ORACLE COMMUNICATIONS

An Oracle White Paper
August 2013

What Is an Enterprise Session Border Controller?

ORACLE

Introduction

Enterprise communications is in a state of transformation. Businesses are replacing conventional private branch exchange (PBX) systems with Voice over IP (VoIP) and Unified Communications (UC) solutions and cloud-based services to improve collaboration and productivity, as well as to contain capital and operating expenses. Today's mobile information professionals are no longer tethered to the office phone system—they can conduct business and interact with colleagues and customers from any place, at any time.

As IT organizations make the transition to VoIP and UC, they must implement new systems and practices to safeguard IT infrastructure, secure communications, and preserve the high service levels users have come to expect from the corporate phone system and the public telephone network. The enterprise session border controller (E-SBC) is specifically designed to overcome the complex security, interoperability, and service quality challenges that IT teams encounter when implementing VoIP, UC, and mobility initiatives.

Operating at the session layer, E-SBCs connect the enterprise communications infrastructure to the public internet, private IP networks, and one or more Session Initiation Protocol (SIP) trunk service providers. They terminate and reoriginate each communications session, enabling the E-SBC to manage and control traffic, apply enterprise policies, and provide the cornerstone for a secure, efficient UC solution.

Redefining Enterprise Communications

Rapid advances in mobile technology and the growing adoption of VoIP and rich media communications are fundamentally reshaping business communications. The era of the office telephone system is coming to a close. Enterprise communications is in transition from time-division multiplexing (TDM) to IP, from the premises to the cloud, and from voice to multimodal communications.

Figure 1. Business, cultural, and technology trends are transforming enterprise communications.

A number of business, cultural, and technology trends are driving the transformation of enterprise communications and affecting IT planners:

- **Bring Your Own Device (BYOD) initiatives.** The lines between home and work devices are blurring. Workers need full, convenient, and secure access to all their business communications and collaboration tools, regardless of what device they are using or where they are working. By 2014, 80 percent of the global workforce will be eligible to participate in a BYOD program.[1]
- **Unified Communications (UC).** Traditional telephone calls are giving way to rich multimedia, multiparty interactions that combine voice, video, chat, and web collaboration. Enterprises are leveraging HD videoconferencing and telepresence systems to conduct meetings remotely, and deploying UC solutions such as Microsoft Lync to boost productivity and collaboration for mobile workers.
- **Emerging cloud services.** A growing variety of cloud-based solutions—videoconferencing services, customer relationship management systems, and contact center services—will enable IT organizations to eliminate capital equipment cost and complexity, accelerate service deployment, and focus on business innovation rather than the underlying telecommunications infrastructure.

[1] Gartner, "Creating a Bring Your Own Device Policy," April 2011.

- **Communications-enabled business processes (CEBP).** Many enterprises are embedding UC capabilities—voice, video, and chat—directly into business processes and line-of-business applications. By intelligently orchestrating real-time communications sessions with presence information and business rules, organizations reduce process inefficiencies and improve decision-making, employee productivity, and customer service.

SIP has emerged as the predominant signaling protocol for IP communications. Many service providers now offer SIP trunking solutions, which provide cost-effective and flexible alternatives to conventional T1/E1 primary rate interface (PRI) circuits. Supported in a wide range of communications platforms (UC servers, IP PBXs, and videoconferencing servers) and endpoints (desk phones, smartphones, and tablets), the SIP standard can help IT organizations reduce expenses, eliminate vendor lock-in, and enjoy greater choice when provisioning end users.

E-SBCs enable

- Secure SIP trunking
- Consolidated VoIP and UC networks
- IP contact centers
- Access to cloud and hosted IP communications services
- Remote workers and branch offices

E-SBCs Protect and Control IP Communications

Extending real-time IP communications across network borders introduces a variety of security, interoperability, and service quality challenges. Conventional IP networking devices—routers, firewalls, and traffic shapers—are not designed to manage real-time communications and do not address the unique security vulnerabilities, interoperability issues, or service quality concerns introduced by different VoIP, IP PBX, and UC systems.

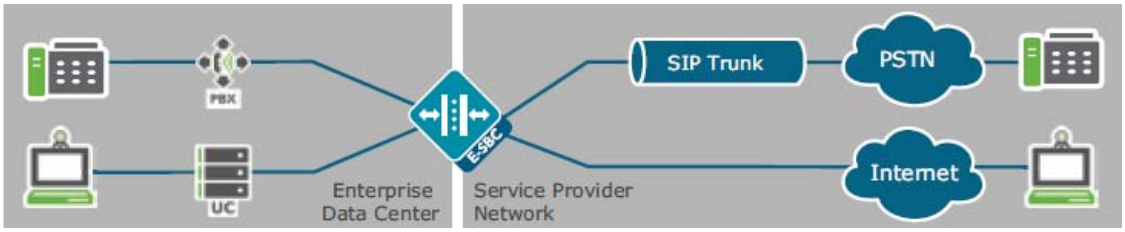

Figure 2. E-SBCs connect and control the traffic flowing through the enterprise real-time communications infrastructure to the public internet, other private IP networks, and SIP trunk service providers.

Typically deployed in the demilitarized zone (DMZ), E-SBCs operate at the session layer, processing traffic that uses real-time communications protocols, primarily SIP. Importantly, E-SBCs completely terminate and reoriginate each communications session, which enables the E-SBC to inspect traffic and apply granular control and policies. Businesses use E-SBCs to connect and control the traffic flowing through the enterprise real-time communications infrastructure to the public internet, other private IP networks, and to one or more SIP trunk service providers. Through SIP trunks, E-SBCs manage and control communication with the Public Switched Telephone Network (PSTN) and cloud-hosted

services. The E-SBC can also interconnect premises-based systems, including legacy PBXs, UC systems such as Microsoft Lync, and contact center environments.

As enterprises migrate to IP communications, they must find new ways to efficiently manage IT assets and safeguard communications—all while continuing to deliver the quality service levels that users have come to expect from the corporate phone system and the PSTN. E-SBCs are specifically designed to mitigate the complex security, interoperability, and service quality issues that IT organizations often encounter when implementing VoIP, UC, and BYOD initiatives and extending real-time IP communications across network borders.

TABLE 1. SPECIFIC SESSION FUNCTIONS PERFORMED BY E-SBCS

SESSION FUNCTION	DESCRIPTION
Protocol manipulation	For interoperability between premises-based systems and SIP trunk services, as well as multivendor systems
Protocol interworking	For example, SIP-to-H.323 interworking
Robust security	Through deep packet inspection
Encryption interworking	Go from encrypted to in-the-clear communications or encrypted Secure Real-time Transport Protocol (SRTP) to IP Security (IPsec)
Session prioritization, classification, and rate limiting	For quality of service (QoS), emergency calling (911), and service-level agreement (SLA) assurance
Session routing	For failover, least cost routing, and load balancing
Codec translation or renegotiation	For bandwidth optimization
Session replication	For centralized recording or compliance

E-SBCs Do More than Firewalls

It is important to understand the fundamental differences between an E-SBC, which is designed to manage and control real-time voice and video communications sessions, and a conventional security product like a firewall, which is intended primarily to block or allow data communications flows.

IP communications sessions are composed of signaling information (data used to set up and control sessions) and media information (digitized voice and video). Signaling information and media information flow under the direction of different IP protocols and move over separate paths.

SIP is used to establish and manage sessions. Real-time Transport Protocol (RTP) is used to deliver the associated audio and video streams. SIP servers (there are various types) are responsible for enabling sessions between two or more parties.

Most IP firewalls offer only basic support for SIP; they provide access control lists (ACLs), which can be configured to permit or reject SIP traffic based on the addressing information contained in the SIP signaling streams. Firewalls cannot actively manipulate nor control real-time IP communications sessions in the way an E-SBC can.

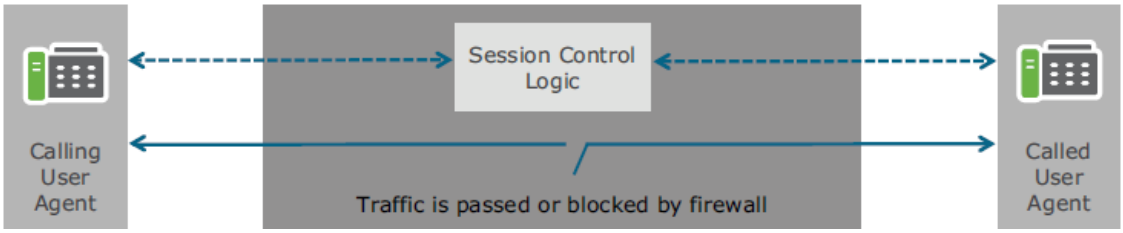

Figure 3. Most IP firewalls offer only basic support for SIP.

The difference lies in the underlying architecture. In SIP parlance, a SIP firewall is implemented as an SIP proxy server, which is responsible for relaying and controlling SIP signaling information, but is not actively involved in the RTP media path (the audio and video streams).

An E-SBC, on the other hand, is implemented as a back-to-back user agent (B2BUA), which actively processes both the signaling and media paths. A B2BUA terminates a session from one SIP entity (a calling party) and establishes a distinct session with another SIP entity (a called party). This enables an E-SBC to inspect and manipulate the contents of the entire session to enforce security policies and efficiently manage enterprise communications.

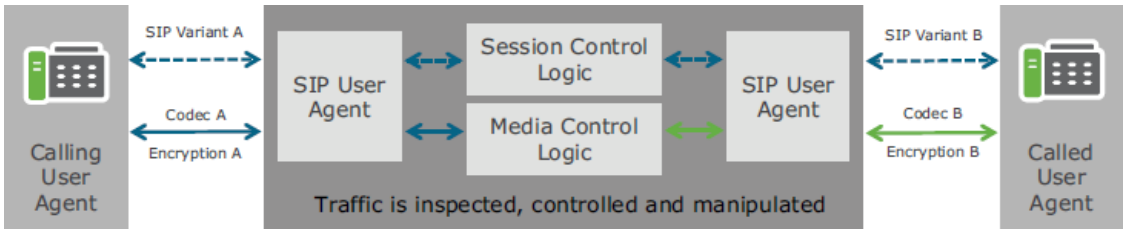

Figure 4. An E-SBC acts as a SIP back-to-back user agent.

Unlike a firewall, an E-SBC maintains session state and controls and manipulates SIP signaling plus associated RTP media streams. For example, an E-SBC keeps pinholes open for the duration of a communications session, whereas a firewall will close and reopen a pinhole using different port numbers, which can disrupt a session.

Building a Foundation for Scalable, Secure Communications

IT organizations often run into interoperability and interworking issues when extending real-time IP communications across network borders. SIP specifications are designed to be highly flexible; they give engineers a variety of implementation choices and offer many optional features and functions. As a result, it is not uncommon for different vendors (and service providers) to introduce solutions that are fully SIP-compliant, yet difficult to make work together. Interoperability challenges can delay VoIP and UC initiatives, lead to cost overruns, and drain limited IT resources.

E-SBCs allow you to build an enterprise UC architecture that can scale and accommodate new functions and systems—all while maintaining control and securing your communications. With the capability to maintain session state and manipulate RTP media streams as well as SIP signaling, the E-SBC can apply dynamic trust levels based on observed end-point behavior. The E-SBC can execute more-comprehensive, granular security controls encompassing a wide variety of communications networks.

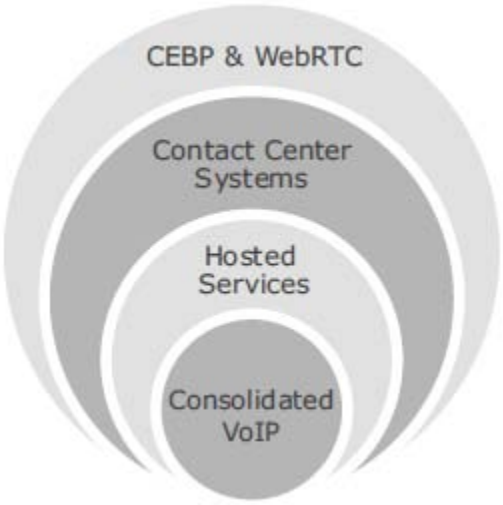

Figure 5. E-SBCs provide a fundamental building block for secure, scalable enterprise UC architectures.

Installed at the edge of the enterprise network, the E-SBC functions as a distinct demarcation point for external services (SIP trunking services, hosted services, cloud-based services, and so on). The E-SBC delineates the enterprise network from the service provider network, provides a distinct security perimeter, and makes it easier to isolate and troubleshoot problems.

In addition, by consolidating all real-time communications traffic, the E-SBC provides a central control point for classifying and prioritizing diverse traffic types—voice, video, and UC—prior to service provider hand-off. As such the E-SBC serves as a central point for SLA monitoring, and prioritizes and allocates limited bandwidth resource across all types of applications. Building a secure, comprehensive communications infrastructure that is able to accommodate different existing systems, legacy applications, and emerging IP-based functionality is no mean feat. Furthermore, satisfying increasing security and regulatory requirements with limited IT resources presents an even greater challenge to the IT manager.

Benefits of a True E-SBC

Greater IP Network Security

E-SBCs provide IP network–specific security capabilities to protect against denial-of-service (DoS) attacks and other malicious threats such as man-in-the-middle attacks. E-SBCs also provide IP address and topology concealment features to safeguard privacy and confidentiality, encryption capabilities to prevent eavesdropping and impersonation, and access control to prevent fraud and service theft.

Platform for Interoperability

E-SBCs provide extensive protocol normalization and mediation functions that mitigate multivendor interoperability and multiprotocol interworking issues. E-SBCs also provide comprehensive network address translation (NAT) and firewall traversal features for extending VoIP and UC sessions across network boundaries in a seamless manner. E-SBC interoperability capabilities help IT organizations accelerate deployment, while keeping implementation and support costs in check.

Increased Service Quality and Availability

Given end users' expectations, IP communications networks must deliver PSTN-like availability and service quality. Best-of-breed E-SBCs protect against service overloads by balancing loads across trunks and rerouting sessions to circumvent equipment and network problems. They also provide QoS marking, virtual local area network (VLAN) mapping, and admission control capabilities that enable network administrators to set service levels and manage service quality.

Cost Management and Avoidance

E-SBCs help IT organizations manage costs by consolidating network infrastructure to make more efficient use of network resources as communication needs increase. They support session control features to route calls across trunks and service providers (least cost routing) as well as codec renegotiation and translation capabilities to optimize wide area network (WAN) bandwidth.

Ensured Regulatory Compliance

Established methods and procedures for securing, controlling, and recording circuit-switched TDM calls are not easily extended to packet-based IP communications. E-SBCs help healthcare organizations maintain the confidentiality and integrity of customer interactions and help financial services record and archive required calls for regulatory oversight.

Many organizations throughout the world are required to support emergency calls (911 calls). E-SBCs provide security features to ensure session privacy and confidentiality, session replication capabilities to centralize and consolidate IP call recording, and session prioritization features to ensure that emergency calls take precedence.

Conclusion

UC solutions, smartphones, and tablets are ushering in a new era of enterprise communications where one-on-one phone calls give way to rich multimedia, multiparty experiences. By replacing and augmenting legacy TDM voice networks with converged IP networks that deliver voice, video, and data over a common infrastructure, IT organizations can eliminate inefficiencies, contain equipment and operations expenses, and transform the corporate network into a competitive advantage.

E-SBCs provide a fundamental building block for secure, scalable enterprise UC architectures. They can extend existing investments as well as integrate new, multimodal communications systems. E-SBCs enable businesses to realize all the benefits of interactive IP communications—greater productivity, improved collaboration, and lower costs—without compromising security, reliability, or service quality.

What Is an Enterprise Session Border Controller?
August 2013

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

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

Hardware and Software, Engineered to Work Together