# Avaya SBCE 7.0 Security Configuration and Best Practices Guide

**Release: 7.0**
**Issue: 1.0**
**December 2015**

**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/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" 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.

**Hosted Service**

"**Hosted Service**" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

**Hosted Service**

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, 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**

**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.

**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 is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products," or such successor site as designated by Avaya. 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 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, 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 written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Virtualization**

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

**Third Party Components**

"**Third Party Components**" mean certain software programs or portions thereof included in the Software or Hosted Service 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"). As required, 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 products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

**Service Provider**

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

**Compliance with Laws**

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

**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.

**Security Vulnerabilities**

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

**Trademarks**

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), 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, Hosted Service(s) 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 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

# Introduction

This document provides an overview of security configuration and best practices for SBCE Release 7.0. The goal is to equip Avaya partners, customers, and sales and system engineers with the information required to configure 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 at this date. 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 Management 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 zones are like dedicated networks for particular functions or services. They do not need to have access from or to any other zones because they only accommodate the data they are built for.

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 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 admin guide and app notes for admission control configuration in Endpoint Flows and Domain Policies.

## 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 website 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 becomes more common. However, some network security professionals are concerned that DMZ virtualization might decrease security. This 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 SBC refer to VMware best practices guide for DMZ - http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf

Because of this following is our order of preference:

1. Physical appliance
2. Vmware –DMZ with Separate Physical Trust Zones – Aura and ASBCE  located in separate servers
3. Vmware - DMZ with Virtual Separation of Trust Zones – Aura and ASBCE located in same servers and are separated by virtual trust zones. need strong audit controls to ensure that you avoid misconfiguration. Virtual servers must use the physical network and pass through physical security devices to communicate ASBCE trust zones. In other words use separated NICs for trusted and untrusted zones.
4. Vmware – collapsed DMZ - This completely virtual infrastructure can fully enforce isolation and security between the ASBCE zones. This will be complex and highly risky.  So, least preferred and we don’t recommend this option.

Management/services should always use separate NIC.

## 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.

Default configuration

Single source DoS threshold value is 300 (default) SIP messages per 5sec and Action is **Alert**.

Recommended initial configuration

For Trunk solution the configuration Single source DOS threshold value should be **20** 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, it is recommended that based on the traffic it needs to be tuned to avoid false positives/ negatives.

Default configuration

Phone DoS/DDoS threshold value is 200 (default) SIP messages per 3sec and action is **Alert**.

Recommended initial configuration

For Trunk solution the configuration Phone DoS/DDoS threshold value should be **10** SIP messages per 3sec 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 sec 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 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 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** min.

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. 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).

| 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).

| 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. 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).

| 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).

| 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 will be dropped while those which violate syntax rules will be repaired (either re-written, truncate, rejected, or dropped, depending upon 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 | 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.
- compares how encryption

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.
Refer to Chapter 9 in the Administering Avaya Session Border Controller for Enterprise guide for configuring the TLS for remote worker solution.

Avaya SBCE supports SRTP for encrypting the media traffic to prevent eavesdropping. Refer to the Chapter 5 in Avaya SBCE admin guide for configuring SRTP as part of Media rules.

## Secure Remote Access

### Setting files and firmware files

In Remote Worker solution Avaya phones uses HTTP/HTTPS to get initial configurations settings file(46xx_settings.txt) and firmware upgrades. 96x1 phones supports 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. Refer to Avaya SBCE admin guide for configuring the TLS mutual authentication in the TLS profile.

Please note all the phones does not support mutual authentication for firmware download, refer to the phone documentation for the support and configuration to enable TLS mutual authentication for firmware download.

**Recommended configuration and procedures TLS mutual authentication**

Configure SBCE http proxy service for https(no http) for settings file and firmware download. Do not use relay service for file downloads.

Phone staging:

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.