Session Initiation Protocol (SIP) trunking is a Voice over Internet Protocol (VoIP) service based on the Session Initiation Protocol by which Internet telephony service providers deliver telephone services and unified communication to customers equipped with private branch exchange (IP-PBX) facilities. SIP 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.

Flexible and cost-effective, SIP trunks make a great deal of business sense to deploy because your organization can use the converged Internet Protocol (IP) connection for all communication with calls routed over your carrier’s IP backbone using Voice over Internet Protocol (VoIP).

Yet as with any technology, SIP trunking requires some education to derive maximum benefit from a SIP trunking solution and it also it pays to understand its dimensions especially security and deployment challenges. Fortunately, with the right solution the necessary security can be enabled and deployment challenges resolved.

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

**Starting Points**

IP technology has radically transformed voice and data communications and has also transformed the ways we think about voice and data communications. Historically where separate infrastructures were needed to carry different types of traffic, now one 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.
SIP trunking, which uses the VoIP standard to establish an Internet-based connection between the public switched telephone network and your enterprise’s SIP-compatible gateway or IP Private Branch Exchange (PBX) is also changing the way businesses and organizations communicate.

The benefits of SIP trunking are many. It eliminates the need for costly time-division multiplexing 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 time slot capacity of time-division multiplexing trunks and call capacity can be scaled easily. Bandwidth can be allocated dynamically based on the application mix or number of sessions to help ensure optimal performance of applications in use.

A Different Frame of Mind

Just as VoIP originally enabled voice convergence with your enterprise local area network (LAN), SIP trunking enables voice convergence externally over the wide area network/Internet. And for that reason, it requires a change in the way your enterprise should think about your 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 your enterprise’s borders. Because your voice network is no longer isolated and self-contained, 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 Session Initiation Protocol trunk, yet it is all too often overlooked. Any comprehensive security solution for Session Initiation Protocol trunking must provide:

• **Enablement**: facilitation of seamless and secure enterprise communications with high quality of service;

• **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 Session Initiation Protocol 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 return on investment.

### 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 Public Switched Telephone Network connectivity because there is no need to own lines or Time-division multiplexing equipment (which also has the longer-term advantage of lower maintenance costs). SIP trunks can also support a greater number of lines than conventional 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 Time-division multiplexing-based Public Switched Telephone Network scenario.

As an example, consider a large enterprise of 2,500 employees with an over subscription rate of 10:1 (10 users to 1 SIP Session) and an estimated long-distance tariff for traditional long distance calling of $0.04 per minute. If 250 simultaneous voice calls must be supported at any given time using Time-division multiplexing, it would be necessary to deploy 11 primary rate interface connections over T1 lines to meet the demands. And if a Time-division multiplexing gateway does not already exist, one would have to be deployed at a significant capital cost.

The same organization with the same needs could deploy Session Initiation Protocol trunks to support 250 simultaneous Voice over Internet Protocol calls in a Session Initiation Protocol trunk scenario. The session border controller in the network demilitarized zone can be either the industry standard carrier Session Border Controller or a purpose built Avaya Session Border Controller for Enterprise. In either case the long-distance cost Session Border Controller could potentially be half that of the Public Switched Telephone Network scenario.

It’s not surprising then that enterprises are moving to SIP trunks to shed the cost of Public Switched Telephone Network 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, more and more enterprises are realizing SIP trunks also support real-time unified communications applications, which provides the potential to increase the productivity of their workforces. In large part, one of the most important decision to make when moving to SIP trunks is in selecting 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 Time-division multiplexing and Internet Protocol) to process enterprise call functions
- User devices connected to the internal network
- Border elements that create a ‘demilitarized zone’ between the internal network and the Internet beyond the point where the SIP trunk connects for to the Internet telephony service provider’s network.

Key functions required within a conventional SIP trunk architecture include: topology hiding, Quality of Service 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. And there are PBX’s that claim SIP interoperability that really possess fairly basic capabilities. They may be able to direct traffic to specific Internet Protocol 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. These issues can generally be addressed by purchasing the right equipment and asking the right questions about its capabilities.

The right questions to ask:

• Does it perform NAT Transversal and Topology Hiding?
• Does it do SIP Normalization?
• Does it maintain SIP-NAT bindings?
• Does it perform access control?
• Is it protocol repair capable?

Security

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.

While SIP trunking provides many benefits as well as flexibility, distinct and more intensive security requirements required versus Time-division multiplexing. A Time-division multiplexing Public Switched Telephone Network gateway provides an explicit demarcation point between the enterprise network and service provider combined with engrained security features. So it is extremely difficult for a malicious external user to traverse the network interconnection and access the enterprise network through the traditional that trunk but it is fairly easy to do so when the interconnect point is Internet Protocol.
Because SIP trunks offer direct IP connectivity to the enterprise network, they are inherently more insecure than the Time-division multiplexing trunks. One Time-division multiplexing 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 (an attempt to make a computer or network resource unavailable to its intended users) and the damage that may be caused. Implementing an Avaya Session Border Controller for Enterprise that is interoperable with all variations of SIP and has sufficient intelligence to facilitate the secure interactions with a variety devices can solve the problem, Avaya Session Border Controller for Enterprise is designed to solve deployment issues, prevent attacks and deliver value to the enterprise. It helps you meet the requirements of enablement, control, protection, demarcation and return on investment.

**Enablement and Protection: Interlinked**

Important from an enablement standpoint is Network Address Translation traversal and how to protect against outside threats. Network Address Translation traversal is the process by which IP address information is modified inside of IP header messages. Because IP traffic is routed by headers, devices need to be able to look into packets and read the embedded 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, the body that monitors communication fraud, the crime of ‘Phreaking’ (hacking into a PBX and using it to route calls) actually costs United Kingdom businesses $2 billion to $2.4 billion per year¹. Authorities estimate that telecoms fraud caused by security gaps cost businesses nearly $80 billion per year². Other common attacks include Denial of Service/Distributed Denial of Service; Distributed Denial of Service message floods and fuzzing; stealth Denial of Service; and spoofing attacks. A Denial of Service attack on a VoIP system can be used to flood 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. Other threats such as call hijacking, fraud and eavesdropping are also perils, and must be secured against with encryption and authentication. If the signalling and media traffic used for voice communication is not secured, voice packets can be captured and conversations reconstructed.

---

¹ The Communications Fraud Association - 2011
² Communications Fraud Control Association (CFCA) 2008 Survey.
In addition to protecting its network against attacks, your 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 Session Initiation Protocol Trunk Securely and Effectively

As mentioned previously, a Session Border Controller for Enterprise communicating via SIP to the IP-PBX, facilitates essential functions such as routing and Network Address Translation traversal, and provides security capabilities such as threat protection, access control, policy enforcement and privacy. In other words, to enable, control and protect enterprise Voice over Internet Protocol traffic. An Avaya Session Border Controller gives you that.

Your 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/Network Address Translation traversal and encrypted signaling and media proxy (Transport Layer Security and Secure Real-time Transport Protocol)
- **Demarcation**: clear line of defense and termination for Session Initiation Protocol trunks within the enterprise

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; from conventional notions of what the network perimeter is to the kinds of functions required for security. The edges of the network are no longer “hard”: all manner of traffic flows in and out. SIP-enabled effective communications must 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 Avaya Session Border Controller for Enterprise deployed between the network’s internal and external firewalls because it can perform all the necessary functions for enablement, control and protection of Voice over Internet Protocol communications.
Summary

Avaya Session Border Controller for Enterprise offers one of the industry’s best real-time application-layer protection against toll fraud and other VoIP/unified communications threats allowing enterprises to enjoy the benefits of SIP trunks.

The Avaya Session Border Controller for Enterprise enables safe SIP trunks for enterprises by:

- Creating a demarcation point for your enterprise and enforcing fine-grained security policies.
- Protecting against threats by blocking them at the enterprise perimeter.
- Performing firewall/Network Address Translation traversal to simplify the deployment of SIP trunks.
- Easily upgrading to advanced functionality, safe for any device over any network.

Built on a real-time platform and based on the ground breaking vulnerability research, the Avaya Session Border Controller for Enterprise has the most up-to-date protection against communications threats.
About Avaya
Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, data solutions and related services to companies of all sizes around the world. For more information please visit www.avaya.com.

Learn More
To learn more and to obtain additional information such as white papers and case studies about Avaya Session Border Controller for Enterprise please contact your Avaya Account Manager or Authorized Partner or visit us at www.avaya.com/usa/product/avaya-aura