IntelePeer

The Cloud Communications Company

SIP SECURITY

JULY 2014

Executive Overview

As with any data or communication service, it's important that all enterprises understand potential security issues related to SIP Trunking. This paper provides an overview of relevant industry requirements and recommendations along with how those requirements are addressed when using SIP Trunking services. Additionally, information regarding secure connectivity options and best practices is included to enable enterprise managers to have meaningful discussions with service providers in order to evaluate service offerings and minimize potential risks and interoperability concerns when connecting multiple vendor platforms. This paper also provides a short review of compliance and regulatory requirements that have either been issued or come into effect since the initial release of the paper in July 2013.

General Security Requirements

While all managers intuitively understand that security is an important consideration, it can add complexity and expense to business operations. Before addressing specific requirements for SIP Trunks it's useful to review general security requirements that apply across all technologies. Some industries have specific legal requirements regarding security in addition to industry best practices. Ineffective security can also have significant financial impacts for enterprises in addition to the loss of customer confidence and potential regulatory consequences.

Most Recent Compliance Changes and Updated Requirements

Since network security and the related compliance are an ongoing and ever changing set of overlapping standards and best practices, it's useful to monitor updated requirements. The two most prevalent changes over the past year have been the introduction of the PCI DSS Version 3.0 (effective January 1, 2014) and the Final Rule regulations (effective September 23, 2013) that included extension of HIPAA's definition of "covered entities" to include Business Associates. A common theme between them is the need for written agreements with outside entities and subcontractors that may store, process, or transmit covered data. Additionally, the various regulators have provided updated guidance regarding the circumstances under which companies have to disclose information about breaches. Individual states have also layered on their own requirements—with 47 states and most US territories having their own sets of disclosure laws.

Information Security

Security is not just an issue for the data or telecommunications networks. All enterprises have a range of security requirements and industry recommendations that span all aspects of their operations. That means that each individual employee is subject to security and disclosure rules in addition to the network infrastructure. Three of the common categories of information subject to governmental collection and disclosure rules include Call Detail Records (CDR), Personally Identifiable Information (PII), and Customer Proprietary Network Information (CPNI). To further complicate matters, there can be different requirements for how the information is handled whether it's being stored ("data at rest") or during any kind of transfer process ("data in motion"). Table 1 below has a summary of common requirements.

Regulation/Recommendation	Applicable Industry	Additional Information
Payment Card Industry (PCI)	Any company that processes, stores, or transmits credit card information	PCI Data Security Standard (PCI DSS 3.0) has different requirements based on transaction volume. Link encryption is an important component.
Health Insurance Portability and Accountability Act (HIPPA) and Health Information Technology for Economic and Clinical Health Act (HITECH)	Health Care	Requires encryption if data includes Personal Health Information (PHI) or Electronic Health Records (EHR). May also require a Business Associate Agreement (BAA) with 3rd parties.
Gramm-Leach-Bliley Act (GLBA)	Financial Services	Covers collection, sharing, and protection of consumer financial data.
Federal Information Security Management Act (FISMA)	US Government Agencies and Contractors	Different levels of security based on operational or mission requirements.
ISO/IEC 27002	General Industry	Related standard ISO/IEC 27001 is the applicable certification standard.

Table 1: Common Security Regulations or Recommendations

Impacts of Ineffective PBX and Telecommunications Security

In telecommunications environments most consumers and individuals seem to be primarily concerned with privacy and potential eavesdropping on their phone conversations (referred to as the media payload for IP services). In such instances, breaches in service provider or enterprise security could certainly cause either a marketing impact or unintended information disclosure.

However, the far more common (and perhaps more financially harmful) threats to companies and service providers come from attacks and disruptions to the signaling protocols rather than the media payload. Frequent threats include toll fraud, Telephony Denial of Service (TDoS), and spoofed or missing caller ID information. These can result in both direct and indirect loss of revenue or additional expenses. Indirect losses are generally related to service disruptions and loss of productivity, such as when dealing with a TDoS attack. Direct losses can include loss of revenue and fraudulent charges as well as governmental penalties.

Toll fraud is generally related to international long distance calls, especially to countries that have relatively less communications infrastructure and higher tariffs than other parts of the world. For contact centers, spoofed caller ID information could either cause an agent to misidentify an inbound caller as part of an identity theft scenario or to incorrectly dial an outbound number that violates a do-not-call list, with a subsequent penalty of up to $16,000. In 2013 alone, experts estimate an annual fraud loss of more than $46B USD. Table 2 below has more detailed information.

Experts estimate annual fraud losses in 2013 were $46.3 Billion (USD).
The top 5 fraud loss categories reported by operators were:

$4.96 Billion (USD)	Subscription Fraud
$4.32 Billion (USD)	PBX Hacking
$3.84 Billion (USD)	Account Take Over / Identity Theft
$2.88 Billion (USD)	VoIP Hacking
$2.40 Billion (USD)	Dealer Fraud

Source: 2013 CFCA Global Fraud Loss Survey

Table 2: Top 5 Estimated Annual Fraud Losses

Logical and Configuration Security

In addition to the previously discussed information security, which spans all aspects of an enterprise, there are specific security expectations for the communication services and networks. The most commonly recognized is encryption, but authentication and network monitoring are also important to minimize potential fraud. For example, a service provider can monitor typical customer usage and implement calling pattern detection to shut down international calls at unusual times or to unusual destinations to reduce toll fraud. An additional security practice that is important to minimize TDoS attacks is to mask or hide the network topology from outside probing.

While encryption for stored data has become more common, it isn't allows implemented during transmission. In some cases, that's due to perceptions (not necessarily true) of network performance degradation and delay as well as additional costs and complexity for encryption. In other cases, the regulation or legal requirements aren't always specific (e.g. current HIPAA guidance calls for encryption during transmission if it is "reasonable and appropriate"). Encryption and authentication should be used together with a reputable Certificate Authority (CA) to provide source IP address verification and to encrypt both the media payload and signaling. Given the state of current decryption tools and computer processing power, encryption configurations should be set to a minimum of 2048 bit depth. Note that not all hardware or service providers can support higher levels of encryption.

SIP Trunking Connectivity Options

There are two general deployment considerations that need to be made to deploy SIP Trunks. One is the equipment and configuration at the customer location. This typically comes down to whether to use routers and firewalls or an Enterprise Session Border Controller (E-SBC). The choice is typically a function of the capital costs and desired network capacity. In either situation, the SIP Trunking provider will have an SBC in their network. The other consideration is the type of access link. For many years the standard practice for network connection security has been to use either dedicated access links or some sort of encrypted Virtual Private Network (VPN). However, there are both cost and performance considerations that make public Internet access very compelling for SIP Trunks.

The two most common dedicated access technologies used with SIP Trunks are Multiprotocol Label Switching (MPLS) and VPNs. These are typically recommended by the largest legacy service providers. While these technologies address most security requirements, there are drawbacks. One area for direct comparison with public access is the relatively higher cost for either service. These services also tend to be inflexible and relatively slower to deploy than public Internet access connections. That greatly minimizes one of the strengths of SIP Trunking, flexibility. Another issue that can be very difficult to troubleshoot is potential impacts to Quality of Service (QoS) due to an unknown number of network segments or hops from the customer location to the service provider's switching equipment.

As customers have grown more familiar with SIP Trunking services, the most common access method has been through their existing Internet service provider using Over-The-Top (OTT) connectivity while employing the standard encryption and security configurations for SIP Trunks. It is not only more cost effective by sharing bandwidth with other network services, but many customers experience improved QoS through high bandwidth connections with reduced numbers of hops into the SIP service provider networks.

Encryption Over SIP Trunks

SIP Trunks use two different protocols to provide encryption security. Signaling uses Transport Layer Security (TLS). This provides encryption from the customer location to the service provider's signaling gateway. The actual voice conversation or media payload (e.g. video call) uses Secure Real-time Transport Protocol (SRTP). This can actually provide end-to-end encryption all the way through the SIP service provider's network. Diagram 1 below shows the separation of these two flows.

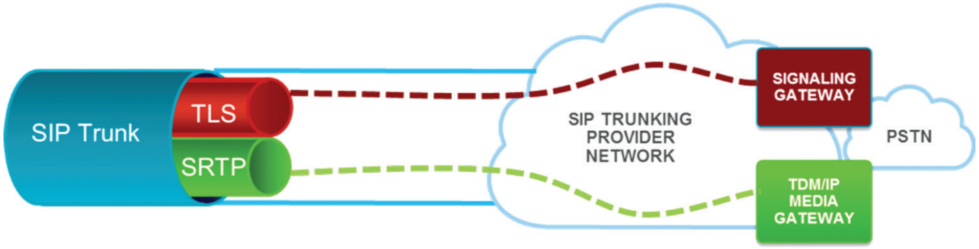

Diagram 1: Separation of Signaling and Media Flows in a SIP Trunk

Router/Firewall Deployments

One common configuration for SIP Trunking access is to use an enterprise's existing router and firewall equipment. Diagram 2 below shows this using an OTT link to provide the SIP trunk through an existing Internet service provider. Since it uses existing equipment, this kind of deployment can have very low capital costs. However, it is typically used only in smaller enterprise deployments since there may be quality issues with high volumes of dynamic voice traffic or Unified Communication (UC) sessions.

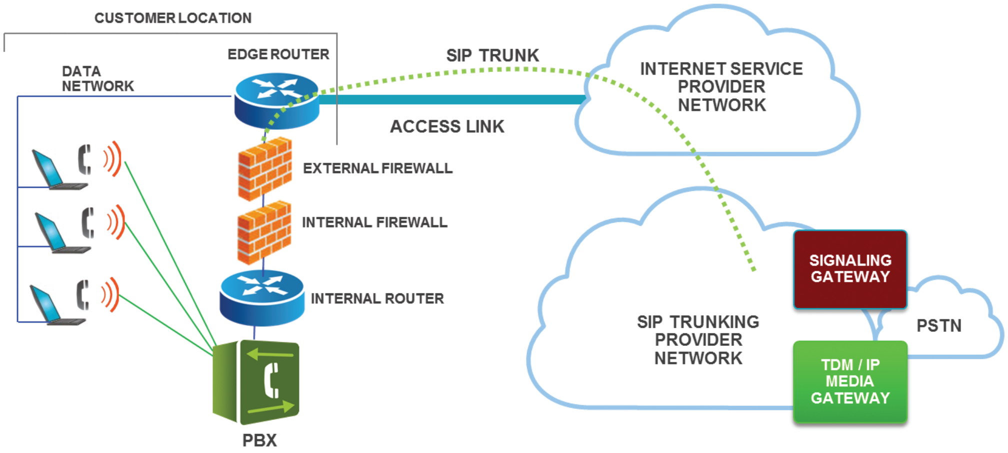

Diagram 2: SIP Trunk Security Configuration Using Existing Routers and Firewalls

E-SBC Deployments

Larger enterprises and higher volume deployments will typically deploy an E-SBC at the customer location. Although it comes at a relatively higher capital cost, there are a number of additional advantages to an E-SBC deployment beyond just additional capacity. Most E-SBCs provide full support for TLS/SRTP encryption as well as acting as a Back-to-Back User Agent (B2BUA). Since the E-SBCs support TLS/SRTP, it eliminates any additional cost and complexity for separate hardware to enable encryption (as long as the service provider also supports TLS/SRTP). They also provide support for dial plans, transcoding, and session management during overall IP network migrations. Many E-SBCs even provide native support for vendor applications such as UC platforms.

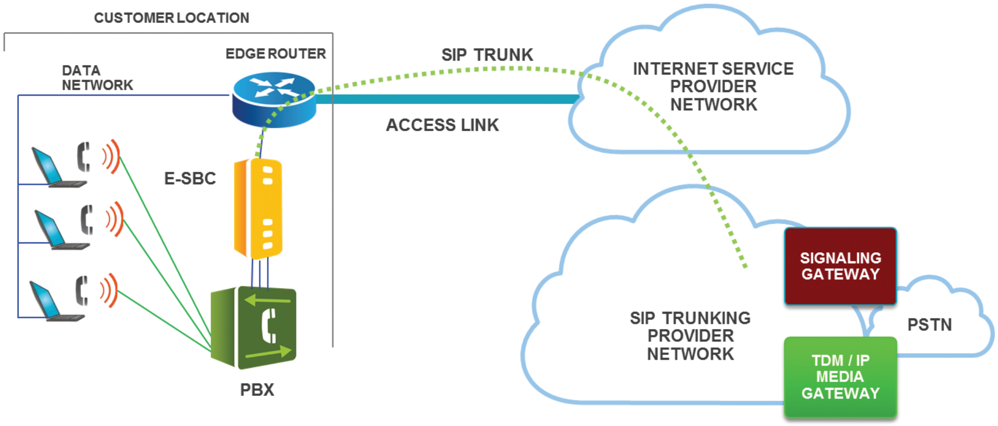

Diagram 3: SIP Trunk Security Configuration Using E-SBC

SIP Trunking Vendor Evaluation

Given that IP services over SIP Trunks are based on common industry standards, it would seem that all service providers could just be evaluated based on straightforward metrics such as monthly recurring costs. However, there are a number of other criteria that are important to consider in order to understand overall service expectations as well as total costs.

Security and encryption on SIP Trunks are basic service requirements. With a properly configured TLS/SRTP deployment, SIP Trunk encryption and security meet all appropriate compliance requirements and provide ongoing business continuity with high QoS and minimal overhead or network delay. One of the best ways to assure this is to check vendor qualification for TLS/SRTP SIP security. For example, there are a large number of hardware vendors and service providers that are qualifiedfor interoperability with UC platforms. However, those same vendors are not necessarily qualified for TLS/SRTP for those platforms. That requires separate testing and qualification. That also means that a vendor or service provider can't self-certify. Only the UC platform vendor or an independent lab can provide qualification.

A SIP Trunking service provider should support multiple hardware and platform options, with applicable security certifications. TLS/SRTP interoperability across all network elements and the SIP Trunking provider's network provide the best assurance of security. An enterprise's deployment options shouldn't be limited to a single vendor based on limited certification of the SIP Trunking provider.

A SIP Trunking provider should have extensive experience supporting OTT services. Many legacy service providers still promote MPLS/VPN solutions, mainly because they can charge higher rates. However, those services don't help to unlock the full potential for flexible configurations and lower cost structure of SIP Trunking.

A SIP Trunking provider's operations center should provide proactive network monitoring for early toll fraud detection and the ability to rapidly shut down potentially fraudulent activity.

SIP Trunking Security With IntelePeer

As an industry leader in providing cloud-based, IP communications and collaboration services for enterprises, IntelePeer has significant experience with a wide range of SIP hardware and platform multi-vendor networks using TLS/SRTP secured SIP Trunks. That not only means that an enterprise's existing equipment is likely certified to work with IntelePeer's network, but also that no enterprise is limited in their future vendor migration plans. IntelePeer recognizes that there is no single solution that best fits the needs of every enterprise. IntelePeer has vendor interoperability qualification with all of the top SIP hardware and UC platform vendors including Microsoft, Avaya, Cisco, Unify, Asterisk, ShoreTel, Interactive Intelligence, Mitel, NEC and Allworx. In addition, IntelePeer is the first US-based SIP Trunking service provider with Microsoft qualifications for Lync 2010 and Lync 2013 for TLS/ SRTP SIP security.

Security and encryption for SIP Trunks is an absolute requirement in today's networks so IntelePeer does not charge any additional fees for TLS/SRTP encryption. With a highly redundant network and availability of more than 99.999%, IntelePeer has the experience and expertise to satisfy SIP Trunking security requirements. Since more than 90% of IntelePeer's enterprise customers get their SIP Trunking services via OTT from their existing Internet provider they are well positioned for rapid configuration changes and able to benefit from the economies of scale through aggregate bandwidth sharing of their voice and data networks.

Conclusion

Although there are a wide range of enterprise security and compliance requirements, SIP Trunking has built-in security and encryption protocols that are sufficient to meet or exceed those requirements. However, those protocols, including TLS and SRTP, require additional configurations and implementations by enterprises, hardware vendors, and SIP Trunking service providers. By having sufficient knowledge of potential vendor issues, intelligent choices can be made with regard to appropriate deployment choices to take advantage of all the feature, productivity, and cost benefits of SIP Trunking while also maintaining network encryption and security standards.

GLOSSARY

Back-To-Back User Agent (B2BUA) – logical element in a SIP network that may provide some combination of call management, network interworking, or masking of network topology

Call Detail Record (CDR) – information generated by telecommunications equipment describing a particular phone call including the phone numbers of both the calling and receiving parties, call duration, and other data

Certificate Authority (CA) – an entity that issues digital certificates used to encrypt/decrypt data. The digital certificate verifies the ownership of a public key by the named subject of the certificate.

Customer Proprietary Network Information (CPNI) – information collected by telecommunications companies regarding customer calls (CDR) and related data that may appear on their telephone bill

Over The Top (OTT) – delivery of services via another company's network infrastructure or service, such as an Internet service provider only being responsible for transporting IP packets and not signaling or other services

Personally Identifiable Information (PII) – information that can be used to identify, contact, or locate a single individual either by itself or in conjunction with other data

Secure Real-Time Protocol (SRTP) – a specific profile of Real-time Transport Protocol (RTP) to provide encryption, message authentication, and integrity of the communications media stream

Telephony Denial of Service (TDoS) – flooding telephony-related networks, websites or other telecommunications servers with massive volumes of traffic meant to disrupt services. Contact centers are the most frequent targets.

Transport Layer Security (TLS) – protocol for encryption, authentication, and integrity frequently using cryptographic keys before data is exchanged

Health Insurance Portability and Accountability Act (HIPAA) – provides standards and specifications for the security of patient information and limiting access to that information

Health Information Technology for Economic and Clinical Health Act (HITECH) – adds additional requirements for Electronic Health Records (EHR) and disclosure rules for breaches in conjunction with the rules for HIPAA

Payment Card Industry Data Security Standard (PCI DSS) – provides a standardized set of basic security requirements for all entities that process, store or transmit cardholder information

www.intelepeer.com

Corporate Headquarters
177 Bovet Suite 400
San Mateo, CA 94402
T: 650.525.9200
F: 650.287.2628