



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 with NAT Traversal - 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 with both near-end and far-end network address translation (NAT) traversal.

Information in these Application Notes has been obtained through DeveloperConnection compliance testing and additional technical discussions. Testing was conducted via the DeveloperConnection 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 with both near-end and far-end network address translation (NAT) traversal.

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. Both sites have a Juniper Networks Netscreen 50 firewall at the edge of the network restricting unwanted traffic between the untrusted network and the enterprise, as well as performing NAT. NAT is provided by mapping the internal host address to a static public WAN address for each server that needs to be accessed externally such as IPCS. Port address translation is not being performed at the enterprise. IPCS connects to a separate port of the firewall representing the demilitarized zone (DMZ) of the enterprise. The firewall will allow incoming SIP and RTP traffic directed to IPCS. Outbound traffic will be unrestricted.

All SIP traffic flows through IPCS at each site. In this manner, IPCS can protect the local site's infrastructure 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 the main site 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 two Avaya 4600 Series IP Telephones (with SIP firmware), 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 the main site is mapped to telephone extensions at the main site. There are two Windows PCs on site; one is used as a TFTP server and the other is used to manage IPCS.

Located at the branch site 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 two Avaya 4600 Series IP Telephones (with SIP firmware). It also has a TFTP server and a Windows PC to manage IPCS.

The Avaya 4600 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 the main site and dev4.com for the branch. SIP telephones at both sites use the local TFTP server to obtain their configuration files.

All calls originating from Avaya Communication Manager at the main site and destined for the branch will be routed through the on-site Avaya SES to the on-site IPCS via the data firewall and from IPCS to the untrusted IP network via the data firewall. Once across the untrusted network, the call enters the branch site via the data firewall located there and routed to the local IPCS. From IPCS, the call is routed to Avaya SES via the data firewall and finally to Avaya Communication Manager. Calls from the branch to the main site follow this same path in the reverse order.

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 3.1, Step 6**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.

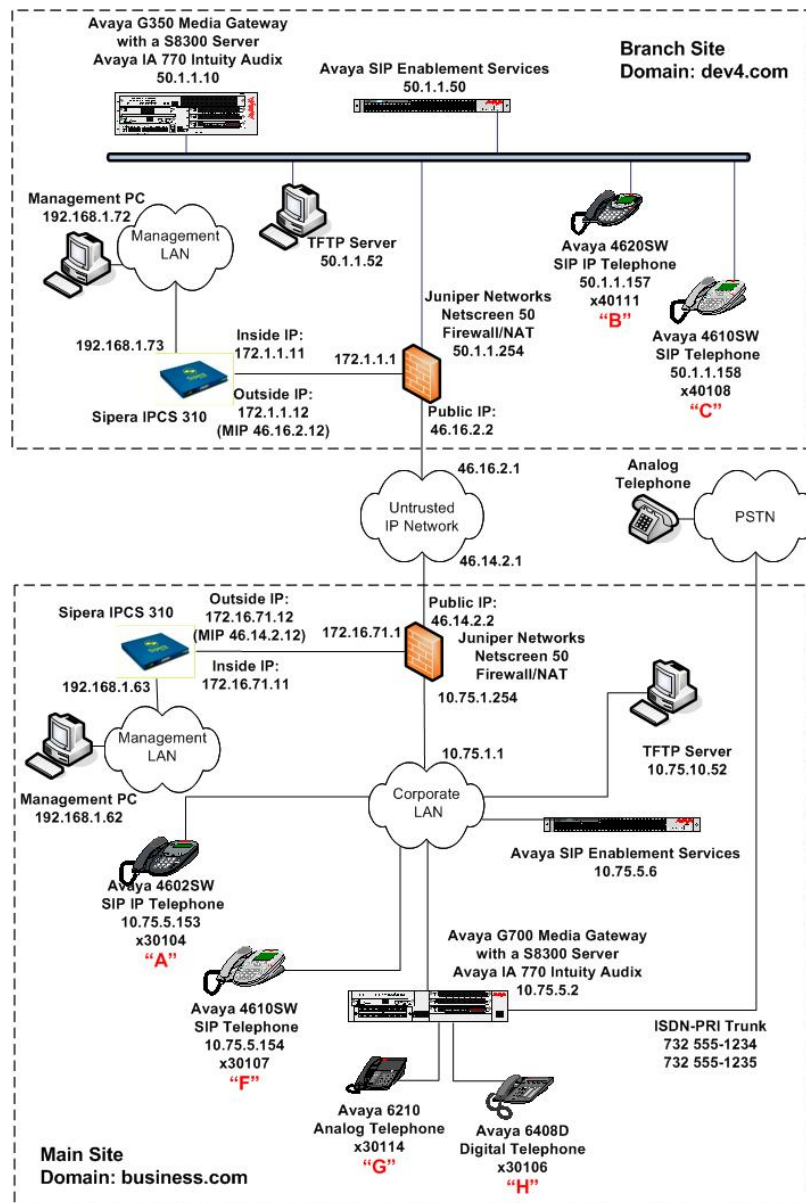


Figure 1: IPCS 310 Test Configuration

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 Gateway Avaya IA 770 Intuity Audix	Avaya Communication Manager 4.0 Service Pack (R014x.00.0.730.5-13566)
Avaya S8300 Server with Avaya G350 Media Gateway Avaya IA 770 Intuity Audix	Avaya Communication Manager 4.0 Service Pack (R014x.00.0.730.5-13566)
Avaya SIP Enablement Services	3.1.2
Avaya 4602SW IP Telephone Avaya 4610SW IP Telephones Avaya 4620SW IP Telephone	SIP version 2.2.2
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (Management PC and TFTP Server)	Windows XP Professional
Juniper Networks Netscreen 50	5.4.0r1.0
Sipera IPCS 310	3.1 (Build Q07) plus Linux configuration change to support UDP fragmentation

3. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration at the main site to support the network shown in **Figure 1** and is 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 a second SIP connection using the SIP domain of the branch site. Avaya Communication Manager will use this connection when routing calls to Avaya SES bound for the branch site. Avaya SES will use the domain of the branch to route the call to the local IPCS.

To support the SIP endpoints in **Figure 1**, it is necessary to configure Off-PBX Stations (OPS) for each SIP endpoint. The configuration of the OPS stations is not directly related to the interoperability of IPCS, 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.

This configuration must be repeated for Avaya Communication Manager at the branch using values appropriate for the branch from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions. In addition, **Steps 12 and 13 in Section 3.1** are not required at the branch because the branch does not have any trunks to the PSTN.

3.1. Initial SIP Connection

Step	Description
1.	<p>Use the display system-parameters customer-options command to verify that sufficient SIP trunk capacity exists. On Page 2, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. 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.</p> <p>The license file installed on the system controls the maximum permitted. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> display system-parameters customer-options OPTIONAL FEATURES Page 2 of 10 IP PORT CAPACITIES Maximum Administered H.323 Trunks: 100 32 Maximum Concurrently Registered IP Stations: 100 0 Maximum Administered Remote Office Trunks: 0 0 Maximum Concurrently Registered Remote Office Stations: 0 0 Maximum Concurrently Registered IP eCons: 0 0 Max Concur Registered Unauthenticated H.323 Stations: 0 0 Maximum Video Capable H.323 Stations: 0 0 Maximum Video Capable IP Softphones: 0 0 Maximum Administered SIP Trunks: 100 44 Maximum Number of DS1 Boards with Echo Cancellation: 0 0 Maximum TN2501 VAL Boards: 0 0 Maximum Media Gateway VAL Sources: 0 0 Maximum TN2602 Boards with 80 VoIP Channels: 0 0 Maximum TN2602 Boards with 320 VoIP Channels: 0 0 Maximum Number of Expanded Meet-me Conference Ports: 0 0 (NOTE: You must logoff & login to effect the permission changes.) </pre> </div>
2.	<p>In order to support SIP the following features must be enabled. Use the display system-parameters customer-options command to verify that the following fields have been set to y.</p> <p style="margin-left: 40px;">Page 4: Enhanced EC500? y Page 4: ISDN-PRI? y Page 4: IP trunks? y</p> <p>If a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.</p>

Step	Description										
3.	<p>Use the change node-names ip command to assign the node name and IP address for Avaya SES. In this case, SES and 10.75.5.6 are being used, respectively. The node name SES will be used throughout the other configuration forms of Avaya Communication Manager. In this example, procr and 10.75.5.2 are the name and IP address assigned to the Avaya S8300 Server.</p> <div data-bbox="315 401 1383 600"> <pre>change node-names ip</pre> <div> <div>Page 1 of 2</div> <div> <div>IP NODE NAMES</div> <table> <tr> <th>Name</th><th>IP Address</th></tr> <tr> <td>SES</td><td>10.75.5.6</td></tr> <tr> <td>default</td><td>0.0.0.0</td></tr> <tr> <td>myaudix</td><td>10.75.5.7</td></tr> <tr> <td>procr</td><td>10.75.5.2</td></tr> </table> </div> </div> </div>	Name	IP Address	SES	10.75.5.6	default	0.0.0.0	myaudix	10.75.5.7	procr	10.75.5.2
Name	IP Address										
SES	10.75.5.6										
default	0.0.0.0										
myaudix	10.75.5.7										
procr	10.75.5.2										

Step	Description
4.	<p>Use the change ip-network-region <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 Signaling Group form as shown in Step 6. 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.</p> <p>On the IP Network Region form:</p> <ul style="list-style-type: none"> ▪ The Authoritative Domain field is configured to match the domain name configured on Avaya SES. In this configuration, the domain name is business.com. This name will appear in the “From” header of SIP messages originating from this IP region. ▪ Enter a descriptive name for the Name field. ▪ 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. ▪ 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. ▪ The default values can be used for all other fields. <div data-bbox="315 1169 1399 1726" style="border: 1px solid black; padding: 10px;"> <pre> change ip-network-region 1 IP NETWORK REGION Region: 1 Location: Authoritative Domain: business.com Name: default MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 Inter-region IP-IP Direct Audio: yes UDP Port Min: 2048 IP Audio Hairpinning? n 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? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 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? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 </pre> </div>

Step	Description																
5.	<p>Use the change ip-codec-set <i>n</i> command, where <i>n</i> is the codec set value specified in Step 4, 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.</p> <div><div>change ip-codec-set 1</div><div>Page1 of 2</div><div>IP Codec Set</div><div>Codec Set: 1</div><table><thead><tr><th>Audio Codec</th><th>Silence Suppression</th><th>Frames Per Pkt</th><th>Packet Size(ms)</th></tr></thead><tbody><tr><td>1: G.711MU</td><td>n</td><td>2</td><td>20</td></tr><tr><td>2: G.729AB</td><td>n</td><td>2</td><td>20</td></tr><tr><td>3:</td><td></td><td></td><td></td></tr></tbody></table></div>	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)	1: G.711MU	n	2	20	2: G.729AB	n	2	20	3:			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)														
1: G.711MU	n	2	20														
2: G.729AB	n	2	20														
3:																	

Step	Description
6.	<p>Use the add signaling-group <i>n</i> command, where <i>n</i> is the number of an unused signaling group, to create the SIP signaling group as follows:</p> <ul style="list-style-type: none"> ▪ Set the Group Type field to <i>sip</i>. ▪ The Transport Method field will default to <i>tls</i> (Transport Layer Security). 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 <i>SES</i>) 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 IP Node Names form shown in Step 3. 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 S8300 Server. ▪ Ensure that the recommended TLS port value of 5061 is configured in the Near-end Listen Port and the Far-end Listen Port fields. ▪ In the Far-end Network Region field, enter the IP network region value assigned in the IP Network Region form in Step 4. This defines which IP network region contains the Avaya SES server. If the Far-end Network Region 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. ▪ Enter the domain name of Avaya SES in the Far-end Domain field. In this 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 Direct IP-IP Audio Connections field is set to <i>n</i>. For interoperability, this field (also know as media shuffling) must be disabled for the SIP trunk. ▪ The DTMF over IP 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. <div data-bbox="315 1314 1416 1814" style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <pre> add signaling-group 1 SIGNALING GROUP Page 1 of 1 Group Number: 1 Group Type: sip Transport Method: tls Near-end Node Name: procr Far-end Node Name: SES Near-end Listen Port: 5061 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Domain: business.com Bypass If IP Threshold Exceeded? n DTMF over IP: rtp-payload Direct IP-IP Audio Connections? n IP Audio Hairpinning? n Enable Layer 3 Test? n Session Establishment Timer(min): 120 </pre> </div>

Step	Description
7.	<p>Add a SIP trunk group by using the add trunk-group <i>n</i> command, where <i>n</i> is the number of an unused trunk group. For the compliance test, trunk group number 1 was chosen.</p> <p>On Page 1, set the fields to the following values:</p> <ul style="list-style-type: none"> ▪ Set the Group Type 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. ▪ Set the Service Type field to <i>tie</i>. ▪ Specify the signaling group associated with this trunk group in the Signaling Group field as previously specified in Step 6. ▪ 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. ▪ The default values may be retained for the other fields. <div data-bbox="315 877 1399 1220"> <pre> 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 Queue Length: 0 Service Type: tie Auth Code? n Signaling Group: 1 Number of Members: 24 </pre> </div>
8.	<p>On Page 2:</p> <ul style="list-style-type: none"> ▪ The Preferred Minimum Session Refresh Interval field should be set the same for all SIP trunks at both sites. This field determines how often INVITE messages are sent during an active call to keep the session alive. The compliance test used a value of 120 sec. ▪ The default values may be retained for the other fields. <div data-bbox="315 1514 1399 1814"> <pre> change trunk-group 1 Page 2 of 21 Group Type: sip TRUNK PARAMETERS Unicode Name? y Redirect On OPTIM Failure: 5000 SCCAN? n Digital Loss Group: 18 Preferred Minimum Session Refresh Interval(sec): 120 </pre> </div>

Step	Description																		
9.	<p>On Page 3:</p> <ul style="list-style-type: none">Verify the Numbering Format field is set to <i>public</i>. This field specifies the format of the calling party number sent to the far-end.The default values may be retained for the other fields. <div><div>add trunk-group 1Page3 of 21</div><div>TRUNK FEATURES</div><div>ACA Assignment? nMeasured: noneMaintenance Tests? y</div><div>Numbering Format: publicUI Treatment: service-provider</div><div>Replace Unavailable Numbers? n</div><div>Show ANSWERED BY on Display? y</div></div>																		
10.	<p>Use the change public-unknown-numbering 0 command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in Step 7. 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 calling party number will be sent to the far-end in the SIP “From” header.</p> <div><div>change public-unknown-numbering 0Page1 of 2</div><div>NUMBERING - PUBLIC/UNKNOWN FORMAT</div><div><table><thead><tr><th>Ext Len</th><th>Ext Code</th><th>Trk Grp(s)</th><th>CPN Prefix</th><th>Total CPN Len</th><th></th></tr></thead><tbody><tr><td>5</td><td>3</td><td>1</td><td></td><td>5</td><td>Total Administered: 4</td></tr><tr><td>5</td><td>3</td><td>99</td><td></td><td>5</td><td>Maximum Entries: 240</td></tr></tbody></table></div></div>	Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len		5	3	1		5	Total Administered: 4	5	3	99		5	Maximum Entries: 240
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len															
5	3	1		5	Total Administered: 4														
5	3	99		5	Maximum Entries: 240														

Step	Description
11.	<p>Create a route pattern that will use the SIP trunk that connects to Avaya SES. This route pattern will be used as a default route for SIP calls in Step 12. Some transfer scenarios using alpha-numeric handles (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.</p> <p>To create a route pattern, use the change route-pattern <i>n</i> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the Pattern Name field. Set the Grp No field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level (FRL) 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.</p> <pre> 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 Intw 1: 1 0 2: 3: 4: 5: 6: n user n user n user n user n user n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 3 4 W Request Dgts Format Subaddress 1: y y y y y n n rest none 2: y y y y y n n rest none 3: y 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 </pre>
12.	<p>Use the change locations 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 Main and shown in the example below. Enter the route pattern number from the previous step in the Proxy Sel Rte Pat field. The default values may be retained for all other fields.</p> <pre> change locations LOCATIONS ARS Prefix 1 Required For 10-Digit NANP Calls? y Loc Name Timezone Rule NPA ARS Atd Disp Prefix Proxy Sel No Offset FAC FAC Parm Rte Pat 1: Main + 00:00 0 1 1 2: 3: </pre>

Step	Description																																										
13.	<p>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.</p> <p>Use the change ars analysis <i>n</i> command to add an entry in the ARS Digit Analysis Table for the dialed string beginning with <i>n</i>. In the example shown, PSTN numbers that begin with 1732 and 11 digits long use route pattern 2. Route pattern 2 routes calls to the ISDN-PRI trunk between the main site and the PSTN shown in Figure 1. The configuration of the PRI trunk is beyond the scope of these Application Notes.</p> <div><div>change ars analysis 1732</div><div>ARS DIGIT ANALYSIS TABLE</div><div>Location: all</div><div>Percent Full: 3</div><div>Page 1 of 2</div><table><tr><th>Dialed String</th><th>Total Min</th><th>Total Max</th><th>Route Pattern</th><th>Call Type</th><th>Node Num</th><th>ANI Req'd</th></tr><tr><td>1732</td><td>11</td><td>11</td><td>2</td><td>fnpa</td><td></td><td>n</td></tr><tr><td>174</td><td>11</td><td>11</td><td>deny</td><td>fnpa</td><td></td><td>n</td></tr><tr><td>175</td><td>11</td><td>11</td><td>deny</td><td>fnpa</td><td></td><td>n</td></tr><tr><td>176</td><td>11</td><td>11</td><td>deny</td><td>fnpa</td><td></td><td>n</td></tr><tr><td>177</td><td>11</td><td>11</td><td>deny</td><td>fnpa</td><td></td><td>n</td></tr></table></div>	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	1732	11	11	2	fnpa		n	174	11	11	deny	fnpa		n	175	11	11	deny	fnpa		n	176	11	11	deny	fnpa		n	177	11	11	deny	fnpa		n
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd																																					
1732	11	11	2	fnpa		n																																					
174	11	11	deny	fnpa		n																																					
175	11	11	deny	fnpa		n																																					
176	11	11	deny	fnpa		n																																					
177	11	11	deny	fnpa		n																																					
14.	<p>To map a PSTN number to a station at the main site, use the change inc-call-handling-trmt trunk-group <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.</p> <div><div>change inc-call-handling-trmt trunk-group 2</div><div>INCOMING CALL HANDLING TREATMENT</div><div>Per Call Night</div><div>CPN/BN Serv</div><div>Page 1 of 3</div><table><tr><th>Service/ Feature</th><th>Called Len</th><th>Called Number</th><th>Del</th><th>Insert</th></tr><tr><td>tie</td><td>11</td><td>17325551234</td><td>11</td><td>30104</td></tr><tr><td>tie</td><td>11</td><td>17325551235</td><td>11</td><td>30106</td></tr></table></div>	Service/ Feature	Called Len	Called Number	Del	Insert	tie	11	17325551234	11	30104	tie	11	17325551235	11	30106																											
Service/ Feature	Called Len	Called Number	Del	Insert																																							
tie	11	17325551234	11	30104																																							
tie	11	17325551235	11	30106																																							

3.2. Second SIP Connection

Step	Description																												
1.	<p>Create a new SIP signaling group using the same procedure as shown in Section 3.1, Step 6. Use the same parameters with the following exception. Set the Far-end Domain field to the SIP domain of the branch site. The compliance test used signaling group 6 as shown below.</p> <div data-bbox="315 453 1399 945" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <div style="display: flex; justify-content: space-between;"> add signaling-group 6 Page 1 of 1 </div> <div style="text-align: center; margin-top: 10px;"> SIGNALING GROUP </div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Group Number: 6</td> <td style="width: 50%;">Group Type: sip</td> </tr> <tr> <td></td> <td>Transport Method: tls</td> </tr> <tr><td colspan="2"> </td></tr> <tr> <td>Near-end Node Name: procr</td> <td>Far-end Node Name: SES</td> </tr> <tr> <td>Near-end Listen Port: 5061</td> <td>Far-end Listen Port: 5061</td> </tr> <tr> <td></td> <td>Far-end Network Region: 1</td> </tr> <tr> <td colspan="2">Far-end Domain: dev4.com</td> </tr> <tr><td colspan="2"> </td></tr> <tr> <td></td> <td>Bypass If IP Threshold Exceeded? n</td> </tr> <tr><td colspan="2"> </td></tr> <tr> <td>DTMF over IP: rtp-payload</td> <td>Direct IP-IP Audio Connections? n</td> </tr> <tr> <td></td> <td>IP Audio Hairpinning? n</td> </tr> <tr> <td>Enable Layer 3 Test? n</td> <td></td> </tr> <tr> <td>Session Establishment Timer(min): 120</td> <td></td> </tr> </table> </div>	Group Number: 6	Group Type: sip		Transport Method: tls			Near-end Node Name: procr	Far-end Node Name: SES	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? n		IP Audio Hairpinning? n	Enable Layer 3 Test? n		Session Establishment Timer(min): 120	
Group Number: 6	Group Type: sip																												
	Transport Method: tls																												
Near-end Node Name: procr	Far-end Node Name: SES																												
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? n																												
	IP Audio Hairpinning? n																												
Enable Layer 3 Test? n																													
Session Establishment Timer(min): 120																													
2.	<p>Create a new trunk group using the same procedure as shown in Section 3.1, Step 7 - 9. Use the same parameters 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 6 with the following values.</p> <ul style="list-style-type: none"> ▪ Group Name: <i>Site2SES</i> ▪ TAC: <i>106</i> ▪ Signaling Group: <i>6</i> 																												

Step	Description																																																																																																																																																																																				
3.	<p>Use the change public-unknown-numbering 0 command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in Step 2. In the example shown below, all calls originating from a 5-digit extension beginning with 4 and routed across trunk group 6 will be sent as a 5-digit calling number. This calling party number will be sent to the far-end in the SIP “From” header.</p> <div><div>change public-unknown-numbering 0</div><div>Page 1 of 2</div><div>NUMBERING - PUBLIC/UNKNOWN FORMAT</div><table><thead><tr><th>Ext Len</th><th>Ext Code</th><th>Trk Grp(s)</th><th>CPN Prefix</th><th>Total CPN Len</th><th></th></tr></thead><tbody><tr><td>5</td><td>3</td><td>1</td><td></td><td>5</td><td>Total Administered: 4</td></tr><tr><td>5</td><td>4</td><td>6</td><td></td><td>5</td><td>Maximum Entries: 240</td></tr><tr><td>5</td><td>3</td><td>99</td><td></td><td>5</td><td></td></tr></tbody></table></div>	Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len		5	3	1		5	Total Administered: 4	5	4	6		5	Maximum Entries: 240	5	3	99		5																																																																																																																																																													
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len																																																																																																																																																																																	
5	3	1		5	Total Administered: 4																																																																																																																																																																																
5	4	6		5	Maximum Entries: 240																																																																																																																																																																																
5	3	99		5																																																																																																																																																																																	
4.	<p>Create a route pattern for use by Automatic Alternate Routing (AAR) when routing calls to the branch site.</p> <p>Use the change route-pattern n command, where n is the number of an unused route pattern. Enter a descriptive name for the Pattern Name 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 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.</p> <div><div>change route-pattern 6</div><div>Page 1 of 3</div><div>Pattern Number: 6</div><div>Pattern Name: Site2SES</div><div>SCCAN? n</div><div>Secure SIP? n</div><table><thead><tr><th>Grp No</th><th>FRL</th><th>NPA</th><th>Pfx</th><th>Hop</th><th>Toll</th><th>No.</th><th>Inserted</th><th>DCS/ IXC</th></tr><tr><th></th><th></th><th></th><th>Mrk</th><th>Lmt</th><th>List</th><th>Del</th><th>Digits</th><th>QSIG</th></tr><tr><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Intw</th></tr></thead><tbody><tr><td>1:</td><td>6</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td>n user</td></tr><tr><td>2:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n user</td></tr><tr><td>3:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n user</td></tr><tr><td>4:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n user</td></tr><tr><td>5:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n user</td></tr><tr><td>6:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n user</td></tr></tbody></table><table><thead><tr><th>BCC</th><th>VALUE</th><th>TSC</th><th>CA-TSC</th><th>ITC</th><th>BCIE</th><th>Service/Feature</th><th>PARM</th><th>No.</th><th>Numbering</th><th>LAR</th></tr><tr><th></th><th>0</th><th>1</th><th>2</th><th>M</th><th>4</th><th>W</th><th>Request</th><th></th><th>Dgts</th><th>Format</th></tr><tr><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Subaddress</th><th></th></tr></thead><tbody><tr><td>1:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td>rest</td><td>none</td></tr><tr><td>2:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td>rest</td><td>none</td></tr><tr><td>3:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td>rest</td><td>none</td></tr><tr><td>4:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td>rest</td><td>none</td></tr><tr><td>5:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td>rest</td><td>none</td></tr><tr><td>6:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td>rest</td><td>none</td></tr></tbody></table></div>	Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC				Mrk	Lmt	List	Del	Digits	QSIG									Intw	1:	6	0						n user	2:								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.	Numbering	LAR		0	1	2	M	4	W	Request		Dgts	Format										Subaddress		1:	y	y	y	y	y	n	n		rest	none	2:	y	y	y	y	y	n	n		rest	none	3:	y	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
Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC																																																																																																																																																																													
			Mrk	Lmt	List	Del	Digits	QSIG																																																																																																																																																																													
								Intw																																																																																																																																																																													
1:	6	0						n user																																																																																																																																																																													
2:								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.	Numbering	LAR																																																																																																																																																																											
	0	1	2	M	4	W	Request		Dgts	Format																																																																																																																																																																											
									Subaddress																																																																																																																																																																												
1:	y	y	y	y	y	n	n		rest	none																																																																																																																																																																											
2:	y	y	y	y	y	n	n		rest	none																																																																																																																																																																											
3:	y	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																																																																																																																																																																											

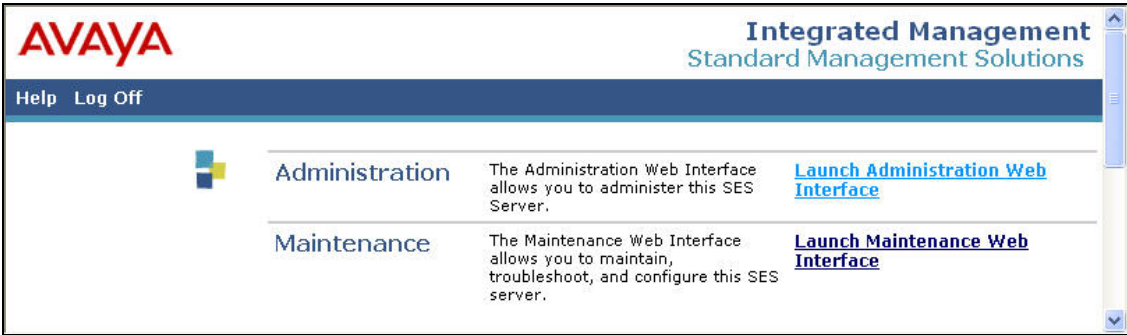
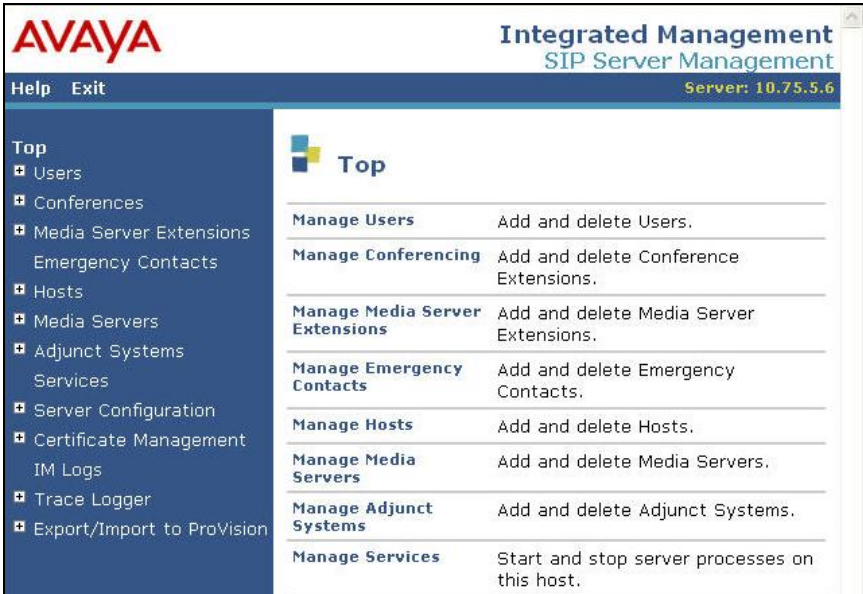
Step	Description																																																	
5.	<p>Use the change aar analysis 4 command to add an entry in the AAR Digit Analysis Table for the dialed string beginning with 4. In the example shown, numbers that begin with 4 and are 5 digits long use route pattern 6. Route pattern 6 routes calls from the main site to the branch via the second SIP trunk with the far-end domain set to the SIP domain of the branch site (dev4.com).</p> <div><div>change aar analysis 4</div><div><div>Page1 of 2</div><div>AAR DIGIT ANALYSIS TABLE</div><div>Percent Full:3</div><table><tr><th>Dialed String</th><th>Total Min</th><th>Total Max</th><th>Route Pattern</th><th>Call Type</th><th>Node Num</th><th>ANI Req'd</th></tr><tr><td>4</td><td>5</td><td>5</td><td>6</td><td>aar</td><td></td><td>n</td></tr><tr><td>5</td><td>7</td><td>7</td><td>254</td><td>aar</td><td></td><td>n</td></tr><tr><td>6</td><td>7</td><td>7</td><td>254</td><td>aar</td><td></td><td>n</td></tr><tr><td>7</td><td>7</td><td>7</td><td>254</td><td>aar</td><td></td><td>n</td></tr><tr><td>8</td><td>7</td><td>7</td><td>254</td><td>aar</td><td></td><td>n</td></tr><tr><td>9</td><td>7</td><td>7</td><td>254</td><td>aar</td><td></td><td>n</td></tr></table></div></div>	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	4	5	5	6	aar		n	5	7	7	254	aar		n	6	7	7	254	aar		n	7	7	7	254	aar		n	8	7	7	254	aar		n	9	7	7	254	aar		n
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd																																												
4	5	5	6	aar		n																																												
5	7	7	254	aar		n																																												
6	7	7	254	aar		n																																												
7	7	7	254	aar		n																																												
8	7	7	254	aar		n																																												
9	7	7	254	aar		n																																												


4. Configure Avaya SES

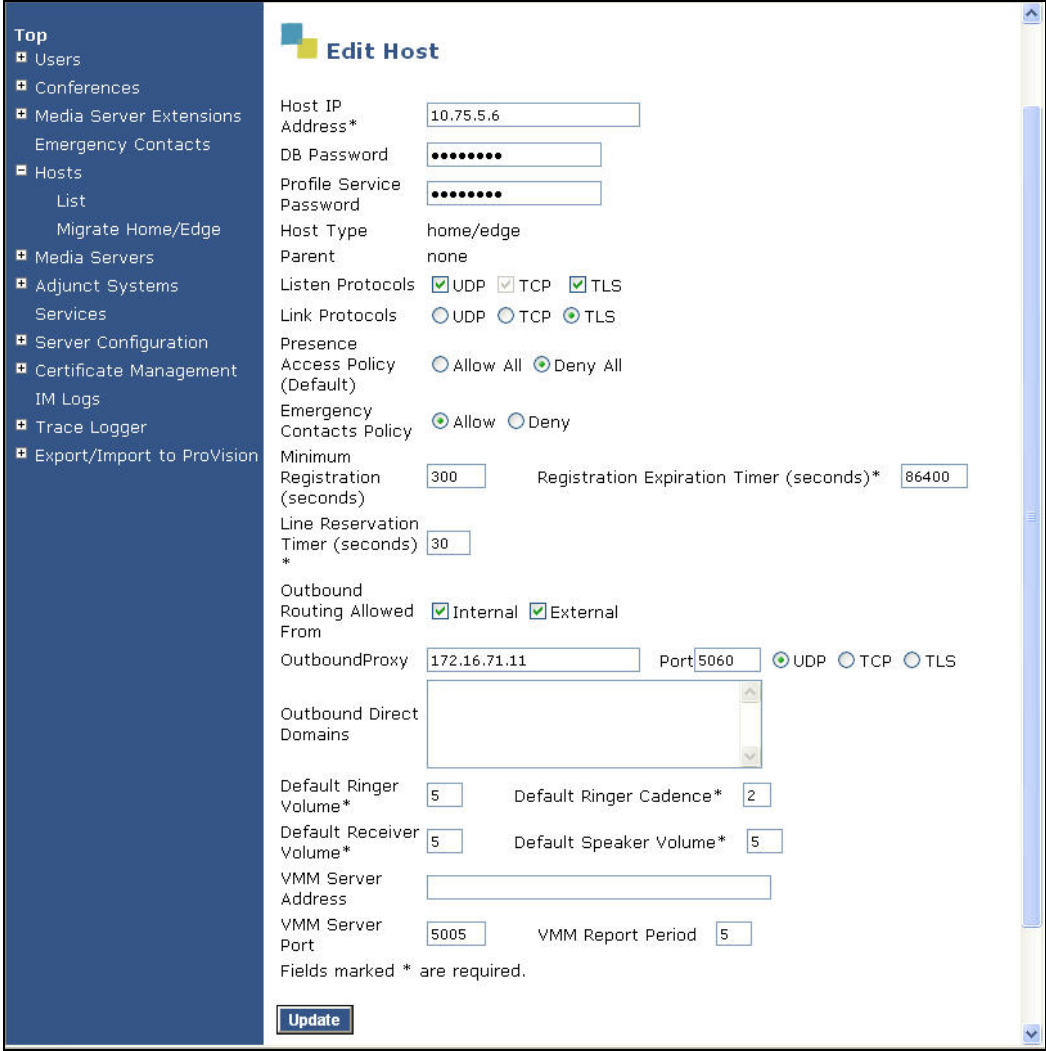
This section covers the configuration of Avaya SES at the main site. The configuration must be repeated for Avaya SES at the branch using values appropriate for the branch from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

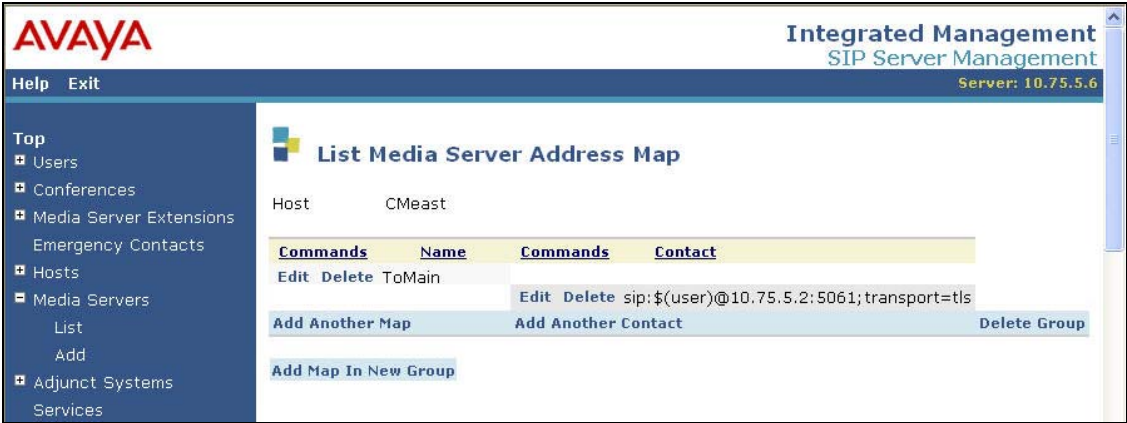
Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that the Avaya SES software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify 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].

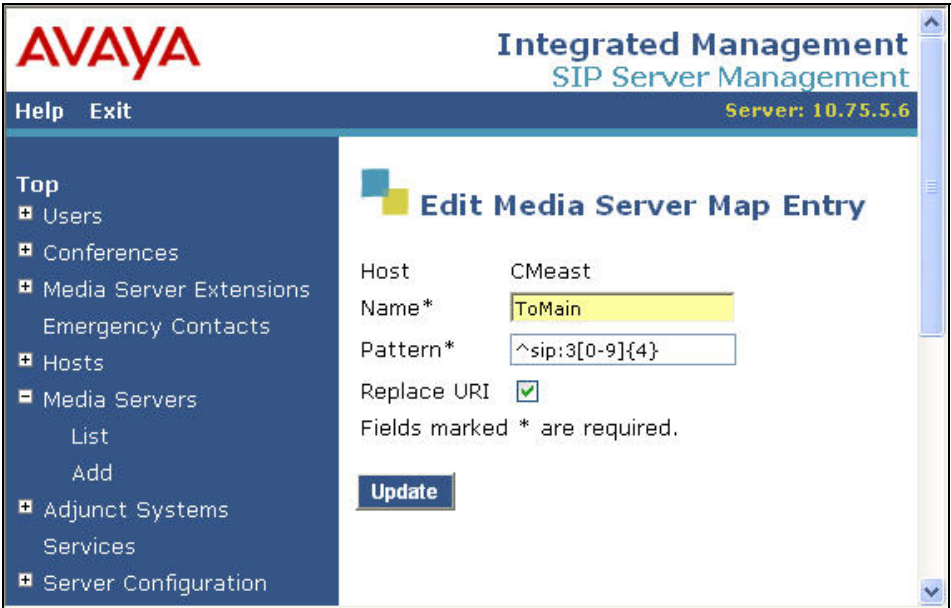
Each SIP endpoint used in the compliance test requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of IPCS so it is not included here. These procedures are covered in [5].

Step	Description
1.	<p>Access the Avaya SES administration web interface by entering <a href="http://<ip-addr>/admin">http://<ip-addr>/admin as the URL in an Internet browser, where <ip-addr> is the IP address of the Avaya SES server.</p> <p>Log in with the appropriate credentials and then select the Launch Administration Web Interface link from the main page as shown below.</p> 
2.	<p>The Avaya SES Top page will be displayed as shown below.</p> 

Step	Description
3.	<p>After making changes within Avaya SES, it is necessary to commit the database changes using the Update link that appears when changes are pending. Perform this step by clicking on the Update link found in the bottom of the blue navigation bar on the left side of any of the Avaya SES administration pages as shown below. It is recommended that this be done after making any changes.</p> 
4.	<p>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 Top page shown in the previous step.</p> <ul style="list-style-type: none"> • SIP Domain: <i>business.com</i> (To view, navigate to Server Configuration→System Parameters) • Host (Avaya SES IP address): <i>10.75.5.6</i> (To view, navigate to Host→List; Click Edit) • Media Server (Avaya Communication Manager) Interface Name: <i>CMeast</i> (To view, navigate to Media Server→List; Click Edit) • SIP Trunk IP Address (Avaya S8300 Server IP address): <i>10.75.5.2</i> (To view, navigate to Media Server→List; Click Edit)

Step	Description
5.	<p>Set the outbound proxy of Avaya SES to the local 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 server was used in the compliance test, the DNS look-up will fail and Avaya SES will route the call to the outbound proxy (the local IPCS). The local IPCS will then be responsible for routing the call to the remote IPCS at the branch.</p> <p>To configure the proxy settings, navigate to Hosts→Lists in the left pane. Select the Edit link next to the host name of Avaya SES (not shown). In the Edit Host window that appears, configure the following:</p> <ul style="list-style-type: none"> • Outbound Routing Allowed From: Check both <i>Internal</i> and <i>External</i>. • Outbound Proxy: IP address of the local IPCS. Port field is set to 5060. Select the UDP radio button. 

Step	Description
6.	<p>A media server address map is needed to route calls from the branch site to a non-SIP phone at the main site. This is because neither the caller nor the called party is a registered user on 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 created.</p> <p>To configure a media server address map:</p> <ul style="list-style-type: none"> Navigate to Media Server→List in the left pane. In the List Media Servers window that appears (not shown), click on the Map link next to the host name of the Avaya S8300 Server running Avaya Communication Manager. The List Media Server Address Map window will appear as shown below. If no other maps exist, click Add Map In New Group. If adding another map for the same media server, click Add Another Map. In either case, a window similar to the one shown in the Step 7 will appear, for entering the map data. <p>The example below shows the media server address map, named ToMain, after it was created. For simplicity, the media server address map was configured to match all calls dialed with a 5 digit number beginning with 3. To view or edit the contents of the map, click the Edit link next to the map name (see Step 7).</p> <p>After configuring the map, the initial Contact information is populated automatically and directs the calls to the IP address of the Avaya S8300 Server (10.75.5.2) using port 5061 and TLS as the transport protocol. The user portion in the original request URI is substituted for \$(user). For the compliance test, the Contact field for the media server address map is displayed as:</p> <pre> sip:\$(user)@10.75.5.2:5061;transport=tls </pre> 

Step	Description
7.	<p>The content of the media server address map is described below.</p> <ul style="list-style-type: none"> • Name: Contains any descriptive name • Pattern: Contains an expression to define the matching criteria for calls to be routed from the branch site to the local Avaya Communication Manager. The example below shows the expression used in the compliance test. This 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]. • Replace URI: Check the box. <p>If any changes are made, click Update.</p> 

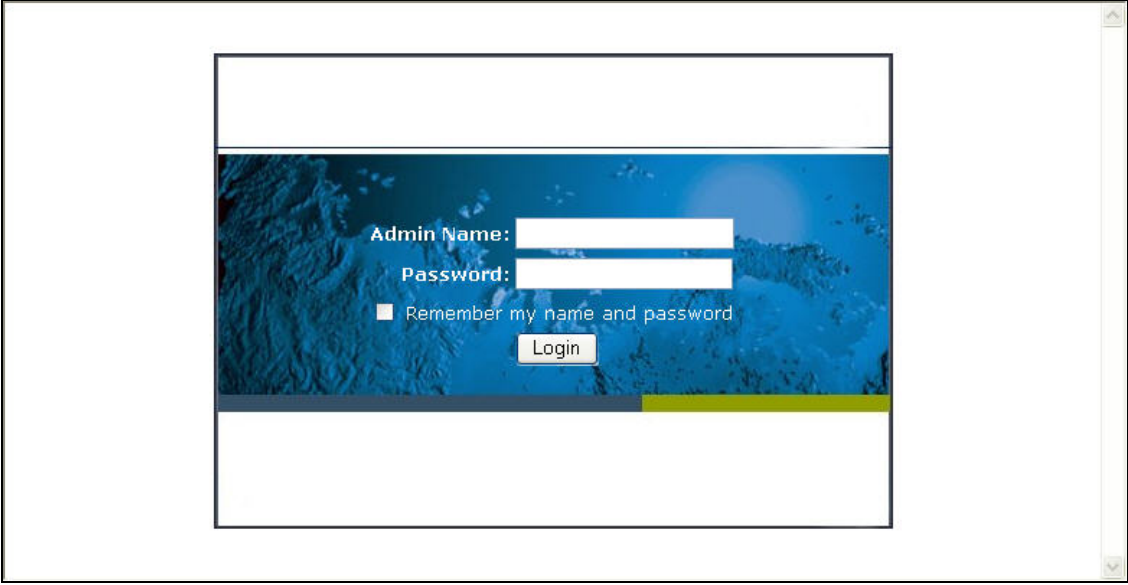
5. Configure the Avaya SIP Telephones

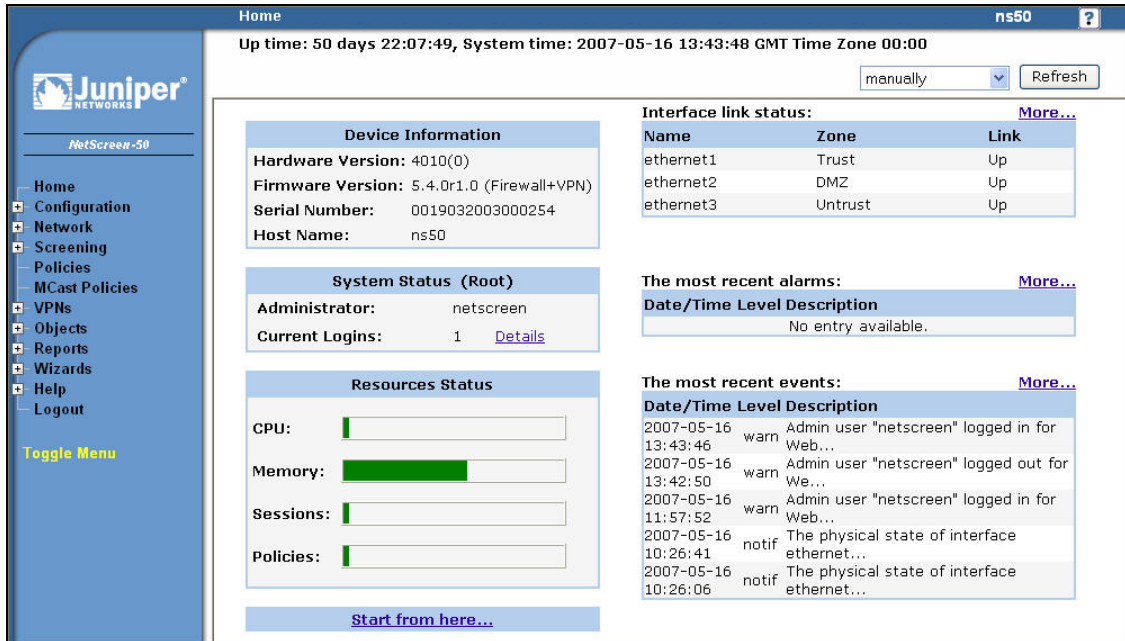
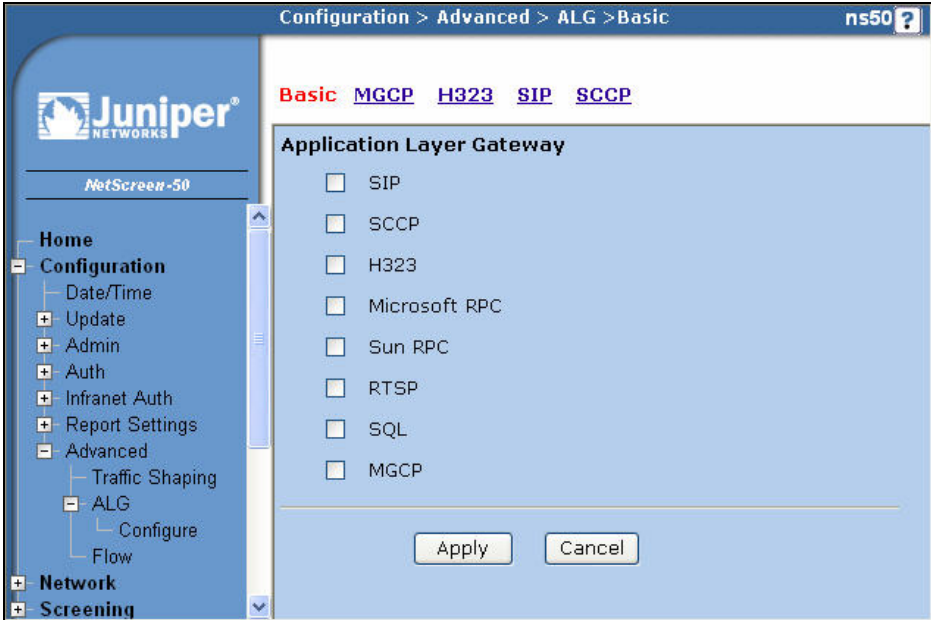
The SIP telephones at each site will use the local Avaya SES as the call server. The table below shows an example of the SIP telephone networking settings for each site.

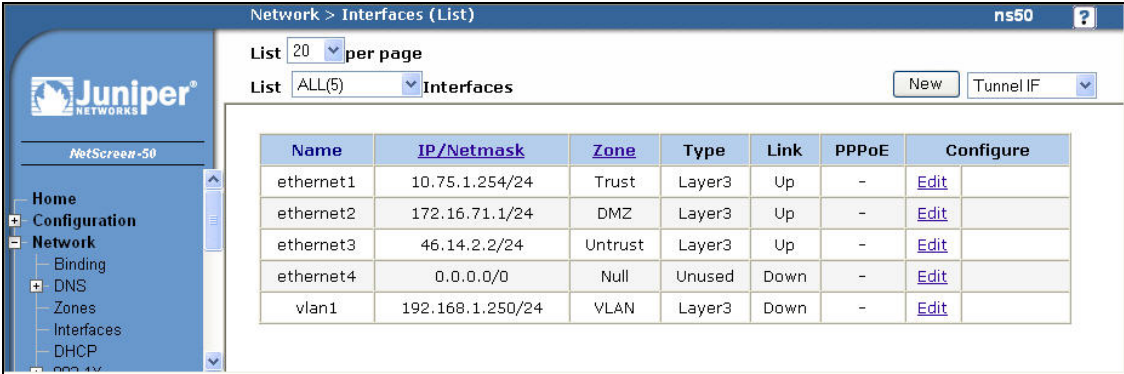
	Main Site	Branch Site
IP Address	10.75.5.153	50.1.1.157
Subnet Mask	255.255.255.0	255.255.255.0
Call Server	10.75.5.6	50.1.1.50
Router	10.75.5.1	50.1.1.254
File Server	10.75.10.52	50.1.1.52

6. Configure Juniper Networks Netscreen 50

This section covers the configuration of the Netscreen 50 firewall at the main site. It must be repeated for the Netscreen 50 at the branch using values appropriate for the branch from **Figure 1**.

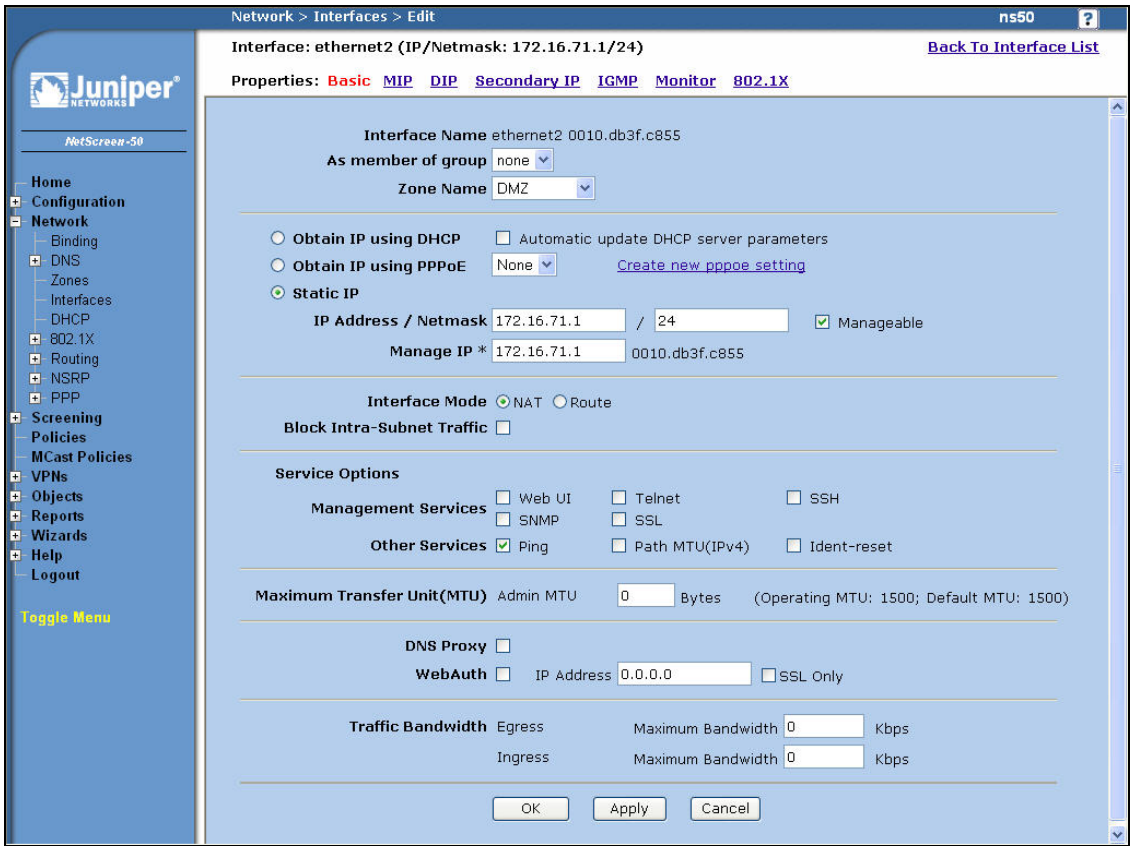
Step	Description
1.	<p>The Netscreen 50 is configured via a web browser. To access the web interface, enter <a href="http://<ip-addr>">http://<ip-addr> in the address field of the web browser, where <ip-addr> is the IP address of the Netscreen 50.</p> <p>Log in with the appropriate credentials. Click Login.</p> 

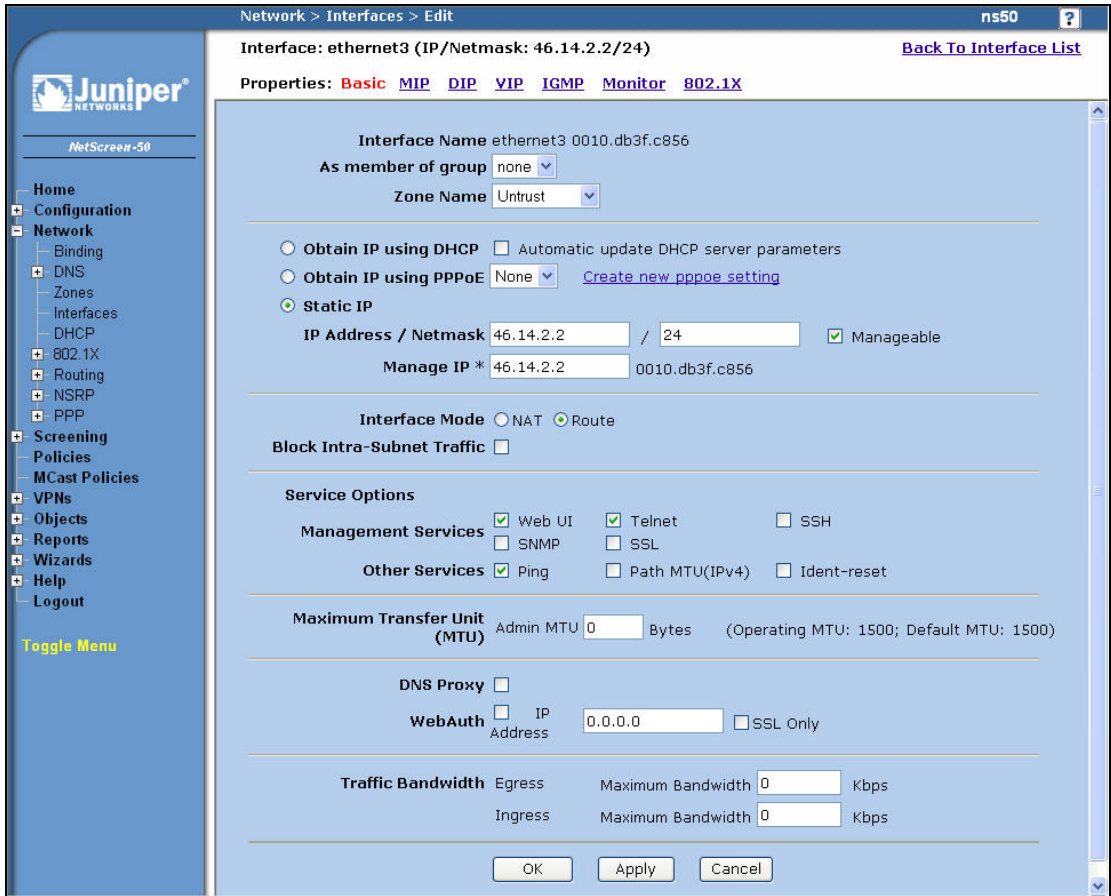
Step	Description
2.	<p>The main page appears as shown below.</p> <div></div>
3.	<p>Application Layer Gateway (ALG) The SIP ALG function must be disabled. From the left pane, navigate to Configuration→Advanced→ALG→Configure. Uncheck the box next to SIP. The other settings can remain unchanged. Click Apply.</p> <div></div>

Step	Description
4.	<h3>Interfaces</h3> <p>To configure the interfaces of the firewall, navigate to Network→Interfaces in the left pane of the window. As a result of the factory defaults, four interfaces named ethernet1 – ethernet4 that correspond to the four physical ports on the device will appear in the table in the right pane. Other logical interfaces may also be present.</p> <p>For the compliance test, interfaces ethernet1 – ethernet3 were used. The example below shows the interface list after these interfaces were configured for testing. To view the configuration of each interface, click Edit next to the interface of interest.</p> 

Step	Description
5.	<p>Interface – ethernet1 (Private)</p> <p>The interface, ethernet1, was configured as follows:</p> <ul style="list-style-type: none"> • Zone Name: <i>Trust</i> This is the private side of the firewall. • Static IP: Select this radio button. • IP Address / Netmask: Enter the IP address and netmask for the private side of the firewall. • Manageable: Check this box to allow the firewall to be managed from this interface. The compliance test used this interface to manage the device. • Manage IP: If the Manageable box is checked, enter the same address as used in the IP Address field. • Interface Mode: Select the Route button. • Service Options: Check the box next to any service that will be available on this interface. <p>Default values may be retained for all other fields. Click OK.</p>

The screenshot shows the Juniper NetScreen-50 configuration page for the 'ethernet1' interface. The breadcrumb trail is 'Network > Interfaces > Edit'. The interface name is 'ethernet1' with IP/Netmask '10.75.1.254/24'. A 'Back To Interface List' link is present. The 'Properties' section includes links for Basic, MIP, DIP, Secondary IP, IGMP, Monitor, and 802.1X. The left sidebar shows a navigation tree with categories like Home, Configuration, Network, Binding, DNS, Zones, Interfaces, DHCP, 802.1X, Routing, NSRP, PPP, Screening, Policies, MCast Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. The main configuration area is divided into sections: Interface Name (ethernet1 0010.db3f.c850), As member of group (none), Zone Name (Trust), IP configuration (Static IP selected, IP Address/Netmask 10.75.1.254/24, Manageable checked, Manage IP * 10.75.1.254 0010.db3f.c850), Interface Mode (Route selected), Block Intra-Subnet Traffic (unchecked), Service Options (Management Services: Web UI, SNMP, Telnet, SSH, SSL; Other Services: Ping, Path MTU(IPv4), Ident-reset), Maximum Transfer Unit (MTU) (Admin MTU 0 Bytes, Operating MTU: 1500, Default MTU: 1500), DNS Proxy (unchecked), WebAuth (IP Address 0.0.0.0, SSL Only unchecked), and Traffic Bandwidth (Egress and Ingress Maximum Bandwidth 0 Kbps). At the bottom are OK, Apply, and Cancel buttons.

Step	Description
6.	<p>Interface – ethernet2 (DMZ)</p> <p>The interface, ethernet2, was configured as follows:</p> <ul style="list-style-type: none"> • Zone Name: DMZ This is the zone which will contain IPCS. • Static IP: Select this radio button. • IP Address / Netmask: Enter the IP address and netmask for the DMZ of the firewall. • Manageable: Check this box to allow the firewall to be managed from this interface. This was not required for the compliance test but was enabled. • Manage IP: If the Manageable box is checked, enter the same address as used in the IP Address field. • Interface Mode: Select the NAT button. • Service Options: Check the box next to any service that will be available on this interface. <p>Default values may be retained for all other fields. Click OK.</p> 

Step	Description
7.	<p>Interface – ethernet3 (Public)</p> <p>The interface, ethernet3, was configured as follows:</p> <ul style="list-style-type: none"> • Zone Name: <i>Untrust</i> This is the public side of the firewall. • Static IP: Select this radio button. • IP Address / Netmask: Enter the IP address and netmask for the DMZ of the firewall. • Manageable: Check this box to allow the firewall to be managed from this interface. This was not required for the compliance test but was enabled. • Manage IP: If the Manageable box is checked, enter the same address as used in the IP Address field. • Interface Mode: Select the Route button. • Service Options: Check the box next to any service that will be available on this interface. <p>Default values may be retained for all other fields.</p> <p>NAT is performed on this interface. However, instead of setting the Interface Mode above to NAT, a static translation is defined using mapped IP (MIP) addresses. Select the MIP link at the top of the page to define these mappings.</p>  <p>The screenshot shows the Juniper NetScreen-50 configuration page for the 'ethernet3' interface. The breadcrumb trail is 'Network > Interfaces > Edit'. The interface name is 'ethernet3' with IP/Netmask '46.14.2.2/24'. The 'Zone Name' is set to 'Untrust'. Under 'Obtain IP', the 'Static IP' option is selected. The 'IP Address / Netmask' is '46.14.2.2 / 24' and 'Manageable' is checked. The 'Manage IP *' field contains '46.14.2.2' and '0010.db3f.c856'. The 'Interface Mode' is set to 'Route'. Under 'Service Options', 'Web UI', 'Telnet', and 'Ping' are checked. The 'Maximum Transfer Unit (MTU)' is set to 'Admin MTU 0 Bytes'. The 'DNS Proxy' and 'WebAuth' options are unchecked. The 'Traffic Bandwidth' section shows 'Egress' and 'Ingress' both set to 'Maximum Bandwidth 0 Kbps'. Buttons for 'OK', 'Apply', and 'Cancel' are at the bottom.</p>

Step	Description
8.	<p>Mapped IP Addresses (MIP)</p> <p>Mapped IP addresses were used to map a public accessible IP address to a host IP address on the private or DMZ side of the firewall. Each mapping was created by selecting the New button. A new page is opened (not shown) where the address mapping information can be entered and submitted.</p> <p>The MIP list below shows the two mapped IP addresses. Only the first entry was needed for the compliance test. The second entry was not used. The first entry maps a public IP address to the public side of IPCS which resides in the DMZ. The Netmask value of 255.255.255.255 used in the entry indicates that a single IP address, not a range of addresses, is being mapped with that particular entry. The VRouter field refers to the virtual router used. Only one virtual router, <i>trust-vr</i>, was used in the compliance test, so the VRouter field was set to this value. More information on the topic of virtual routers can be obtained from [7].</p> <p>After creating the MIPs, click on the Basic link to return to the previous page. On the Basic page, click OK.</p>

Network > Interfaces > Edit > MIP (List)

ns50

Interface: ethernet3 (IP/Netmask: 46.14.2.2/24)

[Back To Interface List](#)

Properties: [Basic](#) [MIP](#) [DIP](#) [VIP](#) [IGMP](#) [Monitor](#) [802.1X](#)

New

Mapped IP	Host IP	Netmask	VRouter	Configure
46.14.2.12	172.16.71.12	255.255.255.255	trust-vr	In use
46.14.2.52	10.75.10.52	255.255.255.255	trust-vr	In use

Juniper

Networks

NetScreen-50

Home

Configuration

Network

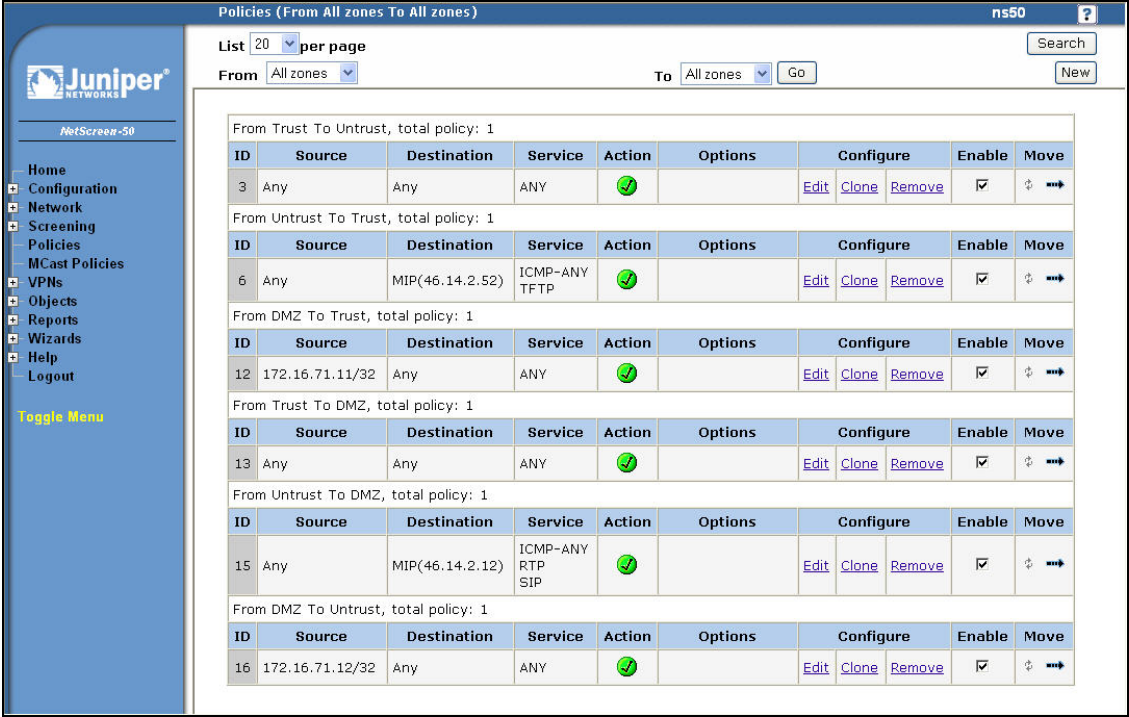
Binding

DNS

Zones

Interfaces

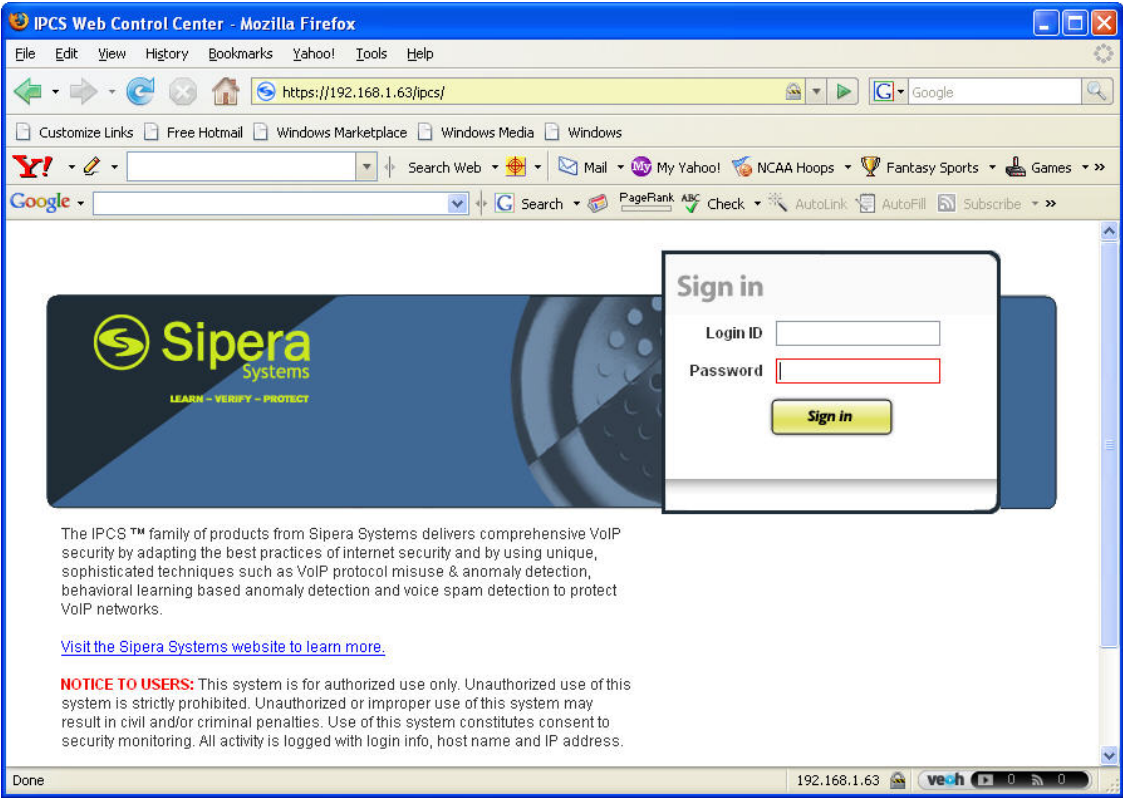
DHCP

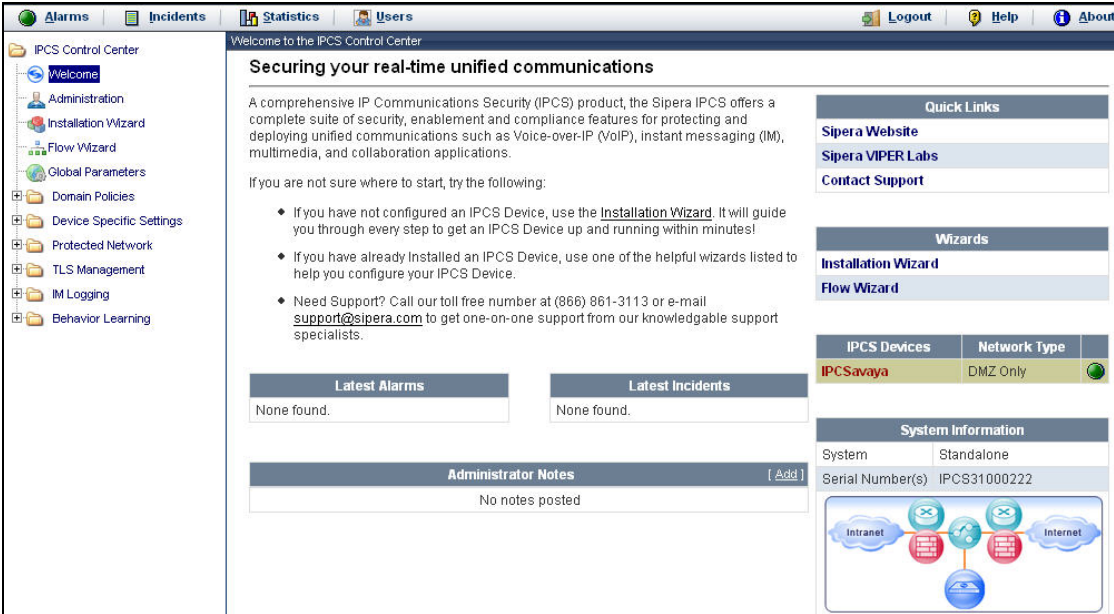
Step	Description
9.	<p>Policies</p> <p>Policies define the traffic that is allowed to flow through the firewall. To configure a policy, navigate to Policies in the left pane. Each policy is created by selecting a From zone and a To zone from the pull-downs at the top of the Policies page and clicking the New button. A new page is opened (not shown) where the policy information can be entered and submitted.</p> <p>The list below shows the policies used for the compliance test. Steps 4 – 7 have previously defined the following:</p> <ul style="list-style-type: none"> Trust zone: Connects to the private enterprise LAN. DMZ zone: Connects to IPCS. Untrust zone: Connects to the public untrusted IP network. <p>The policies used in the compliance test are summarized as follows:</p> <ul style="list-style-type: none"> Policy 3 and 13: Traffic is unrestricted in the direction of Trust to Untrust, and Trust to DMZ. Policy 6: Not required for compliance test. Policy 12: Any traffic from the IPCS private address is allowed from the DMZ to the Trust zone. Policy 15: SIP, RTP and ICMP traffic (for pings) to the public mapped IP address of IPCS is allowed from the Untrust to DMZ zones. The ICMP traffic is not required for the compliance test. Policy 16: Any traffic from the public internal IP address of IPCS is allowed from the DMZ to Untrust zone. 

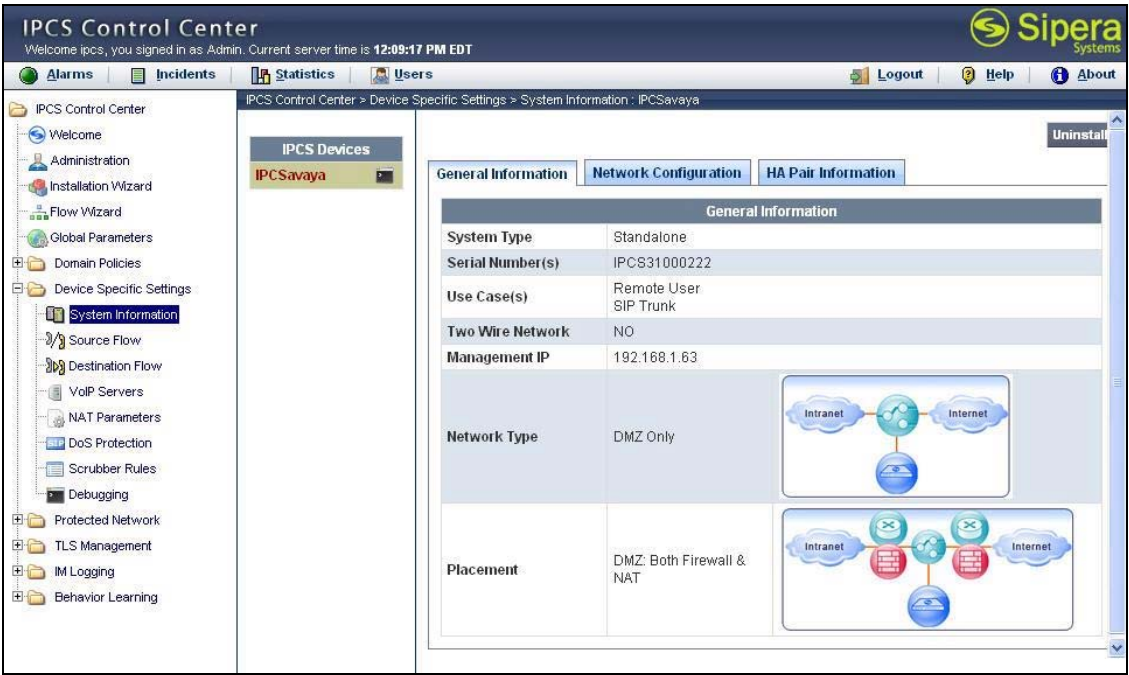
Step	Description								
10.	<p>Services</p> <p>The services used in the policies in Step 9 were standard services defined by the firewall with the exception of the service called RTP. RTP does not use a set of well known ports, so a custom service must be created by the user to define the ports and transport protocol that define the service RTP. To create a custom service, navigate to Objects→Services→Custom from the left pane. Click on the New button. A new page is opened (not shown) where the policy information can be entered and submitted.</p> <p>The table below shows the custom service named RTP used for the compliance test. It shows the source port as any valid UDP port and the destination port as any UDP port between 10000 – 20000 or 56000 - 59200. These ports were chosen based on default values used by IPCS for RTP traffic. The range of ports used can be further restricted as long as the range of ports are compatible to the ports used by IPCS and the remote endpoints. Even though the range of ports used by the compliance test was large, the firewall policy only allows this traffic to a single host (IPCS).</p> <div><div><div>Objects > Services > Custom</div><div>ns50</div><div>?</div></div><div><div>List 20 per page</div><div>New</div></div><div><table><thead><tr><th>Name</th><th>Transport Protocol and Parameters</th><th>Timeout (min)</th><th>Configure</th></tr></thead><tbody><tr><td>RTP</td><td>UDP src port: 0-65535, dst port: 10000-20000 UDP src port: 0-65535, dst port: 56000-59200</td><td>1</td><td>Edit Remove</td></tr></tbody></table></div></div>	Name	Transport Protocol and Parameters	Timeout (min)	Configure	RTP	UDP src port: 0-65535, dst port: 10000-20000 UDP src port: 0-65535, dst port: 56000-59200	1	Edit Remove
Name	Transport Protocol and Parameters	Timeout (min)	Configure						
RTP	UDP src port: 0-65535, dst port: 10000-20000 UDP src port: 0-65535, dst port: 56000-59200	1	Edit Remove						

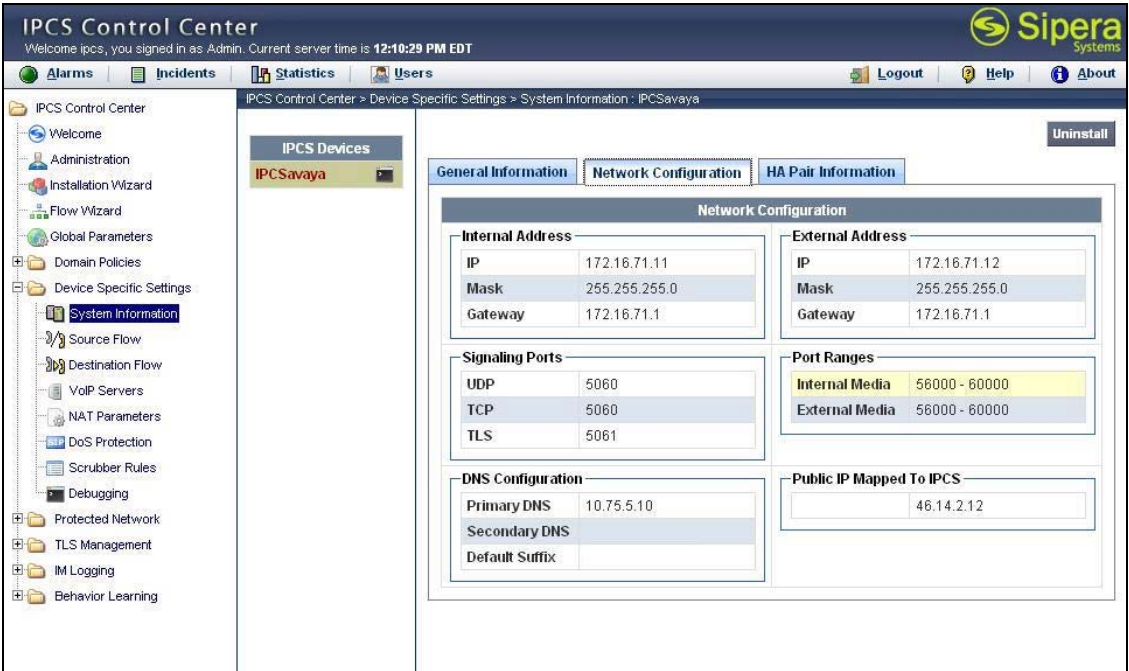
7. Configure Sipera IPCS

This section covers the configuration of IPCS at the main site. It must be repeated for IPCS at the branch using values appropriate for the branch from **Figure 1**. It is assumed that the IPCS software has already been installed. For additional information on these installation tasks, refer to [8].

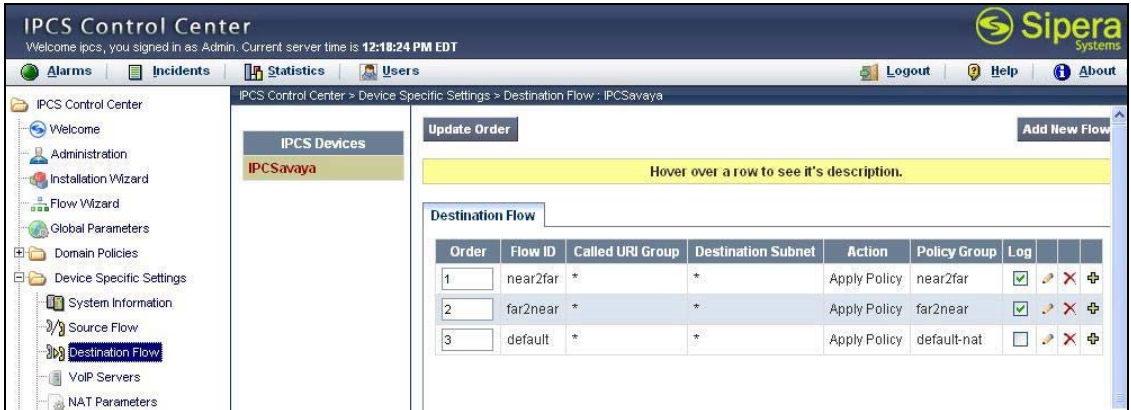
Step	Description
1.	<p>IPCS is configured via the Mozilla Firefox web browser. IPCS does not support Internet Explorer. To access the web interface, enter <a href="https://<ip-addr>/ipcs/">https://<ip-addr>/ipcs/ in the address field of the web browser, where <ip-addr> is the IP address of IPCS.</p> <p>Log in with the appropriate credentials. Click Sign In.</p> 

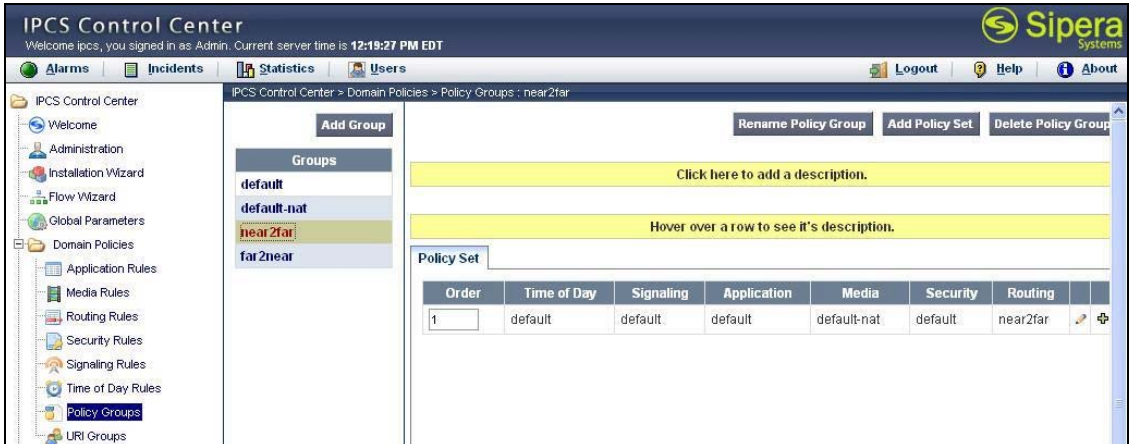
Step	Description
2.	<p>The main page of the IPCS Control Center will appear.</p> 

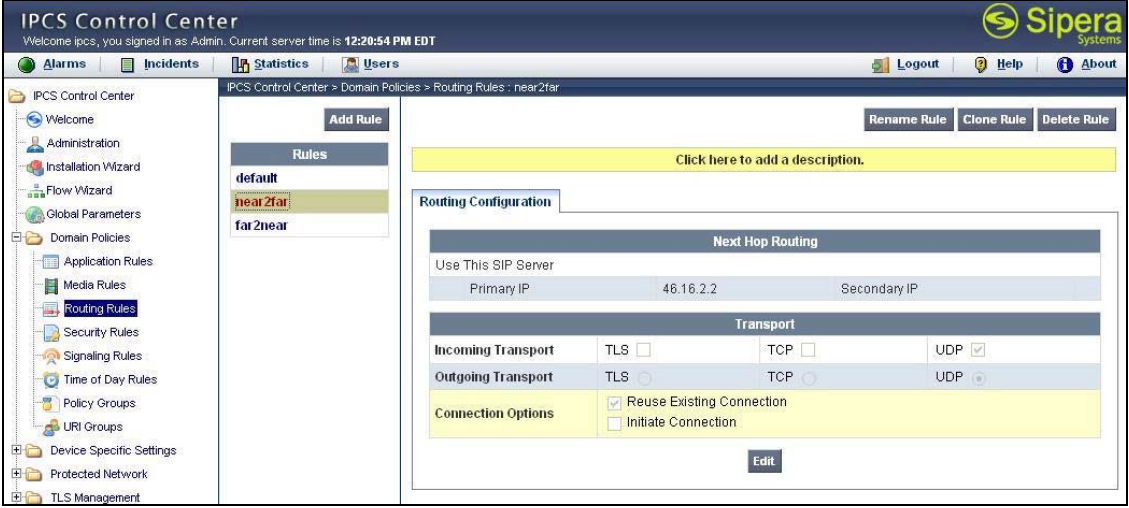
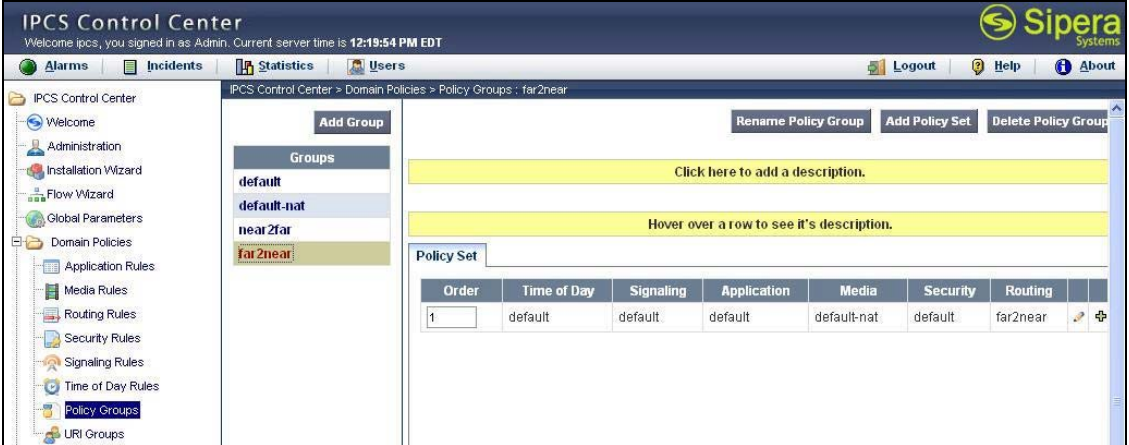
Step	Description
3.	<p>To view system information that was configured during installation, navigate to IPCS Control Center→Device Specific Settings→System Information. From the list of IPCS Devices in the middle pane, select the only IPCS located at the main site named IPCSavaya. The system information is shown in the right pane. The General Information tab shows the values of the following key parameters.</p> <ul style="list-style-type: none"> • System Type: <i>Standalone</i> • Management IP: IP address of management port • Network Type: <i>DMZ Only</i> • Placement: <i>DMZ: Both Firewall & NAT</i> <p>Click the Network Configuration tab to view the network settings.</p> 

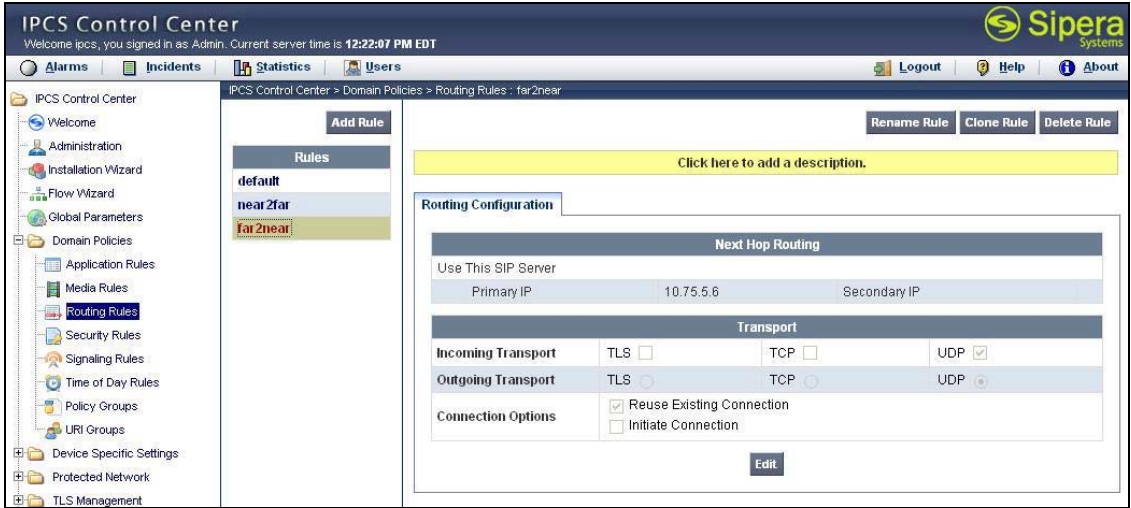
Step	Description
4.	<p>The Network Configuration tab shows the Internal Address, External Address, and DNS Configuration information provided during installation and corresponds to Figure 1. The compliance test did not use a DNS server, but an entry was required by IPCS. An arbitrary IP address was used for the Primary DNS field. In addition, the Public IP Mapped To IPCS value was provided during installation. Default values were used for all other fields.</p> 

Step	Description
5.	<p>Source Flows</p> <p>A source flow defines a collection of traffic based on its source parameters and maps it to a destination flow ID. The destination flows are shown in Step 6 and ultimately will define the policy and routing applied to the source traffic defined in the source flow.</p> <p>To define a new source flow, navigate to IPCS Control Center→Device Specific Settings→Source Flow. Select the IPCS device name in the middle pane. Select the Add New Flow button in the right pane. A new page is opened (not shown) where the source flow information can be entered and submitted.</p> <p>The list below shows the source flows used for the compliance test. The first entry below shows any traffic coming from Source Subnet 46.16.2.0/24 (public WAN side) was mapped to destination flow (Flow ID) <i>far2near</i>. The second entry below shows any traffic coming from Source Subnet 10.75.5.0/24 (private LAN side) was mapped to destination flow (Flow ID) <i>near2far</i>.</p> <div></div>

Step	Description
6.	<p>Destination Flows</p> <p>A destination flow defines a collection of traffic based on its destination parameters and maps a Policy Group and Action to the flow. The criteria defined in the destination flow is applied to the traffic coming from the source flow in Step 5 which has already applied a set of criteria based on the source parameters.</p> <p>To define a new destination flow, navigate to IPCS Control Center→Device Specific Settings→Destination Flow. Select the IPCS device name in the middle pane. Select the Add New Flow button in the right pane. A new page is opened (not shown) where the source flow information can be entered and submitted.</p> <p>The list below shows the destination flows used for the compliance test. The first destination flow below (<i>near2far</i>) shows that the destination criteria will match anything, since both the Called URI Group and Destination Subnet columns contain a *. In addition, the <i>near2far</i> flow has an Action of <i>Apply Policy</i> and a Policy Group of <i>near2far</i>. Thus, the result of the <i>near2far</i> destination flow is to apply the <i>near2far</i> policy to all traffic from source flow 2 (Source Subnet 10.75.5.0/24). Similarly, the <i>far2near</i> destination flow will result in applying the <i>far2near</i> policy to all traffic from source flow 1 (Source Subnet 46.16.2.0/24).</p> 

Step	Description
7.	<p>Policy Group (<i>near2far</i>)</p> <p>A policy group defines a set of rules that may be applied to different aspects of the destination flow.</p> <p>To define a new policy group, navigate to IPCS Control Center→Domain Policies→Policy Groups. Select the Add Group button in the middle pane. A new page is opened in the right pane (not shown) where the policy group information can be entered and submitted.</p> <p>The example below shows the <i>near2far</i> policy group assigned to the <i>near2far</i> destination flow in the previous step. The default rule is assigned to each policy category except for Media and Routing. The Media rule is assigned <i>default-nat</i>. For details on the default rules, including <i>default-nat</i>, see [9]. The Routing rule, <i>near2far</i>, is defined in the next step.</p> 

Step	Description
8.	<p>Routing Rule (<i>near2far</i>) A routing rule defines how routing is performed on the destination flow.</p> <p>To define a new routing rule, navigate to IPCS Control Center→Domain Policies→Routing Rules. Select the Add Rule button in the middle pane. A new page is opened in the right pane (not shown) where the routing rule information can be entered and submitted.</p> <p>The example below shows the <i>near2far</i> rule assigned to the <i>near2far</i> policy group in the previous step and used by the <i>near2far</i> destination flow. In this rule, the next hop is defined as the mapped public IP address of the far-end IPCS (46.16.2.12). It also specifies the use of UDP for the transport protocol in both the incoming and outgoing directions.</p> 
9.	<p>Policy Group (<i>far2near</i>) Repeat Step 7 to create the <i>far2near</i> policy group shown below.</p> 

Step	Description
10.	<p>Routing Rule (<i>far2near</i>) Repeat Step 8 to create the <i>far2near</i> routing rule shown below and used by the <i>far2near</i> destination flow. In this rule, the next hop is defined as the IP address of the local Avaya SES (10.75.5.6). All other values are configured the same as Step 8.</p> 

8. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of Siperia 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.

8.1. General Test Approach

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

8.2. Test Results

IPCS 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 from both SIP and non-SIP endpoints at the main site to the branch site.
- Calls from the branch site to both SIP and non-SIP endpoints at the main site.
- 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 an IPCS 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 3.1, Step 6**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.
- With two IPCS devices in the signaling path, additional Via and Route headers are added to the SIP messages. In some scenarios, this leads to a UDP packet that is too large and is fragmented. To handle this case, a configuration change was required in the Linux OS of the IPCS device. This change was tested as part of the compliance test and all test cases affected by the fragmented packet passed. This Linux change is expected to be included in a future release of the IPCS installer software. For more information, contact Sipera technical support.

9. 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 at the main site to the branch site.
- Verify that calls can be placed from the branch site to both SIP and non-SIP endpoints at the main site.

10. Support

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

11. Conclusion

Sipera IPCS passed compliance testing with the observations listed in **Section 8.2**. These Application Notes describe the procedures required to configure Sipera IPCS to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support SIP trunking between enterprise locations with NAT traversal as shown in **Figure 1**.

12. 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] *Concepts and Examples ScreenOS Reference Guide*, Release 5.4.0, Rev.B.
- [8] *IPCS210_310 Installation Guide (230-5210-31)*.
- [9] *IPCS Administration Guide (010-5310-31)*.

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

Product documentation for Netscreen products may be found at <http://www.juniper.net>.

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

©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ 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.