



# **Avaya Session Border Controller for Enterprise Overview and Specification**

Release 6.3  
Issue 3  
October 2014

## Notice

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

## Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

## Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

## Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The

applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Software" means Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed, or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

## License types

**Designated System(s) License (DS).** End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

**Concurrent User License (CU).** End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

## Heritage Nortel Software

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

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

## Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available

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

### **Preventing Toll Fraud**

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

### **Avaya Toll Fraud intervention**

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com).

### **Trademarks**

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

### **Downloading Documentation**

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

### **Contact Avaya Support**

See the Avaya Support website: <http://support.avaya.com> for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

## Contents

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| <b>Chapter 1: Introduction</b>                                            | <b>7</b>  |
| Purpose                                                                   | 7         |
| Intended audience                                                         | 7         |
| Document changes since last issue                                         | 7         |
| Related resources                                                         | 8         |
| Documentation                                                             | 8         |
| Training                                                                  | 9         |
| Viewing Avaya Mentor videos                                               | 9         |
| Support                                                                   | 9         |
| Warranty                                                                  | 10        |
| <b>Chapter 2: Avaya Session Border Controller for Enterprise overview</b> | <b>11</b> |
| Advanced Services                                                         | 11        |
| Standard services                                                         | 12        |
| Functional entities                                                       | 13        |
| Signaling element                                                         | 13        |
| Media element                                                             | 14        |
| Element and management provisioning                                       | 14        |
| Avaya SBCEdeployment                                                      | 15        |
| Deployment models                                                         | 15        |
| Deployment modes                                                          | 16        |
| Additional network security deployment                                    | 17        |
| Feature description                                                       | 18        |
| Media anchoring                                                           | 18        |
| Media unanchoring                                                         | 19        |
| Remote worker configuration                                               | 19        |
| Remote management services                                                | 19        |
| Signaling manipulation                                                    | 20        |
| SIP trunking                                                              | 20        |
| UCID                                                                      | 21        |
| Support for video SRTP                                                    | 22        |
| REFER Handling                                                            | 23        |
| Multi Device Access                                                       | 25        |
| Reinvite handling                                                         | 26        |
| RTCP Monitoring                                                           | 26        |
| Reverse proxy                                                             | 31        |
| Far End Camera Control                                                    | 33        |
| Binary Floor Control Protocol                                             | 33        |
| Forward Error Correction                                                  | 38        |
| User registration                                                         | 38        |
| Real Time SIP Server Status                                               | 38        |

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| Licensing requirements.....                                       | 39        |
| Single Sign-On and Identity Engine.....                           | 39        |
| Multiple Avaya SBCE deployment .....                              | 39        |
| WebRTC-enabled call handling.....                                 | 41        |
| Virtualization architecture overview.....                         | 42        |
| SRTP overview.....                                                | 43        |
| Multiple subnet and multiple interfaces.....                      | 44        |
| Overview.....                                                     | 51        |
| Support for Linux 6.4.....                                        | 52        |
| <b>Chapter 3: Interoperability.....</b>                           | <b>54</b> |
| Product compatibility.....                                        | 54        |
| Avaya SBCE supported servers.....                                 | 54        |
| Avaya products.....                                               | 55        |
| Third-party product requirements.....                             | 56        |
| Operating system compatibility.....                               | 56        |
| <b>Chapter 4: Performance specifications.....</b>                 | <b>57</b> |
| Capacity and scalability specification.....                       | 57        |
| Redundancy and high availability.....                             | 58        |
| Avaya SBCE high availability.....                                 | 58        |
| EMS replication.....                                              | 59        |
| <b>Chapter 5: Environmental requirements.....</b>                 | <b>60</b> |
| Altitude requirements.....                                        | 60        |
| Hardware dimensions.....                                          | 60        |
| <b>Temperature and humidity requirements.....</b>                 | <b>61</b> |
| Power requirements.....                                           | 61        |
| Physical system protection requirements.....                      | 62        |
| Regulatory standards.....                                         | 62        |
| <b>Chapter 6: Security.....</b>                                   | <b>63</b> |
| Security specification.....                                       | 63        |
| Unified communications intrusion protection.....                  | 63        |
| Attack protection.....                                            | 64        |
| Avaya SBCE hardening.....                                         | 65        |
| Protection against layer 3 and layer 4 floods and port scans..... | 65        |
| DoS security features.....                                        | 66        |
| Protocol scrubber.....                                            | 67        |
| Topology hiding.....                                              | 67        |
| Firewall rules.....                                               | 67        |
| Port utilization specification.....                               | 71        |
| Management interface port restrictions.....                       | 71        |
| TCP packets.....                                                  | 72        |
| SSH port.....                                                     | 72        |
| Additional port assignments.....                                  | 72        |
| <b>Chapter 7: Licensing requirements.....</b>                     | <b>74</b> |

Avaya SBCE license features..... 74

WebLM server details..... 75

**Glossary**..... 76

# Chapter 1: Introduction

---

## Purpose

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

---

## Intended audience

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

---

## Document changes since last issue

The following features were added since the previous issue:

- Reinvite
- Radvision interoperability
- Redhat migration phase 1
- Multiple subnets
- Multiple interfaces
- VLAN routing and tagging
- Support for changing management IP
- Virtualization
- Multi-tenant enhancements
- Routing
- Load-balancing
- Multi-data center failover
- Reverse proxy implementation
- IDE SSO interoperability

- WebLM Support
- TURN/STUN implementation
- Serviceability-traceSBC
- SIP trunk status
- Display registered devices
- Media unanchoring

The following feature is modified since the previous issue:

- DoS security

---

## Related resources

---

### Documentation

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

| Title                                                                                      | Description                                                                                                                  | Audience                                      |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Implementation                                                                             |                                                                                                                              |                                               |
| <i>Deploying Avaya Session Border Controller for Enterprise</i>                            | Hardware installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network. | Implementation engineers                      |
| <i>Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment</i> | Virtual installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.  | Implementation engineers                      |
| <i>Upgrading Avaya Session Border Controller for Enterprise</i>                            | Procedures for upgrading to Avaya SBCE 6.3                                                                                   | Implementation engineers                      |
| Maintenance and Troubleshooting                                                            |                                                                                                                              |                                               |
| <i>Administering Avaya Session Border Controller for Enterprise</i>                        | Configuration and administration procedures.                                                                                 | Implementation engineers, Administrators      |
| <i>Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise</i>      | Troubleshooting and maintenance procedures                                                                                   | Implementation engineers, and Sales engineers |

---

## Training

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

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

---

## Viewing Avaya Mentor videos

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

### About this task

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

### Procedure

- To find videos on the Avaya Support website, go to [support.avaya.com](http://support.avaya.com) and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to [www.youtube.com/AvayaMentor](http://www.youtube.com/AvayaMentor) and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 **Note:**

Videos are not available for all products.

---

## Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

---

## Warranty

Avaya provides a one-year limited warranty on Avaya SBCE hardware and 90 days on Avaya SBCE software. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the support details for Avaya SBCE in the warranty period is available on the Avaya Support website <http://support.avaya.com/> under **Help & Policies > Policies & Legal > Warranty & Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

# Chapter 2: Avaya Session Border Controller for Enterprise overview

Avaya SBCE provides security to SIP-based Unified Communications (UC) networks. Avaya SBCE is available in two versions: Advanced Services and Standard Services. Either version can reside on supported servers for Release 6.3. For information about supported servers, see the Avaya SBCE supported servers section.

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

- Standalone configuration

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

- Multiple server configuration

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

- High availability (HA) configuration

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

## Related Links

[Avaya SBCE supported servers](#) on page 54

---

## Advanced Services

Advanced Services is a specialized Unified Communications (UC) security product. Advanced Services protects all IP-based real-time multimedia applications, endpoints, and network infrastructure from potentially catastrophic attacks and misuse. This product provides the real-time

flexibility to harmonize and normalize enterprise communications traffic to maintain the highest levels of network efficiency and security.

Advanced Services provides the security functions required by the ever changing and expanding UC market. Advanced Services protects any wire-line or wireless enterprise or service provider that has deployed UC. Avaya SBCE, from malicious attacks. These attacks can originate from anywhere in the world anytime. Advanced Services is the only UC-specific security solution that effectively and seamlessly incorporates all approaches into a single, comprehensive system.

Avaya SBCE Advanced Services incorporates the best practices of all phases of data security to ensure that new UC threats are immediately recognized, detected, and eliminated. Advanced Services incorporates security techniques that includes UC protocol anomaly detection and filtering and behavior learning-based anomaly detection. Together, these techniques monitor, detect, and protect any UC network from any known security vulnerabilities such as:

- Validate and support remote users for extension of Avaya Aura® UC services.
- Encryption services such as SRTP.

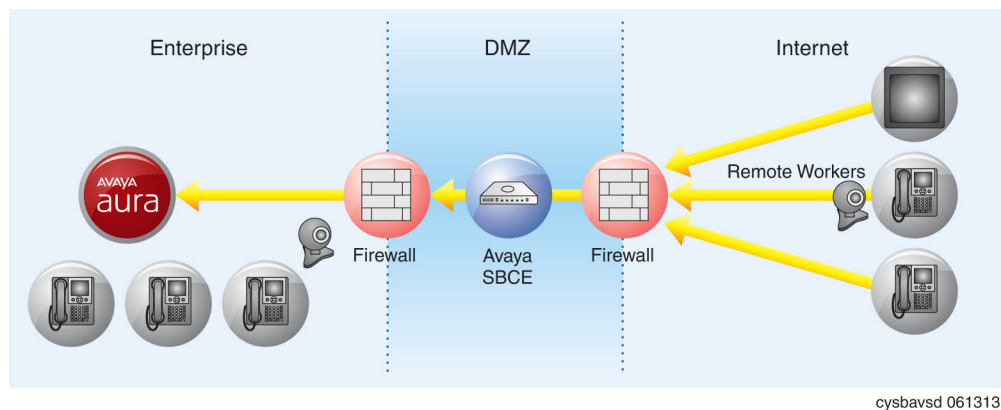


**Figure 1: Advanced Services Solution**

---

## Standard services

Avaya Session Border Controller for Enterprise 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 typical SBCs.

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

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

features the unique Signaling Manipulation module (SigMa module), which dramatically simplifies the deployment of SIP trunks. The SigMa module streamlines integration of SIP trunks into thousands of variations of enterprise SIP telephony environments, greatly reducing implementation time. As a result, SIP trunk deployment in many standard configurations can occur in 2 hours or less.

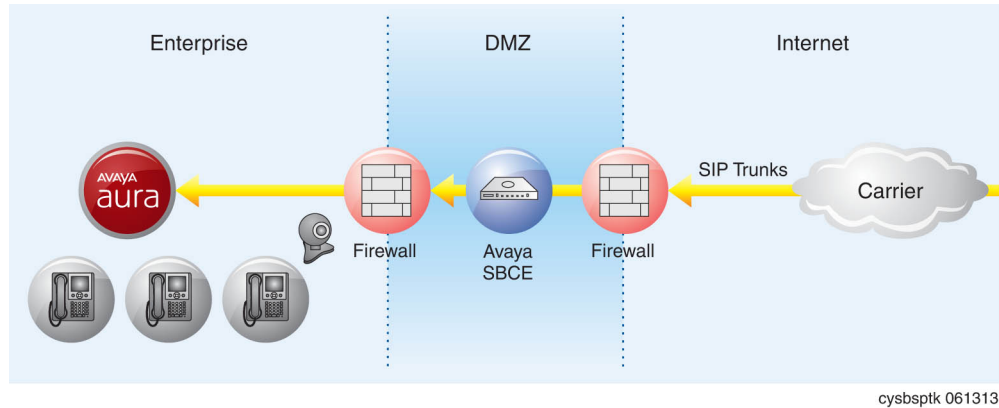


**Figure 2: SIP trunking**

---

## Functional entities

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

---

## Signaling element

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

The Signaling element provides the following features:

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

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

This entity also provides the configuration information to the remote endpoints. The Signaling element uses http or https to send the Personal Profile Manager (PPM) information to the phone.

---

## Media element

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

The Media element provides the following features:

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

---

## Element and management provisioning

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

Element and management provisioning provides the following features:

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

---

# Avaya SBCEdeployment

This section covers the following:

- Deployment models
- Deployment modes
- Additional network security deployment

---

## Deployment models

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

- **Standalone configuration:** In the standalone configuration, the Avaya SBCE and EMS coreside in the same physical server. In this deployment, the phones maintain two separate socket connections to Avaya SBCE, at two different IP addresses hosted by Avaya SBCE. One of the sockets handles traffic destined to primary Session Manager, the other manages traffic destined to secondary Session Manager.
- **Multi-server configuration:** A multi-server configuration requires EMS and Avaya SBCE to be deployed on different servers.
- **High availability (HA) configuration:** A High availability (HA) configuration requires a separate EMS server. Avaya SBCE HA pairs can be deployed in an enterprise in a parallel mode configuration. In the parallel configuration, the signaling packets are routed only to the active or primary Avaya SBCE, which performs all data processing. The interface ports on the standby Avaya SBCE do not process any traffic. The Management interfaces on the Avaya SBCE appliances have different IP addresses, but the signaling or media interfaces have the same IP address. Upon failover, the standby Avaya SBCE advertises its new MAC as the L2 address for the common IP address. The Avaya SBCE devices are synchronized via the heartbeat on the dedicated interfaces, and both Avaya SBCE devices are in continuous communication with the Avaya EMS.

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

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

For more information about virtualization, see *Deploying Avaya SBCE in Virtualized Environment*.

## Deployment modes

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

Regardless of the deployment scenario, the security products offer 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 in-line, is the simplest and most basic deployment. The Avaya SBCE is positioned at the edge of the network in the DMZ. The Avaya SBCE is directly inline with the call servers, and protects the enterprise network against all inadvertent and malicious intrusions and attacks.

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

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

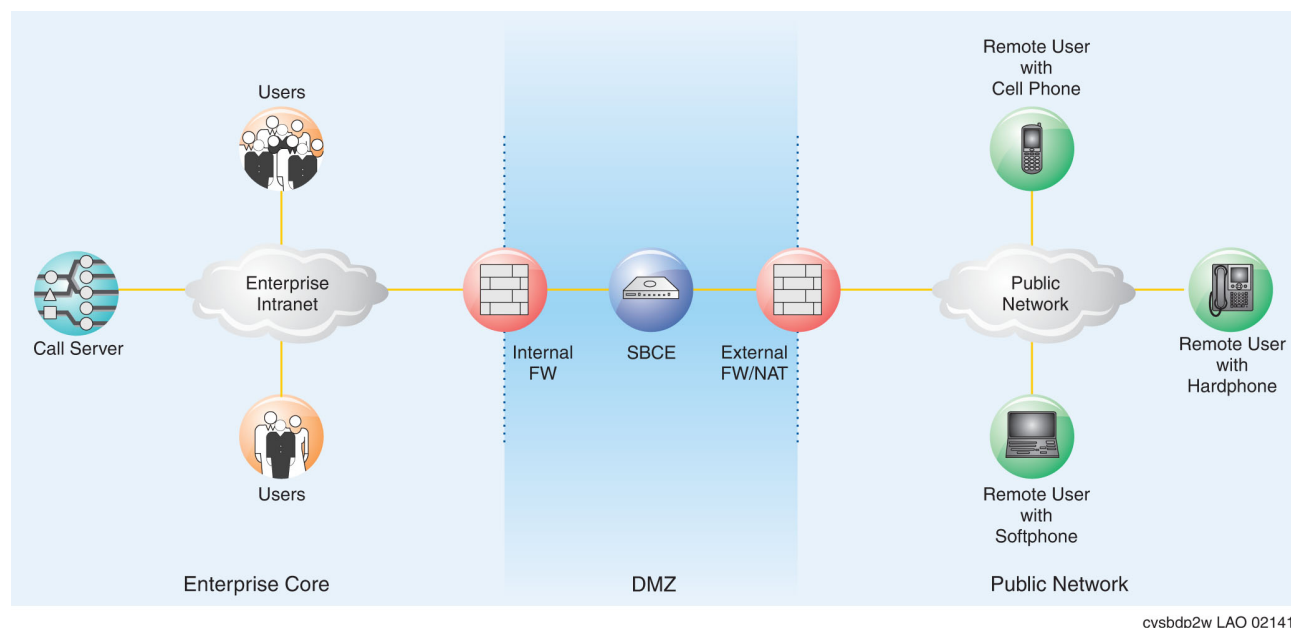


**Figure 3: Avaya SBCE Deployment – Two-Wire**

### One-wire deployment

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

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

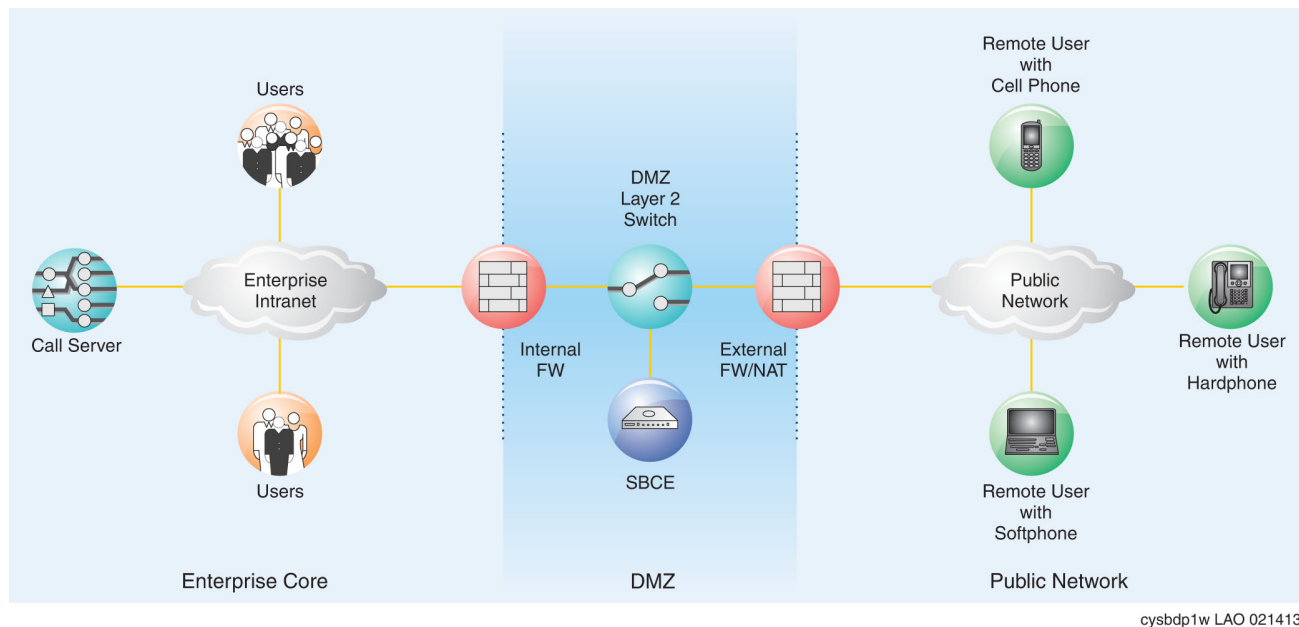


**Figure 4: Avaya SBCE Deployment – One-Wire**

## Additional network security deployment

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

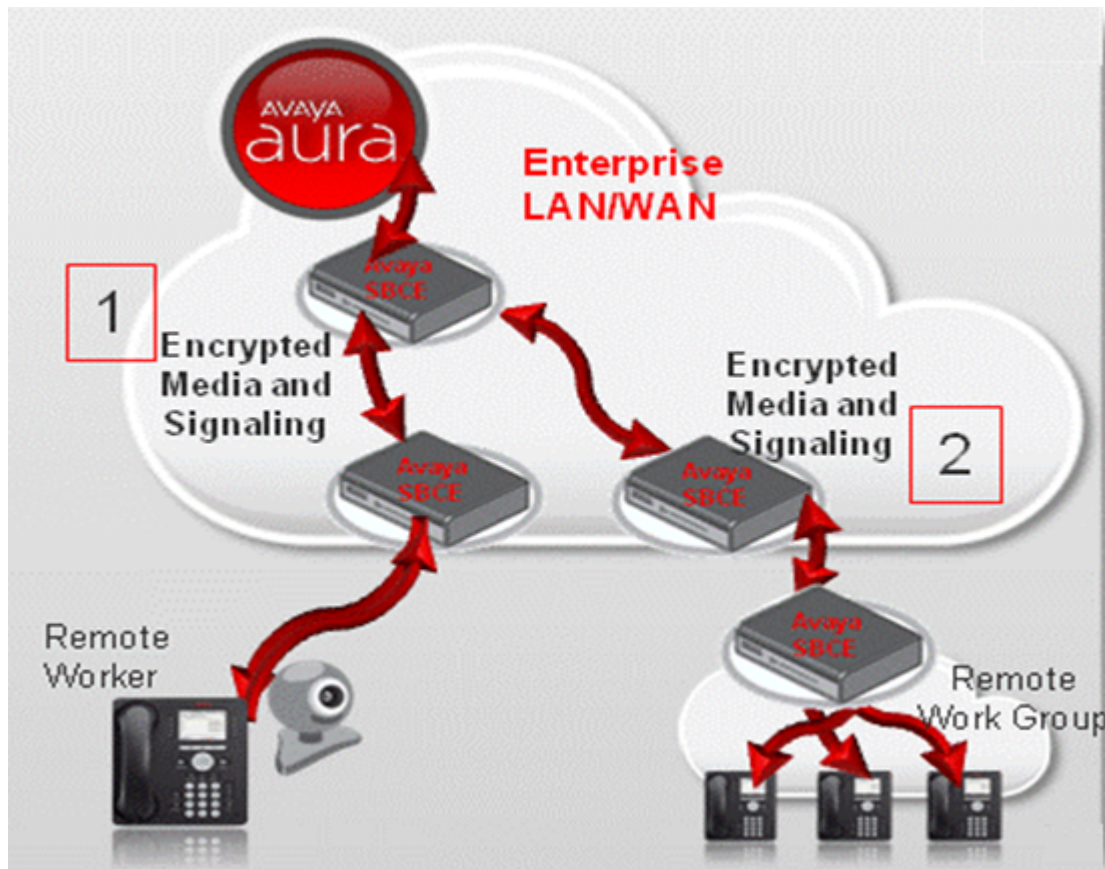


**Figure 5: Additional network security deployment**

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

## Feature description

### Media anchoring

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

## Media unanchoring

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

## Remote worker configuration

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

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

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

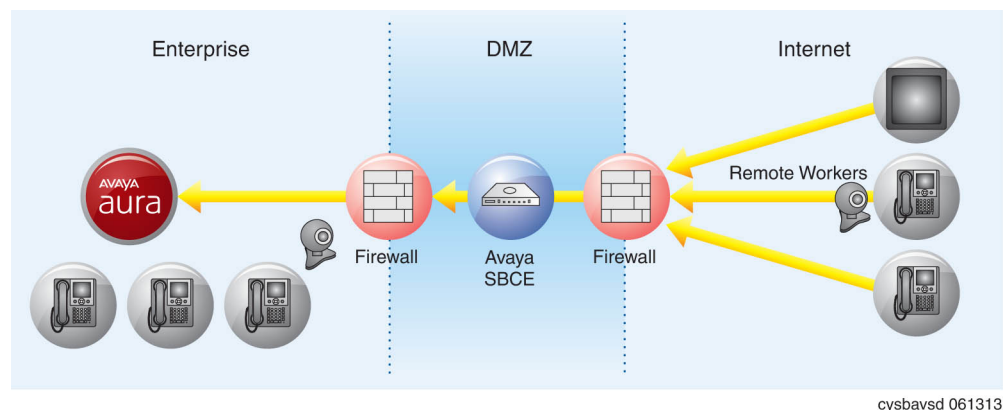


**Figure 6: Remote worker**

## Remote management services

An IP Office Secure Sockets Layer (SSL) virtual private network (VPN) service provides secure tunneling between an Avaya services or support site and an Avaya SBCE that is installed at a

customer site. With the secure tunnel, Avaya service providers can offer remote management services such as fault management, monitoring, and administration to IP Office customers.

Avaya SBCE also supports remote access through the SAL gateway.

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

---

## Signaling manipulation

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

---

## SIP trunking

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

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

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

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

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

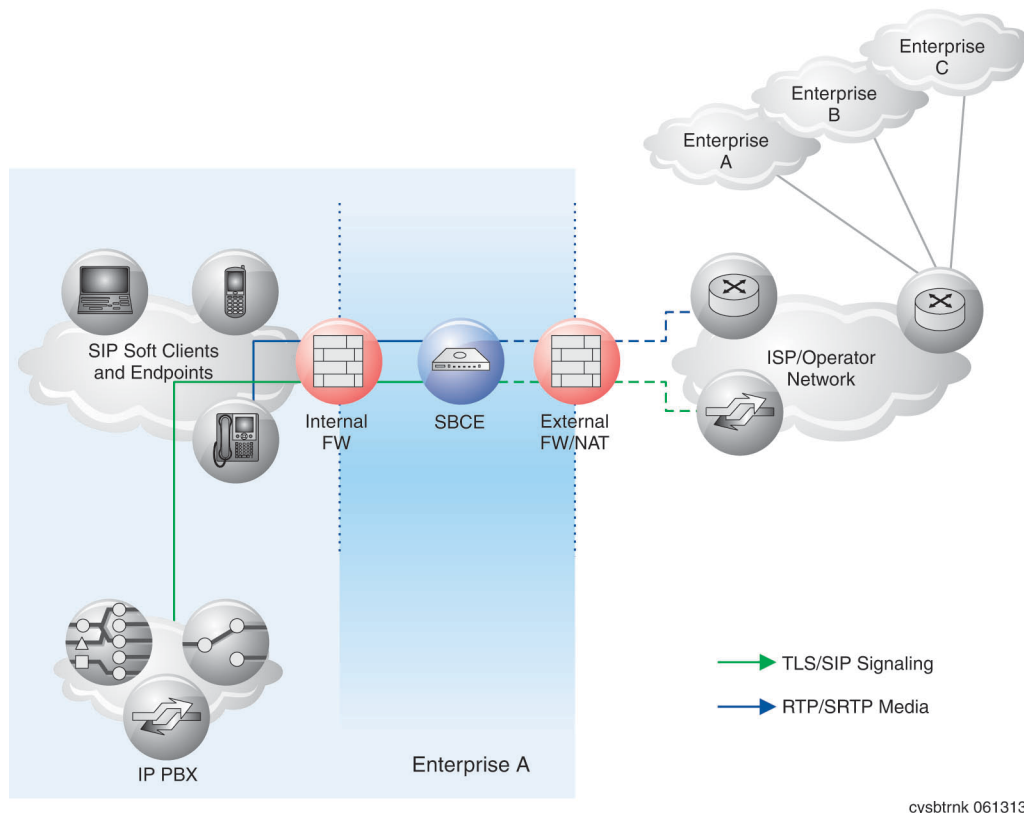


**Figure 7: SIP Trunking**

## UCID

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

### AACC

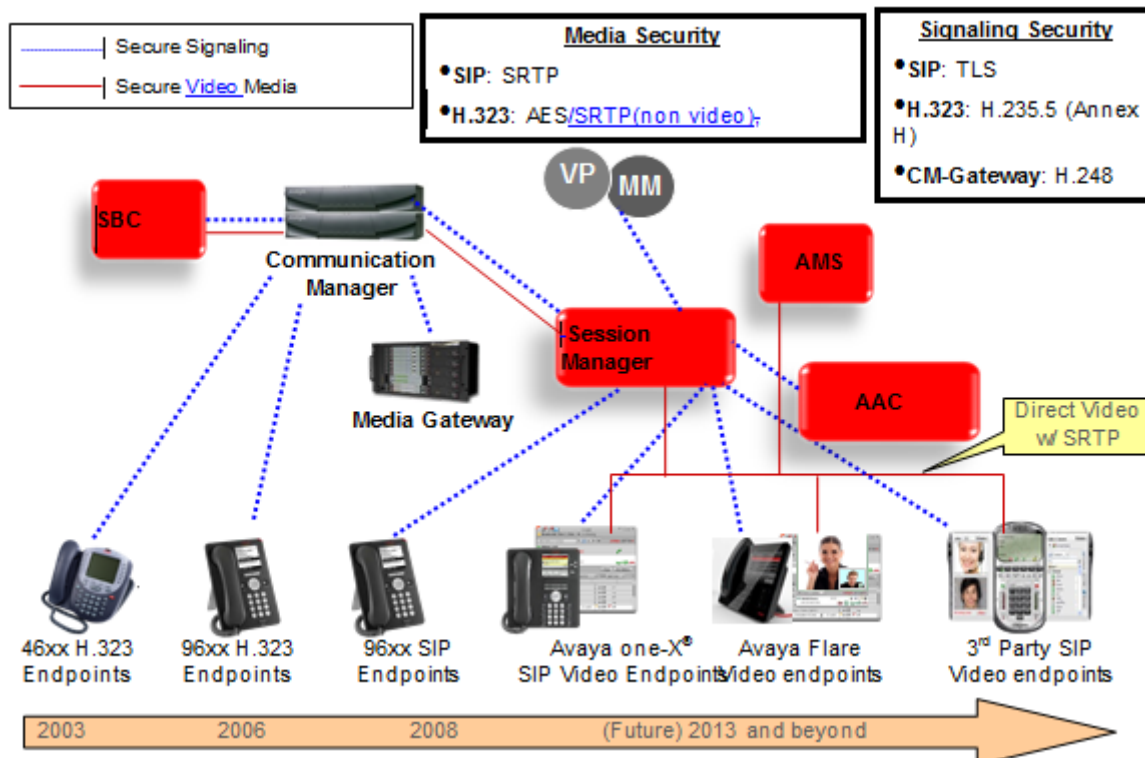
The generation of UCID by Avaya Aura<sup>®</sup> Session Border Controller is required in Avaya Aura<sup>®</sup> Contact Center 7.0 environment. A UCID is assigned to any incoming call at the border SBC so that AACC has a unique handle for each call. For instance, AACC then monitors or controls any application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

### CC Elite

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

## Support for video SRTP

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



### Supported user cases

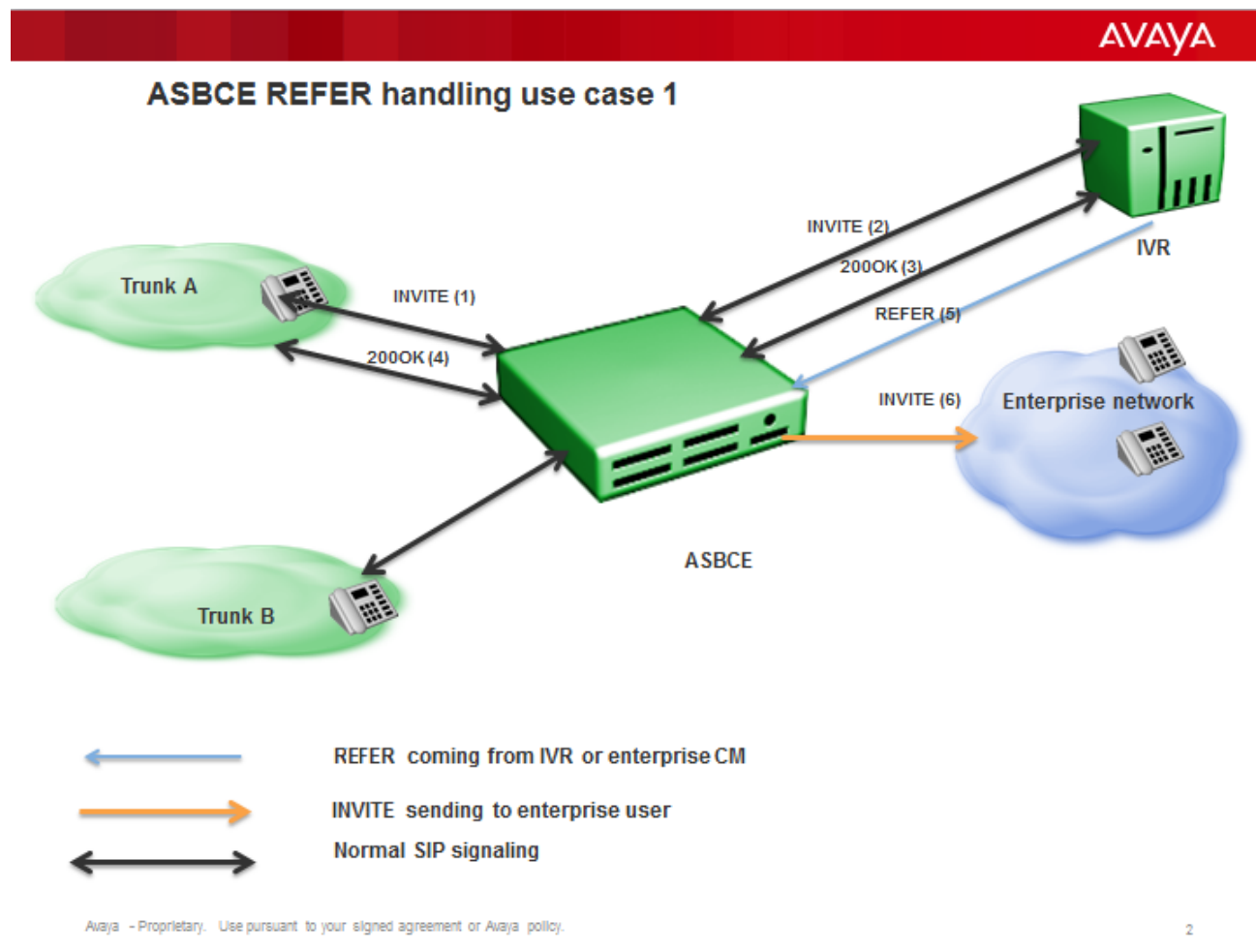
- (Desktop Users) – Avaya SIP Video Endpoint, such as 1XC to 1XC SRTP encrypted SIP video call : Enabling video calls between two video-enabled IntereXchange carrier SIP endpoints. All standard telephony and video features such as mute, transfer, and hold can be used.
- (Mixed) SIP SRTP video call between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

## REFER Handling

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

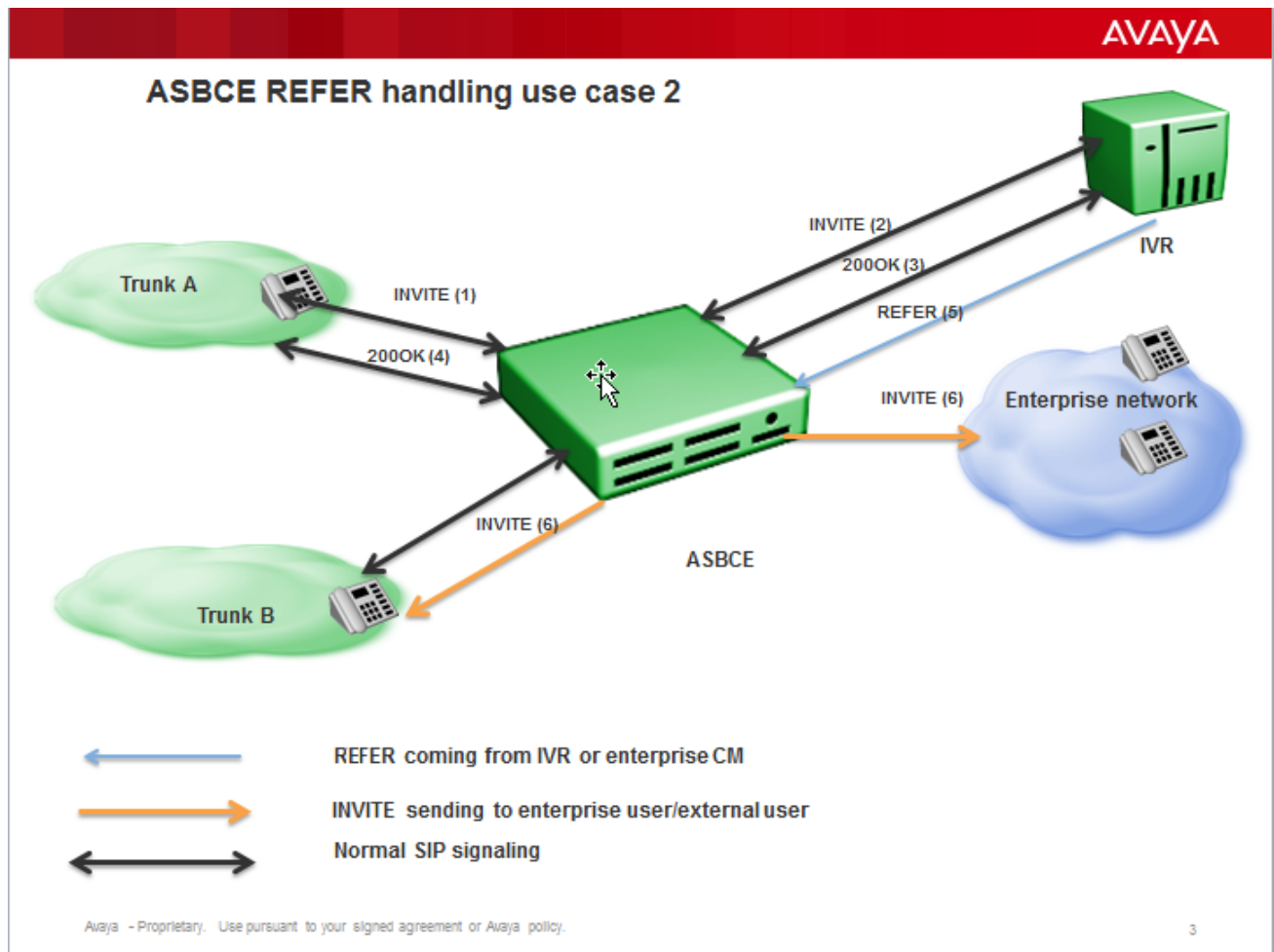
### Use case 1

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



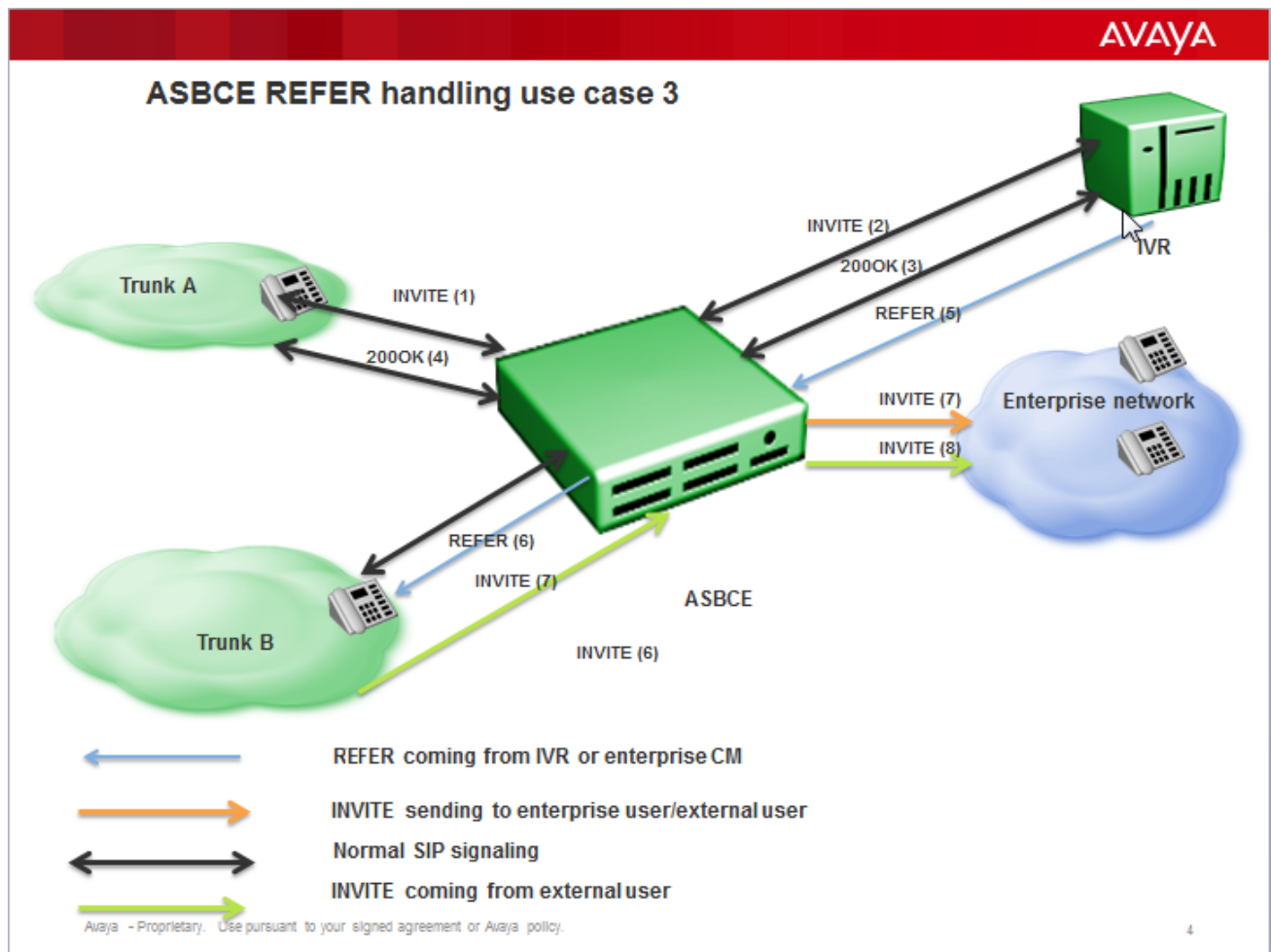
### Use case 2

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



### Use case 3

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



## 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.

### Solution Overview

The Multi Device Access feature consists of the same user and extension using the same AOR to register multiple devices to Session Manager. 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. Those devices can join the call

using this dialog information. The display shows a two-party call, and not a conference. Only one active MDA call is maintained for a call involving AAC.

---

## Reinvite handling

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

---

## RTCP Monitoring

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

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

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

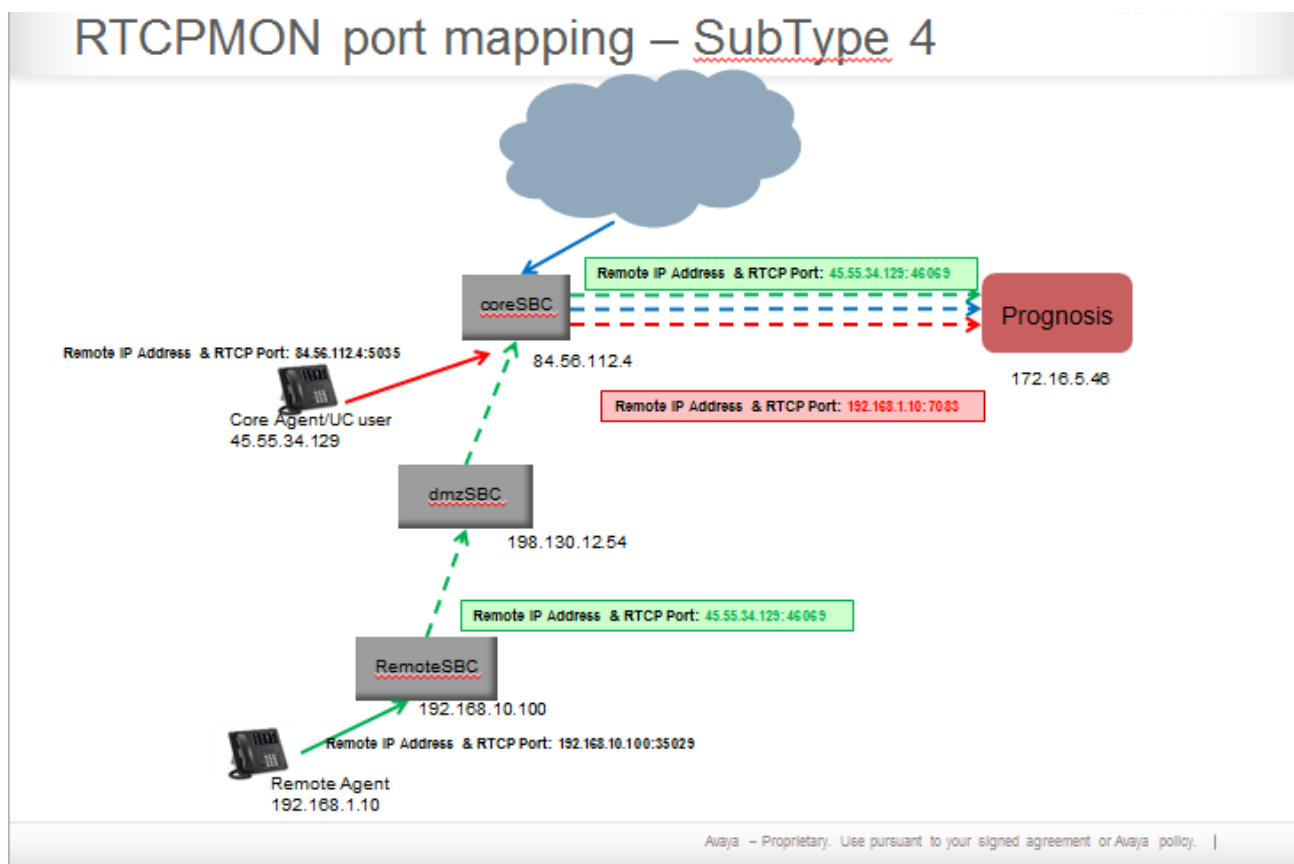
If mapping exists in the SBC for SSRC1 and SSRC2, then SBC will use the mapping information to rewrite the following in the RTCPMON packets to be sent to Prognosis.

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

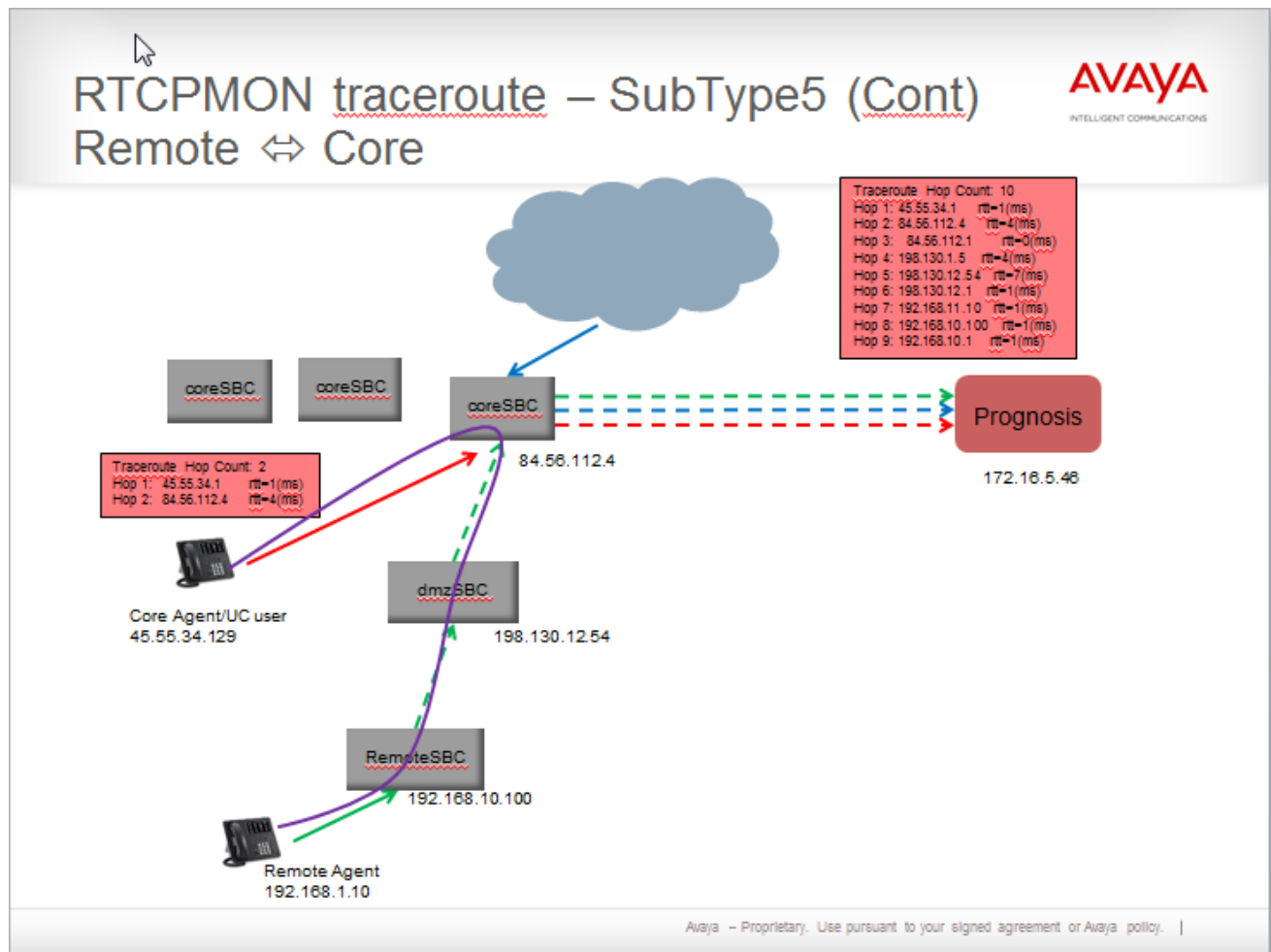
Processed RTCPMON packets will now be sent to Prognosis based on the information filled in by SBCE.

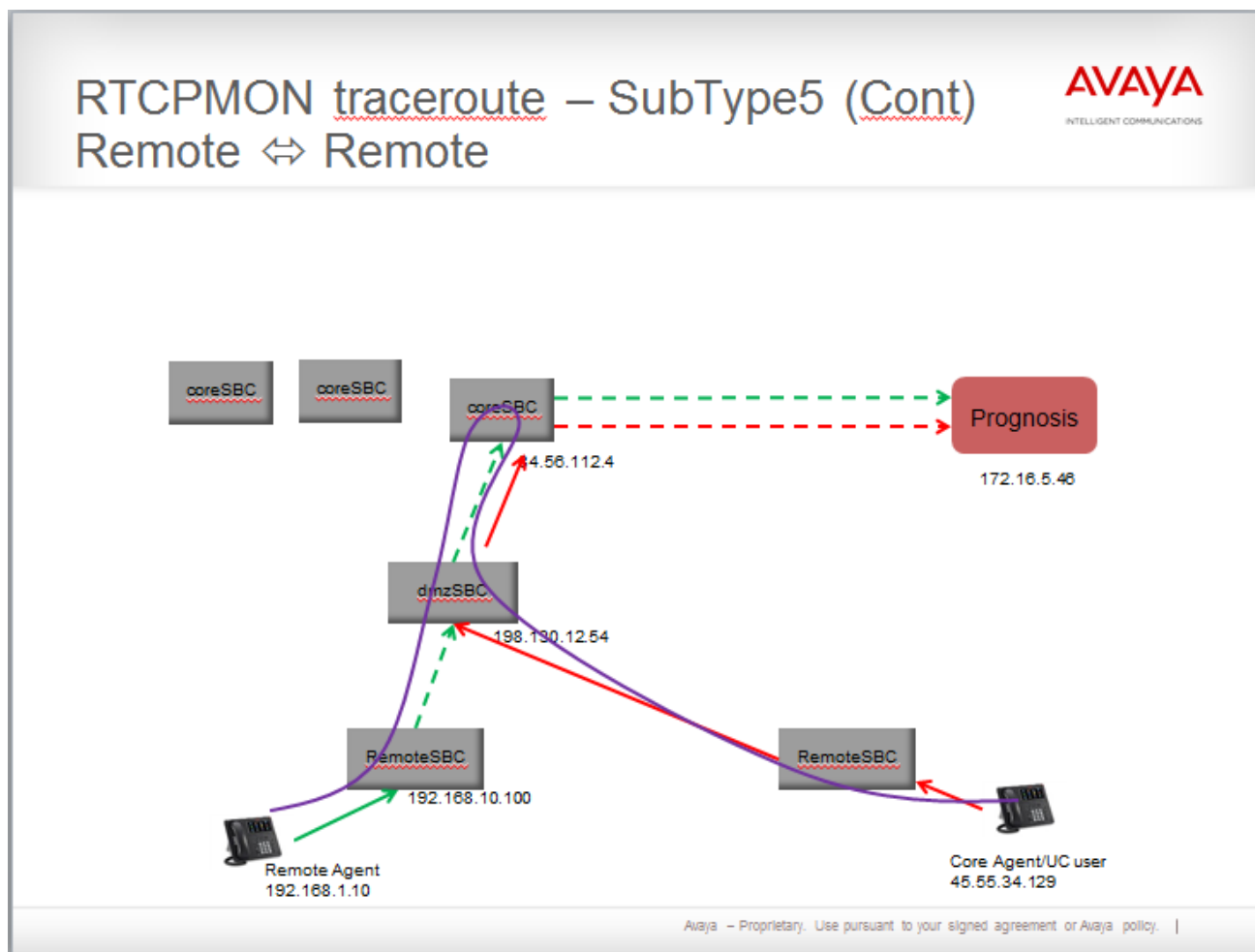
### Modes of configuration

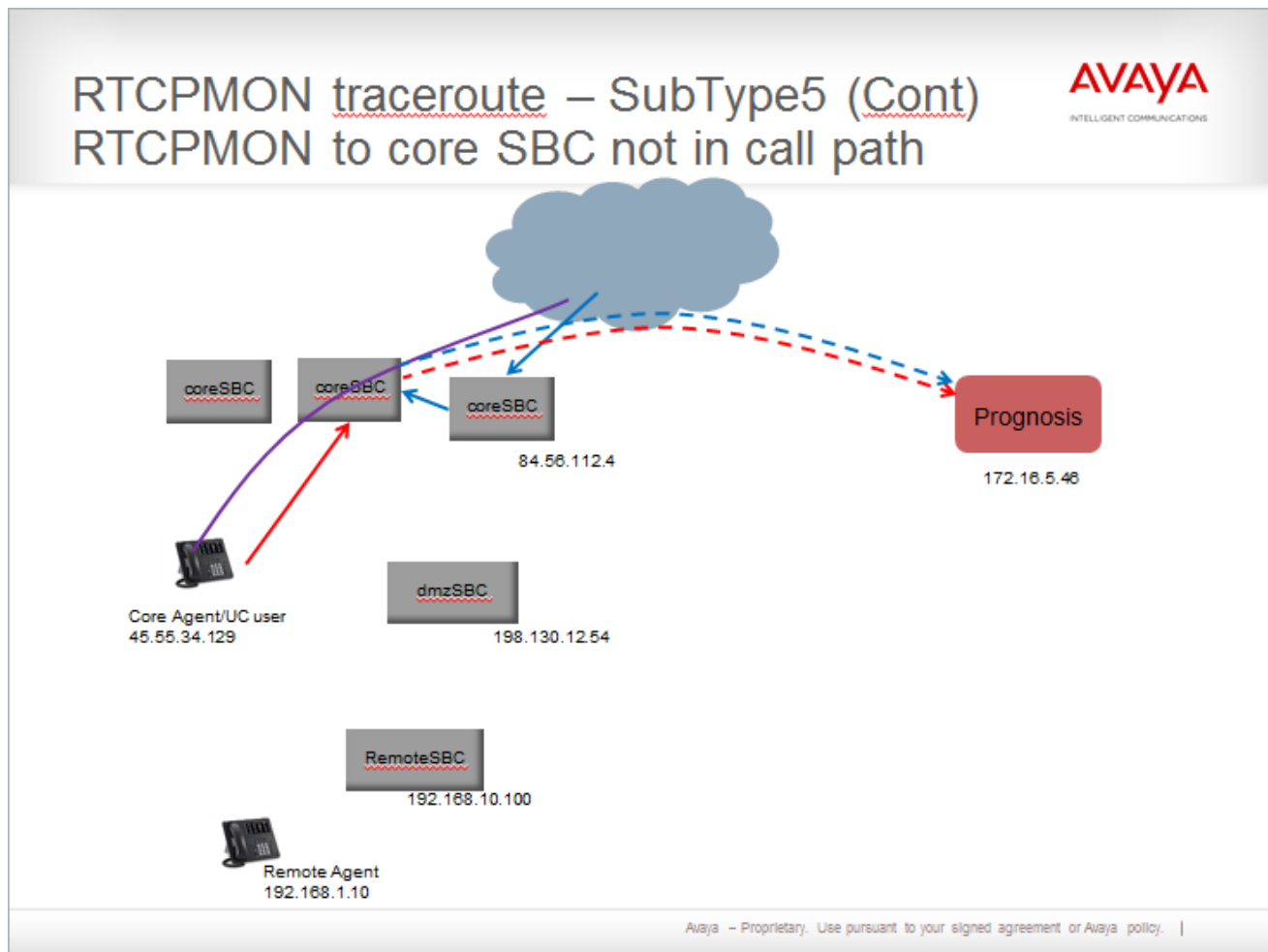
- **END-END Rewrite:** SBC updates the RTCP subtype-4 packet from the media terminating endpoint. In Subtype-4, SBC rewrites the Remote IP Address field with the Remote endpoint address who is the recipient of the RTCP packets. End-end rewrite must be configured in all SBC devices which have media terminating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



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







- **Bridging:** 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 SBC devices.

**\* Note:**

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

## Reverse proxy

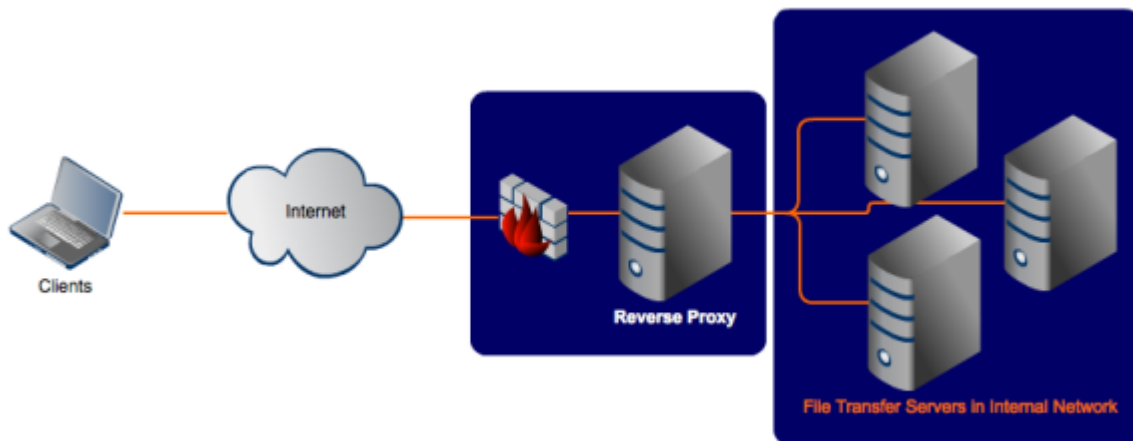
A reverse proxy is a web server that terminates connections with clients and makes new ones to backend servers on their behalf.

A backend server is defined as a server that reverse proxy makes a connection with in order to fulfill the client's request. 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 as it's a server that receives requests from the Internet and forwards (proxies) them to a small set of servers, usually located on an internal network and not directly accessible from outside. It's reverse, because a traditional (outbound) proxy

receives requests from a small set of clients on an internal network and forwards them to the Internet.

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



## Advantages of Reverse Proxies

- 1. Security:

A reverse proxy can hide the topology and characteristics of your back-end 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.

- 2. Caching:

The reverse proxy can also act as a cache. You can either have a dumb cache that simply 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 back-end servers.

- 3. Compression:

In order 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 back-end servers that would otherwise have to do the compression, and makes debugging requests to, and responses from, the back-end servers easier.

- 4. Simplifies access control tasks

Clients only have a single point of access, you can concentrate access control on that single point.

- 5. Aggregating Multiple Websites Into the Same URL Space

In a distributed architecture, it's desirable to have different pieces of functionality served by isolated components. A reverse proxy can route different branches of a single URL address space to different internal web servers.

- 6. 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 back-end servers.

## 7. Authentication

Reverse proxy can use client's certificates to verify their identity.

## 8. Whitelisting of users

It can block or allow a specific set of users to access the resources.

## 9. SSL Termination

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

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

---

## Far End Camera Control

Avaya SBCE 6.3 supports FECC Offer and Answer in SDP. Avaya SBCE checks if the media application line uses the H.224 codec. Any other media application line without an H.224 codec type is ignored.

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

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

Avaya SBCE supports High Availability on FECC media application line. If FECC media application is negotiated end-to-end by Offer and Answer exchange, Avaya SBCE continues to relay FECC media after failover.

---

## 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. Radvision 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.

The switched video stream uses only one presentation channel for multiple main video streams. BFCP messages control how multiple video streams access and use the shared video channel.

## Detailed description of Binary Floor Control Protocol

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

### Terminologies

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

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

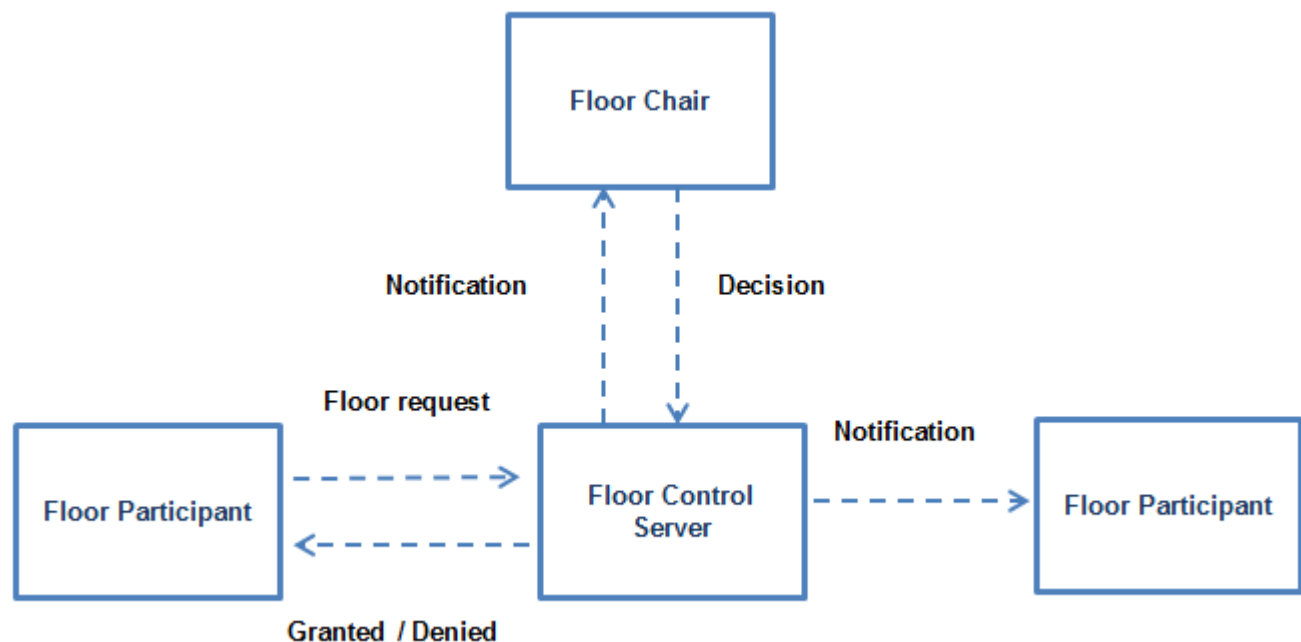


Figure 8: BFCP components

## Functioning of BFCP

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

Avaya SBCE Release 6.3 relays BFCP control messages to control the presentation channel. Avaya SBCE supports BFCP for only two video channels, one of which is a video presentation channel.

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

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

## SDP Offer and Answer exchange rules

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

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

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

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

## Architecture of Binary Floor Control Protocol

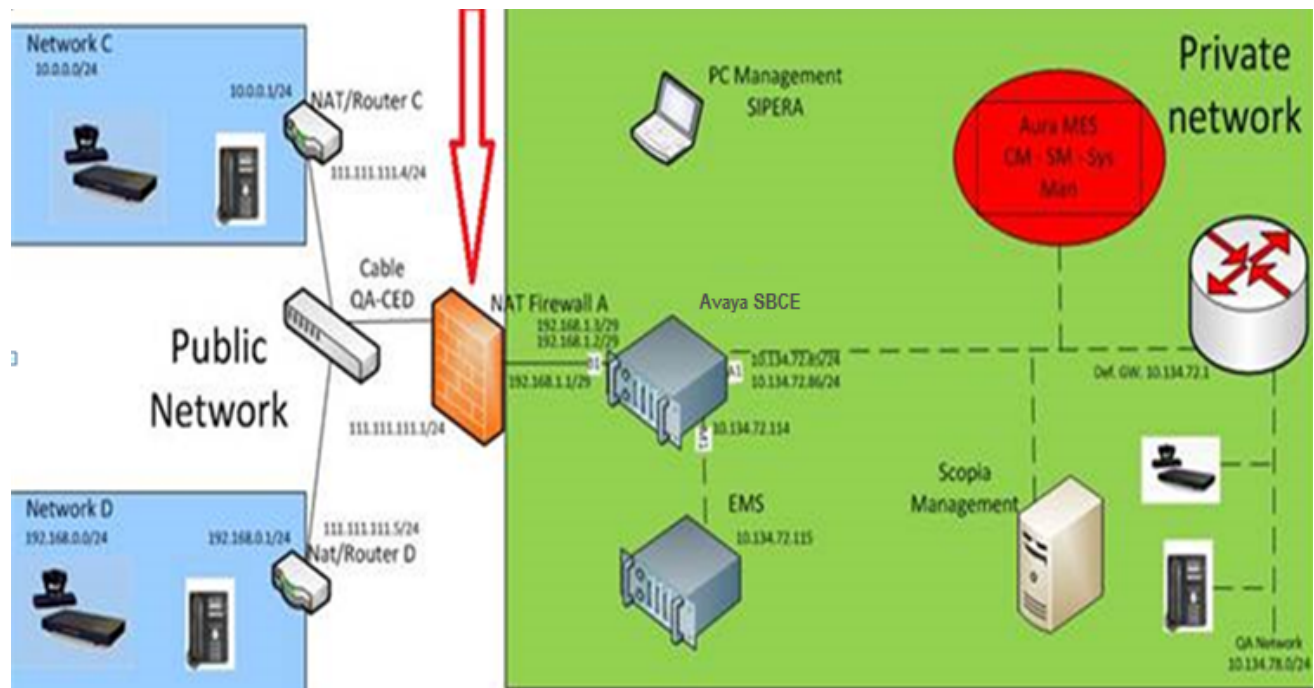


**Figure 9: BFCP architecture**

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

## Binary Floor Control Protocol scenarios

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

### Remote Worker XT-client calls XT-MCU

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

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

**Remote Worker XT-MCU calls internal XT-client**

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

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

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

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

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

| Sr No. | Sender                           | floor-ctrl | setup attribute | connection | BFCP application line     |
|--------|----------------------------------|------------|-----------------|------------|---------------------------|
| 4      | Avaya SBCE responds to Elite MCU | c-only     | active          | new        | Valid connection and port |

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

### Failover or network outage

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

---

## Forward Error Correction

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

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

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

---

## User registration

With Avaya SBCE Release 6.3, you can view the list of users that are registered through Avaya SBCE. You can also enter custom search criteria for the fields that are displayed on the system.

---

## Real Time SIP Server Status

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

For the servers to show up in the Status window, you must configure server heartbeat in Server Configuration. The SIP Server status is useful to determine which server is active when primary and secondary servers are available in the network.

---

## Licensing requirements

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

The license file contains the following information:

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

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

- Licensed features
- Licensed capacity

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

---

## Single Sign-On and Identity Engine

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

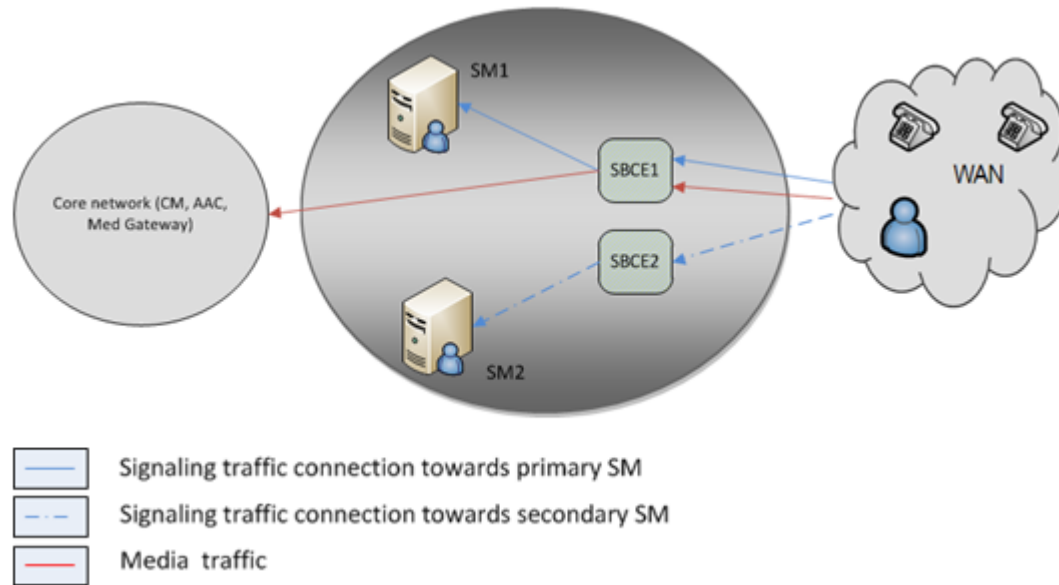
---

## Multiple Avaya SBCE deployment

In a Geo-redundant deployment, you can deploy two different Avaya SBCE devices in two different data centers. You can deploy these Avaya SBCE devices in a High Availability mode or a non-High Availability mode.

### Multiple Avaya SBCE deployment in the non-HA mode

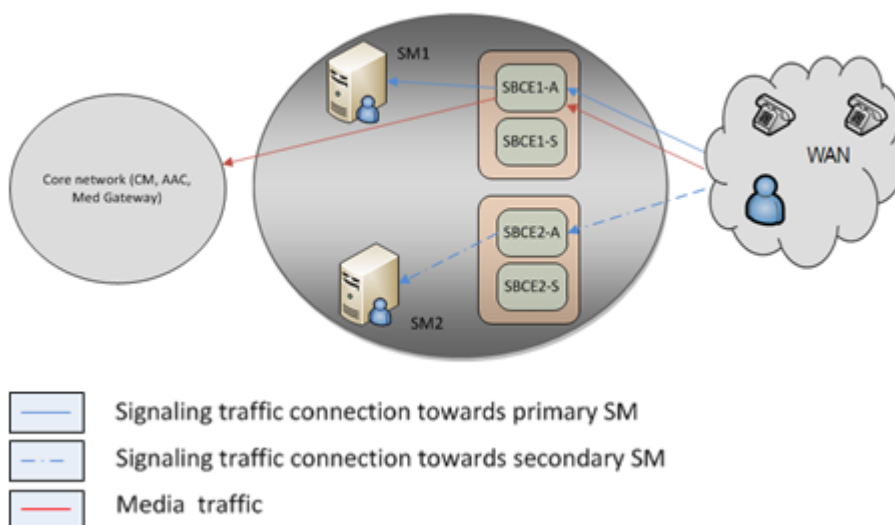
In the following diagram, SBCE1 and SBCE2 are two different physical devices deployed in different data centers. The endpoints have one connection with SBCE1 corresponding to the primary Session Manager, SM1. The second connection with SBCE2 corresponds to the secondary Session Manager, SM2.



## Multiple Avaya SBCE deployment in the HA mode

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

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



---

## WebRTC-enabled call handling

Avaya SBCE supports incoming calls from WebRTC-enabled web browsers to an external network to an internal Avaya Aura® networks with SIP at the core. For example, a consumer of an organization can call an Avaya Aura® network by using a WebRTC-enabled browser from the external network. This WebRTC call is possible if the organization discloses the organization website to real-time multimedia calls and enables the browser with APIs for real-time multimedia communication. The signaling and media traverse the border edge of the enterprise network that contains the firewall and Avaya SBCE in DMZ. In this scenario, Avaya SBCE, Avaya Aura® Collaboration Environment, and Avaya Media Server together function as the WebRTC-SIP gateway. This gateway cannot receive any signaling or media. Therefore, the signaling and media must traverse the border edge of the enterprise network. Avaya SBCE relays HTTP signaling using the Reverse Proxy feature and the media relay 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 by functionalities within the TURN/STUN server functionality built in Avaya SBCE.

### Note:

- WebRTC to SIP multimedia calls is not supported in Release 6.3. In this release, the WebRTC solution supports only audio with G711 codec. Avaya SBCE does not support the OPUS codec, but supports G711. A solution is configured with High Availability (HA) functionality so that new WebRTC calls can be started from the HA pair if the active or primary Avaya SBCE is nonfunctional. However, the solution does not provide HA survivability, therefore, the existing calls do not work after the primary Avaya SBCE becomes nonfunctional.
- Avaya does not support incoming calls from an external Avaya SBCE network to an internal network between WebRTC-enabled browsers.
- Avaya SBCE does not support NATting of WebRTC calls. The Turn relay address must be configured on the external interface of the Avaya SBCE. This address must be exposed on the external firewall of the DMZ. However, the external firewall must still provide layer 3 protection for the TURN relay address. The enterprise gateway router must be configured to route any packet through the external firewall. The packets can be destined for the external address of Avaya SBCE that is visible to public network. Currently, WebRTC does not have a mechanism to hide the external interface address of Avaya SBCE in DMZ from the public network.

## Performance

The WebRTC snap-in supports 1800 simultaneous calls at the rate of 28,000 BHCC in the following deployment models:

- Collaboration Environment (CE) server
- Avaya Aura® Session Border Controller for Enterprise (SBCE) server
- Avaya Media Server (MS) servers

The performance stated is for Avaya Aura® Collaboration Environment WebRTC-SIP gateway solution. Avaya SBCE performance reaches at least up to 7000 relay sessions.

For more information about WebRTC, see *Avaya WebRTC Snap-in Reference*.

## Virtualization architecture overview

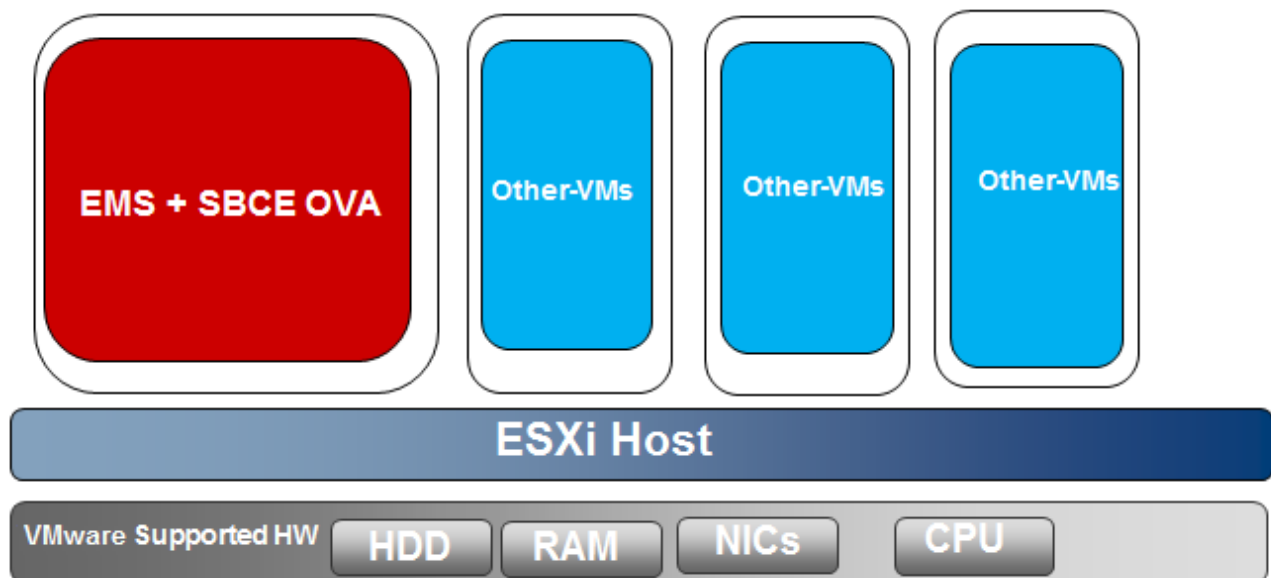
For deployment on VMware-certified hardware, Avaya SBCE is packaged as vAppliance ready (OVA) to run in the virtualized environment. Therefore, from Release 6.3, Avaya SBCE is also available for VMware-based deployments.

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

The Avaya SBCE OVA files are offered as vAppliance for EMS and Avaya SBCE configurations. Use the EMS OVA file for EMS-only deployments. Use the Avaya SBCE OVA file for EMS plus Avaya SBCE or Avaya SBCE only deployments. The .ova file for each deployment is available in Product Licensing and Delivery System (PLDS).

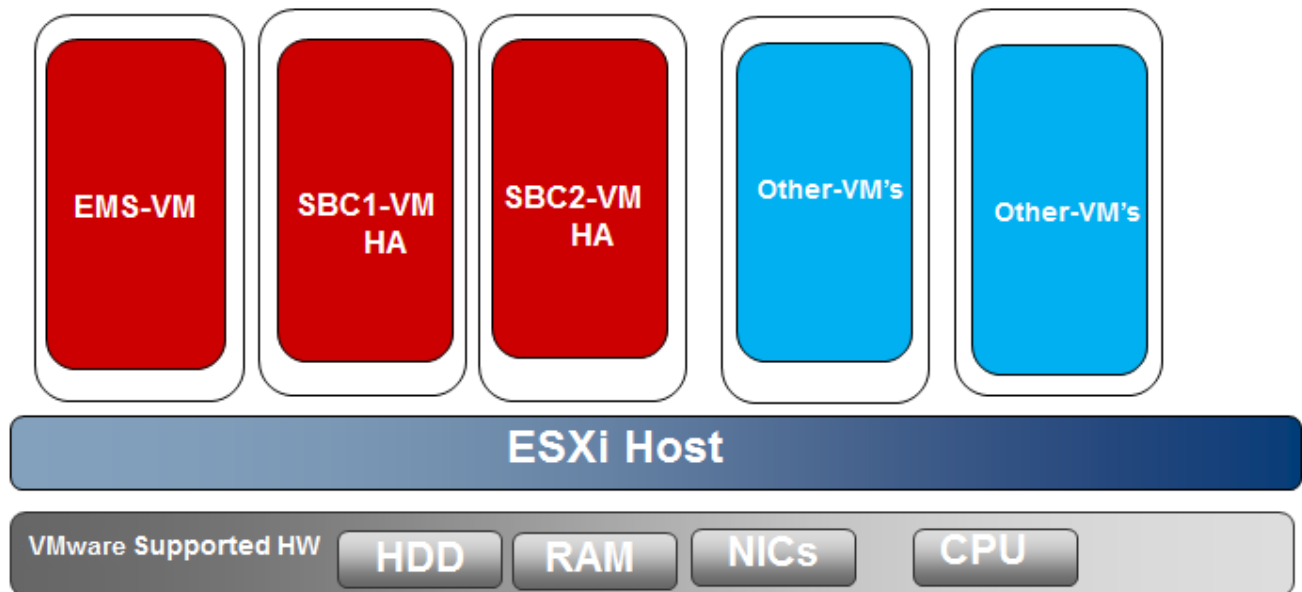
### Avaya SBCE standalone mode

The OVA file for standalone deployments includes OVA configurations for both Avaya SBCE and EMS. For Avaya SBCE mode, use the Avaya SBCE OVA file for installation.



### EMS and SBC in High Availability (HA) mode

For HA mode, use separate OVA files for EMS and Avaya SBCE.



## Virtual LAN

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

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

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

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

### \* Note:

A VLAN is supported on a data interface only.

## SRTP overview

Avaya SBCE 6.3 supports encrypted audio and multiple video media such as main video, video presentation, and Far End Camera Control (FECC) based on SDP capability negotiation.

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

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

**\* Note:**

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

## SRTP considerations

Avaya SBCE supports:

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

---

## Multiple subnet and multiple interfaces

### Multiple subnets

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

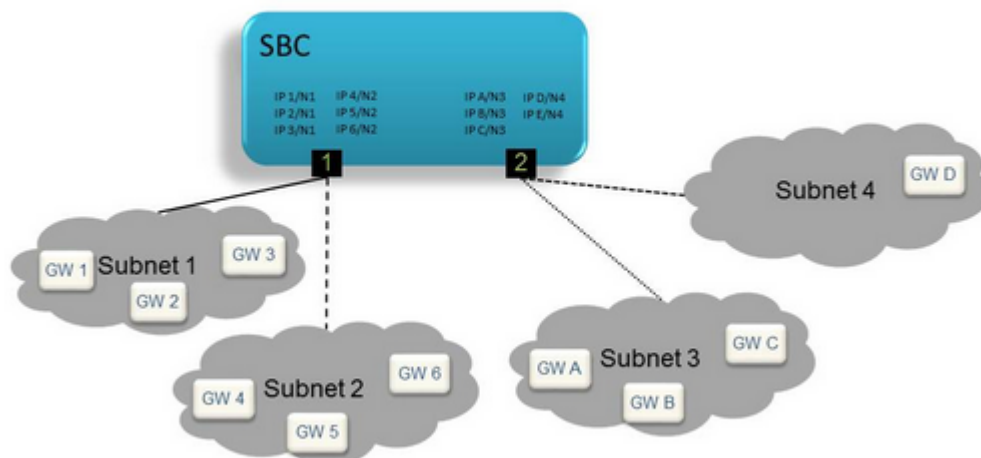


**Figure 10: Connectivity to multiple subnets on a single data interface**

In [Figure 10: Connectivity to multiple subnets on a single data interface](#) on page 45, subnets 1 and 2 are reachable through interface 1, while subnets 3 and 4 are reachable through interface 2.

### Overlapping address spaces

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

### VLAN support

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

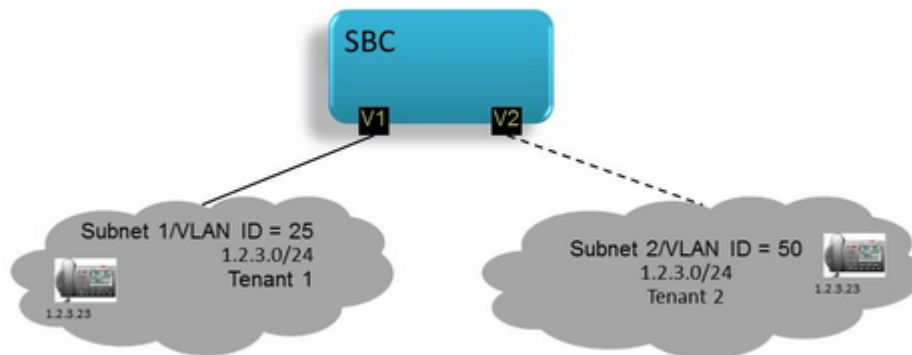


Figure 11: VLAN support

## Deployment examples

### Avaya SBCE connected to multiple subnets on a single interface

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

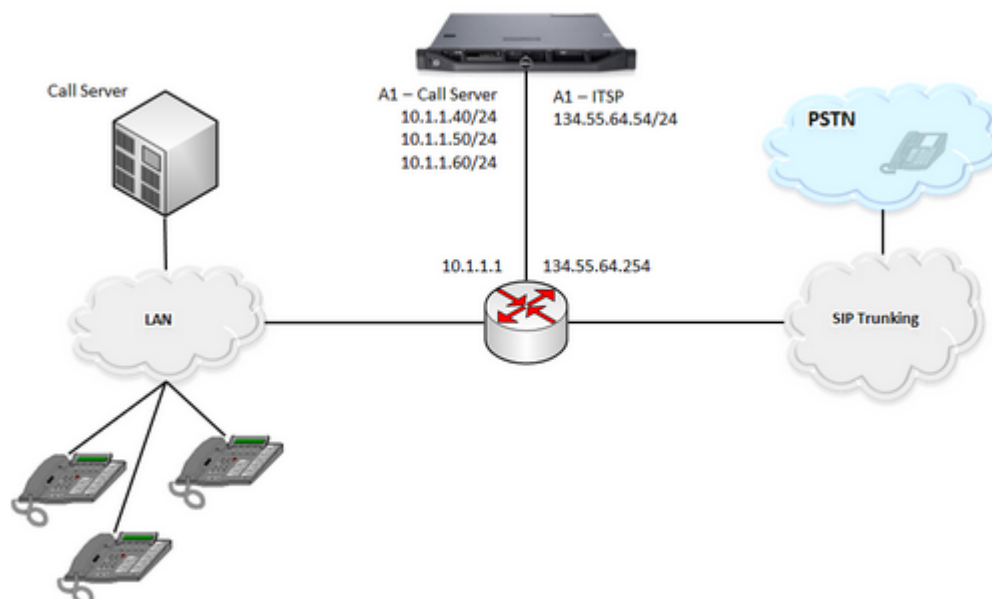


Figure 12: Avaya SBCE connected to multiple subnets on a single interface

### Configuration details

- **Interfaces and purposes:** This configuration uses only the A1 Avaya SBCE data interface. With the help of the next-hop router, this data interface provides connectivity to two different

networks: the call server network and the ITSP network. This configuration uses three Avaya SBCE IP addresses: two for the call server network and one for the ITSP network.

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

### Avaya SBCE connected to multiple subnets on two interfaces

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

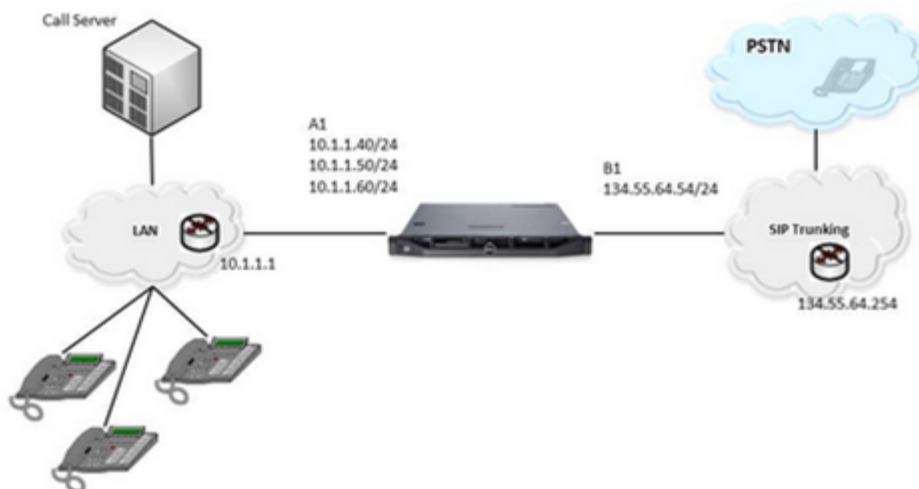


Figure 13: Avaya SBCE connected to multiple subnets on two data interfaces

#### Configuration details

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

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

## Avaya SBCE connected to multiple subnets by using a single VLAN

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

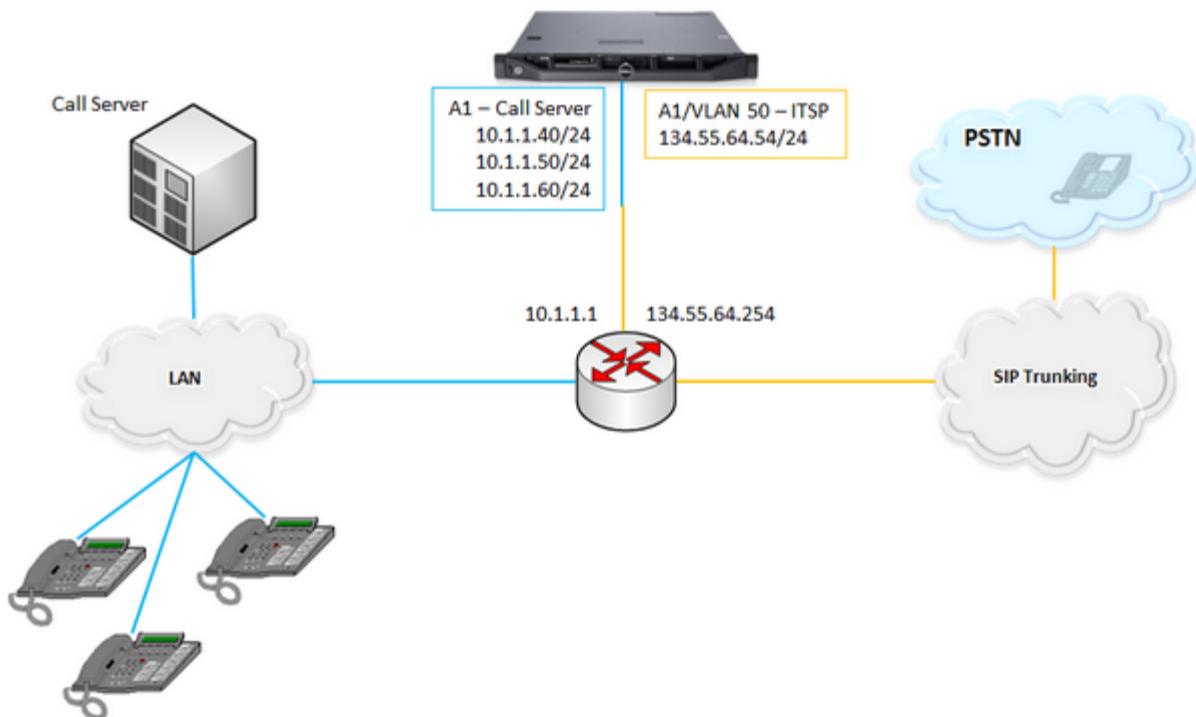


**Figure 14: Avaya SBCE connected to multiple subnets, using a single VLAN and a single data interface**

### Configuration details

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

button located in the **Device Specific Settings > Network Management > Interfaces** tab. Initially, keep the VLAN interface disabled. Then enable both the A1 and ITSP VLAN interfaces while other interfaces remain disabled.

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

## Multiple gateways on the same network

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

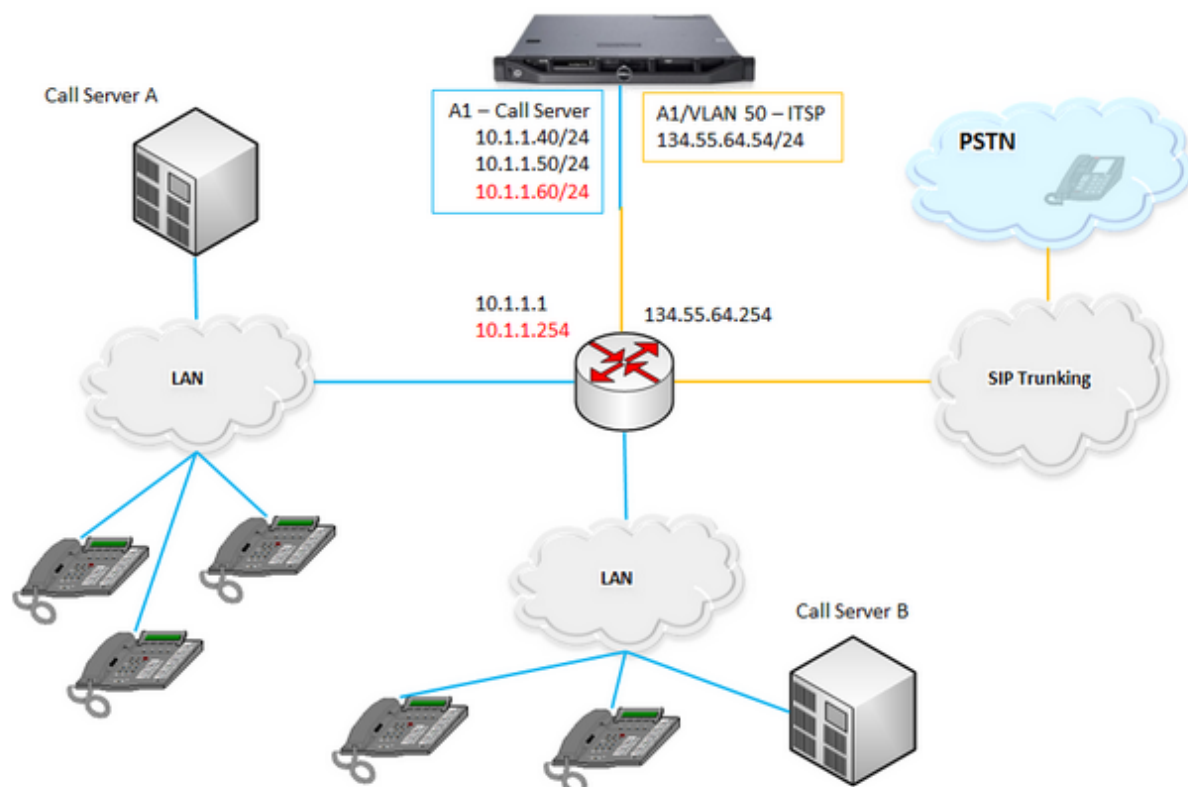


Figure 15: Multiple gateways on the same network

### Configuration details

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

default gateway on the call server network. Additionally, Avaya SBCE uses the 10.1.1.254 gateway to reach call server B, as the default gateway in this example is unable to reach the network.

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

## Multiple tenants, call servers, and Avaya SBCE interfaces

This scenario uses all four Avaya SBCE data interfaces. Avaya SBCE connects to two tenant networks, each with a unique set of remote workers. Avaya SBCE also connects to three other networks, each with a call server. Each call server is reached through a separate physical interface, which provides a measure of redundancy when one or more call servers stop responding. This type of load balancing and redundancy is a new feature in Release 6.3.

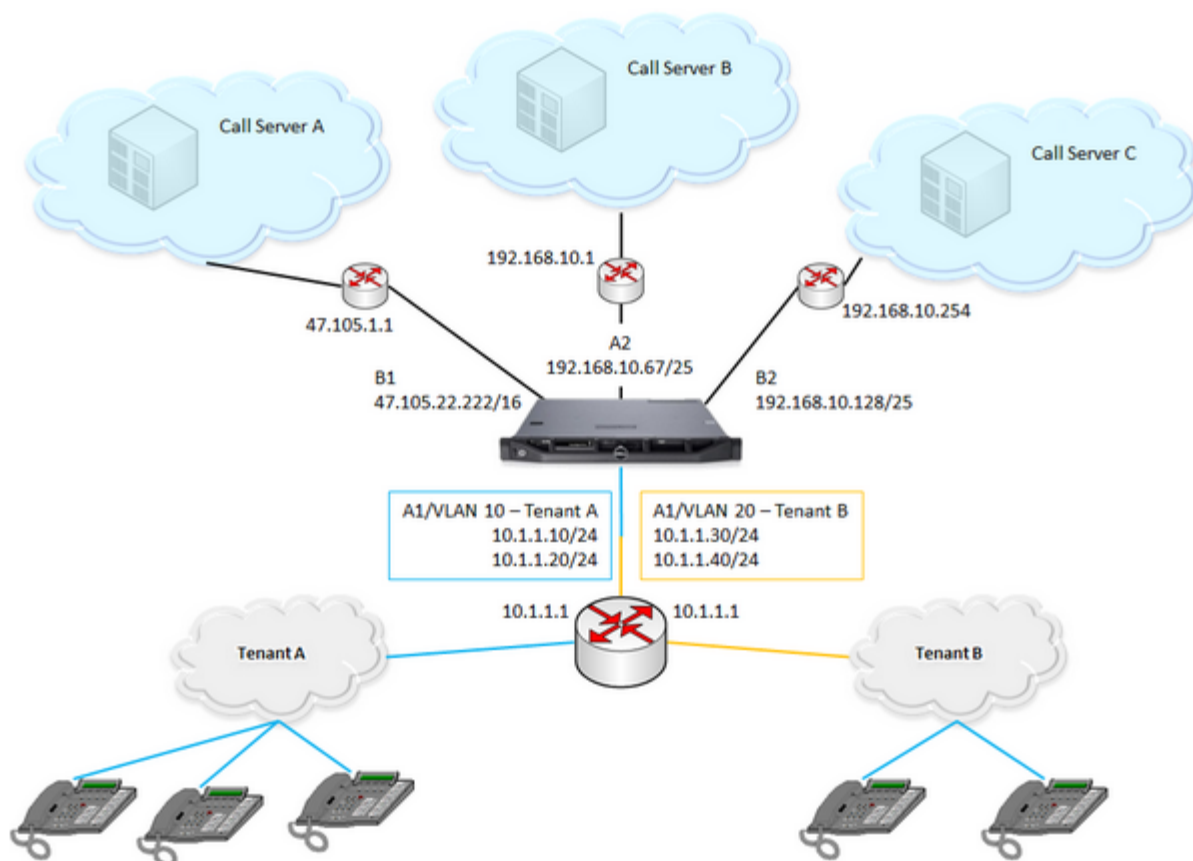


Figure 16: Multiple tenants, call servers, and Avaya SBCE interfaces

### Configuration details

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

B (in orange) uses VLAN 20. The gateway router on the A1 interface provides connectivity to both tenant VLANs.

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

**\* Note:**

You can attach tenants to the B1 interface and connect call server A through the A1 interface. The physical ports retain their historical names: A1, A2, B1, and B2.

- **Surrounding networking equipment:** This configuration supports corresponding mapping between SBC NICs and physical server NICs. Configure the gateway on the A1 interface to support VLAN 10 and VLAN 20, and the associated gateway IP addresses. You do not need to configure the other three gateways on A2, B1, or B2 separately. If Avaya SBCE is running on a virtual machine, configure VMWare vSwitch and the physical interfaces on the server. If each physical interface on Avaya SBCE uses a separate vSwitch and each vSwitch connects to a separate physical interface on the server, connect vSwitch to a physical port setup. . Configure up to four vSwitches.
- **Avaya SBCE Network interfaces:** When you configure VLANs on Avaya SBCE, the first step is always to create the VLAN interfaces. In this example, two VLAN interfaces are created to support the two tenant networks. First, the VLAN for tenant A on interface A1. Then, the VLAN for tenant B on A1. The remaining networks use physical interfaces on Avaya SBCE. Finally, enable all the interfaces: the two VLANs as well as A2, B1, and B2.
- **Networks connected to Avaya SBCE:** In this example, the 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.

---

## Overview

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

SIP and PPM traffic is encrypted especially in Remote Worker configurations. Checking encrypted traffic with a network capture is difficult and time consuming. The delay occurs because the unencrypted private key of the 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 SBCE log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, you can use the tool easily even in case of TLS and HTTPS. traceSBC can parse the log files downloaded from the SBC. traceSBC can also process log files real time on the 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.

## SIP and PPM logging administration

Starting from Release 6.3, SIP and PPM logging is always enabled by default.

## Log files

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

### Log locations:

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

Active files are of the following format:

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

Inactive or closed files are of the following format:

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

## Advantages

### Memory

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

### Processor

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

---

## Support for Linux 6.4

Avaya SBCE 6.3 supports Redhat Enterprise Linux (RHEL) 6.4. Previously, Avaya SBCE included various Linux kernel versions and distributions, which support the various computing elements across different Avaya SBCE models.

Maintaining various kernel versions poses problems because the kernel and distribution are at the foundation of the platform software. Supporting different kernel versions is impractical because of the following reasons:

- Opening the product to security vulnerabilities: Keeping the kernels up-to-date with all the security patches is a challenge.
- Propagation of versioning into the application software: If application software relies on an underlying kernel or distribution feature and that feature is not available across all versions, different flavors of application code is supported to deal with each different distribution.
- Potential licensing issues: Some vendors require a license fee to support their flavor of the Linux kernel, and any associated tool chain or distribution. MontaVista charges a license fee to support the Linux kernel.

To avoid kernel management issues, the Avaya SBCE platform now uses the standard Linux distribution used across most Avaya Linux-based products, and corresponds to kernel version 2.6.32. This distribution and kernel is used on all SBC platforms, both Octeon- and non-Octeon based.

After this change, Avaya SBCE can also benefit from the operating system fixes made for other Avaya products.

You can enable the Avaya operating system with networking support.

# Chapter 3: Interoperability

## Product compatibility

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

### Avaya SBCE supported servers

| Server                                                                                                                                                                                                                                 | Processors                                  | System Memory             | On-board Storage                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|---------------------------|-------------------------------------------------|
| Dell R210 II XL (core)                                                                                                                                                                                                                 | Intel Xeon E3-1220 3.10 GHz Quad Core/4T    | 4 GB (DDR3 1333MHz)       | 500 GB (3.5-in SATA 3Gb/s – 7.2K)               |
| Dell R210 II (core)                                                                                                                                                                                                                    | Intel Xeon E3-1230 3.20 GHz Quad Core/4T    | 4 GB (DDR3 1333MHz)       | 500 GB (3.5-in SATA 3Gb/s – 7.2K)               |
| Dell R210 II XL (EMS)                                                                                                                                                                                                                  | Intel Pentium G850 2.90 GHz Dual Core/2T    | 2 GB (DDR3 1333MHz)       | 2 x 500 GB (3.5-in SATA 3Gb/s – 7.2K)           |
| Dell R620                                                                                                                                                                                                                              | Intel® Xeon® E5-2600, Dual core             | 32 GB (DDR3 1333)         | 2.5-in SATA 3Gb/s – 7.2K                        |
| HP DL 360 G7                                                                                                                                                                                                                           | Intel Xeon 5600 series, Quad core           | up to 192 GB (DDR3 RDIMM) | 3 x 146GB HP SAS SFF 15K hard disks in hot-swap |
| HP DL 360 G8                                                                                                                                                                                                                           | Intel® Xeon® E5-2400                        | up to 384GB               | (8) SFF SAS/SATA/SSD                            |
| Supermicro AMAX (EMS)                                                                                                                                                                                                                  | Intel Core 2 Duo E6400 2.13 GHz – Dual Core | 2 GB (DDR2 667MHz)        | 2 x 160 GB (3.5-in SATA 3Gb/s – 7.2K)           |
| <p> <b>Note:</b><br/>Only upgrades from the previous version are supported for AMAX servers. New installation of Avaya SBCE is not supported on</p> |                                             |                           |                                                 |

| Server                   | Processors                              | System Memory                | On-board Storage                    |
|--------------------------|-----------------------------------------|------------------------------|-------------------------------------|
| AMAX servers.            |                                         |                              |                                     |
| Portwell CAD-0208 (core) | Intel® Atom D510<br>1.66GHz - Dual Core | 2GB (SO-DIMM<br>DDR2 667MHz) | 320GB (2.5-in SATA 3Gb/s –<br>7.2K) |

**\* Note:**

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

## Avaya products

### SIP Trunking

The following products are compatible with Avaya Session Border Controller for Enterprise Release 6.3 for SIP Trunking.

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

### Mobile Workspace User (Remote Worker)

The following products are compatible with Avaya Session Border Controller for Enterprise Release 6.3 for Mobile Workspace User.

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

| Product                       | Release                                                      |
|-------------------------------|--------------------------------------------------------------|
| Avaya Communicatorfor Android | Mobile Workspace User with Avaya Aura® Release 6.2 and later |
| E.129                         | Mobile Workspace User with Avaya Aura® Release 6.2 and later |
| B.179                         | Mobile Workspace User with Avaya Aura® Release 6.2 and later |
| ACA                           | Mobile Workspace User with Avaya Aura® Release 6.2 and later |
| SIP Agent                     | Mobile Workspace User with Avaya Aura® Release 6.2 and later |

---

## Third-party product requirements

### External SAL gateway

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

---

## Operating system compatibility

The Avaya SBCE and EMS use RedHat Enterprise Linux 6.5 on all platforms.

# Chapter 4: Performance specifications

## Capacity and scalability specification

|                                                    | Portwell                                           | Dell R210 II XL                                                                             | Dell R620                                                                                   | HP DL360 G8                                                                                 | VMware                                                                                         |
|----------------------------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
|                                                    | Single Availability (SA) only                      | Single availability (SA) and High availability (HA)<br>One- and three-server configurations | Single availability (SA) and High availability (HA)<br>One- and three-server configurations | Single availability (SA) and High availability (HA)<br>One- and three-server configurations | Single availability (SA) and High availability (HA)<br>HA can be based on VM or in application |
| <b>Maximum simultaneous sessions: SIP Trunking</b> | 500<br>(above 150 consider other platforms and HA) | 6000                                                                                        | 6000                                                                                        | 6000                                                                                        | 250                                                                                            |
| <b>Maximum simultaneous sessions: Advanced</b>     | 250<br>(above 150 consider other platforms and HA) | 2000                                                                                        | 2000                                                                                        | 2000                                                                                        | 250                                                                                            |
| <b>Maximum simultaneous sessions: Encryption</b>   | 250<br>(above 150 consider other platforms and HA) | 1200                                                                                        | 1200                                                                                        | 1200                                                                                        | 250                                                                                            |
| <b>Maximum simultaneous sessions: Scopia Video</b> | N/A                                                | 200                                                                                         | 200                                                                                         | 200                                                                                         | 25                                                                                             |

The capacity specifications are based on:

- Codec specification: The G711 codec with 20 ms packetization time is used with all audio sessions.
- Call Model: The SIP RFC call model in trunk mode is used to establish these capacity specifications.

- Avaya SBCE Configuration: Default logging levels are used, and security features are turned off.

For Geo-redundant HA systems or for an EMS controlling multiple HA pairs, at least 150ms delay on a layer 2 round trip is required.

---

## Redundancy and high availability

These features are available with EMS, Dell R210 II XL, Dell R620, HP DL360 G7, and HP DL360 G8 platforms. These features are also available for Avaya SBCE deployed in a virtualized environment.

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

### **Note:**

Avaya SBCE devices in a HA configuration must be on a different subnet from the Avaya core PBXs, Gateways, phones, and any other devices that do not support Gratuitous ARP (GARP). The switch or router to which Avaya SBCE is connected must support GARP. For elements that do not support GARP, a GARP-aware router or switch must be introduced between these elements and the Avaya SBCE. This switch handles GARP packets sent from the Avaya SBCE. All IP addresses configured in the Network Configuration screen are shared between both HA devices in HA deployment mode. The HA devices are also configured with private, default IPs which are used to replicate signaling and media data between each other. The configured interfaces are inoperative on the standby or secondary device until it becomes active or primary. When the devices switch, the active device sends a GARP message to update the ARP tables of the neighboring HA device to begin receiving traffic.

---

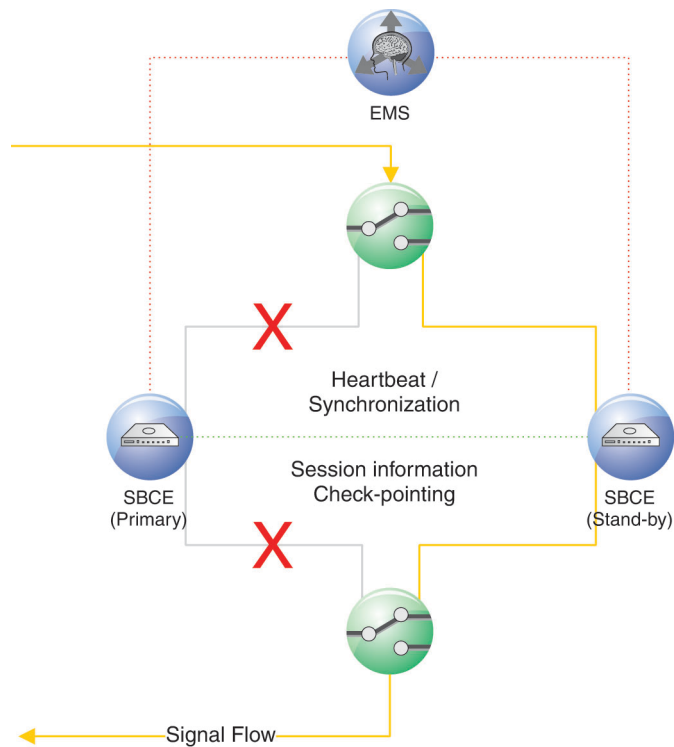
## Avaya SBCE high availability

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

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

When the Avaya EMS detects a failure on the active Avaya SBCE, the active SBC network interface ports are automatically disabled. The ports of the standby SBC are enabled. Failure detection and

operational transfer occur without dropping packets or adding any significant amount of latency into the data paths. The EMS reports the change in status to the EMS for action by the system administrator.



cysbtpcl LAO 021413

**Figure 17: Typical Avaya SBCE HA – Parallel Mode Topology (colocated)**

## EMS replication

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

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

# Chapter 5: Environmental requirements

---

## Altitude requirements

### Dell R210 II XL altitude ranges

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

---

## Hardware dimensions

| Server                   | Height             | Width                      | Depth                | Weight              |
|--------------------------|--------------------|----------------------------|----------------------|---------------------|
| Dell R210 II XL (Core)   | 1.7 in. (4.32 cm)  | 17.10 in. (43.45 cm)       | 15.50 in. (39.37 cm) | 15.5 lbs. (7.03 kg) |
| Dell R210 II (Core)      | 1.7 in. (4.32 cm)  | 17.10 in. (43.45 cm)       | 15.50 in. (39.37 cm) | 15.5 lbs. (7.03 kg) |
| Dell R210 II XL (EMS)    | 1.7 in. (4.32 cm)  | 17.10 in. (43.45 cm)       | 15.50 in. (39.37 cm) | 15.5 lbs. (7.03 kg) |
| Dell PowerEdge R620      | 1.7 in. (4.318 cm) | 17.1 in. (43.434 cm)       | 26.9 in. (68.326 cm) | 41.0 lbs (19.1 kg)  |
| AMAX (EMS)               | 1.7 in. (4.32 cm)  | 17.1 in. (43.45 cm)        | 15.50 in. (39.37 cm) | 15.5 lbs. (7.03 kg) |
| Portwell CAD-0208 (core) | 1.65 in. (4.20 cm) | 7.10 in. (18.03 cm)        | 5.90 in. (14.98 cm)  | 15.5 lbs. (7.03 kg) |
| HP Proliant DL360 G8     | 1.7 in. (4.318 cm) | 17.1 in. (43.434 cm)       | 27.5 in. (69.85 cm)  | 42.3 lbs (19.19 kg) |
| HP Proliant DL360 G7     | 1.7 in. (4.32 cm)  | 16.78 in. (42.62 cm)<br>cm | 27.38 in (69.53 cm)  | 35.20 lb (15.97 kg) |

## Temperature and humidity requirements

| Server                   | Operating Temperature              | Storage Temperature                | Relative Humidity                              |
|--------------------------|------------------------------------|------------------------------------|------------------------------------------------|
| Dell R210 II XL (core)   | 50 °F to 95 °F (10 °C to 35 °C)    | -40 °F to 149 °F (-40 °C to 65 °C) | 20% to 90%, noncondensing                      |
| Dell R210 II (core)      | 50 °F to 95 °F (10 °C to 35 °C)    | -40 °F to 149 °F (-40 °C to 65 °C) | 20% to 90%, noncondensing                      |
| Dell R210 II XL (EMS)    | 50 °F to 95 °F (10 °C to 35 °C)    | -40 °F to 149 °F (-40 °C to 65 °C) | 20% to 90%, noncondensing                      |
| Dell R620                | -40 °F to 149 °F (-40 °C to 65 °C) | -40 °F to 149 °F (-40 °C to 65 °C) | 5% to 95%                                      |
| AMAX (EMS)               | 50 °F to 95 °F (10 °C to 35 °C)    | -40 °F to 158 °F (-40 °C to 70 °C) | 8% to 90%, noncondensing                       |
| Portwell CAD-0208 (core) | 41 °F to 95 °F (5 °C to 35 °C)     | 32 °F to 158 °F (0 °C to 70 °C)    | 20% to 90%, noncondensing                      |
| HP DL 360 G7             | 50 °F to 95 °F (10 °C to 35 °C)    | -40 °F to 158 °F (-40 °C to 70 °C) | 5% to 95% nonoperating<br>10% to 90% operating |
| HP DL 360 68             | 50 °F to 95 °F (10 °C to 35 °C)    | 101.7 °F (38.7 °C)                 | 5 to 95% nonoperating<br>10 to 90% operating   |

**\* Note:**

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

## Power requirements

| Server                 | Input                   | Nominal (110 V) | AC Power Max |
|------------------------|-------------------------|-----------------|--------------|
| Dell R210 II XL (core) | 110–240 VAC auto switch | 2 A             | 250 W        |
| Dell R210 II (core)    | 110–240 VAC auto switch | 2 A             | 250 W        |
| Dell R210 II XL (EMS)  | 110–240 VAC auto switch | 2 A             | 250 W        |
| Dell R620              | 110–240 VAC             | 2 A             | 750 W        |
| AMAX (EMS)             | 110–240 VAC auto switch | 2 A             | 250 W        |

| Server                   | Input                   | Nominal (110 V) | AC Power Max          |
|--------------------------|-------------------------|-----------------|-----------------------|
| Portwell CAD-0208 (core) | 110–240 VAC auto switch | 2 A             | 60 Watt Power Adapter |
| HP DL360p G7             | 100–120 VAC             | 5.5 A           | 526 W                 |
| HP DL360p G8             | 100–240 VAC             | 15 A            | 308.95 W              |

## Physical system protection requirements

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

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

### Note:

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

## Regulatory standards

Avaya SBCE servers conform to the following standards.

| Server                   | Certifications                                                                                                                                                           |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dell R210 II XL (core)   | CSA, FCC, UL, RoHS                                                                                                                                                       |
| Dell R210 II (core)      | CSA, FCC, UL, RoHS                                                                                                                                                       |
| Dell R210 II XL (EMS)    | CSA, FCC, UL, RoHS                                                                                                                                                       |
| AMAX (EMS)               | <ul style="list-style-type: none"> <li>• USA: UL listed, FCC</li> <li>• Canada: CUL listed</li> <li>• Europe: CE Mark</li> <li>• EN 60950/IEC 60950-compliant</li> </ul> |
| Portwell CAD-0208 (core) | CE, FCC, UL                                                                                                                                                              |

# Chapter 6: Security

---

## Security specification

---

### Unified communications intrusion protection

Traditional intrusion prevention systems (IPS) monitor network traffic to gather and analyze information from various parts of the network to identify possible security breaches. This information is used for subsequent prevention or mitigation. Unlike traditional IPS, Avaya SBCE security products detect any anomalous event, including day zero attacks. Additionally, also prevents virtually any type of intrusion from outside the enterprise and misuse from within the enterprise. This capability is because of the unparalleled flexibility and fine-grain tuning allowed when network security administrators establish Unified Communications rule sets. The Avaya SBCE IPS security feature includes:

- **Flood and Fuzzing Protection:** Protection from volume-based Denial-of-Service (DoS) and malformed message or fuzzed attacks. Customized protocol scrubbing rules detect and remove malformed messages that might cause call servers or other critical network components to stop responding. Malformed messages can also make other portions of the communications infrastructure vulnerable because of degraded performance of critical Unified Communications systems components, such as servers and endpoints.
- **Media Anomaly Prevention:** Selectively enables the media traffic and enforces rules on the traffic carried. The traffic flow is based on the negotiated signaling and other configured policies, such as prevent video or prevent modem/FAX.
- **Spoofing Prevention:** Various validation techniques are applied to detect and prevent spoofing, including the end-point fingerprints for different message fields to trigger other validations and verifications.
- **Stealth Attack Prevention:** Based on the learned call behavior patterns of subscriber endpoints, Avaya SBCE security products can detect any nuisance and annoying calls to a particular destination or user. These products can selectively block the subscribers from whom the calls originate.
- **Reconnaissance Prevention:** Avaya SBCE security products detect and block application layer scan reports and block the attackers that originate them.

---

## Attack protection

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

### Monitoring

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

 **Note:**

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

### Detection

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

The detection capability is also able to collect and correlate multiple events and activities from different nodes and endpoints in the network to accurately detect attacks. These attacks might otherwise have escaped unnoticed if reported only by a single point in the network. The detection capability can inspect the sequence and content of messages to detect protocol anomalies and any instances of endpoint scanning. Finally, the detection capability of the Avaya SBCE solution can validate the source of a suspected malicious call or attack by implementing a unique detection technique that is based upon learned caller fingerprints.

Avaya SBCE security products can continuously learn call patterns and endpoint fingerprints. These products can also constantly analyze raw event data based on specific user-definable criteria and

take automatic action. Therefore, Avaya SBCE security products can evolve and adapt automatically to effectively counter any new or existing threat.

## Protection

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

---

## Avaya SBCE hardening

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

Outbound traffic is unrestricted.

---

## Protection against layer 3 and layer 4 floods and port scans

### ICMP flood prevention

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

### Port scan blocking

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

### Data interface restrictions

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

### TCP signaling level flood control

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

- TCP SYN

- FIN
- RST

## System-wide security settings

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

The Avaya SBCE has the following protection types:

- General Protection
- Management Interface Restrictions
- Data Interface Restrictions

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

For Avaya SBCE, there are no restrictions on the internal Ethernet interface, ethbint, and external Ethernet M1 interface, ethext, on the Com Express coprocessor board in the Avaya SBCE box.

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

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

## Installation security

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

---

## DoS security features

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

- For Remote Worker, the input is taken from Number of remote workers and Max Concurrent Sessions
- For Trunk, the input is taken from Max Concurrent Sessions
- For Remote Worker and Trunk, the input is taken from Number of remote workers and Max Concurrent Sessions

Rules for setting threshold values for different types of traffic:

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

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

List of recommended threshold values:

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

---

## Protocol scrubber

Protocol scrubbing uses a sophisticated statistical mechanism to thoroughly check incoming SIP signaling messages for various types of protocol-specific events and anomalies. The protocol scrubber verifies certain message characteristics such as proper message formatting, message sequence, field length, and content against templates received from Avaya. Messages that violate the security rules dictated by the scrubber templates are dropped while messages that violate syntax rules are repaired. Messages are repaired by rewriting, truncating, rejecting, or dropping, depending on the processing rules imposed by the templates. Protocol scrubbing rule templates are prepared by Avaya and the user can edit the templates minimally.

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

---

## Topology hiding

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

---

## Firewall rules

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

- Common rules
- Management rules

- Data interface rules

## Common rules

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

- ICMP restrictions
- Portscan detection
- KILLSCAN rules

### ICMP restrictions

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

### Detecting Portscan

#### Procedure

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

### KILLSCAN rules

1. Remove the current IP from the portscan list.
2. Any IP address sending packets with FIN, PSH, and URG flags set, but without SYN, RST, or ACK flags is added to the portscan list.
3. Any IP address sending packets with SYN and RST flags set is added to the portscan list.
4. Any IP address sending packets with FIN and SYN flags set is added to the portscan list.
5. Any IP address sending packets with FIN flags set, but without SYN, RST, PSH, ACK, or URG flags is added to the portscan list.
6. Any IP address sending packets with FIN, SYN, RST, PSH, ACK, and URG flags set is added to the portscan list.
7. Any IP address sending packets without any FIN, SYN, RST, PSH, ACK, or URG flags set is added to the portscan list.
8. Any IP address sending packets with FIN, SYN, RST, PSH, ACK, and URG flags set is added to the portscan list.

9. Drop all packets from any IP in the portscan list.

## Management and MGMTPROTECT rules

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

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

### Management rules

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

### TCP flood restrictions for all ports

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

### SSH rules

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

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

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

## HTTPS rules

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

## DNS rules

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

## OpenVPN rules

- Any IP address sending, on TCP port 1194, packets with the SYN flag but, without RST or ACK is added to the ovpsyn list.
- For any IP address in the ovpsyn list that sends, on TCP port 1194:  
Ten packets with the SYN flag but, without RST or ACK in one second during the TTL of the previous packet sent, drop the packet.  
Five packets with the SYN flag but, without RST or ACK in one second during the TTL of the previous packet sent, reject the packet. Send an ICMP port unreachable message.

## Data interface rules

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

- Follow DATAIFPROTECT rules.
- Accept all packets.

## Protect-socket command

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

- Any IP address sending a packet to the specified IP and port with the SYN flag but not RST or ACK is added to the apprules list.

- For any IP address in the apprules list that sends:
  - Ten packets with the SYN flag, but without RST or ACK to the specified IP and port in one second during the TTL of the previous packet sent, drop the packet.
  - Five packets with the SYN flag, but without RST or ACK to the specified IP and port in one second during the TTL of the previous packet sent, reject the packet. Send an ICMP port unreachable message.
- If the protection scheme is given as 1, also follow these rules:
  - For any IP address that sends twenty packets in state ESTABLISHED to the specified IP and port in one second, drop the packet.
  - Keep a record of any IP address that sends a packet in the ESTABLISHED state to the specified IP and port.
  - For any IP address that sends three packets in the NEW state to the specified IP and port in one second, drop the packet.
  - Keep a record of any IP address that sends a packet in the NEW state to the specified IP and port.
- Delete any existing rule for accepting packets.
- Accept all packets.

---

## Port utilization specification

---

### Management interface port restrictions

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

#### Internal – Between one or more SBCs and the EMS

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

#### External – Between the EMS and SBCs and an external device

1. SSH TCP-222.
2. HTTPS TCP-443.
3. Syslog TCP/UDP-514.
4. NTP UDP-123.
5. DNS TCP/UDP-53 for DNS and the signaling and media ports.

6. SNMP Versin. 2 or 3 UDP-161 + 162. The SNMP agent receives requests on UDP port 161, and the SNMP manager receives notifications for traps and InformRequests on port 162

---

## TCP packets

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

---

## SSH port

The following rules apply to the SSH port:

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

---

## Additional port assignments

### DNS server

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

### SNMP

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

### Syslog

If you have your own Syslog, open the Syslog UDP port 514 on Avaya SBCE through the EMS GUI. Then, Avaya SBCE can access the Syslog from the DMZ.

### Media ports

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

### SIP signaling ports

The following ports are default ports. Other ports can be configured.

- TCP/UDP 5060
- TLS 5061

**HTTP/HTTPS ports**

These ports are used for Personal Profile Management (PPM) communications and configuration files and firmware downloads. Configure these ports on Avaya SBCE through the EMS GUI. Then, the phones can login and download configuration files from Avaya HTTP server or HTTPS server.

- HTTP port 8080 or port 80
- HTTPS port 443

**LDAP/LDAPS ports**

- LDAP port 389
- LDAPS port 636

**Shared Control port**

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

# Chapter 7: Licensing requirements

Avaya Session Border Controller for Enterprise uses the Avaya Product Licensing and Delivery System (PLDS) to create release 6.3 licenses and download Avaya SBCE software. The license file generated by PLDS is downloaded to the EMS. PLDS is not integrated with WebLM. Use PLDS to perform operations such as license activations, license upgrades, license moves and software downloads.

There are two licensed versions of Avaya SBCE:

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

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

 **Note:**

Licenses and a WebLM server are required for an upgrade to Release 6.3 or a new installation of Avaya SBCE Release 6.3.

---

## Avaya SBCE license features

| License feature                   | Description                                                                                  |
|-----------------------------------|----------------------------------------------------------------------------------------------|
| VALUE_SBCE_STD_SESSION            | Specifies the number of trunking session licenses.                                           |
| VALUE_SBCE_ADV_SESSION            | Specifies the number of session licenses for remote worker, media recording, and encryption. |
| VALUE_SBCE_ELEMENTS_MANAGED       | Specifies the maximum number of Avaya SBCE elements managed.                                 |
| VALUE_SBCE_ENCRYPTION             | Specifies the Avaya SBCE encryption.                                                         |
| VALUE_SBCE_VIDEO_CONF_SVC_SESSION | Specifies the maximum number of Avaya SBCE video conferencing sessions.                      |
| FEAT_SBCE_HIGHAVAILABILITY_CONFIG | Specifies the configuration of HA for the setup.                                             |

---

## WebLM server details

Avaya SBCE uses WebLM for licensing requirements.

The license file contains the following information:

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

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

- Licensed features
- Licensed capacity

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

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

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

For installing a license through a local WebLM server on :

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

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



### Warning:

Virtual EMS cannot run a local WebLM.

# Glossary

|                                             |                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ARP</b>                                  | Address Resolution Protocol                                                                                                                                                                                                                                                                                                                |
| <b>Codec</b>                                | Coder/Decoder                                                                                                                                                                                                                                                                                                                              |
| <b>Day Zero Attack</b>                      | See <i>Zero-Day Attack</i> .                                                                                                                                                                                                                                                                                                               |
| <b>DDoS</b>                                 | Distributed Denial-of-Service                                                                                                                                                                                                                                                                                                              |
| <b>Demilitarized Zone (DMZ)</b>             | 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.                                          |
| <b>Denial-of-Service (DoS)</b>              | 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.                                                                                                                                                          |
| <b>Digest Authentication (DA)</b>           | 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. |
| <b>Distributed Denial-of-Service (DDoS)</b> | 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.                                                                  |
| <b>DMZ</b>                                  | Demilitarized Zone                                                                                                                                                                                                                                                                                                                         |
| <b>DoS</b>                                  | Denial-of-Service                                                                                                                                                                                                                                                                                                                          |
| <b>DoW</b>                                  | Day-of-Week                                                                                                                                                                                                                                                                                                                                |
| <b>EMS</b>                                  | Element Management System                                                                                                                                                                                                                                                                                                                  |
| <b>FW</b>                                   | Firewall                                                                                                                                                                                                                                                                                                                                   |
| <b>GARP</b>                                 | Gratuitous Address Resolution Protocol                                                                                                                                                                                                                                                                                                     |
| <b>GUI</b>                                  | Graphical User Interface                                                                                                                                                                                                                                                                                                                   |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HA</b>                         | High-Availability <i>or</i> Harvest Attack                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>High-Availability</b>          | The SBCE feature that allows two SBCE security devices to be deployed as an integral pair, wherein one of the devices functions as the Primary and the other as an Alternate or Standby. Connected by a heartbeat signal and shared database, the two SBCE security devices provide failover protection in the event one of the devices malfunctions.                                                                                                                                                                                     |
| <b>HTTP</b>                       | Hypertext Transfer Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>ICMP</b>                       | Internet Control Message Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>ICMP</b>                       | Internet Control Message Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>IM</b>                         | Instant Messaging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Intrusion</b>                  | A malicious user or process deliberately masquerading as a legitimate user or process.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>IP</b>                         | Internet Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>IPS</b>                        | Intrusion Protection System                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>ITSP</b>                       | Internet Telephony Service Provider                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Latency</b>                    | 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.                                                                                                                                                                                                                                                                                                   |
| <b>MAC</b>                        | Message Authentication Code                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>MCD</b>                        | Machine Call Detection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>NAT</b>                        | Network Address Translation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>NTP</b>                        | Network Time Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>RTP</b>                        | Real-Time Transport Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>SBC</b>                        | Session Border Controller                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>SBCE</b>                       | Session Border Controller for Enterprise                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Secure Sockets Layer (SSL)</b> | <p>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).</p> <p>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</p> |

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

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

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

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SIP</b>        | Session Initiation Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>SNMP</b>       | Simple Network Management Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>SPAM</b>       | <p>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.</p> <p>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).</p> |
| <b>Spoof</b>      | 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).                                                                                                                                                                                                                               |
| <b>SRTP</b>       | Secure Real-Time Transport Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>SSL</b>        | Secure Socket Layer                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>STUN</b>       | Simple Traversal of UDP through NAT                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>TCP</b>        | Transmission Control Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>TCP/IP</b>     | Transmission Control Protocol / Internet Protocol                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>TFTP</b>       | Trivial File Transfer Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>TLS</b>        | Transport Layer Security                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>ToD</b>        | Time-of-Day                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Tromboning</b> | The situation where RTP media traffic originates at a certain point within a network and follows a path out of that network into another network (the access network, for example) and back again to a destination close to where it originated. See <i>Anti-Tromboning</i> .                                                                                                                                                                                      |

|                        |                                                                                                                                                                                                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tunneling</b>       | 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.                                                                                                                                                         |
| <b>TURN</b>            | Traversal Using Relay NAT                                                                                                                                                                                                                                                                                        |
| <b>UDP</b>             | User Datagram Protocol                                                                                                                                                                                                                                                                                           |
| <b>VM</b>              | Voice Mail                                                                                                                                                                                                                                                                                                       |
| <b>VoIP</b>            | Voice-over-Internet Protocol                                                                                                                                                                                                                                                                                     |
| <b>VPN</b>             | Virtual Private Network                                                                                                                                                                                                                                                                                          |
| <b>Zero-Day Attack</b> | 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. |
| <b>Zombie</b>          | An IP network element that has been surreptitiously taken over by an attacker, usually without the user's knowledge.                                                                                                                                                                                             |

# Index

## Numerics

|                      |                    |
|----------------------|--------------------|
| 9608 deskphone ..... | <a href="#">55</a> |
| 96x1 deskphone ..... | <a href="#">55</a> |

## A

|                                                                     |                                                              |
|---------------------------------------------------------------------|--------------------------------------------------------------|
| additional network security deployment .....                        | <a href="#">17</a>                                           |
| advanced services offer .....                                       | <a href="#">11</a>                                           |
| altitude requirements .....                                         | <a href="#">60</a>                                           |
| AMAX server .....                                                   | <a href="#">54</a> , <a href="#">60–62</a>                   |
| anomaly detection .....                                             | <a href="#">11</a> , <a href="#">13</a> , <a href="#">64</a> |
| Avaya SBCE                                                          |                                                              |
| architecture overview .....                                         | <a href="#">42</a>                                           |
| Avaya SBCE connected to multiple subnets, using a single VLAN ..... | <a href="#">48</a>                                           |
| Avaya SBCE connected to multiple subnets on two interfaces .....    | <a href="#">47</a>                                           |
| Avaya SBCE deployment models .....                                  | <a href="#">15</a>                                           |

## B

|                             |                    |
|-----------------------------|--------------------|
| BFCP                        |                    |
| architecture .....          | <a href="#">36</a> |
| description .....           | <a href="#">34</a> |
| overview .....              | <a href="#">33</a> |
| BFCP architecture .....     | <a href="#">36</a> |
| border access control ..... | <a href="#">16</a> |
| borderless UC .....         | <a href="#">12</a> |

## C

|                                 |                    |
|---------------------------------|--------------------|
| call handling                   |                    |
| WebRTC .....                    | <a href="#">41</a> |
| call pattern detection .....    | <a href="#">64</a> |
| call rates .....                | <a href="#">57</a> |
| capacities                      |                    |
| call rates .....                | <a href="#">57</a> |
| sessions .....                  | <a href="#">57</a> |
| users .....                     | <a href="#">57</a> |
| certifications of server .....  | <a href="#">62</a> |
| codec validation .....          | <a href="#">14</a> |
| command                         |                    |
| protect-socket .....            | <a href="#">70</a> |
| common firewall rules .....     | <a href="#">67</a> |
| common rules .....              | <a href="#">68</a> |
| Communication Manager .....     | <a href="#">55</a> |
| Communication Server 1000 ..... | <a href="#">55</a> |
| compatible products             |                    |
| Avaya .....                     | <a href="#">55</a> |
| mobile workspace user .....     | <a href="#">55</a> |
| SIP trunking .....              | <a href="#">55</a> |

|                           |                    |
|---------------------------|--------------------|
| concurrent sessions ..... | <a href="#">57</a> |
| control center .....      | <a href="#">64</a> |

## D

|                                     |                                                                 |
|-------------------------------------|-----------------------------------------------------------------|
| data interface firewall rules ..... | <a href="#">67</a>                                              |
| data interface restrictions .....   | <a href="#">66</a>                                              |
| Debian Linux .....                  | <a href="#">56</a>                                              |
| debian package install .....        | <a href="#">66</a>                                              |
| Dell R210 II .....                  | <a href="#">54</a> , <a href="#">57</a> , <a href="#">60–62</a> |
| denial of service .....             | <a href="#">66</a>                                              |
| deploy                              |                                                                 |
| multiple SBCE in HA mode .....      | <a href="#">40</a>                                              |
| multiple SBCE in non-HA mode .....  | <a href="#">39</a>                                              |
| deployment                          |                                                                 |
| multiple SBCE .....                 | <a href="#">39</a>                                              |
| detecting                           |                                                                 |
| portscan .....                      | <a href="#">68</a>                                              |
| detection .....                     | <a href="#">64</a>                                              |
| dimensions of server .....          | <a href="#">60</a>                                              |
| DNS rules .....                     | <a href="#">70</a>                                              |
| DNS server port .....               | <a href="#">72</a>                                              |
| document changes .....              | <a href="#">7</a>                                               |
| DoS activity reporting .....        | <a href="#">66</a>                                              |
| DoS attacks .....                   | <a href="#">11</a>                                              |
| dynamic trust scores .....          | <a href="#">64</a>                                              |

## E

|                                             |                                         |
|---------------------------------------------|-----------------------------------------|
| element management system .....             | <a href="#">11</a>                      |
| EMS .....                                   | <a href="#">11</a>                      |
| EMS takeover .....                          | <a href="#">59</a>                      |
| end-point fingerprints .....                | <a href="#">64</a>                      |
| environmental requirements for server ..... | <a href="#">61</a> , <a href="#">62</a> |

## F

|                                  |                    |
|----------------------------------|--------------------|
| failover .....                   | <a href="#">58</a> |
| far end camera control .....     | <a href="#">33</a> |
| firewall rules                   |                    |
| common .....                     | <a href="#">67</a> |
| data interface .....             | <a href="#">67</a> |
| management .....                 | <a href="#">67</a> |
| firewall rules, generating ..... | <a href="#">70</a> |
| Flare Experience for iPad .....  | <a href="#">55</a> |
| Flare Experience for PC .....    | <a href="#">55</a> |
| flood protection .....           | <a href="#">63</a> |
| floor .....                      | <a href="#">34</a> |
| floor chair .....                | <a href="#">34</a> |
| floor control .....              | <a href="#">34</a> |
| floor control server .....       | <a href="#">34</a> |
| floor participant .....          | <a href="#">34</a> |

|                                              |                                         |                                                               |                                                                                   |
|----------------------------------------------|-----------------------------------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Forward Error Correction                     |                                         | media                                                         |                                                                                   |
| FEC .....                                    | <a href="#">38</a>                      | unanchor .....                                                | <a href="#">19</a>                                                                |
| fuzzing protection .....                     | <a href="#">63</a>                      | media anchoring .....                                         | <a href="#">18</a>                                                                |
| <b>G</b>                                     |                                         | media anomaly prevention .....                                | <a href="#">63</a>                                                                |
| GARP support .....                           | <a href="#">58</a>                      | media element .....                                           | <a href="#">13</a> , <a href="#">14</a>                                           |
| <b>H</b>                                     |                                         | media ports .....                                             | <a href="#">72</a>                                                                |
| hardware platforms .....                     | <a href="#">11</a>                      | Medpro TN2302 circuit pack .....                              | <a href="#">58</a>                                                                |
| hardware warranty .....                      | <a href="#">10</a>                      | mobile workspace user .....                                   | <a href="#">19</a>                                                                |
| header manipulation .....                    | <a href="#">20</a>                      | monitoring .....                                              | <a href="#">64</a>                                                                |
| high availability .....                      | <a href="#">58</a>                      | monitoring, detection and protection .....                    | <a href="#">64</a>                                                                |
| Avaya SBCE .....                             | <a href="#">58</a>                      | MontaVista Linux .....                                        | <a href="#">56</a>                                                                |
| HTTP/HTTPS ports .....                       | <a href="#">72</a>                      | multiple gateways on the same network .....                   | <a href="#">49</a>                                                                |
| https rules .....                            | <a href="#">70</a>                      | multiple subnet .....                                         | <a href="#">44</a>                                                                |
| <b>I</b>                                     |                                         | multiple subnet overview .....                                | <a href="#">44</a>                                                                |
| ICMP                                         |                                         | multiple subnet scenario                                      |                                                                                   |
| restrictions .....                           | <a href="#">68</a>                      | Avaya SBCE connected to multiple subnets on two               |                                                                                   |
| identity engine .....                        | <a href="#">39</a>                      | interfaces .....                                              | <a href="#">47</a>                                                                |
| information management subsystem .....       | <a href="#">14</a>                      | multiple subnet scenarios                                     |                                                                                   |
| in-line deployment .....                     | <a href="#">15</a> , <a href="#">16</a> | multiple gateways on the same network .....                   | <a href="#">49</a>                                                                |
| intelligence element .....                   | <a href="#">13</a> , <a href="#">14</a> | multiple subnets on a single interface, using a single        |                                                                                   |
| IP Office .....                              | <a href="#">55</a>                      | VLAN .....                                                    | <a href="#">48</a>                                                                |
| IP Office SSL .....                          | <a href="#">19</a>                      | single data interface .....                                   | <a href="#">46</a>                                                                |
| IPTable firewall rules .....                 | <a href="#">65</a>                      | multiple subnets on a single interface .....                  | <a href="#">46</a>                                                                |
| <b>K</b>                                     |                                         | multiple tenants, call servers, and all Avaya SBCE interfaces |                                                                                   |
| KILLSCAN                                     |                                         | .....                                                         | <a href="#">50</a>                                                                |
| rules .....                                  | <a href="#">68</a>                      | <b>N</b>                                                      |                                                                                   |
| <b>L</b>                                     |                                         | NAT traversal .....                                           | <a href="#">14</a>                                                                |
| layer 3 and 4 security features .....        | <a href="#">65</a>                      | network security .....                                        | <a href="#">17</a>                                                                |
| license administration                       |                                         | <b>O</b>                                                      |                                                                                   |
| WebLM support .....                          | <a href="#">39</a>                      | offer and exchange rules for BFCP .....                       | <a href="#">34</a>                                                                |
| license download .....                       | <a href="#">74</a>                      | on-board storage .....                                        | <a href="#">54</a>                                                                |
| license feature                              |                                         | one-wire deployment .....                                     | <a href="#">15</a> , <a href="#">16</a>                                           |
| SBCE .....                                   | <a href="#">74</a>                      | one-X Communicator .....                                      | <a href="#">55</a>                                                                |
| licensing                                    |                                         | one-X Mobile SIP iOS .....                                    | <a href="#">55</a>                                                                |
| advanced services .....                      | <a href="#">74</a>                      | OpenVPN rules .....                                           | <a href="#">70</a>                                                                |
| standard services .....                      | <a href="#">74</a>                      | <b>P</b>                                                      |                                                                                   |
| Linux operating system .....                 | <a href="#">56</a>                      | parallel mode configuration .....                             | <a href="#">58</a>                                                                |
| logging .....                                | <a href="#">51</a>                      | platform capacities .....                                     | <a href="#">57</a>                                                                |
| <b>M</b>                                     |                                         | PLDS .....                                                    | <a href="#">74</a>                                                                |
| management firewall rules .....              | <a href="#">67</a>                      | port assignments                                              |                                                                                   |
| management interface port restrictions ..... | <a href="#">71</a>                      | DNS .....                                                     | <a href="#">72</a>                                                                |
| management interface restrictions .....      | <a href="#">66</a>                      | HTTP/HTTPS .....                                              | <a href="#">72</a>                                                                |
| master storage repository .....              | <a href="#">14</a>                      | media .....                                                   | <a href="#">72</a>                                                                |
| MDA .....                                    | <a href="#">25</a>                      | SIP signaling .....                                           | <a href="#">72</a>                                                                |
|                                              |                                         | SNMP .....                                                    | <a href="#">72</a>                                                                |
|                                              |                                         | Syslog .....                                                  | <a href="#">72</a>                                                                |
|                                              |                                         | port restrictions .....                                       | <a href="#">71</a>                                                                |
|                                              |                                         | port scan blocking .....                                      | <a href="#">65</a>                                                                |
|                                              |                                         | Portwell CAD-0208 .....                                       | <a href="#">54</a> , <a href="#">57</a> , <a href="#">60</a> – <a href="#">62</a> |
|                                              |                                         | power requirements of server .....                            | <a href="#">61</a>                                                                |

|                                                           |        |                                                  |            |
|-----------------------------------------------------------|--------|--------------------------------------------------|------------|
| Presence Services .....                                   | 55     | SIP decoding .....                               | 13         |
| processors .....                                          | 54     | SIP signaling ports .....                        | 72         |
| product compatibility .....                               | 54     | SIP trunking .....                               | 20         |
| <b>R</b>                                                  |        | SIP trunk integration module .....               | 12         |
| Radvision and Avaya SBCE interoperability with SRTP ..... | 43     | SIP validation .....                             | 13         |
| real time                                                 |        | site requirements                                |            |
| SIP Server Status .....                                   | 38     | safety .....                                     | 62         |
| reconnaissance prevention .....                           | 63     | SNMP ports .....                                 | 72         |
| REFER .....                                               | 23     | software warranty .....                          | 10         |
| registered users                                          |        | spoofing .....                                   | 11, 13, 63 |
| user registrations .....                                  | 38     | SRTP considerations .....                        | 44         |
| reinvite .....                                            | 26     | SRTP encryption of media .....                   | 16         |
| related documentation .....                               | 8      | SRTP support .....                               | 43         |
| remote user .....                                         | 19     | SSH port rules .....                             | 72         |
| remote worker .....                                       | 19     | SSH rules .....                                  | 69         |
| replication                                               |        | SSL VPN .....                                    | 19         |
| EMS .....                                                 | 59     | standard services                                |            |
| restrictions                                              |        | configuration .....                              | 12         |
| data interface .....                                      | 65     | offer .....                                      | 12         |
| reverse proxy .....                                       | 31     | stealth attack prevention .....                  | 63         |
| RHEL support .....                                        | 52     | support .....                                    | 9          |
| RTCP .....                                                | 26     | remote .....                                     | 19         |
| RTP anomaly detection .....                               | 14     | support under warranty .....                     | 10         |
| rules                                                     |        | Syslog port .....                                | 72         |
| data interface .....                                      | 70     | system configurations .....                      | 11         |
| firewall .....                                            | 70     | system memory .....                              | 54         |
| <b>S</b>                                                  |        | system requirements                              |            |
| safety requirements .....                                 | 62     | altitude .....                                   | 60         |
| SAL gateway .....                                         | 56     | humidity .....                                   | 61         |
| SBCE                                                      |        | power .....                                      | 61         |
| license feature .....                                     | 74     | temperature .....                                | 61         |
| SBC hardening .....                                       | 65     | <b>T</b>                                         |            |
| scenarios .....                                           | 36     | TCP flood restrictions .....                     | 69         |
| screened subnet deployment .....                          | 15, 16 | TCP packets restrictions .....                   | 72         |
| scrubber rules package .....                              | 67     | TCP signaling level                              |            |
| scrubber templates .....                                  | 67     | flood control .....                              | 65         |
| security life cycle .....                                 | 11     | TCP signaling level flooding control rules ..... | 65         |
| security settings .....                                   | 66     | thermal requirements .....                       | 62         |
| server                                                    |        | TN2302 circuit pack .....                        | 58         |
| certifications .....                                      | 62     | topology hiding .....                            | 67         |
| dimensions .....                                          | 60     | traceSBC                                         |            |
| environmental requirements .....                          | 61     | log files .....                                  | 52         |
| humidity requirements .....                               | 61     | overview .....                                   | 51         |
| power requirements .....                                  | 61     | traceSBC advantages .....                        | 52         |
| temperature requirements .....                            | 61     | training .....                                   | 9          |
| servers .....                                             | 54     | two-wire deployment .....                        | 15, 16     |
| Session Manager .....                                     | 55     | <b>U</b>                                         |            |
| SigMa module .....                                        | 12     | UCID .....                                       | 21         |
| signaling decryption .....                                | 13     | UC proxying .....                                | 12         |
| signaling element .....                                   | 13     | unified communication policies .....             | 65         |
| signaling manipulation .....                              | 20     | unified communications security .....            | 11         |
| single sign on .....                                      | 39     | user capacities .....                            | 57         |
| SIP call processing .....                                 | 20     |                                                  |            |

**V**

|                                              |                    |
|----------------------------------------------|--------------------|
| videos .....                                 | <a href="#">9</a>  |
| virtual private network TLS encryption ..... | <a href="#">16</a> |
| VLAN                                         |                    |
| use .....                                    | <a href="#">43</a> |

**W**

|                      |                    |
|----------------------|--------------------|
| warranty .....       | <a href="#">10</a> |
| WebLM .....          | <a href="#">74</a> |
| server details ..... | <a href="#">75</a> |
| WebRTC               |                    |
| call handling .....  | <a href="#">41</a> |