

Oracle Enterprise Session Border Controller

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

OVERVIEW

Enterprise voice, video and unified communications services are vulnerable to cyber-attacks, 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 Communications 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 cyber-attacks 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, UCC and contact center systems to public network services, including SIP trunking services, the Internet and cloud applications.

NEW FEATURES IN RELEASE 8.3

Public Cloud Support	<ul style="list-style-type: none"> • Oracle Cloud Infrastructure • Amazon EC2, including native HA support • Microsoft Azure
Advanced Media Termination for Microsoft Teams and WebRTC	<ul style="list-style-type: none"> • ICE-lite support • RTP/RTCP muxing • Comfort Noise Generation
New platforms	<ul style="list-style-type: none"> • Quad 10GbE NIU for Acme Packet 6350
REST API	<ul style="list-style-type: none"> • For monitoring and performance KPIs
Peering/Interconnect	<ul style="list-style-type: none"> • SIP/SIP-I interworking • RingBack tone emulation (DSP-based)
Virtualization (vSBC) Upgrades	<ul style="list-style-type: none"> • RTCP generation on vSBC • SW-based SILK transcoding
Serviceability	<ul style="list-style-type: none"> • Alarm for TLS certification expiration • SW-based SILK transcoding
Miscellaneous	<ul style="list-style-type: none"> • KPML and 2833 dual interworking • MSRP support for E-SBC (Cavium platforms)

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 160,000 RTP sessions
- Scalable to 40,000 SIPREC sessions
- Proven multivendor UC and Service Provider interoperability
- Genesys PureEngage contact center certified
- Microsoft TEAMS certified for Direct Routing, in both non-Media Bypass and Media Bypass modes
- Public Cloud support:
 - Microsoft's Azure
 - Amazon's AWS
 - Oracle's OCI
- VNF HEAT Templates
- REST APIs

STRONG SECURITY

IP communications are susceptible to cyber-security threats, including Distributed Denial of Service (DDoS) attacks, fraud and privacy breaches that result in lost revenue and productivity, poor customer experiences, compliance violations and damages to the corporate brand. The Oracle Communications Enterprise Session Border Controller protects IP-based systems and services from these threats and delivers secure, private voice, video and UC sessions across trusted and untrusted networks alike.

The E-SBC incorporates Oracle's S.A.F.E. Architecture, a comprehensive vision focusing on world-class Security, being Application aware, Flexible delivery and Extensible platforms. The E-SBC's own architecture protects communications confidentiality and integrity and ensures the availability of services, systems and applications. It 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. The E-SBC provides topology hiding to prevent reconnaissance and enumeration by hackers and DTMF suppression to enable PCI compliance in contact centers.

For enhanced communications privacy, the E-SBC is both Federal Information Processing Standard (FIPS) 140-2 and Joint Interoperability Testing Command (JITC) compliant. FIPS is a standard for cryptographic modules protecting sensitive information in computer systems for U.S. government and military use, and for highly-regulated industries such as finance, healthcare and utilities. JITC certification enables an asset to be listed on the Department of Defense Approved Product List (APL).

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 3rd-party SIPREC compliant Session Recording Servers (SRS), has a rich SIPREC load balancing functionality, and supports up to 10 simultaneous SRS destinations (e.g. Biometrics, Compliance, Speech Analytics, GeoRed).

The E-SBC is available in two virtualized machine environment (VME) editions, including a Small Footprint VME, which enable more efficient usage of computing resources and eases any future migration of this service to a range of cloud deployment models. To this end and for investment protection, it supports both the Type 1 and Type 2 hypervisors which are used by popular cloud services, including: KVM, ESXi, OVM and Hype-V.

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 to ensure business continuity during network failures or impairments.

It features carrier-grade 1:1 high availability that continuously monitors the E-SBC's health and routes sessions

Key Business Benefits

- Protects IT-based services, applications and infrastructure
- Guards against cyber-attacks
- Accelerates service deployment

New Features in E-SBC 8.3

- Public Cloud Support
 - Oracle Cloud (OCI)
 - Amazon EC2 (AWS), including native HA
 - Microsoft Azure
- Advance Media Termination for Microsoft TEAMS and WebRTC
 - ICS-lite support
 - RTP/RTCP muxing
 - Comfort noise generation
- Quad 10GbE NIU support for AP 6350, providing increased SIPREC capacity
- Performance and monitoring REST APIs
- Peering/Interconnect:
 - SIP/SIP-I interconnect
 - RingBack tone emulation
- Virtualization Upgrades:
 - SW-based SILK transcoding
 - RTCP generation for vSBC
- Alarm for TLS certification expiration

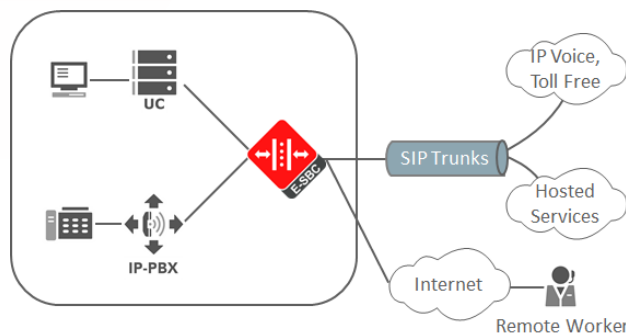
from active to standby units with no loss in session state or impact to user experience. The E-SBC dynamically routes sessions to protect against failures anywhere in the network. It can optimize performance across multiple SIP trunk services by routing sessions based on observed QoS and balancing loads.

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.

APPLICATIONS

Businesses install the Oracle Communications Enterprise Session Border Controller at 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 Communications Enterprise Session Border Controller connects disparate IP communications networks securely

Related Products

The following products support Oracle Enterprise Session Border Controller:

- Oracle Enterprise Operations Monitor
- Oracle Enterprise Telephony Fraud Monitor
- Oracle Enterprise Communications Broker
- Oracle Communications Interactive Session Recorder
- Oracle Communications Session Delivery Manager

CRITICAL ENTERPRISE SBC FEATURES & CAPABILITES

FEATURE	CAPABILITES
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) • FIPS Compliant and being validated, including MSRP FIPS for VME, 1100 & 3900 platforms. (All prior images, including ECz8.2.0 are FIPS Certified.) • JITC Compliant and being validated. (Image ECz8.2.0 is JITC Certified.)

INTEROPERABILITY	<ul style="list-style-type: none"> • SIP message normalization • Response code translation • 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 • 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 (Acme Packet 1100)	<ul style="list-style-type: none"> • Four FXS and four FXO ports • Support for fax interworking with T.38 transcoding
EURO ISDN BRI (Acme Packet 1100)	<ul style="list-style-type: none"> • Four BRI ports

ORACLE ENTERPRISE SBC SESSION CAPACITY¹

	VME (S.F.) ^A	VME	AP1100	AP3900	AP4600	AP6300	AP6350	AP6350 w/ NIU ^B
Session Capacity	25-2,200	25-16,000	25-360	25-8,000	25-32,000	25-80,000	25-80,000	25-160,000
RTP Sessions	2,200	16,000	360	8,000	32,000	80,000	80,000	160,000
SRTP Sessions		4,000	450	4,000	16,000	40,000	40,000	45,000
SIPREC Sessions	800	6,850	180	6,000	16,000	20,000	20,000	40,000
Transcoded Sessions^C			360	6,250	15,000	60,000	60,000	60,000

NOTES:

A. (S.F.) is the "Small Footprint VME"

B. 6350 NIU uses the Quad Port NIU

C. Transcoded sessions benchmarked for G.711 <-> G.729

ORACLE SOFTWARE VIRTUAL MACHINE-BASED E-SBC SPECIFICATIONS²

FEATURES	VIRTUAL MACHINE EDITION (VME)
Session Capacity	Up to 16,000 sessions (See Footnote #2)
Transcoded CODECS	G.711μ-Law, G.711A-Law, G.729, G.729A, G.729B, AMR, AMR-WB, iLBC, OPUS, SILK
Encryption	Software-based SIP/TLS and SRTP support
Management	SNMP agent, XML configuration files, Syslog, SFTP, RADIUS interfaces
Preferred VM Environments	VMware ESXi, KVM, Oracle Virtual Machine (OVM), Microsoft Hyper-V
Minimum Capacity Configuration	2 CPU cores, 4 GB of RAM and 20G storage

¹ Performance and capacity vary by codec, signaling protocol, call flow, configuration, and feature usage.

² Not supported on virtual E-SBC: Online certificate status protocol, IPsec(some aspects), fax transcoding, SCTP on Melanox platform, ICMP over IPv6.

ORACLE APPLIANCE-BASED E-SBC SPECIFICATIONS



FEATURE	ACME PACKET 1100	ACME PACKET 3900	ACME PACKET 4600	ACME PACKET 6350
Chassis	1U, shelf/table or rack mount	1U, rack mount	1U, rack mount	3U, rack mount
Oracle EOM Integration	Embedded probe supports both end-of-call QoS reporting, and 10 second interval interim QoS reporting, to the 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	32GB fast mSATA drive for runtime image, backup configurations and local call detail record (CDR) backup	Standard 120GB SSD for CDR storage, log files, other permanent file storage; 4GB of memory used for boot up only	Standard 480GB SSD for CDR storage, log files, other permanent file storage; 16GB for Acme Packet OS and configuration	Standard 480GB SSD for CDR storage, log files, other permanent file storage; 16GB for Acme Packet OS and configuration
Supported CODECs	AMR, AMR-WB(G.722.2), CN, EVS, ERVC, EVRC-0, EVRC-B, G.711μ-Law, G.711A-Law, G.722, G.723, G.723.1, G.726, G.726-16,-24,-32,-40, G.729, G.729A, G.729AB, GSM-FR, iLBC, OPUS, SILK, T.38, T.38OFD, TTY			
Transcoding	Transcoding supported on all platforms between any of the following: AMR, AMR-WB(G722.2), CN, EVS, ERVC, EVRC-0, EVRC-B, G.711μ-Law, G.711A-Law, G.722, G.723, G.723.1, G.726, G.726-16,-24,-32,-40, G.729, G.729A, G.729AB, GSM-FR, iLBC, OPUS, T.38 transcoding to/from G.711μ-Law & G.711A-Law, T.38OFD, TTY(except on AP1100)			
Encryption	TLS session setup, and SRTP media encryption & 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		

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.

Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com/oracle

 facebook.com/oracle

 twitter.com/oracle

Integrated Cloud Applications & Platform Services

Copyright © 2020, 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. 0120