

Avaya Solution & Interoperability Test Lab

# Application Notes for Configuring Borderware SIPassure with Avaya SIP Enablement Services and Avaya Communication Manager to Support Remote Users - Issue 1.0

#### Abstract

These Application Notes describe the procedures for configuring Borderware SIPassure with Avaya SIP Enablement Services and Avaya Communication Manager.

Borderware SIPassure is a SIP security gateway that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network secured by SIPassure.

Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the procedure for configuring Borderware SIPassure with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

Borderware SIPassure is a SIP security gateway that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network secured by SIPassure.

#### 1.1. Configuration

**Figure 1** illustrates the test configuration. The test configuration shows two sites connected by an untrusted IP network. The main office has a SIPassure at the edge of the network and the branch office does not. The remote SIP endpoints will direct SIP and RTP traffic to the public IP address of SIPassure. SIPassure in return will direct SIP and RTP traffic on behalf of these endpoints to Avaya SES. SIPassure uses its private LAN IP address to communicate with Avaya SES. In this manner, SIPassure can protect the main site infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams.

Located at the main office is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Endpoints include two Avaya 4600 Series IP Telephones (with SIP firmware), an Avaya 4600 Series IP Telephone (with H.323 firmware), an Avaya 6408D+ Digital Telephone, and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. One PSTN number assigned to the ISDN-PRI trunk at the main office is mapped to a telephone extension at the main office. The other is mapped to a telephone extension at the branch office.

The Avaya 4600 Series IP Telephone is registered to Avaya Communication Manager and the Avaya 4600 Series SIP Telephones are registered directly to Avaya SES. All calls originating from Avaya Communication Manager at the main office and destined for the branch office will be routed through the on-site Avaya SES, SIPassure and across the untrusted IP network.

Located at the branch office are two Avaya 4600 Series SIP Telephones. These telephones register with Avaya SES through SIPassure. These telephones use the public IP address of SIPassure at the main office as their configured server. SIPassure will forward any registration messages it receives from the remote endpoints to Avaya SES. All calls originating from the branch office are routed across the untrusted IP network, through SIPassure and Avaya SES to Avaya Communication Manager at the main office.

All SIP telephones at both sites use the TFTP server at the main site to obtain their configuration files. All non-SIP traffic (including these TFTP transfers) bypasses SIPassure and flows through a parallel connection through the untrusted network which would be protected by a traditional data firewall.

For interoperability, direct IP to IP media (also known as media shuffling) must be disabled on the SIP trunk in Avaya Communication Manager (see **Section 3, Step 6**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.



**Figure 1: SIPassure Test Configuration** 

# 2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya S8300 Server with Avaya G700 Media	Avaya Communication Manager 4.0
Gateway	Service Pack (R014x.00.0.730.5-13566)
Avaya IA 770 Intuity Audix	
Avaya SIP Enablement Services	3.1.2
Avaya 4602SW IP Telephone	SIP version 2.2.2
Avaya 4610SW IP Telephone	
Avaya 4620SW IP Telephones	
Avaya 4625SW IP Telephone	H.323 version 2.7
Avaya 6408D+ Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (Management PC and TFTP Server)	Windows XP Professional
Borderware SIPassure	3.0.1 (Build 3.0.7) with Update 1

# 3. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration to support SIP. It is typically comprised of two parts. The first part is the configuration of the SIP connection to Avaya SES required of any Avaya SES installation. The second part describes the configuration of Off-PBX stations (OPS) for each SIP endpoint. The configuration of the OPS stations is not directly related to the interoperability of SIPassure, so it is not included here. The procedure for configuring OPS stations can be found in [4].

The following configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration in this section, perform a **save translation** command to make the changes permanent.

Step	Description				
1.	Use the <b>display system-parameters customer-options</b> command to verify that sufficient SIP trunk capacity exists. On <b>Page 2</b> , verify that the number of SIP trunk supported by the system is sufficient for the number of SIP trunks needed. Each Si call between two SIP endpoints (whether internal or external) requires two SIP trun for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone v only use one trunk.				
	feature is not enabled or there is insufficient capacity, contact sales representative to make the appropriate changes.	an authorized Avaya			
	display system-parameters customer-options OPTIONAL FEATURES	Page 2 of 10			
	IP PORT CAPACITIES Maximum Administered H.323 Trunks: 100 Maximum Concurrently Registered IP Stations: 100 Maximum Administered Remote Office Trunks: 0 Maximum Concurrently Registered IP eCons: 0 Maximum Concurrently Registered IP eCons: 0 Max Concur Registered Unauthenticated H.323 Stations: 0 Maximum Video Capable H.323 Stations: 0 Maximum Video Capable IP Softphones: 0 Maximum Number of DS1 Boards with Echo Cancellation: 0 Maximum TN2501 VAL Boards: 0 Maximum TN2602 Boards with 30 VoIP Channels: 0 Maximum TN2602 Boards with 320 VoIP Channels: 0 Maximum Number of Expanded Meet-me Conference Ports: 0 (NOTE: You must logoff & login to effect the permissi	USED 32 0 0 0 0 0 0 44 0 0 0 0 0 0 0 0 0 0 0 0			
2.	In order to support SIP the following features must be enabled <b>system-parameters customer-options</b> command to verify the have been set to <i>y</i> .	l. Use the <b>display</b> at the following fields			
	If a required feature is not enabled, contact an authorized Ava make the appropriate changes.	ya sales representative to			

tep		Description				
3.	Use the change	node-names ip command to assign	the node nam	e and	l IP ado	dress for
	Avaya SES. In this case, <i>SES</i> and <i>10.75.5.6</i> are being used, respectively. The node name <i>SES</i> will be used throughout the other configuration forms of Avaya					
	Communication Manager In this example <i>procr</i> and 10 75 5.2 are the name and IP					and IP
	addrass assigned to the Aveve \$2200 Server					
	address assigne	d to the Avava \$8300 Server				
	address assigne	d to the Avaya \$8300 Server.				
	address assigne	d to the Avaya S8300 Server.				_
	address assigne	d to the Avaya S8300 Server.		Page	1 of	2
	address assigne	d to the Avaya S8300 Server.		Page	l of	2
	change node-na	d to the Avaya S8300 Server. mes ip IP Address		Page	l of	2
	change node-na	d to the Avaya S8300 Server. mes ip IP NODE NAMES IP Address 10.75.5.6		Page	l of	2
	change node-na Name SES default	d to the Avaya S8300 Server. mes ip IP Address 10.75.5.6 0.0.0.0		Page	1 of	2
	change node-na Name SES default myaudix	d to the Avaya S8300 Server. mes ip IP Address 10.75.5.6 0.0.0.0 10.75.5.7		Page	1 of	2

Description
Use the <b>change ip-network-region</b> <i>n</i> command, where <i>n</i> is the number of the region to be changed, to define the connectivity settings for all VoIP resources and IP endpoints within the region. Select an IP network region that will contain the Avaya SES server. The association between this IP network region and the Avaya SES server will be done on the <b>Signaling Group</b> form as shown in <b>Step 6</b> . In the case of the compliance test, the same IP network region that contains the Avaya S8300 Server and Avaya IP Telephones was selected to contain the Avaya SES server. By default, the Avaya S8300 Server and IP telephones are in IP network region 1.
<ul> <li>On the IP Network Region form:</li> <li>The Authoritative Domain field is configured to match the domain name configured on Avaya SES. In this configuration, the domain name is <i>business.com</i>. This name will appear in the "From" header of SIP messages originating from this IP region.</li> <li>Enter a descriptive name for the Name field.</li> <li>By default, IP-IP Direct Audio (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G700 Media Gateway. This is true for both intra-region and inter-region IP-IP Direct Audio. Shuffling can be further restricted at the trunk level on the Signaling Group form.</li> <li>The Codec Set is set to the number of the IP codec set to be used for calls within this IP network region. If different IP network regions are used for the Avaya S8300 Server and the Avaya SES server, then Page 3 of each IP Network Region form must be used to specify the codec set for inter-region communications.</li> <li>The default values can be used for all other fields.</li> </ul>
change ip-network-region 1       Page 1 of 19         IP NETWORK REGION         Region: 1         Location:         Authoritative Domain: business.com         Name: default         MEDIA PARAMETERS       Intra-region IP-IP Direct Audio: yes         Codec Set: 1         Intra-region IP-IP Direct Audio: yes         UDP Port Min: 2048         UDP Port Max: 3329         DIFFSERV/TOS PARAMETERS         RTCP Reporting Enabled? y         Call Control PHB Value: 46         Audio Hairpinning? n         UDP Port Max: 3329         DIFFSERV/TOS PARAMETERS         Audio Hairpinning? n         UDP Port Max: 3329         DIFFSERV/TOS PARAMETERS         Audio Hairpinning? n         UDP Port Max: 3329         DIFFSERV/TOS PARAMETERS         Audio PHB Value: 46         USE Default Server Parameters? y         Video PHB Value: 26         802.1P/Q PARAMETERS         Call Control 802.1p Priority: 6         Audio 802.1p Priority: 5 <t< th=""></t<>

Step			D	escription				
5.	Use the <b>change ip-codec-set</b> $n$ command, where $n$ is the codec set value specified in <b>Step 4</b> , to enter the supported audio codecs. Multiple codecs can be listed in priority order to allow the codec to be negotiated during call establishment. The list should include the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test.							
	change ip-codeo	c-set l IP	Codec Set	:	Pa	ge lof	2	
	Codec Set: Audio Codec 1: G.711MU 2: G.729AB 3:	1 Silence Suppression n n	Frames Per Pkt 2 2	Packet Size(ms) 20 20				

Step	Description
6.	Use the <b>add signaling-group</b> <i>n</i> command, where <i>n</i> is the number of an unused
	signaling group, to create the SIP signaling group as follows:
	<ul> <li>Set the Group Type field to <i>sip</i>.</li> </ul>
	<ul> <li>The Transport Method field will default to <i>tls</i> (Transport Layer Security).</li> </ul>
	TLS is the only link protocol that is supported for communication between
	Avaya SES and Avaya Communication Manager.
	• Specify the Avaya S8300 Server (node name <i>procr</i> ) and the Avaya SES server
	(node name SES) as the two ends of the signaling group in the Near-end Node
	Name and the Far-end Node Name fields, respectively. These field values are
	taken from the <b>IP Node Names</b> form shown in <b>Step 3</b> . For alternative
	configurations that use a C-LAN board, the near (local) end of the SIP signaling
	group will be the C-LAN board instead of the Avaya \$8300 Server.
	<ul> <li>Ensure that the TLS port value of 5001 is configured in the Near-end Listen</li> <li>Port and the Far and Listen Port fields</li> </ul>
	I use for any use for the Listen for the list of the l
	- In the <b>Fai-chu Network Region</b> field, enter the If network region value assigned in the <b>IP Network Region</b> form in <b>Sten 4</b> . This defines which IP
	network region contains the Avava SFS server. If the <b>Far-end Network</b>
	<b>Region</b> field is different from the near-end network region, the preferred codec
	will be selected from the IP codec set assigned for the inter-region connectivity
	for the pair of network regions.
	<ul> <li>Enter the domain name of Avava SES in the Far-end Domain field. In this</li> </ul>
	configuration, the domain name is <i>business.com</i> . This domain is specified in
	the Uniform Resource Identifier (URI) of the SIP "To" header in the INVITE
	message.
	• The <b>Direct IP-IP Audio Connections</b> field is set to <i>n</i> . For interoperability,
	this field (also know as media shuffling) must be disabled for the SIP trunk.
	• The <b>DTMF over IP</b> field must be set to the default value of <i>rtp-payload</i> for a
	SIP trunk. This value enables Avaya Communication Manager to send DTMF
	transmissions using RFC 2833.
	The default values for the other fields may be used.
	add signaling-group 1 Page 1 of 1 SIGNALING GROUP
	Group Number: 1 Group Type: gip
	Transport Method: tls
	Near-and Node Names program Far-and Node Names SES
	Near-end Listen Port: 5061 Far-end Listen Port: 5061
	Far-end Network Region: 1 Far-end Domain: business.com
	Dimond If ID Threshold Europeded
	Bypass II IP Inreshotd Exceeded? n
	DTMF over IP: rtp-payload Direct IP-IP Audio Connections? n
	Enable Layer 3 Test? n
	Session Establishment Timer(min): 120

Step	Description
7.	Add a SIP trunk group by using the <b>add trunk-group</b> $n$ command, where $n$ is the
	number of an unused trunk group. For the compliance test, trunk group number 1 was
	chosen.
	On <b>Page 1</b> , set the fields to the following values:
	• Set the <b>Group Type</b> field to <i>sip</i> .
	• Choose a descriptive Group Name.
	• Specify an available trunk access code (TAC) that is consistent with the
	existing dial plan.
	<ul> <li>Set the Service 1 ype field to <i>ne</i>.</li> <li>Specify the signaling group associated with this trunk group in the Signaling</li> </ul>
	• Specify the signaling group associated with this trunk group in the Signaling
	Specify the Number of Members supported by this SIP trunk group As
	mentioned earlier, each SIP call between two SIP endpoints (whether internal
	or external) requires two SIP trunks for the duration of the call. Thus, a call
	from a SIP telephone to another SIP telephone will use two SIP trunks. A call
	between a non-SIP telephone and a SIP telephone will only use one trunk.
	<ul> <li>The default values may be retained for the other fields.</li> </ul>
	add trunk-group 1 Page 1 of 21
	TRUNK GROUP
	Group Number: 1 Group Type: sip CDR Reports: y
	Group Name: SES Trk Grp COR: 1 TN: 1 TAC: 101 Direction: two-way Outgoing Display? n
	Dial Access? n Night Service:
	Queue Length: 0 Service Type: tie Auth Code? n
	Signaling Groups 1
	Number of Members: 24
8.	On Page 3:
	<ul> <li>Verify the Numbering Format field is set to <i>public</i>. This field specifies the</li> </ul>
	format of the calling party number sent to the far-end.
	<ul> <li>The default values may be retained for the other fields.</li> </ul>
	add trunk-group 1 Page 3 of 21
	ACA Assignment? n Measured: none
	Maintenance Tests? y
	Numbering Format: public
	UUI Treatment: service-provider
	Replace Unavailable Numbers? h
	Show ANSWERED BY on Display? y

Step	Description
9.	Use the <b>change public-unknown-numbering 0</b> command to define the full calling
	party number to be sent to the far-end. Add an entry for the trunk group defined in
	<b>Step 7</b> . In the example shown below, all calls originating from a 5-digit extension
	beginning with 3 and routed across trunk group 1 will be sent as a 5 digit calling
	number. This colling nexts number will be cent to the for and in the SID "From"
	number. This canning party number will be sent to the far-end in the SIP From
	header.
	change public-unknown-numbering 0 Page 1 of 2
	NUMBERING - PUBLIC/UNKNOWN FORMAT
	Ext Ext Trk CPN CPN
	Len Code Grp(s) Prefix Len
	Total Administered: 4
	5 3 99 5 Maximum Entries. 240
10.	Create a route pattern that will use the SIP trunk that connects to Avava SES. This
	route pattern will be used as a default route for SIP calls in <b>Step 11</b> . Some transfer
	scanarios using alpha numeric handles (i.e. user names) instead of extensions require a
	scenarios using alpha-numeric nancies (i.e., user names) instead of extensions require a
	default route pattern. These call scenarios were not tested as part of the compliance
	test, however, the creation of this default route pattern is included here for
	completeness
	completeness.
	completeness.
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b>
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Crn Na</b> field to the trunk group number grouted for the SID trunk. Set
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for
	To create a route pattern, use the <b>change route-pattern</b> $n$ command, where $n$ is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of $\theta$ is the least restrictive level. The default values
	To create a route pattern, use the <b>change route-pattern</b> $n$ command, where $n$ is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of $0$ is the least restrictive level. The default values may be retained for all other fields.
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of $\theta$ is the least restrictive level. The default values may be retained for all other fields. Change route-pattern 1 Page 1 of 3
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of $\theta$ is the least restrictive level. The default values may be retained for all other fields. Change route-pattern 1 Page 1 of 3 Pattern Name: SIP
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of $\theta$ is the least restrictive level. The default values may be retained for all other fields. Change route-pattern 1 Page 1 of 3 Pattern Number: 3 Pattern Name: SIP SCCAN? n Secure SIP? n GCS/ IXC
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.              change route-pattern 1
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.              (change route-pattern 1
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of $\theta$ is the least restrictive level. The default values may be retained for all other fields. Change route-pattern 1 Pattern Number: 3 Pattern Name: SIP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw I: 1 0 n user n user 1: 1 0 n u
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields. <b>change route-pattern 1 Page 1 of 3 Pattern Number: 3 Pattern Name: SIP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits Opts Intw i: 1 0 n user n user n user n user n user f: 1 0 f: 1 0</b>
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields. $ \frac{change route-pattern 1}{Pattern Number: 3 Pattern Name: SIP} Page 1 of 3 Pattern Number: 3 Pattern Name: SIP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted Dgts I: 1 0 Dgts I: 1 0 Dgts Dgts Dgts Dgts Dgts Dgts Dgts Dgts$
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.           change route-pattern 1       Page 1 of 3         Pattern Number: 3       Pattern Name: SIP         SCCAN? n       Secure SIP? n         Grp FRL NPA Pfx Hop Toll No. Inserted       DCS/ IXC         No       Mrk Lmt List Del Digits       QSIG         Dgts       Intw         1: 1       0       n user         3:       n user       n user         4:       n user       n user         0 1 2 3 4 W       Request       DGLE Service/Feature PARM No. Numbering LAR
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.           change route-pattern 1       Page 1 of 3         Pattern Number: 3       Pattern Name: SIP         SCCANF n       Secure SIP? n         Grp FRL NPA Pfx Hop Toll No. Inserted       DCS/ IXC         No       Mrk Lmt List Del Digits       QSIG         Dgts       Intw         1: 1       0       n user         3:       n user       n user         6:       n user       n user         0 1 2 3 4 W       Request       Dgts       none         1: yyyyyn n       rest       none       yrest
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.           change route-pattern 1       Page 1 of 3         Pattern Number: 3       Pattern Name: SIP         SCCAN? n       Secure SIP? n         Grp FRL NPA Pfx Hop Toll No. Inserted       DCS/ IXC         No       Mrk Lmt List Del Digits       QSIG         Dgts       Intw       n         1: 1       0       n       user         6:       n       user       n         1: 1       0       12 3 4 W       Request       Dgts         1: Y Y Y Y Y n n       rest       none       none         2: Y Y Y Y Y n n       rest       none       none         3: Y Y Y Y Y n n       rest       none       none
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.           change route-pattern 1       Page 1 of 3         Pattern Number: 3       Pattern Name: SIP         SCCAN? n       Secure SIP? n         Grp FRL NPA Pfx Hop Toll No. Inserted       DCS/ IXC         No       Mrk Lmt List Del Digits       QSIG         Dgts       Intw         1: 1       0       n       user         6:       n       user         0 1 2 3 4 W       Request       TC BCIE Service/Feature PARM No. Numbering LAR         0 1 2 3 4 W       Request       none         1: yyyyyn n       rest       none         2: yyyyyn n       n       rest       none         3: yyyyyn n       rest       none       none
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields. <b>change route-pattern 1 Page 1 of 3 Pattern Number: 3 Pattern Name: SIP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted No Mrk Lmt List Del Digits Dgts Intw i: 1 0 i: 1 0 ii: 1: 1: 1: 1: 1: 1: 1: 1: 1: 1: 1: 1: 1:</b>
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.           change route-pattern 1       Page 1 of 3         Pattern Number: 3       Pattern Name: SIP         SCCAN? n       Secure SIP? n         Grp FRL NPA Pfx Hop Toll No. Inserted       DCS/ IXC         No       Mrk Lmt List Del Digits       QSIG         0 1 2 3 4 W       Request       ITC BCIE Service/Feature PARM No. Numbering LAR         0 1 2 3 4 W       Request       n user         1: yy y yy n n       rest       none         3: yy y yy n n       rest       none         4: yy y yy n n       rest       none         5: yy y yy n n       rest       none         6: yy y yy n n       rest       none
	To create a route pattern, use the <b>change route-pattern</b> <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level ( <b>FRL</b> ) field to a level that allows access to this trunk for all users that require it. The value of <i>0</i> is the least restrictive level. The default values may be retained for all other fields.           change route-pattern 1       Page 1 of 3         Pattern Number: 3       Pattern Name: SIP         SCCAN? n       Secure SIP? n         Grp FRL NPA Pfx Hop Toll No. Inserted       QSIG         No       Mrk Lmt List Del Digits       QSIG         1: 1       0       n       user         3:       1       n       user         6:       n       user       n         1: y y y y y n n       rest       none         3: y y y y n n       rest       none         4: y y y y y n n       rest       none         5: y y y y y n n       rest       none         6: y y y y y n n       rest       none         6: y y y y y n n       rest       none

Step	Description				
11.	Use the <b>change locations</b> command to assign the default SIP route pattern to the location. All IP endpoints, both local and remote, are part of a single logical location in Avaya Communication Manager with the default name of <i>Main</i> and shown in the example below. Enter the route pattern number from the previous step in the <b>Proxy</b> Sel Rte Pat field. The default values may be retained for all other fields.				
	change locations Page 1 of 4 LOCATIONS				
	ARS Prefix 1 Required For 10-Digit NAMP Calls? yLoc NameTimezone Rule NPA ARS AtdDisp PrefixProxy SelNoOffsetFAC FACParmRte Pat1: Main+ 00:000112:::3::				
12.	Automatic Route Selection (ARS) is used to route calls to the PSTN. In the compliance test, PSTN numbers that begin with 1732 were used for testing.Use the change ars analysis n command to add an entry in the ARS Digit Analysis Table for the dialed string beginning with n. In the example shown, PSTN numbers that begin with 1732 and 11 digits long use route pattern 2. Route pattern 2 routes calls 				
	176     11     11     deny     fnpa     n       177     11     11     deny     fnpa     n				
13.	To map a PSTN number to a station at the main or branch office, use the <b>change inc- call-handling-trmt trunk-group</b> <i>n</i> command, where <i>n</i> is the trunk group number connected to the PSTN from the Avaya G700 Media Gateway. The compliance test used trunk group 2 to connect to the PSTN. This trunk group configuration is not shown in these Application Notes. The example below shows two incoming 11-digit numbers being deleted and replaced with the extension number of the desired station.				
	tie 11 17325551235 11 30101				

# 4. Configure Avaya SES

This section covers the configuration of Avaya SES. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that the Avaya SES software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the **Setup** screens of the administration web interface have been used to initially configure Avaya SES. For additional information on these installation tasks, refer to [5].

Each SIP endpoint used in the compliance test, requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of SIPassure so it is not included here. These procedures are covered in [5].

SIPassure registers to Avaya SES on behalf of each of the remote users by serving as a proxy of the registration request from the remote endpoint to Avaya SES. Thus, SIPassure appears as a set of endpoints to Avaya SES. As a result, no outbound proxy settings, address maps or trusted host settings are required on Avaya SES to route calls to or to support the remote users.

<u>)</u>			Description	
	Access the Avaya http:// <ip-addr>/a address of the Ava</ip-addr>	SES administration <u>dmin</u> as the URL in tya SES server.	on web interface by enter in an Internet browser, w	ing here <i><ip-addr></ip-addr></i> is the I
	Log in with the ap Web Interface lin	propriate credentian k from the main p	als and then select the La bage as shown below.	aunch Administration
	and the second second second second second second		Standar	d Manadament Solutions
	Help Log Off		otundu	a Management Solutions
	Help Log Off	Administration	The Administration Web Interface allows you to administer this SES Server.	Launch Administration Web Interface

		Integrated Managemen
Heln Exit		SIP Server Managemen
Theip Late		
Top ■ Users	🚪 Тор	
Conferences Media Server Extensions	Manage Users	Add and delete Users.
Emergency Contacts	Manage Conferencing	Add and delete Conference Extensions.
<ul> <li>Husts</li> <li>Media Servers</li> </ul>	Manage Media Server Extensions	Add and delete Media Server Extensions.
Services	Manage Emergency Contacts	Add and delete Emergency Contacts.
<ul> <li>Server Configuration</li> <li>Certificate Management</li> </ul>	Manage Hosts	Add and delete Hosts.
IM Logs	Manage Media Servers	Add and delete Media Servers.
<ul> <li>Trace Logger</li> <li>Export/Import to ProVision</li> </ul>	Manage Adjunct Systems	Add and delete Adjunct Systems.
	Manage Services	Start and stop server processes on this host.
nges using the <b>Update</b> link by clicking on the <b>Update</b> left side of any of the Avaya	vaya SES, it is n that appears whe link found in the a SES administra	ecessary to commit the da on changes are pending. Pe bottom of the blue naviga ation pages as shown below
by clicking on the <b>Update</b> link by clicking on the <b>Update</b> left side of any of the Avaya commended that this be done	vaya SES, it is n that appears whe link found in the a SES administra after making any	ecessary to commit the da on changes are pending. Pe bottom of the blue naviga- ation pages as shown below y changes.
nges using the <b>Update</b> link by clicking on the <b>Update</b> left side of any of the Avays commended that this be done	vaya SES, it is n that appears whe link found in the a SES administra after making any	ecessary to commit the da on changes are pending. Po e bottom of the blue naviga ation pages as shown below y changes. Integrated Managemen SIP Server Managemen
nges using the <b>Update</b> link by clicking on the <b>Update</b> left side of any of the Avaya ommended that this be done	vaya SES, it is n that appears whe link found in the a SES administra after making any	ecessary to commit the da on changes are pending. Pe bottom of the blue naviga- ation pages as shown below y changes. Integrated Managemen SIP Server Managemen Server: 10.75.5
nges using the <b>Update</b> link o by clicking on the <b>Update</b> left side of any of the Avay ommended that this be done Help Exit Top Users Conferences Media Server Extensions	vaya SES, it is n that appears whe link found in the a SES administra after making any <b>Top</b> Manage Users	ecessary to commit the da en changes are pending. Pe bottom of the blue naviga ation pages as shown below y changes. Integrated Managemen SIP Server Managemen Server: 10.75.5
Avaya nges using the Update link by clicking on the Update left side of any of the Avaya ommended that this be done Avaya Help Exit Top " Users " Conferences " Media Server Extensions Emergency Contacts " Heat	vaya SES, it is n that appears whe link found in the a SES administra after making any <b>Top</b> Manage Users Manage Conferencing	ecessary to commit the da en changes are pending. Pe e bottom of the blue naviga ation pages as shown below y changes. Integrated Managemen SIP Server Managemen SIP Server Managemen Server: 10.75.5 Add and delete Users. Add and delete Conference Extensions.
Avaya nges using the Update link by clicking on the Update left side of any of the Avaya ommended that this be done Avaya mended that this be done Avaya Help Exit Top <sup>a</sup> Users <sup>a</sup> Conferences <sup>b</sup> Media Server Extensions Emergency Contacts <sup>a</sup> Media Servers <sup>a</sup> Media Servers	vaya SES, it is n that appears whe link found in the a SES administra after making any <b>Top</b> Manage Users Manage Conferencing Manage Media Server Extensions	ecessary to commit the da en changes are pending. Pe e bottom of the blue naviga- ation pages as shown below y changes. Integrated Managemen SIP Server Managemen SIP Server Managemen Server: 10.75.5 Add and delete Users. Add and delete Conference Extensions. Add and delete Media Server Extensions.
Available Servers Media Servers Media Servers Adjunct Systems Services	vaya SES, it is n that appears whe link found in the a SES administra after making any Top Manage Users Manage Conferencing Manage Media Server Extensions Manage Emergency Contacts	ecessary to commit the da en changes are pending. Pe e bottom of the blue naviga- ation pages as shown below y changes. Integrated Managemen SIP Server Managemen SIP Server Managemen Server: 10.75.5 Add and delete Users. Add and delete Conference Extensions. Add and delete Media Server Extensions. Add and delete Emergency Contacts.
Help Exit Top Conferences Media Servers Media Servers Adjunct Systems Services Server Configuration Configuration Configuration Configuration Configuration	vaya SES, it is n that appears whe link found in the a SES administra after making any <b>Top</b> Manage Users Manage Conferencing Manage Media Server Extensions Manage Emergency Contacts Manage Hosts	ecessary to commit the da en changes are pending. Pe bottom of the blue naviga- ation pages as shown below y changes. Integrated Managemen SIP Server Managemen Server: 10.75.5 Add and delete Users. Add and delete Conference Extensions. Add and delete Media Server Extensions. Add and delete Emergency Contacts. Add and delete Hosts.
Haking changes within A ages using the <b>Update</b> link by clicking on the <b>Update</b> eft side of any of the Avay mmended that this be done Available Help Exit Top Users Conferences Media Server Extensions Emergency Contacts Media Servers Adjunct Systems Services Server Configuration Certificate Management IM Logs	vaya SES, it is n that appears whe link found in the a SES administra after making any <b>Top</b> Manage Users Manage Conferencing Manage Media Server Extensions Manage Emergency Contacts Manage Media Servers	ecessary to commit the da en changes are pending. Pe e bottom of the blue naviga ation pages as shown below y changes. Integrated Managemen SIP Server Managemen SIP Server Managemen Server: 10.75.5 Add and delete Users. Add and delete Conference Extensions. Add and delete Media Server Extensions. Add and delete Emergency Contacts. Add and delete Hosts. Add and delete Media Servers.
References Media Servers Media Server Media Server M	vaya SES, it is n that appears whe link found in the a SES administra after making any Top Manage Users Manage Conferencing Manage Media Server Extensions Manage Hosts Manage Hosts Manage Media Servers Manage Adjunct Systems	ecessary to commit the da en changes are pending. Pe bottom of the blue naviga- ation pages as shown below y changes. Integrated Managemen SIP Server Managemen Server: 10.75.5 Add and delete Users. Add and delete Users. Add and delete Conference Extensions. Add and delete Media Server Extensions. Add and delete Emergency Contacts. Add and delete Hosts. Add and delete Media Servers. Add and delete Media Servers. Add and delete Media Servers. Add and delete Media Servers.

Step	Description				
4.	As part of the Avaya SES installation and initial configuration procedures, the				
	following parameters were defined. Although these procedures are out of the scope of				
	these Application Notes, the values used in the compliance test are shown below for				
	reference. After each parameter is a brief description of how to view the value from				
	the Avaya SES administration home page shown in the previous step.				
	• SIP Domain: <i>business.com</i>				
	(To view, navigate to <b>Server Configuration→System Parameters</b> )				
	• Host (SES IP address): 10.75.5.6				
	(To view, navigate to <b>Host→List</b> ; Click <b>Edit</b> )				
	Media Server (Avaya Communication Manager) Interface Name: <i>CMeast</i>				
	(To view, navigate to <b>Media Server→List</b> ; Click <b>Edit</b> )				
	• SIP Trunk IP Address (Avaya S8300 Server IP address): 10.75.5.2				
	(To view, navigate to <b>Media Server→List</b> ; Click <b>Edit</b> )				

# 5. Configure the Avaya SIP Telephones

The SIP telephones at the main office will use Avaya SES as the call server. The SIP telephones at the branch site will use the public IP address of SIPassure as the call server.

The table below shows an example of the SIP telephone networking settings for both the main and branch offices.

	Main Site	Branch Site
IP Address	10.75.5.153	50.1.1.155
Subnet Mask	255.255.255.0	255.255.255.0
Call Server	10.75.5.6	46.14.2.80
Router	10.75.5.1	50.1.1.254
File Server	10.75.10.52	10.75.10.52

## 6. Configure Borderware SIPassure

This section covers the configuration of SIPassure. It is assumed that the SIPassure software has already been installed. For additional information on these installation tasks, refer to [7].

tep		Description
1.	SIPassure is configured via a v http:// <ip-addr> in the address address of SIPassure.</ip-addr>	web browser. To access the web interface, enter s field of the web browser, where <i><ip-addr></ip-addr></i> is the IP
	Log in with the appropriate cre	edentials. The main page will appear as shown below.
	sipassic basiness community Server reavity	<b>v</b>
	Summary	Attacks
	sipassure.business.com Server Time: Tue Apr 24 10:49:47 EDT 2007 Uptime: 8 mins SIP Status: Running SIP Uptime: 7 minutes	Impersonation Deregister Hijack Malformed Relay Server IP Spam Big Hops 7 Hour Day Week Call Charts
	Status Load Averages: 0.00, 0.05, 0.05 Swap Space: 2055MB - Total 8MB - Used CPU: 3.30% Memory: 6.50% Refresh Refresh Logging Turn Off Debugging Mode:	Call Volume
	Version: 3.0.1 (Build Number 3.0.7) Installed: 2007-04-04 Copyright	© 2004 - 2006 Border/Ware Technologies Inc. All rights reserved.

Step	Description
2.	The initial server parameters are configured as part of the installation procedures. This
	includes the server name, server type and both public and private IP addresses. For
	details on these procedures see [7]. To view these settings, navigate from the <b>Platform</b>
	tab to <b>Platform→Server Management</b> .
	The example below shows the settings used for the compliance test. The <b>Host Name</b>
	was set to <i>sipassure</i> . The Server Type was set to SIP & RTP. Interface - em0 was set
	to the WAN (public) IP address and Interface - em2 was set to the LAN (private) IP
	address.
	The default values were used for the remaining fields. If any values were modified,
	click Save.
	SAF TARAMAS
	Activity Configuration Policies Subscribers Tools Platform
	4 sipassure.business.com - Platform :: Server Management
	Sever Details
	Host Name: sipassure *
	Server Type: SIP & RTP
	Status: Running Stop Processing
	Support Access
	Support Access is not installed.
	Clustering
	Enable Clustering:
	Cluster Interface: em1 💌
	Set as Standby: 📃 Set sipassure as a Standby server.
	Network Interfaces
	Interface 1 - em0: 46.14.2.80, Active, Enabled, WAN, autoselect
	Interface 2 - em2.     Interface 2 - em1:     No corrier Dischlad - autoselect
	Reboot & Shutdown
	Reboot. Restart server: sipassure
	Shutdown server:: Shutdown Shutdown server: sipassure
	Caution: If you modify a network interface for a system, that system must be rebooted to complete the changes.
	Covo Depart
	Save Kesel

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

17 of 26 BorderSipRemUsr

<ul> <li>3. Additional parameters configured during installation can be viewed by nave the Platform tab to Platform→Basic Network. The Domain Name field the SIP domain of Avaya SES as shown in Section 4, Step 4. The Gateward set to the default gateway for the public IP interface.</li> <li>No email server or DNS server was used in the compliance test. However requires entries in these fields, so an arbitrary value was entered for each. server is needed for the customer to receive notifications of software updated.</li> </ul>	vigating from d was set to <b>ay</b> field was r, SIPassure The email tes that have so used to ent, the DNS
No email server or DNS server was used in the compliance test. However requires entries in these fields, so an arbitrary value was entered for each. server is needed for the customer to receive notifications of software update	r, SIPassure The email ates that have so used to ent, the DNS
been uploaded and not yet installed. In a redundant configuration, it is also send notifications that a failover has occurred. In a production environment server would be used to resolve host names within the VoIP network.	
If a NTP server is used, it should be set to the same clock source (NTP ser Avaya SES and Avaya Communication Manager. The default values can be used for the remaining fields. If any values were click <b>Save</b> .	rver) as re modified,
Activity       Configuration       Policies       Subscribers       Tools       Platform	iout Contraction of the second
Host Details	
Disable Firewall Disables all Firewall policies on SIPassure and opens the system up to all net	atwork traffic. Only
Domain Name: business.com	
Gateway: 46.14.2.1 *	
Email Server: email sample.com *	
Syslog Host:	
Domain Name Server Settings	
Name Server 1: 46.14.2.1 *	
Name Server 2:	
Name Server 3:	
NTD Course Configure	
NTP Server 1:	
NTP Server 2:	
NTP Server 3:	
limezone	
Zone: New_York	
Save Reset	
Version: 3.0.1 (Build Number 3.0.7) Installed: 2007-04-04	Logged In: admin
Copyright@ 2004 - 2006 BordertWare Technologies Inc. All rights reserved.	$\sim$

<ul> <li>4. Basic Settings To configure or verify the basic settings, navigate from the Configuration tab to Configuration→SIP. Verify the SIP Port field is set to the default value of 5060. This is the port which SIPassure will listen for SIP messages. Verify the TLS Port field is set to the default value of 5061. This is the port which SIPassure will listen for secure SIP messages using TLS. The Log Level field was set to Debug for the testing Normally, it would be set to the default value of Error to reduce the amount of logging under normal conditions. The default values can be used for the remaining fields. Scroll down to configure additional parameters. </li> <li> Will State Settings Basic Settings BiP Port SiP Port Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access. Basic Settings Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access. Disc Settings Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access. Disc Settings Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access. Disc Settings Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access. Disc Setting Port Seture port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access. Disc Seture port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access. Disc Seture port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access.</li></ul>	Step	Description
Activity       Configuration       Policies       Subscribers       Tools       Platform         sipassure.business.com       Configuration       SIP Configuration       Image: Configuratio	4.	Basic Settings To configure or verify the basic settings, navigate from the Configuration tab to Configuration→SIP. Verify the SIP Port field is set to the default value of 5060. This is the port which SIPassure will listen for SIP messages. Verify the TLS Port field is set to the default value of 5061. This is the port which SIPassure will listen for secure SIP messages using TLS. The Log Level field was set to Debug for the testing. Normally, it would be set to the default value of <i>Error</i> to reduce the amount of logging under normal conditions. The default values can be used for the remaining fields. Scroll down to configure additional parameters.
sipassure.business.com - Configuration :: SIP Configuration         Basic Settings         SIP Port:       5060 *         Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access.         TLS Port:       5061 *         SECURE port       5061 *         SECURE port       5061 *         SECURE port on which to listen for SIP messages         STUN Port:       3478 *         Port on which to listen for STUN messages. Set to 0 to disable the processing of STUN messages.         External IP       Public IP address of firewall. Enter a value only if the SIPassure is behind a NAT firewall.         Log Only:       Don't stop attacks, log them only         Log Level:       Debug		Activity Configuration Policies Subscribers Tools Platform
Basic Settings         SIP Port       5060 *       Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access.         TLS Port       5061 *       Secure port on which to listen for SIP messages         STUN Port       3478 *       Port on which to listen for STUN messages. Set to 0 to disable the processing of STUN messages.         External IP address;       Public IP address of firewall. Enter a value only if the SIPassure is behind a NAT firewall.         Log Only:       Don't stop attacks, log them only         Log Level:       Debug		sipassure.business.com - Configuration :: SIP Configuration
SIP Port.       5060 *       Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access.         TLS Port.       5061 *       Secure port on which to listen for SIP messages         STUN Port.       3478 *       Port on which to listen for STUN messages. Set to 0 to disable the processing of STUN messages.         External IP address:       Public IP address of firewall. Enter a value only if the SIPassure is behind a NAT firewall.         Log Only:       Don't stop attacks, log them only         Log Level:       Debug		Basic Settings
TLS Port:       5061 *       Secure port on which to listen for SIP messages         STUN Port:       3478 *       Port on which to listen for STUN messages. Set to 0 to disable the processing of STUN messages.         External IP address:       Public IP address of firewall. Enter a value only if the SIPassure is behind a NAT firewall.         Log Only:       Don't stop attacks, log them only         Log Level:       Debug		SIP Port. 5060 * Port on which to listen for SIP messages. Note: Port 10101 cannot be used as this is reserved for Support Access.
STUN Port       3478       Port on which to listen for STUN messages. Set to 0 to disable the processing of STUN messages.         External IP address:       Public IP address of firewall. Enter a value only if the SIPassure is behind a NAT firewall.         Log Only:       Don't stop attacks, log them only         Log Level:       Debug		TLS Port. 5061 * Secure port on which to listen for SIP messages
External IP       Public IP address of firewall. Enter a value only if the SIPassure is behind a NAT firewall.         address:       Don't stop attacks, log them only         Log Level:       Debug		STUN Port. 3478 * Port on which to listen for STUN messages. Set to 0 to disable the processing of STUN messages.
Log Only: Don't stop attacks, log them only Log Level: Debug		External IP Public IP address of firewall. Enter a value only if the SIPassure is behind a NAT firewall. address:
Log Level: Debug		Log Only. Don't stop attacks, log them only
		Log Level: Debug

SIP Settings         Set the SIP Proxy Server to the IP address of Avaya SES. Verify the Port field to the default value of 5060. This is the port which SIPassure will send SIP sign: messages. Check the Process all SIP messages box.         The default values can be used for the remaining fields. Scroll down to configure additional parameters.         SiP Settings         Protocols colspan of the books for force and subject to the books for force a	OTT O		Description
Set the SIP Proxy Server to the IP address of Avaya SES. Verify the Port field to the default value of 5060. This is the port which SIPassure will send SIP sign: messages. Check the Process all SIP messages box. The default values can be used for the remaining fields. Scroll down to configure additional parameters.           SP Settings         Image: SiP Prox Server 107565         Image: SiP Prox Server 107565         Image: SiP Prox Server 107565           SP Settings         Image: SiP Prox Server 107565         Image: SiP Prox Server 107565         Image: SiP Prox Server 107565           Add Feoror         Image: SiP Prox Server 107565         Image: SiP Prox Server 107565         Image: SiP Prox Server 107565           Add Feoror         Image: SiP Prox Server 107565         Image: SiP Prox Server 107565         Image: SiP Prox Server 107565           Add Feoror         Image: SiP Prox Server 107565         Port to which to direct 9P messages         Image: SiP Prox Server 10756           Add Feoror         Image: SiP Prox Server 10756         Port Server 107566         Image: SiP Prox Server 107566           Use DRY codd for each and the side server 10756         Port Server 107566         Image: SiP Prox Server 107566           Use SRY codd for each and the side server 107566         Port Server 107566         Image: SiP Prox Server 107566           Use SRY codd for each and the side server 107566         Port Server 107566         Port Server 107566           Use SRY codd for each and the side server 107566         Port Server 107566	SIP Settings		
to the default value of <i>5060</i> . This is the port which SIPassure will send SIP sign: messages. Check the <b>Process all SIP messages</b> box. The default values can be used for the remaining fields. Scroll down to configure additional parameters.           SP Settings       IP address or FOON (o.g. % my company com) to which to direct SIP messages.         Add Precord       IP address or FOON (o.g. % my company com) to which to direct SIP messages.         Add Precord       IP address or FOON (o.g. % my company com) to which to direct SIP messages.         Add Precord       IP address or FOON (o.g. % my company com) to which to direct SIP messages.         Add Precord       IP address or FOON (o.g. % my company com) to which to direct SIP messages.         Add Precord       IP address or FOON (o.g. % my company com) to which to direct SIP messages.         Add Precord       IP address or FOON (o.g. % my company com) to which to direct SIP messages.         Add Precord       IP address or FOON (o.g. % my company com) to which to direct SIP messages.         Use FOON STAY       Use BRY needs and foreth messages for raddy of Hop Energine Fourth Star Program of the	Set the SIP Pro	oxy Server to	the IP address of Avaya SES. Verify the Port field is
<pre>messages. Check the <b>Process all SIP messages</b> box.</pre> The default values can be used for the remaining fields. Scroll down to configure additional parameters. <pre>SIP Settings SIP Prove Server 107.55.6</pre>	to the default va	alue of <i>5060</i> .	This is the port which SIPassure will send SIP signal
The default values can be used for the remaining fields. Scroll down to configure additional parameters.  SP Settings SP Prove Server: 107555 Port 10755 Port 10755 Port 10755 Port 10755 Port 10755 Port 10755 Port 1075 Port 10755 Port 1075 Port 10	messages. Che	ck the <b>Proces</b>	s all SIP messages box.
The default values can be used for the remaining fields. Scroll down to configure additional parameters.           SIP Settings       ID2556       * IP address or FQON (e.g. tip.mycompany.com) to which to direct SIP messages         Port       9000 *       Porto Weich address or FQON (e.g. tip.mycompany.com) to which to direct SIP messages         Port       9000 *       Porto Weich address or FQON (e.g. tip.mycompany.com) to which to direct SIP messages         Porto Weich address or FQON (e.g. tip.mycompany.com) to which to direct SIP messages       Porto Weich address or FQON (e.g. tip.mycompany.com) to which to direct SIP messages         Use Recode       Interpret to the state of the state			
additional parameters.  SIP Settings  Port  SIP Prov Server: Port  SIP Prov Port  SIP P	The default value	ues can be use	ed for the remaining fields. Scroll down to configure
SIP Settings       IP address or FODN (e.g. 'b), my company, com) to which to direct SIP messages         Part       900**         Part       900***         Part       900****         Part       900*******         Part       900***********************************	additional parai	meters.	
SIP Settings         SIP Settings         Port, 9000         Port, 90000         Port, 90000         Port, 900000         Port, 9000000000000000000000000000000000000			
SIP Provy Server: 107.55.5   Port 90000*   Port or bink to direct SIP messages   Port or bink to direct SIP messages   Proves and Via   Proves and Via   Use Roctors   Proves Server:   Proves Server:   Proves Server:   Use Roctors   Proves Server:   Provess Server	SIP Settings		
Port       5060 *       Port to which direct SP messages         If the option is disabled, PR and Via headers will not be added by SIPassure to SIP messages, endeting the SIPassure for SIP messages.         Use Route       If the option is disabled, PR and Via headers will not be added by SIPassure to SIP messages, endeting the SIPassure for SIP message.         Use Route       If the option is disabled, PR and Via headers will not be added by SIPassure to SIP message.         Use Route       If the option is disabled, PR and Via headers will not be added by SIPassure to SIP message.         Use Route       If the option is disabled, PR and Via headers will not be used.         Weep original       Use Reference to resolve a request URIs hostmane (If the portis unspecified         Registration filter       Period (see) at which to forward a registration to the Provy Server. Registrations forwarded to the Pow Server, and will appear to have been sent directify in the VANI. If the option is called by the optic serve will be changed to the SiPassure's LA address and the ressages will appear to have originated from the Server, such as packets that are sent to this server because if it is default gateware or a static route. (This opti is disable) these messages will only be processed if they are sent from the LAN.         Encode Contact       Encode the Contact with the SIPassure's interface IP and the message's source IP/port. Do not disable this option if ony of your phones are behind a router or firewait.         Use RTP Proxy for I local calls box.       Check the Proxy Server is a B21 box.         Use RTP Proxy for II and IP is antis di	SIP Proxy Server:	10.75.5.6	<sup>4</sup> IP address or FQDN (e.g. 'sip.mycompany.com') to which to direct SIP messages
Add Record       If this option is disabled, RF and Via headers will not be addres by more IBPs and Prove Bereas.         In deal not Via       If this option is disabled, RF and Via headers will not be addres by more IBPs and Prove Bereas.         In deal not Via       If this option is disabled, RF and Via headers will not be addres by more IBPs and Prove Bereas.         In deal not Via       If this option is disabled, RF and Via headers will not be addres by more IBPs and Prove Bereas.         In deal not Via       If this option is disabled, RF and Via headers will not be addres by address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course PI address of a UDP message received from the WAN in the big option is enabled; the course P	Port:	5060 *	Port to which to direct SIP messages
Use Route Use Route route and Route headers for routing, if Yad Root-Route has not been checked, some Prove Server moutes that this option to disable the source if Pariset is option to the Prove Server route that this option is disabled, the source if Pariset is option if any of your phones are equest UR's hostname if the port is unsepecified to the Pawil have the Expires field set to this value.   Registration filter Image: Prove Server and use the source if Pariset is option is snabled, the source if Pariset is option is analysic, the source if Pariset is option is analysic, the source if Pariset is option is snabled, the source if Pariset is of this server, south as pare to have been send reactly the When this option is snabled, the source if Pariset is a default gravery or on a static route. If this option is disabled, the source if Pariset is a default gravery or on a static route. If this option is analysic, these messages will only the process off they are sent from the LAN.   RTP Settings Check the Use RTP Proxy for local calls box. Check the Proxy Server is a B21 box.   The default values can be used for the remaining fields. Click Save.   RTP Settings   Use RTP Prov for is analysic.   Use RTP Prov for is analysic.   If this option is disabled, the RTP proxy will not be used when a phone calls another with the set another with the set and the independence.   RTP Settings   Use RTP Prov for is analysic.   Use RTP Proxy for local calls box. Check the Use Advent a phone calls another with the set another with the set and the rute set when a phone calls another with the set another in different subnets.   RTP Settings   Use RTP Prov for is a sabled. The RTP proxy will not be used when a phone calls another with the set another with the set an informatic is	Add Record- Route and Via headers:		If this option is disabled, RR and Via headers will not be added by SIPassure to SIP messages, rendering the SIPassure 'invisible'. This may be required by some ISPs and Proxy Servers.
Use DNS BKY       Use SKV records to resolve a request URI's hostname (fthe port is unspecified records to resolve a request URI's hostname (fthe port is unspecified period (acc) at which to forward a registration to the Proxy Server. Registrations forwarded to the Proxy Server and WAR source IP address and UP message received from the WAR in the implicit of the source IP address will be changed to the SiPassure's LM address and the message will appear to have orginated form the Server have orginated form the Server have orginated form SiPassure's LM address and the message will appear to have orginated for this server, such as practed the address will be changed to the SiPassure's LM address and the message will appear to have orginated form the Server have orginated for the server have orginated the server have orginated form the Server have orginated for the server such as practed from the LMA. The odd is able this option if any of your phones are behind are not desting the server such as practed for the contact with the SiPassure's interface IP and the message's source IP port. Do not disable this option if any of your phones are behind a router of frewall.         RTP Settings       Encode for the remaining fields. Click Save.         The default values can be used for the remaining fields. Click Save.         RTP Fostings       If this option is disabled, the RTP proxy will not be used when a phone calls another with the serve include in the serve base are public IP und are indifferent subnets.         RTP Settings       If this option is disabled, the RTP proxy will not be used when a phone calls another with the serve include in the serve include in the serve include incluses.         Were than a set of RTP proxy of the prove serve as a Back to Back User Agent and processes RTP taff. The senting public is ena	Use Route headers:		Use Record-Route and Route headers for routing. If 'Add Record-Route' has not been checked, some Proxy Server products may require that this option be disabled.
Registration filter Period (sec) at which to forward a registration to the Proxy Server. Registrations forwarded to the Power or address of a UDP message received from the VAW and the message will appear to have or address of a UDP message received from the VAW and the message will appear to have or address of a UDP message received from the VAW. This option is realisable, the source P address will be changed to the SIPsasure's LA address and the message will appear to have or address will be changed to the SIPsasure's LA address and the message will appear to have or address will be changed to the SIPsasure's LA address and the message will appear to have or address of address of a UDP message's source IP/port. Do not headers:   Process all SIP Process all SIP UDP message's source IP/port. Do not disable this option if any of your phones are behind a router or firewall.   RTP Settings Encode the Contact with the SIP assure's interface IP and the message's source IP/port. Do not disable this option if any of your phones are behind a router or firewall.   RTP Settings If this option is disabled, the FTP proxy Server is a BS2 box.   The default values can be used for the remaining fields. Click Save.   RTP Settings If this option is disabled, the FTP prox will not be used when a phone calls another with the sar buble. IP this option if your phones may not be able to send RTP traffic to each other duck (i.e. the yeak we the same public IP traffic to each other duck (i.e. the yeak we the same public IP traffic to each other duck (i.e. the yeak we the same public IP to the set of the receive (i.e. the yeak we the same public IP to the set of the receive (i.e. the yeak we the same public IP to the set of the receive (i.e. the yeak we the same public IP to the set of the receive (i.e. the yeak we the same public IP to the set of the receive (i.e. the yeak we the same public	Use DNS SRV records:		Use SRV records to resolve a request URI's hostname if the port is unspecified
Keep original www.viscore IP       When this option is enabled, the source IP address, of a UDP message received from the WAV- address;         Process all SIP with source IP       When this option is disabled, the source IP address will be charged to the SIPAssure's LA address;         Process all SIP with source IP       Process all SIP with source IP address will be charged to the SIPAssure's LA address and the messages will appear to have beginned to the SIPAssure's LA address and the messages will only be processed if they are sent from the LAN.         Encode Contact       Process all SIP UDP messages including those thave originated from SIPAssure, with so phile is disabled, these messages will only be processed if they are sent from the LAN.         Encode the Contact with the SIPAssure's INFace IP and the message's source IP/port. Do not disable this option if any oryour phones are behind a router or freewall.         RTP Settings         Check the Use RTP Proxy for local calls box. Check the Proxy Server is a B21 box.         The default values can be used for the remaining fields. Click Save.         RTP Settings         We make and the same public IP. Enable this option is disabled, the RTP proy will not be used when a phone calls another with the same public IP. Enable this option is disabled, the RTP proy will not be used when a phone calls another with the same public IP. Enable this option if your phones may not detend to ther directly, i.e. they have the same public IP but are in different unders.         RTP Settings       Valid mainmum range values are 1025 to 65534         Port range B2BUA:       Check this option if the Proxy	Registration filter period:	0	Period (sec) at which to forward a registration to the Proxy Server. Registrations forwarded to the PS will have the Expires field set to this value.
address and the message will appear to have opinghated from SiPassure.         Process all SiP ∪ Dressages including those that are not destined for this server, such as packets that are sent to this server because it is a default gateway or on a state route. If this opin is disabled, these messages will only be processed if they are sent from the LAN.         Encode Contact readers:       Image: Signature of the message will appear to have opinghated from SiPassure.         RTP Settings       Encode the Contact with the SiPassure's interface IP and the message's source IP/port. Do not disable this option if any of your phones are behind a router or firewall.         RTP Settings       Check the Use RTP Proxy for local calls box. Check the Proxy Server is a B21 box.         The default values can be used for the remaining fields. Click Save.         If this option is disabled, the RTP proxy will not be used when a phone calls another with the sar public (P. Fonable the option (P. Proxy For local calls:         Use RTP Prox for local calls       If this option is disabled, the RTP proxy will not be used when a phone calls another with the sar public (P. Fonable the option from phone may not be able to send RTP traffic to each other during information)         Value to be set for RTP packets that don't have a Type of Service (TOS) byte set       Yalid minimum range values are 1024 to 85533         Port range       2000       Yalid maximum range values are 1024 to 85534         Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffic this server Prox for focal calls' option is ignored).         Wait	Keep original WAN source IP address		When this option is enabled, the source IP address of a UDP message received from the WAN wil not be modified before it is sent to the Proxy Server, and will appear to have been sent directly from the WAN. If this option is disabled, the source IP address will be changed to the SIPassure's LAN
messages:   in dessages:   in dessages:  <	Process all SIP		address and the message will appear to have originated from SIPassure. Process all SIP UDP messages including those that are not destined for this server, such as
Encode Contact       Image: State of the Contact with the SIPassure's interface IP and the message's source IP/port. Do not disable this option if any oryour phones are behind a router or firewall.         RTP Settings       Check the Use RTP Proxy for local calls box. Check the Proxy Server is a B21 box.         The default values can be used for the remaining fields. Click Save.         Image: Straig S	messages:		packets that are sent to this server because it is a default gateway or on a static route. If this option is disabled, these messages will only be processed if they are sent from the LAN.
The default values can be used for the remaining fields. Click Save.         File default values can be used for the remaining fields. Click Save.         Use RTP Proxy for local calls box.         Use RTP Proxy for local calls.         If this option is disabled, the RTP prov will not be used when a phone calls another with the sar public IP. Enable this option flywour phones may note balle to send RTP traffic to each other directly, i.e. they have the same public IP but are in different subnets.         RTP TOS byte:       184         Value to be set for RTP packets that dont have a Type of Service (TOS) byte set         Port range about the set proxy for local calls option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffit this is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).         If this is enabled, then the SIP service         RTP Forsy for local calls option will require a restart of the SIP service         RTP Proxy for local calls option is ignored).         Valid mainmum range values are 1024 to 65533         RTP Fore fis a reset         RTP For f	Encode Contact		Encode the Contact with the SIPassure's interface IP and the message's source IP/port. Do not
RTP Settings         Use RTP Proxy for local calls:       If this option is disabled, the RTP proxy will not be used when a phone calls another with the sar public IP. Enable this option if your phones may not be able to send RTP traffic to each other directly, i.e. they have the same public IP but are in different subnets.         RTP TOS byte:       184         Port range       20000         Walid minimum range values are 1024 to 65533         Port range       65000         Walid maximum range values are 1025 to 65534         Proxy Server is a B2BUA:       Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffit it is is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).         Image:       Caution:         Pressing the Save button will require a restart of the SIP service         Save:       Reset		RTP Proxy fo	on local calls have Charle the Drown Someon is a D2D
KIP Settings         Use RTP Proxy for local calls:       If this option is disabled, the RTP proxy will not be used when a phone calls another with the same public IP. Enable this option if your phones may not be able to send RTP traffic to each other directly, i.e. they have the same public IP but are in different subnets.         RTP TOS byte:       184         Port range       20000         Walid minimum range values are 1024 to 65533         Port range       65000         Walid maximum range values are 1025 to 65534         Proxy Server is a B2DUA:       Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffit fit is is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).         Image:       Caution:         Pressing the Save button will require a restart of the SIP service         Save:       Reset	Check the <b>Use</b> box.	ues can be use	d for the remaining fields. Click <b>Save</b> .
Iteration       public IP. Enable this option if your phones may not be able to send RTP traffic to each other directly, i.e. they have the same public IP but are in different subnets.         RTP TOS byte:       184       Value to be set for RTP packets that don't have a Type of Service (TOS) byte set         Port range       20000       Valid minimum range values are 1024 to 65533         Port range       65000       Valid maximum range values are 1025 to 65534         Port y Server is a B2BUA:       Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffic for the "Use RTP Proxy for local calls" (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).         Image       Caution:         Pressing the Save button will require a restart of the SIP service         Save       Reset         Version: 3.0.1 (Build blumber 3.0.7)       Lower	Check the Use box.	ues can be use	ed for the remaining fields. Click <b>Save</b> .
RTP TOS byte:       184       Value to be set for RTP packets that don't have a Type of Service (TOS) byte set         Port range       20000       Valid minimum range values are 1024 to 85533         Port range       65000       Valid maximum range values are 1025 to 65634         Proxy Server is a B2BUA:       Image: Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traff If this is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).         Image: Caution: Pressing the Save button will require a restart of the SIP service       Save Reset         Version: 3.0.1 (Build blumber 3.0.7)       Image: Caution:	Check the Use box. The default value RTP Settings	ues can be use	ed for the remaining fields. Click <b>Save</b> .
Port range       20000*       Valid minimum range values are 1024 to 65533         Port range       65000*       Valid maximum range values are 1025 to 65534         Proxy Server is a       Imaximum       Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traff         Proxy Server is a       Imaximum       Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traff         Proxy Server is a       Imaximum       Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traff         If this is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).         Imaximum       Caution:         Pressing the Save button will require a restart of the SIP service         Save       Reset         Version: 3.0.1 (Build blumber 3.0.7)       Lower	Check the Use box. The default valu RTP Settings Use RTP Proxy for local calls:	ues can be use	ed for the remaining fields. Click Save.
Port range       65000 *       Valid maximum range values are 1025 to 65534         maximum:       Proxy Server is a B2BUA:       Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traff         Proxy Server is a B2BUA:       Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traff         If this is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP proxy for local calls" option is ignored).         Imaximum:       Caution:         Pressing the Save button will require a restart of the SIP service         Save       Reset         Version: 30.1 (Fluid Number 30.7)       Lower	Check the Use box. The default value RTP Settings Use RTP Proxy for local calls: RTP TOS byte:	ues can be use	ed for the remaining fields. Click Save.
maximum:	Check the Use box. The default value RTP Settings Use RTP Proxy for local calls: RTP TOS byte: Port range minimum	ues can be use ✓ 184 * 20000 *	ed for the remaining fields. Click Save.
Proxy server is a B2BUA:       If this is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).         Caution:       Pressing the Save button will require a restart of the SIP service         Save       Reset         Version: 3.01 (Build blumber 3.0.7)       Lower	Check the Use box. The default valu RTP Settings Use RTP Proxy for local calls: RTP TOS byte: Port range minimum: Port range	ues can be use ✓ 184 * 20000 * 65000 *	ed for the remaining fields. Click Save.
Caution: Pressing the Save button will require a restart of the SIP service  Save Reset  Version: 3.0.1 (Fulld Number 3.0.7)	Check the Use box. The default value RTP Settings Use RTP Proxy for local calls: RTP TOS byte: Port range minimum: Port range maximum:	ues can be use	ed for the remaining fields. Click Save. If this option is disabled, the RTP proxy will not be used when a phone calls another with the same public IP. Enable this option if your phones may not be able to send RTP traffic to each other directly, i.e. they have the same public IP but are in different subnets. Value to be set for RTP packets that don't have a Type of Service (TOS) byte set Valid minimum range values are 1024 to 65533 Valid maximum range values are 1025 to 65534 Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffic
Save Reset	Check the Use box. The default value RTP Settings Use RTP Proxy for local calls: RTP TOS byte: Port range maximum: Port range maximum: Proxy Server is a B2BUA:	ues can be use ✓ 184 * 20000 * 65000 * ✓	ed for the remaining fields. Click Save. If this option is disabled, the RTP proxy will not be used when a phone calls another with the same public IP. Enable this option if your phones may not be able to send RTP traffic to each other directly, i.e. they have the same public IP but are in different subnets. Value to be set for RTP packets that don't have a Type of Service (TOS) byte set Valid minimum range values are 1024 to 65533 Valid maximum range values are 1025 to 65534 Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffic. If this is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).
Version: 3.0.1 (Build Number 3.0.7) Lowes	Check the Use box. The default value RTP Settings Use RTP Proxy for local calls: RTP TOS byte: Port range minimum: Proty Server is a B2BUA: Caution: Pressing the 1	ues can be use	ed for the remaining fields. Click Save. If this option is disabled, the RTP proxy will not be used when a phone calls another with the same public IP. Enable this option if your phones may not be able to send RTP traffic to each other directly, i.e. they have the same public IP but are in different subnets. Value to be set for RTP packets that don't have a Type of Service (TOS) byte set Valid minimum range values are 1024 to 65533 Valid maximum range values are 1025 to 65534 Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffic. If this is enabled, then the RTP proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored).
	Check the Use box. The default value RTP Settings Use RTP Proxy for local calls: RTP TOS byte: Port range minimum: Port range maximum: Proxy Server is a B2BUA: Caution: Pressing the Save Rese	ues can be use	ed for the remaining fields. Click Save. If this option is disabled, the RTP proxy will not be used when a phone calls another with the same public IP. Enable this option if your phones may not be able to send RTP traffic to each other directly, i.e. they have the same public IP but are in different subnets. Value to be set for RTP packets that don't have a Type of Service (TOS) byte set Valid minimum range values are 1024 to 65533 Valid maximum range values are 1025 to 65534 Check this option if the Proxy Server acts as a Back to Back User Agent and processes RTP traffic. If this is enabled, then the RTP Proxy will always be used for local calls (i.e. the value of the "Use RTP Proxy for local calls" option is ignored). estart of the SIP service

Step	Description
7.	<b>SIP Domain</b> Navigate from the <b>Configuration</b> tab to <b>Configuration</b> $\rightarrow$ <b>SIP Domains</b> . The compliance test used a single SIP domain which was entered during installation (see <b>Step 3</b> ). This form may be used to add additional domains.
	Activity       Configuration       Policies       Subscribers       Tools       Platform         Sipassure.business.com - Configuration :: SIP Domains       2         SIP Domain:       Add
	Name
	business.com
	Version: 3.0.1 (Build Number 3.0.7) Installed: 2007-04-04 Copyright© 2004 - 2006 BorderWare Technologies Inc. All rights reserved.
	<

Step	Description
8.	Authentication         Navigate from the Policies tab to Policies→Authentication. Uncheck the         Authentication box since Avaya SES will authenticate the caller.         The default values can be used for the remaining fields. Click Save.
	Activity         Configuration         Policies         Subscribers         Tools         Platform           sipassure.business.com - Policies :: Authentication         @
	Authentication
	Authenticate: Use SIP Digest authentication for INVITE and REGISTER messages from within the SIP domain. NOTE: If this is set, the SIP prov Server must not perform authentication or a race condition will result.
	Authentication Method: Database If RADIUS, set a Radius server to use
	Authenticate Bye: 🔲 Prevents third-parties from terminating an in-progress call
	Authenticate Transfer: Authenticate REFER messages to prevent a third-party from hijacking a call and transferring it to himself.
	Check From:       Check that the caller's From URI matches his authentication username. Prevents a caller from spoofing his phone number. NOTE: Either SIPassure and/or the Proxy Server must perform INVITE authentication.         Set Display Name:       Sets an INVITE message's Display Name to match the name associated with the caller's authentication username. Prevents a caller from spoofing their display name. NOTE: The caller must be added in the Subscribers-Manage Subscribers page. Either SIPassure and/or the Proxy Server must perform INVITE authentication.
	Check         If user 'A' is allowed to register user 'B's phone, user 'A' can hijack incoming calls to 'B'. This option prevents           Register/Deregister         this, Also prevents user 'A' from deregistering user 'B's devices. NOTE: Either SIPassure and/or the Proxy           Theft:         Server must perform REGISTER authentication.
	Caution: Pressing the Save button will require a restart of the SIP service  Save Reset
	Version: 3.0.1 (Build Number 3.0.7) Logged In: admin Installed: 2007-04-04 Copyright© 2004 - 2006 BorderWare Technologies Inc. All rights reserved.

Step	Description
9.	Anti-Spam Settings
	The Anti-Spam Settings were disabled for the compliance test. To configure these settings, newigate to <b>Policies teb to Policies</b> Anti Spam Settings. The example
	settings, havigate to <b>Foncies</b> tab to <b>Foncies</b> Anti-Spain Settings. The example
	below shows all the settings were unchecked. However, for a customer installation,
	Borderware nightly recommends that Anti-Spam protection be enabled to allow normal
	call traffic and flag or block abnormal calling patterns. For more information on now
	to configure the Anti-Spam settings, see [9].
	tuopol
	Activity Configuration Policies Subscribers Tools Platform
	🔺 sipassure.business.com - Policies :: Anti-Spam Settings 🕜
	Anti-Spam Settings
	Check Relaying: 🔲 Prevents outside callers from using this server to route calls to outside destinations
	Check Server Contact: D Prevents users from registering as this server; prevents infinite loops
	Check Spam: 🔲 Check calls from external SIP domains against the spam rules.
	Check Internal Spam: 🔲 Check internal calls from SIP domains managed by this SIP assure against the spam rules.
	Check Cancels: Disallow a hacker from cancelling a ringing call.
	Caution: Pressing the Save button will require a restart of the SIP service
	Save Reset
	Version: 3.0.1 (Build Number 3.0.7) Installed: 2007-04-04 Copyright@ 2004 - 2006 Border/Ware Technologies Inc. All rights reserved.

# 7. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of Borderware SIPassure with Avaya SIP Enablement Services and Avaya Communication Manager. This section covers the general test approach and the test results.

#### 7.1. General Test Approach

The general test approach was to make calls through SIPassure using various codec settings and exercising common PBX features. Calls were made between the branch office and the main office, between the branch office and the PSTN, and within the branch site.

### 7.2. Test Results

SIPassure passed compliance testing. The following features and functionality were verified. Any observations related to these tests are listed at the end of this section.

- Successful registrations of endpoints at the main and branch offices.
- Calls between the branch office and SIP endpoints at the main office.
- Calls between the branch office and non-SIP endpoints at the main office.
- Calls between the branch office and the PSTN.
- Intra-branch calls
- G.711u and G.729AB codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Conference On Answer, Call Park, Call Pickup, Automatic Redial and Send All Calls. For more information on FNEs, please refer to [4].
- Proper system recovery after a SIPassure restart and loss of IP connection.

The following observations were made during the compliance test:

- For interoperability, direct IP to IP media (also known as media shuffling) must be disabled on the SIP trunk in Avaya Communication Manager (see **Section 3, Step 6**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.
- For interoperability, local SIP endpoints must register with SES and do not have the option to register through SIPassure as the remote endpoints do. Thus, SIPassure will not be able to protect Avaya SES and Avaya Communication Manager from SIP attacks from internal users.

### 8. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya SES web administration interface, verify that all remote endpoints are registered with Avaya SES using the private IP address of SIPassure. To view, navigate to Users→Registered Users.
- Verify that calls can be placed between the branch office and SIP endpoints at the main office.
- Verify that calls can be placed between the branch office and non-SIP endpoints at the main office.
- Verify that calls can be placed between the branch office and the PSTN.
- Verify that calls can be placed between endpoints at the branch office.

# 9. Support

For technical support on SIPassure, contact the Borderware reseller or distributor from where SIPassure was purchased.

CTM; Reviewed:	
SPOC 6/28/2007	

# 10. Conclusion

Borderware SIPassure passed compliance testing with the observations listed in **Section 7.2**. These Application Notes describe the procedures required to configure Borderware SIPassure to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support remote users as shown in **Figure 1**.

# 11. Additional References

- [1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 5.0, February 2007.
- [2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007.
- [3] SIP support in Avaya Communication Manager Running on the Avaya S3800, S8400, S8500 Series and S8700 Series Media Server, Doc # 555-245-206, Issue 6.1, March 2007.
- [4] Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0, version 6.0, Doc # 210-100-500, Issue 9, June 2005
- [5] Installing and Administering SIP Enablement Services, Doc# 03-600768, Issue 4, May 2007.
- [6] Avaya IA 770 INTUITY AUDIX Messaging Application, Doc # 11-300532, May 2005.
- [7] Borderware SIPassure Installation Guide, Version 3.0, September 21, 2006.
- [8] Borderware SIPassure Quick Install Guide, October 6, 2006.
- [9] Borderware SIPassure Users Guide, Version 3.0, August 11, 2006.
- [10] Borderware SIPassure Update 3 Release Notes, October 19, 2006.
- [11] Borderware SIPassure Update 3.0.7 Release Notes, pending completion.

Product documentation for Avaya products may be found at http://support.avaya.com.

Product documentation for SIPassure can be obtained from a Borderware reseller or distributor.

#### ©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by <sup>®</sup> and <sup>TM</sup> are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.