

WHITE PAPER

SIP Trunks

KEEPING YOUR UC SYSTEM SECURE

Table of Contents

1. Executive summary	3
2. Security considerations for SIP trunks	5
2.1. Threats	5
2.2. Importance of stable platform	5
3. SIP, NATs and Enterprise Firewalls	6
4. Methods for solving NAT/firewall traversal if SIP.	7
4.1. SIP-capable firewalls	7
4.2. Enterprise session border controllers	9
4.3. Session border controllers at the service provider edge.	10
5. SIP proxy-based firewalls and enterpriseSBCs: security advantages of the SIP proxy.	11
5.1. Controlling media	11
5.2. SIP signaling	12
6. Which NAT/firewall traversal solution is right for you?	13
7. Conclusion	15
Figure 1. Positioning of NAT traversal solutions	3
Figure 2. TBD	7
Figure 3. B2BUA functionality	9
Figure 4. Session Border Controller at the Service Provider	10
Figure 5. Positioning of NAT traversal solutions	13
Figure 6. Security and Flexibility.	14

1. Introduction

The appeal of Session Initiation Protocol (SIP) trunks as a means of connecting UC systems to the outside world is growing in popularity. SIP trunks offer lower operating costs, more flexibility in ordering service and capacities and advanced features, such as virtual phone numbers in different geographies, which let companies establish a virtual worldwide presence.

In contrast to legacy PRI trunks, SIP trunks use IP-based protocols that require a system to be opened up to a wide area network (WAN) that should be assumed insecure.

Customers must educate themselves about the salient security aspects pertaining to SIP trunks and how to ensure the appropriate level of security.

SIP was developed by the Internet Engineering Task Force (IETF) and has become a leading signaling protocol for establishing real-time communications, including voice-over-IP (VoIP) calls.

However, SIP-based communication originating from outside the enterprise does not automatically reach users on the local area network (LAN) as it has to traverse firewalls and/or routers that perform Network Address Translation (NAT). Firewalls are designed to prevent inbound communications from unknown sources and the NAT feature gets in the way of proper addressing of users and devices on the LAN.

The choice of method for traversing firewalls/NATs is, to a large extent, dependent on the answer to the question: "Who should be in control of your SIP trunk security: the enterprise firewall administrator or the service provider?"

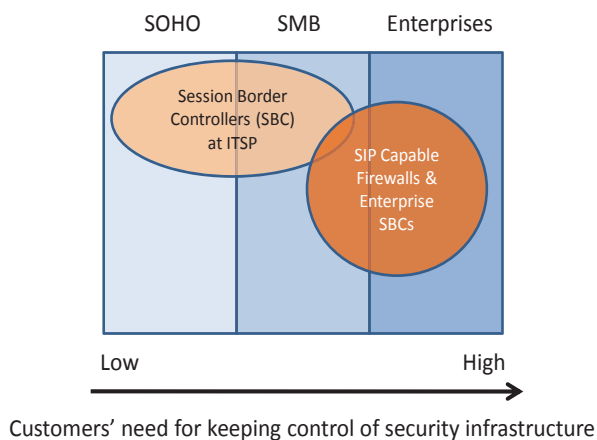


Figure 1 - Positioning of NAT traversal solutions

Session Border Controllers at Service Provider: The service provider is in control

Most service providers use some sort of session border controller (SBC) in their core network to perform a number of tasks related to their SIP services. One of these tasks is to make sure that the SIP services can be delivered to their customers. They may use protocols like STUN, TURN or ICE for this by acting as a server component for these protocols. However, not all clients support these protocols so the SBC may also use far-end-NAT traversal (FENT) technology for NAT traversal. This solution only works with firewalls that are open from the inside, and may not work with all equipment and in all call scenarios. FENT also removes control from the firewall, which must be sufficiently open to allow FENT from the service provider SBC to work.

SIP-capable Firewalls or enterprise SBC: The firewall administrator is in control

This option solves the problem where it occurs: at the firewall or in tandem with an existing firewall using an enterprise SBC. When deployed at the enterprise edge, the SBC offers the same security and control as it does for the service provider's core network. The enterprise SBC typically has a built-in SIP proxy and/or back-to-back user agent (B2BUA) functionality to give unparalleled flexibility for enterprise deployments.

There are special security and functional requirements that make a SIP-capable firewall or enterprise SBC the solution of choice. Firstly, this is the only solution that allows the firewall to maintain control of what traffic can be traversed between the LAN and the outside world. Secondly, such an SBC or firewall is fully SIP aware and can act as the bridge between SIP implementations that differ slightly between vendors, a common phenomenon that is seen despite SIP maturing as a standard.

Most vendors of SBCs for service providers have products that can be deployed at the enterprise edge. ShoreTel resells the Ingate SIParator enterprise SBC that performs the abovementioned functions.

2. Security considerations for SIP trunks

2.1 Threats

Connecting any device to the Internet or WAN can expose the entire network to many types of threats. One example is a brute force attack where the intruder tries to log into a service using a user/password database with a huge number of username and password combinations. The intruder tries each until finally succeeding in finding the right one. Once access has been granted the intruder may be able to launch other types of attacks based on known vulnerabilities to the service in question and in this way get access to other services or data.

Another example of a threat would be denial of service (DoS) attacks where the attacker uses many different hosts or “bots” to send a large number of packets to overwhelm the host, causing it to go down.

The above are two examples of traditional data communication attacks. These and many others can easily be leveraged into attacks on UC or IPBX systems.

2.2 Importance of a stable platform

Firewall vendors have developed significant expertise in securing data communication. They know how to implement stable systems that are locked down to only admit services that have been configured to pass through. Firewalls inspect and log traffic and they can even block suspected attacks including traffic from known bad sources.

Firewalls alone cannot prevent DoS attacks, but they can be hardened to withstand attacks, making them more resilient. More importantly, they can be built to protect the enterprise LAN from the DoS attack itself. A good enterprise SBC should have the same stability and resiliency—essentially a firewall “specialized in VoIP.”

3 SIP, NATs and Enterprise Firewalls

The market for SIP-based real-time communications is expected to grow significantly going forward.

Today's SIP implementations are both robust and feature rich. However, SIP-based communications cannot reach LAN users behind firewalls and NATs automatically, because firewalls are designed to prevent inbound unknown communications. NAT hides the private IP addresses on the LAN, stopping users on the LAN from being addressed from the outside. Very few, if any, communications are received directly from outside the LAN, so only authorized users can gain access to our networks and the valuable information stored on our local servers and computers.

The NAT that is created on the firewall or by routers is also a part of the security fabric. NATs are necessary primarily because the Internet IPv4 standard does not support enough unique IP addresses to allow all of the devices connected to the Internet to have their own identity through a unique IP address. With NAT, only the firewall or router is given a publicly routable IP address. Each device is then assigned a private IP address that is only known inside the firewall-protected space. While this works fine for the types of traffic that are typically supported on the LAN, it prevents inbound communications from reaching the intended recipient behind the firewall because the IP address of the client device is unknown and not routable.

Finally, most firewalls do not support the SIP protocol. As with all other protocol types, the firewall must recognize the format of the signaling in order to admit it to the network. Since many firewalls installed today do not support SIP, the inbound traffic will be stopped for this reason alone.

So why is this important?

There are a number of available methods for firewall traversal. Each has its own benefits, but many have significant drawbacks. These drawbacks impact security. The choice of method for traversing firewalls/NATs determines the amount of control and security you maintain of your network.

- Is your security best left to your firewall administrator?
- Your ITSP?
- Also, does the solution need to work with all ITSPs, or only one specifically?
- How SIP-compliant does it really need to be?
- Will SIP interoperability issues affect security?

The answers can help determine which method of firewall/NAT traversal is right for your network.

The choice of traversal method also has an impact on the future-proofing of your network. The use of SIP is expanding from SIP trunking (voice) to video and beyond. When SIP is widely deployed, interaction becomes more collaborative, with partners, vendors, employees and even customers using the most effective tool for every occasion, whether that be instant messaging, presence, voice, video, application sharing, white boarding or file sharing.

Investing in the appropriate solution allows the enterprise to grow with the expanding role of SIP.

4. Methods for solving NAT/firewall traversal of SIP

Eventually, all firewalls will need to be SIP capable in order to support the wide-scale deployment of SIP trunks and SIP based real-time communications. In the interim, several solutions are available to work around the firewall/NAT traversal issues that limit SIP-based communication.

4.1 SIP-capable firewalls

This is a long-term solution where the problem is solved where it occurs, at the enterprise firewall or in tandem with the firewall using an enterprise session border controller.

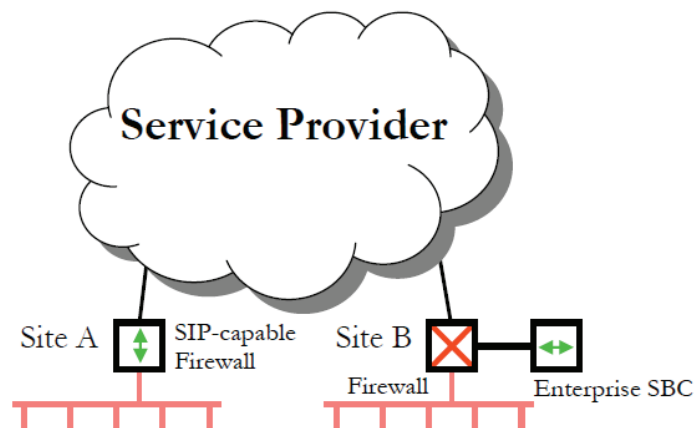


Figure 2

4.1.1 SIP ALG-based SIP-capable firewalls

The majority of all SIP-capable firewalls today use the SIP Application Level Gateway (ALG) architecture. This works for basic call scenarios but has limited functionality for real deployments of enterprise SIP-based real-time communications. The SIP ALG architecture tries to solve the firewall traversal problem of SIP traffic by “taking care of the SIP packets on the fly,” making sure that they reach the right destination on the LAN. This architecture does not provide the enterprise with the full protection and flexible functionality of a SIP proxy-based firewall solution.

4.1.2 SIP proxy-based SIP-capable firewalls

The SIP proxy architecture is a complete solution to the firewall and NAT traversal issues presented by the enterprise firewall. A proxy is designed to briefly stop the packets so that each signaling packet can be inspected before the header information is rewritten and the packets are delivered to the appropriate endpoints. This provides the enterprise with a flexible, controlled implementation of SIP-based communications.

In addition, the SIP proxy can offer benefits not available with the ALG architecture.

- Far-end NAT traversal to support remote workers such as road warriors and home users
- Encrypted SIP signaling (TLS) and media (SRTP)
- Authentication
- Advanced filtering
- Advanced routing and control features
- Intelligence to enable the firewall to act as a backup for a hosted or centralized IP-PBX

To gain unparalleled flexibility, some SIP proxy solutions, including the one from ShoreTel and Ingate, also embed a so-called back-to-back-user-agent (B2BUA) functionality. The B2BUA allows the firewall to have two different call legs in the same session, one on each side of the firewall. This can help if for example the ITSP does not support call transfers with the SIP method REFER. The firewall can then utilize “local call transfer” by just changing the call leg on the LAN side from one client to the other.

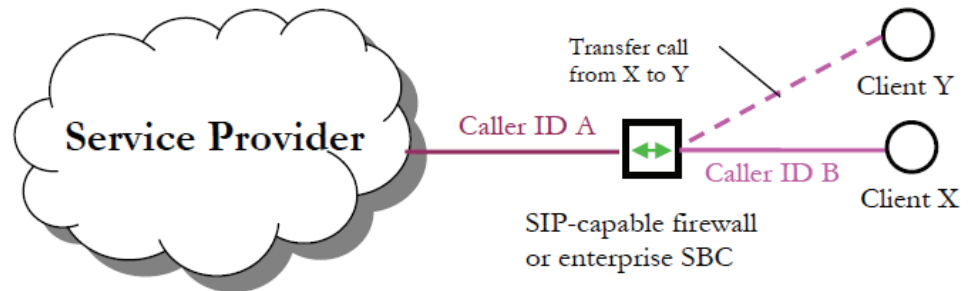


Figure 3 - B2BUA functionality

4.2. Enterprise session border controllers

Many enterprise customers are reluctant to replace their existing firewalls with new SIP-capable firewalls because they have spent a great deal of effort setting up security policies. Yet enterprises must overcome the limitations of their existing firewalls, whether they have firewalls with no SIP functionality or SIP ALG firewalls with limited SIP functionality.

This need has triggered the development of a new type of product which some people call the "enterprise session border controller." The Ingate SIParator as offered by ShoreTel is an example of such a device designed to work in networks where a corporate firewall is already in place. The SIParator can be considered a firewall just for SIP traffic which can be installed either in a standalone configuration, or as part of the DMZ of the existing firewall. Essentially the SIParator assumes control of SIP traffic without involving the existing firewall in the process.

4.3. Session border controllers at the service provider edge

Most service providers use some sort of SBC in their core network to perform a number of tasks related to their SIP services. One of these tasks is to make sure that the SIP services can be delivered to their customers.

The SBC at the service provider may use a far-end NAT traversal (FENT) technology for NAT traversal. Typically, FENT is implemented by continuously sending dummy packets through the firewall to keep pinholes open for the media to cross, or by asking the client to re-register in short intervals to keep those ports available.

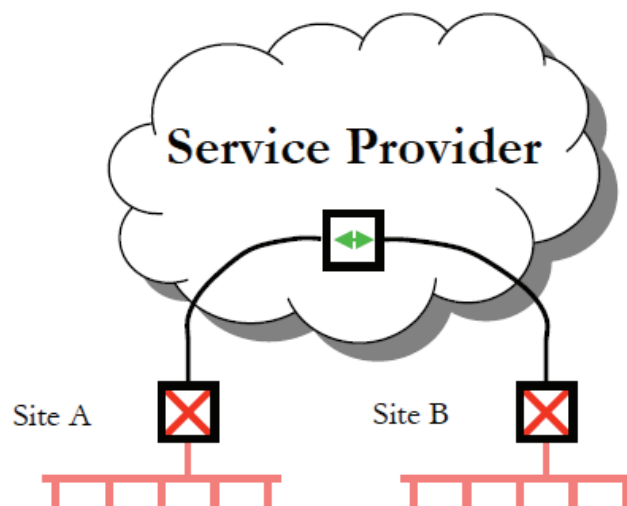


Figure 4 - Session Border Controller at the Service Provider

5. SIP proxy-base firewalls and enterprise SBCs: security advantages of the SIP proxy

5.1 Controlling media

SIP proxy technology is an excellent way to add a level of control to the flow of SIP media. This control offers tremendous advantages with regard to security.

The main purpose of SIP is to set up a media session between clients. Media is handled by other protocols (often RTP). For media to traverse the enterprise edge, the SIP proxy must dynamically open the media ports for media to flow during the duration of the call. As soon as the call is completed the media ports are closed. This behavior is much more secure than solutions with non-SIP-aware firewalls/border elements where a media port range constantly needs to be open. In general the SIP proxy approach is more secure than the IETF specified STUN/TURN/ICE methods, which requires that ports are left open from the inside of the firewall to allow media port negotiation to succeed.

In addition to the dynamic opening and closing of media ports, the edge device should only accept incoming media from the endpoint that receives media from the edge device. This protects against hackers trying to inject media from other endpoints or devices.

To protect media from being overheard by unauthorized persons, media encryption comes into play. The industry has chosen SRTP using descriptions for key exchange as the de facto standard for media encryption. Using SRTP to encrypt media traversing the Internet effectively stops eavesdropping. The integrity of the call is much stronger than ever possible on PSTN.

5.2. SIP signaling

Firewalls with a SIP server and full SIP proxy play a critical role in maintaining enterprise security, and securing VoIP. They can rewrite SIP signaling and process in a very flexible way, ensuring correct routing and interoperability with other systems built to RFC 3261 and related standards.

One important part of the SIP proxy is the SIP parser. The SIP parser verifies that the SIP message is valid and that it may be forwarded to the local LAN. Malformed SIP messages are discarded. The SIP parser must be robust enough to withstand any types of malformed SIP messages without crashing. Also, to mitigate DoS attacks, the parser should be able to process a very large number of packets.

The SIP proxy should include support for the optional loop detection mechanism defined in the SIP specification. This mechanism discerns whether a SIP message is looping (sending the SIP message to itself) and, if so, aborts this behavior. This detection mechanism also protects against DoS attacks where a SIP message is constructed to create loops and thus keep the SIP proxy too busy to engage in useful processing.

To protect resources, e.g. a PSTN gateway, authentication of SIP users should be supported. The standard means of authentication of SIP users is via the digest protocol. SIP users' credentials should be stored in a centralized database e.g. on a RADIUS server. This is more secure and likely easier to maintain.

SIP signaling consists of messages in ASCII text (plain text), and is therefore easy to read and manipulate. It is strongly recommended to encrypt and authenticate SIP signaling. This is normally achieved by supporting TLS or MTLS. MTLS is the most secure method as both server and client mutually authenticate each other using CA-signed certificates or certificate chains.

To provide greater and more flexible protection mechanisms, filters are useful features. A typical filter would include the following features:

- SIP methods can be allowed or prohibited per network.
- Authentication can be enabled or disabled per network and SIP method.
- SIP messages can be filtered on content type.
- Incoming callers can be restricted to a white list; this list can be individually enabled/disabled per user.
- A filter based on from/to header can be used to allow or disallow processing.

6. Which NAT/firewall traversal solution is right for you?

The choice of method for traversing firewalls/NATs is, to a large extent, dependent on the answer to the questions:

- Who should be in control of your security infrastructure: the firewall administrator or a service provider?
- Do we want a solution that is predictable and functions reliably with SIP standard compliant equipment or is it sufficient with a best effort solution that works in certain scenarios and maybe only with a specific operator?

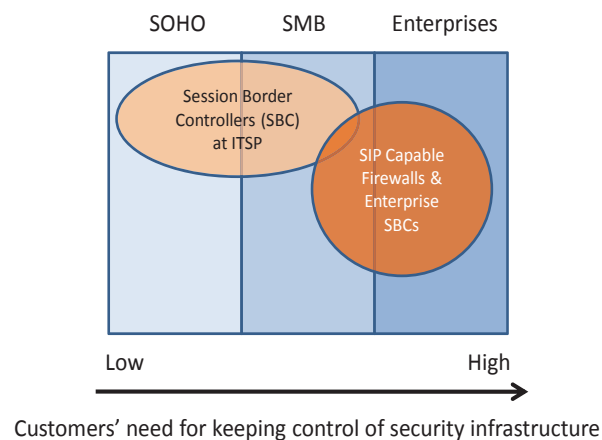


Figure 5 - Positioning of NAT traversal solutions

The choice of NAT/firewall traversal solution must be selected with two very important things in mind:

- 1) The level of security policy and control you need
- 2) The level of flexibility required for configuration. Do you have a solution that is specific to an Internet Service Provider (ITSP) and might lock you in ?

The level of security policy and control you need

If you run a business and want to maintain control of your own security infrastructure—with a high security policy, e.g. all ports in your firewall closed from the inside and deep packet inspection of the SIP traffic—then there is really only one choice: a SIP proxy-based SIP-capable firewall or a SIP proxy-based enterprise SBC.

If you have no or a very low security policy and do not mind that a service provider asks you to open up certain ports in your firewall, then you may consider the far-end NAT traversal solution offered by the SBC in the ITSP’s core network. With this solution control of your security infrastructure is given to the service provider.

The level of flexibility in terms of configuration you need

Even if you are not too concerned about security you want to make sure that your SIP trunking solution works without any issues against a variety of ITSPs. Investing in an enterprise SBC can give you the flexibility to adapt to a variety of SIP implementations.

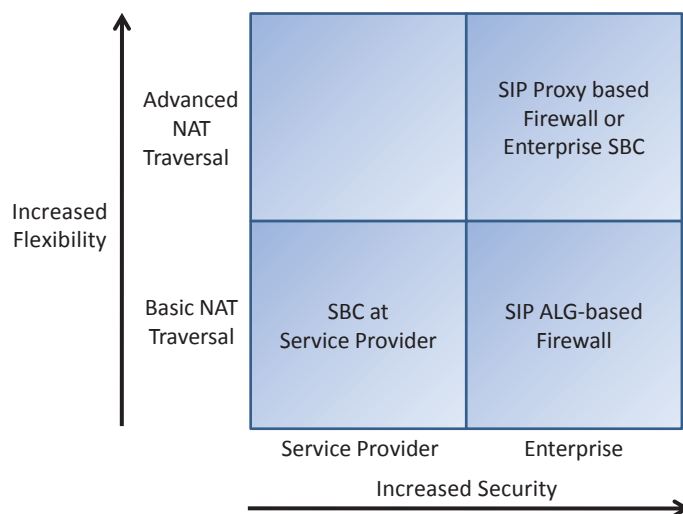


Figure 6 – Security and Flexibility

7. Conclusion

We are entering a time of global connectivity in which the SIP protocol has gained wide acceptance by vendors and service providers. However, the issue of NAT traversal is still an impediment to widespread adoption of SIP and the reality of converged communications. Enterprises of all sizes are looking for the right solution to bring the benefits of such collaboration into their network, and to do so while maintaining security and control.

SIP-capable firewalls and SIP-enabling edge devices provide the means to solve the traversal issue even in scenarios where there are tight security policies and SIP devices on the LAN that are used for communication with the outside world.

The choice really comes down to the level of control that an organization is willing to cede to third parties or to the clients and users themselves. SIP-capable firewalls and enterprise SBCs offer the greatest amount of control with flexibility for the company to deploy the communication tools that it needs without sacrificing the security and integrity of the enterprise network.

About Ingate

Ingate® Systems develops firewall technology and products that enable SIP-based live communication for the enterprise while maintaining control and security at the network edge. Ingate has a long history of developing next-generation firewall technology that solves the NAT/firewall traversal issue with SIP communications. In addition to an extensive line of Ingate Firewalls®, the company also produces the award-winning Ingate SIParator®, a device that connects to an existing network firewall to seamlessly enable SIP communications. Ingate products currently protect the networks of retail companies, financial institutions, industrial firms, government agencies and small-to-large enterprises throughout Europe, Asia and North America. Ingate Systems AB is headquartered in Sweden with offices in Stockholm and Linköping. Its wholly-owned subsidiary, Ingate Systems Inc., is located in Hollis, New Hampshire, with a U.S. technology center in Frisco, Texas. For more information on Ingate Systems, visit www.ingate.com.

ABOUT SHORETEL

ShoreTel is the provider of brilliantly simple Unified Communication (UC) solutions based on its award-winning IP business phone system. We offer organizations of all sizes integrated, voice, video, data, and mobile communications on an open, distributed IP architecture that helps significantly reduce the complexity and costs typically associated with other solutions. The feature-rich ShoreTel UC system offers the lowest total cost of ownership (TCO) and the highest customer satisfaction in the industry, in part because it is easy to deploy, manage, scale and use. Increasingly, companies around the world are finding a competitive edge by replacing business-as-usual with new thinking, and choosing ShoreTel to handle their integrated business communication. ShoreTel is based in Sunnyvale, California, and has regional offices and partners worldwide. For more information, visit shoretel.com.

WORLD HEADQUARTERS	960 Stewart Drive, Sunnyvale, CA 94085 USA. shoretel.com +1 (800) 425-9385 Toll Free +1 (408) 331-3300 Tel. +1 (408) 331-3333 Fax
EMEA	+800 408 33133 Freephone +44 (1628) 826300 Tel.
ASIA PACIFIC	+61 (0)2 9959 8000 Tel.

