Who Needs an Enterprise Session Border Controller?

What key challenges does an eSBC address for providers and subscribers of IP-based business communications?

PATTON®
let's Connect!™

Contents

Authored by

W. Glendon Flowers
Product Marketing Manager,
Patton Electronics Co.

Printed in the USA.

Executive Summary

This paper covers how an Enterprise Session Border Controller (eSBC) addresses key challenges the various players in the arena of All-IP (or legacy-IP hybrid) business communications face today.

We explain how and why network operators (carriers) and service providers (including cloud and OTT) that attempt to implement SIP-trunking or hosted-communication services without an eSBC (or with a bad one) cut corners on quality, security and reliability—with potentially catastrophic consequences.

While outlining the important functions an eSBC can provide, we argue providers should never offer IP-communication services without this essential network element. Subscribers should never accept such services without an eSBC—or else install their own.

Background: The (Inevitable) Transition to IP Communications

Over the past decade Internet Protocol (IP) telephony or Voice-over-IP (VoIP) has become the de facto standard for business communications. The business VoIP service market is expected to reach $35 billion by 2018[1].

Although many companies still use their legacy Public Switched Telephone Network (PSTN) lines and voice equipment (traditional TDM*-based PBX** [or key systems] and phones), SIP trunks, IP phones, IP PBXs, and—more recently—unified communications software are now commonplace. The new IP-based products and solutions will surely supplant traditional voice technologies eventually. As usual, all actors in the arena looking for ways to leverage the new and evolving packet-based communication technologies to save money, make money, ***avoid pain***, and increase productivity.

Equipment manufacturers, software vendors, services providers and their business customers all have skin in the game. New business models have emerged: downloadable or hosted IP PBX software (3CX for example), cloud-based and Over the Top (OTT) delivery of SIP trunking and unified communications services are among them.

Trending: SIP Trunk Adoption

Regarding trends in SIP trunk adoption, according to the October 2015 IHS Infonetics survey report[2], we may observe the following:

- Today 45% of businesses in North America use Session Initiation Protocol (SIP) technology for at least some of their voice communications. With legacy T1

*Time Division Multiplexing **Private Branch Exchange

trunk subscriptions shrinking fast, that number is expected to reach 62% by 2017.

- The currently crowded market where no single player dominates is wide open for new SIP trunking providers.
- Surprisingly, those surveyed did ***not*** cite cost savings as the chief driver for implementing a SIP trunk. Instead flexibility, easier management, and improved reliability were named as primary considerations.
- Many businesses are migrating to SIP trunking, yet few have made a complete system-wide conversion. Among those replying to a survey, SIP-based telephony represents less than 50% of overall voice trunk capacity.

Dangerous Temptation (Don't fall for it!)

For businesses that deploy SIP trunks (whether primarily to cut costs, or for other reasons mentioned above) and for service providers seeking to profit by SIP trunk delivery, it may be tempting to cut corners by using lower cost network elements, or by omitting devices that some might consider non-essential but nice-to-have. With dangerous (and costly!) consequences, some consider the Enterprise Session Border controller as falling into in this category.

SIP Trunking Risks

More than once we have heard the question posed: "Why can't I just connect my IP phone or my IP PBX to a SIP trunk?" Our answer: "Well maybe you can, but the risks will probably not be worth it to you."

For **business subscribers** such risks may include:

- Unexpected and unexplainably high phone bills [toll fraud]. During 2013 Internet-based toll fraud cost small businesses victims $4.73 billion globally[3]. According to the latest Communications Fraud Control Association (CFCA) report, that number reached $6.08 billion in 2015[4].

- Network failure and downtime [denial of service (DoS) attacks or security breaches (hacking, spamming, tampering, etc.)]
- Failed, delayed, over-budget implementation project [interoperability issues with provider protocols and devices (softswitch, routers) and subscriber-owned (on-premise) devices and software]

- Unintelligible or garbled sounding phone calls [Quality of Service (QoS), jitter, packet loss, etc.]

For **carrier/service providers** the risks are similar:

- **Security**—subscribers poking and meddling with your WAN
- **Liability**—responsibility for malicious intrusions from your WAN into your subscriber's LAN
- **Service quality**—losing subscribers because of poor voice quality or unreliable service
- **Interoperability**—potential business customers have selected innumerable brands of (traditional or IP-based) PBXs and phones. How many can you realistically certify for guaranteed interoperability with your network elements, protocols, and services?

VoIP Technology Challenges

Any technological breakthrough involves pros and cons—expected benefits and unintended (negative) consequences. VoIP technology offers many benefits. For business customers, VoIP offers lower communications costs and enables richer productivity-boosting communication features. For carriers and service providers, VoIP enables converged network architectures that promise lower operating expenses along with new revenue-generating opportunities from IP-based service offerings. Yet the technology brings with it some "under-the-hood"[5] issues that give rise to the vulnerabilities outlined above.

The primary technical challenges introduced by packet-based telephony include the following:

- **Firewall holes**—Admitting voice traffic into the company LAN requires disabling certain firewall mechanisms to create "pinholes" for packet-based (VoIP) phone calls. Session Initiation Protocol (SIP) signaling and Real Time Protocol (RTP) media ports must be unblocked, leaving the enterprise network vulnerable to **snooping**, **hacking**, and **toll fraud**.

- **Interoperability**—SIP technology is a "soft" standard. Carriers, service providers, and vendors of VoIP hardware and software implement the protocol in different ways, creating incompatibilities interoperability failures). That means new VoIP installations are likely to require extensive testing and troubleshooting, with possible replacement of non-interoperable elements before the system finally works.
- **Bandwidth management**—Voice traffic is much more sensitive to packet loss, transmission delays, and speed variations (jitter) than other types of data (email, websites, file transfers, and so on). So when a co-worker initiates a large file transfer, or watches online video, voice quality typically suffers, and calls may disconnect midstream.
- **Reliability**—The old copper-wire telephone network is comparatively simple, and extremely reliable. The Internet…not so much. IP telephony runs over a complex computer-based network that is unfortunately characterized by occasional outages. Such network failures can cause gaps in a company's phone service resulting in disrupted communications and loss of business continuity.

The Solution: a High-Quality eSBC

For carrier providers as well as their business subscribers, employing a robust, feature-rich eSBC at the subscriber premise addresses the above liabilities of VoIP technology. Such a device should provide the following functions:

- **Security**—Network separation/demarcation/split domain, intrusion prevention, encryption
- **Interop assurance**—SIP normalization
- **Voice quality assurance**—Quality of service
- **Bandwidth management**—WAN optimization, transcoding
- **Business continuity**—Network survivability, PSTN fallback, SIP registration
- **Legacy support**—Classic telephony ports for IP-enabling traditional TDM trunks, PBXs and phones
- **Auto-provisioning**—Web-based automatic configuration download and service activation

Vendor Selection

Before we describe these functions in further detail, an important caveat must be made: not all eSBCs on the market provide the comprehensive function set we have outlined. So, while an eSBC is critically important for a successful SIP-trunking customer experience, **it is equally important to select the *right* eSBC**—one that delivers ***all*** the required functions for the customer's environment and application.

Security

VoIP systems can be vulnerable to cyber-attacks such as eavesdropping, voice or VoIP phishing (vishing)[6], theft of service (toll fraud), identity theft, call tampering, malware or virus infections or SPAM over Internet Telephony (SPIT)[7]. To protect a business subscriber against such security threats, a good eSBC should provide the following functions:

1. **Network separation**. A high-quality eSBC will provide a rich set of security features that protect the provider WAN network and the customer LAN from *each other*, as well as from external security vulnerabilities. Serving as a clear (physical and logical) demarcation point, the best eSBC solutions provide a divided configuration architecture that isolates WAN-facing parameter settings from the LAN-facing configuration. Such separation protects each side of the demarc from legal and professional liabilities, as well as (possibly unintended) tampering or human operator errors.
2. **Intrusion Prevention**. Protocol mechanisms that protect against intrusions from unauthorized sources include such IP router functions as address filtering, Network Address Translation (NAT) and stateful firewall. These, combined with registration, authentication and access control at the SIP protocol level, are necessary.
3. **Encryption**. Failing to encrypt the SIP signaling data can expose such information as user credentials, phone numbers, IP addresses and aspects of the company network topology to malicious intruders. To prevent such "man-in-the-middle" attacks as wire-tapping, eavesdropping, and hacking, both SIP signaling information and media content (digitized voice) must be protected (hidden) by encryption. An early technology solution that covers both concerns is VoIP-over-VPN technology (Virtual Private Network tunneling with IPsec encryption). Although setting up the VPN tunnel does tax the WAN connection (at both ends of the call) with additional overhead, it provides a strong level of VoIP security. More recent encryption standards, which are more efficient with respect to bandwidth consumption and designed specifically for IP telephony, are the Transport Layer Security (TLS) protocol for signaling and Secure Real-time Transport Protocol (SRTP) for media content. For secure business-class VoIP, an eSBC must provide at least one of these encryption solutions.

Interop Assurance

Although SIP, as specified by Internet Engineering Task Force (IETF), is classified as a standard, there is in reality no such thing as a “standard” implementation of the protocol in the real world. The SIP working group[8] has defined about eighty Request for Comments (RFCs), while as of this writing, over thirty RFC drafts remain in progress. With so many optional feature [such as Connected Line Identification Presentation (COLP), Advice of Charge (AOC), etc.], there is a great deal of variation in how vendors choose to implement the specifications in their commercial products and services. For example, some systems (Microsoft Skype for Business for example) employ Transmission Control Protocol (TCP) for SIP transport, while other implementations employ User Datagram Protocol (UDP). The two solutions are not interoperable.

SIP normalization. The bottom line is…without an eSBC to translate (normalize) between the various "dialects" of the SIP protocol, a subscriber's chosen PBX and phones may or may not work with a given providers SIP trunking service, softswitch, and network. To address this challenge, either the provider or the subscriber should select and deploy a high-quality eSBC—one that has been tested and certified to provide SIP normalization for interoperability between most of the PBX and phone products on the market and all major-brand network operators and ITSPs.

Voice Quality Assurance

Quality of service. Since VoIP traffic shares the WAN connection (Internet access link) with the rest of the company's data traffic, measures are required to ensure the phone calls don't get bullied by bigger data streams (large file transfers, streaming music and/or video). The eSBC should provide dual Quality of Service (QoS) mechanisms that include:

- **Bandwidth Reservation**—minimum link capacity allocated for voice packets
- **Downstream QoS**—throttling mechanisms that limit and slow down large downstream data bursts to prevent flooding the capacity of the link.

Bandwidth Management

WAN Optimization. For a business, the capacity (bandwidth) of the Internet connection is a critical resource. A good eSBC can help a company manage that resource more effectively. The CEO's phone call with a key client, business partner, lawyer, or bank should take priority over the YouTube video his son is watching in a cubicle down the hall. By identifying traffic types, and dividing into segments for data, voice, video, and so on, portions of the WAN link can be allocated with appropriate capacity for each data type.

Transcoding. Finally, LAN capacity is normally much greater than the WAN access link. So intra-office callers (behind the eSBC) can benefit from the enhanced quality of high-bandwidth G.711 or high-density (HD) G.722 voice CODECs. The eSBC can reduce WAN-access bandwidth requirements by converting those high-bandwidth LAN calls into lower-bandwidth G.729 calls for transport on the WAN uplink (and vice versa).

Business Continuity (Network Survivability)

PSTN Fallback. Only a hardware eSBC device with legacy telephony ports (PRI, BRI, T1, E1, FXS, FXO) can provide PSTN fallback when the Internet link goes down. An eSBC that provides a failover mechanism (such as IP-link redundancy), and that also provides media gateway and IP routing functions, can deliver survivability for voice ***and data*** over a fallback connection to the local phone company (PSTN).

SIP Registrar. Within the office, an eSBC that provides SIP registrar functionality can support local (intra-office) SIP calls over the company LAN—without any external net-

work connections (standalone survivability). Further, by registering as SIP terminals with the local eSBC, the VoIP phones can still make calls over the PSTN during lost connectivity to the SIP service provider.

Legacy support

According to a recent survey[9], 44.14% of responding businesses had transitioned to an IP-based PBX, while only 1.55% still relied solely on a TDM-based PBX. Yet over **45%** were operating with a hybrid solution of legacy TDM and SIP/VoIP telephony systems. Clearly legacy is not dead!

So, what's going on here? While the advantages of IP telephony may be compelling, trashing a working, bought-and-paid-for legacy PBX solution seems counter-intuitive to many businesses. Instead, why not IP-enable existing legacy phone systems and get the best of both worlds?

An eSBC that provides legacy interfaces that IP-enable existing ISDN and POTS business phone systems helps businesses preserve the value and extend the useful life of their of their capital investments in traditional telephony solutions. While taking advantage of the cost-saving and operational benefits of IP telephony, such solutions enable companies to migrate to converged communications at the pace they deem most comfortable and cost-effective.

Auto-provisioning

Finally, in today's world of ubiquitous Internet connectivity and computer automation, doesn't it seem a bit ridiculous to expect a phone company to have to send a man in a truck to each and every business they sign up as a new subscriber? Right. The best eSBC vendors include some sort of automated provisioning service. The on-premise IT person for the business subscriber should only need to plug in the cables and power up the device. A good one will automatically download the customized configuration and activate service with the ITSP. So, make sure you pick a good one.

Conclusion

The short answer to the question "Who needs an Enterprise Session Border Controller?" is "Everybody." Everybody being those who are concerned about:

- Toll fraud.
- Denial of service attacks
- Snoopers, eavesdroppers, and hackers
- Garbled, unintelligible voice quality
- Failed, delayed and/or over-budget deployments due to interop failures
- Disrupted business communications (lost revenues) stemming from system downtime

Carrier-providers and their enterprise subscribers must recognize the eSBC is a necessary network element for successful implementation of any IP-based business communications solution.

So, more specifically, **for all the reasons explained above**…

ITSPs—Internet Telephony Service Providers, (including providers of cloud-based or hosted services) should provide an eSBC to each subscriber as part of the SIP trunking service package. By testing and certifying interoperability with a selected eSBC vendor that interoperates with popular PBX and phone solutions, the network operator can:

- Expand potential customer base by serving a broad variety of IP-based and traditional TDM products.
- Simplify and streamline customer turn-up with a standardized interface at the customer premise.
- Eliminate costly truck rolls for new subscribers—provided the eSBC vendor offers an automated provisioning service.

OTT Providers—Over the Top (**OTT**) providers of SIP trunking, cloud-based, and/or hosted telephony services do not control the access link to the subscriber, since it is provided by a third-party network operator. That makes it much harder to control (assure/guarantee) the service quality and customer experience. If the access-link provider does not supply a good eSBC with strong QoS mechanisms, then the OTT provider had better do so.

Further, an eSBC that includes link-monitoring capabilities (for example the Broadsoft PacketSmart probe), enables the OTT to analyze, troubleshoot, and fault-isolate quality issues (packet loss, jitter, etc.) related to the delivered connection—and hold the operator accountable for providing remedial measures.

Enterprises—If the service provider you're considering for a SIP-trunk, hosted, or cloud-based communication service doesn't bundle in an eSBC, shouldn't you be wondering at this point what they are thinking? That said, there may be scenarios (most likely in remote/rural regions) where the only available local provider doesn't supply an eSBC as part of the service offering. In such a case, if you are going to transition to IP telephony, you probably should select and install your own eSBC.

Endnotes

1 http://searchunifiedcommunications.techtarget.com/news/2240221255/Business-VoIP-services-market-to-reach-35-billion-by-2018

2 http://www.infonetics.com/pr/2015/SIP-eSBC-Survey-Highlights.asp

3 http://www.nytimes.com/2014/10/20/technology/dial-and-redial-phone-hackers-stealing-billions-.html

4 http://www.informationsecuritybuzz.com/study/survey/the-rise-and-fall-of-global-telecom-fraud

5 http://www.scmagazine.com/exploiting-voip-vulnerabilities-to-steal-confidential-data/article/111091/

6 http://searchunifiedcommunications.techtarget.com/definition/vishing

7 http://searchunifiedcommunications.techtarget.com/definition/SPIT

8 https://tools.ietf.org/wg/sip

9 https://www.edgewaternetworks.com/2016/01/cloud-and-hosted-service-adoption-surprisingly-low

PATTON®
Let's Connect!™

7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
tel: **+1.301.975.1007**
fax: **+1.301.869.9293**
web: **www.patton.com**
email: **marketing@patton.com**
Document: 07M-WNAESBC-WP