

Multi-Service Business Gateway (MSBG)

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



Table of Contents

1	Con	ponents Information	7
	1.1 1.2 1.3	Introduction Check Point AudioCodes MSBG	7 8 8
2	Che	ck Point Setup Notes	9
	2.1 2.2 2.3	Check Point Configuration Special Instructions for Check Point Configuration Other Comments	9 27 27
3	MSE	3G Setup Notes	29
	3.1	Configuring AudioCodes MSBG	29
4	Troubleshooting		41
	4.1 4.2	Online Monitor Configuring AudioCodes MSBG for Syslog Server	41 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 <u>support@audiocodes.com</u>, 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'.

Security 📰 NAT 🏭 SmartDefense 🖳 Content Inspection	SmartDefense Services	🖸 VPN 🙀 QoS 🛄 Deskt	op
	م م_م	New Community	Meshed
	a a	 VPN Communities View 	Star
	MSBG_TO_APC	Sort by	
		View 🕨	
		Print	R.

Step 2: Create a New Community – General

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

Star Community Propertie	es - MSBG_TO_APC X
Star Community Propertie	S - MSBG_TO_APC General Name: MSBG_TO_APC Comment: Color: Image: Im
	Community Traffic Security Policy Accept all encrypted traffic Advanced Note: The rule applies for all Internally Managed community members. Log Traffic as defined in Global Properties, Logging Tab: Log
	OK Cancel Help



Step 3: Create New Community – Center Gateways

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

General Center Gateways	Center Gateways
- Satellite Gateways - VPN Properties - Tunnel Management	All the connections between the Gateways below and the Satelli Gateways will be encrypted. Participant Gateways:
Hanner Hangenreik Er Advanced Settings	<u>N</u> ew
	Add Edit <u>R</u> emove

Add Cente	er Gateways		×
	fw		
The car	ndidates must	be defined as:	
1. VPN 2. Versio 3. Host,	installed. on NG FP3 an .Gateway, Ga	id above (Only for Ir teway Cluster or Inti	nternally managed). eroperable Device
	OK	Cancel	Help

Step 4: Create a New Community – Add Center Gateway

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

Star Community Properties - MSBG_TO_APC	×
General Center Gateways VPN Properties Tunnel Management Advanced Settings	



Step 5: Create a New Community - Satellite Gateways

Click Add.

General	Satellite Gateways
Satellite Gateways	All the connections between the Gateways below and the Cente
VPN Properties	Cateways will be encrypted.
- Advanced Settings	
	New

i i	
	V
ne candidates must be defi	ined as:
VPN installed. Version NG FP3 and abov Host Gateway, Gateway	ve (Only for Internally managed) Cluster or Interoperable Device

Step 6: Create New Community – Add Satellite Gateways

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

Star Community Propertie	s - MSBG_TO_APC	×
General Center Gateways Satellite Gateways VPN Properties Tunnel Management ⊕ Advanced Settings	Satellite Gateways All the connections between the Gateways below and the Center Gateways will be encrypred. Participant Gateways: FW-MSBG New	
	Add <u>E</u> dit <u>R</u> emove	



Step 7: Create a New Community - VPN Properties

ieneral	VPN Properties	
Center Gateways Satellite Gateways /PN Properties	IKE (Phase 1) Properties	
unnel Management dvanced Settings	Perform key exchange encryption with:	3DES 💌
_	Perform <u>d</u> ata integrity with:	MD5
	IPsec (Phase 2) Properties	
	Perform IPsec data encryption with:	3DES 💌
	Perform data integrity with:	MD5

- 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.

ar Community Propertie	s - MSBG_TO_APC	
; General	Tunnel Management	
 Center Gateways Satellite Gateways VPN Properties 	Permanent Tunnels	
Tunnel Management	🔲 Set <u>P</u> ermanent Tunnels:	
⊡- Advanced Settings	On all tunnels in the community	
	On all tunnels of specific <u>G</u> ateways	S <u>e</u> lect Gateways
	f C On specific tunnels in the community	Select Permanent Tunnels
	🔲 Enable <u>R</u> oute Injection Mechanism (RI	M) Settings
	Tunnel <u>d</u> own track:	Log
	Tunnel up tra <u>o</u> k:	Log
	VPN Tunnel Sharing	,
	Control the number of VPN tunnels opened bet	ween peer Gateways
	One VPN tunnel per each pair of <u>h</u> osts	
	One VPN tunnel per subnet pair	
	🔿 One VPN tunnel per Gateway pair	
	This community contains member Gateways that use custom settings for VPN tunnel sharing.	More Information
	ОК С	ancel Help



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.

General Center Gateways Satellite Gateways VPN Properties Tunnel Management Advanced Settings WPN Routing MEP (Multiple Entr Excluded Services Shared Secret Advanced VPN Pr Wire Mode	Excluded Services The following services are excluded from the community. Connections with these services will not be encrypted and will not match rules specifying the community in the VPN column. IFF IPSEC	
	Add Edit Remove	

Step 11: Create a New Community – Shared Secret

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

General	Shared Secret		
	Each External member secret with all internal r	ret for all External members will have the following nembers in this community.	
MEP (Multiple Entr, Excluded Services Shared Secret Advanced VPN Pr Wire Mode	Peer Name FW-MSBG	Shared Secret	
	Edit	Bemove	

Step 12: Create a New Community – Insert Secret

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

General	Shared Secret		
 General Center Gateways Satellite Gateways VPN Properties Tunnel Management Advanced Settings VPN Routing MEP (Multiple Entr, Excluded Services 	Each External member secret with all internal n	ret for all External members will have the following nembers in this community.	
 Shared Secret Advanced VPN Pr 	Peer Name	Shared Secret	
Wire Mode	Fw-MSBG		
	<u>E</u> dit Insert Secret	<u>R</u> emove	I
	Enter secret:	•••••	
	ОК	Cancel	Help



Step 13: Create a New Community – Advance VPN Properties

Fill as below.

General	Advanced VPN Properties
Satellite Gateways	IKE (Phase 1)
VEN Properties Tunnel Management Advanced Settings VEN Bouting	Use Diffie-Hellman group: Group 2 (1024 bit)
- MEP (Multiple Entr	Renegotiate IKE security associations every 🛛 👖 🕺 minutes
 Excluded Services Shared Secret 	Use aggressive mode
Advanced VPN Pr Wire 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
	Reset All VPN Properties
	NAT
	Disable NAT inside the VPN community Advanced

Step 14: Create a New Community – Shared Secret

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

General	Wire Mode
Center Gateways	
Satellite Gateways	Bypass the Firewall
VPN Properties	
Tunnel Management	Allow uninspected encrypted traffic between Wire mode interfaces
Advanced Settings	of this Community's members
VPN Routing	Wire mode routing - Allow members to route upinspected
MEP (Multiple Entr	encrypted traffic in VPN routing configurations
Excluded Services	
- Shared Secret	
Advanced VPN Pr	
Wire Mode	



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).

teway Cluster Properties	i - fw	
General Properties Cluster Members	VPN This module participates in the following VPN Communities:	
E Topology	MSBG_TO_APC	
NAT SmartDefense	Traditional mode IKE properties	1
VPN VPN Advanced	General	
Eink Selection Enk Selection Access Authentication SmartDirectory (LDAP) SmartView Monitor	Support key exchange encryption with: Support data integrity with: MD5 MD5 MD5 MD5 MD5 MD5 MD5 MD5	
Coperative Enforcem Advanced	Support authentication methods: Image: Pre-Shared Secret Edit Secrets Image: Public Key Signatures Specify	
Shar	Exportable for SecuRemote/SecureClient ed Secret Advanced	
	Fw-MSBG xxxx Edit Remove Remove	
	Enter secret Secret Set	
	OK Cancel Help	

Step 16: Interoperable Device – Setup

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

🖃 🚨 Interoperable Devices

Step 17: Interoperable Device – General Properties

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

General Properties Interoperable Device - General Properties	
Topology	
IP Address: @et-address">MSBG WAN Address>@et-address Dynamic Address	ss
Comment:	_
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'.

Interoperable Device - FV	V-MSBG				×
General Properties Topology ⊕ VPN	Topology Get				
	Name	IP Address	Network Mask	IP Addresses behi	
	•			F	
	Add.	Edit	Bemove		
			11200212		
	VPN Domain				·
	C All IP Addresses	s behind Gateway b	ased on Topology inl	formation.	
	Manually define	ed 🕂 MS	BG_Lan_VPN_172.1	7.15 💌 New	

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.

Traditional mode configuration...

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

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

Traditional mode IKE properties	×
General	
Support key exchange encryption v Support key exchange encryption v AES-256 Support AES-256 Support AES-	With: Support data integrity with: MD5
Support authentication methods:	Edit Secrets
Public Key Signatures	Set Matching Criteria in the VPN page
	Advanced
ОК	Cancel Help

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

Click Advanced.

<u>A</u> dvanced	
------------------	--

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

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

Traditional mode advanced IKE properties
Support Diffie-Hellman groups for IKE (phase 1) Security associations
Rekeying Parameters
Renegotiate IKE (phase 1) Security associations every 🛛 🗧 Minutes
Renegotiate IPsec (IKE phase 2) Security associations every 3600 📑 Seconds
🔲 Renegotiate IPsec (IKE phase 2) Security associations every 🛛 50000 📑 KBytes
Misc
Support aggressive mode
OK Cancel Help

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 H MSBG_Lan_VPN_172.17.170.0	₩ MSBG_Lan_VPN_172.17.170.0	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**).

▲				IN/	alcome to MSRG admin LS
					elcome to MISBO admin 3
Home WAN Ac	cess Loc	al Network	Services	~	System
Overview Settings Users Network Connection	s Monitor Routing	Configuration File	Diagnostics	Objects and Rule	5
em					
Network Connections					
7					
Name			Statu	S	Act
🗞 LAN Hardware Ethernet Switch	;	1 Ports Connected			2
🔉 WAN Ethernet		Connected			<u>\</u>
WPN IPSec- APC		Connected			<u>\</u>
💷 VPN IPSec - Emea		Connected			5
💷 VPN IPSec - Allogix		Connected			N N
WPN IPSec- TX		Connected			S S
WPN IPSec - S1		Connected			5
W VPN IPSec - RAI		Connected			~
VPN IPSec Incoming Connection		Waiting for Connect	ion		~
I 2TP Server		Waiting for Incomin	a Connections		~
			9		2
New Connection					

Click the **New Connection** link.

Step 2: Connection Wizard

Next.

_								Welcome to MSBG	admin Site Map
	Home		WAN Acces	s	Local Network	Services		System	
Overview	Settings Us	rs Networ	rk Connections	Monitor Ro	uting Configuration File	Diagnostics	Objects and Ru	les	
		001110		ur networking	needs				



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

ć S AudioC	odes							Voi	ce Home 🐋
							Welc	ome to MSBG admi	n Site Map Logout
	Ho	me	WAN Access	Loca	al Network	Services	s	System	
Overview	Settings	Users	Network Connections	Monitor Routing	Configuration File	Diagnostics	Objects and Rules		
Con	nect to	o a Vi	 Choose your VPN conr VPN Client or Connect to your Virtual Private N VPN Server Enable Virtual P locations. 	e Network nection type: Point-To-Point r business networ Network (VPN) ove Private Network (V	k from home or and sr the Internet. PN) connections to Next	Internet	sing a er		

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

Step 4: VPN Client or Point-To-Point





Step 5: Internet Protocol Security (IPSec)

									Welcome to MSBG admin	n Site Map Logout
	Hor	me	WAN Acces	is	Local	Network	Services		System	
Overview	Settings	Users	letwork Connections	Monitor	Routing	Configuration F	ile Diagnostics	Objects	and Rules	
/stem										
👗 Inte	rnet Pr	otoco	I Security	(IPSe	ec)					
2,*			- Configure your IPSe	ec connect	tion proper	9				
		,							_	
			Host Name or IP Gateway:	Address o	of Destination	<fw ip=""></fw>				
			Remote IP:			Same as Gatev	vay 💙			
			Encapsulation Ty	pe:		Tunnel 🔽				
			Shared Secret:			KEY Secret nan	ne			
		l		_						
				e 🔶 Ba	ck 🛛 🔶	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

							_	Welcome to MSE	Voice r BG admin S	Home Site Map
	Hom	e	WAN Acces	s	Local Network	Services		System		
Overview	Settings	Users	Network Connections	Monitor	Routing Configuration F	le Diagnostics	Objects and	Rules		
	1001101	i Su	You have successful	lly complete	ed the steps needed to cre	ate the following (connection:			
¥		- 3u	You have successful • IPSec connec	lly complete	ed the steps needed to cre .92.168.15.1	ate the following (connection:			
¥			You have successful • IPSec connect Edit the New!	lly complete stion with 1 y Created (ed the steps needed to cre .92.168.15.1 Connection	ate the following o	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.

									Welcome to MS	obo admini
	Ho	me	WAN Acces	is	Local Net	twork	Services		System	
Overview	Settings	Users	Network Connections	Monitor	Routing C	Configuration File	Diagnostics	Objects and	Rules	
VPN	IPSec	Pro	perties							
VPN Settings	IPSec	· Pro	perties							
VPN Settings	IPSec	· Pro	perties							
VPN Settings	IPSec	Pro	perties		ip	ps0				
VPN Settings	IPSec	• Pro	perties		iF	ps0 Vaiting for Conne	ection			
VPN iettings	IPSec	evice Nan tatus:	perties		ir W	ps0 Vaiting for Conne Always 💌	ection			
VPN Settings R	IPSec Routing IPSec Du St Sc Ne	evice Nan tatus: chedule: etwork:	perties		ir W Z	ps0 Vaiting for Conne Always 💌 WAN 💌	ection			

Step 9: Voice Mail Settings

Routing tab. Do not configure this setting.

					10 M	
	Home	WAN Access	Local Network	Services	Syster	m
Overview	Settings Users I	Network Connections Monitor	Routing Configuration File	Diagnostics	Objects and Rules	
A CONT	IDCan Dram	artian				
Z VIEW	IPSec Prop	enties				
al Settings Ro	uting IPSec					
al Settings Ro	uting IPSec					
al Settings Ro	uting IPSec					
al Settings Ro	Uting IPSee		0			
al Settings Ro	Device Metric	1	0			
al Settings Ro	Device Metric	: pute	0			
al Settings Ro	uting IPSec Device Metric Default Ro Multicast -	: sute · IGMP Proxy Default	0			
al Settings Ro	uting IPSec Device Metric Default Rc Multicast -	: oute - IGMP Proxy Default formation Protocol (PTP)	0			



Step 10: TDM BUS Settings

Routing tab.

Overview	Settings	Users	Network Connections	Monitor	Routing	Config	uration Fil	e Di	agnostics	Objects	and Rules
					100000000						
		-									
VPN	PSec	Prop	erties								
Settings Rou	ting IPSec	14									
and a second	ing n boo										
	He	ost Name o	r IP Address of Dest	ination Gat	eway:	25.2.2	.2				
	Er	ncapsulatio	n Type:			Tunne	el 🔽				
	Lo	cal Subnet	:			IP Sub	onet 🖌				
		Local S	ubnet IP Address:			172	. 17	. 170	. 0	1	
		Local S	ubnet Mask:			255	. 255	. 255	.0		
	R	emote Subr	net:			IP Sub	onet 🗸				
		Remote	Subnet IP Address:			192	168	15	0	1	
		Pemote	a Subnet Maski			255	255	255			
		Kennote	Sublict Mask.			200	. 200	. 200			
	Pr	rotect Proto	col:			All	~				
	K	ev Exchand	e Method:			Auton	natic 💌				
		ey enemang	,e meanoar			- turton	intro (mag				

- 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.

ode:	Main Mode 💌	
ife 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 Se	cret 🔽
IPSec Shared Secret:	Secret	
Encryption Algorithm		
DES-CBC		
✓ 3DES-CBC		
AES128-CBC		
AES192-CBC		
AES256-CBC		
AES256-CBC Hash Algorithm		
☐ AES256-CBC Hash Algorithm ✔ Allow Peers to Use MD5		
AES256-CBC Hash Algorithm Allow Peers to Use MD5 Allow Peers to Use SHA1		
AES256-CBC Hash Algorithm Allow Peers to Use MD5 Allow Peers to Use SHA1 Group Description Attribute		
AES256-CBC Hash Algorithm Allow Peers to Use MD5 Allow Peers to Use SHA1 Group Description Attribute DH Group 1		
AES256-CBC Hash Algorithm Allow Peers to Use MD5 Allow Peers to Use SHA1 Group Description Attribute DH Group 1 UH Group 2		

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...)

Life Time in Seconds (1-86400):	3600
Group Description Attribute	
Same group as phase 1	
O DH Group 1	
O DH Group 2	
O DH Group 5	
Encryption Algorithm	
Allow ESP Protocol with DES-CBC	Encryption
Allow ESP Protocol with 3DES-CBC	C 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.

						Welco	me to MSBG admin	Site Ma
6	Home	WAN Access	;	Local Network	Services	5)	ystem	
Overview	Settings Users	Network Connections	Monitor	Routing Configuration File	 Diagnostics 	Objects and Rules		
Netw	vork Conne	ections						
Netw	vork Conne	Rame			St	atus	Act	ction
	vork Conne	Name		1 Ports C	St Connected	atus	Act	ction
	vork Conne	Name ch		1 Ports O	St Connected ed	atus	Act	ction
	vork Conne ardware Ethernet Switz thernet Sec - Name	Name ch		1 Ports C Connect Waiting f	St Connected ed for Connection	atus	Act	ction

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

Home	WAN Access	Local Network	Services	System
Overview Settings Users	Network Connections Monitor	Routing Configuratio	n File Diagnostics	Objects and Rules
or				
Notwork Compos	tions			Network
Network Connec	ctions			
Name	LAN Hardware Eth	ernet 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 Etherne	t 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	i	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		11.1.1.10	
	10.1.1.10			
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		/4	
Received Bytes	114524822		705037	
Sent Bytes	51884593		14268	
Receive Errors	U		U	
Receive Drops	U		U	
lime Span	1/3:04:30		173:04:30	



CPU: displays online CPU status.

6	112-22-2				Considered (Durate m	admin Site map Logi
	Home	WAN	ACCESS	Local Network	Services	system	
Overview	Settings Us	ers Network Connecti	ons Monitor	Routing Configuration File	Diagnostics Objects a	nd Rules	
		System Has Been U Load Average (1 / S	p For: /15 mins.):	7 days, 5 hours 0.00 / 0.00 / 0.0	0		
		Processes		nongo astrono contrato de transmitati			
		Process	То	al Virtual Memory (VmData)	Heap size (VmSize	:)	
		init	2072 kB		2660 kB		
		SIL	1000 KD		1/90 KD		
		wda	7220 LB		2040 KD		
		wdg	7220 kB 12368 kF		19996 kB		
		wdg openrg I2tod	7220 kB 12368 kB 3096 kB		19996 kB 3684 kB		
		wdg openrg l2tpd pluto	7220 kB 12368 kE 3096 kB 4208 kB		19996 kB 3684 kB 5360 kB		
		wdg openrg l2tpd pluto portmap	7220 kB 12368 kE 3096 kB 4208 kB 1068 kB		19996 kB 3684 kB 5360 kB 1564 kB		
		wdg openrg I2tpd pluto portmap _pluto_adns	7220 kB 12368 kE 3096 kB 4208 kB 1068 kB 4104 kB		19996 kB 3684 kB 5360 kB 1564 kB 4852 kB		

Log: displays online Syslog.

							Welc	come to MSBG	Voice Ho
Hom	•	WAN Acces	55	Local Network	Services	(:	System	
verview Settings	Users Netwo	rk Connections	Monitor	Routing Configuration	on File Diagnostics	Objects	and Rules		
	2	4	Close Press the	Clear Log Download	Log 🔗 Refresh				
ilters Component All New Filter	Information	Severity		Action					
ilters Component All New Filter Time ▼	Information Apply Filters Component	Severity Reset Filters Severity		Action	Details				
iiters Component All New Filter Time ▼ Jan 8 04:08:14 2003	Information Apply Filters Component I PSec	Severity Reset Filters Severity Warning	pluto[44]	Action	Details er of retransmissions	(2) reach	ed STATE,	_MAIN_11. P	No
ilters Component All New Filter Time ▼ Jan 8 04:08:14 2003 Jan 8 04:08:14 2003	Information Apply Filters Component IPSec	Severity Reset Filters Severity Warning Information	pluto[44] acceptab	Action	Details er of retransmissions IKE message less of tyne IPSen IKE	(2) reach	ed STATE	_MAIN_I1. F	No
itters Component All New Filter Time ▼ Jan 8 04:08:14 2003 Jan 8 04:08:14 2003 Jan 8 04:08:14 2003 Jan 8 04:07:04 2003	Apply Filters Component I IPSec I IPSec I IPSec	Severity Reset Filters Severity Warning Information Warning	pluto[44] acceptab pluto[44] pluto[44]	Action Action Prips0" #6: max numble response to our first RATELIMIT: 2 messat I: "lps0" #5: max numble le response to our first	Details er of retransmissions IKE message jes of type IPSec IKE er of retransmissions IKE message	(2) reach packet re (2) reach	ed STATE ported 70 ed STATE	_MAIN_I1. P) second(s) a _MAIN_I1. P	No ago No
iiters Component All New Filter Jan 8 04:08:14 2003 Jan 8 04:08:14 2003 Jan 8 04:07:04 2003 Jan 8 04:07:04 2003	Information Apply Filters Component I PSec I PSec I PSec I PSec	Severity Reset Filters Severity Warning Information Warning Information	pluto[44] acceptab pluto[44] acceptab pluto[44] acceptab	Action Action Prips0" #6: max numble le response to our first : RATELIMIT: 2 messa : "pip0" #5: max numble le response to our first : RATELIMIT: 2 messa;	Details er of retransmissions IKE message les of type IPSec IKE er of retransmissions IKE message les of type IPSec IKE	(2) reach packet re (2) reach packet re	ed STATE ported 70 ed STATE ported 70	_MAIN_II. P J second(s) (_MAIN_II. P J second(s) (No ago No ago
Time マ Jan 8 04:08:14 2003 Jan 8 04:08:14 2003 Jan 8 04:08:14 2003 Jan 8 04:07:04 2003 Jan 8 04:07:04 2003 Jan 8 04:07:04 2003 Jan 8 04:05:54 2003	Apply Filters Component I IPSec I IPSec I IPSec I IPSec I IPSec I IPSec	Severity Reset Filters Severity Warning Information Warning Information Warning	pluto[44] acceptab pluto[44] pluto[44] pluto[44] pluto[44] acceptab	Action Action	Details er of retransmissions IKE message jes of type IPSec IKE er of retransmissions IKE message jes of type IPSec IKE er of retransmissions IKE message	(2) reach packet re (2) reach packet re (2) reach	ed STATE, ported 70 ed STATE ported 70 ed STATE	_MAIN_I1. ft 0 second(s) & _MAIN_I1. ft 0 second(s) & _MAIN_I1. ft	No ago No ago No

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).

										Welcome to MS	SBG admin Site Map Logout
		Но	me	WAN Acc	ess	Local	Network	Services		System	
	Overview	Settings	Users	Network Connections	Monitor	Routing	Configuration F	ile Diagnostics	Objects and	Rules	
Setting	s Syst	tem Se	tting	s							Overview Date and Time
			Syste	em Logging							
			Sy Re	stem Log Buffer Siz mote System Notify Persistent System	e: Level: Log		16 KB				
			Re	mote System Host I	P Address:		10 .1	.1			
			Secu	rity Logging							
			Se Re	curity Log Buffer Siz mote Security Notify	e: Level:		16 KB	. ← 8	Step 3		
			Re	mote Security Host	Log P Address	:	10 .1	.1 .1		=Step 4	
			Outg	oing Mail Server							
			Se Fro	rver: om Email Address:							
			Po	rt:] Server Requires Ar	Ithenticatio	n	25				
					 ✓ 	ок	Apply	Cancel			



Multi-Service Business Gateway (MSBG)

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





www.audiocodes.com