

SIP Trunks provide a flexible and cost effective alternative to using a fixed lined PSTN connection, but installing a trunk service and integrating that service with an IP PBX is not a simple *Plug-and-Play* exercise. UM Labs' SIP Security Controllers simplify this task by hiding the complexity of connecting a corporate IP PBX to the Trunk provider and as a bonus providing much needed security controls for the corporate network.

SIP Trunk services offer an alternative to a fixed line phone connection and are growing in popularity because of the many benefits they provide over standard PSTN services. These benefits include:

- Geographical flexibility. SIP Trunk services enable companies to have phone numbers in any area code or even in a different country. For example a call centre located in the Asia Pacific region could have a range of European and North American numbers.
- Service flexibility. SIP Trunks can normally be provided and upgraded more quickly than PSTN services. In addition, SIP Trunks do not have the same limitations as PSTN. A 30 channel Primary rate ISDN service is limited to 30 calls including all inbound and outbound calls. Upgrading requires additional lines and additional interface cards in the PBX. A SIP trunk service has no such limitations. Calls are limited only by available bandwidth.
- Portability and Disaster recovery. SIP trunks can be re-directed in a matter of seconds. Once a service is established numbers can be moved to another site without re-provisioning or having to set up call forwarding services.

SIP Trunk Implementation

On paper, implementing a SIP Trunk service is easy. You just need to link your SIP based IP PBX to the Trunk provider, or if the PBX runs some other VoIP protocol, link a SIP gateway to the SIP Trunk provider. The link can share an existing MPLS or DSL Internet connection (subject to bandwidth availability). In reality it's not quite that simple.

Implementation Challenges

The challenges that must be addressed to successfully connect a SIP trunk service include:

- Protocol incompatibilities. The Session Initiation Protocol (SIP) includes a large number of options. There are currently over 110 standards documents describing the core protocol and its options. This means that it quite common for PBX and a Trunk service to implement a different set of options and fail to communicate. Protocol incompatibility problems are more likely for larger, more complex PBX systems. Where the PBX includes a number of components, for example a core switch and SIP gateway, the protocol routing between those components can conflict with the routing used by the trunk service.
- Network Address Translation (NAT) problems. NAT is the bane of all SIP implementations because the SIP protocol includes network addresses in its payload. These addresses define the end-points for the media stream, the voice conversation or video session. Standard NAT changes the network addresses used to send and receive SIP requests but does not change the contents of those requests. These means that when a SIP request passes through a NAT gateway the media end-points are incorrect, so although a call may connect neither the caller or called party will be able to hear each other. Unfortunately, NAT is ubiquitous and has to be dealt with. Every Firewall and WiFi gateway and most DSL gateways implement NAT.
- Security. While it is technically possible to configure most corporate firewalls to allow the services needed to connect to a SIP trunk and while it is possible to overcome the NAT challenges, this requires non trivial changes to the firewall's configuration. There is a real risk that these changes will compromise the security of other applications and services on the corporate network. Also these changes are likely to be incompatible with other VoIP connections including links to remote users and branch offices.

Even if these problems are solved, a standard firewall will not protect the PBX from the majority of VoIP specific security threats; even if the firewall vendor claims that the firewall is *SIP Aware* or *VoIP Aware*. These threats include flooding and call disruption threats, toll fraud and unauthorised call monitoring.

The Solution

The range of SIP Security Controllers from UM Labs is designed to simplify the task of linking a corporate IP PBX to a SIP trunk service. Each product in the range from the entry level RC-2100, through the EC-4200 designed for enterprise use, to the carrier grade SC-600 includes a number of features designed to make SIP Trunk connections as near plug-and-play as possible.

Feature	Operational Benefit	Installation Benefit
Gateway architecture partitions Service Provider network from Corporate PBX hiding routing details and protocol options	Fully functional SIP trunk service without compromising other remote connections.	Reduce installation time and risk by presenting a set of standard and compatible SIP functions to both the SIP trunk and corporate PBX.
Local NAT and far-end NAT traversal	Fully operation, fully functional SIP trunk service without compromising other remote connections.	Reduce installation time and risk by addressing all local NAT issues and managing far-end NAT traversal.
Strong IP Level firewall functions	Enables Security Controller to handle all VoIP traffic, offloading this traffic from general purpose firewall and freeing the firewall to handle other applications more efficiently and to maintain effective security controls for those applications.	Reduce installation time and risk by removing the existing general purpose firewall from the equation. Configuring and navigating firewalls is a source of difficulty for most SIP trunk installations.
Application and Content Security Controls	Protect corporate Voice infrastructure from VoIP specific threats that standard firewalls cannot address.	Reduce the risk of compromising the security of critical data applications in an effort to enable the voice service.

About UM Labs UM Labs Ltd. was founded in 2008 by security software pioneers dedicated to the promotion of secure global standards for unified communications. The company has an extensive support organization and partner network, with offices in the following locations:

United Kingdom

Heathrow Blvd 4
280 Bath Road
West Drayton
UB7 0DQ
UK
Phone: +44 20 3021 3200

Website: um-labs.com

USA

5586 Main St, Suite 206
Williamsville
NY 14221
USA
Phone: 716 568-4931

Email: info@um-labs.com

Canada

366 Adelaide St, Suite 301
Toronto, ON
M5V 1R9
Canada
Phone: 416 598-7537

VoIP: sip:info@um-labs.com