

Enterprise Session Border Controller (E-SBC)



APPLICATIONS

- Session Initiation Protocol (SIP) trunking
- Internet Protocol (IP)-enabled contact centers
- Videoconferencing
- Hosted IP communications services
- Remote workers and offices

KEY FEATURES

- Advanced denial of service (DoS) and overload protection
- Fraud prevention
- SIP protocol normalization
- H.323 to SIP protocol interworking
- Optional 1:1 high availability
- On-board Oracle Enterprise Operations Monitor probe
- Scalable from 25 to 80,000 sessions in a single chassis
- Proven multivendor UC and service provider interoperability

KEY BENEFITS

- Accelerate service deployment
- Protect IT infrastructure, services, and applications
- Guard against malicious attacks

The Oracle Enterprise Session Border Controller protects IP communications networks from cyberthreats and fraud, mitigates the effects of network impairments and outages, and cures interoperability problems so that users can enjoy highly secure and reliable voice, video and unified communications services.

Overview

Enterprise voice, video and unified communications services are vulnerable to cyberattacks, outages and interoperability problems that can occur when communications sessions traverse IP network borders. Attacks and outages can disrupt business operations, endanger revenues and tarnish the brand image. Interoperability problems can reduce business agility, delay projects and put IT investments at risk.

The Oracle Enterprise Session Border Controller (E-SBC) is specifically designed to address the unique security, reliability and interoperability problems that can occur when real-time communications sessions cross network borders. It defends against myriad cyberattacks and ensures communications privacy, dynamically routes communications around network faults, and manipulates sessions to resolve interoperability problems.

The E-SBC is a field-proven solution for connecting a wide range of multivendor VoIP, UC and contact center systems to public network services, including telecommunications carrier SIP trunk services, the Internet and cloud communications applications.

Strong Security

IP communications are susceptible to denial of service, fraud and privacy breaches that can result in lost revenue and productivity, poor customer experiences, compliance violations and damage to the corporate brand. The E-SBC protects IP communications systems and services from these threats and delivers secure, private voice, video and UC sessions across trusted and untrusted networks alike.

It features the Net-SAFE architecture, a comprehensive security architecture that protects communications confidentiality and integrity and ensures the availability of services, systems and applications. The E-SBC uses dedicated resources and deep packet inspection technology to identify and block denial of service attacks at line rate while enabling valid communications to continue to flow during an attack.

The E-SBC features white/black listing, rate limiting and granular per-user policies to mitigate fraud risks. It can block calls to known fraudulent destinations, limit calls to unusual or suspicious destination ranges and apply policies to users based on time of day and other parameters.

To protect communications privacy, the E-SBC authenticates and encrypts communications sessions using the same strong algorithms used by the US government for classified information (FIPS 140-2). It features topology hiding to prevent reconnaissance and enumeration by hackers and DTMF suppression to enable PCI compliance in contact centers.

Easy Interoperability

IT managers frequently encounter interoperability problems when connecting on-premise systems to each other and to cloud communications services. These problems can reduce network agility and reliability, delay projects, increase costs and put investments at risk of obsolescence.

The E-SBC features header manipulation capabilities that can resolve a wide range of protocol interoperability problems. An extensive library of application notes dramatically simplifies and accelerates the configuration and deployment of any UC network and SIP trunking service.

An IETF compliant SIPREC trunk recording interface provides a lower cost and more efficient alternative to conventional line-side interfaces for connecting a call recording server to the network. The E-SBC's open standard SIPREC interface is field-proven for interoperability with a wide range of third party call recording servers.

The E-SBC is available in a virtualized software edition that enables easy migration to a range of cloud deployment models. It protects investments by supporting a range of hypervisors used in popular cloud services.

Assured Reliability

Impairments and failures can occur anywhere in a communications network – including the SBC – and they can be difficult to isolate and repair. The Oracle E-SBC includes a complete set of carrier-grade routing and survivability features that ensure business continuity in the face of network failures and impairments.

It features carrier-grade 1:1 high availability that continuously monitors E-SBC health and routes sessions from active to standby units with no loss in session state or impact to user experience. The E-SBC dynamically routes sessions to protect against failures anywhere in the network. It can optimize performance across multiple SIP trunk services by routing based on observed QoS and balancing loads.

To help IT managers monitor and troubleshoot their networks, the Oracle E-SBC features a graphical monitoring and tracing tool that enables them to quickly visualize complex session information. For large networks, an embedded probe enables the E-SBC to integrate with the sophisticated troubleshooting capabilities provided by Oracle Enterprise Operations Monitor.

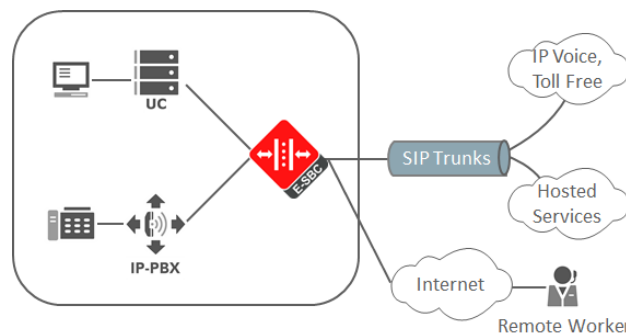
RELATED PRODUCTS

- Oracle Enterprise Communications Broker
- Oracle Enterprise Operations Monitor
- Oracle Communications Interactive Session Recorder
- Oracle Communications WebRTC Session Controller

Applications

Businesses install the Oracle E-SBC at Session Initiation Protocol (SIP) network borders where enterprise communications systems connect to public network services or where disparate multivendor systems must be interconnected. They use the product to:

- Connect to SIP trunking services and the internet
- Access cloud communications services
- Communicate securely with remote workers
- Connect contact center locations and business process outsourcing (BPO) services



Oracle Enterprise Session Border Controller (E-SBC) connects disparate IP communications networks

ORACLE E-SBC SESSION CAPACITY

Model	Session Capacity	Additional Capacities
Acme Packet Virtual Machine Edition	25 – 12,000	<ul style="list-style-type: none"> • 12,000 signaled sessions (media anchored) • 6,000 SRTP sessions • 4000 SIPREC sessions • 2500 transcoded sessions (G.711<->G.729)
Acme Packet 1100	25 - 360	<ul style="list-style-type: none"> • 360 signaled sessions (media anchored) • 180 SRTP call legs • 360 transcoded sessions (G.711<->G.729) • 180 SIPREC sessions • TDM: 1xT1/E1 or 4xT1/E1
Acme Packet 3900	25 – 8,000	<ul style="list-style-type: none"> • 8,000 signaled sessions (media anchored) • 4,000 SRTP call legs • 6,250 transcoded sessions (G.711<->G.729) • 4,000 SIPREC sessions • TDM: 4xT1/E1 • 1,000,000 local route tables
Acme Packet 4600	25 – 32,000	<ul style="list-style-type: none"> • 32,000 signaled sessions (media anchored) • 16,000 SRTP call legs • 15,000 transcoded sessions (G.711<->G.729) • 8,000 SIPREC sessions • 2,000,000 local route tables

Acme Packet 6300	4,000 – 80,000	<ul style="list-style-type: none"> • 80,000 signaled sessions (media anchored) • 32,000 SRTP call legs • 60,000 transcoded sessions (G.711<->G.729) • 16,000 SIPREC sessions • 8,000,000 local route table entries
------------------	----------------	---

Feature	Capabilities
Security	<ul style="list-style-type: none"> • Granular access control • IP address and SIP signaling concealment • Layer three through five topology hiding and signaling overload controls • IP telephony spam protection • Stateful deep packet inspection • Signaling and media encryption • Telephony fraud protection • NIST Suite B cryptography (also available for WebGUI connection)
Interoperability	<ul style="list-style-type: none"> • SIP message normalization • Response code translation • Session Description Protocol (SDP) and Dual Tone Multi-Frequency (DTMF) manipulation • Number and uniform resource identifier (URI) manipulation • Header manipulation rules (HMR) • SIP-H.323 signaling interworking • Protocol interworking: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Stream Control Transmission Protocol (SCTP) • Encryption interworking: Transport Layer Security (TLS), Mutual TLS, Secure Real-time Transport Protocol (SRTP), IP Security (IPsec) • Network address translation (NAT) and firewall traversal • IP address translation: private/public, IPv4/IPv6 • Transcoding • Internet Engineering Task Force (IETF) standard SIP Recording (SIPREC) interface, • Support for Microsoft ELIN Gateway and Avaya Personal Profile Manager proxy • Session routing based on LDAP (Microsoft Active Directory) query • Calling Line Identification Presentation (CLIP/COLP)
Reliability	<ul style="list-style-type: none"> • Standby SIP registrar with caching for remote site survivability • Stateful signaling and media failover • Quality of service (QoS) marking, virtual local area network (VLAN) mapping • Registration storm avoidance • Call rate limit enforcement • Trunk load balancing • Stateful session routing • QoS-based routing • Microsoft Active Directory based routing enhancements • H.323 destination address based routing
Regulatory Compliance	<ul style="list-style-type: none"> • Session prioritization for emergency services • Call detail records (CDRs) with local or remote storage via RADIUS
Cost Management	<ul style="list-style-type: none"> • Least cost routing • CODEC renegotiation
Management	<ul style="list-style-type: none"> • Embedded Oracle Enterprise Operations Monitor probe • Browser-based GUI • SIP monitoring and tracing tool • SNMP agent, XML configuration files, Syslog, SFTP, RADIUS interfaces • Subnet masks for SNMP • Secure WebGUI access with HTTPS
Analog module	<ul style="list-style-type: none"> • Four FXS and four FXO ports • Support for fax interworking with T.38 transcoding

Euro ISDN BRI
module

- Four BRI ports

RACLE SOFTWARE (VM)-BASED E-SBC SPECIFICATIONS¹

Features	Virtual Machine Edition (VME)
Session Capacity	Up to 12000 sessions
Transcoded CODECs	G.711 μ -Law, G.711A-Law, G.729A, G.729B
Encryption	Software-based SIP/TLS and SRTP support
Management	SNMP agent, XML configuration files, Syslog, SFTP, RADIUS interfaces.
Preferred VM Environment	VMware ESXi, KVM, Oracle Virtual Machine (OVM), Microsoft Hyper-V
Minimum Capacity Configuration	4 CPU cores, 16 GB of RAM and 40G storage

¹ Not supported on software-based E-SBC: System access control lists, physical layer link redundancy, SIP port mapping, source-based routing, jumbo packets, online certificate status protocol, IPsec, fax transcoding, IPv6, secure control transmission protocol, bandwidth policing, mid-reserve bandwidth for session agents

ORACLE APPLIANCE-BASED E-SBC SPECIFICATIONS


Feature	Acme Packet 1100	Acme Packet 3900	Acme Packet 4600	Acme Packet 6300
Chassis	1U, shelf/table or rack mount	1U, rack mount	1U, rack mount	3U, rack mount
Oracle EOM Integration	Monitoring probe is queried by EOM	10 second interval Quality of Service updates sent to EOM	10 second interval Quality of Service updates sent to EOM	10 second interval Quality of Service updates sent to EOM
Registration Capacity	5,000 (UDP/TCP) 5,000 (TLS)	80,000 (UDP/TCP) 30,000 (TLS)	500,000 (UDP/TCP) 250,000 (TLS)	500,000 (UDP/TCP) 300,000 (TLS)
Storage & Memory	32 GB fast mSATA drive for runtime image, backup configurations and local call detail record backup	Standard 120GB SSD for call detail record storage, log files, other permanent file storage 4GB of memory used for boot up only	Standard 80GB SSD, optional 400GB SSD for call detail record storage, log files, other permanent file storage 16 GB for Acme Packet OS and configuration	40GB or 600GB disk drive for call detail record storage, log files, other permanent file storage 16 GB for Acme Packet OS and configuration
Supported CODECs	G.711 μ -Law, G.711A-Law, G.722, G.722.2, G.723.1, G.726, G.729A, G.729B, AMR, GSM-FR, iLBC, T.38, EVRC, EVRC-B, OPUS, SILK			
Transcoding	Transcoding supported on all platforms between any of the following: G.711 μ -Law, G.711A-Law, G.722, G.722.2, G.723.1, G.726, G.729A, G.729B, AMR, GSM-FR, iLBC, EVRC, EVRC-B. OPUS/SILK transcoding not supported on AP3820 or AP4500. T.38 transcoding to/from G.711 μ -Law, G.711A-Law			
Encryption	TLS session setup, and SRTP media encryption and decryption in software	IPSec tunnel and TLS session setup, IPsec and SRTP traffic encryption and decryption in hardware		
Management	SNMP, Syslog, SFTP, RADIUS interfaces	SNMP agent, XML configuration files, Syslog, SFTP, RADIUS interfaces.		



CONTACT US

For more information about [insert product name], visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

 blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0218



Oracle is committed to developing practices and products that help protect the environment