

June 15, 2015

9 Reasons to Have Your Own SBC

The big reasons why an on-premises session border controller is necessary.

SIP has been around since the late 1990s, but confusion still exists about what exactly it is and what it can do. Most telephony people understand that SIP changes the way we make voice and video calls, but their understanding is often sketchy.

The confusion surrounding SIP is often greatest when it comes to the Session Border Controller (SBC). People know that it's part of a SIP solution, but they are unsure of exactly why. Unfortunately, even those folks who have a reasonable understanding of what an SBC is used for are still confused as to its placement in the network. Does it sit on the network edge or inside the DMZ? What is its relationship with a company's existing data firewall? Can I split two SBCs between my geographically separated data centers? These questions stymie many experienced voice and telephony managers and their staff.

However, as important as all those questions are, there is a very basic one that needs to be asked and answered first. "My SIP carrier has an SBC in its network. Do I need one, too?"

The simple answer is "yes," but if you are like me, you require more than that. So, in no particular order, here are nine good reasons:

1. I live in a gated community, but I still lock my doors

My home Internet is delivered by Comcast and I am positive that they have a firewall on their end. That doesn't mean that my wireless router and many PCs don't implement their own firewalls. Comcast's firewall is designed to protect their network against anything running on mine. It's not meant to protect me from all the nasty stuff that might be lurking out there on the Internet. That's my responsibility.

The same holds true for a session border controller. A SIP carrier will always have an SBC on its end of the network, but like that Comcast firewall, it's there to protect the carrier against me. Personally, I want control over my own security and I am not about to trust that someone else may or may not protect me from the bad guys. An enterprise's first line of defense needs to be an SBC that it owns, configures, and manages.

2. SIP Firewall

At its core, an SBC is a SIP firewall. It performs deep packet inspection to ensure that only properly formatted SIP messages enter an enterprise's network. It maintains a list of known "SIP viruses" (e.g. SIP Vicious) and prevents them from wreaking havoc on your users, servers, and services. It stops denial of service (DOS) and distributed denial of service (DDOS) attacks. It maintains a black list of IP addresses of known hackers. It monitors failed login attempts and blocks potential hackers. It prevents registration floods from bringing down your call server.

3. Call Admission Control

Only you know the bandwidth configuration and usage of your network, so it makes sense that an enterprise's SBC perform call admission control duties. These duties need to extend to all forms of communication. A high definition video call will consume significantly greater bandwidth than an audio call. An SBC can ensure that call quality remains high regardless of your chosen form of communication.

4. Network Address Translation

The world ran out of IPV4 addresses a long time ago and nearly every enterprise uses a large number of private IP addresses and a very small number of public IP addresses. Since IP addresses are embedded inside SIP messages, you need something to map those private addresses to a small pool of public addresses. This Network Address Translation (NAT) can be performed by your enterprise SBC. Without a NAT element, SIP communication outside the bounds of your network is impossible.

5. Adaptation

I deal with medium to large enterprises on a daily basis and it's rare to find one that isn't a hodge-podge of communications systems, software versions, applications, and trunk providers. Sadly, even though SIP is "a standard," there are a number of variants and interpretations that make interoperability much more difficult than it should be.

SBCs offer adaptation tools that manipulate SIP messages into forms that different vendors and products require. This allows Cisco to speak to Avaya to speak to Nortel to speak to AT&T.

6. Media Twining

We've all called into a contact center and heard the words, "This call may be recorded for quality purposes." In the TDM world, you typically had to have special hardware to tap into a trunk and split the audio into two different paths. A number of SBCs do that in software, making them the perfect spot to implement call recording.

7. Transcoding and Translation

Transcoding and translation are required when you have two different communications elements that need to interact with each other, but don't have a common form of speech. For instance, you might need to translate H.323 to SIP. You might also need to transcode codecs -- e.g. G.729 to G.711. Other transcoding/translating opportunities include IPV6 to IPV4, SRTP to RTP, and TLS to unencrypted SIP.

Your carrier will not do this for you and a customer-premise SBC is required.

8. WebRTC Gateway

WebRTC is the new kid on the block, and enterprises are looking for ways to welcome him to the neighborhood. They've invested big dollars into their current contact center solutions and want to integrate WebRTC into those existing practices.

As they did with transcoding and translation, SBC vendors recognized the need to blend this new technology with legacy communications and are adding WebRTC gateway functionality into

their products. This allows enterprises to WebRTC-enable existing contact center agents with a single edge device.

9. Routing

Remember the hodge-podge of communications systems and applications that I constantly run into? An SBC can also help your enterprise route SIP sessions between them. A common case would be to have one ingress/egress point for SIP trunks that is distributed amongst a number of disparate SIP PBXs. Centralization of resources not only makes maintenance easier, but it saves money by eliminating duplication.

Mischief Managed

There may be a few more reasons why an on-premises SBC is a necessity, but these are the big ones. Clearly, security is important, but so are routing, translation, call admission control, etc. Even in the cases where an enterprise shares these responsibilities with its SIP carrier, some form of local control is required. As I said earlier in this article, you might live in a gated community, but you still lock your doors.



This article was published on the web site www.nojitter.com

Andrew Prokop has been heavily involved in the world of communications since the early 1980s. He holds five United States patents in SIP technologies and was on the teams that developed Nortel's carrier-grade SIP soft switch and SIP-based contact center. His software currently exists inside products from Avaya and Genband. He has now found a home at Arrow Systems Integration where he holds the position Director of Vertical Industries. Through customer engagements, users groups, tradeshow, and webinars Andrew has been an evangelist for SIP as a transformational technology for enterprises and their customers. Andrew understands the needs of the enterprise and has the background and skills necessary to assist companies as they drive towards a world of dynamic and immersive communications. Andrew is an active blogger and his widely read blog, SIP Adventures, discusses every imaginable topic in the world of unified communications. He is just as comfortable writing at the 50,000 foot level as he is discussing the subtle nuances of a particular SIP header. Andrew can be found on Twitter at @ajprokop.