DevConnect Program

Application Notes for Mutare Voice Traffic Filter with Avaya Aura® Session Manager and Avaya Session Border Controller using On-Premise Deployment– Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Mutare Voice Traffic Filter with Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller 10.1 using an on-premise deployment. Mutare Voice Traffic Filter is a call filtering solution that screens inbound and outbound calls to/from an Avaya Aura® network. Unwanted calls are either dropped or redirected to a specified destination. In this compliance test, Mutare Voice Traffic Filter connected to Avaya Aura® Session Manager and Avaya Session Border Controller (SBC) via a SIP trunk.

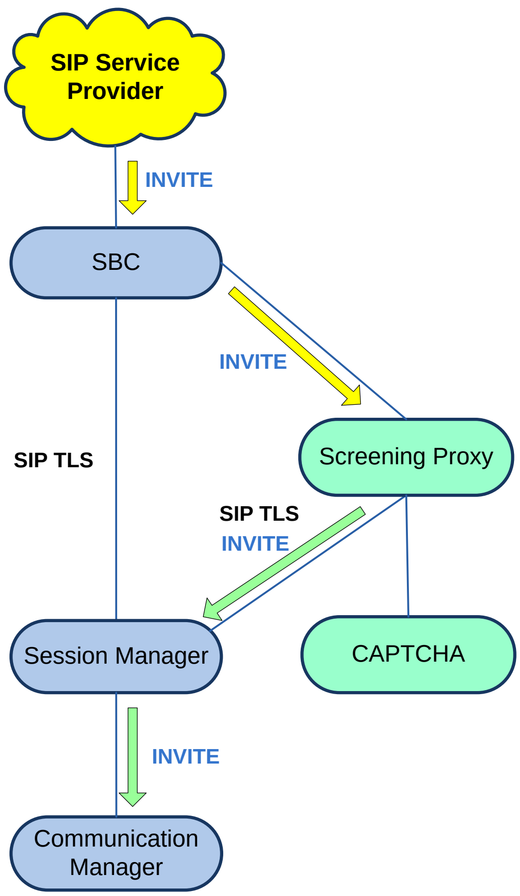
Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

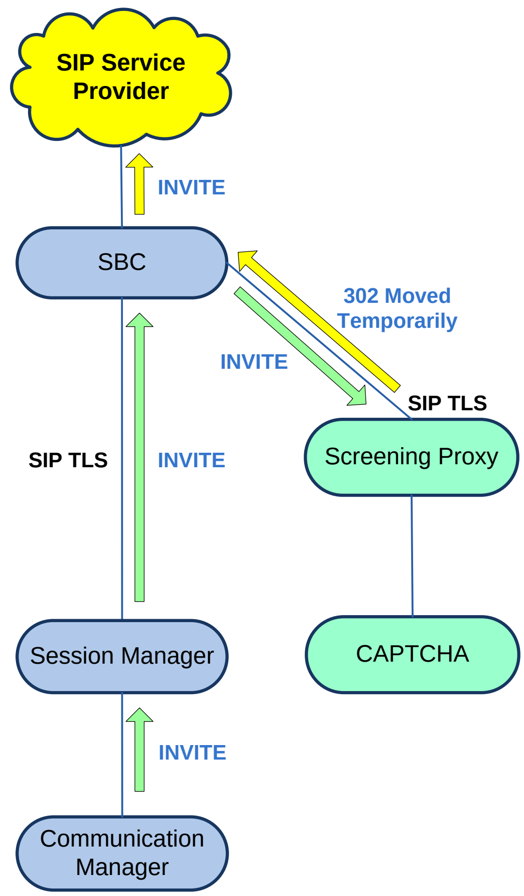
1. Introduction

These Application Notes describe the configuration steps required to integrate Mutare Voice Traffic Filter with Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller (SBC) 10.1 using an on-premise deployment. In this compliance test, Mutare Voice Traffic Filter connected to Session Manager and Avaya SBC via a SIP trunk using TLS/SRTP.

Mutare Voice Traffic Filter is a call filtering solution that screens inbound and outbound calls to/from an Avaya Aura® network. Voice Traffic Filter examines the SIP signaling information and makes call filtering decisions based on 5 layers of protection that include a threat radar, STIR/SHAKEN data, custom rules, dynamic robocall database, and Voice CAPTCHA. For inbound calls, legitimate calls are passed from Avaya SBC to Voice Traffic Filter proxy server, and then to Session Manager via a SIP trunk. The latter passes the call to Avaya Aura® Communication Manager. For outbound calls, legitimate calls are passed from Avaya SBC to Voice Traffic Filter proxy server, and then back to Avaya SBC using 302 Moved Temporarily with destination to the SIP service provider. Unwanted calls are either dropped or redirected to a specified destination. Such destinations can include an announcement, voicemail, or any other valid extension or PSTN number.



Incoming Call Screening – Call Allowed



Outgoing Call Screening – Call Allowed

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. Feature testing focused on making inbound calls from the PSTN and verifying that Voice Traffic Filter applied the appropriate call treatment to caller IDs that were matched against the enterprise, whitelist, enterprise blacklist and dynamic robocall database Unwanted were either dropped or redirected to a specified destination. Similar tests were performed to verify that outbound calls from the Avaya Aura® network to the PSTN were given the appropriate call treatment.

Serviceability testing focused on verifying that Voice Traffic Filter came back into service after the Voice Screening Proxy was restarted or the network connection was restored.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and Mutare Voice Traffic Filter used TLS/SRTP encryption features. TLS transport was used with Mutare Voice Screening Proxy and SRTP was used with Mutare Voice CAPTCHA.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing a SIP trunk from Voice Screening Proxy to SBC using TLS transport and verifying the exchange of SIP OPTIONS messages.
- Establishing a SIP trunk from Voice Screening Proxy to Session Manager using TLS transport and verifying the exchange of SIP OPTIONS messages.
- Using G.711 codec support and SRTP for secure media to Voice CAPTCHA. If Voice CAPTCHA is applied to an inbound call, the caller would be prompted to enter a security code to ensure that the call is not a robocall.
- Filtering inbound and outbound calls through Voice Traffic Filter by matching the caller ID against the enterprise blacklist and dynamic robocall database.

- Applying the appropriate configured action for inbound calls, including Allow, Drop, Route, CAPTCHA Drop and CAPTCHA Route.
- Applying the appropriate configured action for outbound calls, including Allow, Drop, and Route.
- Verifying that SBC routes call to a secondary route, if Voice Traffic Filter is not available, and that the call is completed successfully.
- Proper system recovery after a reboot of the Voice Screening Proxy and loss of network connectivity.

2.2. Test Results

All test cases passed.

2.3. Support

Technical support on Mutare Voice Traffic Filter can be obtained through the following:

- **Phone:** +1 (855) 782-3890
- **Email:** help@mutare.com
- **Web :** https://www.mutare.com/contact

3. Reference Configuration

Figure 1 illustrates the test configuration for Mutare Voice Traffic Filter, which consisted of Mutare Voice Screening Proxy and Mutare Voice CAPTCHA in the enterprise network and the Mutare Rules Engine Application Server and the Dynamic Robocall Database in the Private Mutare Cloud.

Voice Traffic Filter connects to SBC and Session Manager via SIP trunks using TLS/SRTP. The SIP trunk to Session Manager is used for inbound PSTN calls only. Voice CAPTCHA may be applied to calls to request the caller to enter a security code to ensure that the call is not a robocall.

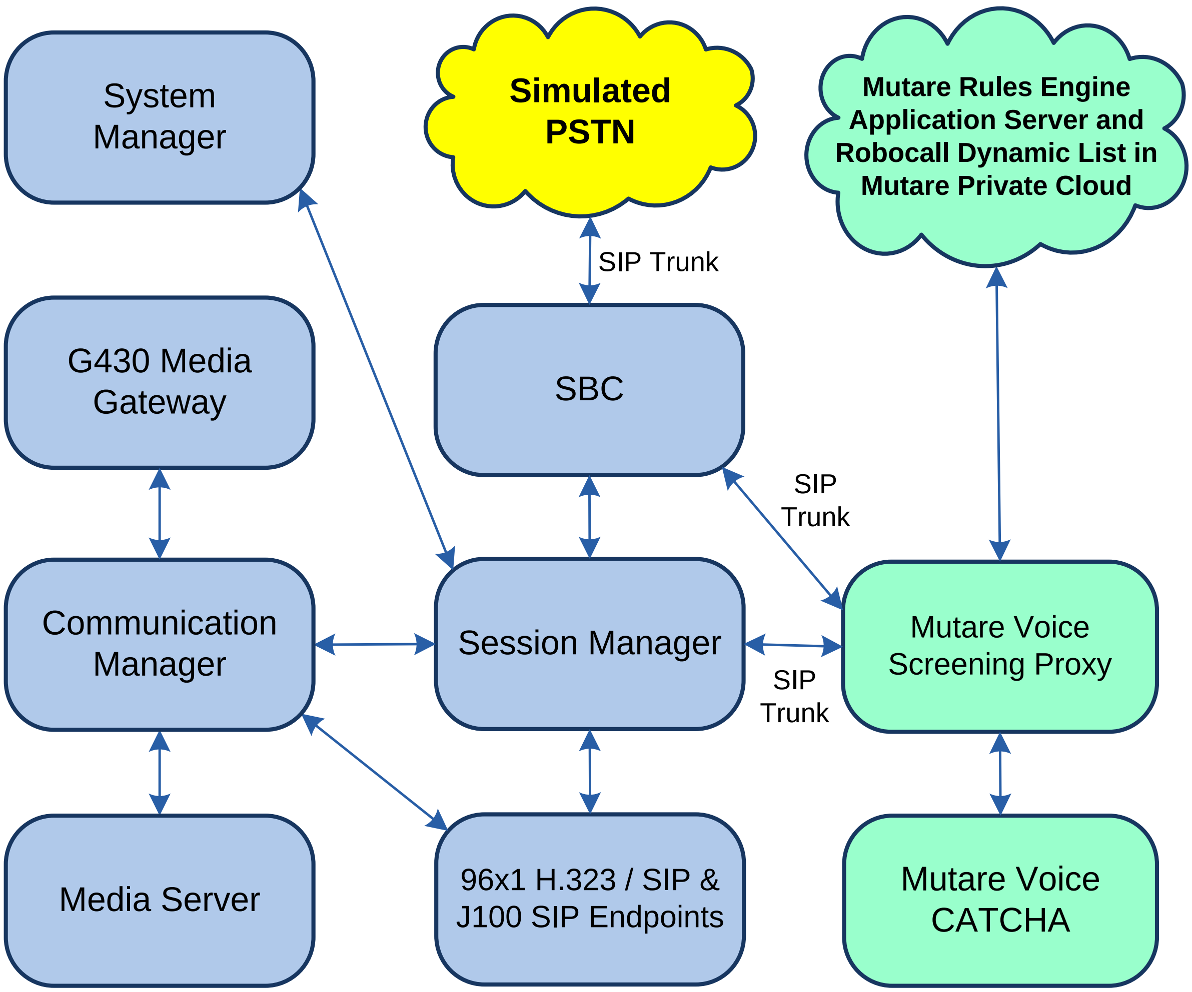


Figure 1: Avaya SIP-based Network with Mutare Voice Traffic Filter

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.1.3.1.0-FP3SP1
Avaya G430 Media Gateway	FW 42.22.0
Avaya Aura® Media Server	10.1.0.125
Avaya Aura® System Manager	10.1.3.1 Build No. – 10.1.0.0537353 Software Update Revision No: 10.1.3.1.0716149 Service Pack 1
Avaya Aura® Session Manager	10.1.3.1.1013103
Avaya Session Border Controller	10.1.2.0-64-23285
Avaya 96x1 Series IP Deskphones	6.8.5.4.10 (H.323)
Avaya J100 Series IP Phones	4.1.1.0.7 (SIP)
Mutare Rules Engine Application Server	3.6.1.0
Mutare Voice Screening Proxy	2.4.11 (OpenSIPS)
Mutare Voice CAPTCHA	1.10.7-release-19 (FreeSwitch)

5. Configure Avaya Aura® Session Manager

This section covers the SIP trunk configuration between Session Manager and Voice Screening Proxy. The configuration includes:

- SIP Entity for Voice Screening Proxy
- Entity Link for Voice Screening Proxy
- SIP Monitoring on Session Manager

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of System Manager. Log in with the appropriate credentials.

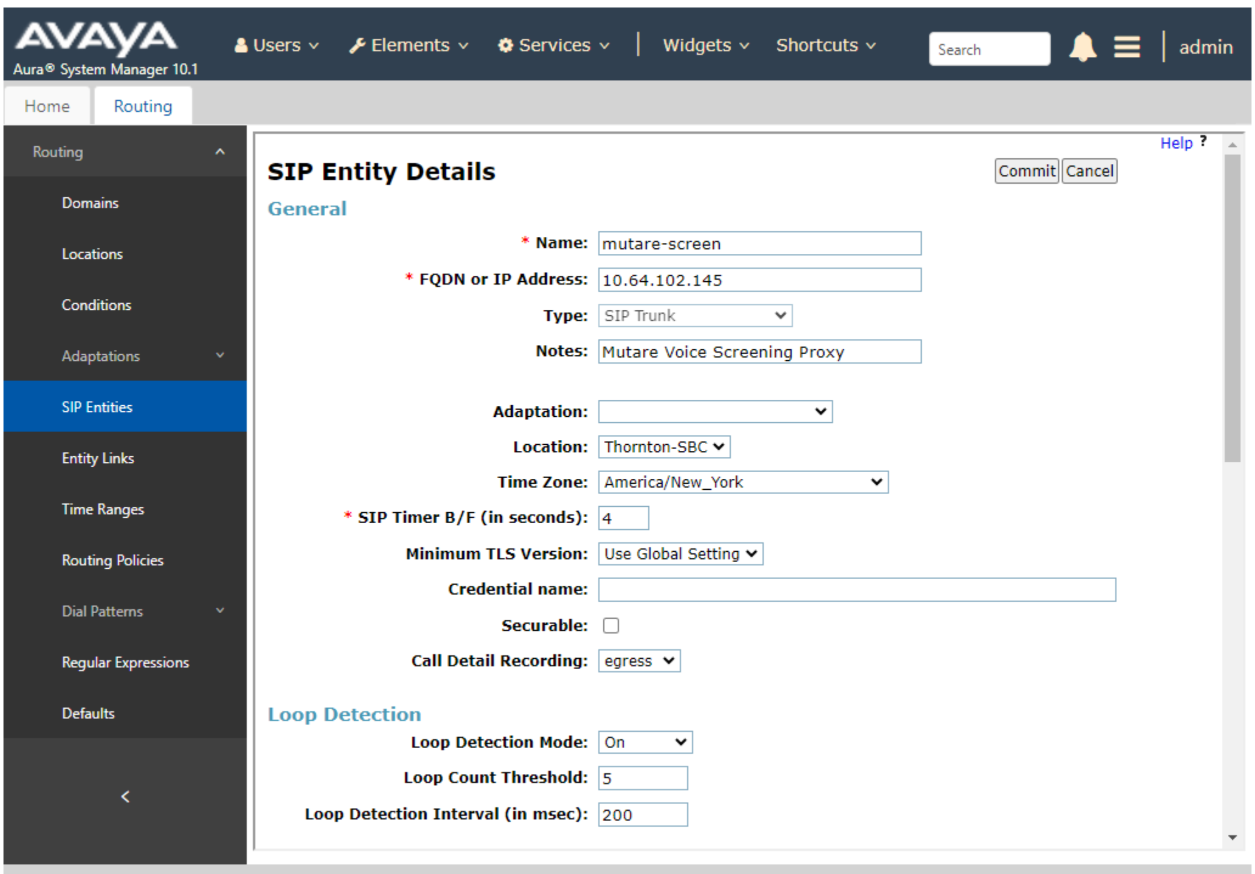
Note: It is assumed that basic configuration of Session Manager has already been performed, including SIP trunks and call routing to Communication Manager and SBC. *This section will focus on the configuration of the SIP trunk to Mutare Voice Screening Proxy*.

5.1. Add SIP Entity for Voice Screening Proxy

Add a SIP Entity for Voice Screening Proxy by navigating to **Elements → Routing → SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for Voice Screening Proxy.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

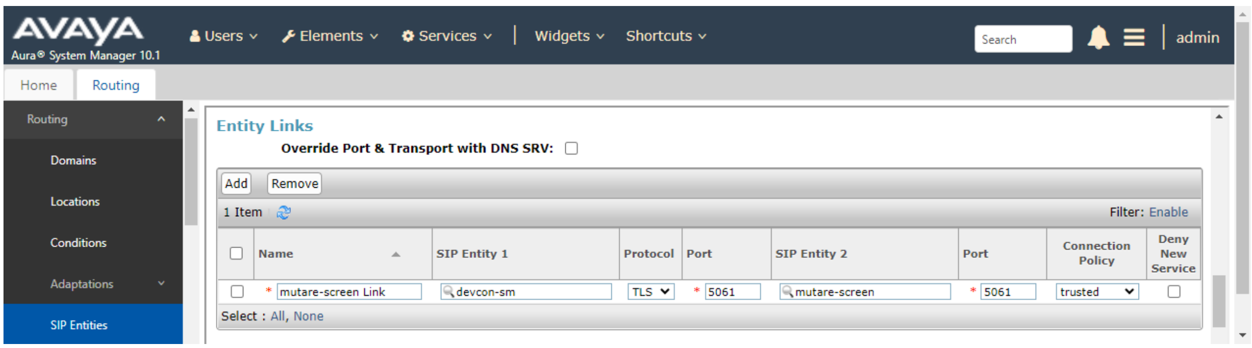
- **Name:** A descriptive name (e.g., *mutare-screen*).
- **FQDN or IP Address:** The IP address of Voice Screening Proxy (e.g., *10.64.102.145*).
- **Type:** Select *SIP Trunk*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.



Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name (e.g., *mutare-screen* Link).
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TLS*.
- **Port:** Set to *5061*.
- **SIP Entity 2:** Specify the Voice Screening Proxy entity name configured above.
- **Port:** Set to *5061*.
- **Connection Policy:** Set to *trusted*.

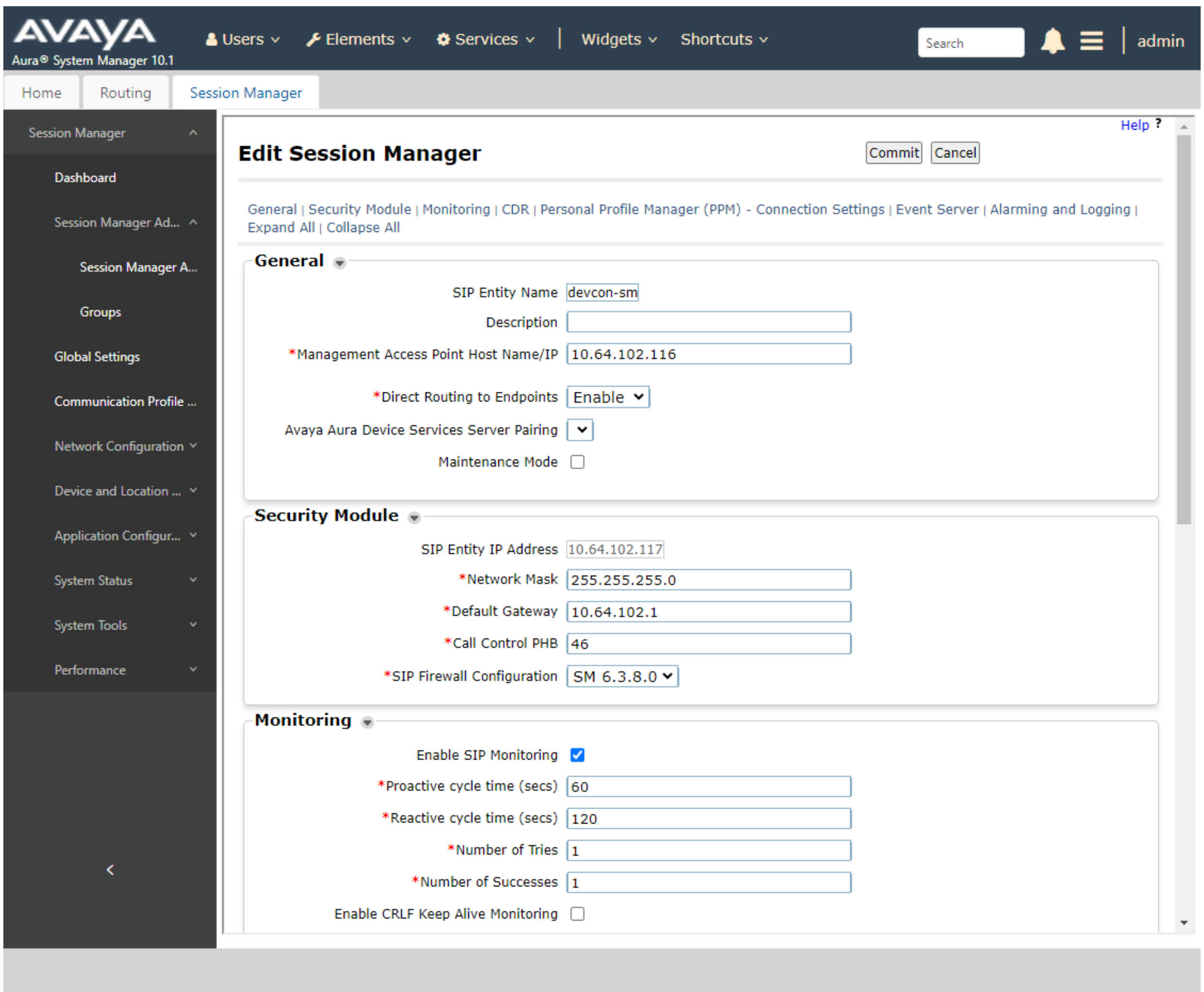
Note: In the compliance test, Avaya Aura® System Manager was used as the Certificate Authority (CA) and the trusted CA certificate was already imported to Session Manager (not shown in these Application Notes).



5.2. Enable SIP Monitoring on Session Manager

Verify that monitoring is enabled for Session Manager. Navigate to **Elements → Session Manager → Session Manager Administration**, select the appropriate Session Manager and click **Edit** (not shown). This assumes that Session Manager has already been configured System Manager.

Next, scroll down to the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to Voice Screening Proxy. Ensure that monitoring is enabled and use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every 60 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.



6. Configure Avaya Session Border Controller

This section covers the SBC configuration required to establish a SIP trunk to Voice Screening Proxy, allow routing of SIP messages to Voice Screening Proxy via Server Flows, and exchange media with Voice CAPTCHA using SRTP. For inbound PSTN calls, SBC routes calls to Voice Screening Proxy as the primary route, if available. Legitimate calls are then passed from Voice Screening Proxy directly to Session Manager, bypassing SBC, and then to Communication Manager. For outbound calls to the PSTN, SBC routes calls to Voice Screening Proxy, if available. Legitimate calls are then passed back to SBC using 302 Moved Temporarily and then routed to the PSTN. If Voice Screening Proxy is not available, SBC routes inbound PSTN calls directly to Session Manager and outbound calls directly to the PSTN.

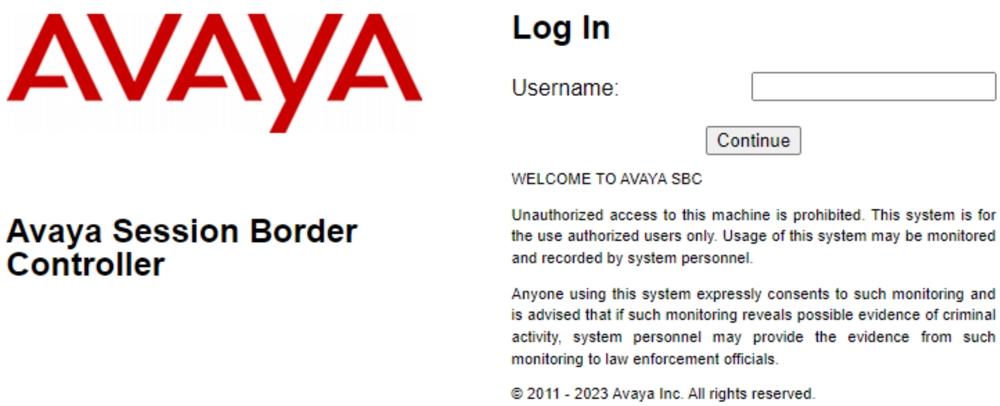
This section covers the following SBC configuration:

- Launch SBC Web Interface
- Administer Server Interworking
- Administer SIP Servers
- Administer Routing Profiles
- Administer Topology Hiding
- Administer URI Groups
- Administer Media Rules
- Administer End Point Policies
- Administer TLS Management
- Administer Media Interfaces
- Administer Signaling Interfaces
- Administer Server Flows

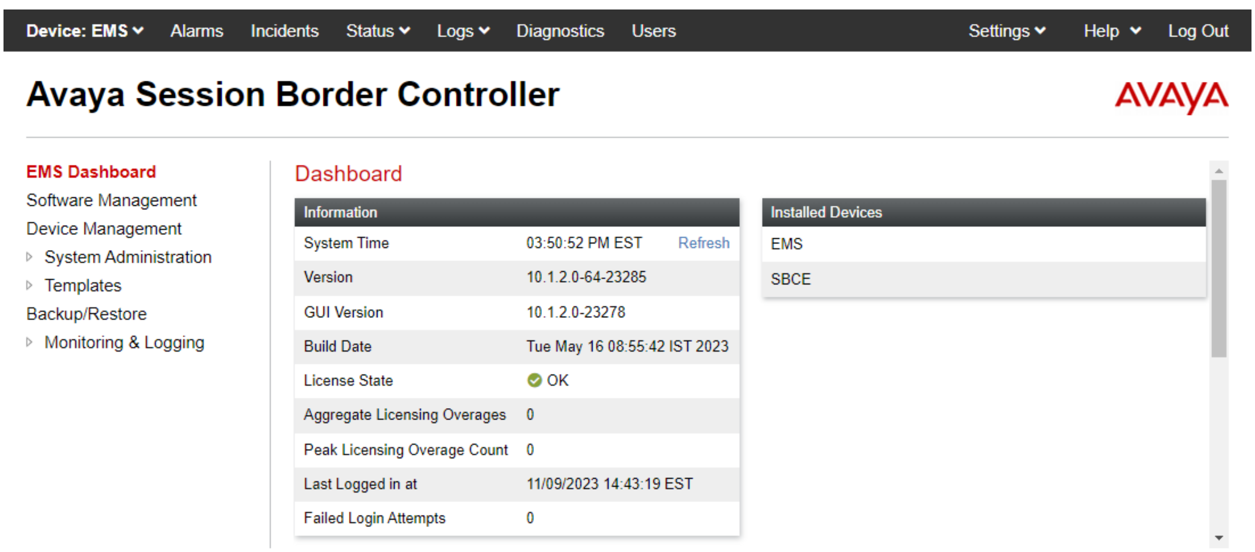
Note: It is assumed that basic SBC configuration has already been performed, including SIP trunk and routing to Session Manager and PSTN. However, any changes required to the existing configuration will be covered.

6.1. Launch SBC Web Interface

Access the SBC web interface by using the URL **https://<*ip-address*>/sbc** in an Internet browser window, where **<*ip-address*>** is the IP address of the SBC management interface. The screen below is displayed. Log in using the appropriate credentials.



After logging in, the Dashboard will appear as shown below. All configuration screens of the SBC are accessed by navigating the menu tree in the left pane. Select **Device → SBCE** from the top menu.

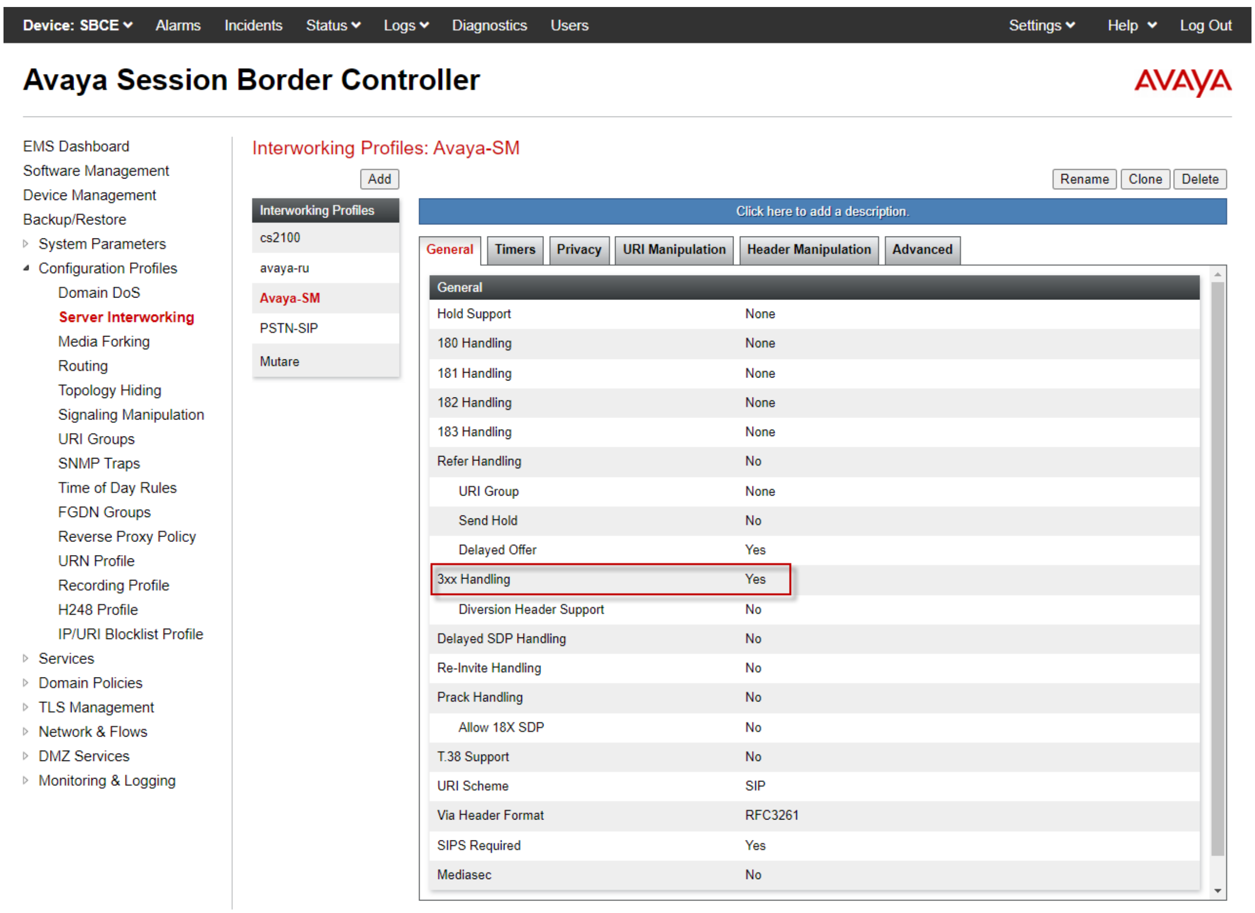


6.2. Administer Server Interworking

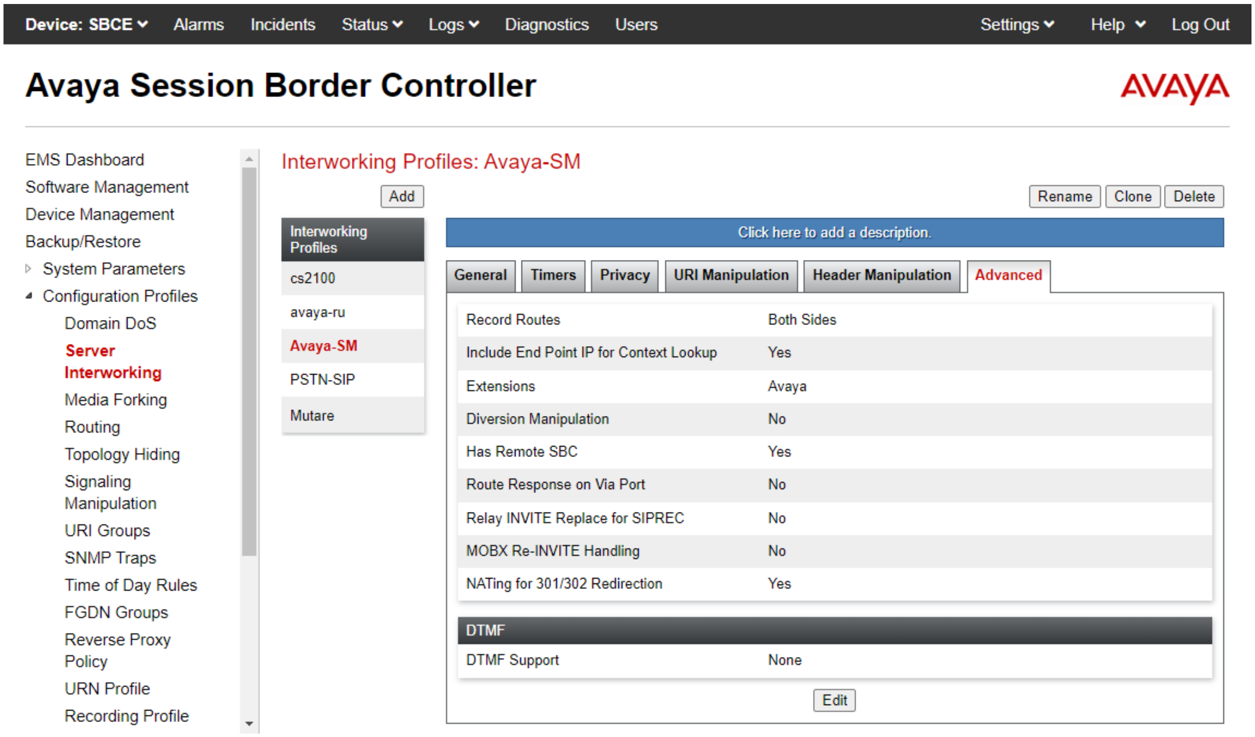
A **Server Interworking** profile defines a set of parameters that aid in interworking between the SBC and a connected server, such as Session Manager, Voice Screening Proxy, and the PSTN. **Server Interworking** profiles were added or changed for Session Manager and Voice Screening Proxy. The PSTN profile is not shown as no changes to the existing configuration were required.

6.2.1. Server Interworking Profile for Session Manager

Modify the **Server Interworking** profile for Session Manager by navigating to **Configuration Profiles → Server Interworking** from the left pane. Click on the Session Manager profile, select the **General** tab, and then click on the **Edit** button (not shown). Enable **3xx Handling** as shown below so that SBC handles 3xx responses locally, which was required for outbound calls only. For outbound calls, SBC routes the call to Voice Screening Proxy, which then responds with a 302 Moved Temporarily with new Contact information, if it is a legitimate call that should be routed to the PSTN.

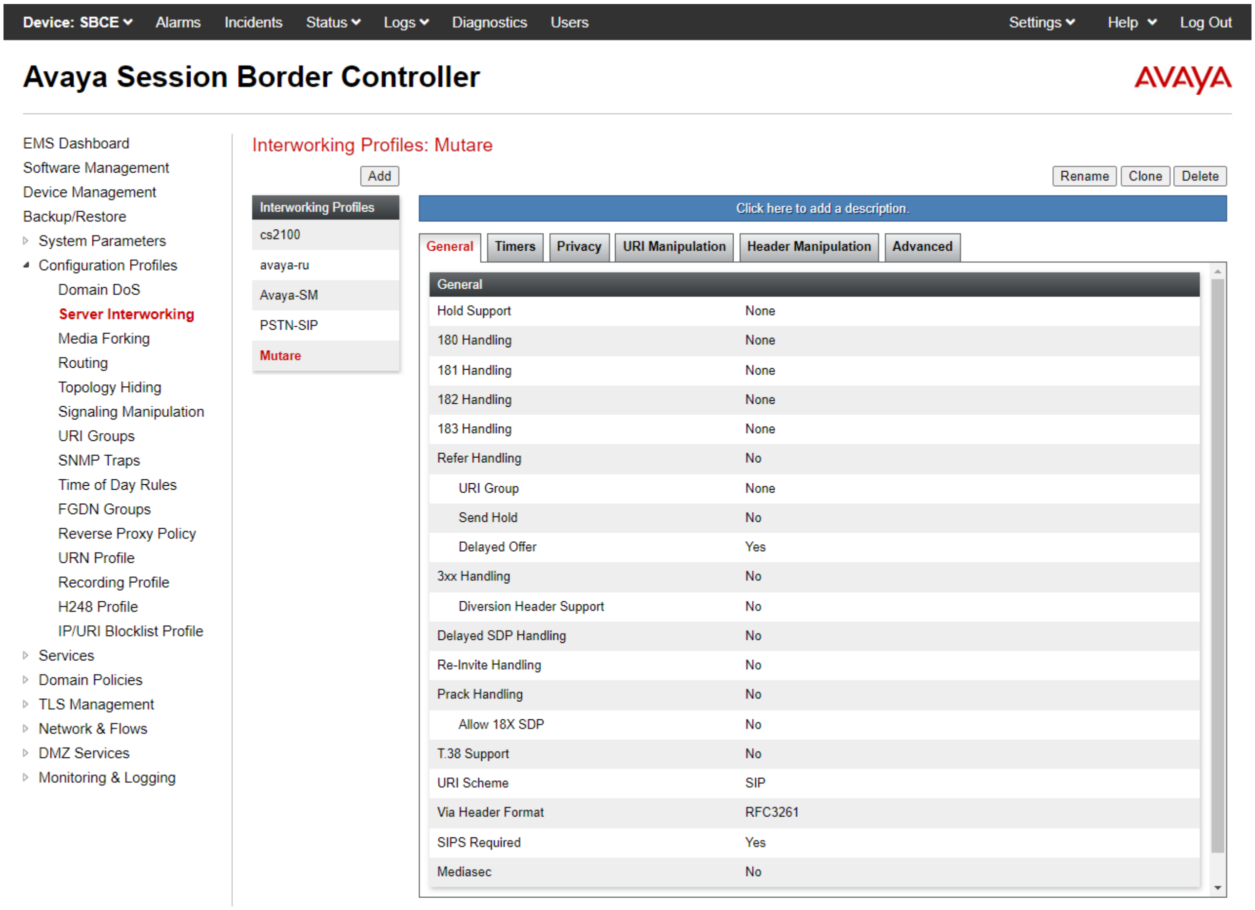


Select the **Advanced** tab and configure the fields as shown below.

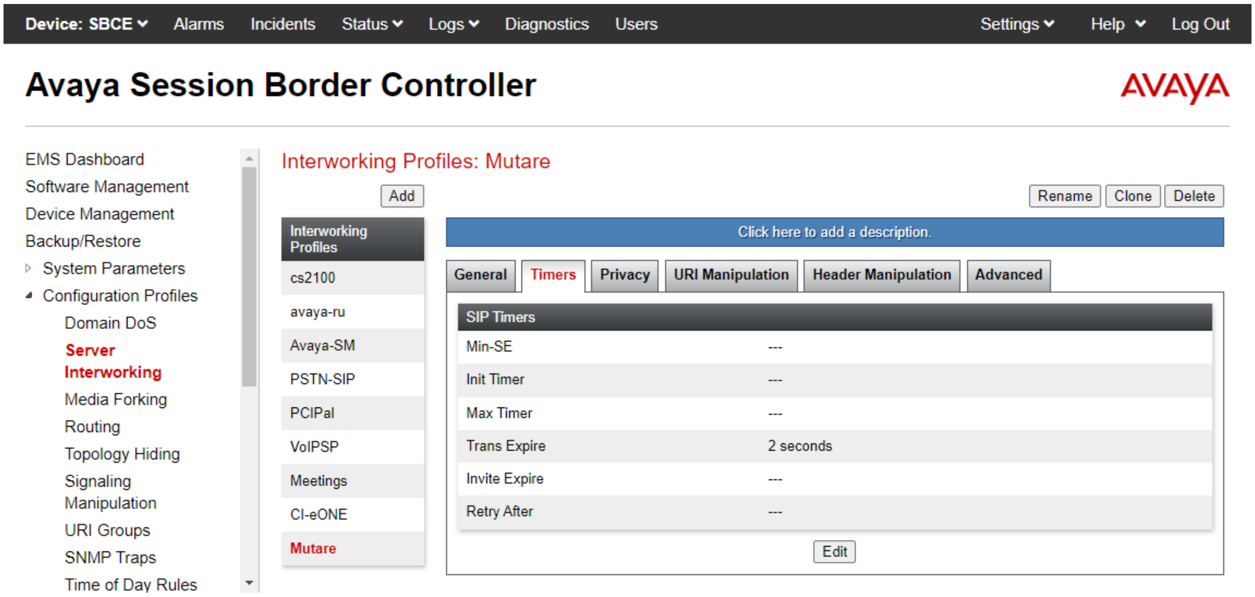


6.2.2. Server Interworking Profile for Voice Screening Proxy

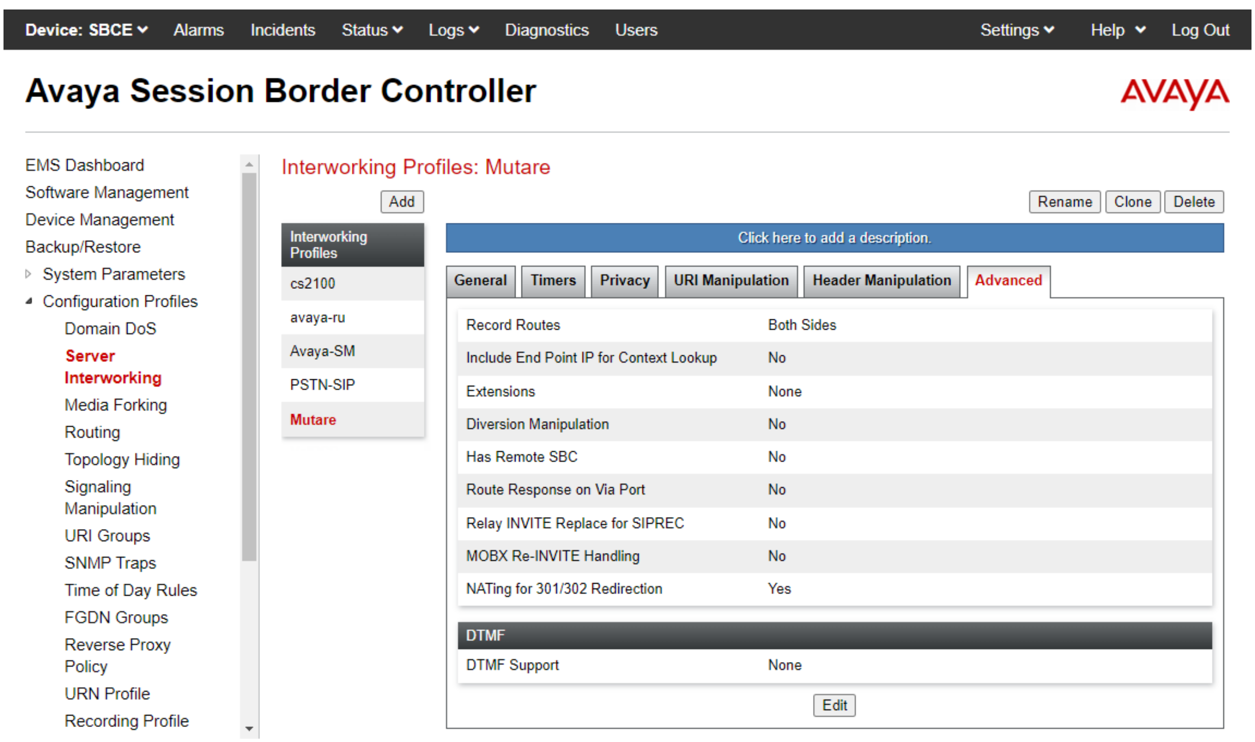
The Voice Screening Proxy profile was cloned from **avaya-ru** profile and then modified. The Server Interworking profile was named *Mutare*. The **General** tab shown below was configured with default settings.



Select the **Timers** tab and set **Trans Expire** to an appropriate short duration. In the compliance test, two seconds was used as the allotted time for SBC to wait for a route response from Voice Screening Proxy before routing to the secondary route (i.e., either Session Manager or the PSTN depending on call direction).



Select the **Advanced** tab and configure the fields as shown below.

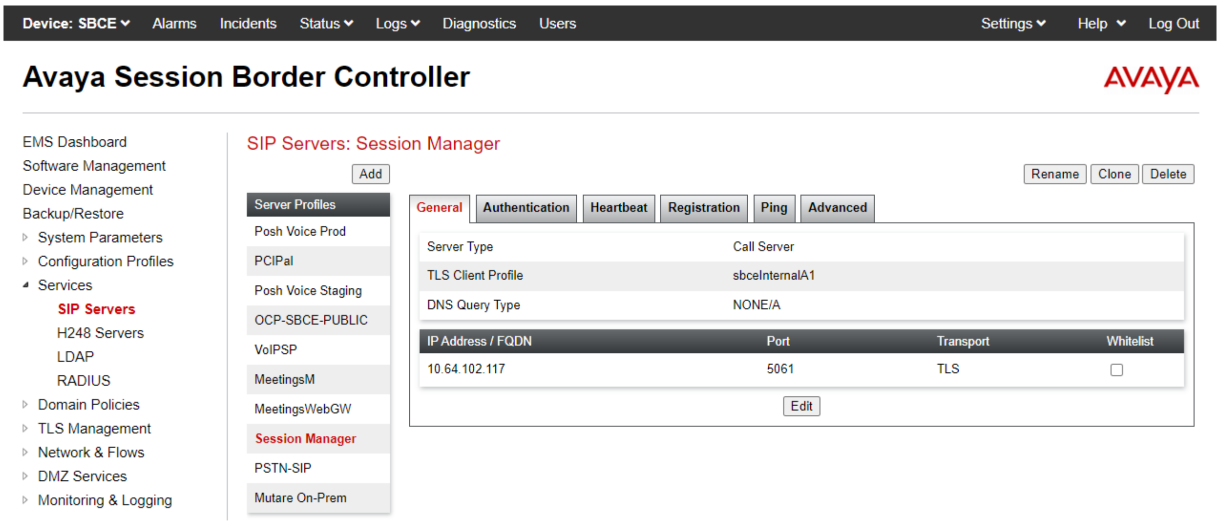


6.3. Administer SIP Servers

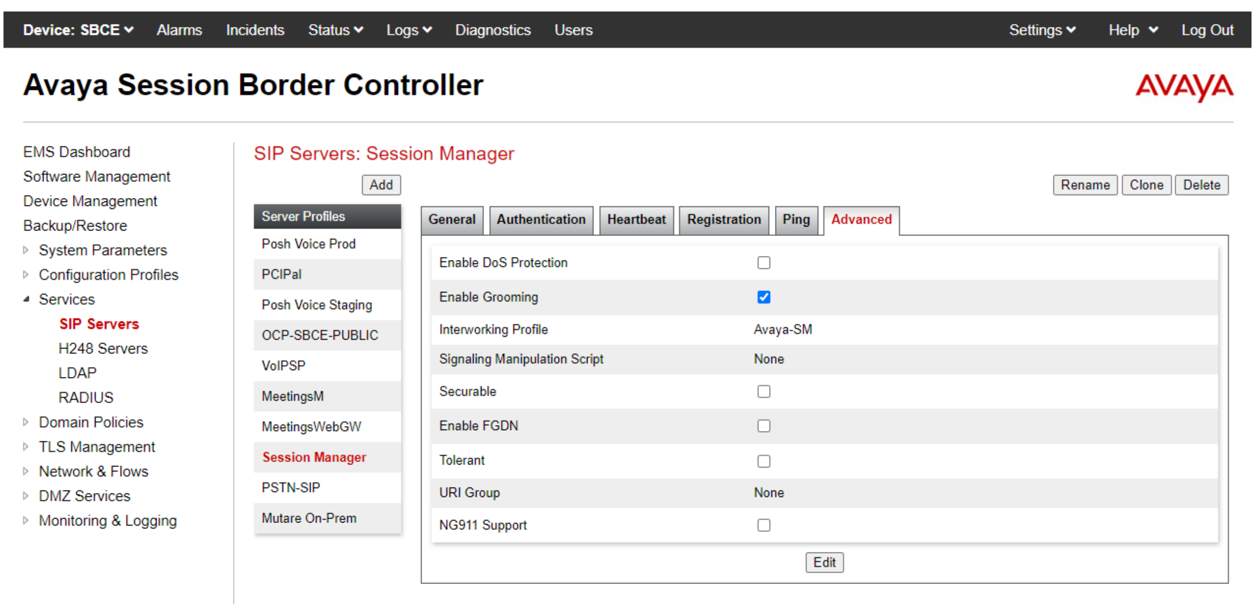
A **SIP Server** definition is required for each server connected to SBC. Add or modify a **SIP Server** for Session Manager and Voice Screening Proxy. TLS transport was used for the SIP trunk to Session Manager and Voice Screening Proxy.

6.3.1. SIP Server for Session Manager

To define a SIP server, navigate to **Services → SIP Servers** from the left pane to display the existing SIP server profiles. Click **Add** to create a new SIP Server or select a pre-configured SIP server to view its settings. The **General** tab of the Session Manager SIP Server was configured as shown below. TLS transport was used for the Session Manager SIP trunk.

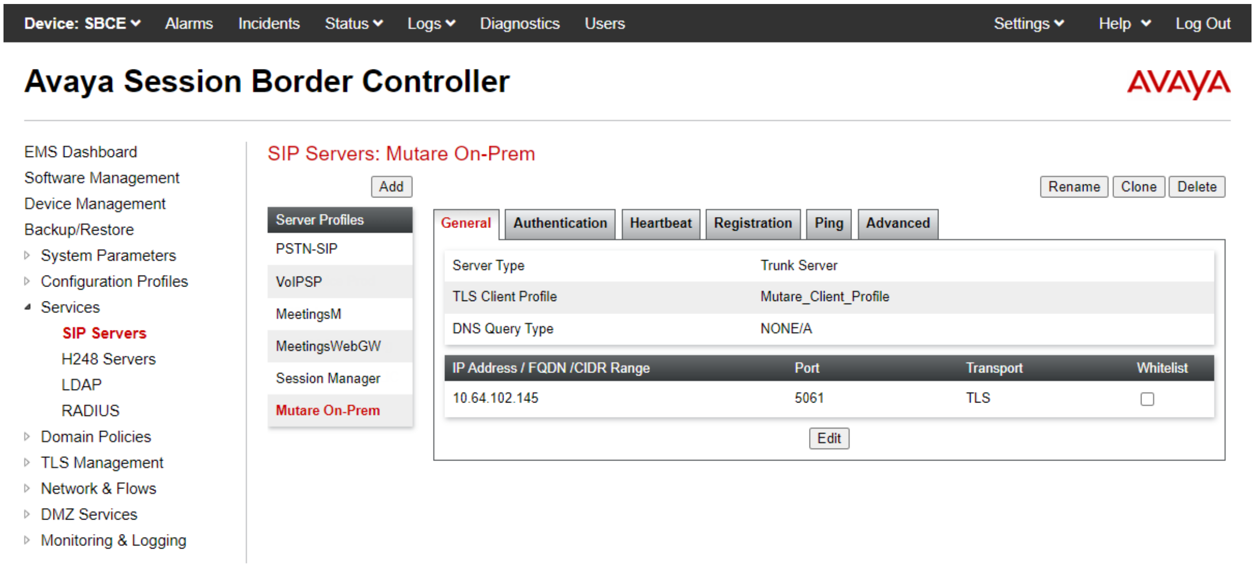


The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 6.2.1**. All other tabs were left with their default values.

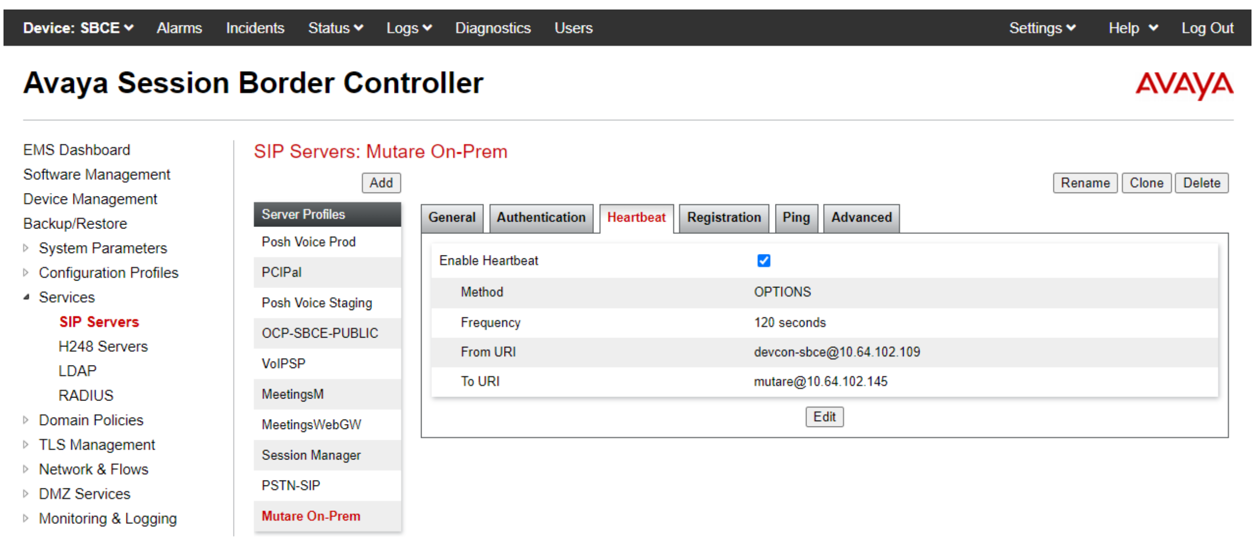


6.3.2. SIP Server for Voice Screening Proxy

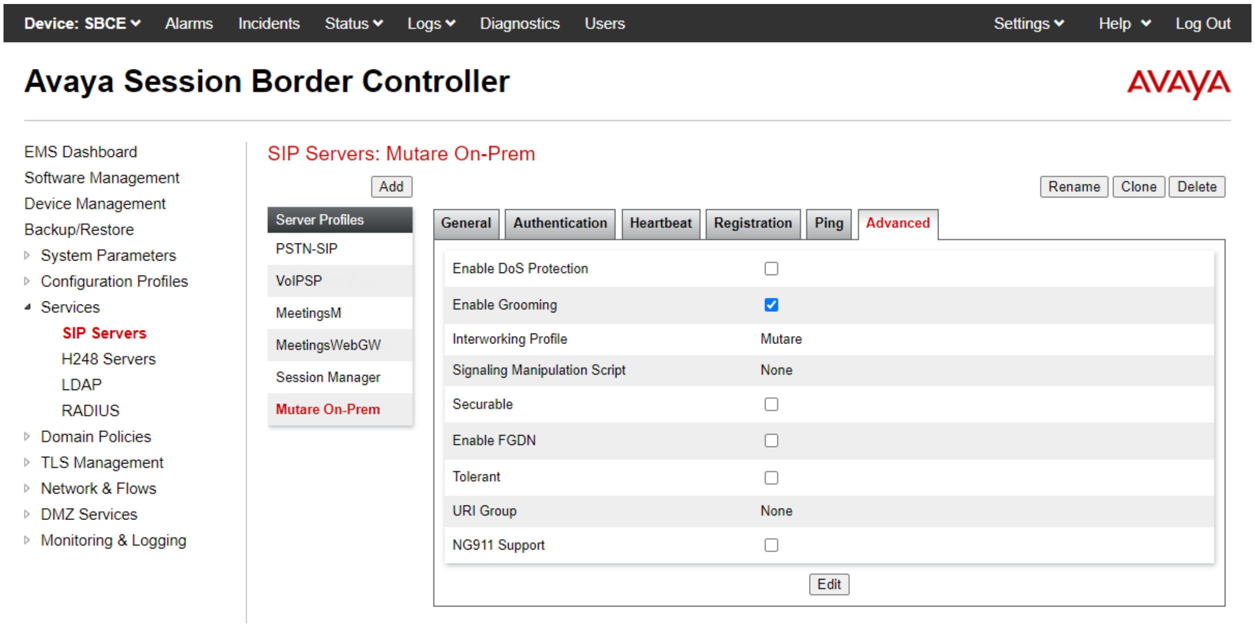
To define a SIP server, navigate to **Services → SIP Servers** from the left pane to display the existing SIP server profiles. Click **Add** to create a new SIP Server. The **General** tab of the Voice Screening Proxy SIP Server was configured shown below. TLS transport was used for the SIP trunk. Set **TLS Client Profile**, which was configured in **Section 6.9**.



Select the **Heartbeat** tab and enable Heartbeats so SBC sends SIP OPTIONS to Voice Screening Proxy. Specify the frequency and appropriate URIs as shown below.



The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 6.2.2**. All other tabs were left with their default values.

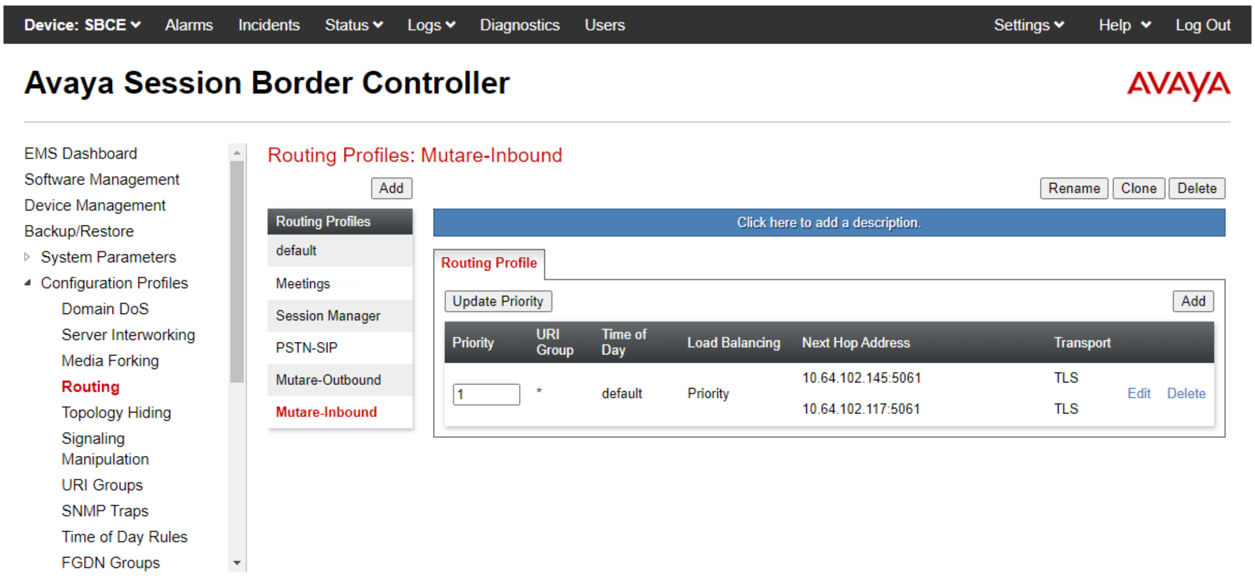


6.4. Administer Routing Profiles

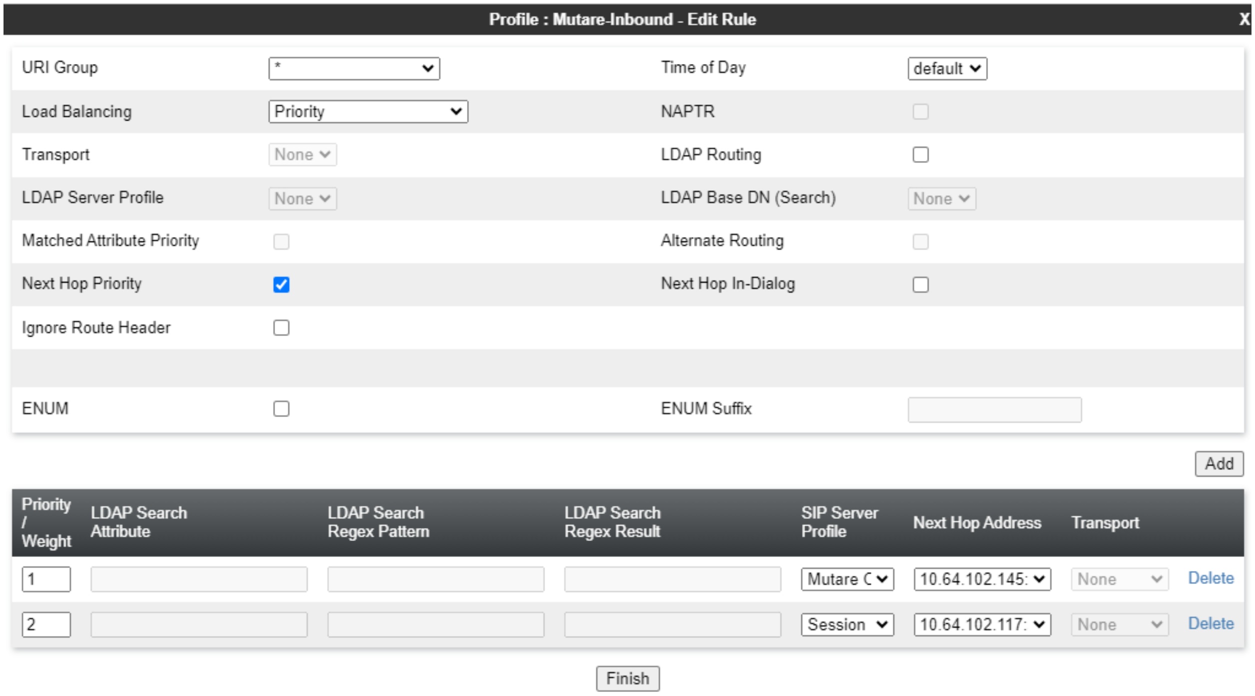
A **Routing Profile** is used to specify the next-hop for a SIP message. A routing profile is applied only after the traffic has matched a Server Flow defined in **Section 6.12**. Add routing profiles for inbound and outbound calls with a primary and secondary route. In each case, the primary route is Voice Screening Proxy and the secondary route is either Session Manager or the PSTN depending on call direction.

Select **Configuration Profiles → Routing** from the left pane to add two routing profiles for inbound and outbound calls, named *Mutare-Inbound* and *Mutare-Outbound*, respectively.

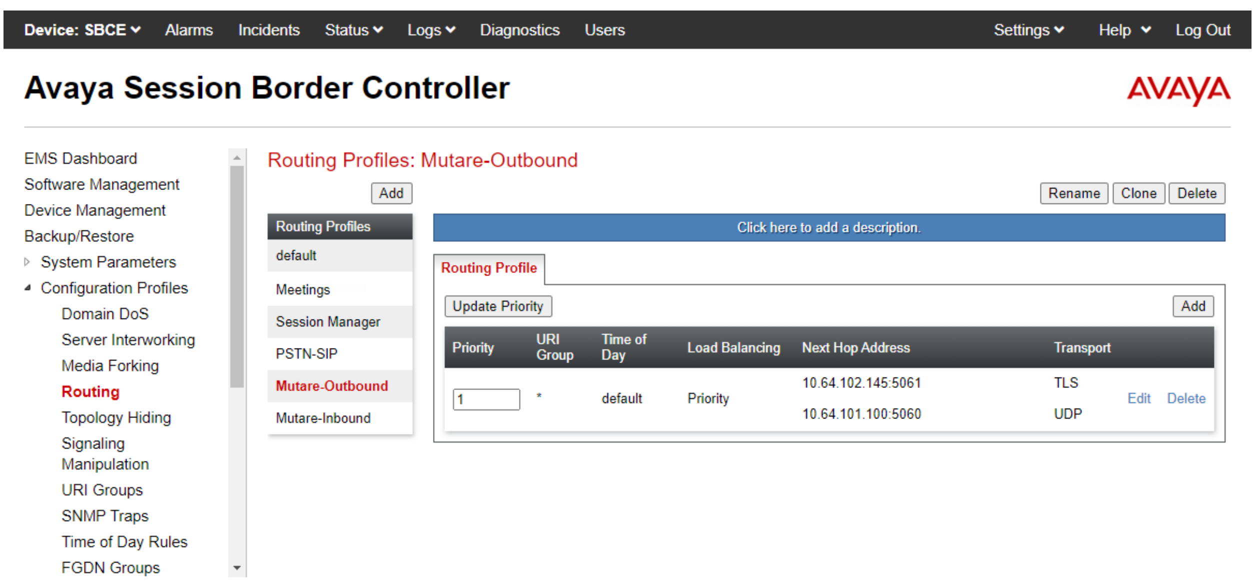
Mutare-Inbound is shown below, which routes calls to Voice Screening Proxy as the primary route, if available. Otherwise, the call is routed to Session Manager as the secondary route.



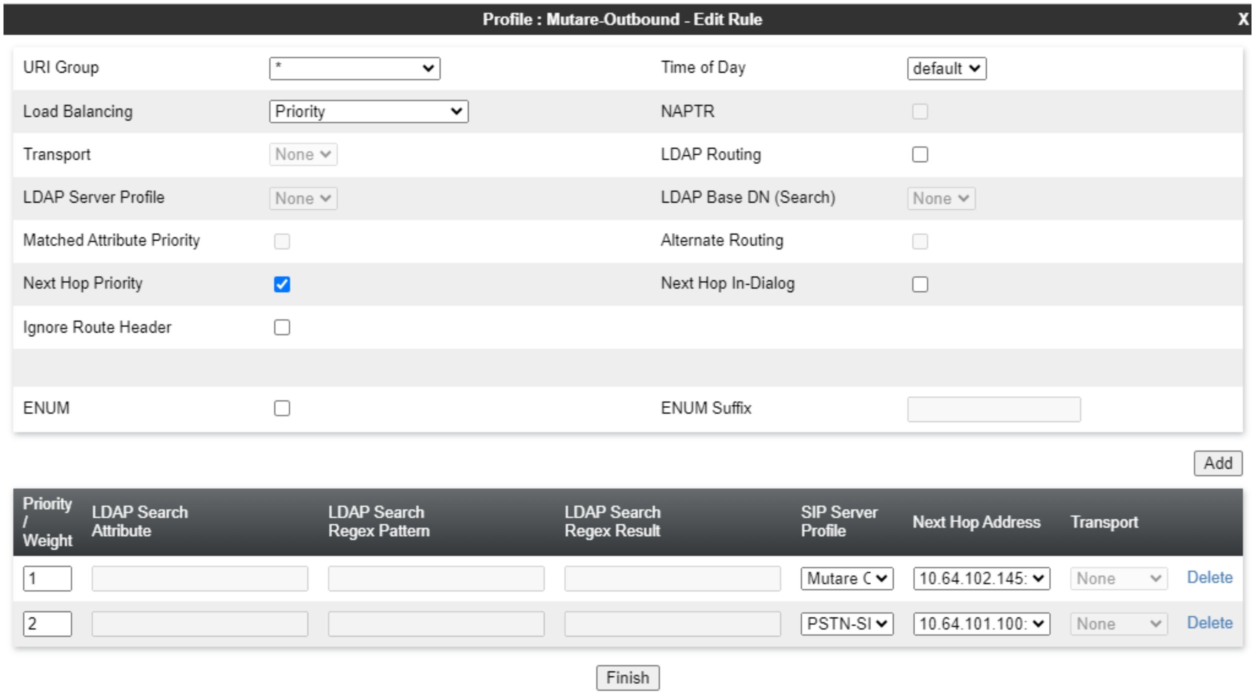
The details of the *Mutare-Inbound* routing profile are shown below.



Mutare-Outbound is shown below, which routes calls to Voice Screening Proxy as the primary route, if available. Otherwise, the call is routed to the PSTN as the secondary route.

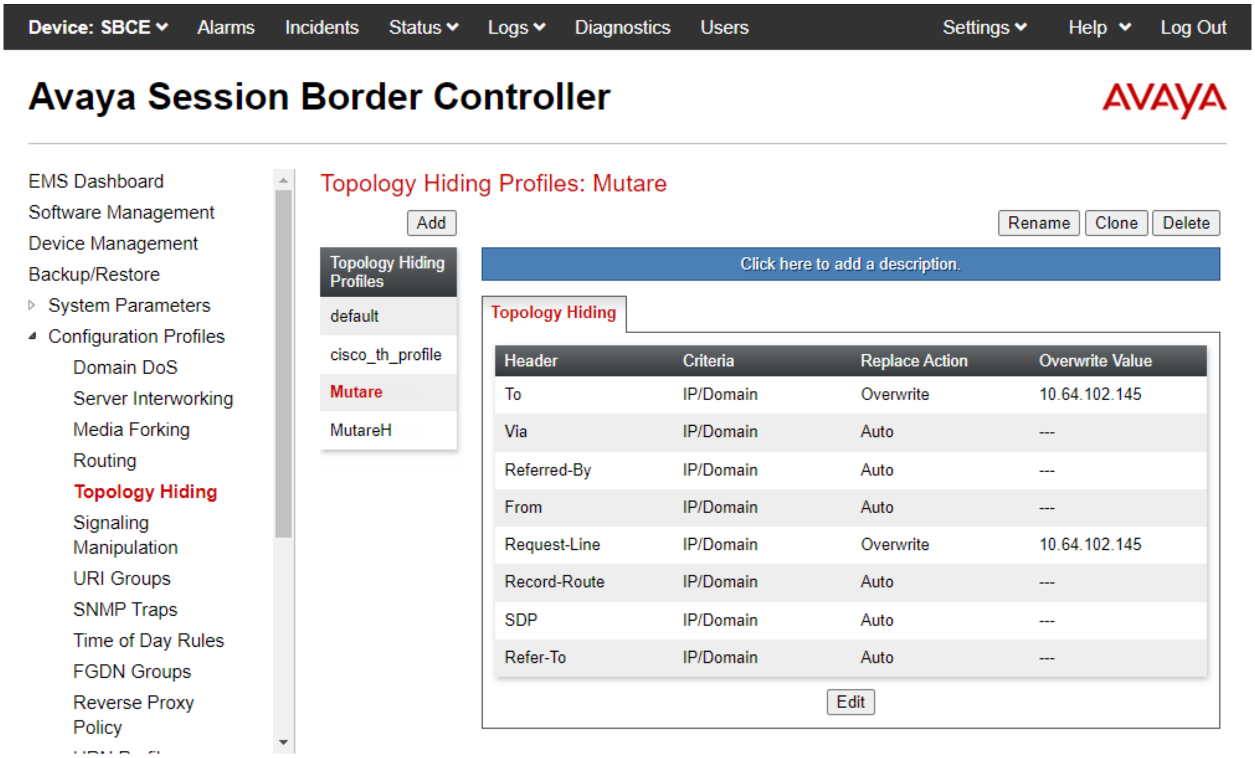


The details of the *Mutare-Outbound* routing profile are shown below.



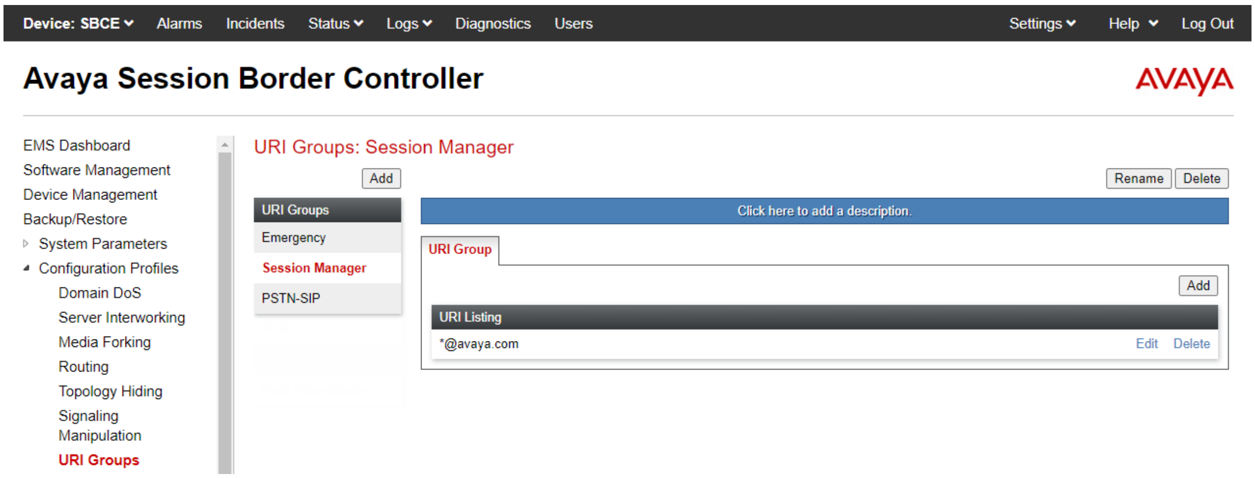
6.5. Administer Topology Hiding

Configure **Topology Hiding** to change the domain in the Request-URI and To header to the Voice Screening Proxy IP address. Navigate to **Configuration Profiles → Topology Hiding** to make the changes shown below.



6.6. Administer URI Groups

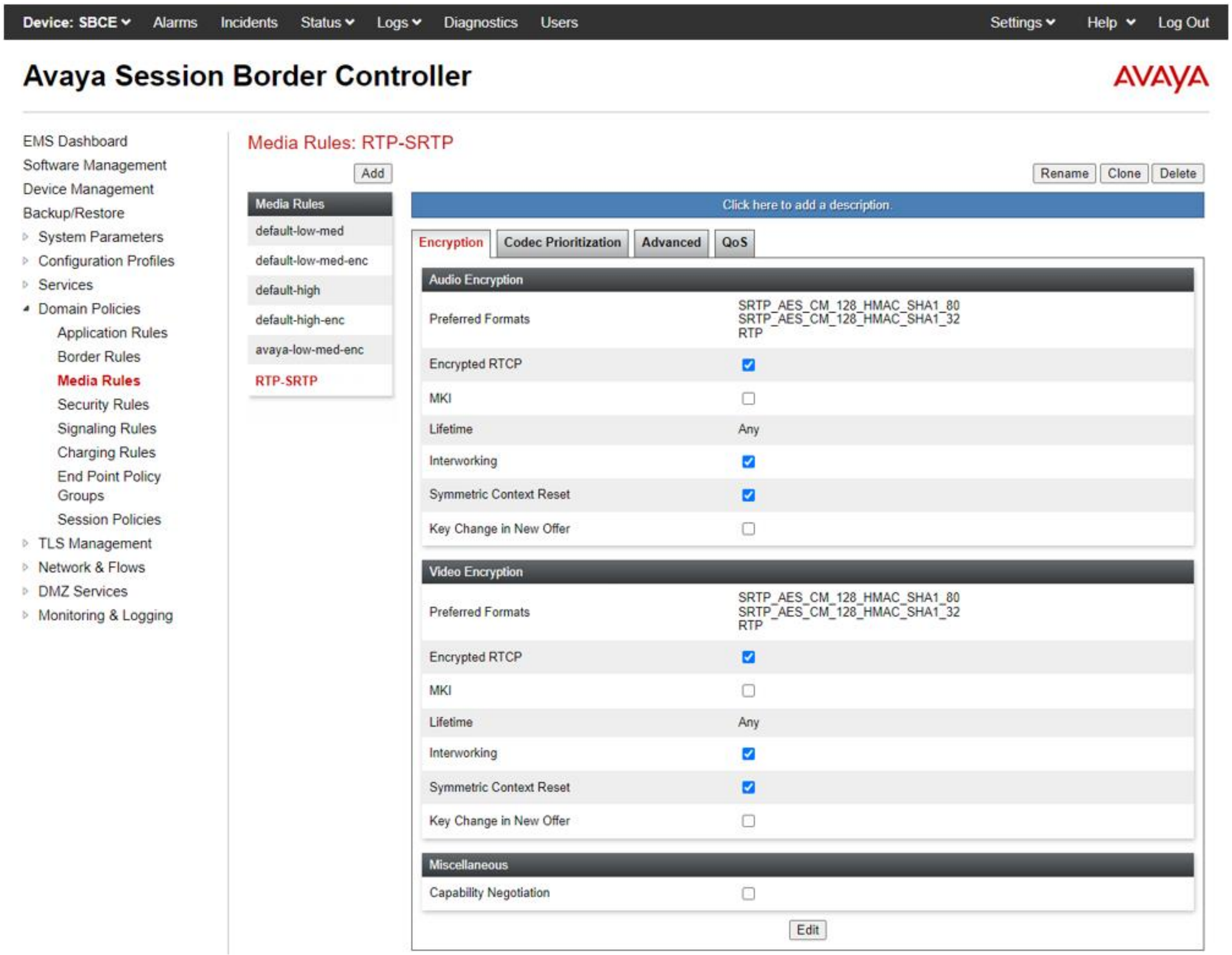
A **URI Group** is used to distinguish calls originated from the Avaya Aura® network to the PSTN (i.e., outbound calls). Navigate to **Configuration Profiles → URI Groups** to add a URI group. The following URI group, named *Session Manager*, identifies calls arriving from Session Manager, designated with *avaya.com* as the domain in the From header of the SIP INVITE. Inbound calls from the PSTN would specify *devcon.com* as the domain in the From header of the SIP INVITE. By applying this URI group to a server flow in **Section 6.12**, SBC examines the domain in the From header to determine if the server flow is a match.



6.7. Administer Media Rules

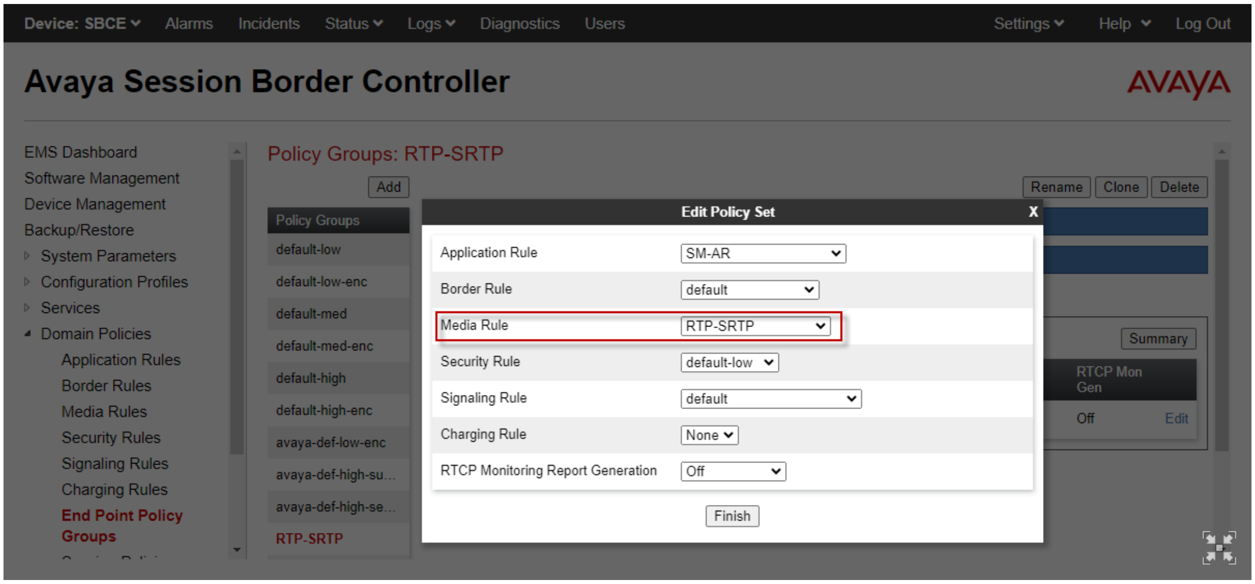
A **Media Rule** defines RTP media packet parameters, such as the packet encryption techniques to use for a call. In the compliance test, a **Media Rule** named *RTP-SRTP* was used for inbound and outbound calls, which allowed SRTP when using Voice CAPTCHA.

Navigate to **Domain Policies → Media Rules** and configure the media rule as shown below.



6.8. Administer End Point Policy

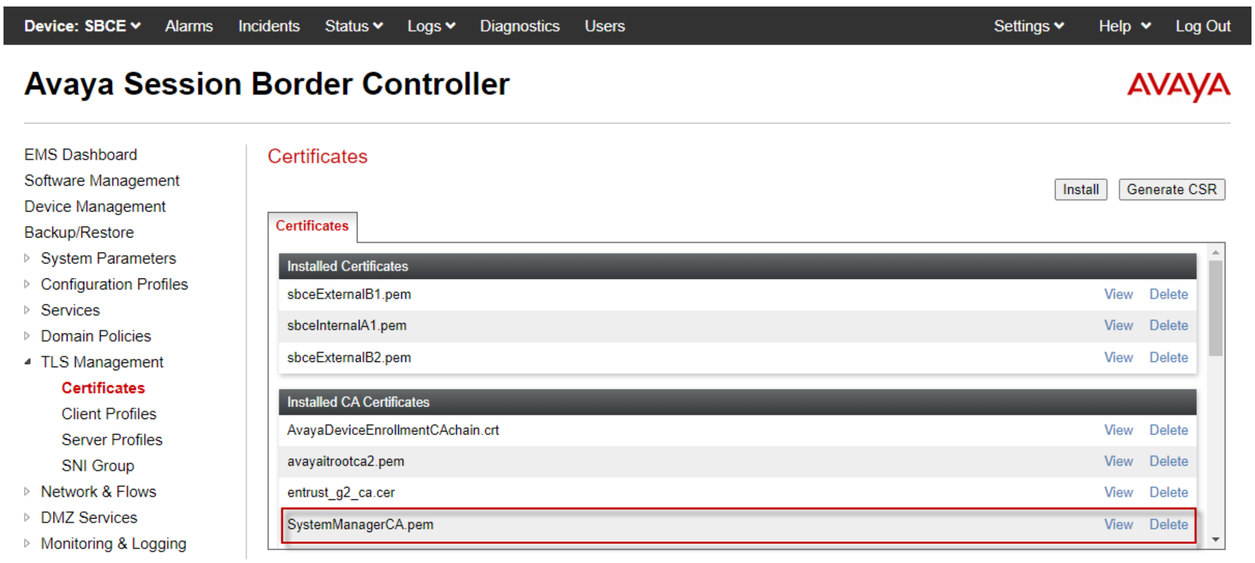
An **Endpoint Policy Group** is a set of policies that will be applied to traffic between the SBC and a connected server, such as Session Manager, Voice Screening Proxy, and the PSTN. The *RTP-SRTP* end point policy is shown below with the *Media Rule* set to the one configured above. This media rule was used for all calls.



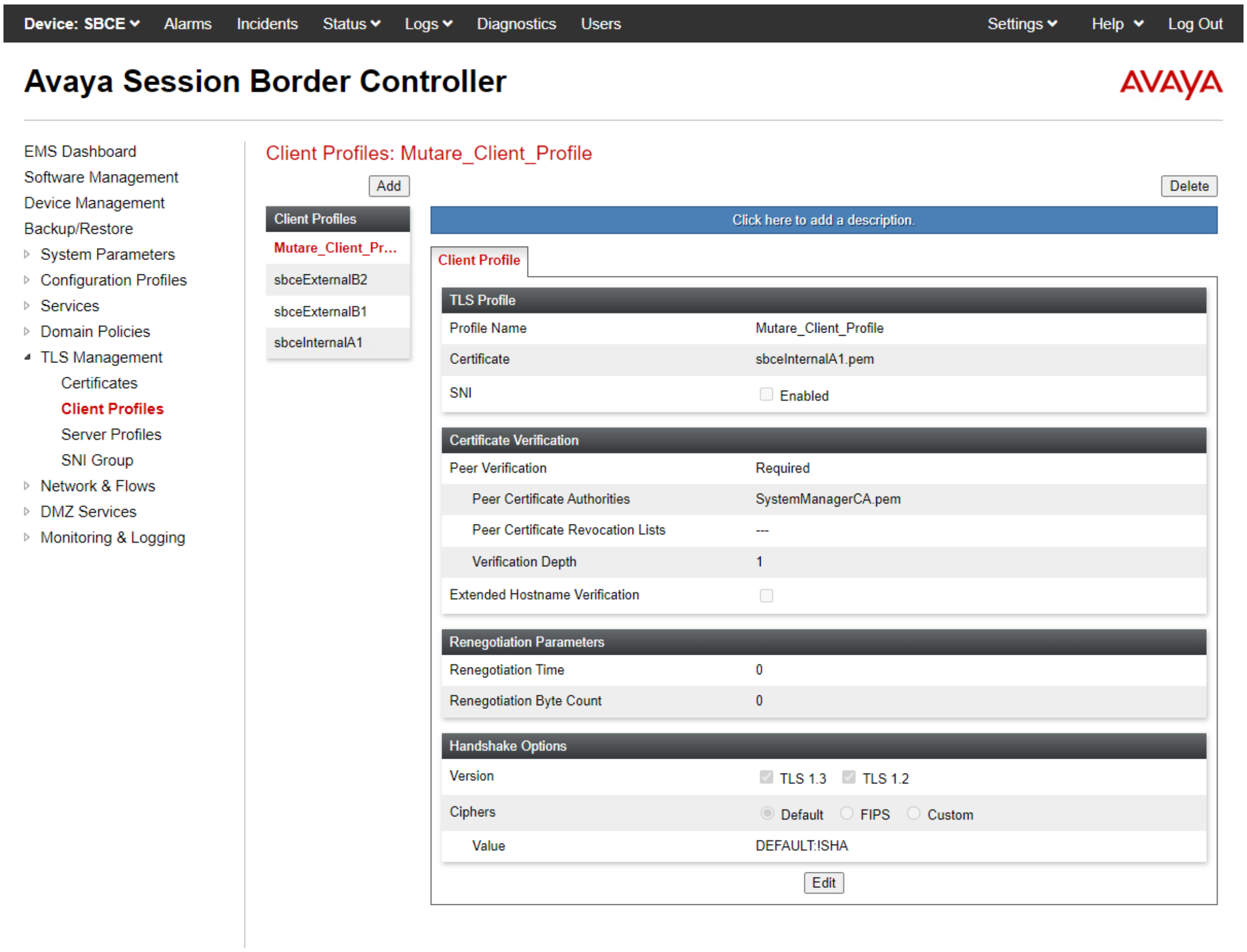
6.9. Administer TLS Management

This section covers TLS management, including importing the trusted CA certificate from System Manager, creating the TLS client profile for Voice Screening Proxy, and creating the TLS server profile for the internal SBC interface used by Voice Screening Proxy. In the compliance test, System Manager was used as the Certificate Authority (CA) and the trusted CA certificate was imported to Session Manager, SBC, and Voice Screening Proxy. In addition, System Manager, as the CA, created Identity certificates for the SBC interfaces, which were also imported (not shown).

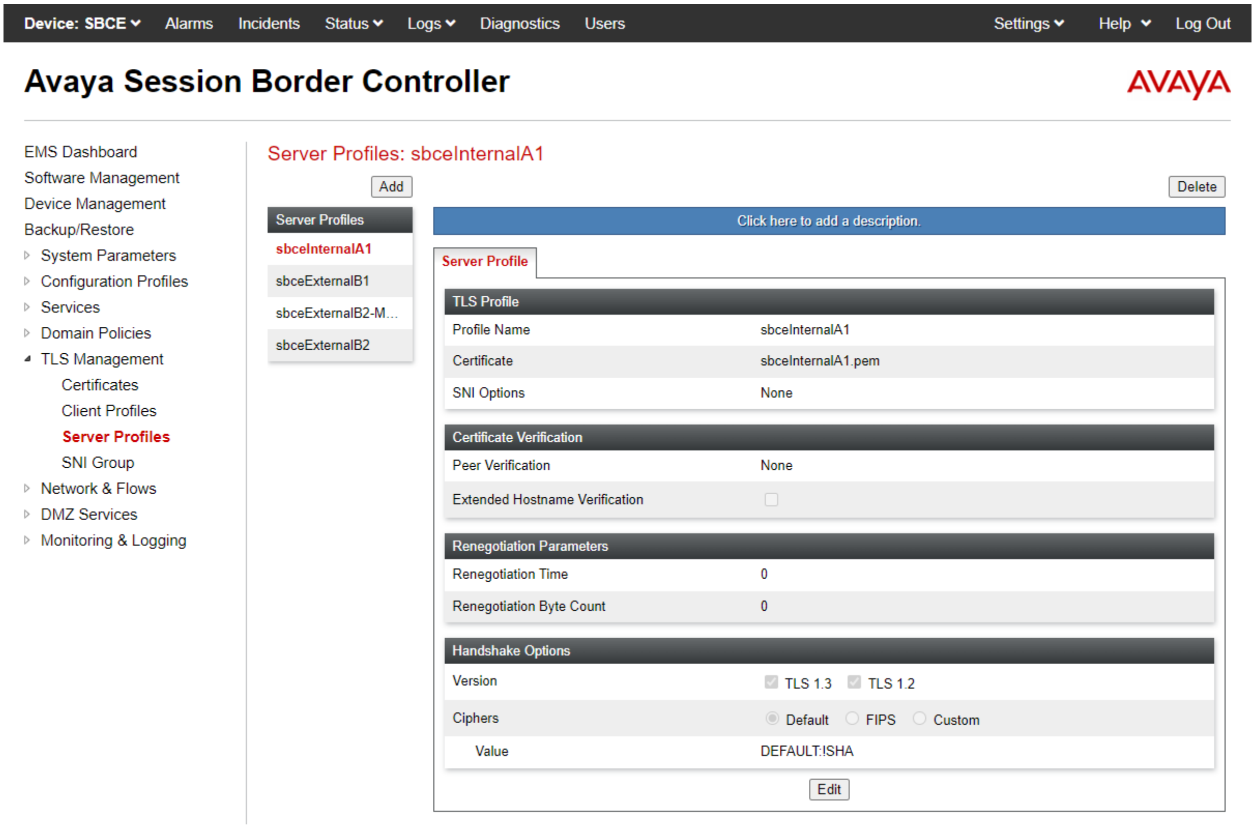
Navigate to **TLS Management → Certificates** and verify that the trusted CA certificate has been installed as shown below.



Navigate to **TLS Management → Client Profiles** and create a **Client Profile** for Voice Screening Proxy as shown below. Set **Certificate** to the identity certificate assigned to the internal SBC interface, which connects to Voice Screening Proxy. For **Peer Certificate Authorities**, select the trusted CA certificate (i.e., *SystemManagerCA.pem*) installed above. Set the **Verification Depth** to *1*. Default values for the remaining fields may be used.



The following **Server Profile** is assigned to the A1 internal interface covered in **Section 6.11**. Voice Screening Proxy connects to the SBC A1 interface.

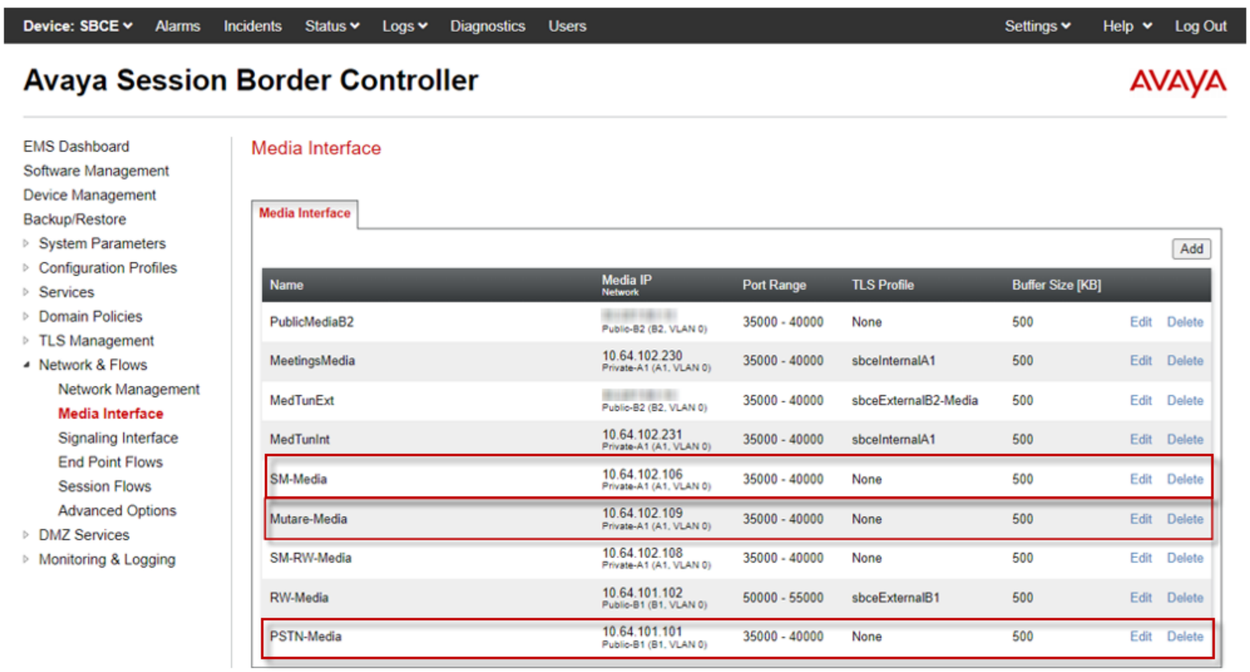


6.10. Administer Media Interfaces

A **Media Interface** defines an IP address and port range for transmitting media. Create a media interface for Voice Screening Proxy. In the compliance test, the media interface was named *Mutare-Media*.

Navigate to **Networks & Flows → Media Interface** to define a new Media Interface. In the compliance test, the following interfaces were defined. The media interfaces used for this solution are listed below.

- **SM-Media:** Media interface used by Session Manager to send and receive media.
- **Mutare-Media:** Media interface used by Voice CAPTCHA to send and receive media.
- **PSTN-Media:** Media interface used by PSTN to send and receive media.

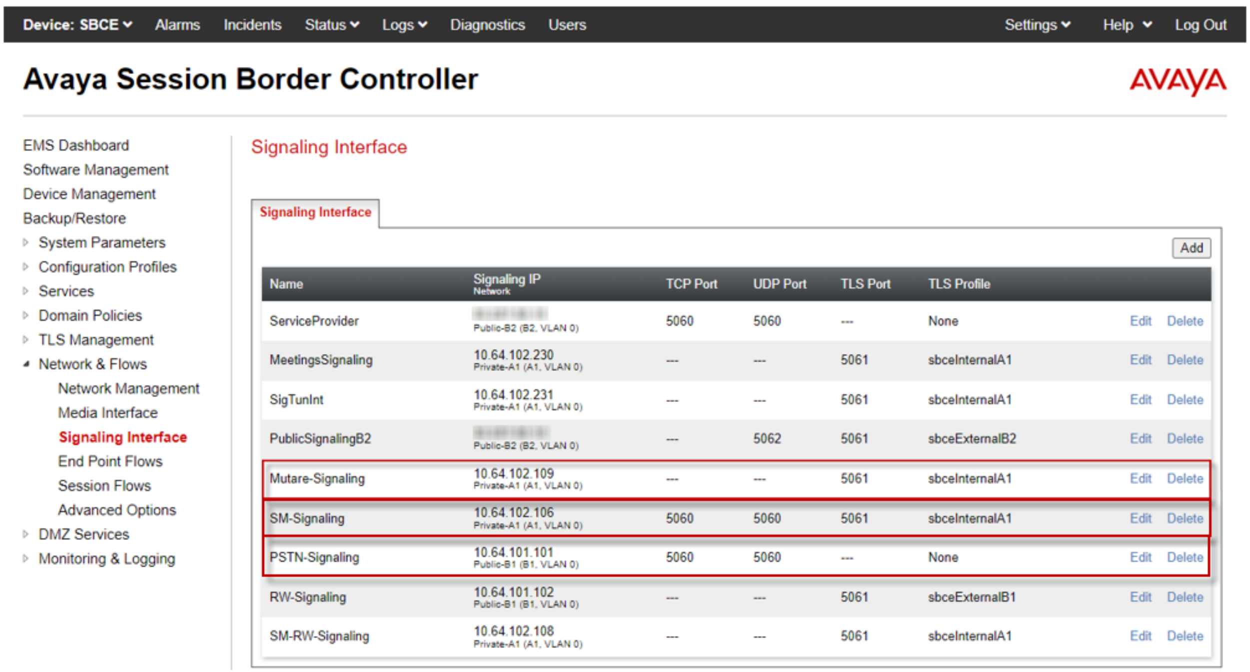


6.11. Administer Signaling Interfaces

A signaling interface defines an IP address, protocols and listen ports that SBC can use for signaling. Create a signaling interface for Voice Screening Proxy. In the compliance test, the signaling interface was named *Mutare-Signaling*.

Navigate to **Networks & Flows → Signaling Interface** to define a new **Signaling Interface**. In the Compliance Test the following interfaces were defined. For security reasons, public IP addresses have been redacted. The signaling interfaces used for this solution are listed below.

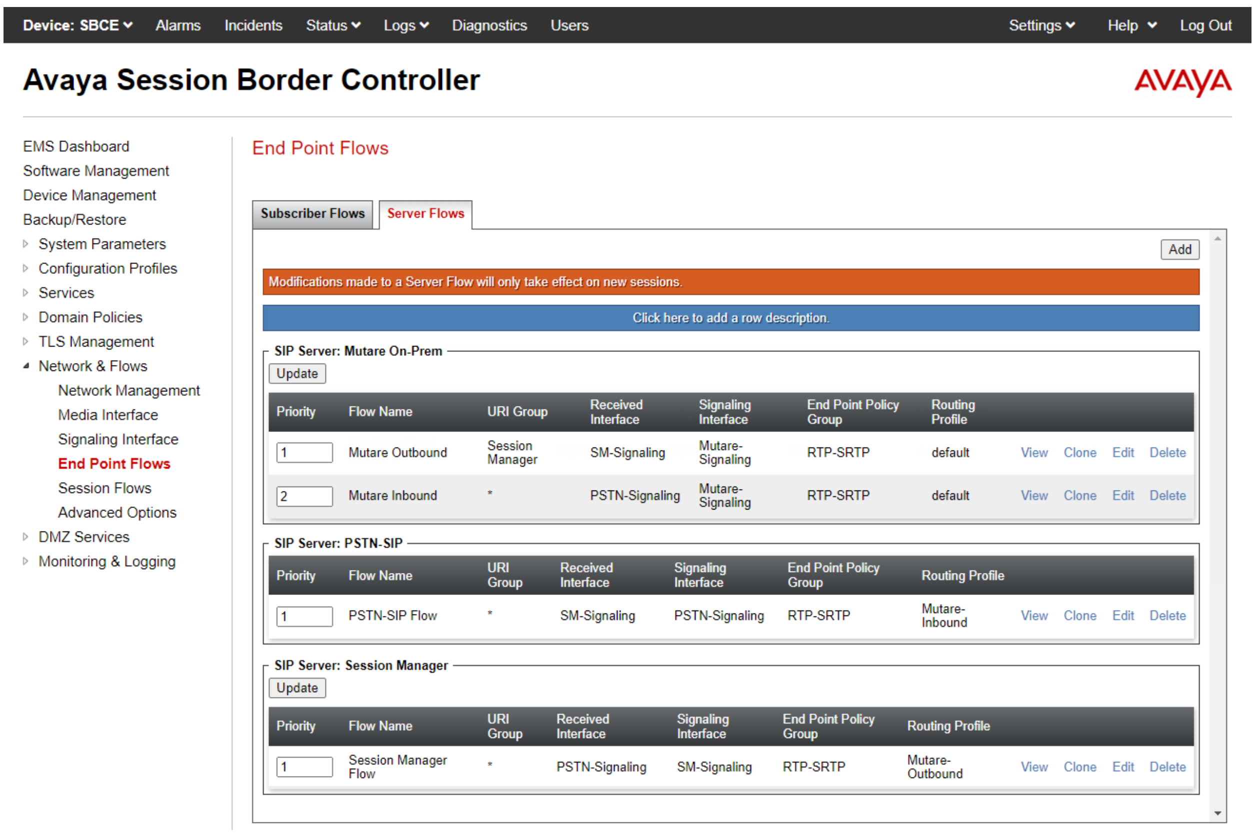
- **SM-Signaling:** Signaling interface used by Session Manager for SIP signaling.
- **Mutare-Signaling:** Signaling interface used by Voice Screening Proxy for SIP signaling.
- **PSTN-Signaling:** Signaling interface used by PSTN for SIP signaling.



6.12. Administer End Point Flows

Endpoint Flows are used to determine the endpoints (connected servers) involved in a call in order to apply the appropriate policies. When a packet arrives at SBC, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow matches. Once the flow is determined, the flow points to policies and profiles that control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the compliance test, the endpoints were Session Manager, Voice Screening Proxy, and the PSTN.

Navigate to **Network & Flows → End Point Flows → Server Flows** and select the **Server Flows** tab. The configured **Server Flows** used in the compliance test are shown below. The following subsections will review the settings for each server flow.



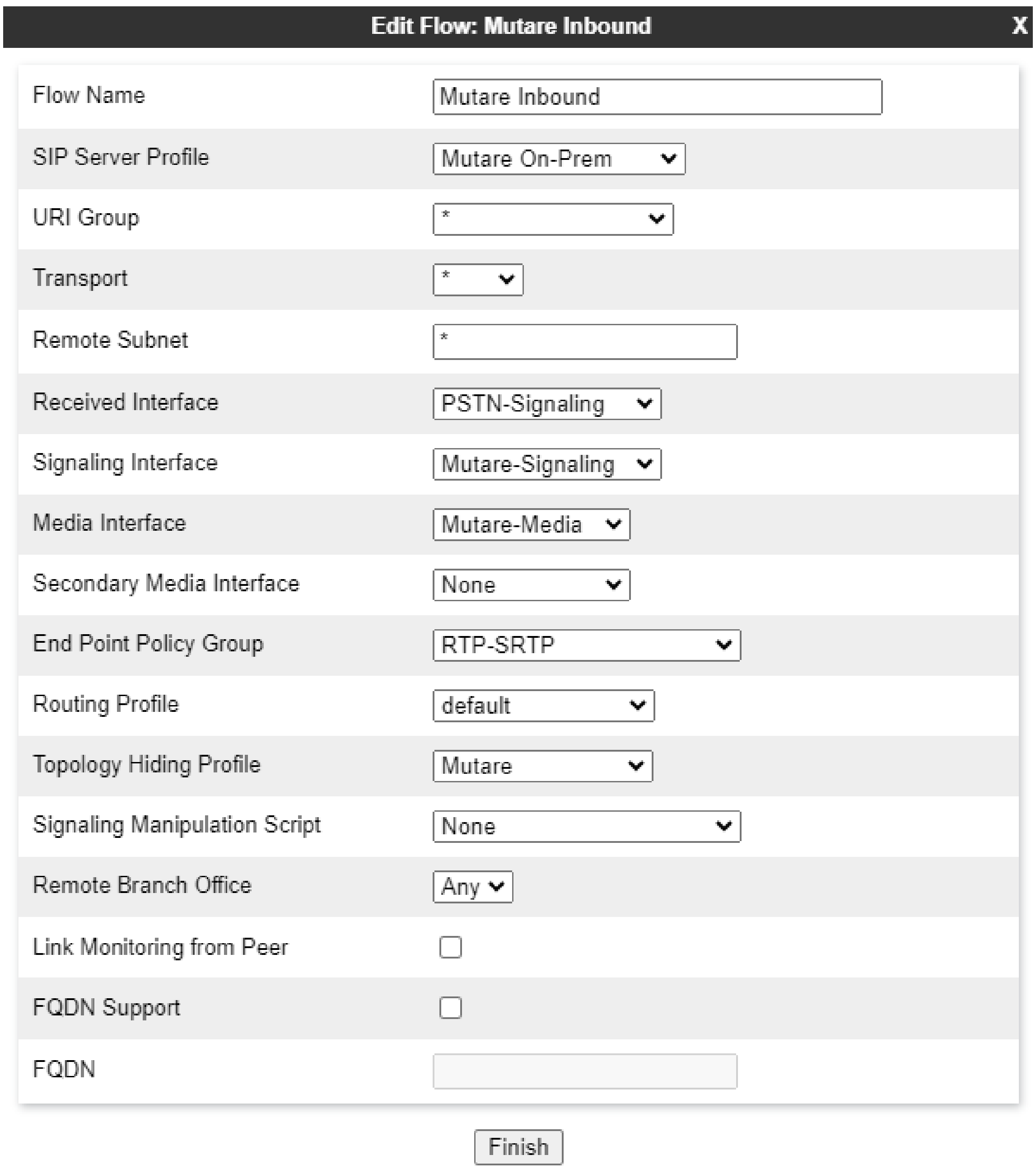
The following table shows how the server flows are used for inbound and outbound calls. The source and destination flows are processed before SBC sends a SIP message to Voice Screening Proxy.

Call Direction	**Source Flow**	**Destination Flow**	**Actions**
Inbound Call	PSTN-SIP Flow	Mutare Inbound	1. SBC sends SIP INVITE to Voice Screening Proxy. 2. Voice Screening Proxy forwards SIP INVITE to Session Manager for legitimate calls.
Outbound Call	Session Manager Flow	Mutare Outbound	1. SBC sends SIP INVITE to Voice Screening Proxy. 2. Voice Screening Proxy responds with 302 Moved Temporarily for legitimate calls. 3. SBC routes call to PSTN, the secondary route in the *Mutare-Outbound* routing profile.

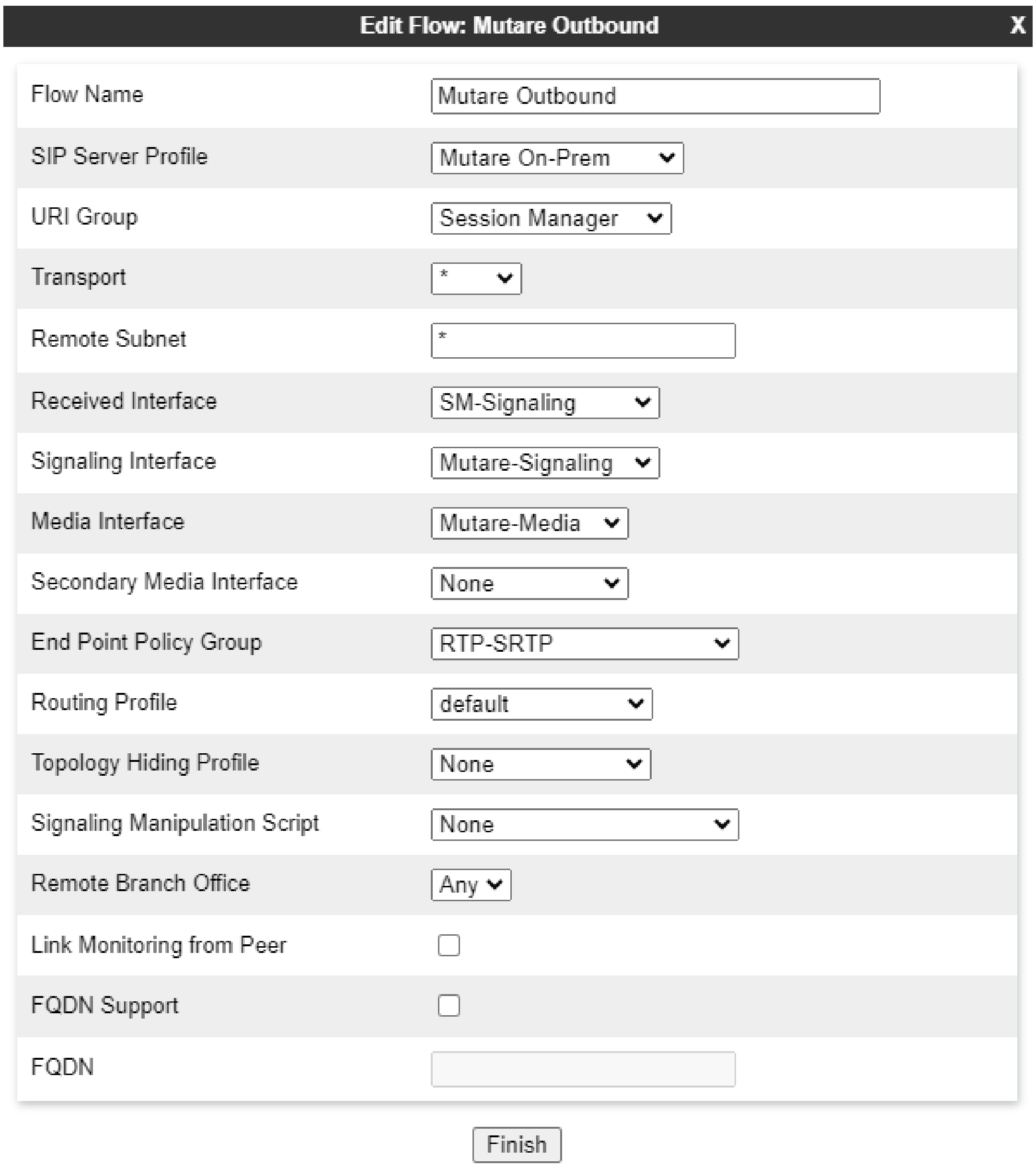
6.12.1. Server Flows for Voice Screening Proxy

In the compliance test, two server flows were created under Voice Screening Proxy for inbound and outbound calls.

For inbound PSTN calls, the *Mutare Inbound* server flow shown below is used as the destination flow when SBC receives a call from the PSTN, and then routes the call to Voice Screening Proxy as the primary route. If it is a legitimate call, Voice Screening Proxy will pass the call to Session Manager. The **Topology Hiding Profile** is used to change the domain in the Request-URI and To header to the Voice Screening Proxy IP address.

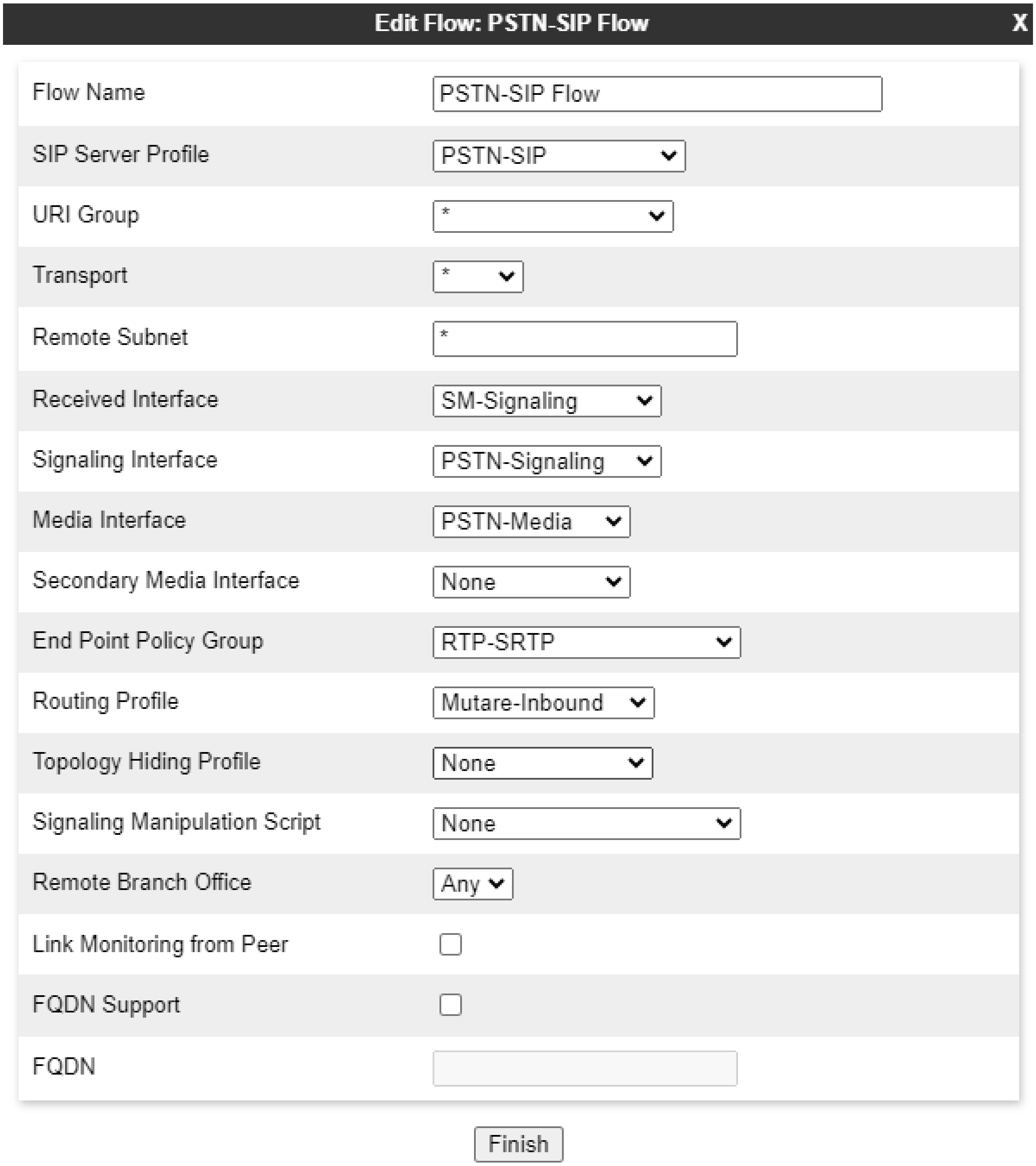


For outbound PSTN calls, the *Mutare Outbound* server flow shown below is used as the destination flow when SBC receives a call from Session Manager and then routes the call to Voice Screening Proxy as the primary route. If it is a legitimate call, Voice Screening Proxy will respond to SBC with a 302 Moved Temporarily with new Contact information. Since the 3xx response is handled by SBC, as configured in **Section 6.2.1**, SBC will re-route the call to the PSTN as the secondary route using the new Contact information. Since Voice Screening Proxy sends the PSTN domain (e.g., *devcon.com*) in the Contact information, this server flow will not match, because of the *Session Manager* URI group. The second server flow (*Mutare Inbound*) will not match either, because of the Received Interface mismatch. The call had arrived on the *SM-Signaling* interface. Therefore, SBC will re-route the call using the next hop in the *Mutare-Outbound* routing profile specified under Session Manager server flows, which is the PSTN.



6.12.2. Server Flows for PSTN

Inbound PSTN calls will match *PSTN-SIP Flow* shown below as the source flow. The **Routing Profile**, *Mutare-Inbound*, will route the call to Voice Screening Proxy as the primary route. The secondary route to Session Manager will only be used if Voice Screening Proxy is not available.



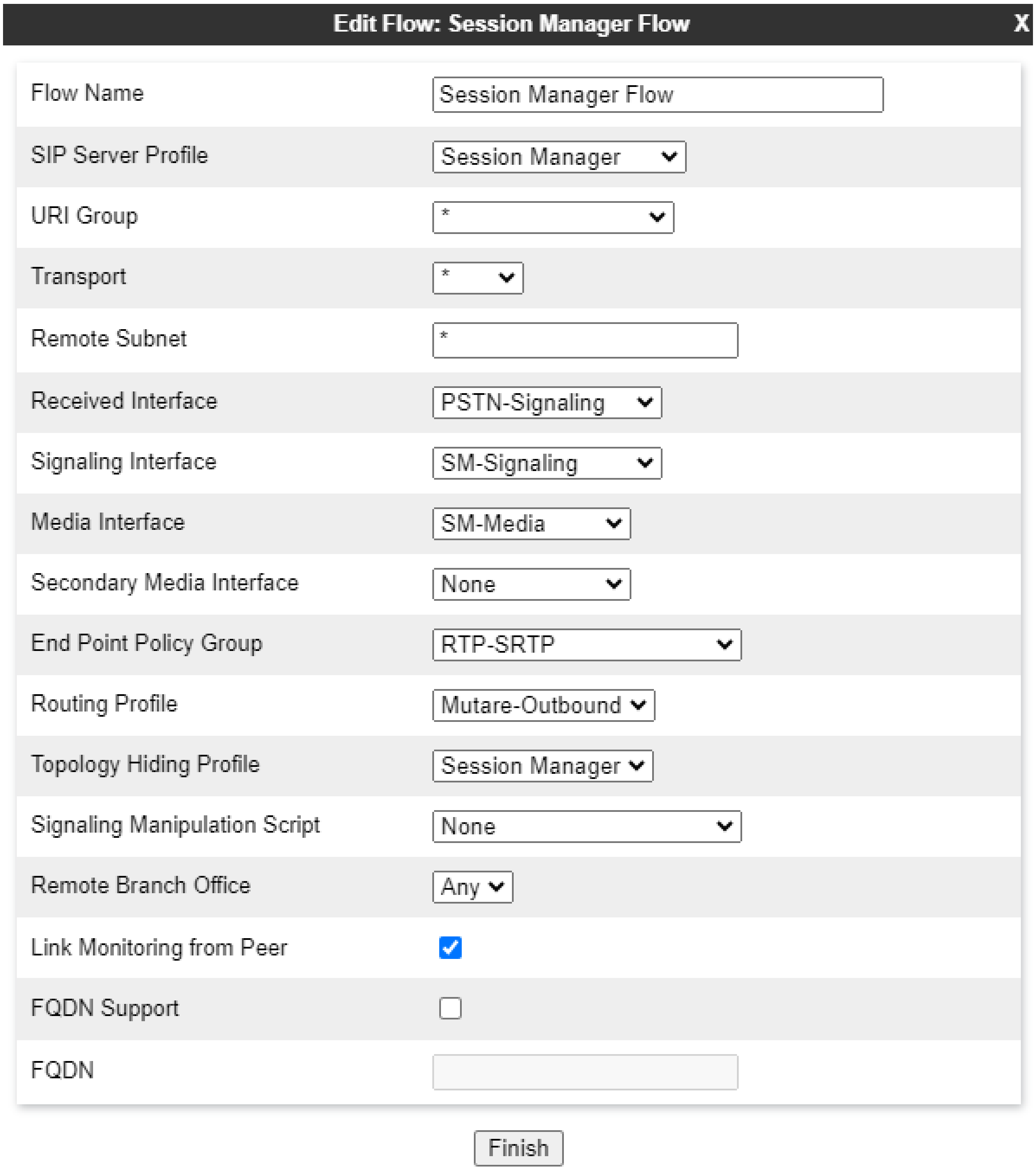
Edit Flow: PSTN-SIP Flow

Flow Name	PSTN-SIP Flow
SIP Server Profile	PSTN-SIP
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	SM-Signaling
Signaling Interface	PSTN-Signaling
Media Interface	PSTN-Media
Secondary Media Interface	None
End Point Policy Group	RTP-SRTP
Routing Profile	Mutare-Inbound
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☐
FQDN Support	☐
FQDN	

Finish

6.12.3. Server Flows for Session Manager

Outbound PSTN calls will match *Session Manager Flow* shown below as the source flow. The **Routing Profile**, *Mutare-Outbound*, will route the call to Voice Screening Proxy as the primary route. The secondary route to PSTN will be used if Voice Screening Proxy responds with a 302 Moved Temporarily or if Voice Screening Proxy is not available.



7. Configure Mutare Voice Traffic Filter

This section provides the procedure for configuring Voice Traffic Filter. The procedure includes the following areas:

- Configure Voice Screening Proxy
    - Modify opensips.cfg
    - Administer SQL
    - Administer TLS Certificates
- Enable SRTP on Voice CAPTCHA
- Administer Control Panel
- Administer Custom Rules

The configuration of Voice Traffic Filter is typically performed by Mutare operations technicians. The procedural steps are presented in these Application Notes for informational purposes. This section assumes that values for API URL, Connect URL, appliance ID, account ID, and token have all been obtained from Rules Engine Application Server and configured on Voice Screening Proxy.

7.1. Configure Voice Screening Proxy

This section covers the Voice Screening Proxy configuration.

7.1.1. Modify opensips.cfg

Modify the **opensips.cfg** file located on Voice Screening Proxy Server in the **/etc/opensips** directory. This requires logging in with super user credentials. The **opensips.cfg** file should be changed as follows:

- Configure the Voice Screening Proxy IP address and enable TLS.
- Configure the Voice CAPTCHA IP address.
- Specify the location of the TLS certificates.
- Make changes to the routing logic, including:
    - Remove the Route header in the SIP ACK and BYE messages to Session Manager.
    - Identify outbound calls.
- When responding with 302 Moved Temporarily, specify the PSTN domain (e.g., *devcon.com*) in the Contact header.

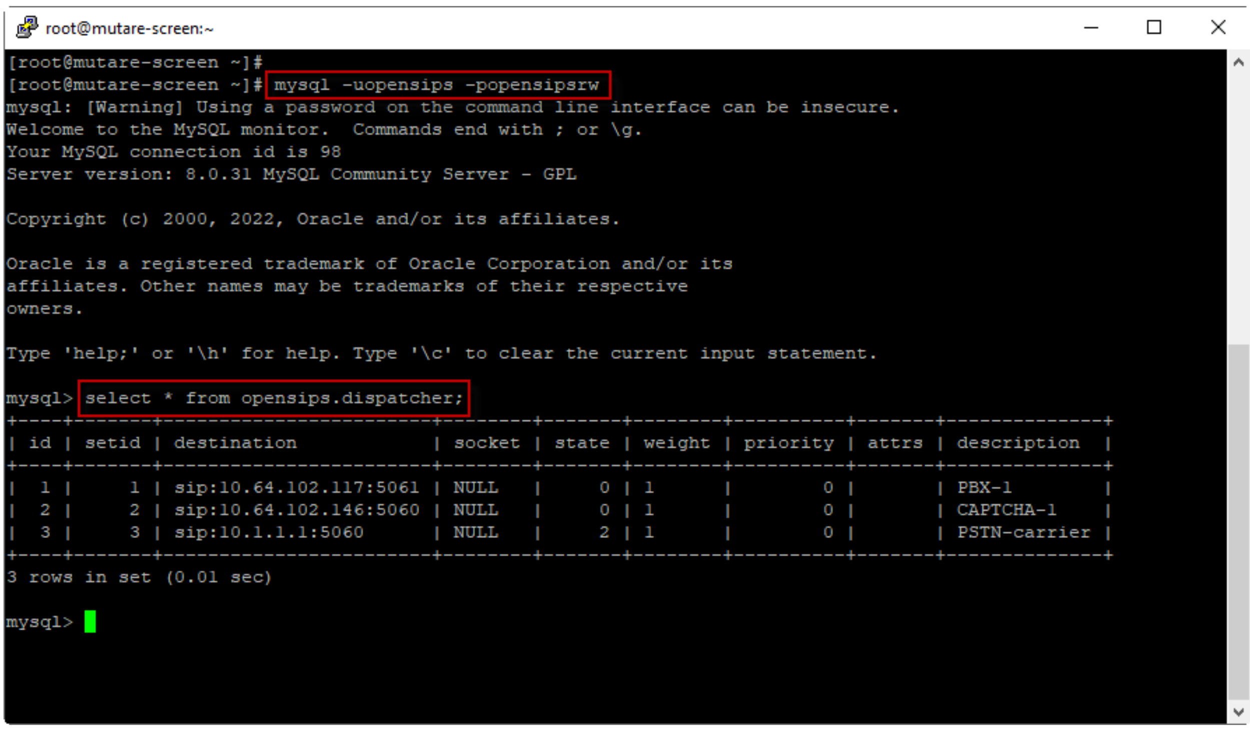
The **Appendix** provides excerpts of the **opensips.cfg** file that were changed to support the changes above in the compliance test.

7.1.2. Administer SQL

Log into the Voice Screening Proxy using super user credentials, and from the command line, enter the two SQL commands shown below to update the next hop destination to the IP address of the Session Manager signaling interface.

- `mysql -uopensips -popensipsrw`
- `UPDATE opensips.dispatcher set destination='sip:10.64.102.117:5061' where id=1;`

Enter the second SQL command below to ensure the TCP socket was set correctly.



```
root@mutare-screen:~
[root@mutare-screen ~]#
[root@mutare-screen ~]# mysql -uopensips -popensipsrw
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 98
Server version: 8.0.31 MySQL Community Server - GPL

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from opensips.dispatcher;
+----+-------+------------------------+--------+-------+--------+----------+-------+--------------+
| id | setid | destination            | socket | state | weight | priority | attrs | description  |
+----+-------+------------------------+--------+-------+--------+----------+-------+--------------+
|  1 |     1 | sip:10.64.102.117:5061 | NULL   |     0 | 1      |        0 |       | PBX-1        |
|  2 |     2 | sip:10.64.102.146:5060 | NULL   |     0 | 1      |        0 |       | CAPTCHA-1    |
|  3 |     3 | sip:10.1.1.1:5060      | NULL   |     2 | 1      |        0 |       | PSTN-carrier |
+----+-------+------------------------+--------+-------+--------+----------+-------+--------------+
3 rows in set (0.01 sec)

mysql>
```

7.1.3. Administer TLS Certificates

This section covers creating TLS certificates using Open SSL for Voice Screening Proxy. Voice Screening Proxy will generate a Certificate Signing Request (CSR) to be signed by the System Manager CA. Log into Voice Screening Proxy as root and following these steps:

1. Type the **cd /var/tmp** command to change directory.

2. Generate a CSR with the following command:

   openssl req -newkey rsa:2048 -keyout proxyprivatekey.key -out mutareproxy.csr
   Provide a passphrase: **1234**

3. Remove the passphrase from private key with the following command:

   openssl rsa -in proxyprivatekey.key -out proxykey.key
   Enter the passphrase: **1234**

   The output file should now be unencrypted. To verify, open the file with a text editor.

4. Transfer **mutareproxy.csr** to System Manager CA and generate a signed certificate (e.g., **mutarescreen.pem**).

5. Transfer **mutarescreen.pem** and **SystemManagerCA.pem** certificates to the /var/tmp folder in the Voice Screening Proxy server.

6. Type **cd /etc/opensips/tls/user** to change directory.

7. Enter the following commands:

   cp /var/tmp/proxykey.key user-privkey.pem
   cp /var/tmp/mutarescreen.pem user-cert.pem
   cp /var/tmp/SystemManagerCA.pem user-calist.pem

8. Type **service opensips restart**.

7.2. Enable SRTP on Voice CAPTCHA

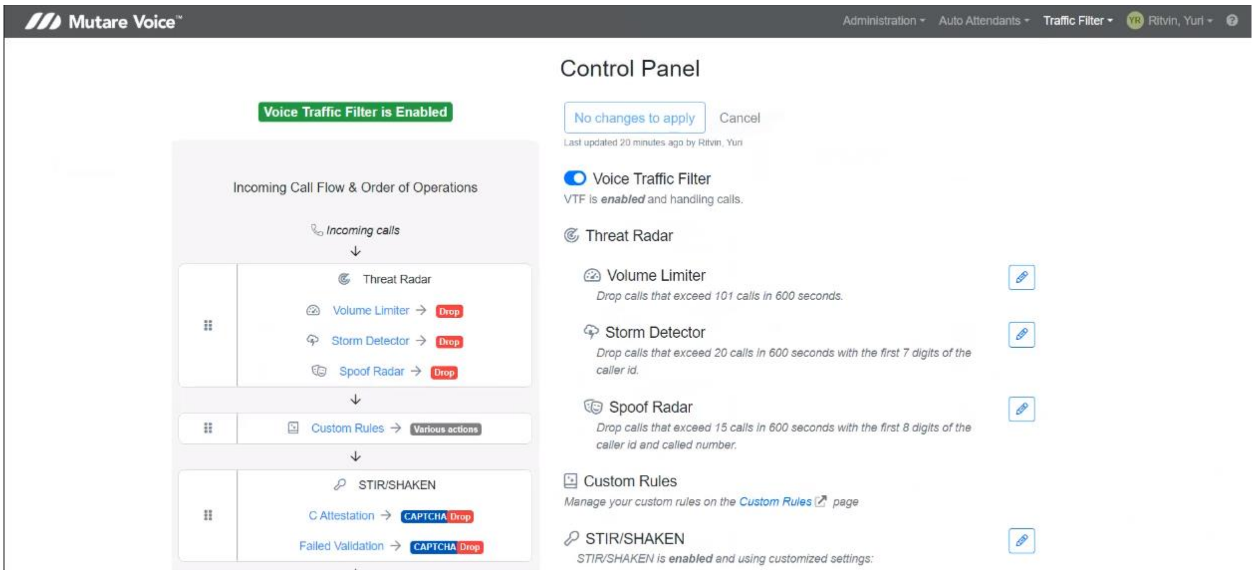
Log into Voice CAPTCHA as root and set the **rtp_secure_media** to *optional* in **/etc/freeswitch/vars.xml** with the following line. This allows Voice CAPTCHA to accept/offer SAVP/AVP with SAVP preferred.

```
<X-PRE-PROCESS cmd="set" data="rtp_secure_media=optional"/>
```

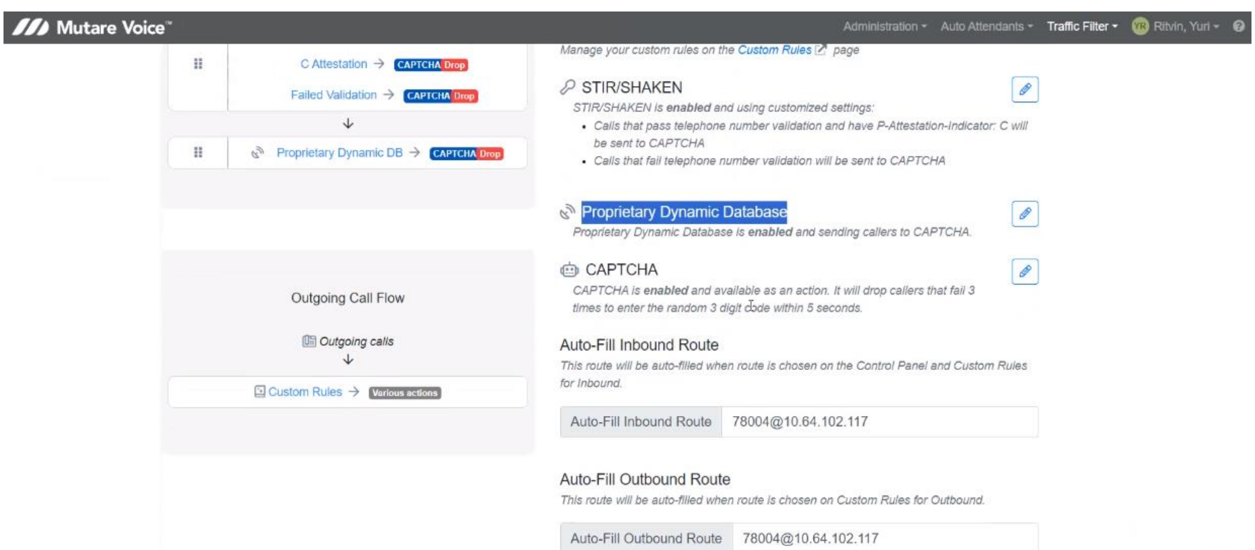
7.3. Administer Control Panel

Access the Mutare Voice web interface by using the URL **https://<*ip-address or FQDN*>** in an Internet browser window, where <*ip-address*> or <*FQDN*> is the IP address or FQDN of the Rules Engine Application Server. Log in with admin credentials (not shown).

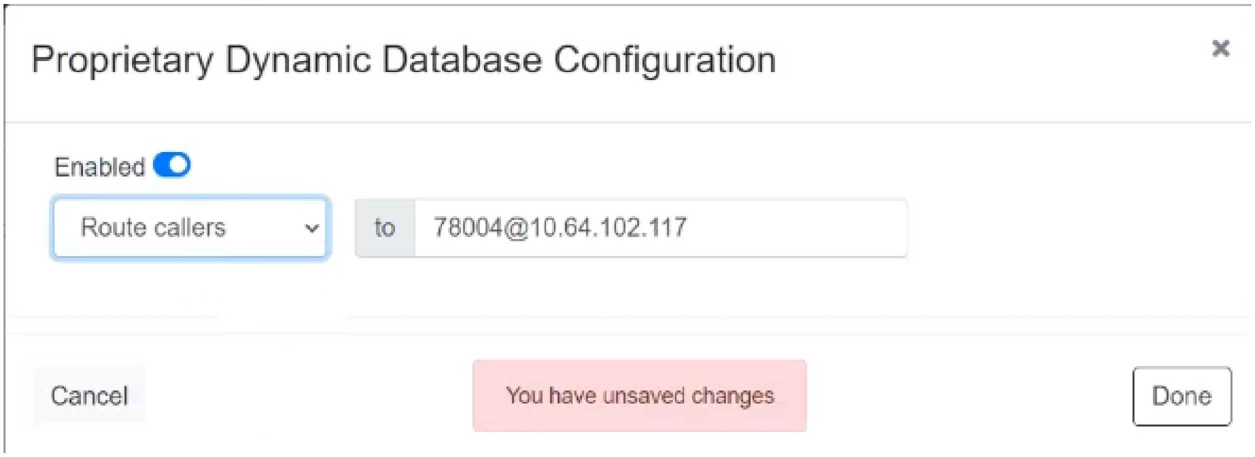
From the Mutare Voice web interface, select **Traffic Filter → Control Panel** from the top menu to display the screen below. Enable **Voice Traffic Filter** as shown below to allow calls to be analyzed by the traffic filter.



To allow Voice Traffic Filter to apply the dynamic robocall database to incoming calls, click the **Edit** button by **Proprietary Dynamic Database** shown below.



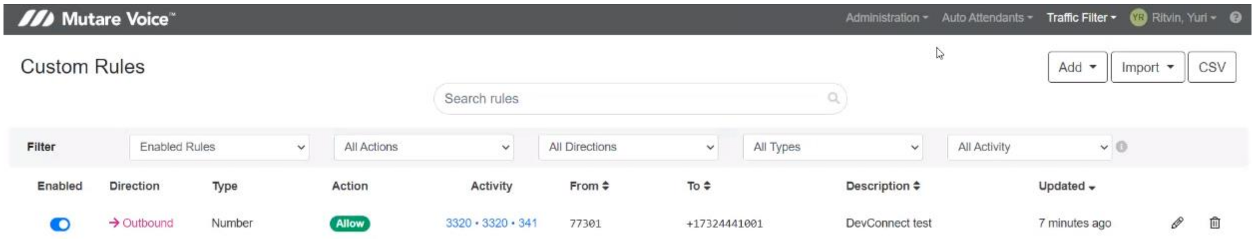
In **Proprietary Dynamic Database Configuration**, enable the rule and select an action. In the example below, spam calls are routed to extension 78004. Additional actions include dropping unwanted calls and prompting the caller for a security code as determined by Voice CAPTCHA.



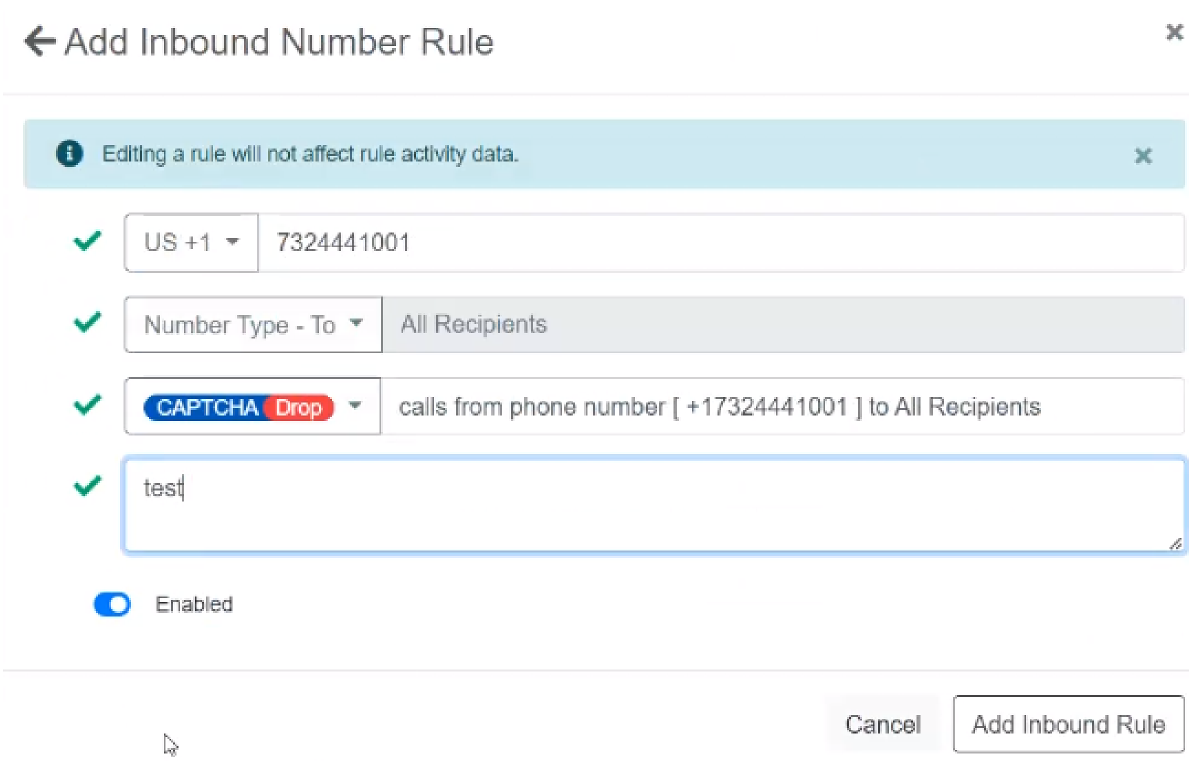
Scroll down to **CAPTCHA Configuration** section to enable Voice CAPTCHA as shown below. Actions, such as *Drop* and *Route* are allowed as shown below. This section also specifies other settings such as the number of digits and number of retries.

7.4. Administer Custom Rules

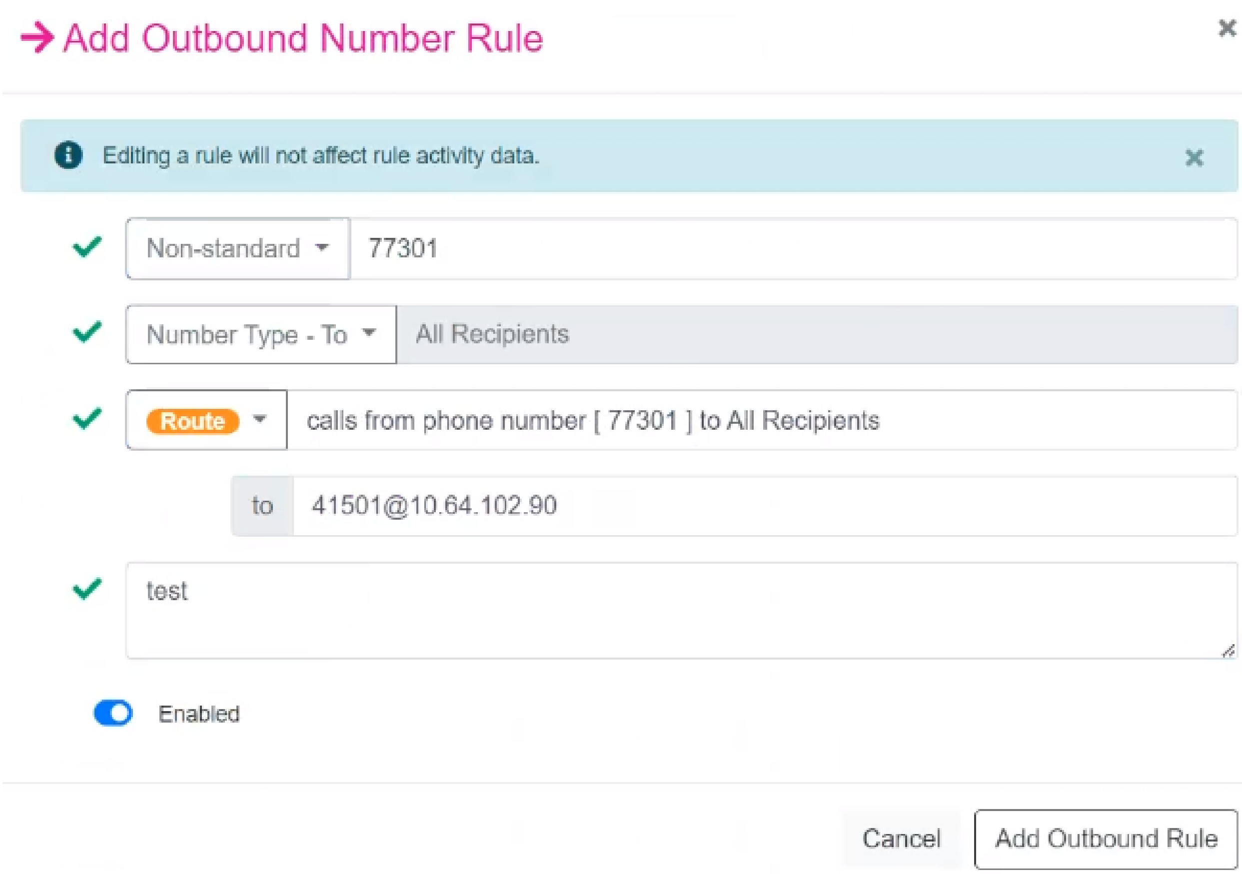
Select **Traffic Filter → Custom Rules** from the top menu to display the **Custom Rules** screen below. Click **Import** to import a CSV file with existing numbers or **Add** to add individual numbers. In the compliance testing, inbound or outbound number rules were selected from the **Add** drop-down.



The following example is an **Add Inbound Number Rule**. Set the number type to *US +1* followed by a 10-digit number. If the caller ID matches the specified 10-digit number, then this rule is applied. Next, specify the action to take if the caller ID matches the rule. The options are *Allow*, *Drop*, *Route*, *CAPTCHA Drop*, and *CAPTCHA Route*. In the following example, *CAPTCHA Drop* was selected, which means that the caller will be prompted for a CAPTCHA code. If the code is entered correctly, the inbound call is allowed to complete; otherwise, the call is dropped. Lastly, enter a description and then click *Add Inbound Rule*. Note that the Allow action is for the whitelist. These rules are applied before the dynamic robocall database, if enabled. That is, if a caller ID in on the whitelist and also in the robocall list, the call is allowed to complete.



The following example is an **Add Outbound Number Rule**. Set the number type to *Non-standard* followed by a 5-digit number. If the caller ID matches the specified 5-digit number, then this rule is applied. Next, specify the action to take if the caller ID matches the rule. In this example, *Route* was selected, which means that an unwanted call will be routed to the specified route-to number (i.e., *41501*). Lastly, enter a description and then click *Add Outbound Rule*. Note that the Allow action is for the whitelist. These rules are applied before the dynamic robocall database, if enabled. That is, if a caller ID in on the whitelist and also in the robocall list, the call is allowed to complete.



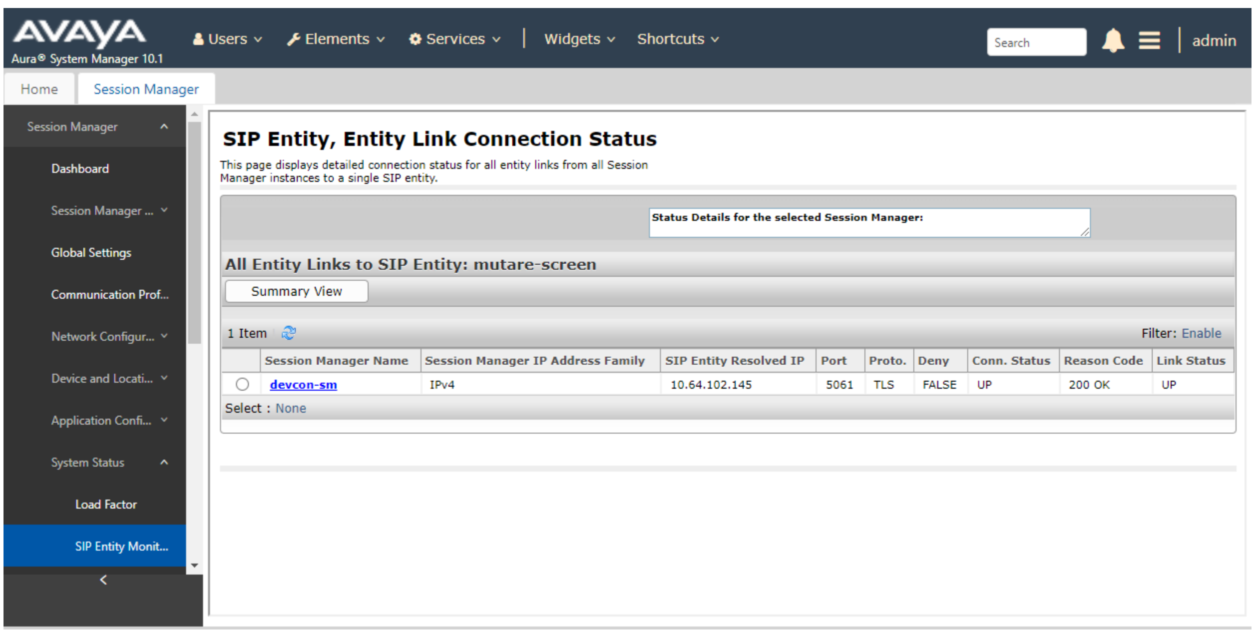
8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Session Manager, SBC, and Voice Traffic Filter.

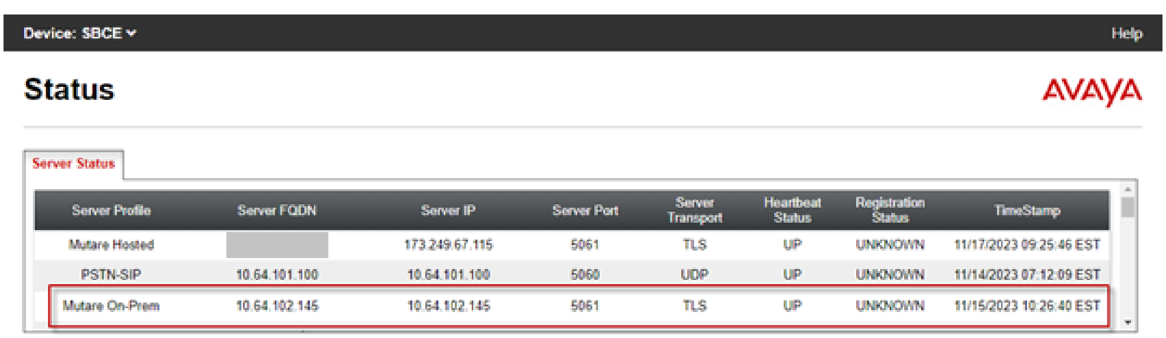
1. From the System Manager home page (not shown), select **Elements → Session Manager** from the top menu to display the **Session Manager Dashboard** (not shown).

   Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the Voice Traffic Filter entity name from **Section 5.1**.

   The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are "UP", as shown below.



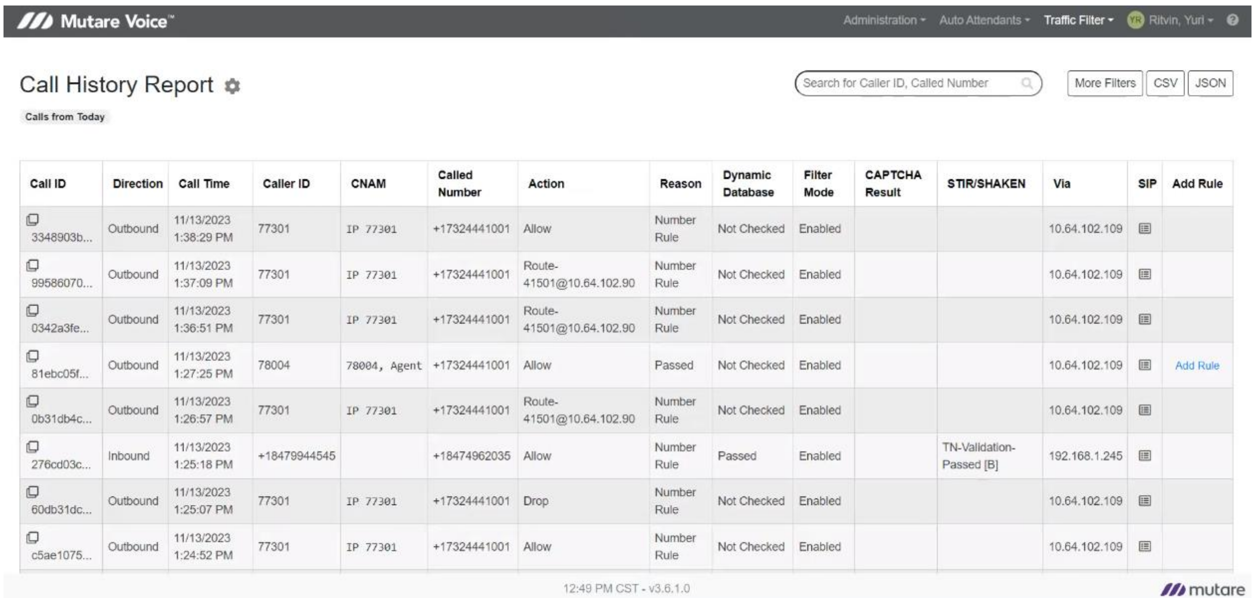
2. To verify the SIP trunk between SBC and Voice Screening Proxy is in-service, navigate to **Status → Server Status** in the SBC web interface. The **Heartbeat Status** should be *UP* as shown below.



3. Configure custom rules to analyze inbound and outbound calls.

4. Place inbound and outbound PSTN calls and verify that the appropriate call treatment was applied.

5. Verify that **Call History Report** reflects that the appropriate action was taken. A sample **Call History Report** is shown below.



Call ID	Direction	Call Time	Caller ID	CNAM	Called Number	Action	Reason	Dynamic Database	Filter Mode	CAPTCHA Result	STIR/SHAKEN	Via	SIP	Add Rule
3348903b...	Outbound	11/13/2023 1:38:29 PM	77301	IP 77301	+17324441001	Allow	Number Rule	Not Checked	Enabled			10.64.102.109		
99586070...	Outbound	11/13/2023 1:37:09 PM	77301	IP 77301	+17324441001	Route-41501@10.64.102.90	Number Rule	Not Checked	Enabled			10.64.102.109		
0342a3fe...	Outbound	11/13/2023 1:36:51 PM	77301	IP 77301	+17324441001	Route-41501@10.64.102.90	Number Rule	Not Checked	Enabled			10.64.102.109		
81ebc05f...	Outbound	11/13/2023 1:27:25 PM	78004	78004, Agent	+17324441001	Allow	Passed	Not Checked	Enabled			10.64.102.109		Add Rule
0b31db4c...	Outbound	11/13/2023 1:26:57 PM	77301	IP 77301	+17324441001	Route-41501@10.64.102.90	Number Rule	Not Checked	Enabled			10.64.102.109		
276cd03c...	Inbound	11/13/2023 1:25:18 PM	+18479944545		+18474962035	Allow	Number Rule	Passed	Enabled		TN-Validation-Passed [B]	192.168.1.245		
60db31dc...	Outbound	11/13/2023 1:25:07 PM	77301	IP 77301	+17324441001	Drop	Number Rule	Not Checked	Enabled			10.64.102.109		
c5ae1075...	Outbound	11/13/2023 1:24:52 PM	77301	IP 77301	+17324441001	Allow	Number Rule	Not Checked	Enabled			10.64.102.109		

9. Conclusion

These Application Notes described the configuration steps required for Mutare Voice Traffic Filter to interoperate with Avaya Aura® Session Manager and Avaya Session Border Controller using an on-premise deployment. All test cases were completed successfully.

10. Additional References

This section references the product documentation relevant to these Application Notes.

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023, available at http://support.avaya.com.

[2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 12, September 2023, available at http://support.avaya.com.

[3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

[4] *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 5, October 2023, available at http://support.avaya.com.

[5] *Mutare Voice Traffic Filter Admin Guide*, Version 3.6.0, April 7, 2023.

11. APPENDIX – opensips.cfg

This section contains excerpts from the **opensips.cfg** file in Voice Screening Proxy used for the compliance test. The text in bold highlights the required changes described in **Section 7.1.1**.

```
#------------------
#For UDP connection the section below is unremarked
listen=udp:10.64.102.145:5060
children=32

#For UDP connection the section above is unremarked
#------------------

listen=tls:10.64.102.145:5061

listen=hep_udp:10.64.102.145:9060
listen=hep_tcp:10.64.102.145:9060

server_header = "Server: ScP-W1"
user_agent_header = "User-Agent: ScP-W1"

####### Modules Section ########

#set module path
mpath="/usr/lib64/opensips/modules/"

loadmodule "tls_mgm.so"
loadmodule "proto_udp.so"
loadmodule "proto_tcp.so"
loadmodule "proto_tls.so"
loadmodule "tm.so"
loadmodule "sl.so"

                                     ooo

#set this server specific values
modparam("cfgutils", "shvset", "myip=s:10.64.102.145")
modparam("cfgutils", "shvset", "sbc=s:170.140.36.8")
modparam("cfgutils", "shvset", "with_tls=s:1")
modparam("cfgutils", "shvset", "with_tcp=s:0")
modparam("cfgutils", "shvset", "with_nat=s:0")

modparam("tls_mgm", "server_domain", "mutare=10.64.102.145:5061")
modparam("tls_mgm", "certificate", "[mutare]/etc/opensips/tls/user/user-cert.pem")
modparam("tls_mgm", "private_key", "[mutare]/etc/opensips/tls/user/user-privkey.pem")
modparam("tls_mgm", "ca_list", "[mutare]/etc/opensips/tls/user/user-calist.pem")
modparam("tls_mgm", "tls_method", "[mutare]TLSv1_2")
modparam("tls_mgm", "require_cert", "[mutare]0")
modparam("tls_mgm", "verify_cert", "[mutare]0")

modparam("proto_tls", "tls_port", 5061)
modparam("proto_tls", "tls_max_msg_chunks", 16)

                                     ooo

modparam("dispatcher", "db_url", "mysql://opensips:opensipsrw@localhost/opensips")
modparam("dispatcher", "ds_ping_method", "OPTIONS")
modparam("dispatcher", "ds_ping_interval", 30)
modparam("dispatcher", "ds_probing_sock", "udp:10.64.102.145:5060")
modparam("dispatcher", "ds_probing_list", "2") # The setid '2' is for CAPTCHA for SIP
OPTIONS ping.
```

```
modparam("dispatcher", "ds_probing_mode", 1)
modparam("dispatcher", "ds_probing_threshhold", 1)
modparam("dispatcher", "options_reply_codes", "404")

                                     ooo

####### Routing Logic ########
# main request routing logic

route {
    #script_trace( 1, "$rm from $si, ruri=$ru/$du", "Trace");

    force_rport();

    #initial requests

        $var(user)="osips@vtf.local";
        $var(trace_id) = "tid";

        if (is_method("OPTIONS|NOTIFY|PUBLISH|SUBSCRIBE")) {
           sip_trace("$var(trace_id)", "t", "sip|xlog", "$var(user)");
           xlog("$rm request from $si, $fU, $ua\n");
           sl_send_reply("200","OK");
           exit;
        }

           if nat_uac_test("15") {
                fix_nated_contact();
                xlog("$ci | Contact was fixed for $rm from $fU, $si\n");
           }

           if (is_method("INVITE")) {
               sip_trace("$var(trace_id)", "d", "sip|xlog", "$var(user)");
               if ($shv(with_nat) == "1") {
                  if (!ds_is_in_list("$si","","2")) {
                     fix_nated_sdp("2");
                     xlog("$ci | SDP was fixed for $rm from $fU, $si\n");
                  }
               }
           }

    # CANCEL processing
           if (is_method("CANCEL")) {
                     if (t_check_trans())
             t_relay();
             exit;
          }

    t_check_trans();

        if (has_totag()) {
            if (loose_route()) {
               xlog("$ci | Route parameters are $rr_params for $rm from $si, $fU to
$rU\n");

            $var(user)="osips@vtf.local";
            $var(trace_id) = "tid";

            if (is_method("REFER")) {
               xlog("$ci | REFER_received from $si, $fU to $tU\n");
            }
```

```
            if (is_method("INVITE")) {
               xlog("$ci | RE-INVITE_received from $si, $fU to $tU\n");
            }

            if (is_method("ACK")) {
                  xlog("$ci | ACK received from $si, $fU to $rU\n");
                  if ($shv(with_tls) == "1")
                      $fs = "tls:" + $shv(myip) + ":5061";
                  if ($shv(with_tcp) == "1")
                      $fs = "tcp:" + $shv(myip) + ":5060";
                  if ($rd == "10.64.102.146")
                      $fs = "udp:" + $shv(myip) + ":5060";

                  if ($rd == 10.64.102.109) {
                     if (remove_hf("Route"))
                        xlog("Removed header $hdr(Route)\n");
                  }
            }

        if (is_method("BYE")) {
               xlog("$ci | BYE received from $si, $fU to $rU\n");
                  if ($shv(with_tls) == "1")
                      $fs = "tls:" + $shv(myip) + ":5061";
                  if ($shv(with_tcp) == "1")
                      $fs = "tcp:" + $shv(myip) + ":5060";
                  if ($rd == "10.64.102.146")
                      $fs = "udp:" + $shv(myip) + ":5060";

                  if ($rd == 10.64.102.109) {
                     if (remove_hf("Route"))
                        xlog("Removed header $hdr(Route)\n");
                  }

                                        ooo

                # Outbound call's identifier
                if ($si == 10.64.102.109) {
                if ($fd == "avaya.com") {
                $avp(direction) = "outbound";
                ## $var(did_adjusted) = "+" + $(tU{s.substr,9,0});
                }
                }

                                        ooo

route [relay] {
           xlog("In route[relay]: $rm to $ru | Call-ID: $ci\n");

               if ($rd == "10.64.102.146")
                   $fs = "udp:" + $shv(myip) + ":5060";

       remove_hf("X-captcha*", "g");
       remove_hf("X-cid*", "g");
           t_on_reply("1");
           t_on_failure("1");
           if (!t_relay()) {
                send_reply("500","Internal Errors");
           }
           exit;
}

route [fast_failover] {
```

```
           xlog("$ci | In route[fast_failover]: $rm to $ru\n");

        $var(user)="osips@vtf.local";
        $var(trace_id) = "tid";

           if (is_method("INVITE")) {
              $var(Via0) = $hdr(Via);
              $var(Via1) = $(hdr(Via)[1]);
              xlog("Via 0 is $var(Via0), Via 1 is $var(Via1)\n");

              if replace("SIP/2.0/UDP 10.64.102.146", "SIP/2.0/TLS 10.64.102.146")
                 xlog("Via header has been fixed\n");
           }

           remove_hf("X-captcha*", "g");
           remove_hf("X-cid*", "g");
             $T_fr_timeout = 2;

           if ($shv(with_tls) == "1")
               $fs = "tls:" + $shv(myip) + ":5061";
           if ($shv(with_tcp) == "1")
               $fs = "tcp:" + $shv(myip) + ":5060";
           if ($rd == "10.64.102.146")
               $fs = "udp:" + $shv(myip) + ":5060";

             t_on_reply("1");
           t_on_failure("2");

           if (!t_relay()) {
                send_reply("500","Internal Errors");
           }
           exit;
}

onreply_route[1] {
        xlog("Reply from $fu to $tU with $T_reply_code\n");
        $var(user)="osips@vtf.local";
        $var(trace_id) = "tid";

        if ($rd == "10.64.102.146")
            $fs = "udp:" + $shv(myip) + ":5060";

        if replace("SIP/2.0/TLS 10.64.102.146", "SIP/2.0/UDP 10.64.102.146")
            xlog("Via header has been fixed\n");

    remove_hf("X-captcha*", "g");
        remove_hf("X-cid*", "g");

                                        ooo

route[redirection] {
           xlog("$ci | Call from $fu in route [redirection} should go to $ru\n");
           #$rd = $shv(sbc);
           #$rd = $fd;
           $rd = "devcon.com";
           xlog("$ci | Call from $fu in route [redirection} will go to $ru\n");
           remove_hf("Contact");
           t_reply("302", "Moved temporarily");
           exit;
}
```

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.