SIPREC Configuration Guide

Avaya Aura Communication Manager and Session Manager with Avaya Session Border Controller for Enterprise

December 2022

Document History

Rev. No.	Date	Description
1.0	December 19, 2022	SIPREC- Configuration Guide

Table of Contents

Table of Figures

1 Audience

This document is intended for technical staff and Value Added Resellers (VAR) with installation and operational responsibilities. This configuration guide provides steps for configuring **SIPREC** using **Avaya Aura Communication Manager (Avaya Aura CM), Avaya Aura Session Manager (Avaya Aura SM)** with **Avaya Session Border Controller for Enterprise (Avaya SBCE)** to connect to **Amazon Chime SDK Voice Connector** for streaming audio to Amazon Kinesis Video Streams (KVS).

The information in this document is for informational purposes only. AWS does not guarantee the accuracy of this document and AWS has no responsibility or liability for errors or omissions related to this document. The document is subject to change without notice and should not be construed as a commitment by AWS.

1.1 Amazon Chime SDK Voice Connector

Amazon Chime SDK Voice Connector is a pay-as-you-go service that enables companies to make or receive secure phone calls over the internet or AWS Direct Connect using their existing telephone system or session border controller (SBC). The service has no upfront fees, elastically scales based on demand, supports calling both landline and mobile phone numbers in over 100 countries, and gives customers the option to enable inbound calling, outbound calling, or both.

Amazon Chime SDK Voice Connector uses the industry-standard Session Initiation Protocol (SIP). Amazon Chime SDK Voice Connector does not require dedicated data circuits. A company can use their existing Internet connection or AWS Direct Connect public virtual interface for SIP connectivity to AWS. Voice connectors can be configured in minutes using the AWS Management Console or Amazon Chime API. Amazon Chime SDK Voice Connector offers cost-effective rates for inbound and outbound calls. Calls into Amazon Chime meetings, as well as calls to other Amazon Chime SDK Voice Connector customers are at no additional cost. With Amazon Chime SDK Voice Connector, companies can reduce their voice calling costs without having to replace their on-premises phone system.

2 SIP Trunking Network Components

The network for the SIP trunk reference configuration is illustrated below and is representative of Avaya Aura CM and Avaya Aura SM with Avaya SBCE configuration.

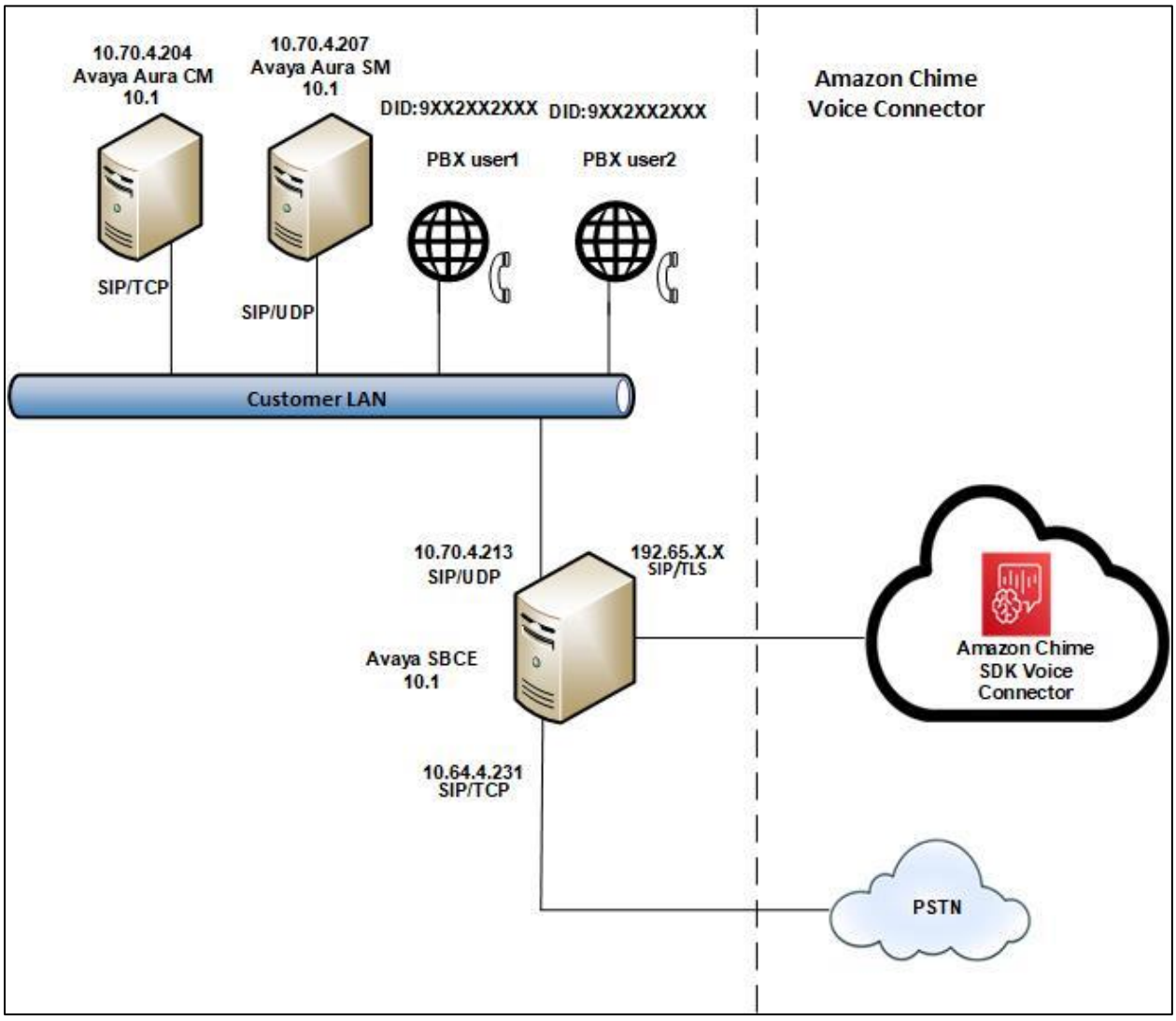

Figure 1 Network Topology

2.1 Hardware Components

- UCS-C240 VMWare server running ESXi 6.0 or later used for the following virtual machines
    - Avaya Aura
        - Communication Manager
        - Session Manager
- Avaya SBCE running on UCS-C240-Virtual Machine
- Avaya one-X IP Phone(s)– 9641G

2.2 Software Requirements

- Avaya Aura
    - Communication Manager: 10.1
    - Session Manager: 10.1
    - System Manager: 10.1
- Avaya Session Border Controller for Enterprise : 10.1.0.0-32-21432

3 Features

3.1 Features Supported

- SIPREC

3.2 Features Not Supported

- None

3.3 Features Not Tested

- None

3.4 Caveats and Limitations

- Amazon Chime SDK Voice Connector uses E164 numbering format for SIP Trunking Service, Signaling Manipulation rule is used to modify the Request URI towards SIP recorder.
- Avaya SBCE is violating the RFC while constructing the UPDATE and BYE towards the SIP Recorder, Avaya provided the Hotfix (sbce-10.1.0.0-34-21958-hotfix-05192022) to resolve the issue.

4 Configuration

The specific values listed in this guide are used in the lab configuration described in this document and are for illustrative purposes only. You must obtain and use the appropriate values for your deployment. Encryption is always recommended if supported.

4.1 Configuration Checklist

In this section we present an overview of the steps that are required to configure **Avaya Aura CM, Avaya Aura SM and Avaya SBCE** for SIP Trunking with **Amazon Chime SDK Voice Connector.**

Steps	Description	Reference
Step 1	Avaya Aura CM Configuration	Section 4.2
Step 2	Avaya Aura SM Configuration	Section 4.3
Step 3	Avaya SBCE Configuration	Section 4.4

Table 1 – PBX Configuration Steps

4.2 Avaya Aura CM Configuration

This section with screen shots taken from Avaya Aura CM used for the interoperability testing gives a general overview of the PBX configuration.

4.2.1 Avaya Aura CM Login

- Avaya Aura CM configuration is done via SAT simulator through PuTTY.
- Log in using an appropriate User ID and Password.

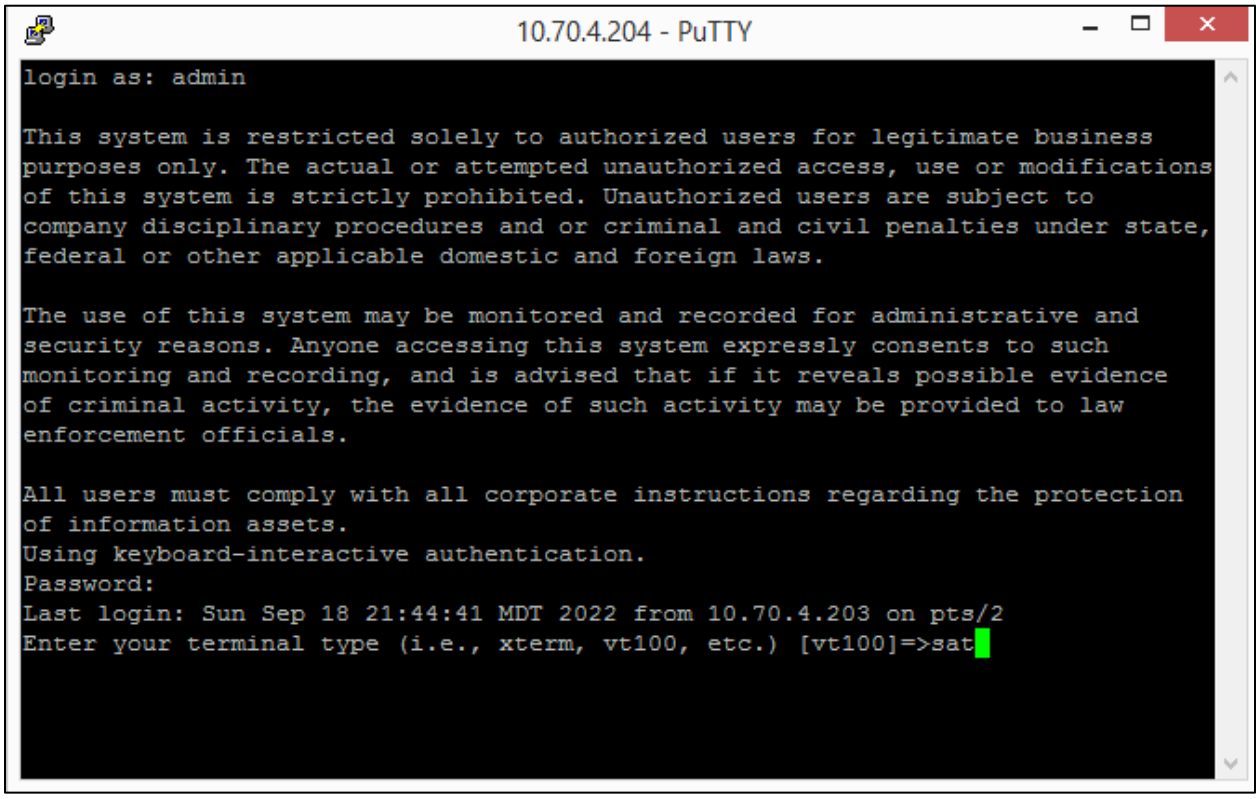

Figure 2: Avaya Aura CM login

4.2.2 IP Node Name

- Use the **Change node-names ip** command to verify that node names are defined for Avaya Aura CM (**procr**) and Session Manager (**AASM10**). The node names are needed for configuring the Signaling Group.

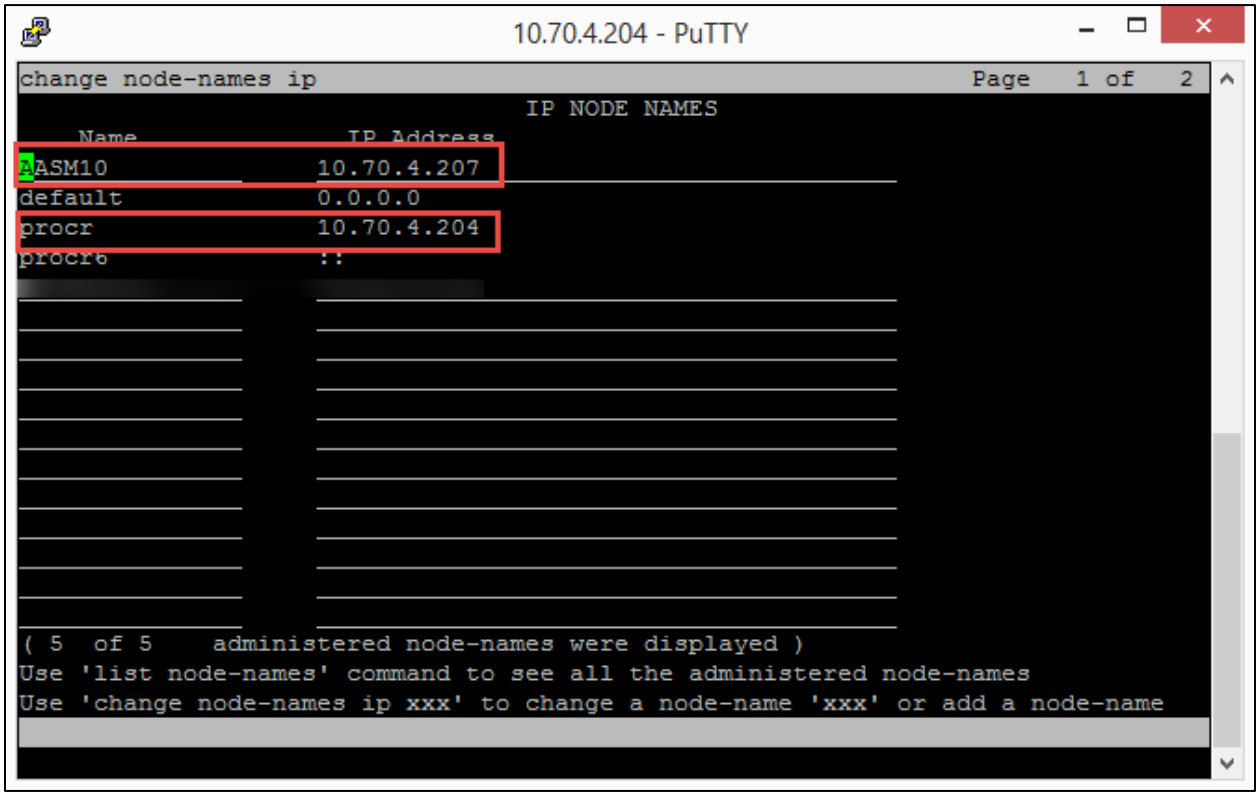

Figure 3 IP Node Name

4.2.1 IP Codec Set

- Use **change ip-codec-set 2** to define list of codecs for calls between Avaya Aura CM and SM.

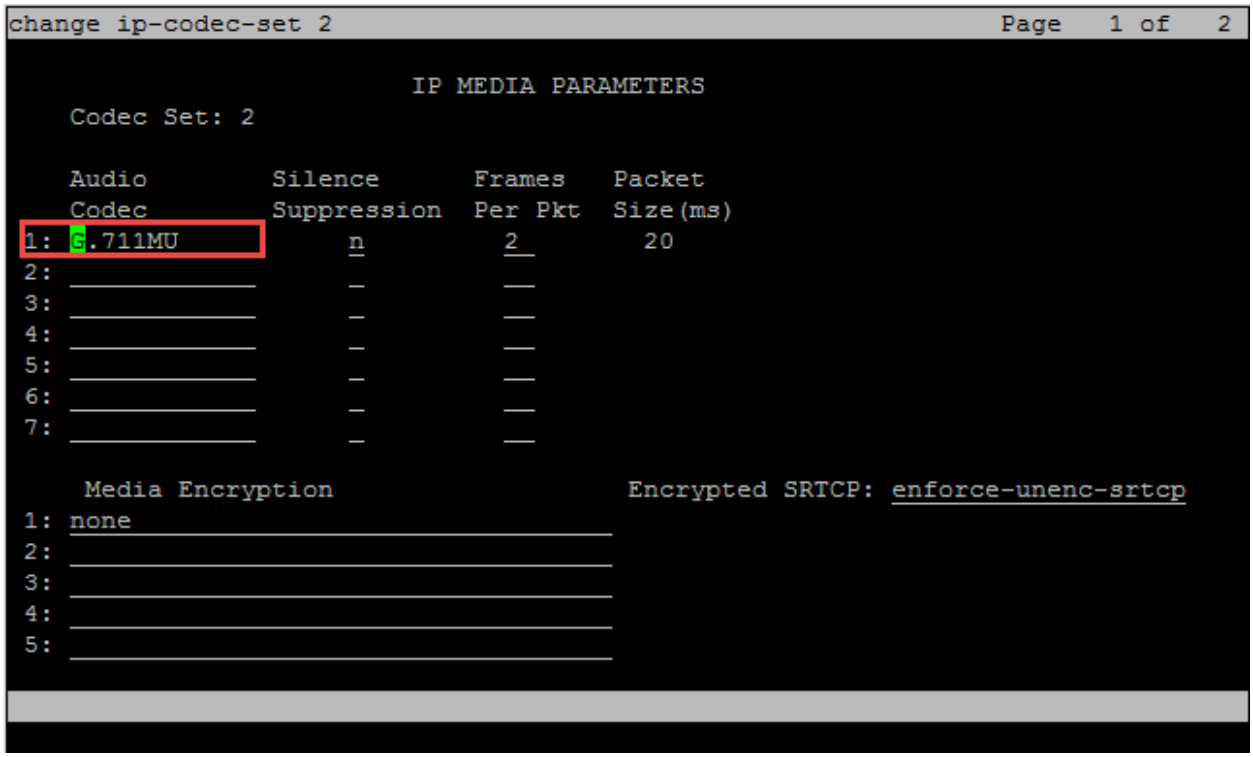

Figure 4 IP Codec Set

4.2.2 IP Network Region

- Use **change ip-network-region 2** to define the network region
- *Authoritative Domain*: Domain name **lab.XXXXXXXX.com**
- *Codec Set*: Enter codec set **2** created in Section 4.2.1
- *Intra-region IP-IP Direct Audio*: **yes**
- *Intra-region IP-IP Direct Audio*: **yes**

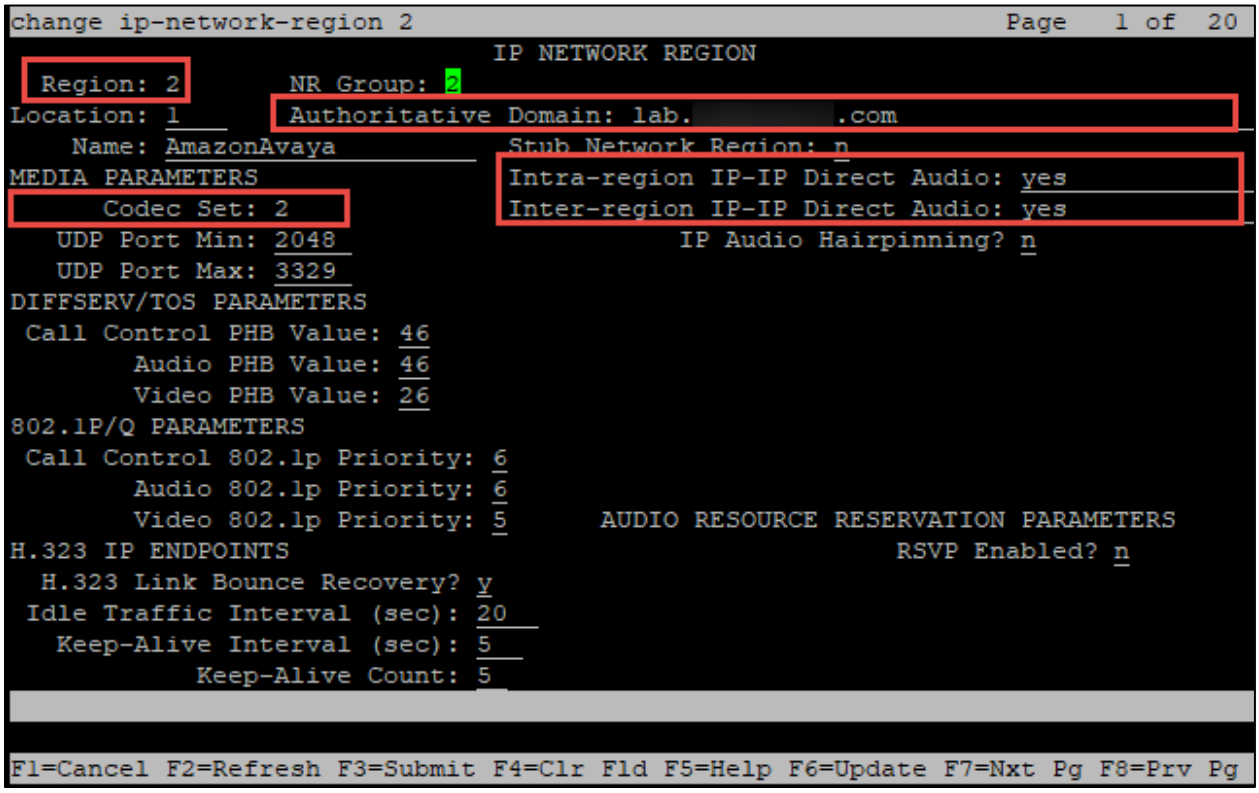

Figure 5 IP Network Region

4.2.3 Signaling Group

- Command **add signaling group 1** was used to create Signaling Group. Use **change signaling group 1** to modify existing signaling group.
- Set *Group Type*: **sip**
- Set *Transport Method*: **tcp**
- Set *Peer Detection Enable*: **y**
- Set *Near-end Node Name*: **procr**
- Set *Near-end Listen Port*: **5060**
- Set *Far-end Node Name*: **AASM10**
- Set *Far-end Listen Port*: **5060**
- Set *Far-end Network Region*: **2**
- Set *Far-end Domain*: **lab.xxxxxxxx.com**
- Set *DTMF over IP*: **rtp-payload**
- Set *Direct IP-IP Audio Connections*: **n**
- Leave other fields to default value

```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1                    Group Type: sip
  IMS Enabled? n                  Transport Method: tcp
       Q-SIP? n
    IP Video? n                                          Enforce SIPS URI for SRTP? n
 Peer Detection Enabled? y  Peer Server: SM                                Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: AASM10
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain: lab.        .com
                                                  Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                     RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload                Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                        IP Audio Hairpinning? n
         Enable Layer 3 Test? y                 Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? y          Alternate Route Timer(sec): 6

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 6 Signaling Group

4.2.4 Trunk Groups

- Trunk group **1**is used for trunk to Avaya SM. Command **add trunk group 1** is used to create Trunk Group. Use **change trunk group 1** to modify existing trunk group.
- Set *Group Type*: **sip**
- Set *Group Name*: **SIP Trunk**
- Set *TAC*: **#001**
- Set *Direction*: **two-way**
- Set *Service Type*: **tie**
- Set *Member Assignment Method*: **auto**
- Set *Signaling Group*: **1** (created in section 4.2.3)
- Set *Number of Members*: **10**

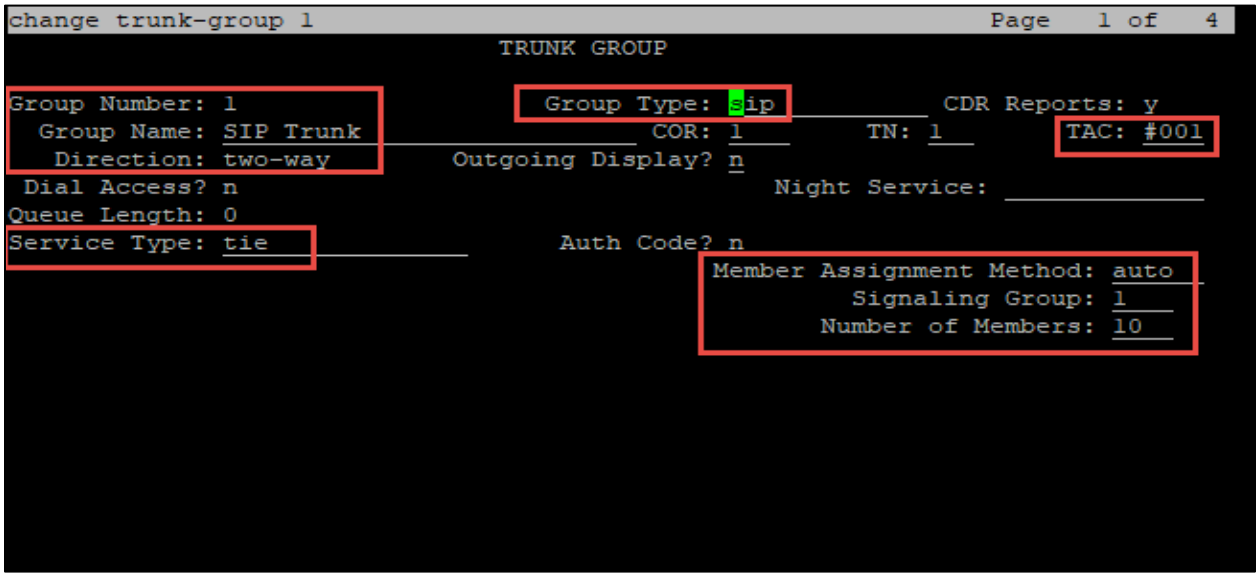

Figure 7 Trunk Group

- Set *Preferred Minimum Session Refresh Internal (sec)*: **900**

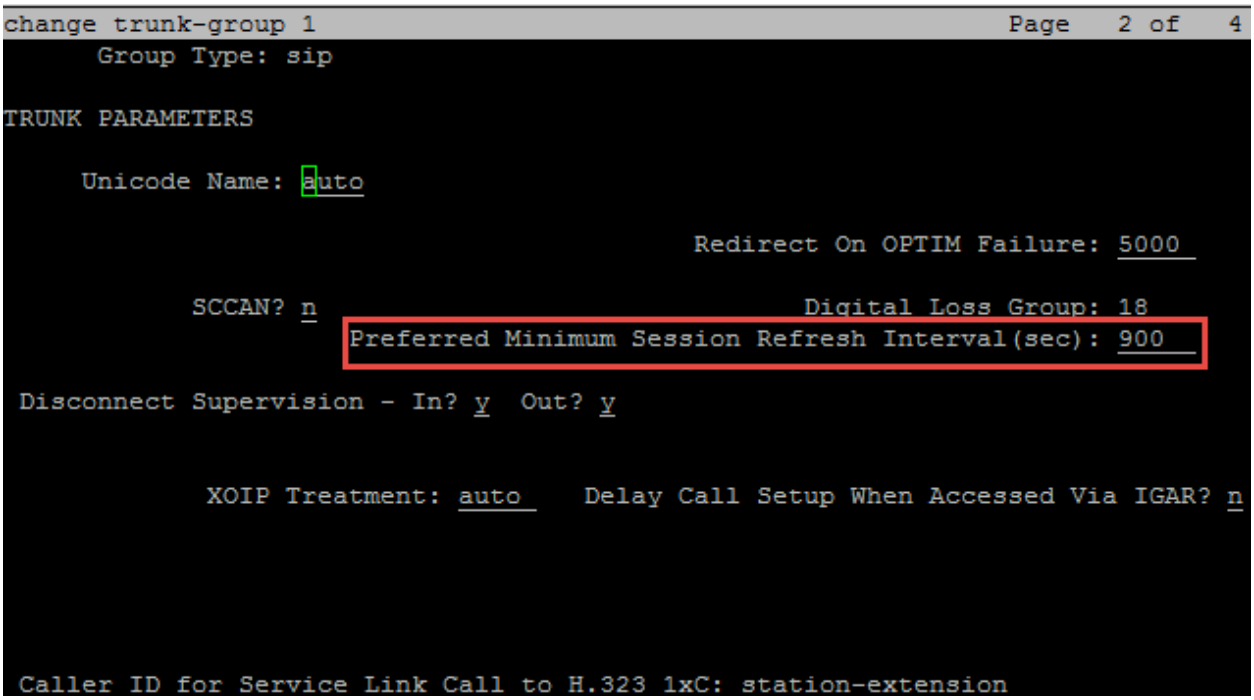

Figure 8 Trunk Group Continuation

- Set *Numbering Format*: **Public**
- Set *Replace Restricted Numbers*: **yes**

```
change trunk-group 1                                          Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y


   Suppress # Outpulsing? n  Numbering Format: public
                                                UUI Treatment: service-provider
                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y
```

Figure 9 Trunk Group Continuation

- Set *Telephone Event payload Type*: **101**
- Set *Identity for calling Party Display*: **From**
- Leave all other fields to default values

```
change trunk-group 1                                          Page   4 of   4
                              PROTOCOL VARIATIONS

                                        Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                          Send Transferring Party Information? y
                                  Network Call Redirection? n

                                    Send Diversion Header? y
                                  Support Request History? y
                             Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
     Resend Display UPDATE Once on Receipt of 481 Response? n
                        Identity for Calling Party Display: From
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
          Enable Q-SIP? n
          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                  Request URI Contents: may-have-extra-digits
```

Figure 10 Trunk Group Continuation

4.2.5 Route Pattern

- Use **change-route-pattern x** command to specify the routing preference. Route pattern **1** is used for SIP trunk to Avaya SM.
- Set *Pattern Name*: **to AASM10**
- Set *Grp No*: **1** (created in Section 4.2.4)
- Set *FRL*: **0**
- Set *Numbering Format*: **unk-unk**
- Leave all other fields to default values

```
change route-pattern 1                                          Page   1 of   4
                 Pattern Number: 1      Pattern Name: to AASM10
   SCCAN? n    Secure SIP? n     Used for SIP stations? n

   Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
   No          Mrk Lmt List Del  Digits                          QSIG
                                 Dgts                            Intw
1: 1    0                                                        n    user
2:                                                               n    user
3:                                                               n    user
4:                                                               n    user
5:                                                               n    user
6:                                                               n    user

    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W    Request                               Dgts Format
1: y y y y y n  n           rest                                 unk-unk   none
2: y y y y y n  n           rest                                           none
3: y y y y y n  n           rest                                           none
4: y y y y y n  n           rest                                           none
5: y y y y y n  n           rest                                           none
6: y y y y y n  n           rest                                           none
```

Figure 11 Route Pattern

4.2.6 Outbound Call Routing

- For outbound call to PSTN through Amazon Chime SDK Voice Connector SIP trunking, Automatic Route Selection (ARS) is used. Use command **change ars analysis x** to configure the routing table.
- Set *Dialed String*: **214242**
- Set *Min*: **10**
- Set *Max*: **12**
- Set *Route Pattern*: **1** (created in section 4.2.5)
- Set *Call Type*: **natl**

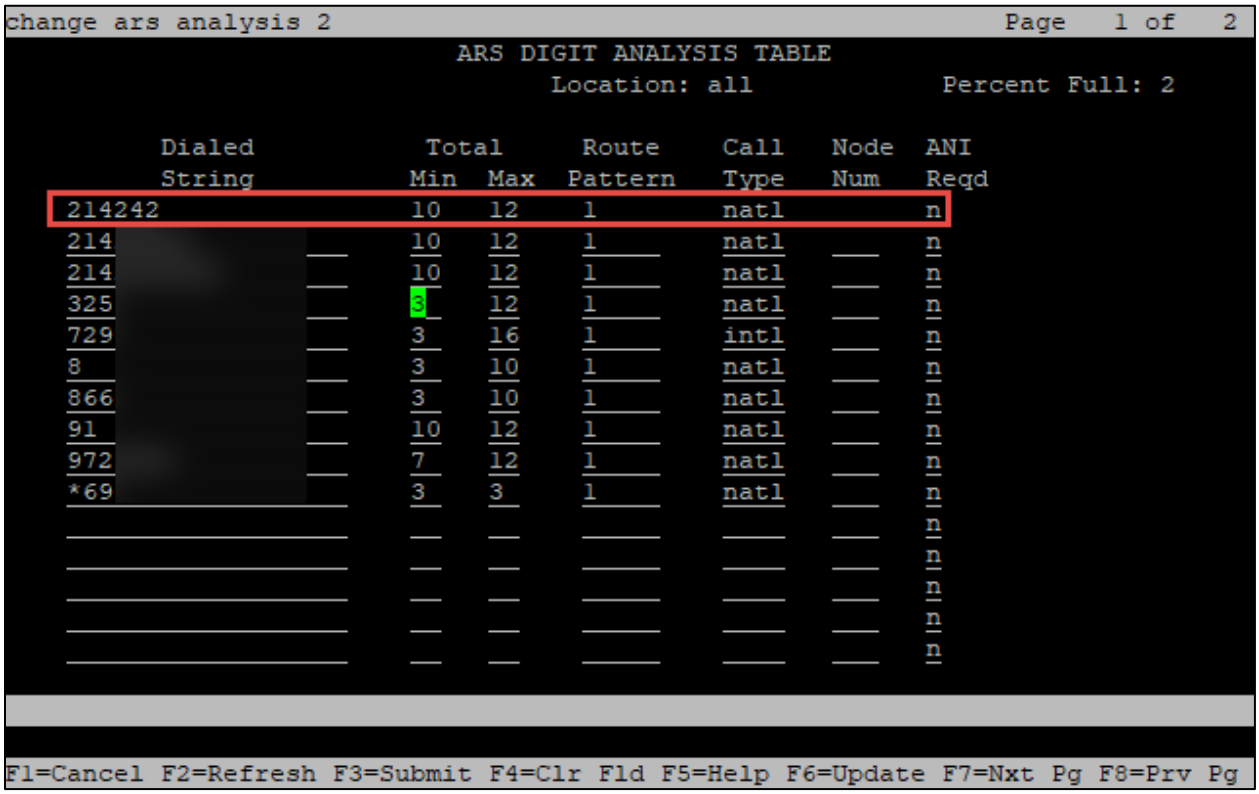

Figure 12 Outbound Call Routing

4.2.7 Outbound Caller ID

- Amazon Chime SDK Voice Connector SIP Trunk requires E164 Caller ID for outbound calls. Command **change public-unknown-number x** is used to configure the outbound caller ID for Extensions.
- Set *EXT Len*: **4**
- Set *EXT Code*: **2923**
- Set *Trk Grp*: **1** (created in section 4.2.4)
- Set *CPN Prefix*: **97XXXXXXXX.** (Replace XXXXXXXX with the numbers to be prefixed)
- Set *Total CPN Len*: **10**

```
change public-unknown-numbering 1                          Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                                 Total
Ext  Ext             Trk        CPN              CPN
Len  Code            Grp(s)     Prefix           Len
                                                    Total Administered: 5
 4   2000            5          97259            10    Maximum Entries: 240
 4   2005            1          04320            10
 4   2501            1          97259            10 Note: If an entry applies to
 4   2923            1          97259            10 a SIP connection to Avaya
 4   5992            1          91927            10 Aura(R) Session Manager,
                                                    the resulting number must
                                                    be a complete E.164 number.

                                                    Communication Manager
                                                    automatically inserts
                                                    a '+' digit in this case.

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 13 Outbound Caller ID

4.2.8 Inbound Call Routing

- For Inbound call to Avaya PBX from PSTN through Amazon Chime SDK Voice Connector SIP trunking, inc-call-handling-trmt-trunk-group is used. Use command **change inc-call-handling-trmt trunk-group x** to configure the routing table.
- Set *Number Len*: 10
- Set *Number Digits*:**9725XXXXXXX**
- Set *Del*: 10

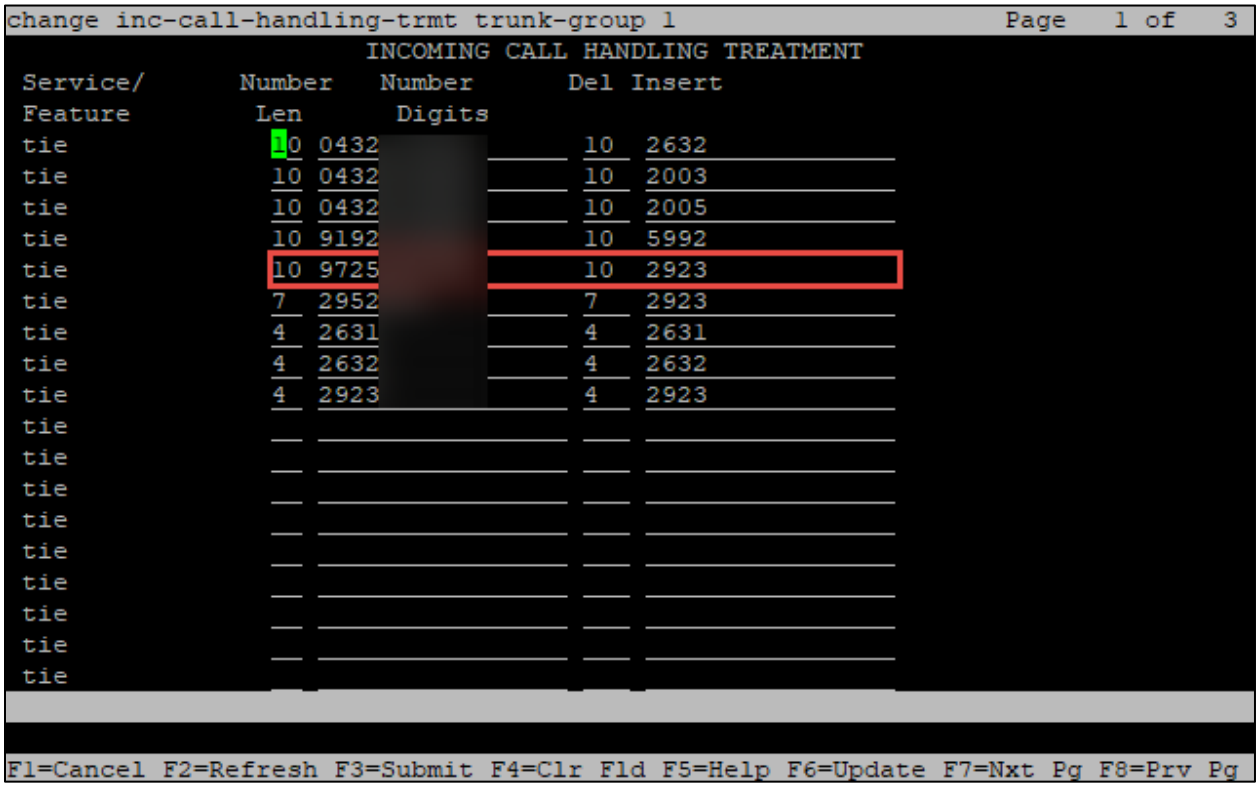

Figure 14 Inbound call routing

4.3 Avaya Aura Session Manager Configuration

4.3.1 Avaya Aura SM login

- Avaya Aura Session Manager Configuration is accomplished through the Avaya Aura System Manager
- Access Avaya Aura System Manager Web login screen via **https://<IP Address/FQDN>**
- Enter the login credentials
- Click **Log On**

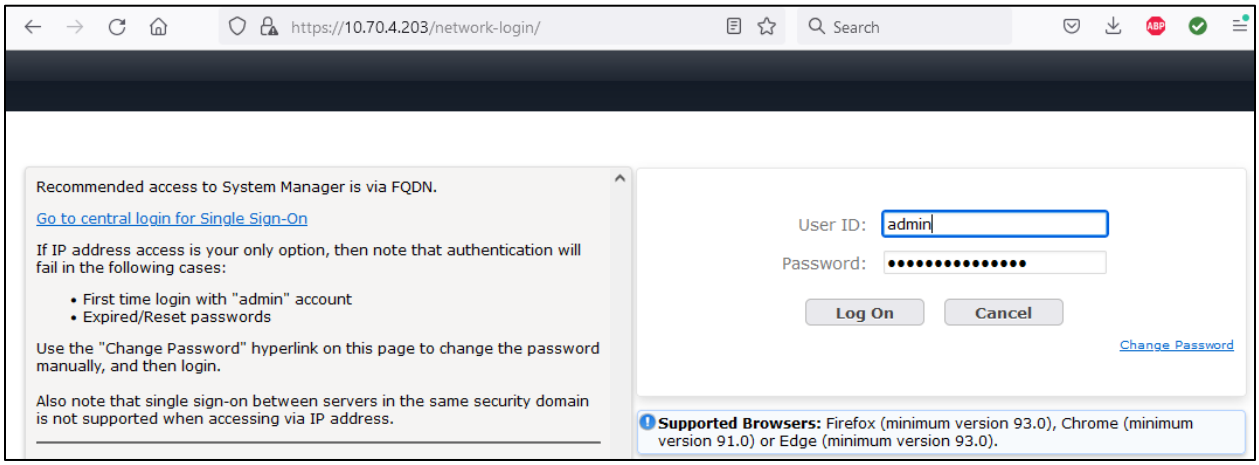

Figure 15 Avaya Aura SM login

4.3.2 Domain

- Navigate to **Elements** > **Routing**

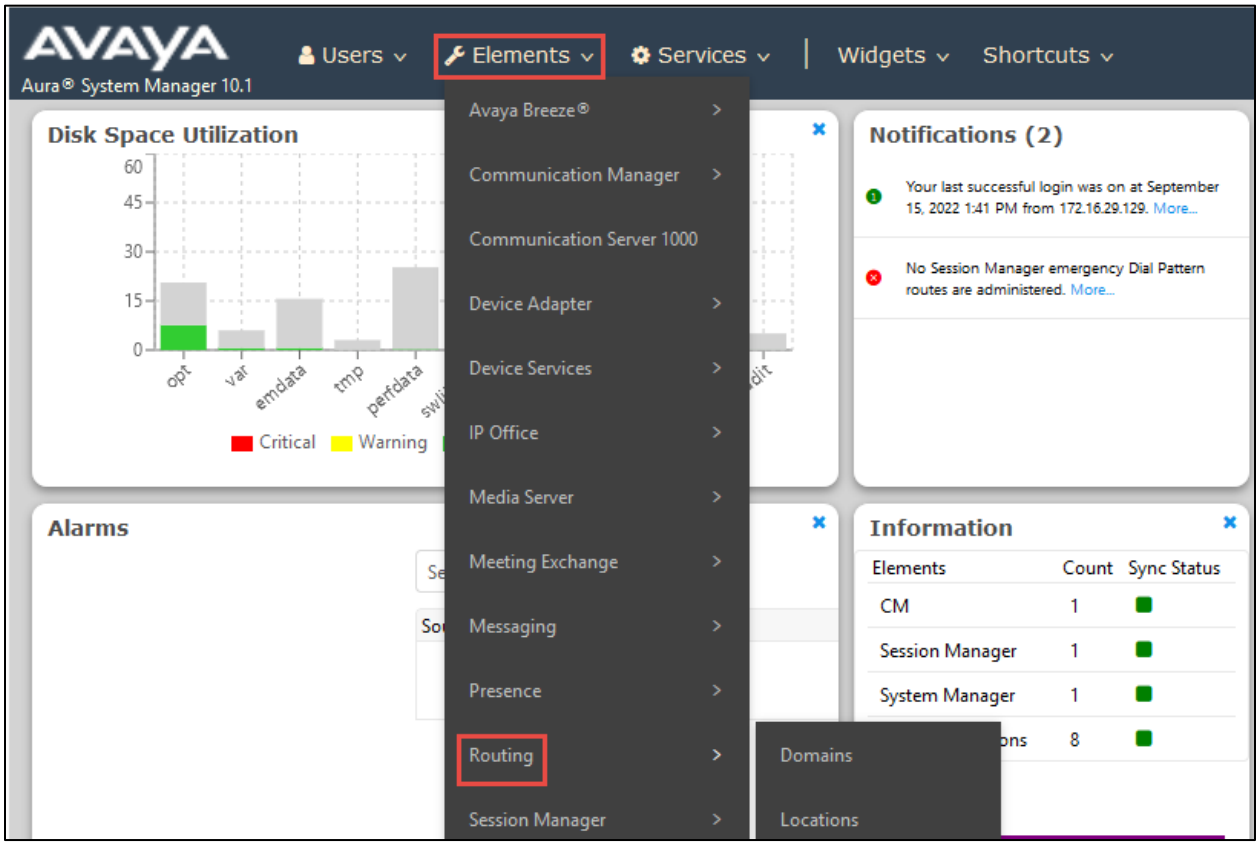

Figure 16 Routing

- Navigate to **Routing** > **Domains**
- Click **New**

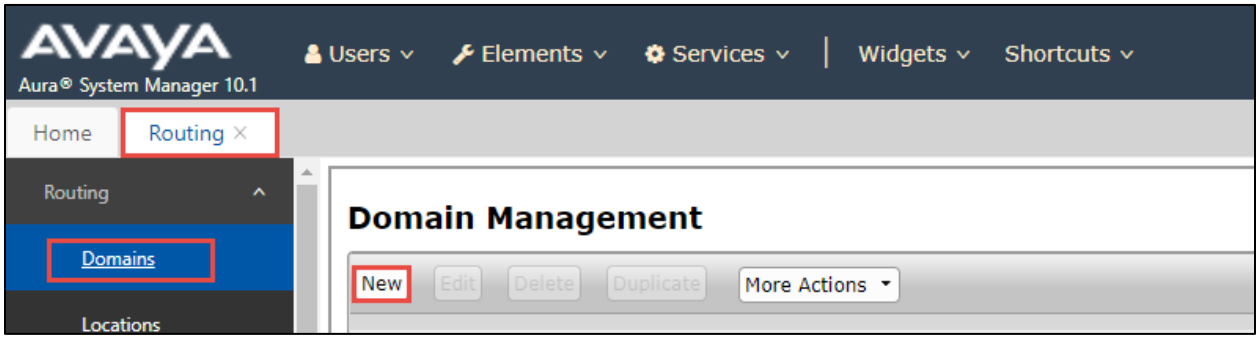

Figure 17 Add Domain

Set *Name*: Enter the domain name of Avaya Aura PBX, **lab.XXXXXXX.com**

- Set *Type*: **sip**
- Click **Commit**

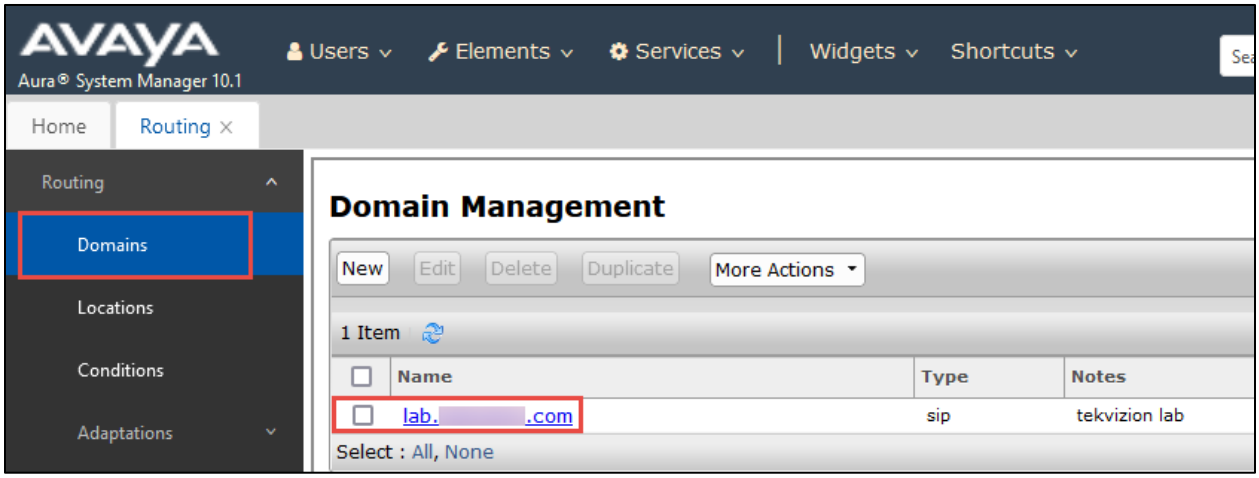

Figure 18 Domain

4.3.3 Locations

- Navigate to **Routing > Locations**
- Select **New**

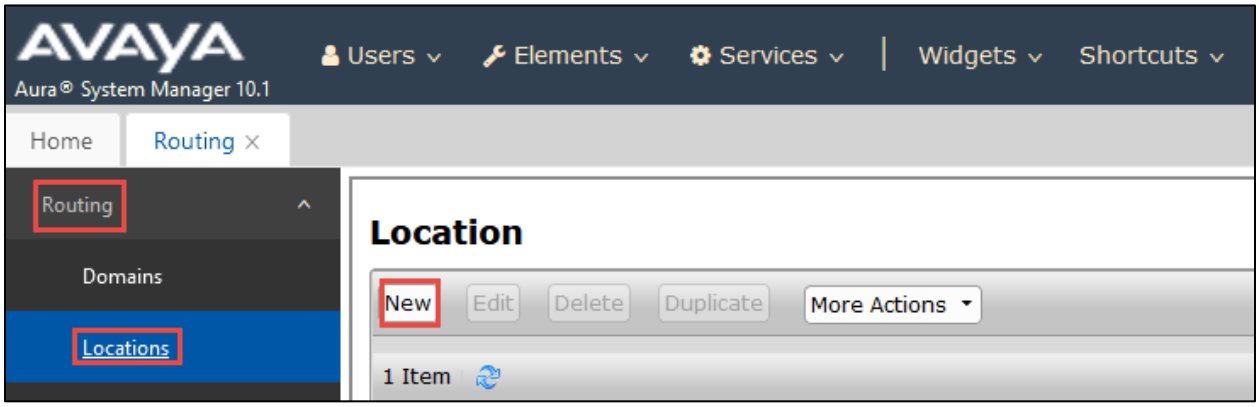

Figure 19 Locations

- Set *Name*: **Plano**

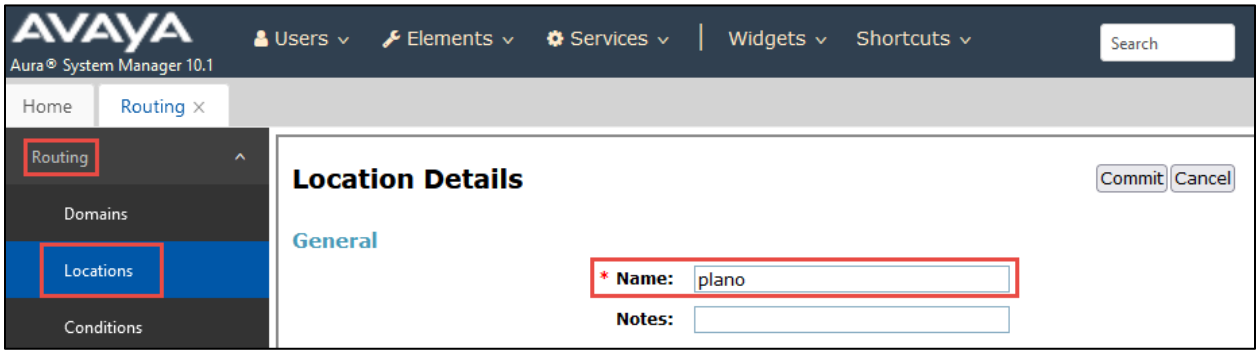

Figure 20 Locations continuation

- Under *Location Pattern*, select **Add** to add **IP Address** Patterns for different networks that communicates within the location
- Set *IP Address Pattern*: **10.70.4.***
- Leave all other fields to default values
- Click **Commit**

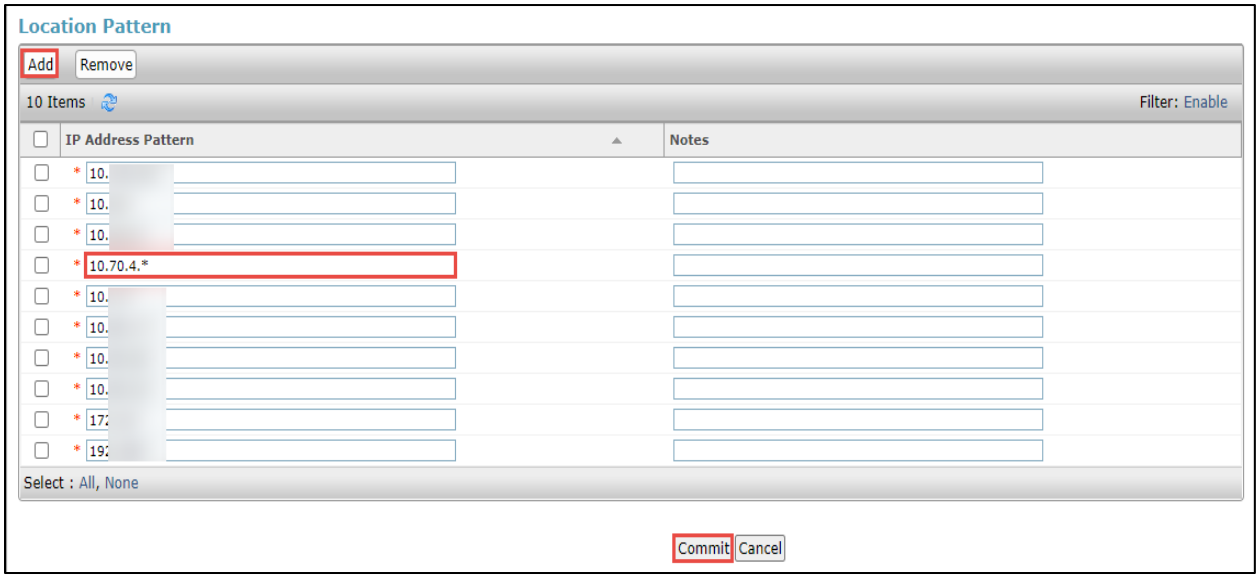

Figure 21 Locations continuation

4.3.4 Adaptations

- Amazon Chime SDK Voice Connector uses E164 numbering format for SIP Trunking Service. Adaptation was created at the Session Manager to manipulate the digits sent to Amazon network via Avaya Session Border Controller for Enterprise (Avaya SBCE).
- Navigate to **Routing > Adaptations**. Click **New**
- Set *Adaptation Name*: **Adapter for SBC**
- Set *Module Name*: **DigitConversionAdapter**
- Set *Module Parameter Type*: **Name-Value Parameter** is selected from the drop down, Click **Add**
- Set *Name/Value*: **fromto/true**
- Set *Name/Value*: **odstd/10.70.4.213** (Avaya SBCE LAN IP is entered)
- Set *Name/Value*: **osrcd/10.70.4.207** (Avaya Aura SM IP is entered)
- Under **Digit Conversion for Incoming Calls to SM**, click **Add**

Matching Pattern	Min/Max	Delete Digits	Insert Digits	Address to Modify
972598	**10/36**	**10** – Deletes	2923	Destination – Modifies digits in **TO** header and sends it to Avaya CM

Figure 22 Digit Conversion to Avaya CM

- Under **Digit Conversion for Outgoing Calls from SM**, click **Add**

Matching Pattern	Min/Max	Delete Digits	Insert Digits	Address to Modify
214242	**10/36**	**0**	**+1** – Insert **+1** in front of 214242 patterns	Destination – Modifies the digits in **TO** header and sends it to Amazon

Figure 23 Digit Conversion to Amazon

- Leave all other fields at default values
- Click **Commit**

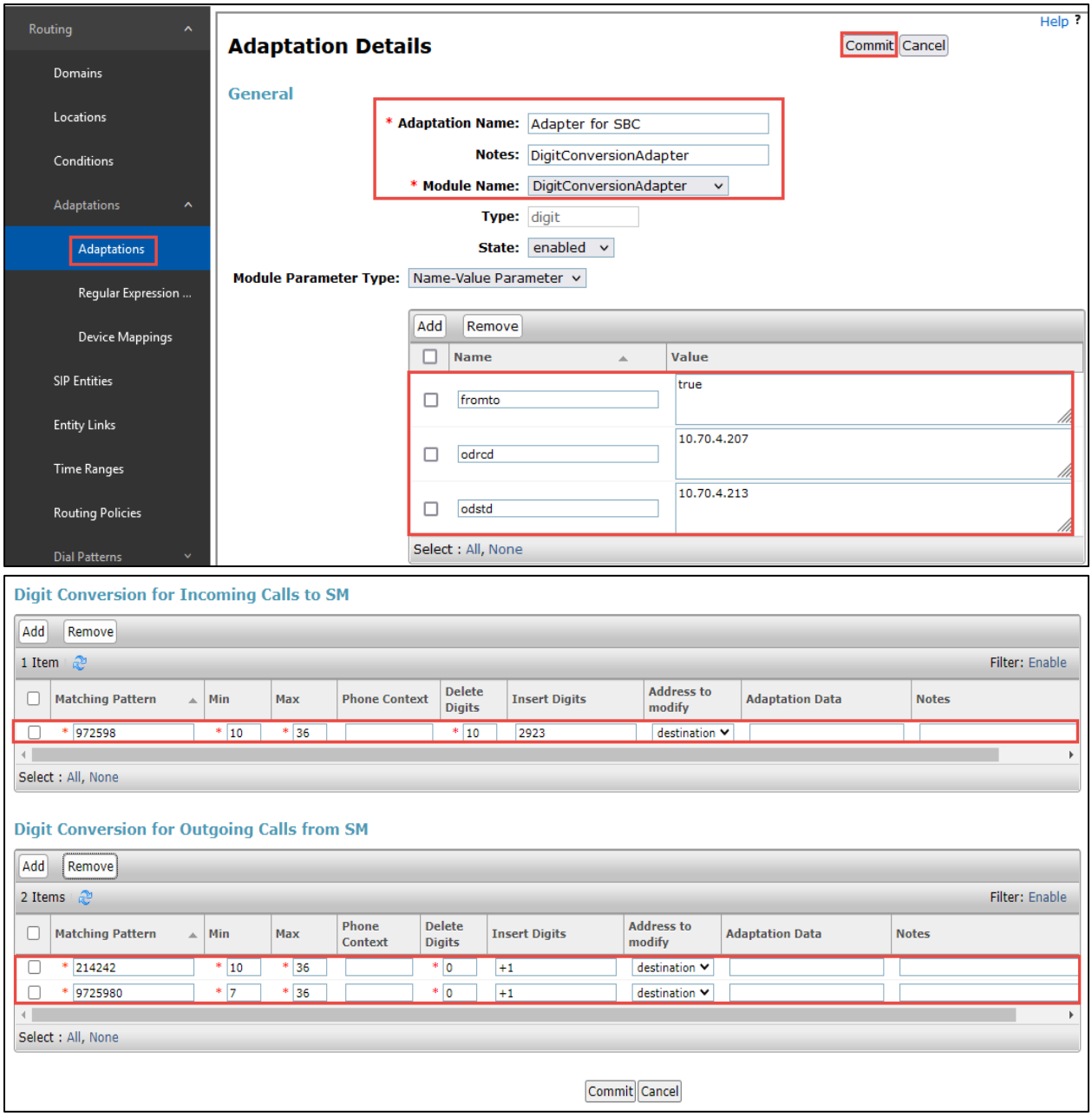

Figure 24 Adaptation for Amazon

4.3.5 SIP Entities and Entity Links

SIP Entity for Avaya Aura Session Manager

- Navigate to: **Routing > SIP Entities**. Click **New**
- Set *Name*: Enter name of the host, **AASM10**
- Set *FQDN or IP Address*: Enter the **SIP address** of the **Session Manager**
- Set *Type*: **Session Manager** is selected from the drop down
- Set *Location*: Select the **location** (created in Section 4.4.3)
- Set *TCP/TLS Failover Port*: **5060/5061**
- Click **Add** to assign Domain **lab.xxxxxxxx.com** for the following Ports and Protocols
- Port **5060** and Protocol **TCP/UDP**
- Port **5061** and Protocol **TLS**
- Click **Commit**

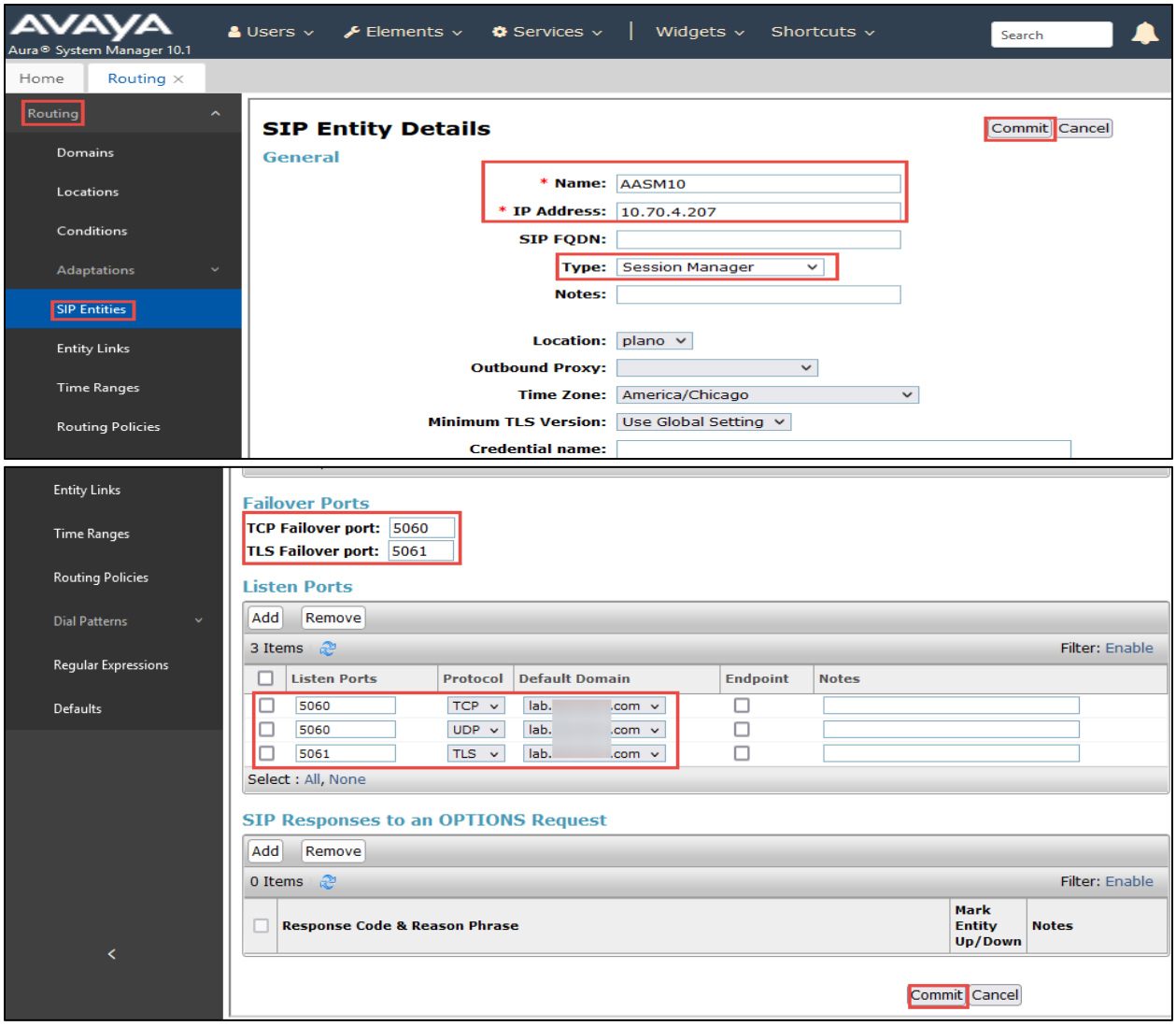

Figure 25 SIP Entity for Avaya SM

SIP Entity and Entity Links for Avaya Aura Communication Manager

- Set *Name*: **AACM10**
- Set *FQDN or IP Address*: Enter the **IP address** of **Avaya Aura Communication Manager**
- Set *Type*: **CM**
- Click **Commit**

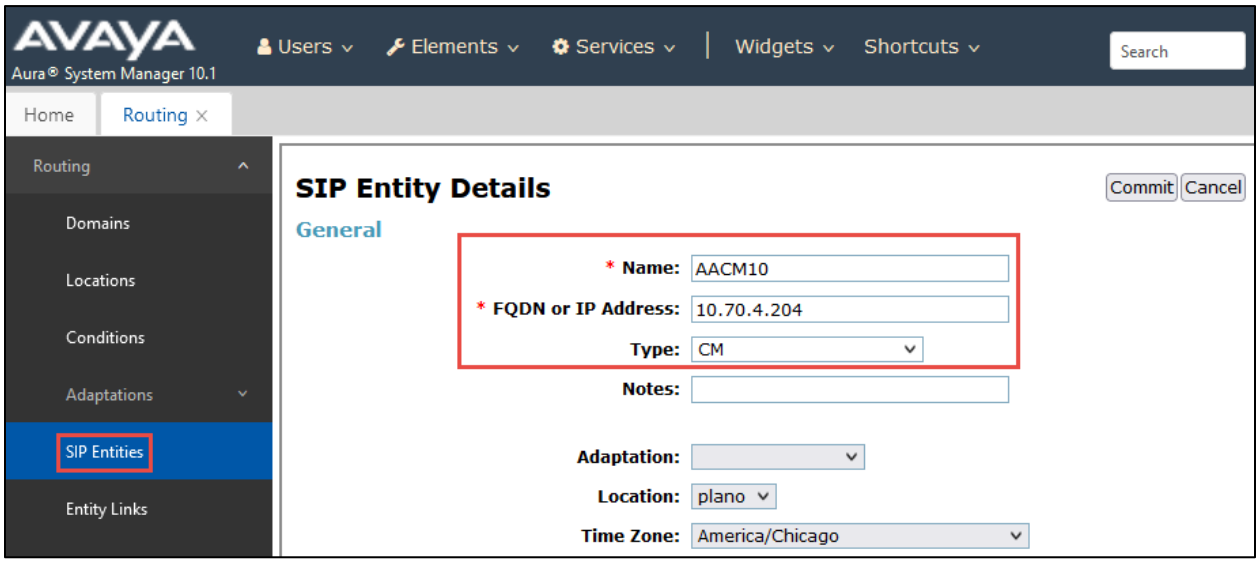

Figure 26 SIP Entity and Entity Links for Avaya CM

- Under *Entity Links*, Click **New**

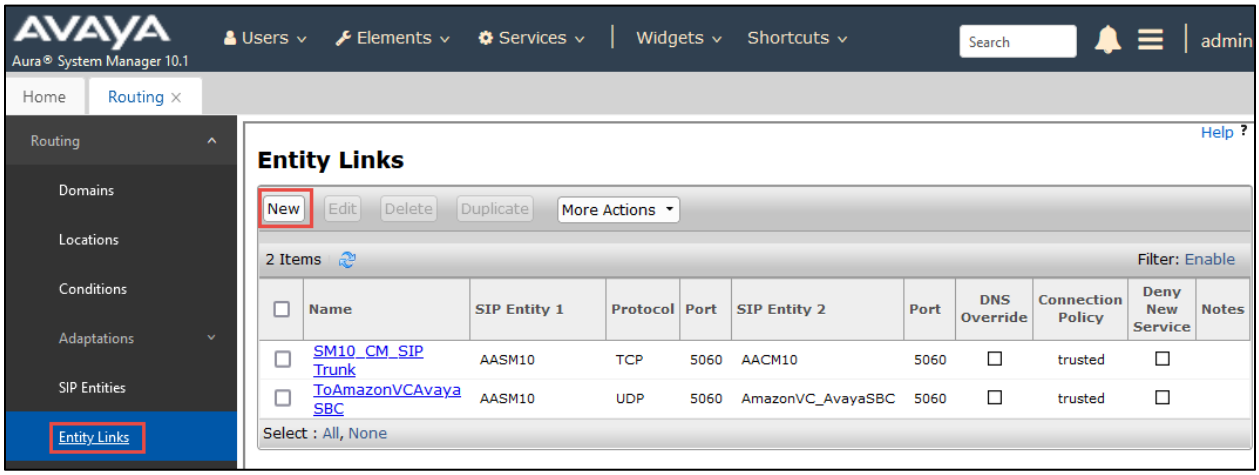

Figure 27 SIP Entity and Entity Links for Avaya CM continuation

- Set *Name*: **SM10_CM_SIP Trunk**
- Set *SIP Entity 1*: Select the SIP entity **AASM10**
- Set *SIP Entity 2*: **AACM10**
- Set *Protocol*: **TCP**
- Set *Ports*: **5060**
- Set *Connection Policy*: **trusted**
- Leave all other fields to default values
- Click **Commit**

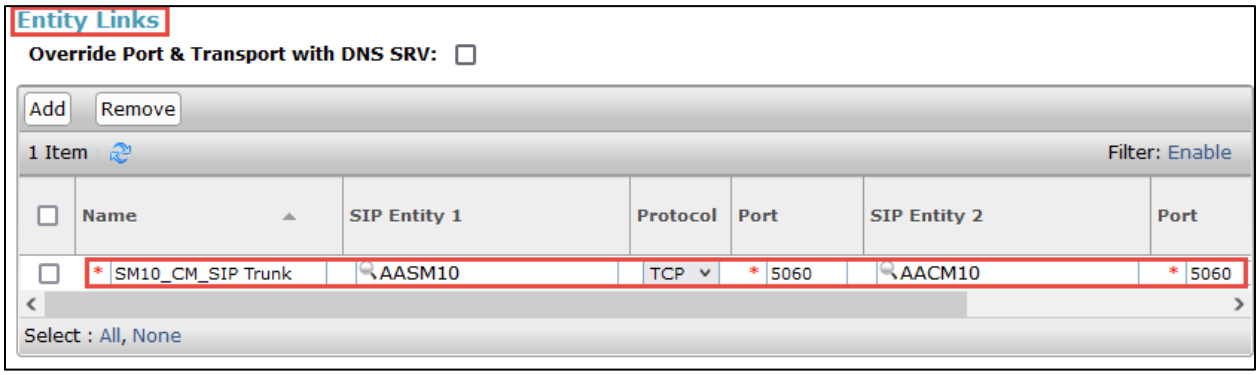

Figure 28 SIP Entity and Entity Link for Avaya CM continuation

SIP Entity and Entity Links for Avaya SBCE

- Set *Name*: **AmazonVC_AvayaSBC**
- Set *FQDN or IP Address*: Enter the **IP address** of **Avaya SBCE** interface facing Avaya Aura SM
- Set *Adaptation*: Select the **Adaptation** for Avaya SBCE configured in Section 4.3.4
- Set *Location*: Select the **location** created in Section 4.3.3
- Click **Commit**

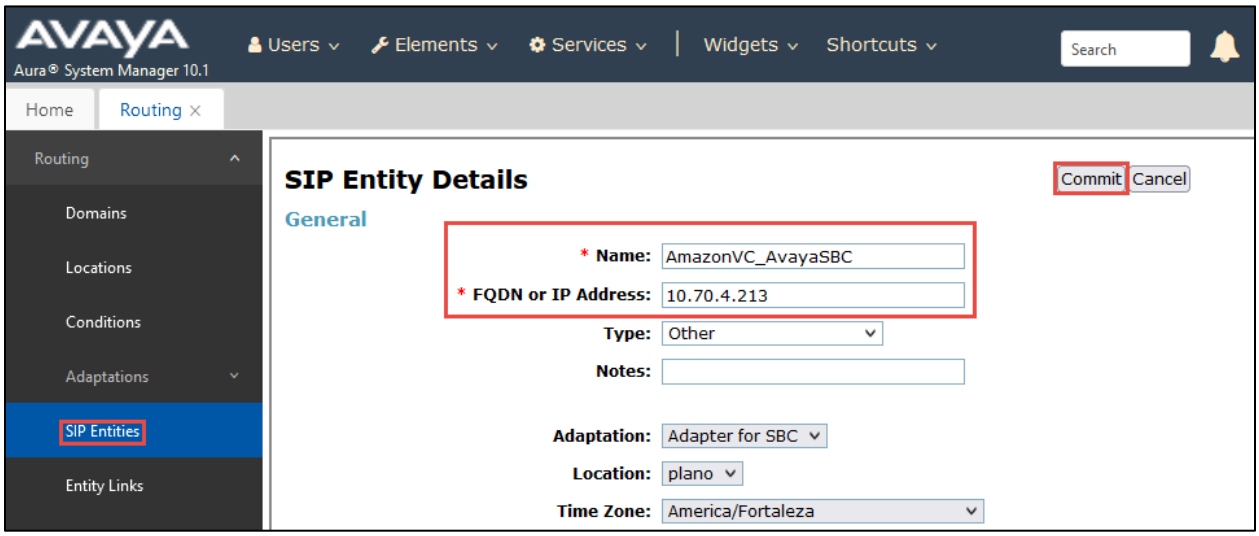

Figure 29 SIP Entity and Entity Link for Avaya SBCE

- Under *Entity Links*, Click **New**

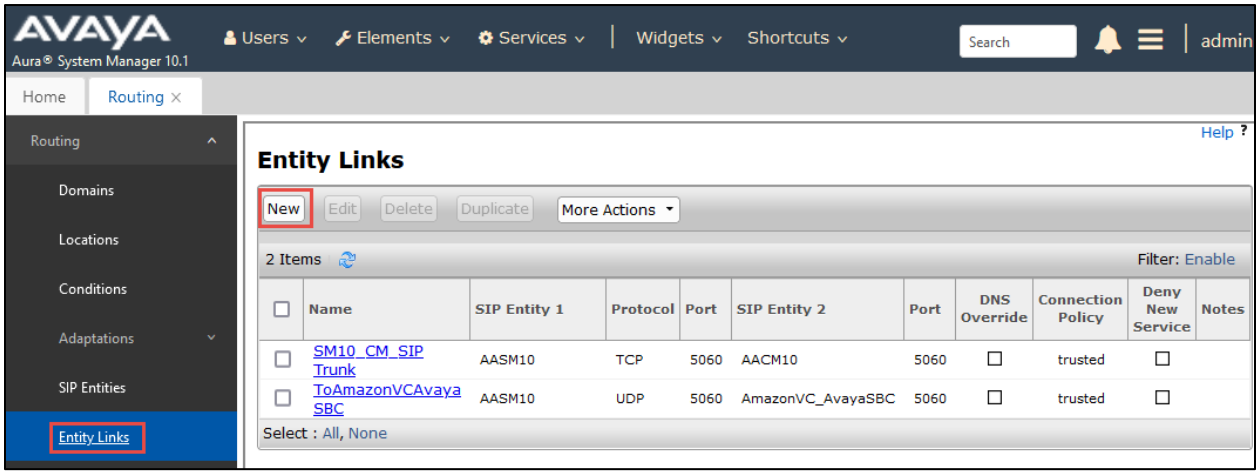

Figure 30 SIP Entity and Entity Link for Avaya SBCE continuation

- Set *Name*: **ToAmazonVCAvayaSBC**
- Set *SIP Entity 1*: Select the SIP Entity **AASM10**
- Set *SIP Entity 2*: **AmazonVC_AvayaSBC**
- Set *Protocol*: **UDP**
- Set *Ports*: Set both Ports to **5060**
- Set *Connection Policy*: **trusted**
- Leave all other fields to default values
- Click **Commit**

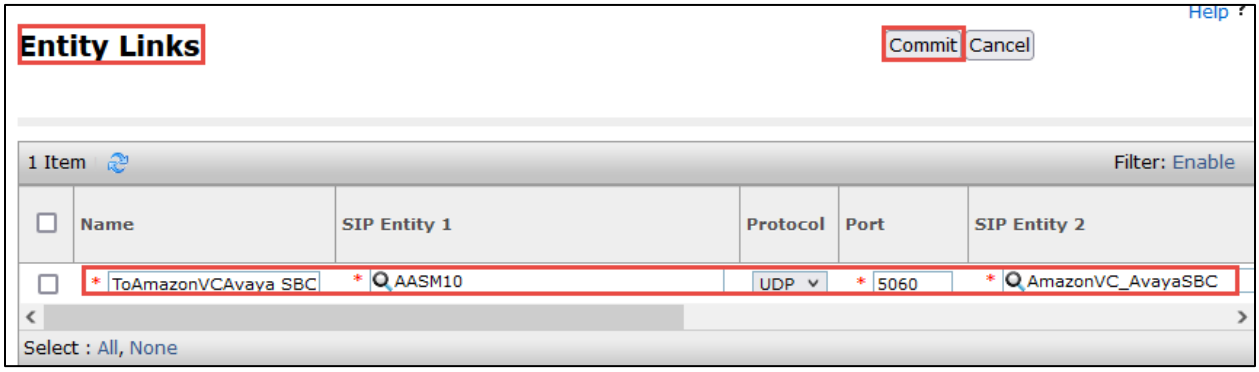

Figure 31 SIP Entity and Entity Link for Avaya SBCE continuation

4.3.6 Routing Policies

Routing policy to Avaya Aura CM

- Navigate to: **Routing** > **Routing Policies**. Click **New**
- Set *Name*: **SM to CM**
- Click **Select** under **SIP Entity as Destination** and the **SIP Entities** window is displayed

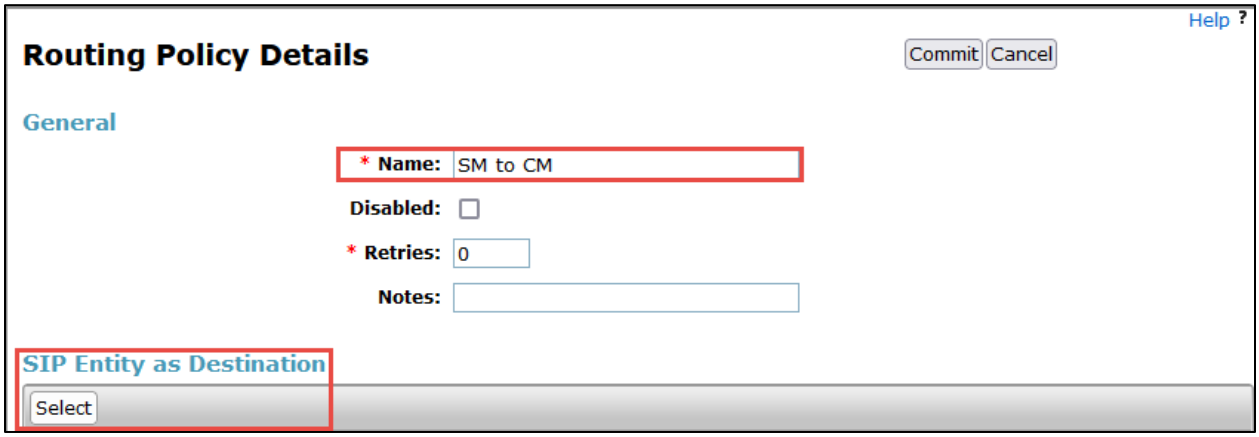

Figure 32 Routing Policy for Avaya CM

- Check the radio button beside **AACM10** as destination SIP Entity (configured in Section 4.3.5)
- Click **Select** and return back to **Routing Policy** Details page

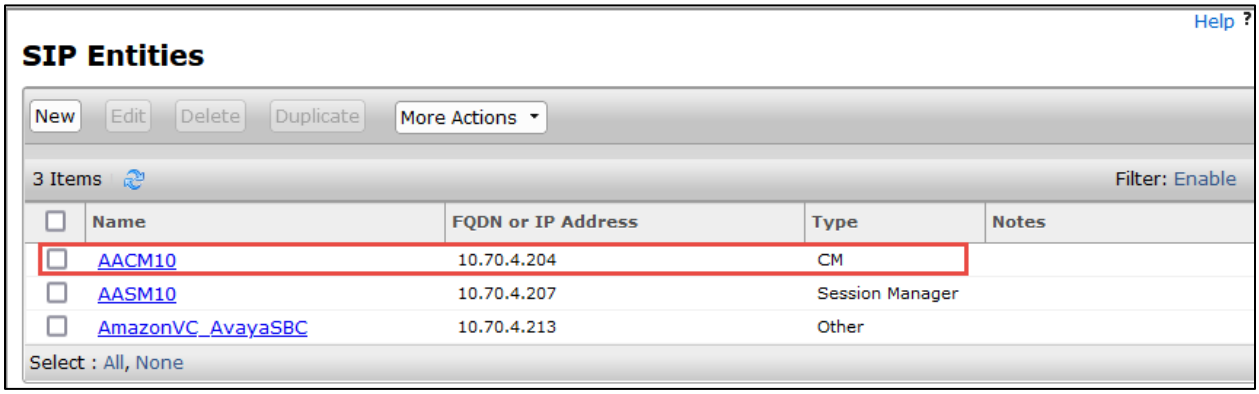

Figure 33 Routing Policy for Avaya CM continuation

Leave all other fields at default values

- Click Commit

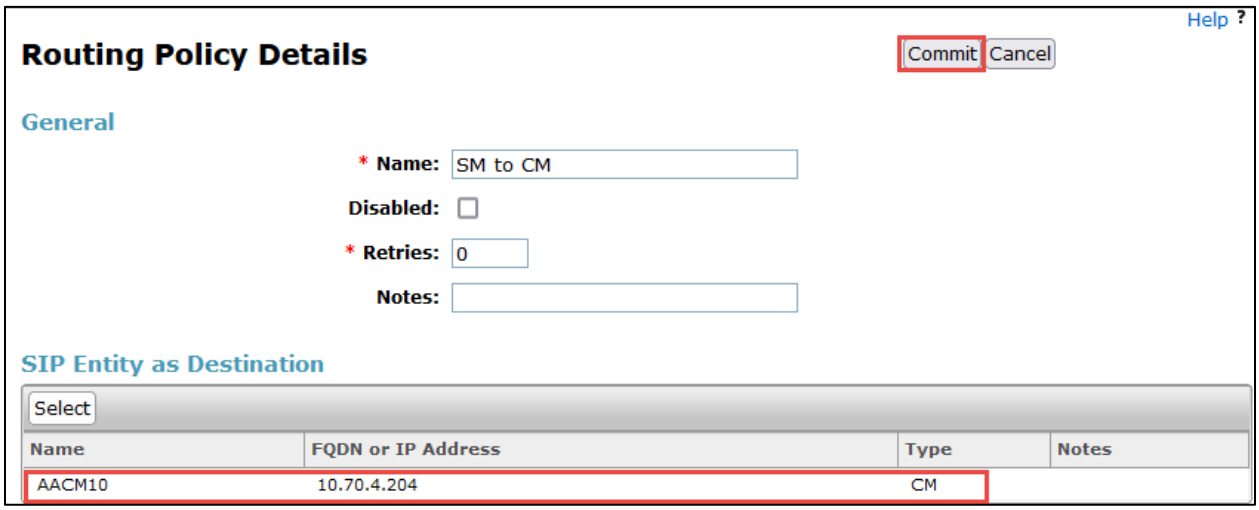

Figure 34 Routing Policy for Avaya CM continuation

Routing policy to Avaya SBCE

- Set Name: **AmazonVCAvayaSBC**
- Click **Select** under **SIP Entity as Destination** and **SIP Entities** window is displayed.

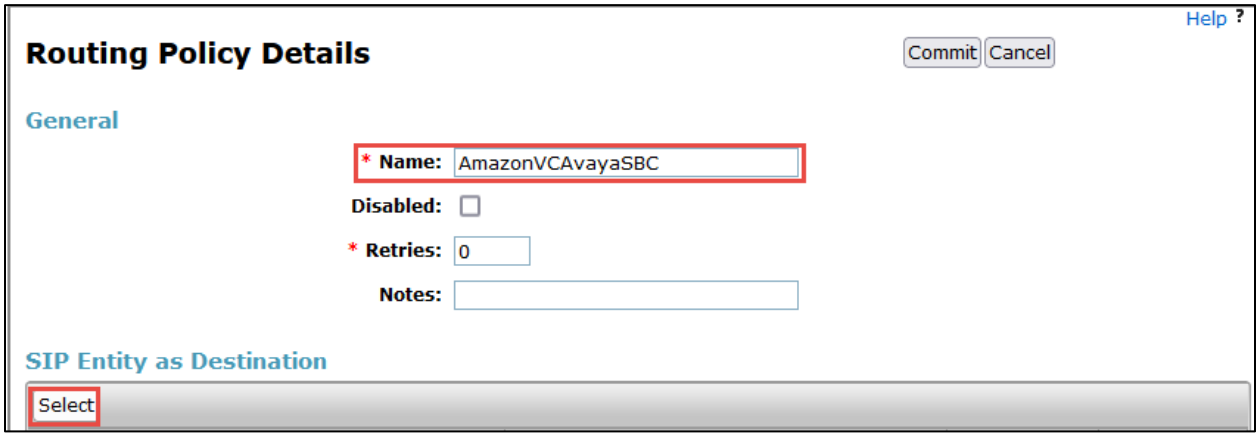

Figure 35 Routing Policy for Avaya SBCE

- Check the radio button beside **AmazonVC_AvayaSBC** as destination SIP Entity (configured in Section 4.3.5)
- Click **Select** and return back to **Routing Policy Details** page

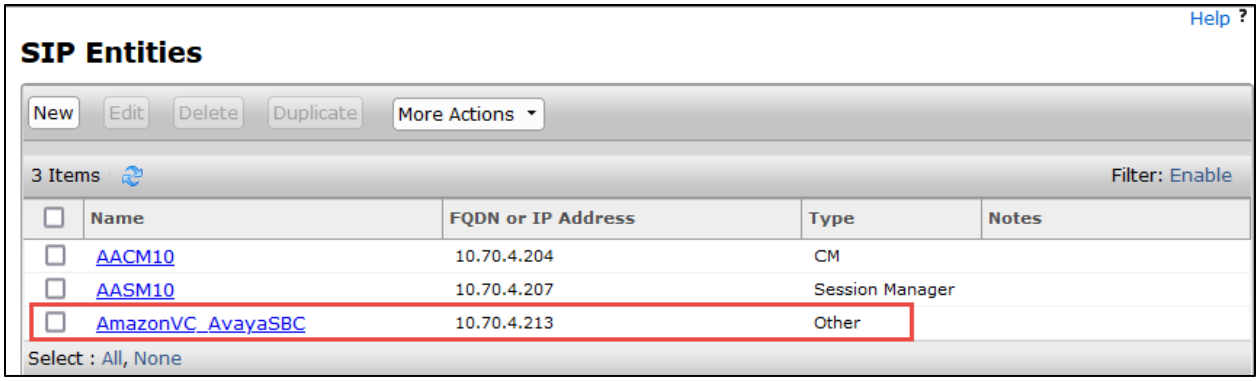

Figure 36 Routing Policy for Avaya SBCE continuation

- Leave all other fields to default values
- Click **Commit**

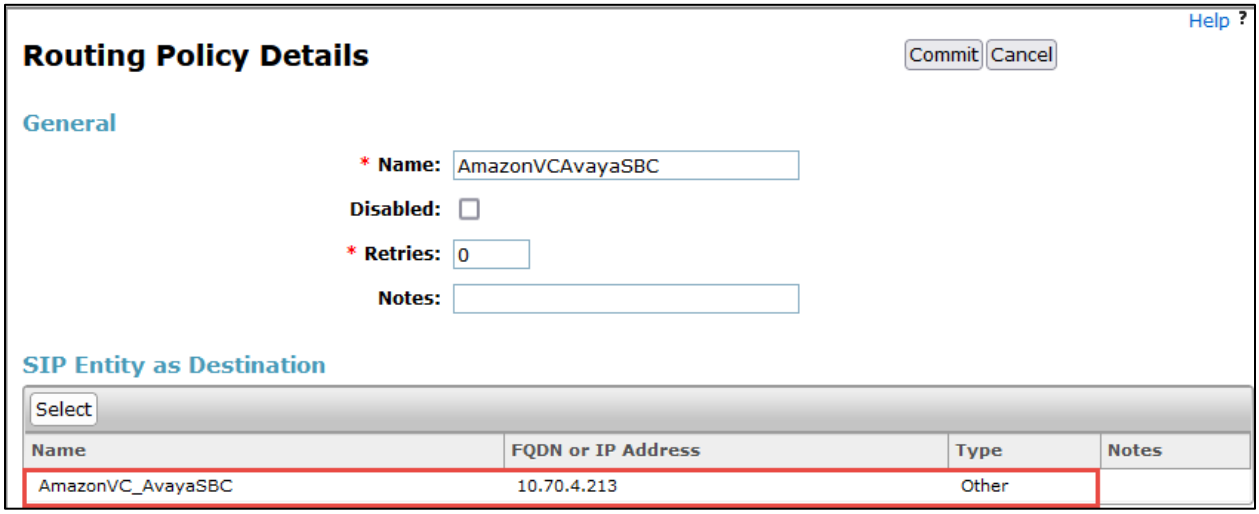

Figure 37 Routing Policy for Avaya SBCE continuation

4.3.7 Dial Patterns

Dial Pattern for Avaya Aura CM

- Navigate to: **Routing** > **Dial Patterns**. Click **New**
- Set *Pattern*: **972598**
- Set *Min*: **6**
- Set *Max*: **36**
- Under **Originating Locations and Routing Policies**, Click **Add**, at the new window
- *Originating Location*: Select **Plano** (created in Section 4.3.3)
- *Routing Policies*: Select **SM to CM** under Routing Policies
- Click **Select** to return to **Dial Pattern Details** page
- Leave all other fields to default values.
- Click **Commit**

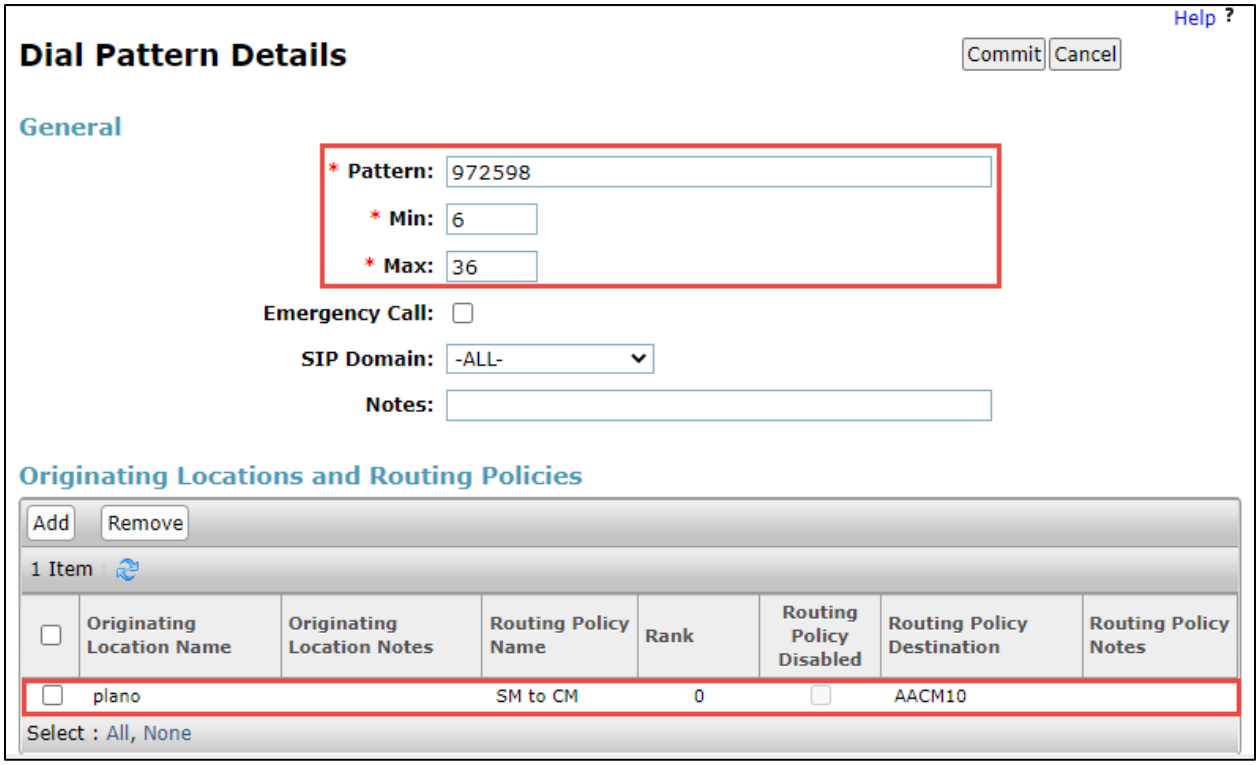

Figure 38 Dial Pattern to Avaya CM

Dial Pattern to Amazon Chime SDK Voice Connector via Avaya SBCE

- Navigate to: **Routing** > **Dial Patterns**. Click **New**
- Set *Pattern*: **214242**
- Set *Min*: **10**
- Set *Max*: **12**
- Under **Originating Locations and Routing Policies**, Click **Add**, at the new window
- *Originating Location*: Select **Plano** (created in Section 4.4.3)
- *Routing Policies*: Select **AmazonVCAvayaSBC** under **Routing Policies**
- Click **Select** to return to **Dial Pattern Details** page
- Leave all other fields to default values.
- Click **Commit**

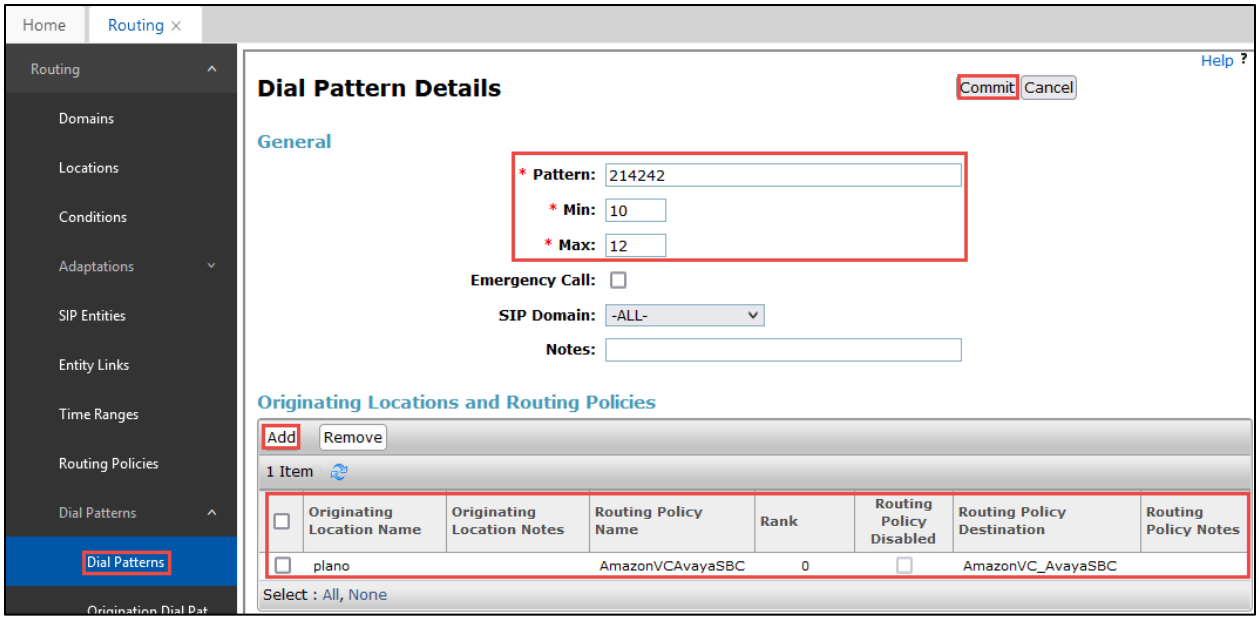

Figure 39 Dial Pattern to Amazon via Avaya SBCE

4.4 Avaya SBCE Configuration

4.4.1 Avaya SBCE login

- Log into Avaya Session Border Controller for Enterprise (SBCE) web interface by typing "**https://X.X.X.X/sbc**".
- Enter the **Username** and **Password**
- Click **Log In**

Figure 40 Avaya SBCE Login

- Under Device, select **ASBCE10** from drop down to expand the configuration for Avaya SBCE.

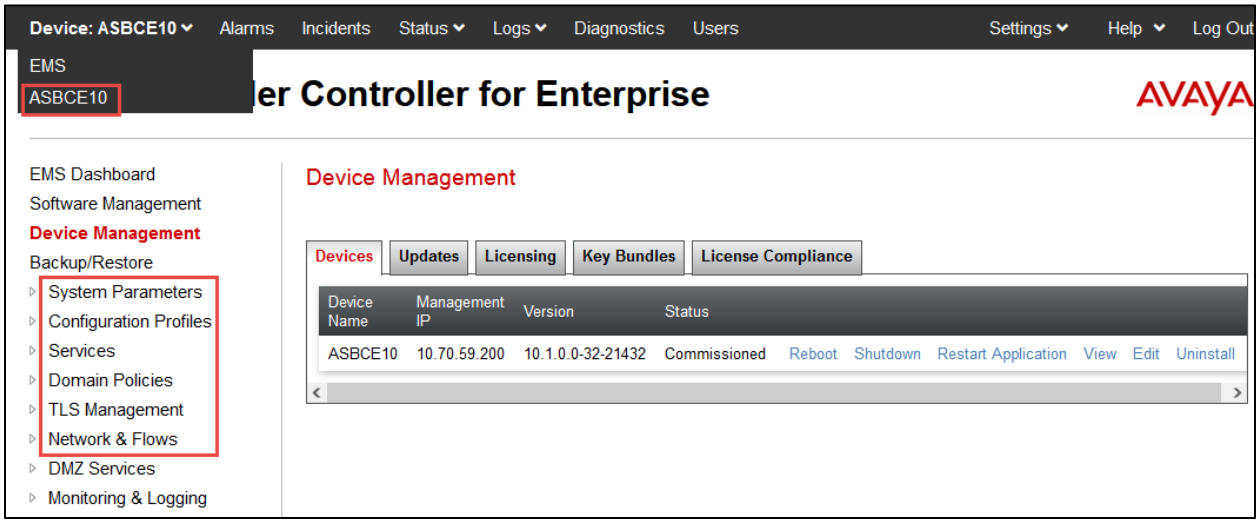

Figure 41 Selection of Avaya SBCE Device

4.4.2 Server Interworking

Server Interworking for Avaya SM

- Navigate to: **Configuration Profiles > Server Interworking**
- Select the predefined Interworking Profile **avaya-ru**, click **Clone**
- Set Clone Name: **AASM10.1**
- Click **Finish**

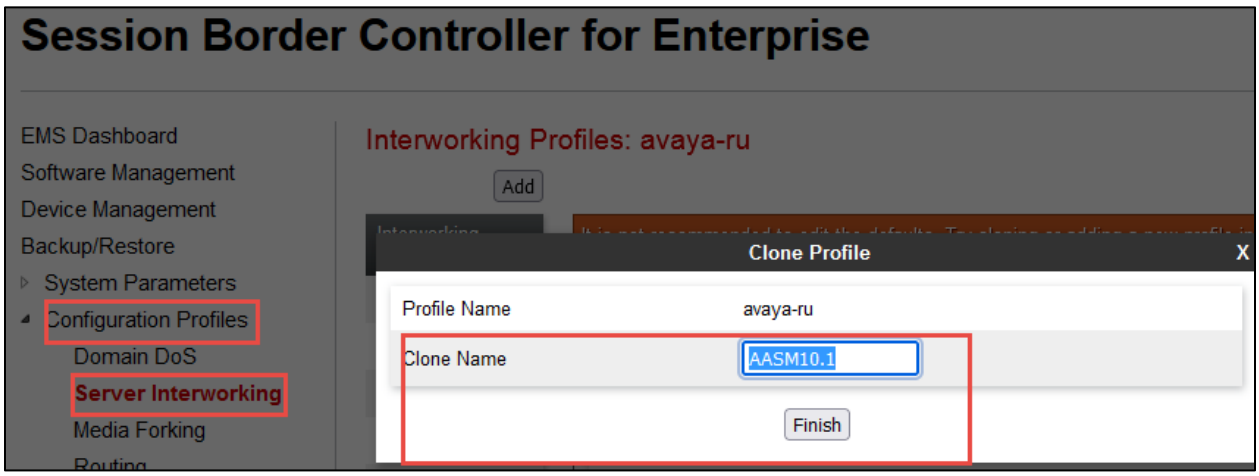

Figure 42 Server Interworking profile for Avaya SM

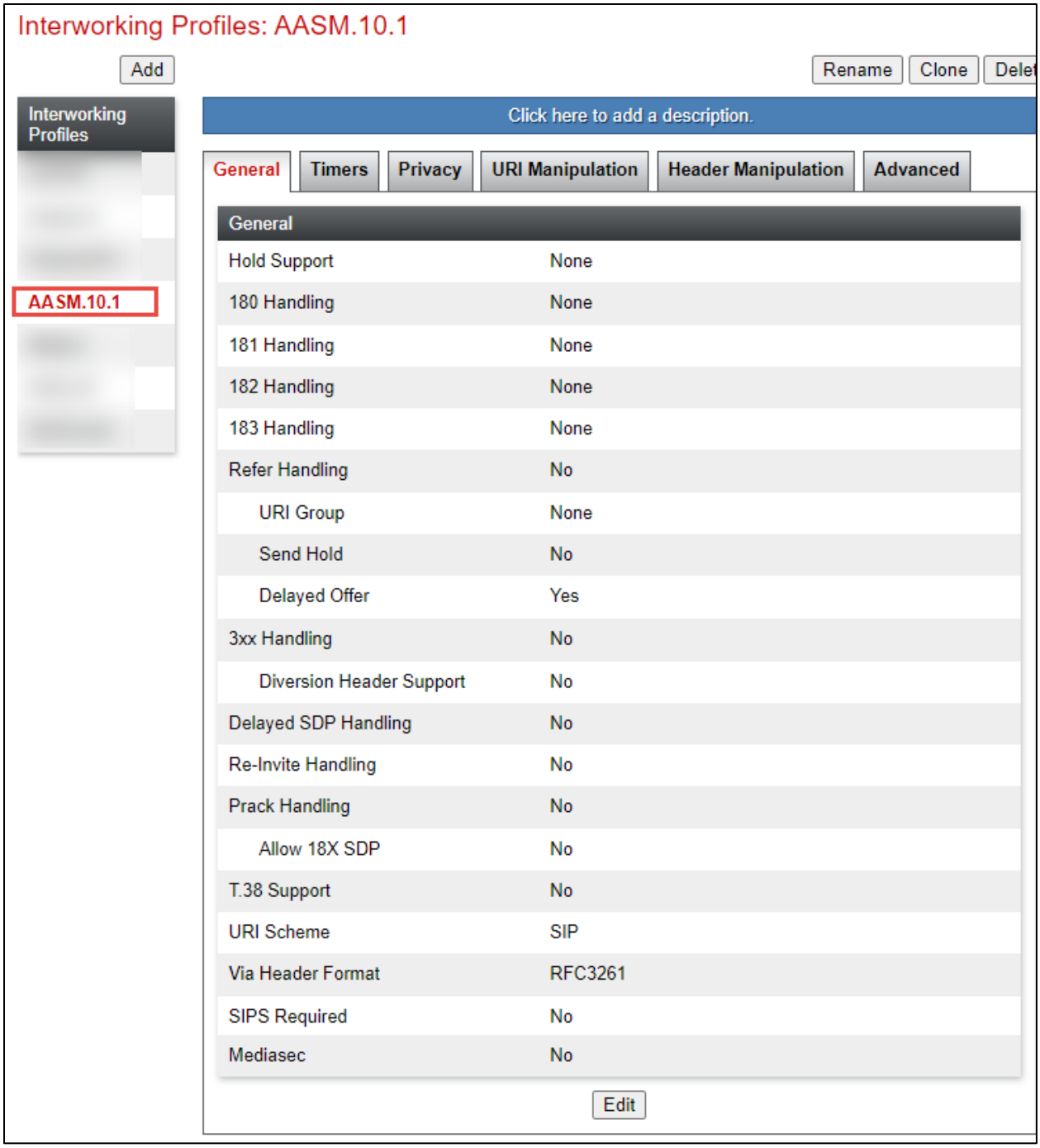

Figure 43 Server Interworking profile for Avaya SM continuation

Server Interworking for PSTN

- Repeat the same procedure to create the Interworking Profile to PSTN

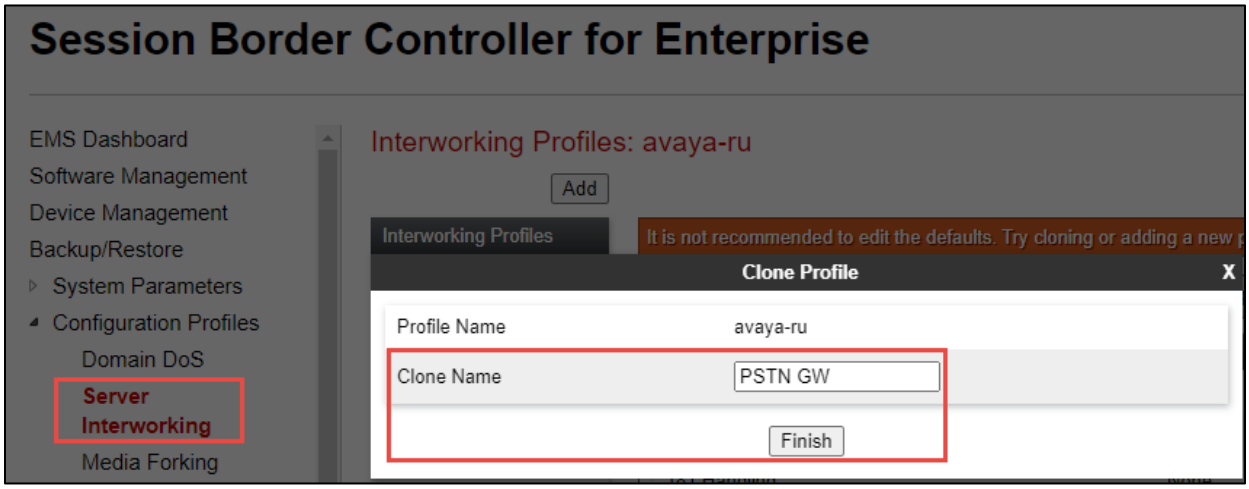

Figure 44 Server Interworking profile for PSTN

Server Interworking for Amazon Chime SDK Voice Connector

- Repeat the same procedure to create the Interworking Profile to Amazon Chime SDK Voice Connector

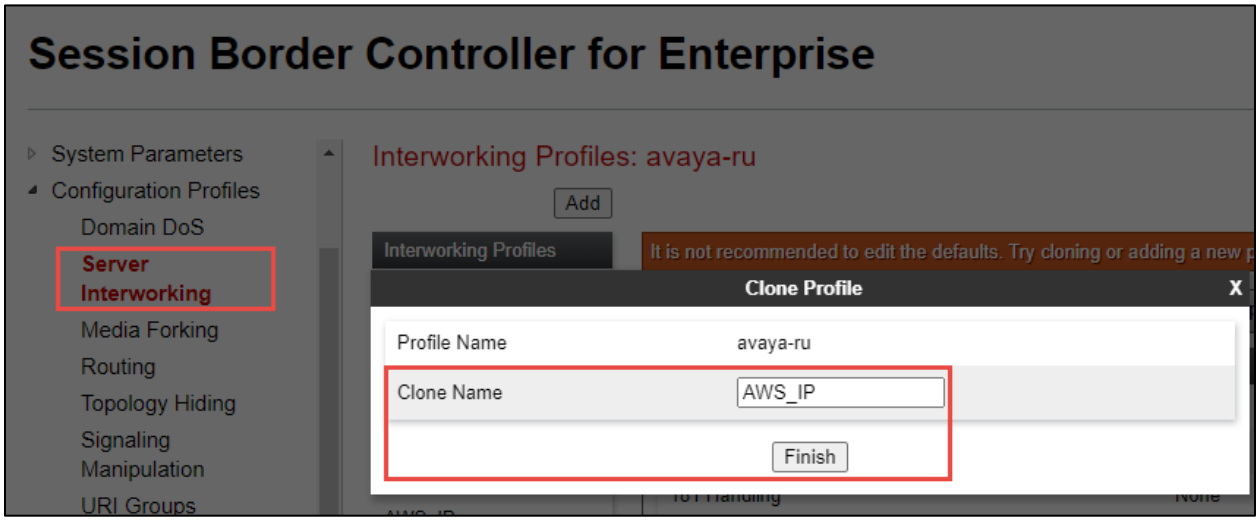

Figure 45 Server Interworking profile for Amazon

4.4.3 SIP Servers

SIP Server for Avaya SM

- Navigate to **Services** > **SIP Servers**
- Click **Add**
- Set *Profile Name*: **Avaya**
- Click **Next**

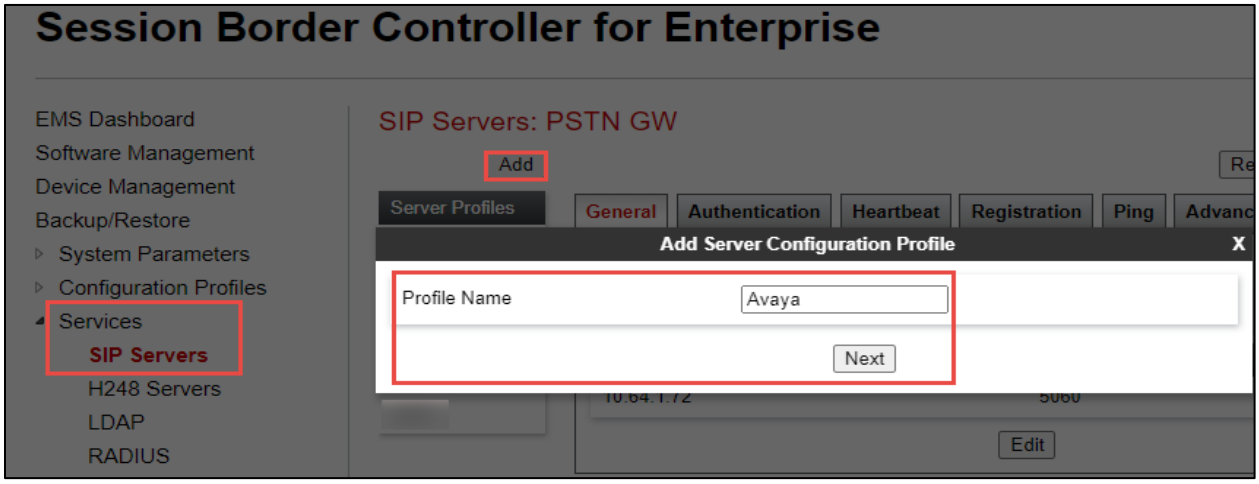

Figure 46 SIP Server for Avaya SM

Set *Server Type*: Select **Trunk Server** from the drop down

- Set *IP Address/FQDN*: Enter the **Avaya Aura Session Manager SIP IP Address**
- Set *Port*: **5060**
- Set *Transport*: **UDP**
- Click **Finish**

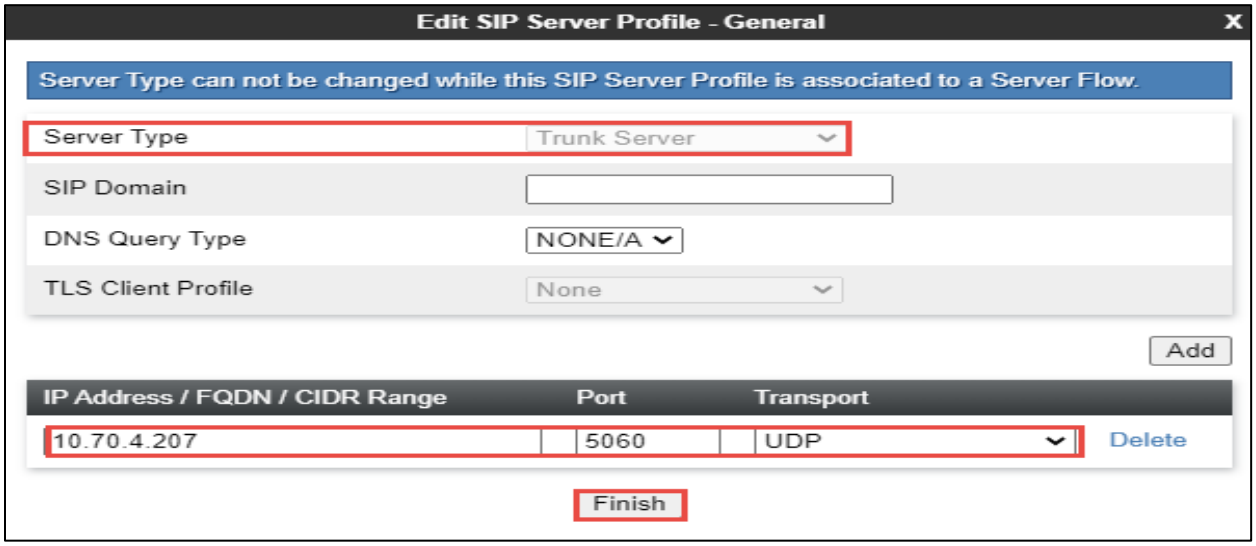

Figure 47 SIP Server for Avaya SM Continuation

- Navigate to **Advanced** tab
- Set *Enable Grooming*: **Checked**
- Set *Interworking Profile*: Select **AASM 10.1** (created in section 4.4.2)
- Click **Finish**

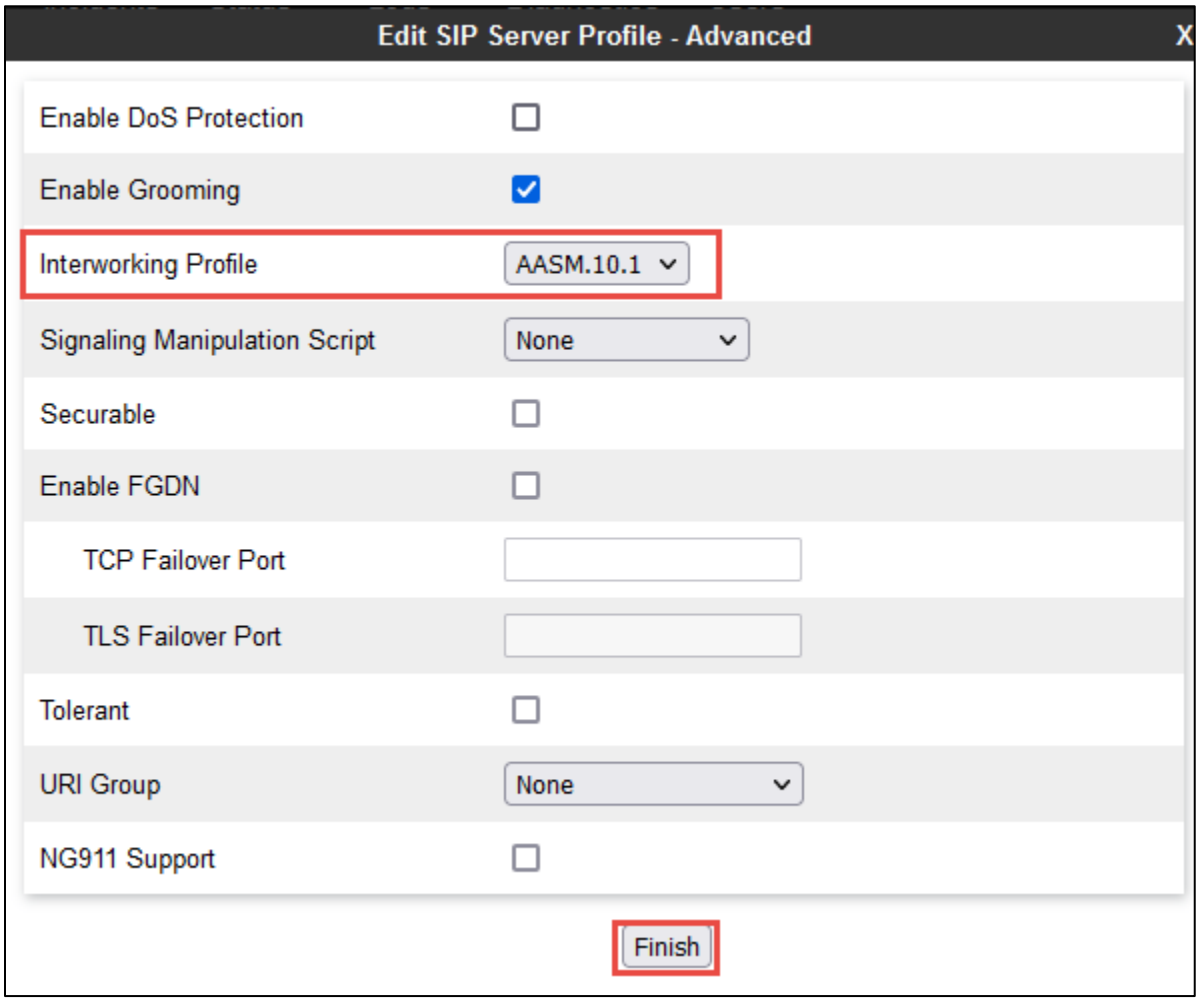

Figure 48 SIP Server for Avaya SM Continuation

SIP Server for PSTN

- Navigate to **Services** > **SIP Servers**
- Click **Add**
- Set *Profile Name*: **PSTN GW**
- Click **Next**

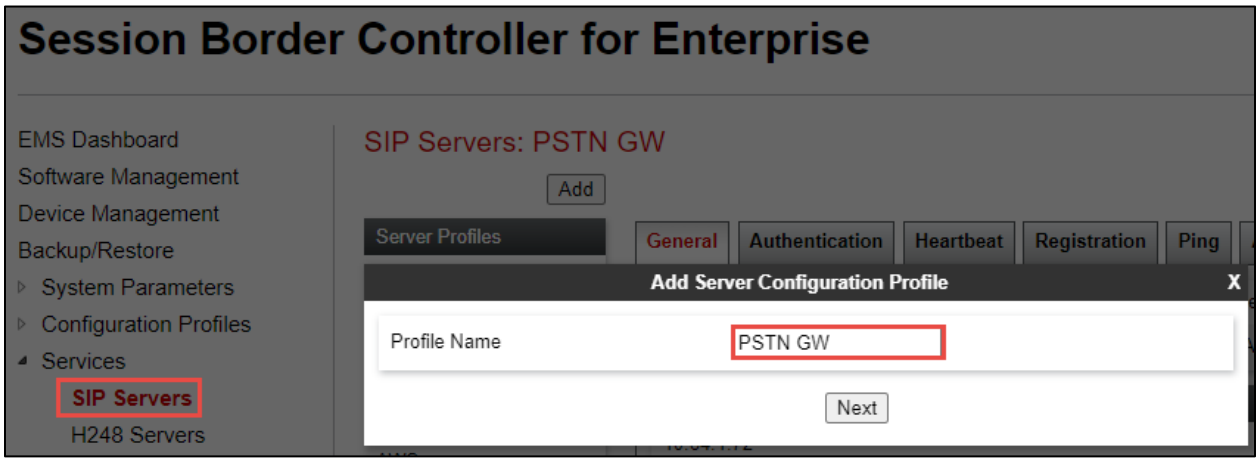

Figure 49 SIP Server for PSTN

Set *Server Type*: Select **Trunk Server** from the drop down

- Set *IP Address/FQDN*: Enter the **PSTN IP Address**
- Set *Port*: **5060**
- Set *Transport*: **TCP**
- Click **Finish**

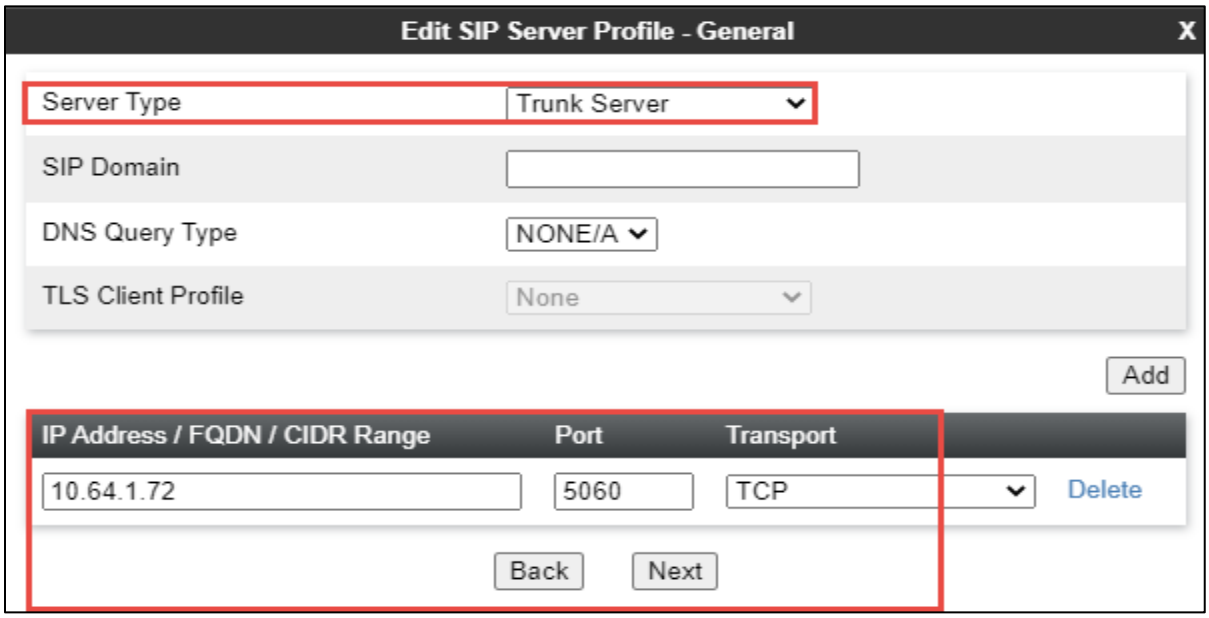

Figure 50 SIP Server for PSTN continuation

Navigate to **Advanced** tab

- Set *Interworking Profile*: Select **PSTN GW** (created in section 4.4.2)
- Click **Finish**

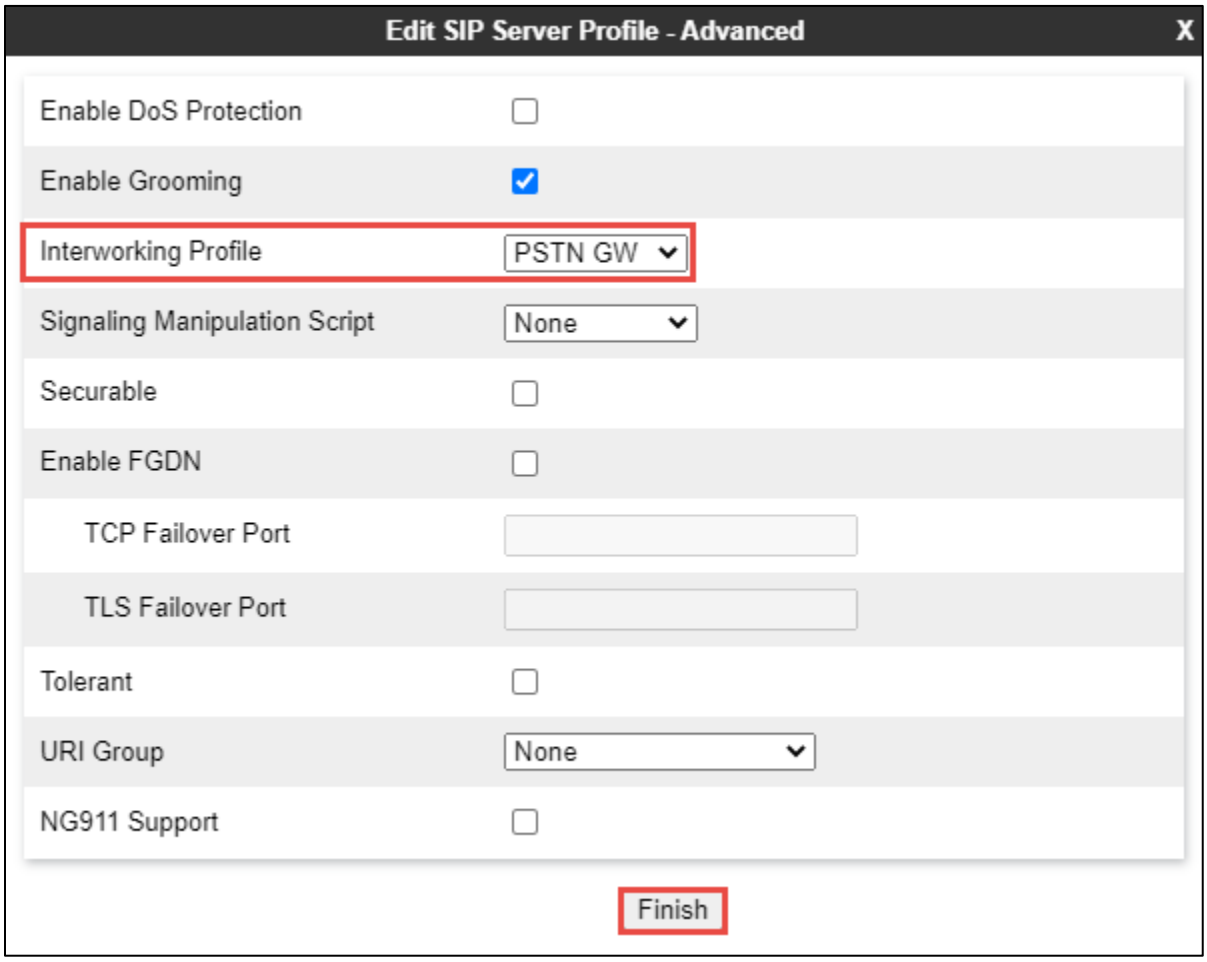

Figure 51 SIP Server for PSTN continuation

SIP Server for Amazon Chime SDK Voice Connector

- Navigate to **Services** > **SIP Servers**
- Click **Add**
- Set *Profile Name*: **AWS**
- Click **Next**

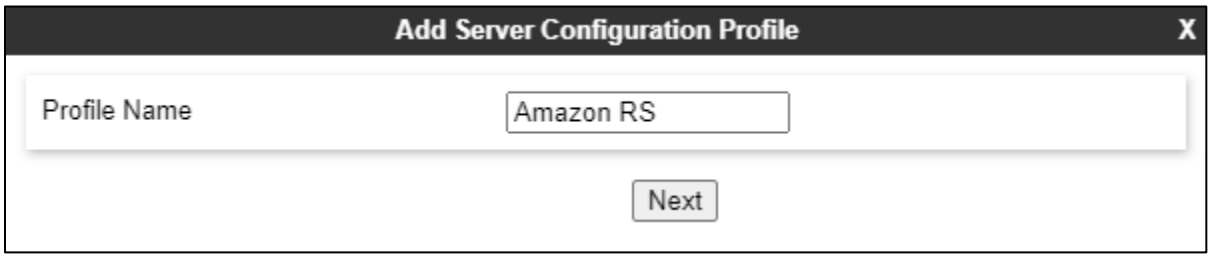

Figure 52 SIP Server for Amazon

Set *Server Type*: Select **Recording Server** from the drop down

- TLS Client Profile: SBCWAN (created in section 4.4.13)
- Set *IP Address/FQDN*: Enter the **Amazon Chime SDK voice Connector Outbound Host Name**
- Set *Port*: **5061**
- Set *Transport*: **TLS**
- Click **Finish**

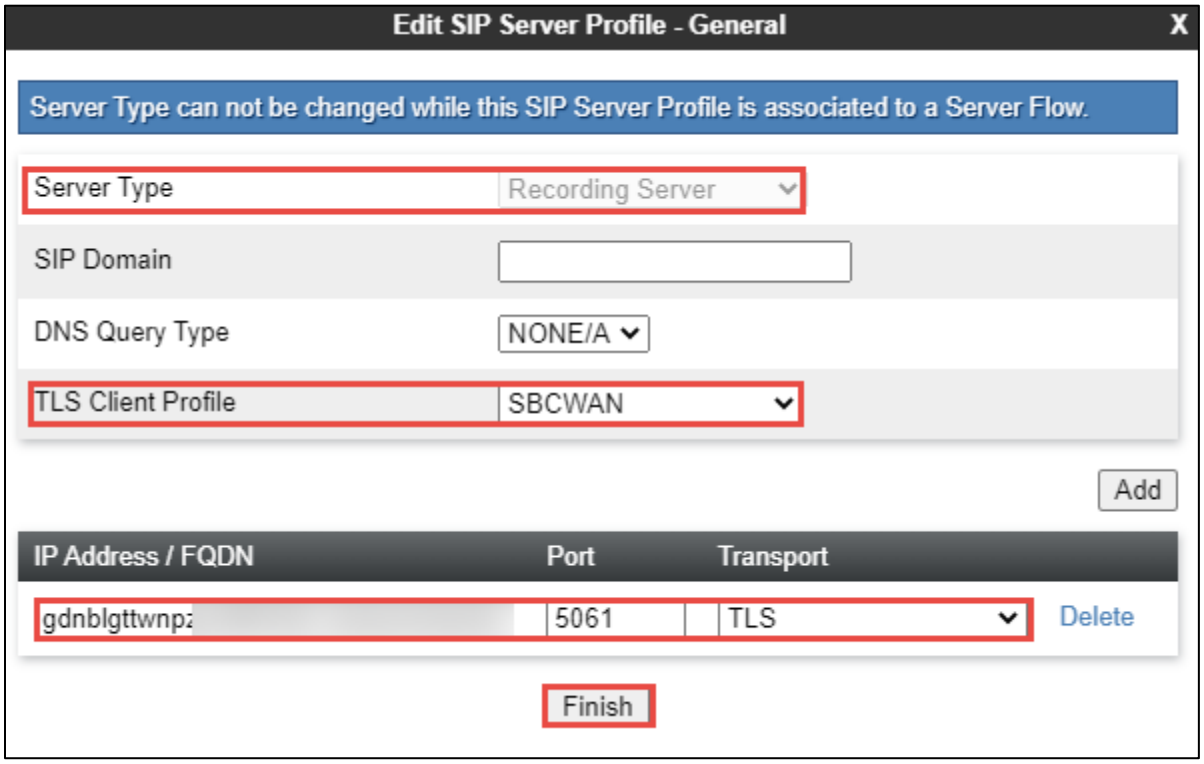

Figure 53 SIP Server for Amazon continuation

Navigate to **Advanced** tab

- Set *Interworking Profile*: Select **AWS_IP** (created in section 4.4.2)
- Set Signaling Manipulation Script: Select **AMZURI** (Created in Section 4.4.15)
- Click **Finish**

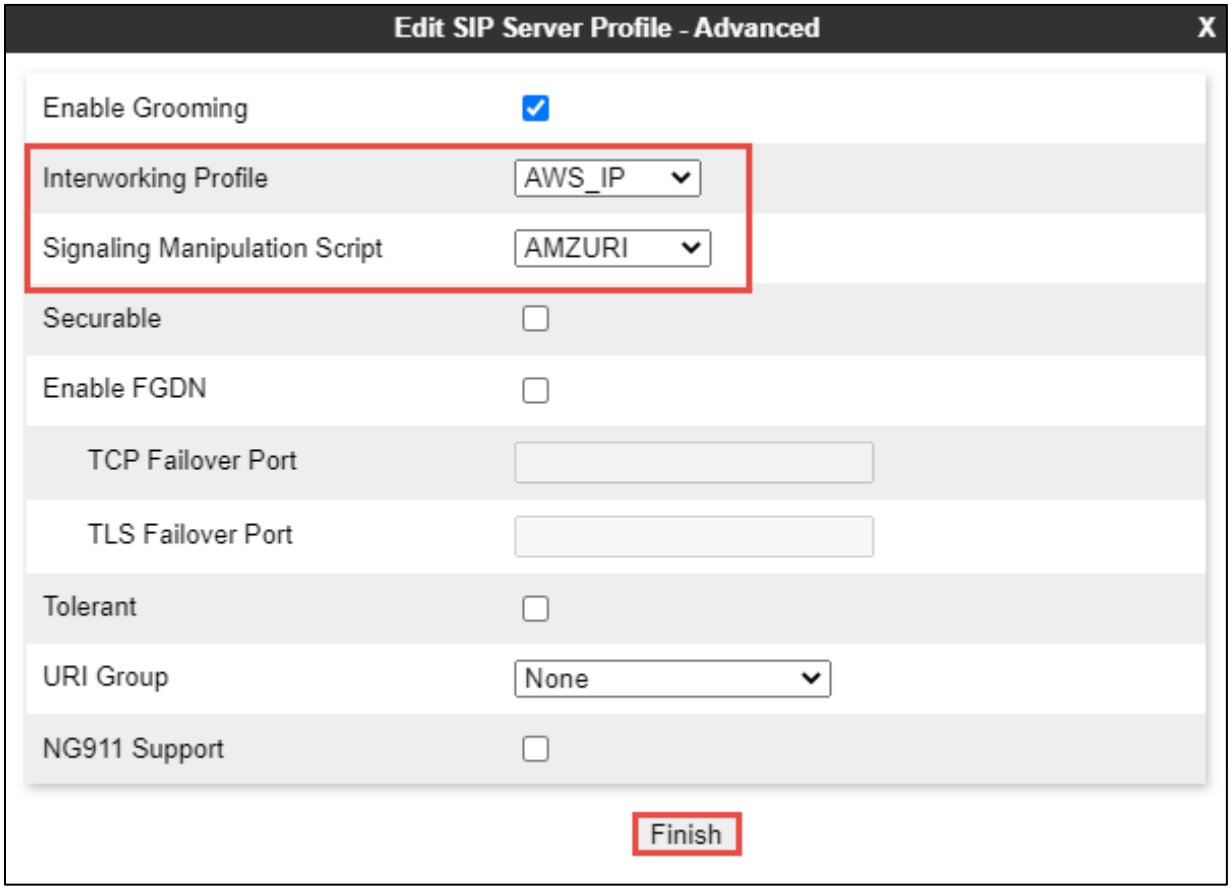

Figure 54 SIP Server for Amazon continuation

4.4.4 Topology Hiding

Topology hiding profile for Avaya SM

- Topology Hiding profiles are added for Avaya SM to overwrite and hide certain headers
- Navigate to: **Configuration Profiles > Topology Hiding**
- Select the Profile **default**. Click **Clone**
- Set *Clone Name*: **Avaya_SM**
- Click **Finish**

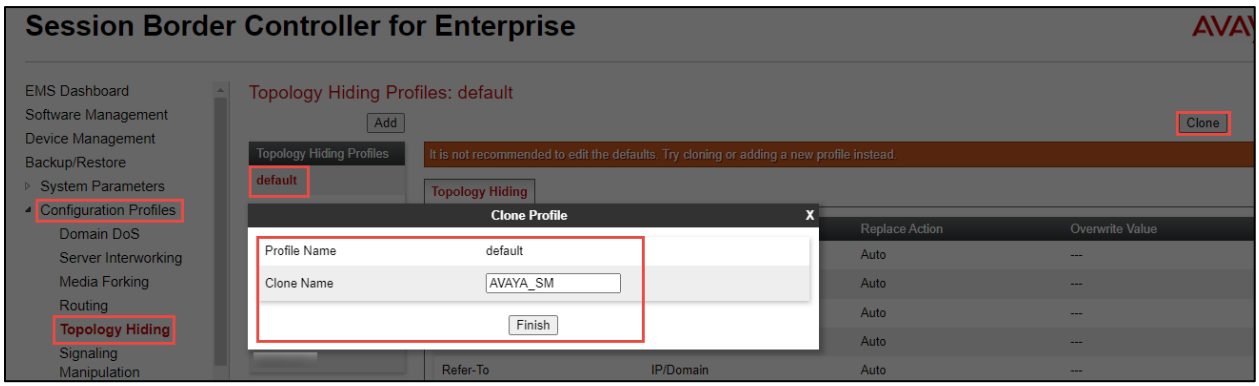

Figure 55 Topology Hiding Profile for Avaya SM

- Select the newly created profile **Avaya_SM** and Click **Edit**
- Set *Header*: **Request-Line, To, From** are selected
- Set *Replace Action*: **Overwrite**
- Set *Overwrite Value*: **lab.xxxxxxxx.com**

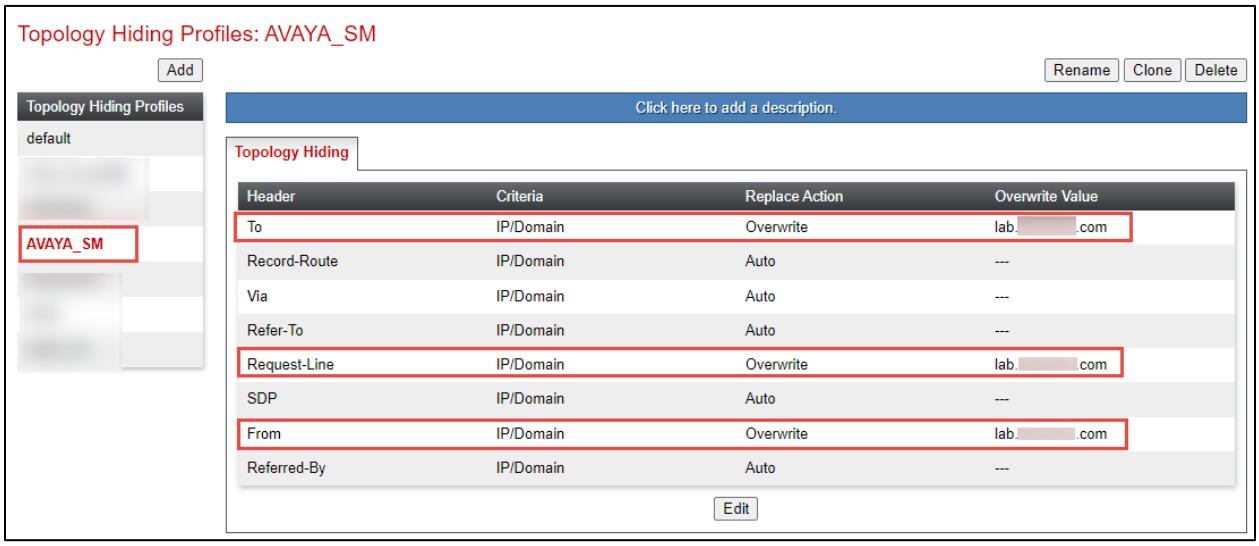

Figure 56 Topology Hiding Profile for Avaya SM continuation

Topology hiding profile for PSTN

- Repeat the same procedure to create the profile for **PSTNGW**
- *Overwrite Value*: Replace the **To** header and **Request-Line** header with **IP address of PSTN**
- Click **Finish**

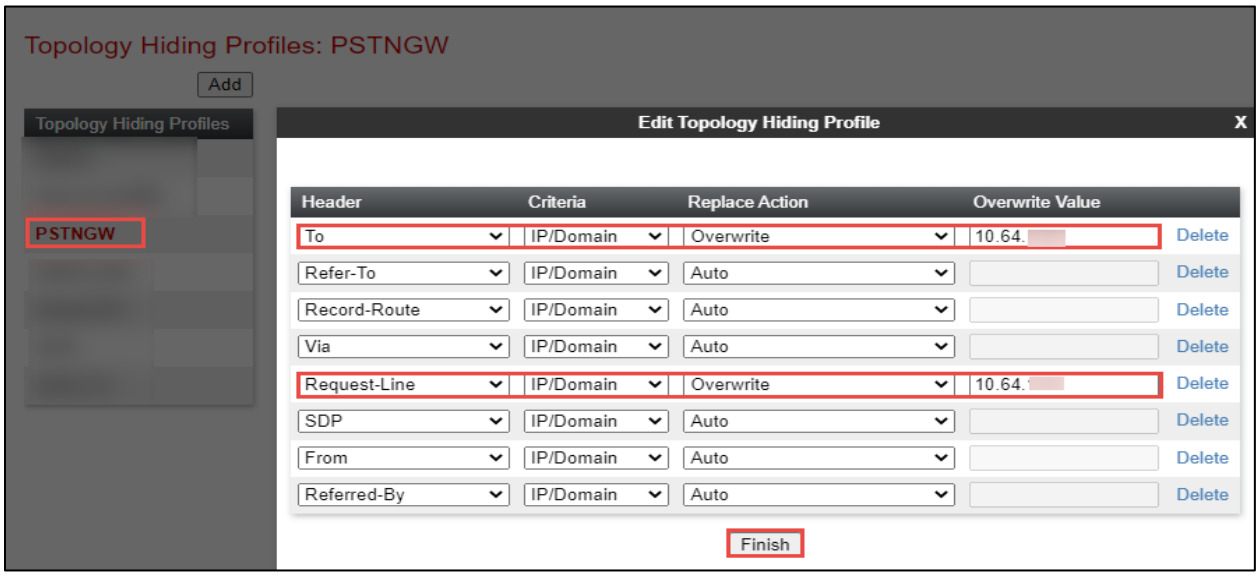

Figure 57 Topology Hiding Profile for PSTN

Topology hiding profile for Amazon Chime SDK Voice connector

- Repeat the same procedure to create the profile for **AWS_TH**
- *Overwrite Value*: Replace the **To** header and **Request-Line** header with **Amazon Chime SDK Voice Connector Outbound Host Name**
- Click **Finish**

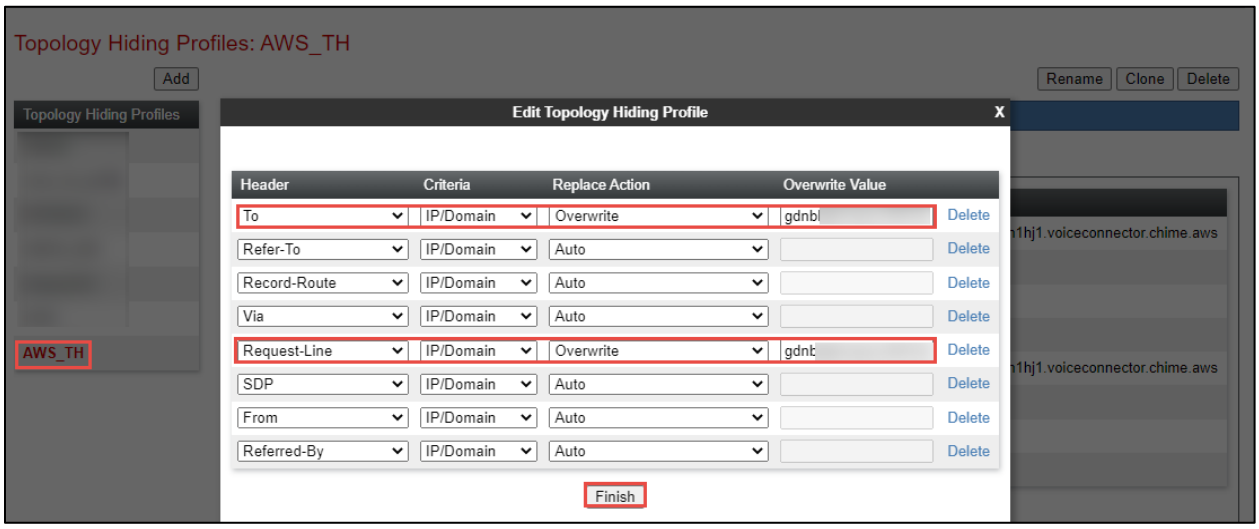

Figure 58 Topology Hiding Profile for Amazon

4.4.5 Routing

Routing for Avaya SM

- Navigate to: **Configuration Profiles > Routing**
- Click **Add**
- Set *Profile Name*: **Avaya_SM**
- Click **Next**

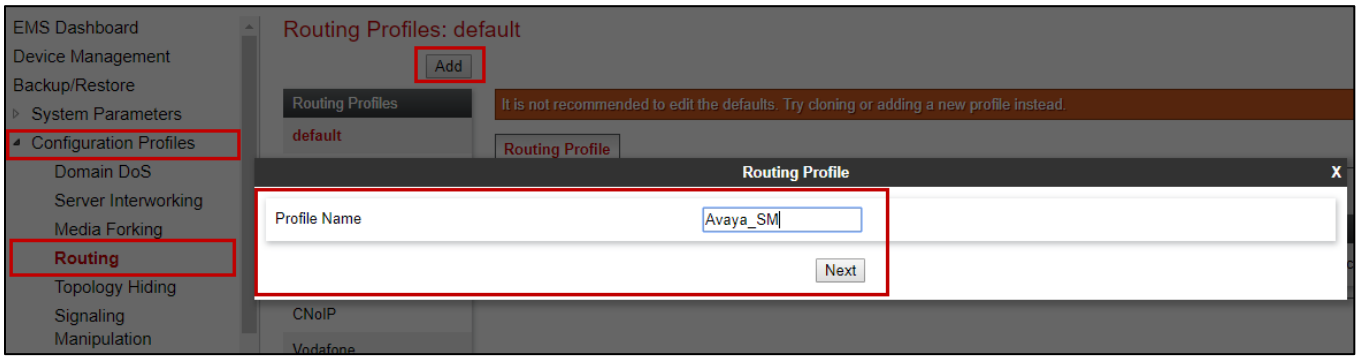

Figure 59 Routing for Avaya SM

- At Routing Profile Window, Click **Add**
- Set *Priority/Weight*: **1**
- Set *Server Configuration*: **Avaya_SM** (configured in section 4.4.3)
- The **Server IP, Port** and **Transport Protocol** populates automatically
- Click **Finish**

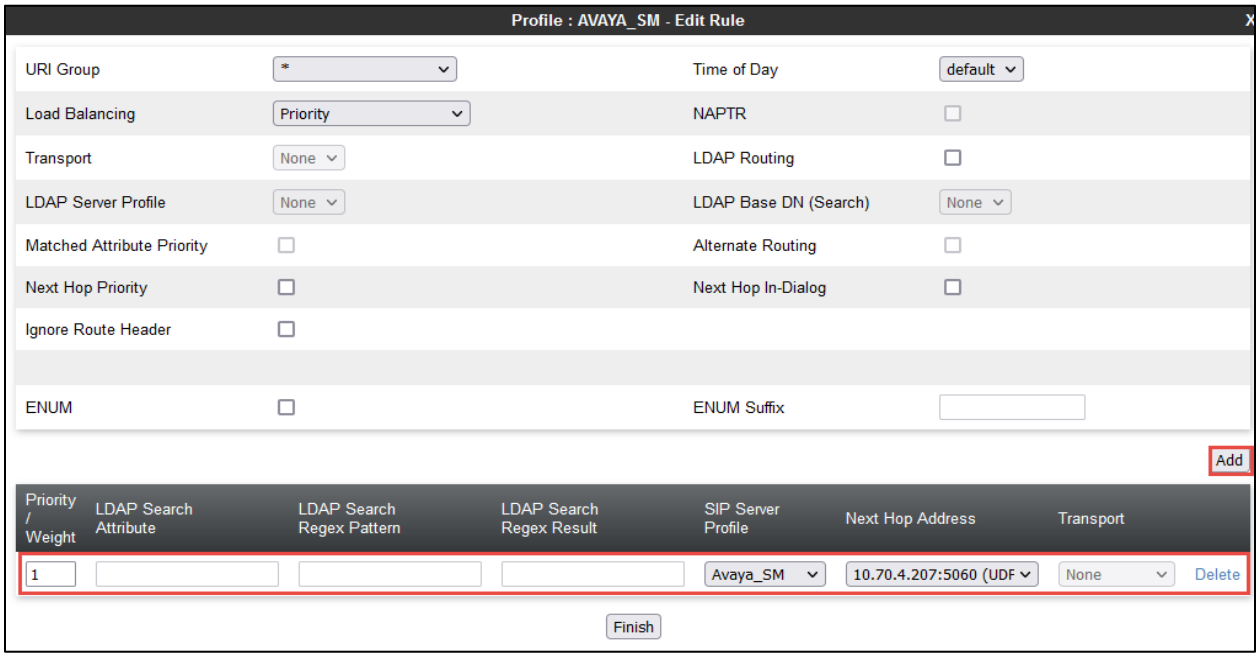

Figure 60 Routing for Avaya SM continuation

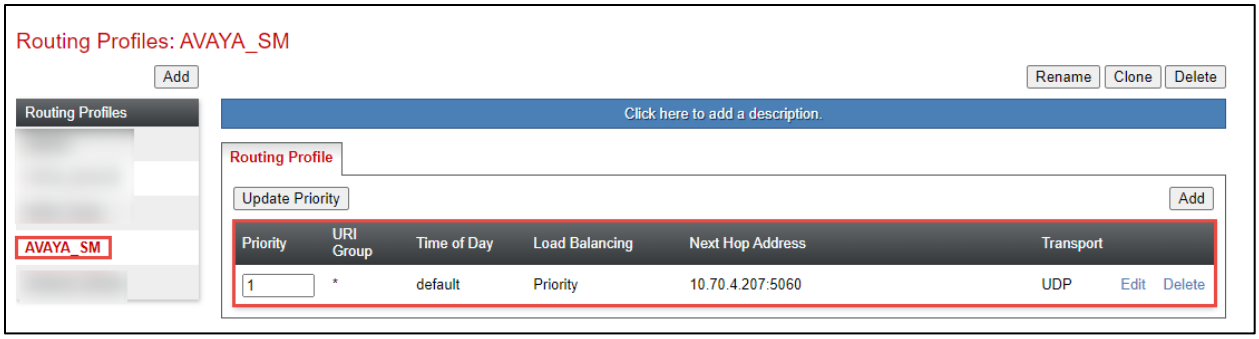

Figure 61 Routing for Avaya SM continuation

Routing for PSTN

- Repeat the same steps to create the Routing Profile for **PSTN**
- Set *Priority/Weight*: **1**
- Set *Server Configuration*: **PSTN GW** (configured in section 4.4.3)
- The **Server IP, Port** and **Transport Protocol** populates automatically
- Click **Finish**

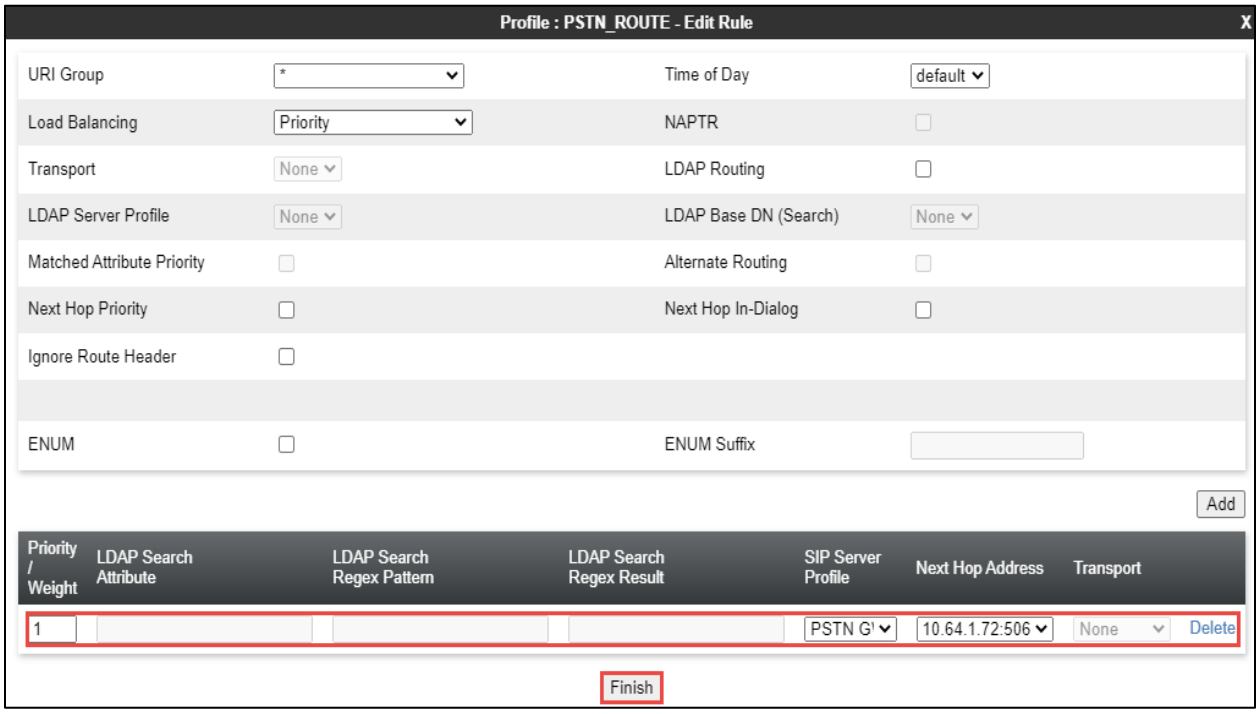

Figure 62 Routing for PSTN

Routing for Amazon

- Repeat the same steps to create the Routing Profile **Amazon_Route** for Amazon
- Set *Priority/Weight*: **1**
- Set *Server Configuration*: **Amazon RS** (configured in section 4.4.3)
- The **Server IP/FQDN, Port** and **Transport Protocol** populates automatically
- Click **Finish**

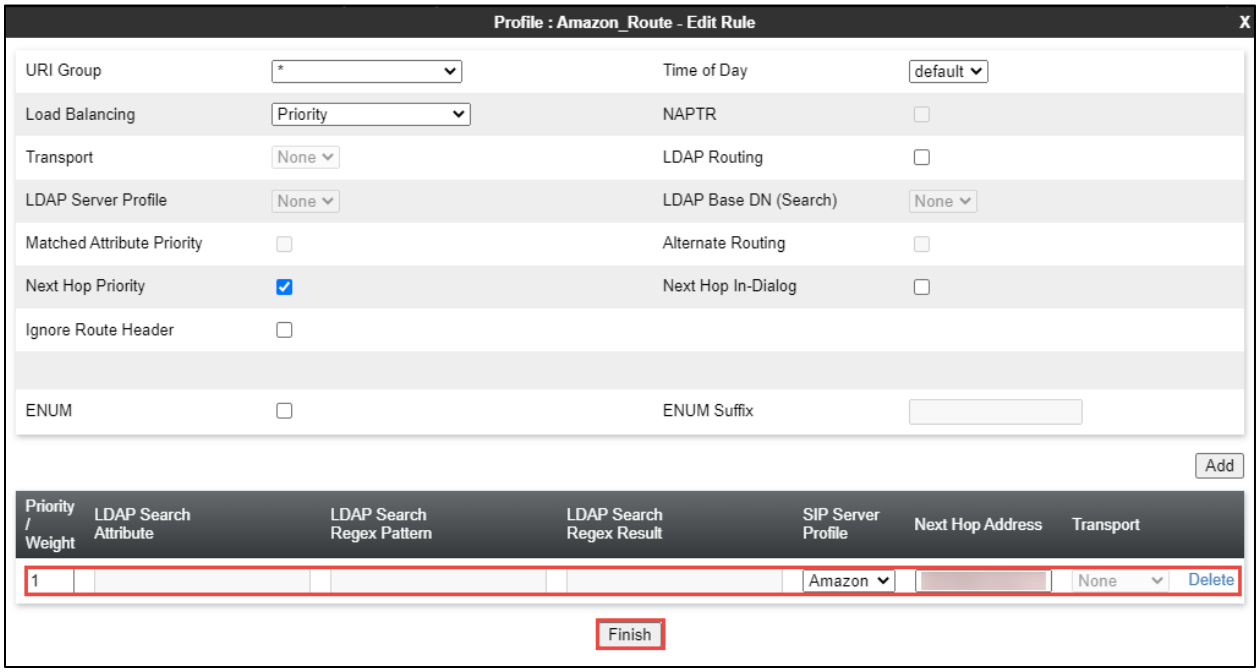

Figure 63 Routing for Amazon

4.4.6 Recording Profile

- Navigate to: **Configuration> Recording Profile**
- Click **Add**
- Set *Profile Name*: **Amazon_RP**
- Click **Next**

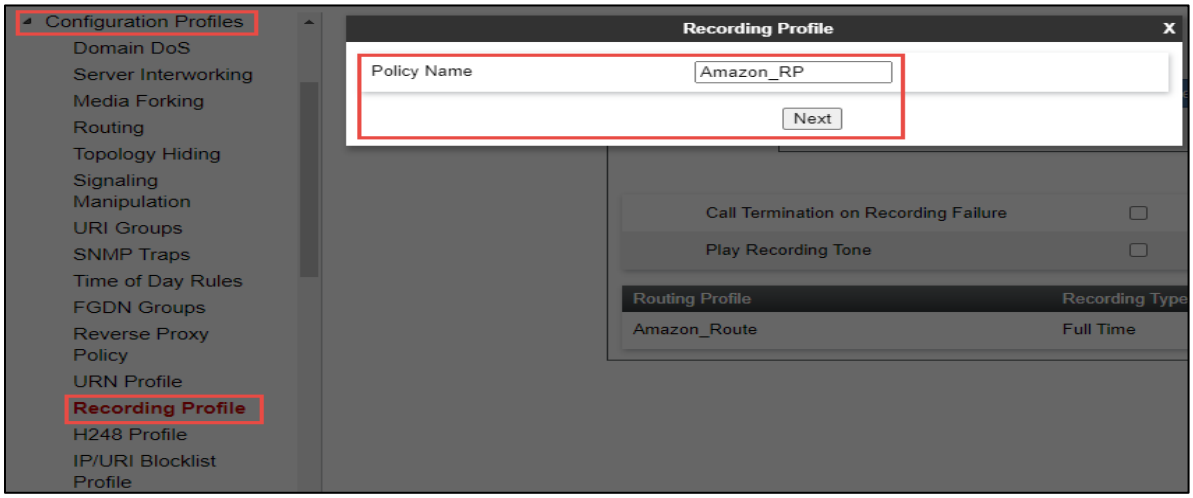

Figure 64 Recording Profile for Amazon

- Set Routing Profile: Select **Amazon_Route** (configured in section 4.4.5)
- Set Recording Type: Select **Full Time** from the dropdown
- Click **Finish**

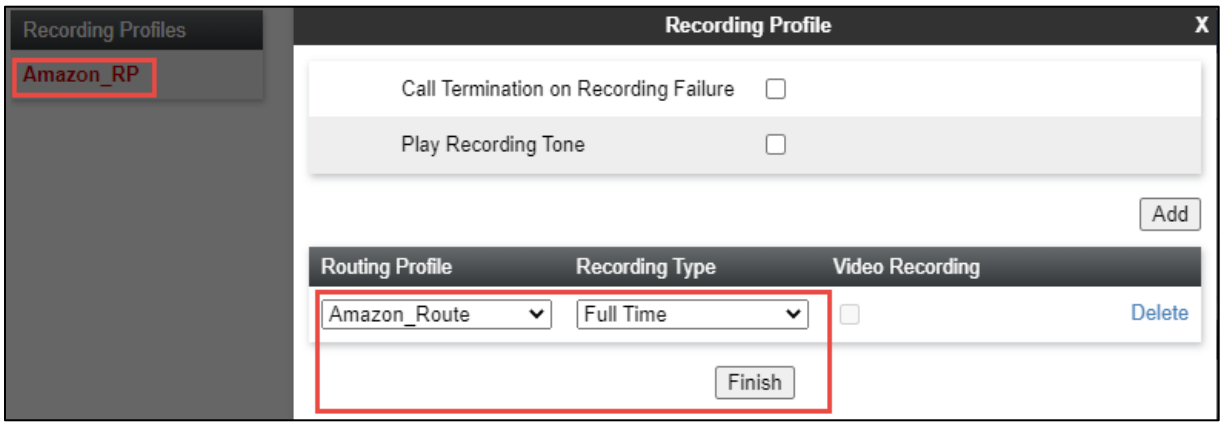

Figure 65 Recording Profile continuation for Amazon

4.4.7 Session Policies

- Navigate to: **Domain Policies > Session Policies**

- Select **default** under Session Policies, Click **Clone**
- Set *Profile Name*: **Amazon_SP**
- Click **Next**

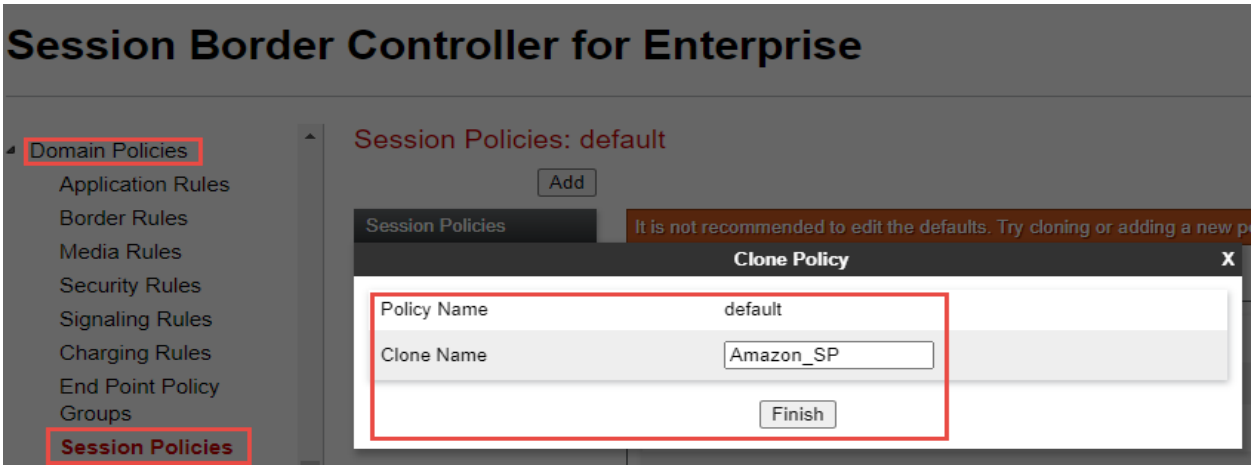

Figure 66 Session Profile for Amazon

- Media Anchoring: **Checked**
- Recording Server: **Checked**
- Set Routing Profile: Select the route profile **Amazon_RP** (configured in section 4.4.6)
- Click **Finish**

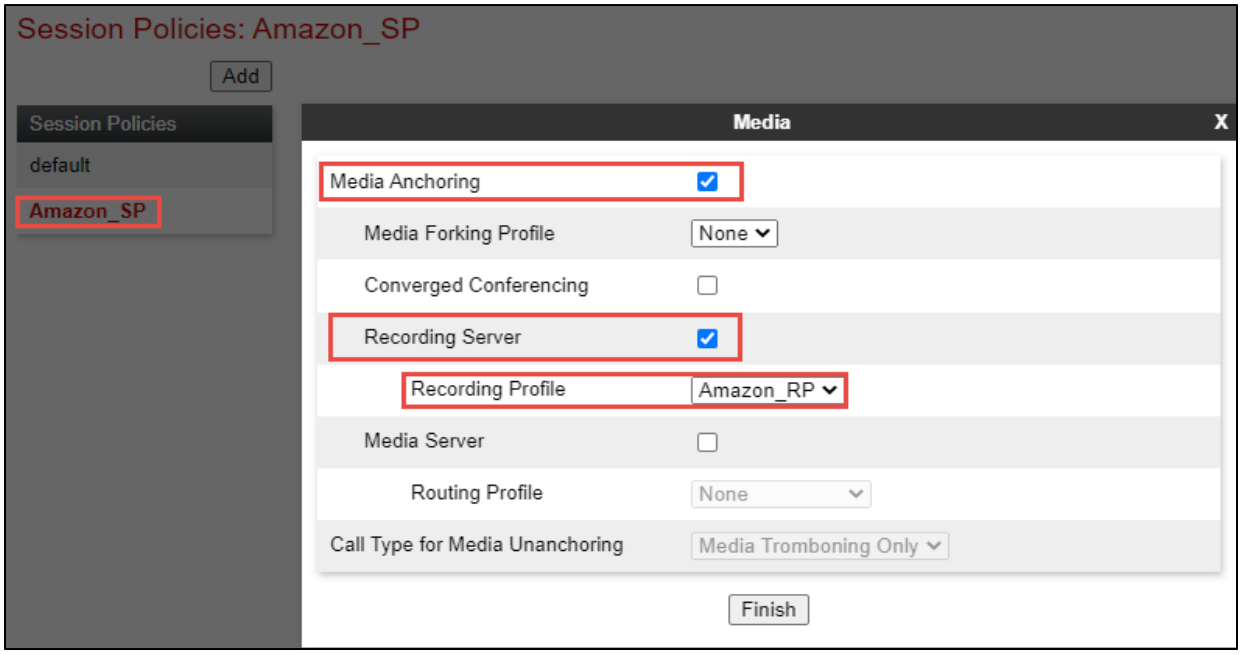

Figure 67 Session Profile Continuation for Amazon

4.4.8 Session Flows

- Navigate to: **Network and Flows> Session Flows**

- Click **ADD**
- Set *Name*: **Amazon_SF**
- Select Session Policy: **Amazon_SP** (configured in section 4.4.7)
- Click **Finish**

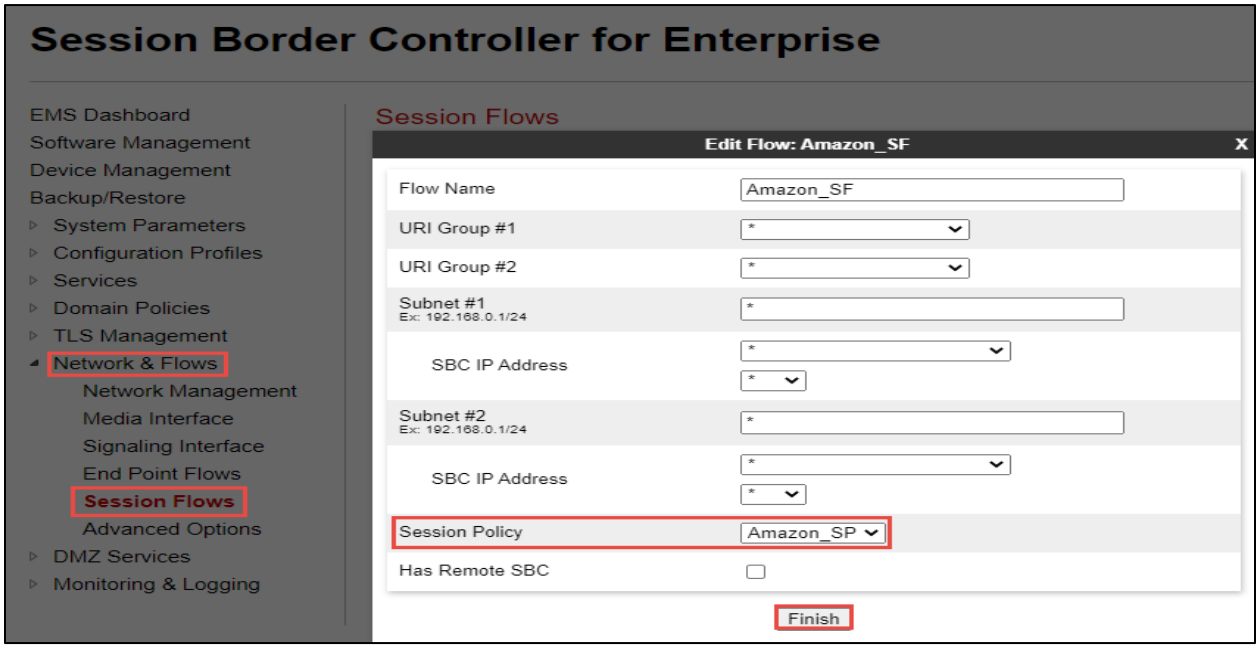

Figure 68 Session Flow for Amazon

4.4.9 Signaling Rules

Signaling rule for Avaya

- Navigate to: **Domain Policies > Signaling Rules**
- Select **default** under Signaling Rules, Click **Clone**
- Set *Name*: **Avaya_SM**
- Click **Finish**

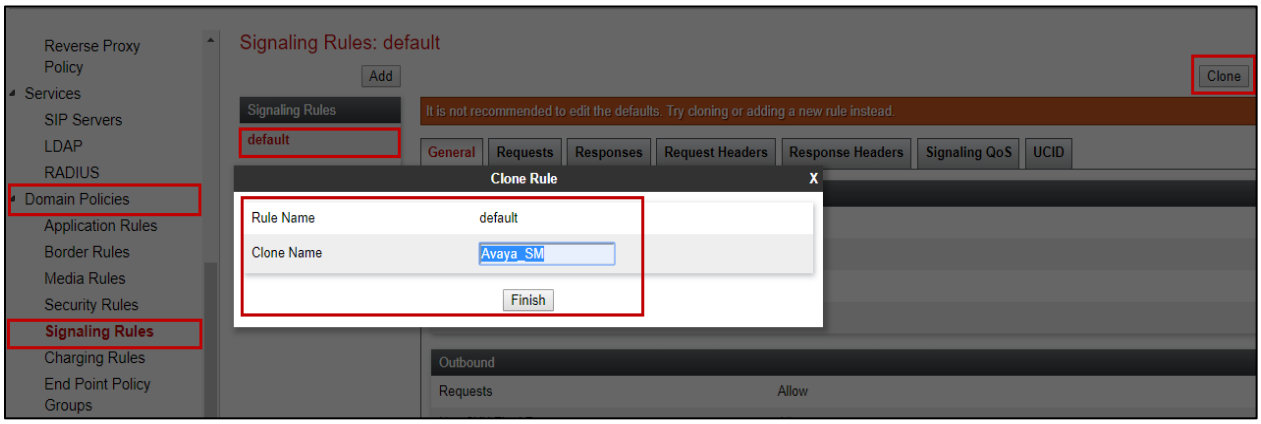

Figure 69 Signaling Rules for Avaya SM

- Select the newly cloned Signaling Rule **Avaya_SM**, under tab Request Headers, Click **Add In Header Control**
- Set *Proprietary Request Header*: **Checked**
- Set *Header Name*: **AV-Global-Session-ID**
- Set *Method Name*: Select **ALL** from the drop down
- Set *Header Criteria*: **Forbidden**
- Set *Presence Action*: **Remove header** is selected from the drop down
- Click **Finish**

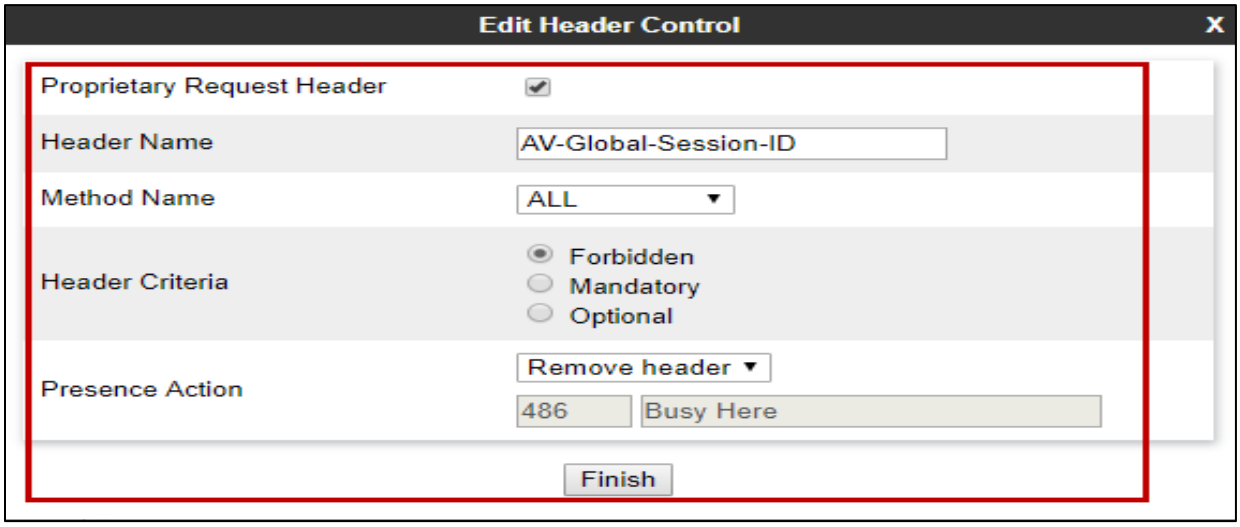

Figure 70 Signaling Rules for Avaya SM continuation

- Repeat the same steps for all other required headers

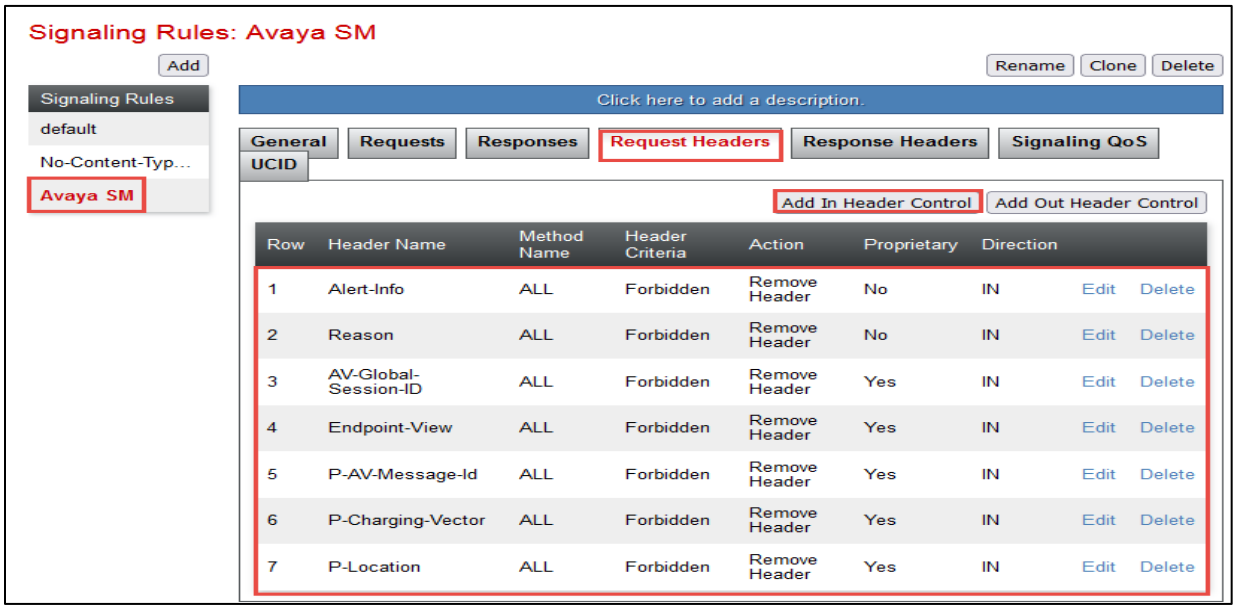

Figure 71 Signaling Rules for Avaya SM continuation

- Repeat the same steps for Response Headers

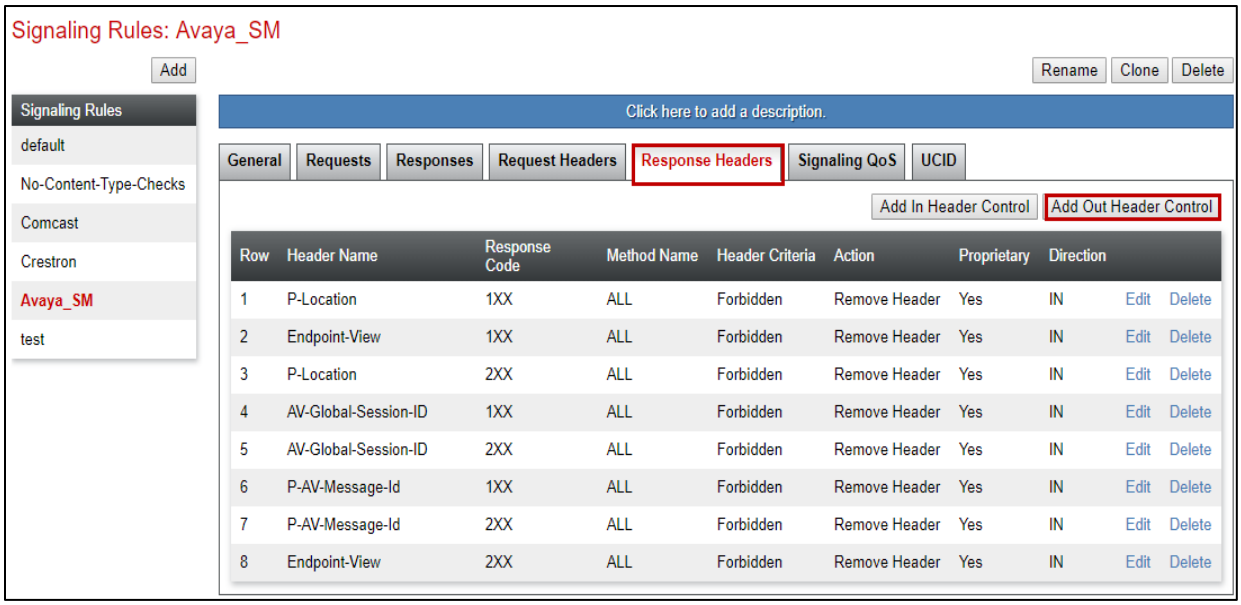

Figure 72 Signaling Rules for Avaya SM continuation

4.4.10 End Point Policy Groups

End Point Policy Group for Avaya SM

- A new End Point Policy Group is created for Avaya Aura Session Manager.
- The **default-low** policy group is used for the Amazon Chime SDK Voice Connector.
- Navigate to: **Domain Policies > End Point Policy Groups**
- Select **default-low** under Policy Groups
- Click **Clone**
- Set *Clone Name*: **Avaya_SM**
- Click **Finish**

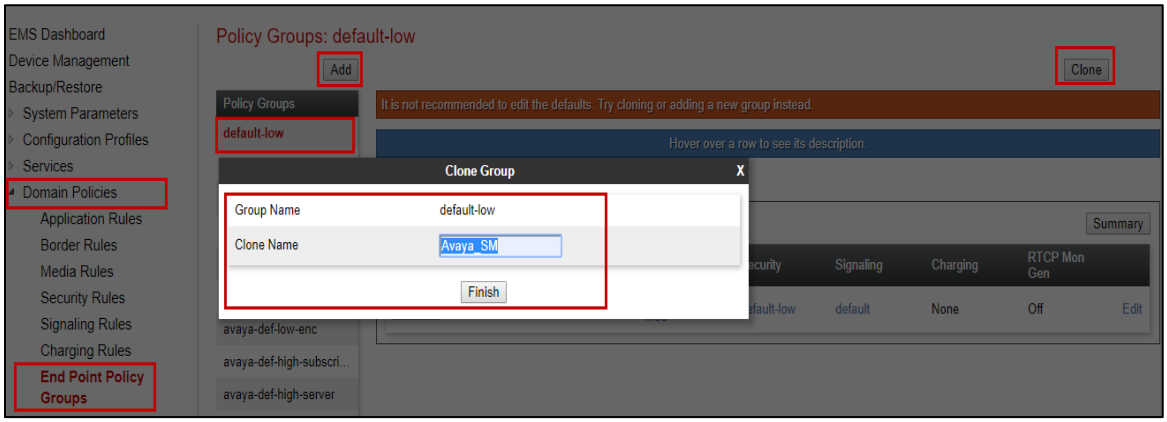

Figure 73 End Point Policy Group for Avaya SM

- Select the newly cleated Group **Avaya_SM**, Click **Edit**
- Set *Signaling Rule*: **Avaya_SM**
- Click **Finish**

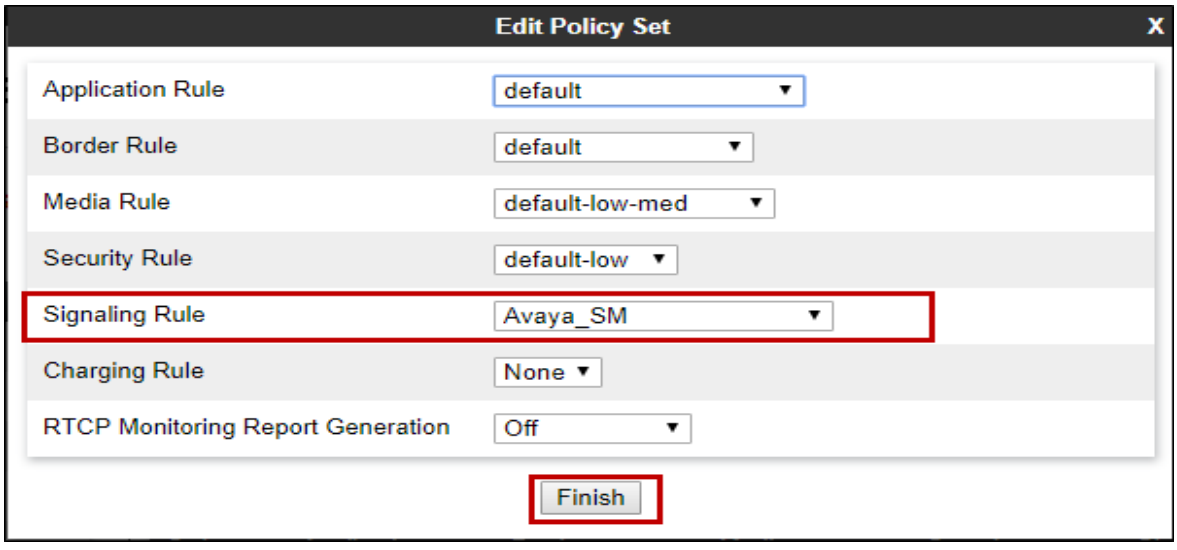

Figure 74 End Point Policy Group for Avaya SM Continuation

End Point Policy Group for PSTN

- Repeat the same steps to create End Policy Group for PSTN

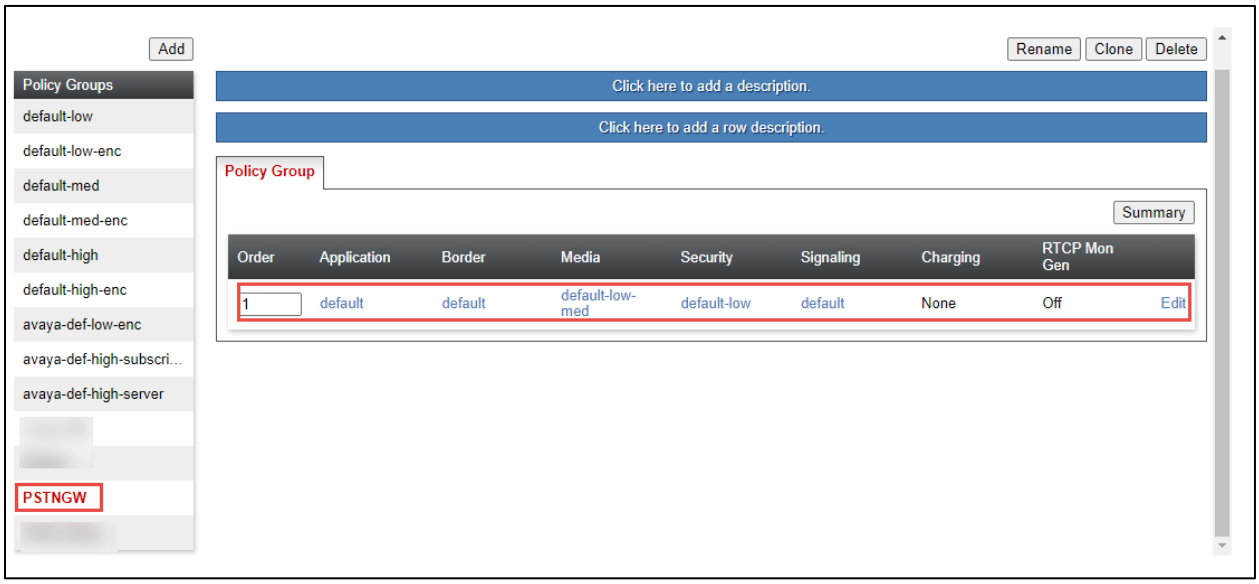

Figure 75 End Point Policy Group for PSTN

End Point Policy Group for Amazon

- Repeat the same steps to create End Policy Group for Amazon Chime SDK Voice Connector
- Select Media Rule: **AWS_MR** (configured in section 4.4.14)

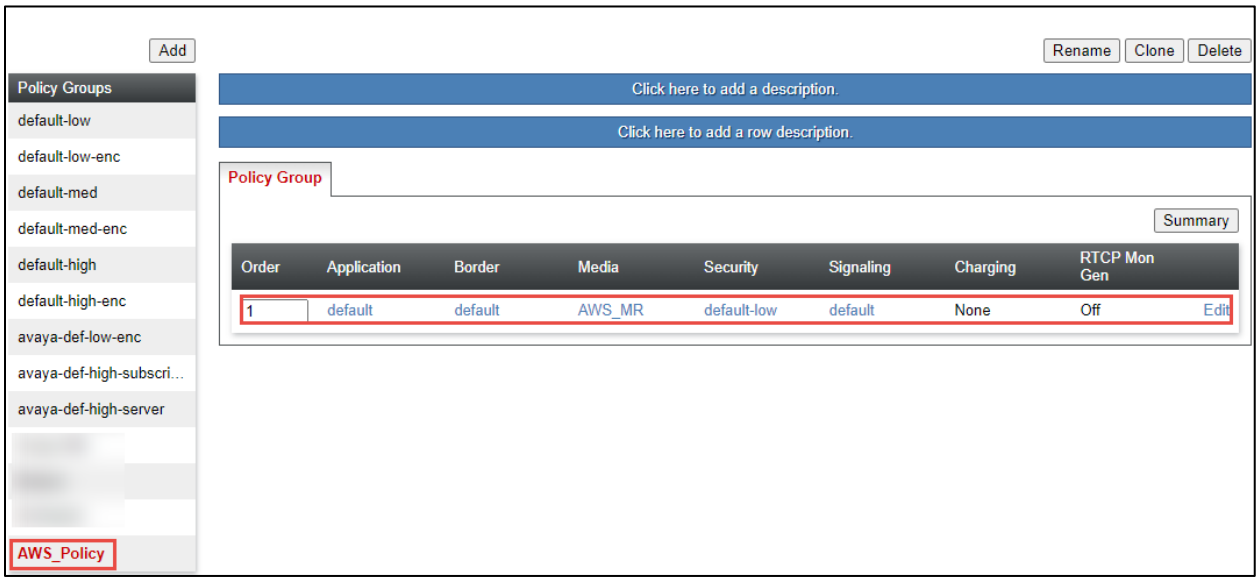

Figure 76 End Point Policy Group for Amazon

4.4.11 Media Interface

- Navigate to: **Network & Flows > Media Interface**. Click **Add**
- Set *Name*: **MI_LAN** is given here
- Set *IP Address*: Select **SBC_LAN** from the drop down and the **IP address** populates automatically. The IP address for Interface facing Avaya Aura SM is 10.70.4.213
- Set *Port Range*: **35000-40000**
- Click **Finish**

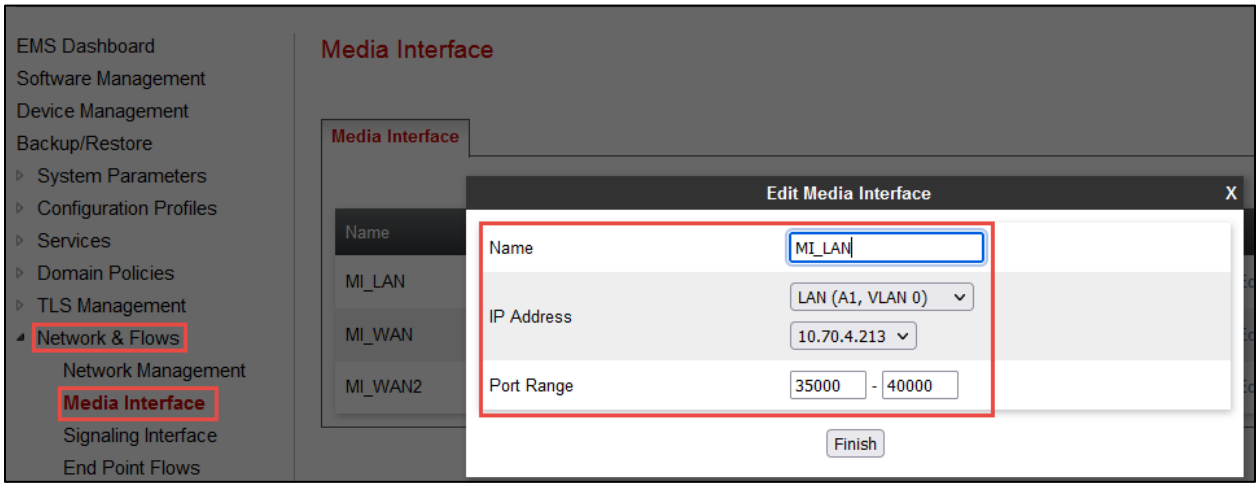

Figure 77 Media Interface facing Avaya SM

- Repeat the same steps to create a Media Interface facing PSTN

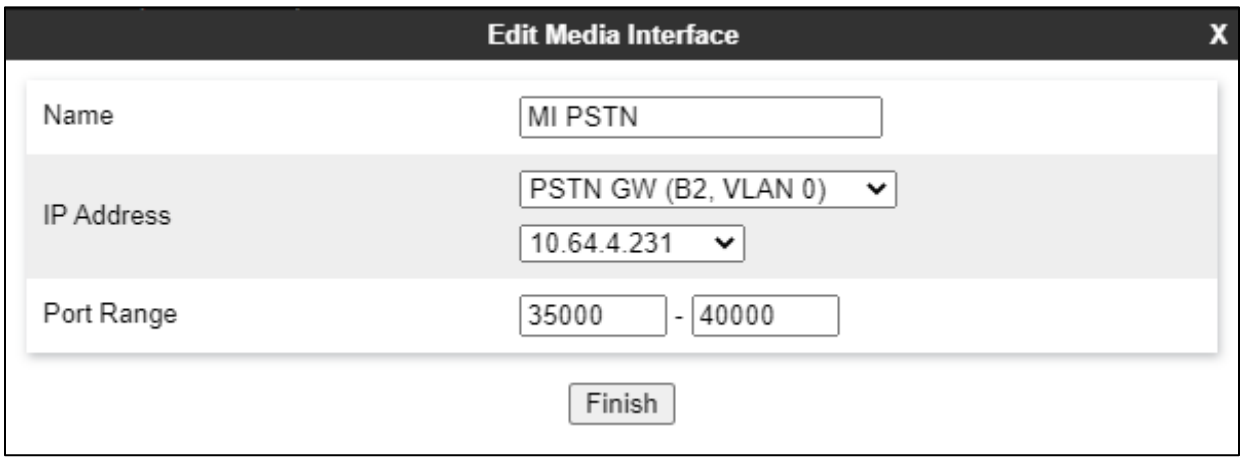

Figure 78 Media Interface facing PSTN

- Repeat the same steps to create a Media Interface facing Amazon Chime SDK Voice Connector

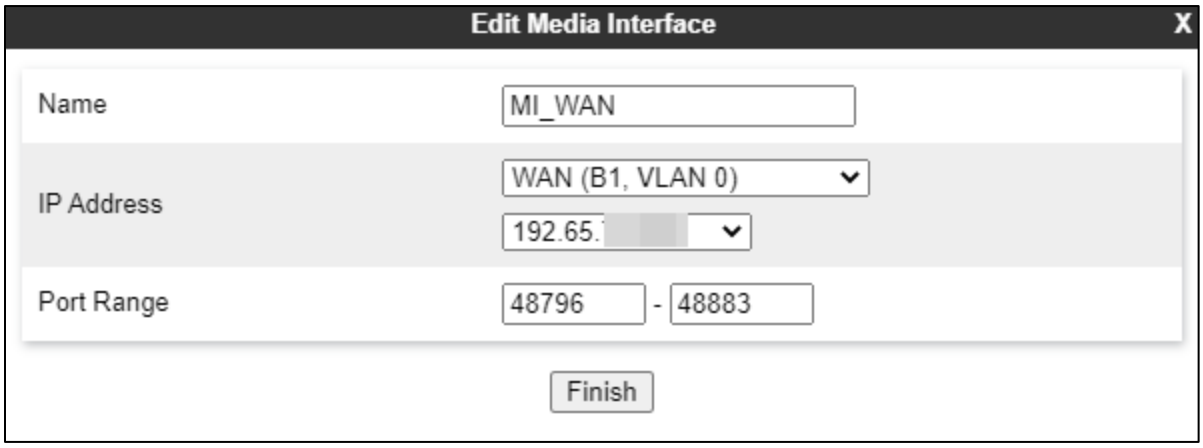

Figure 79 Media Interface facing Amazon

4.4.12 Signaling Interface

Signaling Interface for Avaya SM

- Navigate to: **Network & Flows > Signaling Interface**. Click **Add**, new **Add Signaling Interface** window appears
- Set *Name*: **SI_LAN** is given for the interface facing Avaya Aura SM
- Set *IP Address*: Select **LAN (A1,VLAN 0)**
- Set *UDP Port*: **5060**
- Click **Finish**

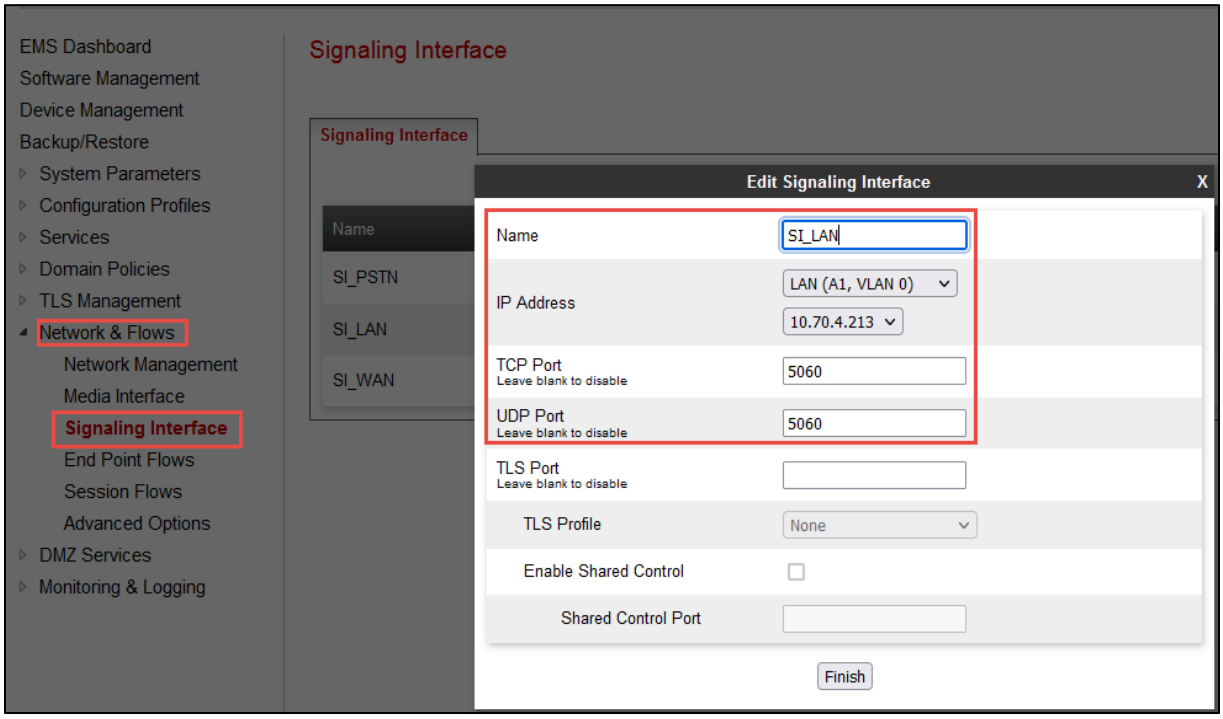

Figure 80 Signaling Interface facing Avaya SM

Signaling Interface for PSTN

- Repeat the same steps to create the Signaling Interface facing PSTN. TCP is used between Avaya SBCE and PSTN.

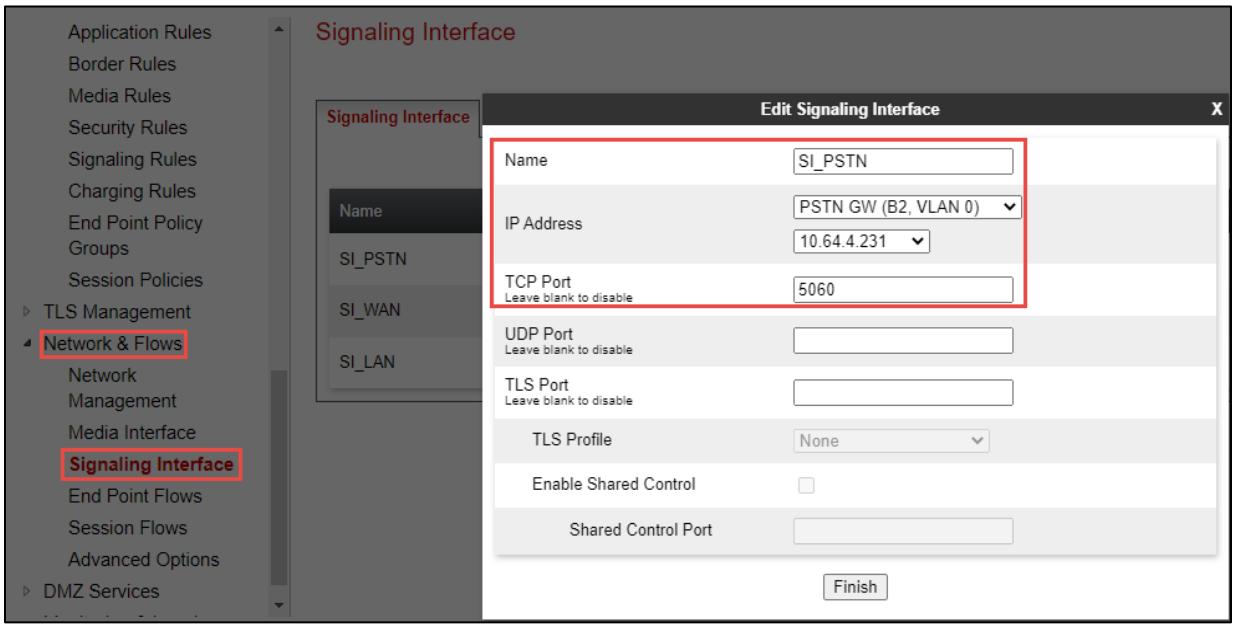

Figure 81 Signaling Interface facing PSTN

Signaling Interface for Amazon Chime SDK Voice Connector

- Repeat the same steps to create the Signaling Interface facing Amazon. TLS is used between Avaya SBCE and Amazon Chime SDK Voice Connector.

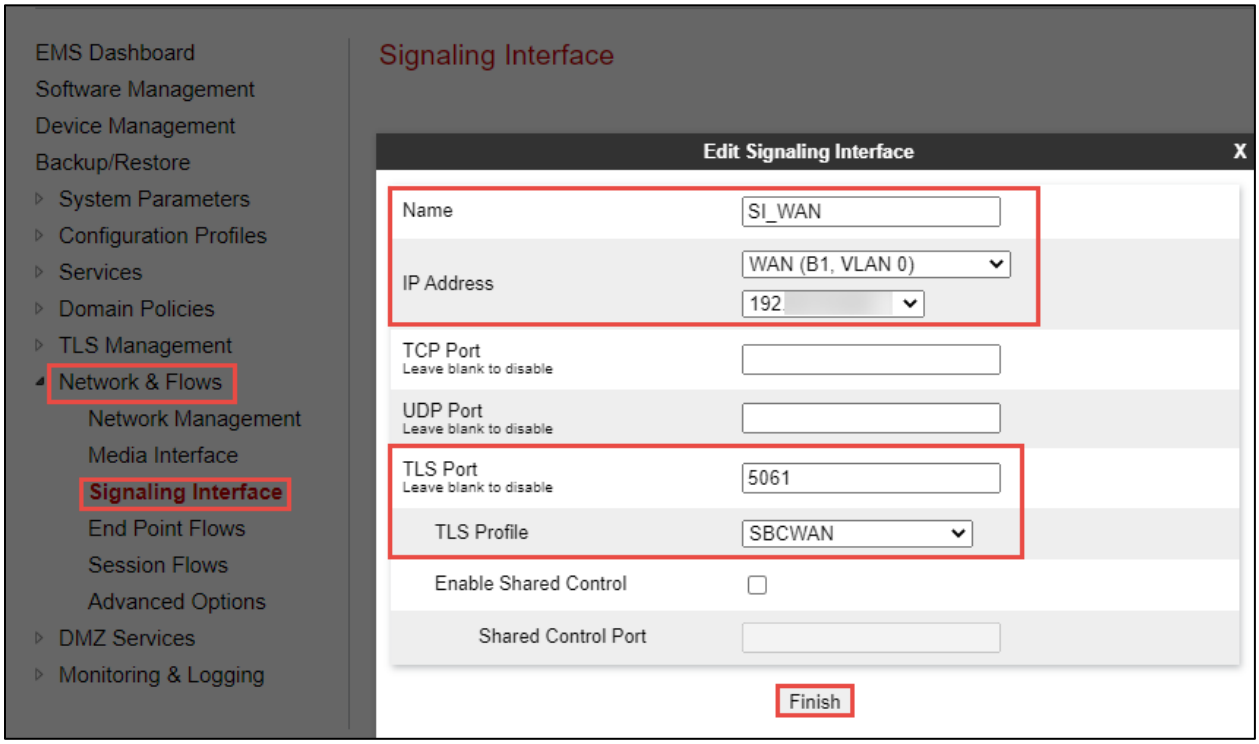

Figure 82 Signaling Interface facing Amazon

4.4.13 End Point Flows

- Navigate to: **Network & Flows > End Point Flows > Server Flows**. Click **Add**
- Set *Flow Name*: **Avaya_SM**
- Set *SIP Server Profile*: **Avaya** created in section 4.4.3 is selected
- Set *Transport*: *****
- Set *Received Interface*: **SI_PSTN**
- Set *Signaling Interface*: **SI_LAN**
- Set *Media Interface*: **MI_LAN**
- Set *End Point Policy Group*: **Avaya SM** (section 4.4.10)
- Set *Routing Profile*: **PSTN_ROUTE** (section 4.4.6)
- Set *Topology Hiding Profile*: **AVAYA_SM** (section 4.4.4)
- Click **Finish**

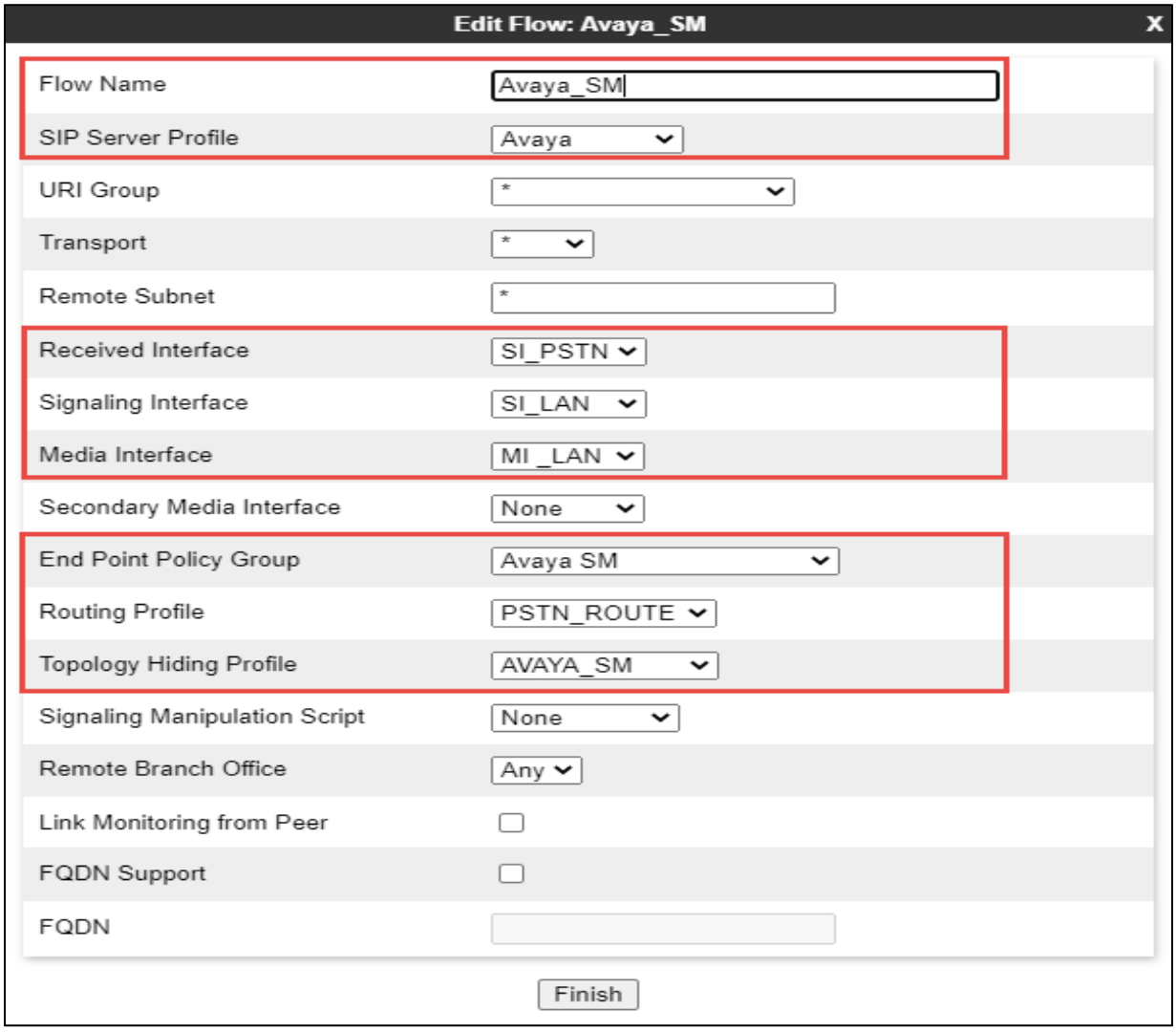

Figure 83 Server Flow for Avaya SM

- Repeat the same steps to create a Server Flow for PSTN.

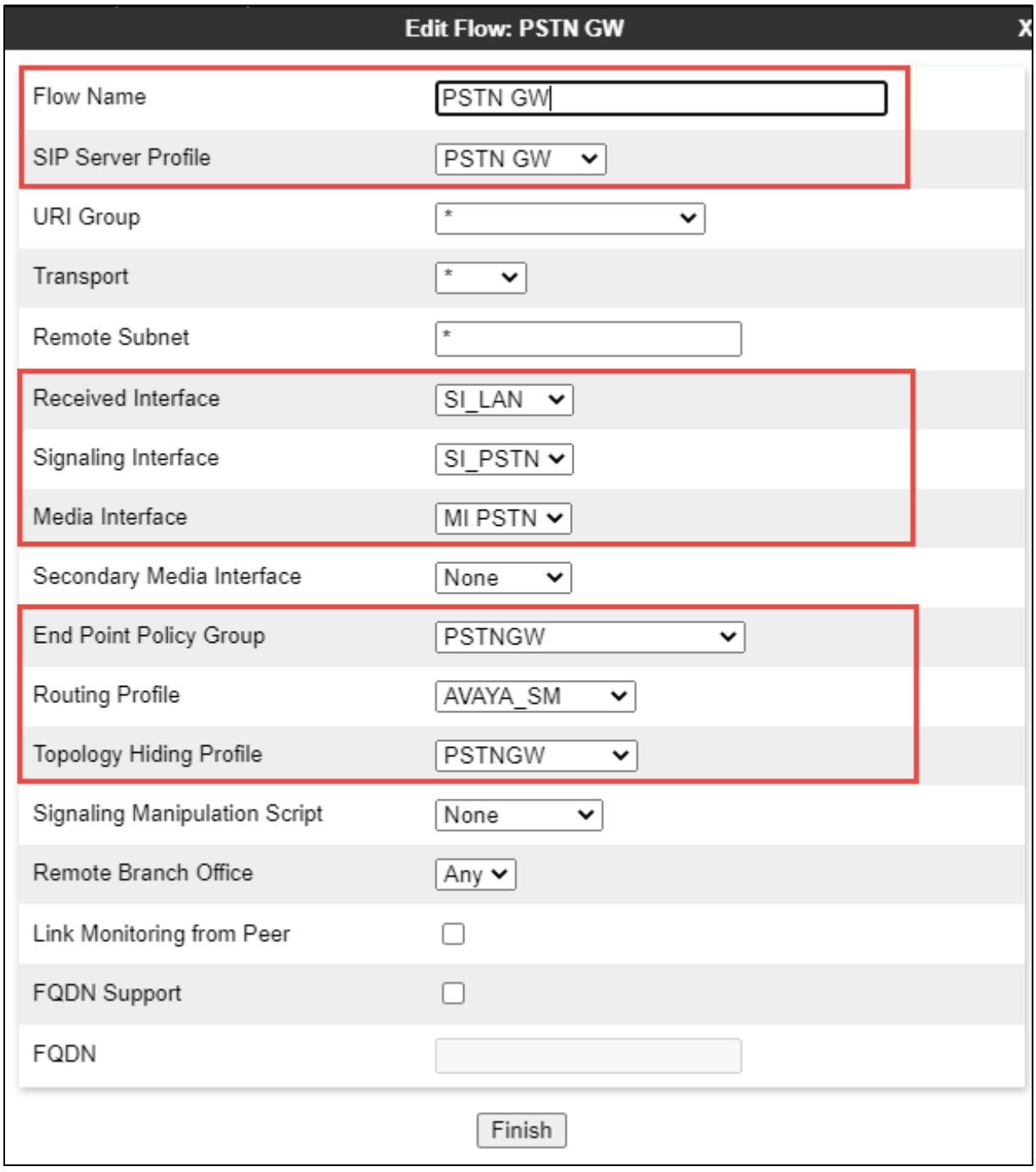

Figure 84 Server Flow for PSTN

- Repeat the same steps to create a Server Flow for Amazon Chime SDK Voice Connector

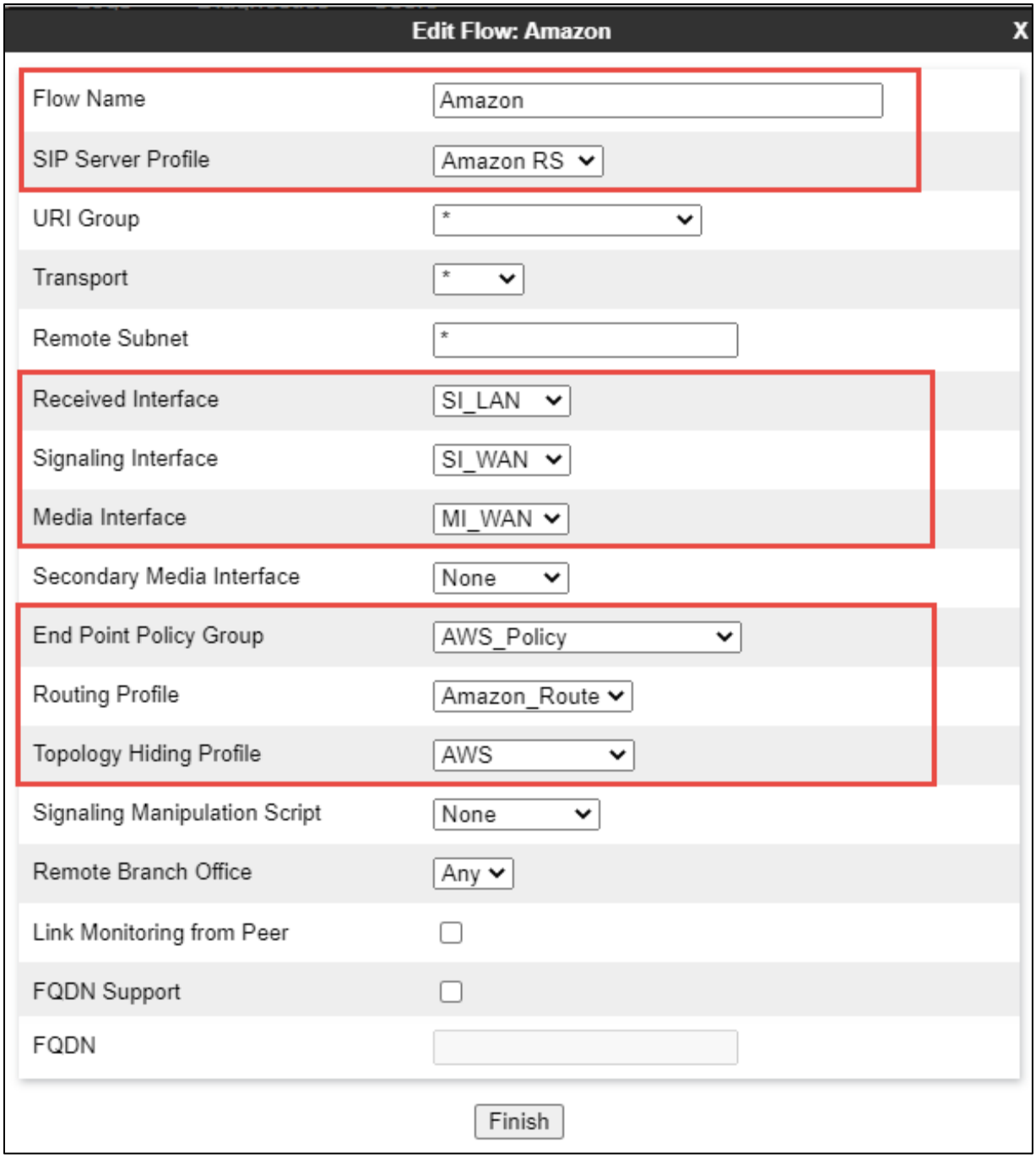

Figure 85 Server Flow for Amazon

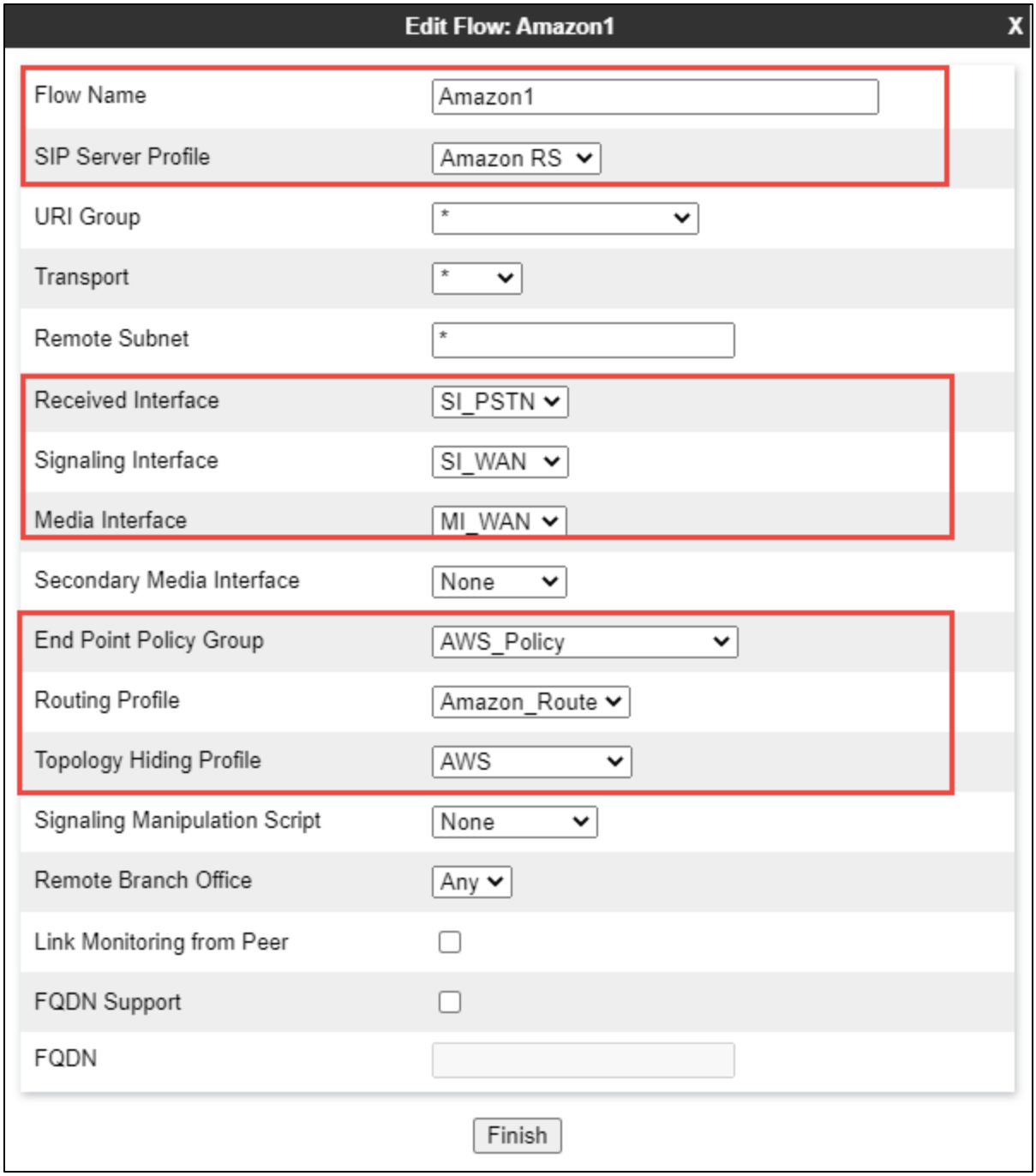

Figure 86 Server Flow for Amazon Continuation

4.4.14 TLS Configuration

The following are necessary steps to configure the protocol TLS between Avaya SBCE and Amazon Chime SDK Voice Connector

- Navigate to: **TLS management > Certificates**. Click **Install**
- Set *Type*: Select **CA Certificate**
- Set *Name*: **AmazonRootCA**
- Set *Allow weak Certificate/Key*: **Checked**
- Set *Certificate File*: Click **Choose File** to select Amazon Root CA
- Click **Upload**

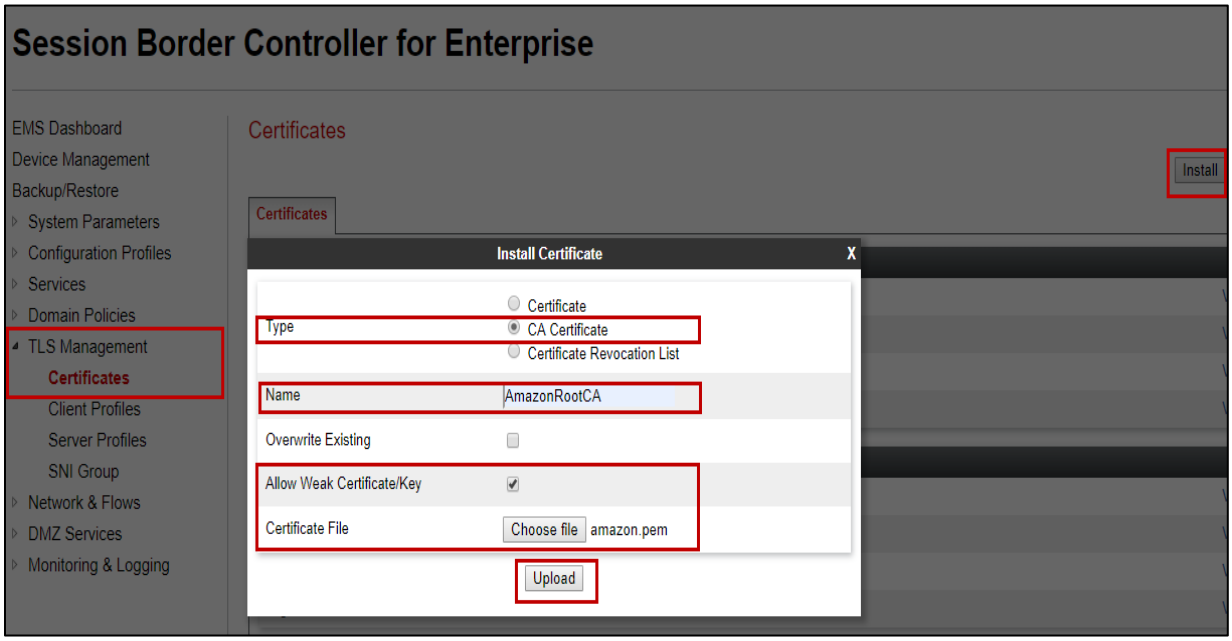

Figure 87 Upload Amazon Root CA

Client Profile for Amazon Chime SDK Voice Connector

- Navigate to: **TLS management > Client Profiles**. Click **Add**
- Set *Profile Name*: **SBCWAN** is given for interface facing Amazon Chime SDK Voice Connector
- Set *Certificate*: select server certificate **asbce10.crt** for Avaya SBCE interface facing Amazon Chime SDK Voice Connector
- Set *Peer Certificate Authorities*: Select **AmazonRootCA.Pem** which is uploaded in previous step
- Set *Verification Depth*: 5
- Click **Next**

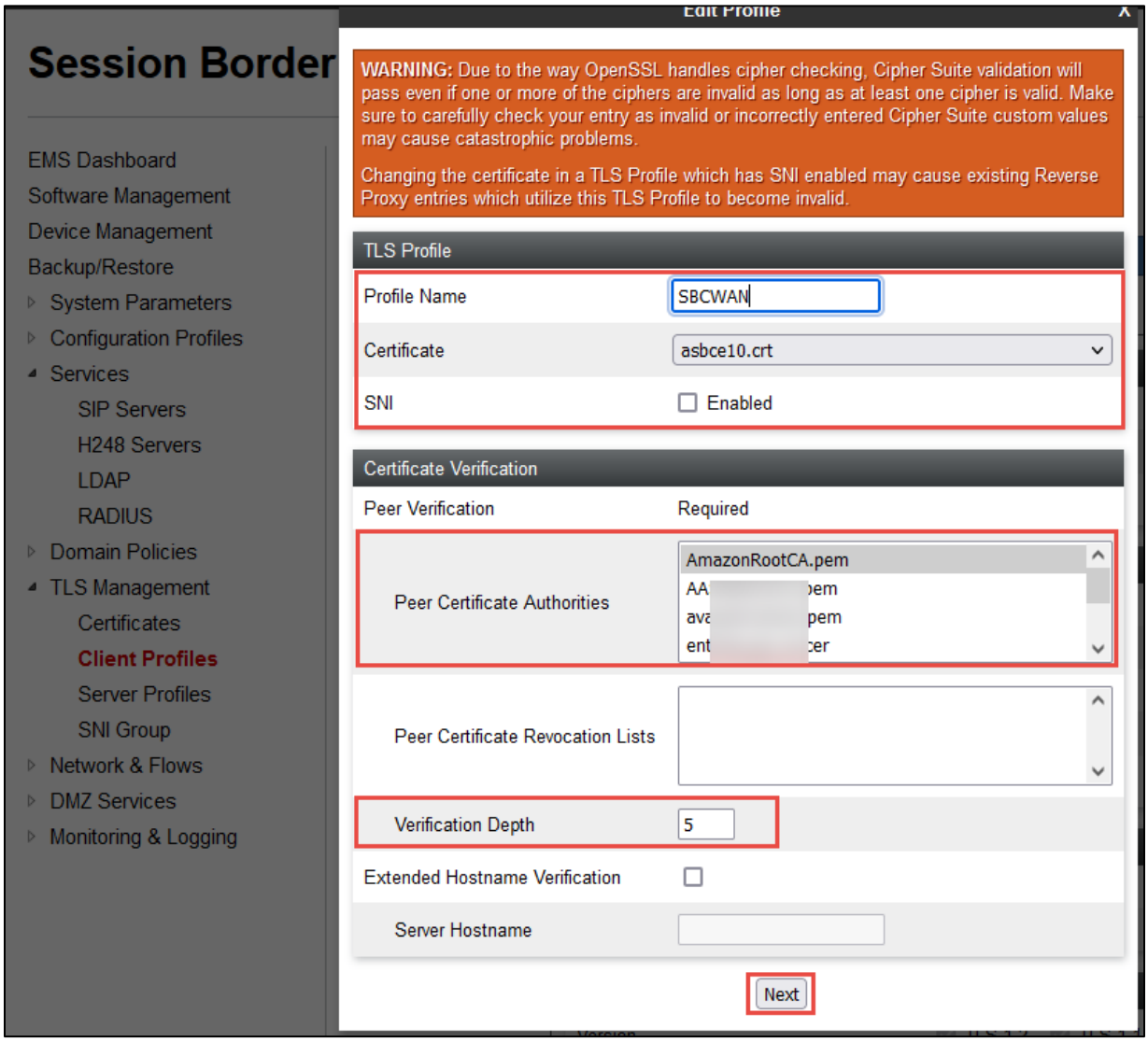

Figure 88 Client Profile facing Amazon

- Set *Version*: Select all **3 TLS versions**
- Click **Finish**

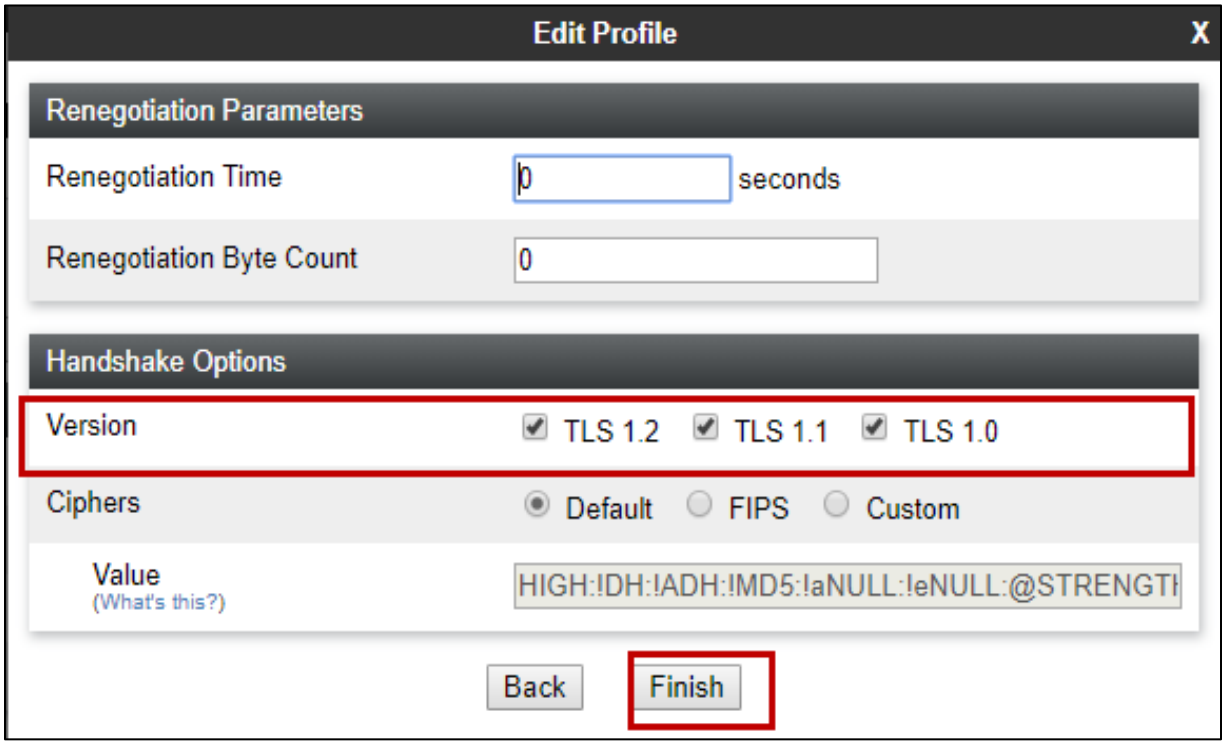

Figure 89 Client Profile facing Amazon Continuation

Server Profile for Amazon Chime SDK Voice Connector

- Navigate to: **TLS management > Server Profiles**. Click **Add**
- Set *Profile Name*: **SBCWAN** is given for interface facing Amazon Chime SDK Voice Connector
- Set *Certificate*: Select server certificate **asbce10.crt** for Avaya SBCE interface facing Amazon Chime SDK Voice Connector
- Set *Peer Verification*: **None**
- Click **Next**

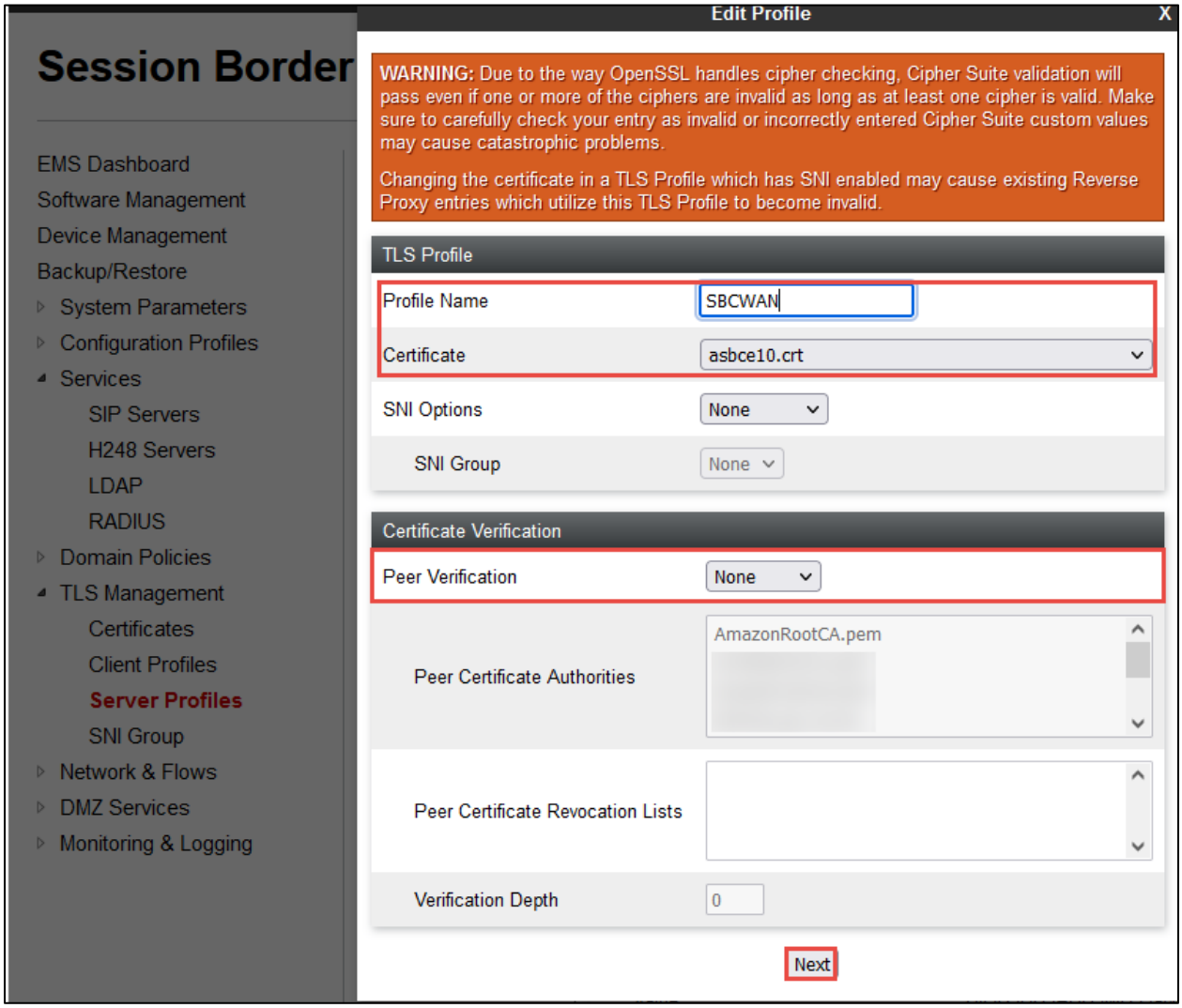

Figure 90 Server Profile facing Amazon

- Set *Version*: Check all **3 TLS versions**
- Click **Finish**

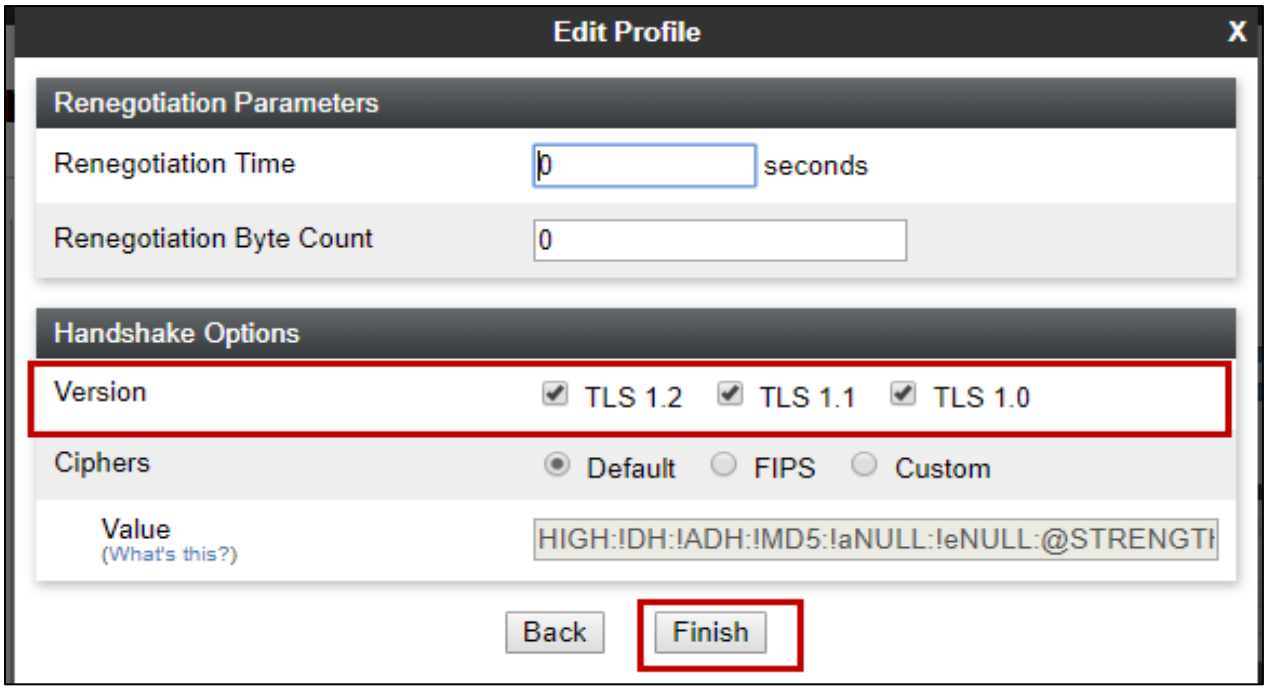

Figure 91 Server Profile facing Amazon Continuation

Configure SRTP

- Navigate to: **Domain Policies > Media Rules**
- Select Media Rule **default-high-enc**, Click **Clone**
- Set *Clone Name*: **AWS MR**
- Click **Finish**

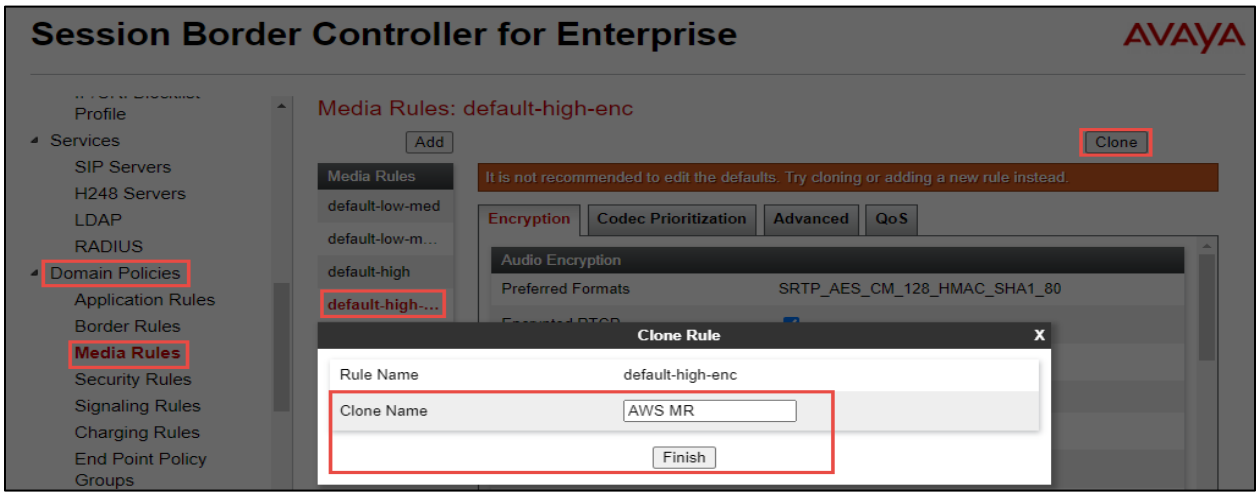

Figure 92 Media Rule – Amazon

- Select newly created Media Rule **AWS MR**, Click **Edit**
- Set Preferred Format #1: **SRTP_AES_CM_128_HMAC_SHA1_80**
- Set Interworking under Audio Encryption: **Unchecked**
- Click **Finish**

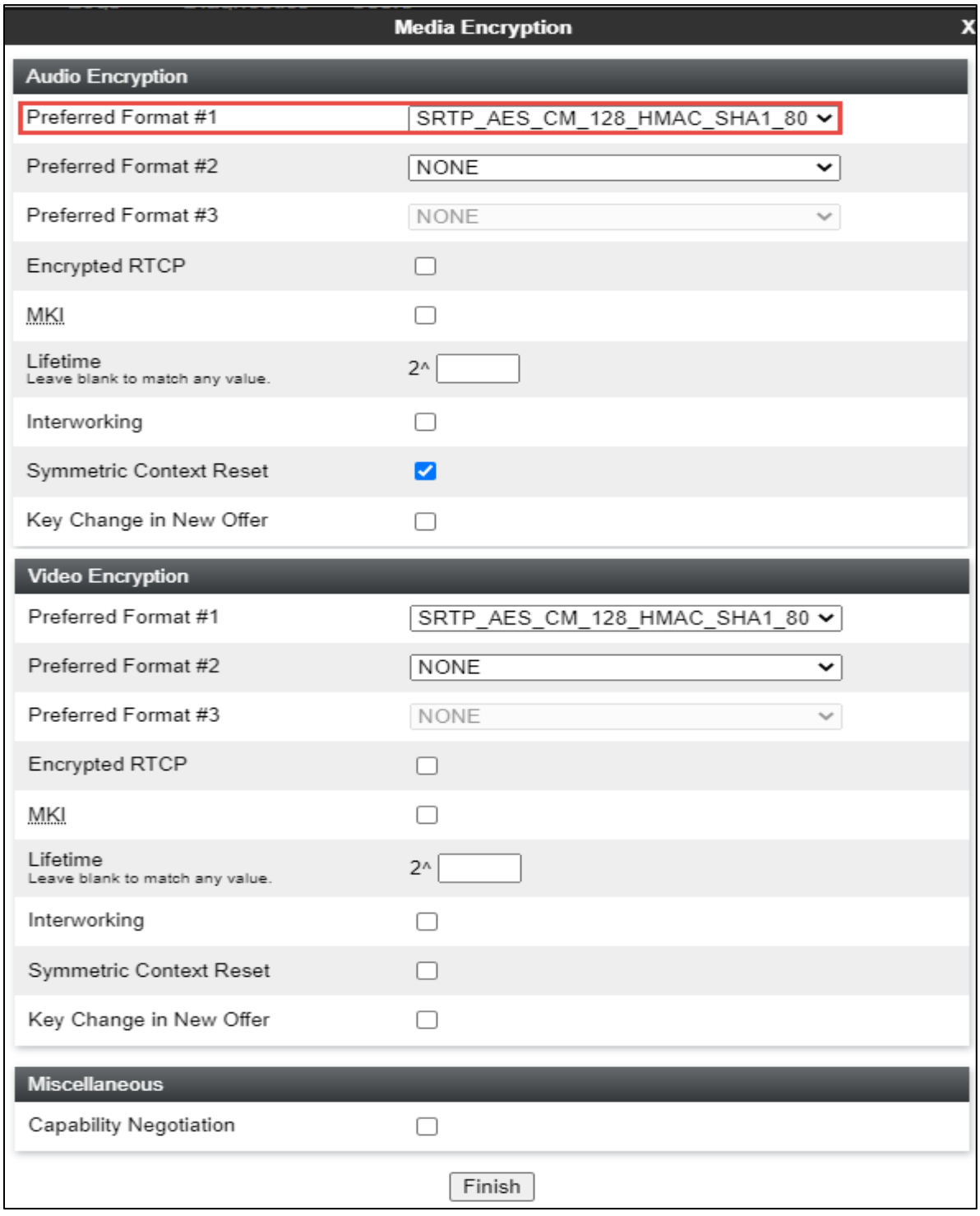

Figure 93 Media Rule – Amazon Continuation

Edit End Point Policy Groups

- Navigate to: **Domain Policies > End Point Policy Groups**
- Select **AWS** under Policy Groups
- Set *Media Rule*: Select **AWS_MR**
- Click **Finish**

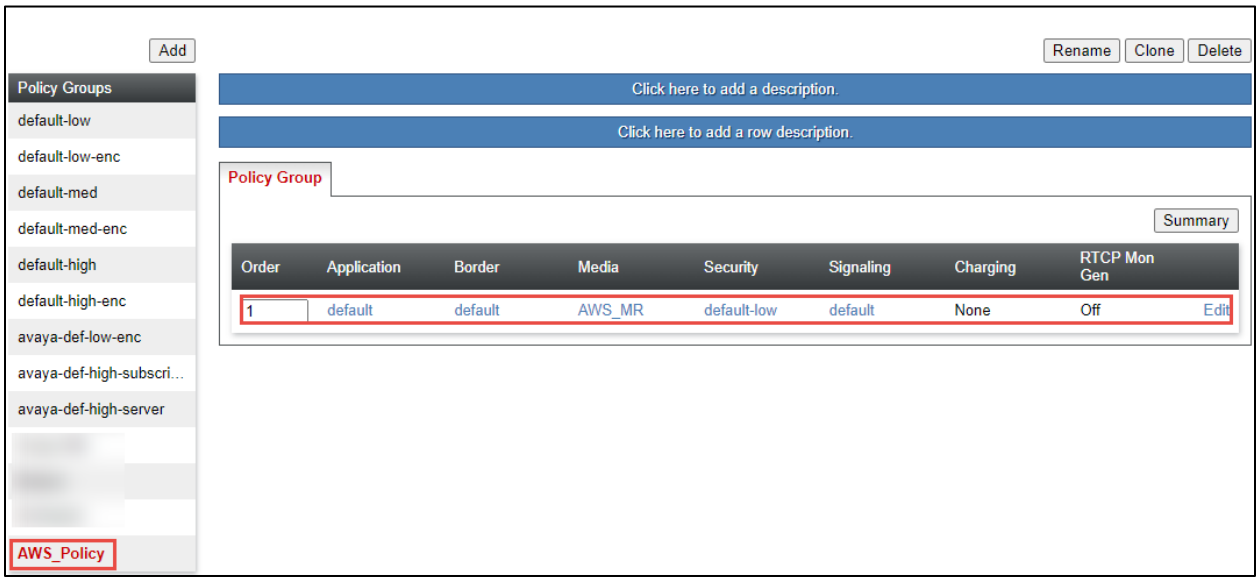

Figure 94 Edit End Point policy Group – Amazon

4.4.15 Signaling Manipulation

- Navigate to **Configuration Profiles>Signaling Manipulation**
- Click **ADD**
- Set *Title:* ***AMZURI***
- *Provide the required manipulation rule and Click* ***Save***

Figure 95 Signaling Manipulation Rule for Amazon