



Avaya Session Border Controller for Enterprise Overview and Specification

Release 6.2
Issue 2
December 2013

Notice

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya 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](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.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo/> under the link "Heritage Nortel Products", 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, 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.

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 Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

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.

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

Chapter 1: Introduction.....	7
Purpose.....	7
Intended audience.....	7
Document changes since last issue.....	7
Related resources.....	8
Documentation.....	8
Training.....	8
Avaya Mentor videos.....	9
Support.....	9
Warranty.....	9
Chapter 2: Avaya Session Border Controller for Enterprise overview.....	11
Advanced Services.....	11
Basic Services.....	13
Functional entities.....	14
Signaling element.....	14
Media element.....	15
Intelligence element.....	15
Deployment modes.....	16
Two-wire deployment.....	16
One-wire deployment.....	17
Feature description.....	18
Media anchoring.....	18
Media forking.....	18
Mobile workspace user.....	19
Remote management services.....	20
Signaling manipulation.....	20
Signaling forking.....	20
SIP trunking.....	20
UCID.....	22
Support for Video SRTP.....	22
REFER Handling.....	23
Multi Device Access.....	26
Reinvite handling.....	27
New in this release.....	27
Chapter 3: Interoperability.....	29
Product compatibility.....	29
Avaya SBCE supported servers.....	29
Avaya products.....	29
Third-party product requirements.....	30
Operating system compatibility.....	31
Chapter 4: Performance specifications.....	33
Capacity and scalability specification.....	33
Redundancy and high availability.....	33
Avaya SBCE high availability.....	34

EMS replication.....	35
Chapter 5: Environmental requirements.....	37
Altitude and air pressure requirements.....	37
Hardware dimensions and clearance requirements.....	37
Temperature and humidity requirements.....	38
Power requirements.....	38
Physical system protection requirements.....	39
Regulatory standards.....	39
Chapter 6: Security.....	41
Security specification.....	41
Unified communications intrusion protection.....	41
Attack protection.....	42
Avaya SBCE hardening.....	43
Protection against layer 3 and layer 4 floods and port scans.....	43
DoS security features.....	45
Protocol scrubber.....	46
Topology hiding.....	46
Firewall rules.....	46
Port utilization specification.....	51
Management interface port restrictions.....	51
TCP packets.....	52
SSH port.....	52
Additional port assignments.....	52
Chapter 7: Licensing requirements.....	55
Glossary.....	57
Index.....	61

Chapter 1: Introduction

Purpose

This document describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.

Intended audience

This document is intended for people who want to gain a high-level understanding of the product features, functions, capacities, and limitations.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Added UCID feature.
- Added support for Video SRTP.
- Added REFER handling.
- Added Multi Device Access.
- Added Reinvite handling.
- Modified section on DoS security features.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at <http://support.avaya.com>

Title	Description	Audience
Implementation		
Installing Avaya Session Border Controller for Enterprise	Hardware installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.	Implementation Engineers
Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading: • Software-only from Sipera 4.0.5 to Avaya SBCE 6.2 • Avaya Aura® Session Border Controller 6.0 to Avaya SBCE 6.2	Implementation Engineers
Administration		
Administering Avaya Session Border Controller for Enterprise	Configuration and administration procedures.	Implementation Engineers, Administrators

Training

The following course is available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
5U00090E	Knowledge Access: Avaya Session Border Controller

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <http://support.avaya.com>, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to <http://www.youtube.com/AvayaMentor> and perform one of the following actions:
 - Enter a key word or key words in the Search Channel to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

 Note:

Videos are not available for all products.

Support

Visit 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.

Warranty

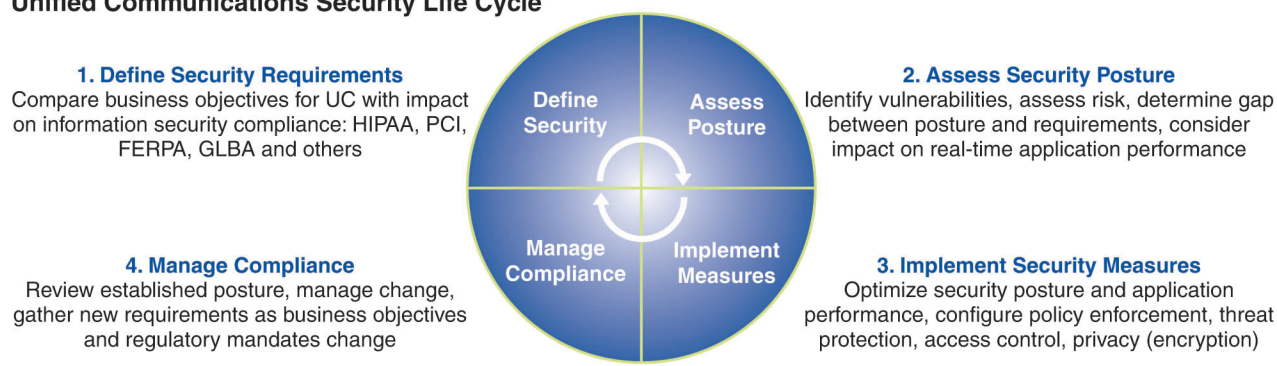
Avaya provides a one-year limited warranty on Avaya SBCE hardware and 90 days on Avaya SBCE software. Refer to the sales agreement or other applicable documentation for detailed terms and conditions of the limited warranty. In addition, a description of Avaya's standard warranty, and details for support under warranty, are available at the Avaya Support website <http://support.avaya.com/> or the Enterprise portal <http://enterpriseportal.avaya.com/ptWeb/gs/services/SV0452/JobAidsTools>.

Chapter 2: Avaya Session Border Controller for Enterprise overview

The Avaya SBCE delivers security to a SIP-based Unified Communications network. It is available in two versions: Advanced Services and Basic Services. Either version can reside on one of two servers, the Dell R210 II XL or the Portwell CAD-0208. The smaller Portwell CAD-0208 server provides identical capabilities to the Dell R210 II XL, except that it does not offer media forking or high-availability support for media and signaling .

The Avaya SBCE has two main components: the Session Border Controller (SBC) and a management system called the Element Management System (EMS). In the simplest configuration, the SBC and EMS co-reside in the same physical server. High availability configurations require a separate EMS server.

Unified Communications Security Life Cycle



cysbucyc LAO 021813

Figure 1: Avaya SBCE UC Security Solution

Advanced Services

Advanced Services is a highly specialized Unified Communications (UC) security product that protects all IP-based real-time multimedia applications, endpoints and network infrastructure from potentially catastrophic attacks and misuse. It provides the real-time flexibility to harmonize and normalize all types of enterprise communications traffic to maintain the highest levels of network efficiency and security.

Advanced Services provides the security functions required by the ever changing and expanding UC market. It protects from malicious attacks that can arise from anywhere in the

world at any time, attacks that are targeted at any wire-line or wireless enterprise or service provider that has deployed UC. Avaya SBCE Advanced Services is the only UC-specific security solution that effectively and seamlessly incorporates all existing approaches into a single, comprehensive system. Advanced Services:

- Protects session-based, real-time Internet Protocol (IP) communications applications such as UC, Instant Messaging (IM), video, and multimedia.
- Prevents the unauthorized use of the UC network infrastructure's assets.
- Protects the privacy of the real-time multimedia user.
- Protects the entire network infrastructure, including all endpoints, from various UC-specific Denial-of-Service (DoS) signaling and media attacks ranging from simple, brute-force flood and harvesting attacks to the more sophisticated zombie, spoof, and malicious user-driven distributed, stealth, blended, zero-day, and SPAM attacks.
- Provides unparalleled protection to all SIP-based UC networks.

Avaya SBCE Advanced Services incorporates the best practices of all phases of data security to ensure that new UC threats are immediately recognized, detected, and eliminated. Not only does it have the unique ability to dynamically learn various aspects of real-time multimedia user behavior, it also handles different UC protocol misuse and voice SPAM attacks. Advanced Services incorporates security techniques that includes UC protocol anomaly detection and filtering and behavior learning-based anomaly detection. Together, these techniques monitor, detect, and protect any UC network from any known security vulnerabilities such as:

- Pre-DoS reconnaissance attacks (i.e., Call Walking or Directory Harvesting and Toll Fraud or unauthorized toll calls).
- Flood Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks
- Stealth DoS / DDoS attacks
- Message Fuzzing (Buffer Overflow and Malformed Messages)
- Spoofing
- Media Anomalies
- Session Anomalies
- Protocol Misuse
- Rogue Media

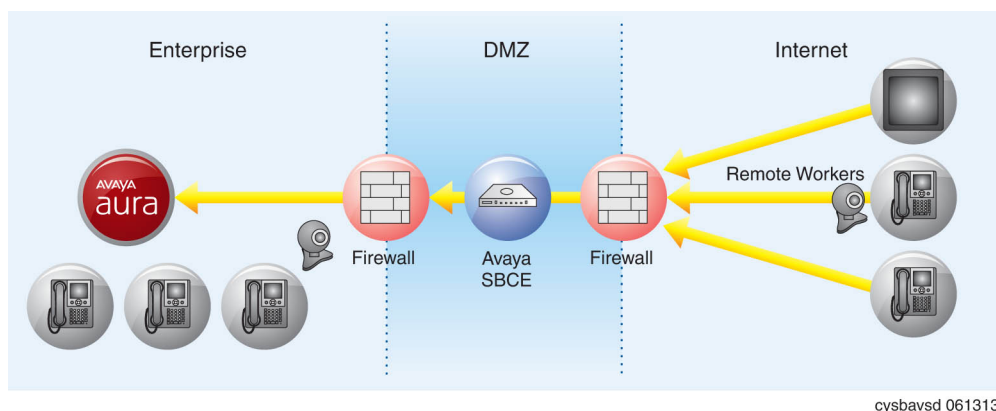


Figure 2: Advanced Services Solution

Basic Services

Avaya Session Border Controller for Enterprise Basic Services provides a subset of the functionality of the Advanced Services offer. It has all the functionality required for an enterprise to terminate SIP trunks without the complexity and higher price associated with typical SBCs.

Avaya SBCE Basic Services is a true enterprise session border controller (SBC), not a repackaged carrier SBC. It provides a lower-cost alternative to the more expensive Carrier SBCs, while at the same time providing an Enterprise SBC that is affordable, highly scalable, and easy to install and manage. It is a plug-and-play solution for Enterprises and Small to Medium Businesses.

Based on Avaya's extensive experience in SIP trunk deployments, supporting hundreds of thousands of enterprise users, Avaya SBCE Basic Services features the unique Signaling Manipulation module (SigMa module), which dramatically simplifies the deployment of SIP trunks. The SigMa module streamlines integration of SIP trunks into any of thousands of variations of enterprise SIP telephony environments, greatly reducing implementation time. As a result, SIP trunk deployment in many standard configurations can occur in two hours or less.

Avaya SBCE Basic Services offers:

- Industry standard SBC functionality with Avaya's industry-leading VoIP, SIP, and Unified Communications security expertise.
- Upgrade options to comprehensive application-layer communications security, UC firewalling, archiving compliance, VoIP and UC proxying, teleworkers, Borderless UC, advanced endpoint security, and the industry's best protection against VoIP toll fraud and UC intrusion.

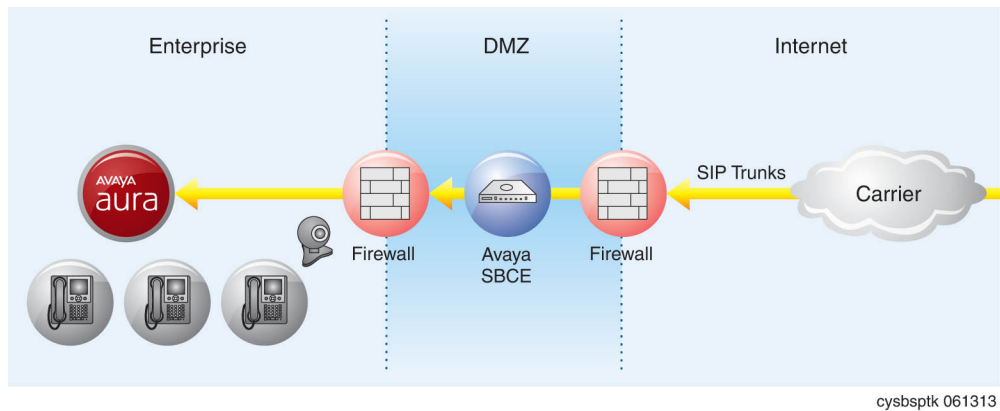


Figure 3: Basic Services Solution

Functional entities

Avaya SBCE security products perform security functions using three interrelated and complementary functional entities (*signaling*, *media*, and *intelligence*). These functional entities can either be packaged in the same physical unit, or deployed separately throughout the enterprise network.

Signaling element

The Signaling element is the primary call signaling protection subsystem. It is typically deployed at the edge of the network, in the DMZ. Functioning as a proxy, the Signaling element accounts for less than 2 ms of the entire end-to-end latency budget.

The Signaling element provides the following features:

- Inline signaling decryption and secure key management (TCP and TLS support)
- Hardware-accelerated SIP decoding
- Enhanced SIP validation (source limiting, policy enforcement, and DDoS detection)
 - NAT/FW traversal
 - SIP network protection
 - SIP trunk and encrypted voice extranet protection
 - Protocol anomaly detection and prevention
 - SIP source limiting
 - DoS and DDoS attack detection and prevention

- Message sequence anomaly detection and prevention
- Continuous user behavior learning
- By-pass for all non-SIP traffic (ARP, DNS, ICMP, STUN, and TURN)
- Domain-based policy filtering based upon user-definable call source and destination criteria
- Fingerprint anomaly detection
- Behavior anomaly detection
- Spoofing and machine-generated call detection (MCD)
- Alarm generation and incident reporting to the Avaya SBCE intelligence functional element

This entity also provides the configuration information to the remote endpoints; it transmits the Personal Profile Manager (PPM) information to the phone, over http or https.

Media element

The media element is the primary RTP media protection subsystem. It is typically deployed in the network in conjunction with the Signaling element. The Media element can be deployed in a distributed model as a separate physical entity within a network to facilitate various types of network topologies. When deployed separately, the Media element is 'slaved' to a particular Signaling element to provide seamless RTP security and NAT traversal. In either deployment, the Media element accounts for less than 100 μ s of the end-to-end latency budget.

The Media element provides the following features:

- Media policy enforcement
- RTP anomaly detection
- Timing and bandwidth validation
- Codec validation
- FAX and modem tone detection intelligence

Intelligence element

The Intelligence element is the primary UC security information management subsystem of the Avaya SBCE solution. Its primary purpose is to receive the variously formatted event and alarm reports from the different security components in the network and to store, normalize, aggregate and correlate that information into a comprehensive format that allows distributed attacks to be effectively detected and mitigated.

The Intelligence function provides the following features:

- Event log collection
- Propagate instructions to the Signaling entity to execute preventative actions
- Propagate alarms to network management systems
- Maintains caller Trust Scores, White Lists, and Black Lists
- Master storage repository for callers and domains
- Maintain per-user, per-caller, and per-network element behavior models on a ToD and DoW basis

Deployment modes

Avaya SBCE security products can be deployed in either of two basic modes: *two-wire (In-line)* or *one-wire (Screened Subnet Mode)*. The mode selected depends upon organizational security needs and requirements. Avaya SBCE devices can be deployed in these modes with or without Transport Layer Security (TLS) / Secure Real-Time Transport Protocol (SRTP) encryption.

Regardless of deployment scenario the security products offer complete flexibility and intuitive configuration. They do not require any management on the endpoints in addition to what is necessary to enable TLS/SRTP and digest authentication.

Two-wire deployment

The two-wire topology (also referred to as *in-line*) is the simplest and most basic deployment. Positioned at the edge of the network in the DMZ, directly in-line with the call servers, the Avaya SBCE protects the enterprise network against all types of inadvertent and malicious intrusions and attacks.

In this configuration, the Avaya SBCE performs border access control functionality such as Firewall / Network Address Translation (FW/NAT) traversal (both internal and external), access management and control based on user-configurable domain policies, and intrusion functionality to protect against DoS, spoofing, and stealth attacks, along with voice SPAM.

The two-wire Avaya SBCE deployment enables TLS encryption of the signaling traffic and SRTP encryption of the media traffic.

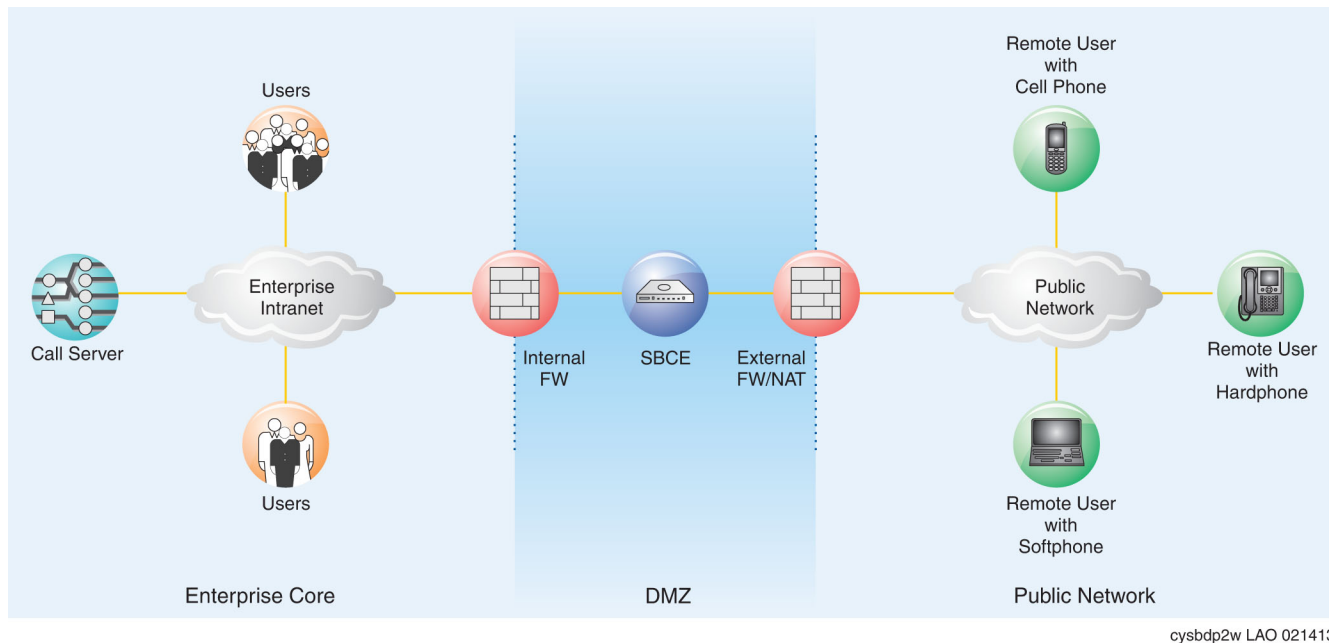
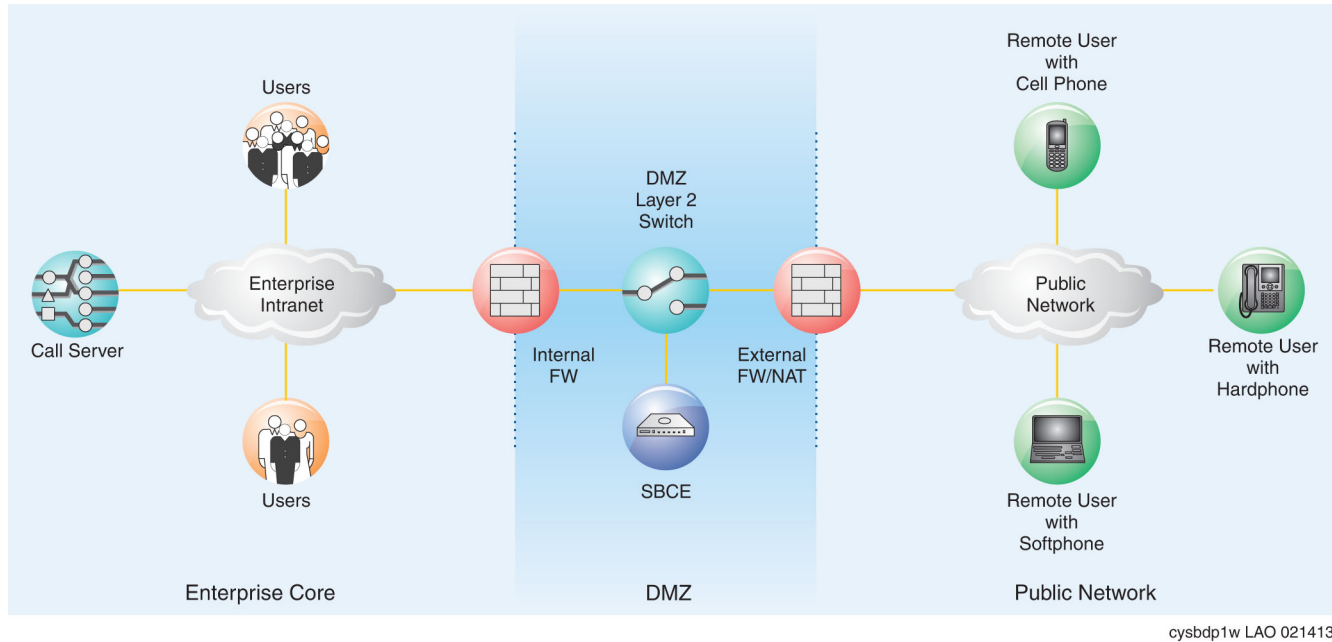


Figure 4: Avaya SBCE Deployment – Two-Wire

One-wire deployment

With the one-wire deployment (also referred to as the *screened subnet*), the Avaya SBCE is deployed in the enterprise DMZ, but not directly in-line with the enterprise call servers. The SBC is in the direct signaling path, uses a single Ethernet interface, and is the next hop for SIP traffic.

The Avaya SBCE in a one-wire deployment provides a high level of security functionality characteristic of in-line deployment. It does not add any latency to time-critical, multimedia applications such as video conferencing or music-on-demand as compared to a two-wire deployment.



cysbdp1w LAO 021413

Figure 5: Avaya SBCE Deployment – One-Wire

Feature description

Media anchoring

The Avaya SBCE anchors the media streams of all media that passes through the SBC. This allows the SBC to perform functions such as SRTP termination (where the SBC decrypts or encrypts RTP traffic based on security policies), NAT traversal, or Media Forking. All supported configurations require Media Anchoring.

Media forking

Advanced Services offer only.

With Media Forking users can configure the Avaya SBCE to copy RTP streams to an external recording device. Customers can use Media Forking to meet compliance requirements or to ensure the quality of the media stream.

When Media Forking is enabled, the SBC anchors the media streams between the remote endpoints and uses a network interface to mirror the media traffic to a compatible recording device. The SBC also rewrites IP/Port headers in the relevant RTP messages to ensure that

the IP/Port in the message matches the respective addresses in the SIP signaling messages.

If the external recording device also requires call detail: the device can use APIs provided by the deskphone to retrieve information; or Signaling Forking can forward signaling data to the device.

Media Anchoring must be enabled for Media Forking to function properly.

Mobile workspace user

Advanced Services offer only.

Mobile Workspace User (previously called Remote Worker) gives SIP, remotely-located users access to the internal enterprise Unified Communication (UC) network by implementing comprehensive UC security features. These features include sophisticated firewall/NAT traversal, encryption, user authentication, and session and endpoint call policy enforcement.

Mobile Workspace User is available for SIP deployments. It uses authentication to verify the legitimacy of the remote user and decrypts TLS-encrypted signaling SIP traffic in real-time. Once decryption is completed, the Avaya SBCE analyzes traffic for anomalous behavior, attacks, and intrusions, and applies the user-defined UC policies.

If the call is from a remotely located Mobile Workspace User (outside the enterprise network) to an internal user (inside the core enterprise network), the Avaya SBCE in the enterprise DMZ also decrypts the SRTP media coming in to the enterprise from the external IP network (the Internet). The SBC performs any required Network Address Translation (NAT), analyzes traffic for anomalous behavior, and applies the relevant UC media policies. The Avaya SBCE in the DMZ passes the RTP stream to the intended recipient.

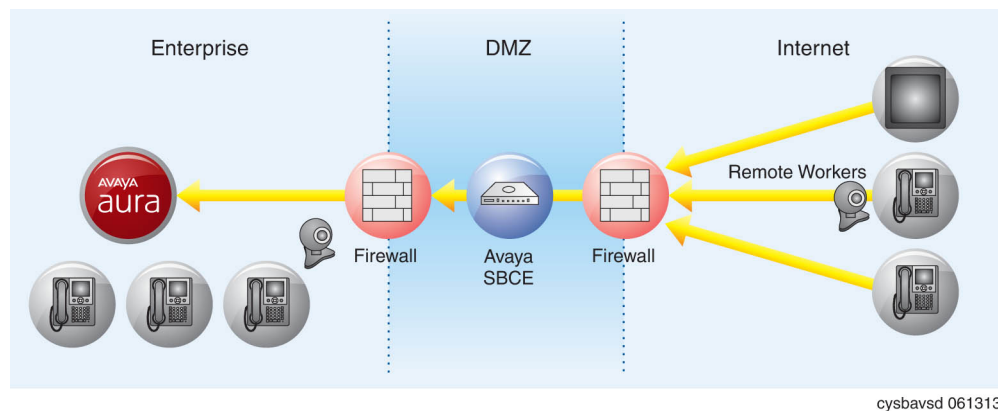


Figure 6: Mobile Workspace User

Remote management services

An IP Office Secure Sockets Layer (SSL) virtual private network (VPN) service provides secure tunneling between an Avaya services/support site and an Avaya SBCE that is installed at a customer site. The secure tunnel allows Avaya service providers to offer remote management services such as fault management, monitoring, and administration to IP Office customers.

Remote Management Services gives Avaya customer support agents easy access to the Session Border Controller GUI/SSH.

Signaling manipulation

Avaya SIP signaling header manipulation lets users add, change, and delete any of the headers and other information in a SIP message. It gives flexibility to configure this manipulation at each flow level using a proprietary scripting language.

Signaling forking

Advanced Services offer only.

Signaling Forking forwards copies of signaling data to an external recording device. Customers can use Signaling Forking to keep records of each call's signaling stream for quality assurance and debugging. With Signaling Forking, the original call progresses as normal, while the SBC creates a copy of only the signaling stream. The SBC sends the copy to the alternate destination.

SIP trunking

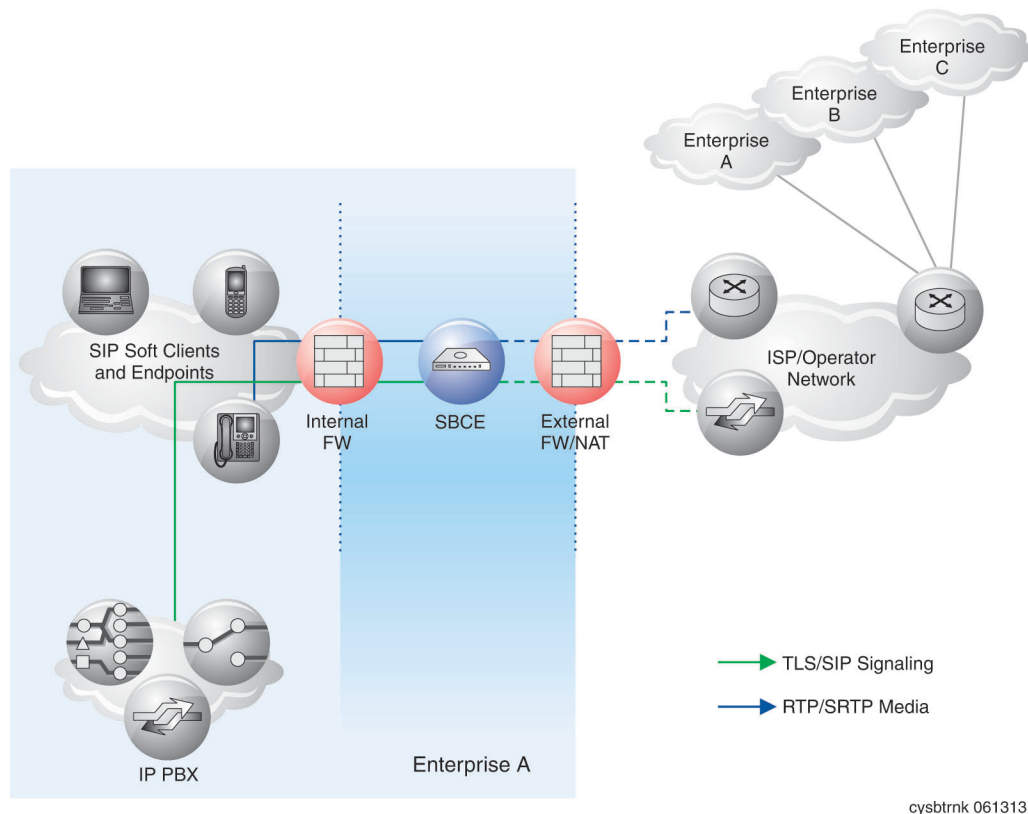
SIP Trunking allows SIP trunk-enabled enterprises to completely secure SIP connectivity over the Internet via SIP Trunking services obtained through an Internet Telephony Service Provider (ITSP).

SIP trunking ensures the privacy of all calls traversing the enterprise network, while maintaining a well-defined demarcation point between the core and access network. In addition, the SIP trunking feature allows an enterprise to maintain granular control through well-defined domain policies securing customers' SIP implementations/servers from known SIP and Media vulnerabilities.

Because the Avaya SBCE is deployed in the enterprise DMZ as a trusted host, all SIP signaling traffic destined for the enterprise is received by the external firewall and sent to the Avaya SBCE for processing.

If the signaling traffic is encrypted, the Avaya SBCE decrypts all TLS encrypted traffic and looks for anomalous behavior before forwarding the packets through the internal firewall to the appropriate IP PBX in the enterprise core to establish the requested call session.

When a valid call session has been set up, Real-Time Transport Protocol (RTP) or Secure Real-Time Transport Protocol (SRTP) media packets are allowed to flow through the external firewall to the Avaya SBCE in the DMZ. The SBC then looks for anomalous behavior in the media before passing the RTP/SRTP stream on to the intended endpoint.



cysbtrnk 061313

Figure 7: SIP Trunking

UCID

The UCID is an Avaya proprietary call identifier used in Contact Center applications for monitoring, control and recording of calls at non SIP interfaces of CTI. It can be also be used to track call history.

AACC

The generation of UCID by Avaya Aura[®] Session Border Controller is required in Avaya Aura[®] Contact Center 7.0 environment. A UCID is assigned to any incoming call at the border SBC so that AACC has a unique handle for each call. For instance, AACC then monitors or controls any application including call recorder using the CTI interface and the UCID for the call.

CC Elite

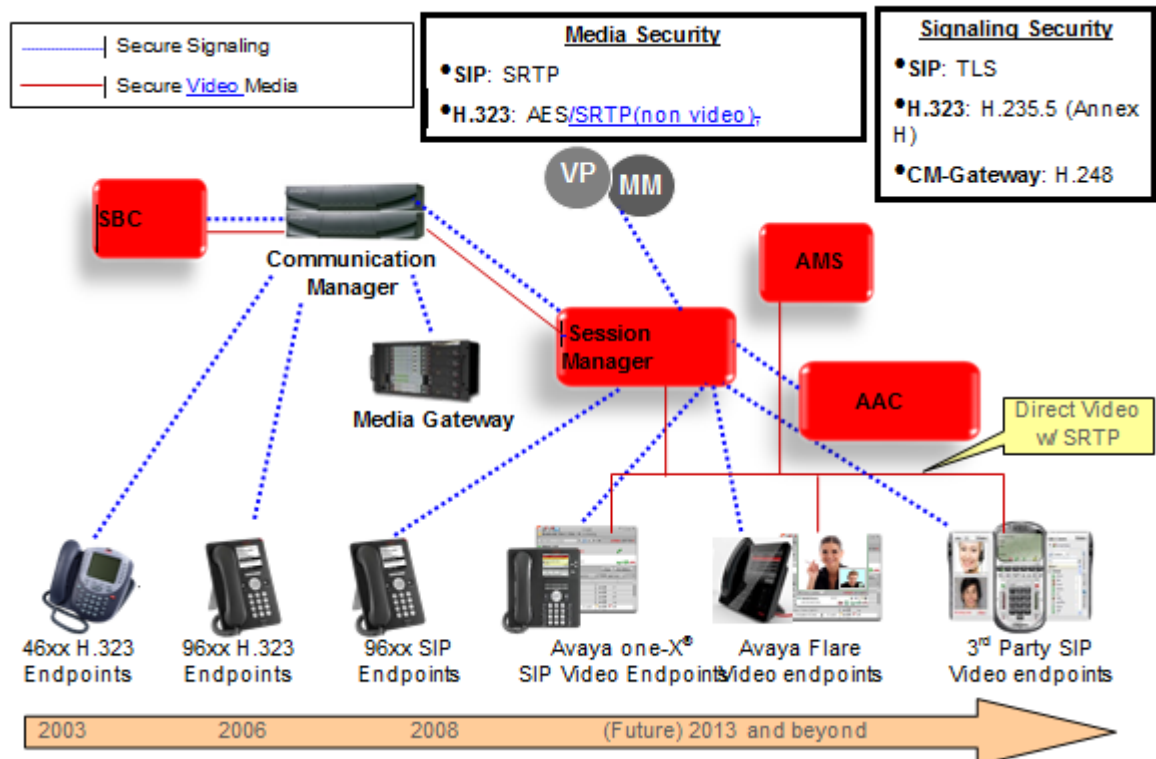
The generation of UCID by Avaya Aura[®] Session Border Controller does not impact Avaya Aura[®] Call Center Elite. In this scenario, contact center application receives a unique identifier of the call from Avaya Aura[®] Communication Manager. SBC generates a UCID for all incoming SIP calls and ACM reuses the same UCID. No conflict of UCID occurs among ACM, SBC, and Contact Center Applications. In case of features like call holding, an association is maintained between the new UCID and parent UCID by ACM.

Call recording

One of the main uses of the UCID feature is call recording in contact centers. UCID generated by SBC is notified to AACC or CC Elite which then sends the UCID to Call Recorder and reports events on agent. Call recorder sends a single step conference to ACM. ACM shuffles the call to a media gateway and sends a mixed send only stream to call recorder.

Support for Video SRTP

Avaya Aura[®] Communication Manager supports SRTP for video when appropriate settings are enabled in the system parameter features table. The enabling of SRTP for video in a SIP-to-SIP call is based on the policy set in the ip-codec-set table. The cryptosuite filtering based on ip-codec-set rules do not apply to video media stream, and the ip-codec-set rules only enable the SRTP policy for video media stream.



Supported user cases

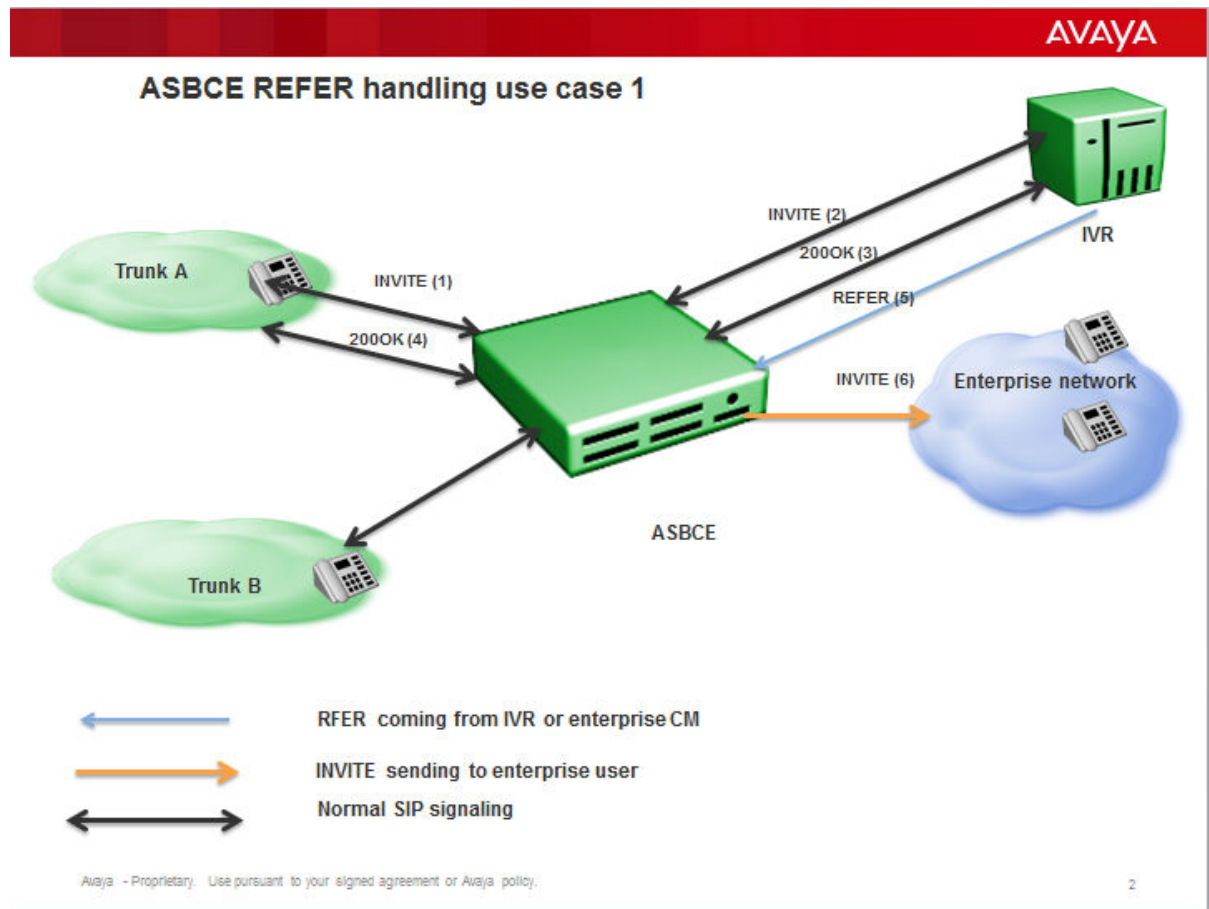
- **(Desktop Users) – Avaya SIP Video Endpoint (e.g. 1XC) to 1XC SRTP encrypted SIP video call** : Enabling video calls between two video-enabled IntereXchange carrier SIP endpoints. All the standard telephony and video features such as mute, transfer, and hold can be used.
- **(Mixed) SIP SRTP video call between 1XC and third party (SIP) video endpoint**: Third-party devices can be registered to the URE as with 1XC. However, PPM configuration, user or station profile, will be unavailable to those devices. Third— party SIP endpoints might include video conference hardware. It also includes SRTP-capable video endpoints calling non-SRTP video endpoint and vice versa.
- **(Third Party) SIP video call between third party (SIP) video endpoints**

REFER Handling

When REFER handling is enabled, SBC translates the incoming SIP request to a SIP INVITE request based on the Request URI Group selected. REFER message comes from enterprise like Communication Manager, or IVR and SBCE handles that REFER going towards trunk server based on the trunk server interworking profile configuration. Following are three use cases for REFER handling.

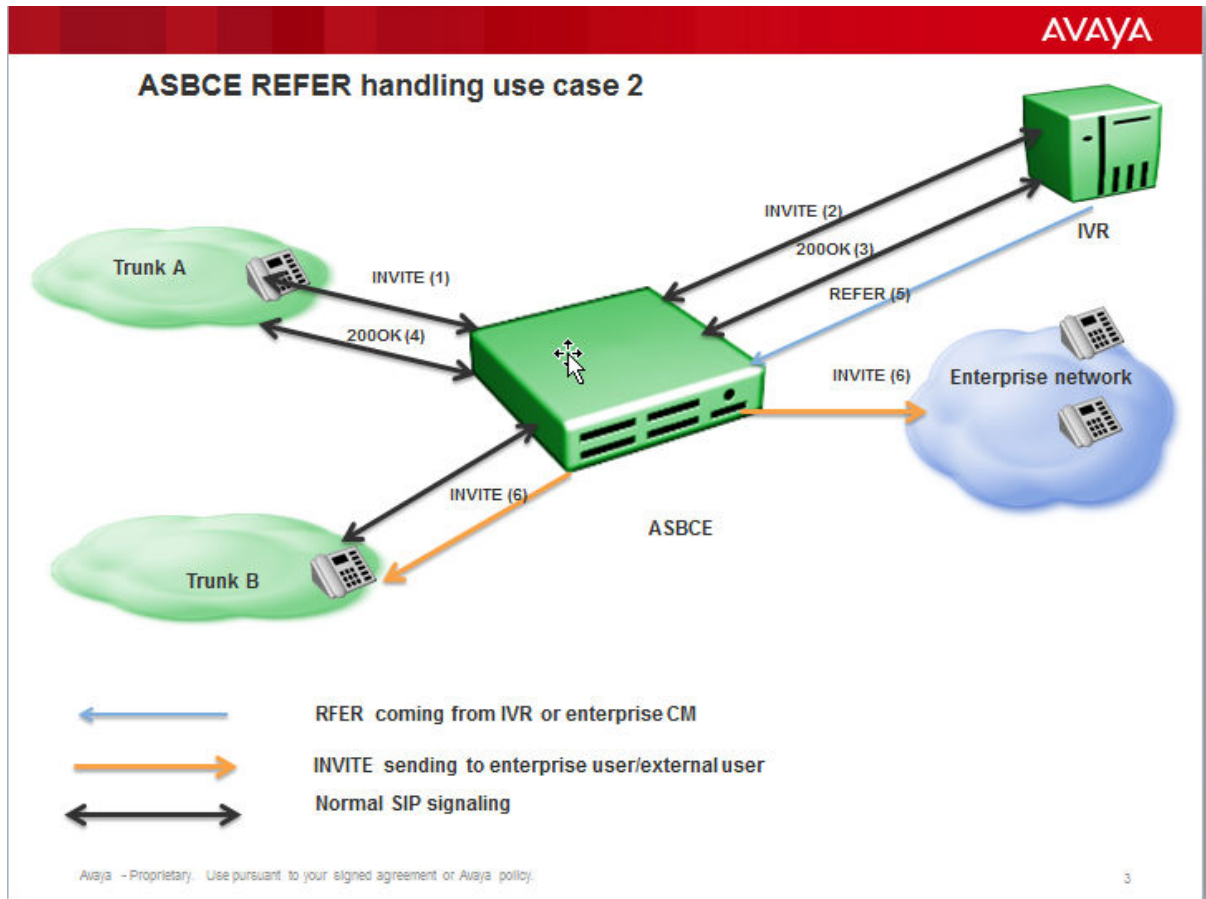
Use case 1

ASBCE consumes REFER message and routing INVITE towards enterprise user.



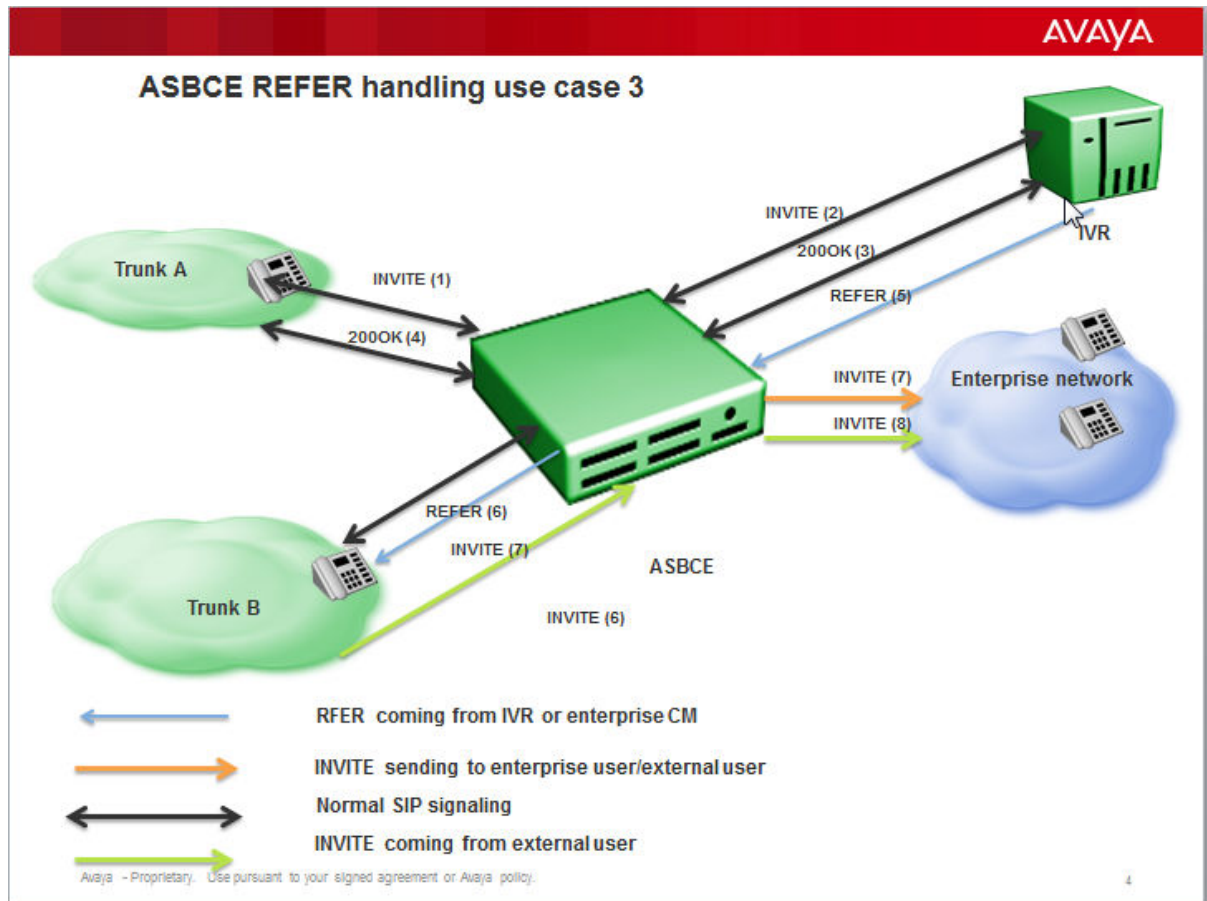
Use case 2

ASBCE consumes REFER and sending INVITE towards trunk user/enterprise user based on routing profiles created to route the new INVITE. INVITE created from REFER is routed using URI based routing. Need to create routing entries in the trunk server routing profile to route the request to external trunk as default is routed back to enterprise server. In aura AST2 transfer mode, ASBCE should always route the new INVITE towards the enterprise server as ASBCE will not find the dialog to replace.



Use case 3

ASBCE consumes some REFER messages based on configured URI group under refer handling configuration. In this case some REFER messages are relayed to the external trunk based on URI group configuration. External trunks generate new INVITE to towards the target users.



Multi Device Access

With the Multi Device Access (MDA) feature a user can access calls on multiple devices of various capabilities, but using the same number. All devices of the user will ring for an incoming call, and the user can answer with the chosen device or a paired mobile device. After the call is answered, the remaining devices stop ringing. If the user wants to use a device with better capability it is joined with the existing call using that device. Hence a conference is created on ACM and the user can manually disconnect the previous device. This procedure is known as a handoff. In case of an AAC— hosted conference, the last MDA device to join the call remains active and all earlier devices are dropped.

Solution Overview

The Multi Device Access feature consists of the same user and extension using the same AOR to register multiple devices to Session Manager. In the current implementation, all the registered devices ring simultaneously and the device on which the user takes the call becomes a device with the active call. Other paired MDA devices receive notification of the active call and dialog information. Those devices can join the call using this dialog information. The

display shows a two-party call, and not a conference. Only one active MDA call is maintained in case of a call involving AAC.

Reinvite handling

Some customers and service providers do not want reinvites to be passed on to the SIP trunk. When reinvites are turned on which have no change in Session Description Protocol, known as Session Refresh Invites, they are blocked by SBC. The same applies for any Hold or Resume invite which has no change in SDP except port, IP and SDP attributes like send rcv, send only, and rcv only.

New in this release

This release adds support for:

- Avaya Access Secure Gateway
- REFER handling
- Reinvite feature
- UCID

Chapter 3: Interoperability

Product compatibility

For the latest and most accurate compatibility information go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

Avaya SBCE supported servers

Server ¹	Processors	System Memory	On-board Storage
Dell R210 II XL (core)	Intel Xeon E3-1220 3.10 GHz Quad Core/4T	4 GB (DDR3 1333MHz)	500 GB (3.5-in SATA 3Gb/s – 7.2K)
Dell R210 II (core)	Intel Xeon E3-1230 3.20 GHz Quad Core/4T	4 GB (DDR3 1333MHz)	500 GB (3.5-in SATA 3Gb/s – 7.2K)
Dell R210 II XL (EMS)	Intel Pentium G850 2.90 GHz – Dual Core/2T	2 GB (DDR3 1333MHz)	2 x 500 GB (3.5-in SATA 3Gb/s – 7.2K)
AMAX (EMS)	Intel Core 2 Duo E6400 2.13 GHz – Dual Core	2 GB (DDR2 667MHz)	2 x 160 GB (3.5-in SATA 3Gb/s – 7.2K)
Portwell CAD-0208 (core)	Intel® Atom D510 1.66GHz - Dual Core	2GB (SO-DIMM DDR2 667MHz)	320GB (2.5-in SATA 3Gb/s – 7.2K)

Avaya products

SIP Trunking

The following products are compatible with Avaya Session Border Controller for Enterprise Release 6.2 for SIP Trunking.

¹ The Dell R210 II XL and Portwell CAD-0208 are the only servers that are available for new installations.

Product	Release
Avaya Aura® Communication Manager	Release 5.2.1 or later
Avaya Aura® Presence Services	Release 6.1.5 or later
Avaya Aura® Session Manager	Release 6.1 or later
Avaya Communication Server 1000	Release 7.5
IP Office	Release 8.1 Release 8.1 FP 1

Mobile Workspace User (Remote Worker)

The following products are compatible with Avaya Session Border Controller for Enterprise Release 6.2 for Mobile Workspace User.

Product	Release
96x1 Deskphones	Supports Mobile Workspace User with Avaya Aura Release 6.2 or later
9608 Deskphone	Supports Mobile Workspace User with Avaya Aura Release 6.2 or later
Avaya one-X® Communicator	Supports Mobile Workspace User with Avaya Aura Release 6.2 or later Video is not supported
Avaya one-X® Mobile SIP iOS	Supports Mobile Workspace User with Avaya Aura Release 6.2 or later
Avaya Communicator for iPad	Supports Mobile Workspace User with Avaya Aura Release 6.2 or later
Avaya Communicator for PC	Supports Mobile Workspace User with Avaya Aura Release 6.2 or later

Third-party product requirements

External SAL gateway

When Secure Access Link (SAL) is used for Avaya services remote access to the Avaya SBCE, the customer must provide a SAL gateway. The SAL gateway can be purchased from Avaya, or it can be provided by the customer if the server complies with the SAL requirements specified on the Avaya Support website at <http://support.avaya.com>. In some cases, a System Platform integrated SAL Gateway can be used in lieu of purchasing an additional server. See Product Support Notice [PSN003058u](#).

Operating system compatibility

- The Avaya SBCE uses MontaVista Linux 5.1 on all platforms
- The EMS uses MontaVista Linux 5.1 on all Dell platforms
- The EMS uses a customized version of Debian Linux on the AMAX server platform

Chapter 4: Performance specifications

Capacity and scalability specification

	Trunk Deployment			Remote worker Deployment		
	Concurrent Sessions in Trunk Deployment (unencrypted)	Concurrent Sessions in Trunk Deployment (encrypted)	CPS	Concurrent Sessions in Remote User Deployment (unencrypted)	Concurrent Sessions in Remote User Deployment (encrypted)	CPS
Dell R210II XL & DELL R210 II	5000	1000	60	2000	1000	20
HP DL360	750	375	12	NA	NA	NA
Micro	500	250	6	500	250	6

The capacity specifications are based on:

- Codec specification – G711 codec with 20ms packetization time, and all sessions are audio sessions.
- Call Model – The call model used to establish the above numbers is the SIP RFC call model in trunk mode.
- Avaya SBCE Configuration – Default logging levels are used, and security features are turned off. CPS measurements are based on 80~ sec hold time. This varies based on the hold time.

Redundancy and high availability

Available with EMS and Dell R210 II XL platform only.

High-Availability (HA) support for both media and signaling ensures Avaya SBCE security functionality is provided continuously, regardless of any hardware or software failures. High

availability requires a minimum of two Avaya SBCE devices and one standalone EMS server.

 Note:

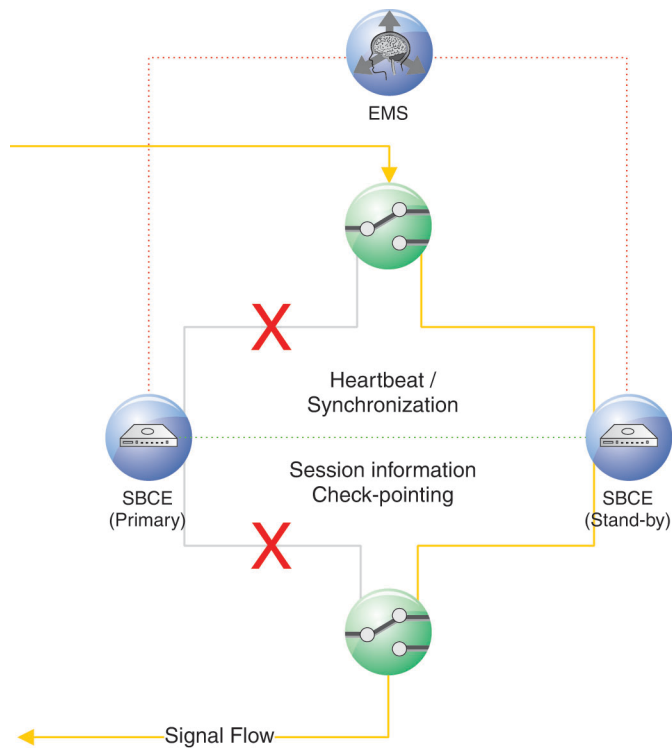
High availability requires GARP support on the connected network elements. In cases like Avaya Medpro and certain Cisco endpoints, which do not support GARP, it is necessary to introduce a GARP aware router/switch between these elements and the Avaya SBCE for it to handle GARP packets sent from the Avaya SBCE.

Avaya SBCE high availability

The Avaya SBCE can be deployed as a pair either in the enterprise DMZ or core, or geographically dispersed, where each Avaya SBCE resides in a separate, physical facility.

In either configuration, Avaya SBCE HA pairs can be deployed in an enterprise in a parallel mode configuration. In the parallel configuration the signaling packets are routed only to the Active (primary) Avaya SBCE, which performs all data processing. The interface ports on the standby Avaya SBCE do not process any traffic. The Management interfaces on the Avaya SBCE appliances have different IP addresses, but the signaling/media interfaces have the same IP address. Upon failover, the standby Avaya SBCE advertises its new MAC as the L2 address for the common IP address. The Avaya SBCE devices are synchronized via the heartbeat on the dedicated interfaces, and both Avaya SBCE devices are in continuous communication with the Avaya EMS.

When a failure is detected on the Active Avaya SBCE by the Avaya EMS, the active SBC network interface ports are automatically disabled while those of the standby SBC are enabled. Failure detection and operational transfer occur without dropping packets or adding any significant amount of latency into the data paths. The EMS reports the change in status to the Avaya SBCE Control Center for action by the system administrator.



cysbtplc LAO 021413

Figure 8: Typical Avaya SBCE HA – Parallel Mode Topology (collocated)

EMS replication

EMS replication gives an enterprise the option of deploying two Avaya EMS servers to ensure uninterrupted network monitoring and control. EMS data is replicated between the servers iteratively as determined by user-defined fields on the EMS GUI interface. These servers can either be located in the same facility or geographically separated.

When one EMS fails, transition to the alternate server is not automatic. The “takeover” requires manual intervention by the administrator. For more information, see *Administering Avaya Session Border Controller for Enterprise*.

Chapter 5: Environmental requirements

Altitude and air pressure requirements

Dell R210 II XL altitude ranges

	Operating altitude	Non-operating altitude
Low limit	-50 ft (-15.2 m)	-50 ft (-15.2 m)
High limit	10,000 ft (3048 m)	35,000 ft (10,668 m)

Hardware dimensions and clearance requirements

	Height	Width	Depth	Weight
Dell R210 II XL (Core)	1.7 in. (4.32 cm)	17.10 in. (43.45 cm)	15.50 in. (39.37 cm)	15.5 lbs. (7.03 kg)
Dell R210 II (Core)	1.7 in. (4.32 cm)	17.10 in. (43.45 cm)	15.50 in. (39.37 cm)	15.5 lbs. (7.03 kg)
Dell R210 II XL (EMS)	1.7 in. (4.32 cm)	17.10 in. (43.45 cm)	15.50 in. (39.37 cm)	15.5 lbs. (7.03 kg)
AMAX (EMS)	1.7 in. (4.32 cm)	17.1 in. (43.45 cm)	15.50 in. (39.37 cm)	15.5 lbs. (7.03 kg)
Portwell CAD-0208 (core)	1.65 in. (4.20 cm)	7.10 in. (1.80 cm)	5.90 in. (1.50 cm)	15.5 lbs. (7.03 kg)

Temperature and humidity requirements

	Operating Temperature ²	Storage Temperature	Relative Humidity
Dell R210 II XL (core)	50 °F to 95 °F (10 °C to 35 °C)	-40 °F to 149 °F (-40 °C to 65 °C)	20% to 90%, non-condensing
Dell R210 II (core)	50 °F to 95 °F (10 °C to 35 °C)	-40 °F to 149 °F (-40 °C to 65 °C)	20% to 90%, non-condensing
Dell R210 II XL (EMS)	50 °F to 95 °F (10 °C to 35 °C)	-40 °F to 149 °F (-40 °C to 65 °C)	20% to 90%, non-condensing
AMAX (EMS)	50 °F to 95 °F (10 °C to 35 °C)	-40 °F to 158 °F (-40 °C to 70 °C)	8% to 90%, non-condensing
Portwell CAD-0208 (core)	41 °F to 95 °F (5 °C to 35 °C)	32 °F to 158 °F (0 °C to 70 °C)	20% to 90%, non-condensing

Power requirements

	Input	Nominal (110V)	AC Power Max
Dell R210 II XL (core)	AC 110V — 240V auto switch	2A	250 Watts
Dell R210 II (core)	AC 110V — 240V auto switch	2A	250 Watts
Dell R210 II XL (EMS)	AC 110V — 240V auto switch	2A	250 Watts
AMAX (EMS)	AC 110V — 240V auto switch	2A	250 Watts
Portwell CAD-0208 (core)	AC 110V — 240V auto switch	2A	60 Watt Power Adapter

² For altitudes greater than 900 m or 2,952 ft, see your Dell documentation for operating temperature ranges.

Physical system protection requirements

The server is equipped with air vents on either side of the equipment chassis, and exhaust vents on the back. Be sure to follow these guidelines:

- Do not block these air vents.
- Do not place the server in a location where dirt or dust might clog the air vents or enter the chassis and damage internal components.
- Do not install the device in or near a source of heat (i.e. proximate high-current or high-power consuming equipment such as switch banks); excessive heat might cause the server to overheat and fail.

 Note:

It is the customer's responsibility to ensure that no environmental hazards (i.e. excessive heat, excessive humidity, or improper ventilation) or electromagnetic interference from proximate equipment interfere with the operation of the Avaya SBCE server.

Regulatory standards

Avaya SBCE servers conform to the following standards.

Server	Certifications
Dell R210 II XL (core)	CSA, FCC, UL, RoHS
Dell R210 II (core)	CSA, FCC, UL, RoHS
Dell R210 II XL (EMS)	CSA, FCC, UL, RoHS
AMAX (EMS)	• USA – UL listed, FCC • Canada – CUL listed • Europe – CE Mark • EN 60950/IEC 60950-compliant
Portwell CAD-0208 (core)	CE, FCC, UL

Chapter 6: Security

Security specification

Unified communications intrusion protection

Unlike traditional intrusion prevention systems (IPS), which monitor network traffic to gather and analyze information from various parts of that network to identify possible security breaches for subsequent prevention or mitigation, Avaya SBCE security products not only detect any anomalous event – including day zero attacks – but also prevent virtually any type of intrusion (attack from outside the enterprise) and misuse (attack from within the enterprise). This is due to the unparalleled flexibility and fine-grain tuning allowed when network security administrators establish Unified Communications rule sets. The Avaya SBCE IPS security feature includes:

- **Flood and Fuzzing Protection** – Protection from volume-based Denial-of-Service (DoS) and malformed message ('fuzzed') attacks. Customized protocol scrubbing rules detect and remove malformed messages that might crash call servers or other critical network components, or make other portions of the communications infrastructure vulnerable because of degraded performance of critical Unified Communications systems components (such as servers and endpoints).
- **Media Anomaly Prevention** – Selectively enables the media traffic and enforces rules on the type of traffic carried, based on the negotiated signaling and other configured policies (for example prevent video or prevent modem/FAX).
- **Spoofing Prevention** – Various validation techniques are applied to detect and prevent spoofing, including the use of end-point 'fingerprints' for different message fields to trigger other validations and verifications.
- **Stealth Attack Prevention** – Based on the learned call behavior patterns of subscriber endpoints, Avaya SBCE security products can detect any nuisance and annoying calls to a

particular destination or user and selectively block only those subscribers from whom those calls originate.

- **Reconnaissance Prevention** – Avaya SBCE security products detect and block application layer scan reports and block the attackers that originate them.

Attack protection

To ensure the integrity of all real-time IP applications, Avaya SBCE security products maintain the highest level of communications network security, reliability, and availability by performing these three critical functions: monitoring, detection, and protection.

Monitoring

Each Avaya SBCE provides complete network security monitoring and management capabilities that encompass each aspect of the UC network, including all endpoints, media gateways, call servers, voice mail (VM) and applications servers. In addition, its monitoring and management capabilities provide a cascaded, multi-layered detection, mitigation, and reporting system that provides real-time information based upon user-definable event thresholds. This system supports a detailed graphical user interface (GUI) called the SBC Control Center. The Control Center can be installed on and run from any Avaya SBCE security device or it can be installed on a separate server platform and used as a stand-alone Element Management System (EMS) that monitors and coordinates the security activities of all Avaya SBCE security devices installed in a network.

Note:

Both the EMS and Avaya SBCE can be installed in one box. However, as your network grows and you require more than one Avaya SBCE, at that time it is recommended that your EMS be installed on a dedicated platform.

Detection

The detection capability of the Avaya SBCE solution uses a host of dynamic and adaptive algorithms to detect any anomalies in the learned caller behavior that are based upon user-definable Time-of-Day (ToD) and Day-of-Week (DoW) criteria. These are flexible enough to accommodate special circumstances such as weekends, holidays, and other user-specified time periods. Complementing these features is the ability to learn and apply dynamic trust scores, starting from an unknown score and either increasing or decreasing to different levels depending upon the caller's behavior pattern (Trusted, Known, Unknown, Suspected, or Spammer), as well as called party feedback (Black List and White List), further enhancing the time-critical ability to detect anomalous behavior.

The detection capability is also able to collect and correlate multiple events and activities from different nodes and end-points in the network to accurately detect attacks which otherwise

might have escaped unnoticed if reported only by a single point in the network. The detection capability can inspect the sequence and content of messages to detect protocol anomalies and any instances of end-point scanning. Finally, the detection capability of the Avaya SBCE solution can validate the source of a suspected malicious call or attack by implementing a unique detection technique that is based upon learned caller fingerprints.

This ability of Avaya SBCE security products to continuously learn call patterns and end-point fingerprints, in addition to being able to constantly analyze raw event data based upon specific user-definable criteria and take automatic action, gives them the unique characteristic of being able to evolve and adapt on their own to effectively counter any new or existing threat.

Protection

The Avaya SBCE provides complete network protection by blocking attacks while at the same time allowing legitimate calls to pass through unimpeded. This exceptional level of protection can be extended either to an individual end-point, a specific group of end-points, or to all the assets in the network based upon highly flexible user-defined rule sets called Unified Communications Policies. These policies can be implemented to precisely discriminate or normalize (aggregate) any incoming or outgoing signaling or multimedia traffic. Thus all IP communication devices (i.e. hard-phones, soft-phones, WiFi phones, and smart phones), call servers, voice mail servers, media servers, media gateways and application servers are protected, effectively securing the entire network from all types of attack.

Avaya SBCE hardening

System level Layer 3/Layer 4 security features include IPTable firewall rules to provide restrictions on INBOUND traffic (effective after content filtering processing for data traffic) to protect the Avaya SBCE from IP/ICMP/TCP level attacks.

OUTBOUND traffic is not restricted.

Protection against layer 3 and layer 4 floods and port scans

ICMP flood prevention

When an ICMP flood from a host is detected, all further requests from that host are blocked for a specified period of time.

Port scan blocking

When a port scan from a host is detected, all further requests from that host are blocked for a specified period of time.

Data interface restrictions

- General protection is provided on all data interfaces.
- TCP signaling level flooding control rules are applied dynamically on application-specified listening IP and listening port.

TCP signaling level flood control

Only a specified number of requests are allowed in a specified time period for each of the following request types:

- TCP SYN
- FIN
- RST

System-wide security settings

System-wide security settings are supported across the entire Avaya product line.

The Avaya SBCE has the following protection types:

- General Protection
- Management Interface Restrictions
- Data Interface Restrictions

For all products, the management interface is dynamically detected from the system configuration.

For Avaya SBCE, there are no restrictions on the internal Ethernet interface (**ethint**) and external Ethernet M1 interface (**ethext**) on the (**Com Express**) co-processor board in the Avaya SBCE box.

To enable Avaya SBCE HA, TCP 1950 ports are allowed bi-directionally on the data interface.

Avaya SBCE HA does not require any extra rules to enable HA traffic.

Application control

The script `protect_socket.sh` takes care of installing rules for data interfaces on demand. It is available from Avaya Customer Support.

Usage: `./protect_socket.sh <IU> <add|del> <scheme> <ip addr> <portnum>`

 Note:

Scheme 0: TCP signaling level flood control

Scheme 1: Additional bandwidth limiting (still experimental – to be applied only on non-signaling ports)

Installation security

On installing the application debian package, rules get added/updated for that version. After reboot, ICU invokes the appropriate rules script for that platform.

DoS security features

The Denial of Service (DoS) security feature of the Avaya SBCE Control Center allows you to view and edit a wide variety of DoS and Distributed Denial-of-Service (DDoS) attack response and control parameters that can then be applied either to individual SIP endpoints or their parent domain. Additionally, the Avaya SBCE supports DoS activity reporting for certain time periods. The server DoS feature and the Domain DoS features are further classified based on traffic types like Remote Worker, Trunk and Remote Worker, and Trunk. The following rules describe the input methods:

- In case of Remote Worker the input is taken from 'Number of remote workers' and 'Max Concurrent Sessions'
- In case of Trunk the input is taken from 'Max Concurrent Sessions'
- In case of Remote Worker and Trunk the input is taken from 'Number of remote workers' and 'Max Concurrent Sessions'

Rules for setting threshold values for different types of traffic:

- Server DoS is applicable for initiated thresholds. Initiated threshold is applicable for any SIP request routed to the server irrespective of any response received or not
- In calculation of all threshold values, 10% of actual value is considered.

- Server DoS can also be applicable for remote worker traffic in case of pending threshold value. Pending threshold means SIP Request for which no corresponding response has come from the server.
- Server DoS feature is also applicable in case of failed threshold value. Failed threshold implies that failure request has come for a SIP request other than 401 and 407.

List of recommended threshold values:

- Recommended threshold value for Single Source DoS feature for remote worker deployment is 300 messages.
- Recommended threshold value for trunk is 15 messages.
- The default threshold value for Avaya remote worker in case of phone DoS is 200 messages.
- The recommended threshold value for Call Walking in case of remote worker deployment: INVITE – 10 messages, Registration – 5 messages, and All – 20 messages.

Protocol scrubber

Protocol scrubbing uses a 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 that violate the security rules dictated by the scrubber templates are dropped while those that violate syntax rules are repaired (rewritten, truncated, rejected, or dropped depending on the processing rules imposed by the templates). Protocol scrubbing rule templates are prepared by Avaya and can only be minimally edited by the user.

Protocol scrubbing for SIP allows you to install a scrubber rules package, enable or disable the scrubber rules contained in the package, and delete the package from the system. In addition, you can view a list of all currently installed scrubber rules.

Topology hiding

Topology hiding allows you to change certain key SIP message parameters to hide or mask how your enterprise network may appear to an unauthorized or malicious user.

Firewall rules

Firewall rules protect the Avaya SBCE, its communications and signaling. They are hard-coded and not configurable. Firewall rules can be divided into the following categories:

- Common rules
- Management rules
- Data interface rules

Common rules

Common rules are applied to all interfaces. They are divided into the following categories:

- ICMP restrictions
- Portscan detection
- KILLSCAN rules

ICMP restrictions

1. Always accept ICMP ping replies.
2. Any IP address sending an ICMP ping request will be added to the "pingflood" list.
3. For any IP in the "pingflood" list that sends an ICMP ping request, drop its request if that IP has sent five ping requests in one second.
4. Accept all other ICMP ping requests.
5. ICMP redirect datagrams for the network are rate-limited to one per second.
6. ICMP redirect datagrams for the host are rate-limited to one per second.
7. ICMP destination unreachable messages are rate-limited to one per second.
8. ICMP time exceeded messages are rate-limited to one per second.
9. ICMP bad IP header messages are rate-limited to one per second.
10. Drop all other ICMP packets.

Portscan detection

1. Follow KILLSCAN rules.
2. Accept all packets with INVALID state.

KILLSCAN rules

1. Remove the current IP from the "portscan" list.
2. Any IP address sending packets with FIN, PSH, and URG flags set but no SYN, RST, or ACK flags is added to the "portscan" list.
3. Any IP address sending packets with SYN and RST flags set is added to the "portscan" list.
4. Any IP address sending packets with FIN and SYN flags set is added to the "portscan" list.
5. Any IP address sending packets with FIN flags set but no SYN, RST, PSH, ACK, or URG flags is added to the "portscan" list.

6. Any IP address sending packets with FIN, SYN, RST, PSH, ACK, and URG flags set is added to the "portscan" list.
7. Any IP address sending packets without any FIN, SYN, RST, PSH, ACK, or URG flags set is added to the "portscan" list.
8. Any IP address sending packets with FIN, SYN, RST, PSH, ACK, and URG flags set is added to the "portscan" list.
9. Drop all packets from any IP in the "portscan" list.

Management and MGMTPROTECT rules

Management rules are applied only to management interfaces. The first step in the management rules is to follow the MGMTPROTECT rules, which can be divided into the following categories:

- TCP flood restrictions
- SSH rules
- HTTPS rules
- DNS rules
- Syslog rules
- OpenVPN rules

Management rules

1. Follow MGMTPROTECT rules.
2. Accept all packets in RELATED or ESTABLISHED state.
3. Accept all packets on TCP port 222.
4. Accept all packets on TCP port 443.
5. Accept all packets on TCP port 53.
6. Accept all packets on UDP port 53.
7. Accept all packets on TCP port 514.
8. Accept all packets on UDP port 514.
9. Accept all packets on UDP port 123.
10. Drop everything else.

TCP flood restrictions (all ports)

1. Any IP address sending packets with FIN flags set but no SYN, RST, PSH, ACK, or URG flags is added to the "finrstlim" list.
2. Any IP address sending packets with RST flags set but no FIN, SYN, PSH, ACK, or URG flags is added to the "finrstlim" list.
3. For any IP address in the "finrstlim" list that sends ten packets in one second, drop its packet.

SSH rules

1. Any IP address sending, on port 222, packets with the SYN flag but not RST or ACK is added to the "sshsyn" list.
2. For any IP address in the "sshsyn" list that sends, on port 222, fifteen packets with the SYN flag but not RST or ACK in one minute during the TTL of the previous such packet sent, drop its packet.
3. For any IP address in the "sshsyn" list that sends, on port 222, ten packets with the SYN flag but not RST or ACK in thirty seconds during the TTL of the previous such packet sent, reject its packet with ICMP port unreachable message.

HTTPS rules

1. Any IP address sending, on port 443, packets with the SYN flag but not RST or ACK is added to the "httpssyn" list.
2. For any IP address in the "httpssyn" list that sends, on port 443, ten packets with the SYN flag but not RST or ACK in one second during the TTL of the previous such packet sent, drop its packet.
3. For any IP address in the "httpssyn" list that sends, on port 443, five packets with the SYN flag but not RST or ACK in one second during the TTL of the previous such packet sent, reject its packet with ICMP port unreachable message.

DNS rules

1. Any IP address sending, on TCP port 53, packets with the SYN flag but not RST or ACK is added to the "dnssyn" list.
2. For any IP address in the "dnssyn" list that sends, on TCP port 53, ten packets with the SYN flag but not RST or ACK in one second during the TTL of the previous such packet sent, drop its packet.
3. For any IP address in the "dnssyn" list that sends, on TCP port 53, five packets with the SYN flag but not RST or ACK in one second during the TTL of the previous such packet sent, reject its packet with ICMP port unreachable message.

Syslog rules

1. Any IP address sending, on TCP port 514, packets with the SYN flag but not RST or ACK is added to the "slogsyn" list.
2. For any IP address in the "slogsyn" list that sends, on TCP port 514, ten packets with the SYN flag but not RST or ACK in one second during the TTL of the previous such packet sent, drop its packet.
3. For any IP address in the "slogsyn" list that sends, on TCP port 514, five packets with the SYN flag but not RST or ACK in one second during the TTL of the previous such packet sent, reject its packet with ICMP port unreachable message.

OpenVPN rules

1. Any IP address sending, on TCP port 1194, packets with the SYN flag but not RST or ACK is added to the "ovpnyn" list.
2. For any IP address in the "ovpnyn" list that sends, on TCP port 1194, ten packets with the SYN flag but not RST or ACK in one second during the TTL of the previous such packet sent, drop its packet.
3. For any IP address in the "ovpnyn" list that sends, on TCP port 1194, five packets with the SYN flag but not RST or ACK in one second during the TTL of the previous such packet sent, reject its packet with ICMP port unreachable message.

Data interface rules

Data interface rules are applied only to data interfaces. The default DATAIFPROTECT rules are all commented out, though additional DATAIFPROTECT rules are dynamically generated by the protect-socket command.

1. Follow DATAIFPROTECT rules.
2. Accept all packets.

Protect-socket command

The protect-socket command takes a hardware type (1U), "add" or "del", a protection scheme (a number), an IP address to protect, and a port to protect. From these, it generates a set of firewall rules to protect that IP and port, all added to the DATAIFPROTECT rule list.

1. Any IP address sending a packet to the specified IP and port with the SYN flag but not RST or ACK is added to the "apprules" list.
2. For any IP address in the "apprules" list that sends ten packets with the SYN flag but not RST or ACK to the specified IP and port in one second during the TTL of the previous such packet sent, drop its packet.
3. For any IP address in the "apprules" list that sends five packets with the SYN flag but not RST or ACK to the specified IP and port in one second during the TTL of the previous such packet sent, reject its packet with ICMP port unreachable message.

4. If the protection scheme is given as “1”, also follow these rules:
 - For any IP address that sends twenty packets in state ESTABLISHED to the specified IP and port in one second, drop its packet.
 - Keep a record of any IP address that sends a packet in state ESTABLISHED to the specified IP and port.
 - For any IP address that sends three packets in state NEW to the specified IP and port in one second, drop its packet.
 - Keep a record of any IP address that sends a packet in state NEW to the specified IP and port.
5. Delete any existing rule for accepting packets.
6. Accept all packets.

Port utilization specification

Management interface port restrictions

Only selected ports are allowed on the management interface, and all other TCP/UDP traffic is blocked on the management interface.

Internal – Between one or more SBCs and the EMS

1. SSH TCP-222
2. HTTPS TCP-443
3. OpenVPN UDP-1194
4. Syslog TCP/UDP-514
5. NTP UDP-123

External – Between the EMS and SBCs and an external device

1. SSH TCP-222
2. HTTPS TCP-443
3. Syslog TCP/UDP-514
4. NTP UDP-123
5. DNS TCP/UDP-53 (for DNS and the signaling and media ports)
6. SNMP (Ver. 2 / 3) UDP-161 + 162 The SNMP agent receives requests on UDP port 161, and the SNMP manager receives notifications (Traps and InformRequests) on port 162.

TCP packets

Only a specified number of TCP packets are allowed from a host within a specified time frame, irrespective of TCP ports.

SSH port

The following rules apply to the SSH port:

- Only a specified number of connections from a host are allowed within a specified time frame.
- Only a specified number of connection requests are responded with ICMP-unreachable
- Further connection requests are dropped until new connection requests stop for a specified period of time.

Additional port assignments

DNS server

If your DNS server is not in the DMZ, open UDP port 53 on the SBCs via the EMS GUI so the SBCs can access the DNS server.

SNMP

If you have your own SNMP, open the SNMP UDP ports 161 and 162 on the SBCs via the EMS GUI so the SBCs can access the SNMP from the DMZ.

Syslog

If you have your own Syslog, open the Syslog UDP port 514 on the SBCs via the EMS GUI so the SBCs can access the Syslog from the DMZ.

Media ports

The default media port range is 35000 to 40000, but other media port ranges can be configured, if a different media port range is required.

SIP signaling ports

The ports listed below are defaults. Other ports may be configured.

1. TCP/UDP 5060
2. TLS 5061

HTTP/HTTPS ports

These ports are used for Personal Profile Management (PPM) communications and configuration files and firmware downloads. Configure these ports on the SBCs via the EMS

GUI so the phones can login and download configuration files from the Avaya HTTP server or HTTPS server.

1. HTTP port 8080 or port 80
2. HTTPS port 443

LDAP/LDAPS ports

1. LDAP port 389
2. LDAPS port 636

Chapter 7: Licensing requirements

Avaya Session Border Controller for Enterprise uses the Avaya Product Licensing and Delivery System (PLDS) to create release 6.2 licenses and download Avaya SBCE software. The license file generated by PLDS is downloaded to the EMS. PLDS is not integrated with WebLM. Use PLDS to perform operations such as license activations, license upgrades, license moves and software downloads.

There are two licensed versions of Avaya SBCE:

- Standard Services delivers secure SIP trunking
- Advanced Services adds Mobile Workspace User, Signaling Forking, Media Replication and other features to the Standard Services offer.

Avaya Aura[®] Mobility Suite and Collaboration Suite licenses include Avaya Session Border Controller for Enterprise.

Glossary

ARP	Address Resolution Protocol
Codec	Coder/Decoder
Day Zero Attack	See <i>Zero-Day Attack</i> .
DDoS	Distributed Denial-of-Service
Demilitarized Zone (DMZ)	A computer network-related term that refers to the “neutral zone” between an enterprise’s private network and outside public network. Typically, a computer host or small network is inserted into this neutral zone to prevent outside users from getting direct access to the internal network.
Denial-of-Service (DoS)	The objective or end-result of certain types of malicious attacks or other activities against a network, where access to network services, resources, or endpoints is prohibited.
Digest Authentication (DA)	A Hypertext Transport Protocol (HTTP) authentication scheme whereby user passwords are encrypted prior to being sent across the Internet, thus certifying the integrity of the Uniform Resource Locator (URL) data. The downside of DA is that although passwords are encrypted, the data being exchanged is not; it is sent in the clear.
Distributed Denial-of-Service (DDoS)	A more sophisticated type of DoS attack where a common vulnerability is exploited to first penetrate widely dispersed systems or individual endpoints, and then use those systems to launch a coordinated attack. Much more difficult to detect than simple DoS attacks.
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DoW	Day-of-Week
EMS	Element Management System
FW	Firewall
GARP	Gratuitous Address Resolution Protocol
GUI	Graphical User Interface
HA	High-Availability or Harvest Attack

High-Availability	The SBCE feature that allows two SBCE security devices to be deployed as an integral pair, wherein one of the devices functions as the Primary and the other as an Alternate or Standby. Connected by a heartbeat signal and shared database, the two SBCE security devices provide failover protection in the event one of the devices malfunctions.
ICMP	Internet Control Message Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IM	Instant Messaging
Intrusion	A malicious user or process deliberately masquerading as a legitimate user or process.
IP	Internet Protocol
IPS	Intrusion Protection System
ITSP	Internet Telephony Service Provider
Latency	The amount of time it takes for a packet to cross a network connection, from sender to receiver. Also, the amount of time a packet is held by a network device (firewall, router, etc.) before it is forwarded to its next destination.
MAC	Message Authentication Code
MCD	Machine Call Detection
NAT	Network Address Translation
NTP	Network Time Protocol
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SBCE	Session Border Controller for Enterprise
Secure Sockets Layer (SSL)	SSL is a commonly-used method for managing the security of a message transmitted via the Internet and is included as part of most browsers and Web server products. Originally developed by Netscape, SSL gained the support of various influential Internet client/server developers and became the de facto standard until evolving into Transport Layer Security (TLS). The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network

or between program layers in the same computer (where a “socket” is an endpoint in a connection). SSL uses the Rivest, Shamir, and Adleman (RSA) public-and-private key encryption system, which also includes the use of a digital certificate.

If a Web site is hosted on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access.

TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.

SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SPAM	A common term used to describe the deliberate flooding of Internet addresses or voice mail boxes with multiple copies of the same digital or voice message in an attempt to force it on users who would not otherwise choose to receive it. SPAM can be either malicious or simply annoying, but in either case the cost of sending those messages are for the most part borne by the recipient or the carriers rather than by the sender (SPAMMER).
Spoof	A prevalent method of deceiving VoIP endpoints to gain access to and manipulate its resources (for example, faking an Internet address so that a malicious user looks like a known or otherwise harmless and trusted Internet user).
SRTP	Secure Real-Time Transport Protocol
SSL	Secure Socket Layer
STUN	Simple Traversal of UDP through NAT
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
ToD	Time-of-Day
Tromboning	The situation where RTP media traffic originates at a certain point within a network and follows a path out of that network into another network (the access network, for example) and back again to a destination close to where it originated. See <i>Anti-Tromboning</i> .

Tunneling	A security method used to ensure that data packets traversing an unsecure public network do so in a secure manner that prevents disruption or tampering.
TURN	Traversal Using Relay NAT
UDP	User Datagram Protocol
VM	Voice Mail
VoIP	Voice-over-Internet Protocol
VPN	Virtual Private Network
Zero-Day Attack	A particular type of exploit that takes advantage of a security vulnerability in a network on the same day that the vulnerability itself becomes generally known. Ordinarily, since the vulnerability isn't known in advance, there is oftentimes no way to guard against an exploit or attack until it happens.
Zombie	An IP network element that has been surreptitiously taken over by an attacker, usually without the user's knowledge.

Index

Numerics

- 9608 deskphone [27](#), [29](#)
- 96x1 deskphone [27](#), [29](#)

A

- advanced services offer [11](#)
- air pressure requirements [37](#)
- altitude requirements [37](#)
- AMAX server [29](#), [37–39](#)
- anomaly detection [11](#), [14](#), [42](#)
- application control [45](#)

B

- basic services [13](#)
 - configuration [13](#)
 - offer [13](#)
- border access control [16](#)
- borderless UC [13](#)

C

- call pattern detection [42](#)
- call rates [33](#)
- capacities [33](#)
 - call rates [33](#)
 - sessions [33](#)
 - users [33](#)
- certifications of server [39](#)
- codec validation [15](#)
- command [50](#)
 - protect-socket [50](#)
- common firewall rules [46](#)
- Communication Manager [29](#)
- Communication Server 1000 [29](#)
- compatible products [29](#)
 - Avaya [29](#)
 - mobile workspace user [29](#)
 - SIP trunking [29](#)
- concurrent sessions [33](#)
- control center [42](#)

D

- data interface firewall rules [46](#)

- data interface restrictions [44](#)
- Debian Linux [31](#)
- debian package install [45](#)
- Dell R210 II [27](#), [29](#), [33](#), [37–39](#)
- denial of service [45](#)
- detection [42](#)
- dimensions of server [37](#)
- DNS server port [52](#)
- document changes [7](#)
- DoS activity reporting [45](#)
- DoS attacks [11](#)
- dynamic trust scores [42](#)

E

- element management system [11](#)
- EMS [11](#)
- EMS takeover [35](#)
- end-point fingerprints [42](#)
- environmental requirements for server [38](#), [39](#)

F

- failover [34](#)
- firewall rules [46](#)
 - common [46](#)
 - data interface [46](#)
 - management [46](#)
- firewall rules, generating [50](#)
- Flare Experience for iPad [27](#), [29](#)
- Flare Experience for PC [27](#), [29](#)
- flood protection [41](#)
- forking [18](#), [20](#)
 - media [18](#)
 - signaling [20](#)
- fuzzing protection [41](#)

G

- GARP support [33](#)

H

- hardware platforms [11](#)
- hardware warranty [9](#)
- header manipulation [20](#)

high availability	33, 34	platform capacities	33
Avaya SBCE	34	PLDS	27, 55
HTTP/HTTPS ports	52	port assignments	52
I		DNS	52
in-line deployment	16	HTTP/HTTPS	52
information management subsystem	15	media	52
intelligence element	14, 15	SIP signaling	52
IP Office	29	SNMP	52
IP Office SSL	20	Syslog	52
IPTable firewall rules	43	port restrictions	51
L		Portwell CAD-0208	27, 29, 33, 37–39
layer 3 and 4 security features	43	power requirements of server	38
license download	55	Presence Services	29
licensing	55	processors	29
advanced services	55	product compatibility	29
standard services	55	R	
Linux operating system	31	reconnaissance prevention	41
M		recording signal data	20
management firewall rules	46	REFER	24
management interface port restrictions	51	reinvite	27
management interface restrictions	44	related documentation	8
master storage repository	15	remote user	19
media anchoring	18	remote worker	19
media anomaly prevention	41	replication	35
media element	14, 15	EMS	35
media ports	52	restrictions	44
Medpro (TN2302) circuit pack	33	data interface	44
mobile workspace user	19	RTP anomaly detection	15
monitoring	42	rules	50
monitoring, detection and protection	42	data interface	50
MontaVista Linux	31	firewall	50
N		rules for data interfaces	45
NAT traversal	15	S	
O		safety requirements	39
on-board storage	29	SAL	27
one-wire deployment	16, 17	SAL gateway	30
one-X Communicator	27, 29	SBC hardening	43
one-X Mobile SIP iOS	27, 29	screened subnet deployment	16, 17
P		scrubber rules package	46
parallel mode configuration	34	scrubber templates	46
		security life cycle	11
		security settings	44
		server	37–39
		certifications	39
		dimensions	37
		environmental requirements	38
		humidity requirements	38

power requirements	38	system configurations	11
temperature requirements	38	system memory	29
servers	29	system requirements	37 , 38
Session Manager	29	air pressure	37
SigMa module	13	altitude	37
signal data recording	20	humidity	38
signaling decryption	14	power	38
signaling element	14	temperature	38
signaling manipulation	20	T	
signaling mirroring service	20	TCP packets restrictions	52
SIP call processing	20	TCP signaling level flooding control rules	44
SIP decoding	14	thermal requirements	39
SIP signaling ports	52	TN2302 circuit pack	33
SIP trunk integration module	13	training	8
SIP trunking	20	two-wire deployment	16
SIP validation	14	U	
site requirements	39	UC proxying	13
environmental, safety, thermal	39	unified communication policies	43
SNMP ports	52	unified communications security	11
software warranty	9	user capacities	33
spoofing	11 , 14 , 41	V	
SRTP encryption of media	16	videos	9
SSH port rules	52	virtual private network TLS encryption	16
SSL	27	W	
SSL VPN	20	warranty	9
stealth attack prevention	41	WebLM	55
support	9 , 20		
contact	9		
remote	20		
support under warranty	9		
Syslog port	52		

