Compliments of Sonus

Sonus Special Edition

Session Border Controllers

FOR DUMMIES®

Learn to:

- Understand the role of SBCs in VoIP networks
- Save money with SBCs
- Maximize the value of an SBC regarding security
- Handle SIP trunking and its variants

Pat Hurley

Session Border Controllers FOR DUMMIES®

SONUS SPECIAL EDITION

by Pat Hurley

John Wiley & Sons, Inc.

Session Border Controllers For Dummies®, Sonus Special Edition
Published by
John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

ISBN 978-1-118-37742-0 (pbk), ISBN 978-1-118-37917-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact `info@dummies.biz`. For details on licensing the *For Dummies* brand for products or services, contact `BrandedRights&Licenses@Wiley.com`.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Vertical Websites

Project Editor: Carrie A. Burchfield

Editorial Manager: Rev Mengle

Acquisitions Editor: Katie Mohr

Business Development Representative: Sue Blessing

Custom Publishing Project Specialist: Michael Sullivan

Composition Services

Sr. Project Coordinator: Kristie Rees

Layout and Graphics: Carrie A. Cesavice, Tim Detrick, Jennifer Mayberry

Proofreaders: Rebecca Denoncour, John Greenough

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing and Editorial for Consumer Dummies

Kathleen Nebenhaus, Vice President and Executive Publisher

Composition Services

Debbie Stailey, Director of Composition Services

Business Development

Lisa Coleman, Director, New Market and Brand Development

Table of Contents

Introduction

Voice over Internet Protocol (VoIP) — or, as the acronym is often pronounced, *voyp* — is the future of voice services. Today, an increasing number of the voice calls you make are converted to VoIP for the in-the-network parts of your calls, because VoIP is more flexible, less expensive, and more efficient in terms of network utilization. But that's really just the beginning. VoIP is becoming more common as an end-to-end service and moving beyond just voice calls into other media, such as videoconferencing, IM and text chat, file and screen sharing, and more.

As with any newer technology, the adoption of VoIP comes with some unique challenges — security risks, implementation and interoperability headaches, and emerging services. But, *Session Border Controllers For Dummies,* Sonus Special Edition, is here to help with timely information about session border controllers (SBCs): devices designed to control the calls (or videoconferencing, or other media) coming in and out of an enterprise's or service provider's VoIP network, while also handling the signaling and media intermediation and translation required to make the VoIP service work smoothly all the time.

About This Book

Session Border Controllers For Dummies, Sonus Special Edition, is a nontechnical book for business decision makers looking to understand the role of an SBC in their VoIP networks. If you want to figure out whether an SBC can provide features that your business and your network need, well, you've come to the right place!

How This Book Is Organized

As is the case in any *For Dummies* book, each chapter is self-contained, so you don't need to read this book from cover to

cover. If you see a chapter in the Table of Contents that you already know everything about, feel free to skip it. Conversely, if you see one that may have just the right information you've been wanting, head straight there.

This book is organized into five chapters.

Chapter 1: Discovering SBCs and How They Protect Your Network

Chapter 1 provides an overview of the SBC. You get a basic understanding of SBCs and why enterprises or service providers need an SBC when they have VoIP or deploy services such as videoconferencing.

Chapter 2: Uncovering the Key Features of SBCs

Chapter 2 digs a bit deeper into the nature of the SBC. How can an SBC stop attacks that threaten the performance of your VoIP network and even cause your business financial harm? What features and tools make up a good SBC? How does an SBC relate or compete with VPN tunneling services and your network data firewall? Good questions. You find out those answers in this chapter.

Chapter 3: Centralizing Your Session Management

VoIP networks without SBCs are often managed in a relatively ad hoc way with different aspects of the overall session and media management performed by different equipment. In this chapter, you look at the benefits of moving all that management functionality into a single device — the SBC. You get a little bit about network analytics, multimedia handling, policy control, dealing with the IPv4 to IPv6 transition, and the attributes of a networked SBC. Also, you discover how an SBC is flexible enough to handle special services and protocols like ENUM.

Chapter 4: Saving Money with an SBC

If you're a finance or C-level executive reader, get your smiling cheeks ready. In this chapter, I talk about ways SBCs save enterprises and service providers some money. Cash. Bucks. Dollars. Mucho dinero!

Chapter 5: Ten Reasons Why You Should Choose Sonus SBCs

Chapter 5 is where I provide some thoughts about the attributes of SBCs that are important to consider when you actually go out and get one for your network. You also see how these important buying criteria are handled by Sonus SBCs.

Icons Used in This Book

This book calls out important bits of information with icons on the left margins of the page. You'll find four such icons in this book:

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

Pay attention to the Remember icon because it points out parts of the text to lock away in your memory for future use.

Watch out! This information tells you to steer clear of things that may cost you big bucks, are time suckers, or are just bad SBC practices.

I try to keep the hardcore techie stuff to a bare minimum. You don't need to know these factoids to get the most out of the book, but they may come in handy.

Chapter 1

Discovering SBCs and How They Protect Your Network

In This Chapter

- Learning the ABCs of SBCs
- Understanding why enterprises and service providers need SBCs

It's far from breaking news to say that telecommunications are vital to just about every type of business out there. Whether a business is extremely technologically sophisticated or at the opposite end of the spectrum, activities such as phone calls, e-mail, electronic financial transactions, video conferencing, file backups, or accessing customer service records on a remote server are going to be part of the day-to-day, business goings-on. Even formerly unwired businesses like food trucks or plumbers now rely on wireless data services for voice calls, to tweet their locations, to take orders via the Web, and even to complete credit card transactions. And remote workers (teleworkers and on-the-road folks like sales personnel) absolutely rely on telecommunications connections back to the mother ship.

Ultimately, unless you own a very small blacksmith shop in an even smaller village, your business relies on telecommunications in one form or another. In this chapter, I introduce the *session border controller* (SBC) — a technology that's designed to help enable and secure important parts of any business' telecommunications infrastructure.

Looking at the SBC's Role

An SBC controls a network by admitting (or not admitting) and then directing communications between two end devices on the network, like a Voice over Internet Protocol (VoIP) call between two phones, or the connection between the web browser on your iPad and the web server you're accessing. These communications are called *sessions.* A video call between two devices is also handled in a similar way. The SBC does this session controlling at the point where traffic is handed off from one network to another (called the *border*). Because of where the SBC fits in the network, it can be usefully implemented by both businesses themselves and also by the service providers who serve them.

As VoIP network owners — both enterprises and service providers — face threats to the security of their network and business, they also face more prosaic issues like how to make VoIP work seamlessly and efficiently while also realizing the cost and bandwidth savings that VoIP promises. That's where the SBC really earns its keep. In this section, you look at the main functions and roles of the SBC.

Protecting and securing the network

The SBC's main role is protecting and securing the network. The SBC is built from the ground up to eliminate spoofing attacks, denial of service attacks, and toll fraud. The SBC secures the network by doing the following:

- Hiding the topology (or architecture) of the network, making it difficult or impossible for bad actors to gain access to vulnerable parts of the network
- Enabling encryption that prevents communications from being illegally intercepted or tampered with
- Detecting and preventing denial-of-service attacks before they can impair network performance

Enabling SIP trunking

Session Initiation Protocol (SIP) is the primary VoIP protocol that enables a session or connection to be made between two end points on the network. *SIP trunking* is a service delivered via SIP that allows a private branch exchange (PBX) system, which is the multiline phone system used by businesses, to aggregate multiple calls, screen shares, or videoconferences over an IP connection.

SIP trunking saves money by allowing a shared data connection to handle voice and related traffic for an enterprise or service provider instead of relying on expensive, dedicated voice lines. In fact, typical savings from SIP trunking, trunking consolidation, and the move to VoIP can reduce traditional enterprise telecom bills by 75 percent. Additionally, the SBC can provide secured access to that SIP trunking service, so an enterprise can maintain security while saving money.

Interconnecting with topology hiding and protocol translation

While security and cost savings (through SIP trunking, covered in the preceding section) are a huge deal when it comes to deciding to deploy an SBC, another factor is equally important: providing 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:** SIP is one protocol with a million little variants as different vendors implement it. The SBC can translate these variants between devices (a process known as *SIP normalization,* covered in more detail in Chapter 2) so calls get through with all their features intact without a hiccup.
- **Translating protocols:** Different VoIP solutions may utilize different audio codecs (see the nearby sidebar titled "A VoIP primer" for more on this) and other protocols that aren't completely supported on both sides of the session. The SBC knows all these protocols and can translate between them on the fly.

A VoIP primer

VoIP (if you want to sound like an industry insider you can pronounce it *voyp*) is a pretty simple concept to understand but one that's essentially taken over the voice telephony world. In the most basic terms, VoIP is simply a voice call that is digitized and broken up into *packets* (chunks of data) and transported across an IP transport network, just like any other bit of data. VoIP calls can be end-to-end (for example, when you make a webcast call from computer to computer) or only the middle part of the call may be carried using VoIP, across the backbone of one or more service providers. This latter scenario is called VoIP backhaul; in this case, one or both ends of the call are converted to/from more traditional voice technologies like TDM (time-division mulitplexing) in the case of legacy, fixed phones, or to 2G mobile telephone protocols like GSM (AT&T) or CDMA (Verizon).

VoIP offers service providers significant cost savings and efficiency benefits because it doesn't need to be carried over expensive copper lines and single-purpose circuits as did previous generations of voice calls. There are two major sets of protocols required to make a VoIP call work:

- **A voice codec:** A coder/decoder that compresses a digital voice signal, allowing it to use less bandwidth
- **A session control protocol:** Handles the dialing and hanging up of the connection between the two ends of the VoIP call

A number of different codecs and session control protocols are in use throughout the world of VoIP, which makes the role of the SBC even more important.

Acting as session traffic cop

The SBC is the gatekeeper to the VoIP network in an enterprise or in a service provider network. In this role, it performs a task known as *session admissions control.* Session admissions control is the process of determining who has access to the network and who doesn't. The SBC is the traffic cop of a VoIP network, keeping your VoIP highways safe and orderly and creating and accessing three lists — whitelists, blacklists, and greylists. More on these lists in Chapter 2.

Understanding the Need for SBCs

SBCs were initially deployed primarily within service provider networks. SBCs ensure that VoIP calls are properly routed between network providers, that differing protocols are understood so the call can be delivered across different networks, and that calls are secured.

As VoIP has become more common — indeed, has become the dominant mechanism for transporting voice calls — the SBC has become useful in more places in the network, including at the border between an enterprise's network and the carrier's.

In this section, I talk about the most prominent reasons why SBC technology is reaching into more parts of the network.

Securing the network

The most talked about driver for the adoption of the SBC is security — and for good reason. VoIP (as well as other session-oriented applications) is an application that by its very nature is exposed to devices and networks that are out of the control of an enterprise or a network provider. VoIP *isn't* like traditional telephony where a very highly circumscribed set of devices, protocols, and private networks are involved in the process of placing and carrying calls. In the old days when you placed a phone call (via landline or cellular), the call was placed on an approved device and carried across the private phone company network.

Like other IP applications, VoIP is often carried over public networks — oftentimes across several public networks — and calls can be initiated or completed on devices, such as personal computers (PCs) or smartphones, by using VoIP apps that aren't under the control and regulation of the phone company. This fact leaves the VoIP world considerably more vulnerable to the same kinds of malicious and fraudulent security threats that any Internet service faces.

Facing the issues

Among the threats that an SBC has been developed to help eliminate are the following:

- **Service theft and fraud:** These attacks happen when a hacker (or organized group of hackers) accesses an inadequately secured VoIP system to route traffic across the network without paying for it. Not only do the hackers use up network resources without paying for them, but also the enterprise or service provider often ends up paying for the unauthorized toll charges.
- **Spoofing:** Spoofing attacks come into play when people deliberately modify or disguise their identities (for example, caller ID phone numbers) on the network. This threat may occur to intercept calls intended for another (legitimate) party or simply in order to confuse or annoy.
- **Denial-of-service (DoS)/Distributed denial-of-service (DDoS) attacks:** DoS attacks and their bigger, badder brother DDoS attacks seek to flood a server or SBC with requests in order to take it out of commission. DoS attacks typically originate from a single point/user, while DDoS attacks can involve sometimes hundreds or even thousands of zombified computers (known collectively as a *botnet,* for robot network).
- **Registration storms:** A registration storm is when thousands or millions of devices attempt to register with the SIP server all at once in a VoIP network.

  

  A registration storm can also occur for non-malicious reasons. For example, after a major network outage, there can be many thousands of VoIP devices all trying to reconnect and re-register with the network at the same time.

Check out Chapter 2 for ways to battle these issues.

Chapter 2

Uncovering the Key Features of SBCs

In This Chapter

- Using an SBC to stop security attacks
- Identifying the key requirements of an SBC
- Looking at alternative options (and why they're less effective)

A session border controller (SBC) is designed to secure the network, prevent fraud, and smooth the way to better interworking between devices, services, and topologies throughout Voice over Internet Protocol (VoIP) or other media sessions such as videoconferencing, instant messaging, or file sharing.

In this chapter, you dig deeper into some of the most important features that SBCs provide in enterprise and service provider networks, find out about how SBCs help stop attacks on a VoIP network, look into the specific characteristics required by a successful SBC, and discover why some alternatives to SBCs, such as tunneling and data firewalls, don't really provide all the functionality an enterprise or service provider requires.

Stopping Attacks with an SBC

Networks are increasingly subjected to both malicious and fraudulent attacks. The common attacks of service theft and fraud, DoS, DDoS, spoofing, and registration storms (all covered in Chapter 1) can be dealt with through SBCs. So what tools should an SBC bring to the table to defeat these attacks? This section tells you.

Media and signaling encryption

This approach applies cryptographic scrambling, called encryption, to both the signaling session initiation protocol (SIP) and media (voice, video, IM, and so on) portion of the call. Encryption provides more than just scrambled data; it also relies on an *authentication mechanism* — a way of identifying that a client is who it says it is. This authentication happens when a client has the proper half of a secret key, known only by that client. A properly implemented encryption system means that malicious parties can't eavesdrop on VoIP calls, videoconferences, and other SIP-based communications.

Topology hiding with B2BUA

A back-to-back user agent (B2BUA) is a system in which SIP calls are controlled by a logical or virtual proxy configured for the call. This agent sets up the pathways across the network for both signaling and data. B2BUA causes all signal and media traffic to run through the SBC and hides the topology, or architecture, of the network so that clients aren't shown things like private IP addresses of servers and devices in the network. The net result is a network that's easily accessible to clients for making and receiving calls, but the "innards" of the network are effectively invisible, which makes them less vulnerable to attack.

List monitoring

The SBC's policy management system monitors incoming requests and calls, uses rules to identify people who are and aren't abusing network resources, and maintains certain lists:

- **Whitelists:** A list of people and devices that *always* has access to the network; examples include your CEO and his home office phone, iPhone, and iPad
- **Blacklists:** A list of people and devices that *never* has access to the network; examples — known spammers, DoS perpetrator, and DDoS perpetrators (more info on DoS and DDoS in Chapter 1)
- **Greylists:** A list of people and devices that sometimes has access to the network; network administrators set policies to determine what criteria must be met to connect these sessions

Identifying the Key Requirements of an SBC

There's more than just security to the role of an SBC. In fact, many in the industry say that it's the security that causes customers to become interested in the SBC, but it's the other functionality that really makes the sale. This other functionality is all about SBCs making VoIP calls work in situations where they may otherwise not work, and beyond that, SBCs make all VoIP services simply work better.

What does it take for an SBC to do this? The functions discussed in the following sections are the essentials.

Normalizing SIP

SIP is the primary protocol that makes the connection between two end points and closes 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 the private phone network. The use of SIP is critical to the ability of disparate network topologies from different vendors to be able to communicate with each other.

SIP is a communications standard authored by a global community of engineers known as the Internet Engineering Task Force (IETF). The standard, however, is more of a series of recommendations and suggestions on how SIP should be implemented. The actual SIP implementations are left up to individual engineers and vendors, resulting in a multiplicity of SIP variations that are technically in compliance with published SIP standards but not necessarily compliant with one another.

There are enough variations in SIP that sometimes two systems connecting to each other using SIP find that they aren't really 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, that

confusion can be overcome by context or by a simple "huh?" But when two machines are talking, that simply isn't going to happen.

An SBC — at least a useful one — 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 is required to 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, and the best SBCs make the whole process transparent and seamless.

Transcoding calls

The SBC's job — or at least an SBC worth its salt — is to *transcode,* or change, codecs as sessions pass through the SBC. The SBC knows which codecs are supported on each side of the network border and is required, using a combination of software and special-purpose digital signal processors (DSPs), to decode and then re-encode the voice or video signal as it crosses the network border.

Many codecs — the encode/decode algorithms that compress voice and other signals (like video streaming across the network in a videoconferencing environment) — are in use in various VoIP and Unified Communications (UC) systems.

UC is the "beyond voice" variant of VoIP, where things like videoconferencing, screen sharing, and instant messaging (IM) are delivered over the VoIP network platform.

Low- and high-bandwidth video and voice codecs are designed differently to work on various devices:

- Computers and tablet devices
- Dedicated VoIP phones
- Mobile devices (smartphones and iPhones)

In a VoIP call (or any session-based communication, for that matter), there are always differing capabilities to support codecs. So if an enterprise's private branch exchange (PBX)

supports one specific codec and the incoming call from an important customer is using a different codec, the SBC will understand both codecs and, in real time and in both directions, modify the codec as the call passes through it.

Some codecs may simply not be implemented on a device for a mixture of reasons:

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

Transcoding frequently comes into play in two specific instances.

HD Voice

The sound quality of voice calls in general has taken a step backwards over the years as convenience (mobile) and economics (VoIP) have caused a movement away from traditional landline phones. A new effort called *High-Definition (HD) Voice* has been brewing in the industry for a few years with a goal of reproducing a greater range of frequencies at higher clarity (known as a *wideband codec*) instead of traditional *narrowband codecs* (so called because they cut off both the top and bottom frequencies normally found in a person's voice).

The result is a voice call that's easier on the ears and that lets you actually tell who's talking (handy during a conference call). It's like moving from AM radio to CD (or, for the modern music buffs out there, to lossless music codecs).

But there's a gotcha to HD Voice — there's no one single implementation of the service and no one single codec in use by every HD Voice-capable system, but having an appropriate SBC in the middle of the call (one with robust transcoding capabilities) solves the problem. The SBC can transcode and keep the call HD all the way (but there's a lot of software and hardware doing some heavy lifting behind the scenes).

Bandwidth restrictions

As much as you may like to have limitless bandwidth available to you, wherever you are (and personally, I'd prefer it to be very inexpensive too!), that's simply not always the case.

Sometimes a call is made to someone who's connected to a mobile network outside of not only 4G but also even 3G coverage. Other times, a call is made to a person in a home office with a dial-up connection or someone using a spotty hotel Wi-Fi connection.

Bandwidth can't always be taken for granted across the entire network portion of an SIP call, videoconference, or screen sharing session. There are codecs available that trade fidelity and audio/video quality for greater compression — thereby using less bandwidth.

You 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 as it does at the border 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

Do you have a Wi-Fi router in your home? Chances are very good that you do and, if that's the case, you probably have a Network Address Translation (NAT) network configured for your laptop, iPad, Android phone, and other devices connected to your home's broadband connection.

NAT is a technology service that translates (it's right in the name) between a single public IP address (the IP address of your broadband cable or DSL modem) and the private IP addresses that your router assigns to all the attached devices on your home network. NAT is a configuration that's used because there aren't enough IP addresses available in the world to assign each and every individual device its own unique address.

There's a newer version of the Internet Protocol, *IPv6* (Internet Protocol version 6) that will eventually replace today's current IPv4. IPv6 increases the number of available IP addresses and eliminates the need for NAT. The gradual adoption of IPv6 actually provides another reason to use an

SBC, because the SBC has the intelligence to let IPv4 and IPv6 network segments talk to each other.

NAT is a neat and inexpensive technology for network addressing because it lets a small pool of IP addresses get used over and over in different private networks while letting the devices attached to that network communicate with the broader Internet using a single, unique public IP address.

The problem with NAT is that creating an end-to-end session is difficult because the IP address of a device on a NAT isn't a public IP address (that would be the IP address of the network itself). This creates issues with end-to-end sessions like VoIP and requires some translation to happen between public and private addresses — translation beyond what the private network's 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 on the end of the session. NAT traversal requires a significant amount of computing capacity in the SBC because a large number of devices participating in VoIP and other sessions are behind a NAT. An SBC requires a lot of processing power to do all the translating and routing required to traverse NATs.

Fax and tone detection

As much as any carrier engineer or enterprise IT professional would like to, it's usually just not possible to have a clean break with the past (like Apple removing the floppy drive from the original iMac). Oftentimes, legacy technologies linger on well past their "sell by" date, and the network needs to support them.

A prominent example of this in the VoIP world is facsimile or fax technology. I've spent enough time in the telecom world to have heard of IP faxing being "the next big thing" for at least 15 years. But that doesn't change the fact that there are still people out there 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 of a fax preamble.

Performance, scalability, resiliency

If you've read the previous few sections talking about all the things that an SBC must do, you may begin to imagine that the SBC can't be a low-powered (computationally speaking), dumb box. And in fact, you'd be right. SBCs need to be powerful and robust devices with the right degree of extra capacity and redundancy to handle not only the average number of calls coming through the system simultaneously, but also to scale up and handle peak calls — like the flood of telephone orders when a hot new product is announced.

When evaluating an SBC's performance, scalability, and resiliency, consider the following factors:

- **CPU utilization:** The SBC does a lot of computationally complex work, what with all of the audio/video transcoding, SIP translation, and other functions that it has to do in essentially real-time (where delays can keep calls from being completed or cause latency and delays in calls); the CPU utilization in both a normal steady state and during peak periods should allow plenty of overhead.
- **Concurrent calls (or sessions) supported:** This objective measurement is simple to understand. How many concurrent calls is the device rated for; how does this match your network's usage patterns; if your usage grows and begins to exceed the capacity of your SBC, how can you upgrade?

  The need for scale becomes very real as multipoint videoconferencing becomes a reality and as the adoption of presence-based communications tools like IM becomes more prevalent.

- **Redundancy:** Put a different way, this means "a lack of single points of failure." An SBC is performing a mission-critical role for an enterprise or carrier. Are there any elements within the SBC that don't have a redundant

element that can take over on a millisecond's notice? If so, remember downtime means lost money (in revenue or employee productivity).

- **Registration rate:** How many clients can the SBC register in a fixed period of time; this relates to the registration storms (see Chapter 1). When a lot of users are connecting at once, make sure the device can handle it.

Why Not Other Options?

In my opinion, the options in this section don't do enough to replace the need for an SBC, but in this section, I'll explore two alternative scenarios and explain why an SBC can do more and do it better.

VPN tunneling

Pretty much all enterprise and carrier IT professionals are old hands at implementing virtual private networks (VPNs). A *VPN* is essentially a private and secured network connection carved out of a shared or public telecommunications facility (like an Internet connection) using encryption and authentication.

Theoretically, all the traffic in a VPN connection flows over a cryptographic *tunnel* (the virtual private connection on the public/shared network) without being seen or accessed by those who aren't authenticated users. This works pretty well for things like allowing branch offices or telecommuters access to shared enterprise network resources or even within a service provider's network to offer private networking services to customers over shared facilities.

Where a VPN can cause trouble and why VPN tunneling isn't optimal for UC with VoIP and other session-connected services are when there's a need to look inside the packets encapsulated in the VPN to route calls and provide services. VoIP packets must be decrypted and acted on — removing the end-to-end encryption element that keeps a VPN secure.

An SBC with *Secure Real-Time Transport Protocol* (SRTP) and *Transport Layer Security* (TLS) allows a high level of security

between the border controller and the target device. Because the session is encrypted, it's thought to have better security than possible on the *Public Switched Telephone Network* (PSTN) — in other words, traditional phone service.

Data firewalls

Let's be frank. Other systems can provide at least some of the security or other functionality that SBCs bring to VoIP and UC networks. But do they do enough?

Every carrier or enterprise network has at least one type of data *firewall* device installed at the edges of the network, designed to allow only appropriate traffic to reach within the network. Firewalls are great at certain things, like keeping unauthorized users off your file servers or even deflecting attacks on your web server.

Theoretically, a data firewall can be configured to allow the opening of *ports* (or communications channels) that allow VoIP sessions to pass through the network and on to appropriate clients within the network. The problem is that VoIP (and UC) sessions are exceedingly dynamic. Calls are set up and taken down frequently and in large numbers. Additional services are added during the middle of a call (for example, when someone begins to IM another user during a conference call, or when someone shares a picture or video during a voice call).

Typically a data firewall just isn't set up to handle this kind of dynamic service provisioning, nor is it particularly VoIP- and SIP-savvy. The result is that a firewall tends to be opened up *too much* when it's used to provide VoIP security, with ports being left open when they aren't currently in use. And without the B2BUA that an SBC provides, intruders are more likely to use those open ports to gain access to parts of your network that you don't want them near.

Chapter 3

Simplifying Your Session Management

In This Chapter

- Using a Session Border Controller to analyze your VoIP traffic
- Dealing with multimedia in your VoIP network
- Localizing your policy control
- Managing remotely
- Flexing your network

Voice over Internet Protocol (VoIP) deployments to date have been relatively simple and functionally limited — focusing on things such as Session Initiation Protocol (SIP) trunking and low-cost consumer VoIP services. That's changing and changing fast as VoIP begins to replace more and more of the circuit-based telephony that historically dominated both fixed and mobile line services. For example, next generation 4G LTE (Long Term Evolution) mobile networks will rely on SIP-based messaging instead of circuit switching for voice calls, SMS, and other services. Similarly, wireline VoIP will continue to grow and related services such as videoconferencing, IP-based text messaging, and new services such as *presence* (essentially a telecom status message that lets your contacts know where you are and what kind of communications you're available to participate in) will all drive communications toward a reliance on sessions and protocols like SIP.

What this means is that yesterday's VoIP network isn't going to cut it, especially when that network isn't equipped with a session border controller (SBC). What's needed to support

the all-IP, mainly session-based future is an SBC that can centralize and remotely control both the signaling (the messages that flow across the network to begin, direct, and end sessions) and the media (the actual voice, video, or data flowing across the network) components of session communications.

In this chapter, I talk about the benefits an SBC can bring to an enterprise or service provider offering VoIP and related services by centralizing the control and routing of your VoIP and related sessions. Without an SBC, the routing, call admission, and processing (such as media transcoding) functionalities required to complete these sessions reside in a number of different devices, each of which must be individually configured and managed. The SBC makes a big difference to the cost and effort of managing a VoIP network by bringing all this functionality into a single device, with a single management system.

Analyzing Your Network Traffic

Traditional VoIP calls are pretty predictable. Network administrators and IT professionals have a good idea what the impact of a normal or even peak load will be. As additional session-based apps are added to the equation, however, that predictable formula tends to go out the window. How much bandwidth will be added to support an addition of a video call to a voice call? How many SIP messages must be sent to add a text component to an audio conference? How about when adding presence information on top of everything?

Both signaling and media impacts of these new applications need to be considered, and the network must maintain certain levels of performance and call or video quality to keep users happy. Consolidating the control of your VoIP SIP sessions on an SBC can alleviate uncertainty and provide you with a robust set of network analytics that let you measure and analyze your network performance across various applications.

When you receive reporting and analysis, you want to see the following factors:

- **Bandwidth:** The amount of bandwidth used by various services, including bandwidth used for both signaling and media transmission purposes

- **Latency:** The delay (measured typically in milliseconds) imposed on your calls due to factors such as network transmission, call routing, and transcoding (see Chapter 2 for more information on transcoding)
- **Jitter:** The variance in latency over time (a signal with the same latency at all times has zero jitter, while one in which the latency varies has some degree of jitter)

  Jitter in this context is often called *packet delay variation*
- **SLA compliance:** The factors — like downtime, call completion percentages, and so on — that play into a service level agreement (SLA) between a carrier and a customer

Multimedia Matters

As SIP sessions move beyond simple voice calls and become more sophisticated, your VoIP network needs to handle more than just audio and its related audio codecs (for more info on codecs, see Chapter 2). Other types of media that may be sent include the following:

- Video
- Text such as instant messaging or SMS
- Files or content for collaboration purposes
- Photos
- Higher quality audio (HD Voice, discussed in Chapter 2)
- Presence status

This media starts flowing across your VoIP network, and in many cases, it's in formats that aren't compatible with both ends of the call. Perhaps the same codecs aren't supported in use on both ends of the session or bandwidth restrictions are occurring on one or the other end of the session.

In these cases, something needs to be done to the media, whether its transcoding (covered in Chapter 2) or perhaps simply *transrating* the media (reducing its bit rate of transmission — sometimes at the expense of audio/video quality).

You can manipulate the data at the endpoints of the session in the client hardware and/or software that's placing the call

and being used by the people at either end of the session. But that's not always possible, and even when it is, it's not always the best approach to take.

Better approaches include the following:

- Let the clients on each end use whatever codec and bandwidth works best for them and use a separate device to perform any necessary transcoding and transrating for each session. That, of course, is exactly the kind of job that an SBC is best at.
- Enforce an adaptive codec policy that lets the best codec to be negotiated based on bandwidth to ensure quality-of-service (QoS).

Localized Policy Control

Like any network, a VoIP network relies on pre-configured policies that govern how calls are prioritized and handled and what to do when something unusual happens (for example, calls from known spammers, too many calls at one time, and so on). *Policies* are essentially performing the task that telephone switchboard operators did in old movies (or in *Mad Men*) by using a set of rules to determine how each incoming and outgoing call is handled, governing network decisions such as

- Call admission control
- Bandwidth utilization and rate limiting
- Least cost routing
- Media paths and routing

An SBC can locally (at the border of an enterprise's network or a service provider's network) enforce the policies you've set for your network. When you can control these policies at the local level, you can reduce response time and latency in the network because policy decisions don't need to refer back to a remote server in another location to be enforced. This local policy enforcement is also cheaper to deploy initially because it doesn't require additional equipment.

Centralized Policy Management

In larger deployments, where multiple SBCs are installed at multiple network borders, the task of individually configuring policies on all SBCs can be tedious and expensive. An alternative to localized policy control (see the preceding section) is further centralization by using a master policy server that can propagate a single set of policy rules (and policy rule changes) to each SBC on the network without requiring an expensive IT professional to manually configure each one.

While this approach may introduce a bit more upfront expense and a small amount of latency into the network, it saves money in the long run while allowing network administrators to quickly roll out policies based on network utilization. Additionally, this sort of centralized management ensures that policies are consistently enforced throughout the network, because policy changes are automatically disseminated to each and every SBC. If you're scaling your network to a large number of sites and SBCs, centralized management is the way to go.

Getting Ready for IPv6

The Internet Protocol (IP) variant that has powered the world through the Internet revolution for the past 20 or so years has an issue and it's a big one. IPv4 — the current version — has a limited number of IP addresses.

Just how limited? Well, there are only (*only*!) about four billion possible IP addresses in IPv4. When IPv4 was developed about 30 years ago, the concept that there would be a need for more than four billion IP addresses probably seemed pretty far-fetched. But 30 years ago people were thinking about IP addresses being assigned to things like personal computers, servers, network routers and the like, and four billion seemed like a pretty good overhead.

Today, however, there are nearly six billion cell phones in the world and with the advent of smartphones, these devices are becoming the equivalent of PCs connected to the Internet. Add in iPads and PlayStations and networked Blu-ray disc players and you get the idea: There are simply more IP-connected devices than IP addresses.

Service providers have used a variety of techniques to accommodate this, like Network Address Translation (NAT), which allows devices on private networks to use a pool of private IP addresses that can be reused on different networks. But NAT can cause issues with some applications (including VoIP — see Chapter 4 for more on this), so something new is on the way: IPv6.

IPv6 increases the address space of IP from 32 to 128 bits, which means that there are potentially more than 3 billion, billion, billion, billion IP addresses available in IPv6 — hopefully enough for another 30 years, at least!

IPv6 is currently, but slowly, being adopted by enterprise and service provider networks around the world. And that's good news, but it also brings up its own issues:

- **Equipment Readiness:** Not every computer, server, router, or other device on the network (both within the enterprise and in the service provider network) is ready for IPv6. So some intermediary device will need to help out that IPv4 gear and let it talk to IPv6 networks.
- **IPv4 – IPv6 Interworking:** Not all networks themselves are going to support IPv6 at the same time. When two clients want to communicate and one is on an IPv4 network and the other on IPv6, something needs to get in the middle and help them communicate.

These issues can be solved by an SBC 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. In this case, the SBC can communicate by using both versions of IP and can do things like connect to an IPv6-only smartphone by using IPv6 while connecting to an IPv4 server by using IPv4.
- The SBC can act as an interworking agent between an IPv4 network and an IPv6 network. In this case, the SBC (which, of course, sits at the network border) can translate all traffic flowing between an IPv4 and an IPv6 network on the fly, as it crosses the network border.

Someday, in the not-so-distant future, you can expect to have all devices and networks running IPv6. Until that day comes, however, the SBC can play a vital role in ensuring a smooth transition to IPv6.

Flexibility Is Key in VoIP

For all its benefits, if there is one thing that VoIP has given up when compared to traditional circuit-switched telephony it's the universal telephone number E.164 that uniquely identifies each phone or station and makes it possible for anyone anywhere in the world to call someone else with just that one bit of information. That's a powerful feature and one that has been hard to replicate in the VoIP world. The fact that VoIP and Unified Communications (UC) systems can offer multiple services (like IM/chat, videoconferencing, presence, and so on) makes the problem even trickier.

A partial solution to this missing piece of the VoIP puzzle is an IETF solution known as *ENUM* (or Electronic Number Mapping System) — also known as Telephone Number Mapping. ENUM is designed to map between traditional telephone numbers and IP addresses, so calls can get through even if they're placed from a traditional phone. ENUM in the Enterprise allows multiple branches and federated companies to perform flexible routing of calls, which saves them money and reduces complexities.

Unfortunately, unlike the original phone numbering system, there's not a bunch of monopoly telephone companies and government agencies driving a consistent, standardized, and universal adoption of ENUM. Instead, ENUM implementations may be carried out privately by a carrier individually, or by a group of carriers. It's a bit of a mess.

An SBC with embedded policy control can help smooth the path to ENUM technology, by handling the heavy lifting of ENUM database dips to ensure mapping and the appropriate call routing.

Chapter 4

Saving Money with an SBC

In This Chapter

- Reducing costs with one-stop management
- Being always available saves you money
- Integrating functionality reduces CAPEX and OPEX
- Growing sessions while saving money

You're all hyped up. You've done all your session border controller (SBC) research. You know the benefits (Chapter 1) and the services (Chapter 2) you get from an SBC. Now, you have to pitch the idea to your CIO or CTO. Everyone — and I mean *everyone* from enterprises to the biggest telecom carriers — is worried about budget and cost control. And while an SBC isn't a massive expense, if your CIO or CTO sees a new budget item, he's going to want some serious justification.

In this chapter, I present the cost savings justifications for SBCs and focus on how an SBC saves money relative to a build-it-yourself approach where you cobble together the functionality of an SBC by using other devices and custom integration efforts.

As a bonus, I give you two case studies showing how SBCs are used in the real world.

Benefitting from One-Stop Management

Localized policy management (see Chapter 3) is a benefit of SBCs from the perspective of cost and performance. The ability to do manage VoIP policies and media/signaling at one point

in your network — right at the border of the network in the SBC — means that you spend less technician time and money managing multiple devices like routers and adding additional transcoders.

If you have a large network — or if your network grows over time — you can further simplify SBC management by using a centralized policy server. In this scenario, you perform your initial configuration and any future policy changes one time in one place (the master policy server) and have those changes automatically circulate through the network to all of your SBCs.

Keeping the Revenue Flowing with Redundancy

Redundancy means that you have capacity and network elements (within a single device in this case instead of in side-by-side installations of similar equipment) which are sitting there in your network, unused. You may wonder: How's that saving me money? Redundancy is responsible, not wasteful because it ensures that your network stays up when something goes wrong and works well when the loads get high. Redundancy keeps your network working and working for you instead of leaving your business stranded and unproductive.

Your VoIP network is used for productive, money-generating business activities all day, every day, whether you're a service provider selling that service or an enterprise using it for your daily business. When you choose an SBC with adequate capacity and with built-in redundancy (see Chapter 2), you make an investment in keeping your network available and your revenue flow intact.

You have a network that's always available — even during peak call conditions, even when some element fails, or even when some malicious party attacks your network.

All networks can fail at some point; oftentimes, something besides the SBC causes the failure. A redundant network provides a graceful recovery by having extra capacity ready to go the instant something stops working.

Perhaps some other element to the network goes out. A well-designed SBC has the ability to quickly recover from these disasters and has the capacity to restore its state and to handle the flood of registrations it faces as the network is restored and all of your VoIP clients are re-registered with the network.

Saving with One Box Instead of Many Devices

Say you wanted all the features and benefits of an SBC, but you decided to just build it yourself. It's possible — perhaps *just* possible — but it's sure not easy. You'd need to cobble together a set of firewalls, routers, servers, gateways, and/or softswitches that could individually handle all the security, Session Initiation Protocol (SIP) translation, media transcoding/transrating, and call admission control functions that an SBC provides.

After you did that, you'd need to write the software code to make it all work and then test it and maintain it. Phew. I'm tired just thinking about you doing this whole process on your own! This endeavor would be both expensive and time consuming. Even if you did all this, you'd then have to buy different devices to support, operate, and maintain the infrastructure — not to mention, hire more people!

Deconstructed SBCs

Some vendors offer *deconstructed* SBCs, which provide functionality in several distinct chassis/systems. For example, one is for signaling functions and another is for media functions. You can present valid arguments either way for this approach as opposed to the more common integrated, single chassis SBC, but keep in mind that a deconstructed SBC won't have all the "one box" cost advantages of an integrated SBC.

But if you consolidated all that functionality into a single hardware device — the SBC — you'd realize big cost savings benefits by integrating functionality into a single unit. These savings include the following:

- **Reduced capital expenses:** Simply put, you have fewer things to buy. For those network elements that you need for other functionality, you don't need to overbuild/overspecify them to allow capacity for the SBC functionality that is handled elsewhere.
- **Operating the devices:** You save money on the following examples:
  - **Real estate:** Whether the SBC is in your telecom equipment room, data center, or collocation facility, you need less rack space for a single box solution.
  - **Power:** You don't need to pay for electricity for devices you don't install!
  - **HVAC:** Ever walk into an equipment room or collocation space? There's a lot of heat being generated by all that equipment, and it costs money to cool it.
- **Reduced configuration and management:** A non-unified solution means that you have to use more than one system to configure, maintain, and manage the system and to process all your configuration and policy changes. An SBC provides a single user interface and a single management console instead of the "swivel chair" approach — where your network manager turns knobs and flips switches on multiple consoles to effect one single change or configuration.

Reducing Cost Per Session

In the old days, when communications meant picking up a circuit-switched phone (or even a cellphone) and dialing a number, there was essentially one session (a call) per user. That led to a very predictable network planning and management model — you knew how many phones you had to support and how often (and for how long) they placed calls. You also knew what your network size needed to be and pretty much what your expenses were.

In a VoIP environment, however, the number of sessions per users is both highly variable and growing rapidly. This is called the Bring Your Own Device (BYOD) effect, and it's being driven by two factors:

- The number of applications that an individual uses has increased with no limit in sight.

  Instead of just making voice calls, users are texting, participating in audio and video conferences, screen sharing and white boarding, sending presence messages, and sharing documents. Each of these applications requires its own session with attendant security, call admission, and call routing functionality.

- The number of devices that individuals use grows rapidly.

  It's no longer a desk phone and a computer terminal — it's no longer even a laptop and a cell phone. Now the users you support may have computers, iPhones, a BlackBerry, Android phones, iPads, ultrabooks . . . you name it. And many enterprises are beginning to support BYOD policies, meaning that a network administrator probably has pretty limited control over the number of devices that a user connects to the network.

Sessions matter a lot because computational costs are associated with each and every session, on each and every device. There may be SIP translation required or media transcoding, for example. Even if there isn't, each session is going to involve processing a media stream and examining signaling messages to determine what can be admitted and how to route it.

That's where the right SBC can play a big role. The right SBC is one with the right amount of capacity and scalability and can handle all the signal routing and transformation required in this new session-rich environment. The math is pretty simple: more services times more devices equals a lot more sessions, even for a constant number of supported users. An SBC can provide the capacity to keep the expense of each of these sessions low by efficiently routing sessions and reducing on-campus bandwidth requirements by transcoding voice and video.

Case Study Examples

Sometimes you need more than a few words of theory to understand how a technology makes a difference in your business — you need to understand how other companies are actually implementing a technology to further their business goals and what their tipping points were to make the changes. Well, there's nothing better than an actual case study so you can see things in action.

In this section, I give you world customer scenarios — places where enterprises have installed SBCs from Sonus to meet security, performance, and service goals in their businesses and saved money while doing so.

For confidentiality reasons, I'm not going to say the names of the companies involved here, but believe me when I say that these are companies you already know.

The airline

A major US-based international airline with more than 50,000 employees became a recent marquee customer for SBCs. The primary voice application for this company supported their global call center. As you may imagine, this undertaking is a massively important function for an airline, dealing with reservations, rewards programs, and the countless flight changes, seating assignments, and related calls that a travel-related business deals with every day.

In addition to the call center, the airline needed to support a large number of other voice lines for things like maintenance and support teams, ground support (baggage, fueling, and so on), logistics, in-cockpit and paging systems, airport ticket counters, a highly mobile workforce, and even systems as seemingly prosaic as airport courtesy phones.

The airline's massive telecom needs faced functional and expense-related issues with its legacy systems. Specifically, the airline wanted to

- Move to an all-IP voice infrastructure without discarding an installed base of legacy equipment

- Save money
- Reap the benefits of Unified Communications (UC) by improving employee productivity
- Maintain voice security
- Improve customer responsiveness and satisfaction in a customer-facing environment

The legacy voice systems — TDM PBXs and circuit-switched (ISDN-PRI) voice circuits — were migrated to IP PBX and SIP trunking to reduce voice costs while not immediately abandoning the installed equipment base. At the same time, the airline wanted to centralize control of its voice communications to best provide load-balancing and least cost routing for inbound IVR (Interactive Voice Response) calls from customers.

The airline needed a solution. The answer was SBCs. The airline installed the Sonus SBC as well as a Sonus Policy Server. The Sonus SBC solved the airline's problems with

- Interoperability between legacy TDM and H.323 voice systems and SIP trunking
- Centralized call control and routing
- Secure access for both on-campus and remote call center agents and mobile employees

The results were impressive. Among other things the airline achieved were the following:

- Reduced call costs
  - Least cost routing for all calls
  - Keeping internal calls on the airline's MPLS network instead of carrying them over a carrier's network
- Reduced network operating expenses
- Lower capital expenditures
- Improved up-time and reliability for call center calls
- Secure connectivity for remote workers and home-based call center employees

The retailer

A US-based retail chain with nearly 2,000 stores wanted to consolidate their voice management into a centralized system while migrating from traditional circuit-switched TDM to SIP trunking for cost reduction purposes. Additionally, the retailer had some specific functionality and security requirements related to its business that required features not provided by all competing solutions.

The retailer's needs included the following:

- Save money with SIP trunking
- A centralized policy and call routing control for all stores
- A rapid roll-out, 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
- Maintain security on all calls

With a Sonus SBC and a Sonus Policy Server, two data centers provided the centralized dial plan for all stores. The initial deployments leveraged Sonus to develop an installation plan, to perform configuration, and to develop and implement a test plan. The initial deployment was successfully defined, designed, tested, and implemented in just a few weeks.

Chapter 5

Ten Reasons Why You Should Choose Sonus SBC

In This Chapter

- Performing under pressure
- Being protected from attack
- Attaining better scaling and deployment

Whether you have an enterprise Voice over Internet Protocol (VoIP) network or you're a service provider offering VoIP services to your customers, a session border controller (SBC) can be the right choice for you. The Sonus SBC is a fast-growing SBC solution on the market, and in this chapter, I provide ten reasons why a Sonus SBC may be the best fit for your network needs.

The Simplicity of Local Policy Configuration

If you're looking at a relatively simple VoIP deployment, why not even make it simpler with a simple policy management deployment? Sonus SBCs offer local policy control systems via an embedded policy engine. That means no extra management equipment to install and a system that has all the intelligence needed to screen, route, and modify calls right in the box.

An embedded policy engine makes deployment simpler and faster and keeps your sessions' latency down because all the routing happens right in the box.

Networked Policy Management

You may find yourself in charge of a larger VoIP deployment where the situation calls for more than one SBC — simply because you have more than one network border at which to install an SBC and utilize SBC functionality.

In these cases, you may need to configure your SBCs on your own and enforce policy changes when you have them (and you *will* have them). Without sending an expensive and already overworked technician out to each location to do the work, if your SBCs are networked — if they're connected to a centralized policy server, that is — you only need to make your changes once in one place. The rest is all automatic. Oh yeah, and there's less chance of a change not happening in one location when you do it this way.

Sonus SBCs can help you with this process. You can configure them individually with the local embedded policy engine, or you can network them and let a central policy server keep everything up to date. It's up to you.

Peak Performance

The simultaneous proliferation of applications and devices has led to a situation where the quantity of VoIP traffic on any network is exploding — no matter how you measure it (more on that in Chapter 4). Bandwidth is up due to new, bandwidth-hungry applications like videoconferencing and screen sharing. The sheer number of sessions is also up because each user on the network is accessing more applications, *and* those users are also bringing more devices on the network. Your SBC is going to get a good workout, so be wise and choose one that's proven to be up to the task.

What's making this phenomenon of rapidly growing sessions even more acute is the adoption of enterprise Bring Your Own Device (BYOD) policies. Under BYOD, employees get what they've always wanted: the ability to dump (or at least augment) their clunky "work phones" and antiquated (and probably boat anchor heavy) "work laptops" for the slick iPhones, Android phones, iPads, MacBook Airs, and Ultrabooks they already own. BYOD causes a real and measurable boom in

the number of devices (and therefore sessions) IT managers and networks need to deal with because individuals use more devices, and employees who may not have been "issued" mobile devices begin using them for work purposes.

BYOD is sometimes also called the *consumerization of IT*.

Sonus SBCs provide peak performance under different load scenarios. They've been tested under extreme conditions and even at levels that simulate a full-fledged network attack. Luckily, Sonus SBCs have been designed to have sufficient overhead to keep up.

Better Transcoding

As more and more devices connect to VoIP and other sessions on the network, they put a burden on the SBC to translate between different media codecs (transcode) flowing across the network. There are, in fact, two related issues here:

- The growing number of devices means a greater diversity of the devices themselves and different devices natively supporting different codecs based on the software loaded on them or their manufacturer's design.

  The SBC is essentially the United Nations translator of VoIP, making sure that two devices with different codec support can communicate by translating them on the fly.

- The number of mobile or remote (like home office) devices grows, and devices often (particularly in the mobile environment) face limited bandwidth.

  The SBC can assist in these situations by transrating (or adjusting media bandwidth) as required to ensure that voice, video, and other media are received on both ends of the call without performance issues.

Both transcoding and transrating are computationally complex processes — imagine what it takes to completely disassemble and reassemble a voice or video stream in real-time without inducing noticeable latency or delay into the stream. Many first-generation SBCs don't even include transcoding/rating functionality and not all that do can scale this feature for thousands of simultaneous sessions.

Sonus SBCs can support high levels of transcoding by using dedicated hardware without any effect on other computational functions, such as security and call admissions control — that the SBC must perform.

Security from Attacks

Securing the VoIP network is an increasingly high priority for enterprises and service providers alike. VoIP networks are subjected to malicious denial-of-service (DoS) attacks, similar to the common attacks on corporate websites and services. VoIP networks are also being targeted for toll fraud, Caller ID spoofing, and other attacks designed to steal services, steal secrets, or generally confuse mission-critical communications. (These attacks are covered in more detail in Chapter 1.)

If you're not actively securing your VoIP network . . . well, you should be. And as VoIP traffic increases, it will get attacked even more. That's just the nature of the beast when the beast is a service connected to public networks and the Internet.

One of the primary functions of any SBC is security, and Sonus SBCs are purpose-built to deliver top protection. Sonus SBCs are designed to

- Provide end-to-end encryption on both the media and the signaling components of network traffic
- Hide the topology of the private portions of your network with B2BUA (see Chapter 2 for more on B2BUA)
- Protect the network from DoS and DDoS attacks, while maintaining the capability to still connect legitimate sessions (DoS/DDoS attacks are covered in more detail in Chapter 1)
- Implement blacklists, greylists, and whitelists to keep bad actors out, fully vet the "iffy" connections, and always let in known good connections (these lists are covered in more detail in Chapter 2)

Advanced Media Support

VoIP is moving from a simple voice call replacement for traditional circuit-switched services to a more varied future in which new services — whether you call them Unified Communications (UC) or just by their individual names — become the predominant traffic over the VoIP network.

There will be new challenges revolving around codec support and bandwidth availability as users communicate with different types of media (video or HD Voice) on a variety of devices and across a variety of networks. Codecs and HD Voice are covered in more detail in Chapter 2.

Today's SBCs have to move beyond their traditional "session traffic cop" role and start dealing with these media issues if they want to be future-ready. Specifically, they need to be built with a robust media component that has both the computational horsepower and the appropriate software to perform on-the-fly the transcoding and transrating (see Chapter 3 for more detail) of all sorts of media.

Sonus is future-ready *today.* Its SBCs have these capabilities currently available.

Prewritten Custom Firmware

Many SBC vendors rely on turnkey, off-the-shelf solutions for their digital signal processing (DSP) functionality. This approach means that these vendors buy not only the hardware but also the firmware software code that provides individual features and determines which codecs are supported.

This approach is easy, but the downfall is the SBC manufacture doesn't control or own that functionality. So if you need a fix or two or want new features added, the manufacture will only come when the third-party vendor makes it.

Sonus takes advantage of commodity DSP chips and off-the-shelf components like the audio or video codec software itself and then does the harder work of developing the firmware that makes it all work. This work means big benefits for you (users of these SBCs) because fixes (if needed) or upgrades

can be implemented much faster. And if you have special circumstances in your VoIP network, you can look for custom firmware programming to make your network work for you.

Plays Well with Others

Different vendors and different VoIP networks may speak in slightly incompatible ways when they use Session Initiation Protocol (SIP), covered more in Chapter 1. The result can be calls that simply can't be completed or are degraded in some way (perhaps missing some functionality). The SBC plays a huge role here in understanding the different variants of SIP on the market and can translate between them on the fly.

Sonus SBCs adhere to industry standards for SIP trunking and other applications and can support all known variants of SIP through SIP normalization — translating between different variants of SIP — both according to static rules set up in the SBC or on the fly as varieties of SIP are encountered by the SBC.

Scales Better

At some point, network traffic may grow to where a hardware upgrade is going to be necessary. Perhaps you've just opened a new call center, or (if you're a service provider) your new consumer VoIP service just grew by 300 percent last year (if so, congratulations!). No matter what SBC you have, the real question isn't *if* you'll ever need to upgrade, but *how*.

That's where Sonus SBCs excel. Sonus uses a three-dimensional approach by discretely separating the processing functionality of the SBC so individual tasks, such as transcoding or encryption, can scale up or down without impacting the performance of other SBC tasks. Sonus divides the SBC's processing into three categories:

- **General computing** for things like policy management and call control
- **Network processing** for networking stuff like the interworkings among different IP protocols and routing packets

- **Media processing** for things like transcoding and transrating (covered in Chapter 3)

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.

Deploys Faster

When it comes time to implement an SBC in your network, you want to do it with the least amount of interruption and the least amount of effort as quickly as possible. Most of the time, you're not going to start off with all the in-house knowledge you need to do this implementation quickly. Sonus Global Services can help you plan, install, test, and turn up your SBC in a purposeful and efficient manner. In fact, Sonus can do it all in as little as 48 hours.

Control your daily business telecommunications with an SBC

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.

- ***Control calls in and out of your VoIP network* — *SBCs handle the signaling and media intermediation and translation***
- ***Protect your network security* — *the SBC acts as your security guard***
- ***Understand system requirements* — *make sure you're equipped for an SBC***
- ***Discover other options* — *and why SBC is still the better choice***

Open the book and find:

- **Ways to protect your network**
- **The key features of SBCs**
- **Why you should choose an SBC**
- **How to save money with an SBC**

Making Everything Easier!™

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

For Dummies®
A Branded Imprint of
WILEY

ISBN: 978-1-118-37742-0
Not for resale