Study On: Session Border Controllers and Impact on Voice and Video Conferencing

Siddarth Kaul & Dr Anuj Jain
Research Scholar Bhagwat University Rajasthan India
Assistant Professor Bhagwat University Rajasthan India

Received: Feb. 12, 2018
Accepted: March 09, 2018

Introduction
A session border controller (SBC) is a device regularly deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications. Early deployments of SBCs were focused on the borders between two service provider networks in a peering environment. This role has now expanded to include significant deployments between a service provider's access network and a backbone network to provide service to residential and/or enterprise customers.

The term "session" refers to a communication between two parties – in the context of telephony, this would be a call. Each call consists of one or more call signaling message exchanges that control the call, and one or more call media streams which carry the call's audio, video, or other data along with information of call statistics and quality. Together, these streams make up a session. It is the job of a session border controller to exert influence over the data flows of sessions.

The term "border" refers to a point of demarcation between one part of a network and another. As a simple example, at the edge of a corporate network, a firewall demarcates the local network (inside the corporation) from the rest of the Internet (outside the corporation). A more complex example is that of a large corporation where different departments have security needs for each location and perhaps for each kind of data. In this case, filtering routers or other network elements are used to control the flow of data streams. It is the job of a session border controller to assist policy administrators in managing the flow of session data across these borders.

The term "controller" refers to the influence that session border controllers have on the data streams that comprise sessions, as they traverse borders between one part of a network and another. Additionally, session border controllers often provide measurement, access control, and data conversion facilities for the calls they control.

What is a session?
A session is a communications interaction that has a defined beginning and end and is effective only when transmitted in real time without latency or delays. Enabling session-based communication requires control of the session from its origination point to its defined end point. To gain the acceptance of users, service provider sand enterprise smust be able to assure secure and high-quality interactive communications end-to-end as sessions traverse multiple IP networks.

Managing Session-Based Communications
To provide secure and high-quality interactive communications, IP networks must be able to manage and integrate the communication flows that constitute a session. Each session includes three sets of bidirectional communication flows:

» Session signaling messages – messages used to initiate, modify or terminate a session
» Media flows – data packets containing the actual media being exchanged
» Media control messages – messages used to compile information to report on QoS levels

A session is initiated with signaling messages. These messages establish a virtual connection between the participants’ personal computers, IP phones, otherrnodes. In addition, they negotiate the IP addresses used for the session's media streams and control the messages and algorithms (codecs) used to digitize analog voice and video.

Various codecs are available for voice and video transmission, each offering trade-offs between quality and bandwidth efficiency. Once the call is initiated, media streams and control messages flow in both directions.
between participants. Signaling messages are also used to transfer a call, place a call on hold, and terminate session. The session based communication includes following three components. Every session includes three sets of bidirectional communication flows:

**Session Signaling messages Media flows**

The management of session-based communications is complicated by the following characteristics of today's IP networks:

» The identities of the participants are difficult to ascertain, and security needs are complex
» The number of session signaling protocols, codecs, and related standards continues to grow
» Addressing schemes are not consistent or compatible across networks
» Bandwidth and signaling element resources are finite
» Interactive communications service provider business models and regulatory compliance requirements continue to evolve and require network flexibility.

Additionally, unlike typical data communications, not all session-based communications can be treated with the same priority. For example, an emergency services (911) call or a high-quality enterprise video conference should take priority over watching TV.

Session border controller enable the delivery of secure, high-quality interactive communications across multiple IP networks.

For a service provider, these include the separate IP networks that constitute fixed-line, mobile, and cable networks. SBCs are deployed at the borders between IP networks, such as between two service providers or between a service provider and its enterprise, residential, or mobile customers.

For an enterprise, SBCs are used to interconnect communications “islands” that exist within the enterprise, connect the enterprise to a wide area service designed for interactive communications (such as a SIP trunk), or enable “federations” between multiple enterprises for B2B communications. Enterprise SBCs (E-SBCs) also enable selected remote locations or mobile workers to securely access enterprise or active communications services via the internet.

SBCs are the only network element capable of integrating the control of signaling messages and media flows used by interactive communications. This capability complements the roles and functionality of routers, soft-switches, and data firewalls that operate within the same network.

SBCs support a broad range of next-generation services and communications applications, providing key control functions for enterprises and service providers alike to uniquely ensure

» Security
» Interoperability and service reach maximization
» Quality of experience (QoE), availability, and service-level agreement (SLA) assurance
» Service revenue optimization and cost management

**What makes SBCs different?**

SBCs are the only network element capable of integrating the control of signaling messages and media flows used by interactive communications. This capability complements the roles and functionality of routers, soft-switches, and firewalls that operate within the same network.

The Evolution to SBC-Enabled IP Communications Prior to the advent of the SBC, IP network infrastructure equipment could initiate and route undifferentiated data but lacked the ability to specifically target the management of interactive communications sessions. The development of the SBC, unlike many other emerging networking products, was not initially catalyzed by standards bodies. Rather, SBCs came about as the result of pragmatic needs of service providers and enterprises that were not met by other types of network elements.

To date, SBCs (now more frequently recognized by standards bodies) have been deployed around the world to support next-generation interactive communications services and applications such as Voice over Internet Protocol (VoIP), video-conferencing, instant messaging (IM), and presence as well as the routing of voice conversations over private as well as public IP networks, including the internet.

SBC Deployment at Access, Interconnect, and Trunking Borders (Refer Figure 1)

SBCs are deployed at the borders of IP networks. The border between two service providers is referred to as an interconnect border; the border between a service provider and its enterprise, residential, or mobile customers is referred to as an access border. Enterprises also deploy E-SBCs at the border between their IP network and their service provider’s network, referred to as the trunking border. The border between enterprise data centers and their employees is referred to as the enterprise access border. SBCs act as the source and the destination for all signaling messages and media stream entering and exiting the network.

To that end, SBCs complement rather than replace existing network and service infrastructure.
At all borders, SBCs are deployed in front of session agents—such as soft-switches, IMS Call Session Control Function (CSCF) elements, IP-enabled mobile switching centers (MSCs), IP PBXs, UC servers, and application servers—and make call acceptance or rejection decisions. This protects the session agent from signaling attacks initiated by hackers and from non-malicious overloads. It also ensures that calls are accepted only when adequate network quality and soft-switch resources are available.

At many borders, SBCs function in parallel with data firewalls, which protect web and application servers and PCs from attacks while the SBC protects session agents. SBCs augment the simple, discrete, packet-by-packet routing decisions that routers make. Unlike routers, SBCs classify flows as interactive communication sessions and make more intelligent routing decisions to ensure secure, high-quality communications.

**SBC Functions**

SBCs apply controls to signaling and media flows as they traverse network borders, enabling the effective delivery of session-based IP communications. For service providers, these controls fall into five basic categories: security, service reach maximization, SLA assurance, revenue optimization and cost efficiency, and regulatory compliance.

- **Security.** SBCs protect themselves, session agents, and other elements of the service delivery infrastructure as well as customer networks, systems, and relationships. They protect customer networks and session privacy and provide DoS/DDoS protection from attacks and non-malicious overloads.
- **Interoperability and service reach maximization.** SBCs extend the reach of IP communications services and applications by maximizing the different types of networks and devices supported. SBCs enable sessions to traverse existing data firewall and network address translation (NAT) device sand to bridge networks that use overlapping IP addresses, virtual private networks (VPNs), and IPv4 and IPv6 addresses.

SBCs can also mediate between different signaling, transport, and encryption protocols; convert between incompatible codecs; and translate signaling layer telephone numbers, addresses, and response codes.

- **Quality, availability, and SLA assurance.** SBCs play a critical role in assuring session capacity and quality. They perform admission and overload control to ensure that both the network and the service/application infrastructure have the capacity to provide high-quality support for sessions. In IMS networks, they also integrate with standard admission control functions such as the Policy Charging and Rules Function (PCRF) and Resource and Admission Control Sub system (RACS). Additionally, SBCs control the quality of network transport and monitor and report actual session quality to determine compliance with performance specifications set forth in SLAs between service providers and enterprises and their users.

- **Revenue optimization and cost management.** SBCs can help service providers increase revenues and profits by protecting against bandwidth and QoS theft, by routing sessions to minimize costs, and by providing accounting and related mechanisms to maximize the number of billable sessions.
They also help enterprises manage costs by consolidating network infrastructure and increasing the efficiency of bandwidth utilization. Enterprises can leverage SBCs to simplify the introduction of new UC applications that improve business processes, to increase customer satisfaction, or to maintain competitive differentiation.

The Videoconferencing Challenge

The ability to conduct face-to-face virtual meetings without the time, expense, and stress of business travel has made videoconferencing a mission-critical application for both large and small enterprises. Despite wave after wave of price, performance, and feature improvements in videoconferencing solutions, enterprises today still face a wide range of deployment challenges including:

Inter-Company (B2B) Communication Issues

Although an extremely important part of securing a private network, enterprise NAT routers and firewalls often wreak havoc on video communications by...

Blocking all incoming call/session requests

Hiding the network addresses of internal devices

Degrading performance by inspecting each packet that traverses the firewall

There are many ways to circumvent video-related NAT / firewall (FW) issues including:

Disable / avoid the firewall or place the video system in the network DMZ

Forward network ports

Deploy a video-friendly firewall or proxy

Deploy a video bridge with dual network ports

Deploy an H.460 or other NAT / FW traversal solution

Leverage a B2B Video Service Provider

While certainly viable, each of the above options involves security, cost, complexity, managerial, and/or performance compromises such as the need to:

Bypass network security by disabling the firewall, forwarding up to thousands of network ports, or via pin holing (which also involves opening ports) through the firewall.

Assign dedicated public IP addresses to each system, which increases cost, limits scalability, and increases security risk.

Deploy additional hardware or software to provide the enterprise dial plan.

Deploy a video-specific, or even H.323 specific, NAT / firewall solution.

Utilize expensive video bridge resources to circumvent the firewall.

Utilize external services and pay the associated monthly and/or usage-based fees.

In addition, these methods resolve the NAT / FW traversal issues of only one side of the video call. If both enterprises involved in communication have not resolved their NAT / FW issues, the video call will still not connect. Furthermore, these solutions / methods tend to be video-specific, meaning that they do not resolve issues for audio (VoIP), streaming, UC, etc. As a result, enterprises must deploy similar devices for other communication systems, resulting in a series of independent communication silos.

Interoperability Issues

Despite the release of a wide range of videoconferencing standards, enterprises still face interoperability issues, including:

Protocol Interoperability – results from the use of different communication protocols (e.g. SIP, H.323) or video / audio compression (e.g. H.264, H.263, G.722, etc.).

Basic Connectivity – an inability to make a successful basic connection, or a loss of functionality, despite the use of the same communication and compression protocols.

Experience Interoperability – providing a less than optimal user experience based on the devices in use and call speed.

Bandwidth Allocation Issues

Today's enterprise data networks host both non-real-time (email, web browsing, file transfers, etc.) and real-time (VoIP, IP video, video streaming, etc.) data traffic. However, these applications use different network / bandwidth management tools (if any at all). As a result, it is all but impossible for an enterprise to efficiently and effectively allocate available network resources to each application.

Additional Issues

Enterprises also face a variety of additional challenges including:

Complexity – the need to select, install, configure, manage, and maintain infrastructure devices for each isolated communication environment (VoIP, videoconferencing, and other rich media applications) results in an expensive, overly complex environment.
SBCs serve multiple purposes within an IP network by offering a wide range of functions within a single element. For example, an SBC can be used in place of a video proxy server, a NAT / firewall traversal solution, a protocol conversion / transcoding solution, a QoS monitoring / management system, and more. This not only simplifies and drives cost out of the environment by decreasing the number of separate devices that must be purchased and managed, but also eliminates the need (and complexity) for the separate devices to interface and communicate with each other. Unlike protocol and application-specific devices (e.g. video gateways), SBCs are designed to handle and improve the performance of virtually any communication medium ranging from audio (VoIP) and video to instant messaging and streaming. This decreases cost and complexity by allowing an enterprise to deploy a single, centralized set of infrastructure devices to support all communication services.

Security Features
The security functions required for real-time voice and video communications are different from those required for data services. These include the following items addressed by SBCs:
- Access Control - SBCs permit only authorized traffic (based on traffic type, originating and/or destination IP address, or other factors) to traverse the network boundaries.
- NAT / Firewall Traversal - SBCs permit authorized traffic to securely traverse the enterprise firewall without the need for expensive, video-only NAT / firewall traversal solutions.
- Flow-Specific Encryption – SBCs provide encryption on a per-flow basis, allowing each participant to use a different encryption protocol. Participants can even use one type of encryption for signaling, and another for media.
- Denial of Service (DoS) Protection - there are many ways to disrupt IP-based communication services including:
  - Malicious attacks (e.g. implantation flaw attacks, flood attacks, application-level attacks, signaling attacks, media attacks, etc.)
  - Non-intentional issues (configuration issues, BOT searches, interoperability issues forcing frequent resend requests, protocol issues a.k.a. protocol fuzzing, etc.). These DoS threats are already commonplace in the VoIP world, and over time will certainly impact the video world in a similar manner. As communication proxies, SBCs buffer communication devices and networks from DoS attacks and can compensate for / correct a wide range of non-malicious issues that could impact service.

Interoperability Features
SBCs act as back-to-back user agents by making individual connections to each participating device and routing the appropriate traffic to and from each device. This allows the SBC to provide:
- Signaling protocol conversions (e.g. between SIP and H.323)
- Transport protocol conversions (e.g. between TCP and UDP)
- Call signaling normalization to eliminate connectivity issues between vendors
- Protocol mediation / methodology conversion to enable advanced features in multi-vendor environments (e.g. change "refer" to "re-invite" to enable call transfer between Avaya and Cisco systems).
- Security interworking to enable secure communication sessions between platforms that use different forms of encryption (e.g. interworking when one side is using SRTP and other is using RTP).
- Enterprise dial plan normalization to enable successful calling between environments using dissimilar dialing plans (e.g. a call that comes in using an E.164 address can be terminate on one side of the SBC, and then re-initiated using a URI-based dial string).

Inefficiency – the fact that each separate communication environment requires similar network elements (e.g. a gatekeeper for H.323 video, and a SIP server for VoIP) and often dedicated support resources doing similar jobs within parallel environments is inefficient and also expensive.

Manageability – the plethora of modality-specific devices and the need to use separate management systems for each application make it difficult, time consuming, and expensive to manage the enterprise communications environment.

Single-vendor vs. best-of-breed - To avoid interoperability issues, enterprises are often forced to deploy a single-vendor solution, even if that single-vendor solution is not best-of-breed in all areas.

Simplifying and Centralizing Video communication with SBCs
There are many reasons for enterprises to use session border controllers within their videoconferencing environment.

Simplicity and Cost Benefits
SBCs allow enterprises to simplify, centralize, and decrease the costs associated with the communications environment.
Management and Quality Assurance Features

The fact that all enterprise communication sessions flow through SBCs allows these devices to play a primary role in session management and control. Key features include:

Bandwidth management – unlike the protocol / application specific bandwidth management tools used by many enterprises today, SBCs are “session-stateful” and can therefore manage bandwidth independently for each communications session. This allows SBCs to provide enterprise-wide bandwidth management across all communication modalities including video, voice, streaming, etc. – on a connection by connection basis. Additional note – Because SBCs manage communications dialogs on a per-session basis, they can allocate bandwidth based on the user experience during each individual communication session and across all modalities. For example, if a streaming session is not providing the appropriate quality of experience, an SBC could increase the bandwidth allocated to that particular stream WITHOUT increasing the bandwidth used by other streams or applications. This level of granularity allows an enterprise to optimize the use of its bandwidth across its global environment and user base.

SBCs also perform intelligent media management to conserve bandwidth on links where it may be preferable to do so. For users residing on the same network or behind a common firewall, for example, SBCs can “release” the media, allowing it to flow locally between users rather than forcing it upstream, through the SBC and back.

Call admission control – since SBCs are aware of all active communication sessions, they are able to provide enterprise-wide call admission control based on a wide array of rules including bandwidth limits, protocol in use, source / destination IP addresses, and more.

Additional SBC Benefits and Advantages

Best of Breed Approach - Unlike dedicated video or VoIP solutions, SBCs tend to be vendor agnostic and have been designed to work in conjunction with other conferencing / rich media infrastructure devices (e.g. video / audio bridges, scheduling systems, etc.). This allows an organization to deploy a multi-vendor environment consisting of best of breed products and solutions without sacrificing efficiency, security, and interoperability.

SIP Trunking – In addition to the above, SBCs allow enterprises to replace conventional TDM PRI / BRI lines with SIP trunks that can support voice, video, and other multimedia applications. Similarly, SBCs allow organizations currently using SIP trunks for voice to use those same trunks for video. The benefits of SIP trunking include cost savings and increased reach, all without sacrificing enterprise security.

Protecting Internet Boundaries – Enterprises today also leverage the public Internet to integrate mobile and remote employees into the enterprise communications mainstream. The same SBC used for other purposes within the enterprise can also secure the Internet border, encrypt and decrypt communications sessions, block non-conformant or unwanted interactive communications traffic, and enable legitimate video, voice and UC sessions to securely traverse Internet firewalls.

An example of how SBCs can simplify and consolidate enterprise communications is shown in the figure 2 below.

Figure 2 below shows an enterprise communications architecture that routes voice, video and data traffic along three functionally separate paths, sometimes referred to as “silos.” In this scenario, all traffic in and out of the network passes through the enterprise firewall en route to its destination. This is an inefficient use of firewall resources since firewalls are not designed to control interactive communications traffic.

Example:- Videoconferencing sessions (SIP, H.323, RTP, H.239, etc.) are routed through a video-specific gateway/proxy that provides NAT/firewall traversal and connects endpoints to the MCU for multipoint conferences within the enterprise.

VoIP sessions (SIP and RTP) are routed through an existing SBC to the IP PBX.

Data traffic is routed through the enterprise firewall to web application servers and/or servers that deliver other business applications.

In other words, within this architecture, the web/data applications and interactive communications (videoconferencing, VoIP, etc.) are not integrated.

Figure 2 shows the same enterprise, this time with an architecture that reduces cost, simplifies traffic flows and integrates web/data and interactive communications applications without compromising enterprise security or application performance. The converged architecture routes all voice, video and unified communications traffic (SIP, H.323, RTP, H.239) through an SBC, offloading the enterprise firewall from processing the rich media traffic. Web/data traffic is still passed securely and efficiently through the firewall, which is now deployed in parallel with the SBC. The SBC delivers the same functionality as the video gateway/proxy, making that element unnecessary. While every SBC offers some degree of session...
security and control, the advanced features described above allow enterprises to simplify their network architecture, decrease cost, increase scale, and improve overall reliability and performance.

Figure 2 – A “Siloed” Communications Environment

In addition to its vendor-neutral positioning, SBC solutions address many of the issues and concerns address previously in this document including:
- Protection against malware / attackssignaling header manipulation
- Advanced QoS measurement to enable intelligent session routing
- Hardware-accelerated encryption
- SBC virtualization allowing each SBC to be configured as multiple virtual SBCs
- Interworking between IPv4 and IPv6
- Efficiently integrate business processes and applications with unified communications.

References
10. "Understanding Session Border Controllers" (PDF). FRAFOS GmbH.