Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Ingate SIParator with Avaya SIP Enablement Services and Avaya Communication Manager to Support SIP Trunking - Issue 1.0

Abstract

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

The Ingate SIParator is a SIP session border controller (SBC) that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via a SIP trunk across an untrusted network.

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

1. Introduction

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

The Ingate SIParator is a SIP session border controller (SBC) that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via a SIP trunk across an untrusted network.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows two enterprise sites connected via a SIP trunk across an untrusted IP network. Alternatively, the test configuration could have shown a SIP service provider connected via a SIP trunk to the main site and the configuration of the main site equipment would have been very similar. The main site has a Juniper Networks Netscreen-50 firewall at the edge of the network restricting unwanted traffic between the untrusted network and the enterprise. Also connected to the edge of the main site is a SIParator SBC. The public side of the SIParator is connected to the untrusted network and the private side is connected to the trusted corporate LAN. The SIParator could also reside in the demilitarized zone (DMZ) of the enterprise but this configuration was not tested.

All SIP traffic between sites flows through the SIParator. In this manner, the SIParator can protect the main 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 the SIParator and flows directly between the untrusted network and the private LAN of the enterprise if permitted by the data firewall.

Connected to the corporate LAN at the main site 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 both SIP and non-SIP endpoints. An ISDN-PRI trunk connects the media gateway to the PSTN.

Located at the branch site 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 both SIP and non-SIP endpoints. For simplicity, there is no network address translation (NAT) being performed at the branch site. All IP addresses located at the branch are routable across the untrusted network.

The SIP endpoints located at both sites are registered to the local Avaya SES. Each site has a separate SIP domain: ***business.com*** for the main site and ***dev4.com*** for the branch. SIP and H.323 telephones at both sites use the local TFTP server to obtain their configuration files.

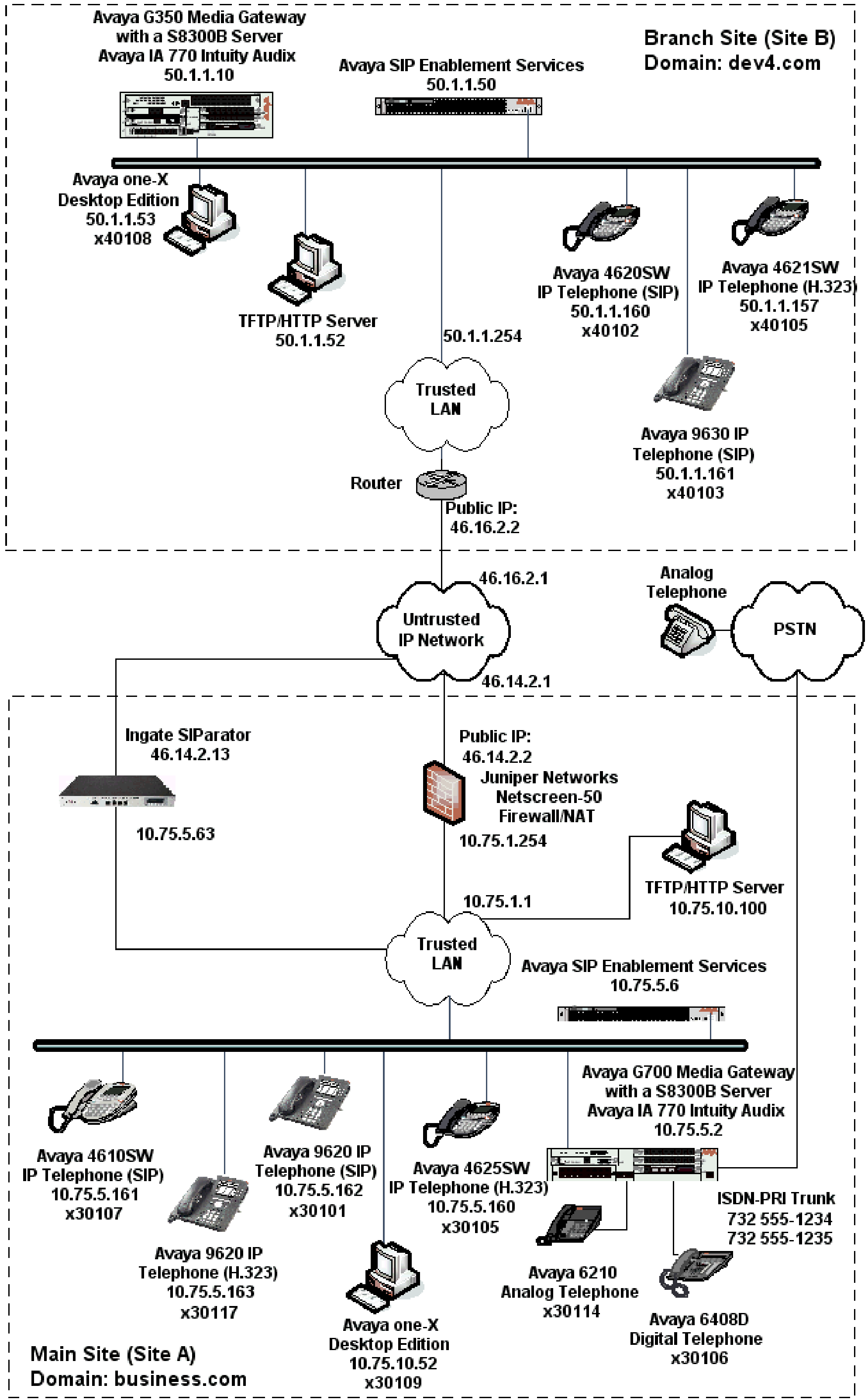


Figure 1: SIParator SIP Trunking Test Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300B Server with Avaya G700 Media Gateway (Main Site) Avaya IA 770 Intuity Audix	Avaya Communication Manager 5.0 Service Pack (R015x.00.0.825.4-15175)
Avaya S8500B Server (Main Site)	Avaya SIP Enablement Services 5.0
Avaya S8300B Server with Avaya G350 Media Gateway (Branch Site) Avaya IA 770 Intuity Audix	Avaya Communication Manager 4.0.1 Service Pack (R014x.00.0.731.2-14300)
Avaya S8500A Server (Branch Site)	Avaya SIP Enablement Services 4.0
Avaya 4621SW IP Telephones (H.323) Avaya 4625SW IP Telephones (H.323)	H.323 version 2.8.3
Avaya 4610SW IP Telephone (SIP) Avaya 4620SW IP Telephones (SIP)	SIP version 2.2.2
Avaya 9620 IP Telephones (H.323)	Avaya one-X Deskphone Edition 1.5
Avaya 9620 IP Telephones (SIP) Avaya 9630 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.0.3
Avaya one-X Desktop Edition (SIP)	2.1 Service Pack 2
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (TFTP/HTTP Server)	Windows XP Professional SP 2
Juniper Networks Netscreen-50	5.4.0r9.0
Ingate SIParator SIP Trunking Module QoS Module (optional)	4.6.2

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

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

Section 3.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with the SIParator.

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

This configuration must be repeated for Avaya Communication Manager at 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.

3.1. Summary of Initial SIP Installation

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

Step	Description
1.	**IP network region** The Avaya S8300 Server, Avaya SES and IP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **display ip-network-region** command to view these settings. The example below shows the values used for the compliance test. ▪ **Authoritative Domain**: ***business.com*** This field was configured to match the domain name configured on Avaya SES. This name will appear in the "From" header of SIP messages originating from this IP region. ▪ **Name**: ***Default*** Any descriptive name may be used. ▪ **Intra-region IP-IP Direct Audio**: ***yes*** **Inter-region IP-IP Direct Audio**: ***yes*** By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Shuffling can be further restricted at the trunk level on the **Signaling Group** form. ▪ **Codec Set**: ***1*** The codec set contains the set of codecs available for calls within this IP network region. This includes SIP calls since all necessary components are within the same region.

```
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
```

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 G.729AB, G.711MU was removed from the list.

```
display 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.729AB           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]. ▪ **Near-end Node Name**: ***procr*** This node name maps to the IP address of the Avaya S8300 Server. Node names are defined using the **change node-names ip** command. ▪ **Far-end Node Name**: ***SES*** This node name maps to the IP address of Avaya SES. ▪ **Far-end Network Region**: ***1*** This defines the IP network region which contains Avaya SES. ▪ **Far-end Domain**: blank This domain will default to the domain specified in the IP network region form in **Step 1.** This domain is sent in the "To" header of SIP messages of calls using this signaling group. ▪ **Direct IP-IP Audio Connections**: ***y*** This field must be set to ***y*** to enable media shuffling on the SIP trunk.

```
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:

                                             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]. ▪ **Signaling Group**: ***1*** This field is set to the signaling group shown in the previous step. ▪ **Number of Members: *10*** This field represents 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.

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

                                                       Signaling Group: 1
                                                     Number of Members: 10
```

Step	Description
5.	**Trunk Group – continued** On **Page 3**: ▪ Verify the **Numbering Format** field is set to ***public***. 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.

```
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 Unavailable Numbers? n



 Show ANSWERED BY on Display? y
```

Step	Description
6.	**Public Unknown Numbering** Public unknown numbering defines the calling party number to be sent to the far-end. An entry was created for the trunk group defined in **Step 4**. 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 is sent to the far-end in the SIP "From" header.

```
change 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: 2
 5  3             1                       5           Maximum Entries: 240
```

3.2. Configure SIP Trunk and Routing to the Branch Site

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

Step	Description
1.	**Signaling Group** For the compliance test, signaling group 6 was used for the signaling group associated with the SIP trunk group defined for branch site calls (see **Step 2**). Signaling group 6 was configured using the same parameters as signaling group 1 in **Section 3.1** with the exception of the far-end domain. The **Far-end Domain** field is set to the SIParator private side IP address. In the case of the branch site, the **Far-end Domain** field would be set to the SIParator public IP address at the main site.

```
display signaling-group 6
                                SIGNALING GROUP

 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: 10.75.5.63

                                             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
2.	**Trunk Group** For the compliance test, trunk group 6 was used for the SIP trunk group defined for branch site calls. Trunk group 6 was configured using the same parameters as trunk group 1 in **Section 3.1, Step 4** except the **Signaling Group** field is set to ***6***. This includes the settings on **Page 3** of the trunk group form (not shown).

```
display trunk-group 6                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 6                    Group Type: sip           CDR Reports: y
  Group Name: Site2SES                    COR: 1        TN: 1        TAC: 106
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 6
                                                     Number of Members: 10
```

Step	Description
3.	**Public Unknown Numbering** A new entry was created for the trunk group defined in **Step 2**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across trunk group 6 will be sent as a 5-digit calling number. This calling party number is sent to the far-end in the SIP “From” header.

```
change 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: 3
 5  3              1                        5           Maximum Entries: 240
 5  3              6                        5
```

Step	Description
4.	**Automatic Alternate Routing** Automatic Alternate Routing (AAR) was used to route calls to the branch site. In the example shown, numbers that begin with 4 and are 5 digits long use route pattern 6. Route pattern 6 routes calls to the SIP trunk defined for branch site calls.

```
display aar analysis 4                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                                            Percent Full:    3

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    4                     5    5     6        aar          n
```

Step	Description
5.	**Route Pattern** For the compliance test, route pattern 6 was used for calls destined for the branch site. Route pattern 6 was configured using the parameters highlighted below. ▪ **Pattern Name**: Any descriptive name. ▪ **Grp No**: ***6*** This field is set to the trunk group number defined in **Step 2**. ▪ **FRL**: ***0*** This field is the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive.

```
change route-pattern 6                                            Page   1 of   3
                    Pattern Number: 6   Pattern Name: Site2SES
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 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
```

4. 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].

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

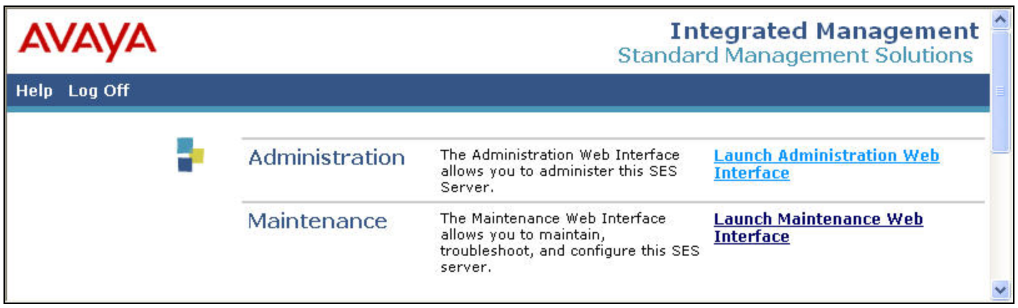
This section is divided into two parts. **Section 4.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations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

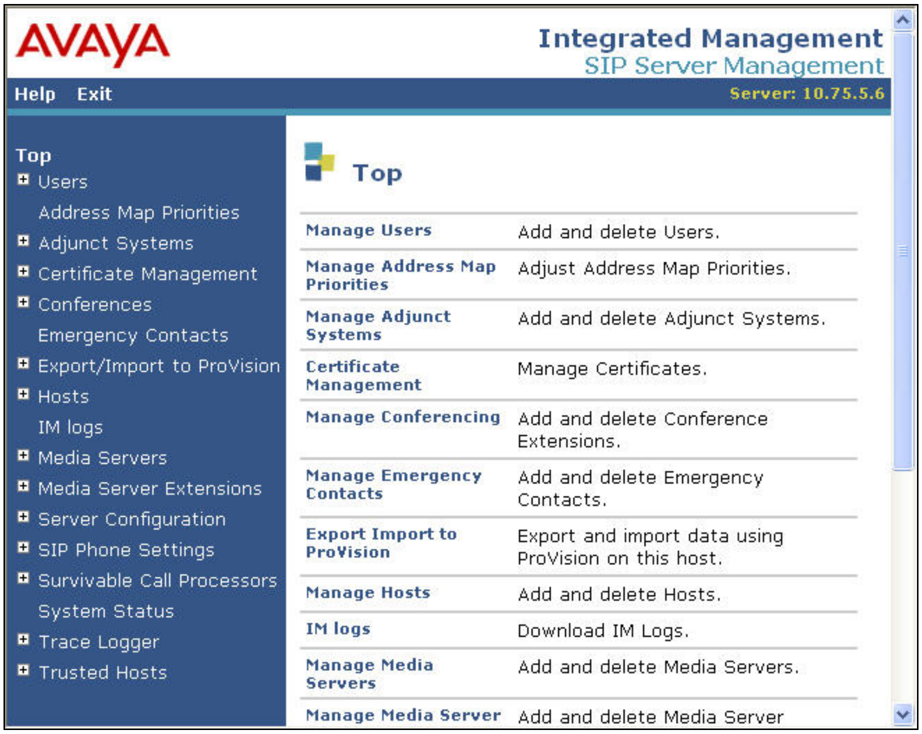
Section 4.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with the SIParator.

This 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.

4.1. Summarize Initial Configuration Parameters

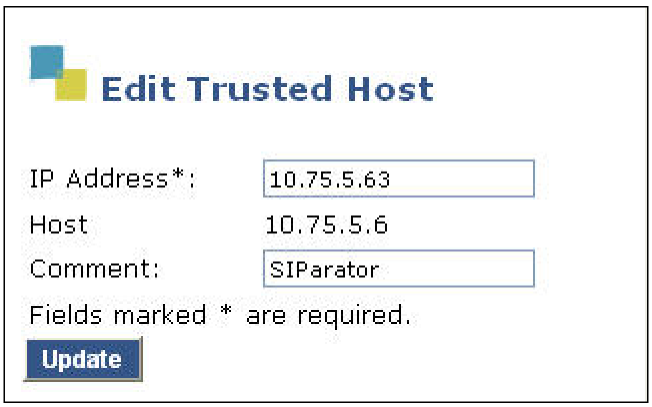
This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description
1.	**Login** Access the Avaya SES administration web interface by entering http://<*ip-addr*>/admin as the URL 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 Administration Web Interface** link from the main page as shown below. 

Step	Description
2.	**Top Page** The Avaya SES **Top** page will be displayed as shown below. 
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 administration home page shown in the previous step. • SIP Domain: ***business.com*** (To view, navigate to **Server Configuration→System Parameters**) • Host IP Address (SES IP address): ***10.75.5.6*** • Host Type: ***SES combined home-edge*** (To view, navigate to **Host→List**; click **Edit**) • Media Server (Avaya Communication Manager) Interface Name: ***CMeast*** • SIP Trunk Link Type: ***TLS*** • SIP Trunk IP Address (Avaya S8300 Server IP address): ***10.75.5.2*** (To view, navigate to **Media Server→List**; click **Edit**)

4.2. SIParator Specific Configuration

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

Step	Description
1.	**Trusted Host** The IP address of the SIParator must be configured as a trusted host in Avaya SES so that SIP messages from the SIParator are not challenged by Avaya SES. To view the trusted host settings, navigate to **Trusted Hosts→List** from the left pane of the Avaya SES window. Click **Edit** next to the trusted host entry associated with the SIParator (not shown). The **Edit Trusted Host** screen will appear. The parameters are described below: • **IP Address**: The private side IP address of the SIParator. • **Comment**: Any descriptive comment. In the case of the branch site, the public IP address of the SIParator will be set up as a trusted host on the branch site Avaya SES. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

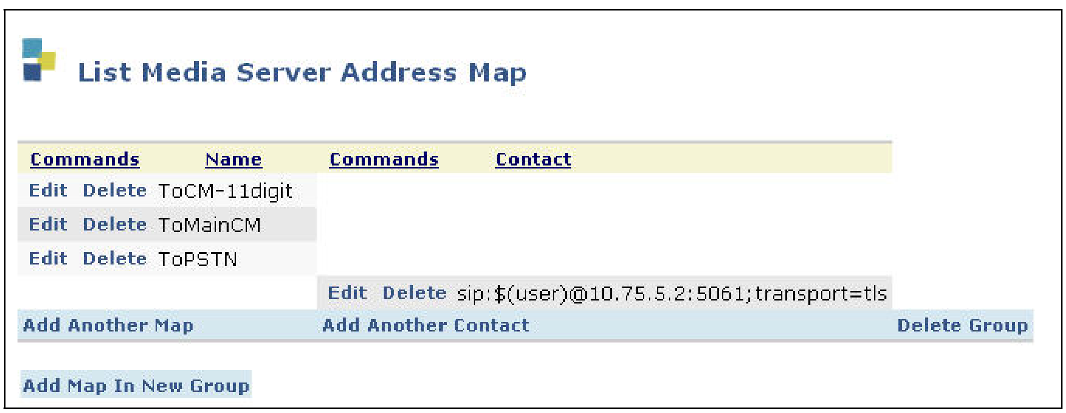
Media Server Address Map
A media server address map is needed to route calls from the remote site to a non-SIP phone at the local site. This is because neither the caller nor the called party is a registered user on Avaya SES with a media server extension assigned to it. Thus, Avaya SES does not know to route this call to Avaya Communication Manager. Thus to accomplish this task, a media server address map is needed.

To view the configured media server address maps, navigate to **Media Server→List** in the left pane. Click the **Map** link next to the Avaya S8300 Server name (not shown). The list of media server address maps will appear. Each map defines criteria for matching calls to Avaya SES based on the contents of the SIP Request-URI of the call. If a call matches the map, then the call is directed to the **Contact**.

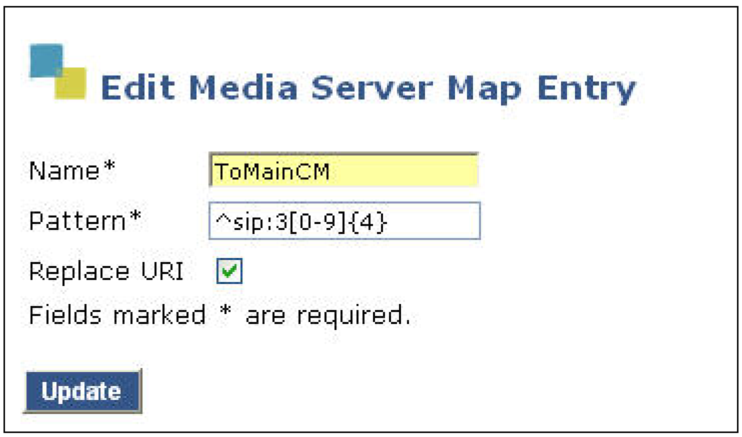
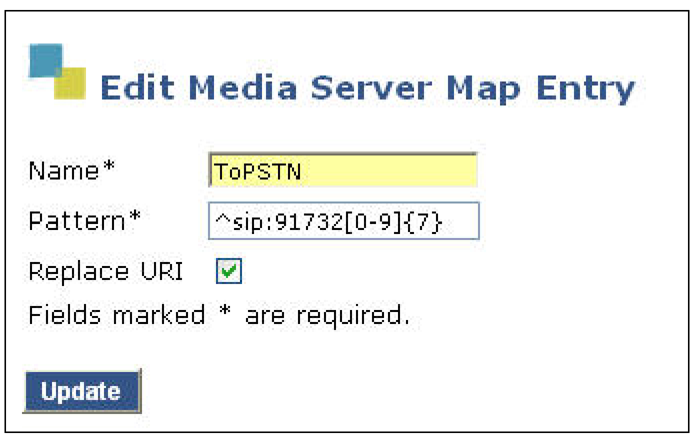
In the example below, three maps are shown. Only the maps named ***ToMainCM*** and ***ToPSTN*** were used for the compliance test. Both of these maps were associated to a **Contact** that directs the calls to the IP address of the Avaya S8300 Server (***10.75.5.2***) using port ***5061*** and ***TLS*** as the transport protocol. The user portion in the original request URI is substituted for ***$(user)*** in the **Contact** expression shown below.

```
sip:$(user)@10.75.5.2:5061;transport=tls
```

To view or edit the call matching criteria of the map, click the **Edit** link next to the map name.



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

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

5. Configure the Avaya SIP Telephones

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

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

6. Configure the Ingate SIParator

This section describes the configuration of the Ingate SIParator. It assumes the SIP Trunking module has been installed. In addition, to support the setting of the Differentiated Services Code Point (DSCP) bits for quality of service, the QoS module must be installed and requires additional licensing.

The SIParator is configured initially with the Ingate Startup Tool. Based on the provided input, the Startup Tool will create an initial configuration that can be uploaded to the SIParator. The results of this configuration can then be viewed or expanded using the SIParator web interface. To access the web interface, enter the IP address of the SIParator as the destination address in a web browser. When prompted for login credentials, enter an appropriate user name and password.

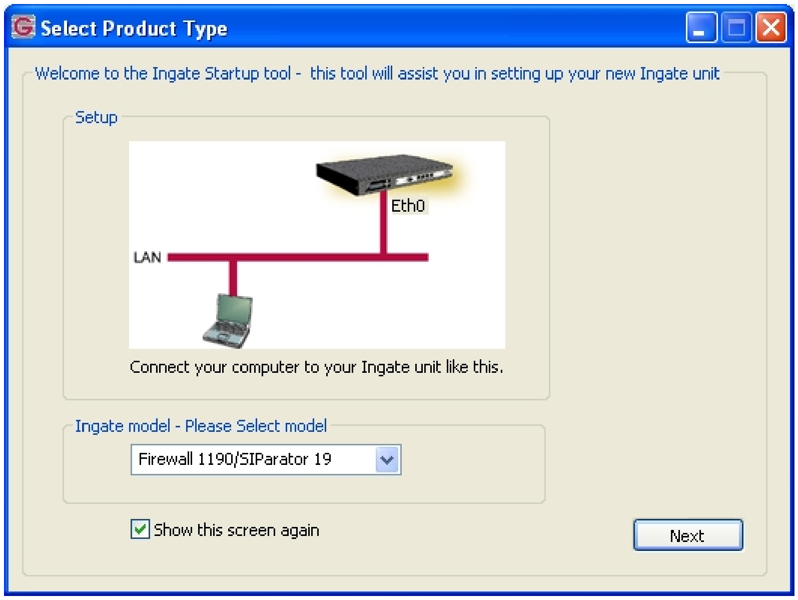
Much of the detailed SIP configuration is not visible from the Startup Tool but is driven by the type of IP-PBX and Service Provider chosen in the Startup Tool. The detailed SIP configuration resulting from the following procedure is captured in **Appendix A** for reference.

Step	Description
1.	**Launch Startup Tool** The Ingate Startup Tool is a windows application which is launched from the Windows Start Menu by navigating to **Start→All Programs→Shortcut to StartupTool.exe**.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Select Product Type

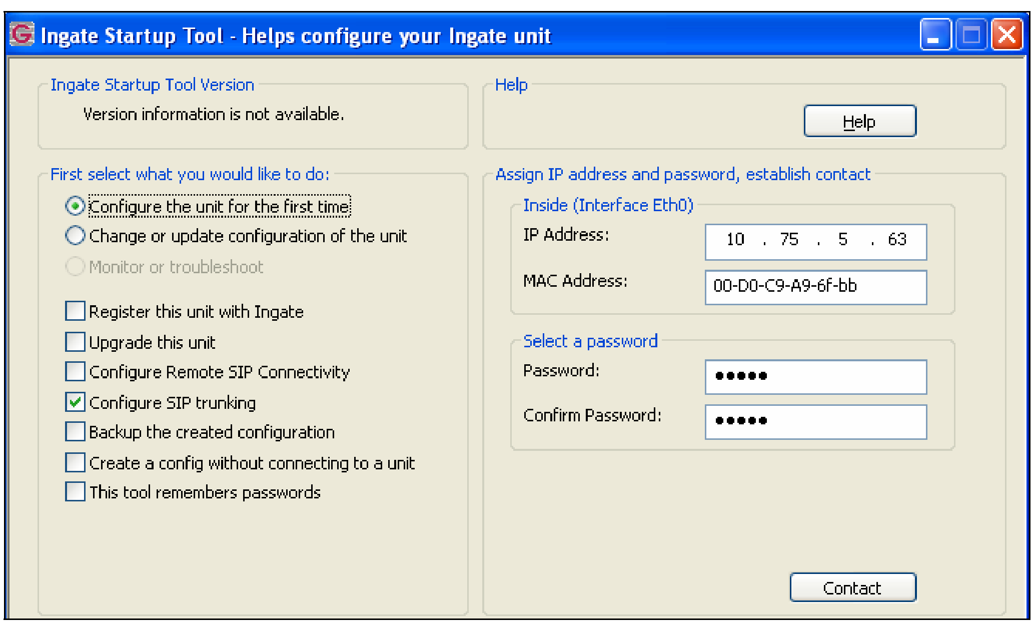
The initial Ingate Startup Tool screen is shown below. Verify the PC is running on the same LAN subnet as the SIParator as shown in the diagram. This is necessary in order to assign the initial IP address to the SIParator from the Startup Tool. Select the SIParator model from the **Ingate model** drop-down menu. Click the **Next** button.



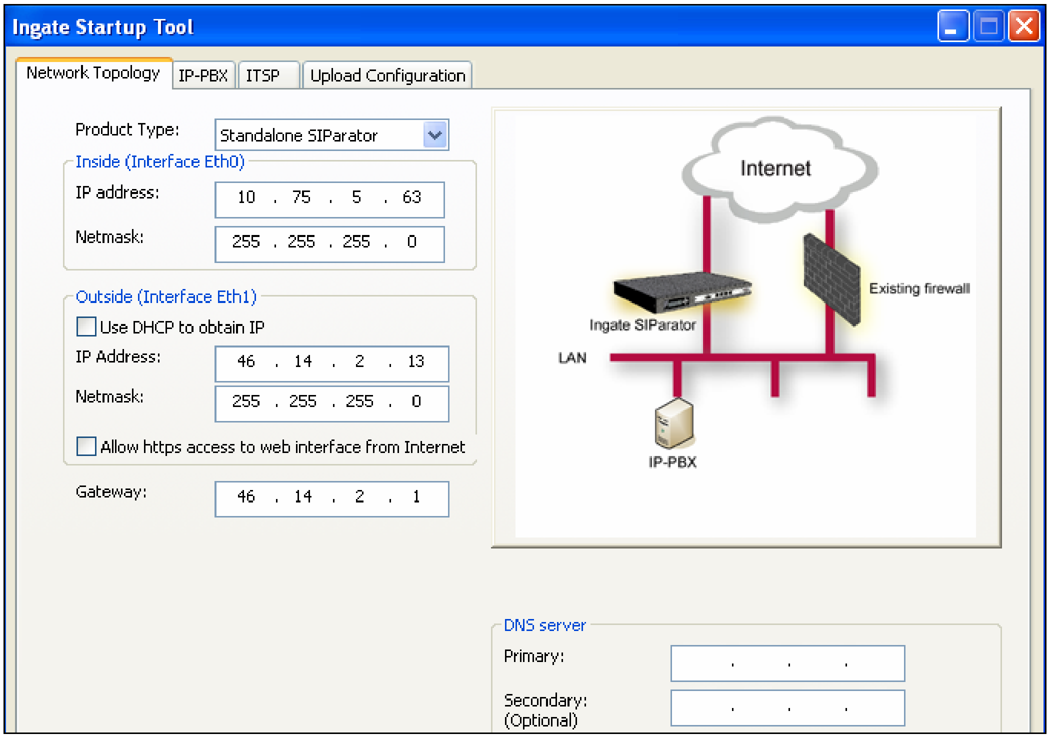
</td></tr>
<tr><td>3.</td><td>

Select Configuration Options and Assign Private IP

Select options for **Configure the unit for the first time** and **Configure SIP trunking**. Enter the inside IP address and a password. Click the **Contact** button to establish a connection to the SIParator.



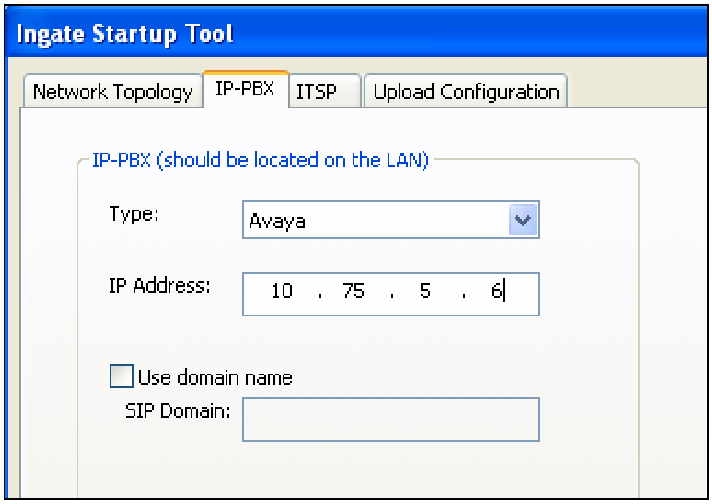
</td></tr>
</table>

Step	Description
4.	**Network Topology** On the next page, select the **Network Topology** tab. Select ***Standalone SIParator*** from the **Product Type** drop-down menu. Enter an IP address and subnet mask for both the inside and outside interfaces as shown in **Figure 1**. The **Gateway** field is set to the IP address of the default gateway on the public side of the SIParator. A DNS server was not used for the compliance test so the DNS server values were left blank. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

IP-PBX Settings

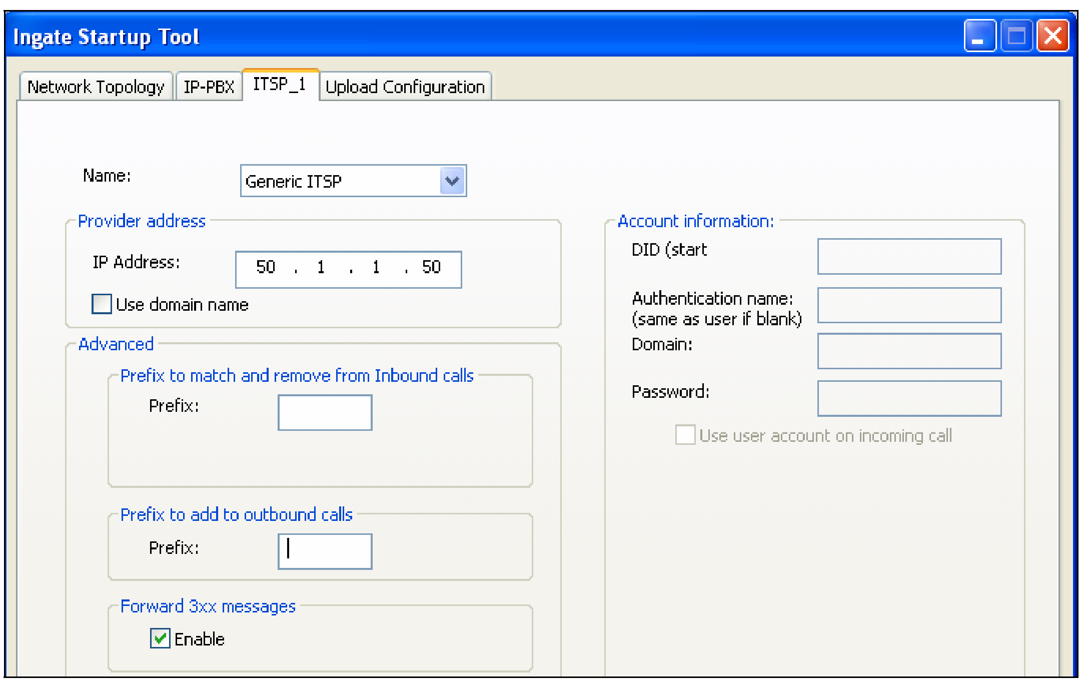
Select the **IP-PBX** tab. Select ***Avaya*** from the **Type** drop-down menu. This will instruct the Startup Tool to configure the SIP parameters on the internal interface to be compatible with the Avaya SES. Enter the Avaya SES IP address in the **IP Address** field.



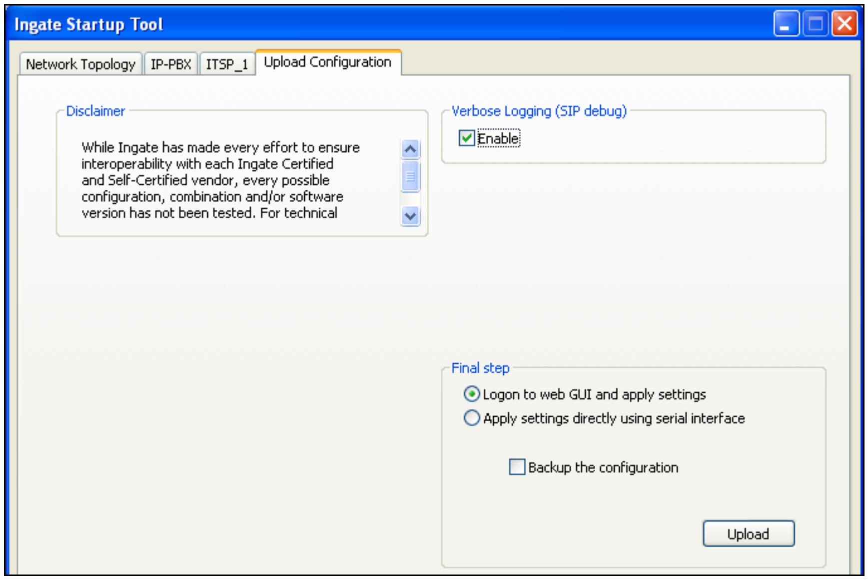
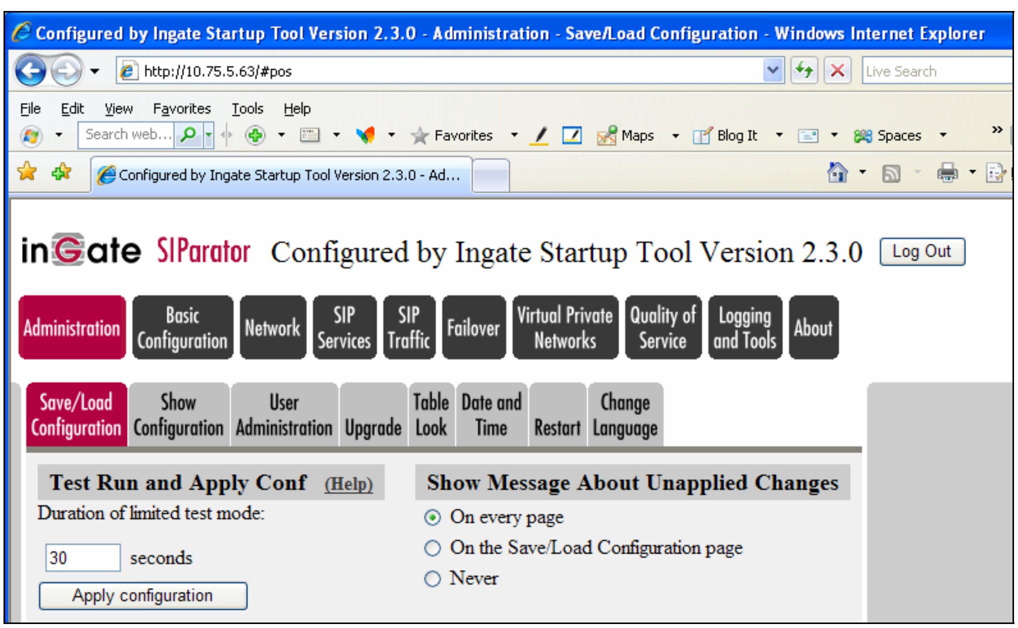
</td></tr>
<tr><td>6.</td><td>

Service Provider Settings

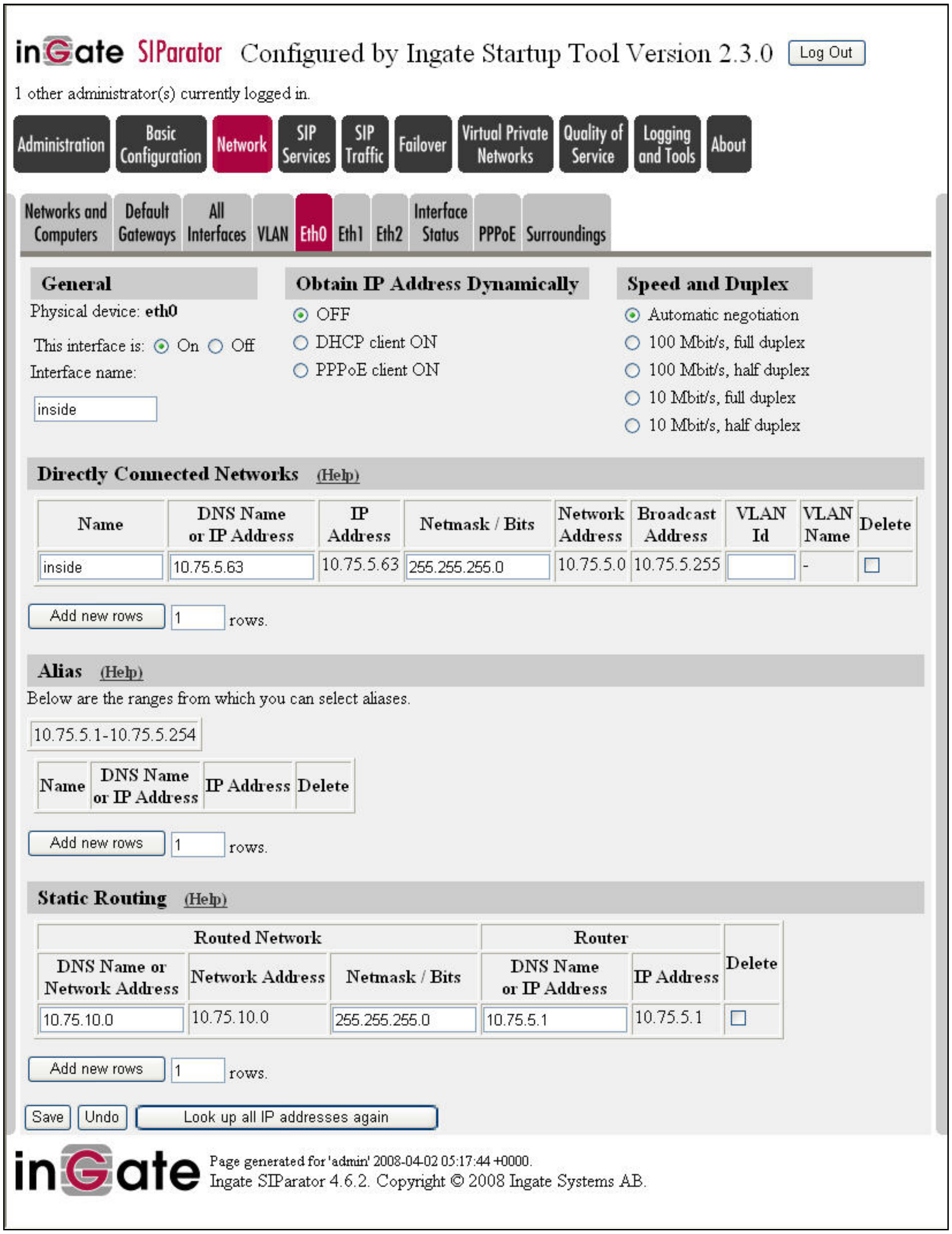
Select the **ITSP_1** tab. Select ***Generic ITSP*** from the **Name** drop-down menu. This will instruct the Startup Tool to configure the SIP parameters on the external interface to be compatible with a generic SIP service provider. In the **IP Address** field, enter the remote Avaya SES IP address on the untrusted side of the SIParator.



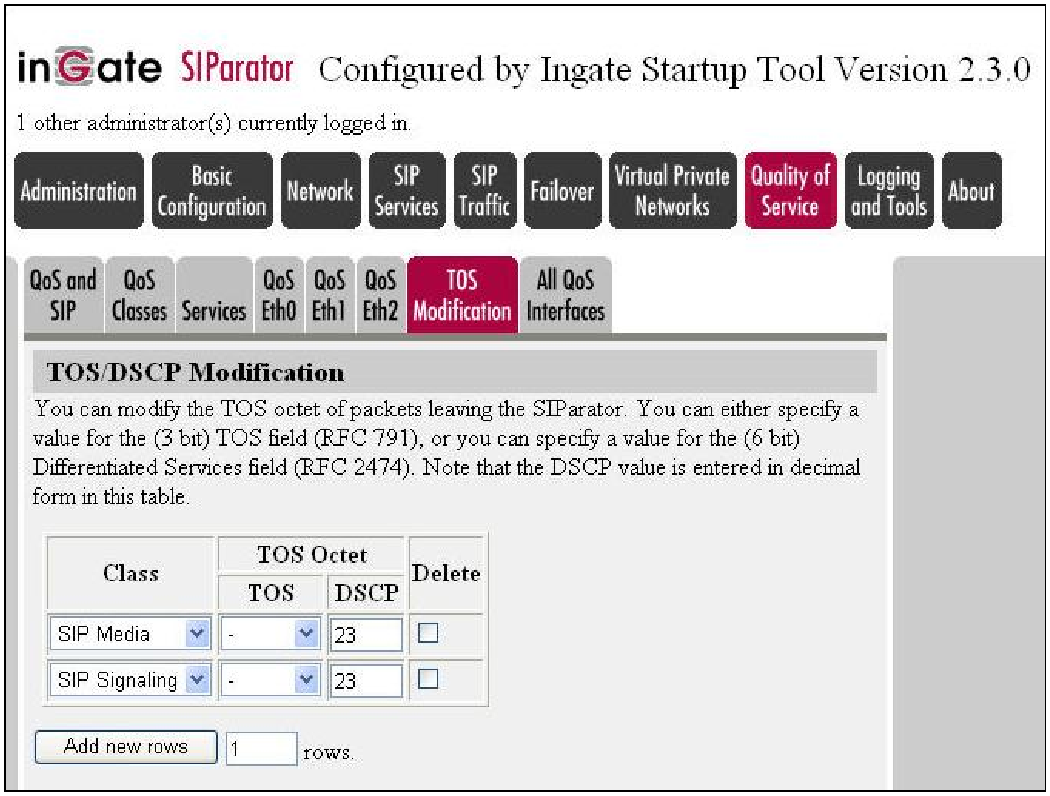
</td></tr>
</table>

Step	Description
7.	**Upload Configuration** Select the **Upload Configuration** tab to upload the configuration to the SIParator. Click the **Upload** button to begin the upload. 
8.	**Apply Configuration** After uploading the configuration, the Startup Tool opens a web browser to the **Administration→Save/Load Configuration** page of the SIParator. Click the **Apply configuration** button to apply the configuration. The Startup Tool configuration is complete at this point. However, additional configuration was required to support all the test cases in the compliance test. This configuration is performed using the SIParator web interface and is covered in the remaining steps. 

Step	Description
9.	**Configure Static Routes** In order to support endpoints on other networks within the enterprise other than the subnet to which the SIParator is directly connected, then a static route must be configured on the internal interface. In the case of the compliance test, one endpoint was located on the 10.75.10.0/24 network. Thus, to view the static route configured for this network, navigate to **Network→Eth0**. Scroll down to the **Static Routing** section. In this case, the routed network with **Network Address *10.75.10.0*** and **Netmask** of ***255.255.255.0*** is reached using **Router IP address *10.75.5.1***.



Step	Description
10.	**Quality of Service** In order to set the Type of Service (TOS) or DSCP bits, the optional QoS module must first be installed. To set the values for these bits, navigate to **Quality of Service→ TOS modification**. In the case of the compliance test, both the SIP media and SIP signaling packets were marked with a DSCP value of 23 (decimal).



7. Interoperability Compliance Testing

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

7.1. General Test Approach

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

7.2. Test Results

The SIParator 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 sites.
- Calls from both SIP and non-SIP endpoints between sites.

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

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya SES web administration interface, verify that all endpoints are registered with the local Avaya SES. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed from both SIP and non-SIP endpoints between sites.

9. Support

For technical support on the SIParator, contact Ingate via the support link at www.ingate.com.

10. Conclusion

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

11. Additional References

[1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 6.0, January 2008.

[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 4, January 2008.

[3] *SIP support in Avaya Communication Manager Running on 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 and Administering SIP Enablement Services*, Doc# 03-600768, Issue 5, January 2008.

[6] *Avaya IA 770 INTUITY AUDIX Messaging Application Release 5.0, Administering Communication Manager Servers to Work with IA 770,* January 2008.

[7] *Concepts and Examples ScreenOS Reference Guide*, Release 5.4.0, Rev.B.

[8] *Ingate SIParator Getting Started Guide*.

[9] *Ingate SIParator Reference Guide.*

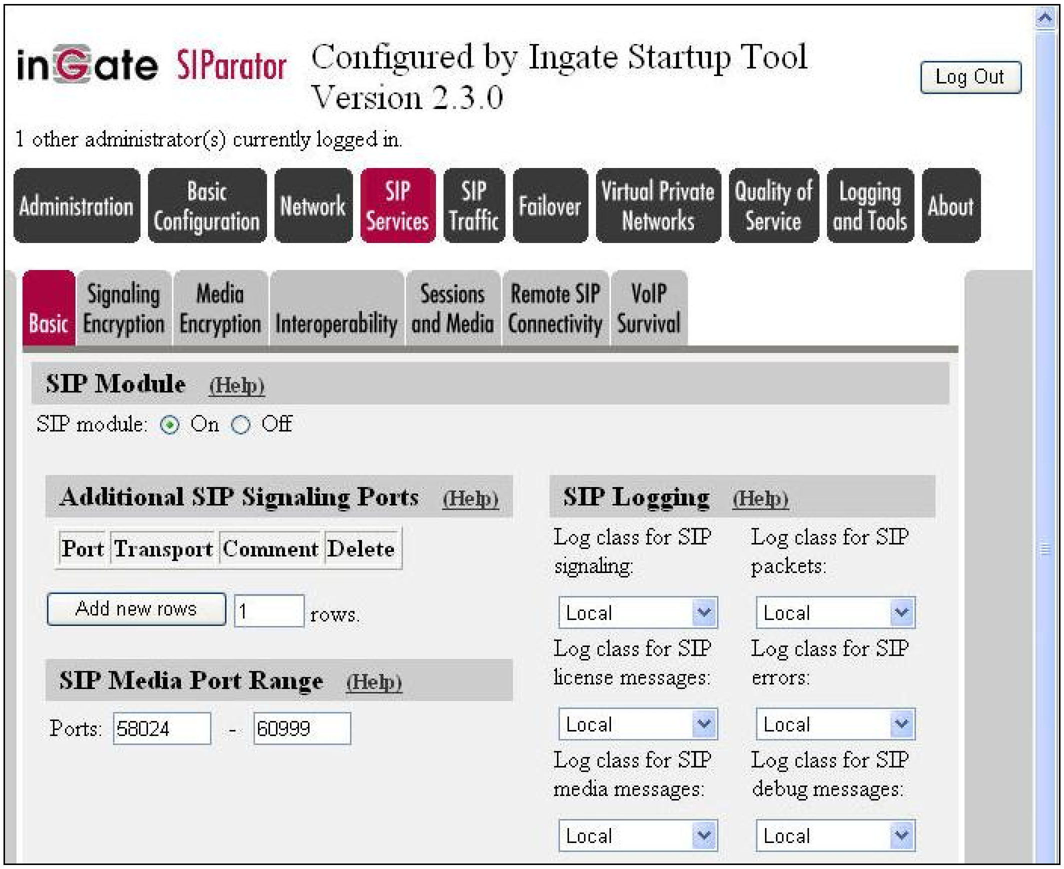
Product documentation for Avaya products may be found at http://support.avaya.com.

Product documentation for the SIParator can be obtained from Ingate. Contact Ingate using the contact link at http://www.ingate.com.

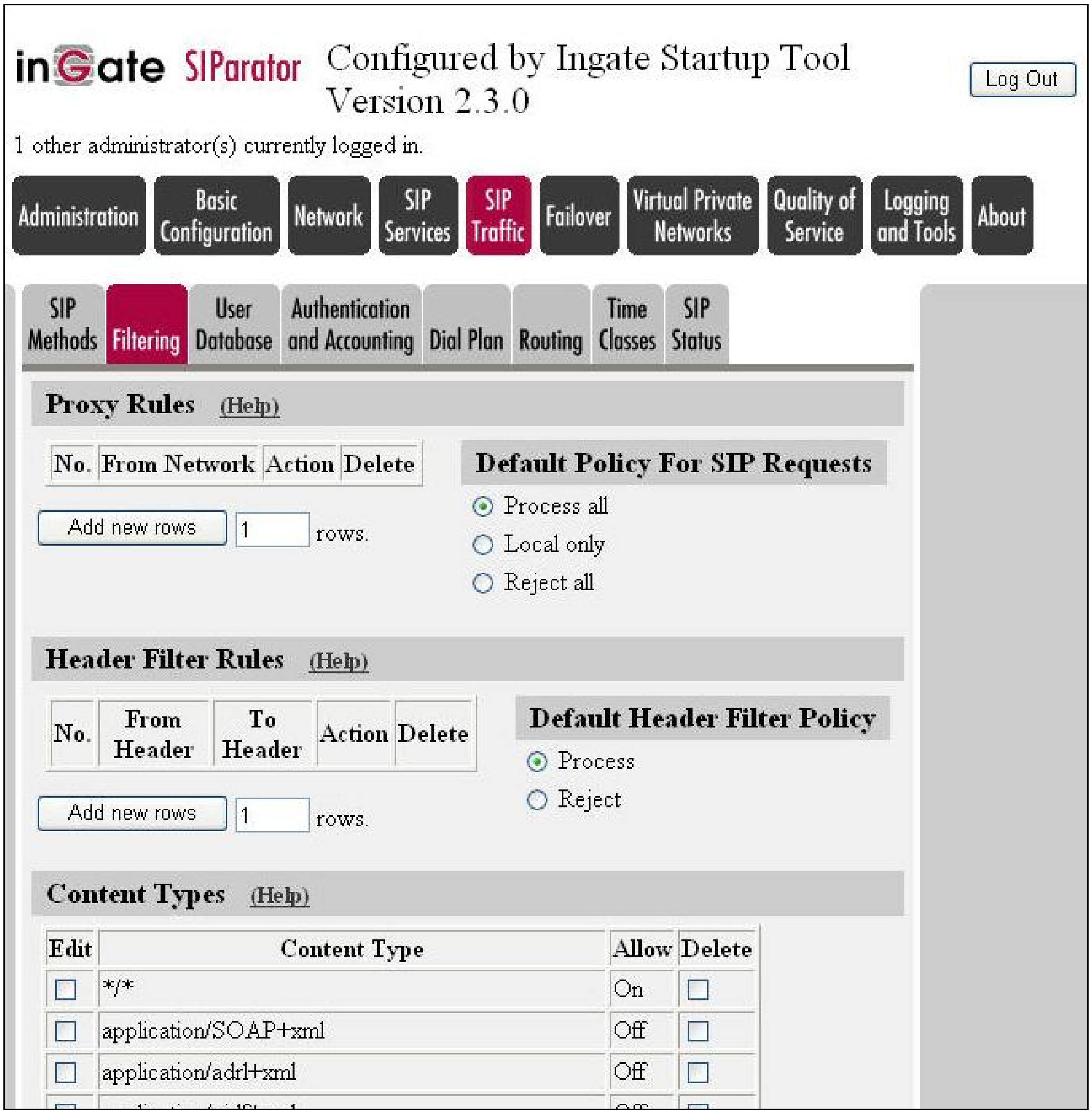
Appendix A: SIParator SIP Configuration

This section contains the key SIP configuration screens resulting from the procedure described in **Section 6** using the Ingate Startup Tool. These screens are included only as a reference with minimal explanation.

SIP Services → Basic Page



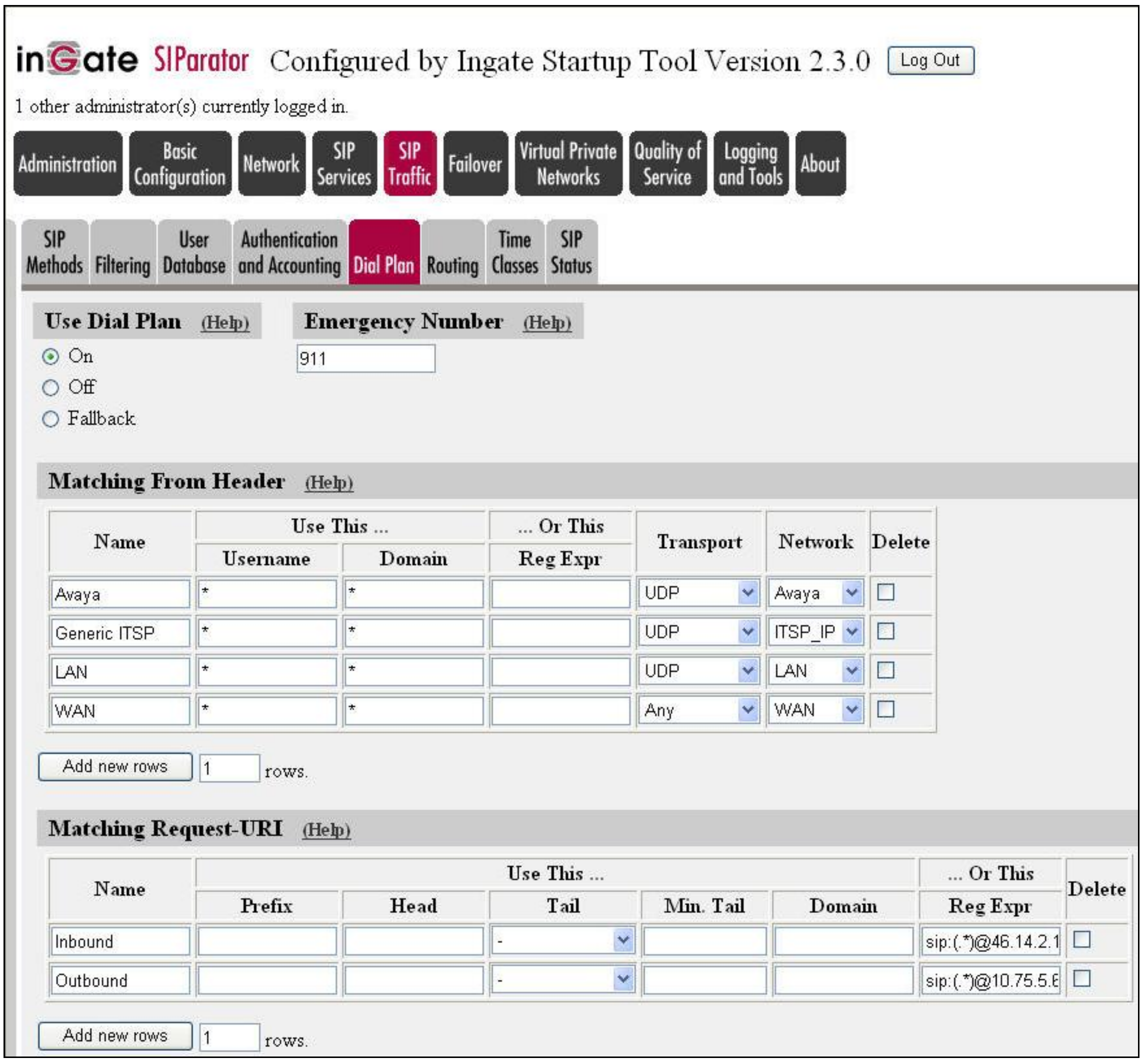
SIP Traffic → Filtering Page
In the **Proxy Rules** section, **Process all** is selected. In the **Content Types** section, the first entry in the table allows all content types (*/*) to be processed.



SIP Traffic → Dial Plan Page (Part 1)

In the **Matching From Header** section, four separate matching criteria are defined that can be used to match the SIP From header. The From header criteria named ***Avaya*** matches traffic from the local Avaya SES. The criteria named ***Generic ITSP*** matches the remote Avaya SES. The criteria named ***LAN*** matches any traffic on the trusted LAN that did not match the local Avaya SES. Lastly, the criteria named ***WAN*** matches any traffic from the WAN that did not match the remote Avaya SES.

In the **Matching Request-URI** section, two separate matching criteria are defined that can be used to match the SIP Request-URI. The Matching Request-URI criteria named ***Inbound*** will match the associated regular expression shown in the table. Similarly, the criteria named ***Outbound*** will match the regular expression associated with it in the table.



SIP Traffic → Dial Plan Page (Part 2)
In the **Forward To** section, two separate forwarding criteria are defined. The Forward To criteria named ***Avaya*** (which is not the same as the Matching From Header criteria named ***Avaya***) will change the Request-URI of the forwarded message using the regular expression associated with it in the table and send the request to the IP address defined in the expression. The Forward To criteria named ***Generic ITSP*** will use its regular expression in the same manner to forward the message.

In the **Dial Plan** section, the criteria defined in the previous three sections are used to define the routing of SIP calls. For example, the first route defines that messages that match the **From Header** criteria named ***Avaya*** and **Request-URI** criteria named ***Outbound*** should be forwarded using the **Forward To** criteria named ***Generic ITSP***.

Forward To (Help)

Name	Subno.	Use This ...	... Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
Avaya	1	-			-	sip:$1@10.75.5.6	☐
Generic ITSP	1	-			-	sip:$1@50.1.1.50	☐

Add new rows 1 groups with 1 rows per group.

Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		E
					Forward	ENUM	
1	Avaya	Outbound	Forward	Generic ITSP			-
2	Generic ITSP	Inbound	Forward	Avaya			-
3	WAN	-	Reject	-			-

Add new rows 1 rows.

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.