Avaya Session Border Controller for Enterprise Overview and Specification

Release 8.0
Issue 1
February 2019

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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of 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: https://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” means an Avaya 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 ONLY IF YOU PURCHASE AN AVAYA 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, HTTPS://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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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 is the software contained within the list of Heritage Nortel Products located at https://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. Unless otherwise stated, 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: https://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 only 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 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 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

You acknowledge and agree that it is Your responsibility 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: https://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).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

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, its licensors, its suppliers, 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.

Contents

Chapter 1: Introduction

Purpose

This document describes tested Avaya Session Border Controller for Enterprise (Avaya SBCE) characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements.

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

Chapter 2: Avaya Session Border Controller for Enterprise overview

Avaya SBCE provides security to SIP-based Unified Communications (UC) networks. Avaya SBCE is available in two versions: Advanced Services and Standard Services. Either version can reside on supported servers. For information about supported servers, see the “Avaya SBCE supported servers” section.

Avaya SBCE has two main components: Session Border Controller (Avaya SBCE) and a management system called the Element Management System (EMS). Depending on the network size and service requirement, you can deploy Avaya SBCE in one of the following configurations:

- Standalone configuration

  In the standalone configuration, the Avaya SBCE and EMS coreside in the same physical server.

- Multiple server configuration

  In the multiple server configuration, EMS and Avaya SBCE are deployed on separate physical servers.

- High availability (HA) configuration

  In the High Availability or HA configuration, Avaya SBCE servers are deployed in pairs. Each pair has one Avaya SBCE server acting as primary while the other is secondary. Both servers are controlled by a single Avaya Element Management System (EMS) device or a replicated EMS pair.

Related links

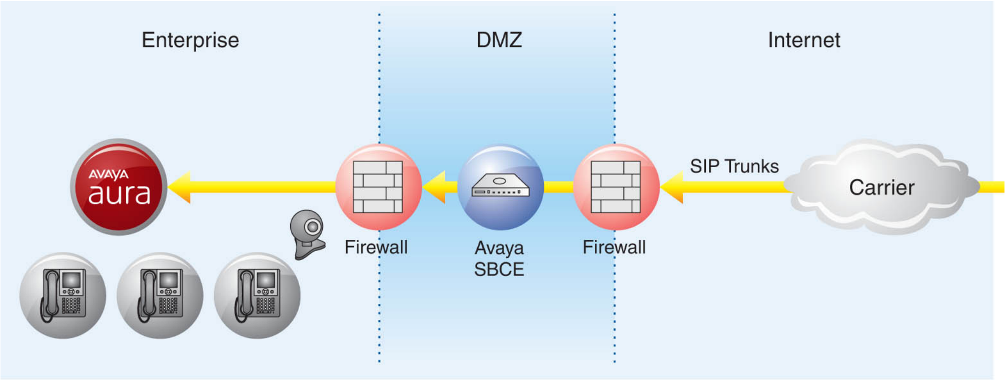
Avaya SBCE supported servers on page 74

Standard services

Avaya SBCE Standard Services provides a subset of the functionality of the Advanced Services offer. Standard services has the functionality required for an enterprise to terminate SIP trunks without the complexity and higher price associated with a typical Session Border Controller (SBC).

Avaya SBCE Standard Services is a true enterprise SBC, not a repackaged carrier SBC. This product provides a lower-cost alternative to the more expensive Carrier SBCs. Standard Services also provide an Enterprise SBC that is affordable, highly scalable, and easy to install and manage. Standard Services is a Plug and Play solution for Enterprises and Small to Medium Businesses.

With this product, customers can benefit from Avaya's extensive experience in SIP trunk deployments and supporting large numbers of enterprise users. Avaya SBCE Standard 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 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 2 hours or less.



cysbsptk 061313

Figure 1: SIP trunking

Advanced Services

Advanced Services is a specialized Unified Communications (UC) security product. Advanced Services protects all IP-based real-time multimedia applications, endpoints, and network infrastructure from potentially catastrophic attacks and misuse. This product provides the real-time flexibility to harmonize and normalize 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. Advanced Services protects any wire-line or wireless enterprise or service provider that has deployed UC, from malicious attacks. These attacks can originate from anywhere in the world anytime. Advanced Services is the only UC-specific security solution that effectively and seamlessly incorporates all approaches into a single, comprehensive system.

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. Advanced Services incorporates security techniques that include UC protocol anomaly detection and filtering, and behavior learning-based anomaly detection. Together, these techniques monitor, detect, and protect any UC network from known security vulnerabilities by:

- Validating and supporting remote users for extension of Avaya Aura® UC services.
- Using encryption services such as SRTP.

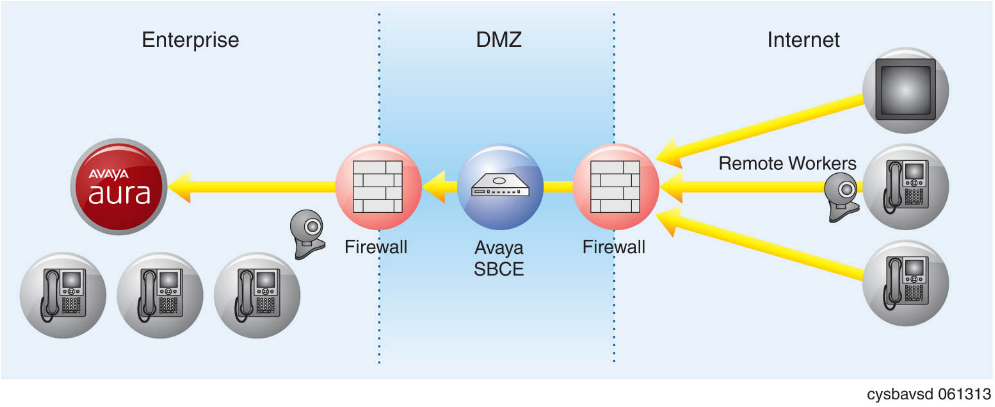


Figure 2: Advanced Services Solution

Functional entities

Avaya SBCE security products perform security functions using three interrelated and complementary functional entities: signaling, media, and intelligence.

Signaling element

The Signaling element is the primary call signaling protection subsystem. The Signaling element 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 end-to-end latency budget.

The Signaling element provides the following features:

- Inline signaling decryption and secure key management through TCP and TLS support
- Enhanced SIP validation through 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
  - Bypass for all non-SIP traffic including ARP, DNS, ICMP, STUN, and TURN
  - Domain-based policy filtering based upon user-definable call source and destination criteria
  - 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. The Signaling element uses http or https to send the Personal Profile Manager (PPM) information to the phone.

Media element

The Media element is the primary RTP media protection subsystem. A Media element is deployed in the network with the Signaling element.

The Media element provides the following features:

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

Element and management provisioning

Element and management provisioning is the primary UC security information management subsystem of the Avaya SBCE solution. Element and management provisioning receives the variously formatted event and alarm reports from the different security components in the network. This system then stores, normalizes, aggregates and correlates the information into a comprehensive format that allows distributed attacks to be effectively detected and mitigated.

Element and management provisioning provides the following features:

- Collects event logs
- Propagates instructions to the Signaling entity for preventive actions
- Propagates alarms to network management systems
- Maintains caller Trust Scores, White Lists, and Black Lists
- Provides a master storage repository for callers and domains
- Maintains per-user, per-caller, and per-network element behavior models on a ToD and DoW basis

Avaya SBCE deployment

Deployment models

Depending on the network size and service requirement, you can deploy Avaya SBCE in one of the following configurations:

- **Standalone configuration**: In the standalone configuration, the Avaya SBCE and EMS coreside in the same physical server. In this deployment, the phones maintain two separate socket connections to Avaya SBCE, at two different IP addresses hosted by Avaya SBCE.
- **Multi-server configuration**: A multi-server configuration requires EMS and Avaya SBCE to be deployed on different servers.
- **High availability (HA) configuration**: A High availability (HA) configuration requires a separate EMS server. 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 or 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 or 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.

These configurations are also available with deployment in the virtualized environment.

Avaya SBCE is packaged as a vAppliance (OVA) ready for deployment on VMware certified hardware to run in VMware environment. From Release 6.3, Avaya SBCE is also delivered in vAppliance (OVA) format for VMware based deployments. Avaya SBCE has a single OVA file for EMS, SBCE+EMS, and Avaya SBCE only deployment. The .ova file is available in PLDS. This configuration supports VMware features, such as vMotion, HA across datacenters, and mixed hardware configuration.

For more information about virtualization, see *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*.

Deployment modes

Avaya SBCE devices can be deployed with or without Transport Layer Security (TLS) or Secure Real-Time Transport Protocol (SRTP) encryption.

Regardless of the deployment scenario, Avaya SBCE offers complete flexibility and intuitive configuration. These products 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 inline, is the simplest and most basic deployment. Avaya SBCE is positioned at the edge of the network in the DMZ. Avaya SBCE is directly inline with the call servers, and protects the enterprise network against all inadvertent and malicious intrusions and attacks.

In this configuration, the Avaya SBCE performs border access control functionality such as internal and external Firewall or Network Address Translation (FW/NAT) traversal, access management and control. These functions are based on domain policies that the user can configure, and intrusion functionality to protect against DoS, spoofing, stealth attacks, and voice SPAM.

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

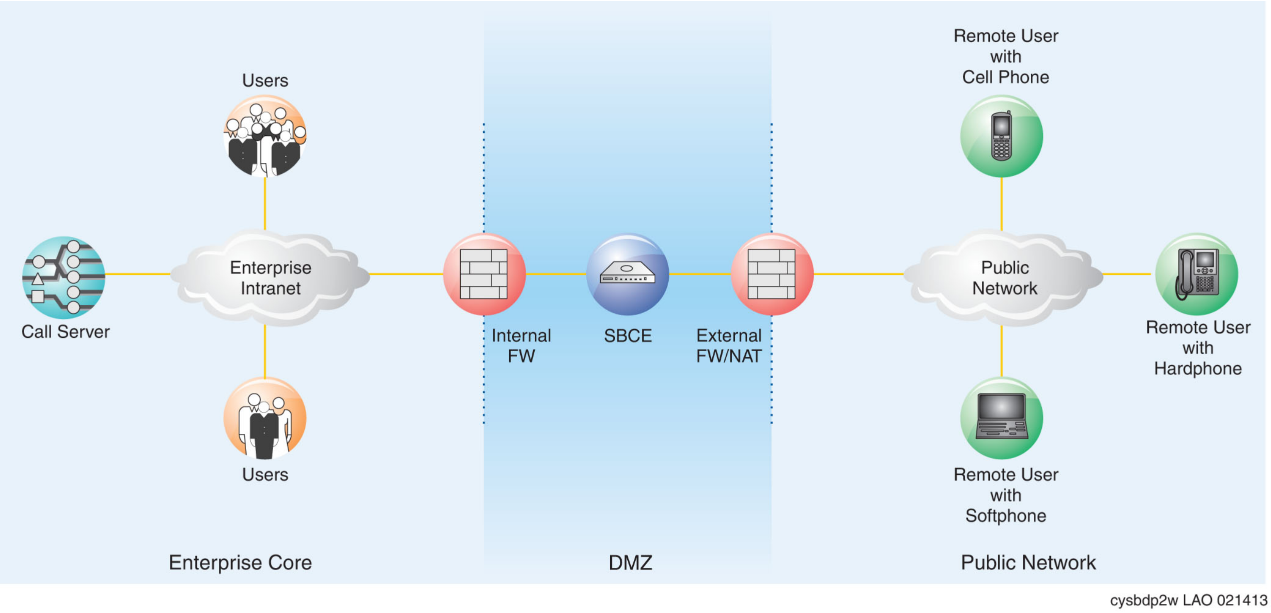


Figure 3: Avaya SBCE Deployment – Two-Wire

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 inline with the enterprise call servers. The Avaya SBCE 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 inline deployment. This deployment 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.

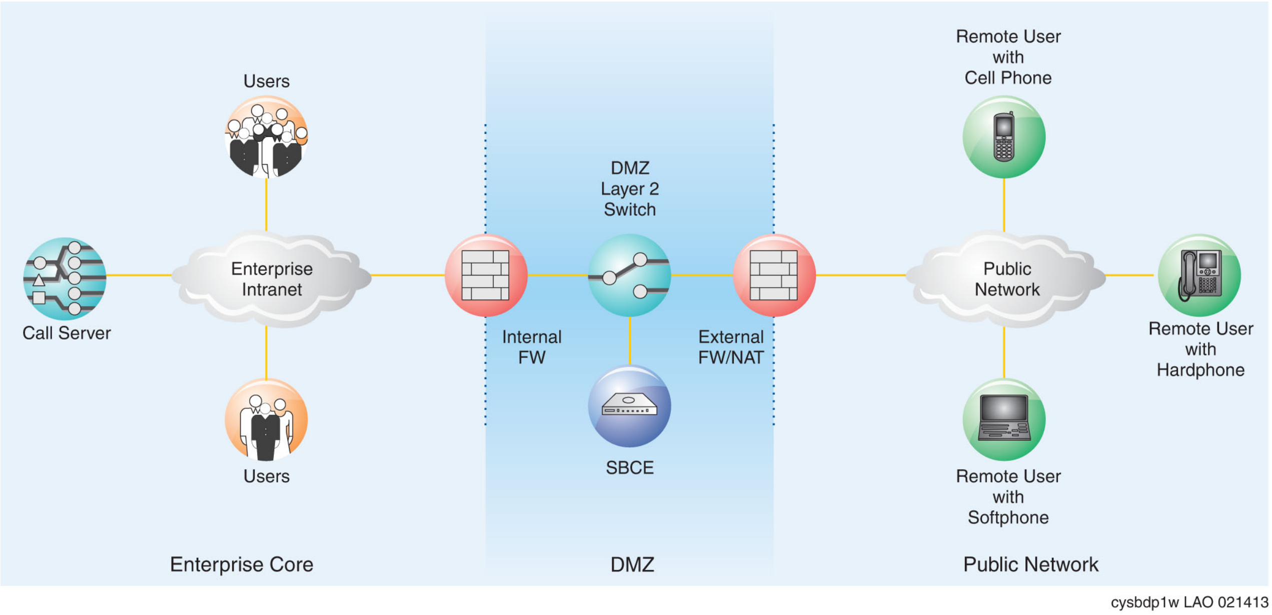


Figure 4: Avaya SBCE Deployment – One-Wire

Supported deployment platforms for SBCE

Virtualization overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture.

Using Avaya Aura® Virtualized Environment, customers with a VMware IT infrastructure can upgrade to the next release level of collaboration using their own VMware infrastructure. For customers who need to add more capacity or application interfaces, Avaya Aura® applications on VMware offer flexible solutions for expansion. For customers who want to migrate to the latest collaboration solutions, Avaya Aura® Virtualized Environment provides a hardware-efficient simplified solution for upgrading to the latest Avaya Aura® release and adding the latest Avaya Aura® capabilities.

For deployment on VMware-certified hardware, Avaya SBCE is packaged as vAppliance ready Open Virtualization Environment(OVA) to run in the virtualized environment. Avaya SBCE is also available for VMware-based deployments.

You can deploy EMS and Avaya SBCE using a single OVA file.

Avaya SBCE supports VMware features, such as vMotion, HA across data centers, and mixed hardware configurations.

The Avaya SBCE OVA files are offered as vAppliance for EMS and Avaya SBCE configurations. The .ova file is available in Product Licensing and Delivery System (PLDS).

Avaya Aura® on Amazon Web Services overview

Amazon Web Services (AWS) is a cloud services platform that enables enterprises to securely run applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

Supporting the Avaya applications on the AWS Infrastructure as a service (IaaS) platform provides the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to operational expense (OPEX).
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.

You can deploy the following Avaya Aura® applications on Amazon Web Services:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Utility Services
- Avaya WebLM
- Presence Services using Avaya Breeze® platform
- Avaya Session Border Controller for Enterprise
- Avaya Aura® Device Services
- Avaya Aura® Application Enablement Services (Software only)
- Avaya Aura® Media Server (Software only)
- Avaya Diagnostic Server (Software only)

The supported Avaya Aura® AWS applications can also be deployed on-premises.

You can connect the following applications to the Avaya Aura® AWS instances from the customer premises:

- Avaya Aura® Conferencing Release 8.0 and later
- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway, G450 Branch Gateway, and G650 Media Gateway

For more information, see *Deploying Avaya Session Border Controller for Enterprise on Amazon Web Services*

Kernel-based Virtual Machine overview

Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

KVM virtualization solution is:

- Cost effective for the customers.
- Secure as it uses the advanced security features of SELinux.
- Performance reliable and highly scalable.
- Open source software that can be customized as per the changing business requirements of the customers.

You can deploy KVM using Nutanix as well.

For more information, see *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*.

Additional network security deployment

This deployment provides protection to the core UC infrastructure while allowing access to services delivered through the core Aura® applications infrastructure. The following diagram shows this deployment.

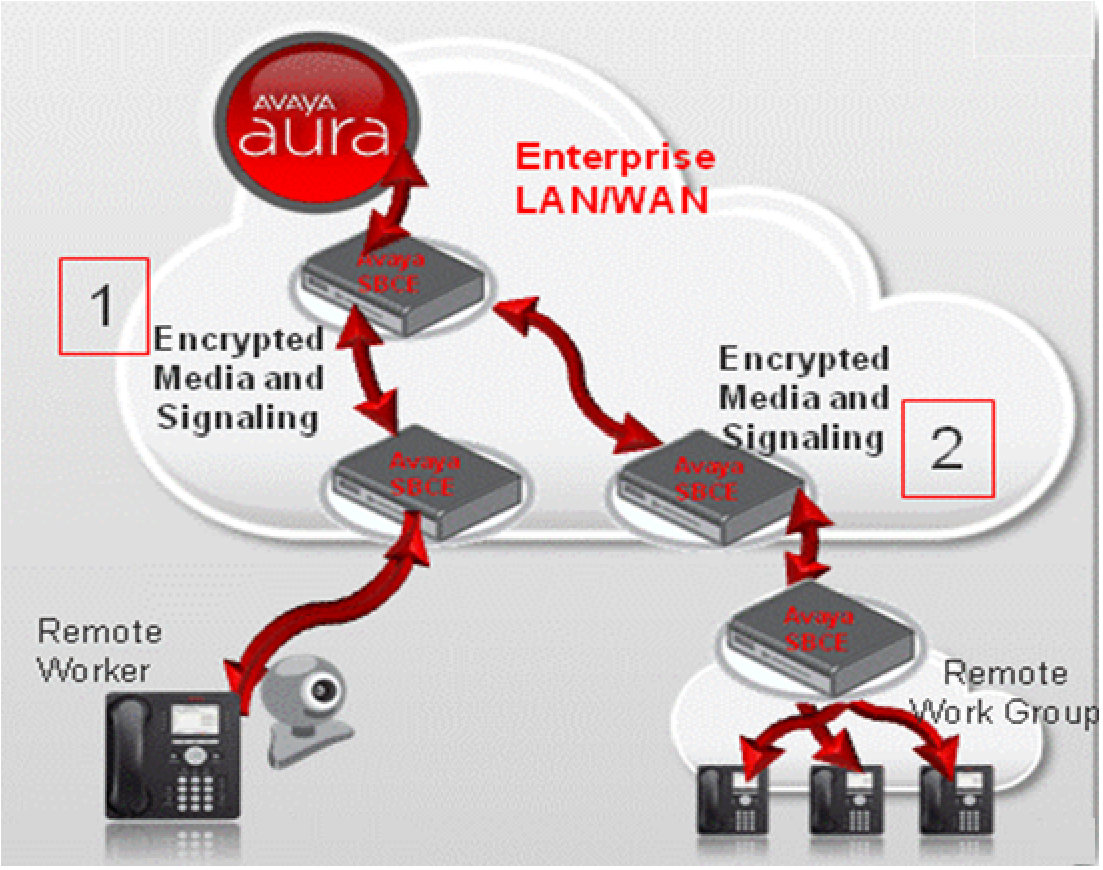


Figure 5: Additional network security deployment

In the diagram, two use cases are depicted. The first configuration shows a back-to-back scenario in which the Aura core is protected by Avaya SBCE internally, and Remote Workers connect to the core via a different Avaya SBCE. Avaya SBCE maintains security and NAT bindings and end-to-end encryption in this back-to-back (B2B) scenario. The second scenario depicts a Remote work group using a Avaya SBCE at the local edge of the group, creating a back-to-back-to-back (B2B2B) scenario. This configuration allows for treatment of the work group as Remote from both the main network and the Aura core and supports encryption of signaling and media from the clients to Avaya SBCE and then to the core if desired. This configuration is supported with Avaya 96x1 SIP clients.

Password policies

The root and ipcs passwords are determined and set during product installation.The EMS GUI has a separate password. When you log in for the first time after installation, the system prompts you to create a new password for accessing the EMS GUI. The default user ID and password is `ucsec`.

Password restrictions are enforced on the ucsec and ipcs accounts. The new password must meet the password criteria of minimum 8 characters, including:

- One uppercase letter, one lowercase letter, and one number.
- One special character from the hyphen (-), underscore (_), at sign (@), asterisk (*), and exclamation point (!).You must not use the number sign (#), dollar sign ($), and ampersand (&).

Note:

The customer network administrator determines the Avaya SBCE CLI root and ipcs passwords during the installation procedure. Two installation steps prompt the installer to enter a chosen password.

New in this release

Avaya Session Border Controller for Enterprise Release 8.0 supports following new features and enhancements:

Avaya Aura® SIP Resiliency

With the SIP Resiliency feature, Avaya SBCE preserves the call by using Session Manager to reconstruct the call between disconnected endpoints. Avaya recommends using the same domain names for signaling groups to support call reconstruction.

The SIP Resiliency feature is applicable for non Avaya Aura® Failover Group Domain Name (FGDN) segments, whereas for FGDN segments the Call Preservation feature of the previous release is applicable.

Simplified deployment

The Simplified Deployment feature provides the following:

- Simplified Backup/Restore provides device specific backup/restore functionality. The device can be EMS or SBC in a multi-SBC configuration.
- Simplified Upgrade/Rollback provides the stage upgrade/rollback to collect logs at each stage and improves error handling. This feature also supports incremental database upgrade, which reduces time for upgrade/rollback and this process is less prone to errors. A post verification check is also added to check whether upgrade/rollback is successful.
- CLI based configuration provides configuration of Avaya SBCE using CLI interface.
- Simplified User Interface feature, enables selecting the device and then configuring the selected device.

Extended hostname validation

With the Extended hostname validation feature, the system validates the host name or domain name of the server with the value of the **subject** or **subjectAltName** field in the identity certificate for establishing the SSL connection.

For the Extended Hostname Validation feature, Avaya SBCE must support TLS Server Name Indication (SNI).

MAC-based LDAP authentication

MAC-based Lightweight Directory Access Protocol (LDAP) authentication feature uses LDAP to authenticate end points based on SIP REGISTER messages. Avaya SBCE supports LDAP version 3.

LDAP based call routing

LDAP based call routing feature routes the SIP INVITE message from a SIP trunk in an enterprise network with multiple SIP call servers.

Support of Avaya Converged Platform

Avaya SBCE supports Avaya Converged Platform 100 series server with profile 3 for less capacity applications and Avaya Converged Platform 100 series server with profile 5 for high capacity applications.

Improved multi-tenancy

With the Improved multi-tenancy feature, you can add new tenants and interfaces without rebooting your system.

Feature description

Media anchoring

The Avaya SBCE anchors the media streams of all media that passes through the Avaya SBCE. With media anchoring, Avaya SBCE can perform SRTP termination, where Avaya SBCE decrypts or encrypts RTP traffic based on security policies and NAT traversal. All supported configurations require Media Anchoring.

Media unanchoring

To enhance bandwidth usage for endpoints within the same subnetwork and to allow direct media to flow between these endpoints, unanchor media for sessions. Use this feature to enhance bandwidth usage when you connect to a managed MPLS network or a cloud network.

Avaya SBCE supports media unanchoring for all non-hairpin calls, including trunk to enterprise, enterprise to trunk, remote to enterprise, and enterprise to remote. Avaya SBCE supports media unanchoring for audio, video, and multimedia calls.

Remote worker configuration

The Remote worker configuration gives remotely located SIP 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.

Remote worker configuration is available for SIP deployments. This configuration uses authentication to verify the legitimacy of the remote user and decrypts TLS-encrypted signaling SIP traffic in real-time. When decryption is completed, the Avaya SBCE analyzes traffic for anomalous behavior, attacks, and intrusions, and applies the user-defined UC policies.

The call can originate from a remotely located Remote worker configuration, outside the enterprise network, to an internal user inside the core enterprise network. Then, the Avaya SBCE in the enterprise DMZ decrypts the SRTP media coming in to the enterprise from the external IP network or the Internet. The Avaya SBCE 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.

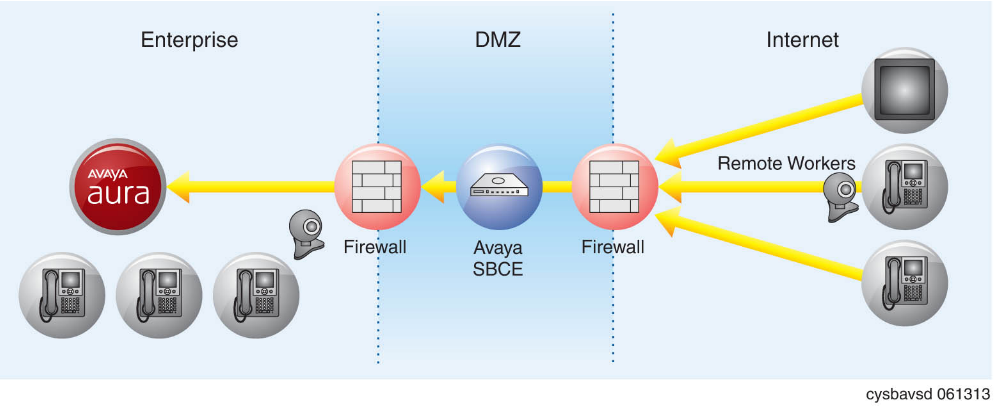


Figure 6: Remote worker

Remote management services

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

Avaya SBCE also supports remote access through the SAL gateway.

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

Signaling manipulation

With Avaya SIP signaling header manipulation, users can add, change, and delete the headers and other information in a SIP message. Signaling manipulation can be configured at each flow level using a proprietary scripting language.

SIP trunking

SIP Trunking allows SIP trunk-enabled enterprises to completely secure SIP connectivity over the Internet through SIP Trunking services obtained from 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 SIP implementations or servers of customers 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.

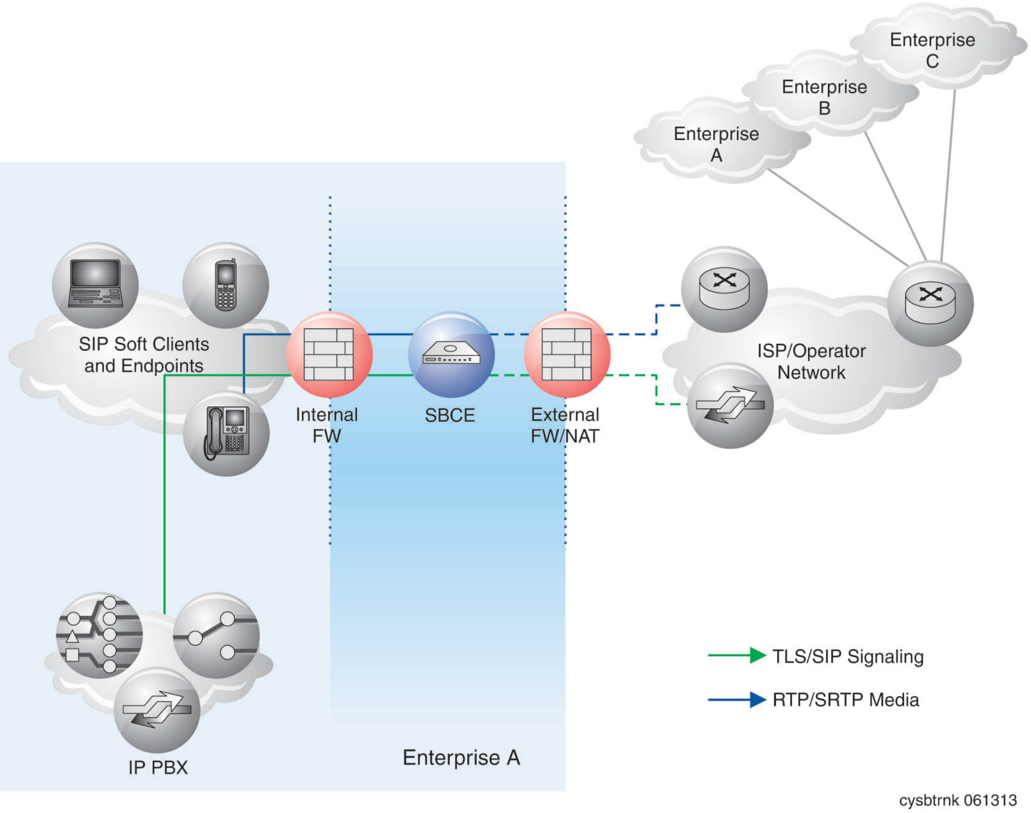


Figure 7: SIP Trunking

UCID

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

AACC

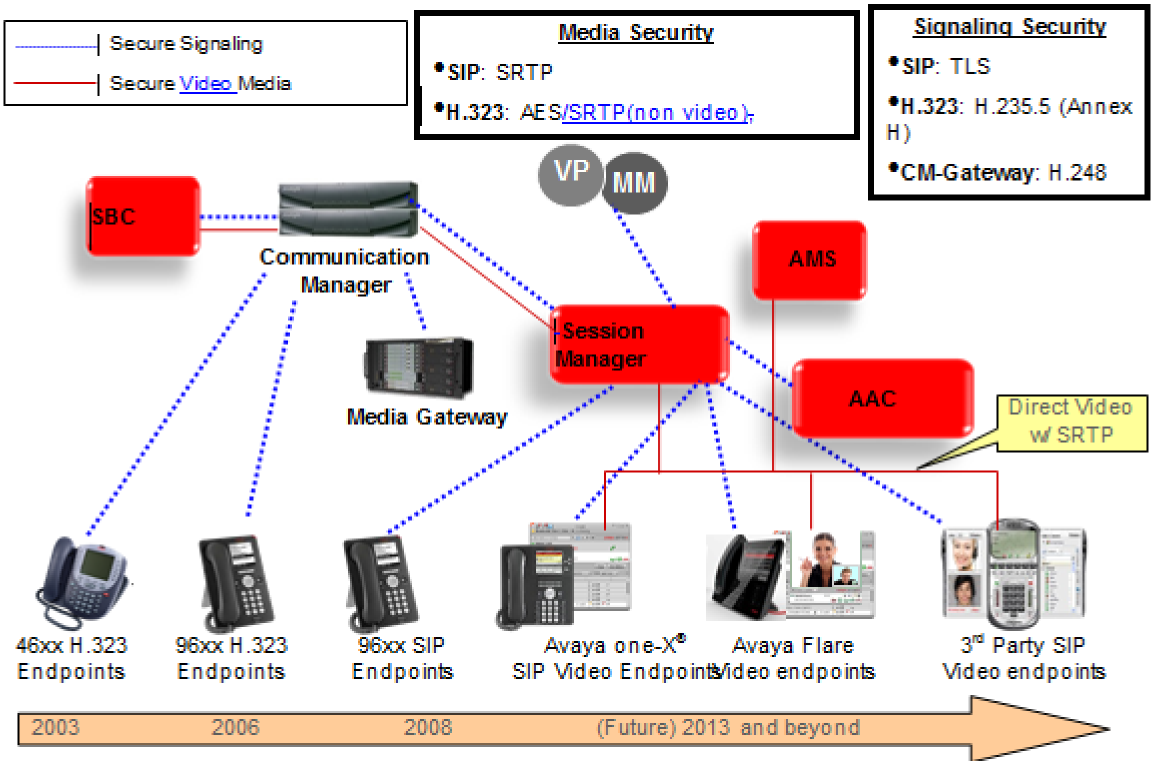
The generation of UCID by Avaya SBCE is required in Avaya Aura® Contact Center 7.0 environment. A UCID is assigned to any incoming call at the border Avaya SBCE so that AACC has a unique handle for each call. For instance, AACC then monitors or controls any application including call recorder using the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

CC Elite

The generation of UCID by Avaya SBCE 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. Avaya SBCE generates a UCID for all incoming SIP calls and ACM reuses the same UCID. No conflict of UCID occurs among ACM, Avaya SBCE, and Contact Center Applications. In features such as call holding, an association is maintained between the new UCID and parent UCID by ACM.

Support for video SRTP

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. The ip-codec-set rules enable the SRTP policy for video media stream.



Supported user cases

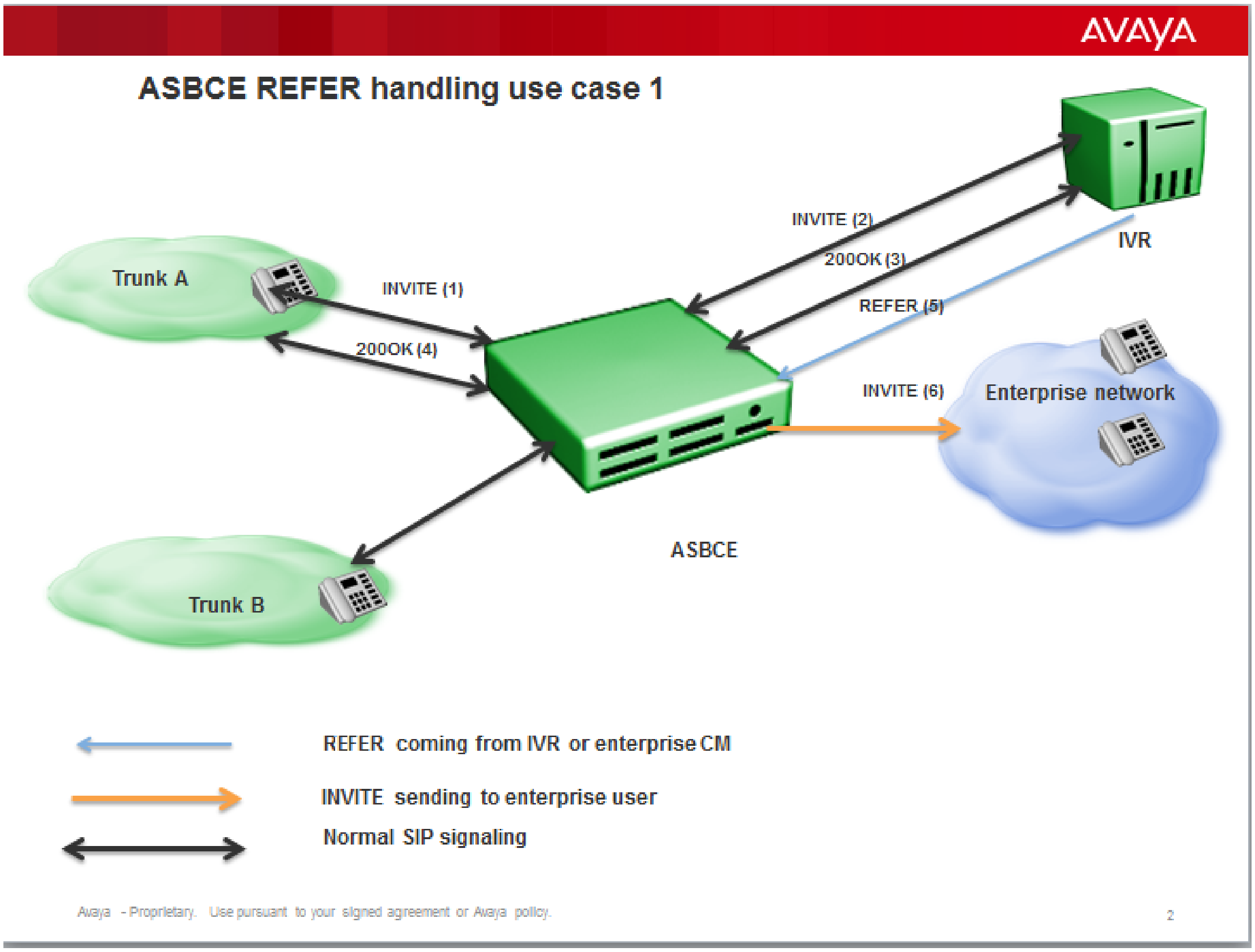
- Desktop Users – Avaya SIP Video Endpoint, such as 1XC to 1XC SRTP encrypted SIP video call : Enabling video calls between two video-enabled IntereXchange carrier SIP endpoints. All standard telephony and video features such as mute, transfer, and hold can be used.
- Mixed – SIP SRTP video call between 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, is unavailable to those devices. Third-party SIP endpoints might include video conference hardware. These endpoints also include 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, Avaya SBCE translates the incoming SIP REFER request to a SIP INVITE request. REFER message comes from enterprise, such as Communication Manager, or IVR and Avaya 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

Avaya SBCE uses REFER message and sends a routing INVITE towards enterprise user.



ASBCE REFER handling use case 1

← REFER coming from IVR or enterprise CM

→ INVITE sending to enterprise user

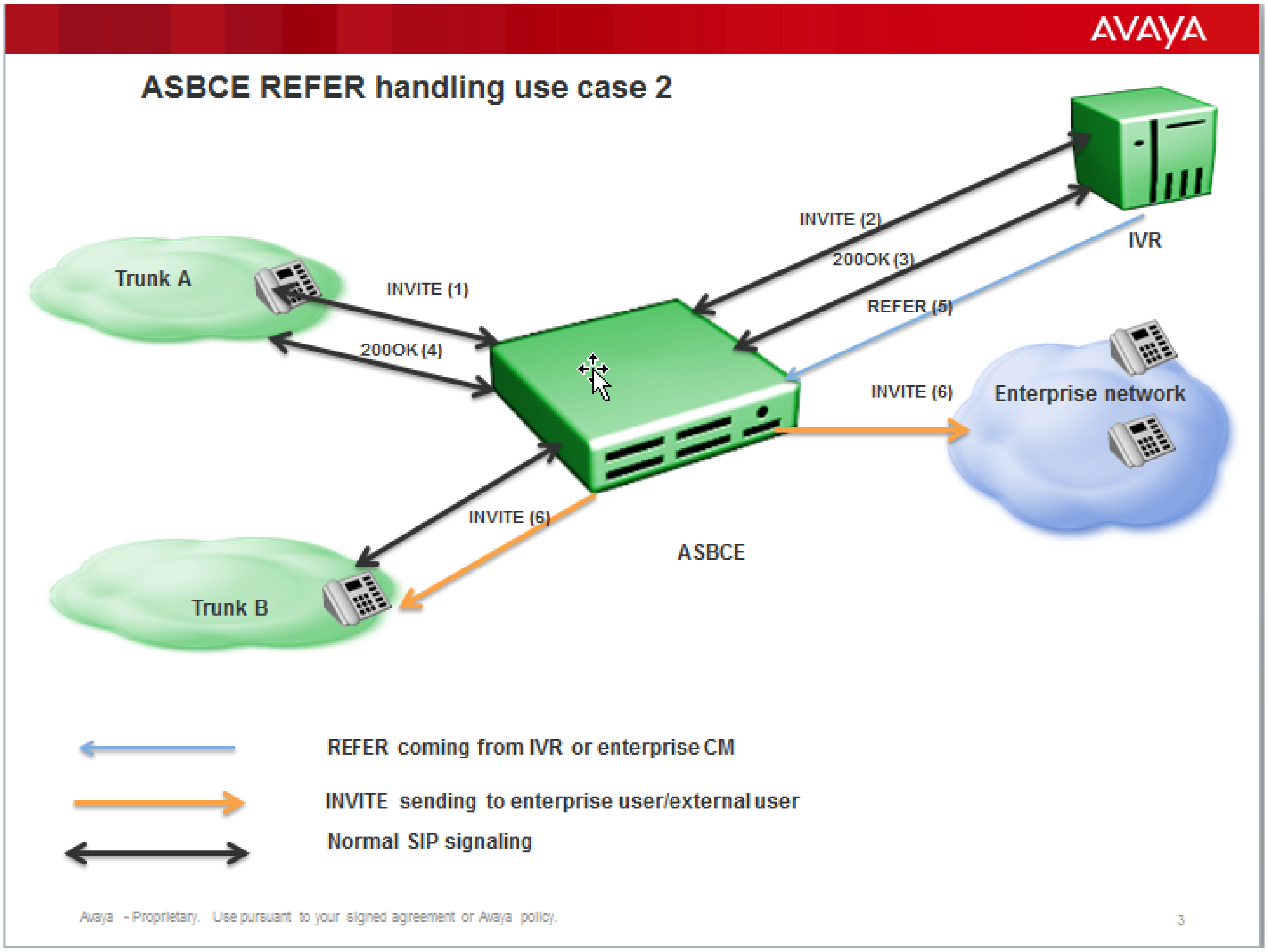
↔ Normal SIP signaling

Avaya - Proprietary. Use pursuant to your signed agreement or Avaya policy.

2

Use case 2

Avaya SBCE uses the REFER message to send an INVITE towards trunk user or enterprise user based on routing profiles created to route the new INVITE. INVITE created from REFER is routed using URI based routing. Routing entries must be created in the trunk server routing profile to route the request to external trunk. By default, the request is routed back to enterprise server. In Aura AST2 transfer mode, Avaya SBCE should always route the new INVITE towards the enterprise server as Avaya SBCE cannot find the dialog to replace.



AVAYA

ASBCE REFER handling use case 2

← REFER coming from IVR or enterprise CM

→ INVITE sending to enterprise user/external user

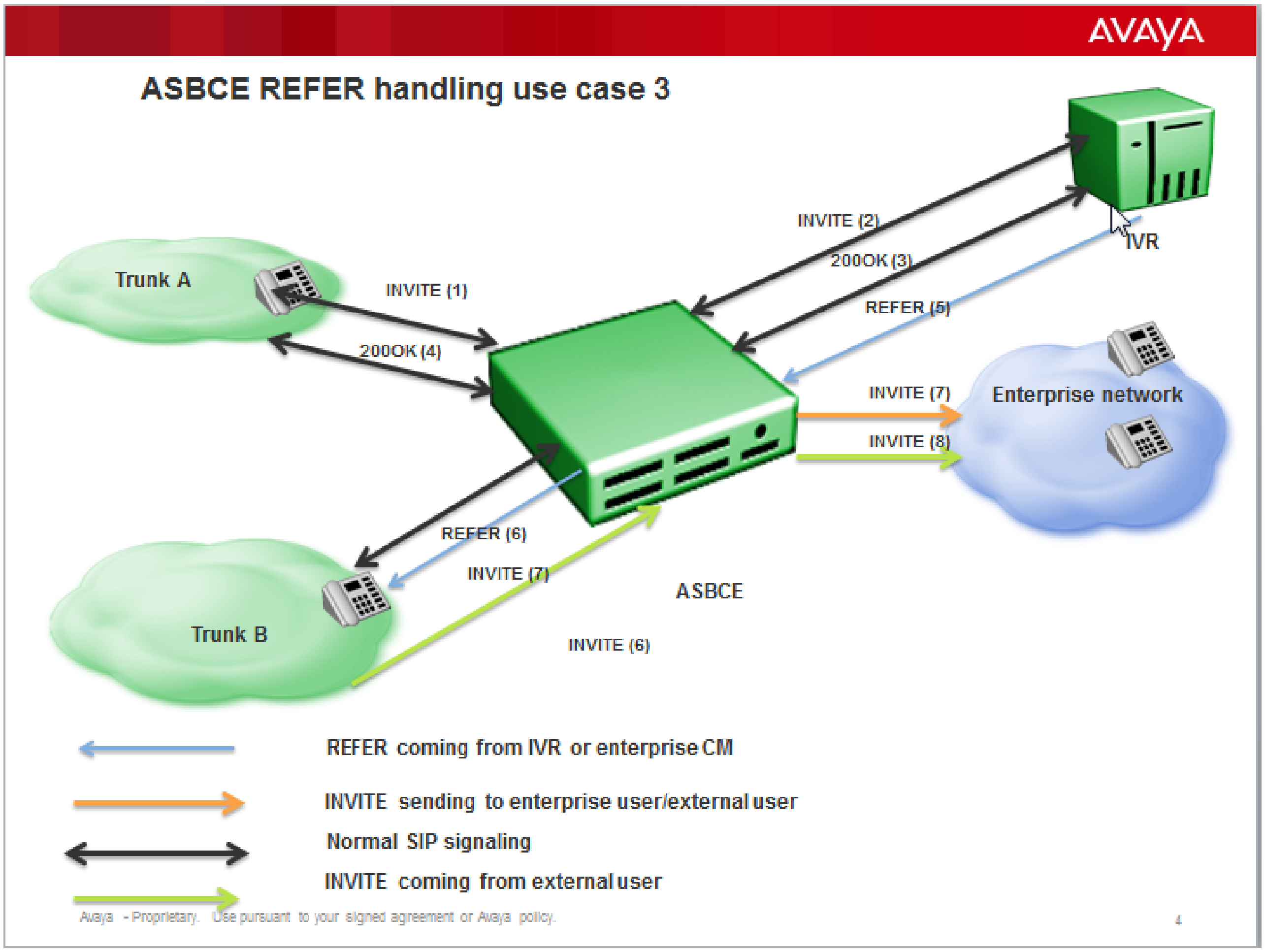
↔ Normal SIP signaling

Avaya - Proprietary. Use pursuant to your signed agreement or Avaya policy.

3

Use case 3

Based on URI group configuration under refer handling configuration, Avaya SBCE uses some REFER messages. Depending on URI group configuration, REFER messages are relayed to the external trunk. External trunks generate new INVITE message for the target users.



← REFER coming from IVR or enterprise CM

→ INVITE sending to enterprise user/external user

↔ Normal SIP signaling

→ INVITE coming from external user

Avaya - Proprietary. Use pursuant to your signed agreement or Avaya policy. 4

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, the user can join 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.

The Multi Device Access feature consists of the same user and extension using the same AOR to register multiple devices to Session Manager. All 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. The paired MDA 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 for a call involving AAC.

Reinvite handling

Some customers and service providers do not want reinvite messages to be passed on to the SIP trunk. Avaya SBCE blocks reinvite messages coming without change in Session Description Protocol, known as Session Refresh Invites. The same rule applies for Hold or Resume invites without change in SDP, except port, IP, and SDP attributes. The SDP attributes include send recv, send only, and recv only.

RTCP Monitoring

The RTCP monitoring feature in Avaya SBCE updates RTCP packet with appropriate endpoint IP address and hop information. Endpoints are configured to send RTCPMON messages to the Avaya SBCE to which the endpoint is registered. A single Avaya SBCE is designated core Avaya SBCE which is sent to Prognosis. Avaya SBCE maintains the RTCP port mapping and updates this mapping on a per call basis as part of the SIP signaling. Avaya SBCE implements a new feature in the application that has the capability to traceroute multiple destinations simultaneously.

- APIs are provided for the SIP Application to fetch the traceroute information for later reuse when modifying the RTCPMON messages.
- Avaya SBCE tracerouting feature implementation reuses the linux based tracerouting APIs.
- The ICMP/UDP/TCP Avaya SBCE configuration modes can use tracerouting and can be administered from GUI.

On receiving RTCPMON message for Prognosis, Avaya SBCE does a lookup in RTCP port-mapping. Avaya SBCE then modifies the remote IP address and RTCP Port in rtcp message Avaya Subtype 4, based on the mapping. Avaya SBCE then appends the trace hop information of the next network node where the RTP packets are forwarded in Avaya Subtype 5. If this Avaya SBCE is the designated core Avaya SBCE, then perform additional steps before forwarding the packets to Prognosis. Determine the SSRC field from RTCP monitoring packets from endpoint, for example SSRC1. Avaya SBCE also determines the SSRC of the incoming RTP stream from media gateway or caller, for example SSRC2. Avaya SBCE creates a mapping key using SSRC1 and SSRC2, if the mapping does not exist.The mapping key contains the following information:

- Media origination IP address or port for SSRC1 – populated from the RTCPMON Subtype 4 message.
- Media origination IP address or port for SSRC2 – populated from the RTCPMON Subtype 4 message.
- Traceroute information for all the hops from the endpoint [Caller] upto the Core Avaya SBCE – Populated from the RTCPMON Subtype 5 Message.
- Traceroute information for all the hops from the endpoint [Callee] upto the Core Avaya SBCE – Populated from the RTCPMON Subtype 5 Message.

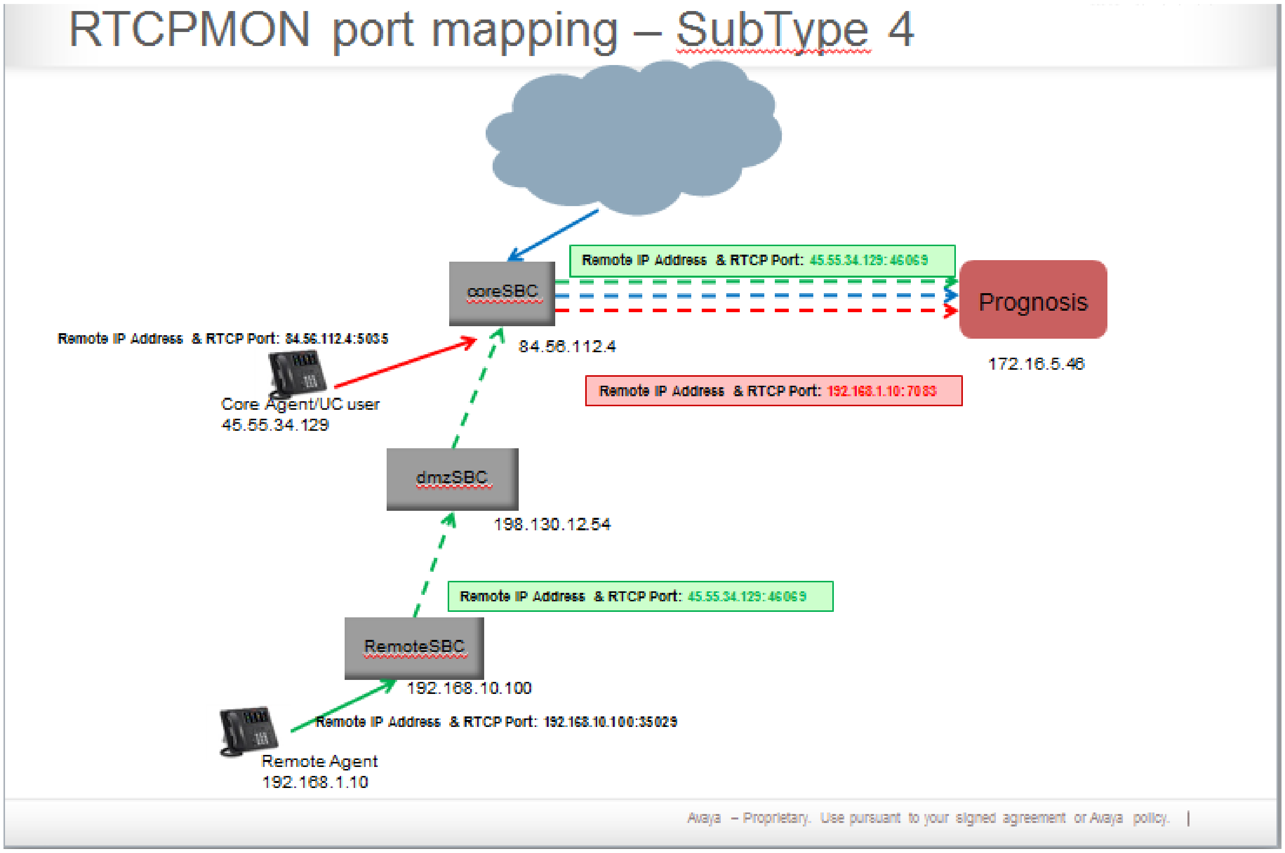
If mapping exists in the Avaya SBCE for SSRC1 and SSRC2, then Avaya SBCE uses the mapping information to rewrite the following in the RTCPMON packets to be sent to Prognosis:

- Subtype 4 RTCPMON.
- Remote IP Address/port of SSRC1 will be set to media origination IP address/port of SSRC2 from the mapping.
- Remote IP Address/Port of SSRC2 will be set to media origination IP address/port of SSRC1 from the mapping.
- Subtype 5
- Trace hop info for SSRC1 will include the current trace hop information received in RTCPMON packet plus trace hop information saved for SSRC2.
- Trace Hop Info for SSRC2 will include the current trace hop information received in RTCPMON packet plus trace hop information saved for SSRC1.

Processed RTCPMON packets will now be sent to Prognosis based on the information filled in by Avaya SBCE.

Modes of configuration

- **END-end Rewrite:** Avaya SBCE updates the RTCP subtype-4 packet from the media terminating endpoint. In Subtype-4, Avaya SBCE rewrites the Remote IP Address field with the Remote endpoint address who is the recipient of the RTCP packets. End-end rewrite must be configured in all Avaya SBCE devices which have media terminating endpoints connected to it directly. No other Avaya SBCE devices exist between that particular Avaya SBCE device and the media terminating endpoints.



RTCPMON port mapping – SubType 4

Remote IP Address & RTCP Port: 45.55.34.129:46069

coreSBC

Prognosis

Remote IP Address & RTCP Port: 84.56.112.4:5035

84.56.112.4

172.16.5.46

Remote IP Address & RTCP Port: 192.168.1.10:7083

Core Agent/UC user
45.55.34.129

dmzSBC

198.130.12.54

Remote IP Address & RTCP Port: 45.55.34.129:46069

RemoteSBC

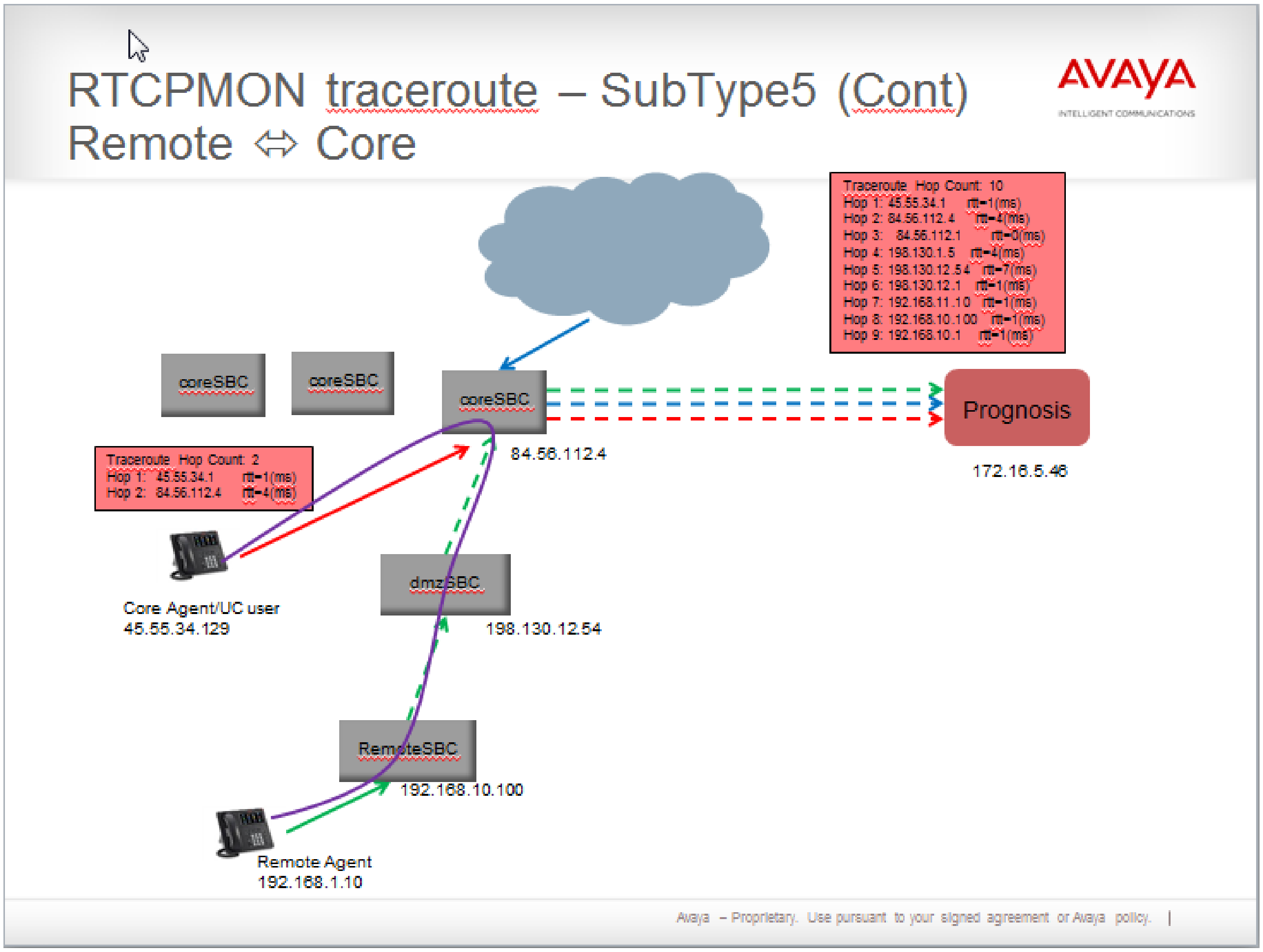
192.168.10.100

Remote IP Address & RTCP Port: 192.168.10.100:35029

Remote Agent
192.168.1.10

Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy. |

- **Hop-by-Hop trace route:** Avaya SBCE updates the RTCP subtype-5 packet with the trace route information. In subtype-5 packet, Avaya SBCE appends the trace route towards the entity to which Avaya SBCE forwards the RTP packet. Avaya SBCE sends the trace route towards the entity from which the Avaya SBCE received the RTP packet. You must configure hop-by-hop trace route for all Avaya SBCE devices.



RTCPMON traceroute – SubType5 (Cont)
Remote ⇔ Core

Traceroute Hop Count: 10
Hop 1: 45.55.34.1 rtt=1(ms)
Hop 2: 84.56.112.4 rtt=4(ms)
Hop 3: 84.56.112.1 rtt=0(ms)
Hop 4: 198.130.1.5 rtt=4(ms)
Hop 5: 198.130.12.54 rtt=7(ms)
Hop 6: 198.130.12.1 rtt=1(ms)
Hop 7: 192.168.11.10 rtt=1(ms)
Hop 8: 192.168.10.100 rtt=1(ms)
Hop 9: 192.168.10.1 rtt=1(ms)

coreSBC

coreSBC

coreSBC
84.56.112.4

Prognosis
172.16.5.46

Traceroute Hop Count: 2
Hop 1: 45.55.34.1 rtt=1(ms)
Hop 2: 84.56.112.4 rtt=4(ms)

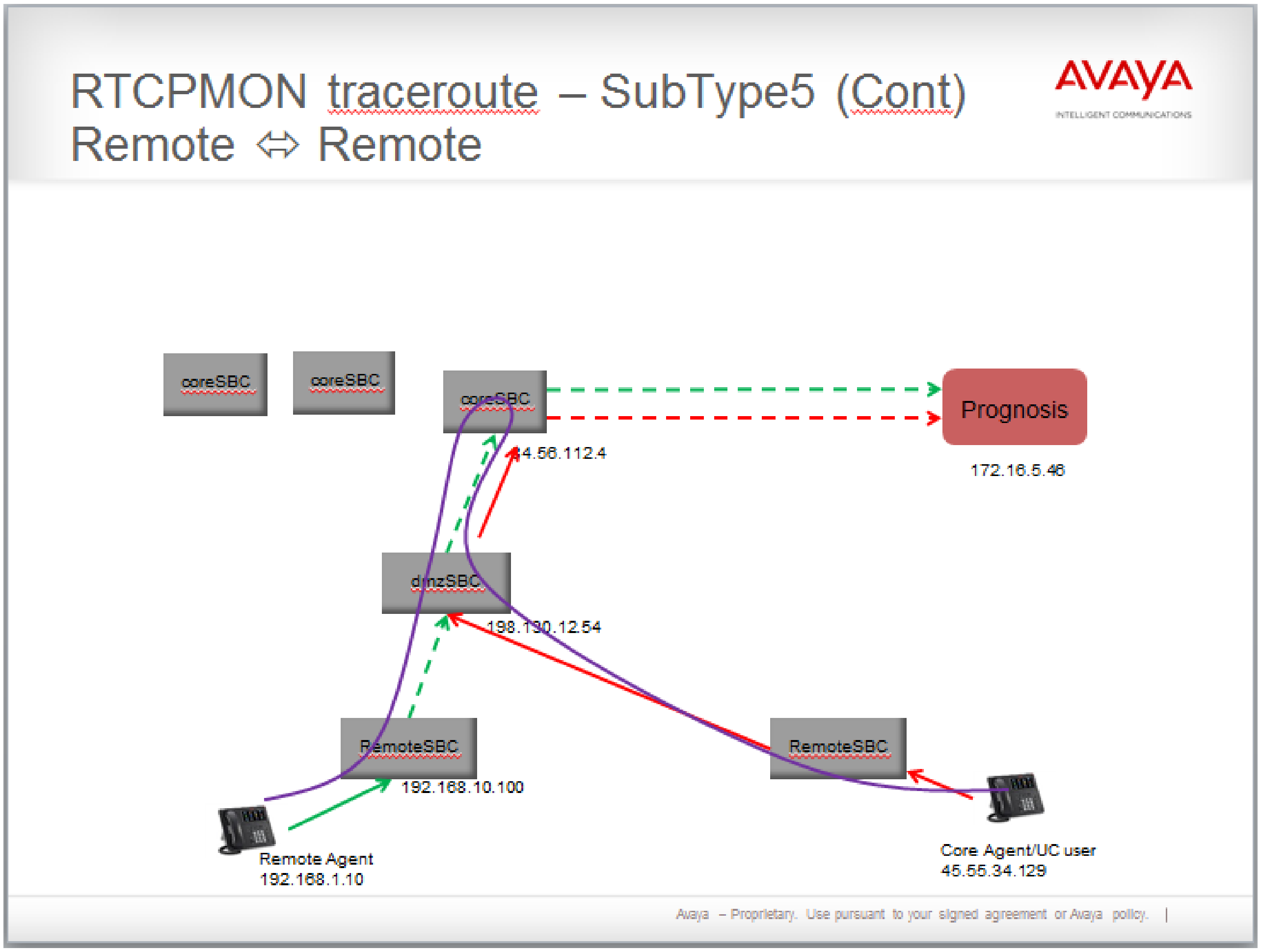
Core Agent/UC user
45.55.34.129

dmzSBC
198.130.12.54

RemoteSBC
192.168.10.100

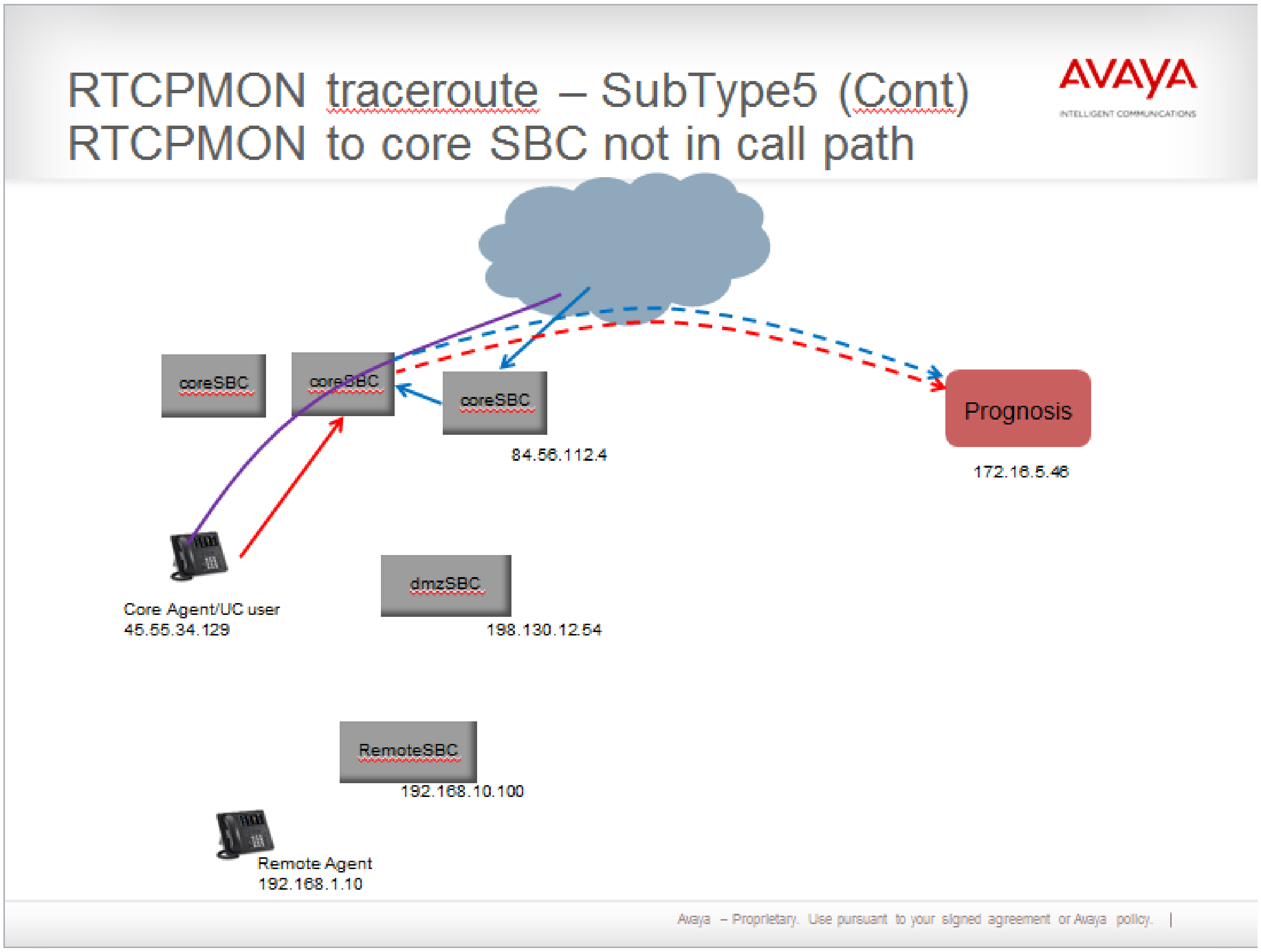
Remote Agent
192.168.1.10

Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy.



RTCPMON traceroute – SubType5 (Cont)
Remote ⇔ Remote

Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy. |



RTCPMON traceroute – SubType5 (Cont)
RTCPMON to core SBC not in call path

Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy. |

- **Bridging:** Avaya SBCE strips the reverse trace routes added by the Hop-by-Hop trace route and appends this data to the RTCP subtype-5 packet coming from the opposite side. Bridging must be configured only in CORE Avaya SBCE devices.

Note:

If a solution includes only one Avaya SBCE, all these configurations are required.

RTCP monitoring report generation

With RTCP monitoring report generation feature. Avaya SBCE receives RTCP streams from a trunk that does not have any Avaya specific control information as present in Avaya endpoints

Avaya SBCE generates an RTCP monitoring report that uses this feature. You must configure Avaya SBCE with the IP address of the RTCP monitoring server to send the generated data

This feature is applicable only for SIP trunks.

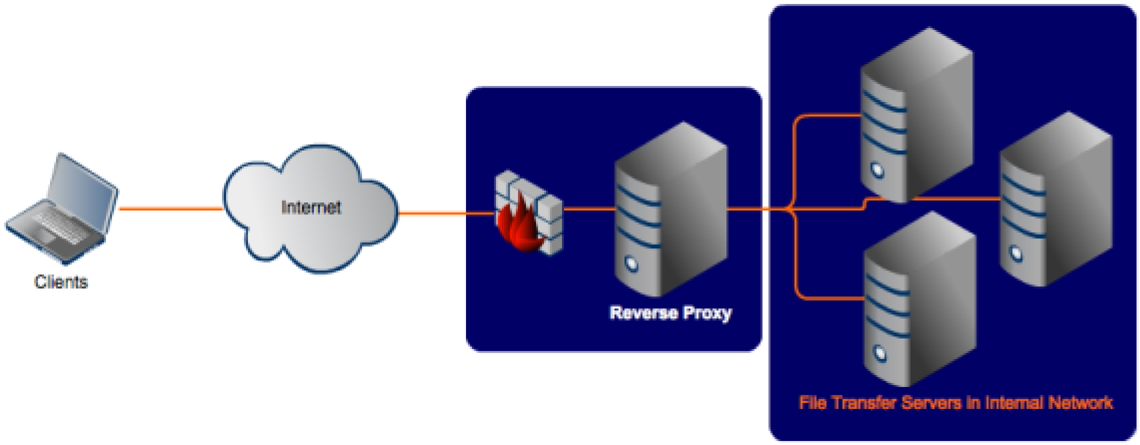
Reverse proxy

A reverse proxy is a web server that terminates connections with clients and makes new connections to backend servers on their behalf.

A backend server is defined as a server to which the reverse proxy makes a connection to fulfill the request from the client. These backend servers can take various forms, and reverse proxy can be configured differently to handle each of them.

A reverse proxy is also known as an inbound proxy, because the server receives requests from the Internet and forwards or proxies them to a small set of servers. The servers are usually located on an internal network and not directly accessible from outside. This proxy is reverse, because a traditional or outbound proxy receives requests from a small set of clients on an internal network and forwards them to the Internet.

The following diagram illustrates the typical configuration of reverse proxy for file transfer servers.



Advantages of Reverse Proxies

- Security:

  A reverse proxy can hide the topology and characteristics of backend servers by removing the need for direct internet access to them. You can place your reverse proxy in an internet facing DMZ, but hide your web servers inside a non-public subnet.

- Caching:

  The reverse proxy can also act as a cache. You can either have a dumb cache that expires after a set period, or better still a cache that respects Cache-Control and Expires headers. This can considerably reduce the load on the backend servers.

- Compression:

  To reduce the bandwidth needed for individual requests, the reverse proxy can decompress incoming requests and compress outgoing ones. This reduces the load on the backend servers that would otherwise have to compress outgoing requests. The reverse proxy makes debugging requests to, and responses from, the backend servers easier.

- Simplifies access control tasks:

  Clients only have a single point of access, you can concentrate access control on that single point.
- Aggregating Multiple Websites Into the Same URL Space:

  In a distributed architecture, different pieces of functionality can be served by isolated components. A reverse proxy can route different branches of a single URL address space to different internal web servers.
- Rewriting request URL:

  Sometimes the URL scheme that a legacy application presents is not ideal for discovery or search engine optimization. A reverse proxy can rewrite URLs before passing them on to your backend servers.
- Authentication:

  Reverse proxy can use client certificates to verify the identity of the client.
- Whitelisting of users:

  Whitelisting can be used to block or allow a specific set of user IP addresses to use the reverse proxy service. For example, if you add a whitelisted user IP address, all IPs other than the whitelisted IP are denied access to use the reverse proxy service.
- SSL Termination:

  The reverse proxy handles incoming HTTPS connections, decrypts the requests, and passes unencrypted requests on to the web servers. This has several benefits:

  - Removes the need to install certificates on many backend web servers.
  - Provides a single point of configuration and management for SSL/TLS.
  - Takes the processing load of encrypting or decrypting HTTPS traffic away from web servers.
  - Makes testing and intercepting HTTP requests to individual web servers easier.

Far End Camera Control

Avaya SBCE supports FECC Offer and Answer in SDP. Avaya SBCE checks if the media application line uses the H.224 codec. Any other media application line without an H.224 codec type is ignored.

Avaya SBCE does not negotiate Offer and Answer SDP for the Far End Camera Control (FECC) media application line. Offer and Answer exchange and negotiation is done end-to-end between the sender and receiver. Avaya SBCE does not support mixed encryption because FECC is tied to Media Rules. Therefore, FECC is encrypted if main video is encrypted. Similarly, FECC is on RTP if the main video is on RTP. If FECC is not negotiated in Offer and Answer end-to-end, the principal video channel works without FECC.

Avaya SBCE applies encryption according to SDP Capability Negotiation and SDES by Avaya SBCE policy.

Binary Floor Control Protocol

To provide continuous presence during video conferencing, applications use the switched video or the mixed and switched video technique.

Avaya Aura® Conferencing uses the switched video technique to provide continuous presence. Video streams are relayed to all participants so that each participant receives the corresponding multiple video streams from the far ends. Avaya Scopia® uses the mixed video technique where a single video media stream is mixed for all participating users.

Through the video channel, one of the continuous presence streams provides information about the presentation apart from the main video. The presentation channel is through the web and not through a video channel. Switched video streams use only one presentation video channel for multiple main video media streams for each participant. Mixed video devices use one video media stream for presentation. The main video media stream displays participants in one frame. The floor control of this presentation video channel is by Binary Floor Control Protocol (BFCP) messages.

BFCP messages control how multiple video streams access and use the shared video channel.

Detailed description of Binary Floor Control Protocol

In a conference, some applications control access to a shared set of resources. With BFCP, these applications provide users coordinated access to the resources.

Terminologies

To understand how BFCP works, you must be familiar with the following terms:

- **Floor**: A temporary permission to access a specific shared resource or set of resources.
- **Floor chair**: A logical entity that manages a floor.
- **Floor control**: A mechanism that enables applications or users to gain shared or exclusive access to the resource.
- **Floor control server**: A logical entity that maintains the state of the floor, including details such as which floors exist and who holds a floor.
- **Floor participant**: A logical entity that requests floors and related information from a floor control server. In floor-controlled conferences, a floor participant might be co-located with a media participant.

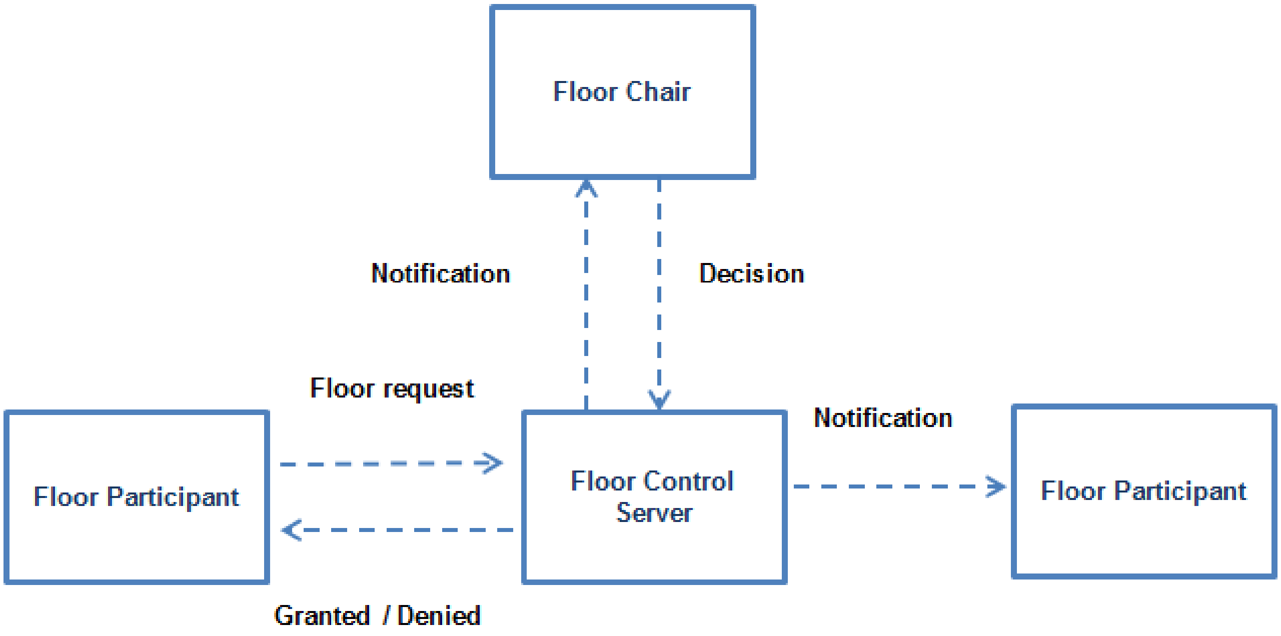


Figure 8: BFCP components

Functioning of BFCP

With BFCP, floor participants can send floor requests to floor control servers and floor control servers can grant or deny access to the requested resource. Also, floor control servers can keep floor participants and floor chairs informed about the status of a given floor or a given floor request.

Avaya SBCE relays BFCP control messages to control the presentation channel. Avaya SBCE supports BFCP for only two video channels, one of which is a video presentation channel.

In this release, Avaya SBCE supports TCP and UDP for the BFCP application.

Avaya SBCE negotiates with Avaya Scopia® MCU or Avaya Scopia® XT clients and obtains the value of the setup attribute as passive. The far-end then starts the TCP connection for the BFCP application. If Avaya SBCE fails to negotiate the setup attribute, the TCP connection is started by Avaya SBCE. However, if the connection is not established due to firewall restrictions, the far-end establishes the TCP connection. All the known attributes, such as floor-control, conf-id, user-id, and floor-id are also relayed in SDP.

SDP Offer and Answer exchange rules

Participants and the floor control server use the SDP offer and Answer exchange rules to establish and authenticate the BFCP connection. Avaya SBCE does not play any role in connection establishment or reestablishment and authentication.

Avaya SBCE negotiates offer and Answer SDP for BFCP based on the following rules:

- Avaya SBCE receives an offer on the incoming leg with the setup attribute as actpass or active. Avaya SBCE answers with the setup attribute as passive with a valid port parameter in the BFCP application line.

- Avaya SBCE sends an offer with the setup attribute as passive on the outgoing leg. The far-end entity answers with the setup attribute as active with the discarded port parameter in the BFCP application line.
- Avaya SBCE receives an offer on the incoming leg with the setup attribute as passive.Avaya SBCE answers with the setup attribute as active with a valid port parameter in the BFCP application line. Avaya SBCE tries to start the TCP connection as indicated by the setup attribute as active. The far-end entity starts the TCP connection on the same connection after time out.
- Avaya SBCE receives an offer with the connection attribute as new. Avaya SBCE answers with a connection attribute as new.
- Avaya SBCE receives an offer with the connection attribute as existing. Avaya SBCE answers with a connection attribute as existing.
- Avaya SBCE starts an offer on the outgoing leg with the connection attribute as new for all cases.

Avaya SBCE relays other BFCP application attributes such as floor-ctrl, label, floorid, confid, and userid. Avaya SBCE negotiates these attribute parameters for the end-to-end connection.

Architecture of Binary Floor Control Protocol

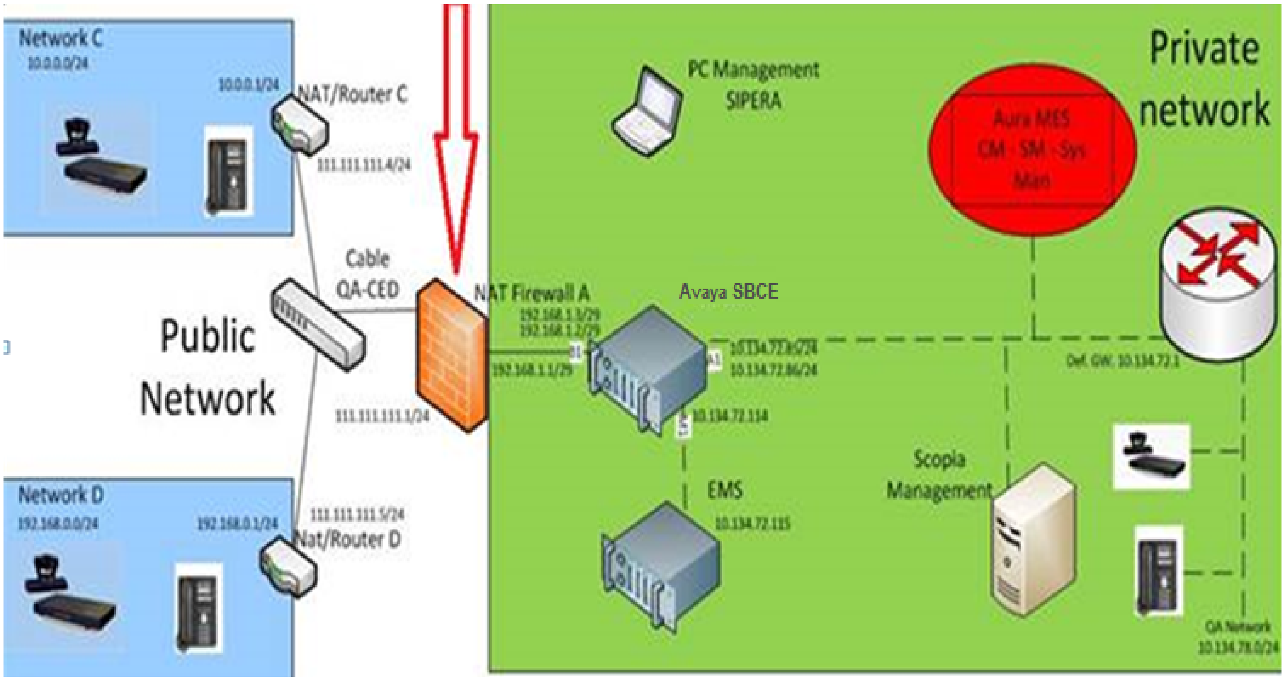


Figure 9: BFCP architecture

An internal firewall exists in most installations on the A1 interface, which is the private interface towards the enterprise. The diagram shows an external firewall on the B1 interface.

Binary Floor Control Protocol scenarios

Examples of scenarios in which BFCP is used and the offer and answer messages for each scenario.

Remote Worker XT-client calls XT-MCU

Sr No	Sender	Floor-ctrl	Setup attribute	Connection	BFCP application line
1	Remote Worker XT-client	c-only	actpass	new	Valid connection and port
2	Avaya SBCE	c-only	passive	new	Valid connection and port
3	XT-MCU	s-only	active	new	Discarded port. For example, 9
4	Avaya SBCE (responds to Remote Worker XT-client)	s-only	passive	new	Valid connection and port

The same parameters are exchanged when a Remote Worker XT-client calls Elite-MCU.

Remote Worker XT-MCU calls internal XT-client

Sr No	Sender	floor-ctrl	setup attribute	connection	BFCP application line
1	Remote Worker XT-MCU	c-s	actpass	new	Valid connection and port
2	Avaya SBCE	c-s	passive	new	Valid connection and port
3	XT-client	c-only	active	new	Discarded port
4	Avaya SBCE	c-only	passive	new	Valid connection and port

XT-MCU internal to enterprise dials out and calls XT-client, which is a remote worker

Sr. no	Sender	floor-ctrl	setup attribute	connection	BFCP application line
1	XT-MCU	c-s	actpass	new	Valid connection and port
2	Avaya SBCE	c-only	passive	new	Valid connection and port
3	Remote worker XT-client	c-only	active	new	Discarded port

Table continues…

Sr. no	Sender	floor-ctrl	setup attribute	connection	BFCP application line
4	Avaya SBCE responds to XT-MCU	c-only	passive	new	Valid connection and port

Elite-MCU Release 8.3 internal to enterprise dials out and calls XT-Client which is remote worker

Sr No.	Sender	floor-ctrl	setup attribute	connection	BFCP application line
1	Elite-MCU	s-only	passive	new	Valid connection and port
2	Avaya SBCE	s-only	passive	new	Valid connection and port
3	Remote worker XT-client	c-only	active	new	Discarded port
4	Avaya SBCE responds to Elite MCU	c-only	active	new	Valid connection and port

After Avaya SBCE responds to Elite MCU, Avaya SBCE does not start any TCP connection towards Elite MCU 8.3. Elite MCU 8.3 times out and tries to establish a TCP connection.

Failover or network outage

In a failover or network outage, an entity tries to reestablish a TCP connection on the existing connection. If the entity fails, Avaya Scopia® does not set up the connection again.

Forward Error Correction

Video over IP requires high bandwidth. Transmission of video data over unreliable communication channels might result in packet loss and error. Forward Error Correction (FEC) is a mechanism to control packet loss and errors in data transmission over the IP network. The sender encodes the messages in a redundant way by using the error-correcting code. The redundancy feature enables the receiver to detect errors and correct the errors without retransmission. This mechanism is useful when communication is one way and has multiple receivers.

The FEC mechanism uses the FEC schemes defined in RFC 5445, the FEC building block defined in RFC 5052, and the SDP signaling defined in RFC 5109. Avaya Scopia® uses the proprietary SDP signaling and FEC building blocks and schemes, which are not compatible with the IETF standard.

FEC detects errors and protects the principal video but does not protect the data for audio channels. FEC is also applicable for H264/SVC video codecs.

User registration

You can view the list of users that are registered through Avaya SBCE in the **Registrations State** column on the User Registrations page. You can also enter custom search criteria for the fields that are displayed on the system.

Real Time SIP Server Status

Avaya SBCE Release 6.3 onwards, you can view the current status of the configured SIP servers. The EMS server displays the connectivity status for trunk servers and enterprise call servers. You can use the **Server Status** option of the **Status** toolbar to view the status of the connection. The Server Status screen displays the list of servers based on the settings on the Server Configuration screen.

For the servers to show up in the Status window, you must configure server heartbeat in Server Configuration.

Licensing requirements

Avaya SBCE uses WebLM version 8.0.0.0 for licensing requirements. You can install the Avaya SBCE license file on Element Management System (EMS) using the Device Management page. Ensure that the license file of the WebLM server displays the product code Session Border Controller E AE. Before you configure the license file, you can view the **License State**, **Grace Period State**, and **Grace Period Expiration Date** fields on the Dashboard page. You have a 30-day grace period from the day of installation or upgrade to install the license. Avaya SBCE works normally during the grace period.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

  The primary host ID of WebLM is used for creating the license file.
- Licensed features
- Licensed capacity

All hardware Avaya SBCE devices can use a local WebLM server for licenses. However, for mixed deployment environments with EMS on VMware and Avaya SBCE on hardware, use a WebLM server installed on VMware or System Manager WebLM.

Avaya SBCE supports pooled licensing. As opposed to static license allocation, Avaya SBCE dynamically reserves and unreserves pooled licenses when needed. For example, customers with multiple Avaya SBCE devices can use a pool of licenses dynamically across the devices as required.

Single Sign-On and Identity Engine

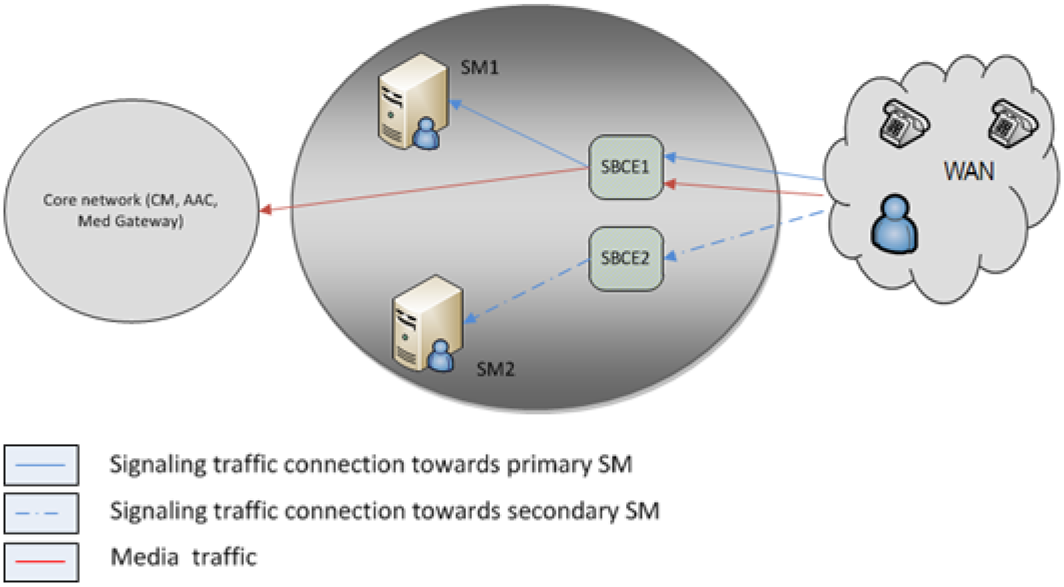
Avaya SBCE uses split DNS for the Single Sign-On and Identity Engine feature. In a split DNS infrastructure, internal hosts are directed to an internal domain name server for name resolution. Internal hosts resolve the IDE domain to an IDE server address. External hosts are directed to an external domain name server for name resolution. External hosts resolve the IDE domain to an Avaya SBCE external address.

Geographic-redundant deployment

In a Geographic-redundant deployment, you can deploy two different Avaya SBCE devices in two different data centers. You can deploy the devices as individual Avaya SBCE devices or devices managed by their own EMS. You can deploy these Avaya SBCE devices in a High Availability mode or a non-High Availability mode.

Geographic-redundant deployment in the non-HA mode

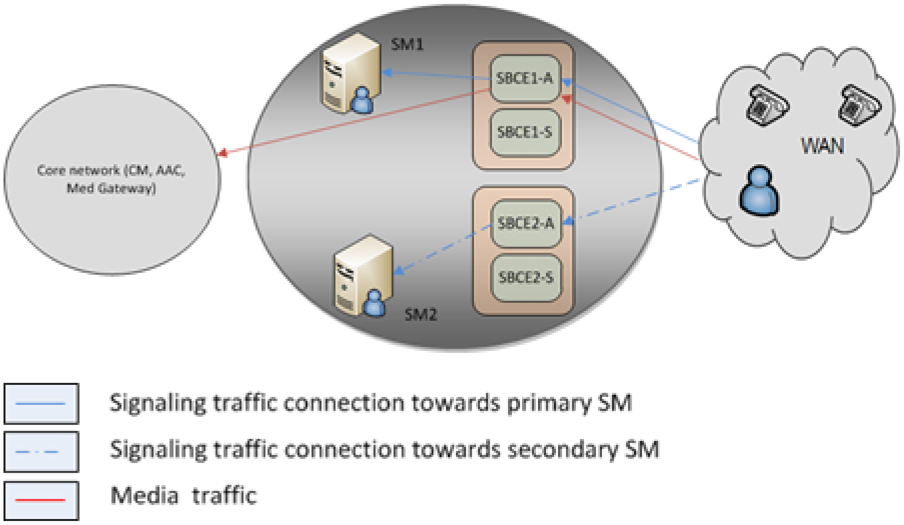
In the following diagram, SBCE1 and SBCE2 are two different physical devices deployed in different data centers. The endpoints have one connection with SBCE1 corresponding to the primary Session Manager, SM1. The second connection with SBCE2 corresponds to the secondary Session Manager, SM2.


SM1
Core network (CM, AAC, Med Gateway)
SBCE1
SBCE2
WAN
SM2
Signaling traffic connection towards primary SM
Signaling traffic connection towards secondary SM
Media traffic

Geographic-redundant deployment in the HA mode

In the following diagram, SBCE1 and SBCE2 are two different physical devices that are deployed in an HA mode in different data centers. The endpoints have one connection with SBCE1-A, that is Active SBCE corresponding to the primary Session Manager, SM1. The second connection is with SBCE2-A, Active SBCE corresponding to the secondary Session Manager, SM2.

During an SBCE1-A fail over, SBCE1-S, which is the standby Avaya SBCE, handles the media of the active calls. During an SBCE2-A fail over, SBCE2-S, which is the standby Avaya SBCE, handles the media of the active calls.


SM1
SBCE1-A
SBCE1-S
Core network (CM, AAC, Med Gateway)
WAN
SBCE2-A
SBCE2-S
SM2
Signaling traffic connection towards primary SM
Signaling traffic connection towards secondary SM
Media traffic

WebRTC-enabled call handling

Avaya SBCE supports incoming calls from WebRTC-enabled web browsers to an internal Avaya Aura® network with SIP at the core. For example, a consumer can call an Avaya Aura® network by using a WebRTC-enabled browser from an external network. This WebRTC call is possible if the organization discloses the organization website to real-time multimedia calls and enables the browser with APIs for real-time multimedia communication. The signaling and media traverse the border edge of the enterprise network that contains the firewall and Avaya SBCE in DMZ. In this scenario, Avaya SBCE, Avaya Breeze® platform, and Avaya Aura® Media Server together function as the WebRTC-SIP gateway. The signaling and media must traverse the border edge of the enterprise network. Avaya SBCE relays HTTP signaling by using the Reverse Proxy feature and the media relay by using TURN Server relay functionality. Additionally, for a WebRTC call, STUN binding, STUN reflexive address discovery, and ICE connectivity checks are required. All these aspects are implemented within the TURN/STUN server functionality built into Avaya SBCE.

A WebRTC-enabled browser supports symmetric NAT and multiple IP addresses.

Avaya SBCE supports TURN using SEND or DATA indication and TURN signaling on TCP, TLS and UDP.

For information about WebRTC performance and capacity, see *Avaya WebRTC Snap-in Reference*.

Virtualization overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture.

Using Avaya Aura® Virtualized Environment, customers with a VMware IT infrastructure can upgrade to the next release level of collaboration using their own VMware infrastructure. For customers who need to add more capacity or application interfaces, Avaya Aura® applications on VMware offer flexible solutions for expansion. For customers who want to migrate to the latest collaboration solutions, Avaya Aura® Virtualized Environment provides a hardware-efficient simplified solution for upgrading to the latest Avaya Aura® release and adding the latest Avaya Aura® capabilities.

For deployment on VMware-certified hardware, Avaya SBCE is packaged as vAppliance ready Open Virtualization Environment(OVA) to run in the virtualized environment. Avaya SBCE is also available for VMware-based deployments.

You can deploy EMS and Avaya SBCE using a single OVA file.

Avaya SBCE supports VMware features, such as vMotion, HA across data centers, and mixed hardware configurations.

The Avaya SBCE OVA files are offered as vAppliance for EMS and Avaya SBCE configurations. The .ova file is available in Product Licensing and Delivery System (PLDS).

Virtual LAN

A Virtual Local Area Network (VLAN) is a logical group of network elements, such as workstations, servers, and network devices spanning various physical networks. A VLAN overlays a virtual layer-2 network on top of a physical layer-2 network by inserting a VLAN tag in the layer-2 header of a packet. VLAN-aware network devices, such as switches, can send packets through the VLAN overlay.

Tag a VLAN to distinctly identify the VLAN as part of a logically different layer-2 network.

The first step for VLAN tagging is to create a VLAN interface. The packets leaving and entering Avaya SBCE on a VLAN use a physical link connected to a physical interface.

The second step is to configure all networks to which Avaya SBCE connects. Each network to which Avaya SBCE connects is defined and attached to an interface.

Note:

A VLAN is supported on data and signaling interface.

SRTP overview

Avaya SBCE supports encrypted audio and multiple video media such as main video, video presentation, and Far End Camera Control (FECC) based on SDP capability negotiation.

If the far-end entity does not support SRTP encryption, Avaya SBCE converts one leg of the call as RTP and the other leg as SRTP by using the SDP negotiation. The conversion between the originating and terminating legs depends on the cipher policy administered on Avaya SBCE.

Avaya SBCE does not use Master Key Index (MKI) and encrypted RTCP for Avaya Scopia® interoperability. Avaya SBCE negotiates the SDP session by using unencrypted RTCP.

✱ **Note:**

Avaya SBCE supports SRTP calls over SIP, but Avaya Aura® supports SRTP calls only when the call uses the TLS protocol.

SRTP considerations

Avaya SBCE supports:

1. Fallback from SRTP to RTP due to bandwidth limitation or change in call toplogy, such as a media server not supporting SRTP and application of music-on-hold.
2. Upgrade from RTP to SRTP.
3. Conversion from RTP to SRTP between the originating and terminating legs after failover.
4. Modification of keys using REINVITE.
5. Fallback from RTP to SRTP after failover.

Multiple subnet and multiple interfaces

Multiple subnets

With Avaya SBCE, customers can connect to multiple subnets from a single interface. Avaya SBCE supports multiple IP addresses for each subnet and a unique next hop gateway for each IP address. Therefore, you can have multiple subnets on the same interface. The interface can be a physical or a VLAN interface.

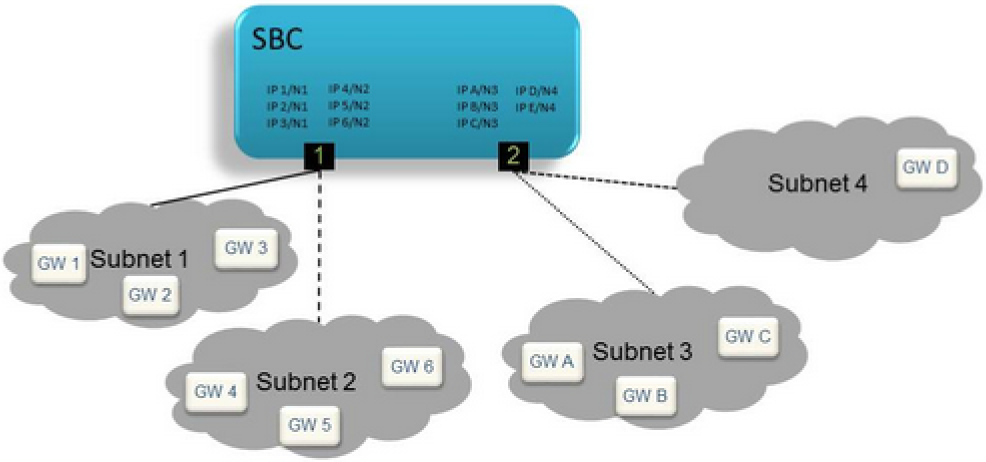


Figure 10: Connectivity to multiple subnets on a single data interface

In Figure 10: Connectivity to multiple subnets on a single data interface on page 46, subnets 1 and 2 are reachable through interface 1, while subnets 3 and 4 are reachable through interface 2.

Overlapping address spaces

You can use multiple subnets to configure cloud-based deployments and multitenancy. In such configurations, Avaya SBCE connects to two or more physically distinct networks that share some or all the IP address space. When you configure overlapped address spaces, multiple endpoints with the same IP address might simultaneously connect toAvaya SBCE. However, Avaya SBCE can distinguish between the connections. Although multiple endpoints use the same IP address, the networks in which the endpoints reside are physically distinct. Avaya SBCE connects to the physically distinct networks by using unique IP addresses in each overlapped address space.

VLAN support

With the virtual LAN (VLAN) capability, a virtual layer-2 network can overlay on a physical layer-2 network by inserting a VLAN tag in the layer-2 header of the packet. Supported network devices can switch such packets through the VLAN overlay. In this release, Avaya SBCE supports VLANs only on the data interfaces.

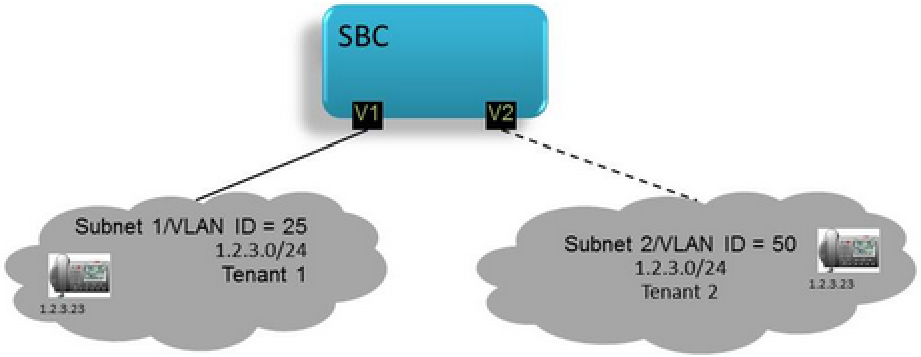


Figure 11: VLAN support

Deployment examples

Avaya SBCE connected to multiple subnets on a single interface

In this scenario, Avaya SBCE connects to multiple subnets on the same data interface.

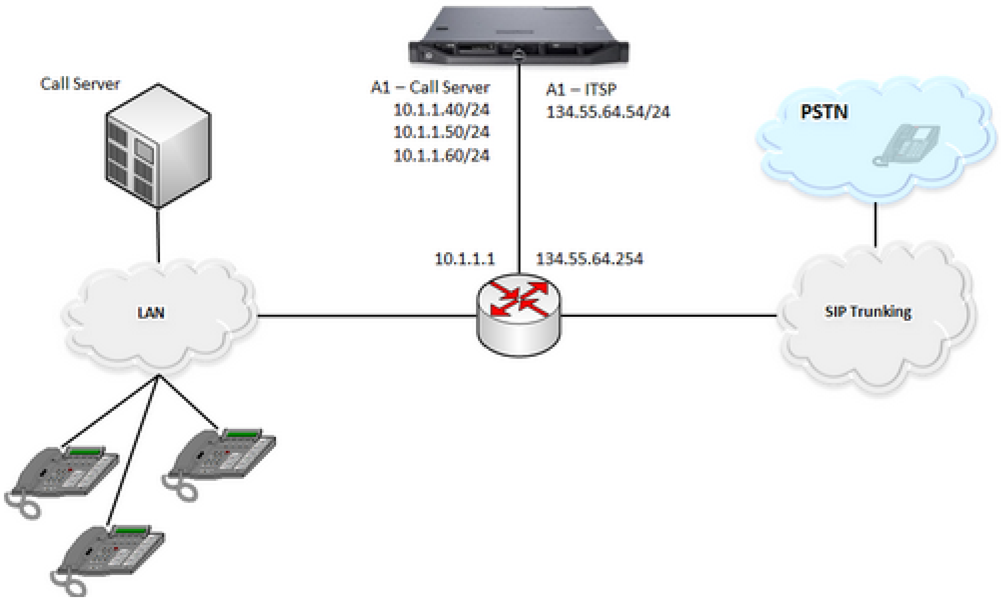


Figure 12: Avaya SBCE connected to multiple subnets on a single interface

Configuration details

- **Interfaces and purposes**: This configuration uses only the A1 Avaya SBCE data interface. With the help of the next-hop router, this data interface provides connectivity to two different networks: the call server network and the ITSP network. This configuration uses three Avaya SBCE IP addresses: two for the call server network and one for the ITSP network.

- **Surrounding networking equipment**: This configuration uses the next-hop router to support multiple gateway addresses on the same physical network connection.
- **Network interfaces**: In this scenario, A1 is enabled. A2, B1, and B2 remain disabled. Enable only one data interface.
- **Networks connected to Avaya SBCE**: In this configuration, two networks are added to the same Avaya SBCE interface. Click the **Networks** tab in **Network & Flows** > **Network Management**. Define the call server network first and then define the ITSP network. Thus, to configure multiple networks on the same Avaya SBCE data interface, add the networks to the same interface when you define the networks.

Avaya SBCE connected to multiple subnets on two interfaces

In this scenario, Avaya SBCE connects to a call server on one interface and a trunk server on another.

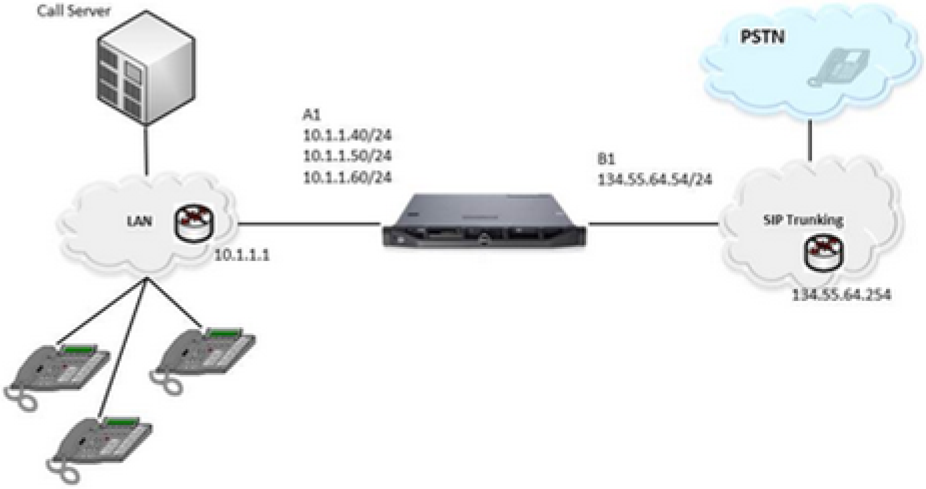


Figure 13: Avaya SBCE connected to multiple subnets on two data interfaces

Configuration details

- **Avaya SBCE interfaces**: This configuration uses four IP addresses: three on the A1 interface and one on the B1 interface.
- **Surrounding networking equipment**: The next-hop routers on both data interfaces do not need to support multiple Avaya SBCE subnets or VLAN tagging.
- **Avaya SBCE network interfaces**: This scenario uses the A1 and B1 interfaces. Ensure that you configure the required interfaces.
- **Networks connected to Avaya SBCE**: In this example, Avaya SBCE connects to two data networks through the A1 and B1 interfaces. Each configured IP address can use a unique next-hop router, if necessary, or the default gateway. Define each network that connects to Avaya SBCE. Use the **Networks** tab in **Network & Flows** > **Network Management** to define the network.

- **Other Avaya SBCE setup**: To configure media and signaling interfaces, flows, and routing profiles, see the related sections.

Avaya SBCE connected to multiple subnets by using a single VLAN

In this scenario, Avaya SBCE connects to a combination of VLAN and non-VLAN networks by using a single data interface.

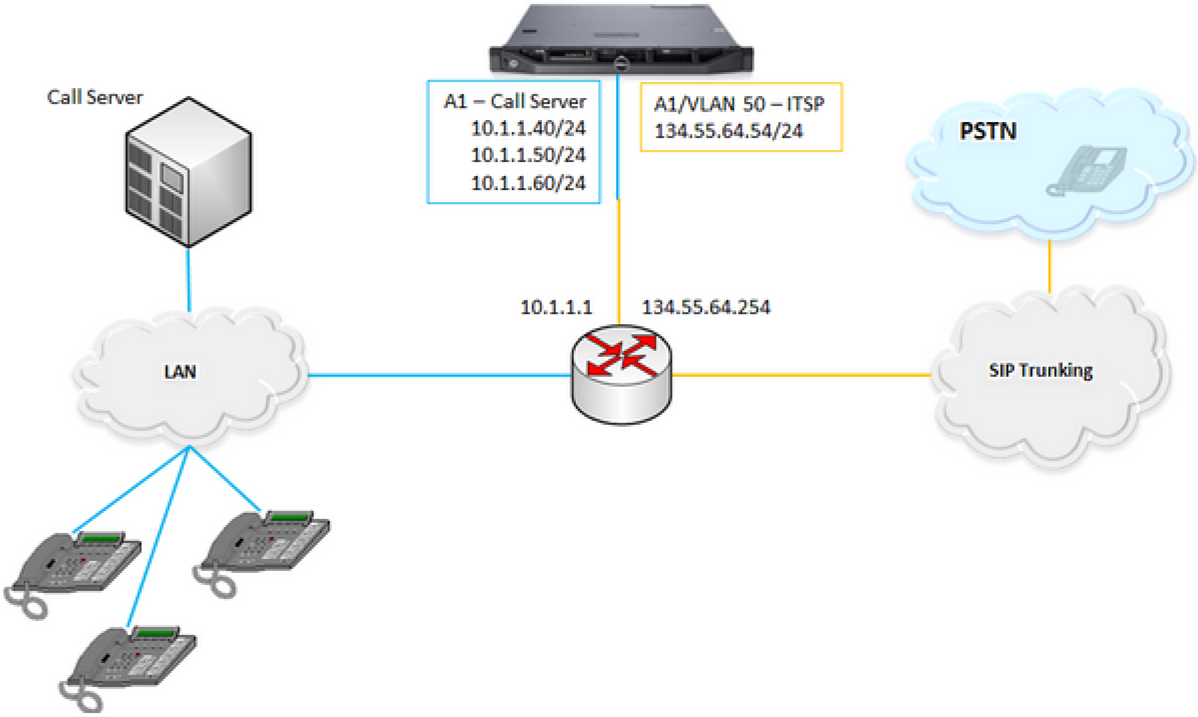


Figure 14: Avaya SBCE connected to multiple subnets, using a single VLAN and a single data interface

Configuration details

- **Interfaces and purposes**: In this scenario, only the A1 Avaya SBCE data interface is used. This data interface provides connectivity to two different networks with the help of the next-hop router: the call server network and the ITSP network. Additionally, one of the networks, the ITSP network, is on a VLAN. Three Avaya SBCE IP addresses are required for the call server network, one VLAN interface on the A1 physical interface, and one Avaya SBCE IP address on the ITSP network.
- **Surrounding networking equipment**: In this example, the next-hop router is configured to support two gateway IP addresses and one VLAN on the same physical port.
- **Network interfaces**: The ITSP network requires VLAN tagging. The ITSP network uses VLAN ID (VID) 50. Packets leaving Avaya SBCE on the ITSP network must contain a VID of 50. To enable VLAN tagging, create a VLAN interface. VLAN interfaces on Avaya SBCE use the underlying facilities of a physical interface A1, A2, B1, or B2. Packets leaving and entering Avaya SBCE on VLAN use the physical link connected to the associated physical interface. Define VLAN interface to connect Avaya SBCE to the ITSP network. Use the **Add VLAN** button located in the **Network & Flows** > **Network Management Interfaces** tab.

Initially, keep the VLAN interface disabled. Then enable both the A1 and ITSP VLAN interfaces while other interfaces remain disabled.

- **Networks connected to Avaya SBCE**: In this example, the ITSP network connects to the VLAN interface on top of the physical A1 interface. Define the call server network in the same way as in other multiple subnet scenarios. Define the ITSP network and use the new VLAN interface.

Multiple gateways on the same network

This configuration includes two gateway routers and two call servers connected to the call server network. In this configuration, only the second gateway can route calls to the second call server.

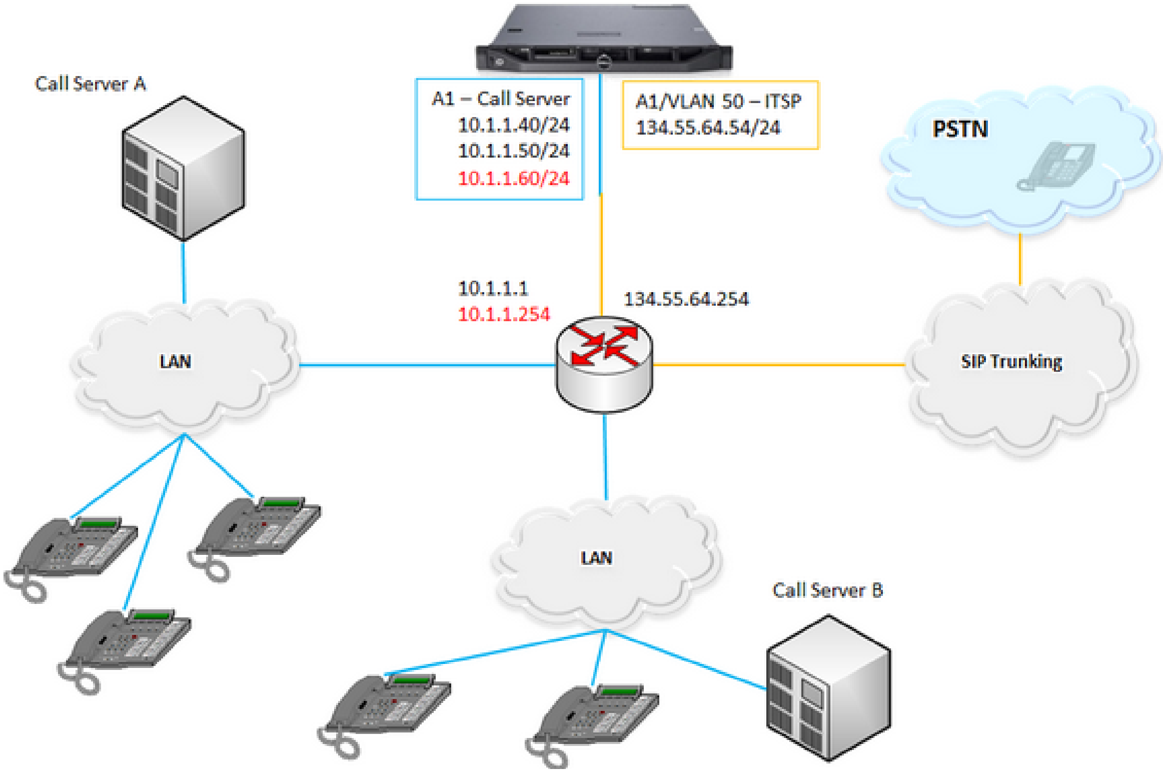


Figure 15: Multiple gateways on the same network

Configuration details

- **Interfaces and purposes**: Only one Avaya SBCE interface connects to both, the call server and ITSP networks. Because the call server network has multiple gateway routers , one of the Avaya SBCE IP addresses on that network provides call routing capabilities to call server B.
- **Surrounding networking equipment**: The next-hop router supports three gateway IP addresses and one VLAN on the same physical port. Two gateway IP addresses are on the call server network, and one is on the ITSP network. The 10.1.1.1 gateway address is the default gateway on the call server network. Additionally, Avaya SBCE uses the 10.1.1.254

gateway to reach call server B, as the default gateway in this example is unable to reach the network.

- **SBC Network Interfaces**: The configuration of the call server and ITSP network interfaces is the same as in the earlier scenarios.
- **Networks connected to Avaya SBCE**: The ITSP network configuration is the same as in the earlier examples. For each attached network, define a default gateway router. Each Avaya SBCE IP address on the network can override the default gateway IP address, if necessary. For example, Avaya SBCE uses 10.1.1.254 as the next-hop router instead of 10.1.1.1.

traceSBC tool

The tcpdump tool is the main troubleshooting tool of Avaya SBCE, which can capture network traffic. Using tcpdump is a reliable way to analyze the information arriving to and sent from Avaya SBCE. However, tcpdump has its own limitations, which can make troubleshooting difficult and time consuming. This traditional tool is not useful in handling encrypted traffic and real-time troubleshooting.

SIP and PPM traffic is encrypted especially in Remote Worker configurations. Checking encrypted traffic with a network capture is difficult and time consuming. The delay occurs because the unencrypted private key of the Avaya SBCE is needed to decrypt the TLS and HTTPS traffic.

The traceSBC tool offers solutions for both issues. traceSBC is a perl script that parses Avaya SBCE log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, you can use the tool easily even in case of TLS and HTTPS. traceSBC can parse the log files downloaded from Avaya SBCE. traceSBC can also process log files real time on Avaya SBCE, so that you can check SIP and PPM traffic during live calls. The tool can also work in the noninteractive mode, which is useful for automation.

SIP and PPM logging administration

SIP logging is always enabled by default. You can enable PPM, STUN, TLS, and AMS logging, if required.

Log files

Avaya SBCE can log SIP messages as processed by different subsystems and also log PPM messages. The traceSBC utility can process the log files real-time by opening the latest log files in the given directories. traceSBC also checks regularly if a new file is generated, in which case the old one is closed and processing continues with the new one. A new log file is generated every time the relevant processes restart, or when the size reaches the limit of ~10 M.

Log locations:

SIP messages are found at `/archive/log/tracesbc/tracesbc_sip/` and PPM messages can be found at `/archive/log/tracesbc/tracesbc_ppm/`.

Active files are of the following format:

```
-rw-rw---- 1 root root 112445 Aug 21 10:12 tracesbc_sip_1408631651
```

Inactive or closed files are of the following format:

```
-rw-rw---- 1 root root 175236 Aug 21 06:33
tracesbc_sip_1408617250_1408620820_1
```

or

```
-rw-rw---- 1 root root 31706 Jul 10 13:34
tracesbc_sip_1436549674_1436553270_1.gz
```

Advantages

Memory

After 10000 captured messages, traceSBC stops processing the log files to prevent exhausting the memory. This check is done during the capture when the tool is parsing the log files. The tool counts the number of SIP and PPM messages in the logs. This number is not the number of messages sent or received on the interfaces. This counter is a summary of messages from all logs, not for each log. Note that this safeguard is present only for real-time mode. When the tool is used in nonreal-time mode, this counter does not stop processing the logs specified in the command line. The counter continues processing the logs specified in the command line to be able to process more files or messages in off-line mode.

Processor

A built-in mechanism is available to prevent high CPU usage. Throttling is not tied to CPU level. In the current implementation, throttling is done by releasing the CPU for a short period after each line of the file is processed. The result is that CPU occupancy is low on an idle system when the tool actively processes large log files. You can disable throttling by the –dt command line parameter which can be useful when processing large log files offline. However, in this case CPU occupancy might go up to 100%, and so you must not use this option on a live system.

Avaya SBCE support for Serviceability Agent

Avaya SBCE contains Serviceability Agent which monitors faults on the system. Serviceability Agent sends SNMPv2c and SNMPv3 notifications to configured destinations through the net-SNMP master agent.

With the support for Serviceability Agent, you can use Avaya SBCE to:

- Manage SNMPv3 users.
- Manage SNMP trap destinations.
- Create, edit, and view SNMP trap profiles.

To ensure that you can view Avaya SBCE alarms on System Manager, you must upload the common alarm definitions file (cadf) to System Manager. For more information about uploading the cadf file, see *Administering Avaya Session Border Controller for Enterprise*.

Multi-tenancy

Avaya SBCE achieves multi-tenancy using multiple tenants, call servers, and Avaya SBCE interfaces.

This scenario uses all four Avaya SBCE data interfaces. Avaya SBCE connects to two tenant networks, each with a unique set of remote workers. Avaya SBCE also connects to three other networks, each with a call server. Each call server is reached through a separate physical interface, which provides a measure of redundancy when one or more call servers stop responding.

Configuration example 1 : Multi-tenancy using multiple tenants, call servers, and Avaya SBCE interfaces

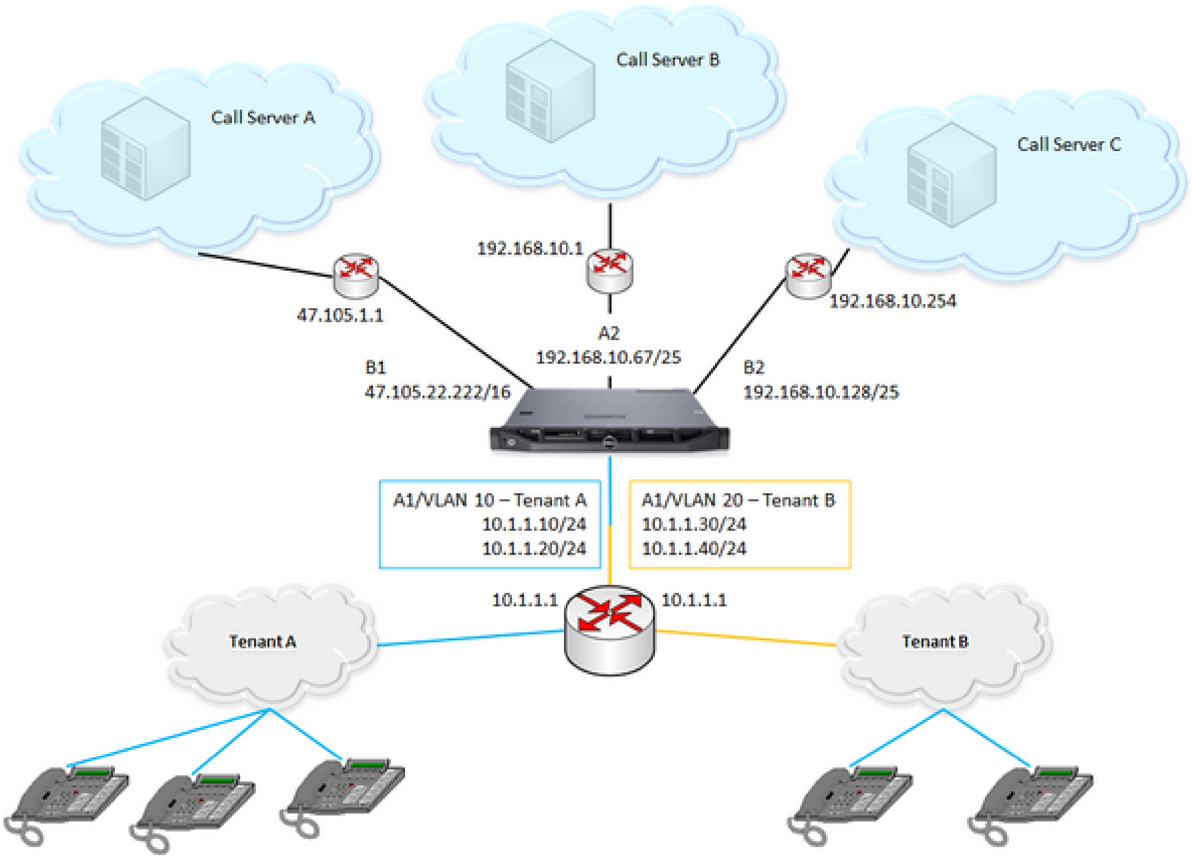


Figure 16: Multiple tenants, call servers, and Avaya SBCE interfaces

- **Interfaces and purposes**: The A1 interface of Avaya SBCE provides connectivity to tenant subnets. Each subnet uses a unique VLAN tag: tenant A (in blue) is on VLAN 10, while tenant B (in orange) uses VLAN 20. The gateway router on the A1 interface provides connectivity to both tenant VLANs.

  The B1 interface provides connectivity to call server A, A2 connects Avaya SBCE to call server B, and B2 connects the network containing call server C.

  Note:

  You can attach tenants to the B1 interface and connect call server A through the A1 interface. The physical ports retain their historical names: A1, A2, B1, and B2.
- **Surrounding networking equipment**: This configuration supports corresponding mapping between SBC NICs and physical server NICs. Configure the gateway on the A1 interface to support VLAN 10 and VLAN 20, and the associated gateway IP addresses. You do not need

to configure the other three gateways on A2, B1, or B2 separately. If Avaya SBCE is running on a virtual machine, configure VMWare vSwitch and the physical interfaces on the server. If each physical interface on Avaya SBCE uses a separate vSwitch and each vSwitch connects to a separate physical interface on the server, connect vSwitch to a physical port setup. Configure up to four vSwitches.

- **Avaya SBCE Network interfaces**: When you configure VLANs on Avaya SBCE, the first step is always to create the VLAN interfaces. In this example, two VLAN interfaces are created to support the two tenant networks. First, the VLAN for tenant A on interface A1. Then, the VLAN for tenant B on A1. The remaining networks use physical interfaces on Avaya SBCE. Finally, enable all the interfaces: the two VLANs as well as A2, B1, and B2.
- **Networks connected to Avaya SBCE**: In this example, Avaya SBCE is attached to five networks. For each attached network, define a default gateway router, beginning with tenant A, followed by tenant B, call server A, call server B, and finally call server C.

Configuration Example 2 : Multi-tenancy using the same IP address

Avaya SBCE supports the use of the same IP address on multiple data interfaces in Avaya SBCE. Customers often share the same address space and service IP address while using multitenant and cloud features. With support for using the same IP address more than one time, more than one customer can use the same IP address to connect to Avaya SBCE.

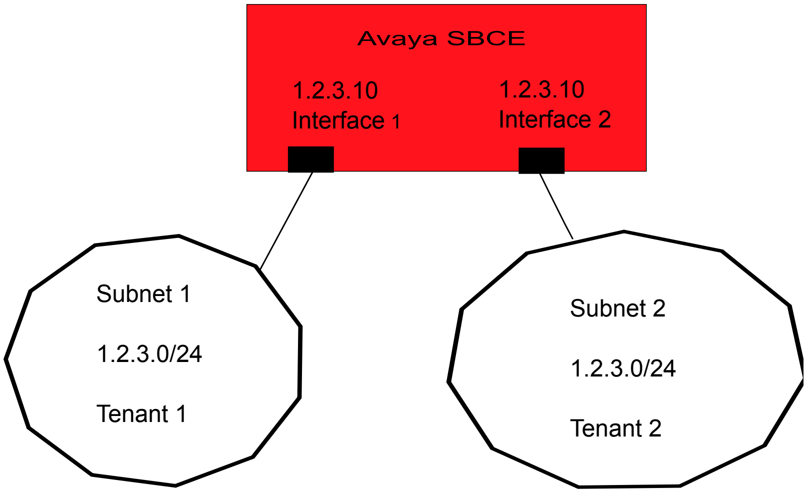


Figure 17: Same IP address used on different interfaces

To permit the use of multiple instances of the same IP, the instances must exist on separate network interfaces, virtual network interfaces, or both. Avaya SBCE separates interface definition from network definition as follows:

- An interface is a combination of a physical port such as A1, A2, B1, and B2, and a vlan ID. A vlan ID can be **no vlan**.
- A network ties a set of Avaya SBCE IPs and gateways with an interface.

Therefore, for two instances of 1.2.3.0 on Avaya SBCE, you must define two interfaces and two networks, so that 1.2.3.0 occurs exactly once within each network.

In this scenario, Avaya SBCE connects to two tenant networks, each with a unique set of remote workers. However, the same IP address is assigned on Avaya SBCE on both the tenant networks.

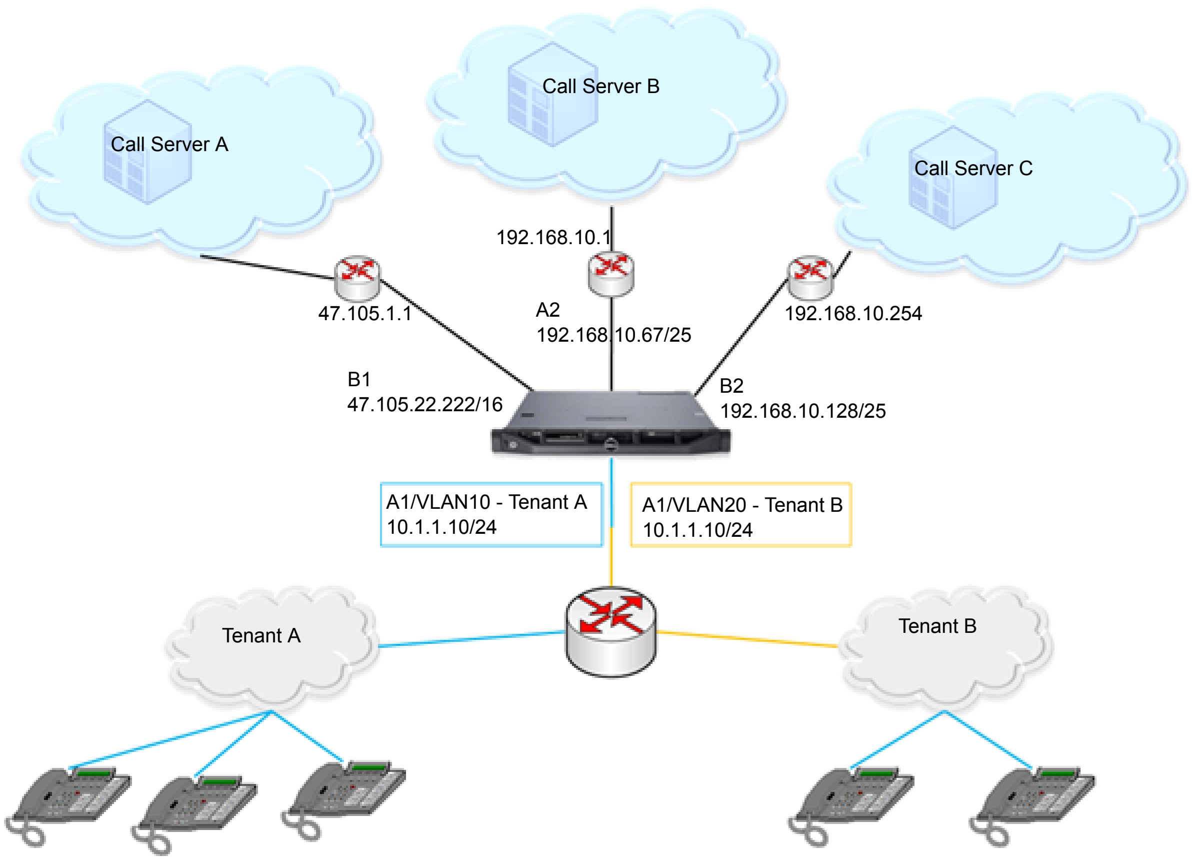


Figure 18: Multiple tenants using the same IP address

The following sections describe the configuration details for this deployment example.

Interfaces and purposes:

The A1 interface of Avaya SBCE provides connectivity to tenant subnets. Each subnet uses a unique VLAN tag: tenant A, highlighted in blue, is on VLAN 10, while tenant B, highlighted in orange, uses VLAN 20. The gateway router on the A1 interface provides connectivity to both tenant VLANs.

The B1 interface provides connectivity to call server A, A2 connects Avaya SBCE to call server B, and B2 connects the network containing call server C.

Surrounding networking equipment:

Configure the gateway on the A1 interface to support VLAN 10 and VLAN 20, and the associated gateway IP addresses. As the Avaya SBCE address on both tenants is the same, the gateway must be able to distinguish between the addresses for both tenant networks.

Network interfaces:

To use the same IP address on Avaya SBCE multiple times, select the **Allow Non-unique IPs for Complex Networks** field on the Network Options page. To configure VLANs on Avaya SBCE, create VLAN interfaces. In this example, two VLAN interfaces are created to support the two tenant networks:

- The VLAN for tenant A on interface A1
- The VLAN for tenant B on A1

The remaining networks use physical interfaces on Avaya SBCE. Finally, enable all the interfaces: the two VLANs as well as A2, B1, and B2.

In this example, the Avaya SBCE is attached to five networks. For each attached network, define a default gateway router and Avaya SBCE IP addresses. Begin with tenant A, followed by tenant B, call server A, call server B, and finally call server C.

Support for IP Office trunk from a dynamic IP address

Avaya SBCE supports an IP Office trunk originating from dynamic IP addresses. The external address of the ISP router or firewall at the remote site is based on Dynamic Host Configuration Protocol (DHCP). Therefore, a static external IP address is unavailable for configuration or installation.

Instead, in the server configuration for Remote Branch Office servers, you can administer an FQDN pointing to a Dynamic DNS record. If the TLS connection from the Remote Branch Office drops, Avaya SBCE resolves the FQDN entry again for all Remote Branch Office servers. If the DNS record TTL value expires, Avaya SBCE queries the DNS for all FQDN entries in the server configuration.

Note:

If a DNS lookup fails, Avaya SBCE tries the DNS lookup every 30 seconds for the first 10 failures and then every 3000 seconds.

Reuse of connection established by IP Office for delivering calls

Avaya SBCE reuses the TLS connection from IP Office for SIP signaling towards the IP Office. The routing profile towards the Remote Branch Office must use a routing entry that matches the server configuration for the Remote Branch Office. For Remote Branch Office routing entries, the transport must be TLS and the **Port** field must be empty.

Avaya SBCE rejects the incoming TLS connection from IP Office if the:

- Required TLS Client Certificate is not configured in IP Office.
- Self-Signed Certificate is presented by IP Office during TLS handshake.
- Peer Verification fails in Avaya SBCE with the TLS Client Certificate presented by IP Office.

If the TLS connection from the Remote Branch Office drops, Avaya SBCE rejects calls originating from the enterprise until the connection is reestablished. Meanwhile, Avaya SBCE displays a 500 server internal error message.

Note:

You can provide custom route entries with the IP Office listen port if you administer DNAT rules in the Firewall or the NAT router.

Secure Client Enablement Services proxy

Client Enablement Services (CES) provides access to many Avaya Unified Communications (UC) capabilities, including telephony, mobility, messaging, conferencing, and Presence Services through a single application. Avaya one-X® Mobile communicates with the CES server by using the CES protocol. To provide CES services to Avaya one-X® Mobile clients outside the enterprise network, Avaya SBCE provides a secure proxy that must be deployed in the enterprise DMZ. Avaya SBCE checks all traffic from Avaya one-X® Mobile clients outside the enterprise network to the CES server.

When a new connection is established from an Avaya one-X® Mobile outside the enterprise network:

- Avaya SBCE checks whether the first message from the Avaya one-X® Mobile device is a login request and forwards the message to the CES server. Avaya SBCE drops all messages received from the Avaya one-X® Mobile device before the login request.
- The CES server authenticates Avaya one-X® Mobile or sends an error message to Avaya SBCE. After authentication failure, Avaya SBCE rejects all subsequent messages from the Avaya one-X® Mobile.
- After authentication, Avaya SBCE forwards all messages from Avaya one-X® Mobile to the CES server.

Avaya SBCE maintains statistics for all login attempts. Avaya SBCE supports at least 10,000 Avaya one-X® Mobile clients on Dell R630 and HP DL360 G9.

Support for integrated Dell Remote Access Card and integrated Lights-Out

Dell Remote Access Controller (DRAC) and HP integrated Lights-Out (iLO) are management tools. These tools provide powerful remote server management features, including control to remotely turn a server on or off. You can use DRAC features to troubleshoot and diagnose issues during a remote server restart. Avaya SBCE supports the following features of the iDRAC Express Card:

- System Provisioning: You can install Avaya SBCE ISO by using iDRAC provisioning features.
- System monitoring and management: You can monitor the status of the server by using iDRAC features.

You can buy the iDRAC card with or without the server. For Dell servers later than the 600 series, the iDRAC express card is part of the base configuration. For these servers, you need not install, back up, or manage another license for the iDRAC express card. However, to upgrade from the express version to the enterprise version, you must buy another license directly from Dell. Similarly, to upgrade from iLO 3 to iLO 4, you must purchase another license from HP.

For more information about installing and using iDRAC, go to http://www.support.dell.com/ and see *Integrated Dell Remote Access Controller User's Guide*.

Supported hardware platforms

Avaya SBCE supports Dell iDRAC and HP iLO on the following platforms:

Platform	iDRAC and iLO support
Portwell CAD 0208	Does not support iDRAC and iLO.
Dell R210 II and R210 II XL	Does not support iDRAC.
Dell R320	Does not support iDRAC.
Dell R620	Does not support iDRAC.
Dell R630	Supports iDRAC 8 express.
HP DL360 G8	Does not support iLO.
HP DL360 G9	Supports iLO 4.

Important:

Dell R210 II and Dell R320 servers do not support iDRAC interfaces, therefore these servers do not support iDRAC.

Previous generation servers have cipher 0 vulnerabilities. Therefore, do not use iDRAC and iLO when iDRAC and iLO are not included with the platform.

SIPREC-based recording solution

Avaya SBCE supports a SIP-based media recording (SIPREC) solution with the following components:

- Avaya SBCE as the SIP Recording Client (SRC)
- Avaya Contact Recorder as the SIP Recording Server (SRS)
- Application Enablement Services for CTI integration
- Contact Center Application Servers such as Avaya Aura® Contact Center and Call Center Elite
- Media anchor points such as Avaya Aura® Media Server or Communication Manager Media Gateway

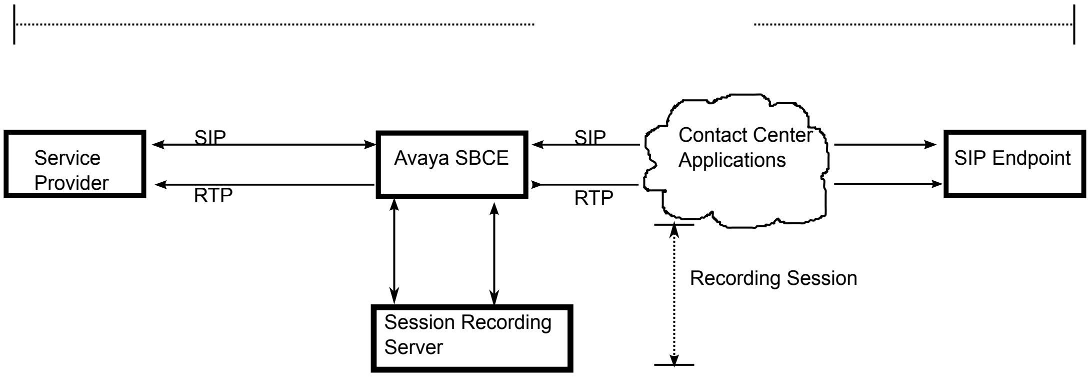


Figure 19: SIPREC-based recording solution architecture

With the SIPREC-based recording solution, Avaya SBCE supports full-time session recording, selective recording, and continuous recording. With full-time session recording, every communication session connected by using Avaya SBCE is recorded.

The recording servers can be colocated with the Avaya SBCE or distributed in different locations. If the SRS and Avaya SBCE are at different locations, ensure that the network does not require Network Address Translation between the SRS and Avaya SBCE devices. You must deploy the Avaya SBCE and Recording Server in a trusted, secured network for privacy and security of the recorded media.

You must have a SIP trunk on Avaya SBCE to ensure that SIPREC functions correctly.

Features for session recording

The following Avaya SBCE features support the recording solution:

- Initiation, modification, and termination of recording session from the SIP Recording Server (SRS) during the recording session.
- Early media clipping avoidance during session setup.
- Wave file played to indicate that the session is being recorded.
- Alternate routing for recording sessions with Round Robin load balancing.

  When a recording session starts, Avaya SBCE starts a timer. When the timer expires, Avaya SBCE triggers alternate routing mechanisms. Avaya SBCE also uses alternate routing mechanisms after receiving the following messages from the recording server: 408,480,486,488, 500, and 503.
- High Availability for the recorder media stream and metadata sent to the Recording Servers.
- Recording Server routing.

  Avaya SBCE communicates with a cluster of Recording Servers. You must administer a URL for each Recording Server in the cluster. Avaya SBCE sends an INVITE message to the Recording Server. When Avaya SBCE sends the Contact URI with the feature tag +sip.src in the INVITE message to the SRS, the SRS identifies a recording session.
- Metadata elements to identify media streams from SRC and SRS.

  Avaya SBCE provides the following metadata elements:

Metadata element	Supporting parameter
Call identifier	UCID
Session Identifier	sdp session id
Participant Identifier	PAI
Stream Identifier	Label on media stream
Stream direction	send, recv and inactive
Timestamp for resynchronization	NA

- No controls from the trunk side of the recording sessions.

  Avaya SBCE uses only the controls specified from Avaya SBCE and at the recording server.
- Unique labels for media streams to identify the media stream for participants in the recording session.
- Security options.

  Avaya SBCE supports an SAVP profile for SRTP sessions and an AVP profile for RTP sessions. Avaya SBCE supports TLS and TCP connection. ACR supports TCP connection with SIP uri scheme using RTP/AVP and SAVP profile.

  Note:

  For SIPREC, Avaya SBCE supports SRTP only with hmac80, because ACR does not support any other cryptographic algorithm.
- REFER handling and redirection supported in recording scenarios.
- SIP recording in translator mode. Avaya SBCE receives media streams and relays them to the Recording Server. Avaya SBCE does not change any data in the media streams.

In addition, Avaya SBCE provides the following features:

- Support for full-time, selective, and continuous recording.
- Support for call termination on recording failure.

  When Avaya SBCE initiates a session towards every configured recording server, there can be scenarios when none of the servers respond. In such scenarios, Avaya SBCE can terminate the session that is initiated or in progress towards the calling or called party. Call termination on recording failure is not supported for remote worker calls.
- Support for recording a remote worker to remote worker call.
- Support for recording in case of downstream forking.

  If Avaya SBCE received multiple forked dialogs, the first dialog received with early media is recorded. Subsequent early media in forked dialogs is not recorded. For final answer, the media stream between the calling and final answered party is recorded.

Selective recording

For selective recording, media is streamed continuously, similar to full-time recording. However, the recording server masks recorded streams until the system detects Computer Telephony

Integration (CTI) events. Therefore, only a portion of the communication session is recorded when the Recording Server cuts through the media stream after receiving CTI events.

With selective recording, bandwidth and processing cycles are conserved because media streams do not flow through the network when recording is not required.

Continuous recording

Avaya SBCE supports continuous recording if the standby recording server has information about the current state of the active recording server. If the active recording server fails, the standby recording server continues recording the communication session. The recording server requests Avaya SBCE to stream the media and metadata for that communication session to the active recording server.

End-to-end secure indication

Avaya endpoints can display an end-to-end secure indicator for calls that use secure protocols for both halves of the call. Avaya SBCE provides a **Securable** field on the Server Configuration page to indicate whether the server is securable. Avaya SBCE uses the **Securable** field to determine whether the trunk and call server can use secure protocols, and sets appropriate values for the Av-Secure-Indication header.

The Av-Secure-Indicator header in the outgoing INVITE message is set to secured when the following conditions are met:

- The trunk server and call server are securable.
- The incoming and outgoing links use TLS and have a secure Audio-Visual Profile (SAVP) or transaction capabilities application part (tcap) messages with an SAVP profile.
- System Manager sends the Av-Secure-Indication header as secured.

Avaya SBCE sets the Av-Secure-Indication header to unsecured when:

- Any condition required for setting the Av-Secure-Indication header to secured is not met.
- The Answer message has an AVP profile.

Subsequent messages such as Update without SDP, PRACK without SDP, and ACK must keep the secure indication value from the response of the previous request.

To make the Trunk server unsecured, the corresponding trunk link with Session Manager must also be unsecured.

Note:

Avaya SBCE depends on Avaya Aura® 7.0 to support the end-to-end secure indication feature. Avaya Aura® 7.0 makes this feature available to users.

Media encryption by using AES-256

Advanced Encryption Standard (AES) is a widely used specification for data encryption. Avaya SBCE supports media encryption by using AES-256.

The AES standards describe a symmetric key algorithm. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Though AES-128 is adequately secure, highly security conscious users might adopt AES-192 or AES-256. To provision this feature, Avaya SBCE supports the following crypto suites:

- AES_256_CM_HMAC_SHA1_32
- AES_256_CM_HMAC_SHA1_80

The following options are available in the **Preferred Format#1**, **Preferred Format#2**, and **Preferred Format#3** fields on the Media Rule page:

- SRTP_AES_CM_256_HMAC_SHA1_32
- SRTP_AES_CM_256_HMAC_SHA1_80

Transcoding

Transcoding translates a media stream encoded by using one codec into a media codec encoded by using another codec. Avaya SBCE performs transcoding when the inbound and outbound entities have incompatible codecs. The Session Description Protocol (SDP) offer contains information about the codecs that the device sending the message prefers. The device that receives the message responds to the SDP offer by using the set of codecs that the receiving device supports.

To enable the transcoding feature, you must go to **Network & Flows** > **Advanced Options**, click the **Feature Control** tab, and select the **Transcoding** check box.

By providing transcoding, Avaya SBCE:

- Optimizes bandwidth availability by enforcing the use of different compression codecs.
- Normalizes traffic in the network to a single codec.
- Reduces the usage of multimedia resource function processors and media gateways to support a large number of codecs.

Avaya SBCE supports audio transcoding and transcoding for trunk deployments. All transcoded calls are anchored to Avaya SBCE. Fax transcoding is not supported. If a call has both audio and video m lines, Avaya SBCE only transcodes the audio. Video calls that require transcoding are converted to audio calls.

Supported transcoding capacities

Server name	Maximum transcoded sessions	Maximum non-transcoded sessions
Dell R210–II XL	100	5000
HP DL360 G8	200	6000
Dell R620	200	6000
Dell R320	200	6000
Dell R630	1000	10000
HP DL360 G9	1000	10000

These capacities vary from codec to codec because, depending on the codec algorithm, the processing CPU cycles differ for each media stream. The estimated capacities are with G711 and G729 codecs and are based on the 180 sec hold/talk time.

Codecs supported for transcoding

The following codecs are supported for transcoding:

- PCMU
- PCMA
- G722
- G729
- G729AB
- G726–32
- OPUS Constrained Narrow Band
- OPUS Narrow Band
- OPUS Wide Band

Support for IPv6 addresses

Avaya SBCE supports IPv6 addresses to SIP trunk servers. To support the transition to IPv6, Avaya SBCE uses dual stack nodes that run both IPv4 and IPv6. Avaya SBCE supports trunk deployments with IPv4 only to the enterprise, and IPv6, dual stack, or IPv4 only towards the trunk or public network.

Avaya SBCE supports the following deployment scenarios:

- Public (untrusted) network: IPv6-only, Dual stack, Mixed mode
- Private/Enterprise (trusted) network: IPv4-only

Avaya SBCE supports:

- IPv6 unique local unicast address and IPv6 global unicast address.
- IPv6 communication with entities such as SIP servers, SIP endpoints, DNS servers, NTP server, syslog server, and Avaya Aura® Media Server.

Note:

If the DNS response has both IPv4 and IPv6 addresses, Avaya SBCE relies on configuration policies to determine the address types to be tried.

- IPv6 communication with EMS.

Avaya SBCE supports:

- IPv6 communication with SIP recording server.
- IPv6 in remote worker deployments.

Avaya SBCE supports the following features over IPv6:

- High availability (HA)
- Access to EMS web interface
- Time synchronization with the configured NTP server
- SIP trunking

Avaya SBCE supports Alternate Network Address Types (ANAT) semantics for SDP to permit alternate network addresses for media streams. ANAT semantics are useful in environments with both IPv4 and IPv6 hosts. When Avaya SBCE receives an SDP offer with ANAT semantics, Avaya SBCE:

- Determines whether the enterprise network uses only IPv4.
- Strips media line grouping and sends only the IPv4 address in the m line if the enterprise network uses IPv4.
- Picks an m line based on ANAT preference configuration and sets the port to 0 in other m lines.

SIP entities that generate an SDP offer with ANAT semantics place the sdp-anat-option-tag in the **Require header** field. Avaya SBCE supports the sdp-anat-option tag. Avaya SBCE supports UDP/RTP, TCP/RTP, TLS/SRTP, and other transport combinations in IPv6-only, dual stack, and mixed mode networks.

If you have an environment with both IPv4 and IPv6 hosts, you must go to **Domain Policies** > **Media Rules**, and select **ANAT Enabled**. For more information, see *Administering Avaya Session Border Controller for Enterprise*.

Edge Server for Converged Conference solution

The Converged Conference solution uses the features of Avaya Scopia® V8.5 and Avaya Aura® Conferencing to provide a converged conferencing and web collaboration solution in a unified architecture.

In the converged conference solution, Avaya SBCE:

- Acts as an Edge Server for the set of converged clients. The Edge Server enables the clients to access enterprise video infrastructure remotely across firewalls that block media ports.

- Provides firewall traversal for SIP, HTTP, and WebRTC devices and tunnels media where the firewall blocks media ports. Avaya SBCE allows streams to come in through known ports for TLS/TCP.
- Makes video federation calls across companies possible. These calls can be across video endpoints between two enterprises that are behind a SIP Gateway or an SBC, and connected by a SIP trunk.
- Facilitates unregistered guest users to dial in to a video conference or dial out from a video conference.

The Converged Conference solution comprises the following:

- Converged Application Server: The components that are colocated on the same server or distributed based on deployment topology and scale. The components include a management application, conference focus, SIP back-to-back user agent, H.323 Gatekeeper, and a Unified User Portal.
- Web Service Gateway (WSGW): The HTTP to SIP Gateway for WebRTC and HTTP clients.
- Web Collaboration Server: Avaya Aura® Conferencing leveraged for real time Web Collaboration.
- Converged Media Server: Software-based media processing for transcoding and composition of video, high scale audio, and WebRTC audio/video support. The server uses the Avaya Scopia® Elite Multipoint Control Unit (MCU) framework. You can also use traditional Elite MCU with hardware accelerator blades as an alternative.
- Converged clients: New set of audio/video clients including Meet Me clients, WebRTC-based Thin Clients such as Simple WebRTC Chat (SWC), Avaya Equinox®, and Scopia XT series of clients.
- Edge Server: Avaya SBCE, Path finder (H.323), and Avaya Scopia® Desktop Server. Avaya SBCE provides Session Border Controller functionality for SIP calls, BFCP/FECC for XT series, reverse proxy functionality for HTTP, and TURN/STUN for WebRTC. Avaya Scopia® Desktop Server is required for handling signaling and media for legacy Avaya Scopia® desktop mobile phones.
- Common management infrastructure for all components and devices.
- Conference recording and a content management system using WildCat.

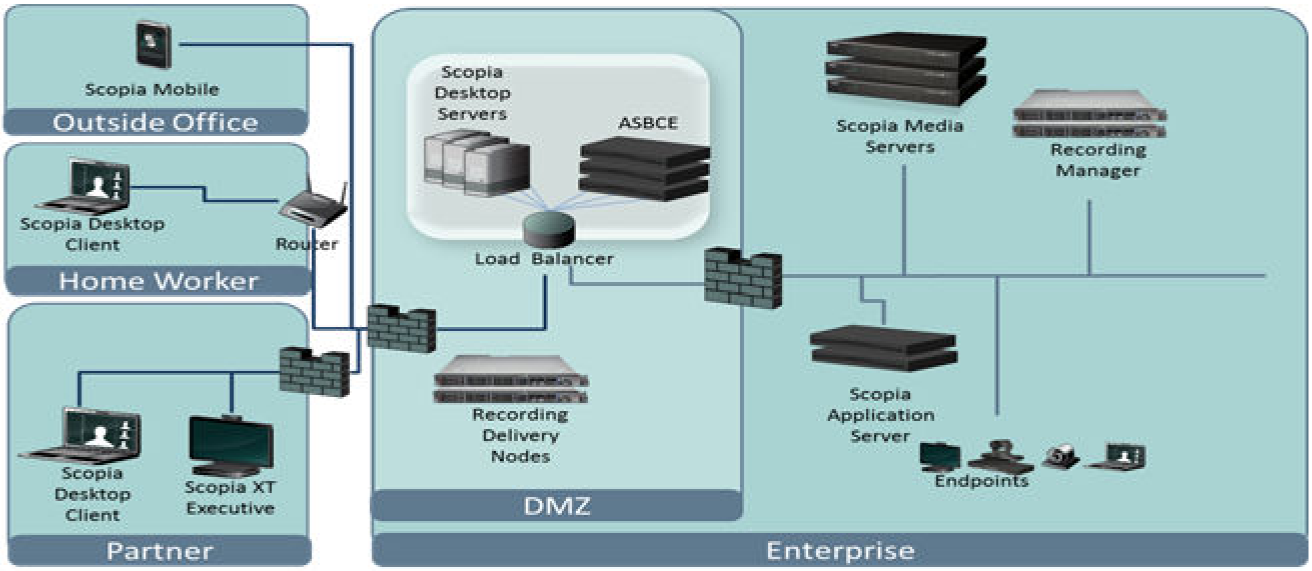


Figure 20: Components of Converged Conference solution with Avaya SBCE as an edge server

The solution supports Avaya Aura®, IP Office, and cloud deployment from small to large distributed deployment, and virtualized deployments on cloud environments.

Avaya SBCE features for the Converged Conference solution

For the Converged Conference solution, Avaya SBCE supports the following:

- TURN/STUN control signaling and media relay UDP for WebRTC with symmetric NATing.
- TURN/STUN over TCP for WebRTC.
- Multiplexing and demultiplexing RTP/RTCP or SRTP/SRTCP on TCP or TLS.
- Relaying media through TURN relay using TCP end-to-end without converting to UDP for the TURN relay.
- Load balancing for TURN.
- Sending the status of devices to Avaya Scopia® management and load balancers.
- Calculating bandwidth for all audio/video sessions. Avaya SBCE provides this input to iVIEW load balancer for effective load balancing.
- Detecting DoS and rate limit the http or https signaling request from remote connections.
- Rewriting URL based on redirection.
- Click to conference for unregistered users. The endpoints can call through Avaya SBCE to Avaya Scopia® MCU without being registered to the authorized domain. For dialed out calls, the FQDN is resolved and DNS priority transport is selected as TLS or TCP.

  For this feature to work, the following configuration changes are required:

  - Create a click to call flow.

- For dialed-out scenarios, configure a valid DNS server or client on Avaya SBCE. Ensure that the receive interface of the click to call flow matches the signaling interface of the inbound flow selected.

ENUM support

Avaya SBCE supports the E.164 Number Mapping (ENUM) protocol. Telephone numbers in the PSTN are organized by using the format specified in the E.164 standard. Conversely, the Internet uses the Domain Name System (DNS) to link domain names to IP addresses. ENUM defines a method to convert a telephone number into a format that can be used with the DNS to look up addressing information such as Uniform Resource Identifiers (URIs). Numbers that conform to the numbering plan defined in E.164 are:

- Limited to 15 digits.
- Prefixed with a plus sign (+) to indicate that the number includes an international country calling code.

ENUM translates E.164 numbers to URIs by using Naming Authority Pointer (NAPTR) records stored in DNS. With ENUM, calls can be completed over the Internet instead of transferring the call to PSTN. Therefore, ENUM provides cost savings for businesses that communicate with other enterprises by using SIP. If the number is unavailable in the ENUM database, Avaya SBCE routes the call to the service provider to send the call to the PSTN.

Process for converting the E.164 number

When a user dials an E.164 number, ENUM constructs an Application Unique String (AUS) from the number by removing all non-digit characters except the plus sign (+). For example, for the dialed number +44-207-946-0148, the AUS is +442079460148.

The AUS is then converted to an initial key, which is a Fully Qualified Domain Name (FQDN), by using the following steps:

1. Remove the leading plus sign (+) from the AUS.
2. Reverse the order of digits and insert dots between the digits. For example, the number 442079460148 is changed to 8.4.1.0.6.4.9.7.0.2.4.4.
3. Append the string .e164.arpa to change the number to a domain name. For example, 8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa.

The domain name is then used to request NAPTR records. The NAPTR records might contain the end result or the NAPTR records generate a new key to request further NAPTR records from the DNS. At the end of this process, a SIP URI is generated, that Avaya SBCE uses to update the request URI, and proceeds with the routing. If a routing entry is not configured in the corresponding routing profile, Avaya SBCE uses this URI to determine the destination.

Call preservation

With the Call preservation feature, the dialog context of the SIP user agent can survive a Session Manager failure even when the Session Manager context is lost. The dialog continues with end-to-end signaling of the intact user agent, through an alternate Session Manager. The Call preservation feature is available only for SIP Routing Element (SRE) flows.

For Call preservation, a Session Manager Failover Group comprising a pair of Session Manager servers is associated with peer entities. The peer entities, such as Avaya SBCE, use enhanced SIP timing and recovery techniques to provide signaling path continuity during Session Manager failure. When Avaya SBCE detects that a Session Manager is unreachable, Avaya SBCE routes the SIP traffic through the alternate Session Manager by using the Failover Group Domain Name (FGDN) in the Session Manager Via and Record-route headers. The FGDN is a fully qualified domain name (FQDN) that resolves to an ordered set of Session Manager servers within a Session Manager Failover Group that provides a high availability SRE service. When the preferred Session Manager becomes unresponsive, the peer SIP entity uses the Session Manager Failover Group Domain resolution to identify and communicate with the alternate Session Manager.

The naming convention for the failover group is as follows:

- Failover group name: *Primary SM-Secondary SM*

  For example, sm1–sm2.
- Primary FGDN: *Primary SM-Secondary SM.sip domain*

  For example, sm1–sm2.example.com.
- Secondary FGDN: *Primary SM-Secondary SM-Identifier.sip domain*

  For example, sm1–sm2–2.example.com.
- Session Manager FQDN: *SM.SM IP Domain*

  For example, sm1.example.com.

The Session Manager failover group can contain two or more Session Manager member instances. The primary Session Manager carries the traffic for the failover group in normal conditions. For more information about administering the Call Preservation feature, see *Call Preservation Feature Description and Administration Guide*.

To support the call preservation feature, Avaya SBCE:

- Maintains an affinity to the last preferred Session Manager in the failover group for every dialog.
- Preserves the failover group target set in the dialog context. This caching in the dialog prevents unnecessary duplicate DNS queries.
- Supports requests with an FGDN in the Via, Next Hop Route, or Record-Route headers.
- Resets the TCP or TLS socket to the failed Session Manager if Avaya SBCE detects that the preferred Session Manager is unreachable.

- Supports Call Preservation only on TCP and TLS transport types.
- Changes the dialog-scoped affinity to the preferred Session Manager only when the preferred Session Manager instance becomes unreachable. Avaya SBCE reevaluates the affinity by selecting one of the following:
    - The alternate Avaya SBCE with highest priority
    - The alternate Session Manager with highest priority, excluding any alternate Session Manager instances in the FG that are already unavailable.
- Detects that a Session Manager is back in service and reachable within the interval configured in the **Frequency** field on the Server Configuration page in the **Heartbeat** tab.

  ! **Important:**

  Heartbeat configuration is mandatory for the Call preservation feature. The heartbeat is used to detect the restored Session Manager.

  Supports provisional response reliability with a 100 rel message and sends PRACK to all received provisional responses.

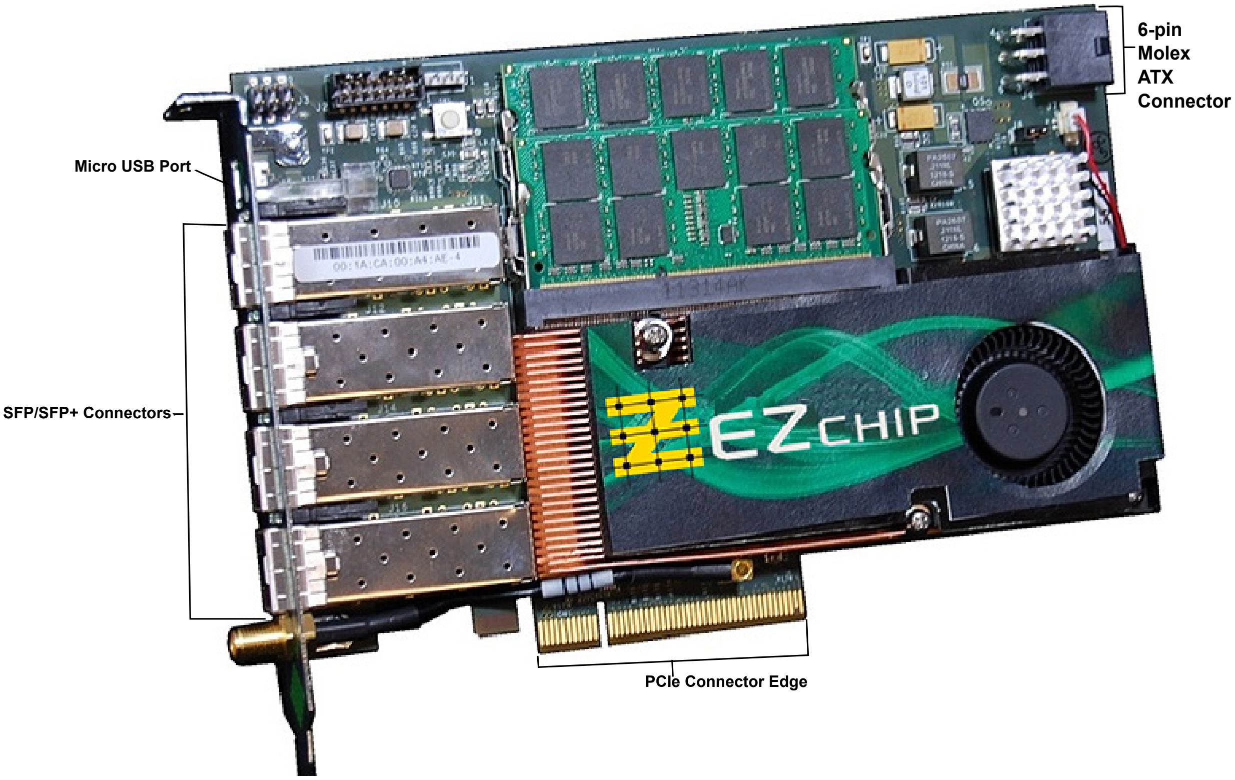
Support for TILEncore-Gx36 Intelligent Application Adapter

For every session, Avaya SBCE supports signaling and media packets. The number of media packets is significantly higher than the signaling packets. When the number of sessions on the Avaya SBCE increases, the CPU available to process media packets can dominate the host server, even before all network bandwidth is occupied. Increasing the amount of CPU available for media packet processing or dataplane processing helps Avaya SBCE support more simultaneous sessions. The TILEncore-Gx36 Intelligent Application Adapter significantly increases the number of data plane cores at lower costs without requiring a larger server.

TILEncore-Gx36 Intelligent Application Adapter overview

TILEncore-Gx36 is a full-height, half-length, single-slot PCIe card comprising a TILEncore-Gx 36-core processor, on-board memory, and other components for packet processing. The adapter requires a single PCIe slot in the host. The adapter functions as a coprocessor within Avaya SBCE. The dataplane software on Avaya SBCE runs on the adapter, and all other software runs on the host server.

This adapter is supported only in HP DL360 G9 and Dell R630.



TILEncore-Gx36 features

Feature	Description
TILE-Gx8036 Processor	Provides a 36-core (tile) Gx8036 processor, with each tile running at 1.2 GHz. Wire-speed packet classification and load-balancing engine that performs initial packet inspection, parsing, and distribution to tiles. Two separate cryptographic engines capable of up to 40 Gbps of throughput.
Network Connectivity	Provides four physical SFP/SFP+ ports. You can configure every port as either 1 Gbps or 10 Gbps Ethernet.
Adapter/Host Interface	Operates under host-based software control. Functions as a standard Network Interface Controller (NIC) for packets such as SIP signaling packets, which the card does not process on board. Supports Message Signaled Interrupts (MSI and MSI-X), with which Receive Side Scaling (RSS) can be used on the host.
Memory	Provides 8 GB or 16 GB DDR3 (DDR3-1600) memory.
Virtualization	Supports Single-Root I/O Virtualization (SR-IOV) with which multiple guest operating systems on a single host server can share the adapter.
Power and Thermal	Can be powered either through the PCIe connector or the ATX power connector. Requires 65 W from the PCIe fingers when powered by using PCIe.

Table continues…

Feature	Description
	Airflow requirements vary between 100 and 400 lfm, depending on the internal configuration of the server.
Ports	Provides four physical network ports, a micro-USB port, and several status indicators on the rear panel of the Gx adapter.
Console connectivity	Provides on-board UART that can be used for a serial connection. Micro-USB connection which supports console connectivity is available on the rear panel of the board. PCIe bus can be used to connect to the adapter over a virtual Ethernet link.
DIP Switches	Provides DIP switches located behind the card that can be used to modify: • Whether the board can boot through the UART and USB interfaces. • PCIe x4 or x8 lane operation. • PCIe operational mode (root complex, endpoint, or auto). • Edge connector power usage. • PCIe reference clock source for host or local.
Supported Servers	Can be hosted on HP DL360 G9 and Dell R630 servers in Avaya SBCE Release 7.1.
Capacity increase	Provides capacity gains of up to 20000 simultaneous sessions for Avaya SBCE with TILEncore-Gx36 Adapter.
High Availability	Supports high availability for homogenous server pairs. In homogenous HA pairs, the Avaya SBCEs are the same type, both HP DL360 G9 or both R630, and either both Gx-enabled, or both server-only.
IPv6	Supports IPv6 addresses for Avaya SBCE with TILEncore-Gx36 Adapter.
Media transcoding	Supports media transcoding by using Avaya Aura® Media Server for Avaya SBCE with TILEncore-Gx36 Adapter.

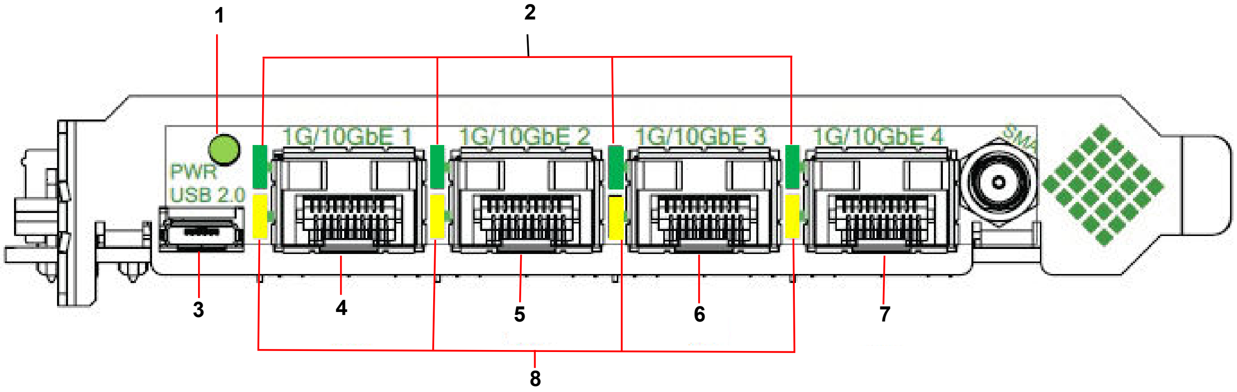
Configuration of TILEncore-Gx36 Adapter installed in Avaya SBCE

- Four 1Gbps SFP transceivers: Avaya SBCE supports maximum 4 Gbps combined bandwidth.
- Boots through the PCIe bus: Adapter software is stored on the disk of the host server. Tools supplied with the Tilera Multicore. Development Environment (MDE) is used to boot the Gx and transfer a bootrom image to the card.
- 8 GB of memory
- Power supplied through the PCIe edge connector: Additional cabling is not required inside the host server chassis.
- Micro-USB serial cable: Avaya SBCEs that use the Gx adapter are shipped with a micro-USB serial cable that can be used to provide console connectivity in the field. The cable is not factory-installed.
- DIP switches: Factory default positions, which provide the necessary configuration that Avaya SBCE requires. For DIP switch specifications, see the Gx36 User Guide.

- Four protected data interfaces on Avaya SBCE: The interfaces are named A1, B1, A2, and B2. The adapter is configured so that these interfaces are arranged, beginning from left, as A1, A2, B1, and B2.

For information about installing the adapter, see the Tilera documentation.

TILEncore-Gx36 Intelligent Application Adapter rear panel



Name	Description
1	Power LED The power LED is lit only when all major board components are powered and functional.
2	Link LEDs The green Link LEDs are lit when the Ethernet link is functional.
3	Micro USB port The micro USB port provides a console connection to the card.
4	B2 network interface This network port operates at 1 Gbps or 10 Gbps depending on the SFP+ type module installed in the port.
5	B1 network interface This network port operates at 1 Gbps or 10 Gbps depending on the SFP+ type module installed in the port.
6	A2 network interface This network port operates at 1 Gbps or 10 Gbps depending on the SFP+ type module installed in the port.
7	A1 network interface This network port operates at 1 Gbps or 10 Gbps depending on the SFP+ type module installed in the port.
8	Activity LEDs

Table continues…

Name	Description
	The yellow activity LEDs are lit when the Avaya SBCE network interfaces are enabled.

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	Processors	System Memory	On-board Storage
Dell R320	Intel® Xeon® E5-2430v2 2.5 GHz, 6 cores–80W	8 GB (DDR4 1600 MT/s UDIMM)	2 x 300 GB 10K SAS
Dell R330	Intel® Xeon® E3-1200v5 3.6 GHz, 4 cores–80W	16 GB (DDR4 2133 MT/s UDIMM)	Up to four 3.5–inch hot-swap HDDs or Up to eight 2.5–inch hot-swap HDDs
Dell R620	Intel® Xeon® E5-2600, Dual core	32 GB (DDR3 1333)	2.5-in SATA 3Gb/s – 7.2K
Dell R630	2 x Intel® Xeon® E5-2640 2.6 GHz, 8 cores–90W	32 GB (DDR4 2133 MT/s RDIMM)	2 x 300 GB 10K SAS
HP DL360 G8	Intel® Xeon® E5-2400	up to 384GB	(8) SFF SAS/SATA/SSD
HP DL360 G9	2 x Intel® Xeon® E5-2640 2.6 GHz, 8 cores–90W	32 GB (DDR4 2133 MT/s RDIMM)	2 x 300 GB 10K SAS
Portwell CAD-0230	Intel® Atom C2000 1.7GHz - Dual Core	2GB (SO-DIMM DDR3 1333MHz)	One 2.5–inch HDD

Note:

Only Dell R210 II XL, Dell R620, Portwell CAD-0208, Portwell CAD-0230, Dell R320, Dell R330, Dell R630, HP DL 360 G8, and HP DL 360 G9 support new installations.

Avaya products

For the latest compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Third-party product requirements

External SAL gateway

When Secure Access Link (SAL) is used for remote access to the Avaya SBCE for Avaya services, the customer must provide a SAL Gateway. Customers can buy the SAL Gateway from Avaya. Customers can also provide the SAL Gateway if the server complies with the SAL requirements specified on the Avaya Support website at http://support.avaya.com. Sometimes, a System Platform integrated SAL Gateway can be used instead of buying another server. See Product Support Notice PSN003058u.

Operating system compatibility

The Avaya SBCE and EMS use RedHat Enterprise Linux 7.x on all platforms.

Chapter 4: Performance specifications

Supported capacity

Server Type	Non-encrypted Sessions with Trunking	Encrypted Remote Worker Users	Encrypted Sessions with Presence	SIPREC with SIP Trunking Replicated Sessions	Scopia Video Sessions	Transcoded Sessions	
	Standard	Advanced		Advanced		Internal	External
Avaya Converged Platform 100 series server with profile 3 (Dell™ PowerEdge™ R640 Server)	14,000	20,000	8,000	6,000	800	1,000	2,500
Avaya Converged Platform 100 series server with profile 5 (Dell™ PowerEdge™ R640 Server)	30,000	20,000	10,000	10,000	800	1,000	5,000
Dell R630 with TILEncore-Gx36 Intelligent Application Adapter	30,000	20,000	7,500	10,000	800	1000	5,000
HP DL360 G9 with TILEncore-Gx36 Intelligent	30,000	20,000	7,500	10,000	800	1000	5,000

Table continues…

Application Adapter							
Dell R630 (High Capacity)	14,000	20,000	7,500	6,000	800	1,000	2,500
HP DL360 G9 (High Capacity)	14,000	20,000	7,500	6,000	800	1,000	2,500
Dell R330 (Mid-Range Capacity)	6,000	5,000	2,000	3,000	200	300	1,250
HP DL360 G9(Mid-Range Capacity)	6,000	5,000	2,000	3,000	200	300	1,250
VMware ESXi 6.x	5,000	6,000	3,000	2,500	200	100	1,250
Portwell CAD 0230	600	500	500	NA	NA	NA	NA
Nutanix	5,000	6,000	3,000	2,500	200	100	1,250

Note:

For the other supported servers which are not listed in the above table, capacity information published in the previous releases apply.

Redundancy and high availability

Redundancy and High Availability (HA) features are available in EMS and Avaya SBCE servers. Hardware that support these features are , Dell R320, Dell R620, Dell R630, Dell R330, HP DL360 G8, and HP DL360 G9 platforms. These features are also available for TILEncore-Gx-enabled servers and Avaya SBCE deployed in a virtualized environment. These features support HA for homogeneous server pairs. In homogenous HA pairs, Avaya SBCE devices are of the same type.

High Availability (HA) support for both media and signaling ensures that Avaya SBCE security functionality is provided continuously, regardless of hardware or software failures. High availability requires minimum two Avaya SBCE devices and one standalone EMS server.

Note:

High availability requires Gratuitous Address Resolution Protocol (GARP) support on the connected network elements. When the primary Avaya SBCE fails over, the secondary Avaya SBCE broadcasts a GARP message to announce that the secondary Avaya SBCE is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBCE IP address. Devices that do not support GARP must be on a different subnet with a GARP-aware router or L3 switch to avoid direct communication. For example, to handle GARP, branch gateways, Medpro, Crossfire, and some PBXs/IVRs must be deployed in a different network from Avaya SBCE, with a router or L3 switch. If you do not put the Avaya SBCE interfaces on a different subnet, after failover, active calls will have a one-way audio. Devices that do not support GARP continue sending calls to the original primary Avaya SBCE.

All IP addresses configured on the Network Configuration screen are shared between both HA devices in HA deployment mode. The HA devices are also configured with private, default IPs that are used to replicate signaling and media data between each other. The configured interfaces are inoperative on the standby or secondary device until the device becomes active or primary. When the devices failover, the active device sends a GARP message to update the ARP tables of the neighboring HA device to begin receiving traffic.

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 or 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 or media interfaces have the same IP address. On failover, the standby Avaya SBCE advertises the new MAC as the L2 address for the common IP address. The Avaya SBCE devices are synchronized through the heartbeat on the dedicated interfaces, and both Avaya SBCE devices are in continuous communication with the Avaya EMS.

On detection of a failure on the active Avaya SBCE, the active SBC network interface ports are automatically disabled. The ports 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.

Note:

EMS is no longer involved for any HA failover. The HA failover is managed by the HA pair.

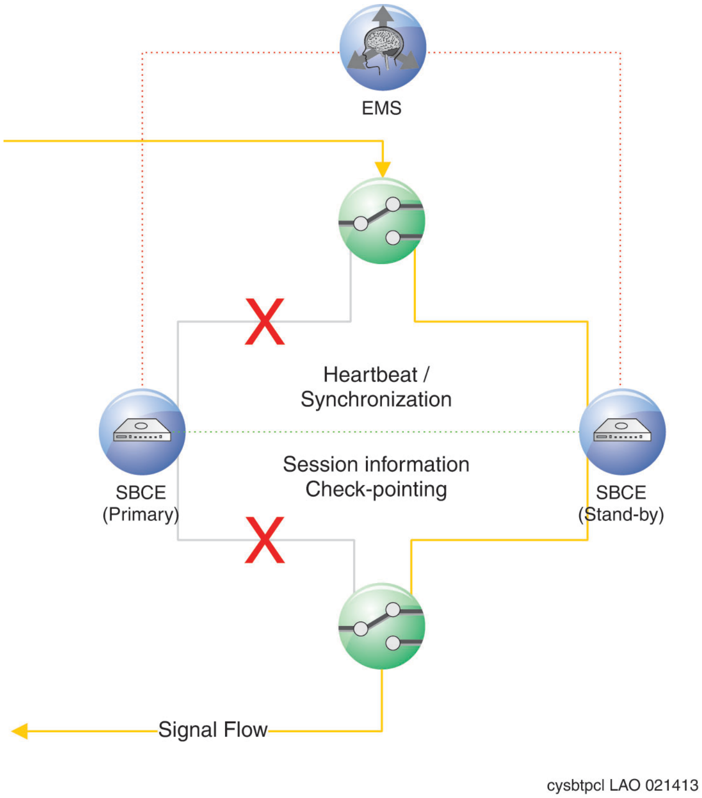


Figure 21: Typical Avaya SBCE HA – Parallel Mode Topology (colocated)

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 be located in the same facility or in different geographic locations.

When one EMS fails, the other EMS is usable without any manual intervention or downtime.

Chapter 5: Environmental requirements

Hardware dimensions

Server	Height	Width	Depth	Weight
Dell PowerEdge R320	1.7 in. (4.318 cm)	17.1 in. (43.434 cm)	24 in (60.69 cm)	25 lbs (11.34 kg)
Dell PowerEdge R330	1.68 in. (4.28 cm)	17.09 in. (43.42 cm)	24 in (61.0 cm)	29.54 lbs (13.4 kg)
Dell PowerEdge R620	1.7 in. (4.318 cm)	17.1 in. (43.434 cm)	26.9 in. (68.326 cm)	41.0 lbs (19.1 kg)
Dell PowerEdge R630	1.7 in. (4.318 cm)	19 in. (48.26 cm)	27.6 in (70.104 cm)	43.0 lbs (19.50 kg)
Portwell CAD-0230	1.65 in. (4.20 cm)	8.27 in. (21.00 cm)	8.27 in. (21.00 cm)	15.5 lbs. (7.03 kg)
HP Proliant DL360 G8	1.7 in. (4.318 cm)	17.1 in. (43.434 cm)	27.5 in. (69.85 cm)	42.3 lbs (19.19 kg)
HP Proliant DL360 G9	1.7 in. (4.318 cm)	17.2 in. (43.68 cm)	27.5 in (69.85 cm)	44.0 lbs (19.95 kg)

Temperature and humidity requirements

Server	Operating Temperature	Storage Temperature	Relative Humidity
Dell R320	50 ºF to 95 ºF (10 ºC to 35 ºC)	-40 ºF to 149 ºF (–40 ºC to 65 ºC)	20% to 80%, noncondensing
Dell R330	41 ºF to 104 ºF (5 ºC to 40 ºC)	23 ºF to 113 ºF (–5 ºC to 45 ºC)	5% to 85%, noncondensing
Dell R620	-40 ºF to 149 ºF (–40 ºC to 65 ºC)	-40 ºF to 149 ºF (–40 ºC to 65 ºC)	5% to 95%
Dell R630	50 ºF to 95 ºF (10 ºC to 35 ºC)	50 ºF to 95 ºF (10 ºC to 35 ºC)	1% to 80%, noncondensing
Portwell CAD-0230	32 ºF to 104 ºF (0 ºC to 40 ºC)	14 ºF to 158 ºF (–10 ºC to 70 ºC)	20% to 90%, noncondensing

Table continues…

Server	Operating Temperature	Storage Temperature	Relative Humidity
HP DL 360 G8	50 °F to 95 °F (10 °C to 35 °C)	101.7 °F (38.7 °C)	5 to 95% nonoperating 10 to 90% operating
HP DL 360 G9	50 ºF to 95 ºF (10 ºC to 35 ºC)	-22 ºF to 140 ºF (-30 ºC to 60 ºC)	8% to 80%, noncondensing

Note:

For altitudes greater than 900 m or 2952 ft, see Dell documentation for operating temperature ranges.

Power requirements

Server	Input	Nominal (110 V)	AC Power Max
Dell R320	110–240 VAC		300 W
Dell R330	110–240 VAC		350 W
Dell R620	110–240 VAC	2 A	750 W
Dell R630	110–240 VAC		750 W
Portwell CAD-0230	12 V DC		40 W
HP DL360p G8	100–240 VAC	15 A	308.95 W
HP DL 360 G9	110–240 VAC		800 W

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, including proximate high-current or high-power consuming equipment such as switch banks. Excessive heat might cause the server to overheat and fail.

Note:

The customer must ensure that environmental hazards do not interfere with the operation of the Avaya SBCE server. These hazards could include excessive heat, excessive humidity, improper ventilation, or electromagnetic interference from proximate equipment.

Regulatory standards

Avaya SBCE servers conform to the following standards.

Server	Certifications
Dell R320	CSA, FCC, CE, UL, RoHS
Dell R330	CSA, FCC, CE, UL, RoHS
Dell R620	CSA, FCC, CE, UL, RoHS
Dell R630	CSA, FCC, CE, UL, RoHS
HP DL360 G8	CSA, FCC, CE, UL, RoHS
HP DL360 G9	CSA, FCC, CE, UL, RoHS
Portwell CAD-0230	CE, FCC

Chapter 6: Security

Security specification

Unified communications intrusion protection

Traditional intrusion prevention systems (IPS) monitor network traffic to gather and analyze information from various parts of the network to identify possible security breaches. This information is used for subsequent prevention or mitigation. Unlike traditional IPS, Avaya SBCE security products detect any anomalous event, including day zero attacks. Additionally, also prevents virtually any type of intrusion from outside the enterprise and misuse from within the enterprise. This capability is because of 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 or fuzzed attacks. Customized protocol scrubbing rules detect and remove malformed messages that might cause call servers or other critical network components to stop responding. Malformed messages can also 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 traffic carried. The traffic flow is based on the negotiated signaling and other configured policies, such as prevent video or prevent modem/FAX.
- Spoofing Prevention: Various validation techniques are applied to detect and prevent spoofing, including the 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 can detect any nuisance and annoying calls to a particular destination or user. These products can selectively block the subscribers from whom the calls originate.
- Reconnaissance Prevention: Avaya SBCE detects and blocks application layer scan reports and blocks the attackers that originate them.

Attack protection

Avaya SBCE security products 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. These capabilities encompass each aspect of the UC network, including all endpoints, media gateways, call servers, voice mail (VM) and applications servers. In addition, the monitoring and management capabilities provide a cascaded, multi-layered detection, mitigation, and reporting system that provides real-time information based on user-definable event thresholds. This system supports a detailed graphical user interface (GUI) called the EMS web interface. The EMS can be installed on and run from any Avaya SBCE security device. The EMS can also be installed on a separate server platform and used as a standalone Element Management System (EMS). This EMS 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, the EMS must be installed on a dedicated platform.

Detection

The detection capability of the Avaya SBCE solution uses numerous 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 algorithms are flexible enough to accommodate special circumstances such as weekends, holidays, and other user-specified time periods. Avaya SBCE solution can also learn and apply dynamic trust scores, starting from an unknown score and either increasing or decreasing to different levels depending upon the behavior pattern of the caller, which could be Trusted, Known, Unknown, Suspected, or Spammer. The dynamic trust score is also dependant upon called party feedback, including (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 endpoints in the network to accurately detect attacks. These attacks might otherwise 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 endpoint 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.

Avaya SBCE security products can continuously learn call patterns and endpoint fingerprints. These products can also constantly analyze raw event data based on specific user-definable criteria and take automatic action. Therefore, Avaya SBCE security products can evolve and adapt automatically to effectively counter any new or existing threat.

Protection

The Avaya SBCE provides complete network protection by blocking attacks while simultaneously passing legitimate calls through unimpeded. This exceptional level of protection can be extended to an endpoint, a specific group of endpoints, or to all assets in the network. Extending this protection is based on highly flexible user-defined rule sets called Unified Communications Policies. These policies can be implemented to precisely discriminate or normalize any incoming or outgoing signaling or multimedia traffic. Thus all IP communication devices, such as hard-phones, soft-phones, Wi-Fi phones, and smart phones are protected effectively. Call servers, voice mail servers, media servers, media gateways, and application servers are also 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. The restrictions are effective after content filtering processing for data traffic to protect the Avaya SBCE from IP/ICMP/TCP level attacks.

Outbound traffic is unrestricted.

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 time.

Port scan blocking

When a port scan from a host is detected, all further requests from that host are blocked for a specified 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 period for 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, ethbint, and external Ethernet M1 interface, ethext, on the Com Express coprocessor board in the Avaya SBCE box.

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

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

Installation security

On installing the application rpm package, rules get added or updated for that version. After restart, ICU invokes the appropriate rules script for that platform.

DoS security features

With the Denial of Service (DoS) security feature of the EMS, you can view and edit DoS and Distributed Denial-of-Service (DDoS) attack response control parameters. These parameters can then be applied either to individual SIP endpoints or their parent domain. Also, 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, such as Remote Worker, Trunk and Remote Worker, and Trunk. The following rules describe the input methods:

- For Remote Worker, the input is taken from Number of remote workers and Max Concurrent Sessions.
- For Trunk, the input is taken from Max Concurrent Sessions.
- For 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 whether any response is received.
- 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. The protocol scrubber verifies certain message characteristics such as proper message formatting, message sequence, field length, and content against templates received from Avaya. Messages that violate the security rules dictated by the scrubber templates are dropped while messages that violate syntax rules are repaired. Messages are repaired by rewriting, truncating, rejecting, or dropping, depending on the processing rules imposed by the templates. Protocol scrubbing rule templates are prepared by Avaya and the user can edit the templates minimally.

Protocol scrubbing for SIP allows you to install a scrubber rules package. You can also 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 installed scrubber rules.

Topology hiding

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

Firewall rules

Firewall rules protect the Avaya SBCE, and communications and signaling for Avaya SBCE. Firewall rules are hard-coded and cannot be configured. 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. Common rules are divided into the following categories:

- ICMP restrictions
- Portscan detection
- KILLSCAN rules

ICMP restrictions

- Always accept ICMP ping replies.
- Any IP address sending an ICMP ping request is added to the pingflood list.
- When an IP in the pingflood list sends an ICMP ping request, drop the request if that IP has sent five ping requests in one second.
- Accept all other ICMP ping requests.
- ICMP redirect datagrams for the network are rate-limited to one per second.
- ICMP redirect datagrams for the host are rate-limited to one per second.
- ICMP destination unreachable messages are rate-limited to one per second.
- ICMP time exceeded messages are rate-limited to one per second.
- ICMP bad IP header messages are rate-limited to one per second.
- Drop all other ICMP packets.

Detecting Portscan

Procedure

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 without 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 without 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

- Follow MGMTPROTECT rules.
- Accept all packets in RELATED or ESTABLISHED state.
- Accept all packets on TCP port 222.
- Accept all packets on TCP port 443.
- Accept all packets on TCP port 53.
- Accept all packets on UDP port 53.
- Accept all packets on TCP port 514.
- Accept all packets on UDP port 514.
- Accept all packets on UDP port 123.
- Drop all other packets.

TCP flood restrictions for all ports

- Any IP address sending packets with FIN flags set, but without SYN, RST, PSH, ACK, or URG flags is added to the finrstlim list.
- Any IP address sending packets with RST flags set, but without FIN, SYN, PSH, ACK, or URG flags is added to the finrstlim list.
- For any IP address in the finrstlim list that sends ten packets in one second, drop the packet.

SSH rules

- Any IP address sending, on port 222, packets with the SYN flag, but without RST or ACK is added to the sshsyn list.
- For any IP address in the sshsyn list that sends, on port 222:

  Fifteen packets with the SYN flag, but without RST or ACK in 1 minute during the TTL of the previous packet sent, drop the packet.

Ten packets with the SYN flag, but without RST or ACK in 30 seconds during the TTL of the previous packet sent, reject the packet. An ICMP port unreachable message is sent for the packet.

HTTPS rules

- Any IP address sending, on port 443, packets with the SYN flag, but without RST or ACK, is added to the httpssyn list.
- For any IP address in the httpssyn list that sends, on port 443:
  - Ten packets with the SYN flag, but without RST or ACK in one second during the TTL of the previous packet sent, drop the packet.
  - Five packets with the SYN flag, but without RST or ACK in one second during the TTL of the previous packet sent, reject the packet. Send an ICMP port unreachable message.

DNS rules

- Any IP address sending, on TCP port 53, packets with the SYN flag, but without RST or ACK is added to the dnssyn list.
- For any IP address in the dnssyn list that sends, on TCP port 53:
  - Ten packets with the SYN flag, but without RST or ACK in one second during the TTL of the previous packet sent, drop the packet.
  - Five packets with the SYN flag, but without RST or ACK in one second during the TTL of the previous packet sent, reject the packet. Send an ICMP port unreachable message.

Data interface rules

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

- Follow DATAIFPROTECT rules.
- 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.

- 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.
- For any IP address in the apprules list that sends:
  - Ten packets with the SYN flag, but without RST or ACK to the specified IP and port in one second during the TTL of the previous packet sent, drop the packet.
  - Five packets with the SYN flag, but without RST or ACK to the specified IP and port in one second during the TTL of the previous packet sent, reject the packet. Send an ICMP port unreachable message.

- 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 the packet.
    - Keep a record of any IP address that sends a packet in the ESTABLISHED state to the specified IP and port.
    - For any IP address that sends three packets in the NEW state to the specified IP and port in one second, drop the packet.
    - Keep a record of any IP address that sends a packet in the NEW state to the specified IP and port.
- Delete any existing rule for accepting packets.
- 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 Avaya SBCEs and the EMS

- SSH TCP-222.
- HTTPS TCP-443.
- OpenVPN UDP-1194.
- Syslog TCP/UDP-514.
- NTP UDP-123.

External – Between the EMS and Avaya SBCEs and an external device

- SSH TCP-222.
- HTTPS TCP-443.
- Syslog TCP/UDP-514.
- NTP UDP-123.
- DNS TCP/UDP-53 for DNS and the signaling and media ports.
- SNMP Version 2 or 3 UDP-161 + 162. The SNMP agent receives requests on UDP port 161, and the SNMP manager receives notifications for traps and InformRequests on port 162

TCP packets

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

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.

Additional port assignments

DNS server

If the DNS server is not in the DMZ, open UDP port 53 on Avaya SBCE through the EMS GUI. Then, Avaya SBCE can access the DNS server.

SNMP

If you have your own SNMP, open the SNMP UDP ports 161 and 162 on Avaya SBCE through the EMS GUI. Then, Avaya SBCE can access the SNMP from the DMZ.

Syslog

If you have your own Syslog, open the Syslog UDP port 514 on Avaya SBCE through the EMS GUI. Then, Avaya SBCE 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 following ports are default ports. Other ports can be configured.

- TCP/UDP 5060
- 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 Avaya SBCE through the EMS GUI. Then, the phones can login and download configuration files from Avaya HTTP server or HTTPS server.

- HTTP port 8080 or port 80
- HTTPS port 443

LDAP/LDAPS ports

- LDAP port 389
- LDAPS port 636

Avaya Aura® Media Server Offloading port

The default port is port 7150.

Shared Control port

In Remote Worker deployments where endpoints are configured in the shared control mode, enable shared control port on the internal interface of Avaya SBCE towards Avaya Aura® network. This port could be any unused TLS port on the internal interface of Avaya SBCE, for example, port 5063 . This port must be enabled on the internal firewall between Avaya SBCE and the Avaya Aura® network.

For more information about port usage, see *Avaya Port Matrix: ASBCE*.

Chapter 7: Licensing requirements

Avaya SBCE uses the Avaya Product Licensing and Delivery System (PLDS) to create Release 8.0 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, Media Replication and other features to the Standard Services offer.

Avaya Aura® Mobility Suite and Collaboration Suite licenses include Avaya SBCE.

Note:

Licenses and a WebLM server are required for an upgrade to Release 8.0 or a new installation of Avaya SBCE Release 8.0.

Avaya SBCE license features

To use a feature, you must ensure that the license file that you upload to WebLM has the appropriate licenses for the feature. You cannot configure or use a feature if the correct license for that feature is not present in the license file.

License feature	Description
VALUE_SBCE_STD_SESSION_1	Specifies the number of standard session licenses.
VALUE_SBCE_STD_HA_SESSION_1	Specifies the number of standard service HA session licenses.
VALUE_SBCE_ADV_SESSION_1	Specifies the number of session licenses for remote worker, media recording, and encryption. **Note:** You must buy and deploy a standard session license with every advanced license feature.

Table continues…

License feature	Description
VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Scopia® video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Scopia® video conferencing HA session licenses.
VALUE_SBCE_CES_SVC_SESSION_1	Specifies the number of Client Enablement Services session licenses.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Specifies the number of Client Enablement Services HA session licenses.
VALUE_SBCE_TRANS_SESSION_1	Specifies the number of transcoding session licenses.
VALUE_SBCE_TRANS_HA_SESSION_1	Specifies the number of transcoding HA session licenses.
VALUE_SBCE_ELEMENTS_MANAGED_1	Specifies the maximum number of Avaya SBCE elements managed.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that download of VMware OVA files is permitted for Avaya SBCE.
VALUE_SBCE_ENCRYPTION_1	Specifies the Avaya SBCE encryption, and is required for advanced licenses.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1	Specifies the configuration of HA for the setup.
FEAT_SBCE_DYNAMIC_LICENSING_1	Specifies that dynamic or pooled licensing is permitted for Avaya SBCE.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies encryption Avaya SBCE encryption only for signaling.

WebLM server details

Avaya SBCE uses WebLM for licensing requirements.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

  The primary host ID of WebLM is used for creating the license file.
- Licensed features

- Licensed capacity

You can install the Avaya SBCE license file on System Manager WebLM, local WebLM, or standalone WebLM server.

Do not use IP OfficeWebLM for installing the Avaya SBCE license file. Avaya SBCE does not support IP OfficeWebLM.

Use the following URL formats for installing a license on the System Manager WebLM server or standalone WebLM server:

- System Manager WebLM server: https://<SMGR_server_IP> :52233/WebLM/LicenseServer
- Standalone WebLM server: https://<WEBLM_server_IP> :52233/WebLM/LicenseServer

For installing a license through a local WebLM server on :

- Avaya SBCE in virtualized environment: Download the WebLM OVA file from PLDS and deploy the OVA file on the virtual machine.
- Avaya SBCE hardware device: Select the **Use local WebLM server** check box.

Options for configuring the WebLM server IP address are available on the System Management page of the EMS web interface.

⚠ **Warning:**

Virtual EMS cannot run a local WebLM.

Chapter 8: 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		
Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading to Avaya SBCE 8.0.	Implementation engineers
Maintenance and Troubleshooting		
Administering Avaya Session Border Controller for Enterprise	Configuration and administration procedures.	Implementation engineers, Administrators
Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	Troubleshooting and maintenance procedures.	Implementation engineers, and Sales engineers
Reference		
Avaya Port Matrix: ASBCE 8.0	Port information.	Implementation engineers, Administrators, and Sales engineers

Related links

Finding documents on the Avaya Support website on page 97

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.

5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Related links

Documentation on page 97

Training

The following courses are 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.

Note:

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

Course code	Course title
2060W	What is new for Avaya Session Border Controller for Enterprise
2066W	Administering the Avaya Session Border Controller for Enterprise
2080C	Implementing and Supporting Avaya Session Border Controller — Platform Independent
2080T	Avaya Session Border Controller for Enterprise Platform Independent and Support Test
2080V	Implementing and Supporting Avaya Session Border Controller — Platform Independent
26160W	Avaya Session Border Controller for Enterprise Fundamentals
7008T	Avaya Session Border Controller for Midmarket Solutions Implementation and Support Test
7008W	Avaya Session Border Controller for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions

Viewing 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.

Procedure

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - 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 website.

  Note:

  Videos are not available for all products.

Support

Go to the Avaya Support website at https://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.

Glossary

ARP	Address Resolution Protocol
Codec	Coder/Decoder
Day Zero Attack	See Zero-Day Attack.
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 end-points, 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.
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message 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 Anti-Tromboning.

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