Configuring the Avaya Session Border Controller for IP Office Remote Workers

September 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose

specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Overview

The Avaya Session Border Controller for Enterprise (SBCE) delivers security to a SIP-based Unified Communications network. This document describes how to configure the SBCE for IP Office Remote Workers.

Remote access

When the SBCE is in an IP OFFICE Solution registration and remote access to the SBCE is done jointly with IP Office. Remote access is thru the SSL VPN on the IP OFFICE and hopping to the SBCE. For more information, see the document “ASBCE GRT Registration and Remote Connectivity via IP Office SSL/VPN NAPT” on support.avaya.com.

Licencing

Licensing takes place once the SBCE is on the network and in the Commissioned state. Retrieval and activation of licensing for Avaya SBCE is done via Avaya’s PLDS (Product Licensing and Distribution System). Access to PLDS is via the Avaya Support Portal at the URL `https://plds.avaya.com`.

For the SBCE, the SBCE EMS element is its own license hst for licensing specific to the SBCE. Licensing is managed for SBCE within PLDS by a user-defined host name and the MAC address of the management interface. ecide on a user defined license host name for the SBCE at the physical site. This will be the license host name used to activate SBCE licenses in PLDS.

On the SBCE, run the command `ifconfig` to determine the MAC address of the management network interface.

- The MAC address of the management interface of the Portwell CAD is the Eth5 port.
- For a single Dell server deployment, the management interface MAC address is the Eth 5 port.

The license file for the SBCE must be uploaded so that Avaya Services can provide support for what the customer is licensed for. Customers are still under the EULA for their license just like in prior releases. After activating the license on PLDS and getting the XML file via emal, use the SBCE management interface to upload and install the license.

To install the license:

1. Log in to the SBCE management interface.
2. In the navigation tree on the left, select **System Management** and then click **Install**.
3. In the Install License window, click Browse and navigate to the license file.
4. You can **Append** the license or **Overwrite**. Only overwrite if required.
5. You can **Group By Product** or **License File**.

Remote Worker best practices

- For all non SIP and media related traffic, or any specific IP Office or endpoint configuration and requirements see *Administering Avaya Flare® Experience IP Office for iPad and Windows*and *Administering Avaya one-X® Mobile for IP Office*.

  For example, XMPP will go direct from endpoint to One-X portal through the firewall and not through the SBCE.
- For security best practices, see the ASBCE Security Configuration Guide.
- For SBCE configuration see *Administering Avaya Session Border Controller for Enterprise*.
- Use encryption with endpoints that are capable. For R9.0, the following table summarizes device specific support.

Client type	Uses to the external interface of the SBCE		
	TLS	SRTP Audio	SRTP Video
Flare Experience for IP Office R1.1.4 (Windows version)	Y	Y	N
Flare Experience for IP Office R1.1.2 (iPad version)	Y	Y	N
one-X Mobile Preferred VoIP client for Android	Y	N	N
one-X Mobile Preferred VoIP client for iOS	N	N	N

Client type	Uses to the external interface of the SBCE		
	TLS	SRTP Audio	SRTP Video
If the mobile client using TLS and/or SRTP will be used to roam from the network on the ASBCE's external interface to the network on the IP Office side of the ASBCE, the transport medium will have to be changed while the mobile client is connected to the network on the IP Office side. IP Office 9.0 does not support direct SRTP connections to these mobile clients and TLS is ONLY supported on the OneX Mobile Preferred VOIP Client for Android.			

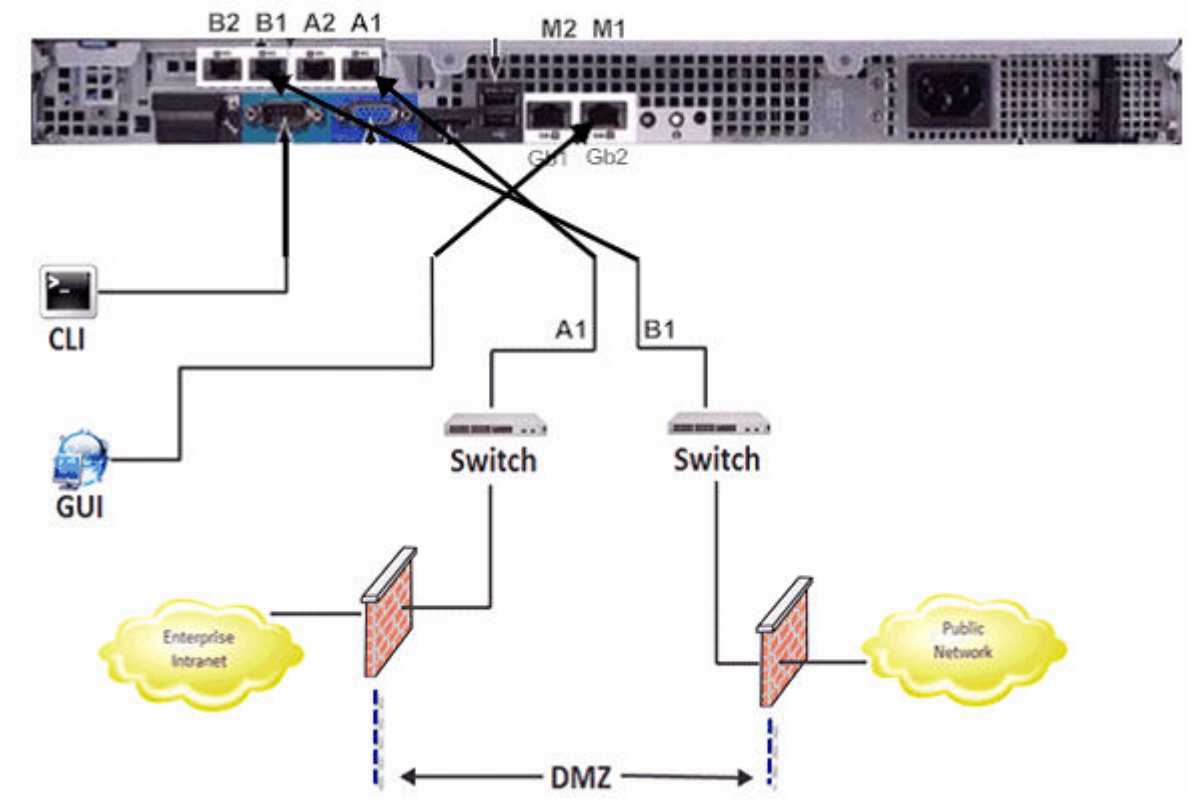
- If Media or Signaling QoS are required, they must be configured on the SBCE as the SBCE does not pass through.
- Customer firewall configuration requires forwarding of video/audio signaling and media ports. SIP ALG’s should be disabled on any firewalls.
- For troubleshooting the best rules to follow are to look at Alarms/Incidents and take a packet capture to determine if the issue is on the SBCE. If further debugging is required, enable debug logs and get the appropriate elogs.
- If doing remote worker and trunking on the same SBCE, you use a second set of IP addresses on the SBCE for trunking. See the SBCE documentation and application notes on configuring SBCE for trunking.
- Review SBCE, IP Office, and endpoint release notes for fixes, limitations, and workarounds.

Chapter 2: Configuring Session Border Controller Enterprise for IP Office Remote Workers

Network interfaces

The example below shows a two wire deployment of a Dell Session Border Controller for Enterprise (SBCE) in a demilitarized zone (DMZ). It is common to have only an external firewall, but it is possible to have a firewall on both sides of the DMZ. For a description of the distinction between one and two wire deployments, see *Avaya Session Border Controller for Enterprise Overview and Specification*.

Single server deployment



The following requirements apply to a single server two wire deployment.

- M1 is used for management.
- A1 is used to communicate with IP Office.
- B1 is used to communicate with the endpoints.
- M1, A1, and B1 all require an IP address. M1 cannot be on the same subnet as A1 or B1.
- If A1 and B1 are on same subnet, you can do a one-wire deployment and use A1 only for data. M1 is still required for management.
-
- Since the Portwell CAD has fewer interfaces, M2 or B2 are not listed on the back. M1, A1, and B1 are the ports used on Portwell SBC hardware as well. All network interfaces on the SBC are auto negotiate, so the switch or router ports that the SBC connects to must also be set to auto negotiate.

Creating a backup

Backup the empty SBCE configuration. This enables you to start again from scratch.

Procedure

1. Login to the SBCE Control Center as `Admin`.
2. In the navigation tree on the left, select **Backup/Restore** and then select the **Snapshots** tab.
3. Click Create Snapshot.
4. Enter a description and then click Create.
5. Click Download and save the file locally.

Next steps

When you have finished the configuration, create another snapshot. See *Administering Avaya Session Border Controller for Enterprise* for a procedure to configure automatic backup to an SFTP server.

Configuring network address translation

If you have a firewall in front or behind the SBCE and are natting the SBCE IP address, you must perform this procedure.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Network Management**.
3. Select the **Network Configuration** tab.
4. Enter the IP address you are natting in the **Public IP** field.
   The SBC will nat the SIP messages with the IP address.

Enabling interfaces

Enable the interfaces A1, internal to the IP Office, and B1, external to the phones, that were configured during installation. If configuring a one-wire deployment, you will only enable A1. For Portwell CAD hardware, B2 and M2 do not exist.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Network Management**.
3. Select the **Interface Configuration** tab.
4. Enable the required interfaces.

Configuring media interfaces

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Media Interfaces**.
3. Click **Add**.
4. Enter the name for internal interface and then select the A1 IP address from the pull down menu.
5. Enter the media port range and click **Finish**.
   The default port range used is 35000-40000.
6. Click **Add**.
7. Enter the name for external interface and then select the B1 IP address from the pull down menu.
8. Enter the media port range and click **Finish**.
   The default port range used is 35000-40000.

Configuring signalling interfaces

Procedure

1. Login to the SBCE Control Center as `Admin`.
2. In the navigation tree on the left, expand **System Management**.
3. Select **Device Specific Settings** and then **Signalling Interfaces**.
4. Click **Add**.
5. Enter the name for internal interface and the select the A1 IP address from the pull down menu.
6. For the transport to be used on that interface, put in the port in the chosen transport field or fields and click Finish.

TCP port 5060 is the required transport for remote workers on IP Office.

7. Click **Add**.
8. Enter the name for external interface and the select the B1 IP address from the pull down menu.
9. For the transport to be used on that interface, put in the port in the chosen transport field or fields and click Finish.

   TCP port 5060 is the required transport for remote workers on IP Office.
10. TLS port 5061 is the preferred transport for remote worker towards the Avaya endpoints if the endpoint supports it. If using TLS, select the default Avaya TLS server profile on the external interface. If the endpoint doesn't support TLS, then use TCP and look at the IP Office remote worker guides for Flare and one-X Mobile clients for information on protocols to use.

Configuring server interworking profiles

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Server Interworking**.
4. The profile used for remote workers on the IP Office is **avaya-ru** server interworking. Highlight the **avaya-ru** profile.
5. Click **Clone**.
6. Enter a name for the profile and click **Finish**.

Configuring phone interworking profiles

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Phone Interworking**.
4. Select the **avaya-ru** profile and click **Clone**.
5. Enter a name for the profile and click **Finish**.

Configuring the call server

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Server Configuration**.
4. Click **Add**.
5. Enter a name.
6. In the **Server Type** field, select **Call Server** from the pull down menu.
7. In the **IP Addresses** field, the IP Office IP address.
8. Check the **Supported Transports** you want to use.

   TCP is required for remote worker but you may have UDP if you are also using the SBC for SIP trunks.
9. In the **Transport Port** fields enter the port to be used (for example port 5060).
10. Click Next three times.
11. Do not enable **Grooming**. IP Office uses different TCP connections to each endpoint.
12. For the interworking profile, choose **avaya-ru** or a cloned version of it.
13. Click **Finish**.

Configuring routing profiles

Routing profiles define packet routing criteria in order to route them to the right destination. Routing profiles are "applied" to Endpoint Flows. Clone an existing routing profile as a starting point or create a new one. Do not change the default profile.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Routing**.
4. Click **Add**.
5. Enter a name for the profile.
6. Click **Next**.
7. In the **Next Hop Server 1** field, enter the IP Office IP address.
   You can use the IP Office fully qualified domain name (FQDN).
   If using a non default port of 5060, you must put the IP colon port in the **Next Hop** field. For example 10.3.3.3:5070.
8. Click on the appropriate **Outgoing Transport** to be used for IP Office.

Configuring topology hiding

Topology Hiding is an SBCE security feature which allows you to change key SIP message parameters to mask how your enterprise network may appear to an unauthorized or malicious user. If required, Topology Hiding is applied to flows. The server flow points towards IP Office and the subscriber flow points towards the endpoints.

Note that if you want to pass what you get from the endpoints, then a Topology Hiding profile is not required.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Topology Hiding**.
4. Click on the default profile and then click **Clone**.
5. Enter a name and click **Finish**.
6. The profile just created is highlighted. Click **Edit**.
   - If IP Office is configured to accept a specific domain then in the **From, To, and Request-Line** field, select **Overwrite**, enter the domain name and click **Finish**.
   - If IP Office is configured to accept a specific domain then in the **From, To, and Request-Line** field, select **Destination IP**and click **Finish**.
   - If no special criteria is required, leave everything as **Auto** and click **Finish**.

Configuring endpoint policy groups

Create a new endpoint policy group. Do not change the default group.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Domain Policies** and then **End Point Policy Groups**.
3. Click **Add** and enter a name for the IP Office server flow.
4. Click **Next**.
5. Choose the appropriate **Rules** and click **Finish**.
6. Click **Add** and enter a name for the subscriber flow.
7. Click **Next**.
8. Choose the appropriate **Rules** and click **Finish**.

Next steps

The following three procedures for end point policy groups show changing the application rule for max sessions, the media rule for QoS and RTP or SRTP, and the signaling rule for QoS.

See *Administering Avaya Session Border Controller for Enterprise* for additional information on domain polices.

Configuring endpoint policy groups application rules

Clone an existing application rule as a starting point or create a new one. Do not change the default.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Domain Policies** and then **Application Rules**.
3. Click **Add** and enter a name for the one to be used by the IP Office End Point Policy Group.
4. Click **Next**.
5. Check **In and Out for Voice**and put in the amount of concurrent sessions required for the license. Put the same value for **Max Concurrent Sessions** and **Max Sessions Per Endpoint**.

   It is best practice to put more than the license as this is not counted one or one with license session. For example, if they have license of 300 concurrent sessions put 500 for each box.

   If you need video, you must do the same for video. If you clone the default, Audio is already enabled you only need to adjust the values and then enable video.
6. Click **Finish**.
7. Repeat to create a rule used by the Subscriber Flow End Point Policy Group. For the subscriber flow rule, put the **Max Concurrent Sessions** higher than the license. However, for **Max Sessions Per Endpoint**, the recommended value is 10. You can use a higher value if required.

Configuring endpoint policy groups media rules

Clone an existing media rule as a starting point or create a new one. Do not change the default.

Media rules are defined under **System Management** > **Domain Policies** > **Media Rules**. The requirements for media rules are as follows.

- It is recommended to clone a profile like the default-low-med profile. The default Media Rule has the **Media QoS** setting of **DSCP EF** enabled.
- When you create a new media rule, the default is . This must be changed tor another option that meets the current requirements.
- On the Media Encryption tab, set the SBC to RTP or SRTP to an endpoint or IP Office. For Media Encryption, set the preferred Audio Format as RTP in the rule for IP Office. Towards the endpoints, the rule used can be set to SRTP if the endpoint supports it. Otherwise use RTP. Ensure Encrypted RTCP is unchecked and Interworking is checked. For Video ensure RTP is selected.
- For all other tabs, use the default settings.

Configuring endpoint policy groups signalling rules

Clone an existing media rule as a starting point or create a new one. Do not change the default.

Media rules are defined under **System Management** > **Domain Policies** > **Signalling Rules**. The requirements for signalling rules are as follows.

- It is recommended to clone a profile like the default-low-med profile. The default Media Rule has the **Signalling QoS** setting of **DSCP AF41** enabled.
- When you create a new signalling rule, the default is **TOS**. This must be changed to **DSCP AF41** or another option that meets the current requirements.
- For all other tabs, use the default settings.

Configuring server flows

A server flow is required for the IP Office.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

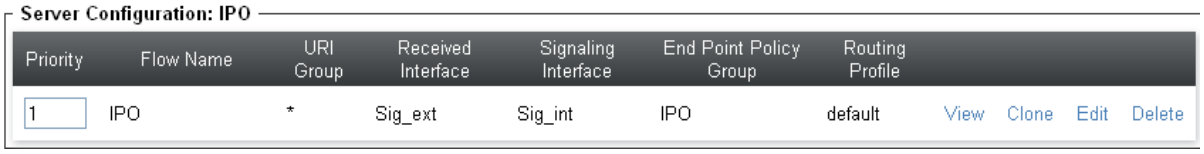
Procedure

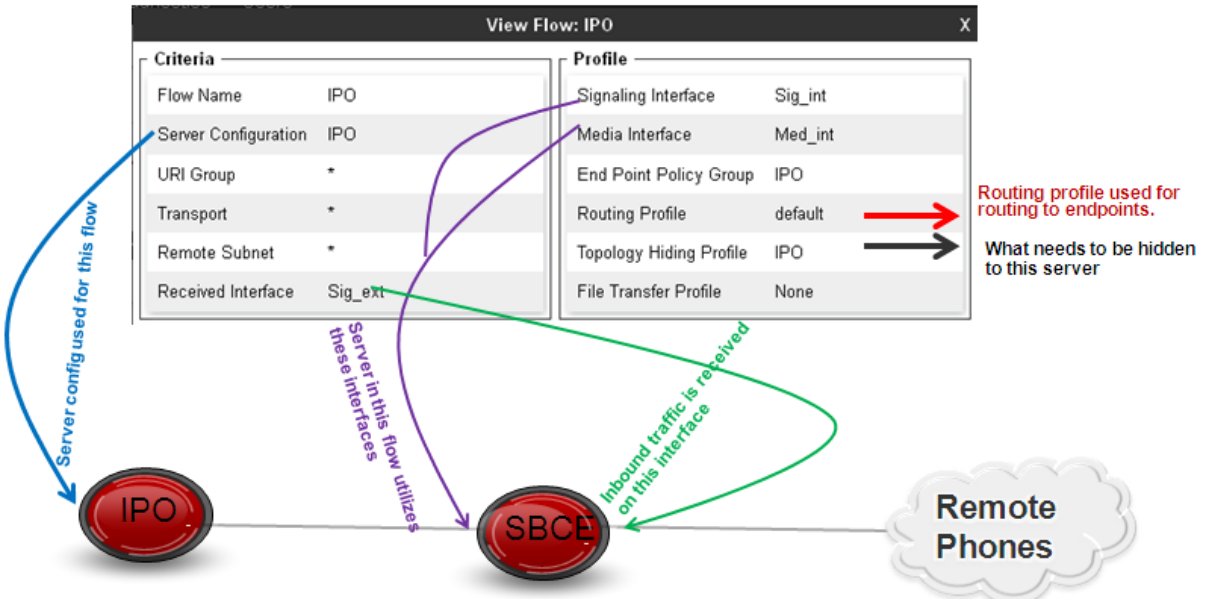
1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **End Point Flow**.
3. Select **Server Flow**.
4. Click **Add**.
5. Enter a name for the IP Office flow.
6. In the **Server Configuration** field, select the IP Office server configuration.
7. In the **Received Interface** field, select the external signaling interface.
8. In the **Media Interface** field, select the IP Office interface.
9. In the **Signaling Interface** field, select the IP Office interface.
10. In the **End Point Policy** field, select the policy group created for IP Office.
11. In the **Routing Profile** field, select the default routing profile.
12. If required, in the **Topology Hiding Profile**, select profile created for IP Office.
13. Click **Finish**.

Example IP Office server flow

Note:

If doing remote worker and trunking to the same SM you will have two SM server flows. One with the remote worker received interface and the default routing profile and the other with the trunk received interface and the to_trunk routing profile





Configuring user agent profiles

User Agent profiles can be created using what the endpoints send in the user agent header. When these profiles are put in a subscriber flow, only phones that match that User Agent are allowed to send registration or other messages through the SBCE.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Global Parameters** and then **User Agents.**.
3. Click **Add**.
4. Enter a description then put in the type of user agent the endpoint you want to allow using regular expression. You can use one type per policy or you can put multiple types in one user agent profile.
5. Click **Finish**.

6. You can add the user agent header to a subscriber flow during the flow configuration or by editing an existing flow. In the subscriber flow **User Agent** field, select the user agent profile.

Configuring subscriber flows

Subscriber flows are required to route registrations and calls from the phones to and from the IP Office.

Before you begin

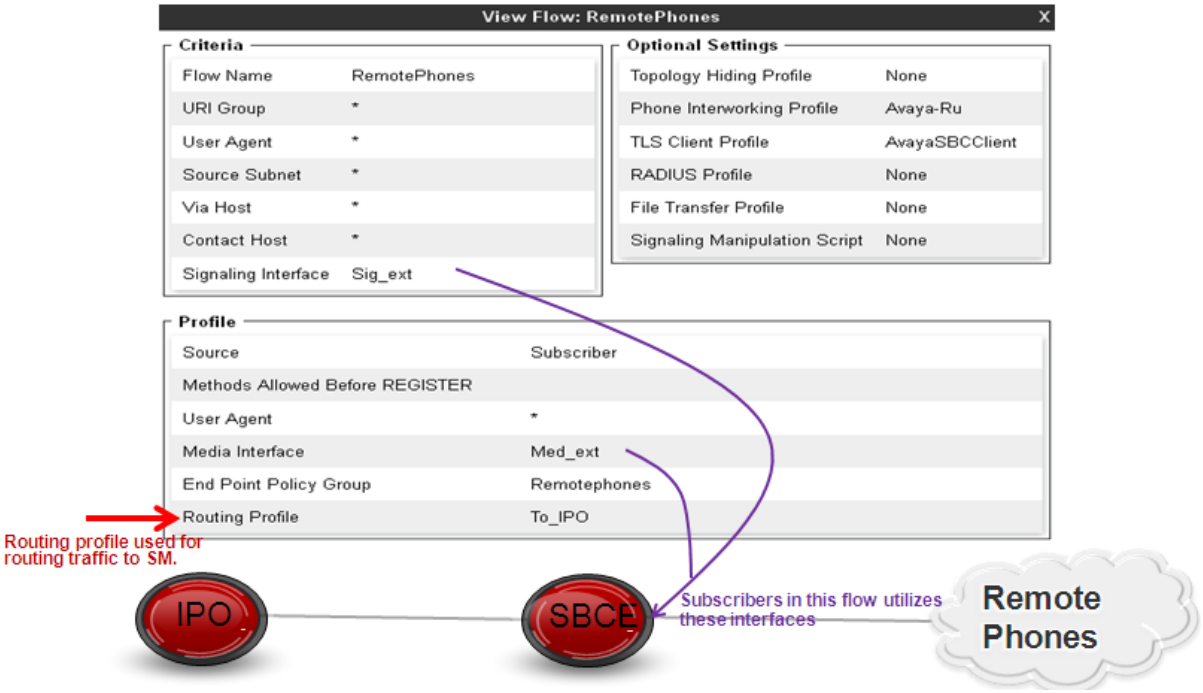
You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **End Point Flow**.
3. Select **Subscriber Flow**.
4. Click **Add**.
5. Enter a name for the end point flow.
6. The **URI Group** and **User Agent** fields can be used to only allow certain DID's or phone types to use that flow.
7. In the Signaling Interface field, select the external signaling interface.
8. Click Next.
9. In the **Media Interface** field, select the external media interface.
10. In the **End Point Policy Group** field, select the policy group created for the endpoints.
11. In the **Routing Profile** field, select the profile to route to the IP Office.
12. The **Topology Hiding** field can be used if you want to send something specific to the phones. It can be left blank.
13. In the **Phone Interworking Profile** field, select **avaya-ru** or the recommended cloned copy of **avaya-ru**.
14. If using TLS, put in the default **TLS Client Profile** called **AvayaSBCClient**.

15. Click **Finish**.

Example subscriber flow



Index