Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager to Support Remote Users with NAT Traversal - Issue 1.0

Abstract

These Application Notes describes the procedures for configuring Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager 5.1.

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 remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network with network address translation (NAT) traversal.

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 describes the procedure for configuring Sipera IPCS 310 with Avaya SIP Enablement Services (SES) and Avaya Communication Manager 5.1.

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 remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network with network address translation (NAT) traversal.

1.1. Interoperability Compliance Testing

The compliance testing tested interoperability between IPCS 310 (software version 3.7.0.Q30) and Avaya SES (5.1) / Avaya Communication Manager (5.1) by making calls between remote users and users at the main site. The following specific SIP telephony functions were tested in the test environment set up for the compliance test:

- Successful registration of remote user SIP endpoints on Avaya SES through IPCS 310
- Calls from remote users with and without NAT to users at the main site via IPCS 310
- Calls from users at the main site to remote users with and without NAT via IPCS 310
- PSTN calls to/from remote users with and without NAT via IPCS 310
- Calls between remote users with and without NAT via IPCS 310
- Basic call scenarios using G.711 and G.729 codecs
- SIPPING-19 supplementary call features (including Hold, Transfer, Conference, Bridged Calls, etc.)
- Advanced call features provided via Feature Name Extensions (FNE) on Avaya Communication Manager (such as Call Forwarding, Call Park, Call Pickup, Automatic Redial, Send All Calls, etc.)
- Voice mail support for remote users
- Different types of remote user SIP endpoints (including Avaya 4600 series IP phones, Avaya 9600 series IP phones, Avaya one-X Desktop Edition soft phone, and Avaya one-X mobile phone)

1.2. Support

Technical support for IPCS 310 can be obtained by contacting Sipera at

- Phone: (866) 861-3113
- Email: support@sipera.com
- Web: http://www.sipera.com

2. Configuration

Figure 1 illustrates the test configuration. The test configuration shows several remote users connected by different means to an untrusted IP network to access the SIP infrastructure at a main enterprise site. The main site has a 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 the main site is an IPCS 310. The public side of the IPCS is connected to the untrusted network and the private side is connected to the trusted corporate LAN. The IPCS is assigned two IP addresses on both its public and private interfaces. One pair (public/private) of IP addresses is used by the remote Avaya one-X Mobile and the Avaya one-X Desktop Edition soft phone while the other pair is used by all other remote endpoints. This separation is necessary for supporting the two sets of remote users internal to the IPCS. The IPCS could also reside in the demilitarized zone (DMZ) of the enterprise but this configuration was not tested.

All SIP traffic between the remote endpoints and the enterprise site flows through the IPCS. In this manner, the IPCS can protect the main site's infrastructure from any SIP-based attacks. In addition, HTTP transfers required by the remote endpoints to gather licensing or configuration data, also passes through the IPCS. All other traffic bypasses the IPCS and flows directly between the untrusted network and the private LAN of the enterprise if permitted by the data 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 an Avaya 4600 Series IP Telephone (with SIP firmware), Avaya 9600 Series IP Telephones (with SIP and H.323 firmware), an Avaya one-X Desktop Edition soft phone, an Avaya 6408D Digital Telephone and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. A PSTN number assigned to the ISDN-PRI trunk at the main site is mapped to a telephone extension at the main site or to a remote telephone extension depending on the test cases being executed.

The SIP endpoints located at the main site are registered to Avaya SES. All calls originating from Avaya Communication Manager at the main site and destined for the remote users will be routed through the on-site Avaya SES, IPCS, and across the untrusted IP network.

The remote users are comprised of the following endpoints:

- One Avaya 4600 and one 9600 Series IP Telephone (with SIP firmware) connected directly to the untrusted network.
- One Avaya 4600 and one 9600 Series IP Telephone (with SIP firmware) connected behind a Netscreen-5GT firewall. This firewall is configured to perform both network address and port translation (NAPT).
- One Avaya one-X Desktop Edition soft phone and one Avaya one-X Mobile phone connected behind a second Netscreen-5GT firewall. This firewall is configured to perform both network address and port translation.

The voice communication across the untrusted network varies depending on the type of remote endpoint. Avaya 9600 IP Telephones use SIP over TLS and SRTP for the media stream. Avaya 4600

IP Telephones use SIP over UDP and RTP for the media stream. The Avaya one-X Desktop Edition soft phone and the Avaya one-X Mobile phone uses SIP over TCP and RTP for the media stream.

The remote users register with Avaya SES through IPCS. These telephones use the public IP address of IPCS at the main site as their configured server. IPCS will forward any registration messages it receives from the remote endpoints to Avaya SES. Thus, the IPCS appears to the Avaya SES as a set of SIP endpoints. All calls originating from the remote users are routed across the untrusted IP network, IPCS and Avaya SES to Avaya Communication Manager at the main site.

All SIP telephones, both local and remote, use the HTTP server at the main site to obtain their configuration files. The same configuration files are used for both local and remote endpoints. The IPCS will perform any address translation of private IP addresses in the configuration files before sending the files to the remote endpoints. All SIP endpoints both local and remote use the same SIP domain: ***business.com***.

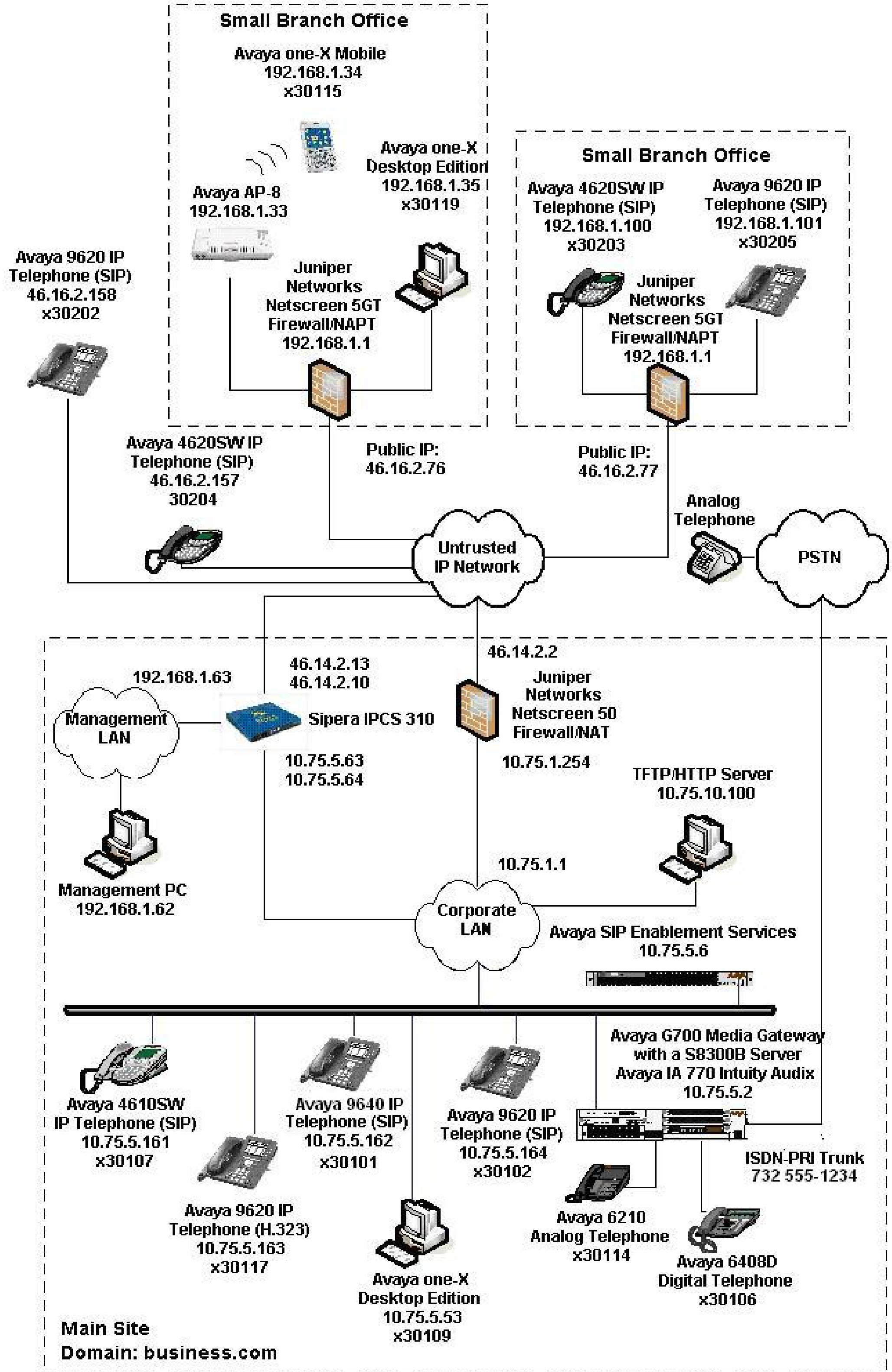


Figure 1: IPCS 310 Test Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server	Avaya Communication Manager 5.1.1 Service Pack (01.1.415.1-16402) with Avaya IA 770 Intuity Audix
Avaya G700 Media Gateway	28.18.0
Avaya SIP Enablement Services (SES)	SES-5.1.1.0-415.1
Avaya 9620 IP Telephone (H.323)	Avaya one-X Deskphone Edition 1.5
Avaya 4610SW IP Telephones (SIP) Avaya 4620SW IP Telephones (SIP)	2.2.2
Avaya 9620 IP Telephones (SIP) Avaya 9630 IP Telephones (SIP) Avaya 9640 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.0.3
Avaya one-X Desktop Edition (SIP)	2.1 Service Pack 2
Avaya AP-8	v2.5.2
Avaya one-X Mobile for Symbian Dual Mode Nokia E61	4.3 FW 3.0633.09.04
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (Management PC and TFTP/HTTP Server)	Windows XP Professional SP2
Juniper Networks Netscreen-50	5.4.0r9.0
Juniper Networks Netscreen-5GTs	5.4.0r3a.0
Sipera IPCS 310	3.7 (Build Q.30)

4. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration at the main site 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 internal SIP endpoint in the configuration as described in [3] and [4].

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 the configuration of the remote SIP endpoints.

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.

4.1. Summary of Initial SIP Installation

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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

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 **display ip-network-region** command to view these settings. The example below shows the values used for the compliance test.

- The **Authoritative Domain** field was configured to match the domain name configured on Avaya 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.
- A descriptive name was entered for the **Name** field.
- **IP-IP Direct Audio** (shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya 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 Group** form.
- The **Codec 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 1 was selected. 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 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
    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
```

</td></tr>
</table>

Step	Description
2.	**Codecs** 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.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729A            n         2        20
 3:
```

Step	Description
3.	**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]. ▪ The **Group Type** was set to ***sip***. ▪ The **Transport Method** was set to the recommended default value of ***tls*** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061.*** ▪ The **Near-end Node Name** was set to ***procr***. This node name maps to the IP address of the Avaya Server. Node names are defined using the **change node-names ip** command. ▪ The **Far-end Node Name** was set to ***SES***. This node name maps to the IP address of Avaya SES as defined using the **change node-names ip** command. ▪ The **Far-end Network Region** was set to ***1***. This is the IP network region which contains Avaya SES. ▪ The **Far-end Domain** was set to ***business.com***. 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. ▪ **Direct IP-IP Audio Connections** was set to ***y***. This field must be set to ***y*** to enable media shuffling on the SIP trunk. ▪ The **DTMF over IP** field was set to the default value of ***rtp-payload***. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833. ▪ The default values were used for all other fields.

```
display signaling-group 1
                                SIGNALING GROUP

 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? y
                                                        IP Audio Hairpinning? n
        Enable Layer 3 Test? n
 Session Establishment Timer(min): 3
```

Step	Description
4.	**Trunk Group** 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 using the parameters highlighted below. All other fields were set as described in [3]. On **Page 1**: ▪ The **Group Type** field was set to ***sip***. ▪ A descriptive name was entered for the **Group Name**. ▪ An available trunk access code (TAC) that was consistent with the existing dial plan was entered in the **TAC** field. ▪ The **Service Type** field was set to ***tie***. ▪ The **Signaling Group** was set to the signaling group shown in the previous step. ▪ 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 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. ▪ The default values were used for all other fields.

```
display 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? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                      Signaling Group: 1
                                                    Number of Members: 24
```

Step	Description

5.	**Trunk Group – continued**
	On **Page 3**:
	▪ The **Numbering Format** field was set to ***public***. This field specifies the format of the calling party number sent to the far-end.
	▪ The default values were used for all other fields.
	<pre>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</pre>

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 **Step 4** and **Step 5**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across any trunk group (**Trk Grp** 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.
	<pre>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
	 5 3 **5** Maximum Entries: 9999</pre>

4.2. OPS Configuration

This section describes the configuration of OPS stations, which is required for each SIP endpoint. These Application Notes assume that all necessary configuration has been performed for the SIP endpoints at the main location including the creation of OPS stations. This section will only focus on the remote endpoints. For complete details on configuring OPS stations refer to [4]. For complete details on configuring a specific endpoint type refer to [7] through [14].

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>System Parameters
Use the display system-parameters customer-options command to verify Avaya Communication Manager has sufficient OPS capacity available to add the OPS stations needed for the remote SIP endpoints in Figure 1. If there is insufficient capacity, contact an authorized Avaya sales representative or business partner to make the appropriate changes.
<pre>
display system-parameters customer-options   Page   1 of 11
                                OPTIONAL FEATURES

     G3 Version: V15   Software Package: Standard
       Location: 1   RFA System ID (SID): 1
       Platform: 12   RFA Module ID (MID): 1

                                                               USED
                                Platform Maximum Ports: 3200 120
                                      Maximum Stations: 2400 50
                              Maximum XMOBILE Stations: 0   0
                    Maximum Off-PBX Telephones - EC500: 0   0
                    Maximum Off-PBX Telephones -   OPS: 100   21
                    Maximum Off-PBX Telephones - PBFMC: 0   0
                    Maximum Off-PBX Telephones - PVFMC: 0   0
                    Maximum Off-PBX Telephones - SCCAN: 0   0
</pre></td></tr>
</table>

Step	Description
2.	**Stations** To add a station, use the **add station *n*** command where ***n*** is an unused extension number. For the Avaya 4600 and 9600 Series IP Telephones, enter the actual phone type in the **Type** field. For the Avaya one-X Desktop Edition and Avaya one-X Mobile enter ***4620*** in the **Type** field. Enter ***IP*** in the **Port** field. Enter a descriptive name in the **Name** field. In the case of the Avaya one-X Desktop Edition, the **IP Soft phone** field must be set to ***y***. Otherwise, set this field to ***n***. The default values may be retained for all other fields. The example below shows the configuration of one of the Avaya 9600 Series IP Telephones.

```
add station 30202                                            Page   1 of   6
                                     STATION

Extension: 30202                         Lock Messages? n               BCC: 0
     Type: 9630                          Security Code:                  TN: 1
     Port: IP                          Coverage Path 1: 1               COR: 1
     Name: Remote SIP1                 Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 30202
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP Soft phone? n

                                              Customizable Labels? y
```

Step	Description
3.	**Stations – Continued** On **Page 2**, set **Restrict Last Appearance** to ***n***. This will allow the last call appearance to be used for either an incoming or outgoing call. Set the **Bridged Call Alerting** field to ***y***. This will allow this station to ring on a bridged call.

```
add station 30202                                            Page   2 of   6
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                    Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? y                       Restrict Last Appearance? n
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: enhanced
    MWI Served User Type:                       Display Client Redirection? n
              AUDIX Name:                      Select Last Used Appearance? n
                                                 Coverage After Forwarding? s

                                               Direct IP-IP Audio Connections? y
  Emergency Location Ext: 30202        Always Use? n IP Audio Hairpinning? n
```

Step	Description
4.	**Stations – Continued** On **Page 3**, under BUTTON ASSIGNMENTS, create the number of call appearances supported by the endpoint. To create a call appearance, enter ***call-appr*** as the button assignment. Most endpoints will use 3 or 4 call appearances; the Avaya one-X Mobile will have 5. Some Feature Name Extensions (FNEs) require the assignment of feature buttons in order to operate. The Automatic Callback FNE requires the assignment of an ***auto-cback*** button. This button assignment is shown in the example below.

```
add station 30202                                             Page   4 of   6
                                    STATION
 SITE DATA
       Room:                                             Headset? n
       Jack:                                             Speaker? n
      Cable:                                            Mounting: d
      Floor:                                         Cord Length: 0
   Building:                                           Set Color:

ABBREVIATED DIALING
     List1:                   List2:                   List3:




BUTTON ASSIGNMENTS
 1: call-appr                          5:
 2: call-appr                          6: auto-cback
 3: call-appr                          7:
 4: call-appr                          8:

    voice-mail Number:
```

Step	Description
5.	**Off-pbx Station Mapping** Map the Avaya Communication Manager extension to the Avaya SES media server extension defined in **Section 5.2**, **Step 2** with the **add off-pbx-telephone station-mapping** command. Enter the values as shown below for all endpoints other than the Avaya one-X Mobile. For the Avaya one-X Mobile settings, see the next step. ▪ **Station Extension**: Avaya Communication Manager extension ▪ **Application**: ***OPS*** ▪ **Phone Number**: Avaya SES media server extension ▪ **Trunk Selection**: The SIP trunk group number defined in **Section 3.1**. ▪ **Configuration Set**: Enter a valid configuration set which contain the default values.

```
add off-pbx-telephone station-mapping                          Page   1 of   2
                 STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station        Application Dial   CC  Phone Number      Trunk       Config
Extension                  Prefix                       Selection   Set
30202             OPS           -     30202              1          1
                                -
```

Step	Description

6.	**Off-pbx Station Mapping – Page 1 Continued**
	For the Avaya one-X Mobile settings, see the values below. For complete details for configuring the Avaya one-X Mobile refer to [13] and [14].
	<pre>add off-pbx-telephone station-mapping Page 1 of 2
	                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION
	
	 Station Application Dial CC Phone Number Trunk Config
	 Extension Prefix Selection Set
	 30115 PVFMC 30115 1 1
	 30115 PBFMC 17325552999 ars 1</pre>

7.	**Off-pbx Station Mapping – Page 2**
	On **Page 2**, set the **Call Limit** to the number of call appearances set on the station form in **Step 4**. Verify that the **Mapping Mode** is set to ***both***. This setting allows the OPS station to both originate and terminate calls. Set the **Bridged Calls** field to ***both*** to allow bridging on this extension. The default values may be retained for all other fields.
	<pre>add off-pbx-telephone station-mapping Page 2 of 2
	                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION
	
	 Station Call Mapping Calls Bridged
	 Extension Limit Mode Allowed Calls
	 30202 4 both all both</pre>

8.	Repeat **Steps 2 - 7** for each remaining remote endpoint.

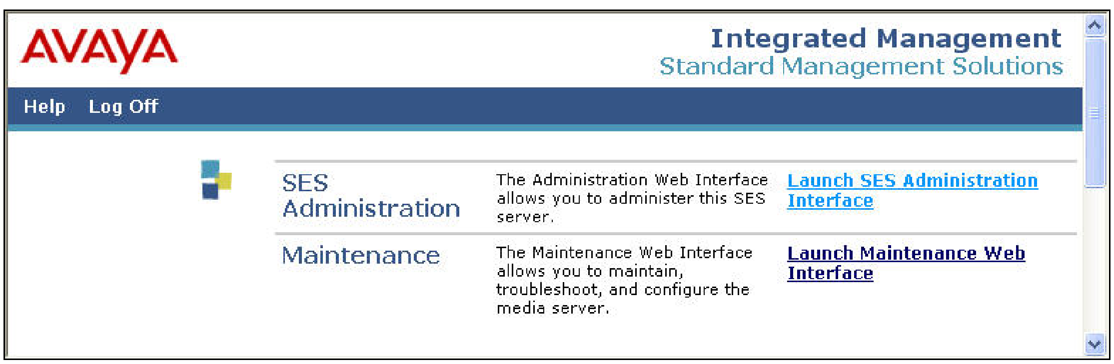
5. Configure Avaya SIP Enablement Services

This section covers the configuration of Avaya SES at the main site. 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].

This section is divided into two parts. **Section 5.1** summarizes the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It also describes any deviations from the standard procedures, if any. Note that this section does not attempt to show the installation procedures in their entirety. **Section 5.2** describes procedures beyond the initial SIP installation procedures that are necessary for interoperating with IPCS. This includes configuration of the remote SIP endpoints. The creation of users and media server extensions for the SIP endpoints at the main site are not covered here. These procedures are covered in [4].

5.1. Summary of Initial Configuration Parameters

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

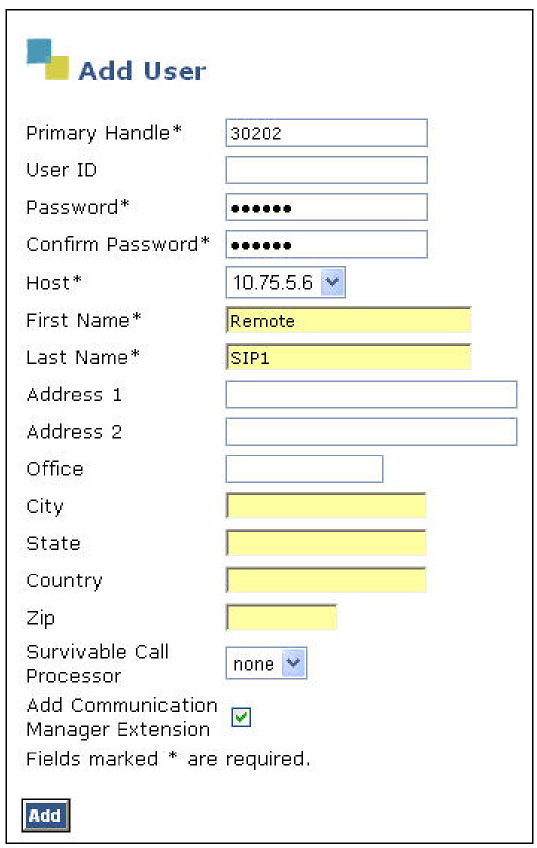
Step	Description
1.	**Login** Access the Avaya SES administration web interface by accessing http://<*ip-addr*>/admin in an Internet browser, where <*ip-addr*> is the IP address of the Avaya SES server. Log in with the appropriate credentials and then select the **Launch SES Administration Interface** link from the main page. 

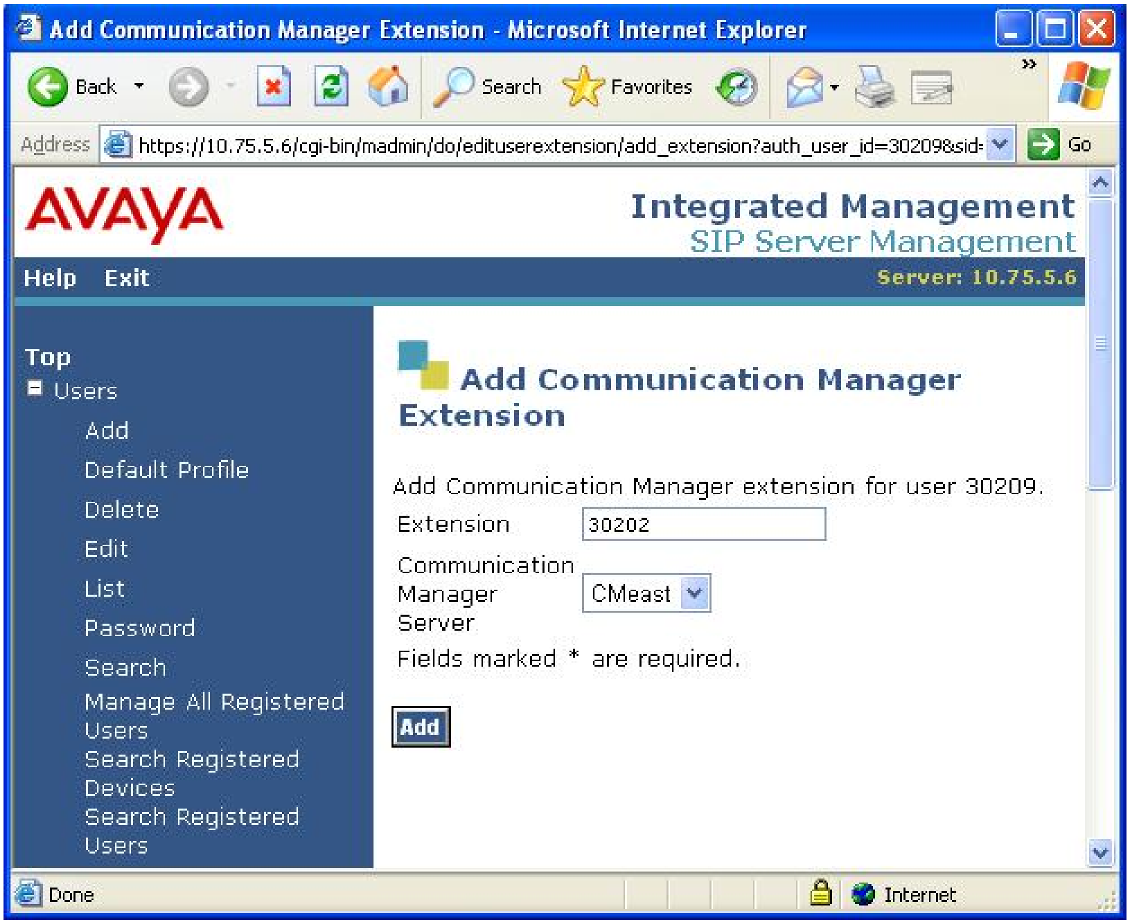
Step	Description
2.	**Top Page** The Avaya SES **Top** Page for the administrative interface will be displayed as shown below.

Step	Description
3.	**Initial Configuration Parameters** 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 **Top** page shown in the previous step. • SIP Domain: ***business.com*** (To view, navigate to **Server Configuration→System Properties**) • Host IP Address (SES IP address): ***10.75.5.6*** • Host Type: ***SES combined home-edge*** (To view, navigate to **Hosts→List**; click **Edit**) • Communication Manager Server Interface Name: ***CMeast*** • SIP Trunk Link Type: ***TLS*** • SIP Trunk IP Address (Avaya Server IP address): ***10.75.5.2*** (To view, navigate to **Media Servers→List**; click **Edit**)

5.2. IPCS Specific Configuration

This section describes additional configuration necessary for interoperating with the IPCS. In particular, this section describes the configuration of user and media server extensions for the remote SIP endpoints.

Step	Description
1.	**SIP Users** A user must be added on Avaya SES for each of the remote SIP endpoints created on Avaya Communication Manager in **Section 4.2**, **Steps 2 – 8**. From the left pane, navigate to **Users** → **Add**. Enter the values as shown below. ▪ **Primary Handle**: Enter the extension for this user. ▪ **Password**: Enter a valid password for logging into the SIP endpoint. ▪ **Confirm Password**: Re-enter the password. ▪ **Host**: Select the Avaya SES server from the pull-down menu. ▪ **First Name**: Any descriptive name. ▪ **Last Name**: Any descriptive name. Check the **Add Communication Manager Extension** checkbox. Click the **Add** button to proceed. A confirmation window will appear. Click **Continue** on this new page to proceed. 

Step	Description
2.	**Communication Manager Extension** The **Add Communication Manager Extension** page will appear. In the **Extension** field, enter the Avaya Communication Manager extension associated with this user created in **Section 4.2**, **Step 2**. In the **Media Server** field, select from the pull-down menu the name of the media server shown in **Section 5.1**, **Step 3**. Click the **Add** button to complete the operation. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>Repeat Steps 1 - 2 for each of the remaining remote SIP endpoints. The following screen shows some of the local and remote SIP endpoints registered with the Avaya SES.

</td></tr>
</table>

6. Configure the Avaya SIP Telephones

The SIP telephones at the main site will use Avaya SES as the call server. The SIP telephones of the remote users will use the mapped public IP address of IPCS as the call server.

The table below shows an example of the SIP telephone network settings for both the main site and the remote users. For complete details on configuring a specific endpoint type refer to [7] through [14]. All local and remote endpoints that use the 46xxxsettings.txt configuration file will use the same file for both 4600 Series and 9600 Series IP Telephones. An example of the file used in the compliance test is shown in **Appendix A**. **Appendix B** shows the configuration file used for the Avaya one-X Mobile.

	Main Site (9600)	**Remote User w/o NAT (9600)**	**Remote User w/ NAT (4600)**
Extension	30101	30202	30203
IP Address	10.75.5.162	46.16.2.158	192.168.1.100
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Call Server	10.75.5.6	46.14.2.13	46.14.2.13
Router	10.75.5.1	46.16.2.1	192.168.1.1
File Server	10.75.10.100	46.14.2.13	46.14.2.13
License Server	N/A	N/A	N/A

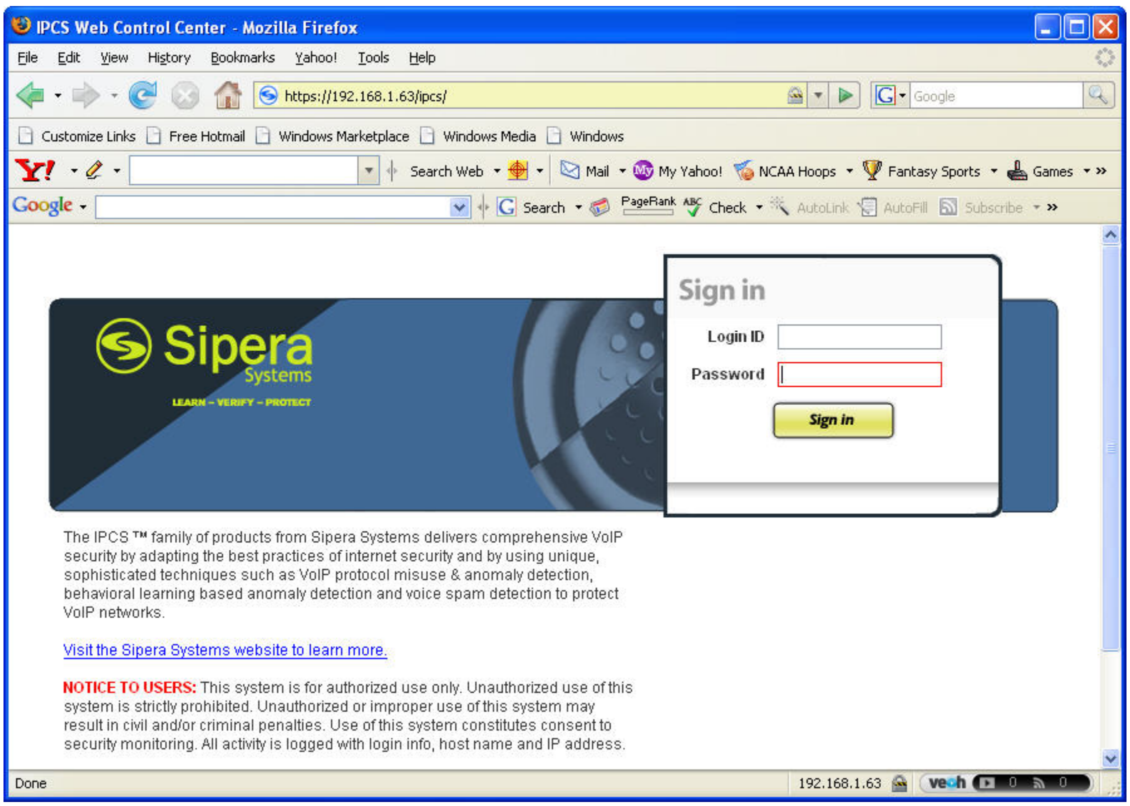
	Remote User w/ NAT (Avaya one-X Desktop Edition)	**Remote User w/ NAT (Avaya one-X Mobile)**
Extension	30119	30115
IP Address	192.168.1.35	192.168.1.34
Subnet Mask	255.255.255.0	255.255.255.0
Call Server	46.14.2.10	46.14.2.10
Router	192.168.1.1	192.168.1.1
File Server	N/A	46.14.2.10
License Server	46.14.2.10	N/A

7. 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 [15].

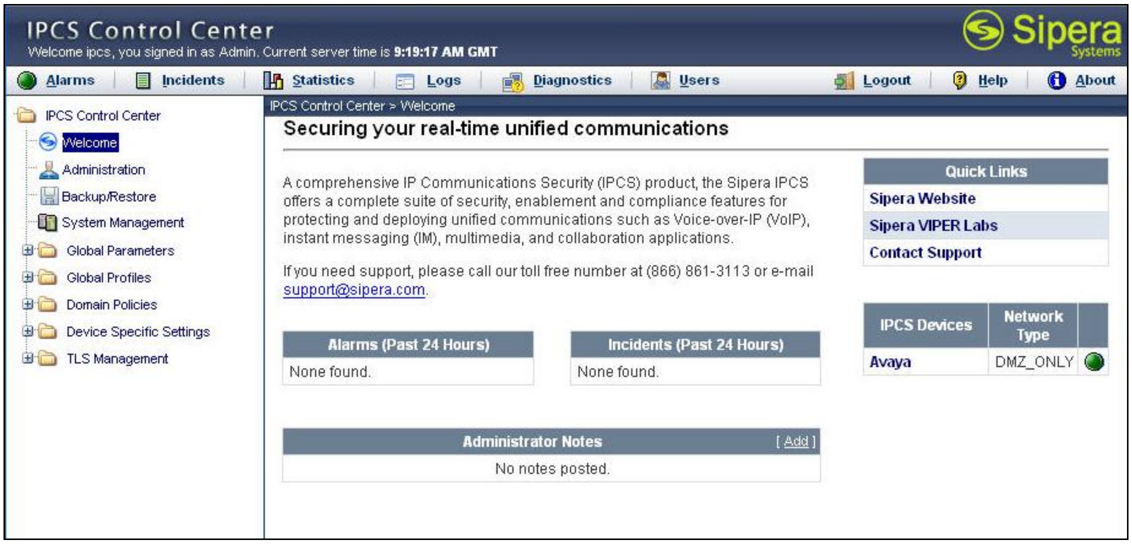
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>IPCS is configured via the Mozilla Firefox web browser. IPCS does not support Internet Explorer. To access the web interface, enter https://<<i>ip-addr</i>>/ipcs in the address field of the web browser, where <<i>ip-addr</i>> is the management LAN IP address of IPCS.

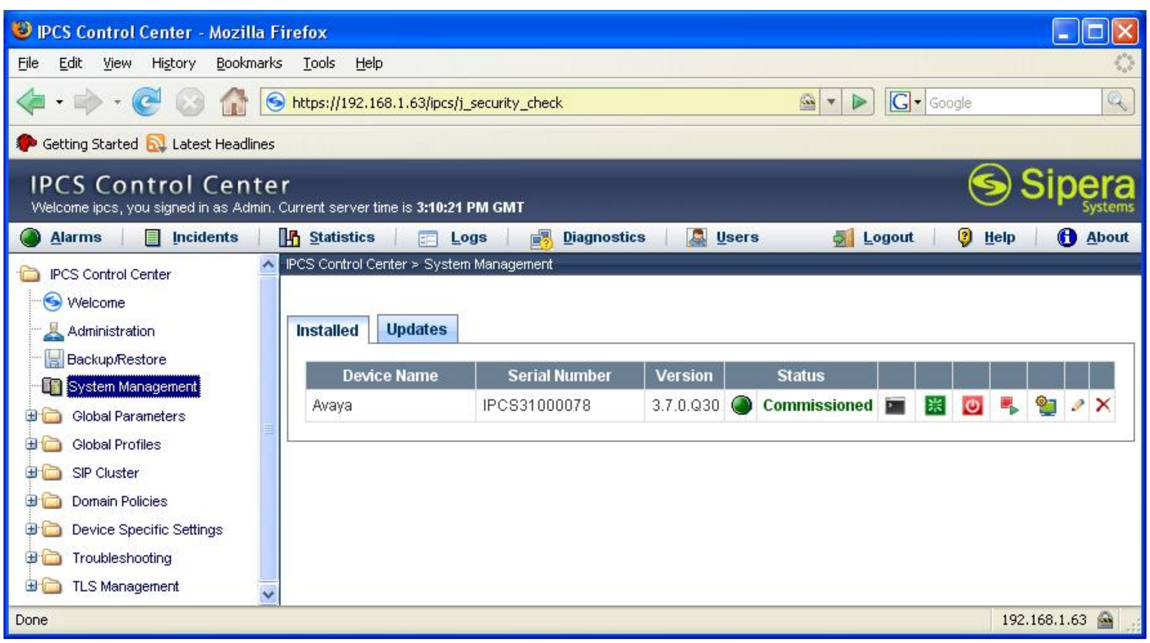
Log in with the appropriate credentials. Click Sign In.



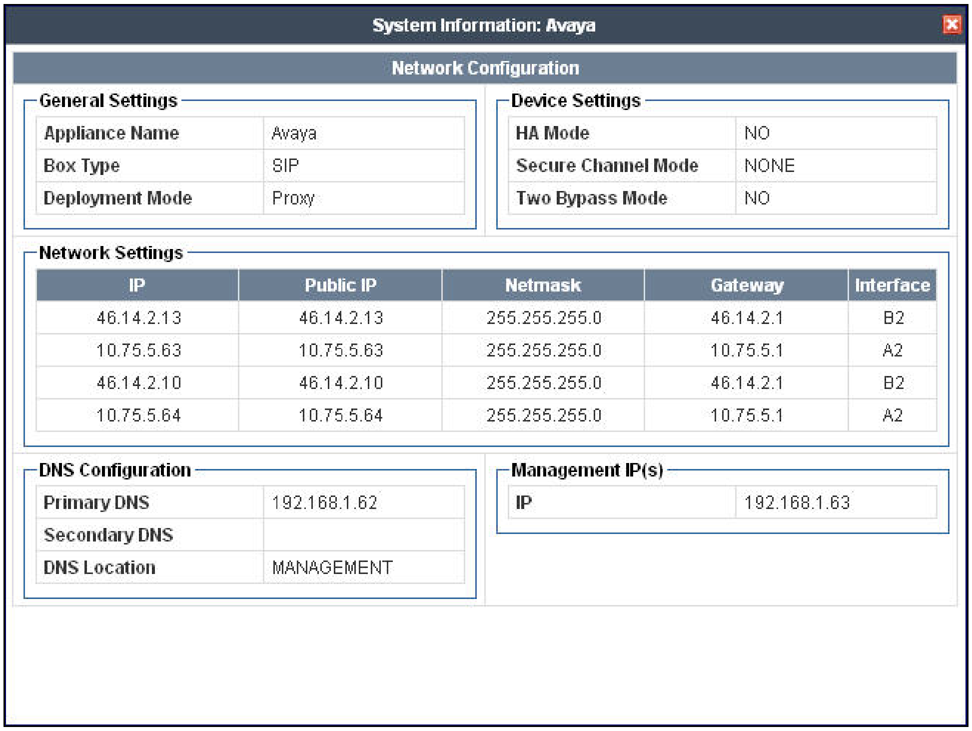
</td></tr>
</table>

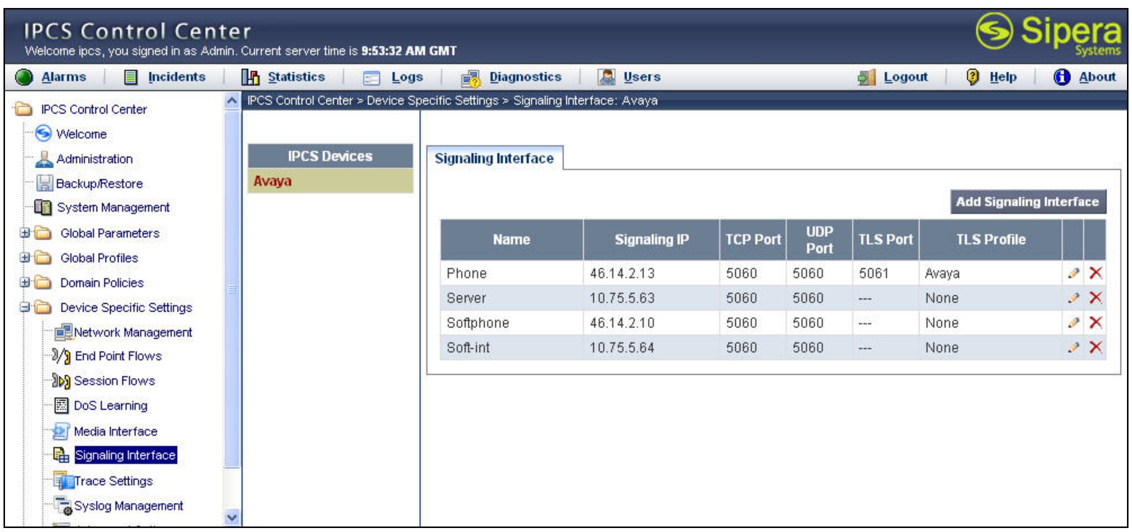
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>The main page of the IPCS Control Center will appear.

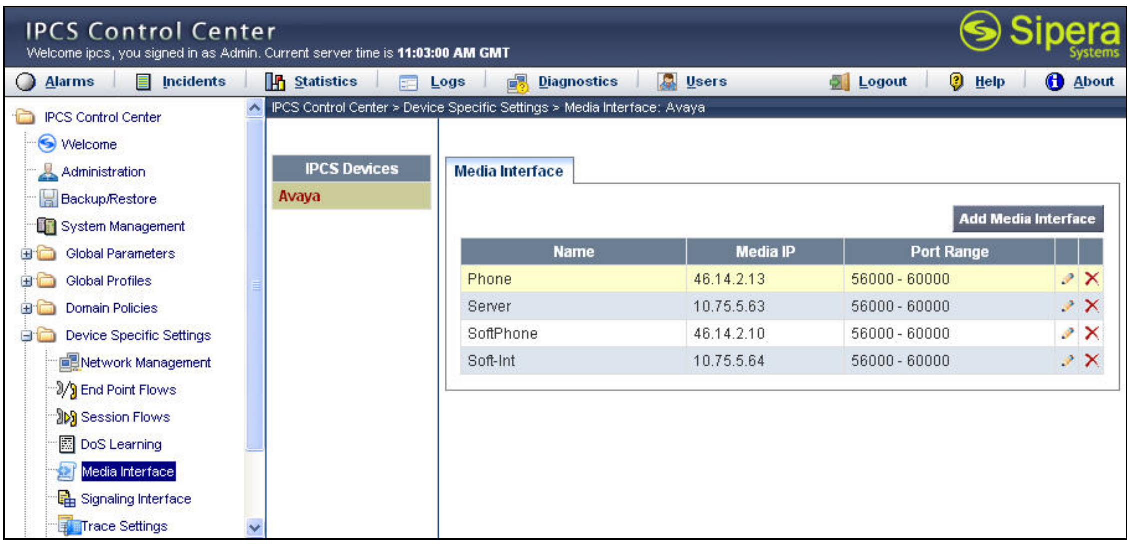

</td></tr>
<tr><td>3.</td><td>To view system information that was configured during installation, navigate to IPCS Control Center→System Management. A list of installed devices is shown in the right pane. In the case of the compliance test, a single device named Avaya is shown. To view the configuration of this device, click the monitor icon (the third icon from the right for the Avaya device entry).


</td></tr>
</table>

Step	Description
4.	The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** 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. The **Box Type** was set to ***SIP*** and the **Deployment Mode** was set to ***Proxy***. Default values were used for all other fields.



Step	Description
5.	**Signaling Interface** A signaling interface is created that maps a signaling interface name to an IP address and a set of ports and transport protocols that can be used on that interface. To define a new signaling interface, navigate to **IPCS Control Center→Device Specific Settings→Signaling Interface**. Select the IPCS device name in the middle pane. Select the **Add Signaling Interface** button in the right pane. A new page is opened (not shown) where the new information can be entered and submitted. The example below shows the four interfaces created for the compliance test, one for each of the IP addresses assigned to IPCS. Only the interface named ***Phone*** supports TLS. All other interfaces support UDP and TCP. It should also be noted that even though the interface names for IP addresses ***46.14.2.10*** and ***10.75.5.64*** are named ***Soft phone*** and ***Soft-int*** respectively, these interfaces were also used for the Avaya one-X Mobile remote user in the compliance test. 

Step	Description
6.	**Media Interface** A media interface maps a media interface name to an IP address and a range of ports that can be used on that interface. A media interface is created similar to a signaling interface by navigating to **IPCS Control Center→Device Specific Settings→Media Interface**. The results used by the compliance test are shown below. It should also be noted that even though the interface names for IP addresses ***46.14.2.10*** and ***10.75.5.64*** are named ***Soft phone*** and ***Soft-Int*** respectively, these interfaces were also used for the Avaya one-X Mobile remote user in the compliance test. 

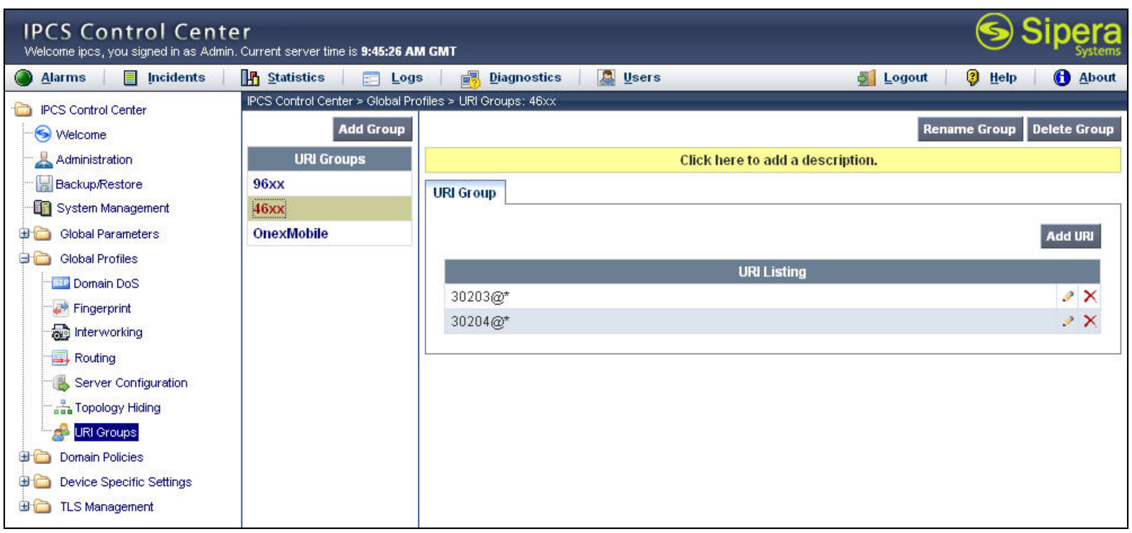
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>

URI Groups

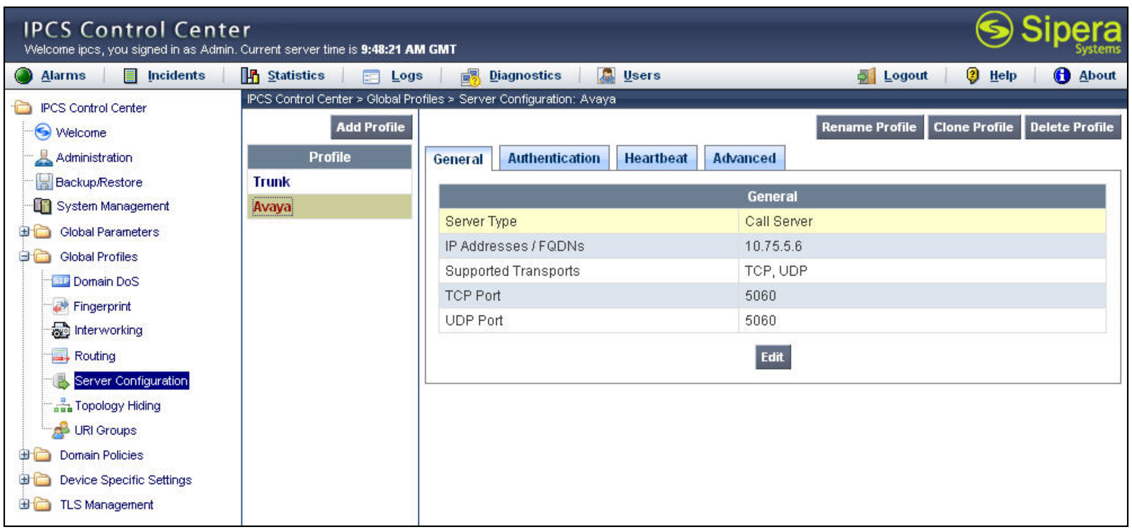
A URI group defines URI matching criteria to be applied to SIP traffic.

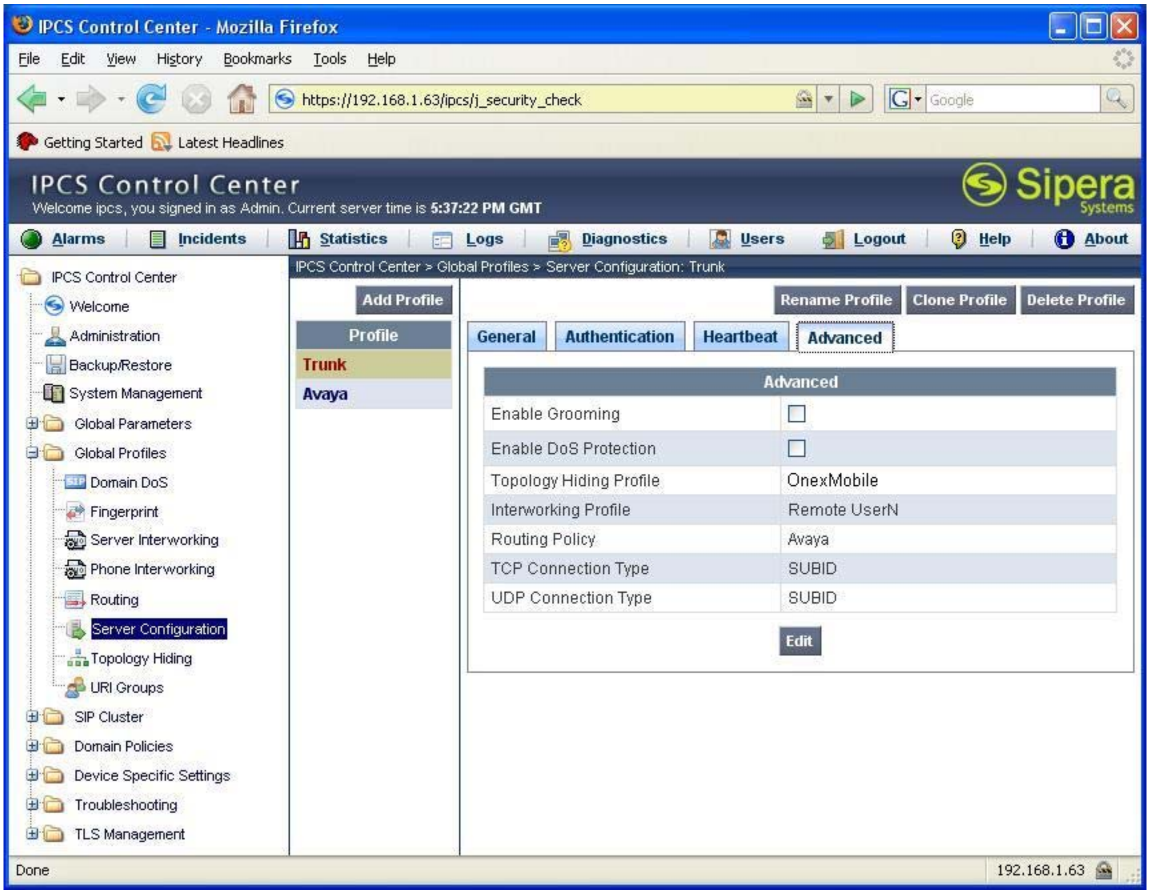
To define a new URI group, navigate to **IPCS Control Center→Global Profiles→URI Groups**. Select the **Add Group** button in the middle pane to enter and submit the new information.

In the case of the compliance test, URI groups were created to identify different groups of remote users. These URI Groups were then used as criteria in defining profile and call flows in subsequent steps. In the example below, the middle pane shows three URI groups that were created – ***96xx, 46xx*** and ***OnexMobile***. Since URI Group ***46xx*** is highlighted, the details of this group are shown in the right pane. This group matches a URI of 30203 from any IP address as indicated by the subsequent @*. It will also match a URI of 30204 from any IP address. 30203 and 30204 are the extensions of the remote Avaya 4600 Series IP Telephones. Similarly, the ***96xx*** URI group contains the extensions of the remote Avaya 9600 Series IP Telephones and the ***OnexMobile*** URI group contains the extensions of the remote Avaya one-X Mobile endpoint as well as the remote Avaya one-X Desktop soft phone endpoint.



</td></tr>
</table>

Step	Description
8.	**Server Definition - General** A server configuration profile is created to define the characteristics of the Avaya SES to which the IPCS will communicate. To define a new server configuration profile, navigate to **IPCS Control Center→Global Profiles→Server Configuration**. Select the **Add Profile** button in the middle pane to enter and submit the new information. The example below shows the server configuration profile named ***Avaya*** used for the compliance test. The General tab shows the **Server Type** as ***Call Server*** and the IP address of the Avaya SES (***10.75.5.6***) in the **IP Addresses/FQDNs** field. The remaining fields show the transport protocols and ports supported for traffic between IPCS and Avaya SES. 

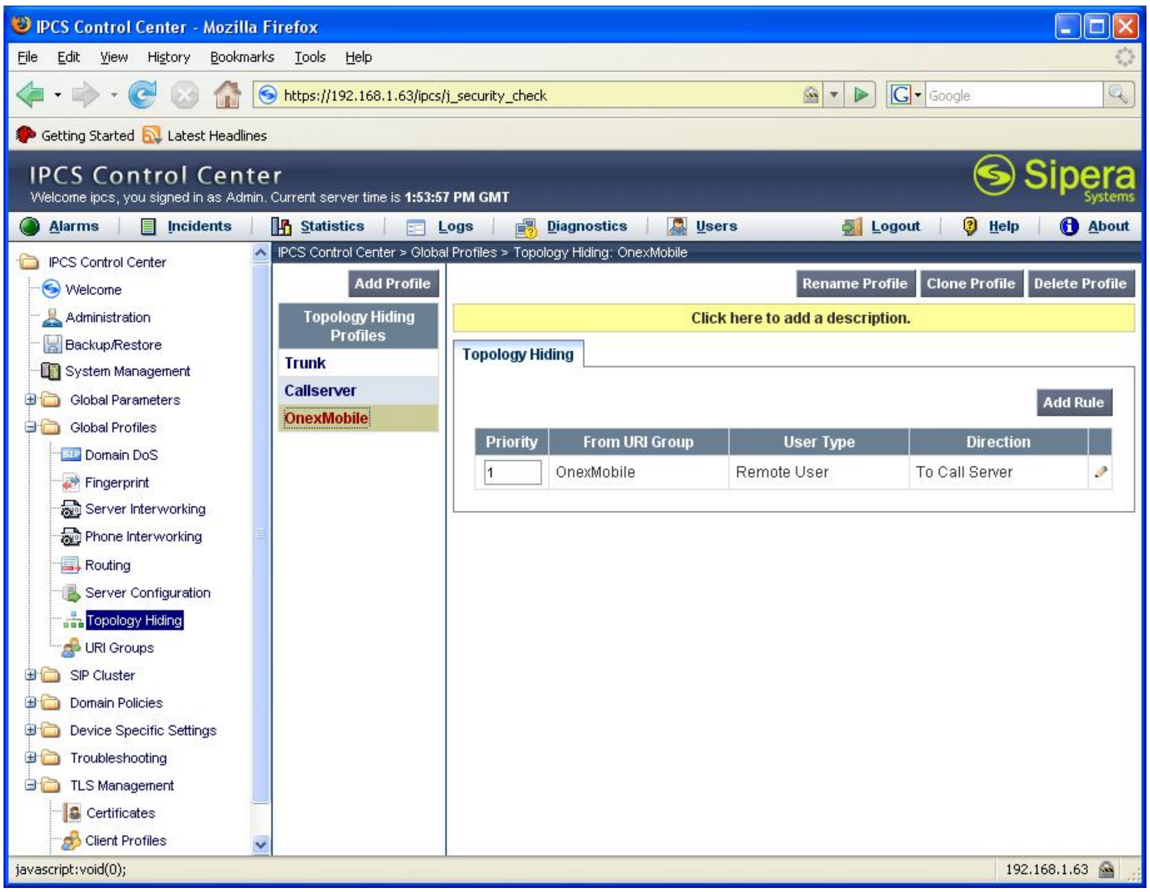
Step	Description
9.	**Server Definition – Advanced** On the **Advanced** tab, profiles are specified that will be applied to traffic between the IPCS and this server (Avaya SES). The **Topology Hiding** and **Interworking** profiles are applied to traffic from the IPCS ***to*** the server and the **Routing** profile is applied to traffic to the IPCS ***from*** the server. These profiles: **Topology Hiding**, **Interworking** and **Routing** are described in **Steps 10 – 13**. Default values were used for all other fields. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>10.</td><td>

Server - Topology Hiding Profile
A topology hiding profile defines how the manipulation of IP addresses and domains is to be applied to SIP messages for traffic from IPCS to the server (Avaya SES).

To define a new topology hiding profile, navigate to **IPCS Control Center→Global Profiles→Topology Hiding**. Select the **Add Profile** 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 profile named ***OnexMobile*** was used for the compliance test. By highlighting this profile in the middle pane, its details are shown in the right pane. The remote one-X Mobile phone and the remote one-X Desktop soft phone will use this profile for all signaling communication.



</td></tr>
</table>

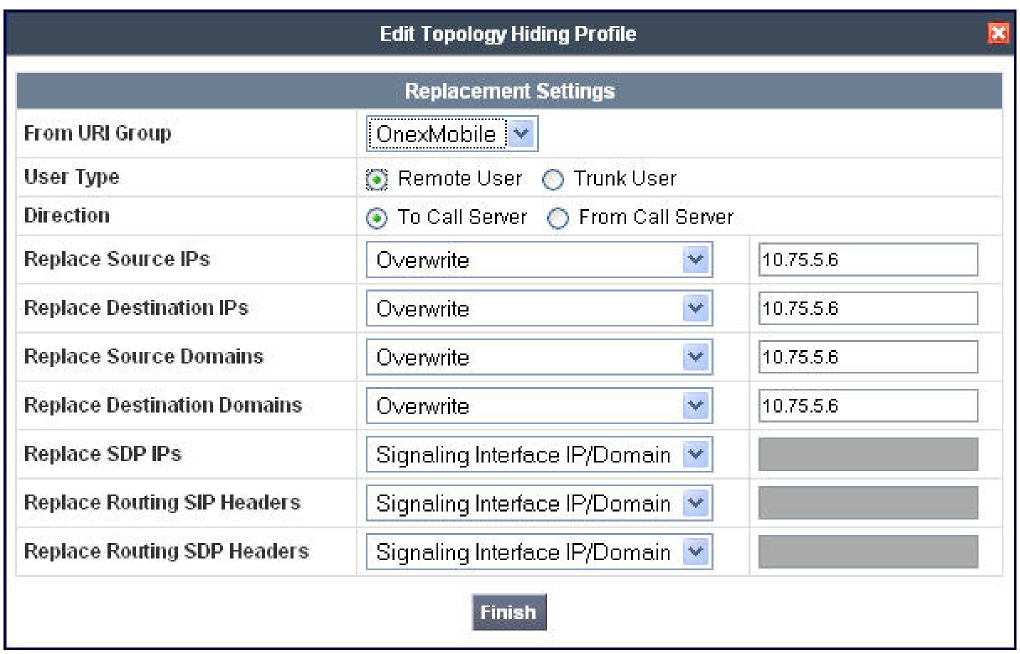
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>11.</td><td>

Server - Topology Hiding Profile - Continued

The topology hiding profile named ***OnexMobile*** was created to aid interworking with the Avaya one-X Mobile remote endpoint. The Avaya one-X Mobile works differently than the other Avaya SIP endpoints. When the Avaya one-X Mobile is configured using an IP address as the SIP proxy and registrar, the Avaya one-X Mobile will use this IP address to route the message as well as use this IP address in the SIP headers instead of using the domain (which is also configured) in the SIP headers. Other Avaya endpoints when configured in this manner will use the domain name in the SIP headers and use the configured SIP proxy and registrar IP addresses only for routing the messages. Thus, a separate Topology Hiding Profile was created to handle this special case.

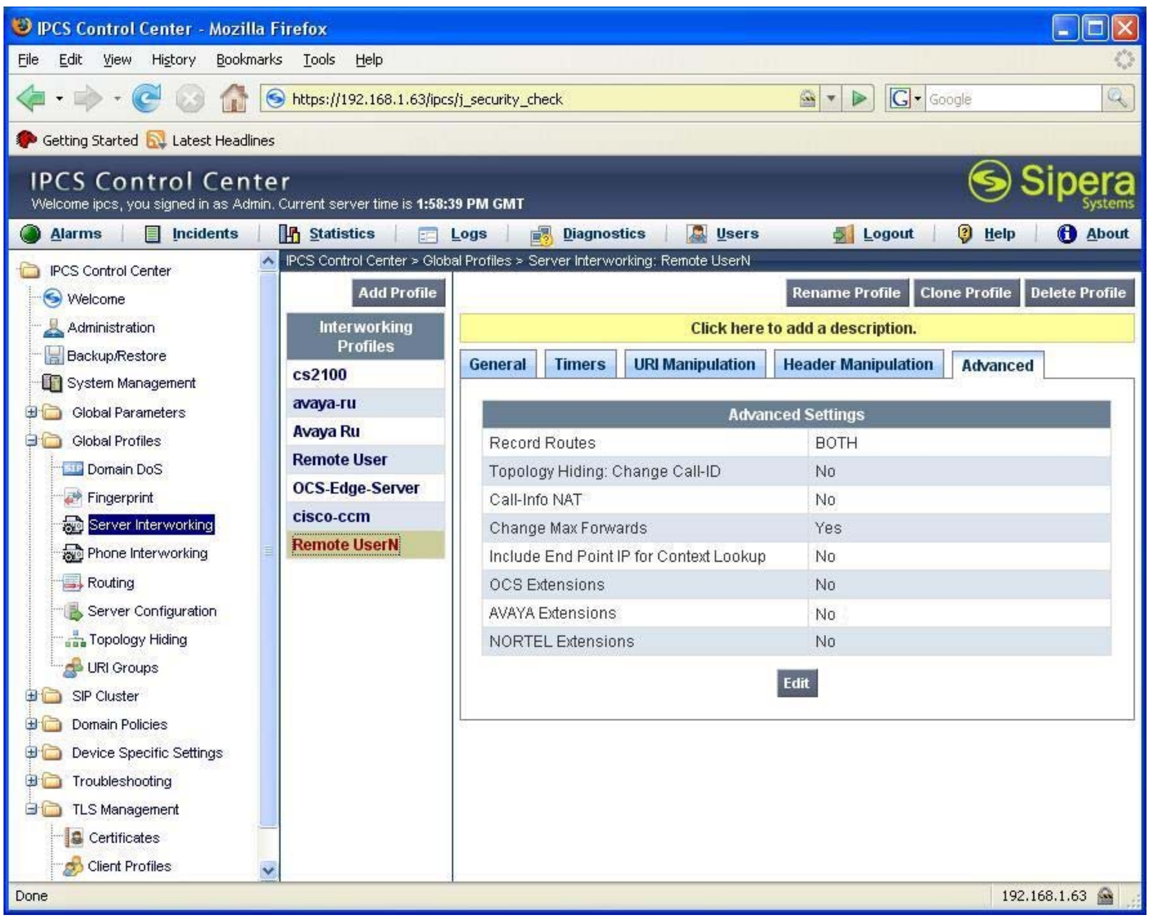
The details of the profile rule (invoked by clicking the Edit button for the rule) shown below specify that for all traffic from the ***OnexMobile*** URI group, the source IPs, destination IPs, source domains and destination domains used in the SIP headers will be overwritten with the IP address of the Avaya SES which is equivalent to using the configured domain in the headers.

It is to be noted that the remote Avaya one-X Desktop soft phone also uses this profile for signaling communication since it is included in the OnxMobile URI Group (**Step 7**). The Avaya one-X Desktop soft phone can work with both IP address and domain name, therefore the rule in this ***OnexMobile*** Topology Hiding Profile can be applied to it with no harm. This configuration makes sense since the remote one-X Desktop soft phone and the remote one-X Mobile phone were physically placed behind the same NetScreen 5GT firewall in the compliance test setup.



</td></tr>
</table>

Step	Description
12.	**Server – Interworking Profile** Server Interworking profile defines how SIP message headers and content (other than the IP addresses) may be manipulated for interoperability with different call servers. To define a new interworking profile, navigate to **IPCS Control Center→Global Profiles→Server Interworking**. Select the **Add Profile** button in the middle pane to enter and submit the new information. In the example below, multiple profiles are shown in the middle pane. Only the profile named ***Remote UserN*** was used for the compliance test. By highlighting this profile in the middle pane, its details are shown in the right pane. On the **Advanced** tab, the **Topology Hiding: Change Call-ID** field was set to ***No*** to disable the changing of the Call-ID in the SIP messages passed through the IPCS to the Avaya SES. Default values were used for all other fields.



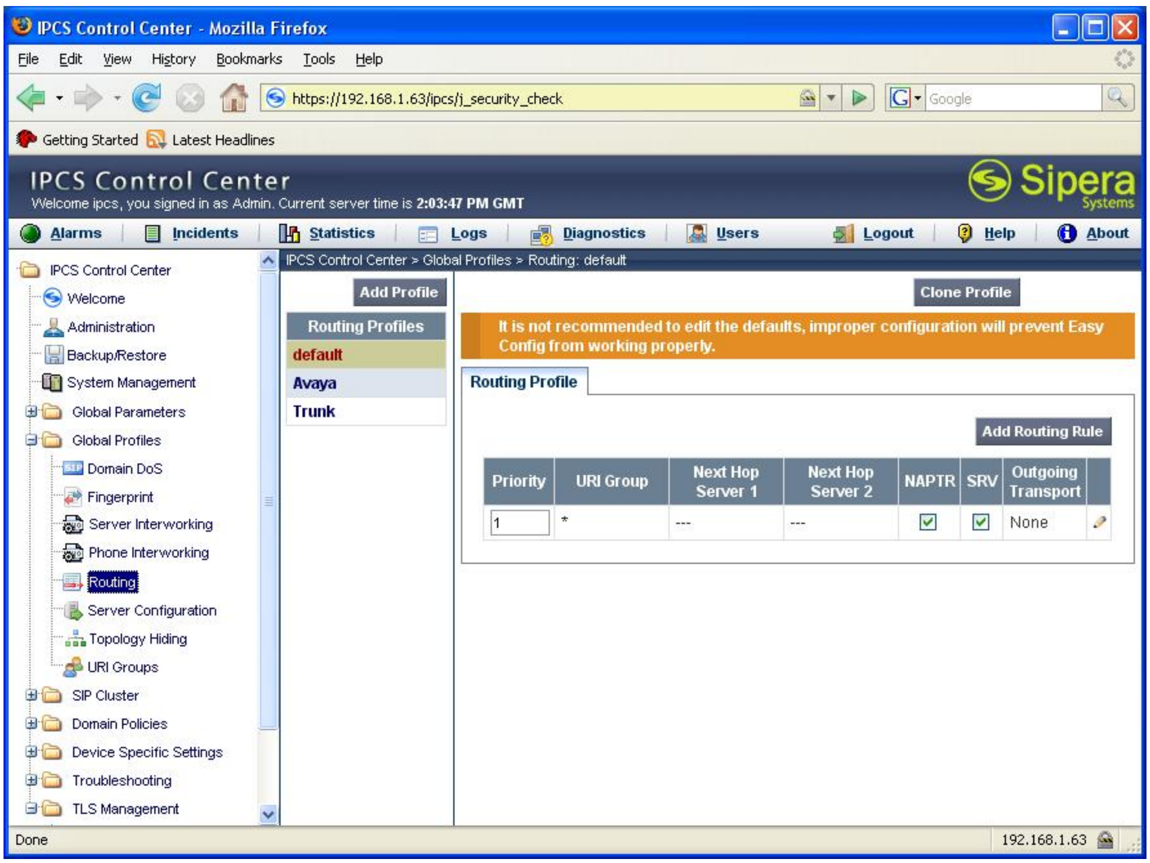
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>13.</td><td>

Server – Routing Profile

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 **IPCS Control Center→Global Profiles→Routing**. Select the **Add Profile** 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 ***default*** and ***Avaya*** were used for the compliance test. By highlighting a profile in the middle pane, its details are shown in the right pane. The ***Avaya*** routing profile is described in **Step 20**. The ***default*** profile is shown below. The ***default*** profile is for routing traffic from the server destined for one of the remote endpoints. Thus, the routing profile is for all URI Groups (**URI Group** = *****) and no server IP address is specified in **Next Hop Server 1** or **Next Hop Server 2** fields. To locate the destination address, the IPCS will use its internal database to identify the IP address associated with the destination extension in the SIP message.

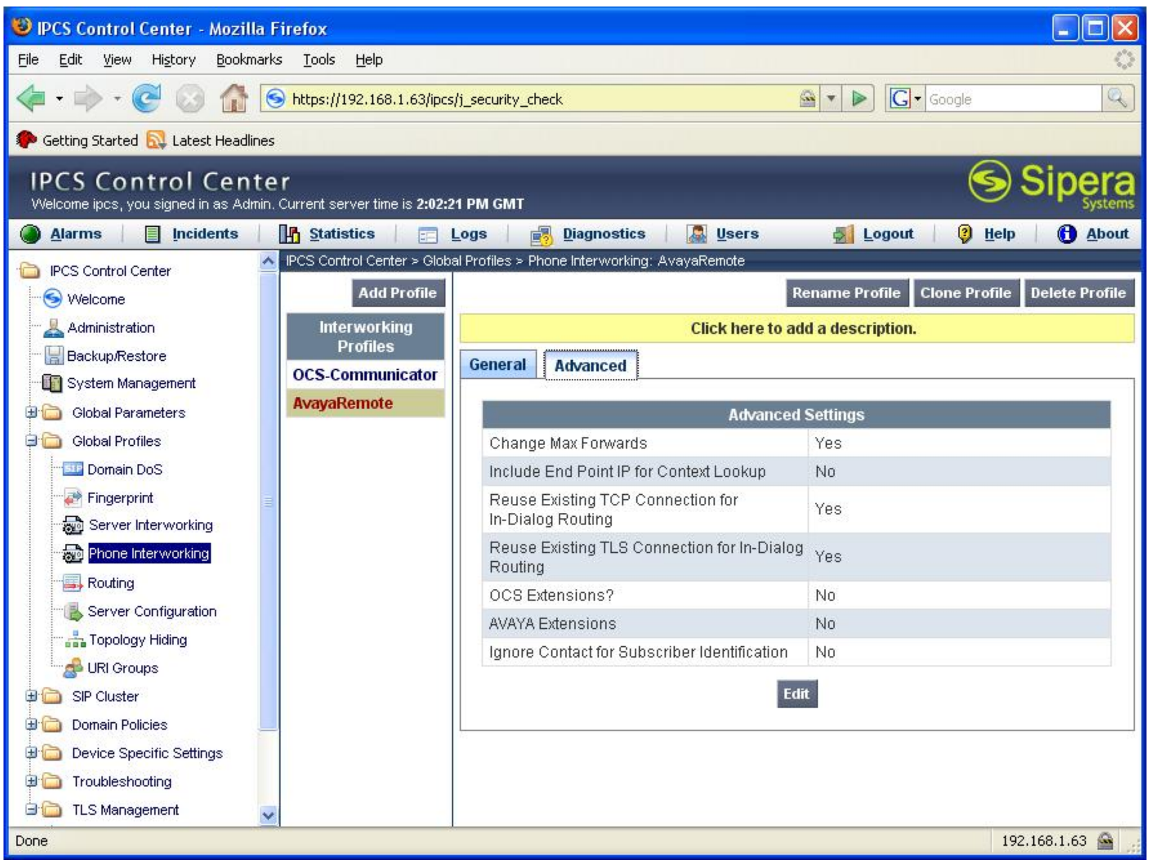


</td></tr>
</table>

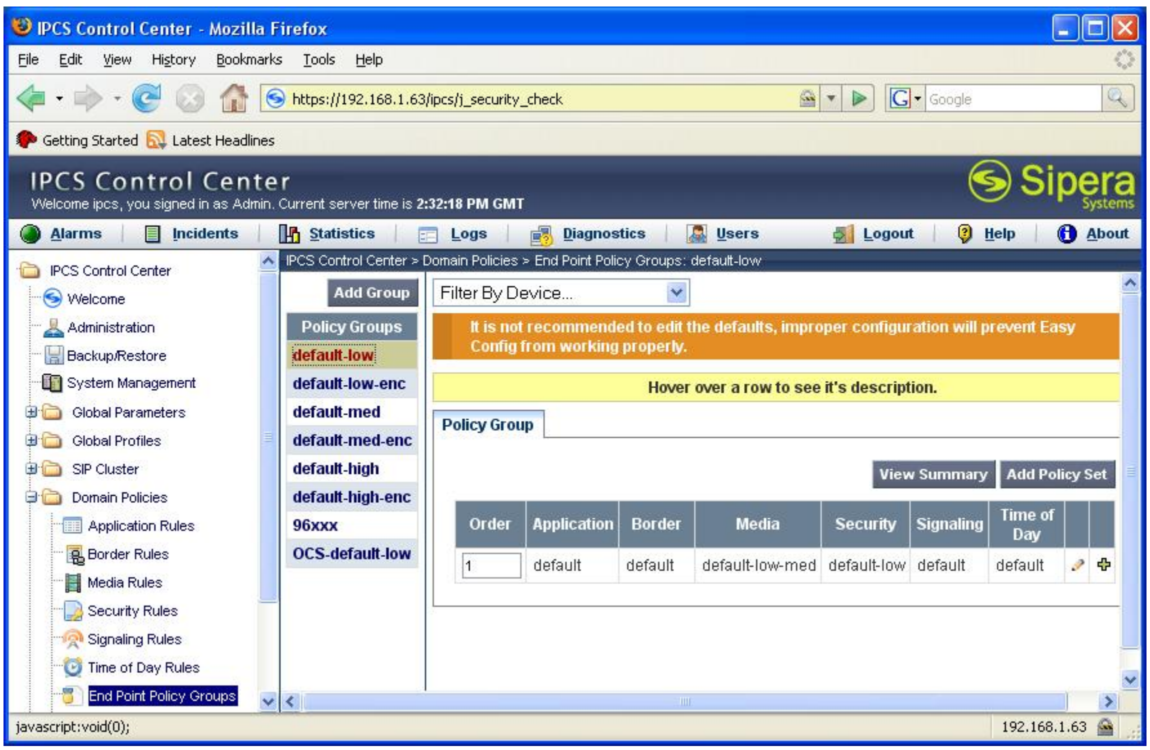
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>14.</td><td>

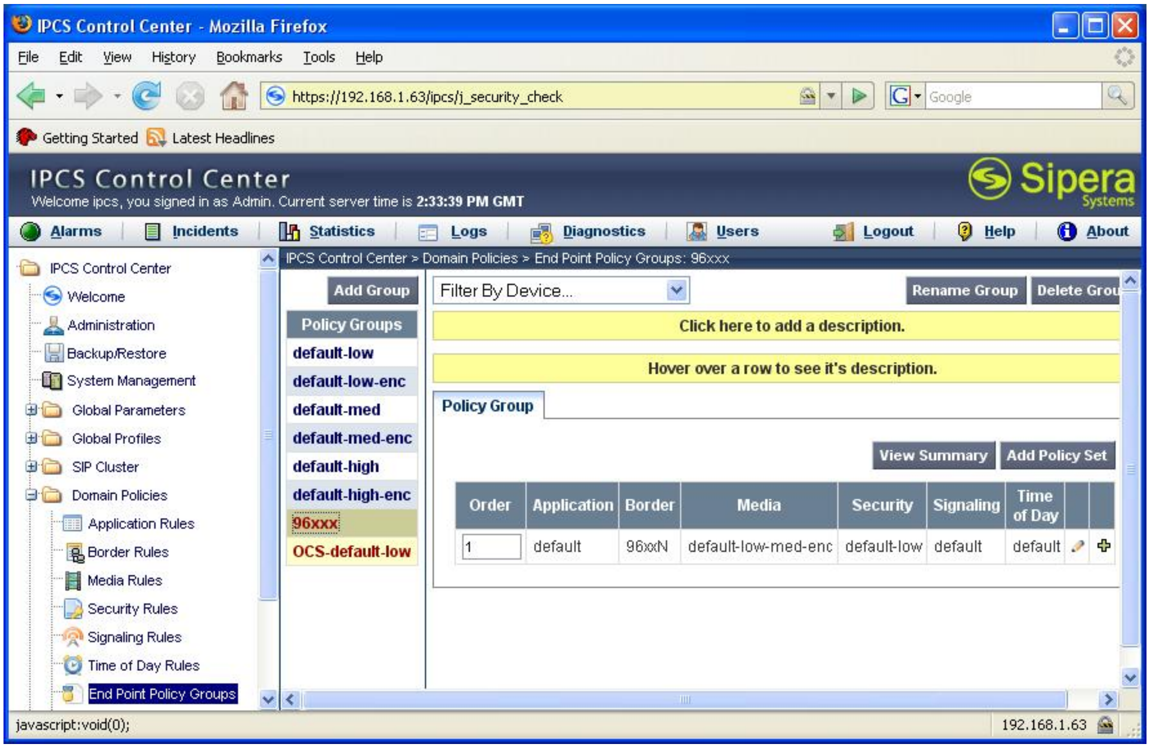
Phone- Interworking Profile
Phone Interworking profile defines how the interoperability with a Call Server provides features applicable to phones. This profile is used in End Point Subscriber Flow configuration (**Step 19**).

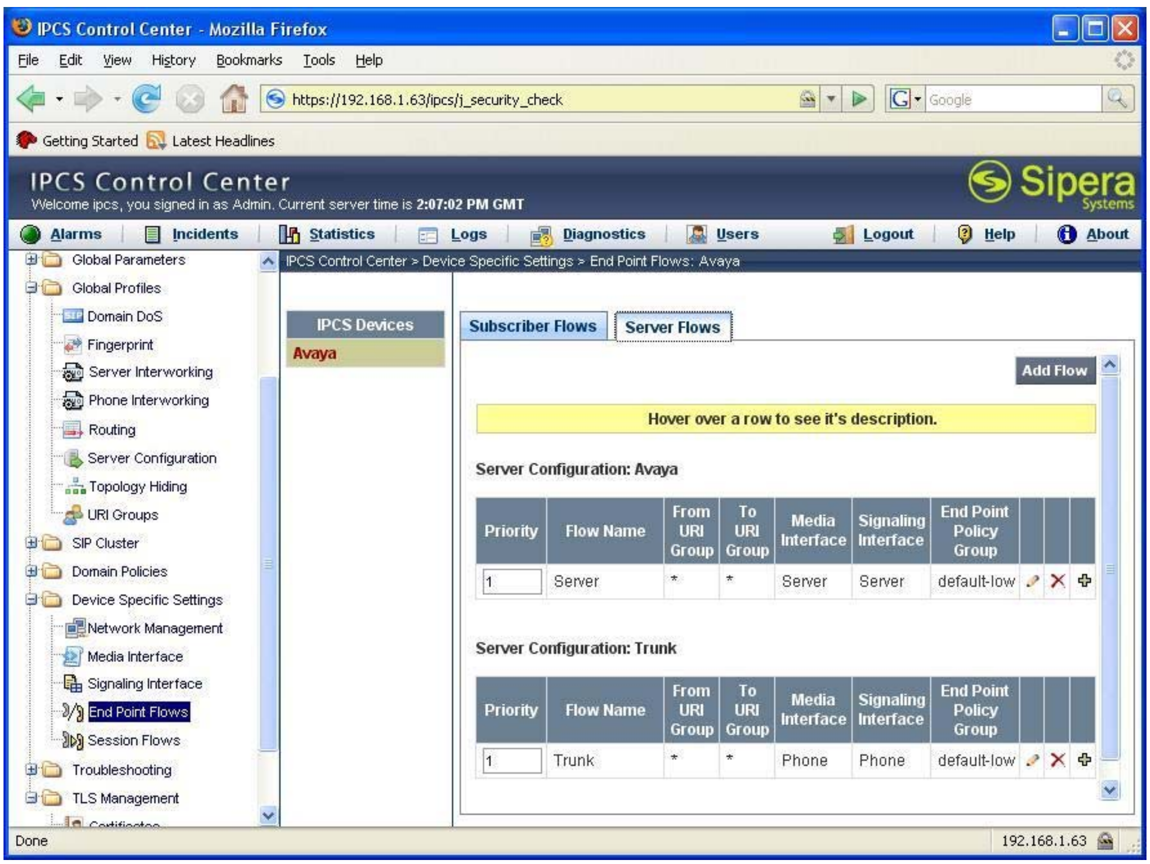
In the example below, 2 profiles are shown in the middle pane. Only the profile named ***AvayaRemote*** was used for the compliance test. In this profile, **Reuse Existing TCP Connection for In-Dialog Routing** and **Reuse Existing TLS Connection for In-Dialog Routing** were set to ***Yes*** to enable Avaya phones with TCP and TLS support at the remote side.



</td></tr>
</table>

Step	Description
15.	**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 **IPCS Control Center→Domain Policies→End Point Policy Groups**. Select the **Add Group** button in the middle pane to enter and submit the information. For the compliance test, two policy groups were used. Policy group ***default-low*** defines the use of unencrypted media (RTP). Policy group ***96xxx*** defines the use of encrypted media (SRTP). The details on the media can be obtained by clicking the Media link in the Policy Group displays shown below. These policy groups will be used in the server and subscriber flows defined in the following steps (**Steps 17-18**). 

Step	Description
16.	**End Point Policy Groups - Continued** Policy group ***96xxx*** defines the use of encrypted media (SRTP). 

Step	Description
17.	**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 **IPCS Control Center→Device Specific Settings→Endpoint Flows**. Select the **Server Flows** tab. Select the **Add Flow** button in the right pane to enter and submit the new information. The example below shows 2 server flows. The first one was the server flow used for the compliance test. It specifies that all traffic to or from any URI Group will be allowed to the server named ***Avaya*** (Avaya SES). Media traffic will use **Media Interface –** ***Server*** (**Step 6**) and signaling traffic will use **Signaling Interface –** ***Server*** (**Step 5**). The **Endpoint Policy Group** named ***default –low*** (**Step 15**) will be applied to this traffic which specifies that the media is unencrypted. 

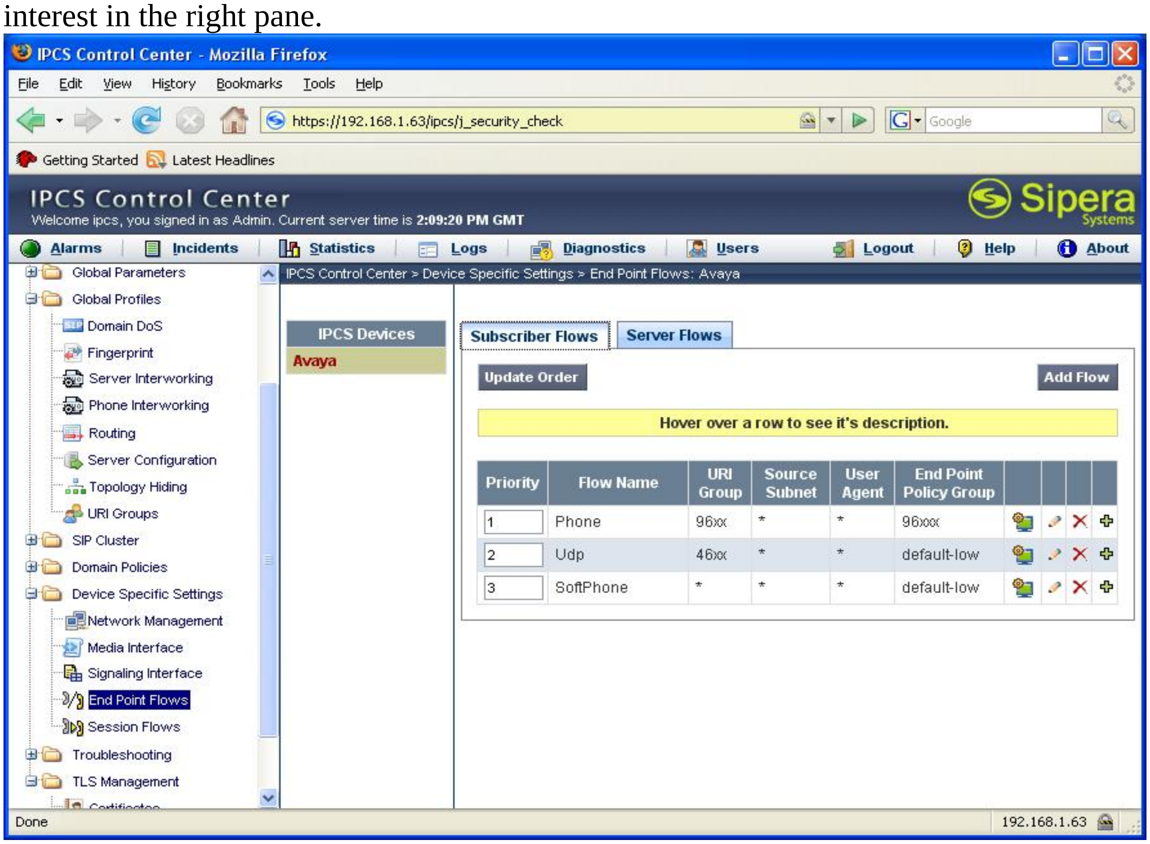
Step	Description
18.	**Subscriber Flows**

A subscriber flow defines what traffic is allowed between the IPCS and the specified endpoints in much the same way the server flow defines the traffic allowed between the IPCS and the server.

To define a new subscriber flow, navigate to **IPCS Control Center→Device Specific Settings→Endpoint Flows**. Select the **Subscriber Flows** tab. Select the **Add Flow** button in the right pane to enter and submit the new information.

Three subscriber flows were created for the compliance test. If the traffic does not match the first flow, then the next flow in the list will be tested until a match is found. The detailed matching criteria are shown in **Step 19**. In the example below, the first flow will match traffic from the remote Avaya 9600 Series IP Telephones. The **Endpoint Policy Group** named ***96xxx*** (**Step 16**) will be applied to this traffic which specifies that the media is encrypted. The second flow will match all traffic from the remote Avaya 4600 Series IP Telephones. The **Endpoint Policy Group** named ***default-low*** (**Step 15**) will be applied to this traffic which specifies that the media is unencrypted. The last flow ***Soft phone*** will match all traffic not matched by flow 1 and 2. This includes traffic from both the remote Avaya one-X Desktop Edition and the Avaya one-X Mobile endpoints. The **Endpoint Policy Group** named ***default-low*** (**Step 15**) will be applied to this traffic which specifies that the media is unencrypted.

To see the complete details of a flow, click the monitor icon associated with the flow of interest in the right pane.



Step	Description
19.	**Subscriber Flow – Details**

The example below shows the details of the first flow (***Phone***) in the list in **Step 18**. Unlike the server flow, parameters such as **Topology Hiding Profile** and **Routing Profile** are defined within the subscriber flow itself. For the server traffic, these parameters were not defined in the flow but were defined in the server configuration.

This flow will match traffic from the remote Avaya 9600 Series IP Telephones since the **URI Group** field is set to ***96xx*** (**Step 7**) and the **Signaling Interface** field is set to ***Phone*** (**Step 5**) in the **Criteria** section. Media traffic will use **Media Interface –** ***Phone*** (**Step 6**). The **End Point Policy Group** used is ***96xxx*** (**Step 16**). The **Phone Interworking Profile** used is ***AvayaRemote*** (**Step 14**). The **Routing Profile** used is ***Avaya*** (**Step 20**).

The other two flows are configured the same as the ***Phone*** flow with the following exceptions:

Flow Udp:

- **URI Group** is set to ***46xx***.
- **End Point Policy Group** is set to ***default-low***.

Flow Soft phone:

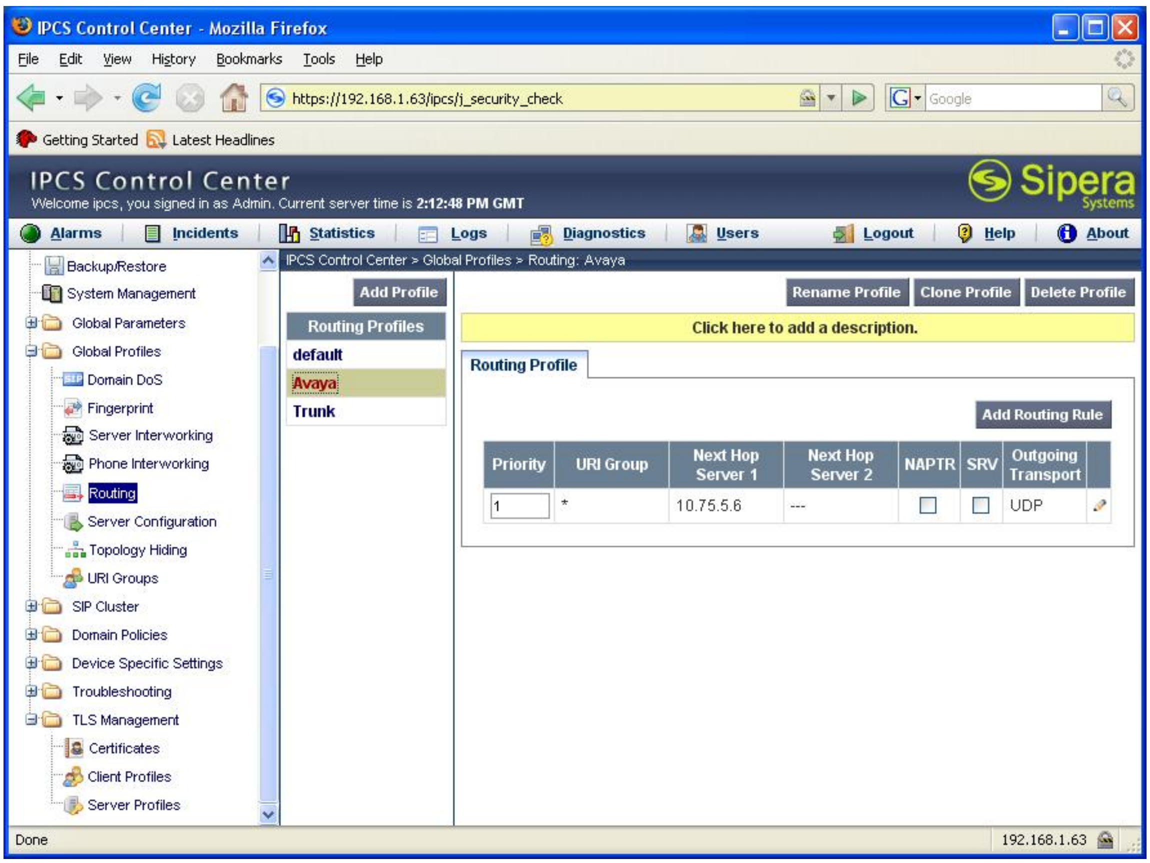
- **URI Group** is set to *****.
- **Signaling Interface** is set to ***Soft phone***.
- **Media Interface** is set to ***Soft phone***.
- **End Point Policy Group** is set to ***default-low***.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>20.</td><td>

Subscriber – Routing Profile
A routing profile defines how a call is to be routed. In this case, the routing profile is applied to calls from the subscriber to IPCS.

To define a new routing profile, navigate to **IPCS Control Center→Global Profiles→Routing**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

The example below shows the routing profile named ***Avaya*** used by all the subscriber flows defined in **Steps 18-19**. It shows that all traffic (**URI Group** = *****) using this profile will be routed to IP address 10.75.5.6 (Avaya SES) as the next hop as defined in the **Next Hop Server 1** field.



</td></tr>
</table>

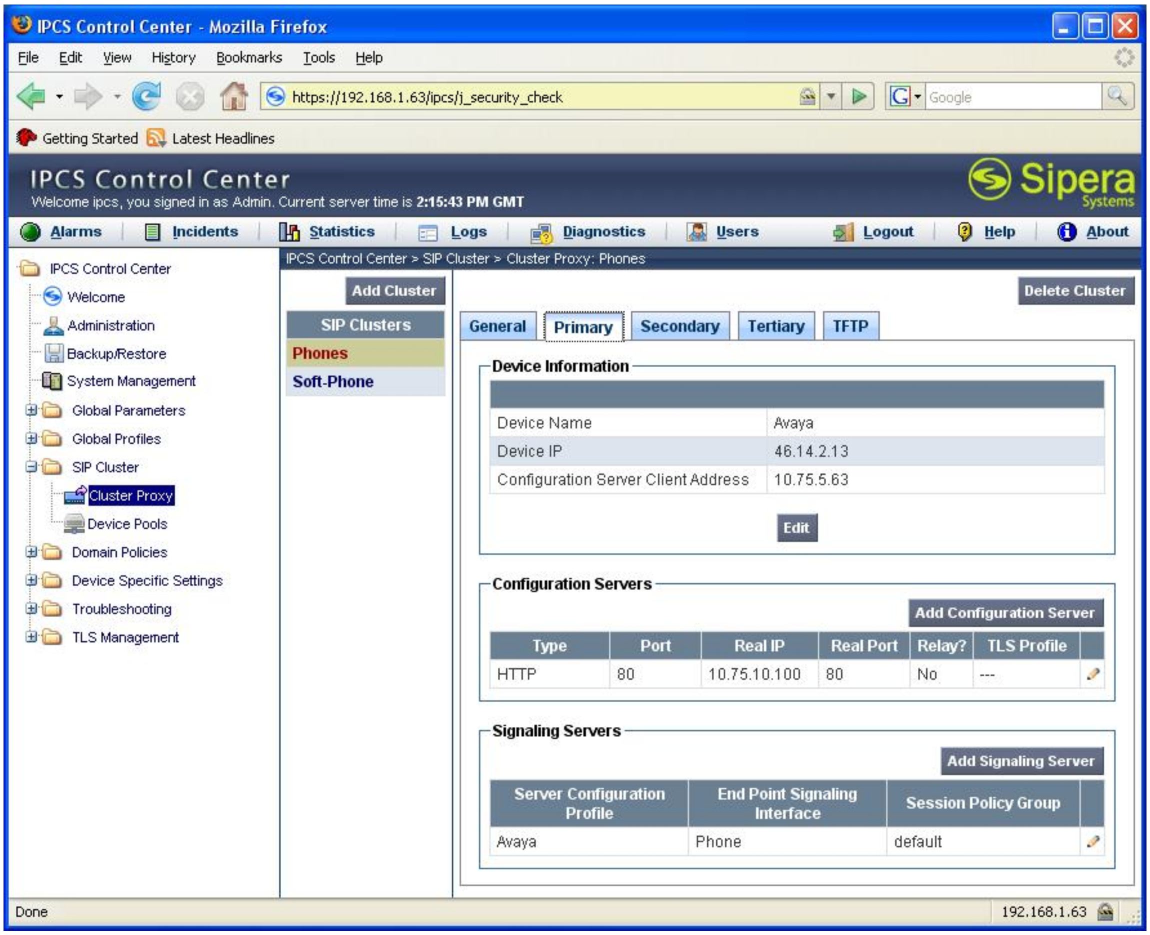
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>21.</td><td>

SIP Clusters

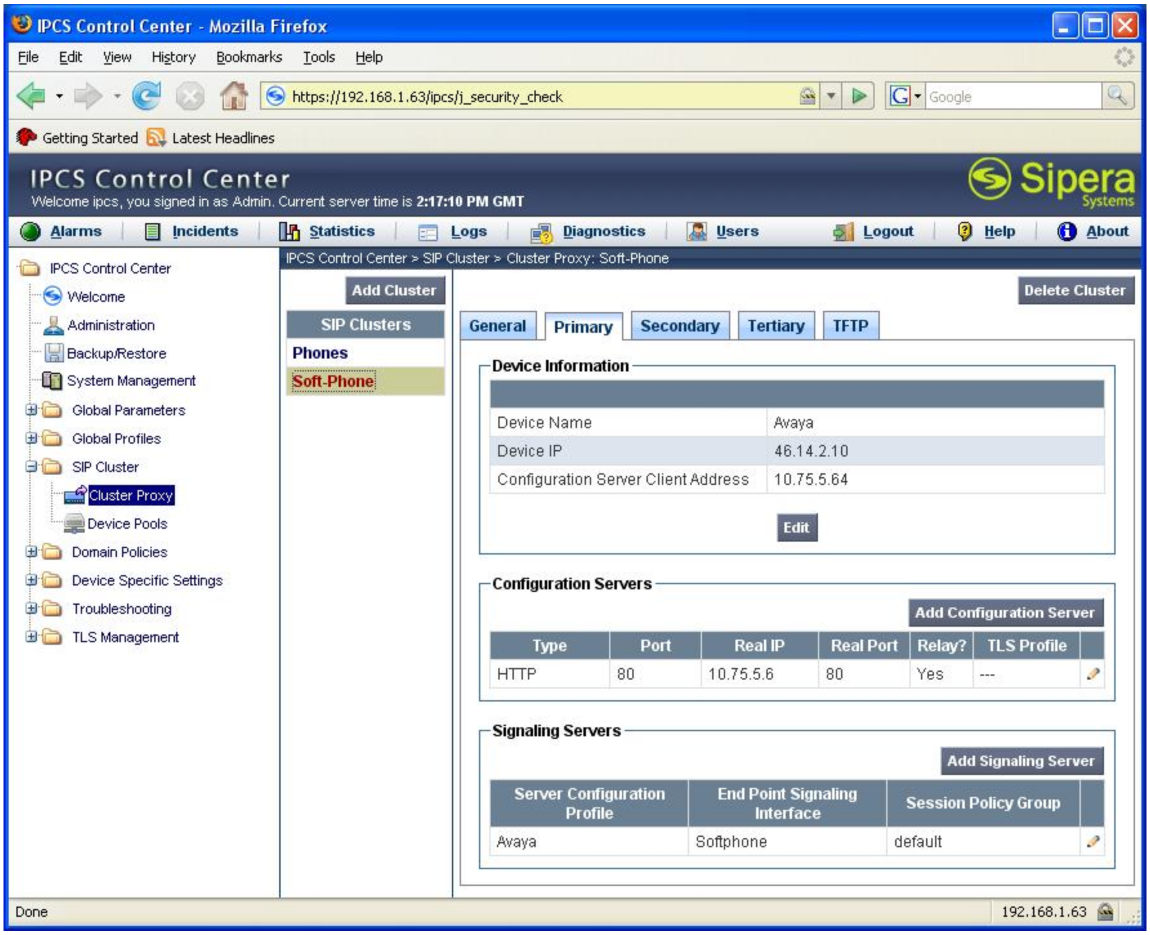
As part of the compliance test, SIP clusters were used to define how HTTP traffic will be routed for different groups of endpoints.

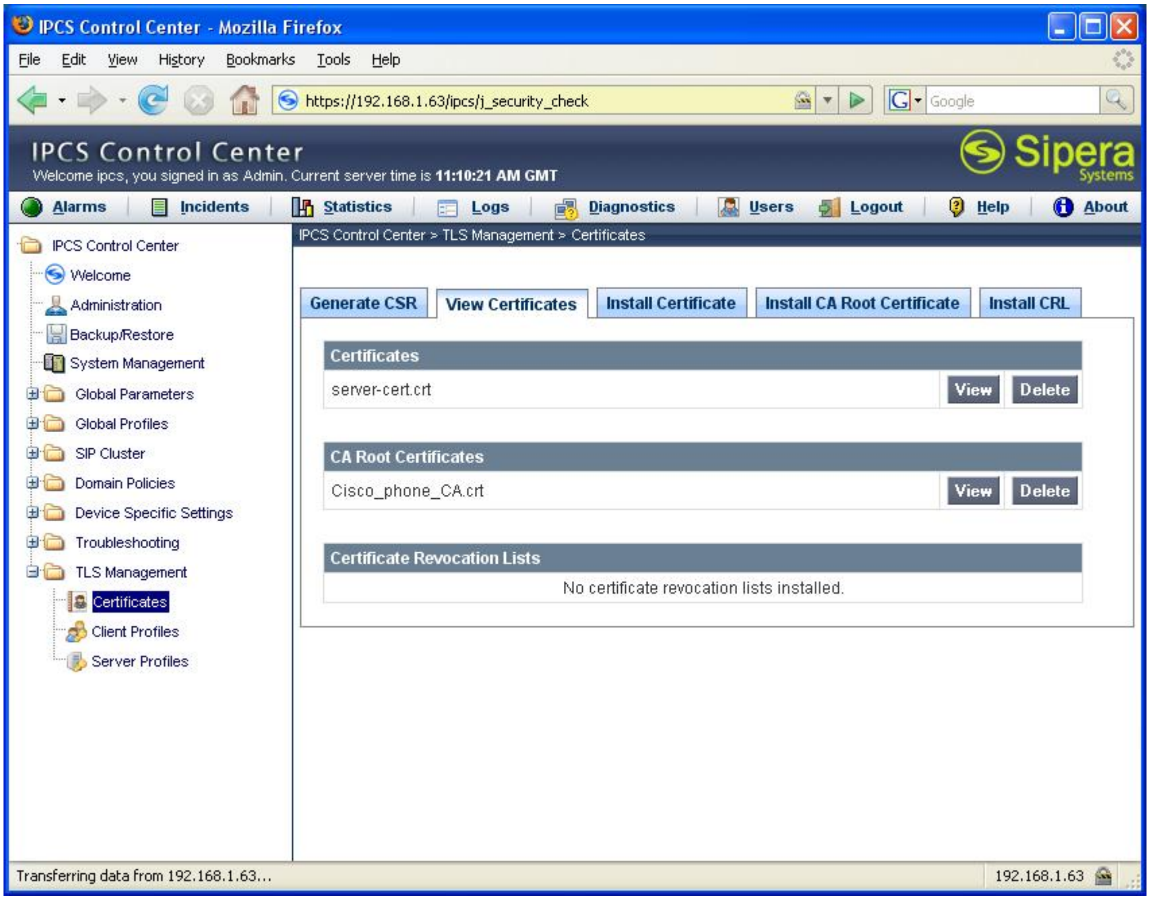
To define a new cluster, navigate to **IPCS Control Center→SIP Cluster**. Select the **Add Cluster** button in the middle pane to enter and submit the new information.

The two clusters used for the compliance test are shown in the middle pane. By highlighting a profile in the middle pane, its details are shown in the right pane. The example below shows the cluster named ***Phones***. It defines that HTTP traffic from the **Device IP *46.14.2.13*** will be routed out the **Configuration Server Client Address *10.75.5.63*** to the internal HTTP server address ***10.75.10.100*** as specified in the **Real IP** field. This enables the remote Avaya 4600 and 9600 Series IP Telephones to get their configuration data via the IPCS.



</td></tr>
</table>

Step	Description
22.	**SIP Clusters -Continued** The example below shows the cluster named ***Soft-Phone***. It defines that HTTP traffic from the **Device IP *46.14.2.10*** will be routed out the **Configuration Server Client Address *10.75.5.64*** to the internal HTTP server address ***10.75.5.6*** as specified in the **Real IP** field. This enables the remote Avaya one-X Desktop Edition to access its license server via the IPCS. 

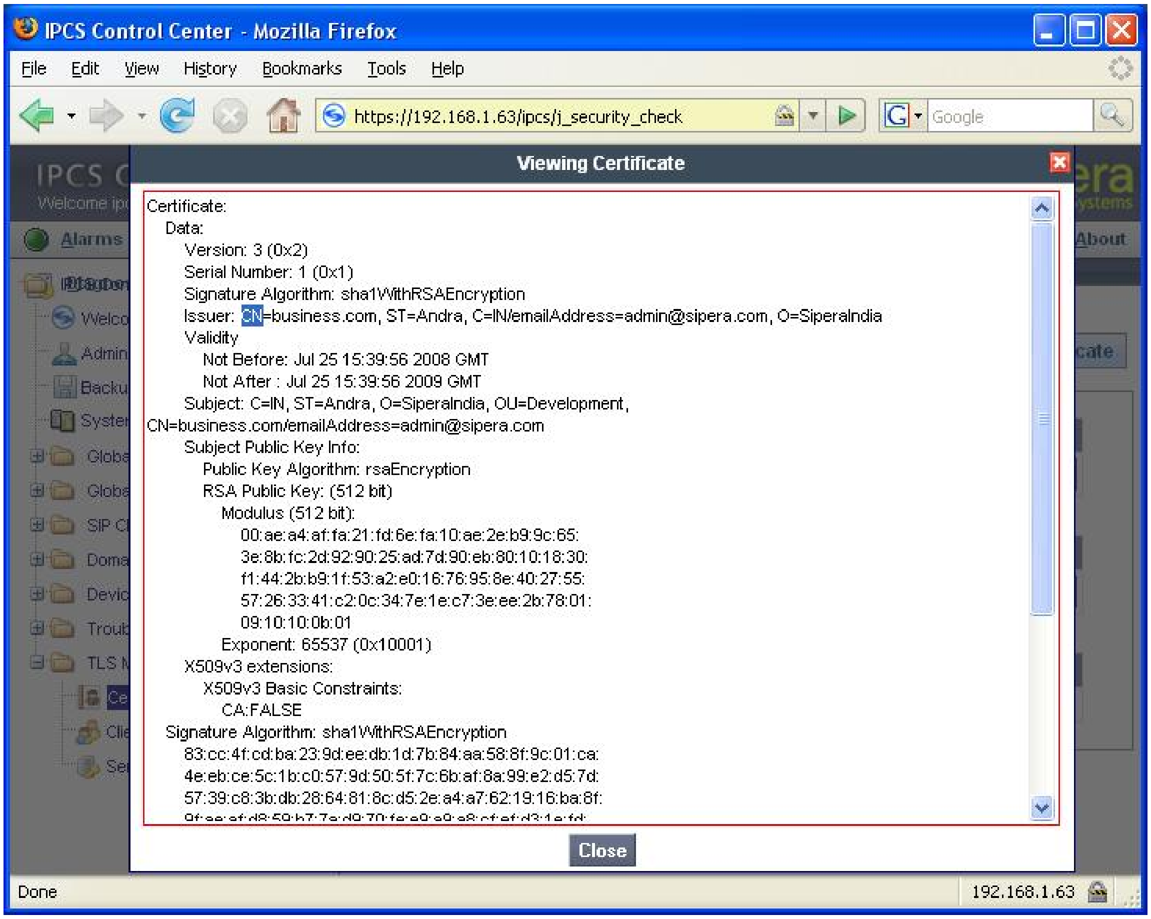
Step	Description
23.	**TLS Certificate** A TLS certificate is used for SIP over TLS. A TLS certificate can be generated and certified by any CA (Certificate Authority). Avaya phones honor the installed certificate on IPCS if the certificate has CN (Connection Name) set to the SES domain. The example below shows the TLS certificate named ***server-cert.crt*** that was generated by IPCS under the **Generate CSR** tab in **TLS Management** and certified by an OpenSSL CA server hosted in the Sipera lab. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>24.</td><td>

TLS Certificate – Continued

Press the **View** button for a certificate to shows details of the certificate.

In the example below for ***server-cert.crt***, CN (Connection Name) is set to ***business.com*** since it is the SES domain name. The Avaya phones accept this certificate while they use TLS for SIP.



</td></tr>
</table>

8. General Test Approach and Test Results

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

8.1. General Test Approach

The general test approach was to make calls through IPCS using various codec settings and exercising common and advanced PBX features. Calls were made between the remote users and the main site, between the remote users and the PSTN, and between the remote users. Different types of remote endpoints were also tested.

8.2. Test Results

IPCS 310 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 local and remote endpoints.
- Calls between a remote user without NAT and both SIP and non-SIP endpoint at the main site.
- Calls between a remote user with NAT and both SIP and non-SIP endpoint at the main site.
- Calls between a remote user with and without NAT and the PSTN.
- Calls between a remote user without NAT and a remote user with NAT.
- Calls between remote users behind the same NAT.
- Calls between remote users behind different NATs.
- G.711u and G.729A codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Voicemail support
- PBX features including Hold, Transfer, Call Waiting, and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions such as Call Forwarding, 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:

- No message waiting indication (MWI) occurred on the remote Avaya 4600 Series SIP telephones.
- The remote one-X mobile phone lost audio after rejoining a parked call (which was from a remote user to the mobile set, parked by the mobile set, and was answered first by another user through FNE).

Both problems were relatively low in severity.

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 remote endpoints are registered with Avaya SES using the private IP address of IPCS. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed between a remote user without NAT and SIP and non-SIP endpoints at the main site.
- Verify that calls can be placed between a remote user with NAT and SIP and non-SIP endpoints at the main site.
- Verify that calls can be placed between remote users with and without NAT.
- From the Avaya Communication Manager SAT, use the **list trace tac** command to verify that the calls between remote users and endpoints at the main site are routed through the configured SIP trunks.

10. 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 remote users with NAT traversal 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 Servers*, 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] *4600 Series IP Telephone LAN Administrator Guide*, Doc # 555-233-507, July 2008.

[8] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Installation and Maintenance Guide Release 2.0*, Doc # 16-601943, Issue 2, December 2007.

[9] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.0*, Doc # 16-601944, Issue 2, December 2007.

[10] *Avaya one-X Desktop Edition Administration*, October 2006.

[11] *Avaya one-X Desktop Edition Release 2.1 Quick Setup Guid*e, Doc # 16-600974, Issue 2, October 2006.

[12] *Avaya one-X Desktop Edition Getting Started, Doc # 16-600973, Issue 2, September 2007.*

[13] *Avaya one-X Mobile for S60 3rd Edition Dual Mode Installation and Administration Guide R4.3*, Doc # 16-601939, Issue 3, October 2007.

[14] *Application Notes for Configuring Avaya one-X Mobile, Avaya AP-8, Avaya SIP Enablement Services and Avaya Communication Manager*, Issue 1.0, October 2007.

[15] *IPCS210_310 Installation Guide (230-5210-31).*

[16] *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.

APPENDIX A: Avaya IP Phone Configuration File Example

This section shows the Avaya IP phone configuration file (46xxsettings.txt) settings used in the compliance test.

```
##########################################################
## Avaya 46xx IP Telephone Settings Script
##########################################################

## ======= SETTINGS FOR SIP Phones ======= ##
SET SNTPSRVR     "10.20.20.250"  ##Time Server
SET GMTOFFSET      "-5:00"
SET DSTOFFSET      "1"
SET DSTSTART       "2SunMar2L"
SET DSTSTOP  "1SunNov2L"
SET DATESEPARATOR "/"         ## Only used by 46xx SIP phones
SET DATETIMEFORMAT "0"        ## Only used by 46xx SIP phones
SET DIALPLAN     "4xxxx|3xxxx|91xxxxxxxxxx|9[2-9]xxxxxxxxx" ## Only used by 46xx
SIP phones
SET DTMF_PAYLOAD_TYPE 127     ## Only used by 96xx SIP phones
SET ENABLE_G729 2
SET MEDIAENCRYPTION "1,2"     ## Only used by 96xx SIP phones

###### SIP Server Parameters #########
SET SIPDOMAIN    "business.com"
SET SIPPROXYSRVR "10.75.5.6"
SET SIPPORT      "5060"
SET SIPREGISTRAR "10.75.5.6"
SET MWISRVR      "10.75.5.6"

###### H323 Server Parameters #########
SET MCIPADD      "10.75.5.2"
SET MCPORT       "1719"

## END OF SETTINGS SCRIPT FILE
```

APPENDIX B: Avaya one-X Mobile Configuration File Example

This section shows the Avaya one-X Mobile configuration file (setting.1xme) settings used in the compliance test.

```
DID_PREFIX = +1555789;
INTERNATIONAL_DIRECT_DIAL_PREFIX = 011;
NATIONAL_DIRECT_DIAL_PREFIX = 1;
HOME_COUNTRY_DIAL_CODE = +1;
ARS_CODE = 9;
EXTENSION_LENGTH = 5;
NATIONAL_NUMBER_LENGTH = 10;
USERS_EMERGENCY_NUMBERS = 123,999,911;
SETTINGS_PIN = 1234;
ENBLOC_DIALING = 0;
DUAL_MODE = 0;
WIFI_THRESHOLD = -80;
WIFI_POLLTIME = 2;

SPEECH_ACCESS_NUMBER = ;
ACTIVE_APPEARANCE_SELECT = 32001;
AUTO_CALL_BACK_TOGGLE = 32002;
CALL_FORWARDING_ALL_ACTIVATION = 32004;
CALL_FORWARDING_BUSY_NO_ANSWER_ACTIVATION = 32005;
CALL_FORWARDING_DISABLE = 32006;
CALLING_PARTY_NUMBER_BLOCK = ;
CALLING_PARTY_NUMBER_UNBLOCK = ;
CALL_PARK = 32007;
CALL_PICKUP_DIRECTED = 32013;
CALL_PICKUP_GROUP = 32009;
CALL_PICKUP_GROUP_EXTENDED = ;
CALL_UNPARK = 32008;
CONFERENCE_ON_ANSWER = 32010;
DROP_LAST_ADDED_PARTY = 32014;
EXCLUSION = ;
HELD_APPEARANCE_SELECT = 32017;
IDLE_APPEARANCE_SELECT = 32018;
OFF_PBX_DISABLE = 32023;
OFF_PBX_ENABLE = 32022;
SEND_ALL_CALLS_DISABLE = 32031;
SEND_ALL_CALLS_ENABLE = 32030;
TRANSFER_TO_COVERAGE = 32027;
TRANSFER_ON_HANGUP = 32026;

SUB_MENU_NAME = More Stuff;
<Voice Mail> = 39000;
<Conference Bridge> = +15553331234;

[SIP_PROFILE]
SIP_PROFILE_NAME = TR15sip;
SIP_DOMAIN = business.com;
SIP_SERVER_IP_ADDR = 46.14.2.10;
SIP_SERVER_PORT = 5060;
SIP_USERNAME = 30115;
SIP_PASSWORD = 123456;
```

```
CM_PRINCIPLE = 30115;
[/SIP_PROFILE]
```

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.