Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 7.2.2 to support Ironton SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 7.2.2 to interoperate with Ironton SIP Trunking Service.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

Ironton SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Ironton's network as an alternative to legacy analog or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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 at the Avaya Solution and Interoperability Test Lab.

©2018 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 4
2. General Test Approach and Test Results 4
   2.1 Interoperability Compliance Testing 5
   2.2 Test Results 6
   2.3 Support 6
3. Reference Configuration 7
4. Equipment and Software Validated 9
5. Configure IP Office 10
   5.1 Licensing 11
   5.2 System 11
      5.2.1 System - LAN1 Tab 11
      5.2.2 System - Telephony Tab 14
      5.2.3 System – VoIP tab 15
      5.2.4 System – VoIP Security Tab 16
   5.3 IP Route 17
   5.4 SIP Line 18
      5.4.1 SIP Line - SIP Line Tab 20
      5.4.2 SIP Line - Transport Tab 21
      5.4.3 Call Details Tab 22
      5.4.4 SIP Line - VoIP Tab 23
      5.4.5 SIP Line – T38 Fax Tab 24
      5.4.6 SIP Line – SIP Advanced Tab 25
   5.5 Users 26
   5.6 Incoming Call Route 27
      5.6.1 Incoming Call Route – Standard Tab 27
      5.6.2 Incoming Call Route – Destinations Tab 28
   5.7 Outbound Call Routing 29
      5.7.1 Short Codes and Automatic Route Selection 29
   5.8 Save Configuration 32
6. Configure Avaya Session Border Controller for Enterprise 33
   6.1 Log in Avaya SBCE 33
   6.2 TLS Management 36
   6.3 Global Profiles 36
      6.3.1 Server Interworking – Avaya-IPO 36
      6.3.2 Server Interworking - SP-General 40
      6.3.3 Server Configuration 43
      6.3.4 Routing Profiles 54
      6.3.5 Topology Hiding 57
   6.4 Domain Policies 60
      6.4.1 Application Rules 60
      6.4.2 Media Rules 62
      6.4.3 End Point Policy Groups 65
   6.5 Device Specific Settings 68
      6.5.1 Network Management 68
      6.5.2 Media Interface 70
      6.5.3 Signaling Interface 72

©2018 Avaya Inc. All Rights Reserved.

6.5.4 End Point Flows 74
7. Ironton SIP Trunking Service Configuration 77
8. Verification and Troubleshooting 78
8.1 Verification Steps 78
8.2 IP Office System Status 78
8.3 IP Office Monitor 80
8.4 Avaya Session Border Controller for Enterprise 81
9. Conclusion 85
10. References 86

©2018 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Ironton SIP Trunking Service and an Avaya SIP-enabled enterprise solution.

In the sample configuration, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500v2 Release 11.0 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 7.2.2 (hereafter referred to as Avaya SBCE), Avaya Communicator for Windows, Avaya Communicator for Web, Avaya Equinox for Windows and Avaya Deskphones, including SIP, H.323, digital, and analog.

The Ironton SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband WAN connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

The terms “service provider” and “Ironton” will be used interchangeable throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by connecting IP Office and the Avaya SBCE to Ironton’s SIP Trunking service across the public internet. The configuration in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). 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.

©2018 Avaya Inc. All Rights Reserved.

2.1 Interoperability Compliance Testing

To verify SIP Trunk interoperability, the following features and functionalities were exercised during the compliance testing:

- SIP Trunk Registration (Dynamic Authentication).
- SIP OPTIONS queries and responses.
- Incoming calls from the PSTN were routed to the DID numbers assigned by Ironton. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x1 Series IP Deskphones (H.323), Avaya 1100 Series IP Deskphones (SIP), Avaya Communicator for Windows, Avaya Communicator for Web, Avaya Equinox for Windows, Avaya 9508 and 1408 Digital Deskphones, and analog Deskphones.
- Outgoing calls to the PSTN were routed via Ironton's network to various PSTN destinations.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. (Testing was performed with codecs: G.711MU and G.729A, Ironton's preferred codec order).
- No matching codecs.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages from PSTN phones).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- T.38 fax.

Note: Remote worker was tested as part of this solution; the configuration necessary to support remote workers is beyond the scope of these Application Notes and is not discussed in these Application Notes.

Items not supported or not tested included the following:

- Inbound toll-free calls, Outbound Toll-Free calls, 911 calls (emergency), "0" calls (Operator), 0+10 digits calls (Operator Assisted) and international calls were not tested.

©2018 Avaya Inc. All Rights Reserved.

2.2 Test Results

Interoperability testing with Ironton was successfully completed with the following observations/limitations.

- **SIP OPTION Messages** – During the compliance test Ironton did not send SIP OPTION messages to IP Office, IP Office did send SIP OPTION messages to Ironton, with Ironton responding with "501 Unsupported Method" instead of a 200 OK, this was sufficient to keep the SIP trunk up in-service.
- **Extra SIP messages sent during Call-Forward and Call-Transfers to the PSTN** – After a call from the PSTN to the enterprise was successfully forwarded or transferred back to another PSTN party using the SIP REFER method, Ironton accepted the SIP REFER messages sent by IP Office with "202 Accepted", which resulted in the SIP trunk channels being released with BYE messages, as expected. After the SIP trunk channels were released IP Office would send "405 Method Not Allowed" and "487 Request Terminated" with Ironton responding with "481 Call Leg Does Not Exist". This behaviour had no negative impact on the transferred call, SIP trunk resources were released successfully after the call transfer, as expected. It's being mentioned here simply as an observation.
- **Caller ID on calls being forwarded to the PSTN** – On calls originated from the PSTN to IP Office stations with the call-forward feature active in the IP Office station to another PSTN number, the caller ID number displayed at the terminating PSTN station was always of the pilot number assigned to the SIP trunk, instead of the originating PSTN number.
- **SIP endpoints may indicate that a transfer failed even when it is successful** – Occasionally on a transfer operation, Avaya IP Office SIP endpoints (Avaya 1100 Series Deskphones and Avaya Communicator for Windows) may indicate on the local call display that the transfer failed even though it was successful. The frequency of this behavior can be reduced by enabling "**Emulate Notify for REFER**" on the IP Office SIP Line (**Section 5.4.6**).
- **Fax support** – Incoming and outgoing fax calls using the G.711 pass-through method failed during the compliance test. T.38 fax calls were successful in both directions (incoming and outgoing). The issue may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay. T.38 Fax Transport should be use with this solution.
- **Conference on Avaya Equinox soft-client** – Conference on the Avaya Equinox for Windows soft-client is not working properly. When the attempt is made to conference active calls in the Avaya Equinox for Windows soft-client by "merging" the calls together, the parties are not joined together into conference, instead a new call is made from the first active call that was held by the Equinox soft-client to the second active call held by the Equinox soft-client, with the Avaya Equinox soft-client unable to merge the active calls together into conference. This issue was only seen on the Avaya Equinox for Windows soft-client. There is no current work-around; if the conference feature is needed on an Avaya soft-client for IP office the Avaya Communicator for Windows soft-client could be used until this issue is resolved by Avaya. This issue is under investigation by Avaya.

2.3 Support

For support on Ironton systems visit the corporate Web page at: https://www.ironton.com/

©2018 Avaya Inc. All Rights Reserved.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 below illustrates the test configuration used. It shows a simulated enterprise site connected to Ironton's network through the public internet.

For confidentiality and privacy purposes, actual public IP addresses and PSTN routable phone numbers (DIDs) used during the compliance testing have been replaced with fictitious IP addresses and PSTN non-routable phone numbers throughout the Application Notes.

The Avaya components used to create the simulated enterprise customer site includes:

- Avaya IP Office 500v2.
- Avaya IP Office Application Server running Avaya Voicemail Pro, Avaya one-X® Portal for IP Office and Avaya WebRTC Gateway.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 11x0 Series SIP IP Deskphones.
- Avaya Communicator for Windows.
- Avaya Equinox for Windows.
- Avaya Communicator for Web.
- Avaya 1408 and 9508 Digital Deskphones.

Located at the edge of the enterprise is the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **B1** is used to connect to the public network, interface **A1** is used to connect to the private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

Also located at the enterprise site is Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codec's. The IP Office **LAN1** interface connects to the inside (A1) interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE (B1) connects to Ironton's network via the public Internet.

The transport protocol between the Avaya SBCE and Ironton, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is SIP over TLS.

For inbound calls, the calls flowed from Ironton to the Avaya SBCE, then to IP Office.

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk, the call was routed to the Avaya SBCE for egress to Ironton's network.

©2018 Avaya Inc. All Rights Reserved.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Ironton's network (refer to **Section 5.7**). The short code 9 was stripped off by IP Office but the remaining N digits were sent unaltered to the network.

In an actual customer configuration, the enterprise site may include additional network components between the service provider and the Avaya IP Office system, such as a session border controller or data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that all SIP and RTP traffic between the service provider and the Avaya IP Office system must be allowed to pass through these devices.

Figure 1: Avaya Interoperability Test Lab Configuration.

©2018 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	11.0.0.0 Build 849
Avaya IP Office DIG DCPx16 V2	11.0.0.0 Build 849
Avaya IP Office Manager	11.0.0.0 Build 849
Avaya IP Office Application Server ▪ Voicemail Pro ▪ Avaya WebRTC Gateway ▪ Avaya one-X® Portal for IP Office	11.0.0.0 Build 849 11.0.0.0 build 481 11.0.0.0 build 849 11.0.0.0 build 457
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.2.2.0-11-15522
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6604
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya Communicator for Windows	2.1.4.0
Avaya Equinox™ for Windows	3.4.5.10.3
Avaya Communicator for Web	1.0.16.2220
Avaya Digital Deskphones 1408	R48
Avaya Digital Deskphones 9508	R60
Lucent Analog Phone	--
Ironton	
PortaOne Soft Switch	MR55
Genband S3	9.3.1

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500v2 also when deployed with all configurations of IP Office Server Edition.

©2018 Avaya Inc. All Rights Reserved.

5. Configure IP Office

This section describes the IP Office configuration required to interwork with Ironton. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. A screen that includes the following may be displayed.

Select **Open Configuration from System**. If the above screen does not appear, the configuration may be alternatively opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window. Select the proper IP Office from the pop-up window, and log in with the appropriate credentials.

The appearance of the Avaya IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the Group pane has been omitted, its content is shown as submenus in the Navigation pane. These panes (Navigation and Details) will be referenced throughout the IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the service provider is assumed to already be in place.

In the sample configuration, the MAC address **00E00706530F** was used as the system name. All navigation described in the following sections (e.g., **License → SIP Trunk Channels**) appears as submenus underneath the system name **00E00706530F** in the Navigation Pane.

©2018 Avaya Inc. All Rights Reserved.

5.1 Licensing

The configuration and features described in these Application Notes require the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

To verify that there is a SIP Trunk Channels License with sufficient capacity, click **License** in the Navigation pane and examine **SIP Trunk Channels** in the Detail pane. Confirm that there is a valid license with sufficient "Instances" (SIP Trunk Channels) in the Details pane.

5.2 System

Configure the necessary system settings. In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.1 System - LAN1 Tab

In the sample configuration, the MAC address **00E00706530F** was used as the system name and the **LAN** port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to Ironton's network via the public internet. The **LAN1** settings correspond to the **LAN** port in IP Office. To access the **LAN1** settings, navigate to **System (1) → 00E00706530F** in the Navigation Pane, then in the Details Pane navigate to the **LAN1→ LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters:

- Set the **IP Address** field to the LAN IP address, e.g., **192.168.128.167**.

©2018 Avaya Inc. All Rights Reserved.

- Set the **IP Mask** field to the subnet mask of the enterprise private network, e.g., **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

The **VoIP** tab as shown in the screenshot below was configured with following settings:

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Select **Preferred** under **H.323 Signaling over TLS**. When enabled, TLS is used to secure the registration and call signaling communication between IP Office and endpoints that support TLS. The H.323 phones that support TLS are 9608, 9611, 9621, and 9641 running firmware version 6.6 or higher.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Ironton.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **SIP Domain Name**.
- Enter the SIP Registrar FQDN of the enterprise under **SIP Registrar FQDN**.
- Check TLS and verify the **TLS Port** numbers under **Layer 4 Protocol** is set to **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP-RTCP**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP and RTCP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP/RTCP traffic is present.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

Note: In the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.2 System - Telephony Tab

Navigate to the **Telephony → Telephony** tab in the Details Pane, configure the following parameters:

- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

5.2.3 System – VoIP tab

For **Codec** settings, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **VoIP** tab and configure the following parameters:

- Select or enter **101** for **RFC2833 Default Payload**. This setting was recommended by Ironton for use with out-of-band DTMF tone transmissions.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific extension. The example below shows the codecs used for IP phones (SIP and H.323). The system's default codecs and order was used.

Note: The codec selections defined under this section (System – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.4** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

©2018 Avaya Inc. All Rights Reserved.

5.2.4 System – VoIP Security Tab

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

Configuring the use of SRTP at the system level is done on the **System VoIP Security** tab using the Media Security setting. The options are:

- Disabled (default).
- Preferred.
- Enforced.

When enabling SRTP on the system, the recommended setting is **Preferred**. In this scenario, IP Office uses SRTP if supported by the far-end, otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the far-end, the call is not established.

To configure the use of SRTP, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **VoIP Security** tab and configure the following parameters:

- Under **Media** select **Preferred** from the pull-down menu.
- Verify that **Strict SIPS** is not checked.
- Under **Media Security Options** ensure that **RTP** is checked under **Encryptions** and **Authentication**.
- Under **Crypto Suites** ensure that **SRTP_AES_CM_128_SHA1_80** is checked.
- Click **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

5.3 IP Route

Create an IP route to specify the IP address of the gateway or router where IP Office needs to send the packets in order to route calls to Ironton's network (if located in a different IP subnet).

In the reference configuration, the IP Office LAN1 interface and the private interface of Avaya SBCE resided in different IP subnets, so an IP route was necessary to specify the IP address of the gateway or router where IP Office needs to send the packets, in order to reach the IP subnet of the private interface of Avaya SBCE.

To create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides (if located in different IP subnets), on the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** of the IP subnet of the private side of the Avaya SBCE, or enter **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office IP subnet.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

5.4 SIP Line

DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., *\temp*) on the same computer where IP Office Manager is installed.

To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template→Open from file**.

©2018 Avaya Inc. All Rights Reserved.

Navigate to the directory on the local machine where the template was copied and select the template.

After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**

The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line **17**).

It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.1** to **5.4.6**.

©2018 Avaya Inc. All Rights Reserved.

5.4.1 SIP Line - SIP Line Tab

On the **SIP Line** tab in the Details Pane, configure or verify the parameters as shown below.

- Leave the **ITSP Domain Name** blank. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- Verify that **URI Type** is set to **SIP URI**.
- Verify that **In Service** box is checked, which is the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (seconds)** is set to **On Demand**.
- Under **Redirect** and **Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Always**.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

5.4.2 SIP Line - Transport Tab

Select the **Transport** tab; configure the parameters as shown below:

- Set the **ITSP Proxy Address** to the inside IP Address of the Avaya SBCE or **10.64.101.243** as shown in **Figure 1**.
- Set the **Layer 4 Protocol** to **TLS**.
- Set **Use Network Topology Info** to **None** (see note below).
- Set the **Send Port** to **5061**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

Note – For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was used in the test configuration. In addition, it was not necessary to configure the **System → LAN1 → Network Topology** tab for the purposes of SIP trunking. If a NAT is used between Avaya IP Office and the other end of the trunk, then the **Use Network Topology Info** field should be set to the LAN interface (LAN1) used by the trunk and the **System → LAN1 → Network Topology** tab needs to be configured with the details of the NAT device.

©2018 Avaya Inc. All Rights Reserved.

5.4.3 Call Details Tab

A SIP URI entry needs to be created to match each incoming number that IP Office will accept on this line. Select the **Call Details** tab, and then click the **Add…** button and the screen shown below will appear. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button. In the example screen below a new entry was added. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an IP Office user. The entry was created with the parameters shown below:

- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Set the **Credentials** field to **0:<None>**
- Set the **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** fields to the values shown in the screenshot below.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).
- Click **OK** to commit again (not shown).

©2018 Avaya Inc. All Rights Reserved.

5.4.4 SIP Line - VoIP Tab

Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- In the sample configuration, the **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line. As shown, the codec order of **G.711 ULAW** and **G.729(a**) were selected for audio.
- Set **Fax Transport Support** to **T.38**.
- Set the **DTMF Support** field to **RFC2833**. This directs IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** field to **Same as System (Preferred)**.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check the **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.3** (System – VoIP tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

©2018 Avaya Inc. All Rights Reserved.

5.4.5 SIP Line – T38 Fax Tab

Select the **T38 Fax** tab, to set the Fax over Internet Protocol parameters of the SIP Line. Set or verify the parameters as shown below:

- Uncheck the **Use Default Values** at the bottom of the screen.
- Set the **T.38 Fax Version** to **0**, Ironton supports T.38 fax version 0.
- Default values may be used for all other parameters.

©2018 Avaya Inc. All Rights Reserved.

5.4.6 SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab.

- Verify that **Call Routing Method** is set to **Request URI**.
- Check the box for **Use PAI for Privacy**.
- Check the box for **Emulate NOTIFY for REFER** (**Section 2.2**).
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

5.5 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.4**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Ext3040 H323**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP Line (**Section 5.4.3**). The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Ironton, note that the "1" was included. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network. This can also be accomplished by activating Withhold Number on H.323 Deskphones (not shown). Click the **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

5.6 Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system. In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** (**Section 5.4.6**) and **SIP URI** (**Section 5.4.3**) and the users **SIP Name** and **Contact**, already populated with the assigned Ironton DID numbers (**Section 5.5**).

5.6.1 Incoming Call Route – Standard Tab

To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**.

On the **Standard** tab of the Details Pane, enter the parameters as shown below.

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4**.
- Default values can be used for all other fields.

©2018 Avaya Inc. All Rights Reserved.

5.6.2 Incoming Call Route – Destinations Tab

- Under the **Destinations** tab, enter "**.**" for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User**, which matches the number present on the user part of the incoming Request URI.
- Click **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

5.7 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance testing.

5.7.1 Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** on the Navigation Pane and select **New**. The screen below shows the short code **9N** created (note that the semi-colon is not used here). In this case, when the IP Office user dials 9 plus any number **N**, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS.

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **9N** was used (note that the semi-colon is not used here).
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group ID** to **50: Main** to be directed to **Line Group 50: Main**, which is configurable via ARS.
- Click the **OK** to commit (not shown).

©2018 Avaya Inc. All Rights Reserved.

The following screen shows a sample ARS configuration for the route **50: Main**. Note the sequence of **X**'s used in the **Code** field of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

To create a short code to be used for ARS, select **ARS → 50: Main** on the Navigation Pane and click **Add** (not shown).

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **1** followed by **10 X**'s to represent the exact number of digits.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **1N**. The value **N** represents the additional number of digits dialed by the user after dialing **1** (The **9** will be stripped off).
- Set the **Line Group ID** to the Line Group number being used for the SIP Line, in this case **Line Group ID 17** was used.
- Set the **Locale** to the specific country and language, in this case **United States (US English)**.
- Click **OK** to commit.

Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

©2018 Avaya Inc. All Rights Reserved.

The highlighted entry below of **1** plus **10** digits (represented by **10 X**'s) was used to make call within the North American Numbering Plan (NANP).

The user dialed **9**, followed by **1** and **10** digits (represented by **10 X**'s). The **9** is stripped off, the remaining digits, including the **1**, are included in the SIP INVITE message IP Office sends to Ironton.

©2018 Avaya Inc. All Rights Reserved.

5.8 Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections.

The following will appear, with either **Merge** or **Immediate** selected, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to proceed.

©2018 Avaya Inc. All Rights Reserved.

6. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to Ironton SIP Trunking Service.

It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

6.1 Log in Avaya SBCE

Use a Web browser to access the Avaya SBCE Web interface. Enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the Avaya SBCE management IP address.

Enter the appropriate credentials and click **Log In**.

©2018 Avaya Inc. All Rights Reserved.

The **Dashboard** main page will appear as shown below.

To view the system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya_SBCE** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.

©2018 Avaya Inc. All Rights Reserved.

The **System Information** window is displayed as shown below.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.

On the previous screen, **A1** corresponds to the inside interface (Private Network side) and **B1** corresponds to the outside interface (Public Network side) of the Avaya SBCE. (Refer to **Figure 1**).

The management IP was blurred out for security reasons. The IP addresses used for the remote worker configuration were also blurred out since the remote worker configuration is beyond the scope of these Application Notes and is not discussed in these Application Notes.

Note: Valid public DNS IP addresses are required with this solution.

©2018 Avaya Inc. All Rights Reserved.

6.2 TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

For the compliance testing, the transport protocol that was used between IP Office and the Avaya SBCE, across the enterprise private IP network (LAN), was SIP over TLS. SIP over UDP was used between the Avaya SBCE and Ironton, across the public Internet.

It is assumed that generation and installation of certificates and the creation of TLS Profiles on the Avaya SBCE have been previously completed, as it's not discussed in this document. Refer to item [**10**] in **Section 10**.

6.3 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

6.3.1 Server Interworking – Avaya-IPO

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned". If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution.

On the left navigation pane, select **Global Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone** on top right of the screen (not shown).

Enter the new profile name in the **Clone Name** field, the name of ***Avaya-IPO*** was chosen in this example. Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

Click **Edit** on the newly cloned ***Avaya-IPO*** interworking profile:

- On the **General** tab, check ***T.38 Support***.
- Leave remaining fields with default values.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **Avaya-IPO** Server Interworking Profile.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **Avaya-IPO** Server Interworking Profile.

©2018 Avaya Inc. All Rights Reserved.

6.3.2 Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the Service Provider.

On the left navigation pane, select **Global Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **Add** (not shown) (note that **Add** is being used to create the SP-General profile instead of cloning the avaya-ru profile).

Enter the new profile name, the name of ***SP-General*** was chosen in this example.

- Click **Next**.

©2018 Avaya Inc. All Rights Reserved.

On the **General** tab, check ***T.38 Support***. Click **Next**, and then click **Finish** on the last tab leaving remaining fields with default values (not shown).

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.

6.3.3 Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (IP Office) and the Trunk Server or SIP Proxy at the service provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** (not shown). Click **Add Profile** (not shown) and enter the profile name: ***IP Office***.

- Click **Next**.

On the **Add Server Configuration Profile** window:

- **Server Type:** Select ***Call Server***.
- **IP Address / FQDN**: ***192.168.128.167*** (IP Address of IP Office).
- **Port:** ***5061*** (This port must match the port number defined in **Section 5.4.2**).
- **Transport**: Select ***TLS***.

©2018 Avaya Inc. All Rights Reserved.

- Select a **TLS Client Profile**.
- Click **Next**.

- Click **Next** on the **Add Server Configuration Profile - Authentication** window (not shown).
- Click **Next** on the **Add Server Configuration Profile - Heartbeat** window (not shown).
- Click **Next** on the **Add Server Configuration Profile - Registration** window (not shown).
- Click **Next** on the **Add Server Configuration Profile - Ping** window (not shown).

On the **Add Server Configuration Profile - Advanced** tab:

- Select ***Avaya-IPO*** from the **Interworking Profile** drop down menu (**Section 6.3.1**).
- Leave the **Signaling Manipulation Script** at the default ***None***.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **IP Office** Server Configuration Profile.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **IP Office** Server Configuration Profile.

To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** (not shown) section and enter the profile name: ***Service Provider UDP***.

- Click **Next**.

©2018 Avaya Inc. All Rights Reserved.

On the **Edit Server Configuration Profile - General** window:

- **Server Type**: Select **Trunk Server**.
- **DNS Query Type**: Select **NONE/A**
- **IP Address / FQDN**: **sip.test.com** (Ironton's SIP proxy server FQDN).
- **Port: 5060**.
- **Transports**: Select **UDP**.
- Click **Next**.

On the **Add Server Configuration Profile - Authentication** tab:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration, the pilot number provided by Ironton for registration purpose was used.
- Leave the **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

- Click **Next** on the **Add Server Configuration Profile - Heartbeat** window (not shown).

©2018 Avaya Inc. All Rights Reserved.

On the **Add Server Configuration Profile - Registration** tab:

- Check the **Register with All Servers** box.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **30** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI**: Use the **User Name** entered above in the **Authentication** screen (**16107941234**) and the Service Provider's SIP proxy server FQDN (**sip.test.com**), as shown on the screen below.
  - **To URI**: Use the **User Name** entered above in the **Authentication** screen (**16107941234**) and the Service Provider Proxy Provider's domain name (**sip.test.com**), as shown on the screen below.
  - Click **Next**.

©2018 Avaya Inc. All Rights Reserved.

Click **Next** on the **Add Server Configuration Profile - Ping** window (not shown).

On the **Add Server Configuration Profile - Advanced** window:

- Select **SP-General** from the **Interworking Profile**.
- Leave all other fields with default values.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **Service Provider UDP** Server Configuration Profile.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Authentication** tab of the newly created **Service Provider UDP** Server Configuration Profile.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Registration** tab of the newly created **Service Provider UDP** Server Configuration Profile.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **Service Provider UDP** Server Configuration Profile.

©2018 Avaya Inc. All Rights Reserved.

6.3.4 Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

To create the inbound route, from the **Global Profiles** menu on the left-hand side (not shown):

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: ***Route_to_IPO_TLS***.
- Click **Next**.

On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: ***1***
- **Server Configuration**: Select ***IP Office***.
- **Next Hop Address** is populated automatically with ***192.168.128.167:5061 (TLS)*** (IP Office IP address, Port and Transport).
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen shows the newly created **Route_to_IPO_TLS** Routing Profile.

Similarly, for the outbound route:

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: ***Route_to_SP_UDP***.
- Click **Next**.

©2018 Avaya Inc. All Rights Reserved.

On the Routing Profile screen complete the following:

- **Load Balancing**: Select ***DNS/SRV***.
- Click on the **Add** button to add a **Next-Hop Address**.
- **Server Configuration**: Select ***Service Provider UDP***.
- **Next Hop Address** is populated automatically with ***sip.test.com:5060 (UDP)*** (Service Provider SIP Proxy FQDN, Port and Transport).
- Click **Finish**.

The following screen capture shows the newly created **Route_to_SP_UDP** Routing Profile.

©2018 Avaya Inc. All Rights Reserved.

6.3.5 Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by IP Office and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone** (not shown).
- Enter the **Profile Name**: ***IP Office***.
- Click **Finish**.

The following screen capture shows the newly added **IP Office** Topology Hiding Profile. Note that for IP Office no values were overwritten (left with default values).

©2018 Avaya Inc. All Rights Reserved.

To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone** (not shown).
- Enter the **Profile Name**: ***Service_Provider***.
- Click **Finish**.

- Click **Edit** on the newly created **Service_Provider** Topology Hiding profile.
- On the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***sip.test.com***) under **Overwrite Value**.
- On the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***sip.test.com***) under **Overwrite Value**.
- On the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***sip.test.com***) under **Overwrite Value**.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly added **Service_Provider** Topology Hiding Profile.

©2018 Avaya Inc. All Rights Reserved.

6.4 Domain Policies

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.4.1 Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

From the menu on the left-hand side, select **Domain Policies → Application Rules** (not shown).

- Click on the **Add** button to add a new rule (not shown).
- **Rule Name:** enter the name of the profile, e.g., ***500 Session***.
- Click **Next**.

- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of ***500*** was used in the sample configuration.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **500 Sessions** Application Rule.

©2018 Avaya Inc. All Rights Reserved.

6.4.2 Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward IP Office and one toward the Service Provider.

To add a media rule in the IP Office direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **IPO_SRTP**.
- Click Next.

©2018 Avaya Inc. All Rights Reserved.

- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption**,** uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous check **Capability Negotiation**.
- Click **Next**.

- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **IPO_SRTP** Media Rule

For the media rule in the Service Provider direction, the existing/predefined media rule **default-low-med** was used.

©2018 Avaya Inc. All Rights Reserved.

6.4.3 End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name:** ***Enterprise***.
- Click **Next**.

- **Application Rule:** ***500 Sessions***.
- **Border Rule:** ***default***.
- **Media Rule:** ***IPO_SRTP*** (**Section 6.4.2**).
- **Security Rule:** ***default-low***.
- **Signaling Rule:** ***default***.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **Enterprise** End Point Policy Group.

Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk.

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name:** ***Service Provider***.
- Click **Next**.

©2018 Avaya Inc. All Rights Reserved.

- **Application Rule:** ***500 Sessions***.
- **Border Rule:** ***default.***
- **Media Rule:** ***default-low-med***.
- **Security Rule:** ***default-low***.
- **Signaling Rule:** ***default***.
- Click **Finish**.

The following screen capture shows the newly created **Service Provider** End Point Policy Group.

©2018 Avaya Inc. All Rights Reserved.

6.5 Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

6.5.1 Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** on the left-hand side, select **Network Management**. Select the **Networks** tab.

In the event that changes need to be made to the network configuration information, they can be entered here.

Use **Figure 1** as reference for IP address assignments.

Note: Only the highlighted entity items were created for the compliance test, and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.

©2018 Avaya Inc. All Rights Reserved.

On the Interfaces tab, click the **Status** control for interfaces **A1** and **B1** to change the status to ***Enabled***. It should be noted that the default state for all interfaces is ***Disabled***, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

©2018 Avaya Inc. All Rights Reserved.

6.5.2 Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface** (not shown).

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** ***Private_med***.
- Under **IP Address** select: ***Network_A1 (A1, VLAN 0)***
- Select **IP Address:** ***10.64.101.243*** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **Port Range:** ***35000-40000***.
- Click **Finish**.

- Select **Add** in the **Media Interface** area (not shown)**.**
- **Name:** ***Public_med***.
- Under **IP Address** select: ***Network_B1 (B1, VLAN 0)***
- Select **IP Address:** ***10.10.80.51*** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range:** ***35000-40000***.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created Media Interfaces.

©2018 Avaya Inc. All Rights Reserved.

6.5.3 Signaling Interface

To create the Signaling Interface toward IP Office, from the **Device Specific** menu on the left-hand side, select **Signaling Interface** (not shown).

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name:** ***Private_sig***.
- Under **IP Address** select: ***Network_A1 (A1, VLAN 0)***
- Select **IP Address:** ***10.64.101.243*** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **TLS Port:** ***5061***.
- Select a **TLS Profile**.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name:** ***Public_sig***.
- Under **IP Address** select: ***Network_B1 (B1, VLAN 0)***
- Select **IP Address:** ***10.10.80.51*** (outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port:** ***5060***.
- Click **Finish**.

The following screen capture shows the newly created Signaling Interfaces.

©2018 Avaya Inc. All Rights Reserved.

6.5.4 End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

©2018 Avaya Inc. All Rights Reserved.

The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows** (not shown**)**, then the **Server Flows** tab. Click **Add** (not shown).

- **Name:** ***SIP_Trunk_Flow_UDP***.
- **Server Configuration**: ***Service Provider UDP***.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: ***Private_sig***.
- **Signaling Interface:** ***Public_sig***.
- **Media Interface**: ***Public_med***.
- **Secondary Media Interface**: ***None***.
- **End Point Policy Group:** ***Service Provider***.
- **Routing Profile:** ***Route_to_IPO_TLS*** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** ***Service_Provider***.
- **File Transfer Profile:** ***None***.
- **Signaling Manipulation Script:** ***None***.
- **Remote Brach Office:** ***Any***.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

To create the call flow toward IP Office, click **Add** (not shown).

- **Name:** ***IP_Office_Flow***.
- **Server Configuration**: ***IP Office***.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: ***Public_sig***.
- **Signaling Interface: Private_sig**.
- **Media Interface**: ***Private_med***.
- **Secondary Media Interface**: ***None***.
- **End Point Policy Group:** ***Enterprise***.
- **Routing Profile:** ***Route_to_SP_UDP*** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** ***IP Office***.
- **File Transfer Profile:** ***None***.
- **Signaling Manipulation Script:** ***None***.
- **Remote Brach Office:** ***Any***.
- Click **Finish**.

©2018 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **End Point Flows**.

7. Ironton SIP Trunking Service Configuration

To use Ironton SIP Trunk service, a customer must request the service from Ironton using the established sales processes. The process can be started by contacting Ironton via the corporate web site at: https://www.ironton.com/ and requesting information.

During the signup process, Ironton and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Ironton's network.

The customer will need to provide the public IP address used to reach the Avaya Session Border Controller for Enterprise (Avaya SBCE).

Ironton will provide the customer the necessary information to configure Avaya IP Office and the Avaya Session Border Controller for Enterprise following the steps discussed in the previous sections, including:

- FQDN to be use for public DNS record queries.
- SIP Trunk registration credentials (User Name, Password, etc.).
- DID numbers.

©2018 Avaya Inc. All Rights Reserved.

8. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting tips that can be used to troubleshoot the solution.

8.1 Verification Steps

The following steps may be used to verify the configuration:

- Verify that endpoints at the enterprise site can place calls to the PSTN.
- Verify that endpoints at the enterprise site can receive calls from the PSTN.
- Verify that users at the PSTN can end active calls to endpoints at the enterprise by hanging up.
- Verify that endpoints at the enterprise can end active calls to PSTN users by hanging up.

8.2 IP Office System Status

The following steps can also be used to verify the configuration.

Use the Avaya IP Office System Status application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office System Status is installed, log in with the proper credentials.

©2018 Avaya Inc. All Rights Reserved.

Select the SIP Line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** is **Idle** for each channel (assuming no active calls at present time).

- Select the **Alarms** tab and verify that no alarms are active on the SIP Line.

©2018 Avaya Inc. All Rights Reserved.

8.3 IP Office Monitor

The IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.

Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting the desired color.

©2018 Avaya Inc. All Rights Reserved.

8.4 Avaya Session Border Controller for Enterprise

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

Alarms: Provides information about the health of the Avaya SBCE.

The following screen shows the **Alarm Viewer** page.

Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.

©2018 Avaya Inc. All Rights Reserved.

The following screen shows the Incident Viewer page.

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

The following screen shows the Diagnostics page with the results of a ping test.

©2018 Avaya Inc. All Rights Reserved.

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Device Specific Settings → Troubleshooting → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

©2018 Avaya Inc. All Rights Reserved.

Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

©2018 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the configuration steps necessary for configuring Session Initiation Protocol (SIP) Trunk Service for an enterprise solution consisting of Avaya IP Office Release 11.0 and the Avaya Session Border Controller for Enterprise Release 7.2.2 to interoperate with Ironton SIP Trunking Service, as shown in **Figure 1**.

Ironton SIP Trunking Service passed compliance testing with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

©2018 Avaya Inc. All Rights Reserved.

10. References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office and the Avaya Session Border Controller for Enterprise, including the following, is available at: http://support.avaya.com/

[1] *Avaya IP Office Platform Solution Description*, Release 11.0, May 2018.
[2] *Avaya IP Office Platform Feature Description*, Release 11.0, May 2018.
[3] *IP Office Platform 11.0 Deploying Avaya IP Office Essential Edition*, Document Number 15-601042, Issue 33g, 20 May 2018.
[4] *Administering Avaya IP Office Platform with Manager*, Release 11.0, May 2018.
[5] *IP Office Platform 10.1 Using Avaya IP Office Platform System Status*, Document 15-601758, Issue 13a, 05 April 2018.
[6] *IP Office Platform 11.0 Using IP Office System Monitor*, Document 15-601019, Issue 09b, 10 may, 2018.
[7] *Using Avaya Communicator for Windows on IP Office*, Release 10, August 2016.
[8] *Avaya Communicator for Web – IP Office Platform: User Guide, Release 1.0, Issue 1.0.18, March 2018.*
[9] *Using Avaya Equinox for IP Office, Release 11.0, June 2018.*
[9] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2.2, Issue 8, June 2018.
[10] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2.2, Issue 10, June 2018.

Additional Avaya IP Office documentation can be found at:
http://marketingtools.avaya.com/knowledgebase/

Product documentation for Ironton SIP Trunking Service is available from Ironton.

©2018 Avaya Inc. All Rights Reserved.

©2018 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. 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.