Firewalls vs. SBCs

Understanding the OSI Stack Model and Implications for RTC

White Paper

Contents

Introduction

Companies of all sizes are implementing VoIP solutions to better support globalized business and mobile workforces. Despite slow adoption in the early days of VoIP, Robert Fine says, “the [VoIP] industry as a whole is set to grow to more than $76 billion in 2015, and the number of small office/home office subscribers is projected to grow to $262 million - a 50 percent increase since 2011.” VoIP adoption isn’t showing any signs of slowing down, but implementation and management isn’t without challenges.

Traditional telephony infrastructures were subject to call diverting, rerouting, and eavesdropping as hackers illegally controlled enterprise telephone networks. PSTN networks are giving way to VoIP solutions, but that doesn’t mean the traditional security concerns are disappearing. Instead, cyber criminals take advantage of the willingness of enterprises to open their communications to the Internet with VoIP.

Many companies believe that firewalls are sufficient security measures to protect against many different threats, but in reality VoIP are best secured with enterprise session border controllers (eSBCs). While firewalls and SBCs seem to accomplish the same security goals, examining their differences at the OSI stack level reveals the need for SBCs to properly ensure VoIP security.

What is the OSI stack model?

An examination of the open system interconnection (OSI) model is essential for understanding the key differences between firewalls and SBCs in communications solutions. The framework splits the process of internetworking into a vertical stack with seven layers. Although the model does not play a real role in the process of sending packets in VoIP, the concept itself is vital to the discussion.

OSI Model

	Data	Layer
Host Layers	Data	**Application** Network Process to Application
	Data	**Presentation** Data Representation and Encryption
	Data	**Session** Interhost Communication
	Segments	**Transport** End-to-End Connections and Reliability
Media Layers	Packets	**Network** Path Determination and IP (Logical Addressing)
	Frames	**Data Link** MAC and LLC (Physical Addressing)
	Bits	**Physical** Media, Signal, and Binary Transmission

Layer 1 – The Physical Layer: This is the mechanical layer of the OSI stack. The physical layer provides means of processing data from service providers or carriers. When two nodes are connected directly, this layer establishes and terminates connections.

Layer 2 – The Data Link Layer: At this layer of the OSI stack, data is both encoded and decoded. It is separated into two sections: media access control (MAC) and logical link control (LLC). The MAC layer is essential in communications as it controls access to data and permits transmission.

Layer 3 – The Network Layer: Switching and routing are the primary function of the network layer. This level of the stack enables traffic control.

Layer 4 – The Transport Layer: This layer completes the data transfer process and is responsible for transferring packets between hosts.

Layer 5 – The Session Layer: This is the first layer that deals with applications. It is responsible for establishing, coordinating, and terminating connections at each end of the conversation.

Layer 6 – The Presentation Layer: By managing data representation, this layer is able to translate encryption and prevent compatibility issues.

Layer 7 – The Application Layer: This is the user-facing layer of the OSI model. User authentication, Quality of Service (QoS) control and application services are managed at this level.

The OSI model helps to clearly differentiate the functions of firewalls and eSBCs. While firewalls control Layer 2 to Layer 4, eSBCs excel in Layer 7 functionality without giving up control of Layer 2 to Layer 4.

Firewalls vs. SBCs:
Implications for real-time communications solutions

Business communications systems are critical and need to be available 24/7 – InfoSec professionals can't just turn traffic on and off at certain ports and still expect a business to run.

Certainly, firewalls can be deployed as a SIP proxy server and that can relay and control SIP signaling information. However, because the server is not actively involved in the real-time transport protocol (RTP) media path, they cannot control real-time communications in a way that ensures a quality voice or video connection. On the other hand, SBCs are designed specifically for IP communications management and security and provide key advantages over standard firewall technology:

- Session Layer (5) control
- Presentation Layer (6) control
- Application Layer (7) control
- Protocol transcoding
- Visibility into voice and video KPIs such as jitter, latency, throughput, and more
- Dynamic policy control for communications applications

In real-world situations, SBCs are fully aware of the SIP stack and can manage both voice and video traffic in real time. Paul Desmond of UC Buyer note put it this way:

"[SBCs] can 'peel the onion and have an inherent awareness of where packets are coming from and going to, how they should be formed and how to identify malformed packets," Negron says. "Those malformed packets may be legitimate packets or could be malicious; with its awareness of the larger picture, an SBC can tell the difference whereas even a SIP-aware firewall could not."

How SBCs ensure VoIP security

SBCs go beyond simple SIP termination and network address translation. According to network security expert Zeus Kerravala, there are five key security concerns that SBCs can take care of that firewalls can't:

Protecting from malicious attacks: When Denial of Service (DoS) and distributed DoS (DDoS) attacks occur, they flood networks with malicious traffic in an attempt to shut down systems and probe for weaknesses. SBCs can easily separate VoIP traffic from the malicious activity allowing only the authorized voice traffic to pass through and dropping the rest.   With an SBC's access to Layer 7 of the OSI model, they can dynamically adjust resource allocation to insulate communications systems from the degradations in Quality of Service that occur with DoS and DDoS traffic spikes.

Toll fraud protection: An increasing amount of hackers are breaking into business VoIP systems to make personal calls. With an SBC in place, organizations can program the VoIP solution to deny secondary dial tones.

Encryption: Real-time communication messages are fairly easy for hackers to intercept. However, Kerravala says, "SBCs use Transport Layer Security to secure the signaling traffic and make it invisible to hackers. To secure media packets and add another layer of protection, SBCs use the Secure Real-time Protocol."

Topology hiding: Communicating between two networks can give unauthorized users access to enterprise network topology. SBCs eliminate this risk by hiding the topology throughout communications.

IP traffic management: Essentially, SBCs limit the number of sessions that can take place at the same time. Much like DDoS protection, IP traffic management ensures Quality of Service by mitigating the effects that massive call volumes can have on the system as a whole.

Avoiding conflicts

As firewalls and security policies have become increasingly complex, the chances of traffic flows being disrupted and real-time communication solutions has also increased. Security teams are constantly updating firewalls, applying patches and writing new access rules. Because these changes are applied to Layers 3 and 4 – and not 5, 6 or 7 – they often wreak havoc with performance at the session and application layers.

There are two basic methods for eliminating the conflicts between firewalls and SBCs and preempting poor voice and video service. The easiest solution is to connect SIP Trunks directly to the SBC and let the appliance take the lead for the security and traffic management of IP Communications.

Companies that prefer to have their firewalls take the lead still need an SBC to prioritize QoS, ensure call quality and enable interoperability across all communications applications. This will help mitigate some of the problems that occur when firewalls redirect traffic at Layers 2-4 and not Layers 5-7. However, they cannot solve others. In this configuration, security teams must make a concerted effort to fully test all changes made to firewalls for their impact on real-time communications prior to deployment. More importantly, they need a way to take firewalls out of band – just for a second – to accurately troubleshoot problems and quickly determine their role in application level problems.

Conclusion: combining SBCs and firewalls ensure total VoIP security

As organizations of all sizes implement VoIP solutions, assuring both security and quality needs to be a priority. While firewalls and ESBCs seem to accomplish similar security goals on the surface, a look at their OSI model functions prove that there are major differences at the QoS level. Real-time communication solutions have unique requirements. Even the slightest disruption at the network level can lead to garbled speech, static-ridden conference calls, video pixilation and sound issues.

Understanding how firewalls and SBCs control traffic and implement security policies is the first step to creating a network design that protects vital communication systems while providing users with the QoS levels they need to do their jobs on a daily basis. Without an SBC in the mix, IT groups will find themselves constantly fielding complaints from users and chasing issues that can be extremely difficult to resolve over the long run.

About Ribbon Communications

Ribbon is a company with two decades of leadership in real-time communications. Built on world class technology and intellectual property, Ribbon delivers intelligent, secure, embedded real-time communications for today's world. The company transforms fixed, mobile and enterprise networks from legacy environments to secure IP and cloud-based architectures, enabling highly productive communications for consumers and businesses. With locations in 28 countries around the globe, Ribbon's innovative, market-leading portfolio empowers service providers and enterprises with rapid service creation in a fully virtualized environment. The company's Kandy Communications Platform as a Service (CPaaS) delivers a comprehensive set of advanced embedded communications capabilities that enables this transformation.

To learn more visit RibbonCommunications.com