Avaya WebRTC Snap-in Reference

Release 3.0
Issue 2
September 2014

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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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 or such successor site as designated by Avaya. 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN 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 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, with the exception of Heritage Nortel Software, 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. "Software" means Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. "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. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance 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, Instance, 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 or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance 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 an Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance 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").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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

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 or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: WebRTC description

Intended audience

This document is intended for people who need to install, configure, and administer the Avaya WebRTC Snap-in. This document contains specific information about this snap-in. For an overview of the Avaya Aura® Collaboration Environment, see the *Avaya Aura® Collaboration Environment Overview and Specification*. For general information about Collaboration Environment snap-in deployment, see *Quick Start to Deploying Avaya Aura® Collaboration Environment Snap-ins*.

Avaya WebRTC Snap-in overview

Description

The Avaya WebRTC Snap-in enables users inside or outside the Enterprise to make a secure call from their web browser to any endpoint to which Avaya Aura® can deliver calls. For example, customers can call from a web browser directly into a Contact Center. The snap-in enables the separate web application to control: the user experience; identity presented for the caller; and authorized destination for the call. The web application can additionally convey context about the call that can be leveraged by Collaboration Environment snap-ins, Contact Center applications, and Contact Center Agents. The Avaya WebRTC Snap-in can also be used to simplify Enterprise operations by enabling click to call from an internal Enterprise website like a corporate directory or helpdesk. The Avaya WebRTC Snap-in is purchased separately from Collaboration Environment and requires its own license file. The Chrome and Firefox web browsers support WebRTC.

Architecture

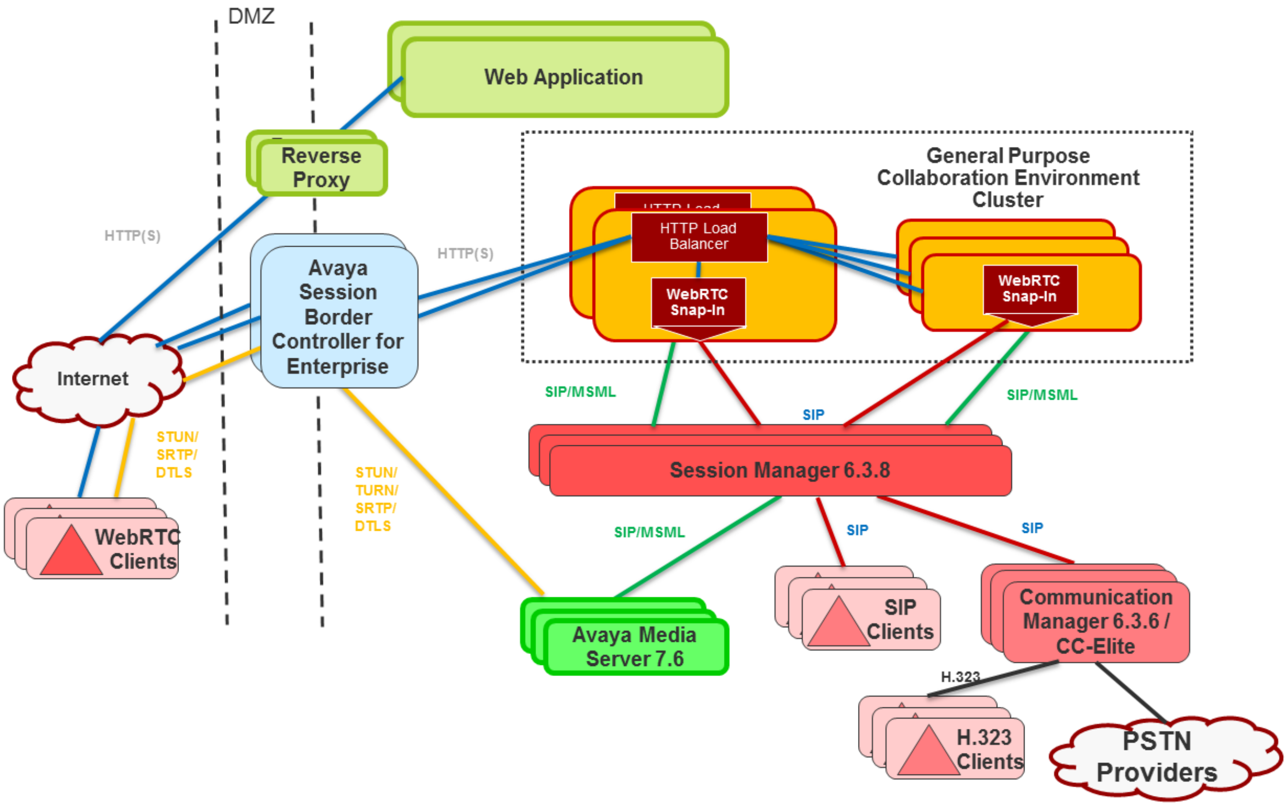
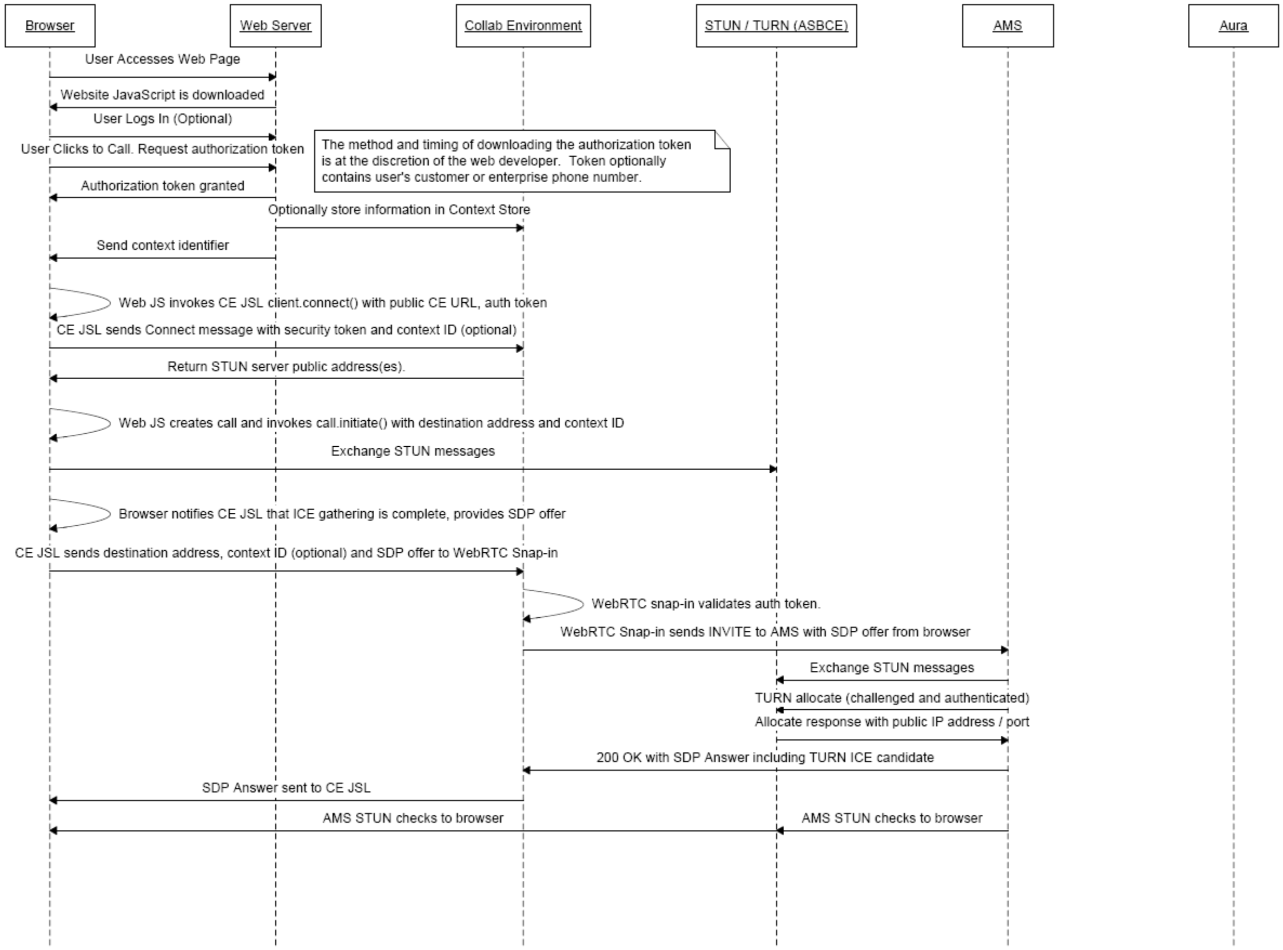
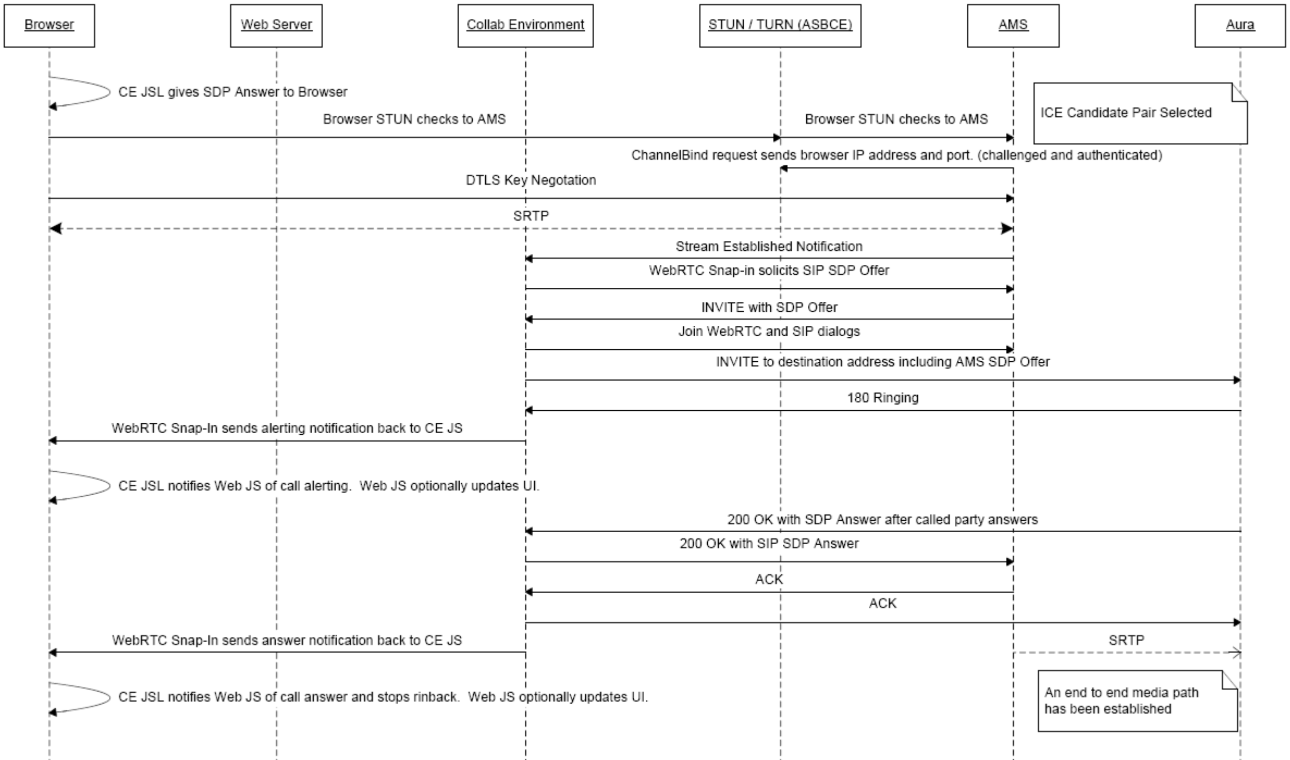


Figure 1: WebRTC architecture diagram

Sequence diagram for a WebRTC call





Features

Security

One of the primary differentiating features for the WebRTC Snap-in is that the web application handles authentication and authorization of calls. This includes the capability to assert a calling user's phone number and restrict the numbers that can be called. The Avaya SBCE enables secure firewall traversal for HTTP and SRTP packets, facilitates sending DTLS to provide secured key exchange for the SRTP flow, and takes care of all security requirements mentioned in the TURN protocol for the solution. Avaya SBCE uses the industry standard TURN protocol. In addition to Avaya SBCE, customers have the option to use an existing reverse proxy / Application Delivery Controller for HTTP signaling between browser and collaboration environment.

API/SDK

One of the benefits of the WebRTC Snap-in API is that it is simple and spares the web developer from needing to know the details of ICE, STUN, TURN, and SDP. As part of the WebRTC solution, there is an SDK available for download from Devconnect website. The SDK provides all of the required resources and javadoc on Javascript library, as well as sample applications.

High Availability

New calls will be established if the Avaya Aura® Collaboration Environment instance is lost and you have a multinode cluster (on a cluster with more than one collaboration instance). Voice calls will continue on a failure, however, a disconnect message will not go through. If an Avaya Media Server

server is lost then any calls going through that server will be lost. Avaya Aura® Session Manager, Avaya SBCE, and Avaya Aura® Communication Manager have their own HA strategies.

Other Features

The WebRTC Solution makes it possible to store contextual data about calls and pass a reference to that data so it is available to Collaboration Designer, Experience Portal, and AES applications.

WebRTC Snap-in example

The WebRTC Snap-in makes something like the following interaction possible.

A customer is filling a loan application out on a bank website. The customer runs into a problem that they need help with, so they click a button on the website and are connected with a bank representative through the browser. Instead of having to go through the typical IVR self-service, the call is routed to a relevant agent immediately. Data about the customer and the loan that they had been working on was sent with the call, so the bank representative is up to speed with the customer's information. WebRTC also asserted the customer's phone number with the call, so they get the same treatment as if they called from that phone.

Chapter 2: Interoperability

Interoperability

Avaya product requirements

- Collaboration Environment 3.0 and newer
- Avaya Media Server 7.6 and newer
- Avaya Aura® Communication Manager 6.3.5 or 6.3.6
- Avaya Session Border Controller for Enterprise 6.3 or newer

  Advanced and Standard Avaya SBCE licenses are required for each concurrent session.

Note:

For the latest and most accurate compatibility information, go to www.avaya.com/Support.

Chapter 3: Snap-in licensing

Some Collaboration Environment snap-ins are separately purchasable from Avaya. They are not included with the Collaboration Environment Platform. Each licensed snap-in, including this one, requires its own license file. Activate and download the file from PLDS and install it on System Manager WebLM.

A single license file supports the current version of the snap-in and all previous versions. New versions of this snap-in will require a new license file. For this reason, different versions of the snap-in may be in different license modes.

Avaya provides a 30–day grace period from the time a license error is first detected. When the error is detected, the snap-in enters license error mode and a major alarm is raised but the snap-in remains fully functional. This provides enough time to fix the error before the snap-in stops working. You can view the **license mode** for the snap-in on the Collaboration Environment **Service Management** page. The license modes are:

- Normal — No license error is detected. Indicated by a green check mark on the **Service Management** page.
- Error — There is a license error, but the snap-in continues to operate normally. The **Service Management** page shows the date that the 30-day grace period expires. Collaboration Environment raises a major alarm when the snap-in enters license error mode.
- Restricted — There is a license error, and the 30–day grace period has expired. The snap-in automatically uninstalls. Collaboration Environment raises a critical alarm when the snap-in enters license restricted mode. To correct this problem, you may need to get a license file if you don’t have one, or update to a license file for the new major release.

Chapter 4: Deployment

Required configuration information worksheet

Information	Details	Your data (for reference during configuration)
Provisioned URL to WebRTC Snap-in	If this is an internal web application then the URL is the Avaya Aura® Collaboration Environment cluster address. If it is external this would be the address of the reverse proxy or the Avaya SBCE. Sample URL: https://myCECluster.example.com:9443/services/WebRTC/WebRtcServlet	
Encryption key used to encrypt the authorization token		
Anonymous URI	This is the phone number or URI used when none is asserted by the web application. The default value is "Anonymous@anonymous.invalid". The Anonymous URI domain needs to match the Far-end domain in the signaling group on Avaya Aura® Communication Manager. The signaling group should correspond to the SIP trunk administered on Avaya Aura® System Manager between Avaya Aura® Session Manager and Avaya Aura® Communication Manager.	
STUN server address	If the Avaya SBCE is in use, then populate one of the SBC IP addresses here. If all browsers are external, this is the public side, or external, IP address. If all browsers are internal, this is the private IP address. If there are both external and internal browsers, use the	

	public side, or external, IP address. Make sure that the enterprise data network is configured to reach the public side, or external, IP address of the SBC.	

Note:

SIP administration needs to use the same transport end to end. TCP and TLS on SIP entity links involved with the WebRTC call flow cannot be combined when using this feature. For example, if the Session Manager to Communication Manager entity link is SIP/TLS, then the Session Manager to Collaboration Environment entity link, the Session Manager to Avaya SBCE entity link, and the Session Manager to Avaya Media Server entity link also need to be SIP/TLS.

Installing the license file

Before you begin

Download the snap-in license file from PLDS. For additional information about downloading a license file from PLDS, see *Administering Avaya Aura® Collaboration Environment* .

Procedure

1. On System Manager navigate to **Home** > **Services** > **Licenses**.
2. Select **Install License**.
3. Browse to the location of the snap-in license.
4. Select the license file and click **Install**.

   The system installs the license file.

   In the left navigation pane, the system displays the snap-in under **Licensed Products**.

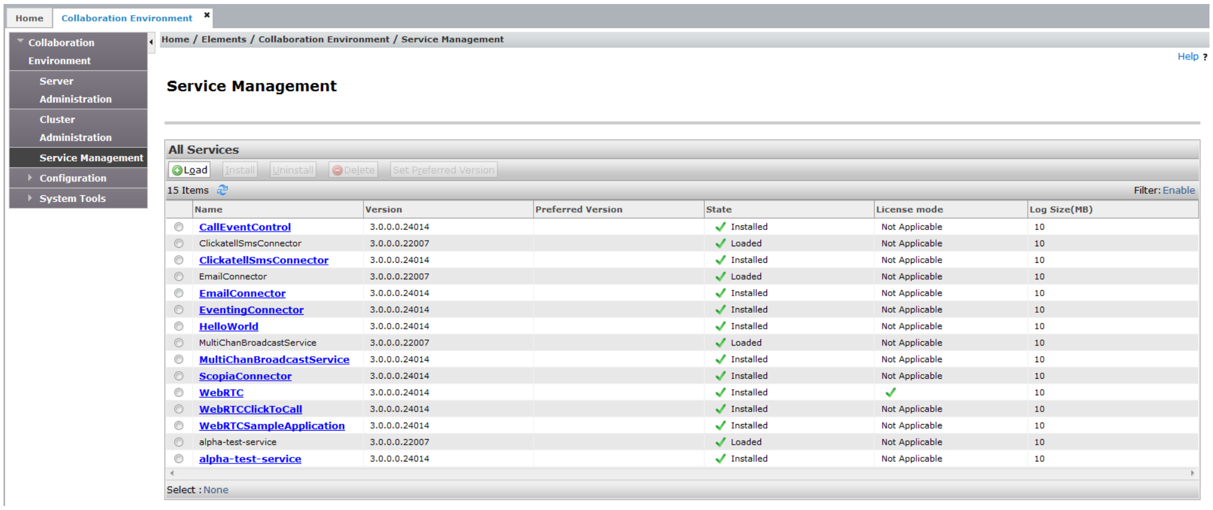
Loading the snap-in

About this task

This task describes how to load a snap-in to System Manager from your development environment or alternate location. You can skip this step when installing a pre-loaded snap-in. Pre-loaded snap-ins are provided without additional charge with the Collaboration Environment Element Manager. Install those you want to use.

Procedure

1. On System Manager navigate to **Home** > **Elements** > **Collaboration Environment** > **Service Management** .



2. Click **Load**.
3. In the Load Service window, click **Choose file**, browse to select your snap-in and click **Open**.

   Your snap-in name ends in .svar.
4. Click **Load** in the Load Service window.

   For Avaya snap-ins only, you will be prompted to accept the Avaya End User License Agreement (EULA).
5. If you agree to the Avaya EULA, click **Accept**.

   Your snap-in displays on the Service Management page with a **State** of **Loaded**.

   If you clicked **Cancel** to reject the agreement, the load stops.

Configuring the WebRTC Snap-in

Procedure

1. Configure the WebRTC Snap-in attributes.
   a. In Collaboration Environment, go to Configuration > Attributes, and then select the Service Clusters or Service Globals tab.
   b. Select `WebRTC` from the **Service** dropdown. If attributes are being configured at the cluster level, select the cluster from the **Cluster** dropdown.
   c. Click the **override default** box for any attributes that need to be configured differently.

The Anonymous URI is one attribute that generally needs to be configured.

d. Click **Commit** to save changes after all attributes have been configured.

2. Configure the HTTP Security.

    a. Go to **Elements > Collaboration Environment > Configuration > HTTP Security**.

    b. On the HTTP CORS tab, add the domain of each web application using the WebRTC Snap-in, and save the change by clicking **Commit**.

    Warning:

    Only select "Allow Cross-origin Resource Sharing for all” to enable HTTP CORS in test environments.

Installing the snap-in

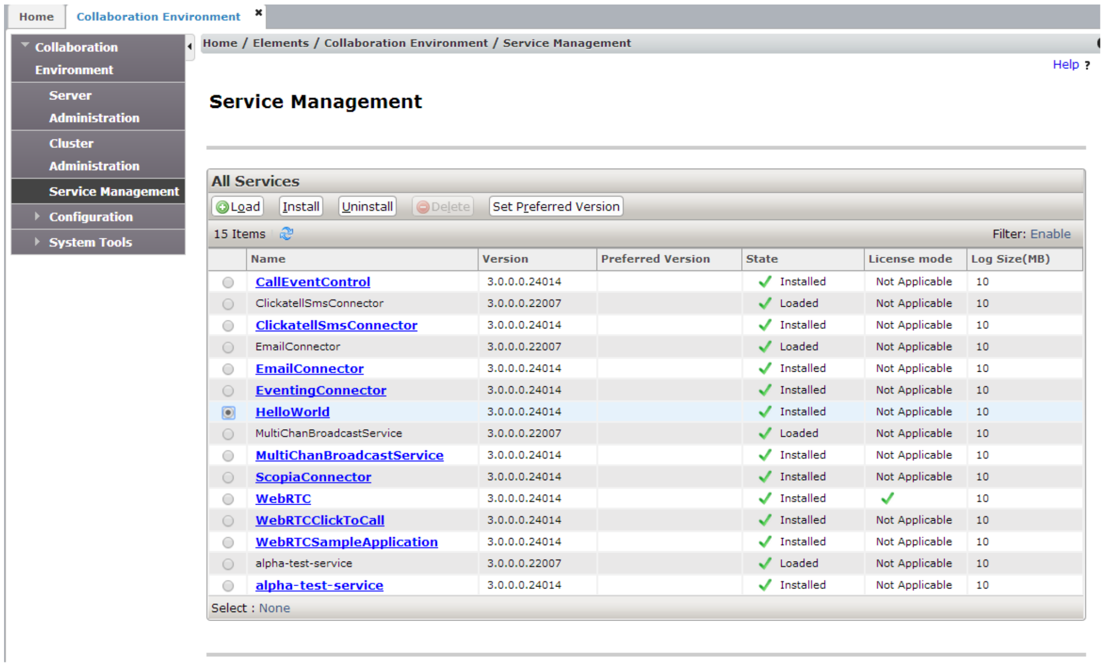
About this task

For .svar files larger than 50 MB, schedule snap-in installation during a maintenance window.

Procedure

1. In System Manager navigate to **Home** > **Elements** > **Collaboration Environment** > **Service Management**.
2. Select the snap-in you want to install.
3. Click **Install**.
4. Select the cluster where you want the snap-in to reside, and click **Commit**.

5. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.



Installed with a green check mark indicates that the snap-in has completed installation on all Collaboration Environment servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all servers.

6. Designate the Preferred Version.

   If you want to designate this newly installed snap-in as the Preferred Version, complete the following steps. Collaboration Environment uses the Preferred Version of a snap-in even if you install a later version of the same snap-in.

   a. From the **All Services** list, select the version of the snap-in that you installed.
   b. Click **Set Preferred Version**.
   c. Select the clusters for which you want this to be the preferred version and click **Commit**.

7. It can take several minutes for System Manager to propagate the snap-in to your Collaboration Environment servers. To track the progress of a snap-in installation:

   a. Click **Server Administration**.
   b. Click the **Name** of any Collaboration Environment server in the cluster on which you installed the snap-in.
   c. Click the **Name** of the snap-in that you installed.

      You can see the **Service Install Status** of the snap-in on each Collaboration Environment server.

Configuring SBC for the WebRTC Snap-in

Before you begin

The Avaya Session Border Controller for Enterprise needs to be installed and working before making the following configuration changes specifically for the WebRTC Snap-in.

About this task

Perform the following administration tasks in Avaya SBCE for the WebRTC Snap-in. The TURN/STUN Service is configured first, followed by configuring the reverse proxy.

Procedure

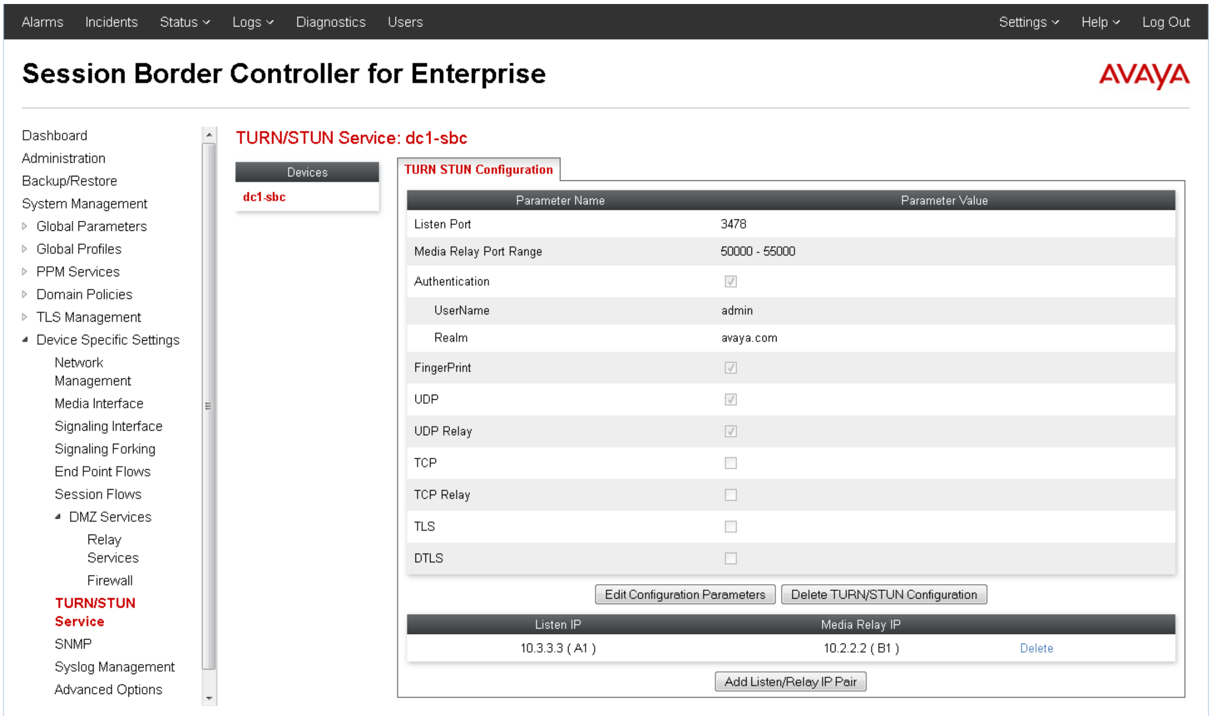
1. Log in to Avaya SBCE and go to **Device Specific Settings** on the left menu. Click on **TURN/STUN Service**, and then click **Edit Configuration Parameters** to fill out the fields on the TURN STUN Configuration tab according to the following table:

   Table 1: TURN/STUN configuration table

Parameter	Details
Listen Port	3478
Media Relay Port Range	This is the port range used for SRTP and STUN packets exchanged between the browser and Avaya Media Server. This range must not overlap port ranges used by the Avaya SBCE for other protocols such as SIP. The default range is 50000 – 55000.
Authentication	The Username and Password must match the credentials set up on the Avaya Media Server server.
Realm	This is the realm used in TURN authentication. In most cases this matches the SIP domain that is in use in the Avaya Aura® system.
FingerPrint	Check the box
UDP	Check the box
UDP Relay	Check the box
TCP	Box should remain unchecked
TCP Relay	Box should remain unchecked
TLS	Box should remain unchecked
DTLS	Box should remain unchecked

2. Click on **Add Listen/Relay IP Pair** to add the Listen/Relay IP Pair for the public and private interfaces. The recommended configuration is to have the Relay address as the Public side, or external, address on the B1 interface and the Listen address as the Private address on the A1 interface. However, Avaya SBCE supports additional interface pairs so it could be B2 and A2.

The example in the following screenshot shows the Listen IP set to Internal SBC IP (A1) — 10.3.3.3. The Media Relay is set to External SBC IP (B1) — 10.2.2.2



3. Go to Device Specific Settings > DMZ Services > Relay Services > Reverse Proxy tab and click **Add** to add the HTTP and HTTPS instances for the reverse proxy.

   The reverse proxy table should be filled out according to the desired target protocol (HTTP or HTTPS).

   - If HTTP is to be used, then only one entry is required. The Listen Port and the Server Port should be set to 80.
   - If HTTPS is to be used, then two entries are required. The first entry should have the Server Port set to 443 and the second entry should have it set to 9443.

   The Listen Port for HTTP or HTTPS can be any unique port relative to the other reverse proxy table entries for this same field. It is recommended that the Listen Port be the same as the Server Port, but it is not required.

   Note:

   HTTP configuration: Port 80 is used to access both the customer developed CE service / WebRTCSampleApplication and the WebRTC service.

   HTTPS configuration: Port 443 is used to access the customer developed CE service / WebRTCSampleApplication and Port 9443 is used to access the WebRTC service. The accessing of Port 9443 is not visible to the end user, but is required for the customer developed CE service / WebRTCSampleApplication to interact with the WebRTC service.

Table 2: Add reverse proxy profile field descriptions

Field	Details
Service Name	Enter a meaningful name for the profile.
Enabled	Check the box to enable to profile.
Listen IP	This is the URL used by the external browser to connect to Avaya Aura® Collaboration Environment, and is usually the B1 interface.
Listen Port	The port number can be any number. This is the port that will be used on the Outside PC browser to connect to the services on CE. The port can be any unique listen port relative to the other reverse proxy table entries for this same field. If a non-standard port is used, this port must be specified in the Collaboration EnvironmentWebRTC Snap-in URL used by the Web Application.
Listen Protocol	Select HTTP or HTTPS
Listen TLS Profile	For HTTP, default is None and the default should be kept.. For HTTPS select `AvayaSBCServer`
Server Protocol	Select HTTP or HTTPS
Server TLS Profile	For HTTP, default is None and the default should be kept. For HTTPS select `AvayaSBCClient`
Connect IP	This is the URL used to reach the WebRTC services on the inside, and is usually the A1 interface.
Load Balancing Algorithm	None is the default. Keep the default.
PPM Mapping Profile	None is the default. Keep the default.
Allow Web Sockets	Leave unchecked
Whitelisted IPs	Leave blank
Server Addresses & Ports	This is the Collaboration Environment Server IP and port. The port can be either 80, 443, or 9443.

4. Go to Device Specific Settings > Advanced Options > Port Ranges tab and configure the **HTTP Port Range**.

   The range should be more than four times the maximum number of simultaneous calls. For example, to support 1000 simultaneous calls the port range should be at least 5000–6000 ports.

5. Go to System Management, select the device name, and click **Restart Application** to activate the changes.

Example

For this section the following IP examples are used:

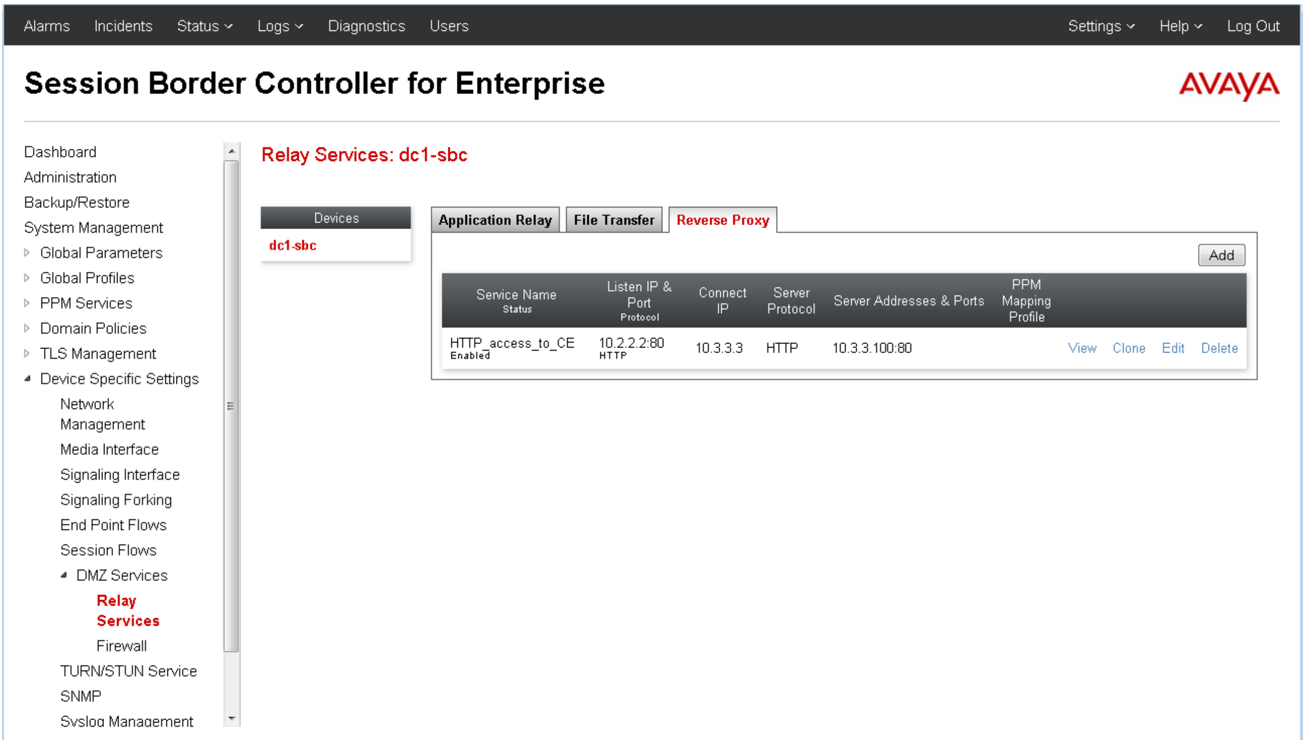
External Subnet = 10.2.2.0/24

- SBC External IP = 10.2.2.2

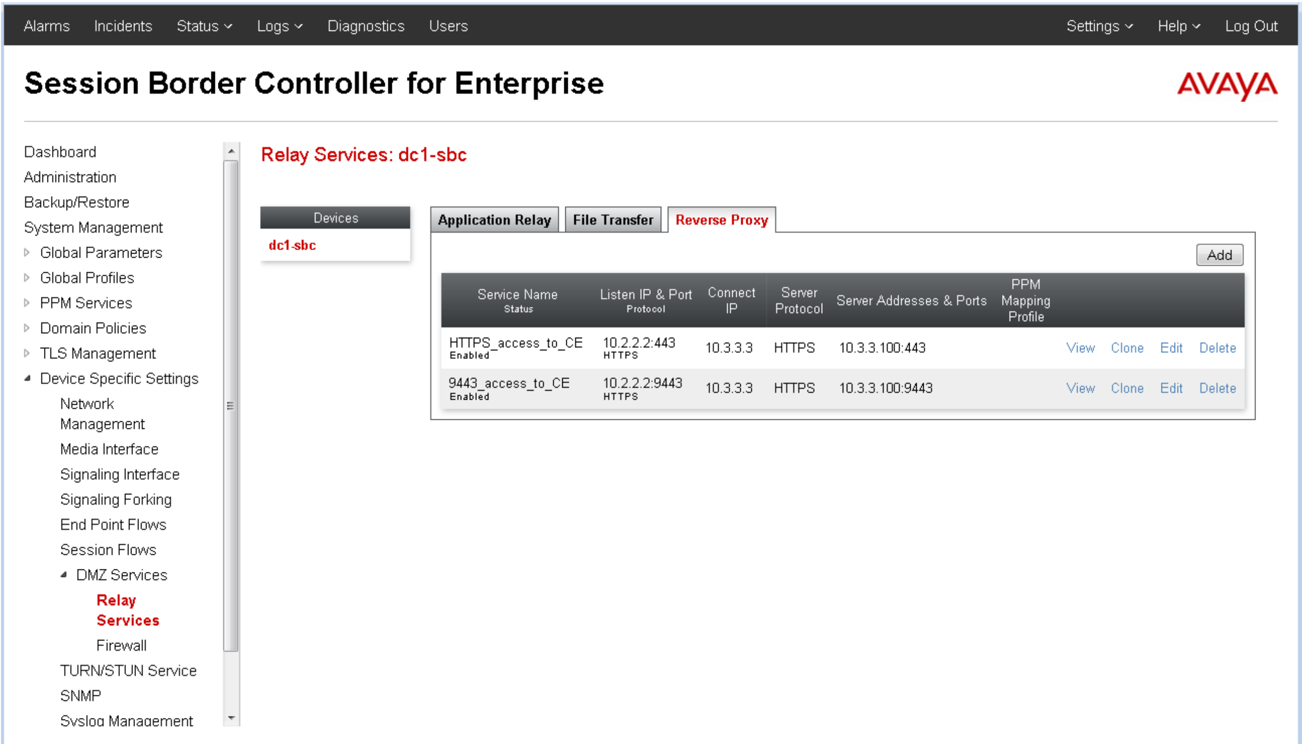
Internal Subnet = 10.3.3.0/24

- SBC Internal IP = 10.3.3.3
- CE Internal IP = 10.3.3.100

HTTP configuration



HTTPS configuration



DMZ Firewall Open Port Requirements

For a complete list of ports utilized by Collaboration Environment, see the Avaya Port Matrix Documents website.

Protocol	Port / Port Range	Description	Communicating Devices
UDP	3478	Listen Port setting on the SBC for the TURN/STUN service	PC (external) <=> SBC (external-B1) SBC (internal-A1) <=> AMS
	50000 - 55000	Media Relay Port Range setting on the SBC	PC (external) <=> SBC (external-B1) SBC (internal-A1) <=> AMS
TCP	80	Required if HTTP is used for service access	PC (external) <=> SBC (external-B1) SBC (internal-A1) <=> CE
	443	Required if HTTPS is used for service access	PC (external) <=> SBC (external-B1) SBC (internal-A1) <=> CE
	9443	Required if HTTPS is used for service access	PC (external) <=> SBC (external-B1) SBC (internal-A1) <=> CE

Figure 2: DMZ open ports

Note:

The SBC Listen ports on B1 of the example can have any TCP port assigned for http, https and 9443. The open port firewall settings for external PCs reaching the SBC should match the SBC Reverse Proxy administration.

Provisioning Avaya Media Server for the WebRTC Snap-in

Before you begin

The Avaya Media Server needs to be set up to work with Avaya Aura® Collaboration Environment as described in *Deploying Avaya Aura® Collaboration Environment* before making the following WebRTC Snap-in changes.

Also, the Avaya Session Border Controller for Enterprise needs to be set up and configured for use with the WebRTC Snap-in before doing these Avaya Media Server configuration steps.

About this task

Perform the following administration tasks in Avaya Media Server for the WebRTC Snap-in.

Procedure

1. Log in to the Avaya Media Server Element Manager.
2. Check that Avaya Media Server nodes and routes are set up correctly.

   See *Deploying Avaya Aura® Collaboration Environment* for details on configuring Avaya Media Server for Avaya Aura® Collaboration Environment.
3. Go to System Configuration > Server Profile > General Settings and enable **Firewall NAT Tunneling Media Processor**
4. Go to System Configuration > Signaling Protocols > SIP > General Settings and enable **Always use SIP default outbound proxy**

   Note:

   SIP administration needs to use the same transport end to end. TCP and TLS on SIP entity links involved with the WebRTC call flow cannot be combined when using this feature. For example, if the Session Manager to Communication Manager entity link is SIP/TLS, then the Session Manager to Avaya Aura® Collaboration Environment entity link, the Session Manager to Avaya SBCE entity link, and the Session Manager to Avaya Media Server entity link also need to be SIP/TLS.
5. Go to System Configuration > Media Processing > ICE > TURN/STUN Servers > Accounts and create a TURN/STUN account. This account ID and password must match the account created on the Avaya SBCE.
6. Go to System Configuration > Media Processing > ICE > TURN/STUN Servers > Servers to add the TURN/STUN connection to the Avaya SBCE server.

7. (Optional) Go to System Configuration > Media Processing > ICE > General Settings and click the **Force Media Through a Configured TURN Server** checkbox.

   Select this option if most browsers are outside of the corporate firewall, and it is desirable to send all UDP traffic through a trusted TURN server rather than using ICE to cross the firewall directly.
8. Save the configuration changes.
9. Restart Avaya Media Server.

Testing the WebRTC Snap-in deployment

About this task

Procedure

1. Confirm that all of the corresponding fields have green check-marks on the Service Management page.
2. Deploy, configure, and run the sample application that is included in the SDK. See: `Avaya-WebRTC-SDK > WebAppSample > documents > WebRTC Sample Application.pdf` for instructions.

Chapter 5: Performance

Performance

The WebRTC Snap-in supports 1800 simultaneous calls at a rate of 28,000 BHCC in the following deployment model:

- 1 Collaboration Environment (CE) server
- 1 Avaya Session Border Controller for Enterprise (Avaya SBCE) server
- 8 Avaya Media Servers

Chapter 6: Security

WebRTC Snap-in security summary

Introduction

The following sections outline several key points about security policy use in the WebRTC Snap-in.

HTTP ingress into the enterprise network

HTTP messages either go through a third-party reverse proxy or through the Avaya SBCE reverse proxy function. This traffic might be challenged and authenticated by the third-party reverse proxy, but usually it is not. HTTP authentication at the enterprise edge would only be applicable for situations where enterprise users were accessing a website that they were using to initiate calls.

While the messages will not be authenticated, other standard reverse proxy policies will be applied.

Validation of the authorization token

The WebRTC Snap-in will validate the authorization token created and encrypted by the web server. If the snap-in can decrypt the token and ensure that the time stamp is valid, it knows that the incoming HTTP request is valid. The time stamp will usually be short lived; on the order of 5-10 seconds to protect against reply attacks. For more information, see the following document in the SDK: `Avaya-WebRTC-SDK > How to Create an Authorization Token.pdf`

Avaya Media Server authentication with TURN server

The only authentication mechanism specified by the TURN specification is digest authentication. In the Avaya Aura® Collaboration Environment WebRTC solution architecture, the client of the TURN server is not a browser, but the Avaya Media Server. A single user name and password will be provisioned in both the Avaya Media Server and Avaya SBCE TURN function for authentication. A suitably strong password should be used.

RTP ingress to the enterprise network

With traditional SIP Border Controllers, the SBC was able to determine which UDP packets to allow into the enterprise because all SIP signaling also passed through the SBC. Any packets coming from an unknown source are discarded.

With WebRTC, on the other hand, there is no standard signaling protocol. Even if the signaling protocol was known, the HTTP-based signaling might not pass through the Avaya SBCE reverse proxy. Therefore the TURN relay will have to have some other means knowing which packets to accept. The ChannelBind TURN request is the key to this. After ICE candidate selection has completed and the Avaya Media Server is aware of the far end IP address / port, Avaya Media Server will issue a ChannelBind request to the TURN server including this information. The TURN server will only accept incoming UDP packets from:

1. An authenticated endpoint or

2. An address specified in a ChannelBind request from an authenticated endpoint.

There is a configuration option on Avaya Media Server that instructs it to only generate TURN candidates. This forces all UDP packets through the TURN server even if they could perhaps have traversed the firewall using hole-punching.

SRTP policy

The media stream between the browser and Avaya Media Server will always be encrypted using SRTP. However, in this release, the media stream between Avaya Media Server and Avaya Aura will not be encrypted.

Chapter 7: Maintenance and Troubleshooting

Maintenance and troubleshooting

If WebRTC calls do not work:

1. Check the HTTP/ HTTPS settings — HTTP OR HTTPS should be used throughout the WebRTC configurations.
2. Check Avaya Media Server node, routes, and outbound proxy configuration. For details see *Deploying Avaya Aura® Collaboration Environment* .
3. Check that the link between Collaboration Environment and System Manager, and System Manager and Avaya Media Server are all either TLS or TCP.
4. Check the Avaya SBCE configuration again, using the steps in this document.

If the WebRTC application was written using the WebRTC Javascript API and still cannot make calls, check that the URL used to connect to WebRTC snap-in is in the following format: http://<ip address>/services/WebRTC/WebRtcServlet or https://<ipaddress>:9443/services/WebRTC/WebRtcServlet to access the snap-in.

See the sample application in the WebRTC SDK for details about using the Javascript library and how to connect to the WebRTC Snap-in.

Log files

The WebRTC Snap-in log files are stored here: /var/log/Avaya/services/WebRTC

Chapter 8: Additional resources

Documentation

See the following related documents at http://support.avaya.com.

Title
Understanding
Avaya Aura® Collaboration Environment Overview and Specification
Implementing
Deploying Avaya Aura® Collaboration Environment
Quick Start to Deploying Avaya Aura® Collaboration Environment Snap-ins
Using
Administering Avaya Aura® Collaboration Environment
Avaya Aura® Collaboration Environment Snap-in Development Guide
Administering Avaya Session Border Controller for Enterprise

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Index