THE INGATE SIPARATOR

WHITE PAPER

Ingate Systems Inc Farley Road Hollis, NH 03049 USA Tel 1-603-883-6569 info@ingate.com www.ingate.com
Ingate Systems AB Box 10013 121 26 Stockholm-Globen Sweden Tel + 46 (0)8 600 77 50 info@ingate.com www.ingate.com

THE INGATE SIPARATOR™

1 Executive Summary

Support for Session Initiation Protocol, or SIP, is essential in today's enterprise communications environment. With the standardization of SIP as *the* Internet protocol for applications such as VoIP, instant messaging and IP telephony, businesses are eager to adapt their existing hardware to accept SIP. However, far too many companies have made substantial investments into legacy firewall technologies that are not capable of supporting this type of communication. In addition, enterprises are reluctant to touch existing security infrastructure for fear of creating security breaches.

The award-winning Ingate SIParator™ addresses these issues by offering the introduction of a SIP-capable communications infrastructure while preserving the investment made in legacy firewalls.

The Ingate SIParator™ works in tandem with any enterprise firewall, preserving security technologies already in place. Its proxy-based solution ensures complete SIP functionality while maintaining the highest degree of security.

With the SIParator™, enterprises of all sizes can safely integrate support for person-to-person communications like VoIP, instant messaging, *etc*. within their organizations without having to take substantial financial losses and without compromising security.

2 Balancing Security and Communication

Running the IT network of a modern enterprise is a constant trade-off between stopping unwanted intrusions while still allowing desired communication flow. One of the most complicated intrusion issues to date – the emergence of the Internet – has presented companies with a tremendous security problem. As a gateway to information globally, such a substantial resource has of course become an integral part of the daily working environment. In fact, its importance to the corporate world is expected to continue to grow. Unfortunately, that gateway is also a portal through which hackers and other unwanted intruders have been able to access the network.

To date, most companies and individuals associate the Internet with email and Web surfing, and in fact it has been those two applications which helped spread Internet usage beyond the boundaries of the "tech gurus" and into the homes, family rooms, schools, *etc.* of the general public. Technology has adapted to accommodate this broad adoption of email and Web surfing: from the increase in broadband access to homes and businesses, to the evolution of enterprise firewalls that stop unwanted intrusions while still allowing email to get through.

Yet email and Web surfing only scratch the surface of the Internet's capabilities. Real-time communications are fast becoming the next big step of Internet usage among businesses and individuals alike. The need for mobility is increasing, and to meet that need hardware and software companies are working diligently to generate applications that allow users to connect faster, better, cheaper – and directly, in real-time. These types of communications are generally known as "real-time person-to-person communications," and include:

- Voice (of which IP telephony / VoIP just is one component)
- Video
- Presence (information on when a person you wish to contact is available, whether or not they are present and how to best reach them)
- Instant messaging
- Conferencing with voice, video and data collaboration

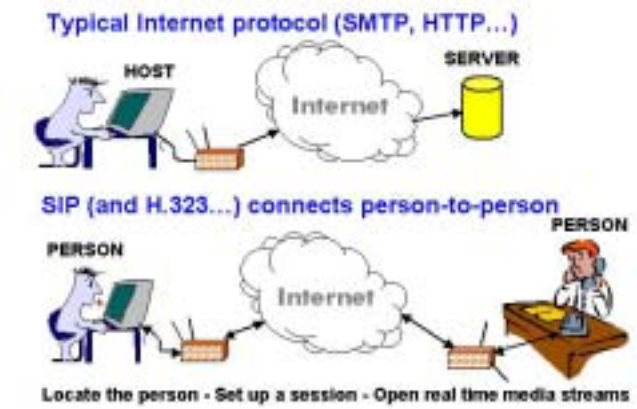
Several forms of Web-based person-to-person communications have been in use for years. The problem has been that software companies have each been using different Internet protocols, making it difficult for IT managers to choose which program will best reach the majority of their audience. However, an IETF signalling standard has recently been established – SIP, or Session Initiation Protocol – which is expected to transform the real-time person-to-person communications playing field by integrating these types of applications. Since demand for such a standard has been tremendous, it is anticipated that adoption of these applications will spread very quickly, enjoying accelerated exponential growth.

With this anticipated growth of, and demand for, SIP-based communications, it is now critical for IT managers to strike that balance between the needs of their constituencies and the security of the enterprise. The logical place on the network to ensure security is the firewall.

3 The Problem of SIP and Security

Many IT managers overlook the importance the firewall plays in the deployment of a SIP-capable enterprise. Yet SIP can pose problems with security, making traversing the firewall one of the first issues to consider when implementing these types of applications.

The first problem is that the media in SIP-based communications (*e.g.* voice and video packets) are sent over dynamically assigned ports that are determined through a negotiation between the two parties of the session. This differs from the host-to-server architecture traditionally used in Web browsing. For SIP, the firewall must be designed to monitor the port negotiation and dynamically open the required port in order to allow SIP media flow.



The second issue has to do with the private IP addresses that result from the use of Network Address Translation (NAT). SIP-based communications clients (whether IP telephones of soft clients on a PC) sitting on a private IP address on the corporate LAN cannot be reached by a call from the outside of the firewall. This is because it is impossible for the caller to know on which (private) IP address the called party is sitting. There is simply no way for a caller to locate their party.

4 Most Firewalls Don't Support SIP

The firewall solution will ultimately determine whether the enterprise will – or will not – be able to accept SIP-based communications. The majority of firewalls currently in-place, as well as those available on the market, do not support SIP. Since the issues noted above actually occur for all similar protocols, it is a common misunderstanding that older firewalls can be reconfigured to handle SIP traffic. That is absolutely not the case. Reconfiguring non-SIP-capable firewalls is not possible. The result is guaranteed to compromise enterprise security.

Unfortunately, most firewalls available on the market are also not SIP-capable. When making the investment to purchase a new firewall solution, it is imperative that IT managers who want to implement SIP-based applications include full support for SIP through a proxy specifically designed for that protocol.

There is another option.

5 Preserving Your Firewall Investment

For companies looking to adopt SIP-based communications but have already made a significant investment in their firewall, options have been limited: buy a new SIP-capable firewall. This becomes an inhibiting factor in the enterprise adoption of SIP based person-to-person communications. A single firewall installation can represent investments of tens of thousands of dollars.

However, the Ingate SIParator™ offers a new solution, one that allows businesses to preserve their initial investment by allowing the introduction of SIP based person-to-person communications applications without replacing the legacy firewall. This significantly reduces the start-up costs of joining the SIP community, all the while providing a secure network.

6 What is a SIParator™?

The Ingate SIParator™, named "Product of the Year" by *Internet Telephony*, is a device that attaches to an existing firewall to make it SIP-capable – instantly. The Ingate SIParator™ contains a SIP proxy and registrar which performs the functions necessary to achieve seamless traversal of the firewall for SIP signalling and media.

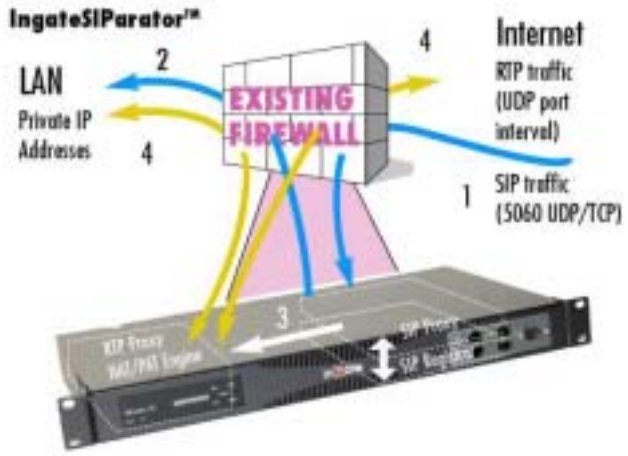
6.1 Who Needs a SIParator™?

The Ingate SIParator™ is suitable for organizations that already have an existing firewall that fulfils all other requirements except SIP support. The Ingate SIParator™ will work together with any existing firewall and very little reconfiguration of the network.

6.2 How Does it Work?

The Ingate SIParator™ effectively serves as a firewall for SIP traffic. The SIP signalling on port 5060 is directed to the IP address of the SIParator™, as is the corresponding media after the endpoints have negotiated the ports to use for this traffic.

In order for SIP traffic to reach the SIParator™ the existing firewall needs to be configured so that port 5060 is statically left open in both directions. The port is only opened between the SIParator™ itself and the outside and inside respectively. The SIP proxy on the SIParator™ will permit only valid SIP traffic to flow across the firewall/SIParator™ pairing.



A configurable range of UDP ports are assigned to the SIParator™ to handle media. This port range is left statically open between the existing firewall and the SIParator™, which manages the dynamic opening and closing of the ports as needed. Because the SIParator™ maintains full control of all SIP sessions it is able to inspect the packets of media traffic to ensure that they belong to a valid active session.

7 SIParator™ Configuration Options

The Ingate SIParator™ can be configured in a variety of ways to cater to the needs of a live network environment. Issues that determine configuration include current load from data traffic on the existing firewall, the capabilities of the existing firewall and the security policies of the organization itself.

7.1 DMZ Configuration

In DMZ configuration, the Ingate SIParator™ is connected through one single interface to the existing firewall. All SIP-signalling and media is routed via the Ingate SIParator™ to user agents on the LAN.

Configuration 1: DMZ Configuration

7.1.1 Requirements

The requirements on the existing firewall for DMZ configuration include making sure that there is a DMZ port available on the firewall to which the SIParator™ can connect. Port 5060 and a range of UDP ports must also be statically opened between the WAN side of the firewall and the SIParator™, and between the SIParator™ and the LAN side of the firewall.

Also, there can not be any NAT traversal between the DMZ and LAN. Additionally, the SIParator™ must have its own separate global IP address.

7.1.2 Advantages

In the DMZ configuration, the SIParator™ features are available to all sub networks behind the firewall. The logging of all traffic can also be maintained by the existing firewall when using the DMZ configuration option.

7.1.3 Disadvantages

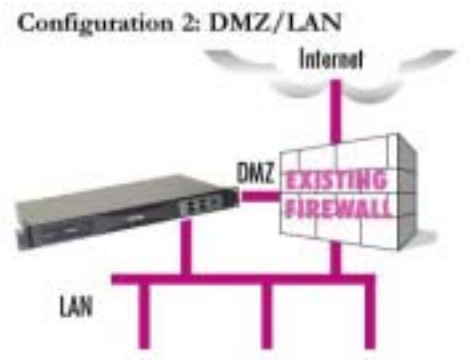
In this configuration, all SIP-related traffic is routed through the existing firewall twice. If the existing firewall is already working near capacity, this can be an issue which may cause overload and/or delay to the media.

7.1.4 Configuration for Internal SIP User Agents

User agents on the LAN (for instance, SIP phones of soft clients) are configured with the SIParator™ as their outbound proxy. In the event that an internal proxy is on the LAN, the Ingate SIParator™ must serve as its outbound proxy. User agents on the LAN cannot use a proxy outside the firewall directly, but the Ingate SIParator™ can be configured to use the external proxy. The user agents will then reach it by going through the SIParator™ as outgoing proxy.

7.2DMZ / LAN Configuration

In the DMZ-LAN configuration, the Ingate SIParator™ is connected through two interfaces: one to the DMZ interface on the existing firewall and the other to the internal LAN. In this configuration, the SIP-signalling and media pass through the firewall once on their way to Internet. For internal traffic (between two clients on the LAN) the traffic will not pass through the firewall at all.



7.2.1 Requirements

The requirements on the existing firewall are identical to that of DMZ configuration.

7.2.2 Advantages

Compared to the DMZ configuration, this architecture decreases the load on the existing firewall. The logging of all traffic can still be maintained by the existing firewall when using the DMZ/LAN configuration option.

7.2.3 Disadvantages

Since the SIParator™ is connected directly onto the LAN, the SIP capabilities that it enables will only be available to that sub network. If the firewall is configured with several internal networks, only the one to which the SIParator™ is connected will be able to use SIP-based applications.

7.2.4 Configuration for Internal SIP User Agents

Internal user agents are configured in the same way as described for the DMZ configuration (see section 7.1.4 above).

7.3 Stand Alone Configuration

The Ingate SIParator™ is connected in parallel with the existing firewall, with one interface to the WAN and one interface to the LAN. No SIP-signalling or media passes through the firewall and therefore this configuration option puts the least requirements on the existing firewall.

7.3.1 Requirements

The only infrastructure requirement for the standalone configuration is the need to dedicate one global IP-address to the SIParator™.

7.3.2 Advantages

This configuration does not put any extra load onto the existing firewall. There are also no requirements for a DMZ or any other feature on the existing firewall.

7.3.3 Disadvantages

In the standalone configuration, the existing firewall loses the ability to control and log SIP-related signalling and media. However, the SIParator™ is designed to take over this critical function, allowing full information on the traffic to still be available.

7.3.4 Configuration for Internal SIP User Agents

Configuration of internal user agents is identical to that of the DMZ configuration.