

Configuration Note
AudioCodes MSBG Site-to-Site VPN
With
Check Point Firewall

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

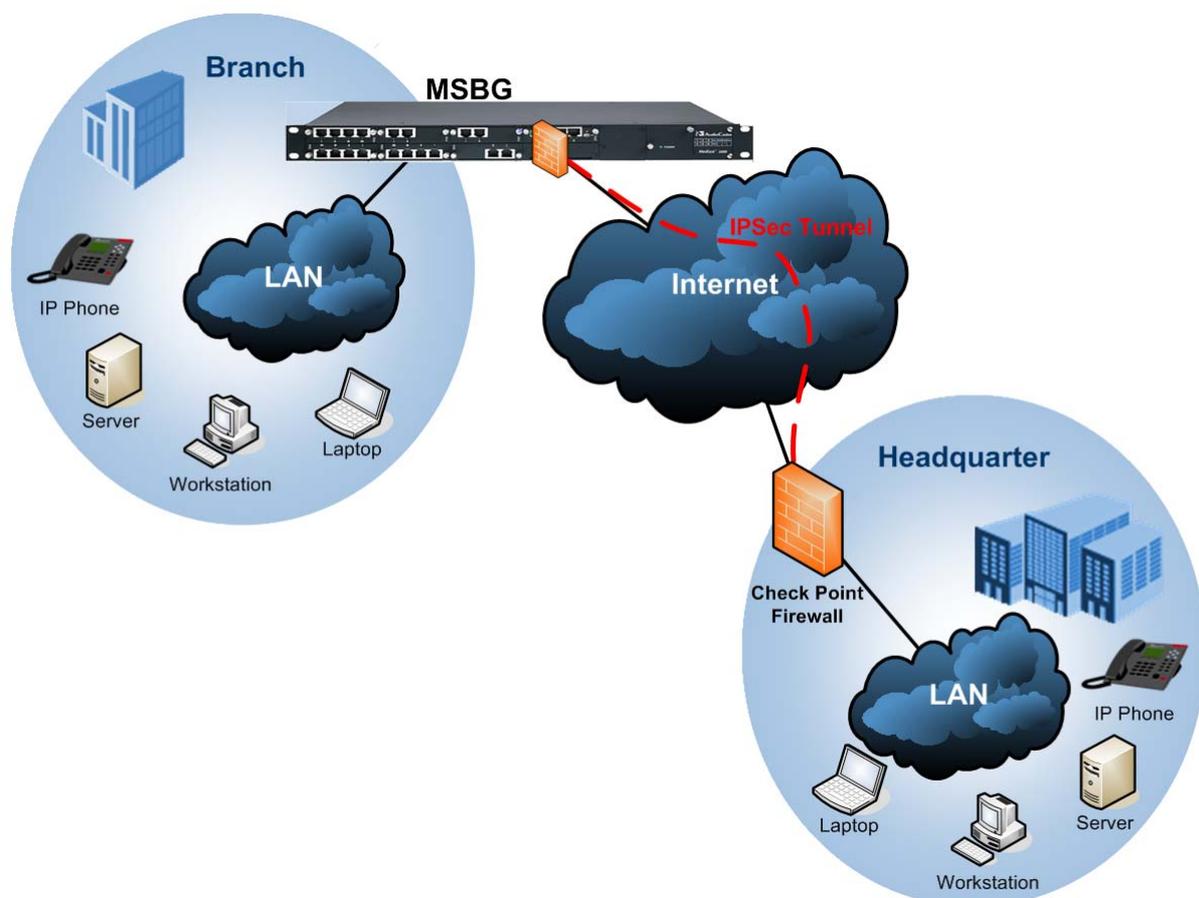
1.1 Introduction

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

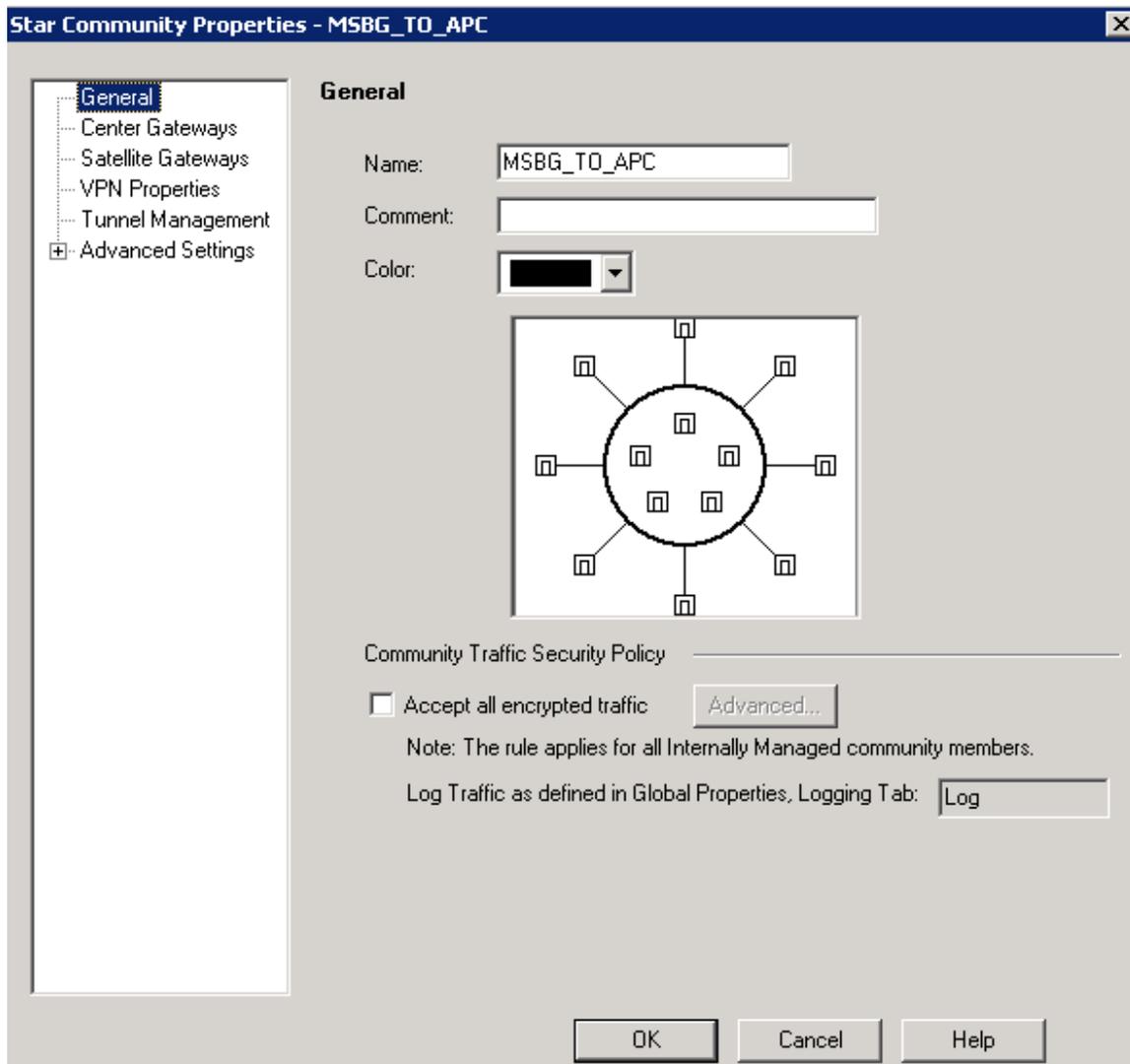
Step 1: Create a New Community

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



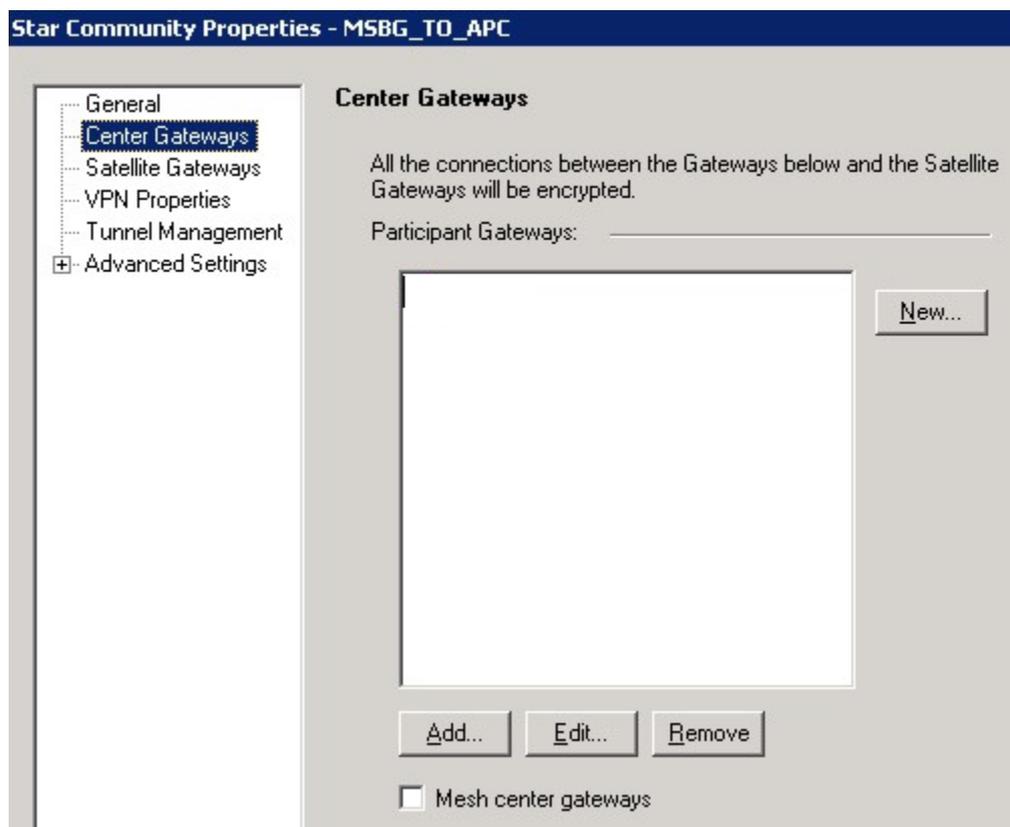
Step 2: Create a New Community – General

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

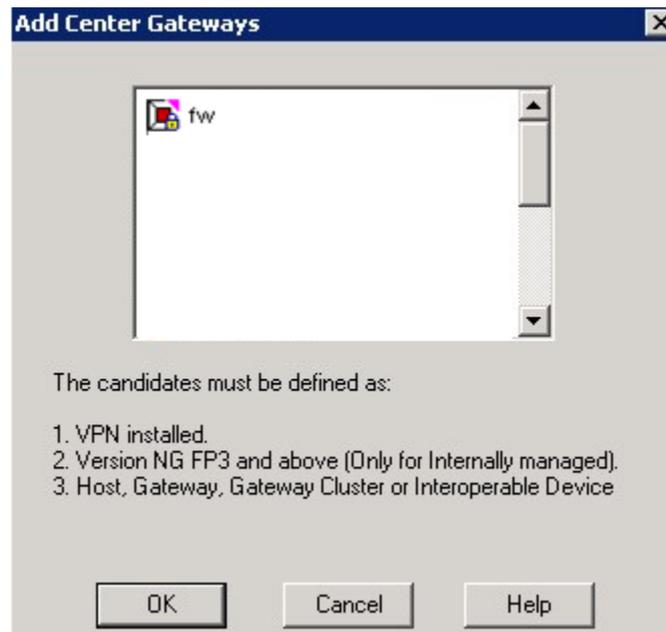


Step 3: Create New Community – Center Gateways

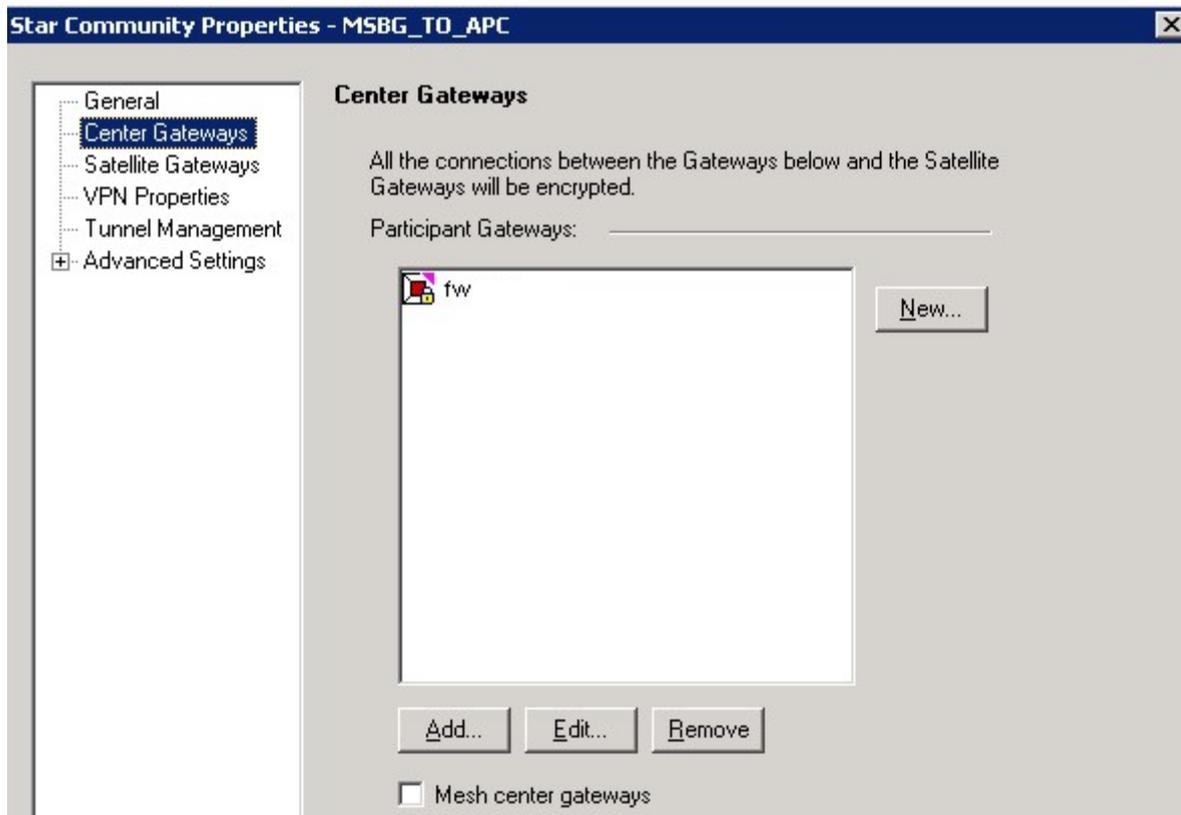
- In 'Center Gateways', click **Add**.



Step 4: Create a New Community – Add Center Gateway

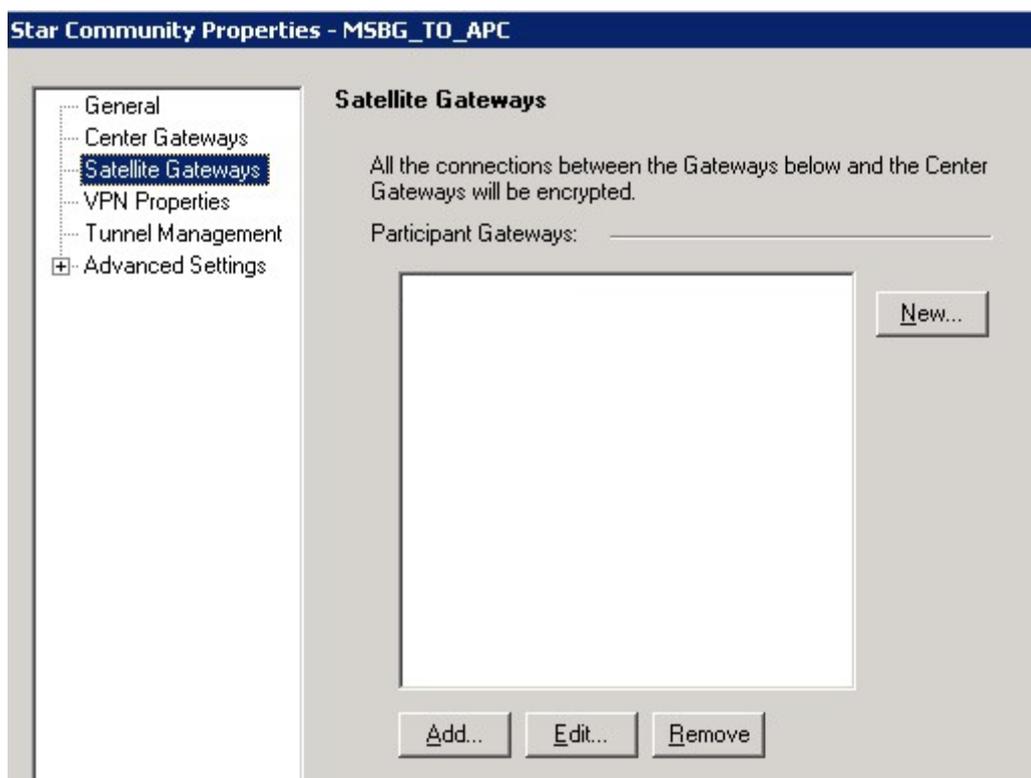


- Select your object from the list (e.g. fw-sys) and then click **OK**.

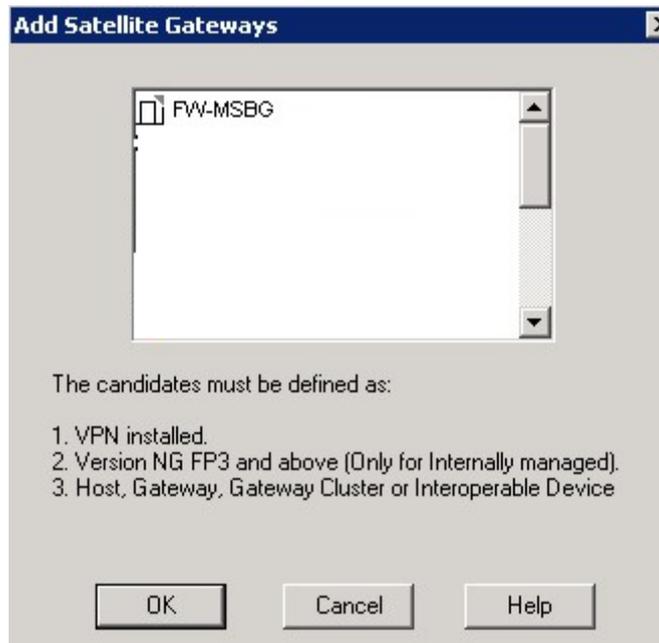


Step 5: Create a New Community - Satellite Gateways

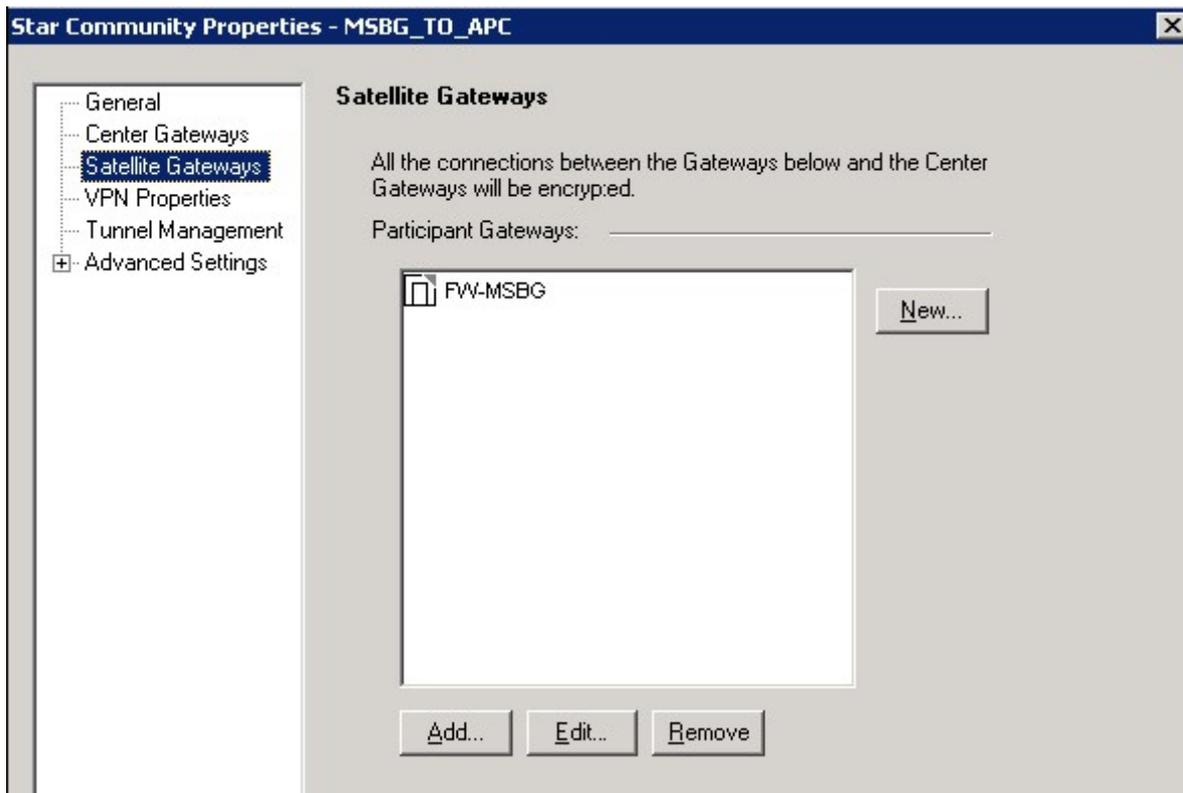
- Click **Add**.



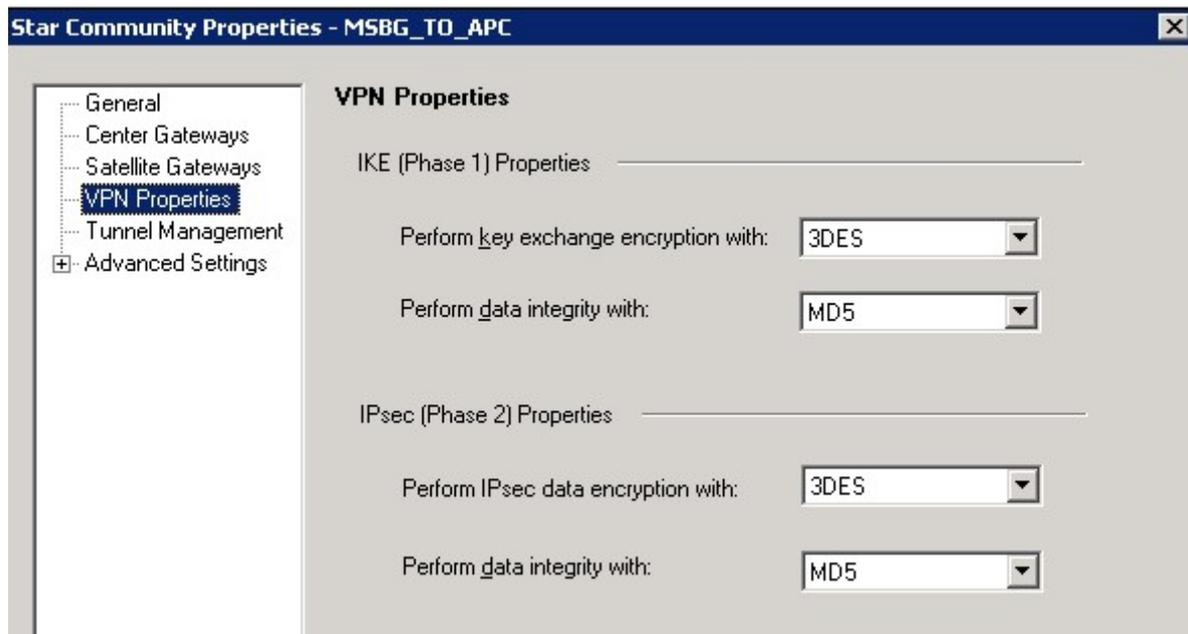
Step 6: Create New Community – Add Satellite Gateways



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



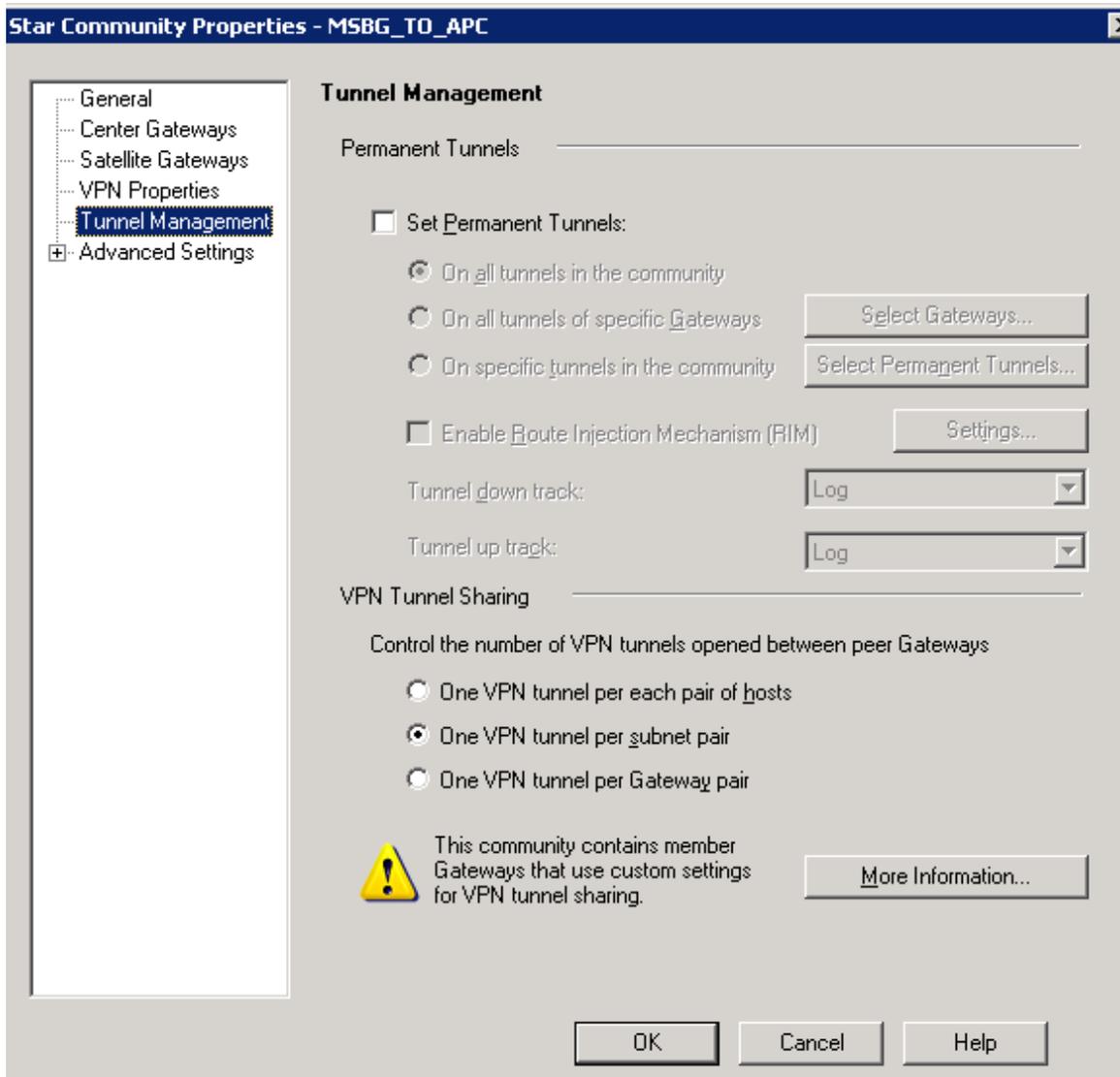
Step 7: Create a New Community - VPN Properties



- 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'.

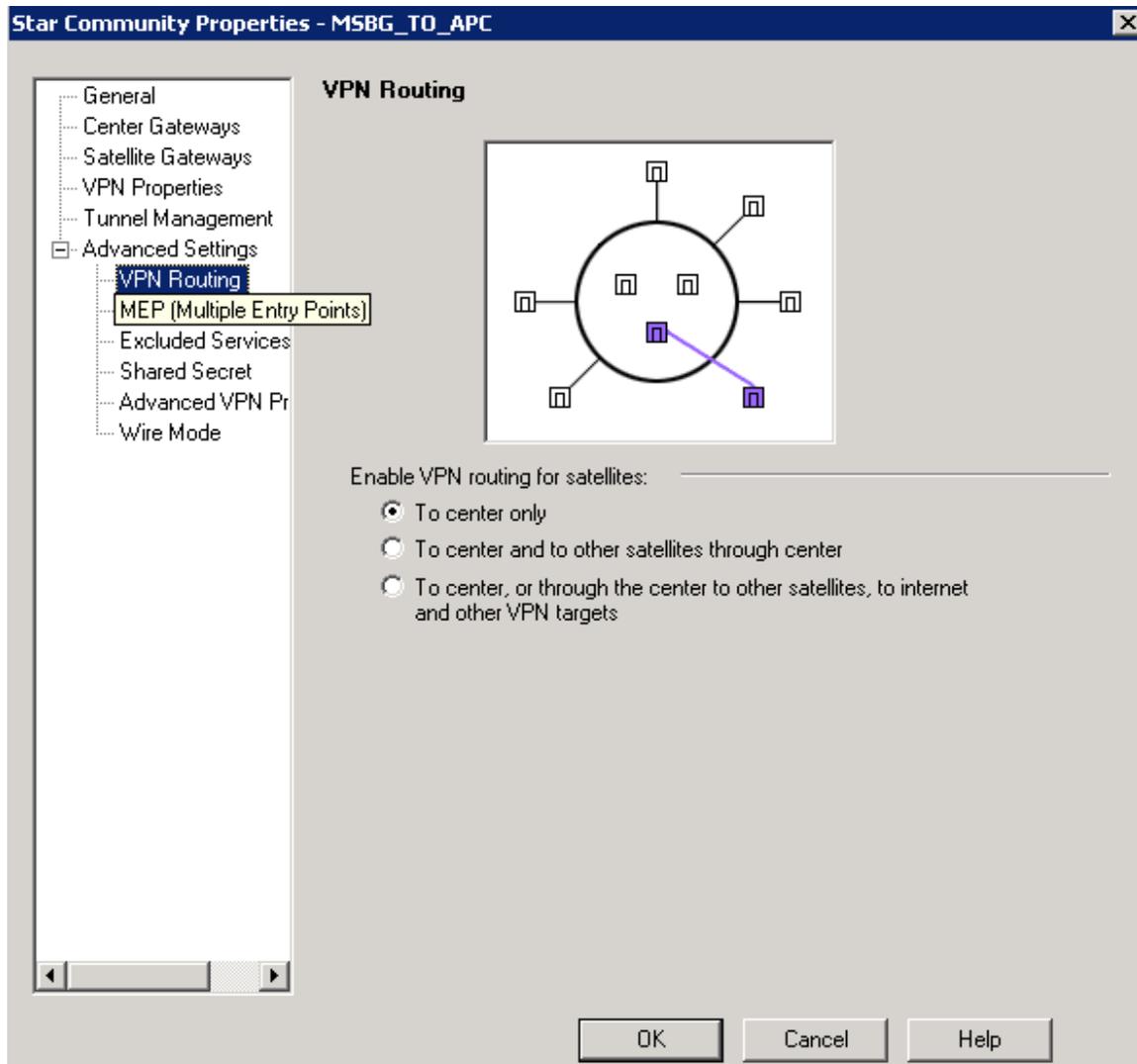
Step 8: Create a New Community – Tunnel Management

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



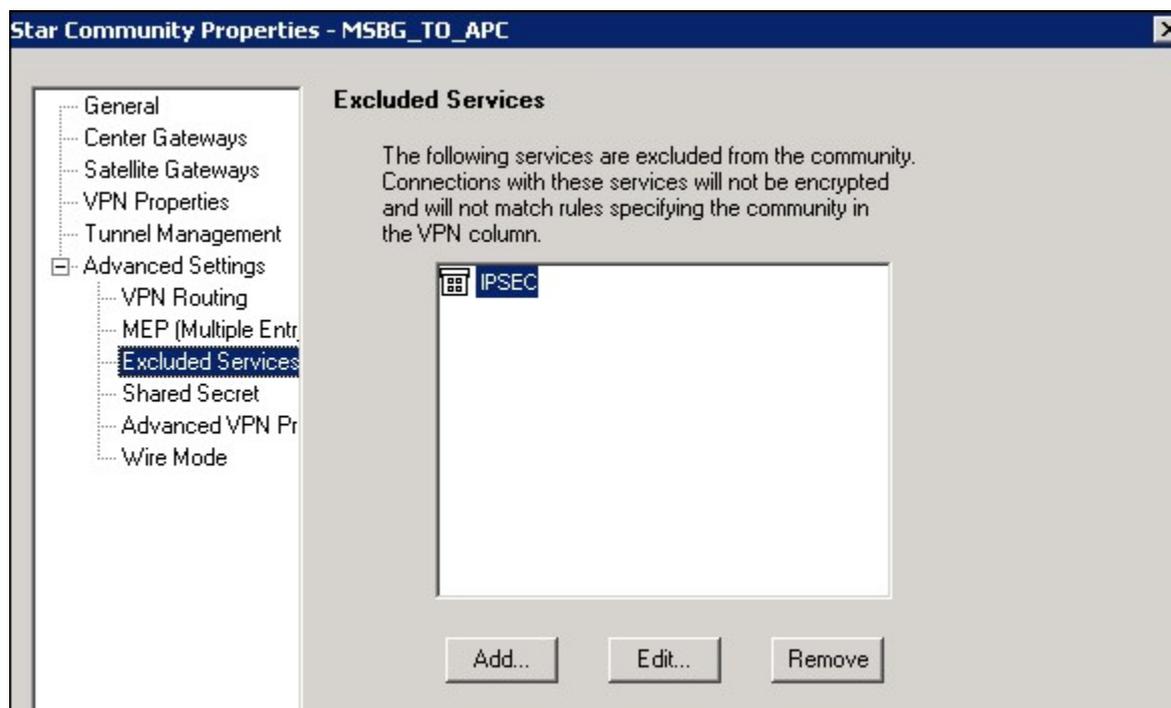
Step 9: Create a New Community – VPN Routing

- Select the 'To center only' option.



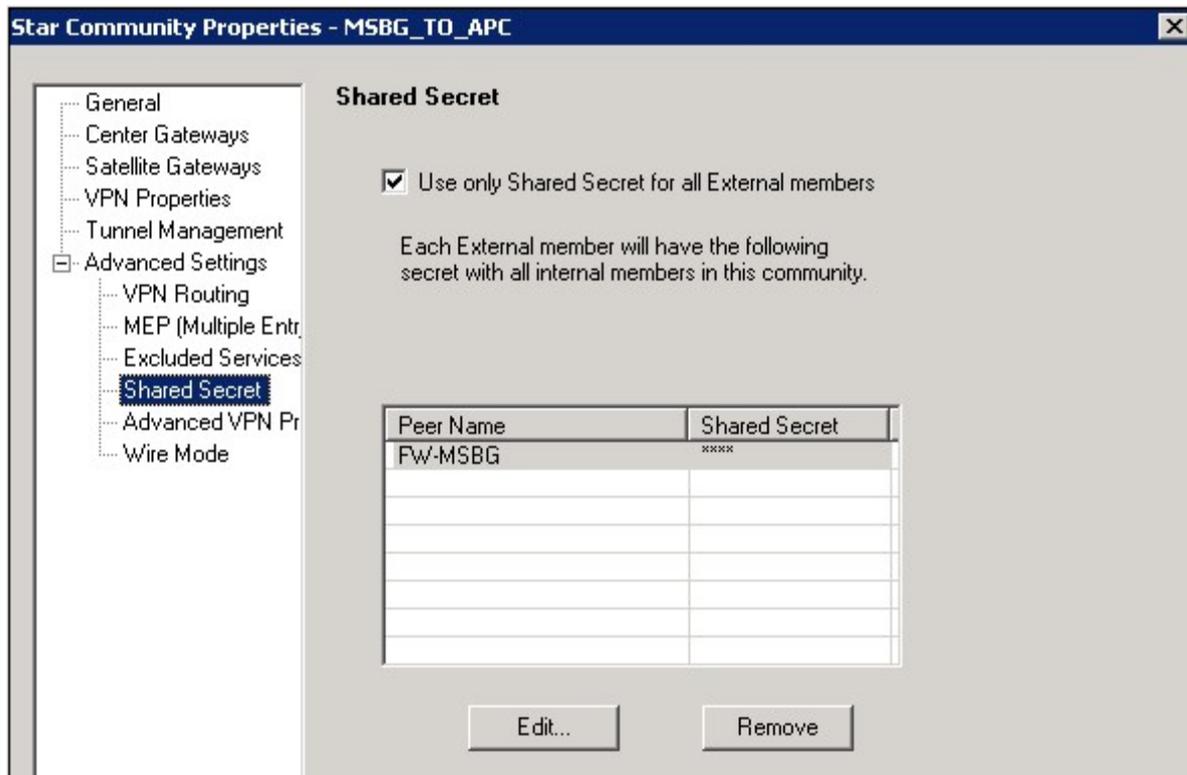
Step 10: Create a New Community – Excluded Services

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



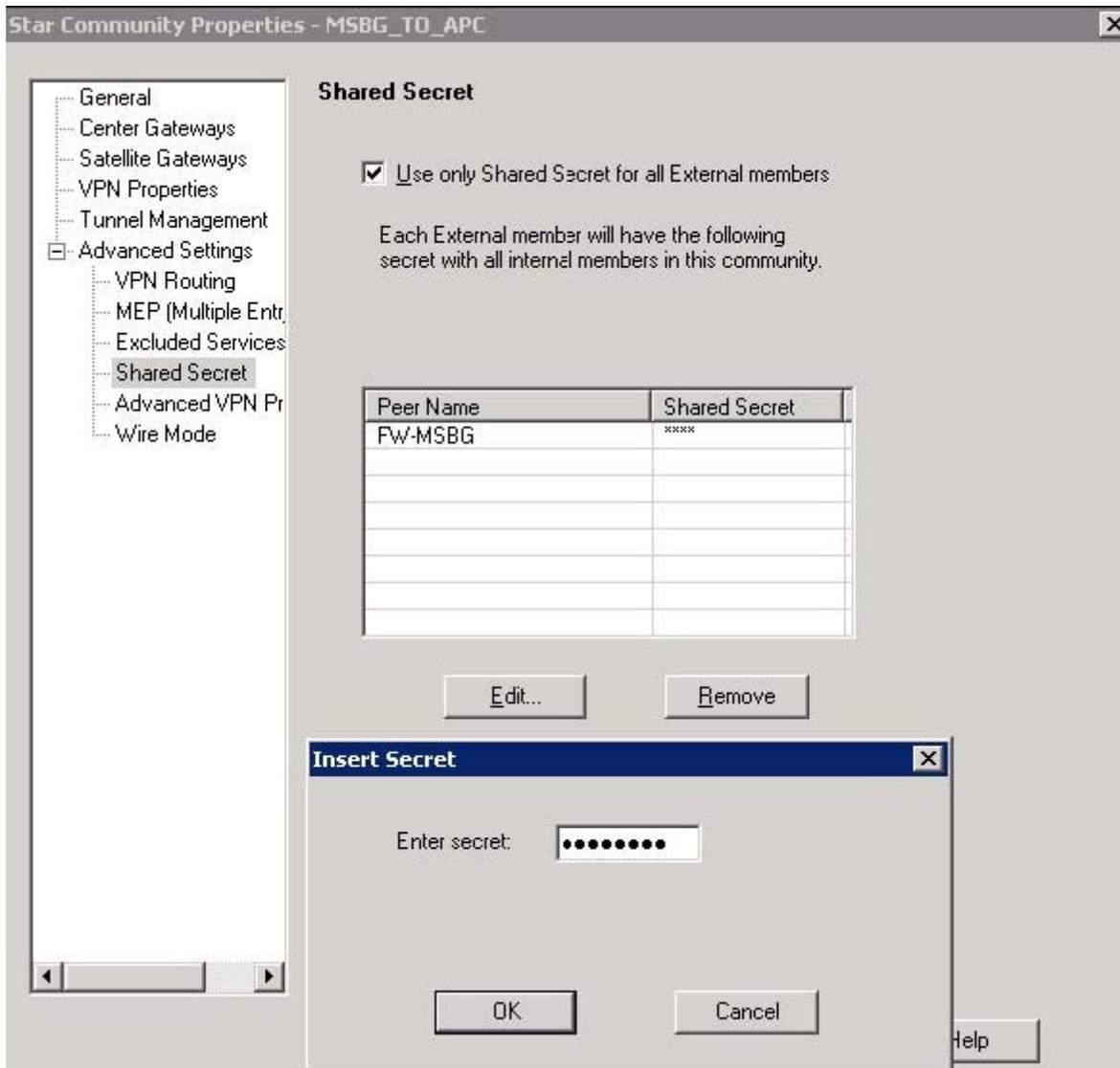
Step 11: Create a New Community – Shared Secret

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



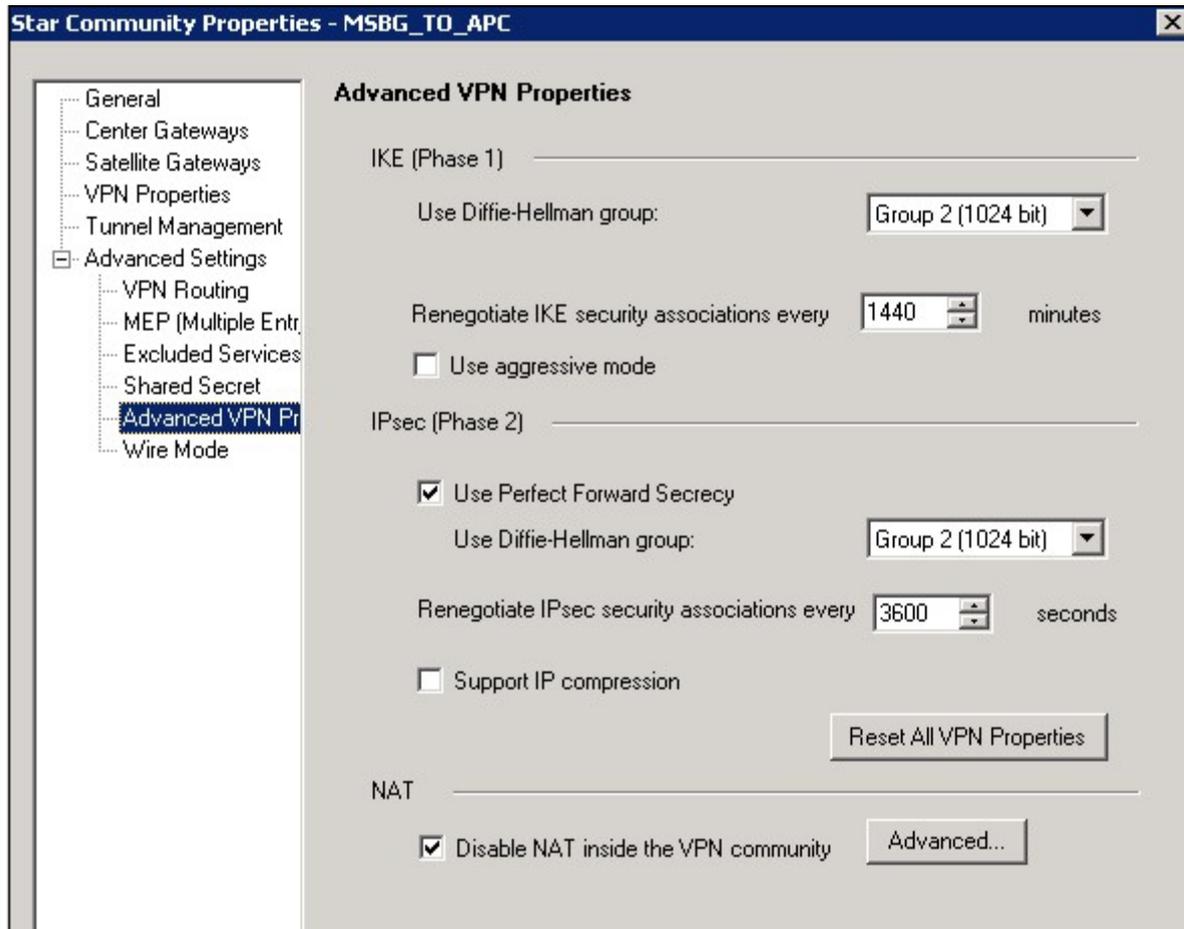
Step 12: Create a New Community – Insert Secret

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



Step 13: Create a New Community – Advance VPN Properties

- Fill as below.



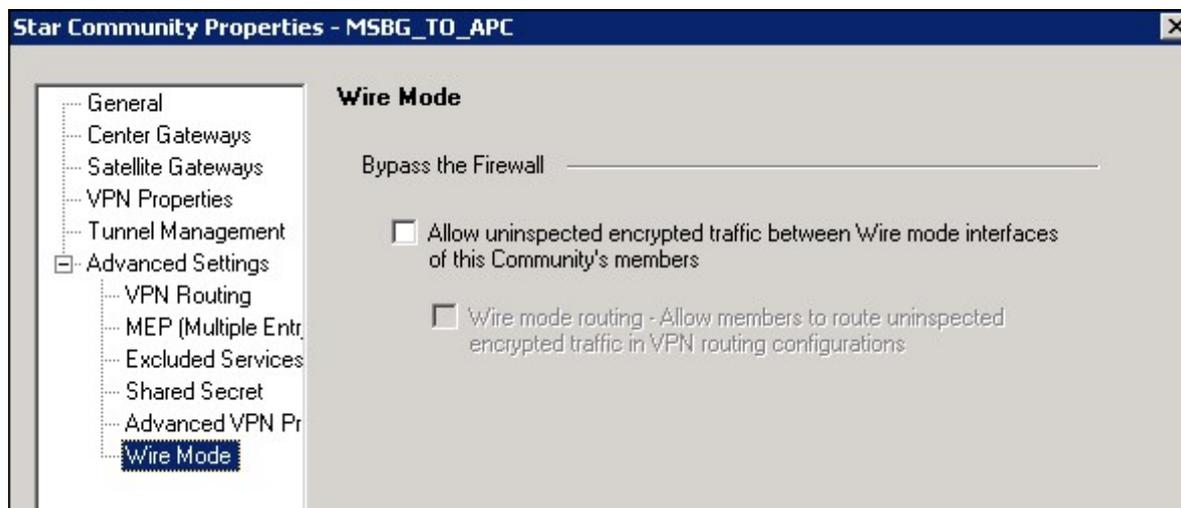
The screenshot shows the 'Star Community Properties - MSBG_TO_APC' dialog box with the 'Advanced VPN Properties' tab selected. The left-hand navigation pane includes options like General, Center Gateways, Satellite Gateways, VPN Properties, Tunnel Management, and Advanced Settings (which is expanded to show VPN Routing, MEP, Excluded Services, Shared Secret, Advanced VPN Properties, and Wire Mode). The main area is titled 'Advanced VPN Properties' and contains the following settings:

- IKE (Phase 1)**
 - Use Diffie-Hellman group: Group 2 (1024 bit)
 - Renegotiate IKE security associations every 1440 minutes
 - Use aggressive mode
- IPsec (Phase 2)**
 - Use Perfect Forward Secrecy
 - Use Diffie-Hellman group: Group 2 (1024 bit)
 - Renegotiate IPsec security associations every 3600 seconds
 - Support IP compression
- NAT**
 - Disable NAT inside the VPN community

Buttons for 'Reset All VPN Properties' and 'Advanced...' are also visible.

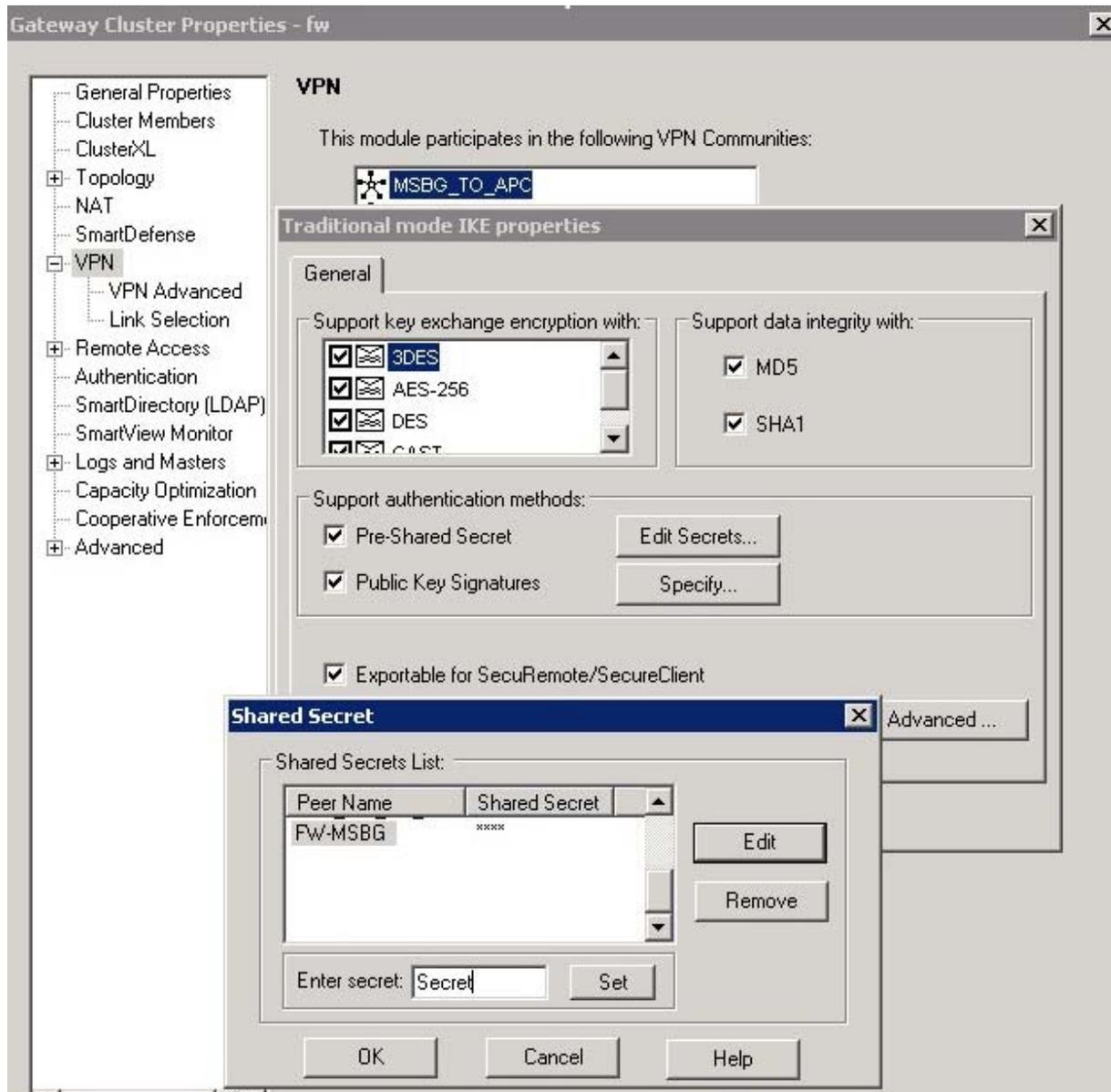
Step 14: Create a New Community – Shared Secret

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



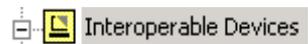
Step 15: Add Secret Password

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).

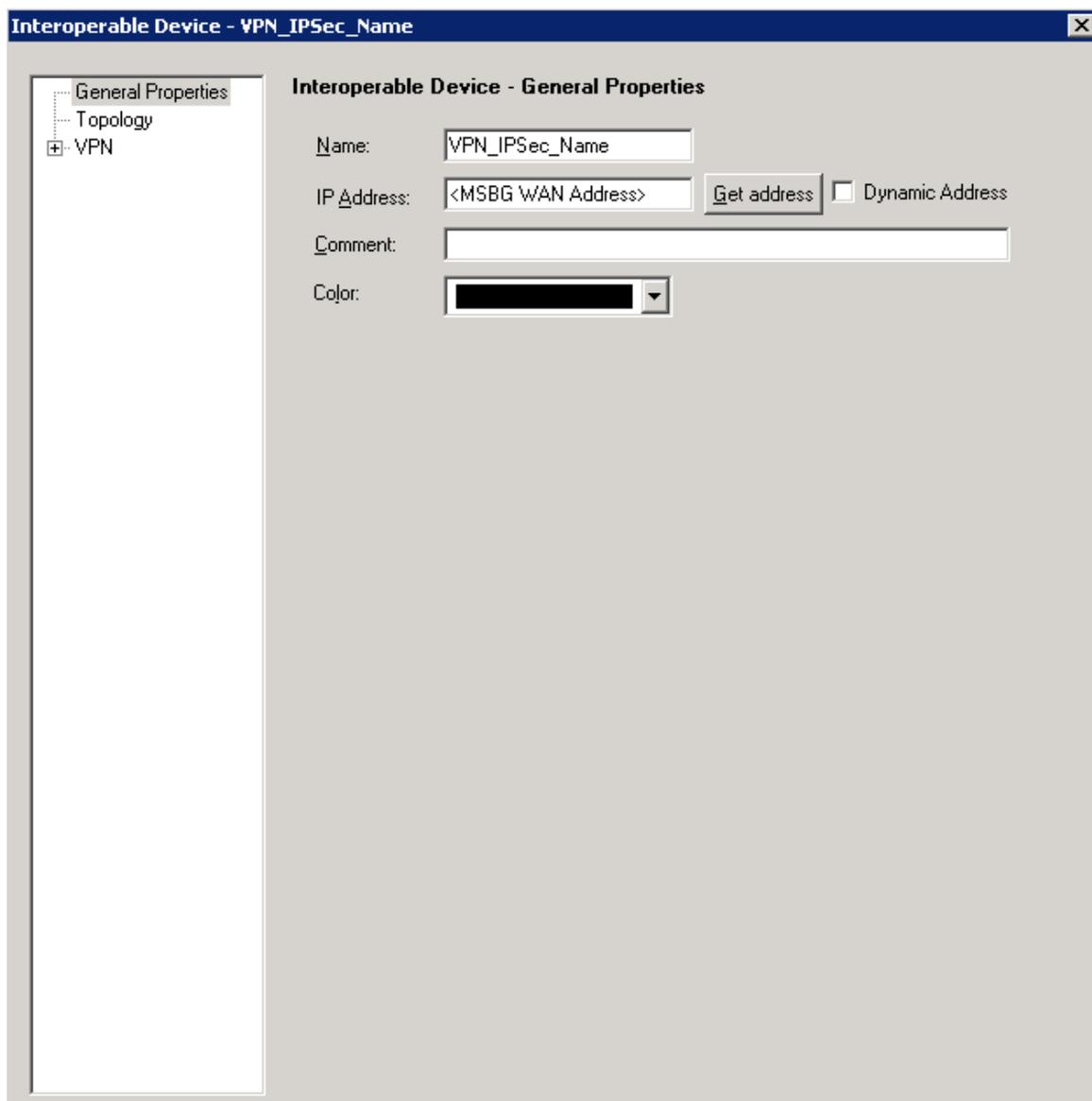


Step 16: Interoperable Device – Setup

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

**Step 17: Interoperable Device – General Properties**

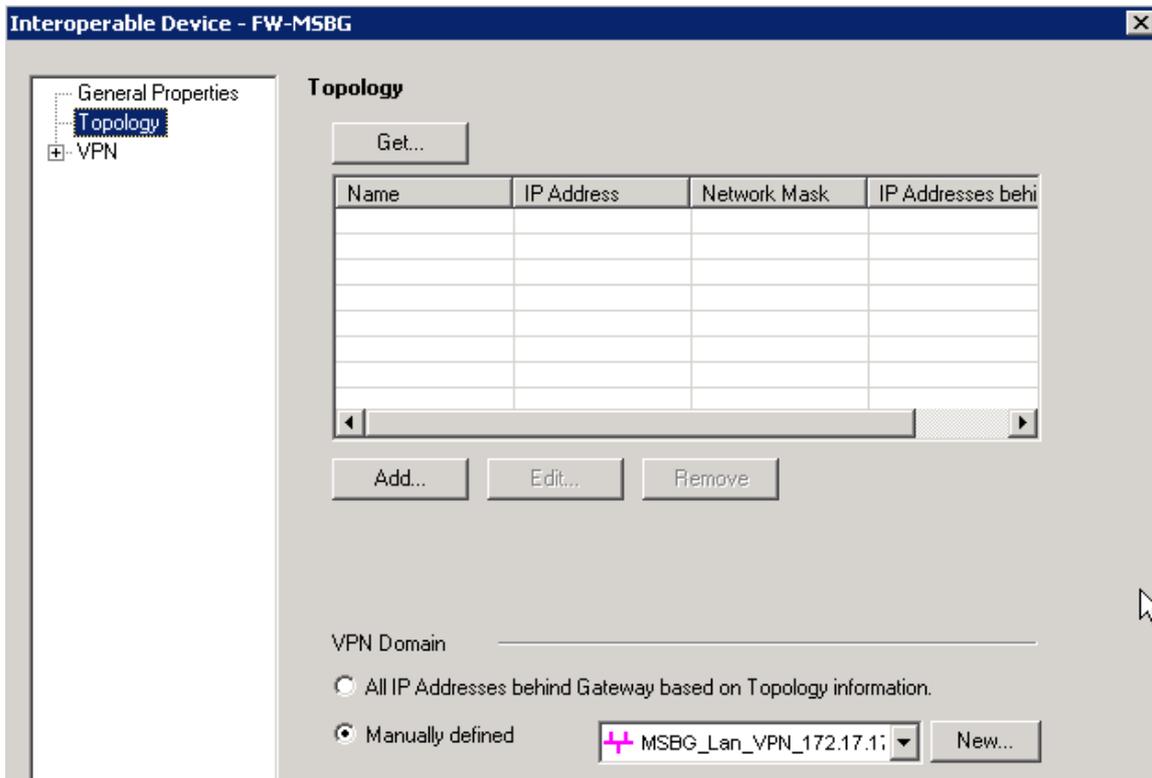
- **Name:** Clearly name.
- **IP Address:** MSBG WAN IP address.

A screenshot of a configuration window titled 'Interoperable Device - VPN_IPSec_Name'. The window has a dark blue title bar with a close button. On the left, there is a tree view with 'General Properties' selected, and 'VPN' expanded. The main area is titled 'Interoperable Device - General Properties' and contains the following fields:

- Name:** A text box containing 'VPN_IPSec_Name'.
- IP Address:** A text box containing '<MSBG WAN Address>', a 'Get address' button, and an unchecked 'Dynamic Address' checkbox.
- Comment:** An empty text box.
- Color:** A color selection dropdown menu showing a black color.

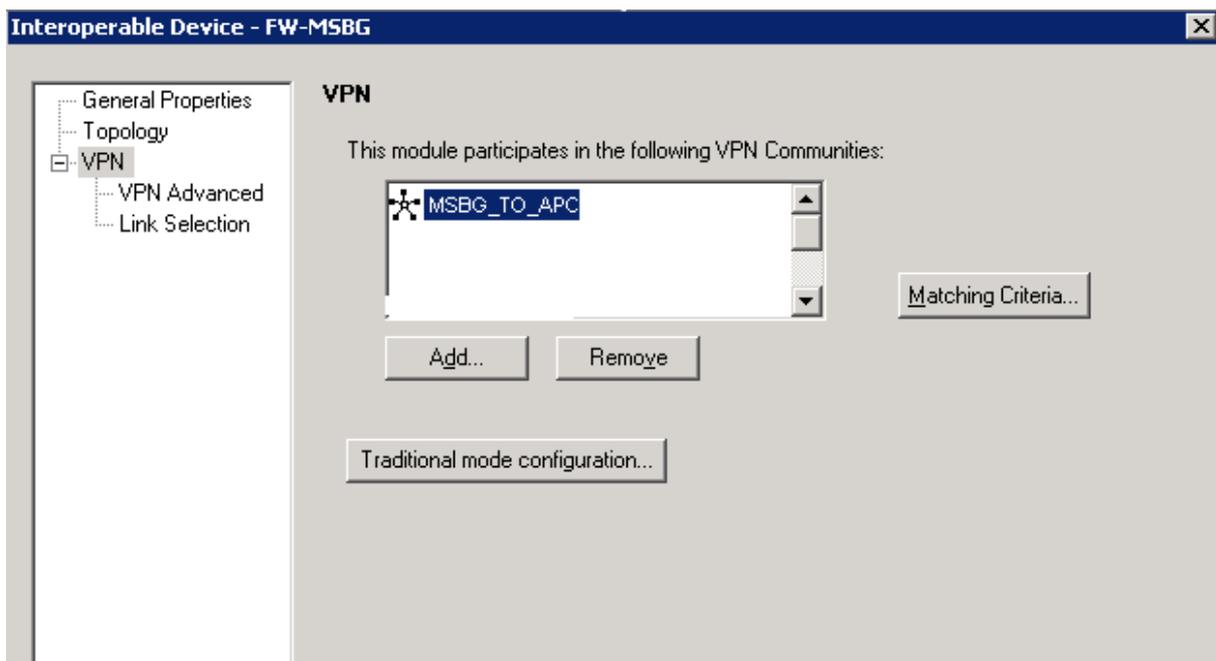
Step 18: Interoperable Device – Topology

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



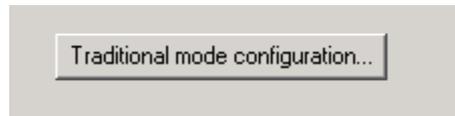
Step 19: Interoperable Device – VPN

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

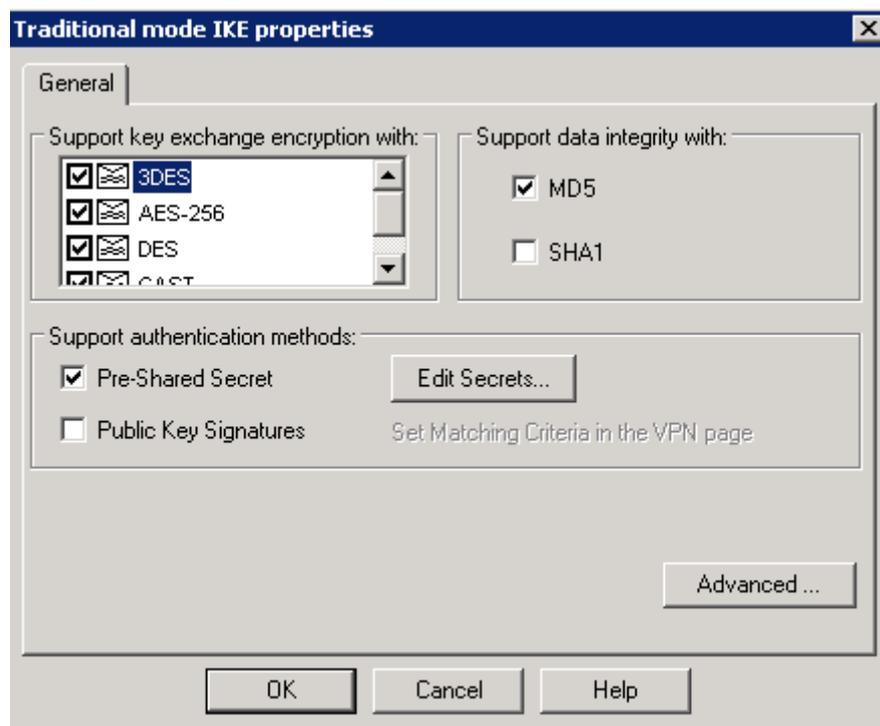


Step 20: Interoperable Device – VPN (Cont...)

- Click **Traditional mode configuration**.

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

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

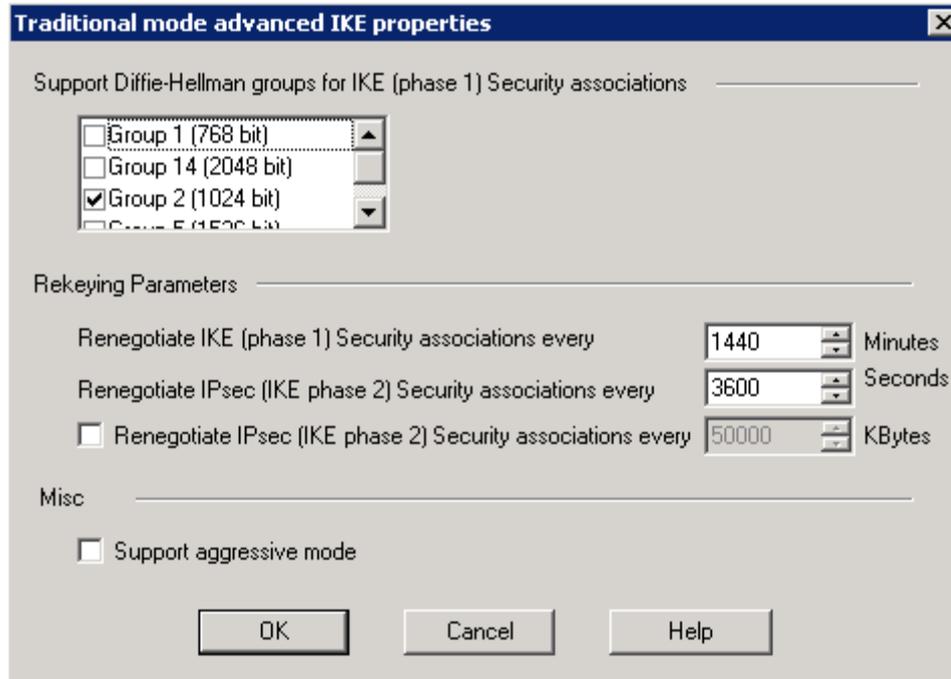
**Step 22: Interoperable Device – VPN (Cont...)**

- Click **Advanced**.



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

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



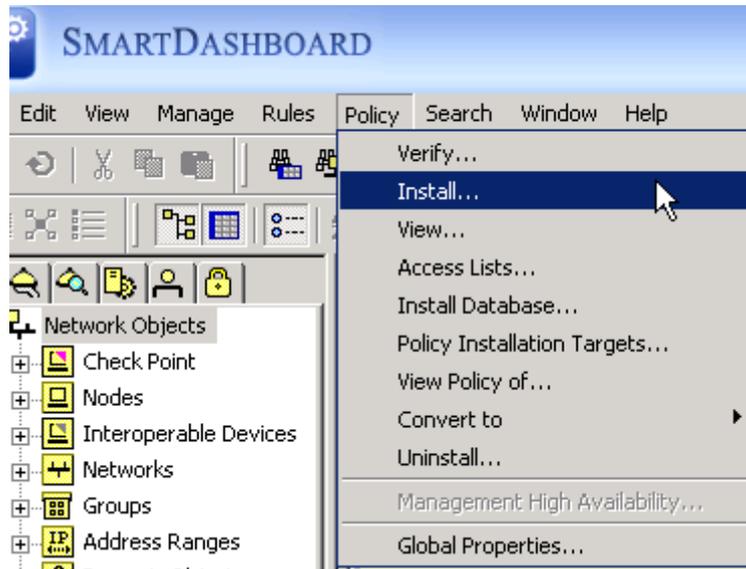
Step 24: Add New Rule – Connection between the VPN LAN to the Local LAN.

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.

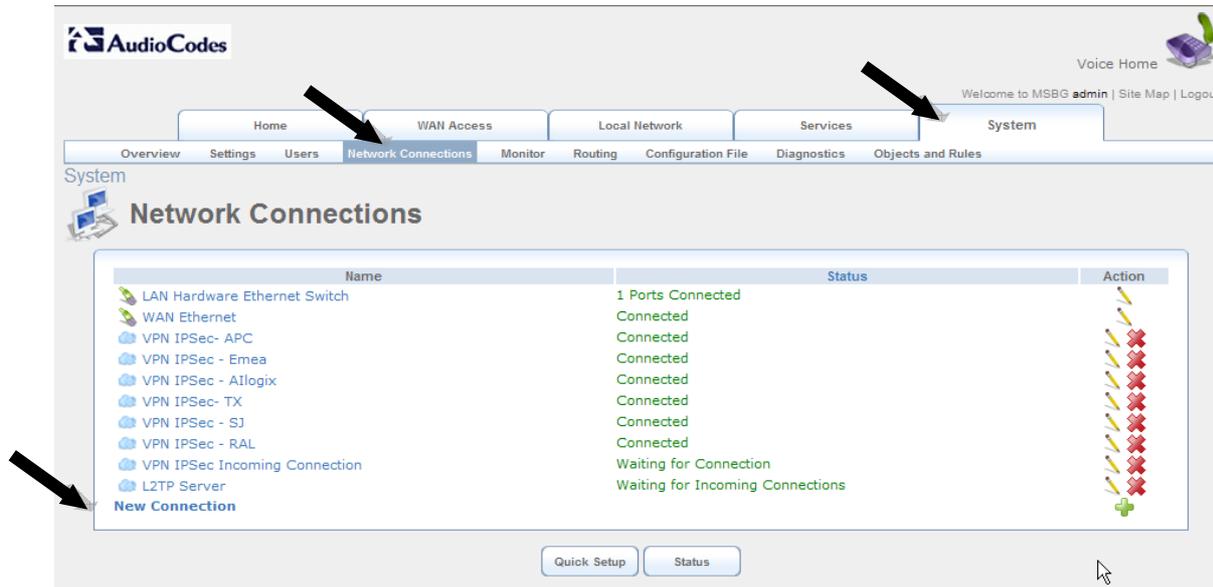
Note the following Web interface guidelines:

- 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

The screenshot shows the AudioCodes MSBG web interface. The top navigation bar includes 'Home', 'WAN Access', 'Local Network', 'Services', and 'System'. Below this is a secondary menu with 'Overview', 'Settings', 'Users', 'Network Connections', 'Monitor', 'Routing', 'Configuration File', 'Diagnostics', and 'Objects and Rules'. The main content area is titled 'System Connection Wizard' and contains the following text:

Choose the type of network connection you want to create, based on your network configuration and your networking needs.

Internet Connection
Connect to the Internet using your external DSL modem, Cable modem or Ethernet connection so you can browse the Web and read email.

Connect to a Virtual Private Network over the Internet
Connect MSBG to a business network using a Virtual Private Network (VPN) so you can work from home, workplace or another location.

At the bottom of the wizard are two buttons: 'Next' (with a right-pointing arrow) and 'Cancel' (with a red X).

- 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



The screenshot shows the AudioCodes MSBG web interface. At the top, there is a navigation bar with tabs for Home, WAN Access, Local Network, Services, and System. Below this is a secondary navigation bar with links for Overview, Settings, Users, Network Connections, Monitor, Routing, Configuration File, Diagnostics, and Objects and Rules. The main content area is titled "System" and "Connect to a Virtual Private Network over the Internet". It prompts the user to "Choose your VPN connection type:" and offers two options: "VPN Client or Point-To-Point" (selected with a radio button and a black arrow) and "VPN Server". Below the options are three buttons: "Back", "Next", and "Cancel".

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

Step 4: VPN Client or Point-To-Point

The screenshot shows the AudioCodes MSBG configuration interface. The top navigation bar includes 'Home', 'WAN Access', 'Local Network', 'Services', and 'System'. The 'System' tab is active, showing sub-tabs for 'Overview', 'Settings', 'Users', 'Network Connections', 'Monitor', 'Routing', 'Configuration File', 'Diagnostics', and 'Objects and Rules'. The 'Network Connections' sub-tab is selected, displaying the 'VPN Client or Point-To-Point' configuration page. The page title is 'VPN Client or Point-To-Point' and it prompts the user to 'Choose one of the following protocols to connect to a remote VPN server:'. Three radio button options are listed: 'Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)', 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)', and 'Internet Protocol Security (IPSec)'. The 'Internet Protocol Security (IPSec)' option is selected, indicated by a black arrow pointing to its radio button. Below the options are three buttons: 'Back', 'Next', and 'Cancel'.

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

Step 5: Internet Protocol Security (IPSec)

Welcome to MSBG admin | Site Map | Logout

Home | WAN Access | Local Network | Services | System

Overview | Settings | Users | Network Connections | Monitor | Routing | Configuration File | Diagnostics | Objects and Rules

Internet Protocol Security (IPSec)

Configure your IPSec connection properties:

Host Name or IP Address of Destination Gateway:	<FW IP>
Remote IP:	Same as Gateway
Encapsulation Type:	Tunnel
Shared Secret:	KEY Secret name

← Back Next → × Cancel

- **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

AudioCodes

Voice Home

Welcome to MSBG **admin** | Site Map | Logout

Home WAN Access Local Network Services **System**

Overview Settings Users **Network Connections** Monitor Routing Configuration File Diagnostics Objects and Rules

System

Connection Summary

You have successfully completed the steps needed to create the following connection:

- IPSec connection with 192.168.15.1

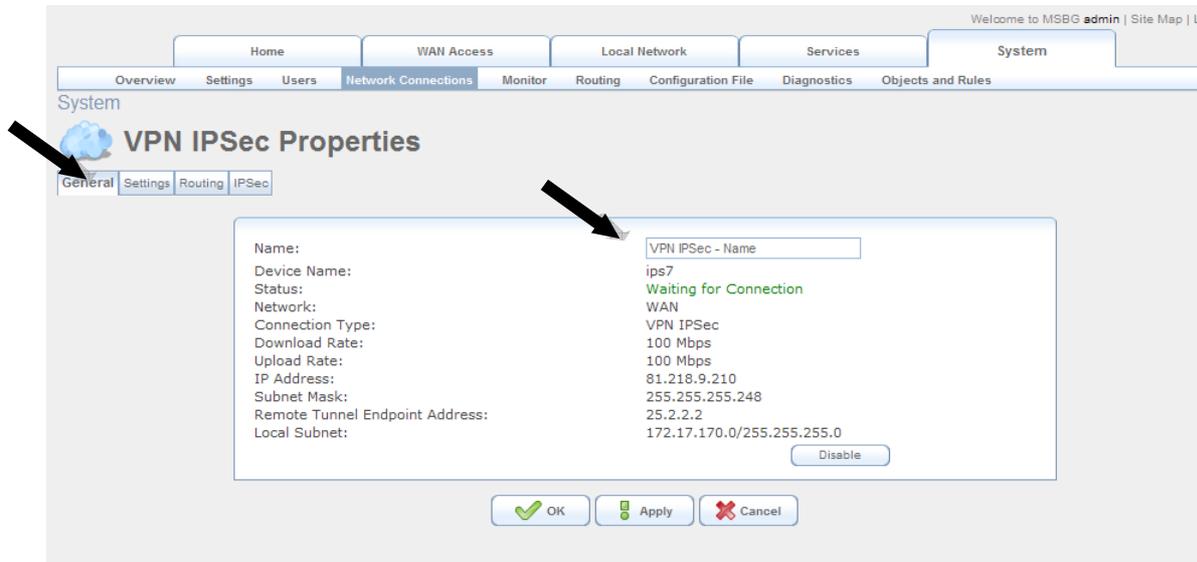
Edit the Newly Created Connection

Press **Finish** to create the connection.

- 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.



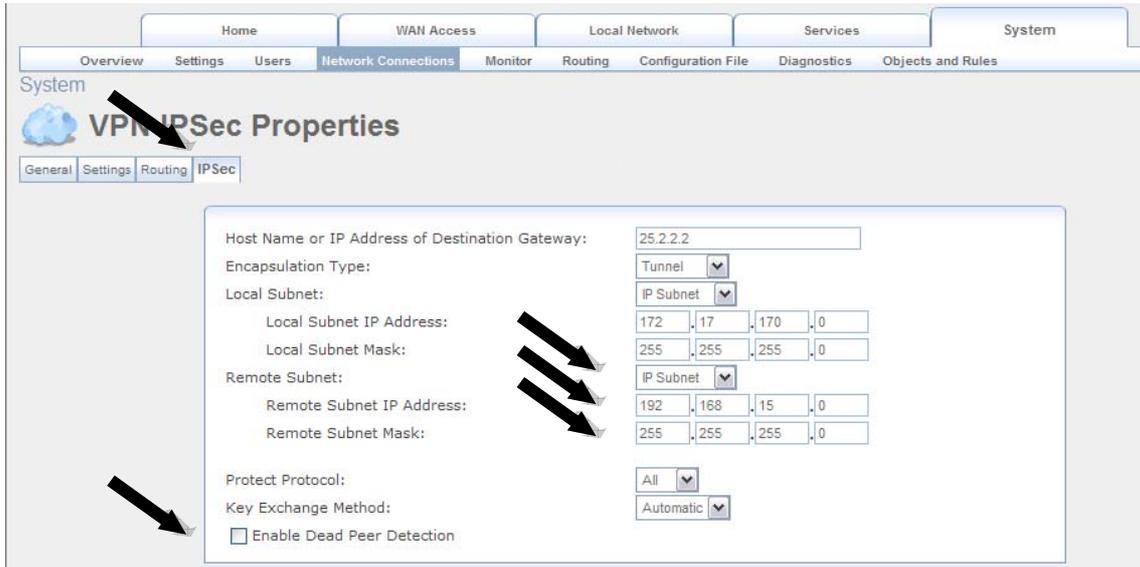
Step 9: Voice Mail Settings

Routing tab. Do not configure this setting.



Step 10: TDM BUS Settings

Routing tab.



System

Overview Settings Users **Network Connections** Monitor Routing Configuration File Diagnostics Objects and Rules

System

VPN IPsec Properties

General Settings Routing **IPsec**

Host Name or IP Address of Destination Gateway: 25.2.2.2

Encapsulation Type: Tunnel

Local Subnet:

Local Subnet IP Address: 172 . 17 . 170 . 0

Local Subnet Mask: 255 . 255 . 255 . 0

Remote Subnet:

Remote Subnet IP Address: 192 . 168 . 15 . 0

Remote Subnet Mask: 255 . 255 . 255 . 0

Protect Protocol: All

Key Exchange Method: Automatic

Enable Dead Peer Detection

- 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...)

IPsec Automatic Phase 1

Mode: Main Mode

Life Time in Seconds (1-28800): 1440

Rekey Margin (start negotiation prior to expiration: 1-540): 540

Rekey Fuzz Percent (can be more than 100 Percent: 1-200): 100

Peer Authentication: IPsec Shared Secret

IPsec Shared Secret: Secret

Encryption Algorithm

DES-CBC

3DES-CBC

AES128-CBC

AES192-CBC

AES256-CBC

Hash Algorithm

Allow Peers to Use MD5

Allow Peers to Use SHA1

Group Description Attribute

DH Group 1

DH Group 2

DH Group 5

- 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...)

IPsec Automatic Phase 2

Life Time in Seconds (1-86400):

Group Description Attribute

Same group as phase 1

DH Group 1

DH Group 2

DH Group 5

Encryption Algorithm

Allow ESP Protocol with DES-CBC Encryption

Allow ESP Protocol with 3DES-CBC Encryption

Allow ESP Protocol with AES-CBC 128-bit Encryption

Allow ESP Protocol with AES-CBC 192-bit Encryption

Allow ESP Protocol with AES-CBC 256-bit Encryption

Authentication Algorithm (for ESP protocol)

Allow Peers to Use MD5

Allow Peers to Use SHA1

- 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.

AudioCodes

Voice Home

Welcome to MSBG admin | Site Map | Logout

Home WAN Access Local Network Services System

Overview Settings Users Network Connections Monitor Routing Configuration File Diagnostics Objects and Rules

System

Network Connections

Name	Status	Action
LAN Hardware Ethernet Switch	1 Ports Connected	
WAN Ethernet	Connected	
VPN IPsec - Name	Waiting for Connection	

New Connection

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

Monitor

Network Connections

Name	LAN Hardware Ethernet Switch	WAN Ethernet	VPN IPsec - Name
Device Name	eth0	eth1	ips0
Status	1 Ports Connected	Connected	Waiting for Connection
Network	LAN	WAN	WAN
Connection Type	Hardware Ethernet Switch	Ethernet	VPN IPsec
Download Rate	100 Mbps	100 Mbps	100 Mbps
Upload Rate	100 Mbps	100 Mbps	100 Mbps
MAC Address	00:90:8f:1e:71:65	00:90:8f:1e:71:66	
IP Address	10.15.7.21	11.1.1.1	11.1.1.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway		11.1.1.10	
DNS Server	10.1.1.11 10.1.1.10	11.1.1.10	
IP Address Distribution	Disabled	Disabled	
Remote Tunnel Endpoint Address			192.168.15.1
Local Subnet			10.15.7.0/255.255.255.0
Remote Subnet			172.17.1.0/255.255.255.0
Received Packets	1309212	5087	
Sent Packets	168265	74	
Received Bytes	114524822	705037	
Sent Bytes	51884593	14268	
Receive Errors	0	0	
Receive Drops	0	0	
Time Span	173:04:30	173:04:30	

Close Automatic Refresh Off Reset Statistics Refresh

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

System Has Been Up For: 7 days, 5 hours
Load Average (1 / 5 / 15 mins.): 0.00 / 0.00 / 0.00

Process	Total Virtual Memory (VmData)	Heap size (VmSize)
init	2072 kB	2660 kB
sh	1060 kB	1796 kB
wdg	7220 kB	9648 kB
openrg	12368 kB	19996 kB
l2tpd	3096 kB	3684 kB
pluto	4208 kB	5360 kB
portmap	1068 kB	1564 kB
_pluto_adns	4104 kB	4852 kB
acm_sync_server	1044 kB	1528 kB

- **Log:** displays online Syslog.

Press the **Refresh** button to update the data.

Time	Component	Severity	Details
Jan 8 04:08:14 2003	IPSec	Warning	pluto[44]: "ips0" #6: max number of retransmissions (2) reached STATE_MAIN_I1. No acceptable response to our first IKE message
Jan 8 04:08:14 2003	IPSec	Information	pluto[44]: RATELIMIT: 2 messages of type IPSec IKE packet reported 70 second(s) ago
Jan 8 04:07:04 2003	IPSec	Warning	pluto[44]: "ips0" #5: max number of retransmissions (2) reached STATE_MAIN_I1. No acceptable response to our first IKE message
Jan 8 04:07:04 2003	IPSec	Information	pluto[44]: RATELIMIT: 2 messages of type IPSec IKE packet reported 70 second(s) ago
Jan 8 04:05:54 2003	IPSec	Warning	pluto[44]: "ips0" #4: max number of retransmissions (2) reached STATE_MAIN_I1. No acceptable response to our first IKE message
Jan 8 04:05:54 2003	IPSec	Information	pluto[44]: RATELIMIT: 6 messages of type IPSec IKE packet reported 70 second(s) ago
Jan 8 04:04:44 2003	IPSec	Information	pluto[44]: RATELIMIT: 2 messages of type IPSec IKE packet reported 1 second(s) ago

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

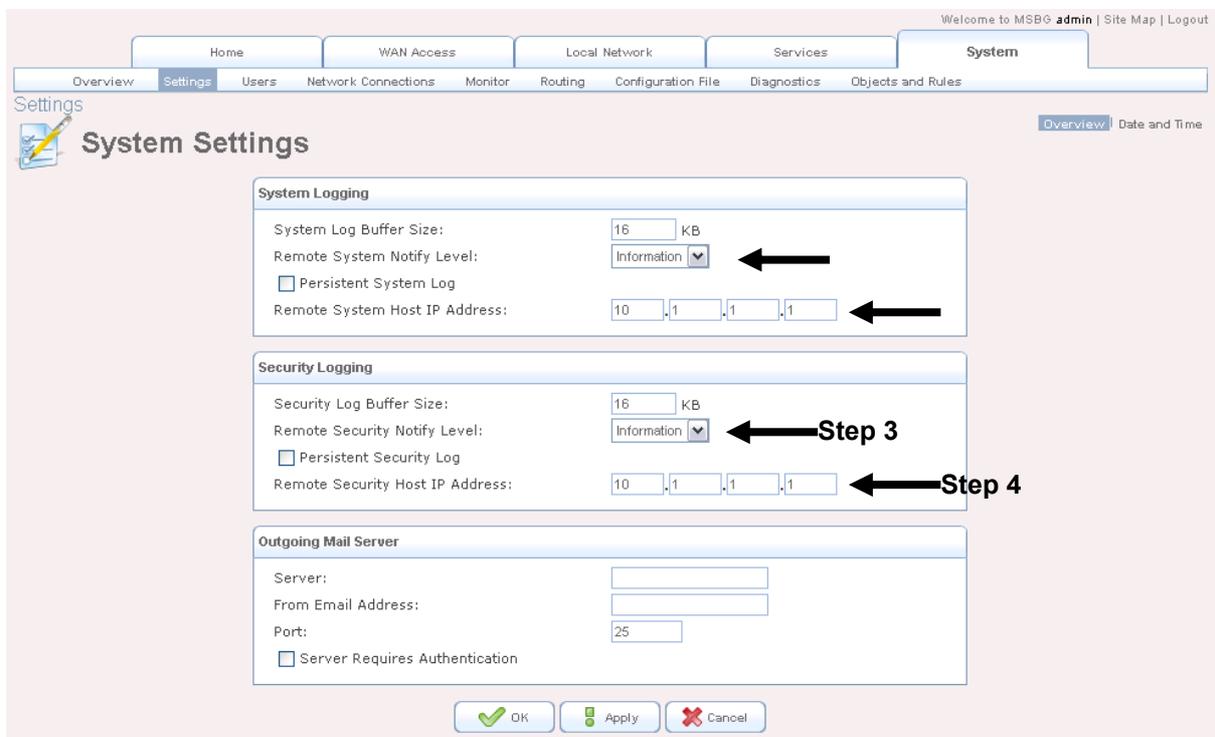
4.2 Configuring AudioCodes MSBG for Syslog Server

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).



The screenshot displays the 'System Settings' page in the MSBG admin interface. The page is titled 'System Settings' and includes a navigation menu at the top with options like Home, WAN Access, Local Network, Services, and System. The 'System' tab is selected, and the 'Settings' sub-tab is active. The main content area is divided into three sections: 'System Logging', 'Security Logging', and 'Outgoing Mail Server'. In the 'System Logging' section, the 'Remote System Notify Level' is set to 'Information' (indicated by a black arrow) and the 'Remote System Host IP Address' is set to '10.1.1.1' (indicated by a black arrow). In the 'Security Logging' section, the 'Remote Security Notify Level' is set to 'Information' (indicated by a black arrow labeled 'Step 3') and the 'Remote Security Host IP Address' is set to '10.1.1.1' (indicated by a black arrow labeled 'Step 4'). The 'Outgoing Mail Server' section is empty. At the bottom of the page, there are three buttons: 'OK', 'Apply', and 'Cancel'.

Configuration Note
AudioCodes MSBG Site-to-Site VPN
With
Check Point Firewall



www.audiocodes.com