Enterprise Session Border Controller (E-SBC)

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 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 SIP network borders where communications systems connect to public network services or where disparate multivendor systems must be interconnected. They use the product to:

- Connect to SIP trunking telecommunications 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 (E-CZ7.4.0 RELEASE)

<table>
<thead>
<tr>
<th>Model</th>
<th>Session Capacity</th>
<th>Additional Capacities</th>
</tr>
</thead>
</table>
| Acme Packet Virtual Machine Edition | 25 – 1,000       | - 1,000 signaled sessions (media anchored)  
- 1,000 SRTP sessions decrypted to RTP  
- 500 SRTP sessions decrypted / re-encrypted  
- 250 SIPREC sessions  
- 100 transcoded sessions (G.711<->G.729)  
- VM configuration with 4 CPU cores, 4GB Memory |
| Acme Packet 1100             | 25 - 360         | - 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       | - 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      | - 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   | - 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 |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>• Granular access control &lt;br&gt;• Layer three through five topology hiding &lt;br&gt;• Signaling overload controls &lt;br&gt;• IP telephony spam protection &lt;br&gt;• Stateful deep packet inspection &lt;br&gt;• Signaling and media encryption &lt;br&gt;• Telephony fraud protection &lt;br&gt;• NIST Suite B cryptography (also available for WebGUI connection)</td>
</tr>
<tr>
<td><strong>Interoperability</strong></td>
<td>• SIP message normalization &lt;br&gt;• Response code translation &lt;br&gt;• Session Description Protocol (SDP) and Dual Tone Multi-Frequency (DTMF) manipulation &lt;br&gt;• Number and uniform resource identifier (URI) manipulation &lt;br&gt;• Header manipulation rules (HMR) &lt;br&gt;• SIP-H.323 signaling interworking &lt;br&gt;• Protocol interworking: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Stream Control Transmission Protocol (SCTP) &lt;br&gt;• Encryption interworking: Transport Layer Security (TLS), Mutual TLS, Secure Real-time Transport Protocol (SRTP), IP Security (IPsec) &lt;br&gt;• Network address translation (NAT) and firewall traversal &lt;br&gt;• IP address translation: private/public, IPv4/IPv6 &lt;br&gt;• Transcoding &lt;br&gt;• Internet Engineering Task Force (IETF) standard SIP Recording (SIPREC) interface &lt;br&gt;• Support for Microsoft ELIN Gateway and Avaya Personal Profile Manager proxy &lt;br&gt;• Session routing based on LDAP (Microsoft Active Directory) query &lt;br&gt;• Calling Line Identification Presentation (CLIP/COLP)</td>
</tr>
<tr>
<td><strong>Reliability</strong></td>
<td>• Standby SIP registrar with caching for remote site survivability &lt;br&gt;• Stateful signaling and media failover &lt;br&gt;• Quality of service (QoS) marking, virtual local area network (VLAN) mapping &lt;br&gt;• Registration storm avoidance &lt;br&gt;• Call rate limit enforcement &lt;br&gt;• Trunk load balancing &lt;br&gt;• Stateful session routing &lt;br&gt;• QoS-based routing &lt;br&gt;• Microsoft Active Directory based routing enhancements &lt;br&gt;• H.323 destination address based routing</td>
</tr>
<tr>
<td><strong>Regulatory Compliance</strong></td>
<td>• Session prioritization for emergency services &lt;br&gt;• Call detail records (CDRs) with local or remote storage via RADIUS</td>
</tr>
<tr>
<td><strong>Cost Management</strong></td>
<td>• Least cost routing &lt;br&gt;• CODEC renegotiation</td>
</tr>
<tr>
<td><strong>Element Management</strong></td>
<td>• Embedded Oracle Enterprise Operations Monitor probe &lt;br&gt;• Browser-based GUI &lt;br&gt;• SIP monitoring and tracing tool &lt;br&gt;• SNMP agent, XML configuration files, Syslog, SFTP, RADIUS interfaces &lt;br&gt;• Subnet masks for SNMP &lt;br&gt;• Secure WebGUI access with HTTPS</td>
</tr>
</tbody>
</table>
### ORACLE SOFTWARE (VM)-BASED E-SBC SPECIFICATIONS

#### Features

<table>
<thead>
<tr>
<th>Virtual Machine Edition</th>
<th>Session Capacity</th>
<th>Supported CODECs</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Up to 1000 sessions</td>
<td>G.711µ-Law, G.711A-Law, G.729A, G.729B</td>
<td>Software-based SIP/TLS and SRTP support</td>
</tr>
</tbody>
</table>

#### Management

- SNMP agent, XML configuration files, Syslog, SFTP, RADIUS interfaces.

#### Preferred VM Environment

- VMware ESXi 5.5

#### Max Capacity Configuration

- 4 CPU cores and 4GB of RAM

---

### ORACLE APPLIANCE-BASED E-SBC SPECIFICATIONS

#### Feature

<table>
<thead>
<tr>
<th>Acme Packet 1100</th>
<th>Acme Packet 3900</th>
<th>Acme Packet 4600</th>
<th>Acme Packet 6300</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>1U, shelf/table or rack mount</td>
<td>1U, rack mount</td>
<td>1U, rack mount</td>
</tr>
<tr>
<td>Oracle EOM Integration</td>
<td>Monitoring probe is queried by EOM</td>
<td>10 second interval Quality of Service updates sent to EOM</td>
<td>10 second interval Quality of Service updates sent to EOM</td>
</tr>
<tr>
<td>Registration Capacity</td>
<td>5,000 (UDP/TCP) 5,000 (TLS)</td>
<td>80,000 (UDP/TCP) 30,000 (TLS)</td>
<td>500,000 (UDP/TCP) 250,000 (TLS)</td>
</tr>
<tr>
<td>Storage &amp; Memory</td>
<td>32 GB fast mSATA drive for runtime image, backup configurations and local call detail record backup</td>
<td>Standard 120GB SSD for call detail record storage, log files, other permanent file storage 4GB of memory used for boot up only</td>
<td>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</td>
</tr>
<tr>
<td>Encryption</td>
<td>TLS session setup, and SRTP media encryption and decryption in software</td>
<td>IPSec tunnel and TLS session setup, IPsec and SRTP traffic encryption and decryption in hardware</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>SNMP, Syslog, SFTP, RADIUS interfaces</td>
<td>SNMP agent, XML configuration files, Syslog, SFTP, RADIUS interfaces</td>
<td></td>
</tr>
</tbody>
</table>

---

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