Compliments of

ribbon

Session Border Controllers

for dummies

A Wiley Brand

Understand why you need SBCs

Save money with SBCs

Maximize cloud security with SBCs

Floyd Earl Smith

7th Ribbon Special Edition

Session Border Controllers

7th Ribbon Special Edition

By Floyd Earl Smith

for dummies®
A Wiley Brand

Session Border Controllers For Dummies®, 7th Ribbon Special Edition

Published by
John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-394-19693-7 (pbk); ISBN: 978-1-394-19694-4 (ebk). Some blank pages in the print version may not be included in the ePDF version.

Publisher’s Acknowledgments

We’re proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Manager and Editor:
Carrie Burchfield-Leighton

Acquisitions Editor: Traci Martin

Sr. Managing Editor: Rev Mengle

Client Account Manager:
Jeremith Coward

Key Ribbon Contributors:
Daniel Teichman, Greg Zweig

Table of Contents

Introduction

In the early days of online communications, many people used phone lines to connect to online services, the Internet, and the web. Today, ironically, a great deal of telephone service is provided over Internet Protocol (IP) networks. And even plain old telephone service (POTS) that uses traditional phone lines may be managed remotely via the Internet.

IP-enabled communications are far more flexible and capable — and operate at lower cost — than the landlines of yesterday. Today's real-time communications no longer just consist of voice calls. They also include team collaboration, video conferencing, instant messaging, presence, and desktop sharing.

Making these applications work together seamlessly requires a signaling protocol, known as Session Initiation Protocol (SIP), which is used to establish communication sessions between parties. As powerful as SIP is, it isn't without challenges. These include differences in implementation between vendors and security concerns involved when transporting communications traffic across the Internet.

A session border controller (SBC) is designed to control real-time communications traversing an enterprise or service provider's IP network. Initially developed as a stand-alone device, SBCs are now also available as software running on commodity servers. SBCs handle all the signaling and media functions, such as interworking and transcoding, required to make SIP-based communications work seamlessly.

About This Book

Session Border Controllers For Dummies, 7th Ribbon Special Edition, is your introduction to the wonderful world of SBCs. This book consists of seven short chapters that explore

- What SBCs are and why they're needed (Chapter 1)
- What else an SBC does in a communications network (Chapter 2)

- How a virtual or cloud-native SBC can benefit enterprises and service providers (Chapter 3)
- SBC use cases and real-world deployment scenarios (Chapter 4)
- How a contact center is dependent on an SBC (Chapter 5)
- How to determine the value and ROI of an SBC (Chapter 6)
- Why your organization needs a Ribbon SBC (Chapter 7)

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out information that you should commit to your non-volatile memory, including important dates.

TIP

The Tip icon points out information that aids in your understanding of a topic or that may save you time, money, or a headache.

WARNING

This information tells you to steer clear of things that may cost you big bucks, are time sinks, or are just poor practice in using an SBC.

Beyond the Book

This book gives you a better understanding of SBCs, but if you're left wanting more, visit the Ribbon website at `www.rbbn.com`. There you can learn more about how Ribbon's expertise helps customers deploy, manage, and optimize their SBCs.

IN THIS CHAPTER

- » **Understanding the role of the SBC in real-time communications**
- » **Recognizing why enterprises and service providers need SBCs**

Chapter 1 Protecting Real-Time Communications with SBCs

Real-time communications in modern businesses include phone calls, video conferencing, chat, text messaging, desktop sharing, and team collaboration. In this chapter, you learn how a session border controller (SBC) enables and secures enterprise and service provider real-time communication infrastructure and services.

Looking at the SBC’s Role

An SBC secures and controls real-time communications by admitting end devices to the session (or not admitting them, as needed), and then directing communications between the end devices and any intermediate devices on the network. Common examples are a Voice over IP (VoIP) call between two phones or a video conference that connects multiple devices.

SBCs are deployed at the network perimeter (that is, at the network's border) so that they can control and secure real-time communications for both enterprises and service providers. An SBC performs the following functions:

- **Securing the real-time communications network:** An SBC protects and secures real-time communications from various threats such as spoofing, distributed denial-of-service (DDoS) attacks, and toll fraud. The SBC secures real-time communications by
  - Acting as a back-to-back user agent (B2BUA), which allows the SBC to hide the topology of the internal Internet Protocol (IP) network, making it difficult or impossible for bad actors to gain access to potentially vulnerable parts of the network
  - Encrypting both signaling and media to maintain privacy and prevent communications from being illegally intercepted or tampered with
  - Detecting and preventing DDoS attacks so that they don't impair network and service performance
  - Enabling call admission control and dynamic blocking of rogue endpoints to avoid telephony denial-of-service (TDoS) threats and toll fraud

  REMEMBER

  Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, modifying, and terminating real-time communication sessions between IP devices. Real-time Transport Protocol (RTP) is a network standard designed for transmitting real-time voice or video across IP networks.
- **Enabling SIP trunking:** An SBC provides a demarcation or termination point of the SIP and RTP connection (often referred to as a SIP trunk) into a communications network. An SBC provides the security, interoperability, and some of the intelligence (for example, where to route SIP calls) needed to safely connect SIP trunks with your network. The SIP service provider also needs an SBC on its side of the SIP trunk to protect its network. You can think of an SBC as providing a SIP firewall that includes a host of value-added services such as intelligent routing controls, signaling and media interworking, resiliency, and the ability to ensure a high quality of service between different network devices.

TIP

Savings from SIP trunking, trunking consolidation, and the move to VoIP and unified communications (UC) can reduce traditional enterprise telecom bills by up to 75 percent, with higher quality of service. Additionally, the SBC can provide secured access to SIP trunking services, so an enterprise can maintain security while saving money.

- **Interconnecting and interworking networks and protocols:** An SBC provides a smooth experience in terms of interconnecting and interworking between different networks and the protocols running over them. Specifically, the SBC performs tasks such as
  - **Dealing with SIP variants:** When SIP was developed and standardized, a lot of flexibility still existed in how specific parameters could be used and populated. This means that SIP has a lot of variants based on different vendor implementations. An SBC can translate these variants between devices (a process known as *SIP normalization,* covered in more detail in Chapter 2) so that calls go through with all their features intact.
  - **Translating protocols:** Different UC solutions may utilize different audio codecs and other protocols that aren't completely supported on both sides of the session. The SBC knows all these protocols and can translate or transcode between them on the fly.
- **Acting as session traffic cop:** The SBC is the gatekeeper to SIP-based services in an enterprise or service provider network. In this role, SBCs perform session admission control, which is the process of determining who has access to the network. This makes the SBC the traffic cop of a SIP network, keeping your SIP highways safe and orderly and creating and accessing three lists: allow lists, block lists, and grey lists (discussed in the later section, "Understanding the Need for SBCs" in this chapter).
- **Intelligent routing and policy controls:** In larger deployments, where multiple SBCs are installed at multiple network connectivity points, the task of individually configuring routing and policies on all SBCs can be tedious and expensive. An alternative to localized policy control is further centralization using a primary policy server to dynamically propagate a single set of routing and policy rules to each SBC on the network.

WARNING

Alternatives to SBCs include virtual private network (VPN) tunnels and firewalls, but each of these alternatives has some disadvantages:

- **VPN tunnels:** A VPN can cause trouble when there's a need to look inside the packets encapsulated in the VPN to route calls and provide services. To enable this, VoIP packets must be decrypted and acted on — removing the end-to-end encryption element that keeps a VPN secure.
- **Firewalls:** A firewall can be configured to allow VoIP traffic to pass through the network to client devices within the network. The problem is that VoIP (and UC) sessions are exceedingly dynamic. Sessions are set up and torn down frequently and in large numbers. Additional services are often added during the middle of a call (for example, when someone begins to instant message another user during a conference call, or when someone shares a picture or video during a voice call). Typically, a firewall just isn't capable of handling this kind of dynamic service provisioning.

Understanding the Need for SBCs

SBCs were initially deployed within service provider networks. SBCs ensure that

- Real-time communication traffic is properly routed between network providers.
- Differing protocols are understood so that the call can be delivered across different networks.
- Calls are secure.

As time-division multiplexing (TDM) PBXs and contact centers have been replaced by IP-based platforms — and, more recently, by cloud-based services — VoIP adoption has become more common in the enterprise, and SBCs have been increasingly deployed at the border between an enterprise's network and the carrier's network. The first driver of SBC implementation within real-time communication networks is security.

VoIP (as well as other session-oriented applications) is an application that, by its very nature, is exposed to devices and networks that are beyond the control of an enterprise or a network provider. VoIP isn't like traditional telephony in which a very highly circumscribed set of devices, protocols, and private networks was involved in the process of placing and carrying calls. In the old days when you placed a phone call, the call was placed on an approved device and carried across the phone company's private network.

REMEMBER

Like other IP applications, VoIP can be carried over one or more public networks. Calls can be initiated or completed on devices, such as personal computers (PCs) or smartphones, using VoIP applications that aren't under the control and regulation of an enterprise or the phone company. While this enables new features, greater flexibility, and lower costs, it also makes the VoIP world considerably more vulnerable, broadening the attack surface to the same kinds of security threats as any other Internet service.

WARNING

Many hackers consider telephony of all kinds fair game for disruption. Steve Jobs and Steve Wozniak, for instance, were involved in "phone phreaking" before they founded Apple in 1976. Service providers are likely to face talented and determined hackers, so robust effort and constant vigilance are a requirement.

Some common VoIP attacks include

- **Service theft and fraud:** Attackers accessing a VoIP system to fraudulently make calls and use network resources without paying for them
- **Spoofing:** Deliberately modifying or disguising an identity (for example, caller ID) on the network
- **DDoS/TDoS attacks:** Flooding a network server or SBC with requests to overwhelm its available resources — a common way to attack and disrupt contact centers
- **Registration storms:** Like a DDoS attack, in which many simulated devices (typically hundreds of thousands to millions) simultaneously attempt to register with a SIP server in a UC network to overwhelm its available resources

An SBC employs various techniques to protect enterprises and service providers from cyberattacks against their real-time communication networks, including the following:

- **Support for media and signaling encryption:** Encryption prevents unauthorized parties from eavesdropping on real-time communications or tampering with a call. Encryption also provides an authentication mechanism to verify that a client is who they say they are. The signaling component of real-time communications is typically secured by Transport Layer Security (TLS) or IP Security (IPsec), while the media layer is secured by Secure Real-time Transport Protocol (SRTP).
- **Dynamic pinholing:** A pinhole is a port opened in a firewall to allow an application to access the IP network. Leaving a port open for an extended period can potentially enable a security breach. SBCs programmatically create pinholes and leave them open for only the short period that a session is active to minimize security exposure. At the end of a session — for example, a voice call — the SBC will close the pinhole. SBCs can then reopen ports as needed to allow trusted applications to send and receive data.
- **Topology hiding with B2BUA:** A B2BUA controls SIP calls by a logical or virtual proxy configured for the call. This agent sets up the pathways across the network for both signaling and media. B2BUA causes all signal and media traffic to run through the SBC and hides the topology, or architecture, of the network so clients aren't shown private IP addresses of servers and devices in the network. The result is a network that's easily accessible to clients for making and receiving calls but whose "innards" are effectively invisible, which makes them less vulnerable to attack.
- **List monitoring:** The SBC's policy management function monitors incoming requests and calls, using rules to identify devices, referred to as *endpoints,* which are and aren't abusing network resources, and maintains certain lists including
  - **Allow lists:** Devices that *always* have access to the network
  - **Block lists:** Devices that *never* have access to the network
  - **Grey lists:** Devices that *sometimes* have access to the network

IPv6 HAS ARRIVED

The IP variant (IPv4) that powered the Internet for many years started to have an issue. IPv4 used a 32-bit address space, which meant that it was limited to only about 4.3 billion addresses — and it ran out of available addresses in 2015.

IPv6, introduced in 2012, increased the address space to 128 bits, which meant that there were 340,282,366,920,938, 463,374,607,431,768,211,456 possible addresses (that’s 340 undecillion, 282 decillion, 366 nonillion, 920 octillion, 938 septillion, 463 sextillion, 463 quintillion, 374 quadrillion, 607 trillion, 431 billion, 768 million, 211 thousand and 456 — seriously).

The move to IPv6 caused other issues. For example, not all networks were configured to support IPv6. When two clients wanted to communicate, and one was on an IPv4 network and the other on IPv6, something needed to be placed in the middle to help them communicate. An SBC serves this purpose. It resolves these issues in two ways:

- An SBC can be dual stacked, meaning it contains the network stack software (the basic network protocol software suite) for both IPv4 and IPv6. The SBC can communicate using both versions of IP; for instance, it can connect to an IPv6-only smartphone using IPv6 while connecting to an IPv4 server using IPv4.
- The SBC can act as an interworking agent between an IPv4 network and an IPv6 network. In this case, the SBC can translate all traffic flowing between an IPv4 and an IPv6 network on the fly, as it crosses the network border.

IN THIS CHAPTER

- **Understanding SIP and call transcoding**
- **Translating NAT traversal**
- **Learning the facts about fax and tone detection**
- **Supporting video**
- **Ensuring performance, scalability, and resiliency in an SBC**

Chapter 2 Identifying the Key Requirements of an SBC

A session border controller (SBC) does much more than just provide security. In fact, many in the telecommunications industry say that it's the security that gets customers interested, but it's the other functionality in an SBC that makes the sale. This other functionality is all about SBCs making Voice over Internet Protocol (VoIP) calls and real-time communications (RTC) work in situations where they otherwise might not work. And, beyond that, SBCs simply make VoIP and RTC services work better.

In this chapter, you find out about all the other essential functions of an SBC.

Normalizing SIP

Session Initiation Protocol (SIP) is the primary protocol that establishes the connection between two endpoints and terminates the connection when the call is finished. At the most basic level, SIP is the VoIP equivalent of the dialing tones that directed old-fashioned analog calls to the right switches and across phone networks. SIP is the common language that telecom providers and equipment makers use to communicate with each other.

SIP is a communications standard drafted by the Internet Engineering Task Force (IETF) in the late 1990s. The standard, however, is more of a series of recommendations and suggestions on how SIP should be implemented than a conclusive specification. The actual SIP implementations are left up to individual engineers and vendors, resulting in SIP variations that are technically in compliance with the published SIP standards but not necessarily interoperable with one another.

Enough variations exist in SIP that sometimes two systems connecting to each other using SIP find that they aren't speaking the same language — the basics are all there but with differing syntax and dialects in what otherwise appears to be a common language (kind of like American English versus British English). There's just enough difference to cause confusion. When two people are talking, such confusion can be overcome by context or by a simple "huh?" But when two devices are talking, that simply isn't going to happen.

REMEMBER

An SBC must be able to speak all the different dialects of SIP and do on-the-fly translations in both directions. So, if a call is crossing a border between a system using Dialect X and another system using Dialect Y, the SBC must find the parts of Dialect X and Y that don't quite match up and convert them back and forth as the call moves across the SBC. It's not rocket science in concept, but it's hard to do, especially within milliseconds; the best SBCs make the whole process transparent and seamless.

Transcoding Calls

Another of the SBC's jobs is to transcode, or change, codecs as media sessions pass through the SBC. The SBC knows which codecs are supported on each side of the network border and is required to decode and then re-encode the voice or video signal as it crosses the network border by using a combination of specialized software or special-purpose digital signal processors (DSPs).

Many codecs — the encode/decode algorithms that compress voice and other signals, such as video streaming across the network in a videoconferencing environment — are in use in various VoIP and unified communications (UC) systems. Low-bandwidth and high-bandwidth video and voice codecs are designed to work on various devices, such as

- Computers and tablets
- Dedicated VoIP phones
- Mobile smartphones

In a VoIP call (or any real-time, session-based communication, for that matter), there are often differing capabilities to support codecs. So if an enterprise's private branch exchange (PBX) or contact center supports one specific codec and an incoming call is using a different codec, the SBC will understand both codecs and transcode between the two codec types in real time and in both directions as the call passes through it. However, some codecs may not be implemented on a device, for a few reasons:

- The developers haven't gotten around to it yet.
- The software licensing fee is too high.
- The device has a relatively "slow" CPU and can't handle the codec computationally.

Transcoding in SBCs frequently comes into play in two specific instances; both are covered in this section.

HD voice

The sound quality of voice calls in general took a step backward over the years as convenience (mobile phones) and economics (VoIP) drove the replacement of traditional landline phones with a range of new devices. However, high-definition (HD) voice reversed that trend. HD voice can reproduce a greater range of frequencies at higher clarity by using wideband codecs rather than traditional narrowband codecs (so called because they cut off both the top and bottom frequencies found in a person's voice). You may have heard the effects of this firsthand because many popular cloud-based collaboration tools such as Teams, Zoom, Webex, and so on use wideband codecs.

WARNING

There's a gotcha to HD voice: There's no single codec used by every HD voice-capable system. However, having an appropriate SBC — one with robust transcoding capabilities — in the middle of the call solves the problem. The SBC can transcode and keep the call HD all the way, but a lot of software and/or hardware are doing some heavy lifting behind the scenes.

Bandwidth restrictions

Sometimes a call is made to someone who's connected to an older mobile network with poor infrastructure. Other times, a call is made to a person in a home office or a hotel with a limited Wi-Fi connection. To address these bandwidth restrictions, codecs that trade fidelity and audio/video quality for greater compression are available, and they use less bandwidth.

Users may not want to default to these low-fidelity codecs all the time, but sometimes they're necessary over at least part of the call's path. An SBC sitting between network segments can recognize this situation and transcode to and from lower-bandwidth codecs when required. This situation is much better than relying on the VoIP clients themselves to do this kind of calculation upfront, especially because not all clients support all codecs.

Dealing with NAT Traversal

Network Address Translation (NAT) converts a public IP address to a private, non-routable IP address. NAT is used because there aren't enough public IP addresses available in the world to assign every device its own unique IP address.

REMEMBER

Internet Protocol version 6 (IPv6) is the newer IP address schema that will eventually replace traditional IPv4 addresses. IPv6 increases the number of available IP addresses and reduces the need for NAT. The gradual adoption of IPv6 is another reason to use an SBC, because the SBC has intelligence that enables IPv4 and IPv6 network segments to talk to each other. See Chapter 1 to find out more about IPv6.

The challenge with NAT is that creating an end-to-end session is difficult because the IP address of a device using NAT isn't a public, routable IP address. This creates issues with end-to-end sessions, like VoIP, and requires some translation to happen between public and private addresses — translation beyond what a network router can do.

Many SBCs explicitly support what's known as NAT traversal, providing the ability to work with VoIP session packets and giving them the instructions they need to get through the NAT router and to the actual device that's at the other end of the session. NAT traversal requires a significant amount of processing power in the SBC because of the large number of devices participating in VoIP and other sessions that may be located behind a NAT gateway.

Fax and Tone Detection

Legacy technologies sometimes linger on well past their "sell by" date — and the network needs to support them. A prominent example is facsimile (fax) technology. There are still people out there (in areas such as medicine, law, and real estate) using fax machines every single day of the week. VoIP systems would, if they could form opinions, probably be opposed to this, but the reality remains.

An SBC, however, can come to the rescue here by incorporating tone detection (the ability to recognize and act on standard analog telephone touch tones) to recognize and then properly route that awful screech that precedes a fax.

Performance, Scalability, Resiliency

SBCs need to be powerful and robust, with the capacity and redundancy not only to handle the average number of calls coming through the system simultaneously but also to scale up and handle peak loads. This is especially critical for contact centers, where every call can equate to a sale or improve customer satisfaction. When evaluating an SBC's performance, scalability, and resiliency, consider the following factors:

- **CPU utilization:** The SBC does a lot of computationally complex work, such as SIP translation, intelligent routing, centralized call recording (SIPRec), and other functions in real time. CPU utilization during both normal and peak periods should allow for sufficient overhead.

- **Concurrent calls (or sessions) supported:** How many concurrent calls is the SBC rated for, and how does this match your network's usage patterns? If your usage grows and begins to exceed the capacity of your SBC, what are your upgrade options?
- **Redundancy:** Put a different way, this means "avoiding single points of failure." SBCs perform a mission-critical role for enterprises and service providers, so you need to know what your redundancy options are and which of those options will work best for your needs.
- **Registration rate:** How many clients can the SBC register in a fixed period? When a lot of users are connecting at once, make sure that the SBC can handle it.
- **QoS policies:** The QoS policy of a network and prioritization of data flows are implemented by the SBC. QoS policies perform such functions as traffic policing, resource allocation, rate limiting, and call admission control (CAC).

IN THIS CHAPTER

- **Defining the virtual SBC**
- **Recognizing the key functions and benefits of a cloud-native SBC**

Chapter 3
Virtualization and Cloud-Native SBC

n this chapter, you learn how virtualization and cloud-native design work and how your organization can benefit from a virtual or cloud-native session border controller (SBC).

Defining a Virtual SBC

Virtualization abstracts software (such as an operating system and installed applications) from the underlying physical hardware on which the software is running. Server virtualization is perhaps the most well-known and widely implemented virtualization technology. But wait, there's more! Other common types of virtualization include

- Application virtualization
- Desktop virtualization
- Storage virtualization
- Network virtualization

Communications systems use virtualization in the design, deployment, and management of network services by separating network functions from hardware devices. This process removes the need for you to purchase dedicated hardware such as routers, firewalls, and SBCs, among others.

A virtual SBC is an SBC implemented entirely in software that can be deployed on commercial, off-the-shelf servers. In many cases, the core of the SBC software is the same code that executes in a hardware-based SBC. However, because the virtual SBC is implemented in software, it can be easily deployed on virtual machines in an on-premises data center, or in a private or public cloud.

TIP

Some of the benefits of virtualization include

- **Efficient resource utilization:** Before virtualization, many data centers used about 10 percent of their total capacity, meaning that nearly 90 percent of their capacity went unused. Virtualization enables organizations to run multiple virtual workloads on a single physical host server, maximizing the utilization of resources such as compute, memory, and storage.
- **Reduced operating expenses:** The cost of rack space, power, cooling, and network connectivity in a data center is incrementally higher for each physical server or appliance that's deployed. Virtualization enables SBCs and/or other applications or network functions to be deployed on a single physical server, thereby reducing costs to the organization.
- **Low total cost of ownership (TCO):** Virtual SBCs provide a much lower TCO than hardware-based SBCs because they run on less expensive, off-the-shelf server hardware. Virtual SBCs also support a pay-as-you-grow model, meaning that businesses don't have to pay for system capacity that isn't yet needed.
- **Faster time to market:** Virtual SBCs allow service providers to deploy new network services very quickly to support changing requirements and seize market opportunities as they arise. This flexibility also reduces risks associated with rolling out new services because service providers can easily try out and modify new service offerings to meet the needs of their customers.

- **Greater agility:** Service providers must be able to quickly scale their services up or down to meet changing market demands. They also need to innovate quickly and get those innovations to market as quickly and easily as possible. Virtual SBCs allow for services to be delivered to customers on private or public clouds to achieve greater agility.

Discovering a Cloud-Native SBC

Virtualization is a key enabling technology for software-only SBCs, but to truly leverage the cloud means going beyond virtualization to adopt cloud-native design and operational principles. A cloud-native SBC

- Takes advantage of microservices design, containers, and automated life cycle management
- Leverages automation, enabling rapid provisioning
- Is characterized by its elasticity — its ability to auto-scale on demand
- Has efficient and reliable resource allocation
- Delivers performance at scale
- Has integration based on open APIs and participates in an open telemetry observability framework
- Can be incorporated into flexible, subscription-based licensing models

When choosing a cloud-native SBC, look for the following important capabilities and features:

- **Run-time-ready instantiation:** Deploying real-time communications in the cloud requires the ability to instantiate an SBC application as rapidly as the real-time service itself. To achieve this level of responsiveness, the SBC needs to be designed using microservices, each of which is instantiated as a separate workload — that is, as a set of computing resources that are required to run the microservice. These workloads are packaged using containers and managed using automated life cycle management software such as Kubernetes.

The result of being run-time ready is service velocity with operational efficiency, because it's possible to instantiate a running, configured SBC that's immediately capable of call processing without the need for operator intervention.

- **Elasticity (auto-scaling):** The advantage of a cloud-native environment is the ease, speed, and ultimately cost-effectiveness with which an SBC can be auto-scaled. With automated life cycle management, provided by Kubernetes, SBC workload scaling can match traffic demand in real time. This rapid scale-up/scale-down functionality is the very essence of elasticity.

  Achieving elasticity also means that instantiation is optimized for both horizontal scaling (adding more workloads) and vertical scaling (adding more capacity or performance within a workload).

- **Optimal load balancing:** Load balancing is the mechanism that optimizes resource utilization, ensuring that traffic is evenly balanced across multiple service instances, in alignment with the dynamic traffic load. With load balancing, variances in traffic are optimized across aggregate capacity; as a result, solution resiliency is increased by avoiding server overload situations that could potentially cause processing failures. Furthermore, traffic will be rebalanced automatically in the event of a workload failure.

  For the SBC application, load balancing must have knowledge of session persistence and the performance status of each workload.

- **Resiliency and high availability:** Certain attributes of an SBC are considered table stakes for deployment. Resiliency and high availability (HA) fit this designation. One goal of a cloud-native design based on microservices is to be able to exceed the fault tolerance that was found in more traditional hardware deployments but to do so without the overhead of multiple hardware platforms. In a cloud-native design, it's possible to support many different redundancy options. For example, this would include active–active configurations, N:1 (this is "N" active nodes backed up by "1" standby node), and N:M (this is "N" active nodes backed up by "M" standby nodes) configurations. A high-availability implementation can maintain session and media continuity in the event of the failure of any workload.

- **Performance at scale:** Performance at scale gets to the very heart of how an ideal SBC is designed and why moving SBCs to a cloud-native deployment model, rather than using traditional, proprietary hardware devices, is imperative. The cloud-native deployment model, based on microservices and containers, makes it possible to enable (turn on) feature capabilities such as encryption, interworking for IPv4 to IPv6 or for Real-time Transport Protocol (RTP) to Secure Real-time Transport Protocol (SRTP), and SIP header manipulation, while also ensuring that they have no impact on overall session performance. For example, call control functions scale based on the rate of calls per second, which is a very different measure than how a transcoding service needs to scale, based on packets per second. Scaling performance for specific microservices also means that a cloud-native SBC is capable of handling sustained denial-of-service (DoS) attacks or registration floods without negative impact on call performance or call quality.
- **Open APIs and integration with an observability framework:** Network functions such as an SBC don't work in a vacuum; they're part of an overall network infrastructure to secure and ensure the delivery of real-time communications. As such, they need to fit into the management infrastructure that an enterprise or service provider has in place. For a cloud-native SBC, this means support for open APIs and integration with an open telemetry-based observability framework.

  Integration for monitoring metrics and logs, and interfacing with open source/third-party tools such as Prometheus and EFK (Elasticsearch, Fluentd, and Kibana), reduces the friction for seamlessly fitting into a framework that is common across multiple cloud-native applications or workloads. For example, while resource utilization statistics are commonly used for life cycle management and load balancing, visibility to them can also be used for capacity planning across all resources in a cloud deployment.
- **Subscription-based, network-wide licensing:** A subscription-based licensing model is appropriate for virtual and cloud-native deployments. Instead of traditional licensing that was typically coupled with a system's capacity, a subscription-based licensing model aligns with the dynamic usage of resources. By extension, licenses need to be available on a network-wide basis because virtual or cloud-native deployments remove the construct of a license tied to a physical device or location.

IN THIS CHAPTER

- » **Supporting unified communications**
- » **Connecting the enterprise**
- » **Securing mobile communications**
- » **Enabling WebRTC**
- » **Improving the contact center experience**

Chapter 4 Deploying SBCs for Different Use Cases

Session border controllers (SBCs) play a role in many different types of environments and use cases such as unified communications (UC), Session Initiation Protocol (SIP) trunking, mobile and IP multimedia subsystem (IMS) networks, interworking with web real-time communications (WebRTC), and contact centers. In this chapter, you discover the unique requirements and challenges for each of these use cases.

Unified Communications

Gone are the days when enterprise communications meant a phone on every employee's desk. Today's employees expect rich, seamless collaboration from almost any desktop or mobile device. Enterprises need to harness the power of unified communications (UC) and the flexibility of bring your own device (BYOD) policies to increase employee productivity, reduce costs, and improve customer service.

Chief information officers (CIOs) are looking to UC and cloud-based services to meet the rising demand for real-time communications, yet a common barrier to UC adoption is a lack of interoperability between the vendor-specific voice, video, and messaging systems that exist in most enterprise networks.

While SIP was meant to break down many of those barriers, even SIP-based systems face issues, and they often require significant interworking and transcoding to provide acceptable levels of interoperability. Thus, most enterprises fall short of a truly unified model of communications and collaboration, potentially limiting the ability of users to easily and consistently consume rich media services.

The road to UC has been paved with wasted time and money: time spent on long service engagements and endless interoperability testing, and money spent on private branch exchange (PBX) upgrades and new equipment. But an SBC can provide a session management framework for UC and SIP communications that coordinates PBXs, room-based videoconferencing, and business collaboration tools across a wide variety of IP devices (smartphones, tablets, and so on), so enterprises can more easily integrate and create a true UC environment.

TIP

As you move more services and applications into the cloud, SBC-based session management unites cloud-based services with your existing on premises-based enterprise communications to ensure a rich, easy-to-manage UC experience.

Enterprise Connectivity

Deployment of SBCs in enterprises is becoming more common as businesses replace legacy PBXs and on-premises contact centers with cloud-based services such as Microsoft Teams, Zoom Phone, Cisco Webex, Genesys Cloud, Five9, NICE CXone, and dozens of similar services. For an enterprise, the SBC is the first line of defense between its telecom provider and its cloud-based collaboration system, providing cost-effective and secure connections across enterprise networks and branch offices.

In addition, enterprises in various industries must comply with regulatory requirements such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and industry standards such as the Payment Card Industry's Data Security Standards (PCI DSS). Enterprises must maintain the highest levels of security to protect their customers' information and maintain regulatory compliance.

Many companies also have branch offices and a mobile or virtual workforce that add to the requirement for reliable and secure communications. In all these areas, the SBC has an important role.

In the enterprise, SBCs provide connectivity, ensure quality of service (QoS), perform prioritization of emergency 911 call routing, enable call recording, and produce call detail records for accounting. SBCs may also provide gateway functionality (connecting analog devices or primary rate interface [PRI] trunks), VoIP mediation, access to public switched telephone networks (PSTNs), and survivability features for the enterprise. The SBC is the secure boundary between the enterprise and service provider networks.

SBCs in the enterprise can be implemented in various deployment options. SBCs can be hardware-based appliances or software-only virtualized or cloud-native solutions, enabling deployment in a data center or in private or public clouds.

Mobile

Real-time communications has changed rapidly from home and office landline phones to widespread use of mobile smartphones. An increasing number of homes no longer even have landline phones, and a growing number of businesses are replacing their landline phones and even IP phones with mobile devices.

WARNING

The proliferation of mobile devices introduces some new scalability and security challenges into a real-time communications architecture. From a scalability standpoint, there are concerns related to the growth of video traffic over the mobile network and the video traffic's volatility. There are also challenges for mobile operators associated with the increased signaling impacts of these devices and associated messaging and presence applications that are common to these devices. A design challenge for the SBC is the impact of mobile devices on the signaling plane of the SBC. Mobile sessions are typically shorter in duration than other device sessions, but the signaling requirements of these devices translate into more concurrent sessions that an SBC must support.

In most countries, mobile data communications are handled by systems in 4G or increasingly in 5G networks. These systems allow for the latest in high-speed data for mobile phones and other mobile devices for streaming video, data from Internet applications, social media, and streaming music services (such as Pandora and Spotify).

4G and 5G networks only support IP packet switching, meaning that network links are shared by packets from multiple communications sessions. In a 4G network, mobile industry standards have settled on the approach of using voice over long term evolution (VoLTE) for delivering voice as a data stream within the LTE data transmission. Similarly, in a 5G network, this same approach leverages voice over new radio (VoNR), which leverages an IP multimedia subsystem (IMS) framework that enables voice and data transmission.

IP Multimedia Subsystem (IMS) Networks

IMS is an integrated framework for telecommunications providers to deliver voice, video, and data using the IP protocol. VoLTE and VoNR standards are based on using IMS for providing voice services over 4G and 5G networks. IMS doesn't specify an SBC in its architecture, but many IMS functions are already inherent in SBCs.

SBCs are the right place to perform the following IMS functions:

- **Proxy-call session control function (P-CSCF):** This provides an entry point into the IMS subsystem from user endpoints. An SBC integrates the P-CSCF with the access border gateway function (A-BGF) to handle the media and signaling data appropriately. The SBC provides capabilities such as network address translation (NAT)/firewall traversal, user identity privacy, encryption, and policy management.
- **Access transfer control function (ATCF) and access transfer gateway (ATGW):** The ATCF and ATGW functions ensure that the handoff of the call doesn't introduce an unacceptable interruption of media flow.

- **Interconnect border control/gateway function (I-BCF/ I-BGF):** Handles the signaling and media of calls. An interconnect SBC performs functions such as network topology hiding, monitoring and lawful intercept, routing of signaling into the core of the IMS, and policy management on a per-trunk basis.

WebRTC

WebRTC is a technology that allows end-users to access phone, video, or texting capability right from a web page and also to share screens (have multiple users see the screen of one user at the same time). The SBC plays an important role in WebRTC, including

- **Enterprise security:** Because WebRTC applications run in a browser and typically transmit application data across the Internet, a risk of attacks on enterprise servers does exist. Consider a case in which a customer initiates a support services call from a WebRTC-enabled web page. If an SBC is placed between the WebRTC application server and the SIP network at the contact center, it can secure the SIP network in the contact center. The SBC can also provide session control and management between the WebRTC server and the SIP server at the contact center.
- **VoIP phone calls:** In this scenario, consider a VoIP call from a WebRTC-enabled web page to a VoIP phone. The SBC provides
  - Security between the WebRTC application server and the SIP network
  - Session control
  - Transcoding between, for example, Opus (the default codec for WebRTC) and G.729 telephony protocols
- **PSTN phone calls:** In this scenario, consider a call from a WebRTC-enabled web page to a landline phone on a PSTN. The SBC provides
  - Security between the WebRTC application server and the TDM gateway
  - Transcoding and internetworking between the WebRTC application server and the TDM network

- **Video support:** Consider a WebRTC-enabled web page initiating a video chat with a non-WebRTC-enabled IP video phone. The SBC provides
  - Transcoding between the VP8 and H.264 video conference codecs, the WebRTC application server, and the IP video phone
  - Protocol internetworking between IPv6 and IPv4, Real-time Transport Protocol (RTP), and Secure RTP (SRTP) for video media transfer
  - QoS and policy control, ensuring that the real-time media data get network priority
- **Lawful intercept:** The SBC supports SIP recording (SIPRec) for lawful intercept of both signaling and media data transferred between the WebRTC server and the destination IP phone.

Contact Center

The contact center brings together the challenges faced by other use cases for SBCs. The contact center is often among the most important functions a business has, and both employee and end-user expectations are high.

Due to the importance of the requirements for both security and quality of service in this crucial function, Chapter 5 is completely dedicated to the role of SBCs in contact centers. Head over there to find out more.

IN THIS CHAPTER

- » Understanding the unique needs of contact centers
- » Improving the contact center experience

Chapter 5 Exploring the Contact Center

In this chapter, you learn how the contact center has evolved into a critical point of, well, contact between a business and its current and future customers. You also discover how a session border controller (SBC) can help address the critical real-time communication challenges the contact center poses to an organization.

Identifying Contact Center Needs

The contact center has evolved from a voice-only call center to an omnichannel experience where agents handle voice, email, chat, text messages, and video calls. However, as much as multichannel is the norm, voice remains the dominant channel between agent and customer.

Regardless of the interaction channel, the contact center is vital to the success of many businesses because it's often the most important point of interaction between a business and its current and future customers. If agents aren't available or the quality of communications is poor for sales situations, prospects will simply hang up and try another company. If support is needed, customers who have a poor experience are likely to form a poor opinion of the company, negatively affecting future purchases. Customers may also create negative online reviews and say negative things to work colleagues, friends, and family about the company and its offerings.

There are few places in businesses where the value of customer interactions is so easy to measure. The value of a completed sale, the number of transactions per minute, and customer satisfaction metrics can all be measured and tied back to contact center performance. It's no wonder that organizations are willing to spend aggressively to ensure that their contact centers are always available and offer the best experience possible.

SBCs play a crucial role in the contact center experience because they're the first point of entry for telecom services. First and foremost, they have to be ultra-reliable, because a failure would risk a reduction in sales revenue or lower customer satisfaction. SBCs also have to thwart telephony denial-of-service (TDoS) attacks that try to block access by overloading the contact center with fake calls, preventing legitimate calls from getting through. SBCs may also be called on to reroute traffic if a contact center is overloaded, or to move traffic based on time of day.

Using an SBC to Improve Efficiency

Contact center efficiency is crucial to customer experience, so agent productivity, security, and quality control are increasingly important. An SBC can add value in these areas:

- **Call recording:** Contact center managers use call recording as an evaluation and training tool to ensure that contact center agents provide the highest level of quality in customer service. Additionally, in certain applications, government regulations require calls to be recorded for legal reasons and for consumer protection.

  Traditionally, call recording in communications networks was done by consuming an extra data port on a switch to replicate the call data to the recording system. Consuming an extra data port to record calls doesn't scale well in many contact centers that need to record each call that comes into the system. Instead, an SBC simply replicates the call session to send the signaling (SIP) and media (RTP) to the recording system, providing reliable data transfer and freeing up data ports to allow more incoming calls from customers.

- **Security for remote agents:** Remote or work-at-home agents enable contact centers to be flexible and scale up or down as business requires without the added expense of office space and facility expansion. Consider, for example, a retailer that sees dramatically higher sales during the holiday season. This retailer can add temporary remote agents to handle peak demand periods. Mobile technology allows workers to work out of their homes with flexible hours, making this arrangement appealing to workers.

  WARNING

  Remote agent configurations do, however, present some challenges for the contact center. Contact centers require a scalable solution in which devices don't need to be configured and agents don't need to use a virtual private network (VPN; see Chapter 1). Security is also an important factor with remote agent configurations because sensitive customer data is exchanged over the network during these interactions. An SBC eliminates the need for a VPN with IP phones, yet still provides the necessary security (see Chapter 1).

- **Internal transfers:** In many cases, calls need to be transferred to a different agent in another contact center within the organization. This can often lead to higher costs and increased security risks if these transfers must traverse public networks. SBCs can identify internal transfers and route the call appropriately to ensure that it stays on the private network, avoiding the additional costs and security risks inherent with traversing public networks.

  One case to consider is a video kiosk in a store where a customer can make a video call to ask for assistance — a call that's routed from a contact center to a remote agent. In a non-SBC environment, this setup is complicated because both voice and video data could travel across multiple networks, requiring each border traversal to be secured. An SBC provides the necessary security, call routing, and load balancing features to make this type of transfer secure and cost efficient.

IN THIS CHAPTER

- Implementing intelligent routing policies
- Managing policy from one pane of glass
- Ensuring availability to critical systems
- Doing more with less (devices)
- Lowering costs

Chapter 6 Determining the Value and ROI of an SBC

You're all hyped up. You've done your research, and you know the benefits (Chapter 1) and services (Chapter 2) you can get from a session border controller (SBC). Now it's time to pitch the investment to your chief financial officer (CFO — who may also be known as your CF-No).

While an SBC doesn't require a massive investment, if your CFO sees a new line item in your budget, they're going to want some serious justification. You need to be prepared to demonstrate the value of an SBC for your organization and estimate the return on investment (ROI). In this chapter, I help you teach your CFO a new word: "Yes" — because while SBC means *session border controller* to you, it'll mean savings beyond compare to your CFO.

Reducing Costs with Intelligent Policies

The robust policy engine in an SBC enables enterprises and service providers to implement intelligent routing policies that can save hundreds of thousands or even millions of dollars annually in toll charges — for example, by routing calls onto least-cost network paths, and by avoiding transferring calls to external public networks whenever possible. An SBC can also reduce expensive downtime and provide enhanced security for both employees and customers, improving metrics such as customer satisfaction and the employer brand.

The same policy engine can move calls away from an overloaded contact center to a back-up site or "follow the sun" so that calls are automatically routed to the right contact center based on time of day. Intelligent policy capabilities enable organizations to implement policies such as

- Optimized call routing
- Custom dialing plans
- Call blocking and screening
- Emergency call routing
- Local number portability lookups
- Caller name delivery

Increasing Efficiency

Localized policy management in an SBC enables organizations to efficiently manage VoIP policies at a single point in your network — right at the network perimeter, where your SBC is already securing and providing interoperability for signaling and media traffic. You spend less time and money managing multiple devices such as routers, firewalls, and transcoders.

TIP

If you have a large network — or if your network grows over time — you can further simplify policy management with a centralized policy server. In this scenario, you perform your initial configuration, and any future policy changes, one time and in one place: on a primary policy server. Your changes are automatically distributed across the network to be invoked as local policy management at all your SBCs.

FLYING HIGH WITH RIBBON SBCs

A U.S.-based, international airline maintains a global contact center to deal with reservations, rewards programs, flight changes, seating assignments, and other business-critical calls. The airline also supports numerous voice applications for maintenance and support teams, ground support (baggage, fueling, and so on), logistics, in-cockpit and paging systems, airport ticket counters, mobile workforce support, and even airport courtesy phones.

The airline faced functional and expense-related challenges with its legacy telecommunications systems. Specifically, the airline needed to

- Migrate its contact center to an all-IP voice infrastructure without discarding its installed base of legacy equipment
- Reduce costs
- Improve employee productivity
- Maintain voice security
- Improve customer experience across a variety of real-time communications applications and devices

To solve these challenges, the legacy voice systems, which were time-division multiplexing (TDM) private branch exchanges (PBXs) and circuit-switched integrated services digital network (ISDN) primary rate interface (PRI) voice circuits, were migrated to a software-based VoIP contact center and session initiation protocol (SIP) trunking to reduce voice costs while still allowing interworking with the installed equipment base. At the same time, the airline was able to centralize control of its voice communications to provide load balancing and least-cost routing for inbound interactive voice response (IVR) calls from customers.

The airline installed Ribbon SBCs and a Ribbon policy and routing server (PSX) to provide

- Interoperability between legacy voice systems and SIP trunking
- Centralized call control and routing
- Secure access for both on-campus and remote contact center agents and mobile employees

(continued)

(continued)

With the Ribbon solution, the airline achieved dramatic results

- Reduced call costs and network operating expenses
- Least-cost routing for all calls
- Keeping internal calls on the airline's internal network instead of routing them across a carrier's network
- Lower capital expenditures
- Improved uptime and reliability for the contact center
- Secure connectivity for remote workers and home-based contact-center agents

Minimizing Costly Downtime

Downtime of business-critical systems — such as your real-time communications — is costly. A robust, highly available SBC is designed with redundant configurations to eliminate single points of failure, providing available capacity during peak loads and seamless failover capability if a critical component fails. A well-designed SBC architecture can recover seamlessly from faults and has the capacity to restore its state and handle a potential flood of VoIP client re-registrations if required.

REMEMBER

A redundant, high-availability architecture is important regardless of whether your SBC (and other components) is hardware-based, virtual, or cloud-native.

Consolidating Multiple Functions

Say you wanted all the features and benefits of an SBC, but you decided to build it yourself. You'd need to cobble together various functions of firewalls, routers, servers, gateways, and multiple protocol stacks to individually handle all the security, SIP translation, media transcoding and transrating, and call admission control (CAC) functions that an SBC provides. But if you consolidated all that functionality into an SBC, you'd realize significant savings:

- **Reduced capital expenditures (CAPEX):** Simply put, you have fewer things to buy, and SBCs cost less money. For those network elements and functions that you need for other functionality, you don't need to overbuild/over-specify them to allow capacity for the SBC functionality that's handled elsewhere.
- **Lower operating expenses (OPEX):** You can save money on recurring expenses such as rack space, power, and cooling with an SBC solution — whether physical, virtual, or cloud native — compared to multiple devices installed in your data center or telecom equipment room.

TIP

Your CF-No will be itching to write you a check when you explain that the choice of an SBC is a classic "buy or build" scenario that reduces CAPEX, lowers OPEX, and offers greater security, less downtime, and enhanced functionality.

Getting Real about Cost Savings

A virtual or cloud-native SBC can save additional money by allowing your business to use common server infrastructure to scale SBC capacity without adding proprietary hardware or requiring significant additional rack space, power, and cooling. Virtual and cloud-native SBCs can be instantiated, provisioned, and configured via automation, providing more rapid and easier deployment in data centers, on customer sites, or on private and public clouds.

SHOPPING FOR AN SBC SOLUTION

A U.S.-based retail chain needed to consolidate its voice management into a centralized system while migrating from legacy circuit-switched TDM to SIP trunking to reduce costs and to implement specific security features.

The retailer's requirements included

- Saving money with SIP trunking
- A centralized policy and call routing control for all stores

(continued)

(continued)

- A rapid rollout, with the ability to convert all stores to SIP trunking within a few years
- Specialized routing for inbound IVR calls directed to its in-store pharmacies (specifically, the ability to provide dial tone to these calls)
- Data security restrictions related to its pharmacy business
- Maintaining security on all calls

To solve its issues, the retailer deployed a Ribbon SBC and PSX in two data centers to provide a centralized dial plan for all stores. The retailer leveraged Ribbon to develop an installation plan, perform configuration, and develop and implement a test plan. The initial deployment was successfully defined, designed, tested, and implemented in just a few weeks. The deployment produced the following results:

- In phase 1, the retailer realized more than $500,000 in annual savings from reduced toll fees and TDM/PRI trunk leases.
- SIP trunking enabled the retailer to buy its SIP sessions “in bulk” and distribute those sessions flexibly across its many stores.
- The retailer connected the multi-vendor PBXs across its stores and managed all its dial plan and routing information in a centralized location. Centralized dial plan management will save the retailer hundreds of hours per week that formerly went to PBX provisioning and upgrades, enabling the retailer’s IT team to divert its internal resources to more critical, revenue-generating projects.
- It provided built-in Transport Layer Security (TLS), Secure Real-time Transport Protocol (SRTP), and Internet Protocol Security (IPsec) encryption with no degradation in SBC session performance.
- It provides much-needed protection against potential network threats such as distributed denial-of-service (DDoS) attacks, which can be particularly damaging to a large retail business during the holiday season — especially for a business that relies heavily on its communications network for both sales and customer service.

IN THIS CHAPTER

- **Improving management efficiency and performing under pressure**
- **Securing the network and ensuring customer experience**
- **Playing well with others and deploying in the cloud**

Chapter 7 Ten Reasons to Choose a Ribbon SBC

Whether you're an enterprise using Voice over Internet Protocol (VoIP) or unified communications (UC), or a service provider offering VoIP or UC services to your customers, your choice of session border controllers (SBCs) is integral to your real-time communications architecture and the success of those services. In this chapter, you discover ten reasons to choose a market-leading Ribbon SBC solution.

Robust Security

Securing the Session Initiation Protocol (SIP) network is a high-priority task for enterprises and service providers alike. Ribbon SBCs are designed to

- Provide end-to-end encryption on both the signaling and media components of network traffic.
- Hide the topology of the private portions of your network with a back-to-back user agent (B2BUA, see Chapter 2).

- Protect the network from distributed denial-of-service (DDoS) and telephony denial-of-service (TDoS) attacks while maintaining the capability to connect legitimate sessions (Chapter 1 describes DDoS/TDoS attacks).
- Implement block lists, grey lists, and allow lists (see Chapter 1).

Peak Performance

The proliferation of applications and devices has led to an explosion in the volume of SIP traffic on enterprise and service provider networks. Ribbon SBCs are designed to deliver peak performance at scale, regardless of traffic load or features that are enabled. They've been field-proven in Tier 1 service providers and in some of the largest enterprises in mission-critical roles, including in demanding verticals such as financial services and healthcare.

High-Scale Transcoding

REMEMBER

Both transcoding and transrating are computationally complex processes — imagine what it takes to completely disassemble and reassemble a voice in real time without inducing noticeable latency or delay into the stream. Not all SBCs can scale transcoding for thousands of simultaneous sessions, but Ribbon's SBCs can scale to support high levels of transcoding without any effect on other computational functions, such as security and call admission control (CAC), that the SBC must also perform.

Advanced Media Support

Today's SBCs need a robust media component that has both the computational horsepower and the sophisticated software to perform on-the-fly transcoding and transrating of all sorts of media. Most enterprise networks are fully converged, meaning that they handle all voice and data traffic. The SBC is an important component for

- Securing converged networks
- Providing quality of service (QoS) to ensure an outstanding customer experience
- Performing the necessary transcoding or transrating to interoperate on all media streams

Interoperability

Different vendors and different VoIP networks may speak in slightly incompatible ways when they use SIP (see Chapter 1). This incompatibility can result in calls that can't be completed or that are degraded in some way (such as missing some functionality). The SBC provides the critical role for interoperating across the different variants of SIP.

TIP

Ribbon SBCs support all known variants of SIP through SIP normalization (translating between different SIP variants), either by using static rules configured on the SBC, or on the fly as different varieties of SIP are encountered by the SBC.

Multiple Certifications

An SBC provides interoperability with real-time communication products from many vendors. With the rapid adoption of unified communications as a service (UCaaS), one of the attributes to look for is certification from leading UCaaS providers such as Microsoft Teams, Zoom, and Ring Central. Ribbon SBCs have been certified for Microsoft Teams Direct Routing, including media bypass and local media optimization options. Ribbon SBCs have also been certified for interoperability with Zoom Phone and Ring Central.

And a special note for those of you who work in the United States federal government: Ribbon has certifications for U.S. government deployment with certified compliance to the Joint Interoperability Test Command (JITC) and Federal Information Processing Standard (FIPS) 140-2 requirements.

Seamless Scalability

Ribbon uses a three-dimensional approach to scalability by separating the processing functionality of the SBC so that individual tasks, such as transcoding or encryption, can scale up or down without impacting the performance of other SBC tasks.

REMEMBER

Ribbon divides SBC processing into three categories:

- Signaling and general computing
- Media processing for networking
- Transcoding

With this approach, when certain functions in your VoIP network need more horsepower, you have it. But you don't lose capacity in other areas that already have a comfortable degree of overhead. Best of all, this fundamental software design works for hardware appliances as well as virtual and cloud-native deployments.

Virtual and Cloud Native

A decade ago, Ribbon innovation introduced the industry's leading software-based virtualized SBC with all the same features as a hardware-based SBC but architected for high availability and scalability. It ran on commercial off the shelf (COTS) platforms for deployment in data centers as well as private and public clouds.

Ribbon innovation has now delivered the next step in SBC evolution with an industry-leading, cloud-native SBC. Optimized to take advantage of microservices design, deployment in containers, automated life cycle management using Kubernetes, and integration with an observability framework, Ribbon's cloud-native SBC further extends and amplifies the attributes of high availability, reliability, and support for new and advanced features, while delivering performance at scale.

Centralized Policy and Routing Control

In conjunction with Ribbon's policy and routing server (PSX), Ribbon SBCs deliver localized policy control without the overhead of separately managing policies at each SBC. Ribbon's PSX delivers policy management in which provisioning policy and routing data is centrally managed and policy and routing information is automatically pushed to every SBC. Not only is this faster, but also it's less prone to error because changes are made once instead of many times (potentially hundreds of times across hundreds of sites).

Proven Track Record

SBCs perform a mission-critical role for enterprises and service providers. As such, you want to make sure you're working with a vendor that has the experience and expertise to deliver a resilient, high-availability solution with no single point of failure. Whether you're deploying an SBC as an appliance, as virtualized software, or as a cloud-native solution, you want to make sure that your SBC vendor understands what you need for success. With more than 20 years of innovation and implementation experience, Ribbon knows how to deliver and has the track record and customer testimonials to prove it.

Secure business telecommunications with SBCs

Unless you own a very small shop in a remote village somewhere without phone or Internet service, you and your company probably rely on telecommunications. In this book, you see how the session border controller (SBC) protects and secures your networks, eliminating spoofing attacks, denial of service attacks, and toll fraud. In addition, you discover other functions that an SBC can provide for your network and how to deploy an SBC in various configurations.

Inside…

- Ways to protect your network
- The key features of SBCs
- The typical use cases for an SBC
- Secure contact center voice services
- How to save money with an SBC
- What to look for when buying an SBC
- Learn about cloud-based SBCs

ribbon™

Floyd Earl Smith has worked in marketing at Apple, HSBC, NGINX, Onehouse, and Visa. He received his BA at the University of San Francisco and his MSc at the London School of Economics. He has written many *For Dummies* books, including *Quantum Computing For Dummies.*

ISBN: 978-1-394-19693-7
Not For Resale

9 781394 196937

for dummies®
A Wiley Brand