

Avaya Solution & Interoperability Test Lab

# **Application Notes for Configuring Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager to Support SIP Trunking - Issue 1.0**

#### Abstract

These Application Notes describe the procedures for configuring Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager.

Sipera IPCS 310 is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via a SIP trunk across an untrusted network.

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

## 1. Introduction

These Application Notes describe the procedures for configuring Sipera IPCS 310 with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

Sipera IPCS 310 is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via a SIP trunk across an untrusted network.

#### 1.1. Configuration

**Figure 1** illustrates the test configuration. The test configuration shows two enterprise sites connected via a SIP trunk across an untrusted IP network. Site 1 has a Juniper Networks Netscreen-50 firewall at the edge of the network restricting unwanted traffic between the untrusted network and the enterprise. Also connected to the edge of site 1 is an IPCS 310. The public side of IPCS is connected to the untrusted network and the private side is connected to the trusted corporate LAN. IPCS could also reside in the demilitarized zone (DMZ) of the enterprise but this configuration was not tested.

All SIP traffic between the sites flows through IPCS. In this manner, IPCS can protect the infrastructure at site 1 from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams. All non-SIP traffic bypasses IPCS and flows directly between the untrusted network to the private LAN of the enterprise if permitted by the firewall.

Located at site 1 on the private LAN side of the firewall is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include Avaya 4600 Series IP Telephones (with SIP and H.323 firmware), Avaya 9600 Series IP Telephones (with SIP and H.323 firmware), an Avaya one-X Desktop Edition, an Avaya 6408D Digital Telephone, and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. The PSTN numbers assigned to the ISDN-PRI trunk at site 1 is mapped to telephone extensions at site 1. There are two Windows PCs on site; one is used as a TFTP/HTTP server and the other is used to manage IPCS.

Located at site 2 on the private LAN side of the firewall is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G350 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include Avaya 4600 Series IP Telephones (with SIP and H.323 firmware), an Avaya 9600 Series IP Telephone (with SIP firmware), and an Avaya one-X Desktop Edition. It also has a TFTP/HTTP server.

The Avaya 4600 and 9600 Series IP Telephones (with SIP firmware) located at both sites are registered to the local Avaya SES. Each enterprise has a separate SIP domain: business.com for site 1 and dev4.com for site 2. SIP telephones at both sites use the local TFTP/HTTP server to obtain their configuration files.

All calls originating from Avaya Communication Manager at site 1 and destined for site 2 will be routed through the on-site Avaya SES to the on-site IPCS and from IPCS to the untrusted IP network. Once across the untrusted network, the call is routed to site 2's Avaya SES and finally to Avaya Communication Manager. Calls from the site 2 to site 1 follow this same path in the reverse order.



Figure 1: IPCS 310 Test Configuration

Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved.

## 2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server (site 1)	Avaya Communication Manager 5.0
	Service Pack (00.0.825.4-15175)
	with Avaya IA 770 Intuity Audix
Avaya G700 Media Gateway (site 1)	27.26.0
Avaya SIP Enablement Services (site 1)	5.0 SP2d
Avaya S8300 Server (site 2)	Avaya Communication Manager 4.0.1
	Service Pack (00.01.731.2-14300)
	with Avaya IA 770 Intuity Audix
Avaya G350 Media Gateway (site 2)	26.33.0
Avaya SIP Enablement Services (site 2)	4.0
Avaya 4621SW IP Telephone (H.323)	2.8.3
Avaya 4625SW IP Telephone (H.323)	
Avaya 4610SW IP Telephone (SIP)	2.2.2
Avaya 4620SW IP Telephone (SIP)	
Avaya 9620 IP Telephone (H.323)	Avaya one-X Deskphone Edition 1.5
Avaya 9630 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP
Avaya 9640 IP Telephones (SIP)	2.0.3
Avaya one-X Desktop Edition (SIP)	2.1 Service Pack 2
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (Management PC and	Windows XP Professional SP2
TFTP/HTTP Server)	
Juniper Networks Netscreen 50	5.4.0r9.0
Sipera IPCS 310	3.6 (Build Q.41)

## 3. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration at site 1 to support the network shown in **Figure 1**. It assumes the procedures necessary to support SIP and connectivity to Avaya SES have been performed as described in [3]. It also assumes that an off-PBX station (OPS) has been configured on Avaya Communication Manager for each SIP endpoint in the configuration as described in [3] and [4].

This section is divided into two parts. **Section 3.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations from the standard procedures, if any.

**Section 3.2** will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with IPCS. It will describe the SIP connection used by Avaya Communication Manager to route calls to Avaya SES bound for site 2.

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

This configuration must be repeated for Avaya Communication Manager at site 2 using values appropriate for site 2 from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

#### 3.1. Summary of Initial SIP Installation

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description
1.	IP network region
	The Avaya S8300 Server, Avaya SES and IP (H.323/SIP) endpoints were located in a
	single IP network region (IP network region 1) using the parameters described below.
	Use the <b>display ip-network-region</b> command to view these settings. The example
	below shows the values used for the compliance test.
	• The <b>Authoritative Domain</b> field was configured to match the domain name
	configured on Avava SES. In this configuration, the domain name is
	business.com. This name appears in the "From" header of SIP messages
	originating from this IP region.
	<ul> <li>A descriptive name was entered for the Name field</li> </ul>
	<ul> <li><b>IP-IP Direct Audio</b> (shuffling) was enabled to allow audio traffic to be sent</li> </ul>
	directly between IP endpoints without using media resources in the Avava Media
	Gateway This was done for both intra-region and inter-region IP-IP Direct Audio
	This is the default setting. Shuffling can be further restricted at the trunk level on
	the Signaling Crown form
	The Cadea Set field was set to the ID and a set to be used for calls within this ID
	- The Could Set field was set to the IP codec set to be used for calls within this IP
	network region. In this case, IP codec set I was selected. If different IP network
	regions are used for the Avaya S8500 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.
	• The default values were used for all other fields.
	display ip-network-region 1 Page 1 of 19 IP NETWORK REGION
	Region: 1
	Location: Authoritative Domain: business.com
	MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes
	Codec Set: 1 Inter-region IP-IP Direct Audio: yes
	UDP Port Max: 3329
	DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y
	Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46 Use Default Server Parameters? v
	Video PHB Value: 26
	802.1P/Q PARAMETERS
	Audio 802.1p Priority: 6
	Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS
	H.323 IP ENDPOINTS RSVP Enabled? n H.323 Link Bounce Recovery? v
	Idle Traffic Interval (sec): 20
	Keep-Alive Interval (sec): 5
	Keep-Alive Count. 5

Step	Description
2.	<b>Codecs</b> IP codec set 1 was used for the compliance test. Multiple codecs were listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The list includes 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. It should be noted that when testing the use of each individual codec, only the codec under test was included in the list.
	display ip-codec-set 1 Page 1 of 2
	IP Codec Set
	Codec Set: 1
	Audio Silence Frames Packet
	1: G.711MU n 2 20
	2: G.729A n 2 20

2	Description
2.	<ul> <li>Signaling Group For the compliance test, signaling group 1 was used for the signaling group associated with the SIP trunk group between Avaya Communication Manager and Avaya SES. Signaling group 1 was configured using the parameters highlighted below. All other fields were set as described in [3]. <ul> <li>The Group Type was set to <i>sip</i>.</li> <li>The Transport Method was set to the recommended default value of <i>tls</i> (Transpor Layer Security). As a result, the Near-end Listen Port and Far-end Listen Port are automatically set to <i>5061</i>.</li> <li>The Near-end Node Name was set to <i>procr</i>. This node name maps to the IP address of the Avaya Server. Node names are defined using the change node- names ip command.</li> <li>The Far-end Node Name was set to <i>SES</i>. This node name maps to the IP address of Avaya SES as defined using the change node-names ip command.</li> <li>The Far-end Network Region was set to 1. This is the IP network region which contains Avaya SES.</li> <li>The Far-end Domain was set to <i>business.com</i>. This is the domain configured on Avaya SES. This domain is sent in the "To" header of SIP INVITE messages for calls using this signaling group.</li> <li>Direct IP-IP Audio Connections was set to <i>y</i>. This field must be set to <i>y</i> to enable media shuffing on the SIP trunk</li> </ul></li></ul>
	<ul> <li>The DTMF over IP field was set to the default value of <i>rtp-payload</i>. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833.</li> <li>The default values were used for all other fields.</li> </ul>
	<ul> <li>The DTMF over IP field was set to the default value of <i>rtp-payload</i>. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833.</li> <li>The default values were used for all other fields.</li> <li>display signaling-group 1         <pre>SIGNALING GROUP Group Number: 1</pre>     Group Type: sip</li></ul>
	<ul> <li>The DTMF over IP field was set to the default value of <i>rtp-payload</i>. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833.</li> <li>The default values were used for all other fields.</li> <li>display signaling-group 1</li></ul>

1	Description
+.	<b>Trunk Group</b> For the compliance test, trunk group 1 was used for the SIP trunk group between Avaya Communication Manager and Avaya SES. Trunk group 1 was configured usin the parameters highlighted below. All other fields were set as described in [3].
	<ul> <li>On Page 1:</li> <li>The Group Type field was set to <i>sip</i>.</li> <li>A descriptive name was entered for the Group Name.</li> <li>An available trunk access code (TAC) that was consistent with the existing dial plan was entered in the TAC field.</li> <li>The Service Type field was set to <i>tie</i>.</li> <li>The Signaling Group was set to the signaling group shown in the previous step.</li> <li>The Number of Members field contained the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the</li> </ul>
	<ul> <li>configuration. 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.</li> <li>The default values were used for all other fields.</li> </ul>
	<ul> <li>configuration. 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.</li> <li>The default values were used for all other fields.</li> </ul>

Step	Description						
5.	Trunk Group – continued						
	On Page 3:						
	• The Numbering Format field was set to <i>public</i> . This field specifies the format of						
	the calling party number sent to the far-end.						
	<ul> <li>The default values were used for all other fields.</li> </ul>						
	display trunk-group 1 Page 3 of 21 TRUNK FEATURES						
	ACA Assignment? n Measured: none Maintenance Tests? y						
	Numbering Format, public						
	UUI Treatment: service-provider						
	Replace Restricted Numbers? n Replace Unavailable Numbers? n						
	Show ANSWERED BY on Display? y						
6.	Public Unknown Numbering						
	Public unknown numbering defines the calling party number to be sent to the far-end.						
	An entry was created that will be used by the trunk group defined in <b>Step 4</b> . In the						
	example shown below, all calls originating from a 5-digit extension beginning with 6						
	and routed across any trunk group ( <b>Trk Grp</b> column is blank) will be sent as a 5-digit						
	calling number. This calling party number is sent to the far-end in the SIP "From"						
	header.						
1							
	display public-unknown-numbering 0 Page 1 of 2 NUMBERING - PUBLIC/UNKNOWN FORMAT						
	Total						
	Ext Ext Trk CPN CPN Len Code Grp(s) Prefix Len						
	Total Administered: 1						
	<b>5 6 5</b> Maximum Entries: 9999						

#### 3.2. Configure SIP Trunk and Routing to Site 2

To communicate to site 2, a second SIP trunk with the appropriate call routing must be configured on Avaya Communication Manager. This SIP trunk will be used to route SIP calls to Avaya SES that are destined the SIP domain at site 2.

Step	Description
1.	<b>Signaling Group</b> Create a new SIP signaling group using the <b>add signaling-group</b> <i>n</i> command where <i>n</i> is the number of an unused signaling group. Use the same parameters as shown in <b>Section 3.1</b> , <b>Step 3</b> with the following exception. Set the <b>Far-end Domain</b> field to the SIP domain of site 2. The compliance test used signaling group 12 as shown below.
	add signaling-group 12 Page 1 of 1 SIGNALING GROUP
	Group Number: 12 Group Type: sip Transport Method: tls
	Near-end Node Name: procr Near-end Listen Port: 5061 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Domain: dev4.com
	Bypass If IP Threshold Exceeded? n
	DTMF over IP: rtp-payload Direct IP-IP Audio Connections? y IP Audio Hairpinning? n Session Establishment Timer(min): 3
2.	<ul> <li>Trunk Group</li> <li>Create a new trunk group using the add trunk-group <i>n</i> command where <i>n</i> is the number of an unused trunk group. Use the same parameters as shown in Section 3.1, Steps 4 - 5 with the following exceptions. Use unique values for the Group Name and TAC fields. Set the Signaling Group field to the signaling group number created in the previous step. The compliance test used trunk group 12 with the following values.</li> <li>Group Name: <i>Sipera</i></li> <li>TAC: <i>112</i></li> <li>Signaling Group: <i>12</i></li> </ul>

Step		Description	
3.	Public Unknown Numbering		
	Public unknown numbering def	ines the calling party number to be sen	t to the far-end.
	The entry created in Section 3.1	, Step 6 applies to all trunks since the	Trk Grp
	column was left blank. Thus, a	separate entry does not need to be crea	ted for this new
	SIP trunk. Based on the previou	is entry, all calls originating from a 5-	ligit extension
	beginning with 6 will be sent as	a 5-digit calling number. This calling	party number is
	sent to the far-end in the SIP "F	rom" header	purty number is
	some to the full one in the Shi fi	ioni neuder.	
4	Route Pattern		
	Create a route pattern for use by	Automatic Alternate Routing $(AAR)$	when routing
	calls to site 2	Automatic Automatic Routing (AMR)	when routing
	calls to site 2.		
	Use the abange route pottern	a command where a is the number of	on unused route
	Use the change foute-pattern /	n command, where $n$ is the number of	Crim Na field to
	pattern. Enter a descriptive nam	e for the <b>Pattern Name</b> field. Set the	Grp No field to
	the trunk group number created	in Step 2. Set the Facility Restriction	Level (FRL)
	field to a level that allows acces	s to this trunk for all users that require	it. The value of
	<b>0</b> is the least restrictive level. T	he default values may be retained for a	all other fields.
	change route-pattern 6	Page	1 of 3
	Pattern Nur	mber: 6 Pattern Name: Site2SES	
	Grp FRI, NPA Pfx Hop Toll N	CCAN? n Secure SIP? n o. Inserted	DCS/ IXC
	No Mrk Lmt List D	el Digits	QSIG
	D	gts	Intw
	$\begin{array}{c} 1: 12  0 \\ 2 \end{array}$		n user
	3:		n user
	4:		n user
	5:		n user
	6:		n user
	BCC VALUE TSC CA-TSC	ITC BCIE Service/Feature PARM No. Numb	pering LAR
	0 1 2 M 4 W Request	Dgts Form	nat
	1	Subaddress	none
	2: v v v v n n	rest	none
	3: y y y y y n n	rest	none
	4: yyyyyn n	rest	none
	5: yyyyyn n	rest	none
	6: уууууп п	rest	none

tep	Description							
5.	Use the change aar ana	lysis 4	comr	nand to a	dd an e	ntry in	the AAR Digit Analysis	
	Table for the dialed strip	ng hegir	nning	with 4 si	nce all	extens	ions at site 2 begin with a 4	
	In the exemple shown in	umbor	that	bogin wit	h 1 on	l oro 5	digita long use route nottern	
	In the example shown, in	In the example shown, numbers that begin with 4 and are 5 digits long use route pattern						
	<b>6</b> . Route pattern 6 route	6. Route pattern 6 routes calls from site 1 to site 2 via the second SIP trunk with the						
	far-end domain set to the	e SIP de	omaiı	n of site 2	(dev4	com)		
	fur end domain set to the		Jinan	1 01 5100 2	(uev 1.	comj.		
	change aar analysis 4						Page 1 of 2	
		A	AR DI	GIT ANALYS	SIS TAB	LE		
							Percent Full: 3	
	Dialed	Tot	al	Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
	4	5	5	6	aar		n	
	5	7	7	254	aar		n	
	5							
	6	7	7	254	aar		n	
	6 7	7 7 7	7 7	254 254	aar aar		n n	
	6 7 8	7 7 7 7	7 7 7	254 254 254	aar aar aar		n n n	

# 4. Configure Avaya SIP Enablement Services

This section covers the configuration of Avaya SES at site 1. 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 that registers with Avaya SES requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of IPCS so it is not included here. These procedures are covered in [5].

This section is divided into two parts. **Section 4.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations from the standard procedures, if any.

**Section 4.2** will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with IPCS.

This configuration must be repeated for Avaya SES at site 2 using values appropriate for site 2 from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

#### 4.1. Summarize Initial Configuration Parameters

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.



Step	Description						
2.	Top Page						
	The Avaya SES <b>Top</b> page will be displayed as shown below.						
	AVAVA Integrated Management						
	Help Exit Server: 10.75.5.6						
	Top Users Top						
	Address Map Priorities  Address Manage Users  Add and delete Users.						
	Certificate Management     Manage Address Map Adjust Address Map Priorities.     Priorities						
	Conferences     Manage Adjunct     Add and delete Adjunct Systems.     Systems						
	Export/Import to ProVision Certificate Manage Certificates.						
	IM logs Manage Conferencing Add and delete Conference Extensions.						
	Media Servers     Manage Emergency     Contacts     Add and delete Emergency     Contacts.						
	Server Configuration SIP Phone Settings ProVision SIP Phone Settings						
	Survivable Call Processors     System Status     System Status						
	Trace Logger     IM logs     Download IM Logs.						
	Trusted Hosts     Manage Media     Add and delete Media Servers.     Servers						
	Manage Media Server Add and delete Media Server						
5.	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 group of parameters is a brief description of how to view the values for that group from the Avaya SES administration home page shown in the previous step.						
	• SIP Domain: <i>business.com</i> (To view, navigate to Server Configuration→System Parameters)						
	<ul> <li>Host IP Address (SES IP address): 10.75.5.6</li> <li>Host Type: SES combined home-edge (To view, navigate to Host→List; click Edit)</li> </ul>						
	<ul> <li>Media Server (Avaya Communication Manager) Interface Name: <i>CMeast</i></li> <li>SIP Trunk Link Type: <i>TLS</i></li> <li>SIP Trunk IP Address (Avaya S8300 Server IP address): <i>10.75.5.2</i> (To view, navigate to Media Server→List; click Edit)</li> </ul>						

#### 4.2. IPCS Specific Configuration

This section describes additional Avaya SES configuration necessary for interoperating with IPCS.

Step	Description
1.	<b>Outbound Proxy</b> Set the outbound proxy of Avaya SES to be the IPCS. When Avaya SES receives a
	call request (INVITE message) with a destination containing a foreign domain (dev4.com), Avaya SES will perform a DNS look-up on this domain. Since no DNS
	route the call to the outbound proxy (IPCS). The IPCS will then be responsible for routing the call to site 2. In addition, Avaya SES will automatically assume that the outbound proxy is a trusted host.
	In the case of site 2 which does not have a local IPCS, set the Avaya SES outbound proxy to be the public IP address of the IPCS at site 1. The IPCS at site 1 will then be responsible for routing these calls to the Avaya SES at site 1.
	To configure the proxy settings, navigate to <b>Hosts</b> $\rightarrow$ <b>Lists</b> in the left pane. In the window that appears (not shown), select the <b>Edit</b> link next to the host name of Avaya SES. In the <b>Edit Host</b> window that appears, configure the following:
	<ul> <li>Outbound Routing Allowed From: Check both <i>Internal</i> and <i>External</i>.</li> <li>Outbound Proxy: IP address of IPCS. Port field is set to 5060. Select the UDP radio button.</li> </ul>
	Edit Host
	Host IP Address* 10.75.5.6
	Profile Service Password*
	Host Type SES combined home-edge Parent none
	Listen Protocols VDP VTCP VTLS
	Policy (Default)  Allow All  Deny All Emergence
	Contacts Policy   Allow  Deny
	Registration 300 Registration Expiration Timer (seconds)* 600 (seconds)
	Line Reservation Timer (seconds) 30 *
	Outbound Routing Allowed 🕑 Internal 🕑 External From
	OutboundProxy 10.75.5.63 Port 5060 OUDP OTCP OTLS
	Outbound Direct Domains
	Default Ringer 5 Default Ringer Cadence 2 Volume*

Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved.

Step	Description				
<u> </u>	Media Server Address Map         A media server address map is needed to route calls from the remote site to a non-SIP         phone at the local site. This is because neither the caller nor the called party is a         registered user on the local Avaya SES with a media server extension assigned to it.         Thus, Avaya SES does not know to route this call to Avaya Communication Manager.         Thus to accomplish this task, a media server address map is needed.         To view the configured media server address maps, navigate to Media Server→List in         the left pane. In the window that appears (not shown), click the Map link next to the         Avaya S8300 Server name. The list of media server address maps will appear. Each         map defines criteria for matching calls to Avaya SES based on the contents of the SIP         Request URL of the call. If a call matches the map, then the call is directed to the				
	<b>Contact</b> . In the example below, three maps are shown. Only the map named <i>ToMainCM</i> was used for the compliance test. This map were associated to a <b>Contact</b> that directs the calls to the IP address of the Avaya S8300 Server ( <i>10.75.5.2</i> ) using port <i>5061</i> and <i>TLS</i> as the transport protocol. The user portion in the original request URI is substituted for $\$(user)$ in the <b>Contact</b> expression shown below.				
	<pre>sip:\$(user)@10.75.5.2:5061;transport=tls To view or edit the call matching criteria of the map, click the Edit link next to the map name.</pre>				
	List Media Server Address Map				
	Commands Name Commands Contact				
1	Edit Delete ToCM-11digit				
	Edit Delete ToMainCM				
	Edit Delete ToPSTN				
	Edit Delete sip:\$(user)@10.75.5.2:5061;transport=tls				
	Add Another Map Add Another Contact Delete Group				
Add Map In New Group					

Step	Description				
3.	Media Server Address Map – continued				
	The content of the media server address map is described below.				
	Name: Contains any descriptive name				
	<ul> <li>Pattern: Contains an expression to define the matching criteria for calls to be routed from the remote site to the local Avaya Communication Manager. For the address map named <i>ToMainCM</i>, the expression will match any URI that begins with <i>sip:3</i> followed by any digit between <i>0-9</i> for the next <i>4</i> digits. Additional information on the syntax used for address map patterns can be found in [5].</li> <li>Replace URI: Check the box.</li> </ul>				
	If any changes are made, click <b>Update</b> .				
	Edit Media Server Map Entry				
	Name* ToMainCM				
	Pattern*				
	Fields marked * are required				
	Fleius markeu - are requireu.				
	Update				
	Update				

## 5. Configure the Avaya SIP Telephones

The SIP telephones at each site will use the local Avaya SES as the call server. The table below shows an example of the SIP telephone network settings for each site.

	Site 1	Site 2
Extension	30107	40102
IP Address	10.75.5.161	50.1.1.160
Subnet Mask	255.255.255.0	255.255.255.0
Router	10.75.5.1	50.1.1.254
File Server	10.75.10.100	50.1.1.52
DNS Server	0.0.0.0	0.0.0.0
SIP Domain	business.com	dev4.com
Call Server or SIP	10.75.5.6	50.1.1.50
Proxy Server		

## 6. Configure Sipera IPCS

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

)	Description	
	IPCS is configured via the Mozilla Firefox web browser. IPCS does not support	
	Internet Explorer. To access the web interface, enter <u>https://<ip-addr>/ipcs</ip-addr></u> in the	
	address field of the web browser, where <i><ip-addr></ip-addr></i> is the IP address of IPCS.	
	Log in with the appropriate credentials. Click Sign In.	
	🕲 IPCS Web Control Center - Mozilla Firefox	
	Elle Edit View History Bookmarks Yahoo! Tools Help	<>
	🖕 • 🗼 • 🕑 🛞 🏠 🕞 https://192.168.1.63/ipcs/ 🔗 • 🍉 💽 • Google	Q
	Customize Links 🗋 Free Hotmail 🗋 Windows Marketplace 🗋 Windows Media 📄 Windows	
	Y 🕐 🔹 💽 🔹 💽 💽 Search Web 🔹 🖗 🗸 🔯 Mail 🗸 🎯 My Yahoo! 🌾 NCAA Hoops 🔹 👰 Fantasy Sports 🔹 📥 Games	* »>
	Google - 💽 🖗 G Search + 🧭 PageRank 🕸 Check + 👯 AutoLink 😨 AutoFill 🔝 Subscribe + »	
	Sign In Later - VERY - PROTECT  Sign in  The IPCS T <sup>M</sup> family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of informat security and by using unique	100.
	security by adapting the best practices of internet security and by during unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks. Visit the Sipera Systems website to learn more.	
	NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.	~
		0

Step			Descriptio	n		
2.	The main page of t	he IPCS Contro	ol Center will a	appear.		
	Ŧ					
	IPCS Control Cent Welcome ipcs, you signed in as Adm	er in. Current server time is 9:19:17	АМ БМТ		9	) Sipera
	Alarms Incidents	Statistics E	ogs 🕴 🛃 Diagnostics	Users	🛃 Logout 🛛 💡 He	lp 🚹 <u>A</u> bout
	IPCS Control Center      Swelcome	Securing your rea	al-time unified comn	nunications		
	Administration	A comprehensive IP Co offers a complete suite protecting and deploying instant messaging (IM),	mmunications Security (IPC of security, enablement and g unified communications s multimedia, and collaboral	CS) product, the Sipera IPCS I compliance features for such as Voice-over-IP (VoIP), tion applications.	Quick I Sipera Website Sipera VIPER Labs Contact Support	Links
	Global Profiles	If you need support, plea support@sipera.com.	ase call our toll free numbe	r at (866) 861-3113 or e-mail	contact support	
	Bright Domain Policies	Alarms (Past 24 None found.	Hours) In None f	cidents (Past 24 Hours) ound.	IPCS Devices Avaya	Network Type DMZ_ONLY
			Administrator Notes No notes posted.	[ <u>Add</u> ]		
		1	Annual Contraction			
3.	To view system inf IPCS Control Cer	formation that v nter→Svstem N	vas configured Management.	during installat A list of install	ion, navigate ed devices is	to shown in
	the right pane. In the	ne case of the co	ompliance test	, a single device	named Avay	<i>a</i> is
	shown. To view the	e configuration	of this device,	click the monit	or icon highli	ghted
	below.					
	IPCS Control Cente	r			6	Sinera
	Welcome ipcs, you signed in as Admin	Current server time is 9:22:37 AM	GMT	Susers	Logout 2 H	Systems
	IPCS Control Center	IPCS Control Center > System Ma	anagement	20010	Testor V	orb
	S Welcome	Installed Updates				
			3			Add Device
	Global Parameters     Global Profiles	Device Name Avaya	Serial Number	Version Status 3.6.0.Q41 (Commissi	oned 🔚 🔣 🔯	<b>■</b> 🔮 🖉 🗙
	Domain Policies     Device Specific Settings					
	TLS Management					
1						

Step		D	escription			
4.	The <b>System Informatio</b> and <b>Management IP</b> in <b>Figure 1</b> . Only the first the compliance test. Th required by IPCS. An a <b>Box Type</b> was set to <b>SL</b> were used for all other f	on screen shows formation provi two entries in t e compliance te rbitrary IP addre <i>P</i> and the <b>Deplo</b> fields.	the Network Setti ded during installat he Network Settin st did not use a DN ess was used for the yment Mode was	ings, DNS C tion and cor ogs list below S server, bu e Primary I set to <i>Proxy</i>	Configuration responds to w were used for at an entry was DNS field. The b. Default values	
		System	Information: Avaya		×	
		Netw	ork Configuration			
	General Settings		Device Settings			
	Appliance Name	Avaya	HA Mode	NO		
	Box Type	SIP	Secure Channel Mo	ode NONE		
	Deployment Mode	Deployment Mode Proxy			i	
	-Network Settings					
	IP	Public IP	Netmask	Gateway	Interface	
	46.14.2.13	46.14.2.13	255.255.255.0	46.14.2.1	B2	
	10.75.5.63	10.75.5.63	255.255.255.0	10.75.5.1	A2	
	46.14.2.10	46.14.2.10	255.255.255.0	46.14.2.1	B2	
	10.75.5.64	10.75.5.64	255.255.255.0	255.255.255.0 10.75.5.1 A2		
	-DNS Configuration					
	Primary DNS	192.168.1.62	IP	192.168.1	192.168.1.63	
	Secondary DNS					
	DNS Location	MANAGEMENT				



Step		Description					
6.	Media Interface A media interface maps a medi that can be used on that interface	a interface name to ce.	an IP address	s and a range of	f ports		
	A media interface is created similar to a signaling interface by navigate to <b>IPCS</b> <b>Control Center→Device Specific Settings→Media Interface</b> .						
	The example below shows four <i>Server</i> were used for the compliant interface of IPCS and the <i>Serve</i>	r interfaces. Only the liance test. The <b>Pho</b> for interface maps to	ne interfaces n pne interface n o the private in	amed <i>Phone</i> an maps to the pub nterface.	nd blic		
	IPCS Control Center         Welcome (pcs, you signed in as Admin, Current server time is *         Alarms       Incidents       Statistics         IPCS Control Center       IPCS Control Center       IPCS Control Center         Statistics       IPCS Devices       IPCS Devices	11:03:00 AM GMT Logs Diagnostics Device Specific Settings > Media Interfac Media Interface	Users De: Avaya	S Logout  🧿 Help	Sipera Systems		
	Backup/Restore     Avaya     System Management     Global Parameters	Name	Media IP	Add Me	dia Interface		
	Global Profiles     E	Phone Server	46.14.2.13	56000 - 60000 56000 - 60000	2 X		
	Device Specific Settings      Device Management      Device Flows	SoftPhone Soft-Int	46.14.2.10 10.75.5.64	56000 - 60000 56000 - 60000	0 × 0 ×		
	Session Flows     Solution     Signaling Interface     Signaling Interface     Trace Settings						

Step	Description				
7.	Server Definition - Gen	eral			
	A server configuration pr	ofile is created to define the chara	cteristics of a server to		
	which the IPCS will com	municate			
		indificute.			
	To define a new server co	onfiguration profile, navigate to II	CS Control		
	Center→Global Profile	s→Server Configuration. Select	the Add Profile button in		
	the middle pane to enter a	and submit the new information.			
	The first screen below sh	ows the server configuration profi	le named <i>Avava</i> used to		
	represent the local Avaya	SFS The General tab shows the	Server Type as <i>Call</i>		
	Server and the ID address	r = 100000000000000000000000000000000000	in the ID		
	Server and the IP address	s of the local Avaya SES (10.75.5.	o) in the IP		
	Addresses/FQDNs field.	. The remaining fields show the tr	ansport protocols and ports		
	supported for traffic betw	veen IPCS and Avaya SES.			
	The second screen shows	the server configuration profile n	amed <i>Trunk</i> used to		
	represent the remote Ava	va SES The General tab shows t	he Server Type as <i>Trunk</i>		
	Server and the ID address	a of the remote A years SES (50.1.1	50) in the ID		
	Server and the IP address	s of the femole Avaya SES (SU.1.1	.50) in the <b>IP</b>		
	Addresses/FQDNs field.				
	IPCS Control Center		Sipera 🔊		
	Welcome ipcs, you signed in as Admin. Current serve	r time is 9:48:21 AM GMT	Systems		
	Alarms Incidents In Statistic	s Eogs Eigenstics Eigenstics Center > Global Profiles > Server Configuration: Avaya	Logout 🦉 Help 🚺 About		
	IPCS Control Center      Sector Velcome	Add Profile	Rename Profile Clone Profile Delete Profile		
	Administration P	rofile General Authentication Heartbeat Advance	d		
	Backup/Restore	Ge	neral		
	System Management Avaya	Server Type Cal	I Server		
	Global Profiles	IP Addresses / FQDNs 10.	75.5.6		
	- Domain DoS	Supported Transports TCI	P, UDP		
	- Fingerprint	UDP Port 500	0		
	Routing		dit		
	Server Configuration				
	Topology Hiding				
	URI Groups				
	Device Specific Settings				
	E Cara TLS Management				
	· · · · · · · · · · · · · · · · · · ·				
	IPCS Control Center		Sinera		
	Welcome ipcs, you signed in as Admin. Current server tim	ie is 10:22:25 AM GMT	Systems		
	Alarms Incidents In Statistics	ter > Global Profiles > Server Configuration: Trunk	🛃 Logout 🛛 🦉 <u>H</u> elp 🚺 <u>A</u> bout		
	₩elcome	Add Profile	Rename Profile Clone Profile Delete Profile		
	- 🤱 Administration Pro	file General Authentication Heartbeat Advanced			
	Backup/Restore Trunk	Gen	eral		
	B Global Parameters	Server Type Trun	k Server		
	Global Profiles	IP Addresses / FQDNs 50.1 Supported Transports TCP	1.50 UDP		
	Finderwint	TCP Port 5060			
	There working	UDP Port 5060			
	Routing	E	lit		
		L			
	RI Groups				
			_		

Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved.

26 of 37 Sipera310CM5Trk



Step			Desc	ription			
9.	Server - Topolo	gy Hiding Pro	ofile				
	A topology hidir	ig profile defin	es how the	manipula	ation of IP add	resses and dom	nains is
	to be applied to S	SIP messages f	or traffic b	etween IF	CS and the set	rver.	
	To define a new	topology hidin	g profile, n	avigate to	o IPCS Contro	ol Center <b>→</b> Gl	obal
	Profiles→Topol	ogy Hiding. S	Select the A	dd Profi	le button in the	e middle pane	to enter
	and submit the n	ew information	1.				
	In the example b	elow, three pro	ofiles are sh	own in th	ne middle pane	e. Only the prof	files
	named Callserve	<b>r</b> and <b>Trunk</b> w	vere used for	or the con	pliance test. T	The Callserver	profile
	was used by the	Avaya server a	nd the Tru	<b>nk</b> profile	e was used by t	the <i>Trunk</i> serv	er. By
	highlighting a pr	ofile in the mid	ldle pane, i	ts details	are shown in t	he right pane.	To see
	the details of a ru	ale, click the pe	encil icon a	ssociated	with the rule of	of interest in th	e right
	pane.						
						$\sim$	
	IPCS Control Cent Welcome ipcs, you signed in as Admin	<b>e r</b> h. Current server time is <b>10:21:32 AM</b>	1 GMT			9	Sipera
	Alarms Incidents	Statistics Eogs	Diagnostics	📓 Users		🛃 Logout   🧿 Help	About
	IPCS Control Center	<ul> <li>IPCS Control Center &gt; Global Prof.</li> <li>Add Profile</li> </ul>	iles > Topology Hiding: Calls	erver		Rename Profile Clone Profile	Delete Profile
		Topology Hiding Profiles			Click here to add a descript	tion.	
	Backup/Restore	Trunk	Topology Hiding				
	🕀 🧰 Global Parameters	OnexMobile					Add Rule
	Global Profiles		Priority	From URI Group	User Type	Direction	
	- Fingerprint		1 *		Trunk User	To Call Server	.0
	Routing		87				
	Carles Server Configuration						
	- A URI Groups						
	🕀 🧰 Domain Policies						
	IRCS Control Cont						Sinora
	Welcome ipcs, you signed in as Admir	e r n. Current server time is 10:20:53 AN	I GMT				Sipera
	Alarms Incidents	Statistics     End Logs     IPCS Control Center > Global Profi	Diagnostics les > Topology Hiding: Trun	Users		🛃 Logout 🛛 😲 Help	About
	S Welcome	Add Profile				Rename Profile Clone Profile	Delete Profile
	Administration	Topology Hiding Profiles			Click here to add a descript	ion.	
	System Management	Callserver	Topology Hiding				
	Global Parameters     Global Profiles	OnexMobile	a				Add Rule
	Domain DoS		Priority *	From URI Group	User Type	Direction	
	Fingerprint				Trank Oser	From Call Server	
	Routing		10				1
	- 📇 Server Configuration						
	URI Groups						
	Louistenti Denesie Belisius						

Step		Description						
10.	Server - Topology Hiding Pr The topology hiding profile na the SIP messages from the rem is set to match on anything (Fu User and the Direction field is local Avaya SES, all external so overwritten with the private IP unchanged.	ofile - Continued amed <i>CallServer</i> was created to note Avaya SES to the local A com URI Group = *), the Use a set to <i>To Call Server</i> . Befor source IP addresses from the r address of IPCS and the sour	to modify IP addresses in avaya SES. Thus, the URI er <b>Type</b> is set to <b>Trunk</b> e sending messages to the remote Avaya SES will be erce domains will be left					
	Edit Topology Hiding Profile							
	Replacement Settings							
	From URI Group	From URI Group *						
	User Type	User Type 🔅 Remote User 💿 Trunk User						
	Direction	💿 To Call Server 🔿 From Call Serve	r 🗤					
	Replace Source IPs	Overwrite 💌	10.75.5.63					
	Replace Destination IPs	Next hop routing entity						
	Replace Source Domains	No Modification 😪						
	Replace Destination Domains	Next hop routing entity						
	Replace SDP IPs	Signaling Interface IP/Domain 👻						
	Replace Routing SIP Headers	Signaling Interface IP/Domain 💌						
	Replace Routing SDP Headers	Signaling Interface IP/Domain 💌						
		Finish						

11.	Server - Topology Hiding Prof The topology hiding profile nam SIP messages from the local Av to match on anything (From UP the Direction field is set to From Average SES, all sources ID address	file - Continued ned <i>Trunk</i> was created to me aya SES to the remote Avay <b>RI Group</b> = *), the User Typ <i>m Call Server</i> . Before sendi	odify IP addresses in the a SES. Thus, the URI is set <b>be</b> is set to <i>Trunk User</i> and
	The topology hiding profile nam SIP messages from the local Av to match on anything ( <b>From UF</b> the <b>Direction</b> field is set to <i>From</i> Average SES, all sources ID address	ned <i>Trunk</i> was created to me aya SES to the remote Avay <b>RI Group</b> = *), the <b>User Tyj</b> <i>m Call Server</i> . Before sendi	odify IP addresses in the a SES. Thus, the URI is set be is set to <i>Trunk User</i> and
	SIP messages from the local Av to match on anything ( <b>From UF</b> the <b>Direction</b> field is set to <i>From</i> Average SES, all sources ID address	aya SES to the remote Avay <b>RI Group</b> = *), the <b>User Tyj</b> <i>m Call Server</i> . Before sendi	a SES. Thus, the URI is set <b>be</b> is set to <i>Trunk User</i> and
	to match on anything (From UF the <b>Direction</b> field is set to <i>From</i>	<b>RI</b> Group = *), the User Tyj <i>m Call Server</i> . Before sendi	be is set to <i>Trunk User</i> and
1	A vove SES, all source ID address	<i>m Call Server</i> . Before senal	
		and from the local Arraya ST	ng messages to the remote
	Avaya SES, all source IF address of IPCS the	ses from the local Avaya SE be destination IP addresses w	yill be overwritten with the
	IP address of the remote Avava	SES, the source domains wi	Il be set to the signaling
	interface IP which results in the	domain being overwritten w	with the public IP address of
	IPCS (see Step 5) and the destir	nation domain is left unchang	ged.
	· · /		·
		Edit Topology Hiding Profile	×
		Replacement Settings	
	From URI Group	*	
	∵useř туре	Tunk User 🐨 Trunk User	
	Direction	🚫 To Call Server 💿 From Call Ser	/er
	Replace Source IPs	Overwrite 💌	46.14.2.13
	Replace Destination IPs	Overwrite 💌	50.1.1.50
	Replace Source Domains	Signaling Interface IP/Domain 💌	
	Replace Destination Domains	No Modification 💌	
	Replace SDP IPs	Signaling Interface IP/Domain 💌	
	Replace Routing SIP Headers	Signaling Interface IP/Domain 💌	
	Replace Routing SDP Headers	Signaling Interface IP/Domain 💌	
		Finish	

Step			Description		
12.	Server – Interwo	orking Profile			
	An interworking	profile defines	how SIP message headers and content (other than the		
	IP addresses) may	y be manipulate	ed for interoperability with different call servers.		
			I I J		
	To define a new i	nterworking nr	ofile navigate to IPCS Control Center→Clobal		
	Profiles→Interworking. Select the Add Profile button in the middle pane to enter and submit the new information				
	In the example below, four profiles are shown in the middle pane. Only the profile				
	named <i>Remote U</i>	ser was used for	or the compliance test. By highlighting this profile in		
	the middle pane,	its details are s	hown in the right pane. On the <b>Advanced</b> tab, the		
	<b>Topology Hiding</b>	g: Change Cal	<b>I-ID</b> field was set to <i>No</i> to disable the changing of the		
	Call-ID in the SI	p messages pas	sed through the IPCS to the Avava SES. Default		
	values were used	for all other fie	alds		
	values were asea	for an other in			
			Cinoro		
	Welcome ipcs, you signed in as Adm	e r in. Current server time is 9:27:22 A	M GMT Sipera		
	🍓 Alarms 📔 Incidents 🗌	👫 Statistics 📄 📰 Log	s 🛃 Diagnostics 🕼 Users 🎒 Logout 🎯 Help 🚯 About		
	IPCS Control Center	IPCS Control Center > Global Pr Add Droffic	ofiles > Interworking: Remote User		
	- S Welcome	Interworking Profiles	Click base to add a description		
		cs2100	General Timers URI Manipulation Header Manipulation Advanced		
	- 🛅 System Management	avaya-ru			
	Global Parameters	Avaya Ru Romoto Usor	Advanced Settings		
	DoS Settings	Keniote User	Topology Hiding: Change Call-ID No		
	Secure Channel	5	Call-Info NAT No		
	Scrubber		AVAYA Extensions No		
	SIP Cluster		Edit		
	User Agents				
	🕀 🧰 Global Profiles				
	- Domain DoS				
	Interworking				
	Routing				
	- 🛃 Server Configuration	~			

Step	Description					
13.	<b>Server – Routing Profile</b> A routing profile defines how a call is to be routed. In this case, the routing profile is applied to calls from the server to IPCS.					
	To define a new routing profile, navigate to <b>IPCS Control Center</b> $\rightarrow$ <b>Global</b> <b>Profiles</b> $\rightarrow$ <b>Routing</b> . Select the <b>Add Profile</b> button in the middle pane to enter and submit the new information.					
	In the example below, three profiles are shown in the middle pane. Only the profiles named <i>Avaya</i> and <i>Trunk</i> were used for the compliance test. By highlighting a profile in the middle pane, its details are shown in the right pane.					
	The first screen below shows the routing profile named <i>Avaya</i> . It shows that all traffic ( <b>URI Group</b> = *) using this profile will be routed to IP address 10.75.5.6 (local Avaya SES) as the next hop as defined in the <b>Next Hop Server 1</b> field.					
	The second screen shows the routing profile named <i>Trunk</i> . It shows that all traffic ( <b>URI Group</b> = $*$ ) using this profile will be routed to IP address 50.1.1.50 (remote Avaya SES) as the next hop as defined in the <b>Next Hop Server 1</b> field.					
	IPCS Control Center         Welcome ipcs, you signed in as Admin. Current server time is 9:30:08 AM GMT					
	IPCS Control Center > Global Profiles > Routing: Avaya         IPCS Control Center > Global Profiles > Routing: Avaya         Welcome       Add Profile         Routing Profiles       Click here to add a description.         Backup/Restore       default         Routing Profile       Routing Profile         System Management       Avaya					
	Image: Color of Ides       Trunk         Color of Ides       Priority       URI Group       Next Hop Server 1       Next Hop Server 2       NAPTR       SRV       Outgoing Transport         Image: Trunk       Priority       URI Group       Next Hop Server 1       Next Hop Server 2       NAPTR       SRV       Outgoing Transport         Image: Routing       Routing       Image: Routing       Ima					
	IPCS Control Center         Welcome ipos, you signed in as Admin. Current server time is 10:19:57 AM GMT         Alarms       Incidents       Statistics       Loggetties					
	PCS Control Center      PCS Control Center > Clobal Profiles > Routing: Trunk     PCS Control Center > Clobal Profile > Routing: Trunk     Over      Add Profile     Add Profile     Add Profile     Add Profile     Click here to add a description.     Delete Profile     Addinistration     Gefault     Routing Profile					
	Image: System Management       Avaya         Image: System Management       Next Hop Server 1       Next Hop Server 2       NAPTR       SRV       Outgoing Transport         Image: System Management         Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       Image: System Management       <					
	Server Configuration					

Step	Description
14.	End Point Policy Groups
	An end point policy group defines a set of rules that may be applied to different aspects of the data traffic. For the compliance test, the end point policy group was used to specify if (and how) the media stream should be encrypted.
	To define a new policy group, navigate to <b>IPCS Control Center→Domain</b> <b>Policies→End Point Policy Groups</b> . Select the <b>Add Group</b> button in the middle pane to enter and submit the information.
	For the compliance test, one policy group was used. Policy group <i>default-low</i> defines the use of unencrypted media (RTP). This policy group will be used in the server flows defined in the next step.

Step	Description
15.	Server Flow
	Many of the previous steps have defined policies that will be applied to traffic if it is present. The server flow defines what traffic is actually allowed between the IPCS and the specified server, as well as which interfaces and media encryption will be used.
	To define a new server flow, navigate to <b>IPCS Control Center</b> $\rightarrow$ <b>Device Specific Settings</b> $\rightarrow$ <b>End Point Flows</b> . Select the <b>Server Flows</b> tab. Select the <b>Add Flow</b> button in the right pane to enter and submit the new information.
	The example below shows the two server flows used for the compliance test. The flow named <i>Server</i> specifies that all traffic to or from any URI Group will be allowed to the server named <i>Avaya</i> (local Avaya SES). Media traffic will use <b>Media Interface</b> – <i>Server</i> and signaling traffic will use <b>Signaling Interface</b> – <i>Server</i> . The <b>Endpoint Policy Group</b> named <i>default –low</i> ( <b>Step 14</b> ) will be applied to this traffic which specifies that the media is unencrypted. In addition, the Topology Hiding, Interworking, and Routing Profiles defined in <b>Steps 9 - 13</b> will be applied where applicable. The flow named <i>Trunk</i> specifies that all traffic to or from any URI Group will be allowed to the server named <i>Trunk</i> (remote Avaya SES). Media traffic will use <b>Media Interface</b> – <i>Phone</i> and signaling traffic will use <b>Signaling Interface</b> – <i>Phone</i> . The <b>Endpoint Policy Group</b> named <i>default –low</i> ( <b>Step 14</b> ) will be applied to this traffic will use <b>Media Interface</b> – <i>Phone</i> and signaling traffic will use <b>Signaling Interface</b> – <i>Phone</i> . The <b>Endpoint Policy Group</b> named <i>default –low</i> ( <b>Step 14</b> ) will be applied to this traffic which specifies that the media is unencrypted. In addition, the Topology Hiding, Interworking, and Routing Profiles defined in <b>Steps 9 - 13</b> will be applied to this traffic which specifies that the media is unencrypted. In addition, the Topology Hiding, Interworking, and Routing Profiles defined in <b>Steps 9 - 13</b> will be applied to this traffic which specifies that the media is unencrypted. In addition, the Topology Hiding, Interworking, and Routing Profiles defined in <b>Steps 9 - 13</b> will be applied where applicable.
	IPCS Control Center Sipera
	Welcome lpcs, you signed in as Admin. Current server time is 10:23:43 AM GMT • Systems           Alarms         Incidents
	Fingerprint     Fingerpri
	Hover over a row to see it's description.
	B Domain Policies Server Configuration: Avaya
	Priority Flow Name Group Group Interface Interface Policy Group
	Media Interface
	Priority Flow Name From Urd 1 to Urd Media Signaling End Point Trace Settings 4 Truck * Phone
	Advanced Options
	L Diamagement

# 7. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager using SIP trunking. This section covers the general test approach and the test results.

### 7.1. General Test Approach

The general test approach was to make calls between the two sites using various codec settings and exercising common PBX features.

#### 7.2. Test Results

IPCS passed compliance testing. The following features and functionality were verified.

- Successful registrations of endpoints at both sites.
- Calls from both SIP and non-SIP endpoints between sites.
- G.711u and G.729A codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, 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 an IPCS restart and loss of IP connection.

## 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 endpoints are registered with the local Avaya SES. To view, navigate to **Users**→**Registered Users**.
- Verify that calls can be placed from both SIP and non-SIP endpoints between sites.

# 9. Support

For technical support on IPCS, contact Sipera support at <u>www.sipera.com/support</u>.

## 10. Conclusion

Sipera IPCS 310 passed compliance testing. These Application Notes describe the procedures required to configure Sipera IPCS 310 to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support SIP trunking between enterprise locations as shown in **Figure 1**.

## 11. Additional References

- [1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 6.0, January 2008.
- [2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 4, January 2008.
- [3] SIP support in Avaya Communication Manager Running on the Avaya S8xxx Server, Doc # 555-245-206, Issue 8, January 2008.
- [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, Administering, Maintaining, and Troubleshooting SIP Enablement Services, Doc# 03-600768, Issue 5, January 2008.
- [6] Avaya IA 770 INTUITY AUDIX Messaging Application, Doc # 11-300532, May 2005.
- [7] *IPCS210\_310 Installation Guide* (230-5210-31).
- [8] IPCS Administration Guide (010-5310-31).

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

Product documentation for IPCS can be obtained from Sipera. Contact Sipera using the contact link at <u>http://www.sipera.com</u>.

#### ©2008 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 DevConnect Program at devconnect@avaya.com.