WHITE PAPER

What is an E-SBC?

acme packet

Executive Summary Enterprise communications is in a state of transformation. Businesses are replacing conventional PBX systems with VoIP and Unified Communications (UC) solutions and cloud-based services to improve collaboration and productivity, as well as to contain capital and operating expenses. No longer tethered to the office phone system, today's mobile information professionals 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 IT teams encounter when implementing VoIP, UC, and Bring Your Own Device (BYOD) initiatives.

Operating at the session layer, E-SBCs connect the enterprise communications infrastructure to the public Internet, private IP networks, and to one or more Session Initiation Protocol (SIP) trunk service providers. Significantly, they terminate and re-originate 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 premise to the cloud, and from voice to multimodal communications.

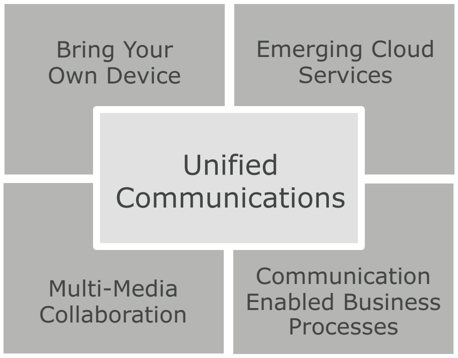

Figure 1: Trends Shaping Enterprise Communications

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

- *Bring Your Own Device 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:* Traditional telephone calls are giving way to rich multimedia, multiparty interactions that combine voice, video, chat, and web collaboration. Enterprises are leveraging HD video conferencing and telepresence systems to conduct meetings remotely, and are deploying unified communications (UC) solutions, such as Microsoft® Lync®, to boost productivity and collaboration for mobile workers.

- *Emerging Cloud Services:* A growing variety of cloud-based solutions—video conferencing 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 underlying telecommunications infrastructure.

- *Communication Enabled Business Processes (CEBP):* Many enterprises are embedding unified communications capabilities—voice, video, 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.

E-SBCs Enable:

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

Session Initiation Protocol 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 PRI circuits. Supported in a wide range of communications platforms (UC servers, IP PBXs, and video conferencing 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.

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

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, 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.

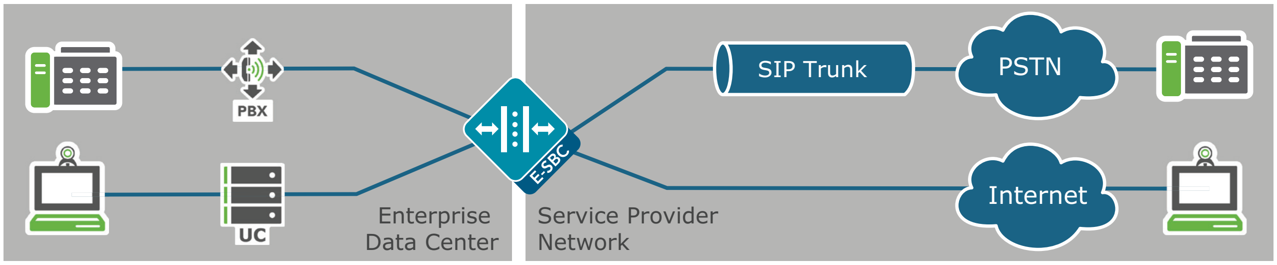

Figure 2: Connecting the Enterprise to the Public Network

Typically deployed in the DMZ, E-SBCs operate at the session layer, processing traffic that uses real-time communications protocols, primarily Session Initiation Protocol. Importantly, E-SBCs completely terminate and re-originate each communications session; this 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 PSTN and cloud-hosted services. The E-SBC can also interconnect premise-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 users have come to expect from the corporate phone system and the public switched telephone network (PSTN). E-SBCs are specifically designed to mitigate the complex security, interoperability and service quality issues 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

Protocol manipulation	For interoperability between premise-based systems & SIP trunk services, as well as multi-vendor 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 SRTP to IPsec
Session prioritization, classification & rate limiting	For Quality of Service, emergency calling (i.e. 911), SLA assurance
Session routing	For failover, least cost routing, 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, compared to 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 and media information flow over separate paths under the direction of different IP protocols.

SIP is used to establish and manage sessions. RTP (Real-time Transport Protocol) 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.

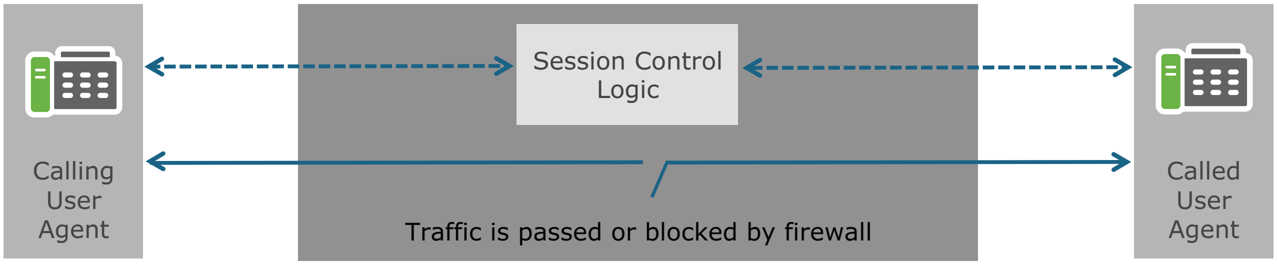

Figure 3: SIP Firewall Implemented as SIP Proxy

Most IP firewalls offer only basic support for SIP; they provide Access Control Lists, 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.

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 (say a calling party) and establishes a distinct session with another SIP entity (say 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.

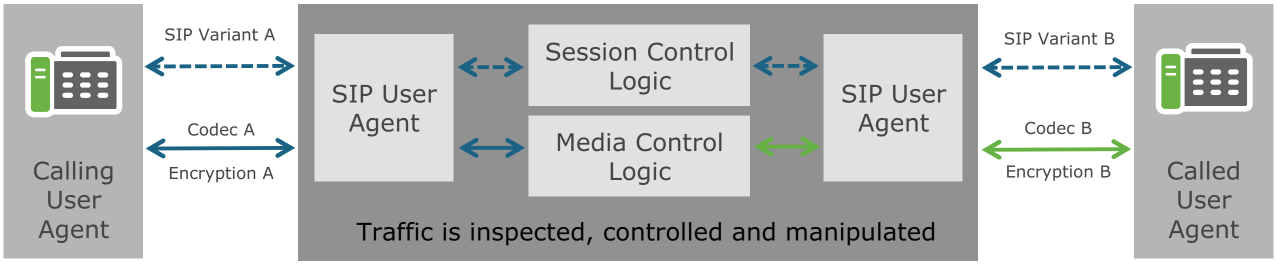

Figure 4: E-SBC Acts as a SIP "Back-to-Back User Agent"

Unlike a firewall, an E-SBC maintains session state and controls and manipulates SIP signaling plus the associated RTP media streams. For example, an E-SBC keeps pinholes open for the duration of a communication 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 are a continuing drain on limited IT resources.

E-SBCs allow you to build an enterprise UC architecture that can scale and accommodate new functions and systems, 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.

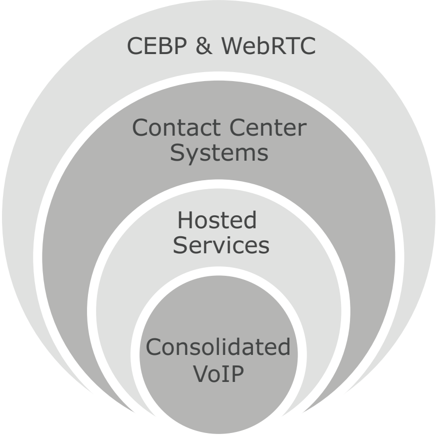

Figure 5: Expanding Enterprise Communications Pipeline

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, etc.). 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, UC—prior to service provider hand-off. As such the E-SBC serves as a central point for service level agreement (SLA) monitoring, and prioritizes and allocates limited bandwidth resource across all types of applications. Building a secure, comprehensive communications infrastructure, 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 Enterprise SBC

Greater IP Network Security

E-SBCs provide IP network specific security capabilities to protect against denial-of-service attacks and other malicious threats such 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, as well as 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' service 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 Quality of Service (QoS) marking, virtual LAN (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, making 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 WAN bandwidth.

Achieve 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 financial services record and archive required calls for regulatory oversight.

Many organizations throughout the world are required to support emergency calls (i.e. 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 emergency calls take precedence.

Conclusion

Unified communications 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 enable businesses to realize all the benefits of interactive IP comunications—greated productivity, improved collaboration, lower costs—without compromising security, reliability, or service quality.

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

For More Information

- Acme Packet
- Acme Packet Enterprise Solutions
- Acme Packet Enterprise Products

About Acme Packet

Acme Packet (NASDAQ: APKT), the leader in session delivery network solutions, enables the trusted, first-class delivery of next-generation voice, video, data, and unified communications services and applications across IP networks. Our Net-Net product family fulfills demanding security, service assurance and regulatory requirements in service provider, enterprise, and contact center networks.

Based in Bedford, Massachusetts, Acme Packet designs and manufactures its products in the USA, selling them through over 250 reseller partners worldwide. More than 1,775 customers in 109 countries have deployed over 19,000 Acme Packet systems, including 89 of the top 100 service providers and 45 of the Fortune 100.

The content in this document is for informational purposes only and is subject to change by Acme Packet without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Acme Packet assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Acme Packet, Acme Packet has no obligation to develop or deliver any future release or upgrade or any feature, enhancement or function.

acme packet

100 Crosby Drive
Bedford, MA 01730 USA
t +1 781.328.4400
f +1 781.275.8800
www.acmepacket.com