection** link.

Step 2: Connection Wizard

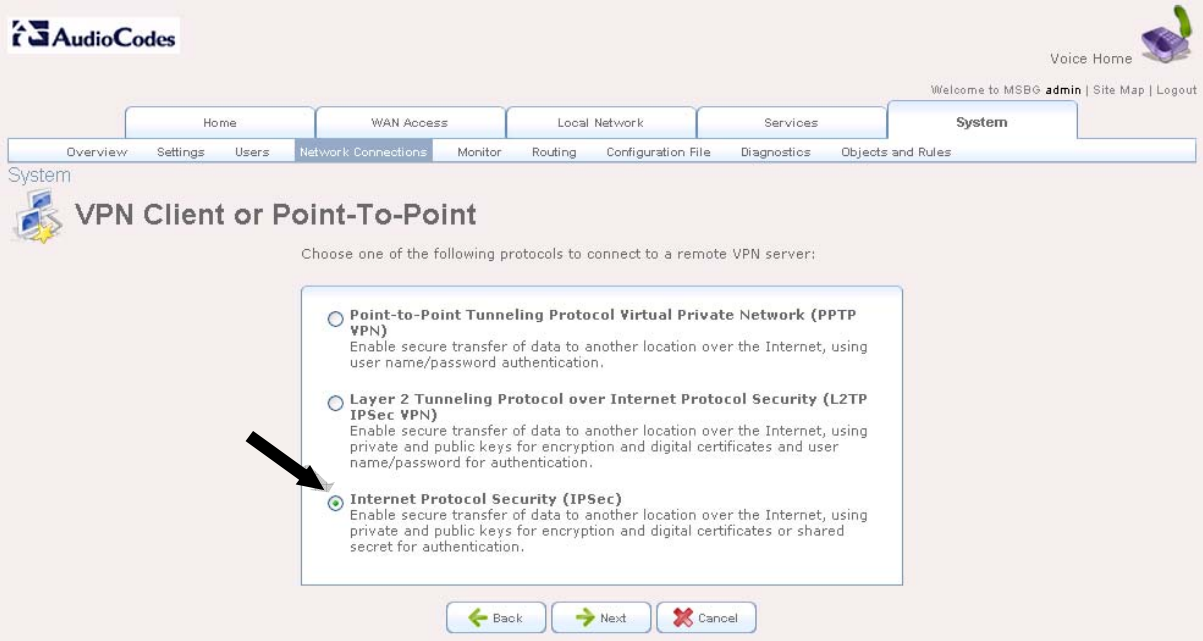


- Select the 'Connect to a Virtual Private Network over the Internet' option, and then click **Next**.

Step 3: Connect to a Virtual Private Network over the Internet

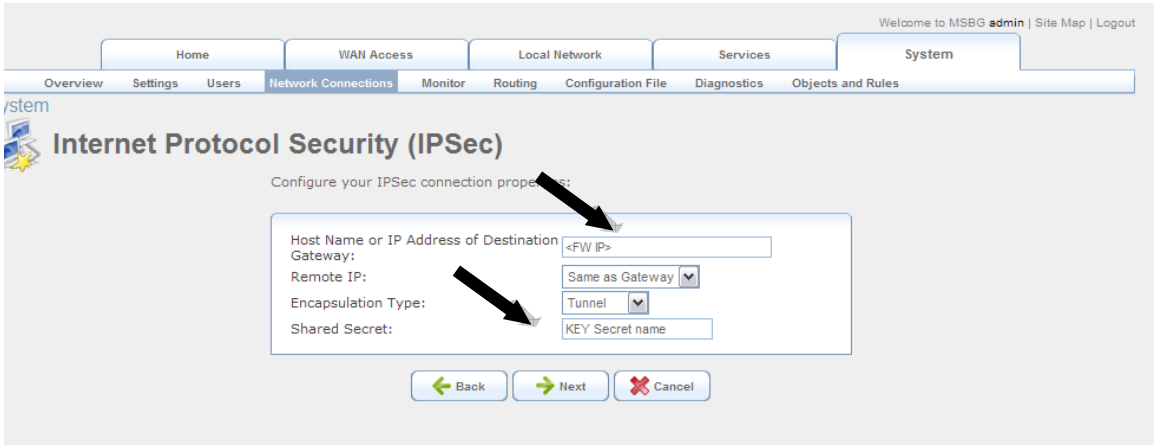
- Select the 'VPN Client or Point-To-Point' option, and then click **Next**.

Step 4: VPN Client or Point-To-Point



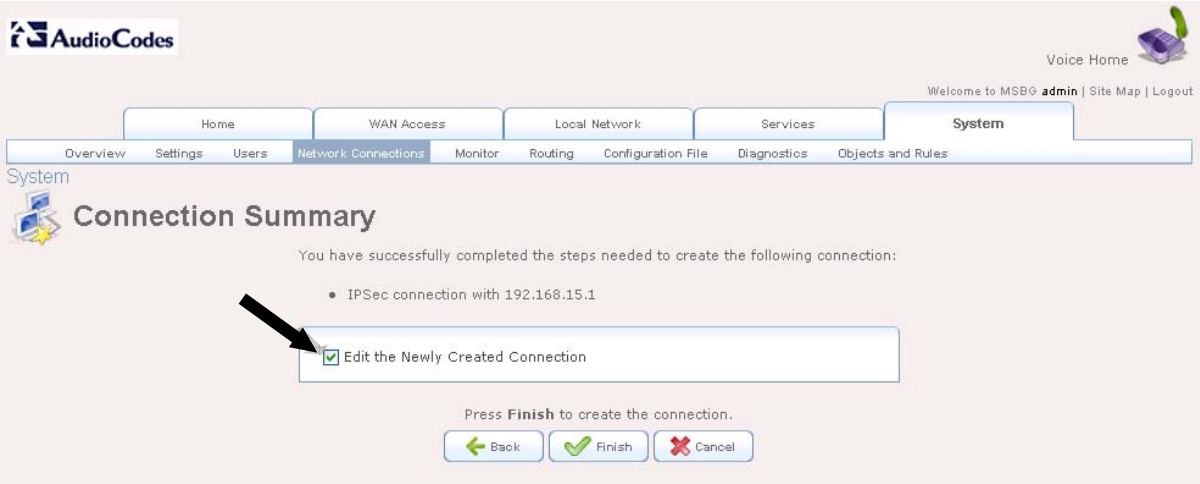
- Select the 'Internet Protocol Security (IPSec)' option, and then click **Next**.

Step 5: Internet Protocol Security (IPSec)



- **Host Name or IP Address of Destination Gateway:** Check Point Firewall IP address (e.g. 192.168.15.1)
- **Remote IP:** Select 'Same as Gateway'
- **Encapsulation Type:** Select 'Tunnel'
- **Shared Secret:** enter same Secret password as you provided in the Check Point Firewall. (e.g. 'Secret')

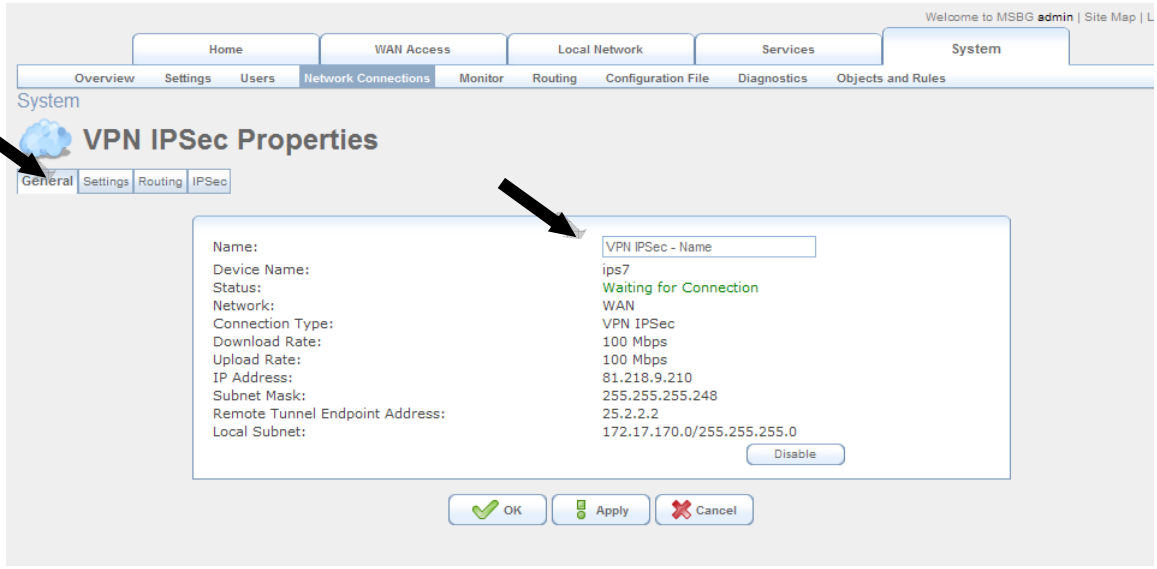
Step 6: Connection Summary



- Mark the 'Edit the Newly Created Connection' check box, and then click **Finish**.

Step 7: VPN IPSec Properties

General tab.



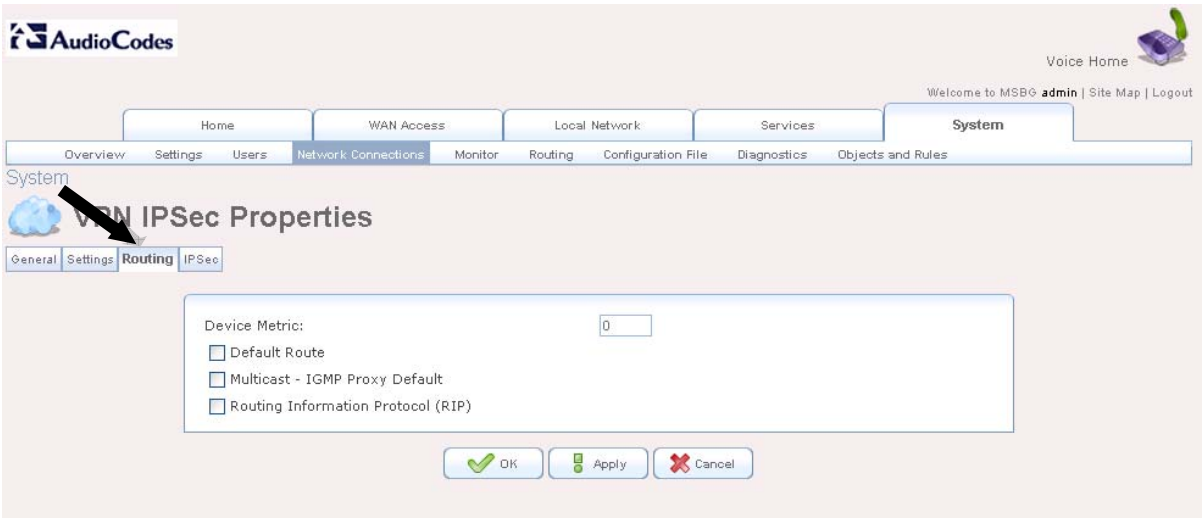
- Enter a name for the connection.

Step 8: Trunk Group Setup

Setting tab. Do not configure this setting.

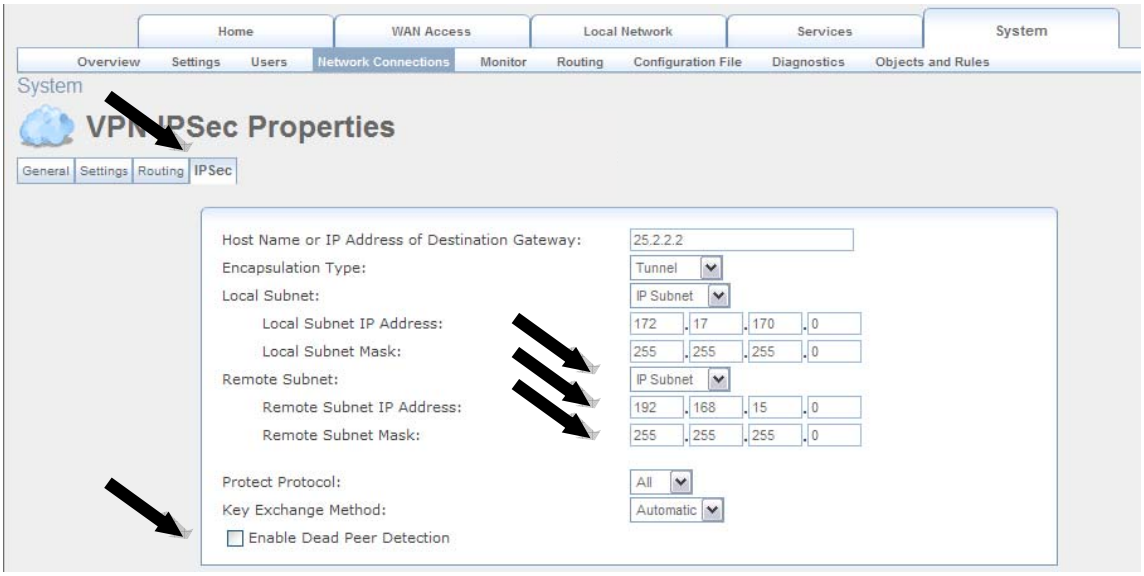
Step 9: Voice Mail Settings

Routing tab. Do not configure this setting.



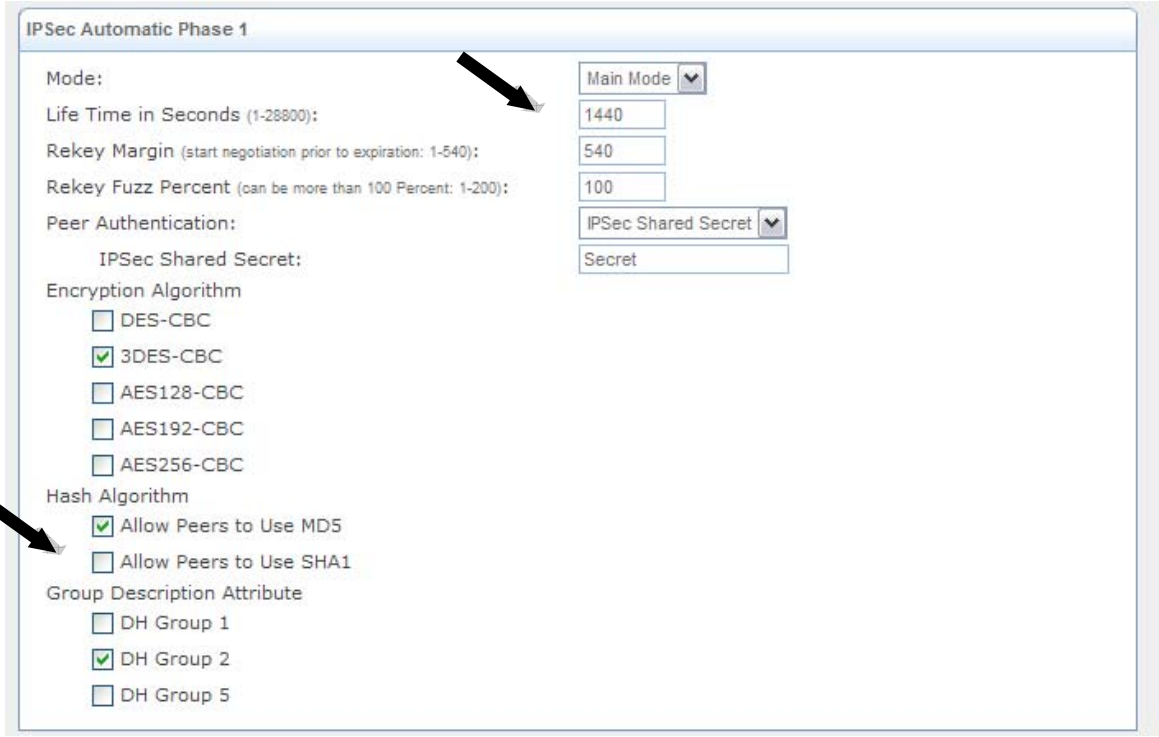
Step 10: TDM BUS Settings

Routing tab.



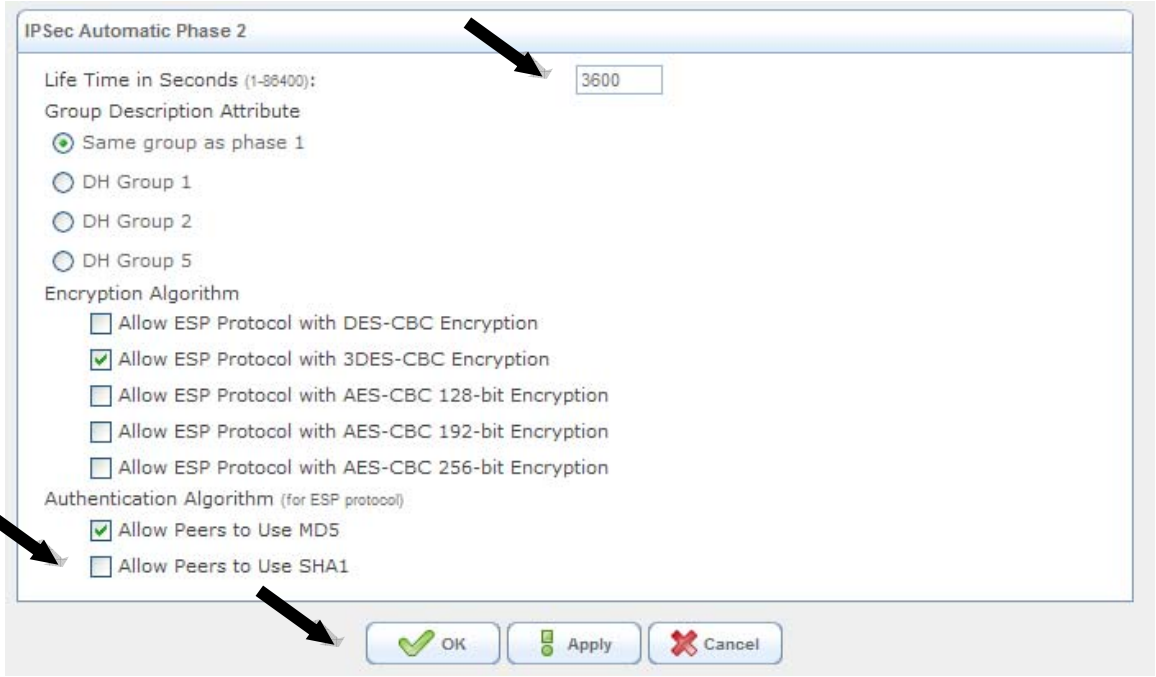
- From the 'Remote Subnet' drop-down list, select 'IP Subnet'.
- Enter in 'Remote Subnet IP Address:' the IP address of the Check Point LAN. (e.g. 192.168.15.0).
- Enter in 'Remote Subnet Mask:' the subnet of the Check Point LAN. (e.g. 255.255.255.0).
- Clear the 'Enable Dead Peer Detection' check box.

Step 11: VPN IPSec Properties (Cont…)



- Set the ‘Life Time in Seconds (1-28800):’ to 1440.
- Clear the ‘Allow Peers to Use SHA1’ check box.

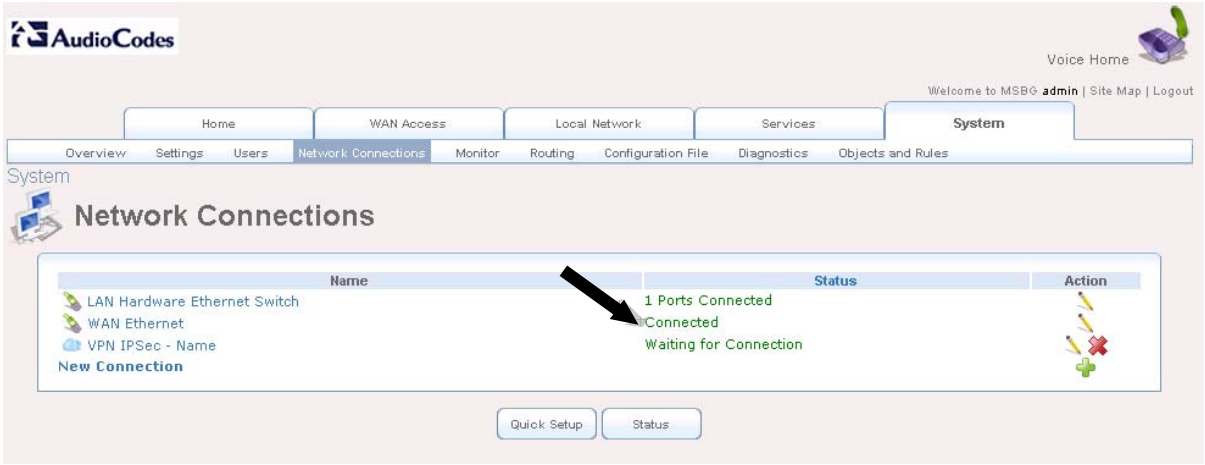
Step 12: VPN IPSec Properties (Cont…)



- Set the 'Life Time in Seconds (1-86400):' to 3600.
- Clear the 'Allow Peers to Use SHA1' check box.

Step 13: Network Connections

- Check that the new VPN connection appears.



After several seconds the new connection changes to "Connected". (If the configuration on the Check Point VPN has already been performed)

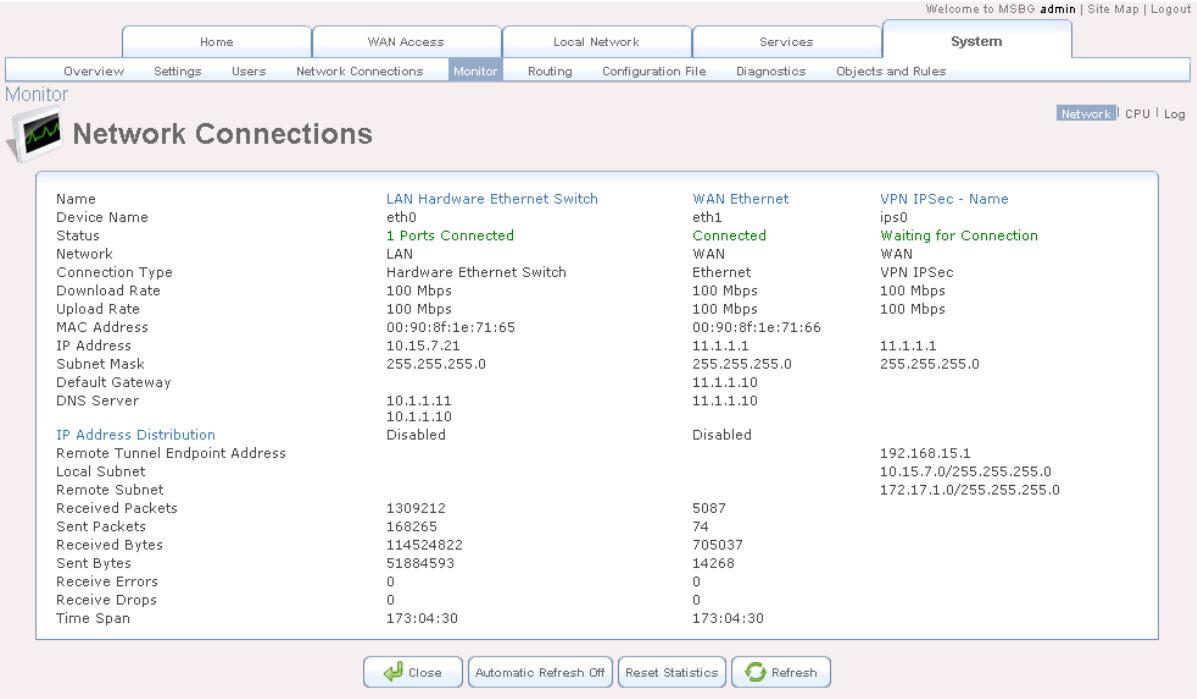
4 Troubleshooting

The tools used for debugging include network sniffer applications (such as Wireshark) and AudioCodes' Syslog protocol.

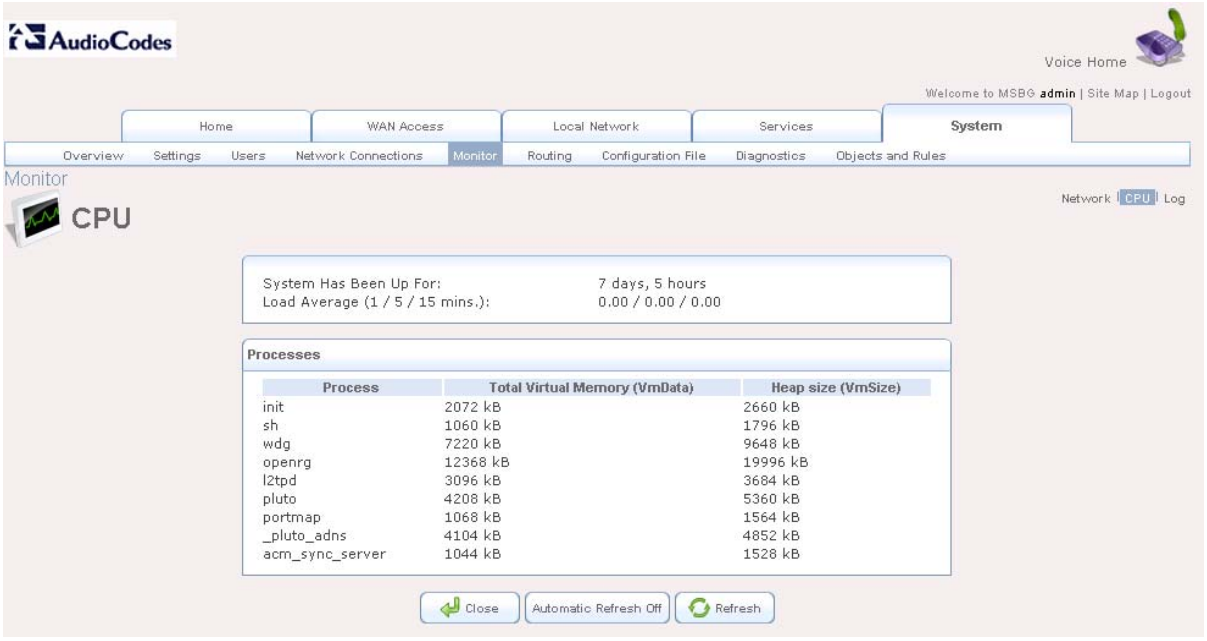
4.1 Online Monitor

Open the 'System Setting' page (**System** > **Monitor**).

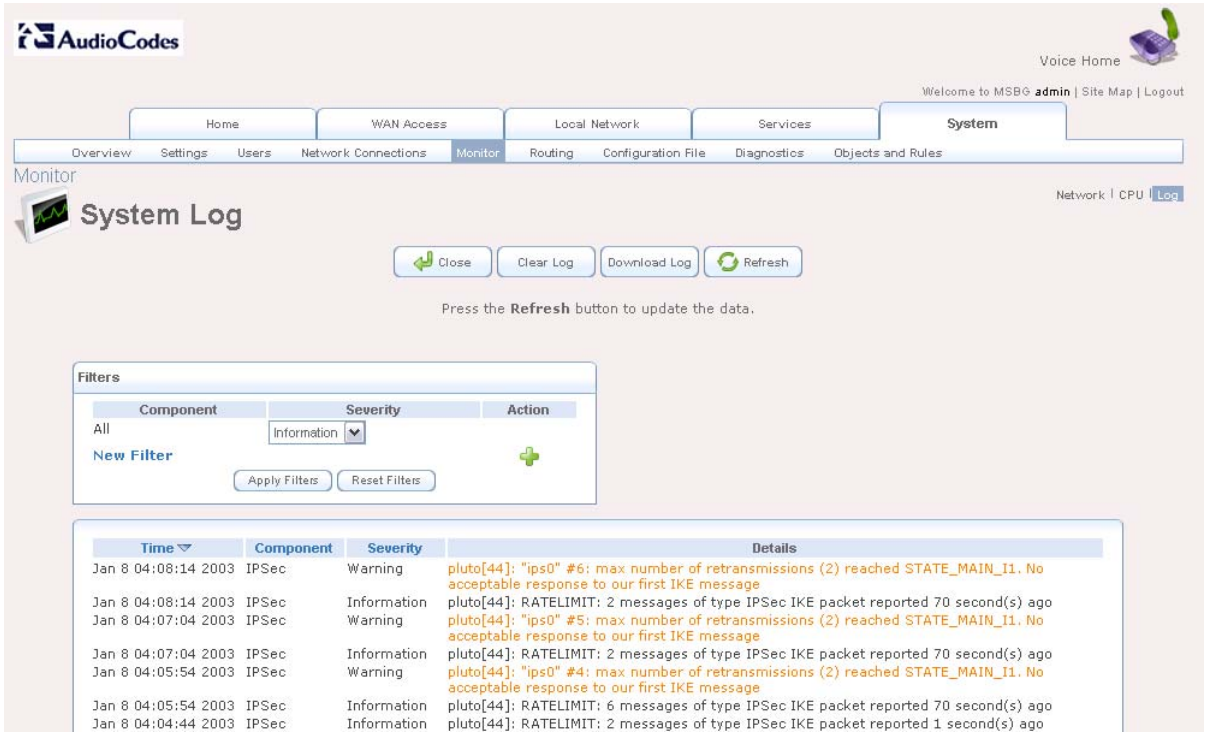
- **Network:** displays online connections status



- **CPU:** displays online CPU status.



- **Log:** displays online Syslog.



You can filter the log by choosing a specific filter from the drop-down list or by creating a 'New Filter' .

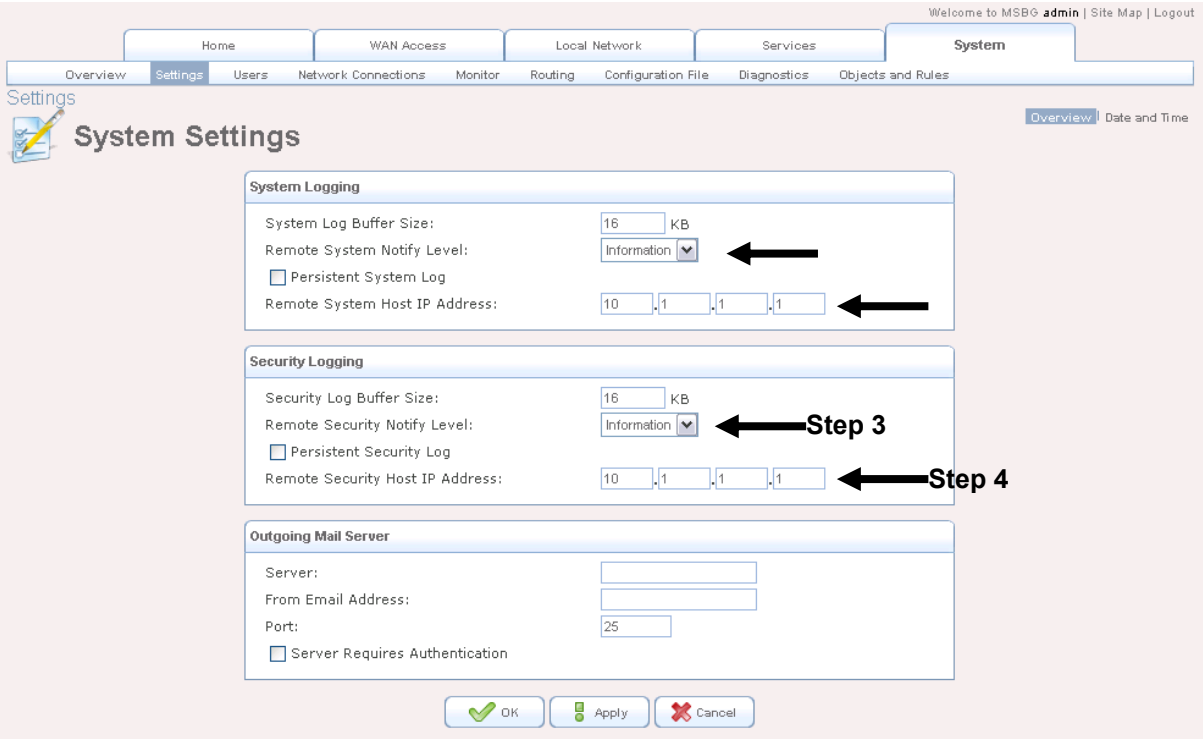
4.2 Configuring AudioCodes MSBG for Syslog Server

The Syslog client, embedded in the AudioCodes MSBG sends error reports/events generated by the gateway application to a Syslog server, using the IP/UDP protocol.

➢ To activate the Syslog client on the AudioCodes MSBG:

1. Open the 'System Setting' page (**System** > **Settings**).
2. Set the parameter 'Remote System Notify Level:' to "Information".
3. Use the parameter 'Remote System Host IP Address:' to define the IP address of the Syslog server you use.
4. Set the parameter 'Remote System Notify Level:' to "Information".
5. Use the parameter 'Remote System Host IP Address:' to define the IP address of the Syslog server you use.

   Note: The Syslog Server IP address must be one that corresponds with your network environment in which the Syslog server is installed (for example, 10.1.1.1).



AudioCodes

Multi-Service Business Gateway (MSBG)

Configuration Note

AudioCodes MSBG Site-to-Site VPN

With
Check Point Firewall

www.audiocodes.com