



## DevConnect Program

---

# Application Notes for Mutare Voice Traffic Filter with Avaya Session Border Controller using Hosted Deployment—Issue 1.0

## Abstract

These Application Notes describe the configuration steps required to integrate Mutare Voice Traffic Filter with Avaya Session Border Controller 10.1 using a hosted 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 Session Border Controller (SBC) via a SIP trunk.

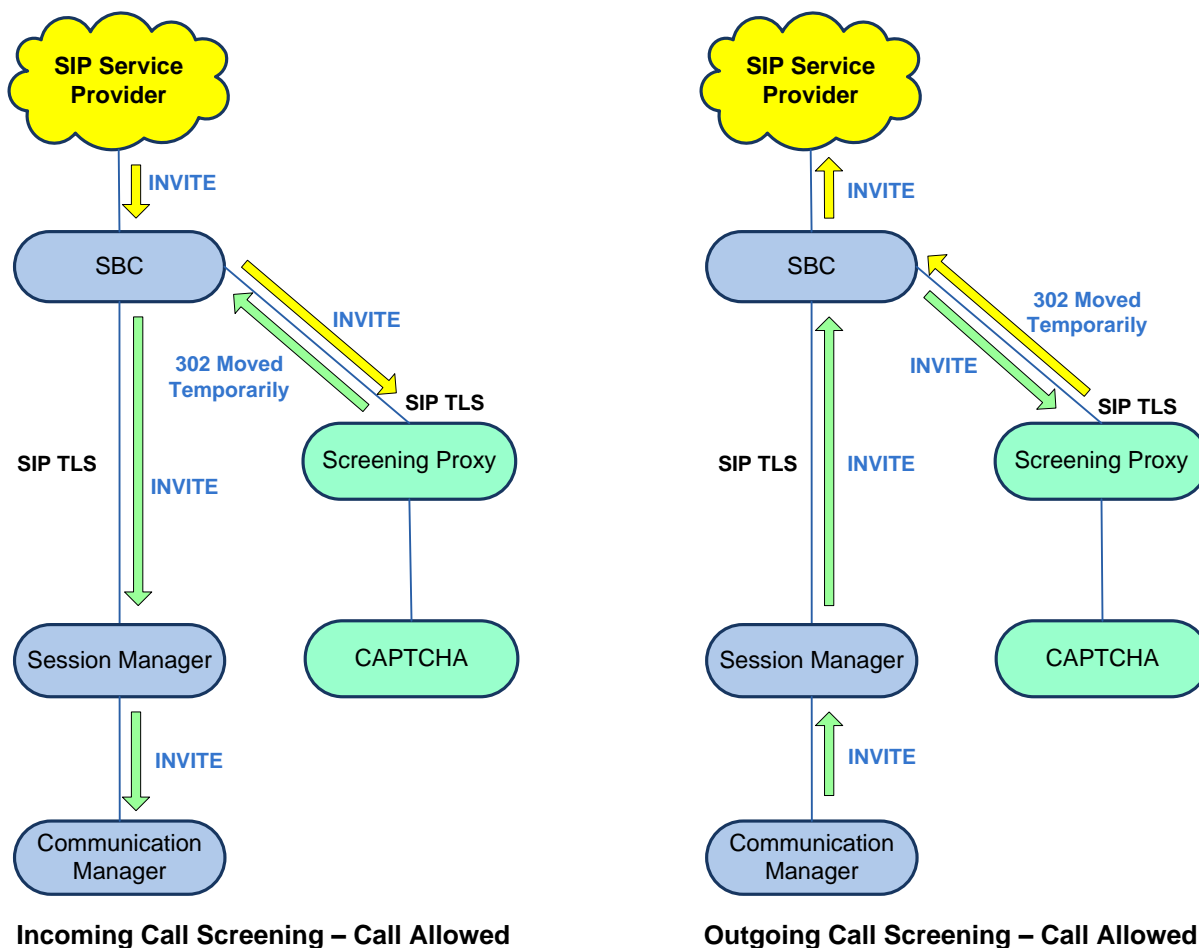
Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 Session Border Controller (SBC) 10.1 using a hosted deployment. In this compliance test, Mutare Voice Traffic Filter in a Mutare Private Cloud connected to 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 and 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. If Voice CAPTCHA is applied to an inbound call, then Voice Screening Proxy responds to Avaya SBC with a SIP REFER (not shown). 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.



## 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.
- 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

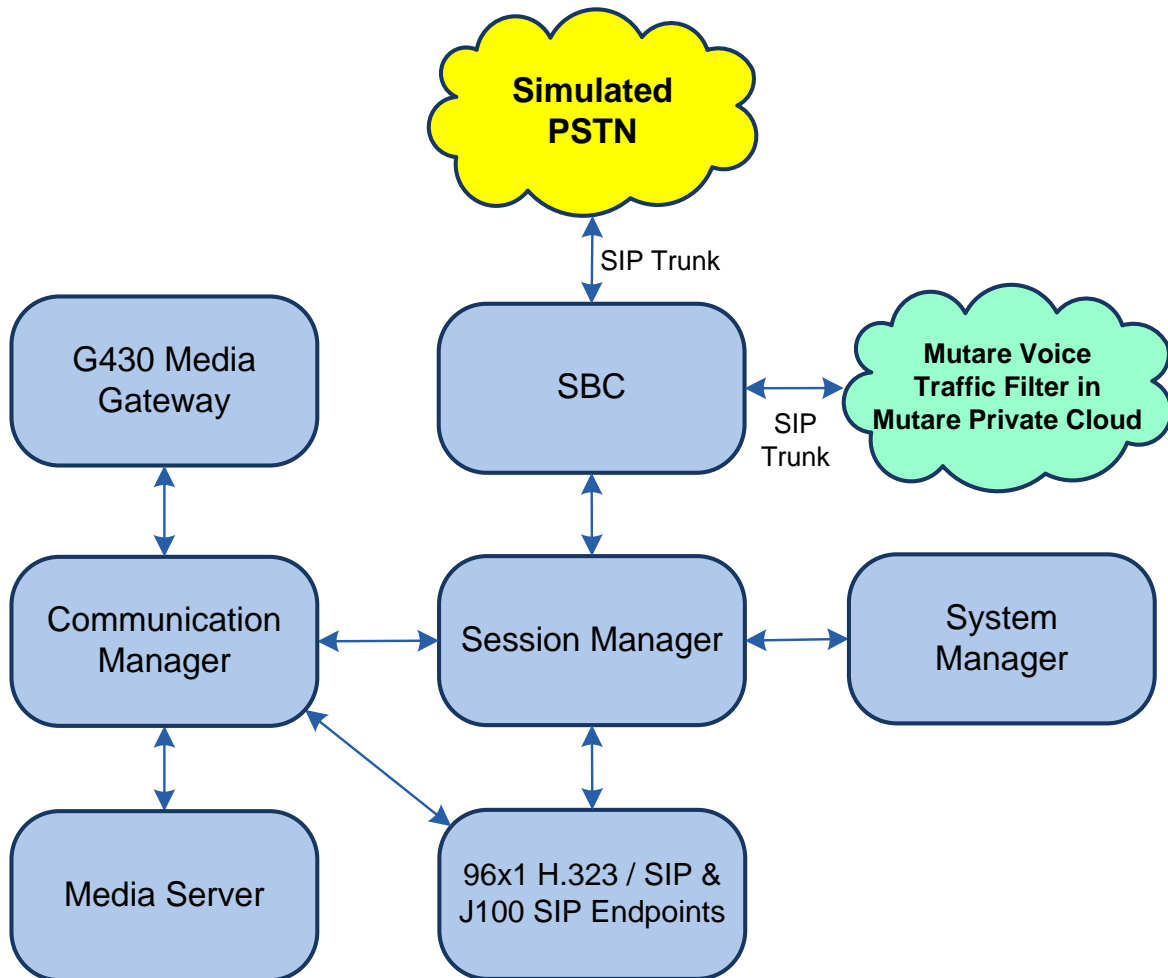
Technical support on Mutare Voice Traffic Filter can be obtained through the following:

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

### 3. Reference Configuration

**Figure 1** illustrates the test configuration for Mutare Voice Traffic Filter, which was located in a Mutare Private Cloud. The solution consisted of Mutare Rules Engine Application Server, Mutare Voice Screening Proxy, Mutare Voice CAPTCHA, and the Dynamic Robocall Database.

Voice Traffic Filter connects to SBC via SIP trunks using TLS/SRTP. 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 in Mutare Private Cloud**

## 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	1.10.6-release-18 (FreeSwitch)

## 5. 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 and outbound PSTN calls, SBC routes calls to Voice Screening Proxy as the primary route, if available. Legitimate calls are then passed back to SBC using 302 Moved Temporarily and then routed to Session Manager or the PSTN. If Voice CAPTCHA is applied to the call, Voice Screening Proxy responds with SIP REFER. 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.

**Note:** Public IP addresses have been redacted for security reasons.

## 5.1. 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.



### Log In

Username:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2023 Avaya Inc. All rights reserved.

## Avaya Session Border Controller

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.

Device: EMS ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard

Software Management

Device Management

- System Administration
- Templates

Backup/Restore

Monitoring & Logging

Dashboard

Information		
System Time	03:50:52 PM EST	<a href="#">Refresh</a>
Version	10.1.2.0-64-23285	
GUI Version	10.1.2.0-23278	
Build Date	Tue May 16 08:55:42 IST 2023	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	11/09/2023 14:43:19 EST	
Failed Login Attempts	0	

Installed Devices

EMS

SBCE



## 5.2. 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, Voice Screening Proxy, and the PSTN.

### 5.2.1. 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 instead of forwarding it to Session Manager. SBC routes calls 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.

The screenshot displays the Avaya Session Border Controller configuration interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. The left sidebar lists various configuration categories, with 'Configuration Profiles' expanded to show 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: Avaya-SM' and features an 'Add' button. Below this is a list of profiles: 'cs2100', 'avaya-ru', 'Avaya-SM' (highlighted), 'PSTN-SIP', and 'Mutare'. The 'Avaya-SM' profile is selected, and its configuration is shown in a tabbed interface with 'General' as the active tab. The 'General' tab contains a table of settings, with '3xx Handling' set to 'Yes' and highlighted by a red box. Other settings include 'Hold Support' (None), '180 Handling' (None), '181 Handling' (None), '182 Handling' (None), '183 Handling' (None), 'Refer Handling' (No), 'URI Group' (None), 'Send Hold' (No), 'Delayed Offer' (Yes), 'Diversion Header Support' (No), 'Delayed SDP Handling' (No), 'Re-Invite Handling' (No), 'Prack Handling' (No), 'Allow 18X SDP' (No), 'T.38 Support' (No), 'URI Scheme' (SIP), 'Via Header Format' (RFC3261), 'SIPS Required' (Yes), and 'MediaSec' (No).

Setting	Value
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	Yes
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
MediaSec	No

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

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesDomain DoSServerInterworkingMedia ForkingRoutingTopology HidingSignalingManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse ProxyPolicyURN ProfileRecording Profile

Interworking Profiles: Avaya-SMAddRenameCloneDelete

Interworking Profiles

cs2100avaya-ruAvaya-SM PSTN-SIPMutare

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

DTMF

DTMF Support	None
--------------	------

Edit

### 5.2.2. 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.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Domain DoS  
Server Interworking  
Media Forking  
Routing  
Topology Hiding  
Signaling Manipulation  
URI Groups  
SNMP Traps  
Time of Day Rules  
FGDN Groups  
Reverse Proxy Policy  
URN Profile  
Recording Profile  
H248 Profile  
IP/URI Blocklist Profile  
Services  
Domain Policies  
TLS Management  
Network & Flows  
DMZ Services  
Monitoring & Logging

Interworking Profiles: Mutare

Add

Rename Clone Delete

Interworking Profiles

cs2100  
avaya-ru  
Avaya-SM  
PSTN-SIP  
Mutare

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

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).

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border ControllerAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesDomain DoSServerInterworkingMedia ForkingRoutingTopology HidingSignalingManipulationURI GroupsSNMP TrapsTime of Day Rules

Interworking Profiles: MutareAddRenameCloneDelete

Interworking Profilescs2100avaya-ruAvaya-SMPSTN-SIPMutare

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

SIP Timers

Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	2 seconds
Invite Expire	---
Retry After	---

Edit

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

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border ControllerAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesDomain DoSServerInterworkingMedia ForkingRoutingTopology HidingSignalingManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse ProxyPolicyURN ProfileRecording Profile

Interworking Profiles: MutareAddRenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	No
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

DTMF

DTMF Support	None
--------------	------

Edit

JAO; Reviewed:  
SPOC 1/8/2024

Avaya DevConnect Program  
©2024 Avaya LLC. All Rights Reserved.

12 of 47  
MutareVTF-H-SBC

### 5.2.3. Server Interworking Profile for PSTN

Modify the **Server Interworking** profile for the PSTN by navigating to **Configuration Profiles** → **Server Interworking** from the left pane. Click on the PSTN profile, select the **General** tab, and then click on the **Edit** button (not shown). Enable **Refer Handling** and **3xx Handling** as shown below so that SBC handles SIP REFER and 3xx responses locally instead of forwarding it to the PSTN. SBC routes calls to Voice Screening Proxy, which then responds with a SIP REFER or 302 Moved Temporarily with new Contact information. Voice Screening Proxy responds with SIP REFER of Voice CAPTCHA is applied to the call. Legitimate calls are then routed to Session Manager.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

Domain DoS

**Server Interworking**

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

H248 Profile

IP/URI Blocklist Profile

▸ Services

SIP Servers

H248 Servers

LDAP

RADIUS

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Interworking Profiles: PSTN-SIP

Add

Interworking Profiles

cs2100

avaya-ru

Avaya-SM

**PSTN-SIP**

PCIPal

VolPSP

Meetings

CI-eONE

Mutare

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
<b>Refer Handling</b>	<b>Yes</b>
URI Group	None
Send Hold	No
Delayed Offer	Yes
<b>3xx Handling</b>	<b>Yes</b>
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

Edit

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

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border ControllerAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesDomain DoSServerInterworkingMedia ForkingRoutingTopology HidingSignalingManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse ProxyPolicyURN ProfileRecording Profile

Interworking Profiles: PSTN-SIP

Add

Interworking Profiles

cs2100avaya-ruAvaya-SMPSTN-SIPMutare

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

Click here to add a description.

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

DTMF

DTMF Support	None
--------------	------

Edit

JAO; Reviewed:  
SPOC 1/8/2024

Avaya DevConnect Program  
©2024 Avaya LLC. All Rights Reserved.

14 of 47  
MutareVTF-H-SBC

### 5.3. Administer SIP Servers

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

#### 5.3.1. 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.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
    **SIP Servers**  
        H248 Servers  
        LDAP  
        RADIUS  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
▸ DMZ Services  
▸ Monitoring & Logging

SIP Servers: Session Manager  
Add  
Server Profiles  
    Posh Voice Prod  
    PCIPal  
    Posh Voice Staging  
    OCP-SBCE-PUBLIC  
    VoIPSP  
    MeetingsM  
    MeetingsWebGW  
    **Session Manager**  
    PSTN-SIP  
    Mutare On-Prem

Rename Clone Delete

General Authentication Heartbeat Registration Ping Advanced

Server Type Call Server  
TLS Client Profile sbceInternalA1  
DNS Query Type NONE/A  
IP Address / FQDN Port Transport Whitelist  
10.64.102.117 5061 TLS ☐  
Edit

The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 5.2.1**. All other tabs were left with their default values.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
    **SIP Servers**  
        H248 Servers  
        LDAP  
        RADIUS  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
▸ DMZ Services  
▸ Monitoring & Logging

SIP Servers: Session Manager  
Add  
Server Profiles  
    Posh Voice Prod  
    PCIPal  
    Posh Voice Staging  
    OCP-SBCE-PUBLIC  
    VoIPSP  
    MeetingsM  
    MeetingsWebGW  
    **Session Manager**  
    PSTN-SIP  
    Mutare On-Prem

Rename Clone Delete

General Authentication Heartbeat Registration Ping Advanced

Enable DoS Protection ☐  
Enable Grooming ☒  
Interworking Profile Avaya-SM  
Signaling Manipulation Script None  
Securable ☐  
Enable FGDN ☐  
Tolerant ☐  
URI Group None  
NG911 Support ☐  
Edit

### 5.3.2. 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 5.9**.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border ControllerAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesSIP ServersH248 ServersLDAPRADIUSDomain PoliciesTLS Management

SIP Servers: Mutare HostedAddRenameCloneDelete

Server ProfilesVoIPSPMeetingsMMeetingsWebGWSession ManagerMutare HostedPSTN-SIPMutare On-Prem

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Server TypeTrunk Server

TLS Client ProfileMutareH\_Client\_Profile

DNS Query TypeNONE/A

IP Address / FQDN / CIDR Range	Port	Transport	Whitelist
10.10.10.10/24	5061	TLS	<input type="checkbox"/>

Edit

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.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border ControllerAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesSIP ServersH248 ServersLDAPRADIUSDomain PoliciesTLS Management

SIP Servers: Mutare HostedAddRenameCloneDelete

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable Heartbeat☒

MethodOPTIONS

Frequency120 seconds

From URIdevcon-sbce@10.10.10.10

To URImutare@10.10.10.10

Edit

JAO; Reviewed:  
SPOC 1/8/2024

Avaya DevConnect Program  
©2024 Avaya LLC. All Rights Reserved.

16 of 47  
MutareVTF-H-SBC



The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 5.2.2**. All other tabs were left with their default values.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services

SIP ServersH248 ServersLDAPRADIUS▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

SIP Servers: Mutare Hosted

Add

RenameCloneDelete

Server Profiles

VoIPSPMeetingsMMeetingsWebGWSession ManagerMutare HostedPSTN-SIPMutare On-Prem

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable DoS Protection☐

Enable Grooming☒

Interworking ProfileMutare

Signaling Manipulation ScriptNone

Securable☐

Enable FGDN☐

Tolerant☐

URI GroupNone

NG911 Support☐

Edit

### 5.3.3. SIP Server for PSTN

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 PSTN SIP Server was configured as shown below.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services

SIP ServersH248 ServersLDAPRADIUS▸ Domain Policies▸ TLS Manaoement

SIP Servers: PSTN-SIP

Add

RenameCloneDelete

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Server TypeCall Server

DNS Query TypeNONE/A

IP Address / FQDN	Port	Transport	Whitelist
10.64.101.100	5060	UDP	<input type="checkbox"/>

Edit

JAO; Reviewed:  
SPOC 1/8/2024

Avaya DevConnect Program  
©2024 Avaya LLC. All Rights Reserved.

17 of 47  
MutareVTF-H-SBC

The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 5.2.3**. All other tabs were left with their default values.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

**SIP Servers**

H248 Servers

LDAP

RADIUS

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

SIP Servers: PSTN-SIP

Add

Server Profiles

Posh Voice Prod

PCIPal

Posh Voice Staging

OCP-SBCE-PUBLIC

VoIPSP

MeetingsM

MeetingsWebGW

Session Manager

Mutare Hosted

**PSTN-SIP**

Mutare On-Prem

General

Authentication

Heartbeat

Registration

Ping

**Advanced**

Enable DoS Protection

☐

Enable Grooming

☒

Interworking Profile

PSTN-SIP

Signaling Manipulation Script

None

Securable

☐

Enable FGDN

☐

Tolerant

☐

URI Group

None

NG911 Support

☐

Edit

## 5.4. 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 5.12**. 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 *MutareH-Inbound* and *MutareH-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.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesDomain DoSServer InterworkingMedia ForkingRoutingTopology HidingSignaling ManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse ProxyPolicy

Routing Profiles: MutareH-Inbound

Add

RenameCloneDelete

Click here to add a description.

Routing Profile

Update PriorityAdd

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.64.102.117:5061	TLS	EditDelete

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

Profile : MutareH-Inbound - Edit Rule

URI Group

\*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

Mutare

None

Delete

2

Session

10.64.102.117

None

Delete

Finish

*MutareH-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.

Device: SBCE Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy

Policy

Routing Profiles: MutareH-Outbound

Add

Routing Profiles

default

Meetings

MutareH-Outbound

Session Manager

PSTN-SIP

Mutare-Outbound

Mutare-Inbound

Click here to add a description.

Routing Profile

Update Priority

Add

Priority

URI Group

Time of Day

Load Balancing

Next Hop Address

Transport

1

\*

default

Priority

10.64.101.100:5061

UDP

Edit Delete

JAO; Reviewed:  
SPOC 1/8/2024

Avaya DevConnect Program  
©2024 Avaya LLC. All Rights Reserved.

20 of 47  
MutareVTF-H-SBC

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

Profile : MutareH-Outbound - Edit Rule

URI Group

\*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

Mutare H

None

Delete

2

PSTN-SI

10.64.101.100

None

Delete

Finish

## 5.5. 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.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesDomain DoSServer InterworkingMedia ForkingRoutingTopology HidingSignaling ManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse Proxy Policy

Topology Hiding Profiles: MutareH

Add

RenameCloneDelete

Click here to add a description.

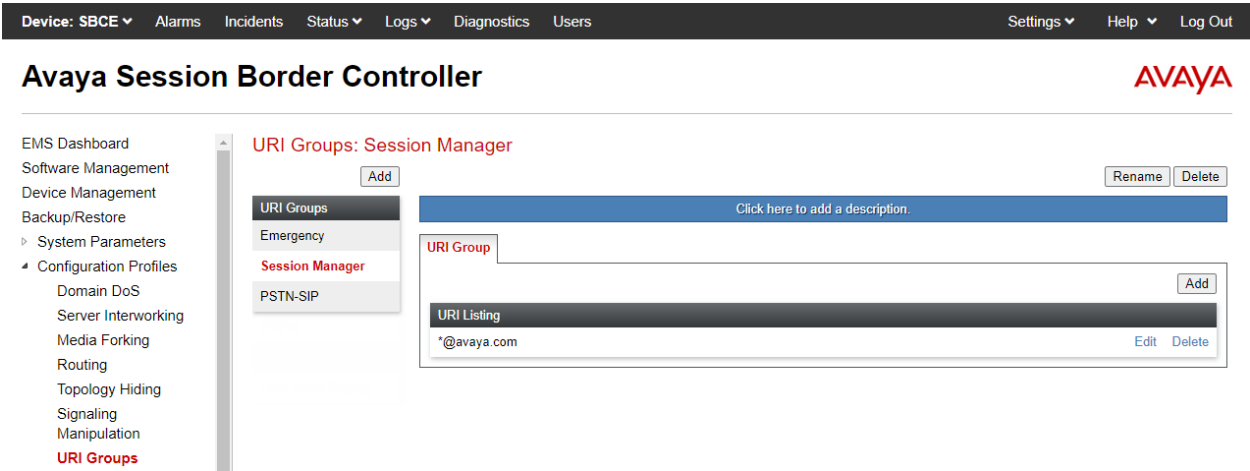
Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	IP:10.10.10.10
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	IP:10.10.10.10
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---

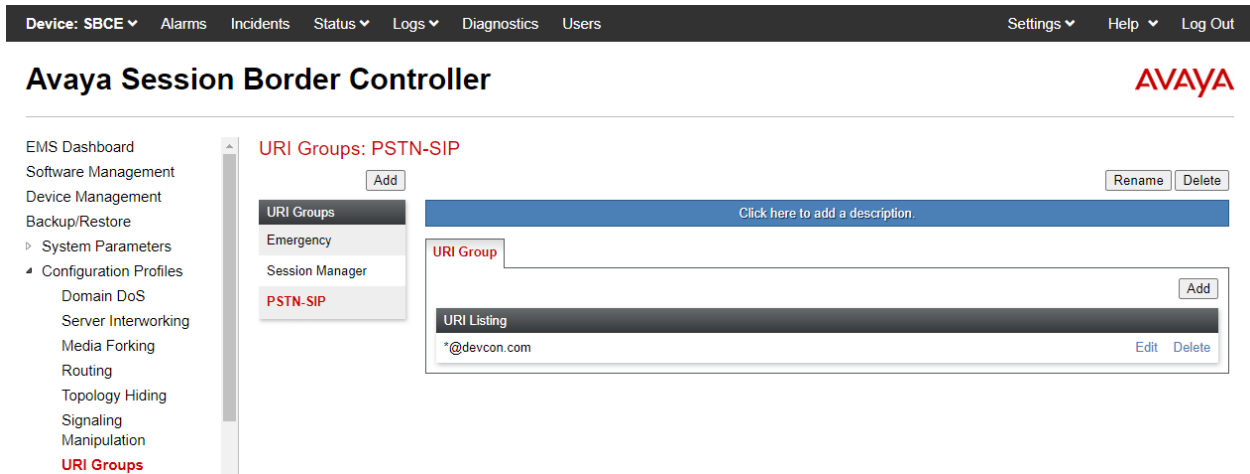
Edit

## 5.6. Administer URI Groups

A **URI Group** is used to distinguish between calls originated from the Avaya Aura® network or the PSTN. 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 5.12**, SBC examines the domain in the From header.



The following URI group, named *PSTN-SIP*, identifies calls arriving from the PSTN, designated with *devcon.com* as the domain in the From header of the SIP INVITE. Outbound calls from Session Manager would specify *avaya.com* as the domain in the From header of the SIP INVITE. By applying this URI group to a server flow in **Section 5.12**, SBC examines the domain in the From header to determine if the server flow is a match.



## 5.7. 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.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border ControllerAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore> System Parameters> Configuration Profiles> Services4 Domain PoliciesApplication RulesBorder RulesMedia RulesSecurity RulesSignaling RulesCharging RulesEnd Point PolicyGroupsSession Policies> TLS Management> Network & Flows> DMZ Services> Monitoring & Logging

Media Rules: RTP-SRTPAddRenameCloneDelete

Media Rulesdefault-low-meddefault-low-med-encdefault-highdefault-high-encavaya-low-med-encRTP-SRTP

Click here to add a description.

EncryptionCodec PrioritizationAdvancedQoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_32 RTP
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_32 RTP
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous

Capability Negotiation	<input type="checkbox"/>
------------------------	--------------------------

Edit

JAO; Reviewed:  
SPOC 1/8/2024

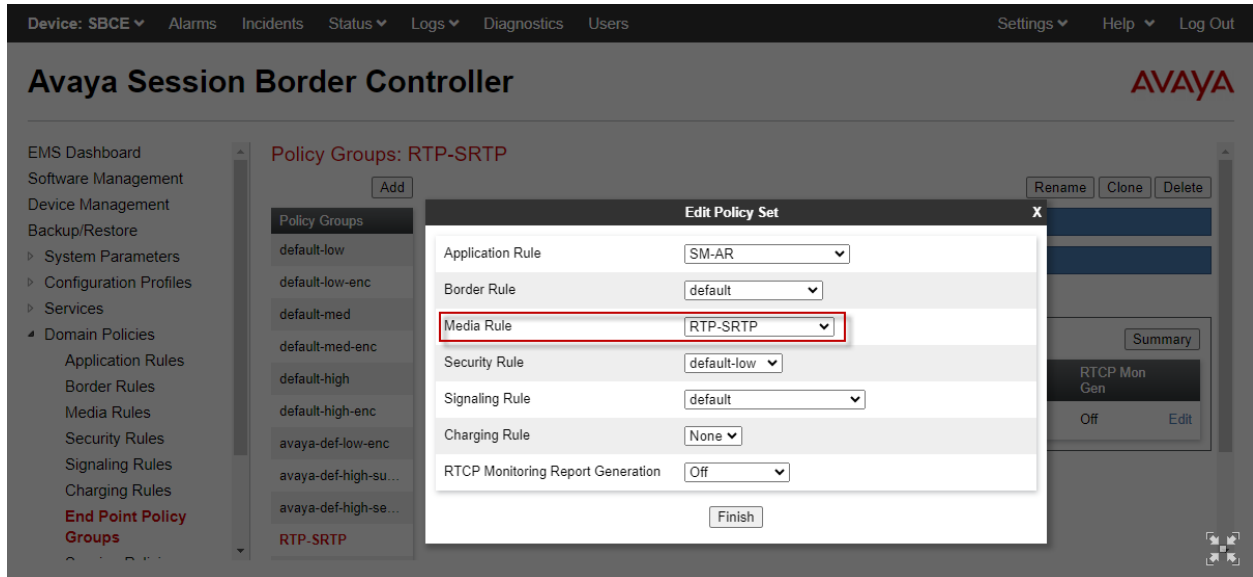
Avaya DevConnect Program  
©2024 Avaya LLC. All Rights Reserved.

24 of 47  
MutareVTF-H-SBC



## 5.8. 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.



## 5.9. Administer TLS Management

This section covers installing the Voice Screening Proxy certificates, configuring the Voice Screening Proxy TLS client profile, and configuring the TLS server profile for the B2 public interface. Voice Screening Proxy communicates with SBC over the B2 public interface. The TLS configuration for Session Manager is assumed to already be in place and is not shown in these Application Notes.

Navigate to **TLS Management → Certificates** and install Voice Screening Proxy certificates. For the compliance test, two intermediate certificates and a CA certificate were installed as shown below.

The screenshot shows the Avaya Session Border Controller (SBC) web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Avaya Session Border Controller' and the Avaya logo. The left sidebar contains a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates (selected), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Certificates' and features 'Install' and 'Generate CSR' buttons. Below these buttons, there are two sections: 'Installed Certificates' and 'Installed CA Certificates'. The 'Installed Certificates' section lists three certificates: sbceExternalB1.pem, sbceInternalA1.pem, and sbceExternalB2.pem, each with 'View' and 'Delete' links. The 'Installed CA Certificates' section lists seven certificates: AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust\_g2\_ca.cer, SystemManagerCA.pem, ocpSystemManagerCA.pem, MutareComodo.crt, MutareSectigo.crt, and MutareUSERTrust.crt, each with 'View' and 'Delete' links. A red box highlights the last three certificates in the 'Installed CA Certificates' section. At the bottom, there is a section for 'Installed Certificate Revocation Lists'.

Installed Certificates	
sbceExternalB1.pem	<a href="#">View</a> <a href="#">Delete</a>
sbceInternalA1.pem	<a href="#">View</a> <a href="#">Delete</a>
sbceExternalB2.pem	<a href="#">View</a> <a href="#">Delete</a>

Installed CA Certificates	
AvayaDeviceEnrollmentCAchain.crt	<a href="#">View</a> <a href="#">Delete</a>
avayaitrootca2.pem	<a href="#">View</a> <a href="#">Delete</a>
entrust_g2_ca.cer	<a href="#">View</a> <a href="#">Delete</a>
SystemManagerCA.pem	<a href="#">View</a> <a href="#">Delete</a>
ocpSystemManagerCA.pem	<a href="#">View</a> <a href="#">Delete</a>
MutareComodo.crt	<a href="#">View</a> <a href="#">Delete</a>
MutareSectigo.crt	<a href="#">View</a> <a href="#">Delete</a>
MutareUSERTrust.crt	<a href="#">View</a> <a href="#">Delete</a>

Installed Certificate Revocation Lists	
--	--

Next, create a **Client Profile** for Voice Screening Proxy as shown below. The **Profile Name** was set to *MutareH\_Client\_Profile* and the B2 public interface certificate was selected. **Peer Verification** was set to *Required* and the Voice Screening Proxy certificates were selected for **Peer Certificate Authorities**. The **Verification Depth** was set to *4* and the **Version** was set to *TLS 1.2*. This client profile was assigned to the Voice Screening Proxy SIP server in **Section 5.3.2**.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border ControllerAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesTLS ManagementCertificatesClient ProfilesServer ProfilesSNI GroupNetwork & FlowsDMZ ServicesMonitoring & Logging

Client Profiles: MutareH\_Client\_ProfileAddDelete

Client ProfilesMutare\_Client\_Pr...sbceExternalB2sbceExternalB1sbceInternalA1MutareH\_Client\_...

Click here to add a description.

Client Profile

TLS Profile

Profile Name	MutareH_Client_Profile
Certificate	sbceExternalB2.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	MutareComodo.crt MutareSectigo.crt MutareUSERTrust.crt
Peer Certificate Revocation Lists	---
Verification Depth	4
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.3 <input checked="" type="checkbox"/> TLS 1.2
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	DEFAULT:!SHA

JAO; Reviewed:  
SPOC 1/8/2024

Avaya DevConnect Program  
©2024 Avaya LLC. All Rights Reserved.

27 of 47  
MutareVTF-H-SBC

The following server profile is assigned to the B2 public interface in **Section 5.11**.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

- Certificates
- Client Profiles
- Server Profiles**
- SNI Group

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Server Profiles: sbceExternalB2

AddDelete

Server Profiles

sbceInternalA1

sbceExternalB1

sbceExternalB2-...

**sbceExternalB2**

Click here to add a description.

Server Profile

TLS Profile

Profile Name

sbceExternalB2

Certificate

sbceExternalB2.pem

SNI Options

None

Certificate Verification

Peer Verification

None

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.3☒ TLS 1.2

Ciphers

☒ Default☐ FIPS☐ Custom

Value

DEFAULT:ISHA

Edit

## 5.10. Administer Media Interfaces

A **Media Interface** defines an IP address and port range for transmitting media. An existing media interface, named *PublicMediaB2*, was used for Voice CAPTCHA.

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.

- **PublicMediaB2:** Media interface used by Voice CAPTCHA to send and receive media.
- **SM-Media:** Media interface used by Session Manager to send and receive media.
- **PSTN-Media:** Media interface used by PSTN to send and receive media.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
    Network Management  
    **Media Interface**  
    Signaling Interface  
    End Point Flows  
    Session Flows  
    Advanced Options  
▸ DMZ Services  
▸ Monitoring & Logging

Media Interface

Media Interface

Add

Name	Media IP Network	Port Range	TLS Profile	Buffer Size [KB]	
PublicMediaB2	Public-B2 (B2, VLAN 0)	35000 - 40000	None	500	Edit Delete
MeetingsMedia	10.64.102.230 Private-A1 (A1, VLAN 0)	35000 - 40000	sbceInternalA1	500	Edit Delete
MedTunExt	Public-B2 (B2, VLAN 0)	35000 - 40000	sbceExternalB2-Media	500	Edit Delete
MedTunInt	10.64.102.231 Private-A1 (A1, VLAN 0)	35000 - 40000	sbceInternalA1	500	Edit Delete
SM-Media	10.64.102.106 Private-A1 (A1, VLAN 0)	35000 - 40000	None	500	Edit Delete
Mutare-Media	10.64.102.109 Private-A1 (A1, VLAN 0)	35000 - 40000	None	500	Edit Delete
SM-RW-Media	10.64.102.108 Private-A1 (A1, VLAN 0)	35000 - 40000	None	500	Edit Delete
RW-Media	10.64.101.102 Public-B1 (B1, VLAN 0)	50000 - 55000	sbceExternalB1	500	Edit Delete
PSTN-Media	10.64.101.101 Public-B1 (B1, VLAN 0)	35000 - 40000	None	500	Edit Delete

## 5.11. Administer Signaling Interfaces

A signaling interface defines an IP address, protocols and listen ports that SBC can use for signaling. An existing signaling interface, named *PublicSignalingB2*, was used for Voice Screening Proxy.

Navigate to **Networks & Flows** → **Signaling Interface** to define a new **Signaling Interface**. In the Compliance Test the following interfaces were defined. The signaling interfaces used for this solution are listed below.

- **PublicSignalingB2:** Signaling interface used by Voice Screening Proxy for SIP signaling.
- **SM-Signaling:** Signaling interface used by Session Manager for SIP signaling.
- **PSTN-Signaling:** Signaling interface used by PSTN for SIP signaling.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
    Network Management  
    Media Interface  
    **Signaling Interface**  
    End Point Flows  
    Session Flows  
    Advanced Options  
▸ DMZ Services  
▸ Monitoring & Logging

Signaling Interface

Signaling Interface

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
ServiceProvider	Public-B2 (B2, VLAN 0)	5060	5060	---	None	Edit Delete
MeetingsSignaling	10.64.102.230 Private-A1 (A1, VLAN 0)	---	---	5061	sbceInternalA1	Edit Delete
SigTunInt	10.64.102.231 Private-A1 (A1, VLAN 0)	---	---	5061	sbceInternalA1	Edit Delete
PublicSignalingB2	Public-B2 (B2, VLAN 0)	---	5062	5061	sbceExternalB2	Edit Delete
Mutare-Signaling	10.64.102.109 Private-A1 (A1, VLAN 0)	---	---	5061	sbceInternalA1	Edit Delete
SM-Signaling	10.64.102.106 Private-A1 (A1, VLAN 0)	5060	5060	5061	sbceInternalA1	Edit Delete
PSTN-Signaling	10.64.101.101 Public-B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
RW-Signaling	10.64.101.102 Public-B1 (B1, VLAN 0)	---	---	5061	sbceExternalB1	Edit Delete
SM-RW-Signaling	10.64.102.108 Private-A1 (A1, VLAN 0)	---	---	5061	sbceInternalA1	Edit Delete

## 5.12. 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.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
    Network Management  
    Media Interface  
    Signaling Interface  
    **End Point Flows**  
    Session Flows  
    Advanced Options  
▸ DMZ Services  
▸ Monitoring & Logging

End Point Flows

Subscriber Flows Server Flows

Add

Modifications made to a Server Flow will only take effect on new sessions.

Click here to add a row description.

SIP Server: Mutare Hosted

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Mutare Hosted Outbound	Session Manager	SM-Signaling	PublicSignalingB2	RTP-SRTP	default	View Clone Edit Delete
2	Mutare Hosted Inbound	PSTN-SIP	PSTN-Signaling	PublicSignalingB2	RTP-SRTP	default	View Clone Edit Delete

SIP Server: PSTN-SIP

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	PSTN-SIP Flow	*	SM-Signaling	PSTN-Signaling	RTP-SRTP	MutareH-Inbound	View Clone Edit Delete

SIP Server: Session Manager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Session Manager Flow	*	PSTN-Signaling	SM-Signaling	RTP-SRTP	MutareH-Outbound	View Clone Edit Delete

JAO; Reviewed:  
SPOC 1/8/2024

Avaya DevConnect Program  
©2024 Avaya LLC. All Rights Reserved.

31 of 47  
MutareVTF-H-SBC

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 Hosted Inbound	<ol style="list-style-type: none"> <li>1. SBC sends SIP INVITE to Voice Screening Proxy.</li> <li>2. Voice Screening Proxy responds with 302 Moved Temporarily for legitimate calls where Voice CAPTCHA <i>is not</i> applied to call.</li> <li>3. Voice Screening Proxy responds with SIP REFER for legitimate calls where Voice CAPTCHA <i>is</i> applied to call.</li> <li>4. SBC routes call to Session Manager, the secondary route in the <i>MutareH-Inbound</i> routing profile.</li> </ol>
Outbound Call	Session Manager Flow	Mutare Hosted Outbound	<ol style="list-style-type: none"> <li>1. SBC sends SIP INVITE to Voice Screening Proxy.</li> <li>2. Voice Screening Proxy responds with 302 Moved Temporarily for legitimate calls.</li> <li>3. SBC routes call to PSTN, the secondary route in the <i>MutareH-Outbound</i> routing profile.</li> </ol>



### 5.12.1. 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 Hosted 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.

**Edit Flow: Mutare Hosted Inbound** X

Flow Name	Mutare Hosted Inbound
SIP Server Profile	Mutare Hosted ▼
URI Group	PSTN-SIP ▼
Transport	* ▼
Remote Subnet	*
Received Interface	PSTN-Signaling ▼
Signaling Interface	PublicSignalingB2 ▼
Media Interface	PublicMediaB2 ▼
Secondary Media Interface	None ▼
End Point Policy Group	RTP-SRTP ▼
Routing Profile	default ▼
Topology Hiding Profile	MutareH ▼
Signaling Manipulation Script	None ▼
Remote Branch Office	Any ▼
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

For outbound PSTN calls, the *Mutare Hosted 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 5.2.1**, 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 Hosted 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 *MutareH-Outbound* routing profile specified under Session Manager server flows, which is the PSTN.

Edit Flow: Mutare Hosted Outbound		X
Flow Name	<input type="text" value="Mutare Hosted Outbound"/>	
SIP Server Profile	<input type="text" value="Mutare Hosted"/>	
URI Group	<input type="text" value="Session Manager"/>	
Transport	<input type="text" value="*/"/>	
Remote Subnet	<input type="text" value="*/"/>	
Received Interface	<input type="text" value="SM-Signaling"/>	
Signaling Interface	<input type="text" value="PublicSignalingB2"/>	
Media Interface	<input type="text" value="PublicMediaB2"/>	
Secondary Media Interface	<input type="text" value="None"/>	
End Point Policy Group	<input type="text" value="RTP-SRTP"/>	
Routing Profile	<input type="text" value="default"/>	
Topology Hiding Profile	<input type="text" value="None"/>	
Signaling Manipulation Script	<input type="text" value="None"/>	
Remote Branch Office	<input type="text" value="Any"/>	
Link Monitoring from Peer	<input type="checkbox"/>	
FQDN Support	<input type="checkbox"/>	
FQDN	<input type="text"/>	
<input type="button" value="Finish"/>		

## 5.12.2. Server Flows for PSTN

Inbound PSTN calls will match *PSTN-SIP Flow* shown below as the source flow. The **Routing Profile**, *MutareH-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** X

Flow Name	<input type="text" value="PSTN-SIP Flow"/>
SIP Server Profile	<input type="text" value="PSTN-SIP"/>
URI Group	<input type="text" value="*/"/>
Transport	<input type="text" value="*/"/>
Remote Subnet	<input type="text" value="*/"/>
Received Interface	<input type="text" value="SM-Signaling"/>
Signaling Interface	<input type="text" value="PSTN-Signaling"/>
Media Interface	<input type="text" value="PSTN-Media"/>
Secondary Media Interface	<input type="text" value="None"/>
End Point Policy Group	<input type="text" value="RTP-SRTP"/>
Routing Profile	<input type="text" value="MutareH-Inbound"/>
Topology Hiding Profile	<input type="text" value="None"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input type="text"/>

Finish

### 5.12.3. Server Flows for Session Manager

Outbound PSTN calls will match *Session Manager Flow* shown below as the source flow. The **Routing Profile**, *MutareH-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.

**Edit Flow: Session Manager Flow** X

Flow Name	<input type="text" value="Session Manager Flow"/>
SIP Server Profile	<input type="text" value="Session Manager"/> ▼
URI Group	<input type="text" value="*"/> ▼
Transport	<input type="text" value="*"/> ▼
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="PSTN-Signaling"/> ▼
Signaling Interface	<input type="text" value="SM-Signaling"/> ▼
Media Interface	<input type="text" value="SM-Media"/> ▼
Secondary Media Interface	<input type="text" value="None"/> ▼
End Point Policy Group	<input type="text" value="RTP-SRTP"/> ▼
Routing Profile	<input type="text" value="MutareH-Outbound"/> ▼
Topology Hiding Profile	<input type="text" value="Session Manager"/> ▼
Signaling Manipulation Script	<input type="text" value="None"/> ▼
Remote Branch Office	<input type="text" value="Any"/> ▼
Link Monitoring from Peer	<input checked="" type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input type="text"/>

**Finish**

## 6. 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 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.

### 6.1. Configure Voice Screening Proxy

This section covers the Voice Screening Proxy configuration.

#### 6.1.1. 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 (not shown).
- Specify the location of the TLS certificates.
- When responding with 302 Moved Temporarily, specify the Avaya Aura® network or PSTN domain in the Contact header for inbound and outbound calls, respectively. In the compliance test, Avaya Aura® network used *avaya.com* and the PSTN used *devcon.com*.

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

#### 6.1.2. Administer TLS Certificates

For the compliance test, two intermediate certificates and one CA certificate from Voice Screening Proxy were installed on SBC in **Section 5.9**. Voice Screening Proxy did not require a certificate for SBC as it trusted the SBC public IP address.

## 6.2. Enable SRTP on Voice CAPTCHA

Log into Voice CAPTCHA as root and set the **rtp\_secure\_media** to *optional* in **/etc/freeswitch/vars.xml.srtp** 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"/>
```

## 6.3. Administer Control Panel

Access the Mutare Voice web interface by using the URL “<http://<ip-address>>” in an Internet browser window, where *<ip-address>* is the IP address 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.

The screenshot displays the Mutare Voice Control Panel. At the top, a green banner indicates "Voice Traffic Filter is Enabled". The left sidebar shows the navigation menu with "Traffic Filter" selected. The main content area is titled "Control Panel" and includes a "No changes to apply" button and a "Cancel" button. Below this, the "Voice Traffic Filter" is shown as enabled, with a note that "VTF is enabled and handling calls." The "Threat Radar" section is also visible, showing "Volume Limiter", "Storm Detector", and "Spoof Radar" all set to "Drop". The "STIR/SHAKEN" section shows "C Attestation" and "Failed Validation" both set to "CAPTCHA Drop".

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

The screenshot shows the Mutare Voice Traffic Filter configuration interface. On the left, a call flow diagram shows 'C Attestation' leading to 'CAPTCHA Drop', 'Failed Validation' leading to 'CAPTCHA Drop', and 'Proprietary Dynamic DB' leading to 'CAPTCHA Drop'. Below this, an 'Outgoing Call Flow' diagram shows 'Outgoing calls' leading to 'Custom Rules' and then 'Various actions'. On the right, a list of custom rules is shown: 'STIR/SHAKEN' (enabled, using customized settings), 'Proprietary Dynamic Database' (enabled, sending callers to CAPTCHA), and 'CAPTCHA' (enabled, dropping callers that fail 3 times). Below the rules, there are sections for 'Auto-Fill Inbound Route' and 'Auto-Fill Outbound Route', both showing the route '78004@10.64.102.117'.

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.

The screenshot shows the 'Proprietary Dynamic Database Configuration' dialog. It has a title bar with a close button. The main content area has a section for 'Enabled' with a toggle switch turned on. Below this, there is a dropdown menu with 'Route callers' selected, followed by a 'to' label and a text input field containing '78004@10.64.102.117'. At the bottom, there are three buttons: 'Cancel', 'You have unsaved changes' (highlighted in red), and 'Done'.

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.

CAPTCHA Configuration

Enabled

Drop

callers that fail

3

times to enter the random

3

digit code within

5

secs.

Use System Default

Cancel

Done

CAPTCHA Configuration

Enabled

Route

callers that fail

3

times to enter the random

3

digit code within

5

secs.

Route to

78004@10.64.102.117

Use System Default

Cancel

Done

6.4. 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.

Mutare Voice

AdministrationAuto AttendantsTraffic FilterRitvin, Yuri

Custom Rules

AddImportCSV

Search rules

Filter	Enabled Rules	All Actions	All Directions	All Types	All Activity			
Enabled	Direction	Type	Action	Activity	From	To	Description	Updated
<input checked="" type="checkbox"/>	→ Outbound	Number	Allow	3320 • 3320 • 341	77361	+17324441001	DevConnect test	7 minutes ago



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 is on the whitelist and also in the robocall list, the call is allowed to complete.

← Add Inbound Number Rule

×

ⓘ

Editing a rule will not affect rule activity data.

×

✓

US +1

7324441001

✓

Number Type - To

All Recipients

✓

CAPTCHA Drop

calls from phone number [ +17324441001 ] to All Recipients

✓

test

Enabled

Cancel

Add Inbound Rule

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.

## → Add Outbound Number Rule



Editing a rule will not affect rule activity data.



Non-standard ▼ 77301



Number Type - To ▼ All Recipients



**Route** ▼ calls from phone number [ 77301 ] to All Recipients

to 41501@10.64.102.90



test

☒ Enabled

Cancel

Add Outbound Rule

## 7. Verification Steps

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

1. 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.

Device: SBCE ▾

Help

### Status

AVAYA

Server Status

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Mutare Hosted			5061	TLS	UP	UNKNOWN	11/17/2023 09:25:46 EST
PSTN-SIP	10.64.101.100	10.64.101.100	5060	UDP	UP	UNKNOWN	11/14/2023 07:12:09 EST
Mutare On-Prem	10.64.102.145	10.64.102.145	5061	TLS	UP	UNKNOWN	11/15/2023 10:26:40 EST

2. Configure custom rules to analyze inbound and outbound calls.
3. Place inbound and outbound PSTN calls and verify that the appropriate call treatment was applied.
4. Verify that **Call History Report** reflects that the appropriate action was taken. A sample **Call History Report** is shown below.

Mutare Voice™

Administration ▾ Auto Attendants ▾ Traffic Filter ▾ Riltvin, Yuri ▾

### Call History Report

Search for Caller ID, Called Number 🔍 More Filters CSV JSON

Calls from Today

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		<a href="#">Add Rule</a>
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		

12:49 PM CST - v3.6.1.0

## 8. Conclusion

These Application Notes described the configuration steps required for Mutare Voice Traffic Filter to interoperate with Avaya Session Border Controller using a hosted deployment. All test cases were completed successfully.

## 9. Additional References

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

- [1] *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 5, October 2023, available at <http://support.avaya.com>.
- [2] *Mutare Voice Traffic Filter Admin Guide*, Version 3.6.0, April 7, 2023.

## 10. 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 6.1.1**.

```
alias=<ScreeningProxyPublicIP>

#-----
#For UDP connection the section below is unremarked
listen=udp: <ScreeningProxyPrivateIP> :5060
children=32

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

listen=tls: <ScreeningProxyPrivateIP>:5061

listen=hep_udp:<ScreeningProxyPrivateIP>:9060
listen=hep_tcp:<ScreeningProxyPrivateIP>:9060

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

##### 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:<ScreeningProxyPrivateIP>")
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=<ScreeningProxyPublicIP>: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:<ScreeningProxyPrivateIP>:5060")
```

```

modparam("dispatcher", "ds_probing_mode", 1)
modparam("dispatcher", "ds_probing_list", "2")
modparam("dispatcher", "ds_probing_threshold", 1)
modparam("dispatcher", "options_reply_codes", "404")

                                ooo

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

route[redirection] {
    if ($fd == "avaya.com") {
        $rd = "devcon.com";
    } else {
        $rd = "avaya.com";
    }
    xlog("$ci | Call from $fU to $rU in route [redirection]. The '302' contact host
is set to $rd\n");
    remove_hf("Contact");
    remove_hf("X-captcha*", "g");
    remove_hf("X-cid*", "g");
    t_reply("302", "Moved temporarily");
    exit;
}

```

---

**©2024 Avaya LLC. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).