An Oracle White Paper
June 2013

# Comparing Session Border Controllers to Firewalls with SIP Application Layer Gateways in Enterprise Voice over IP and Unified Communications Scenarios

# Introduction

Voice over IP (VoIP) and unified communications (UC) are increasingly prevalent as standards-based alternatives to closed proprietary communications systems. The expandability, flexibility, and cost advantages offered by IP networks provide a highly effective means for enterprises and contact centers to communicate, both internally and externally, in today's dynamic business and economic climates.

Because an organization's communications network is a business-critical resource, IP-based enterprise and contact center communications networks, services, and applications must be secured. But other requirements, such as maximizing communication service and application interoperability, assuring service availability and quality levels, complying with government regulations, and controlling costs must also be met for successful VoIP/UC delivery.

# How It Works: Firewalls with SIP Application Layer Gateway versus Session Border Controllers

Enterprise firewalls—ubiquitous in today's IP networks—protect IP data networks, servers, and applications against a variety of threats through stateful inspection and filtering at layers 3 and 4 of the Open Systems Interconnection (OSI) model. To enable basic VoIP connectivity through the firewall, some firewalls add SIP application layer gateways (SIP ALGs) that translate embedded SIP addresses, in effect allowing the firewall to maintain a single end-to-end SIP session between endpoints residing on either side of the firewall.

By comparison, session border controllers (SBCs) implement a SIP back-to-back user agent (B2BUA) as defined in IETF RFC 3261. A B2BUA divides each SIP session into two distinct segments, as shown in the following diagram. In doing so, the SBC is able to completely and effectively control SIP sessions, as well as the associated media flows, in ways that SIP ALGs cannot. This unique capability gives SBCs a clear edge in their ability to securely deliver reliable, high-quality, IP-based interactive communications.

## Firewall with SIP ALG

- Maintains single SIP session through firewall (FW)
- Is fully state-aware at layers 3 and 4
- Only inspects/modifies SIP and Session Description Protocol (SDP) addresses
- Unable to terminate, initiate, reinitiate, or respond to SIP signaling messages
- Only supports static access control lists (ACLs) and policies

## SBC

- Implements SIP B2BUA for complete control
- Is fully state-aware at layers 2 through 7
- Inspects/modifies all SIP and SDP header info
- Can terminate, initiate, reinitiate, and respond to SIP signaling messages
- Supports static and dynamic ACLs and policies

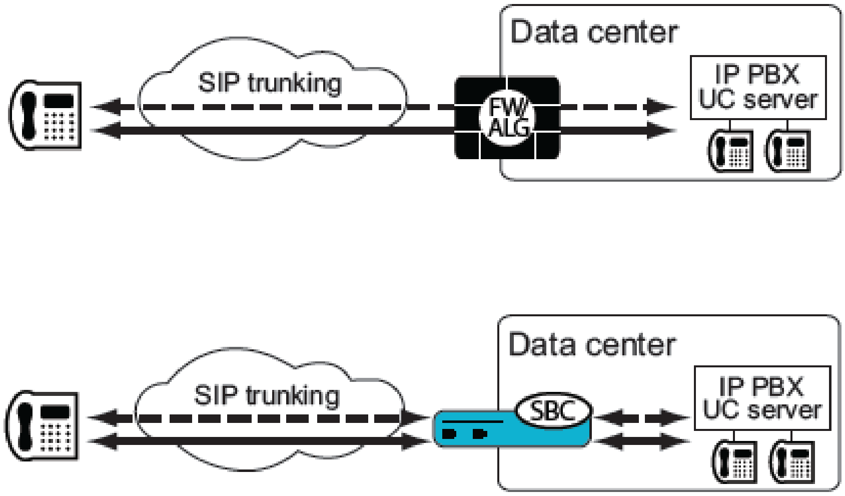

Figure 1. SBCs use a B2BUA to divide each SIP session into two distinct segments.

## Benefits of Session Border Controllers

Session border controllers uniquely provide all controls required for delivering trusted, reliable, and high-quality IP interactive communications:

- **Security:** IP private branch exchange (PBX) and UC server denial of service/distributed denial of service (DoS/DDoS) attack protection, SBC self-protection
- **Communications reach maximization:** IP PBX and UC protocol interworking, remote network address translation (NAT) traversal
- **Service-level agreement (SLA) assurance:** IP PBX and UC server session admission and overload control, data center disaster recovery, remote site survivability, Quality of Experience (QoE)-based routing, SBC high-availability operation
- **Regulatory compliance:** session replication for recording

Data firewalls with application layer gateways (FW/ALG) are only effective securing data-oriented application infrastructure (PCs, servers).

## Use Cases: Session Border Controllers versus Firewalls with SIP Application Layer Gateway

The best way to illustrate the differences between SBCs and FW with SIP ALG is within the context of common enterprise and contact center VoIP/UC use cases. Each of the ten scenarios shown below is accompanied by an associated business challenge, as well as the technical requirements that would have to be met by the network element in order to address that challenge. Each scenario demonstrates conclusively that only session border controllers are capable of meeting all requirements for the successful delivery of enterprise and contact center VoIP/UC services and applications.

**USE CASES: SBCS VERSUS FIREWALLS WITH SIP ALG**

| USE CASE SCENARIO | BUSINESS CHALLENGE | TECHNICAL REQUIREMENTS | SBC | FW/ALG |
|---|---|---|---|---|
| SBC/FW DoS/DDoS self-protection | • Prevent malicious or nonmalicious SIP signaling or media attacks and overloads from making the SBC or FW nonresponsive | • Dynamically block attacks<br>• Detect/reject noncompliant (protocol, signaling, and traffic levels) SIP sessions<br>• Initiate SIP BYE requests to tear down core-side sessions<br>• Statefully control legitimate SIP registrations during overloads | ✓ | |
| Network abuse control | • Prevent unauthorized or fraudulent network usage | • Control number and bandwidth of simultaneous sessions<br>• Strip unauthorized codecs from SDP headers<br>• Scan SIP header attachments for unauthorized content | ✓ | |
| IP PBX and UC protocol interworking | • Translate dissimilar signaling (SIP and H.323), transport (UDP, TCP, SCTP), and encryption protocols (none, TLS, SRTP, IPsec) | • Terminate SIP sessions and translate layer 2-7 protocol information<br>• Fix protocol anomalies and inconsistencies | ✓ | |
| IP PBX/UC server session admission and overload control | • Ensure continuous service availability and quality, even under adverse traffic loads or attack | • Dynamically monitor and control SIP signaling flows to IP PBX/UC servers based upon number of sessions or rate of session establishment | ✓ | |
| Remote site NAT traversal (no SBC or FW w/ALG at site) | • Enable users behind FW/NATs to originate and receive VoIP calls and UC sessions | • Keep remote site FW pinholes open by resetting SIP registration interval to less than FW port TTL and caching SIP registrations by FW IP/port | ✓ | |
| High availability operations | • Ensure no loss of active sessions or session state during SBC or FW failover | • Checkpoint SIP signaling, media, and configuration state between active and standby elements | ✓ | |
| Data center disaster recovery | • Assure constant service availability and quality | • Service provider network SBC: detect failure of primary data center SBC and reroute SIP sessions<br>• Data center SBC: translate rerouted phone numbers in SIP headers to back-up data center phone numbers | ✓ | |
| Remote site survivability<br>using SBC/FW | • Provide alternative path for VoIP/UC traffic when primary path becomes unavailable | • Monitor link and routing state of upstream router and SIP state of data center SBC or IP PBX/UC server | ✓ | |

| | | | | |
|---|---|---|---|---|
| | | • Reroute SIP signaling and media to alternative SIP trunking provider, Public Switched Telephone Network (PSTN) gateway, or Internet upon failure | | |
| QoE-based routing | • Maximize voice quality and reliability of services and applications | • Actively monitor voice QoS thresholds and ASR<br>• Reroute sessions to alternative providers as needed<br>• Release media within access networks to optimize quality | ✓ | |
| Session replication for recording | • Comply with regulatory requirements and maximize customer service quality | • Replicate all SIP signaling and media to recording server(s) in addition to intended recipient<br>• Replicate selective or all sessions | ✓ | |

## Conclusion

Across all use scenarios, only session border controllers meet the requirements for the successful delivery of enterprise and contact center VoIP/UC services and applications. When compared to FW/ALGs, SBCs offer a clear advantage to in their ability to securely deliver reliable, high-quality, IP-based interactive communications.

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

Comparing Session Border Controllers
to Firewalls with SIP Application Layer
Gateway in Enterprise Voice over IP
and Unified Communications Scenarios
June 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

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.

Hardware and Software, Engineered to Work Together