Avaya Session Border Controller Overview and Specification

Release 10.2.1
Issue 1
December 2024

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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.

Service Provider

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 to comply 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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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

Contents

Chapter 1: Introduction

Purpose

This document describes tested Avaya Session Border Controller (Avaya SBC) 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 SBC features, functions, capacities, and limitations.

Chapter 2: Avaya SBC overview

Avaya SBC provides security to SIP-based Unified Communications (UC) networks. Avaya SBC is available in two versions: Standard Services and Advanced Services. Either version can reside on supported servers. For information about supported servers, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

Avaya SBC has two main components: the management system named Element Management System (EMS), and the call processing system named SBC. Depending on the network size and service requirement, you can deploy Avaya SBC in one of the following configurations:

- Standalone configuration

  In the standalone configuration, the EMS and SBC co-reside in the same server.

- Multiple server configuration

  In the multiple server configuration, the EMS and SBC are deployed on separate servers.

- High Availability (HA) configuration

  In an HA configuration, SBC servers are deployed in pairs. Each pair has one SBC acting as the primary while the other SBC is the secondary. Both servers are controlled by a single EMS or a replicated EMS pair.

New in Avaya SBC Release 10.2.1

Support for Red Hat Enterprise Linux 8.10

Avaya SBC uses Red Hat Enterprise Linux 8.10.

Support for Radius over TLS

Avaya SBC supports TLS or UDP protocol for communication between Radius server and Avaya SBC. For TLS, it only uses Mutual Authentication.

Support for Secure Digest Algorithms for SIP Authentication

Avaya SBC supports the following secure digest algorithms for authentication challenge responses:

- MD5 (Message Digest)
- SHA-256 (Secure Hash)
- SHA-512 (Secure Hash)

Secure digest algorithm is a simple challenge-response mechanism that allows a server (service provider) to challenge a client (Avaya SBC) request and allows a client (Avaya SBC) to provide authentication information in response to that challenge.

SHA-256 and SHA-512 are more secure and strong algorithms than the default algorithm, MD5.

For JITC deployments, Avaya SBC uses the algorithms in the following priority order (high to low):

- SHA-512
- SHA-256

For Non-JITC deployments, Avaya SBC uses the algorithms in the following priority order (high to low):

- SHA-512
- SHA-256
- MD5

Support for TTL Override

With this feature, Avaya SBC overrides TTL value in all outgoing media packets. When configured it changes TTL field in IPV4 packets and HopLimit field in IPV6 packets.

This feature will not have any effect on following Avaya SBC media handling features.

- Media tunneling
- Turn Controller

Upgrade simplification

You can upgrade EMS and SBC parallely when upgrading from Release 10.2.x to Release 10.2.1 using CLI.

Zero Down Time support for FlyingVoice endpoints

Avaya SBC supports registrations of Third-party endpoints such as FlyingVoice endpoints. It also supports Zero Down Time workflows.

Support for Live Syslog of SIP messages

Avaya SBC supports Syslog of live SIP messages through **SIP Trace** option in Syslog configuration.

Note:

GDPR configuration and SIP Trace cannot be enabled simultaneously.

Support for Dell R660 and Dell R360 servers

Avaya SBC supports deployment on Dell R660 (Avaya Solutions Platform 110 Appliance server) and Dell R360 servers.

Support ASP 130 Server with KVM Hypervisor

Avaya SBC supports deployment on Avaya Solutions Platform (ASP) 130 Server with Kernel based Virtual Machine (KVM) Hypervisor.

Emergency call routing for Direct Routing users

Emergency call routing for direct routing users can be deployed in the following two ways depending on the emergency calling network within a given country or region.

- Emergency Routing Service Providers (US only)
- Emergency Location Identification Number (ELIN) gateway

Standard services

Avaya SBC 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 SBC 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 SBC 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.

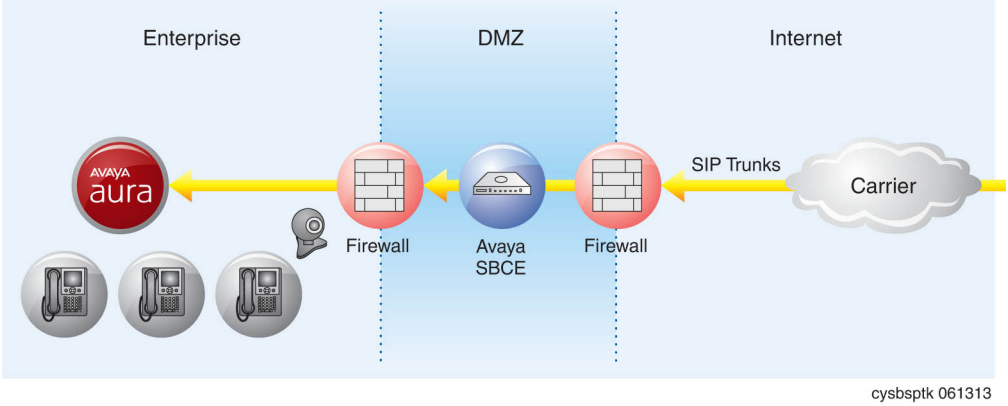


Figure 1: SIP trunking

Advanced Services

Avaya SBC 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 such as denial of service, teardrop, and IP sweep 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 SBC 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.

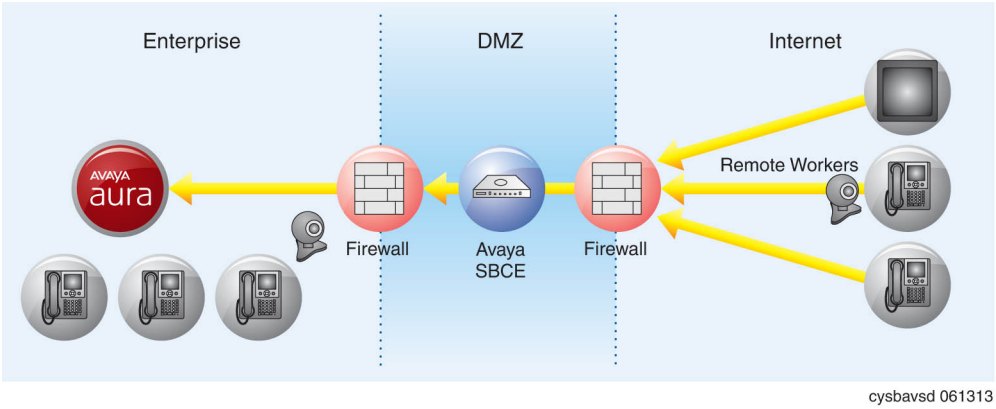


Figure 2: Advanced Services Solution

Functional elements

Avaya SBC 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, such as teardrop attacks and IP sweep attacks
  - Message sequence anomaly detection and prevention
  - Continuous user behavior learning
  - Bypass for all non-SIP traffic including ARP, DNS, ICMP, Simple Traversal of UDP through NAT (STUN), and Traversal Using Relay NAT (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 SBC 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 SBC 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 SBC deployment options

Deployment models

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

- **Standalone configuration**: In the standalone configuration, the SBC and EMS coreside in the same server. In this deployment, the phones maintain two separate socket connections to the SBC, at two different IP addresses hosted by the SBC.
- **Multiple server configuration**: A multiple server configuration requires the EMS and the SBC to be deployed on different servers.
- **High availability (HA) configuration**: A High availability (HA) configuration requires a separate EMS server. SBC 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 SBC, which performs all data processing. The interface ports on the standby SBC do not process any traffic. The Management interfaces on the SBC appliances have different IP addresses, but the signaling or media interfaces have the same IP address. Upon failover, the standby SBC advertises its new MAC as the L2 address for the common IP address. The SBC devices are synchronized via the heartbeat on the dedicated interfaces, and both SBC devices are in continuous communication with the EMS.

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

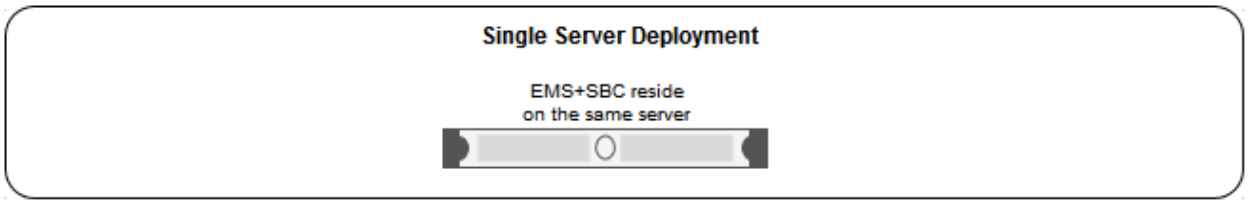
Avaya SBC is packaged as a vAppliance (OVA) ready for deployment on VMware certified hardware to run in VMware environment. Avaya SBC is also delivered in vAppliance (OVA)

format for VMware based deployments. Avaya SBC has a single OVA file for EMS, SBC+EMS, and Avaya SBC 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 on a Virtualized Environment Platform*.

Single server non-HA deployment

In a single server non-HA deployment, the Element Management System (EMS) and SBC software are installed on a single server. Use this deployment scenario when you want to deploy Avaya SBC in a basic mode.



Important:

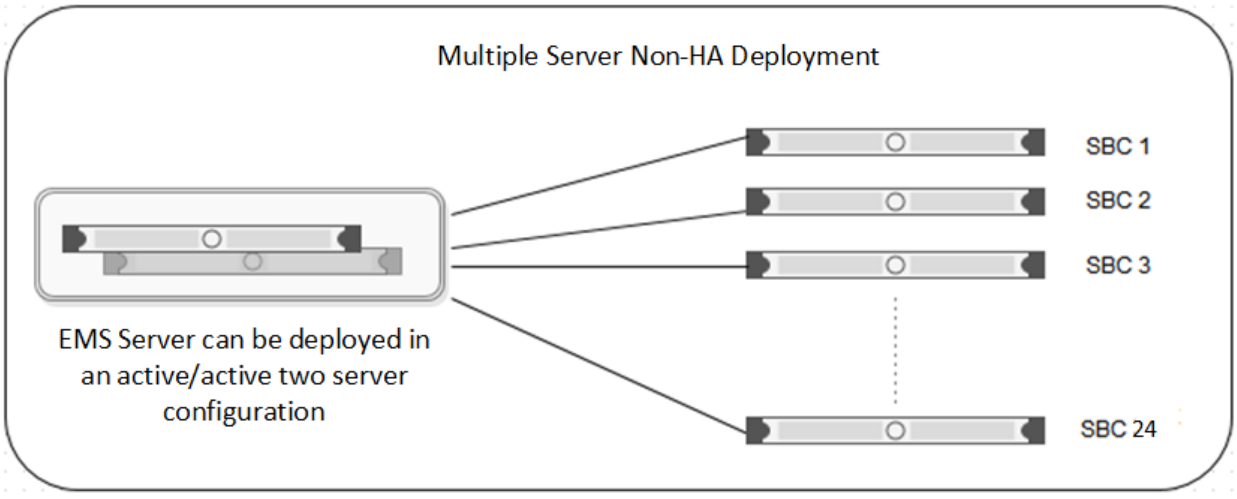
All hardware server types, virtualized environment platforms, and cloud platforms support the single-server non-HA deployment type.

Multiple server non-HA deployment

In a multiple server deployment, the EMS and SBC software are installed on separate servers.

In a non-HA multiple server deployment, you can have one or more SBC servers controlled by a single EMS server or a replicated EMS HA pair. In an active/active deployment, the EMS software is installed on two servers. One EMS server is configured as Primary and the other is configured as Secondary. When using a single EMS server, the EMS server is configured as Primary.

You can have up to 24 individual Avaya SBC servers in this type of configuration.



If you start with a non-HA deployment and want to later move to an HA deployment, you must completely reconfigure the deployment.

Important:

All hardware server types, virtualized environment platforms, and cloud platforms support the multi-server non-HA deployment type.

Multiple server HA deployment

In a multiple server deployment, the EMS and SBC software are installed on separate servers.

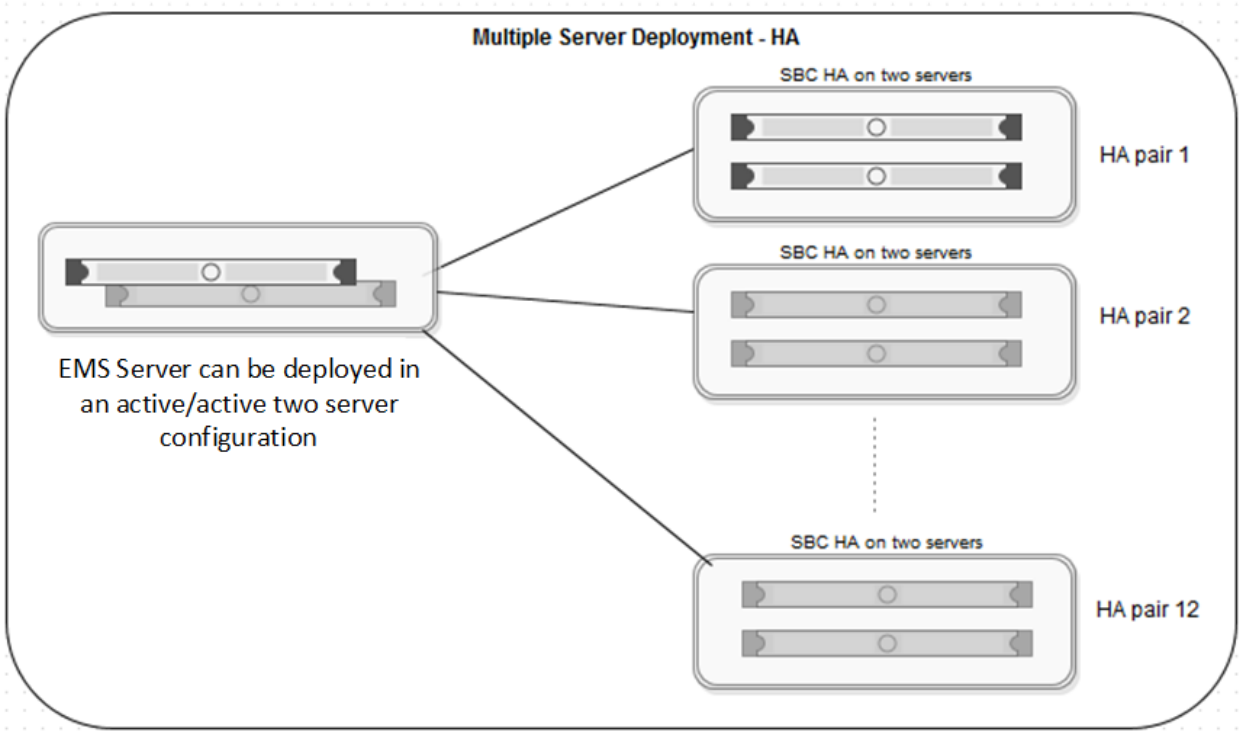
In an HA deployment, SBC servers are deployed in pairs. Each pair has one SBC server configured as Primary while the other is configured as Secondary.

Optionally, the EMS software can be replicated in an active/active HA pair deployment. In an active/active deployment, the EMS software is installed on two servers. One EMS server is configured as Primary and the other is configured as Secondary. An EMS HA pair must be reachable to each other and with the SBC servers, and can be in different geographical locations.

One EMS server or an active/active pair of EMS servers can control up to 12 separate pairs of SBC servers.

Note:

When deploying an HA configuration on Amazon Web Services, you only have to configure the SBC software on the primary device



Important:

All hardware server types, virtualized environment platforms, and cloud platforms support the multi-server HA deployment type.

Although the HA pairs and non-HA deployments are shown separately in this figure, EMS can control both an SBC HA server pair as well as a single SBC server.

SBC HA server pairs must adhere to the following requirements:

- You can enable and use the HA deployment feature only if the license file contains an HA license.
- The HA pair servers must reachable by the EMS or EMS HA pair servers over the Management Plane (M1).
- The HA pair servers must be reachable between the devices over the Management link (M1) .
- The HA pair servers must have the HA link (M2) reachable between the HA pair servers.
- The HA pair servers must set up to have all the data interfaces between the servers replicated so that the servers are connected in same subnets. For example, the A1 data interface in one SBC server should be in the same subnet as the A1 data interface of the paired SBC server. This allows you to meet the requirement that failover be functional in an active/standby mode.
- In a multiple server HA virtualized deployment, when there are multiple HA pairs and automatic IP addressing is being used on the HA link (M2), every HA pair should either have their own isolated vSwitch or each HA pair should use different IP addresses reachable with their HA pairs as stated previously for M2 connectivity.

Note:

Note the following recommendations:

- Connect the HA pair servers back-to-back using automatic IP addressing.
- If the HA pair server M2 links are connected over a network (for example, switches or routers in the same or different locations) and are not in a back-to-back connection, use reachable network IP addresses that have minimum or no latency. You need a good quality connection because HA keep-alive messages and failover messages depend on this link.
- High availability requires Gratuitous Address Resolution Protocol (GARP) support on the connected network elements. When the primary Avaya SBC fails over, the secondary Avaya SBC broadcasts a GARP message to announce that the secondary Avaya SBC is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBC 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 SBC, with a router or L3 switch. If you do not put the Avaya SBC 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 SBC.

Deployment modes

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

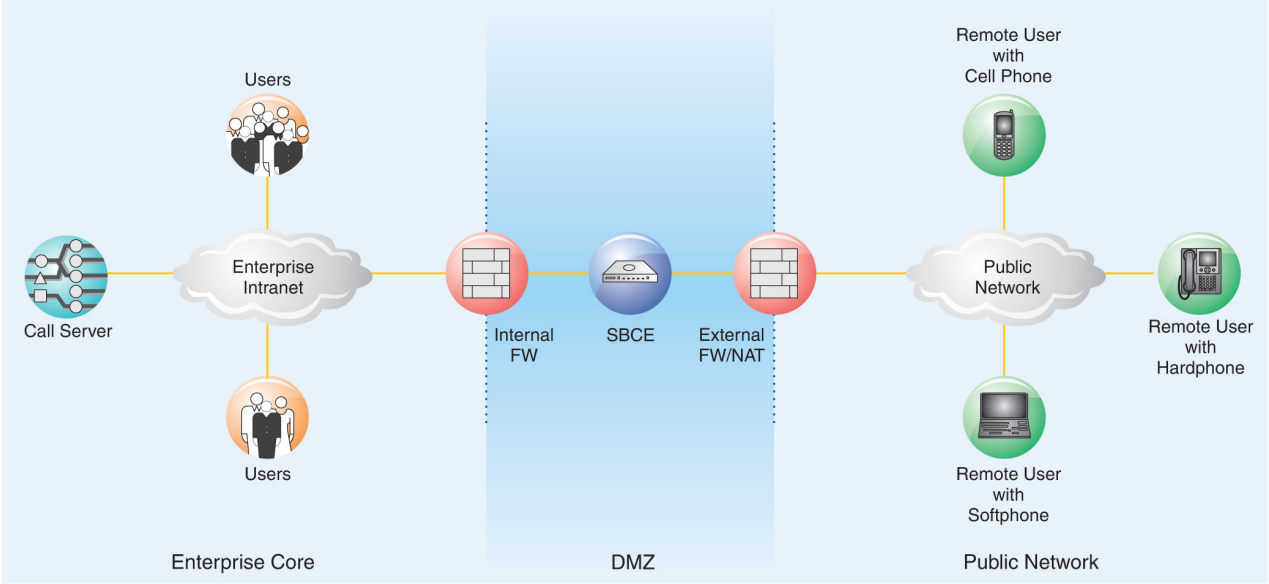
Regardless of the deployment scenario, Avaya SBC offers complete flexibility and intuitive configuration. These products do not require any management on the endpoints in addition to what is necessary to enable TLS, SRTP, and digest authentication.

Two-wire deployment

The two-wire topology, also referred to as inline, is the simplest and most basic deployment. Avaya SBC is positioned at the edge of the network in the DMZ. Avaya SBC 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 SBC 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 SBC deployment enables TLS encryption of the signaling traffic and SRTP encryption of the media traffic.



cysbdp2w LAO 021413

Figure 3: Avaya SBC Deployment – Two-Wire

One-wire deployment

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

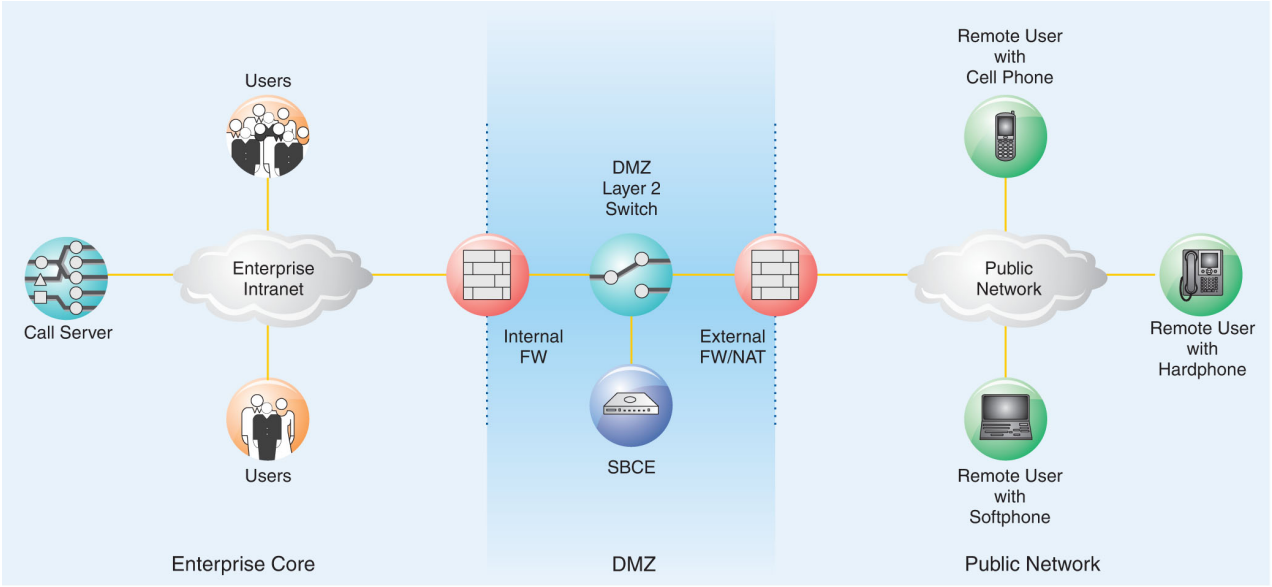


Figure 4: Avaya SBC Deployment – One-Wire

Supported deployment platforms for Avaya SBC

Hardware platforms

The following table lists the Avaya SBC or EMS device configurations supported by each hardware server. The table also contains information about the number of NIC ports available and the hardware category for each server.

Server	NIC Ports	DVD drive	Hardware category	Supported device configuration		
				EMS	SBC	EMS+SBC
Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 3	6	Yes	310	Supported	Supported	Supported
Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 5	6	Yes	310	Supported	Supported	Supported
Dell™ PowerEdge™ R340 Avaya Solutions Platform 110 Appliance server	6	No	310	Supported	Supported	Supported
Dell 3240	5	No	310	Not Supported	Not Supported	Supported

Table continues…

Server	NIC Ports	DVD drive	Hardware category	Supported device configuration		
				EMS	SBC	EMS+SBC
Dell VEP1425N	8 ports available, but only 4 ports are supported	Yes	310	Not supported	Not Supported	Supported
Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A2	6	Yes	310	Supported	Supported	Supported
Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A3	8 ports available, but only 6 ports are supported	Yes	310	Supported	Supported	Supported
Dell R360	6	Yes	310	Supported	Supported	Supported

For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

Virtualized environment platforms

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.

The Virtualized Environment project applies only for VMware and does not include any other industry hypervisor. Virtualized Environment project is inclusive of the Avaya Aura® portfolio.

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

You can deploy EMS and SBC software using a single OVA file.

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

The Avaya SBC OVA files are offered as vAppliance for EMS and Avaya SBC configurations. The OVA file is available the Avaya Support Site or from the Avaya Product Licensing and Delivery System (PLDS).

For more information, see *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*.

Kernel-based Virtual Machine platforms

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 on a Virtualized Environment Platform*.

Amazon Web Services platforms

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

- 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 on an Amazon Web Services Platform*.

Google Cloud Platform

Google Cloud Platform is a cloud services platform that enterprises use to securely run applications on the virtual cloud. Google Cloud Platform integrates the cloud services that are needed to develop, test, deploy, and manage applications, all while taking advantage of the efficiencies of cloud computing.

Supporting Avaya applications on the Google Cloud Platform Infrastructure as a Service (IaaS) platform provides the following benefits:

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

Avaya SBC on Microsoft® Azure overview

Microsoft® Azure (Azure) is a cloud services platform that enables enterprises to run applications on the virtual cloud securely. By deploying Avaya SBC on Azure, you get the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to an 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.

Network security deployments

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.

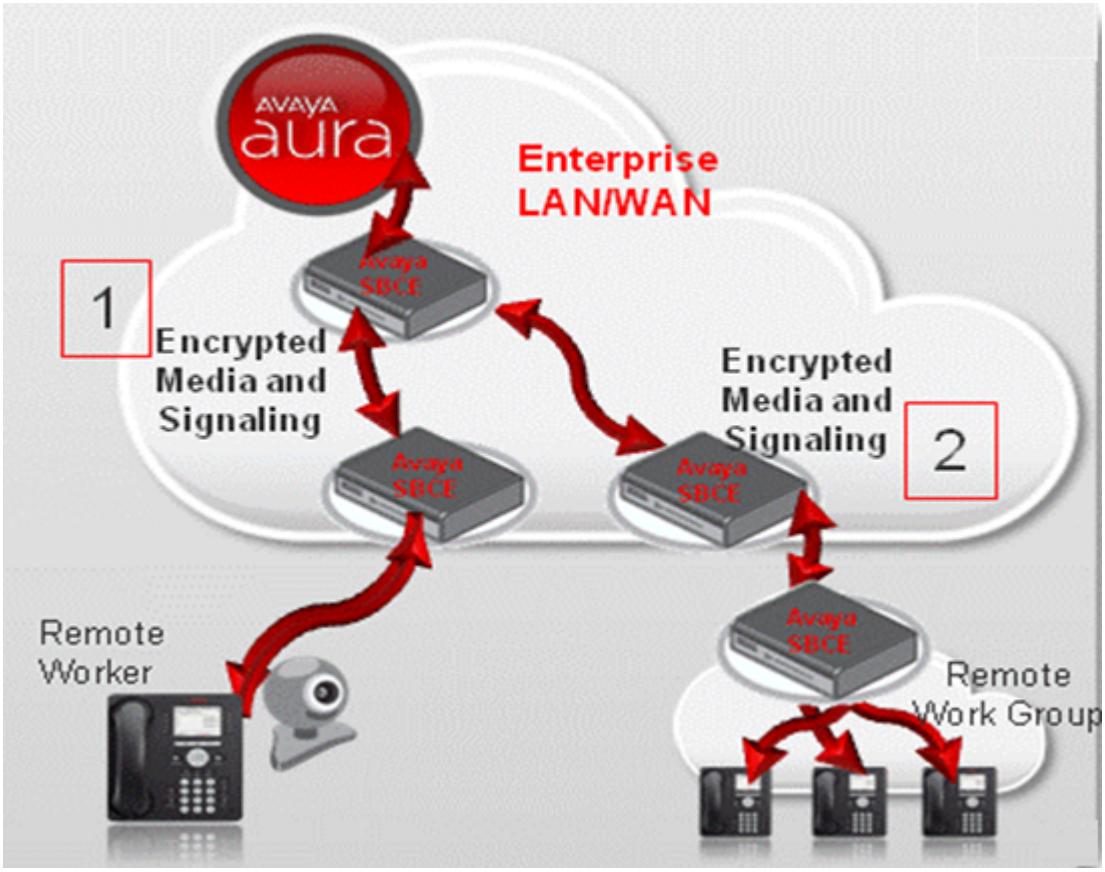


Figure 5: Additional network security deployment

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 SBC internally, and Remote Workers connect to the core via a different Avaya SBC. Avaya SBC maintains security and NAT bindings and end-to-end encryption in this back-to-back scenario. The second scenario depicts a Remote work group using a Avaya SBC at the local edge of the group, creating a back-to-back-to-back 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 SBC and then to the core if desired. This configuration is supported with Avaya 96x1 SIP clients.

Feature descriptions

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 Meetings Server 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.

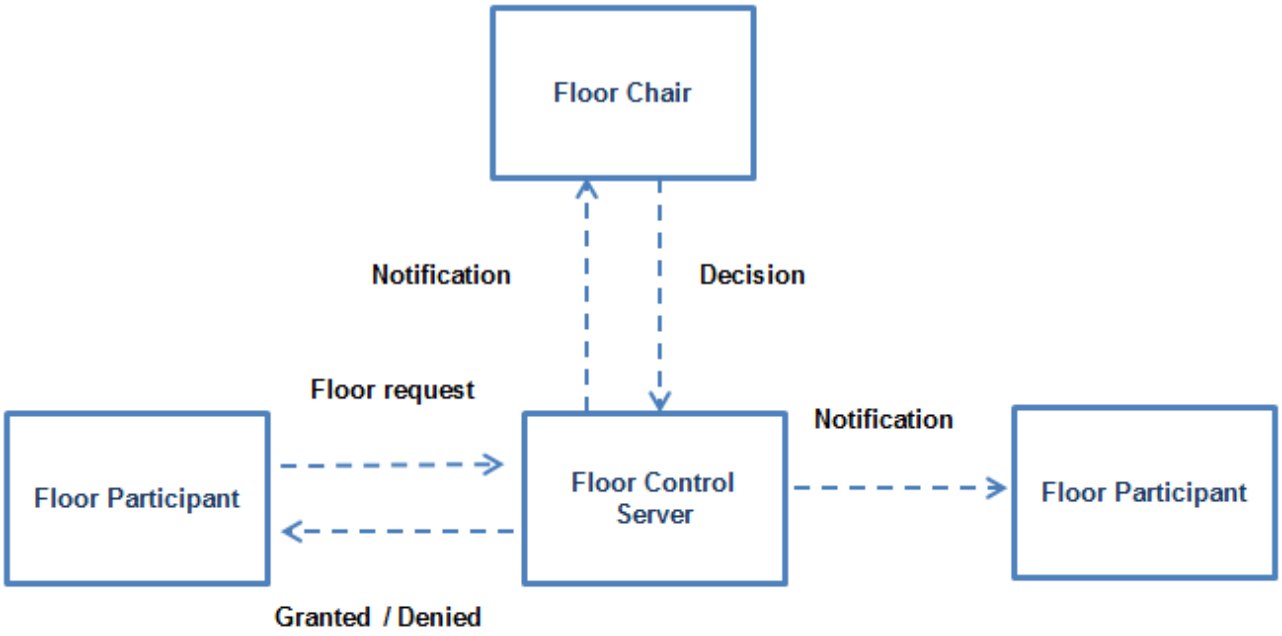


Figure 6: BFCP components

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

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

Avaya SBC negotiates with Avaya Meetings Server MCU or Avaya Meetings Server 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 SBC fails to negotiate the setup attribute, the TCP connection is started by Avaya SBC. 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 SBC does not play any role in connection establishment or reestablishment and authentication.

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

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

- Avaya SBC 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 SBC receives an offer on the incoming leg with the setup attribute as passive.Avaya SBC answers with the setup attribute as active with a valid port parameter in the BFCP application line. Avaya SBC 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 SBC receives an offer with the connection attribute as new. Avaya SBC answers with a connection attribute as new.
- Avaya SBC receives an offer with the connection attribute as existing. Avaya SBC answers with a connection attribute as existing.
- Avaya SBC starts an offer on the outgoing leg with the connection attribute as new for all cases.

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

Architecture of Binary Floor Control Protocol

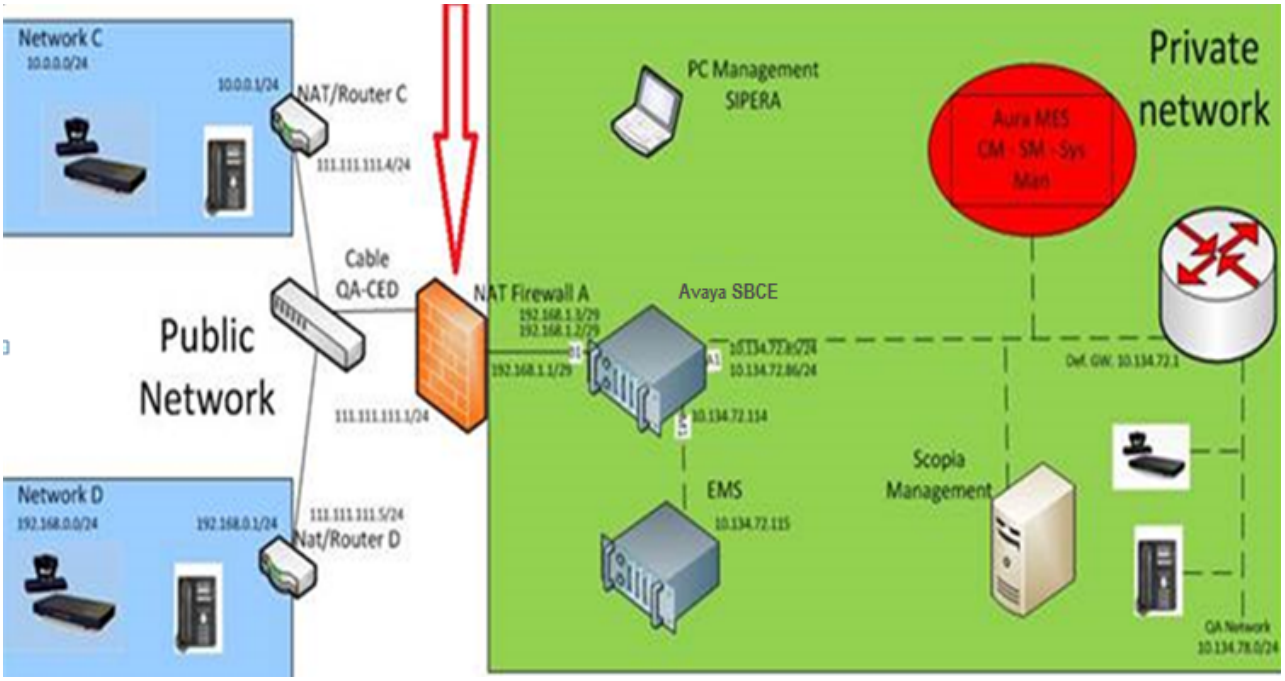


Figure 7: BFCP architecture

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 SBC	c-only	passive	new	Valid connection and port
3	XT-MCU	s-only	active	new	Discarded port. For example, 9
4	Avaya SBC (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 SBC	c-s	passive	new	Valid connection and port
3	XT-client	c-only	active	new	Discarded port
4	Avaya SBC	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 SBC	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 SBC 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 SBC	s-only	passive	new	Valid connection and port
3	Remote worker XT-client	c-only	active	new	Discarded port
4	Avaya SBC responds to Elite MCU	c-only	active	new	Valid connection and port

After Avaya SBC responds to Elite MCU, Avaya SBC 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 Meetings Server does not set up the connection again.

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 for SIP Routing Element (SRE) flows.

For the 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 SBC, use enhanced SIP timing and recovery techniques to provide signaling path continuity during Session Manager failure. When Avaya SBC detects that a Session Manager is unreachable, it uses the Failover Group Domain Name (FGDN) in the Session Manager through and Record-route headers to route the SIP traffic through the alternate Session Manager. 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, refer *Call Preservation Feature Description and Administration Guide*.

To support the Call Preservation feature, Avaya SBC:

- 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 SBC detects that the preferred Session Manager is unreachable.
- Supports Call Preservation on TCP and TLS transport types.
- Changes the dialog-scoped affinity to the preferred Session Manager when the preferred Session Manager instance becomes unreachable. Avaya SBC reevaluates the affinity by selecting one of the following:
  - The alternate Avaya SBC 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.

Edge Server for Converged Conference solution

The Converged Conference solution uses the features of Avaya Meetings Server 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 SBC:

- 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 SBC 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 6000 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 Workplace Client, and Avaya Meetings Server Avaya XT Series series of clients.
- Edge Server: Avaya SBC, Path finder (H.323), and Avaya Scopia Desktop Server. Avaya SBC 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.

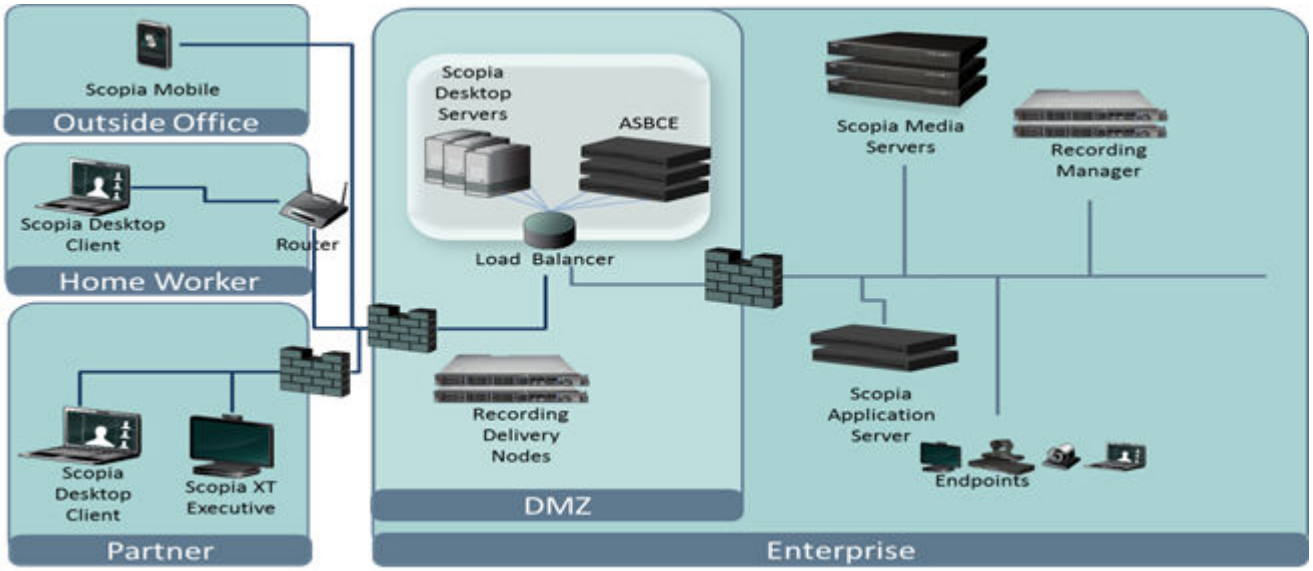


Figure 8: Components of Converged Conference solution with Avaya SBC as an edge server

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

Avaya SBC features for the Converged Conference solution

For the Converged Conference solution, Avaya SBC 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 Meetings Management management and load balancers.
- Calculating bandwidth for all audio/video sessions. Avaya SBC 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 SBC to Avaya Meetings Server 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 SBC. Ensure that the receive interface of the click to call flow matches the signaling interface of the inbound flow selected.

End-to-end secure call indication

Avaya endpoints can display an end-to-end secure indicator for calls that use secure protocols for both halves of the call. Avaya SBC provides a **Securable** field on the Server Configuration page to indicate whether the server is securable. Avaya SBC 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 SBC 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 SBC 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.

ENUM support

Avaya SBC 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 SBC 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 SBC uses to update the request URI, and proceeds with the routing. If a routing entry is not configured in the corresponding routing profile, Avaya SBC uses this URI to determine the destination.

Far End Camera Control

Avaya SBC supports FECC Offer and Answer in SDP. Avaya SBC 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 SBC 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 SBC 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 SBC applies encryption according to SDP Capability Negotiation and SDES by Avaya SBC policy.

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 Workplace Client 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.

GDPR

General Data Protection Regulation (GDPR) prevents the loss of personal data by improving data security.

When GDPR is enabled, Avaya SBC uses a 12-character passphrase that you have provided to encrypt the files in the following folders:

Application logs and trace files: The encrypted files can be stored locally or to a remote log server. When configured to store the encrypted files to a remote log server, the encrypted files are pushed to the server based on the duration defined while configuring the log server. Avaya SBC encrypts the files that reach the maximum size of 10 MB or that are older than 6 hours. Application logs:

- SSYNDI logs: /archive/log/ipcs/ss/logfiles/elog/SSYNDI/
- OAMPSERVER logs: /archive/log/ipcs/ss/logfiles/elog/OAMPSERVER/
- SYSMON logs: /archive/log/ipcs/ss/logfiles/elog/SYSMON/
- Turnserver logs: /archive/log/turnserver/
- Nginx logs: /archive/log/nginx/
- Scrubber logs: /archive/log/scrubber/
- /archive/pcapfiles/IPCS2/

Trace files:

- SIP traces: /archive/log/tracesbc/tracesbc_sip/
- PPM traces: /archive/log/tracesbc/tracesbc_ppm/

Packet captures: The encrypted files can be stored locally or to a remote log server. When configured to store the encrypted files to a remote log server, the encrypted files are pushed to the server based on the duration defined while configuring the log server. Avaya SBC encrypts the files every 15 minutes.

- Pcap files: /archive/pcapfiles/IPCS2/

CDR files: CDR files can be stored locally, to a RADIUS server, or to a CDR adjunct server. When stored locally, the files are encrypted as soon as they are created. When stored in the CDR adjunct server, the files are encrypted as soon as they are created and pushed to the server according to the interval defined in the **Update Interval** field. When stored in the RADIUS server, GDPR has not effect. The files are not encrypted and pushed to the server as soon as they are created.

- CDR files: /archive/cdr/

Note:

Avaya SBC compresses the files before encrypting.

Note:

Before enabling GDPR, Avaya SBC might have unencrypted log information that will not comply to GDPR.

You can use the openssl command to decrypt the files.

Tracesbc: You can now run `tracesbc` in a GDPR-compliant Avaya SBC. However, encrypted records will not show in the `tracesbc` output.

GDPR compliance

The following table lists GDPR requirements and how Avaya SBC supports those requirements.

GDPR Requirement	General GDPR Rule	Avaya SBC Support
Architecture Requirement for Inventory and handling of Personal Data	The architecture should define all interfaces and location for all the instances of personal data to be known. This facilitates the data controller to identify all personal data. The exception to this rule is for any data which is temporary and does not reside less than 24 hours in the system.	Avaya SBC documents all the interfaces and location of personal data in resident memory, data structures, files, CDRs, applications on cloud and distributed In general any such data does not reside in Avaya SBC for more than 24 hours, so Avaya SBC is not exposed to the general applicability of this rule. Subsequent specific rules in this table may be applicable for the Avaya SBC.

Table continues…

GDPR Requirement	General GDPR Rule	Avaya SBC Support
Announcement and transparency on Personal Data Usage	Products that collect, process and/or store personal data and have a user interface to access data must have capability to announce or notify end user of such data.	Avaya SBC has user interface to modify data and also provides APIs to modify data. Avaya SBC does not modify or view personal data, and such notification from the Avaya SBC user interface is not required. In case of any such modification using APIs instead of UI, notification is not required for similar rational as above. Avaya SBC is capable of playing an announcement in case of recording to notify the end user that recording is in progress. Avaya SBC has a capability to interwork on DTMF digits on RTP as per 2833 telephone events to out-of-band SIP Signaling through INFO. In such an interworking case, Avaya SBC should provide an announcement after first collection of digits to notify the end user. In case Avaya SBC is relaying DTMF 2833 telephone events end to end, the role for playing the announcement is not applicable to Avaya SBC but to the entity which consumes the DTMF event.

Table continues…

GDPR Requirement	General GDPR Rule	Avaya SBC Support
Fulfillment of Data subject rights	The architecture should provide privileged users through user interface in case it allows to access, delete modify personal data. In case of absence of user interface, APIs should provide interface for privileged users This rule is not applicable for Personal data which is temporary i.e. less than 24 hours.	Avaya SBC administers network interfaces, network properties, protocol interops and definitions, media rules and policies. Avaya SBC does not have any personal data and there is no requirement for privileged user to access personal data. The personal data stored in Avaya SBC locally is in form of CDRs. In the case of a GDPR-compliant deployment, Avaya SBC should enable the radius interface. This forces all CDRs to be transported via a radius interface to a far end radius server. A high availability of radius interface is also supported in case far end radius server is temporarily unavailable. In case the deployment does not support high availability on the the radius interface, as soon as the radius server comes up all CDRs stored stored in Avaya SBC is pushed to the radius server. Avaya SBC does not store CDRs for more than 24 hours. CDRs should be accessed by privileged user only.
Indicators for call recording	The architecture should provide indications at start of recording for any audio or video call getting recorded. The indication can be in form of visual indication or through announcement	If Avaya SBC records audio or video calls, Avaya SBC plays an announcement at start of recording to notify the end user.
Consent Management	The architecture should provide a user interface to notify consent on viewing/accepting personal data	This is not applicable for Avaya SBC because it does not store any personal data through its UI. In case of other mediums of personal data storage like traces, logs, and CDRs, the storage should be temporary and less than 24 hours beyond which this is redirected to another file server, remote syslog server, or radius server as applicable.

Table continues…

GDPR Requirement	General GDPR Rule	Avaya SBC Support
Personal Data Minimization - processing and storage	The product must only collect and process personal data necessary to perform the purpose of processing. If purpose can be reached without processing and storage of personal data, no processing and storage of personal data should take place	This is not applicable for Avaya SBC. Avaya SBC stores data in resident memory or uses network as storage and maintains minimal set of personal data for media and signal processing The other mediums of storage like logs, traces and CDRs are considered as temporary storage in Avaya SBC.
Privacy by default	The product must ensure by default maximum privacy in protection of personal data	This is not applicable for Avaya SBC. Avaya SBC stores data in resident memory or uses network as storage and maintains minimal set of personal data for media and signal processing The other mediums of storage like logs, traces and CDRs are considered as temporary storage in Avaya SBC.
Unique Access Control for Personal Data	The product shall have an effective, secure and customized access control	The Avaya SBC UI provides role based access control for any change in administration data. Avaya SBC shall also provide role based access control for traces, logs and CDRs.
Security of Processing	The product must implement secured mechanism of processing personal data. This should also be applicable for transit data.	Avaya SBC handles signaling and media which exposes personal data of end user. This data is in transit and at Avaya SBC should be protected using standard encryption mechanism on TLS encryption for signaling and SRTP using SHA-1 and/or SHA-2 for media.
Anonymization and Pseudonymization	The product must define anonymization and pseudonymization techniques to help protect personal data	This is not applicable for Avaya SBC because all personal data is temporary and within 24 hours except for logs and traces which is described in “Fulfillment in Logging and Tracking.”

Table continues…

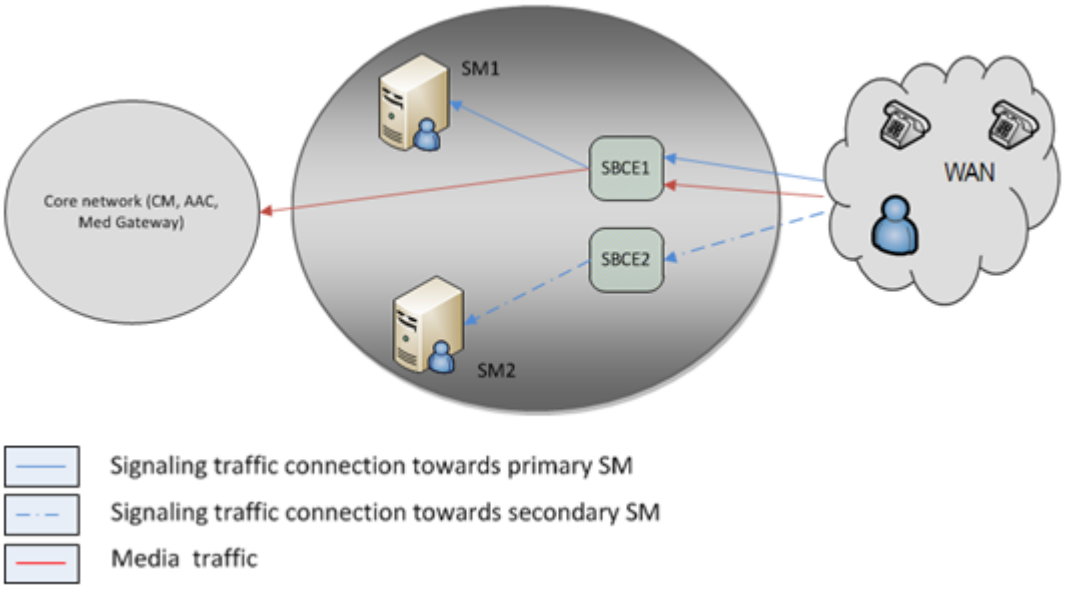
GDPR Requirement	General GDPR Rule	Avaya SBC Support
Fulfillment in Logging and Tracking	The product must describe fulfillment of the requirement around personal data for all logging and tracking mechanism and other solution level interface used for logging and tracking	This is not applicable for Avaya SBC as all logs/traces should not stay more than 24 hours within Avaya SBC and that is considered as temporary data. The logs and traces should be pushed to a remote syslog server on TLS within 24 hours or a lesser time interval administered.
Compliance after Restore operation	The product must comply to personal data compliance after applying a backup and restore	This is not applicable to Avaya SBC.
Documentation of product security	The product must have current security documentation as a prerequisite to any claims of compliance with Data Privacy regulation for Personal Data.	This is not applicable to ASBC as the security documentation is already available
178428-150 Use of Analytics and Diagnostics	The product must support anonymization of any personal data available in any diagnostic , tracing and analytics tool	SBC should anonymize all personal data in trace and logs. Example of personal data is calling party name/number, called party name/number, Identity of user, P-A-I, user name/password, content data in notifies

Geographic-redundant deployment

In a Geographic-redundant deployment, you can deploy two different Avaya SBC devices in two different data centers. You can deploy the devices as individual Avaya SBC devices or devices managed by their own EMS. You can deploy these Avaya SBC devices in a High Availability mode or a non-High Availability mode. You can deploy EMS in High Availability mode in different data centers only if layer 3 connectivity is available between the two data centers.

Geographic-redundant deployment in the non-HA mode

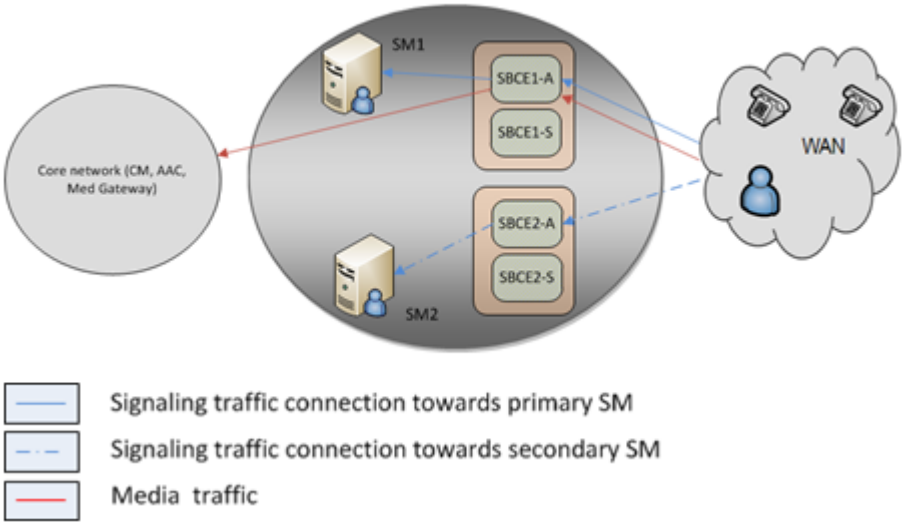
In the following diagram, SBC1 and SBC2 are two different physical devices deployed in different data centers. The endpoints have one connection with SBC1 corresponding to the primary Session Manager, SM1. The second connection with SBC2 corresponds to the secondary Session Manager, SM2.



Geographic-redundant deployment in the HA mode

In the following diagram, SBC1 and SBC2 are two different physical devices that are deployed in an HA mode in different data centers. The endpoints have one connection with SBC1-A, that is Active SBC corresponding to the primary Session Manager, SM1. The second connection is with SBC2-A, Active SBC corresponding to the secondary Session Manager, SM2.

During an SBC1-A fail over, SBC1-S, which is the standby Avaya SBC, handles the media of the active calls. During an SBC2-A fail over, SBC2-S, which is the standby Avaya SBC, handles the media of the active calls.



IP Office trunk support from a dynamic IP address

Avaya SBC 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 SBC resolves the FQDN entry again for all Remote Branch Office servers. If the DNS record TTL value expires, Avaya SBC queries the DNS for all FQDN entries in the server configuration.

Note:

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

IPv6 support

Avaya SBC supports both IPv4 and IPv6 addresses to PSTN (public) SIP trunk servers and private enterprise SIP trunk servers. Avaya SBC uses dual stack nodes that run both IPv4 and IPv6.

In addition to standard IPv4 support, Avaya SBC supports the following features using IPv6:

- 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 SBC relies on configuration policies to determine the address types to be tried.
- IPv6 communication with EMS.

Avaya SBC supports:

- IPv6 communication with SIP recording server.
- IPv6 in Remote Worker deployments.

Avaya SBC supports the following features over IPv6:

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

Avaya SBC 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 SBC receives an SDP offer with ANAT semantics, Avaya SBC:

- 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.

Avaya SBC supports ANAT RFC for audio and video on SIP trunk and Remote Worker deployments. Avaya SBC learns from Registration messages whether remote workers are capable of supporting ANAT and dual stack media interfaces.

SIP entities that generate an SDP offer with ANAT semantics place the sdp-anat-option-tag in the **Require header** field. Avaya SBC supports the sdp-anat-option tag. Avaya SBC supports UDP/RTP, TCP/RTP, TLS/SRTP, and other 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*.

Avaya SBC also supports the following IPv6-related features:

- Avaya SBC terminates SIP IPv6 signaling and converts all SIP signaling headers to corresponding SIP IPv4 addresses. By doing this, Avaya SBC does not expose any IPv6 SIP address anywhere within Avaya Aura® core services.
- When Session Manager also supports SIP IPv6 addresses, you can set a tolerance flag on Avaya SBC to that Avaya SBC may not do a strict conversion or hiding of SIP IPv6 address and pass the IP address to Session Manager.
- Avaya SBC can learn the IPv4 and IPv6 address family dynamically for media and signaling for automatic configuration.
- Avaya SBC supports NAT64 interworking with PSTN providers.
- Avaya SBC supports call flows from mobile PSTNs on IPv6 or IPv4 to dual stack WiFi using both media and signaling services.
- Avaya SBC supports IPv6 to IPv4 conversion on HTTP and PPM messages.
- Avaya SBC does not support TURN on IPv6 nor interworking of IPv6 an IPv4 on TURN media.

Media anchoring

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

Media encryption by using AES-256

Advanced Encryption Standard (AES) is a widely used specification for data encryption. Avaya SBC 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 SBC 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

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

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.

Multi-tenancy

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

This scenario uses all four Avaya SBC data interfaces. Avaya SBC connects to two tenant networks, each with a unique set of remote workers. Avaya SBC 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 SBC interfaces

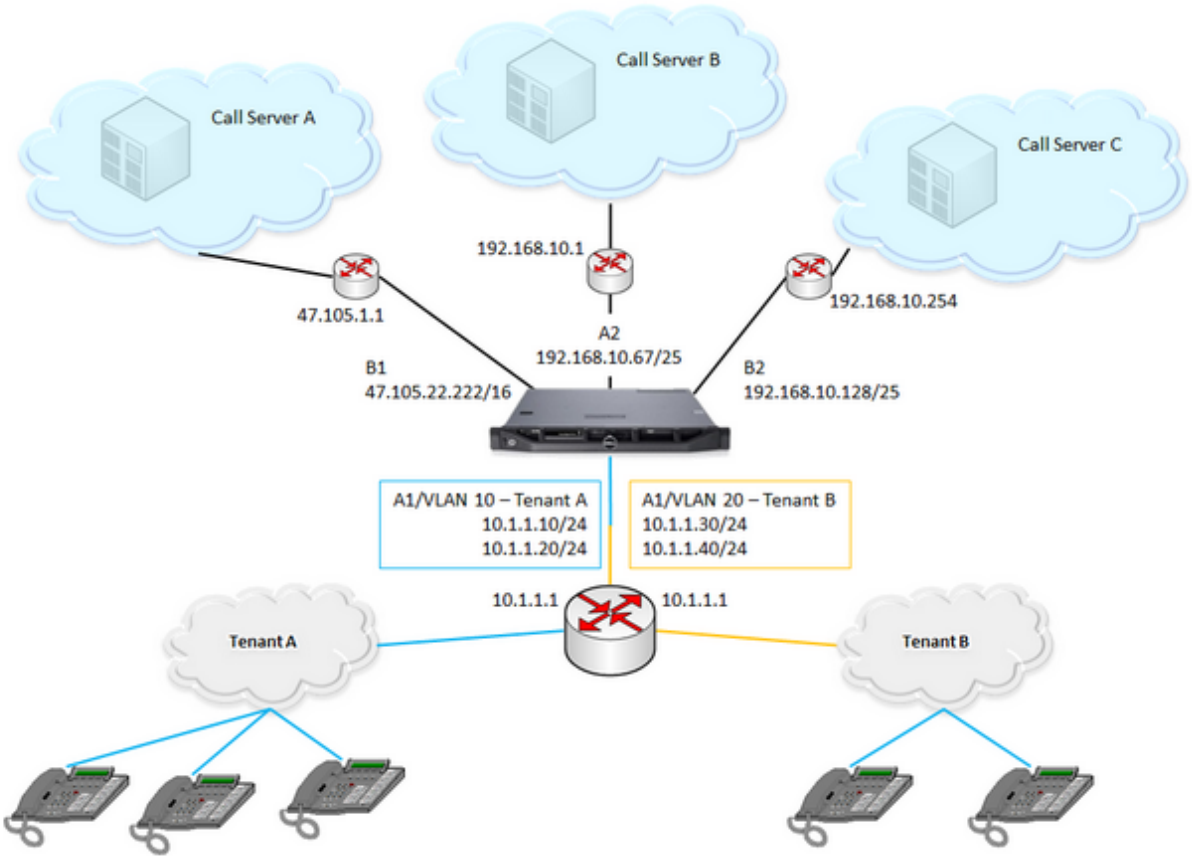


Figure 9: Multiple tenants, call servers, and Avaya SBC interfaces

- **Interfaces and purposes**: The A1 interface of Avaya SBC 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 SBC 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 SBC is running on a virtual machine, configure VMWare vSwitch and the physical interfaces on the server. If each physical interface on Avaya SBC 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 SBC **Network interfaces**: When you configure VLANs on Avaya SBC, 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 SBC. Finally, enable all the interfaces: the two VLANs as well as A2, B1, and B2.
- **Networks connected to** Avaya SBC: In this example, Avaya SBC 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 SBC supports the use of the same IP address on multiple data interfaces in Avaya SBC. 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 SBC.

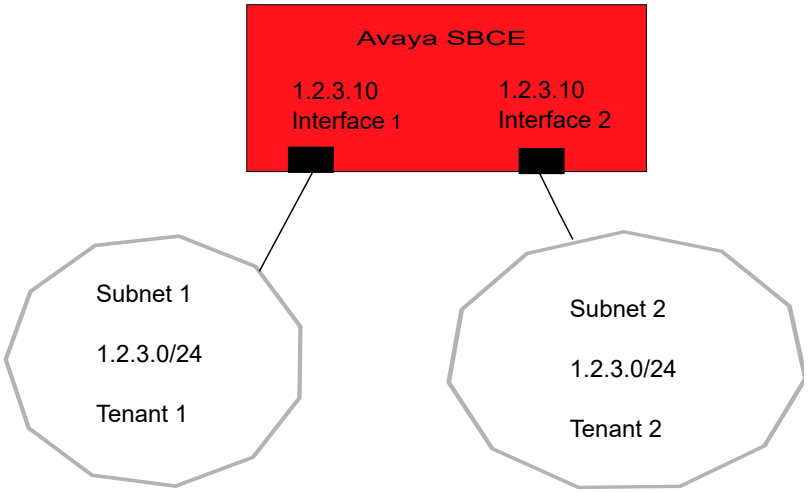


Figure 10: Same IP address used on different interfaces

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 SBC 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 SBC IPs and gateways with an interface.

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

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

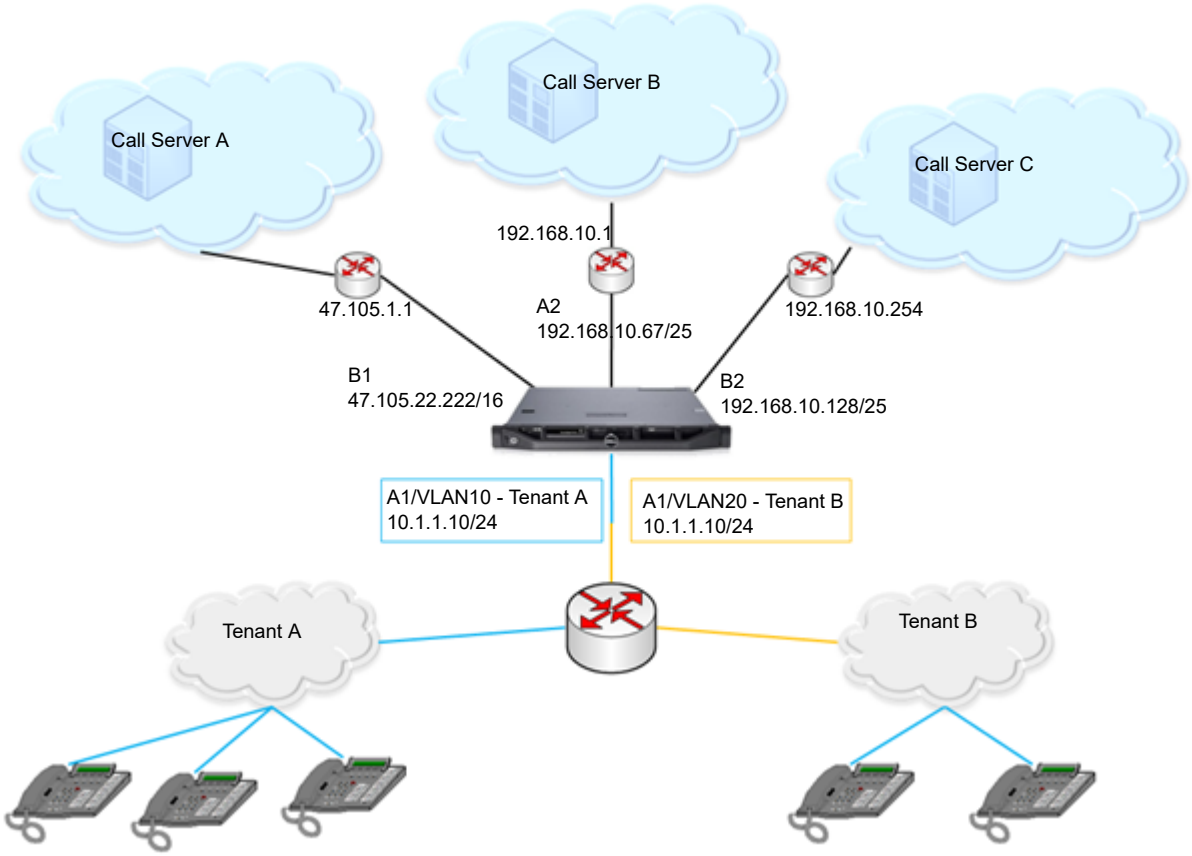


Figure 11: Multiple tenants using the same IP address

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

Interfaces and purposes:

The A1 interface of Avaya SBC 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 SBC 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 SBC 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 SBC multiple times, select the **Allow Non-unique IPs for Complex Networks** field on the Network Options page. To configure VLANs on Avaya SBC, 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 SBC. Finally, enable all the interfaces: the two VLANs as well as A2, B1, and B2.

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

Multiple subnet and multiple interfaces

Multiple subnets

With Avaya SBC, customers can connect to multiple subnets from a single interface. Avaya SBC 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.

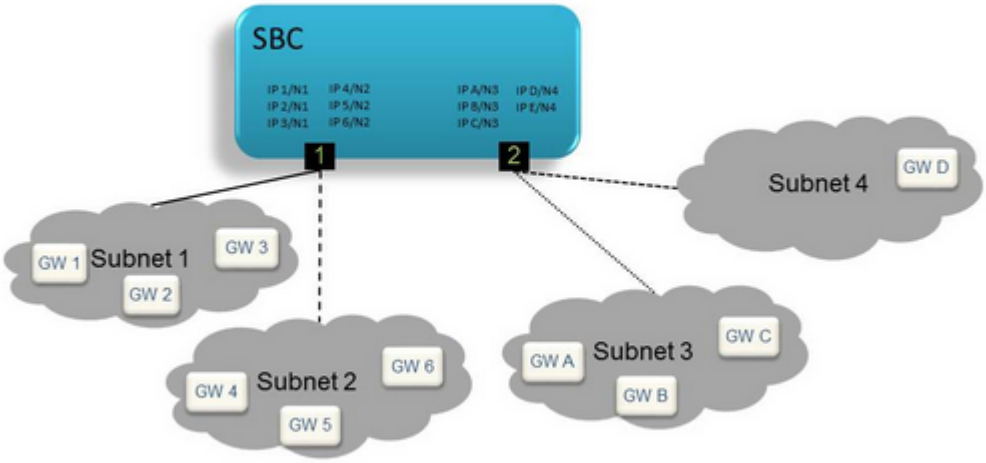


Figure 12: Connectivity to multiple subnets on a single data interface

In Figure 12: 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 SBC 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 SBC. However, Avaya SBC can distinguish between the connections. Although multiple endpoints use the same IP address, the networks in which the endpoints reside are physically distinct. Avaya SBC 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 SBC supports VLANs only on the data interfaces.

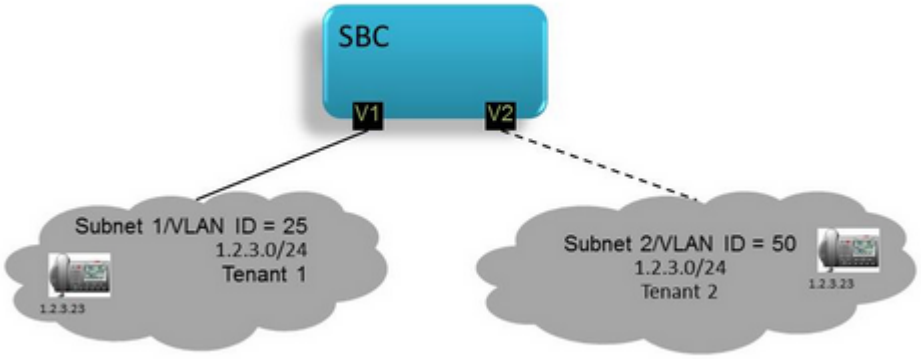


Figure 13: VLAN support

Deployment examples

Avaya SBC connected to multiple subnets on a single interface

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

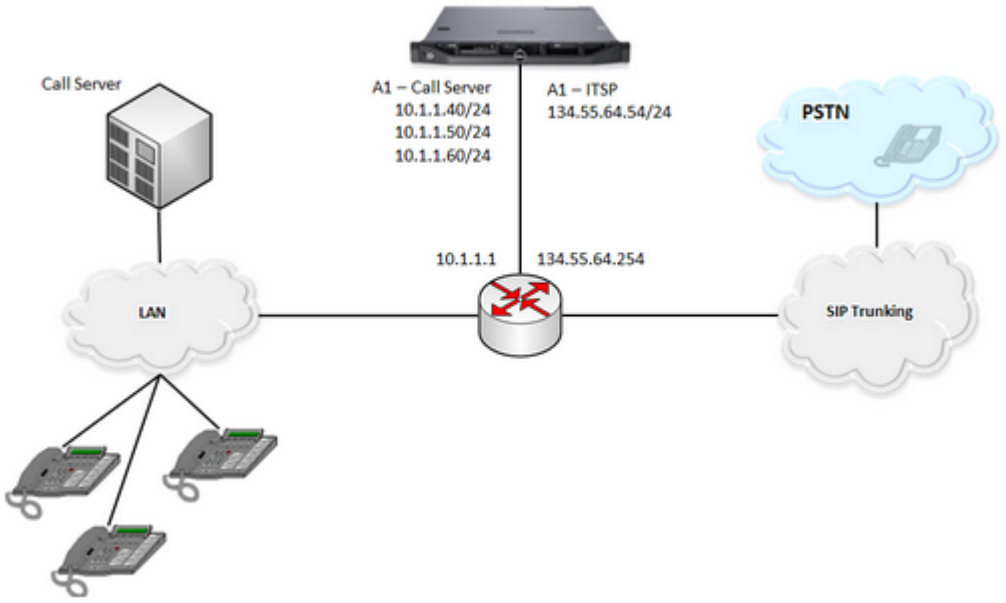


Figure 14: Avaya SBC connected to multiple subnets on a single interface

Configuration details

- **Interfaces and purposes**: This configuration uses only the A1 Avaya SBC 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 SBC 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 SBC: In this configuration, two networks are added to the same Avaya SBC 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 SBC data interface, add the networks to the same interface when you define the networks.

Avaya SBC connected to multiple subnets on two interfaces

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

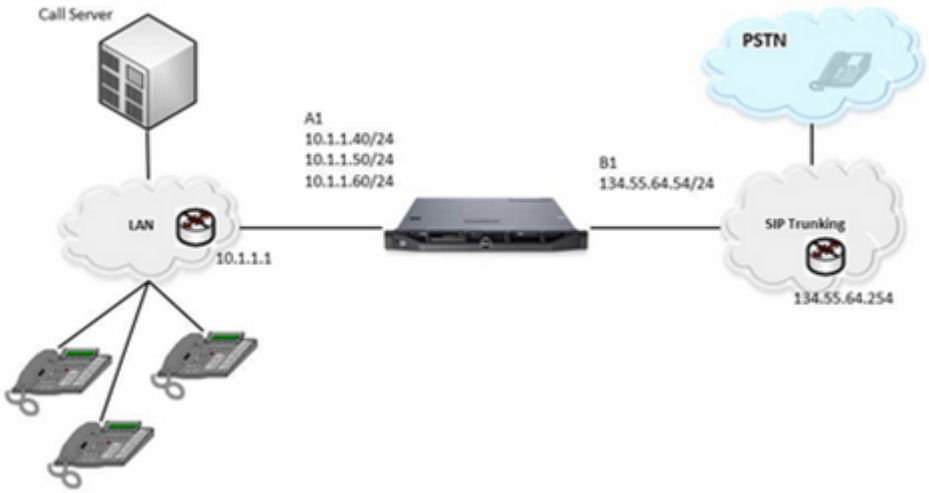


Figure 15: Avaya SBC connected to multiple subnets on two data interfaces

Configuration details

- Avaya SBC **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 SBC subnets or VLAN tagging.
- Avaya SBC **network interfaces**: This scenario uses the A1 and B1 interfaces. Ensure that you configure the required interfaces.
- **Networks connected to** Avaya SBC: In this example, Avaya SBC 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 SBC. Use the **Networks** tab in **Network & Flows** > **Network Management** to define the network.
- **Other** Avaya SBC **setup**: To configure media and signaling interfaces, flows, and routing profiles, see the related sections.

Avaya SBC connected to multiple subnets by using a single VLAN

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

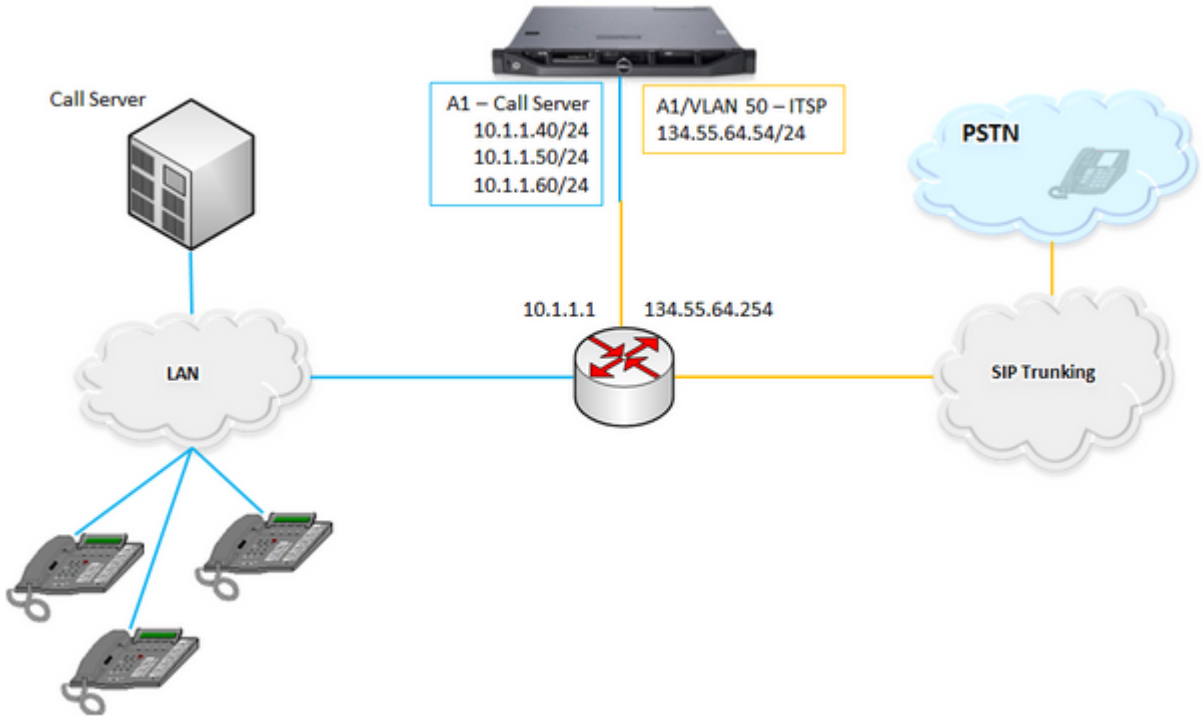


Figure 16: Avaya SBC connected to multiple subnets, using a single VLAN and a single data interface

Configuration details

- **Interfaces and purposes**: In this scenario, only the A1 Avaya SBC 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 SBC IP addresses are required for the call server network, one VLAN interface on the A1 physical interface, and one Avaya SBC 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 SBC on the ITSP network must contain a VID of 50. To enable VLAN tagging, create a VLAN interface. VLAN interfaces on Avaya SBC use the underlying facilities of a physical interface A1, A2, B1, or B2. Packets leaving and entering Avaya SBC on VLAN use the physical link connected to the associated physical interface. Define VLAN interface to connect Avaya SBC 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 SBC: 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.

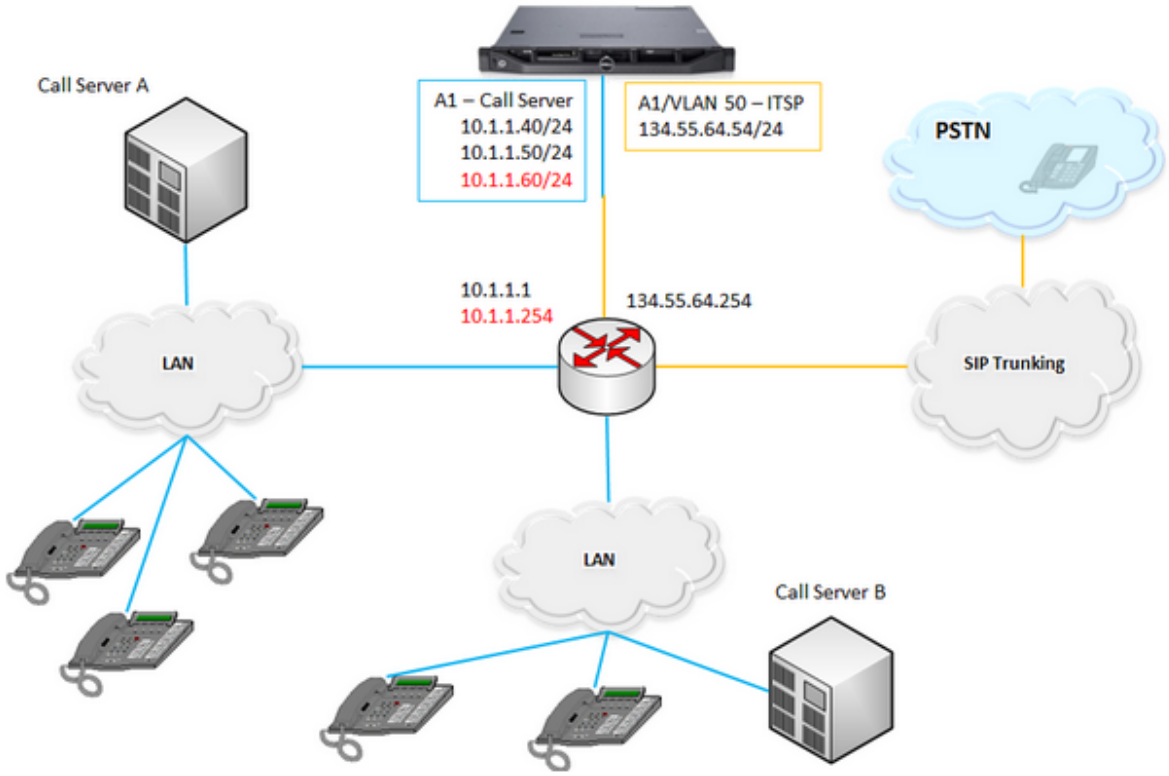


Figure 17: Multiple gateways on the same network

Configuration details

- **Interfaces and purposes**: Only one Avaya SBC interface connects to both, the call server and ITSP networks. Because the call server network has multiple gateway routers , one of the Avaya SBC 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 SBC 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.
- Avaya 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 SBC: The ITSP network configuration is the same as in the earlier examples. For each attached network, define a default gateway router. Each Avaya

SBC IP address on the network can override the default gateway IP address, if necessary. For example, Avaya SBC uses 10.1.1.254 as the next-hop router instead of 10.1.1.1.

Password policies

The `root` and `ipcs` passwords are set during product installation. The EMS GUI has a separate password.

The default user IDs and passwords are the following:

Username	Password
`root`	`@V@Y@_123`
`ipcs`	`Avaya_123`
`ucsec` (GUI only)	`ucsec`

Note:

After the factory reset, the golden password for the root user ID is `Avaya_123`.

Security alert:

You must change the default passwords for the CLI root and ipcs user IDs after the first boot during the installation procedure. When prompted, you must enter and confirm the new password. Password restrictions are enforced on the root, ucsec, and ipcs user IDs. The new password must meet the following criteria:

- Contains at least eight characters.
- Contains one uppercase letter, one lowercase letter, and one number.
- Contains one special character from the following: a hyphen (-), an underscore (_), the at sign (@), an asterisk (*), or the exclamation mark (!). Do not use the pound sign (#), the dollar sign ($), or an ampersand (&).

Server status

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. The Server Status screen displays the list of servers based on the settings on the Server Configuration screen.

Note:

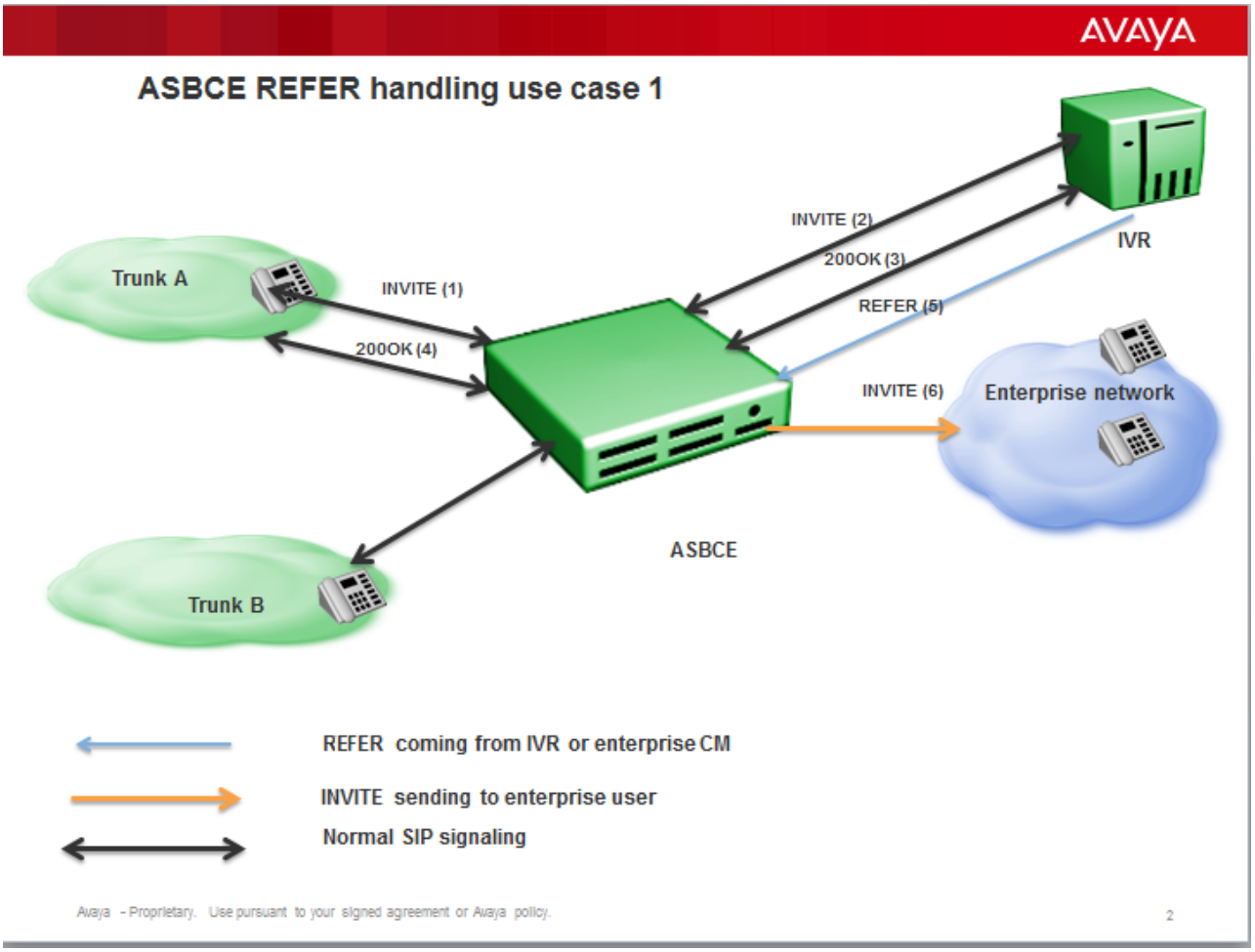
For the servers to appear in the Status window, you must configure the server heartbeat in Server Configuration.

REFER Handling

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

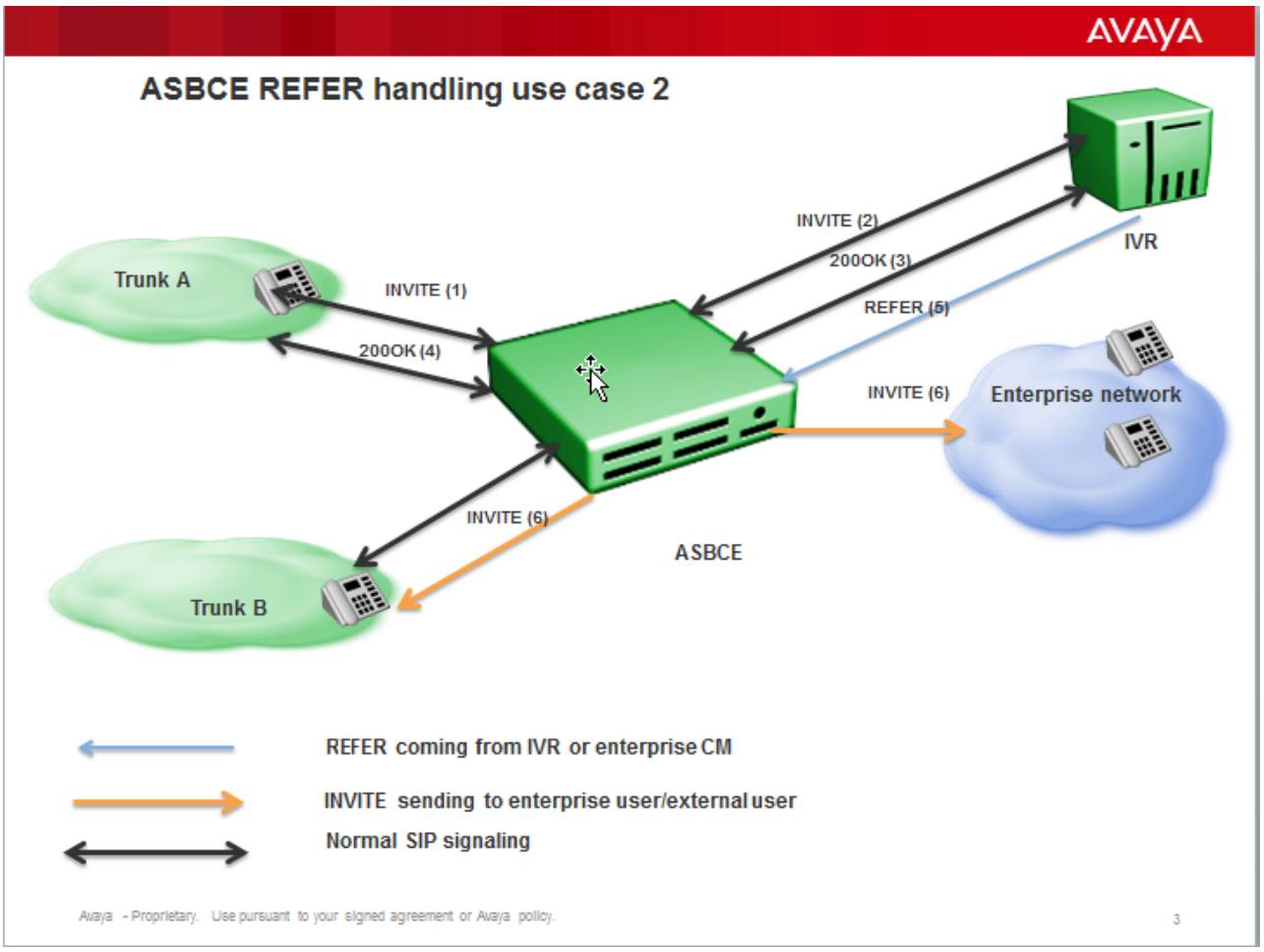
Use case 1

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



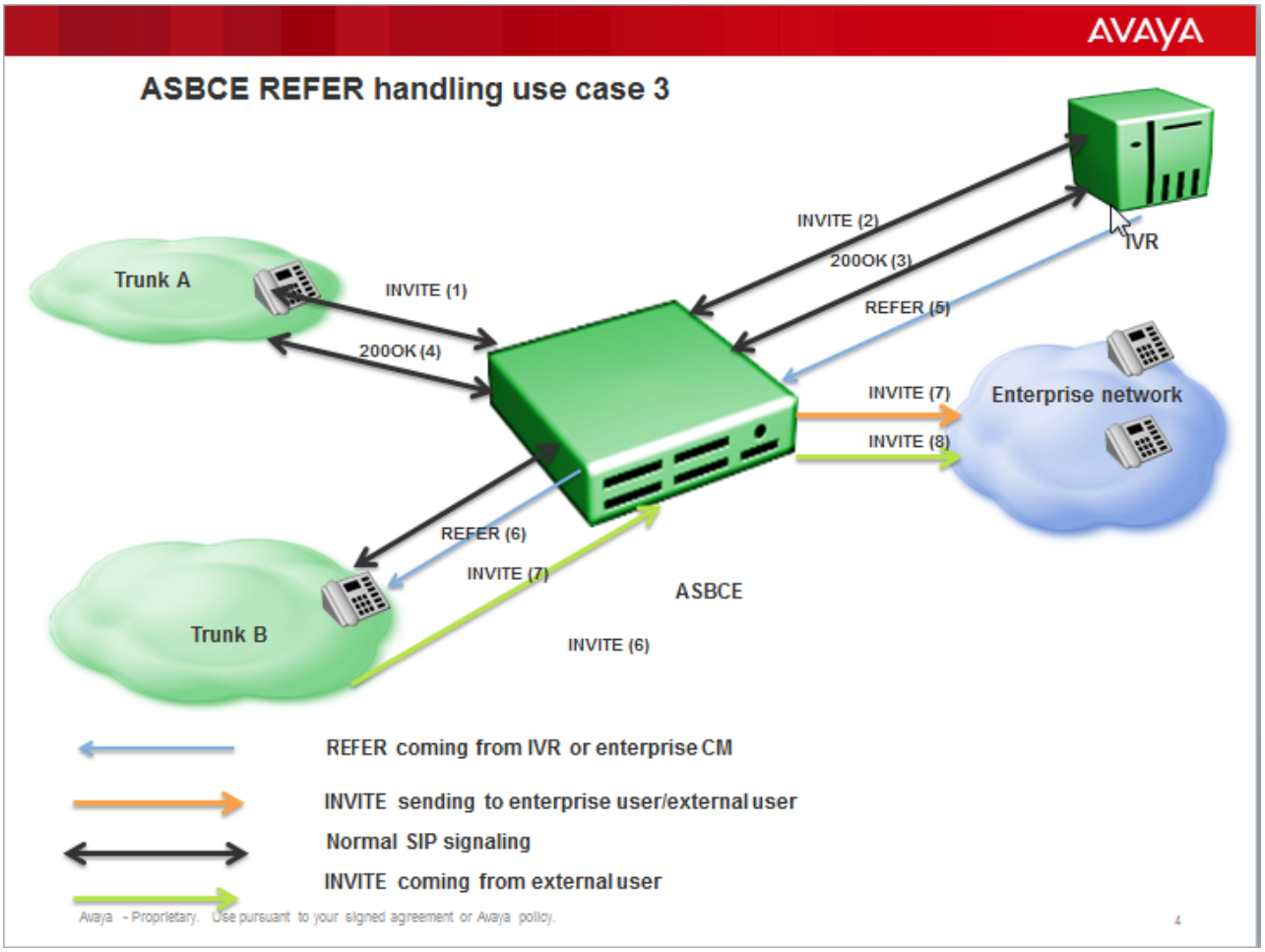
Use case 2

Avaya SBC 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 SBC should always route the new INVITE towards the enterprise server as Avaya SBC cannot find the dialog to replace.



Use case 3

Based on URI group configuration under refer handling configuration, Avaya SBC 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.



Reinvite handling

Some customers and service providers do not want reinvite messages to be passed on to the SIP trunk. Avaya SBC 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.

Remote access for Dell and HP servers

The integrated Dell Remote Access Controller (iDRAC) and HP integrated Lights-Out (iLO) features are management tools that provide powerful remote server management features, including control to remotely turn a server on or off.

You can use iDRAC features to troubleshoot and diagnose issues during a remote server restart. Avaya SBC supports system monitoring and management to 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.

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*.

Similarly, to upgrade from iLO 3 to iLO 4, you must purchase another license from HP.

Supported hardware platforms

The following table shows which Dell and HP platforms support the Dell iDRAC and HP iLO features on Avaya SBC:

Platform	iDRAC or iLO support
Dell R320	Does not support iDRAC.
Dell R620	Does not support iDRAC.
Dell R630	Supports iDRAC 8 express.
Dell R640	Supports iDRAC 9 express.
HP DL360 G8	Does not support iLO.
HP DL360 G9	Supports iLO 4.

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

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 SBC 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 SBC in the enterprise DMZ decrypts the SRTP media coming in to the enterprise from the external IP network or the Internet. The Avaya SBC performs any required Network Address Translation (NAT), analyzes traffic for anomalous behavior, and applies the relevant UC media policies. The Avaya SBC in the DMZ passes the RTP stream to the intended recipient.

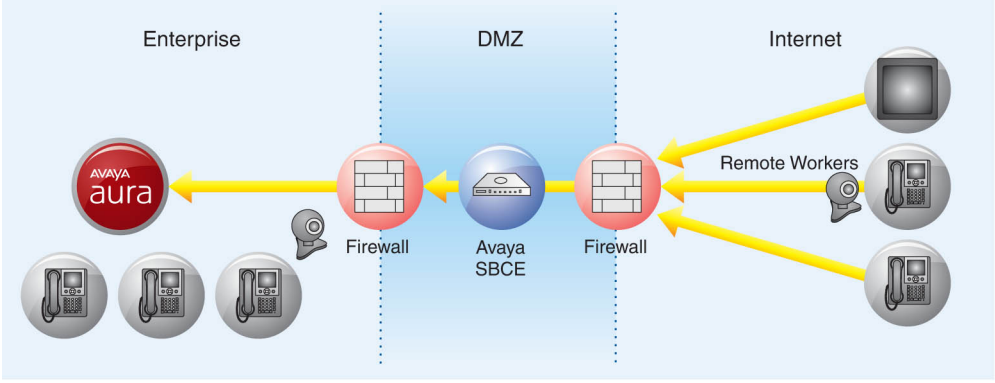


Figure 18: Remote worker

Reuse of connection established by IP Office for delivering calls

Avaya SBC 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 SBC 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 SBC with the TLS Client Certificate presented by IP Office.

If the TLS connection from the Remote Branch Office drops, Avaya SBC rejects calls originating from the enterprise until the connection is reestablished. Meanwhile, Avaya SBC 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.

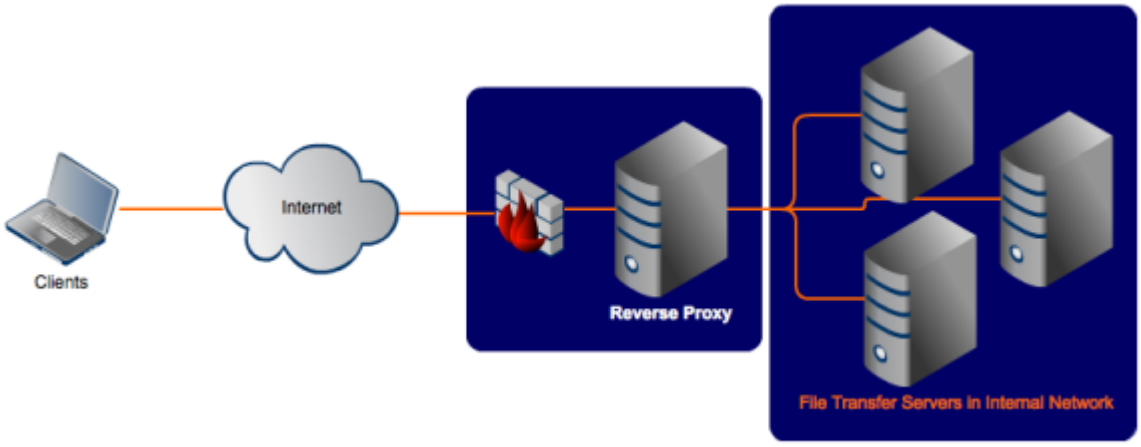
Reverse proxy

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 non-encrypted 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.

RTCP Monitoring

The RTCP monitoring feature in Avaya SBC updates RTCP packet with appropriate endpoint IP address and hop information. Endpoints are configured to send RTCPMON messages to the Avaya SBC to which the endpoint is registered. A single Avaya SBC is designated core Avaya SBC which is sent to Prognosis. Avaya SBC maintains the RTCP port mapping and updates this mapping on a per call basis as part of the SIP signaling. Avaya SBC 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 SBC tracerouting feature implementation reuses the linux based tracerouting APIs.
- The ICMP/UDP/TCP Avaya SBC configuration modes can use tracerouting and can be administered from GUI.

On receiving RTCPMON message for Prognosis, Avaya SBC does a lookup in RTCP port-mapping. Avaya SBC then modifies the remote IP address and RTCP Port in rtcp message Avaya Subtype 4, based on the mapping. Avaya SBC then appends the trace hop information of the next network node where the RTP packets are forwarded in Avaya Subtype 5. If this Avaya SBC is the designated core Avaya SBC, then perform additional steps before forwarding the packets to Prognosis. Determine the SSRC field from RTCP monitoring packets from endpoint, for example SSRC1. Avaya SBC also determines the SSRC of the incoming RTP stream from media gateway or caller, for example SSRC2. Avaya SBC 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] up to the Core Avaya SBC – Populated from the RTCPMON Subtype 5 Message.

- Traceroute information for all the hops from the endpoint [Callee] up to the Core Avaya SBC – Populated from the RTCPMON Subtype 5 Message.

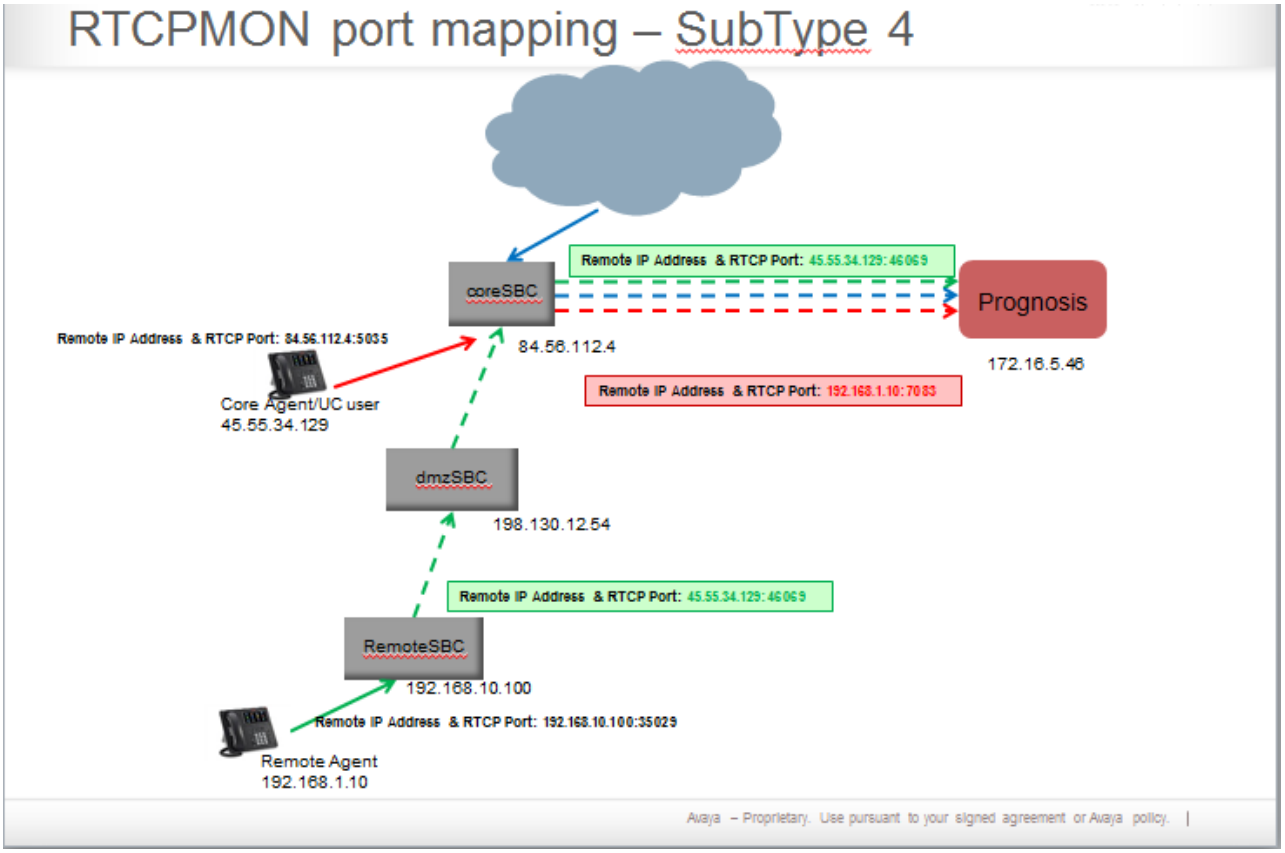
If mapping exists in the Avaya SBC for SSRC1 and SSRC2, then Avaya SBC uses the mapping information to rewrite the following in the RTCPMON packets to be sent to Prognosis:

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

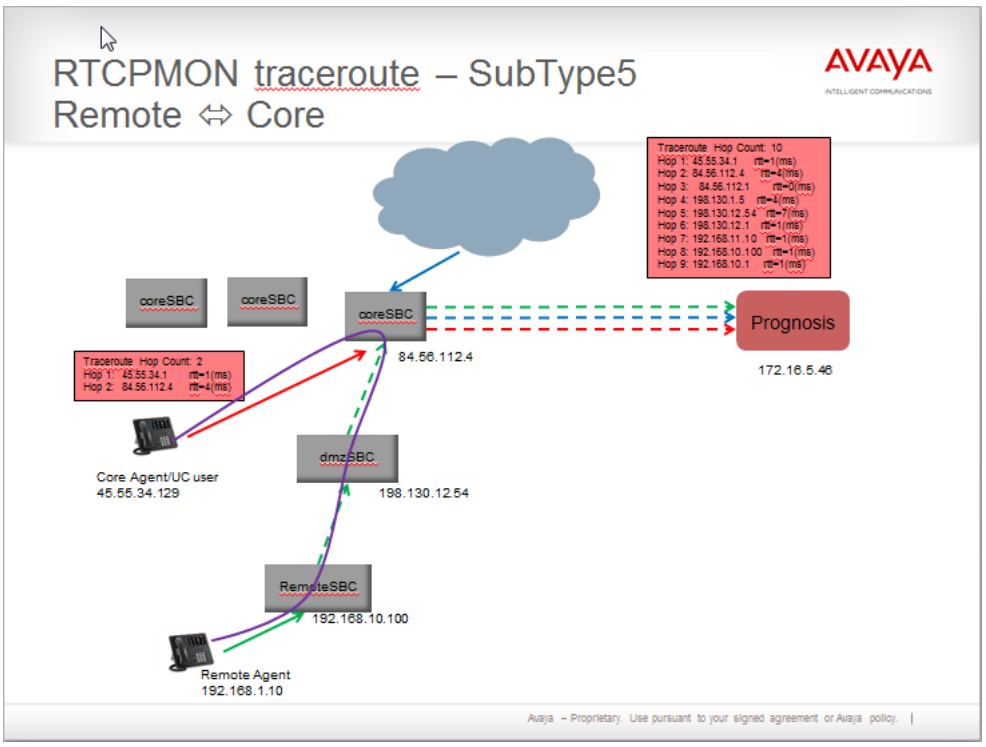
Processed RTCPMON packets will now be sent to Prognosis based on the information filled in by Avaya SBC.

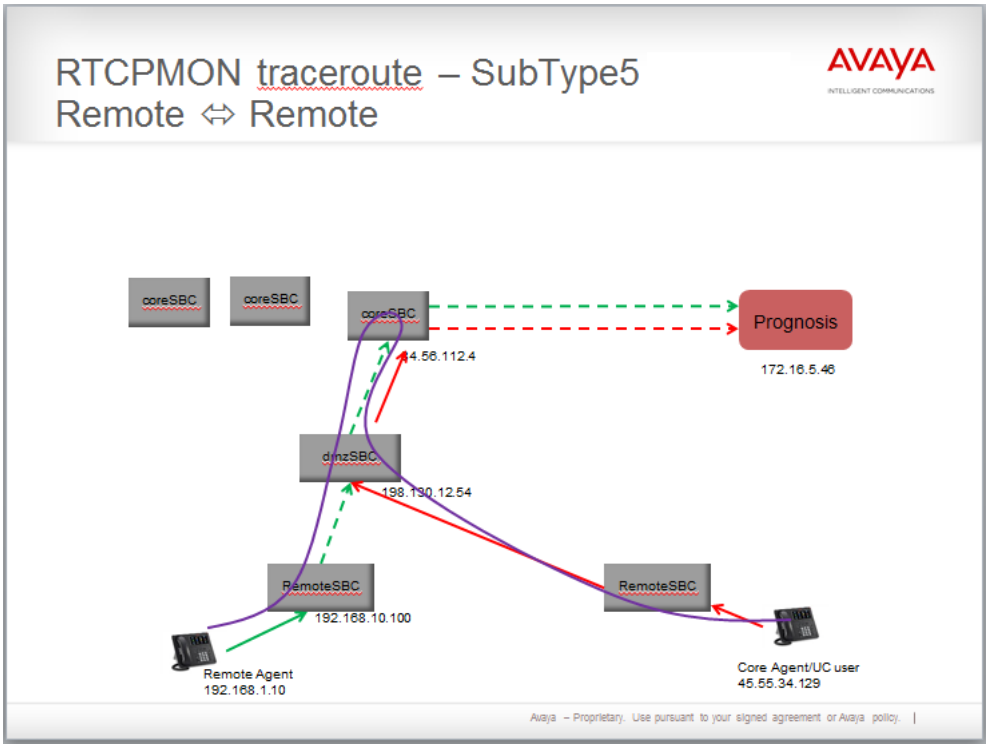
Modes of configuration

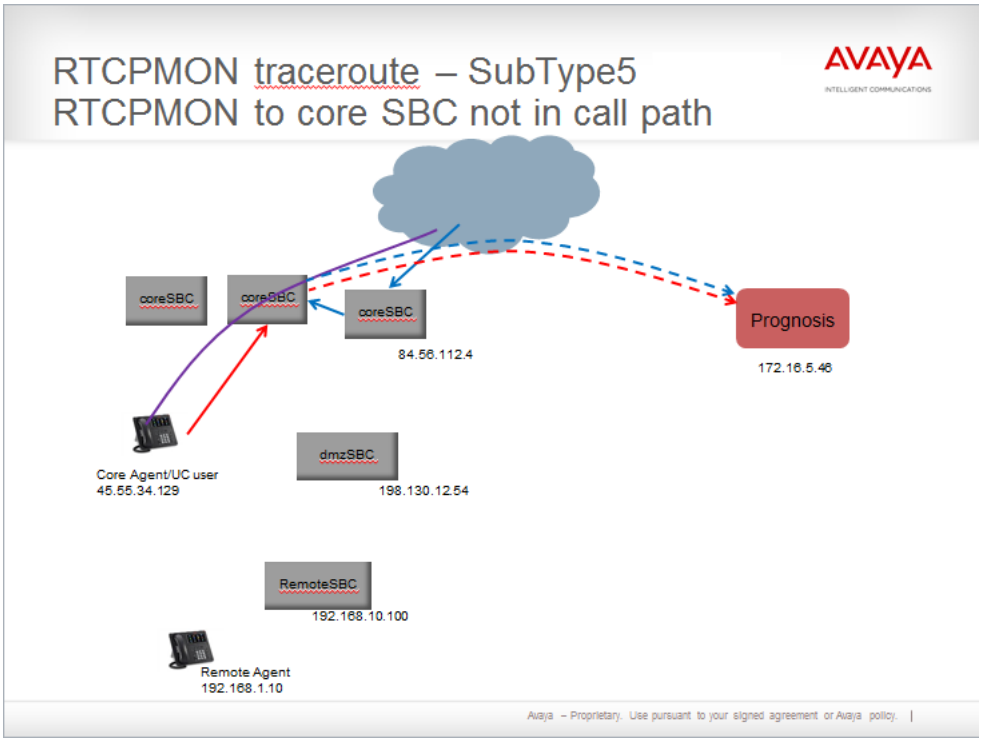
- **END-end Rewrite:** Avaya SBC updates the RTCP subtype-4 packet from the media terminating endpoint. In Subtype-4, Avaya SBC rewrites the Remote IP Address field with the Remote endpoint address who is the recipient of the RTCP packets. End-end rewrite must be configured in all Avaya SBC devices which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



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


RTCPMON traceroute – SubType5
Remote ⇔ Core
AVAYA
INTELLIGENT COMMUNICATIONS
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=3(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
Remote ⇔ Remote
AVAYA
INTELLIGENT COMMUNICATIONS
coreSBC
coreSBC
coreSBC
4.56.112.4
Prognosis
172.16.5.46
dmzSBC
198.130.12.54
RemoteSBC
192.168.10.100
RemoteSBC
Remote Agent
192.168.1.10
Core Agent/UC user
45.55.34.129
Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy.



- **Bridging:** Avaya SBC 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 SBC devices.

Note:

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

RTCP monitoring report generation

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

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

This feature is applicable only for SIP trunks.

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 SBC provides a secure proxy that must be deployed in the enterprise DMZ. Avaya SBC 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 SBC 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 SBC 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 SBC. After authentication failure, Avaya SBC rejects all subsequent messages from the Avaya one-X® Mobile.
- After authentication, Avaya SBC forwards all messages from Avaya one-X® Mobile to the CES server.

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

Serviceability Agent

Avaya SBC 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 SBC to:

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

To ensure that you can view Avaya SBC 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*.

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.

Single Sign-On and Identity Engine

Avaya SBC 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 SBC external address.

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 SBC 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 SBC for processing.

If the signaling traffic is encrypted, the Avaya SBC 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 SBC in the DMZ. The SBC then looks for anomalous behavior in the media before passing the RTP/SRTP stream on to the intended endpoint.

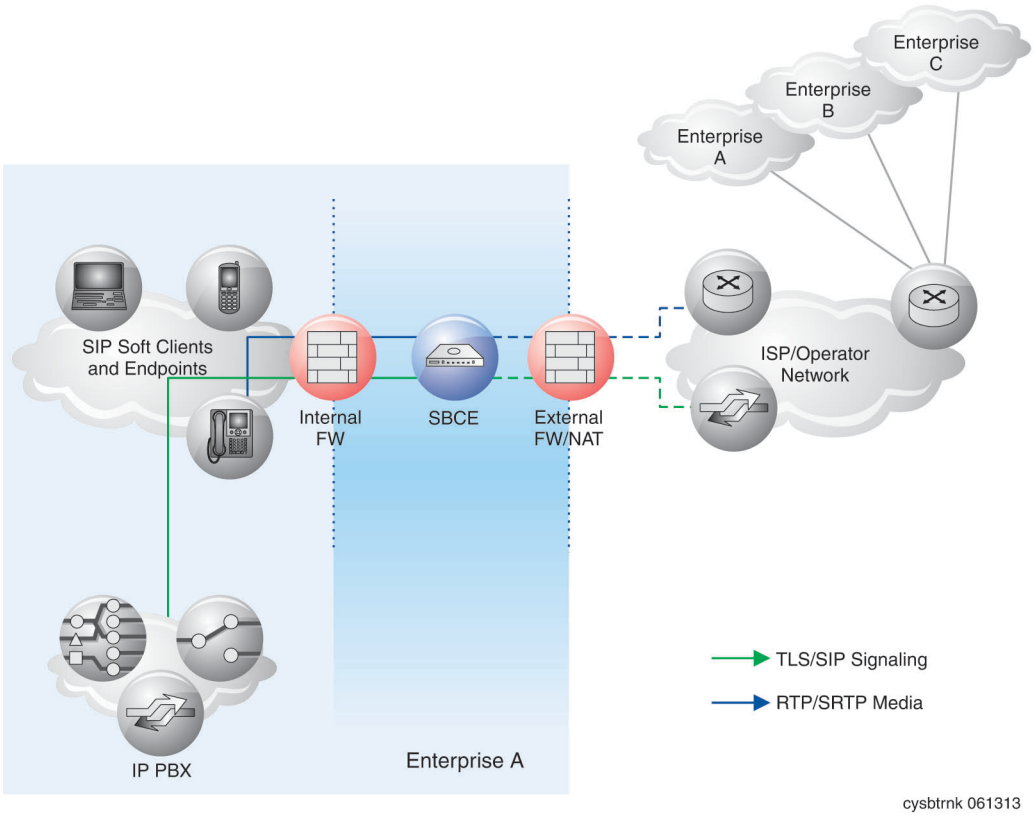


Figure 19: SIP Trunking

SIPREC-based recording solution

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

- Avaya SBC 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

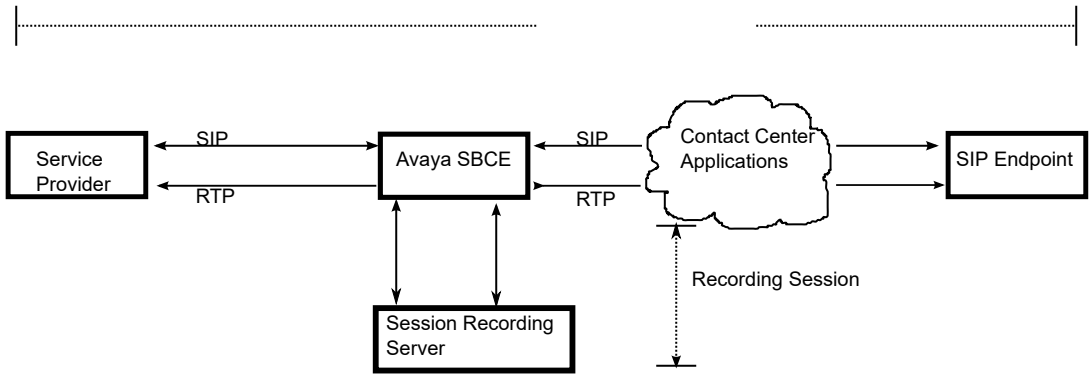


Figure 20: SIPREC-based recording solution architecture

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

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

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

Features for session recording

The following Avaya SBC 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 SBC starts a timer. When the timer expires, Avaya SBC triggers alternate routing mechanisms. Avaya SBC 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 SBC communicates with a cluster of Recording Servers. You must administer a URL for each Recording Server in the cluster. Avaya SBC sends an INVITE message to the Recording Server. When Avaya SBC 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 SBC 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 SBC uses only the controls specified from Avaya SBC and at the recording server.
- Unique labels for media streams to identify the media stream for participants in the recording session.
- Security options.

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

  Note:

  For SIPREC, Avaya SBC 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 SBC receives media streams and relays them to the Recording Server. Avaya SBC does not change any data in the media streams.

In addition, Avaya SBC provides the following features:

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

  When Avaya SBC initiates a session towards every configured recording server, there can be scenarios when none of the servers respond. In such scenarios, Avaya SBC 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 SBC 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.

Licensing for SIPREC sessions

A single SIPREC session requires one standard license and one advanced license for every non-encrypted recorded call. A single SIPREC session on an encrypted call also requires one standard license and one advanced license. However, an encrypted call with multiple SIPREC sessions requires one standard license and multiple advanced licenses depending on the number of SIPREC sessions.

For example, a SIP trunk call that is being recorded across three destinations requires one standard license and one advanced license for the SIP trunk call, plus two additional advanced licenses, for a total of one standard license and three advanced licenses. The same rules apply for an encrypted SIP trunk being recorded across three destinations: one standard license and three advanced licenses.

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 SBC 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 SBC to stream the media and metadata for that communication session to the active recording server.

SRTP overview

Avaya SBC 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 SBC 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 SBC.

Avaya SBC does not use Master Key Identifier (MKI) and encrypted RTCP for Avaya Meetings Server interoperability. Avaya SBC negotiates the SDP session by using non-encrypted RTCP.

Note:

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

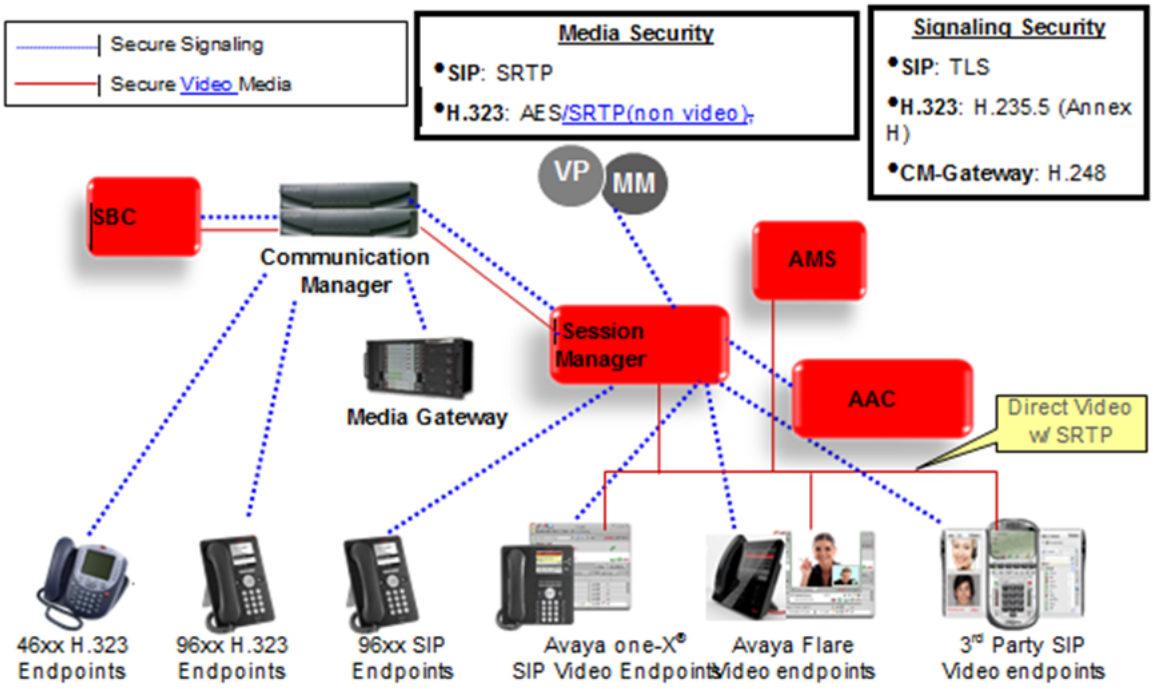
SRTP considerations

Avaya SBC 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.

SRTP video

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 scenarios

- Desktop users – Avaya SIP video endpoint, such as Avaya one-X® Communicator-to-Avaya one-X® Communicator SRTP-encrypted SIP video calls: 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 Avaya one-X® Communicator and third party (SIP) video endpoints: Third-party devices can be registered to the URI as with Avaya one-X® Communicator. However, a 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.

traceSBC

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 non-encrypted private key of the Avaya SBC 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 SBC 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 SBC. traceSBC can also process log files real time on Avaya SBC, 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 testing.

Note:

In Release 10.1.2, traceSBC tool can only be run as "root" user.

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 SBC can log SIP messages as processed by different subsystems and also log PPM messages. The traceSBC utility can process the log files in real-time by opening the most recent 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 of the file reaches the limit of about 10 MBytes.

Log locations:

The traceSBC logs for SIP are available at:

`/archive/log/tracesbc/tracesbc_sip`

The traceSBC logs for PPM are available 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`

Performance benefits

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 non real-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.

Transcoding

Transcoding translates a media stream encoded by using one codec into a media codec encoded by using another codec. Avaya SBC 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 SBC:

- 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 SBC supports audio transcoding and transcoding for trunk deployments. All transcoded calls are anchored to Avaya SBC. If a call has both audio and video lines, Avaya SBC only transcodes the audio. Video calls that require transcoding are converted to audio calls.

Note:

FAX transcoding is not supported.

Supported transcoding capacities

Server name	Maximum transcoded sessions	Maximum non-transcoded sessions
HP DL360 G8	200	6000
Dell R320	200	6000
Dell R620	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 second hold/talk time.

Codecs supported for transcoding

The following codecs are supported for transcoding:

- G711
- G711A
- G711MU
- G711U
- G722
- G726-32

  This codec is available only when **AMS Offloading** is enabled.
- G729
- G729AB
- H224
- H264/SVC
- OPUS Constrained Narrow Band
- OPUS Narrow Band
- OPUS Wide Band
- PCMA
- PCMU
- AMR-WB
- AMR-NB

The following codecs are supported specifically for Teams:

- G711A
- G711U
- G722
- G729
- OPUS

Any codecs not listed here that are used for calls passing through Avaya SBC do not receive any transcoding treatment from Avaya SBC and are simply relayed through the system.

Note:

Avaya SBC does not support the SILK codec, and it can be filtered if required.

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.

Avaya Aura® Contact Center

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

Avaya Aura® Call Center Elite

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

User registration

You can view the list of users that are registered through Avaya SBC 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.

Virtualized environment platforms

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.

The Virtualized Environment project applies only for VMware and does not include any other industry hypervisor. Virtualized Environment project is inclusive of the Avaya Aura® portfolio.

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

You can deploy EMS and SBC software using a single OVA file.

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

The Avaya SBC OVA files are offered as vAppliance for EMS and Avaya SBC configurations. The OVA file is available the Avaya Support Site or from the Avaya Product Licensing and Delivery System (PLDS).

For more information, see *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*.

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 SBC on a VLAN use a physical link connected to a physical interface.

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

Note:

A VLAN is supported on data and signaling interface.

WebRTC-enabled call handling

Avaya SBC 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 SBC in DMZ. In this scenario, Avaya SBC, 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 SBC 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 SBC.

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

Avaya SBC 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 Connect Reference*.

Chapter 3: Interoperability

Product compatibility

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

Interoperability

For information about server compatibility, supported device configurations, third-party product interoperability, and operating system compatibility, refer to *Deploying Avaya Session Border Controller on a Hardware Platform*.

Chapter 4: Performance specifications

Capacity and scalability specification

High-capacity servers

Solutions	Server Type			
	Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance - Profile 5	**Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance - Profile 3**	**Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A3**	**Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A2**
Non-encrypted Sessions	25,000	14,000	25,000	14,000
Encrypted Sessions	20,000	9,000	20,000	9,000
Remote Worker Users (Sessions)	20,000 (10,000)	20,000 (8,000)	20,000 (10,000)	20,000 (8,000)
Avaya Meetings ServerVideo Sessions	800	800	800	800
Transcoding Sessions	1000	1000	1000	1000
TURN/STUN Audio-only Sessions	10,000	6,000	10,000	6,000
TURN/STUN Audio and Video Sessions	1,000	1,000	1,000	1,000
TURN/STUN Tunneling Audio-only Sessions	600	600	600	600
TURN/STUN Tunneling Audio and Video Sessions	300	300	300	300

Table continues…

Solutions	Server Type			
	Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance - Profile 5	Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance - Profile 3	Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A3	Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A2
HTTP Media Audio-only Tunneling Sessions	220	220	220	220
HTTP Media Audio and Video Tunneling Sessions	110	110	110	110

Mid-capacity servers

Solutions	Server Type			
	Dell™ PowerEdge™ R340 Avaya Solutions Platform 110 Appliance	VMware ESXi (4 Vcpu)	Nutanix AHV on Nutanix virtualized environment	Dell R360
Non-encrypted Sessions	6,000	5,000	5,000	6,000
Encrypted Sessions	4,000	3,000	3,000	4,000
Remote Worker Users (Sessions)	5,000 (2,000)	6,000 (3,000)	6,000 (3,000)	5,000 (2,000)
Avaya Meetings Server Video Sessions	200	200	200	200
Transcoding Sessions	150	100	100	150
TURN/STUN Audio-only Sessions	2,200	2,200	1,200	2,200
TURN/STUN Audio and Video Sessions	300	300	300	300
TURN/STUN Tunneling Audio-only Sessions	220	220	220	220
TURN/STUN Tunneling Audio and Video Sessions	110	110	110	110

Table continues…

Solutions	Server Type			
	Dell™ PowerEdge™ R340 Avaya Solutions Platform 110 Appliance	VMware ESXi (4 Vcpu)	Nutanix AHV on Nutanix virtualized environment	Dell R360
HTTP Media Audio-only Tunneling Sessions	220	220	220	220
HTTP Media Audio and Video Tunneling Sessions	110	110	110	110

Additional capacity values for high-capacity and mid-capacity servers

Avaya SBC supports up to 250 Internet telephony service providers (ITSPs) per system.

Note:

Total Number of Non-Encrypted / Encrypted sessions with the configured ITSPs cannot exceed the numbers quoted in the table above.

Avaya SBC supports up to 250 tenants per system.

Note:

Total Number of Remote Worker sessions with the configured tenants cannot exceed the numbers quoted in the table above.

Avaya SBC supports the following reverse proxy capacities per system:

- 500 HTTP requests per second
- 50 TLS connections per second
- 2,000 concurrent webSockets

Low-capacity servers

Solutions	Server Type			
	KVM Virtualized Environment	VMware ESXi (2 Vcpu)	Dell 3240	Dell VEP1425N
Non-encrypted Sessions	1,500	1000	1000	1000
Encrypted Sessions	500	600	700	700
Remote Worker Users (Sessions)	500 (500)	1000 (500)	2000 (700)	2000 (700)
SIPREC	NA	NA	NA	NA
Transcoding Sessions	100	NA	NA	NA

Additional capacity values for for low-capacity servers

Avaya SBC supports up to 25 Internet telephony service providers (ITSPs) per system.

Note:

Total Number of Non-Encrypted / Encrypted sessions with the configured ITSPs cannot exceed the numbers quoted in the table above.

Avaya SBC supports up to 25 tenants per system.

Note:

Total Number of Remote Worker sessions with the configured tenants cannot exceed the numbers quoted in the table above.

Avaya SBC supports the following reverse proxy capacities per system:

- 50 HTTP requests per second
- 5 TLS connections per second
- 200 concurrent webSockets

General capacity considerations

Each value in the tables represent the maximum capacity supported by Avaya SBC for that solution and cannot be combined for overall capacity calculations.

The capacity specifications are based on:

- Codec specification: the G729 and G711 codecs are used for measuring transcoded capacities. Different codecs will have varying results.
- Call model: the SIP RFC call model in trunk mode is used to establish these capacity specifications.
- IPv4 vs. IPv6: IPv4 as the transport protocol for calculating non-encrypted sessions with trunking for the Avaya Solutions Platform 100 series server - Profile 5 (Dell™ PowerEdge™ R640). With IPv6, the value may decrease by 20%.
- All the audio and video session counts are calculated by assuming Avaya SBC anchors media. For all other platforms except Dell 3240, the performance metrics are calculated by testing with the dedicated SBC device managed by a separate EMS.

SIPREC capacities

Each SIPREC stream is equivalent to a one session. For example, a call with single-stream SIPREC is equal to two sessions; an encrypted call with two encrypted sessions is equal to three encrypted sessions.

Note:

For the encrypted session type, both the recorder and contact center line side are encrypted using the same SRTP cryptosuite.

Number of recording streams	Session type	Server Type		
		Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 5	Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 3	Dell™ PowerEdge™ R340 Avaya Solutions Platform 110 Appliance server, and VMware ESXi 7.0/8.0-based server
One	Non-encrypted	15,000	7,000	3,000
	Encrypted	10,000	4,500	2,000
Two	Non-encrypted	10,000	4,666	2,000
	Encrypted	6,666	3,000	1,666
Three	Non-encrypted	7,500	3,500	1,500
	Encrypted	5,000	2,225	1,000
Four	Non-encrypted	6,000	2,800	1,200
	Encrypted	4,000	1,800	800
Five	Non-encrypted	5,000	2,333	1,000
	Encrypted	3,333	1,500	666

Remote Worker capacity considerations

One exception to the standard capacity values is for remote users and Remote Worker call capacity because registration is required for Remote Worker functionality. Mixed usage of the traffic capacities for solutions will vary and must be determined based on these requirements.

While implementing Remote Worker at maximum capacity limits, set registration expiry timers in Session Manager and in every client at a minimum of 3,600 seconds or one hour.

While implementing Remote Worker at maximum capacity limits in one Avaya SBC or HA pair, under worst-case failover conditions, re-registration for 10,000 users can take up to 20 minutes. During re-registration, all ongoing calls continue uninterrupted. However, under worst-case conditions, a user cannot receive or make new calls during this re-registration time period. Distributing users across multiple Avaya SBC systems significantly reduces this re-registration time.

Presence capacity considerations

The stated session capacities in high-capacity servers is achieved without Presence. For every 5,000 users with Presence there is 10% decrement of supported concurrent sessions due to the high resource utilization of Presence traffic. Mid-capacity and low-capacity values are measured with Presence, having an increment of 25 contacts per user.

VMware ESXi capacity considerations

For VMware ESXi 7.0 and 8.0, it is recommended that capacities are measured with 4 CPU and 8 GB RAM. For more information, see *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*.

Avaya Meetings Server considerations

For specific Avaya Meetings Server capacities, see *Deploying Avaya Meetings Server*.

Redundancy and high availability

Redundancy and High Availability (HA) features are available in EMS and Avaya SBC servers. These features are supported in all high capacity and Mid capacity platforms. Avaya SBC also supports homogeneous server pair in HA mode as long as the SBC devices are of the same hardware category. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

High Availability (HA) support for both media and signaling ensures that Avaya SBC security functionality is provided continuously, regardless of hardware or software failures. High availability requires minimum two Avaya SBC 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 SBC fails over, the secondary Avaya SBC broadcasts a GARP message to announce that the secondary Avaya SBC is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBC 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 SBC, with a router or L3 switch. If you do not put the Avaya SBC 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 SBC.

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 SBC high availability

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

In either configuration, Avaya SBC 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 SBC, which performs all data processing. The interface ports on the standby Avaya SBC do not process any traffic. The management interfaces on the Avaya SBC appliances have different IP addresses, but the signaling or media interfaces have the same IP address. On failover, the standby Avaya SBC advertises the new MAC as the L2 address for the common IP address. The Avaya SBC devices are synchronized through the heartbeat on the dedicated interfaces, and both Avaya SBC devices are in continuous communication with the Avaya EMS.

On detection of a failure on the active Avaya SBC, 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.

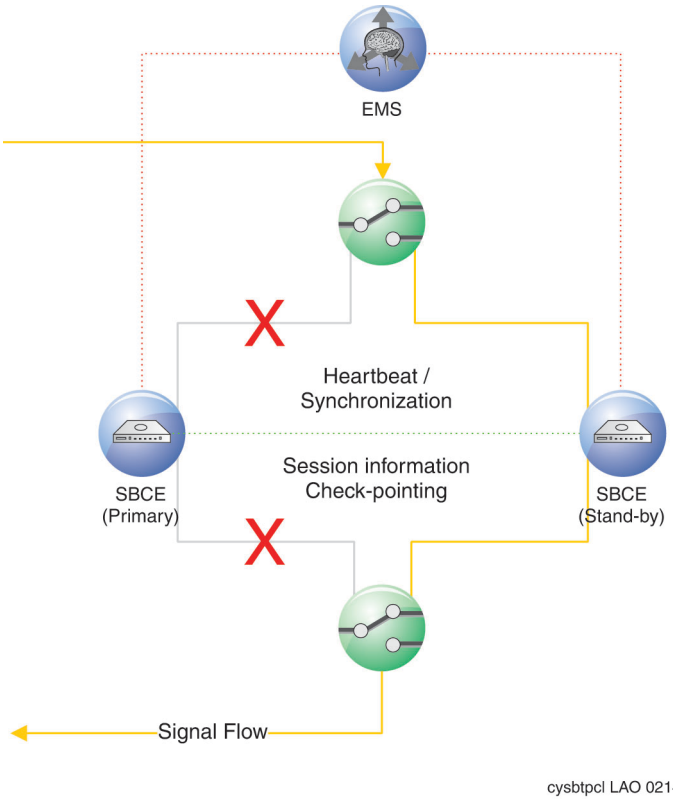


Figure 21: Typical Avaya SBC HA – Parallel Mode Topology (co-located)

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.

Wide area networking requirements

Avaya SBC can be deployed in a single data center or in a dual data center. However, for a dual data center, the following network configuration requirements between the data centers must be met:

- Bandwidth must be equal to or greater than 1 Gbps.
- The network must be reliable. That is, no application-level handling of network disconnects is provided.
- Network latency must be within the following performance limits:
  - Less than or equal to 50 ms — Recommended.
  - 50–100 ms — Some delays in navigation and simple operations. Complex operations, like editing or saving SIP users that traverse multiple systems, may take substantially longer.
  - 100–150 ms — Further performance degradation possible.

This latency information is provided as guidance. Actual performance will depend on the actual network latency between Avaya SBC servers.

Chapter 5: Hardware specifications and requirements

For information about hardware specifications and requirements, refer to *Deploying Avaya Session Border Controller on a Hardware Platform*.

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 SBC 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 SBC 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 SBC 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 SBC detects and blocks application layer scan reports and blocks the attackers that originate them.
- Teardrop attack prevention: Avaya SBC, using built-in Linux and kernel property features, blocks these attacks.
- IP sweep attacks: Avaya SBC supports prevention of IP sweep attacks for ICMP messages using IP table firewall rules.

Attack protection

Avaya SBC security products ensure the integrity of all real-time IP applications. Avaya SBC 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 SBC 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 SBC 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 SBC security devices installed in a network.

Note:

Both the EMS and Avaya SBC can be installed in one box. However, as your network grows and you require more than one Avaya SBC, the EMS must be installed on a dedicated platform.

Detection

The detection capability of the Avaya SBC 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 SBC 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 SBC 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 SBC 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 SBC security products can evolve and adapt automatically to effectively counter any new or existing threat.

Protection

The Avaya SBC 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 SBC 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 SBC 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 SBC 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 SBC, 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 SBC box.

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

Avaya SBC 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 SBC 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. System memory can revert to the true settings if needed, for example, on a return leg of a call.

Firewall rules

Firewall rules protect the Avaya SBC, and communications and signaling for Avaya SBC. 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 22 or 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 22 or 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

For information about port usage, see *Avaya Session Border Controller Port Matrix*.

Chapter 7: Licensing requirements

About licensing requirements

Avaya SBC uses the Avaya Product Licensing and Delivery System (PLDS) to create licenses and download Avaya SBC software. 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 SBC:

- Standard Services delivers non-encrypted 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 SBC.

Avaya SBC uses WebLM version 8.0 or later for licensing requirements. You can install the Avaya SBC license file on a primary Element Management System (EMS) using the Device Management page.

Important:

You must not enable the local WebLM option and install an Avaya SBC license file on the secondary EMS if used in an active-active deployment. If you install a license file on a secondary EMS in an active-active deployment, the licensing system will always show that the secondary EMS is in **OK** state.

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 SBC works normally during the grace period.

Important:

Licenses and a WebLM server are required for new installations or upgrades.

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

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

For integration with Microsoft® Teams, Avaya SBC requires the Premium license and Premium HA license permissions in addition to the Standard Services and Advanced Services licenses.

For the use of AMR-WB codec, Avaya SBC requires counting license for AMR-WB codec license and AMR-WB codec HA tracking license. This is applicable to both static and dynamic licenses.

Initial Grace Period: Initial Grace Period is when Avaya SBC is newly installed and has no connection established to licensing server. When in initial grace period Avaya SBC only allows 100 licenses per feature.

Grace Period: Grace Period is when Avaya SBC loses its connection to licensing server after serving. In Dynamic Licensing Mode, when in Grace Period, State licensing statistics would show 0 and will be updated when connections with the licensing server are restored.

On upgrading to 10.2.1, EMS might display following warnings:

- *This system has one or more SBC(s) that does not have a valid AMR license configuration.*

  This may cause calls to fail or may cause other problems with the attached SBC(s). Check the device settings and license settings to ensure that calls will be processed properly.
- *This system has one or more SBC(s) that appear to have no licensing configuration.*

  This may cause calls to fail or may cause other problems with the attached SBC(s). Check the device settings and license settings to ensure that calls will be processed properly.

These warnings can be corrected by properly configuring licenses for all required features.

Avaya SBC licensed 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.
VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.
VALUE_SBCE_PREM_SESSION	Specifies the number of premium session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_PREM_HA_SESSION	Specifies the number of premium service HA session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Meetings Server 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 SBC elements managed.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that the download of virtual system installation files for VMware, KVM, Amazon Web Services, and Microsoft® Azure is permitted.
VALUE_SBCE_ENCRYPTION_1	Specifies that both media and signaling can be encrypted for Avaya SBC. This license is required when using any advanced licenses.

Table continues…

License feature	Description
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 SBC. The quantity of this license must match the quantity of standard licensing in the system being managed.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies Avaya SBC encryption only for signaling.
VALUE_SBCE_NG911	Specifies the number of AMR-WB codec licenses.
VALUE_SBCE_NG911_HA	Specifies the number of AMR-WB codec HA licenses.

About centralized licensing

Using Centralized Licensing feature, the WebLM server can directly distribute the licenses to Avaya SBC connected to different Element Management System (EMS) in different networks.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Avaya SBC setup.
- Eliminates the need to log in to each WebLM server to manage licenses for each Avaya SBC setup.
- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Avaya SBC.

Note:

- The setup does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Avaya SBC setup.

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
Design		
Avaya Session Border Controller Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBC.	Sales engineers, solution architects, and implementation engineers
Avaya Session Border Controller Release Notes	Describes any last minute changes to the product, including patches, installation instructions, and upgrade instructions.	Sales and deployment engineers, solution architects, and support personnel
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform servers.	IT Management, sales and deployment engineers, solution architects, and support personnel
Implementation		
Deploying Avaya Session Border Controller on a Hardware Platform	Describes how to plan and deploy an Avaya SBC system on the supported set of hardware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Virtualized Environment Platform	Describes how to plan and deploy an Avaya SBC system on customer-provided VMware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Google Cloud Platform	Describes how to plan and deploy an Avaya SBC system on a Google Cloud Platform.	Sales and deployment engineers, solution architects, and support personnel

Table continues…

Title	Description	Audience
Deploying Avaya Session Border Controller on an Amazon Web Services Platform	Describes how to plan and deploy an Avaya SBC system on Amazon Web Services.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Microsoft® Azure Platform	Describes how to plan and deploy an Avaya SBC system on a Microsoft® Azure platform.	Sales and deployment engineers, solution architects, and support personnel
Avaya Session Border Controller Port Matrix	Describes the incoming and outgoing port usage required by the product.	Sales and deployment engineers, solution architects, and support personnel
Upgrading Avaya Session Border Controller	Describes how to upgrade to the latest release of Avaya SBC.	Sales and deployment engineers, solution architects, and support personnel
Installing the Avaya Solutions Platform 110 Appliance	Describes how to install Avaya Solutions Platform 110 Appliance servers.	Sales and deployment engineers, solution architects, and support personnel
Administration		
Administering Avaya Session Border Controller	Describes configuration and administration procedures.	Implementation engineers and administrators
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Session Border Controller	Describes troubleshooting and maintenance procedures for Avaya SBC.	Implementation engineers
Maintaining and Troubleshooting Avaya Solutions Platform 110 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 110 Appliance servers.	Implementation engineers
Using		
Working with Avaya Session Border Controller and Microsoft® Teams	Describes how to set up, maintain, and use Avaya SBC with Microsoft Teams.	Implementation engineers and administrators
Working with Avaya Session Border Controller Multi-Tenancy	Describes how to set up, maintain, and use the Avaya SBC Multi-tenancy feature.	Implementation engineers and administrators
Working with Avaya Session Border Controller Geographic-Redundant Deployments	Describes how to set up, maintain, and use the Avaya SBC Geographic-redundant deployment feature.	Implementation engineers and administrators

For Dell documentation, go to https://www.dell.com/support/.

For HP documentation, go to https://www.hpe.com/support.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.

  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

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
20600W	Avaya Session Border Controller 8.1 Technical Delta
21098W	Session Border Controller 8.0 Technical Delta
20660W	Administering the Avaya Session Border Controller for Enterprise - SIP Trunk
60660W	Administering Avaya SBC Release 8 for Remote Worker
20660T	Administering Avaya SBC Release 8 Test
20800C	Implementing and Supporting Avaya SBC — Platform Independent
20800T	Avaya SBC Platform Independent and Support Test
20800V	Implementing and Supporting Avaya SBC — Platform Independent
26160W	Avaya SBC Fundamentals
7008T	Avaya SBC for Midmarket Solutions Implementation and Support Test
7008W	Avaya SBC for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions

Table continues…

Course code	Course title
71300	Integrating Avaya Communication Applications
72300	Supporting Avaya Communication Applications

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.

- 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`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

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 Avaya SBC feature that allows two Avaya SBC 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 Avaya SBC security devices provide failover protection in the event one of the devices malfunctions.
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IM	Instant Messaging
Intrusion	A malicious user or process deliberately masquerading as a legitimate user or process.
IP	Internet Protocol
IPS	Intrusion Protection System
ITSP	Internet Telephony Service Provider
Latency	The amount of time it takes for a packet to cross a network connection, from sender to receiver. Also, the amount of time a packet is held by a network device (firewall, router, etc.) before it is forwarded to its next destination.
MAC	Message Authentication Code
MCD	Machine Call Detection
NAT	Network Address Translation
NTP	Network Time Protocol
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
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. Avaya SBC supports certificates with 2048-bit or 4096-bit keys. 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

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W