Avaya SBCE 6.3 Security Configuration and Best Practices Guide

Release 6.3
Issue 1.0
October 2014

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: http://support.avaya.com

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE

http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

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 Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

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 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 Web site: http://support.avaya.com

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://support.avaya.com

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

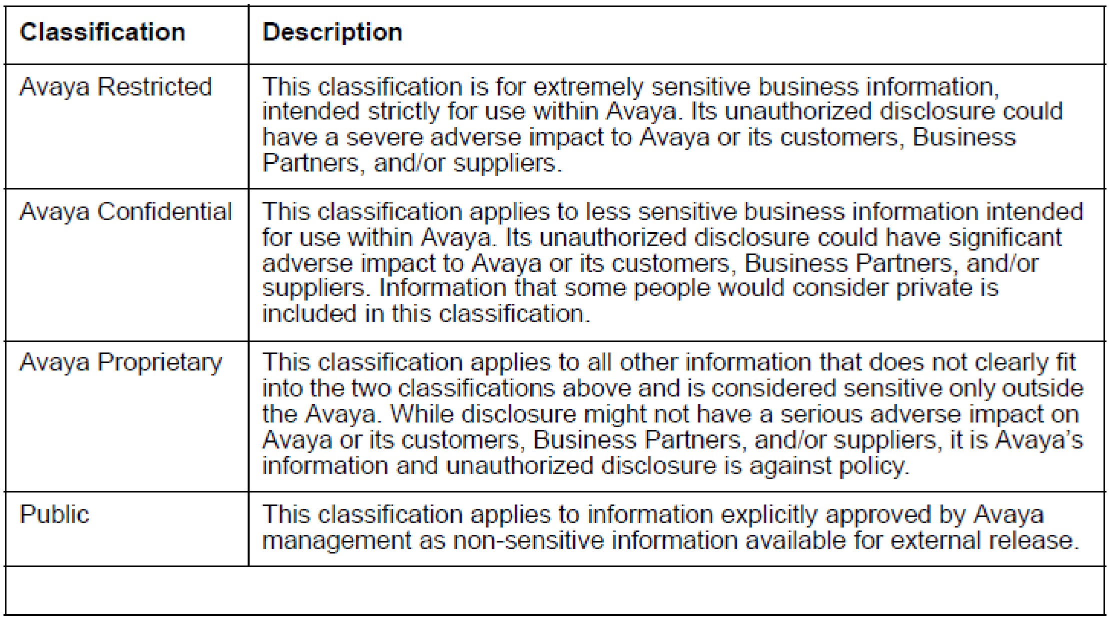
Contents

Introduction

This document provides an overview of security configuration and best practices for Avaya Session Border Controller for Enterprise (SBCE) Release 6.3. The goal of this document is to equip Avaya partners, customers, and sales and system engineers with the information required to configure Avaya SBCE securely.

Information classifications and NDA requirements

This book provides security-related information according to the following information classifications:



Classification	Description
Avaya Restricted	This classification is for extremely sensitive business information, intended strictly for use within Avaya. Its unauthorized disclosure could have a severe adverse impact to Avaya or its customers, Business Partners, and/or suppliers.
Avaya Confidential	This classification applies to less sensitive business information intended for use within Avaya. Its unauthorized disclosure could have significant adverse impact to Avaya or its customers, Business Partners, and/or suppliers. Information that some people would consider private is included in this classification.
Avaya Proprietary	This classification applies to all other information that does not clearly fit into the two classifications above and is considered sensitive only outside the Avaya. While disclosure might not have a serious adverse impact on Avaya or its customers, Business Partners, and/or suppliers, it is Avaya's information and unauthorized disclosure is against policy.
Public	This classification applies to information explicitly approved by Avaya management as non-sensitive information available for external release.

As this book is generally available, the information herein is considered public. While the book contains references to additional information sources, some sources disclose both confidential and proprietary information and require a non-disclosure agreement (NDA) with Avaya.

Disclaimer

Avaya has used reasonable commercial efforts to ensure that the information provided here under is accurate. Avaya might change any underlying processes, architecture, product, description, or any other information described or contained in this document. Avaya disclaims any intention or obligation to update or revise the book, whether as a result of new information, future events, or otherwise. This document is provided "as is," and Avaya does not provide any warranty of any kind, express or implied.

Avaya SBCE security overview

This document describes the security-related considerations, features, and services for Avaya SBCE. As a security product, Avaya SBCE must be resilient to attacks that cause malfunction or theft of service. Avaya SBCE as part of the Avaya solution must be protected from security threats such as:

- Unauthorized access or modification of data

- Theft of data
- Denial of Service (DoS) attacks
- Viruses and Worms
- Theft of data

Avaya multilayer hardening strategy

To prevent security violations and attacks, Avaya SBCE uses the Avaya multilayer hardening strategy:

- Secure by design
- Secure by default
- Secure communications

Secure by design

Secure by design encompasses a secure deployment strategy that separates the management network from the enterprise production network.

The architecture is for the trusted communication framework infrastructure security layer and allows the design of dedicated security zones for:

- Management network
- Untrusted public network
- Trusted Enterprise network

The security zones are like dedicated networks for particular functions or services. The security zones do not need to have access from or to any other zones because the zones only accommodate the data for which they are built.

The management network should be on different VLAN than untrusted and trusted networks on the Avaya SBCE.

Secure by default

Secure by default incorporates a hardened Linux operating system with inherent security features for Avaya SBCE. This hardened operating system provides only the functions necessary to support the core applications, which is important for securing mission-critical call processing applications and protecting the customer from toll fraud and other malicious attacks.

The Linux operating system that Avaya has hardened limits the number of access ports, services, and executables. Also, based on the service, the number of messages or connection rate will be rate limited. These limits protect the system from typical modes of attack. At the same time, the reduction of Linux functions reduces the attack surface which reduces the number of mandatory security patches needed.

Secure Communication

Communications can be secured by encrypting the signaling and media with TLS/SRTP and granular admission control. Criteria used for admission control include source subnet, user agent, and uri group; which can be used to control things like device type and/or users that are allowed thru the SBC. See

Administering Avaya Session Border Controller for Enterprise and related application notes for admission control configuration in Endpoint Flows and Domain Policies.

Example: Avaya recommend use of User Agents.   To create a User Agent Profile, do the following:

1. **Go to Global Parameters>User Agents.**
2. Click Add.
3. Assign the profile a name and the regular expression of the User Agent header. Enter the full User Agent or partial using Regex. An example of a User Agent for a 96x1 is ***Avaya one-X Deskphone**** and this can be found in the User Agent header of messages coming from the endpoint.

The User Agent profile is used on the subscriber flow you create during the remote worker configuration.

Use strong passwords for SIP user login.

Complementing security guides of other Avaya products

This document describes security-related issues and security features of Avaya SBCE. This document complements the security guides that are available for all the managed elements in the Avaya solution. The security guides describe the potential security risks to Avaya products and the features that Avaya products offer to mitigate these security risks.

This document is a descriptive guide, not a procedural guide. Where appropriate, the guide references other product documentation for the actual procedures for configuring and using security features.

Some Avaya Security Guides available on the support.avaya.com are:

- Avaya Toll Fraud Security Guide
- Security Best Practices Checklist for Unified Communications Deployment
- Avaya and Vulnerability Scanning
- Mapping Common Vulnerability Exposure (CVE) numbers to Avaya Security Advisories (ASAs)

Virtualization

Virtualization of SBCs has become more common. However, some network security professionals are concerned that DMZ virtualization might decrease security. This concern is understandable because virtualization involves new terminology and technology. The biggest risk to a DMZ in a virtual environment is misconfiguration, not the technology. Thus, you need strong audit controls to ensure that you avoid misconfiguration, either accidental or malicious. Before deploying Avaya SBCE, refer to the VMware best practices guide for DMZ:
http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf

Avaya SBCE Application security

The Avaya SBCE Control Center allows you to view various security-related features of Avaya SBCE security products, such as:

- Denial-of-Service (DoS) Policies
- Protocol Scrubber Rules
- Encryption
- Secure Remote Access

Denial-of-Service (DoS) Policies

The Avaya SBCE supports following DOS policies:

- **Single Source DoS**: Any type of DoS attack that is directed against one or more enterprise endpoints that originate from a single source. Based on the deployment thresholds for this are configurable. These thresholds are global. Avaya SBCE enforces these thresholds based on the source of an attack. Although default configuration is provided, it is recommended that based on the traffic it needs to be tuned to avoid false positives/ negatives.

  Recommended initial configuration:

  - For Trunk solution the configuration Single source DOS threshold value should be **20(default)** SIP messages per 5sec and Action should be **Block.**
  - For remote worker solution the configuration Single source DOS threshold value should be changed to **300** SIP messages per 5sec and Action should be **Block.**

  If the SBCE is configured for Trunk and Remote worker solution use the remote worker limits.

  - To configure Single source DOS thresholds go to **Global Parameters -> DOS/DDOS -> Single Source DoS**
  - To enable single source DOS feature for the SBCE go to **Device specific settings -> Advanced Options -> Feature control**
- **Phone DoS/DDoS**: A type of DoS attack that is directed against a single enterprise endpoint. Based on the deployment thresholds for this are configurable. These thresholds are absolute. Avaya SBCE enforces these thresholds based on the destination of an attack. This ensures Avaya SBCE can identify DDoS attacks on a particular destination. Although default configuration is provided, the threshold should be tuned based on traffic to avoid false positives/ negatives.

  Recommended initial configuration:

  - For Trunk solution the configuration Phone DoS/DDoS threshold value should be **10 (default)** SIP messages per 3 seconds and Action should be **Block.**
  - For remote worker solution the configuration Phone DoS/DDoS threshold value should be changed to **200** SIP messages per 3 seconds and Action should be **Block.**

If the SBCE is configured for Trunk and Remote worker solution use the remote worker limits.

  - To configure Phone DOS thresholds go to **Global Parameters -> DOS/DDOS -> Phone DoS**
  - To enable Phone DOS feature for the Avaya SBCE go to **Device specific settings -> Advanced Options -> Feature control**

- **Stealth DoS/DDoS** : A type of low-volume DoS attack that is directed against an endpoint. These thresholds are Global. Avaya SBCE enforces these thresholds based on the destination of an attack. This ensures the Avaya SBCE can identify DDoS attacks on a particular destination where the source of the call is constantly changed. Although default configuration is provided, it is recommended that based on the traffic it needs to be tuned to avoid false positives/ negatives.

  By Default this feature will be disabled.

  For Trunk/Remote worker solutions recommended threshold value **5** consecutive average inter call duration threshold violations with average inter call duration threshold of **2** minutes.

  Initially configure Action as **alert** to see if there are any false positives.

  - To configure Stealth DoS/DDoS thresholds go to **Global Parameters -> DOS/DDOS -> Stealth DoS/DDoS.**
  - To enable Stealth DoS/DDoS feature for the SBCE go to **Device specific settings -> Advanced Options -> Feature control**

- **Call Walking**: A type of DoS attack whereby serial calls originating from a single source (normally spoofed) are directed against a sequential group of endpoints. This feature stops the attacks at the reconnaissance phase itself, when an attacker is collecting data to launch attacks. The thresholds are based on unique destinations per minute. Although default configuration is provided, it is recommended that based on the traffic it needs to be tuned to avoid false positives/ negatives.

  By Default this feature will be disabled.

  Recommended thresholds for Trunk/Remote worker solutions:

  - 10 sip messages in 1 min
  - 5 INV in 1 min
  - 5 REG in 1 min

  Initially configure Action as **alert** to see if there are any false positives.

  - To configure Call Walking thresholds go to **Global Parameters -> DOS/DDOS -> Call Walking**
  - To enable Call Walking feature for the SBCE go to **Device specific settings -> Advanced Options -> Feature control**

- **Server DOS:** Per-device signaling and media overload control, call rate control to prevent DoS attacks from reaching service infrastructure such as SIP servers. SIP servers are identified on per IP basis. Since the destination IP of a server cannot be identified before routing is applied, these thresholds are applied after routing. The thresholds are based on both policy and absolute server capacity. Avaya SBCE provides an easy configuration screen for initial recommended thresholds and then admin can adjust the thresholds as needed. The recommended threshold are automatically calculated based on the number of session in SIP Trunk case, or number or potential remote user and number of concurrent sessions in remote user case. Although default configuration is provided, it is recommended that based on the traffic it needs to be tuned to avoid false positives/ negatives.

  Remote worker solution - recommended values for 1000 users and 100 Max Concurrent Sessions (Active calls). Round off to nearest 1000 users and 100 sessions.

SIP Method	Initiated Threshold (per 10 sec)	Pending Threshold	Failed Threshold (per 10 sec)
ALL	16958	1696	1696
INVITE	16	3	2
OPTIONS	2200	440	110
PUBLISH	2200	440	110
REGISTER	2200	440	110
SUBSCRIBE	8800	880	880

Trunk Solution - recommended values for 100 Max Concurrent Sessions(Active calls). Round off to nearest 100 sessions.

SIP Method	Initiated Threshold (per 10 sec)	Pending Threshold	Failed Threshold (per 10 sec)
ALL	227	45	23
INVITE	166	33	17
OPTIONS	20	10	10
PUBLISH	0	0	0

REGISTER	2200	440	110
SUBSCRIBE	0	0	0

To configure Server DoS, go to **Server Configuration -> {Server Profile} -> Advanced Tab and select the Enable DoS Protection checkbox. Next select the Dos Protection tab and recalculate values.**

- **Domain DOS:** This is similar to server DOS. Avaya SBCE provides an easy configuration screen for initial settings and then admin can adjust the thresholds as needed. The recommended threshold are automatically calculated based on the number of session in SIP Trunk case, or number or potential remote user and number of concurrent sessions in remote user case. Although default configuration is provided, it is recommended that based on the traffic it needs to be tuned to avoid false positives/ negatives.

  Remote worker solution - recommended values for 1000 users and 100 Max Concurrent Sessions (Active calls). Round off to nearest 1000 users and 100 sessions

SIP Method	Initiated Threshold (per 10 sec)	Pending Threshold	Failed Threshold (per 10 sec)
ALL	16958	1696	1696
INVITE	16	3	2
OPTIONS	2200	440	110
PUBLISH	2200	440	110
REGISTER	2200	440	110
SUBSCRIBE	8800	880	880

Trunk Solution - recommended values for 100 Max Concurrent Sessions(Active calls). Round off to 100 sessions

SIP Method	Initiated Threshold (per 10 sec)	Pending Threshold	Failed Threshold (per 10 sec)
ALL	227	45	23

INVITE	166	33	17
OPTIONS	20	10	10
PUBLISH	0	0	0
REGISTER	2200	440	110
SUBSCRIBE	0	0	0

To configure Domain DoS go to **Global Profiles -> Domain DoS.** After creating the profile you want to enable it on your Security Rules by going to **Domain Policies -> Security Rules -> {Security Profile} -> Domain DoS and Editing the DoS settings to select the profile created.**

Protocol Scrubber

Protocol Scrubbing is an Avaya SBCE feature that utilizes a highly sophisticated statistical mechanism to thoroughly check incoming SIP signaling messages for various types of protocol-specific events and anomalies. It verifies certain message characteristics such as proper message formatting, message sequence, field length, and content against updatable templates received from Avaya. Typically, messages which violate the security rules dictated by the scrubber templates are dropped while those which violate syntax rules are repaired. How the message is re-written, truncated, rejected, or dropped depends on the processing rules imposed by the templates.

The following Scrubber Packages can be used for Remote Worker/Trunking Scenarios. There could be a common place holder ticket if there are false positives reported for these Scrubber Packages.

Package	**Description**	**Used for**
SPKG0001 - Syntax	Rules are derived based on the SIP 3261 ABNF for mandatory/optional SIP/SDP headers	Trunk
SPKG0002 – Protos	Rules are derived based on the SIP Protos Test Suite [Validates IP Address/Domains] for mandatory/optional SIP/SDP Headers	Trunk, Remote worker
SPKG0003 – Do not Use	Legacy – not applicable to Avaya	Do not Use
SPKG0004 - Avaya	Avaya	Remote worker

To configure Scrubber go to **Domain Policies -> Security Rules -> {Security Profile} -> Scrubber**

For Scrubber default action is **Alert.** To change the Scrubber action go to **Global Parameters -> Scrubber -> Rules.**

Encryption

Encryption can reduce the risk of intercepting phone conversations, voice mail, and the SIP messages that support them both. A call consists of voice (RTP) data and signaling (SIP) messages. Both media and signaling data can pass through many devices and networks, sometimes over a separate network or virtual path from each other. Without encrypting both data types anyone with access could intercept:

- RTP in phone calls and voice mail
- SIP messages

Following table shows how encryption mitigates the vulnerabilities in SIP and RTP.

	Unencrypted (Clear)	**Encrypted**
SIP	Susceptible to message spoofing and registration hijacking	Prevents message spoofing and hides sensitive information
RTP	Vulnerable to eavesdropping	Prevents eavesdropping

Avaya SBCE uses the Transport Layer Security (TLS) protocol as a transport protocol for encrypting SIP messages to prevent eavesdropping and tampering of communications sent across a network.
See Chapter 12 in *Administering Avaya Session Border Controller for Enterprise* to configure the TLS for remote worker solution.

Avaya SBCE supports SRTP for encrypting the media traffic to prevent eavesdropping. See Chapter 5 in *Administering Avaya Session Border Controller for Enterprise* to configure SRTP as part of Media rules.

Certificates

It is recommended to use 3rd Party CA certificates for enhanced security.

Secure Remote Access

Setting files and firmware files

In Remote Worker solution, Avaya telephones use HTTP/HTTPS to get initial configurations settings file (e.g., 46xx_settings.txt) and firmware upgrades. The 96x1 telephones support identify certificates. These certificates can be used for TLS mutual authentication for securing the settings file download and firmware upgrades. To avoid unauthorized access to settings file and firmware files use TLS mutual authentication. See *Administering Avaya Session Border Controller for Enterprise* to configure the TLS mutual authentication in the TLS profile.

Note: Not all the telephones support mutual authentication for firmware download. Refer to the appropriate telephone documentation for the support and configuration to enable TLS mutual authentication for firmware download.

You must always use http reverse proxy service in Avaya SBCE for setting files and firmware files downloads. Do not use relay services.

Recommended configuration and procedures TLS mutual authentication

Configure SBCE http proxy service for https(no http) for settings file and firmware download.

96x1 Phone staging:

96x1 phone firmware 6.3 or later version is required.

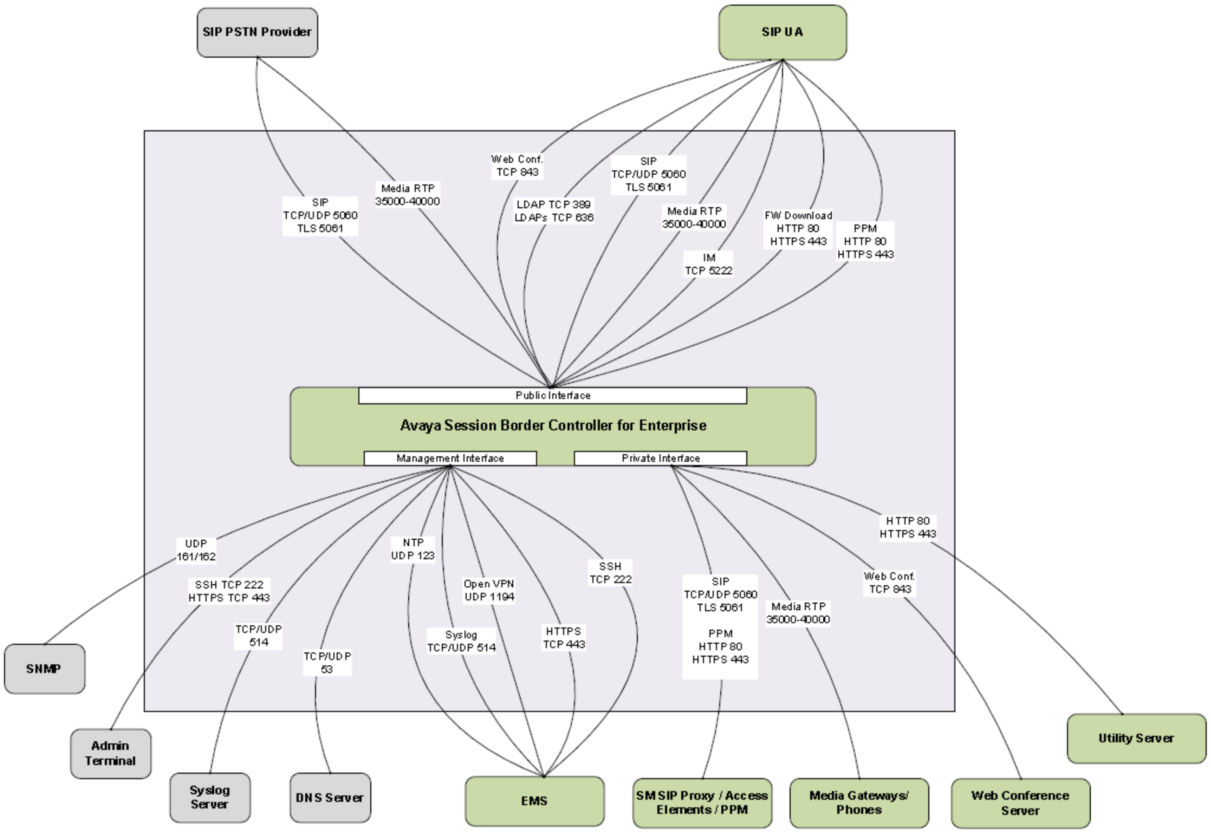
A two-step approach is required if there is no http access from remote locations and mutual authentication is required.

1) The phone must internally download the settings/certificates via http

2) Ready for remote deployment

Port Matrix

Following are the default ports used.


SIP PSTN Provider
SIP UA
SIP TCP/UDP 5060 TLS 5061
Media RTP 35000-40000
Web Conf. TCP 843
LDAP TCP 389 LDAPs TCP 636
SIP TCP/UDP 5060 TLS 5061
Media RTP 35000-40000
IM TCP 5222
FW Download HTTP 80 HTTPS 443
PPM HTTP 80 HTTPS 443
Public Interface
Avaya Session Border Controller for Enterprise
Management Interface
Private Interface
UDP 161/162
SSH TCP 222 HTTPS TCP 443
TCP/UDP 514
TCP/UDP 53
NTP UDP 123
Syslog TCP/UDP 514
Open VPN UDP 1194
HTTPS TCP 443
SSH TCP 222
SIP TCP/UDP 5060 TLS 5061
PPM HTTP 80 HTTPS 443
Media RTP 35000-40000
Web Conf. TCP 843
HTTP 80 HTTPS 443
SNMP
Admin Terminal
Syslog Server
DNS Server
EMS
SM SIP Proxy / Access Elements / PPM
Media Gateways/ Phones
Web Conference Server
Utility Server