DUMPSBOSS.

Avaya Session Border Controller Enterprise Implementation and Maintenance

Avaya 3107

Version Demo

Total Demo Questions: 8

Total Premium Questions: 85

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Avaya Aura® Session Border Controller Enterprise Overview	21
Topic 2, Installation	14
Topic 3, Configuration	31
Topic 4, Maintenance and Troubleshooting	19
Total	85

QUESTION NO: 1

Which troubleshooting tool should be used when an administrator needs to collect packet-level SIP and RTP traffic for detailed analysis?

A. Trace > Packet Capture

B. System Incidents

C. Domain Policy Administration

D. Server Profile

ANSWER: A

Explanation:

Packet Capture is used to collect packet-level traffic for detailed examination. A capture can be opened in a protocol-analysis tool to inspect SIP messages, SDP, RTP packets, source and destination addressing, and packet timing. A Call Trace is useful for targeted SIP signaling associated with a URI, but it does not replace a packet capture when detailed network-level analysis is required. Consult the applicable SBCE maintenance documentation in the Avaya Documentation portal.

QUESTION NO: 2

Which type of information describes a SBC call trace?

A. Payload information: voice, video, or data

B. Signaling level information for a given URI

C. Application information (for example Wireshark, traceSM)

D. Network topology information

ANSWER: B

Explanation:

Signaling level information for a given URI is correct because an Avaya Session Border Controller Enterprise call trace is intended to follow and display the SIP signaling associated with a specific call or endpoint identity. The trace lets an administrator inspect the signaling exchange that establishes, modifies, and clears a session, typically using identifiers such as SIP URIs, Call-ID values, addresses, or other call-selection criteria. This makes call tracing a troubleshooting function for determining how a call was routed and how the SIP dialog progressed through the SBC.

SIP itself is a signaling protocol: it carries requests, responses, routing information, and session-description details used to negotiate a communication session. The media stream is normally carried separately after negotiation, while the call trace focuses on the signaling records needed to diagnose call processing and interoperability behavior. In practice, reviewing the trace can reveal the sequence of SIP messages and the relevant headers for the selected call, allowing an engineer to correlate the SBC's handling of that URI with the call outcome. Avaya publishes SBC Enterprise documentation through its official documentation portal, and the SIP signaling model is defined in RFC 3261. See also the Avaya Documentation portal for the applicable SBC Enterprise implementation and maintenance guide.

QUESTION NO: 3

Which SIP message body normally contains the negotiated codec, media IP address, and UDP port for a voice call?

A. Session Description Protocol (SDP)

B. Via header

C. Contact header

D. Route header

ANSWER: A

Explanation:

Session Description Protocol (SDP) contains the media-session description exchanged during SIP call establishment. SDP identifies media characteristics such as the RTP address, media port, codec payload types, and direction attributes. SBCE uses this information when applying media handling and interworking policies. SIP headers provide signaling and routing information, but the negotiated media description is carried in SDP. The SIP framework is defined in RFC 3261, and SDP is defined in RFC 4566.

QUESTION NO: 4

Where do you implement the restriction that equipment can make calls only during a defined period of the day?

A. Routing Profile

B. Domain Polity Administration

C. Topology Hiding Profile

D. Signaling Interface

ANSWER: B

Explanation:

Domain Polity Administration is the appropriate SBCE administration area for applying time-based calling restrictions to equipment associated with a domain. A domain policy defines how the Session Border Controller Enterprise handles calls for a particular signaling domain, including enforcement of policy controls that govern when calls are permitted. By configuring the applicable time-of-day restriction in the domain policy and associating that policy with the relevant domain, an administrator can allow call activity only during the specified daily interval. This supports operational requirements such as limiting calls from a site, device group, or tenant to business hours, while ensuring the restriction is applied consistently as part of call-policy processing.

Domain policies are central to controlling the treatment and permissions of sessions entering or leaving defined domains on Avaya SBCE. Time-based restrictions should therefore be configured as a domain-level policy control rather than as a network-topology or interface setting. Avaya SBCE product and documentation resources are available through the Avaya Session Border Controller Enterprise product page and the Avaya Support documentation portal.

QUESTION NO: 5

What is the Received Interfaced that is defined in Call Server Flow administration?

A. It is an external interface that rebroadcasts outbound traffic

B. It is an external interface that receives inbound traffic.

C. It is an internal interface that rebroadcasts outbound traffic.

D. It is an internal interface that receives inbound traffic.

ANSWER: D

Explanation:

It is an internal interface that receives inbound traffic.

is correct because the Received Interface in an Avaya Session Border Controller Enterprise Call Server Flow identifies the ingress interface on which the SBCE receives signaling from the enterprise call-server side. Call-server-side signaling is handled on an internal interface, which represents the trusted enterprise network and is used for connections to call-processing components such as Avaya Aura Session Manager or Communication Manager. The Received Interface is therefore an input criterion for the flow: it associates inbound SIP traffic arriving from that internal network with the applicable call-server flow and its subsequent routing and treatment. This selection is important where the SBC has multiple internal network connections or call-server paths, since it allows the administrator to apply the appropriate flow according to the interface that accepted the request. Avaya's SBCE administration and deployment documentation describes the use of internal and external interfaces to separate enterprise-side and service-provider-side signaling, with call-server connectivity configured on the internal side. Consult the Avaya Documentation Portal for the SBCE administration guide applicable to the installed release and the Avaya Support site for release-specific implementation documentation.

QUESTION NO: 6

What is the function of the SBC routing profile?

A. It defines the SIP domain.

B. It defines the destination URI.

C. It defines the next hop for SIP traffic.

D. It defines the complete destination route.

ANSWER: C

Explanation:

"It defines the next hop for SIP traffic." is correct. In Avaya Session Border Controller Enterprise, a routing profile supplies the routing information the SBC uses after call-processing policy determines that a session should be sent toward a particular destination. The profile identifies the SIP next hop, typically through route entries that specify the target server address or fully qualified domain name, port, transport, and related route preference information. This lets the SBC forward SIP signaling to the appropriate downstream system, such as an enterprise call server, service provider, or other SIP peer.

Routing profiles are associated with call-routing policy elements so that matching calls are directed to the intended signaling destination. Their purpose is therefore to define where SIP traffic is forwarded next, rather than merely naming a SIP domain or describing all of the call-routing logic. Avaya's documentation resources for Session Border Controller Enterprise configuration and implementation are available through Avaya Documentation and Avaya Support.

QUESTION NO: 7

In general, SBC incidents indicate what kind of problem?

A. Hardware

B. Operating system

C. Application (SBC) software

D. Visualization layer

ANSWER: C

Explanation:

Application (SBC) software is correct because an incident in Avaya Session Border Controller Enterprise is generally an application-level indication that the SBC software has detected an operational condition needing attention. The incident mechanism is part of the SBC's management and diagnostic framework: it records conditions detected by SBC processes

and services, supplies relevant event details, and helps an administrator identify an issue affecting SBC operation or call processing. Administrators use the incident information together with logs, alarms, traces, and system-status data to assess the condition and determine the appropriate corrective action. This classification is important in maintenance workflows because it directs initial troubleshooting toward the Session Border Controller Enterprise application and its configured services, rather than treating the incident itself as a direct statement about a particular physical component or platform layer. Avaya's product-support resources provide the documentation and maintenance material used to investigate these application-generated conditions, including incident details and diagnostic collection procedures. See the Avaya Session Border Controller Enterprise support page and Avaya Documentation.

QUESTION NO: 8

For Enterprise SBC customers integrated with Communication Manager or Communication Server 1000, which remote access connection model do they use?

A. SSL VPN

B. Secure Access Link (SAL)

C. Modem

D. No remote access / alarming

ANSWER: B

Explanation:

Secure Access Link (SAL) is the remote access connection model used for Avaya Enterprise Session Border Controller deployments integrated with Communication Manager or Communication Server 1000. SAL provides Avaya's managed and secure serviceability framework, allowing authorized support personnel to establish controlled remote maintenance access to customer equipment. The model uses an on-site SAL Gateway or equivalent SAL connectivity architecture to initiate and manage secure connections, rather than exposing the SBC or communication servers directly to the public network. It also supports operational functions such as alarm forwarding, remote diagnostics, maintenance workflows, access authorization, and auditing. For an Enterprise SBC implementation, configuring the applicable SAL connectivity is therefore part of ensuring that Avaya support and service operations can reach the integrated solution in accordance with the customer's security policy and Avaya support procedures. This approach is specifically intended for Avaya solution environments containing products such as Communication Manager, Communication Server 1000, and associated session-management infrastructure. Avaya maintains product documentation and support resources, including SAL-related materials, through its Avaya Support portal.