ENTERPRISE SESSION BORDER CONTROLLERS: SAFEGUARDING TODAY'S AND TOMORROW'S UNIFIED COMMUNICATIONS

ALCATEL-LUCENT OPENTOUCH™
SESSION BORDER CONTROLLER –
A SECURE SOLUTION FOR BORDERLESS
CONVERSATIONS

APPLICATION NOTE

AT THE SPEED OF IDEAS™

Alcatel·Lucent
Enterprise

TABLE OF CONTENTS

Session border controllers (SBCs) have traditionally been used as Session Initiation Protocol (SIP) firewalls in service providers' networks. However, an increasing number of enterprises are deploying an enterprise SBC (E-SBC) because they access their SIP trunking providers through the Internet and need additional security.

As new methods of communication are adopted, E-SBCs become the cornerstone of SIP security. E-SBCs secure and provide the appropriate quality of experience (QoE) to remote workers – a growing trend in many organizations. E-SBCs secure conversations with people outside the organization – a service that is now available and which will gain widespread adoption with the implementation of promising technology, such as WebRTC and cloud deployment models.

This paper explains the role of E-SBCs, describes the Alcatel-Lucent OpenTouch™ blueprint for securing SIP conversations, highlights the benefits and, lastly, considers how SBCs will evolve, both from a technology (WebRTC) and deployment model (cloud) standpoint.

THE ROLE OF ENTERPRISE SESSION BORDER CONTROLLERS

Main drivers for Enterprise SBCs

The three major reasons for E-SBC adoption are described in Table 1.

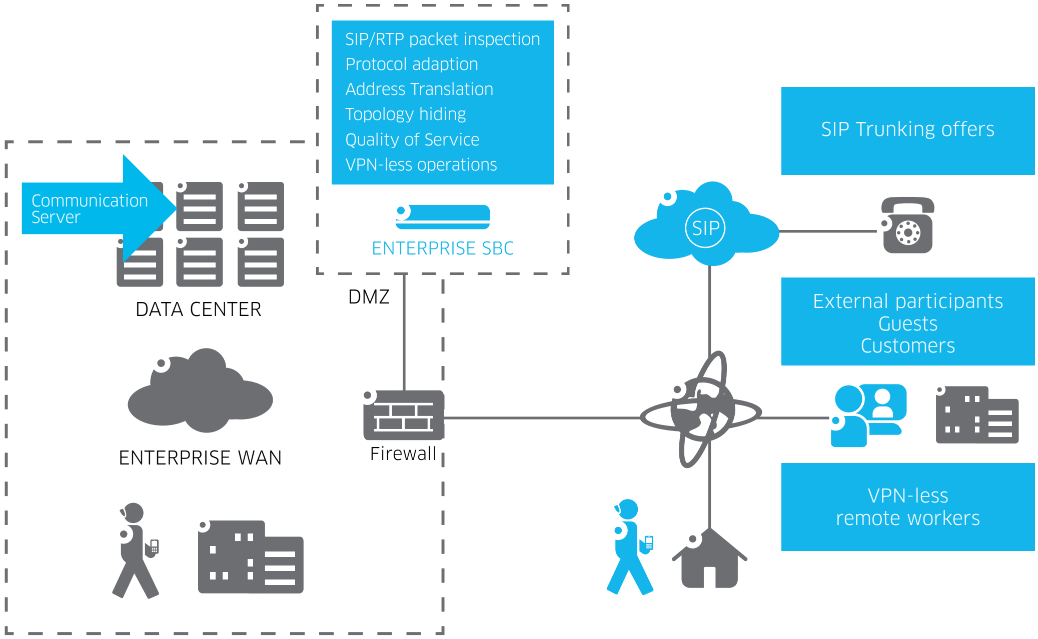
Table 1. Enterprises' main drivers for adopting E-SBCs

Stronger perimeter defense	Enterprises use E-SBCs to secure their networks against SIP-based attacks from the Internet that could compromise communication servers. Hackers mainly target these servers to commit long-distance call fraud. They can also mask calls related to their criminal activity. They may also eavesdrop on communications or jeopardize the business by stopping all of an enterprise's communications.
Improved operational agility	Enterprises using SIP trunks for off-net communications must expose their internal IP topology to service providers. Direct Real-time Transport Protocol (RTP) media connectivity between enterprise devices and the SIP trunking provider improves media quality. An E-SBC provides a demarcation point to hide the enterprise topology and devices. Enterprises can modify their network topology and upgrade devices without affecting the SIP trunking service.
Easier access for mobile employees and guests	E-SBCs can enable mobile employees to use native SIP clients instead of complex virtual private network (VPN) clients to secure communications. They enable guests to use SIP clients to participate in internal enterprise collaboration sessions natively. E-SBCs also allow administrators to simplify the authentication architecture by removing VPNs and their dedicated security policies.

Enterprise SBC position and functions

As shown in Figure 1, E-SBCs perform deep packet inspection of SIP and RTP traffic and complement the firewall's perimeter defense by dynamically opening ports for RTP media streams in the demilitarized zone (DMZ).

Figure 1. E-SBC position and role in the enterprise communication architecture



E-SBCs are demarcation points and provide protocol adaptation between SIP and RTP protocols. They also hide the network topology through address and port translation. In addition, E-SBCs provide fine-grained quality of service (QoS) enforcement by marking SIP and RTP packets. E-SBCs monitor the QoS for RTP streams, which is usually a performance indicator for service level agreements with SIP trunking providers. As E-SBCs perform security at the SIP level, remote workers don't require VPN clients to secure off-site communications. E-SBCs also perform perimeter defense for communications with guests and external participants.

ENTERPRISE SBC IN THE ALCATEL-LUCENT OpenTouch BLUEPRINT

The OpenTouch Suite for Mid-Sized and Large Enterprises (MLE) is the Alcatel-Lucent unified communication and collaboration application. It is deployed in the enterprise datacenter and provides SIP trunking capabilities, web-based collaboration for guests over the Internet, and multi-party, multimedia, multi-device conversation services for employees in the office and on the go.

OpenTouch Suite perimeter defense

As shown in Figure 2, the OpenTouch Suite perimeter defense is an overlay solution to an enterprise's existing security technology, so no disruption to established security policies is required for installation. The OpenTouch Suite defense relies on three optional components, defined in Table 2.

Figure 2. OpenTouch security blueprint

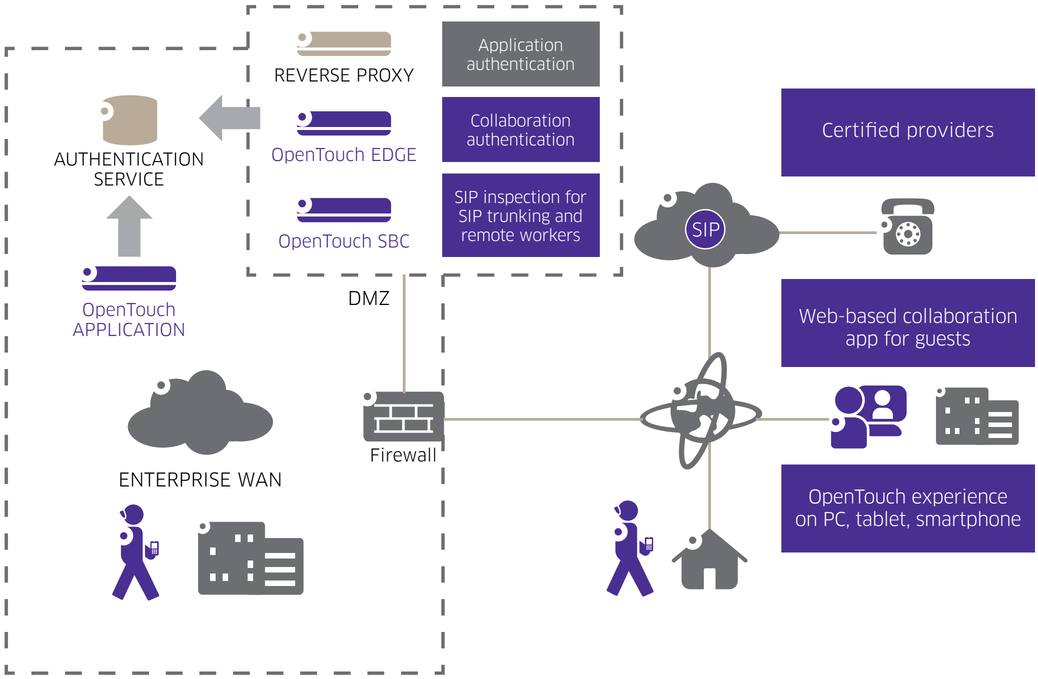

REVERSE PROXY
Application authentication
OpenTouch EDGE
Collaboration authentication
OpenTouch SBC
SIP inspection for SIP trunking and remote workers
AUTHENTICATION SERVICE
OpenTouch APPLICATION
DMZ
Certified providers
SIP
Web-based collaboration app for guests
Firewall
ENTERPRISE WAN
OpenTouch experience on PC, tablet, smartphone

Table 2. OpenTouch security elements in the DMZ

OpenTouch Session Border Controller	This E-SBC performs SIP perimeter defense for SIP trunking and SIP remote workers using a PC, tablet or smartphone. It supports the connectivity needs of organizations from 50 to 5000 users.
OpenTouch Edge Server	This server is a front-end that delivers web-sharing capabilities to OpenTouch remote workers and guests. The front-end authenticates guests via web access codes. The Edge Server screens and forwards legitimate conferencing application traffic to the internal conferencing server (e.g., it will block forged URLs). Depending on the policy, guests may dial-in or dial-out over the public switched telephone network (PSTN).
Reverse proxy	This reverse proxy authenticates and terminates the Transport Layer Security (TLS) connections that secure the web services used by the OpenTouch client applications on PCs, tablets and smartphones. Enterprises requiring a reverse proxy for HTTP translation and to authenticate additional web apps can use it for OpenTouch web services. It connects to the enterprise authentication service.

These components complement the existing firewall and authentication service (Lightweight Directory Access Protocol (LDAP) or RADIUS-based) to smoothly implement SIP communications over the Internet, as described in Table 3.

Table 3. OpenTouch SIP communications over the internet

USE CASE	DEPLOYED COMPONENTS	DIFFERENTIATORS
SIP trunking	OpenTouch SBC	A large number of certified SIP providers are supported when used in conjunction with the OpenTouch telephony module, the OmniPCX Enterprise Communication Server.
Remote workers (voice, video)	OpenTouch SBC, reverse proxy	The zero-touch management for SIP authentication in the SBC improves the total cost of ownership (TCO) for the solution.
Remote workers (voice, video, web sharing)	OpenTouch SBC, Edge Server, reverse proxy	The location within the DMZ protects datacenter applications. No information is stored on the Edge Server to reduce vulnerability to hackers.
Guest access to web conferences	OpenTouch Edge Server	The location within the DMZ protects datacenter applications. No shared document or information is stored on the Edge Server. Guests can dial-in or out over PSTN, policy permitting.

Voice and video over IP for guests

Some organizations want guests in partner organizations to be able to access their web conferencing infrastructure through voice and video over IP. A typical example is business-to-business (B2B) communications between global organizations: voice and video over IP replace international toll-free numbers.

The main issue with this application is how the communications will affect the partner's information technology (IT) infrastructure where the guests are located: voice and video over IP streams must be allowed over the partner's network and through the partner's firewall. This security policy issue is a challenge for most enterprises.

However, if the partner's IT organization allows outgoing SIP and media streams, a dedicated OmniTouch Advanced Communication Server conferencing infrastructure from Alcatel-Lucent will resolve these issues for B2B communications. The infrastructure comprises a conference application and a front-end server in the DMZ. The front-end server terminates VoIP, video over IP and HTTP web conferencing streams from the guests.

THE EVOLUTION OF ENTERPRISE SBC

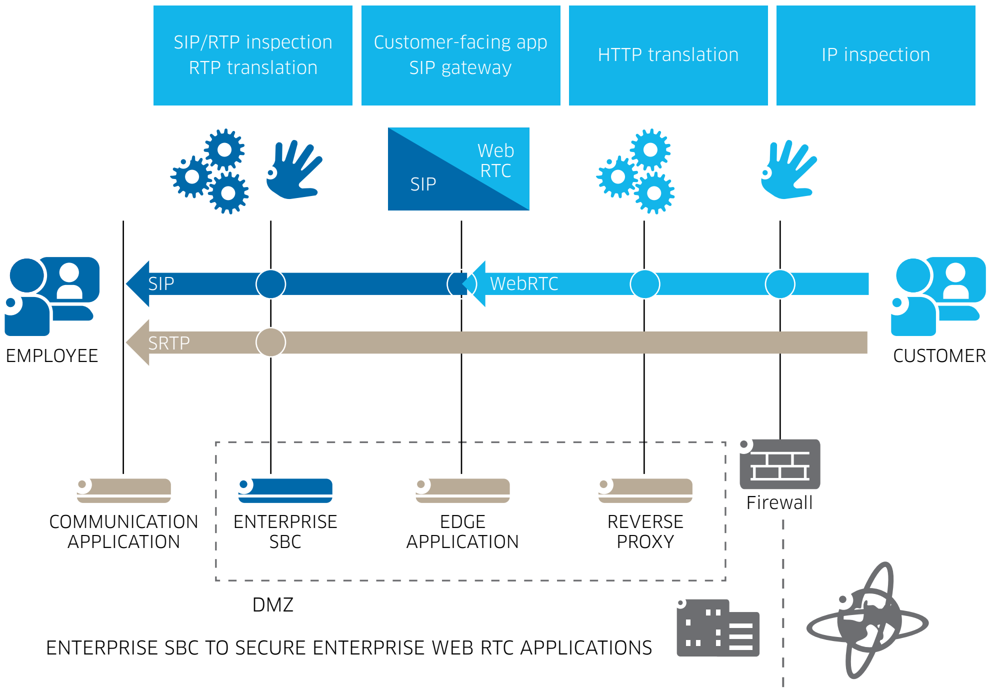
E-SBCs play a significant role in securing today's SIP communications and will also be a key element in the upcoming changes to multimedia communications over the Internet: WebRTC clients and cloud-based services.

Secure WebRTC communications

WebRTC is an emerging technology for standard and native voice and video over IP capabilities in web browsers. No plug-in or downloaded software is needed. The security issues related to accessing the camera and microphone of the device will be handled natively by the browser. When the WebRTC standard is published and adopted by most browsers, the volume of B2B and business-to-consumer (B2C) communications will sharply increase.

B2B and B2C communications need to be secure. As described in Figure 3, an evolution in edge servers is required to implement a back-to-back WebRTC and SIP Agent. E-SBC will control the SIP and RTP streams exchanged between the Enterprise's SIP applications and the WebRTC application.

Figure 3. Call flow of an enterprise WebRTC application



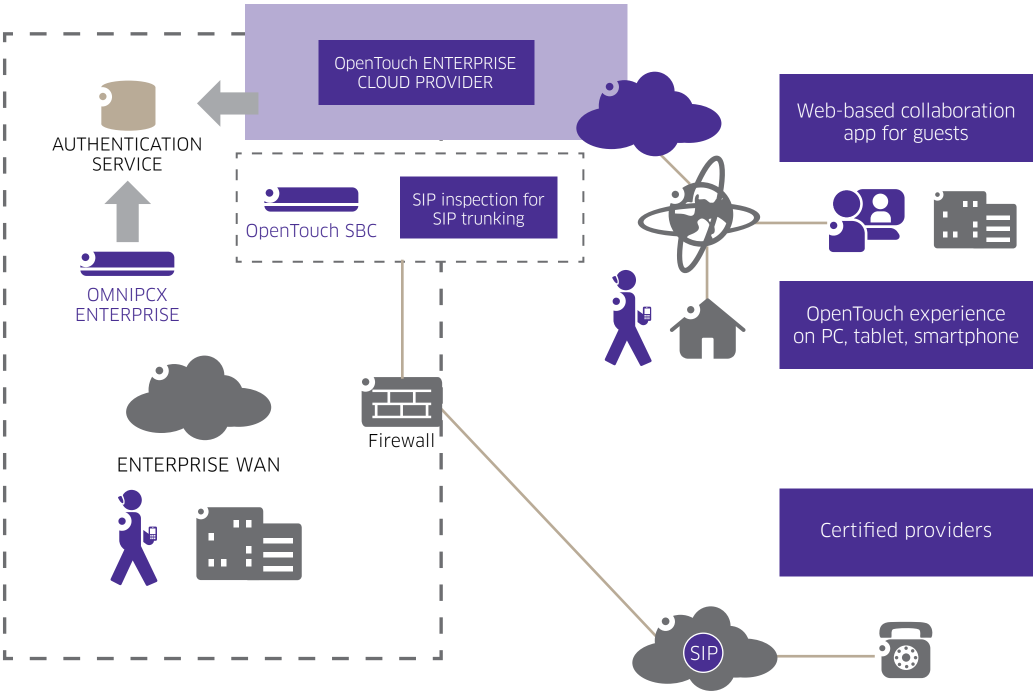
Secure cloud-based communications

Many organizations consider cloud-based services because they are usually accounted for using an operational expense model, which reduces up-front investment and provides licensing flexibility.

Communications services are also delivered via cloud-based providers, such as through a service provider or system integrator using the OpenTouch Enterprise Cloud solution. Depending on the network topology, this solution can rely on OpenTouch SBC technology to secure remote and mobile workers.

Enterprises that have deployed OpenTouch SBC to secure OmniPCX Enterprise SIP trunking and want remote and mobile workers to be connected through the OpenTouch Enterprise Cloud keep their SBC: their remote workers' communications experience through the cloud is similar to being connected to the SBC.

Figure 4. Example of an architecture with hybrid cloud- and premises-based security elements


OpenTouch ENTERPRISE CLOUD PROVIDER
AUTHENTICATION SERVICE
OMNIPCX ENTERPRISE
OpenTouch SBC
SIP inspection for SIP trunking
ENTERPRISE WAN
Firewall
Web-based collaboration app for guests
OpenTouch experience on PC, tablet, smartphone
Certified providers
SIP

CONCLUSION

Many enterprises adopt Enterprise Session Border Controllers to protect their SIP trunking interfaces from call fraud and denial of service attacks.

The Alcatel-Lucent OpenTouch SBC is an E-SBC for organizations with 50 to 5000 users. The OpenTouch SBC and companion servers create a flexible solution that secures SIP trunking and collaboration on the go for employees and guests. This solution is designed as an overlay that complements enterprise firewall and authentication infrastructures to reduce the TCO.

E-SBCs such as the OpenTouch SBC are key security elements for today's unified communications and will be pivotal in upcoming WebRTC and cloud-based technology.

ACRONYMS

B2B: Business-to-business

B2C: Business-to-consumer

DMZ: Demilitarized zone

E-SBC: Enterprise session border controller

HTTP: Hypertext Transfer Protocol

IP: Internet Protocol

PC: Personal computer

PSTN: Public Switched Telecom Network

QoS: Quality of service

RADIUS: Remote Authentication Dial In User Service

RTP: Real-time Transport Protocol

SRTP: Secure Real-time Transport Protocol

SBC: Session border controller

SIP: Session Initiation Protocol

TCO: Total cost of ownership

TLS: Transport Layer Security

VoIP: Voice Over Internet Protocol

VPN: Virtual private network

WebRTC: Web Real-Time Communications

Alcatel·Lucent
Enterprise