

SIP Trunking

Enabling new collaboration and keeping the network safe with an E-SBC

A Sipera Systems White Paper

Summary

SIP (Session Initiation Protocol) trunking extends the capabilities of enterprise telephony systems by enabling new features and functions; the primary method of terminating SIP trunks within the enterprise is via an enterprise session border controller (E-SBC). Flexible and cost-effective, SIP trunks make a great deal of business sense for companies to deploy and use the converged IP connection for all its communication with calls routed over the carrier's IP backbone using voice over IP (VoIP).

Yet as with any technology, SIP trunking requires some education - not all SIP is equal, and to derive the maximum benefit from a SIP trunking solution it pays to understand all the various dimensions including security and deployment challenges. Fortunately, with the right solution all the necessary security can be enabled and deployment challenges resolved.

A comprehensive SIP trunk security solution must provide for four requirements:

Enablement: facilitating enterprises communications in a seamless manner, and in a way that lays the foundation for security.

Control: managing users and their access to services and features to ensure that the system and its resources are being used correctly, in keeping with the needs of the business and overall security policies.

Protection: defending communications against signaling and media vulnerabilities.

Demarcation: clear line of defense and termination for SIP trunks within the enterprise.

This paper will look at the business case for deploying SIP trunks, the requirements for securing SIP trunks and the features needed in a SIP trunk security solution.

Starting Points

By radically transforming voice and data communications, IP technology has also transformed the ways we think about voice and data communications. Where historically separate infrastructures were needed to carry different types of traffic, now one alone can handle it all, yielding significant economies in the process. At the same time, new features and functions are enabled, bringing unprecedented flexibility and convenience to the daily tasks of the enterprise and increasing employee productivity.

All this is true of SIP trunking, which uses the VoIP standard to establish an Internet-based connection between the public-switched telephone network (PSTN) and an enterprise's SIP-compatible gateway or IP PBX.

The benefits of SIP trunking are many. It eliminates the need for costly time-division multiplexing (TDM) trunks and gateways and introduces innovative capabilities to direct and manage communications. For unified communications, SIP trunks deliver expandable bandwidth that enables a new generation of rich media services including: high-fidelity voice, high-definition video, and video-based collaboration.

With SIP, traffic is not limited by the strict timeslot capacity of TDM trunks and call capacity can be scaled easily. Bandwidth can be allocated dynamically based on the application mix or number of sessions to ensure the optimal performance of applications in use.

A Different Frame of Mind

Just as VoIP originally enabled voice convergence with the enterprise LAN, SIP trunking achieves convergence externally over the WAN/Internet. And for that reason, it requires a change in the way enterprises think about their voice networks.

In the past voice networks were truly private, isolated and self-contained; SIP trunks create an interface with the public networks (e.g., the Internet or a service provider network) extending beyond the enterprise's borders. To protect the security of all communications, demarcation points must be well defined, privacy of communications ensured and fine-grained control applied to enforce call routing and security policies.

The Four Essentials

Security is a fundamental prerequisite to an enterprise-grade SIP trunk, yet it is all too often overlooked. Any comprehensive security solution for SIP trunking must provide:

Enablement: facilitation of seamless and secure enterprise communications with high quality of service (QoS);

Control: effective management of users and their access to services, features and functions, ensuring that the system and its resources are utilized in keeping with business needs, user requirements and security policies;

Protection: end-to-end assurance against signaling and media vulnerabilities;

Demarcation: clear line of defense and termination for SIP trunks within the enterprise.

The object is to allow companies to derive the greatest benefit from their SIP trunk solutions, unimpeded, while ensuring the overall integrity of the network and its traffic and show substantial ROI.

The Business Case for SIP Trunks

SIP trunks present a compelling business case to enterprises for a number of reasons. The capital cost is lower than that of traditional PSTN connectivity because there is no need to own lines or TDM equipment (which also has the longer-term advantage of lower maintenance costs) SIP trunks can support a greater number of lines than conventional PRI (primary rate interface) connections. And they can deliver local, toll-free, domestic and international long-distance service at a much lower cost than is possible in a TDM-based PSTN scenario.

By way of example, consider a large enterprise of 2,500 employees with an oversubscription rate of 10:1 and an estimated long-distance tariff for traditional long-distance calling of \$0.04 per minute. In this case, 250 simultaneous voice calls must be supported at any given time. Using TDM, it would be necessary to deploy 11 PRI connections over T1 lines to meet the demands. We will assume a TDM gateway already in place and if not, one would have to be deployed at a significant capital cost.

As FIGURE 1 shows, the E-SBC solution has a rapid payback period in under a month .

TDM Option				Carrier SBC Option				E-SBC Option			
Item	Qty	Unit Cost	Total	Item	Qty	Unit Cost	Total	Item	Qty	Unit Cost	Total
Capital Cost (list price)				Capital Cost (list price)	1	\$48,000	\$48,000	Capital Cost (list price)	1	\$3,900	\$3,900
Total Capital Cost			-	Total Capital Cost			\$48,000	Total Capital Cost			\$3,900
Monthly Operating Costs				Monthly Operating Costs				Monthly Operating Costs			
PRI connection	11	\$1,000	\$11,000	SIP trunk charges	250	\$20	\$5,000	SIP trunk charges	250	\$20	\$5,000
LD charges	25,000	\$0.04	\$1,000	LD charges	25,000	\$0.02	\$500	LD charges	25,000	\$0.02	\$500
Total Monthly Operating Costs			\$12,000	Total Monthly Operating Costs			\$5,500	Total Monthly Operating Costs			\$5,500
PAYBACK				7 Months				2 Weeks			

The same organization with the same needs could deploy SIP trunks to support 250 simultaneous VoIP calls in a SIP trunk scenario and there are 2 options for a session border controller (SBC) in the network DMZ. One is the industry standard carrier SBC and the other is a purpose built Enterprise SBC (E-SBC). The long-distance cost in either SBC case is half that of the PSTN scenario.

It's not surprising then that enterprises are moving to SIP trunks to shed the cost burdens of PSTN trunks and gateways. Increasingly, instead of simply swapping out one infrastructure for the other and using SIP trunking as a means of enabling same-old voice services, enterprises are also more knowledgeable about the ability of SIP trunks to support real-time Unified Communications applications with potential to increase the productivity of their workforces. In large part, the single most important decision to make when moving to SIP trunks is the type of appliance to be used for the enterprise demarcation point.

New Possibilities, New Challenges

The fundamental components of the SIP trunk architecture on the enterprise side include a PBX - either IP-based or hybrid (TDM and IP) - to process enterprise call functions, user devices connected to that internal network, and border elements that create a 'DMZ' between the internal network and the Internet beyond where the SIP trunk connects to the Internet telephony service provider's (ITSP) network. Key functions required within a conventional SIP trunk architecture include: topology hiding, QoS reporting, SIP routing, high availability and threat protection.

One of the challenges associated with SIP trunking today is that there can be many flavors of SIP. Though it is standardized, the standards allow room for flexibility and interpretation. Consequently, a PBX or firewall may be SIP-compliant on paper and still incapable of communicating effectively with other SIP devices.

For example, many PBXs that claim SIP interoperability really possess fairly basic capabilities.

They may be able to direct traffic to specific IP addresses, but lack the finer functionality to perform more advanced calling features. Interoperability is hardly guaranteed, inside the network - or outside of it, in the service provider domain.

Such interworking needs, however, are relatively standard problems solved by standard solutions, provided the correct equipment is purchased. The real problem that needs to be addressed is security. Enterprises tend to trust their carrier's network overlooking the fact that it may not implement the same strong security policy used by the enterprise to protect its network and that any breach on the carrier's network could jeopardize the SIP trunk.

Imagine if one enterprise is attacked. The numerous servers running complex applications could be used to propagate attacks, impairing the trunk and causing denials of service not only to the originating enterprise but also to other customers on the same carrier network.

The Issue of Security

The reality is that in tandem with all the benefits and flexibility SIP trunking provides, it has distinct and more intensive security requirements than TDM. A TDM PSTN gateway provides an explicit demarcation point between the enterprise network and service provider combined with engrained security features. When SIP trunks are implemented, security concerns arise. It is extremely difficult for a malicious external user to traverse the network interconnection and access the enterprise network through the traditional TDM trunk while it is fairly easy to do so when the interconnect point is IP.

Because SIP trunks offer direct IP connectivity to the enterprise network, they are inherently more insecure than the TDM trunks. At the same time, one TDM trunk contains one call while a one megabit link could contain thousands of SIP calls, which increases the risk of a denial of service attack and the damage that may be caused.

These kinds of problems can be solved by implementing an E-SBC, something interoperable with in all variations of SIP and with sufficient intelligence to facilitate the secure interactions of the various devices. Such an E-SBC could, for example, solve deployment issues, prevent attacks and deliver value to the enterprise in the process. Such a mediating device would essentially ensure that the requirements of enablement, control, protection, demarcation and ROI are met.

Enablement and Protection: Interlinked

Enablement falls largely in the arena of SBC where NAT (network address translation) traversal and ensuring interoperability are all considerations. Current SBC's can perform most of the necessary functions, but cannot provide sufficient protection to assure complete communications security.

Important from an enablement standpoint is the matter of NAT (network address translation) traversal. NAT traversal is the process by which IP address information is modified inside of IP header messages and because IP traffic is routed by headers, devices need to be able to look into packets and read the embedded NAT addressing information. Yet traditional firewalls can't do this. Consequently, to permit external traffic to enter the network, service providers often require the enterprise to "open up" the firewall in ways that compromise security, reduce network control at the application layer, and prohibit the effective implementation of routing policies for SIP-based traffic.

Given the plethora of threats facing networks today, such openness is unacceptable. Changes to the firewall will open holes for attacks from external sources such as hackers, malicious users and spammers. According to the Communication Fraud Control Association (CFCA), the body that monitors communication fraud, the crime of 'Phreaking' (hacking into a PBX and using it to route calls) actually costs UK businesses \$2 billion to \$2.4 billion per year. Authorities estimate that telecoms fraud caused by security gaps cost businesses nearly \$80 billion per year. Other common attacks include Denial of Service (DoS)/Distributed Denial of Service (DDoS) message floods and fuzzing, stealth DoS, and spoofing attacks. A DoS attack on a VoIP system, to give an example, floods a phone with spoofed requests that overwhelm the phone's protocol stack and disables the device. A low-volume variation on this kind of attack can cause VoIP phones to ring continuously.

These threats are not the only ones to be concerned about, either: call hijacking, fraud and eavesdropping are also perils, and must be secured against with encryption and authentication. If the signaling and media traffic used for voice communication is not secured, packets can be captured and conversations reconstructed.

For these reasons, and because IP addresses contained within the SIP message headers that are exchanged between service provider and enterprise networks must be publicly routable IP addresses (except in the case of a private WAN), the enterprise has to perform NAT whether a call originates within or outside of its own network.

In addition to protecting its network against attacks, the enterprise must have control over all aspects of its voice, video and data communications. This includes allowing or denying specific signaling, media and applications, and applying specific routing or security policies.

Deploying a SIP Trunk Securely and Effectively

As mentioned previously, what's required in the SIP trunk scenario is an E-SBC communicating via SIP to the IP-PBX, facilitating essential functions such as routing and NAT traversal, and providing security capabilities such as threat protection, access control, policy enforcement and privacy. In other words, to enable, control and protect enterprise VoIP traffic.

The SIP trunk security device should provide for all of the following to ensure the four requirements of enablement, control, protection and demarcation are met:

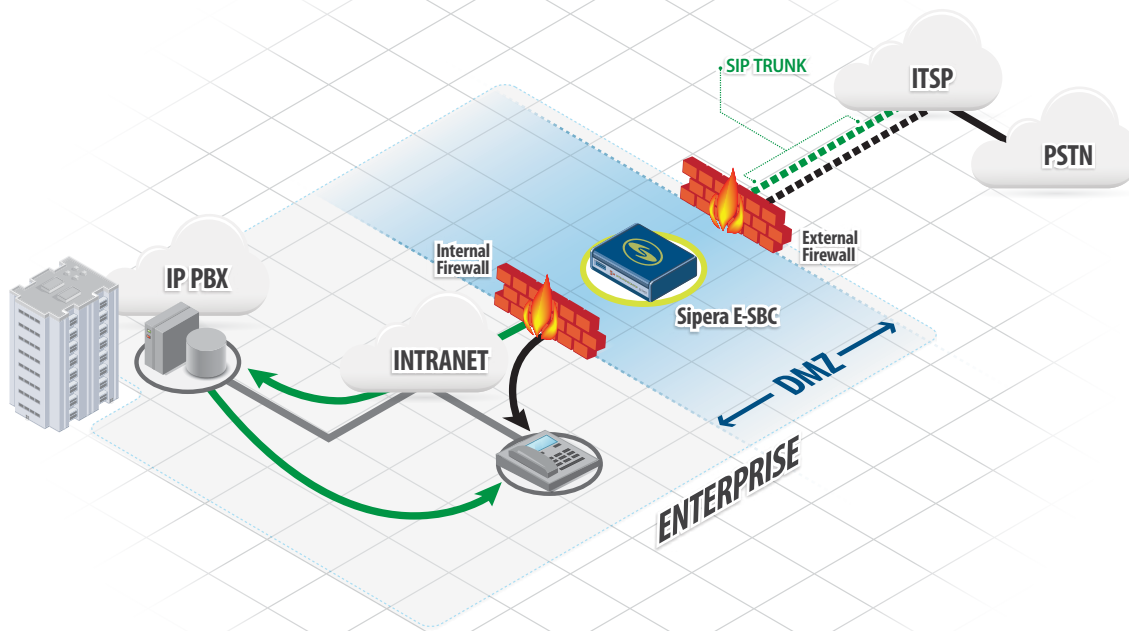
VoIP threat prevention: comprehensive SIP and media protection

VoIP policy compliance: fine-grained policy enforcement

Secure Access: firewall/NAT traversal and encrypted signaling and media proxy (TLS and SRTP)

Demarcation: clear line of defense and termination for SIP trunks within the enterprise.

This VoIP security device deploys at the edge of the enterprise network within the DMZ, between the network's internal and external firewalls to ensure complete protection. The device performs border control functions such as firewall/NAT traversal, access management and control based on Unified Communications policies, and intrusion prevention functionality to defend against denial of service, spoofing, stealth attacks and voice spam.



The Destination: SIP-Enabled Unified Communications

SIP trunking provides a highly economical and versatile communications solution for enterprises eager to capitalize on the benefits of IP networks for both voice and data. Implementing a SIP trunk solution requires a shift in perspective, however, from conventional notions of the network perimeter and the kinds of functions required for security. The edges of the network are no longer “hard”: all manner of traffic flows in and out. To enable effective communications that meet the full range of enterprise requirements and yet protect against signaling and media vulnerabilities, and to handle demarcation and peering issues at the network edge.

A comprehensive SIP trunk solution will include an E-SBC deployed between the network’s internal and external firewalls and perform all the necessary functions for enablement, control and protection of VoIP communications. An E-SBC will provide all the features to ensure truly secure communications.

Sipera’s E-SBC

Sipera’s E-SBC appliance offers the industry’s best real-time application-layer protection against toll fraud and other VoIP/UC threats allowing enterprises to enjoy the benefits of SIP trunks. The E-SBC encrypts the signaling and the media of the SIP trunk, unlike traditional carrier SBCs, with no loss of voice quality.

The E-SBC is the safe SIP trunk choice for enterprise. The E-SBC:

- Serves as the demarcation point for the enterprise VoIP and UC network and enforces fine-grained security policies.
- Protects against SIP and RTP threats by blocking them at the enterprise perimeter.
- Is proven in SIP trunk deployments involving all major VoIP and UC manufacturers and across all verticals.
- Performs firewall/NAT traversal to simplify the deployment of SIP trunks.
- Is upgradable to support the advanced UC security functionality, safe VoIP and UC to any device over any network.

Built on a real-time platform and based on the groundbreaking vulnerability research of VIPER Lab, Sipera’s research and services unit, the E-SBC will have the most up-to-date protection against VoIP/UC threats before and after installation.

SIP Trunking

Enabling new collaboration and keeping the network safe with an E-SBC

A Siper Systems White Paper



UNIFIED COMMUNICATIONS UNLEASHED

About Siper Systems

Sipera Systems is the worldwide leader in solutions for the safe, simple and controlled deployment of IP-based business communications. Siper's groundbreaking Unified Communications (UC) security products are the choice of enterprises and service providers around the globe for deploying secure VoIP, SIP trunks, video conferencing, cloud-based communications, instant messaging, and collaboration tools.

Independent research by industry analysts shows that Siper's solutions can accelerate VoIP and UC project deployment by up to one third. Backed by the industry-leading security research of Siper's VIPER Lab, Siper's solutions provide the best protection against toll fraud, identity theft, denial of service, unauthorized intrusion, eavesdropping and other common business communications threats. Pre-integrated with all market-leading UC vendor solutions, Siper's offerings include the world's first UC security device to be Common Criteria certified, meeting the stringent international standard for IT security.



www.sipera.com

www.twitter.com/siperasystems

Sipera Systems
1900 Firman Drive, Suite 600
Richardson, TX
75081, USA

T: +1 214 206 3210
F: +1 214 206 3215
E: info@sipera.com