The Ingate SIParator

Solving the firewall/NAT traversal issue of SIP

1 Executive Summary

The SIParator is a firewall which can be installed either in the DMZ of an existing firewall, or as a standalone entry point into the LAN. The SIParator's primary function is to resolve the NAT and firewall traversal problem encountered when SIP-based communications are added to the network. The SIParator is designed to first apply strict SIP parser policies to the signaling to verify that the packets are valid. Since the SIParator is built on ICSA-certified firewall technology, the enterprise is assured that it can withstand various types of security attacks in a stable and controlled fashion, providing the enterprise with the tools necessary to control and manage the SIP traffic to the same level as it does with data traffic. With the SIParator the enterprise is in full control of what type of SIP-related media is admitted to the network, and the source and IP addresses of the signaling and media.

2 The Problem with Session Initiation Protocols and Enterprise Firewalls

Session Initiation Protocol (SIP) creates the third big wave of Internet usage after SMTP (email) and HTTP (web). SIP has become the signaling protocol of choice for establishing realtime communications including voice-over-IP (VoIP) and collaboration. The SIP standard is designed to work well with the other protocols used on the Internet and includes several features that support network security, like authentication and encryption. And, because it is a standard protocol, measures can be taken to ensure that the traffic that is being presented to the enterprise is based on properly formed SIP signaling

However, SIP-based communications do not reach users behind firewalls and Network Address Translation (NAT) devices automatically, because firewalls are designed to prevent inbound communications and typically do not support the SIP protocol. Further, the NAT creates private IP addresses which are not publicly routable, meaning that inbound SIP communications cannot reach the intended recipient on the Local Area Network (LAN).

This issue of SIP traffic traversing the enterprise firewall or NAT is critical to any SIP implementation, including VoIP. One solution that is being adopted by enterprises around the world is the Ingate SIParator®, which serves as a firewall that specifically handles SIP traffic. The SIParator is a unique, award-winning device that works in conjunction with an existing network firewall, which means that the enterprise can keep its security infrastructure in place while adopting SIP communications.

This paper will present the security features of that product and its benefits to the enterprise adopting SIP.

With the SIParator in place, the enterprise can manage and control the SIP traffic and establish policies for what is admitted to the network and from where. Most importantly, the SIParator validates the SIP signaling to ensure that the packets are properly formatted. Further, the Ingate SIParator maintains the state of all SIP sessions and rejects any unrelated

SIP packets. And since the SIParator can be configured in the DMZ of an existing firewall, the enterprise is assured that all traffic including SIP is logged by both the firewall and the SIParator for maximum security.

3 The SIParator is a Firewall Specifically for SIP Traffic

The SIParator is designed to be installed in networks which are already protected by a firewall that the management does not wish to replace. The SIParator is a firewall, but has non-configurable factory settings which prevent the admittance of any other protocol except SIP.

The SIParator solves the basic problem of firewall and NAT traversal using a proxy-based implementation. The SIP proxy architecture is a complete solution to the firewall and NAT traversal issues introduced 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 and without degrading the voice or video quality.

Before the signaling is forwarded to the intended end point, it must pass through a strict SIP parser to validate that it is properly-formed SIP signaling. This is a function that is only possible with a proxy solution and provides the enterprise with the assurance that the traffic is properly formed and is not corrupted signaling.

The other benefit of the proxy solution is that the SIParator maintains the state of all SIP sessions. This means that unrelated SIP packets will not be allowed to pass through the SIParator in either direction. This security feature ensures that no session is hijacked for malicious purposes.

Further, the Ingate SIParator is built on an ICSA- (formerly known as the International Computer Security Association) certified firewall architecture, which has been proven to withstand security attacks in a stable and controlled fashion. The SIParator is a firewall that is designed to process only SIP traffic. The SIParator adheres to the ICSA definition of a firewall:

> "A firewall is a single point between two or more networks where all traffic must pass (choke point); traffic can be controlled by and may be authenticated through the device, and all traffic is logged."

In summary, the SIParator is able to perform the following basic and optional functions and supports the security requirements of the enterprise:

3.1 Basic Functions

- **ICSA certified firewall technology**

- **SIP proxy and SIP registrar**

- **Supports all SIP services including voice, video, instant messaging, conferencing, file transfer, application sharing, white boarding *etc.***

- **Near-end NAT traversal** for bringing SIP communications into a network. But as a proxy we not only provide this basic functionality, in conjunction with it we also:
  - Monitor the SIP signaling ports
  - Inspect everything received on those ports with a strict SIP parser to ensure that it is proper SIP signaling (not corrupted)
  - Rewrite the headers to enable the SIP signaling to reach the intended recipient on the inside of the network at their private IP address
  - Dynamically open the media ports to admit voice or video on both UDP and TCP ports
  - Rewrite the headers to deliver the media to the appropriate destination
  - Rewrite the headers of outbound traffic to keep the private IP addresses hidden
  - Maintain the state of all sessions and reject all unrelated SIP packets
  - Close the media ports when the session is finished

- **Extensive filtering and admittance policies, capabilities and packets can be limited based on:**
  - Source IP addresses
  - SIP methods
  - SIP content (media) type
  - Transport methods
  - SIP domain
  - SIP user

- **Authentication against a Radius server or local database**
  - Prevents identity theft and impersonation

- **Encryption for communication privacy and prevention of eavesdropping**
  - Support encrypted SIP signaling using TLS as an added network protection feature and to keep Instant Messages private
  - Support for Microsoft and SRTP (sdescriptions) media encryption
    - Termination, the media to the LAN in the clear
    - Transcoding, translate between media encryption types
    - Pass through, re-encrypt the media with the same algorithm and forward to the LAN.
    - VPN termination supporting IPSec with 3DES and AES encryption and PPTP

- **Standards-based Solution** fully compliant with the SIP standard and interoperable with most major suppliers of SIP products including Avaya, 3Com, Pingtel, Microsoft, Cisco, Snom, Audiocodes, Vegastream, and many others.

- **Excellent control and management** of the SIP traffic passing to and from the corporate network, allowing the enterprise to apply the same level of security policies to the VoIP traffic as it does to data traffic.

- **Extensive logging, reporting and audit capabilities**

- **Security protection against:**
  - Malformed message attacks
  - Buffer overflow attacks
  - Denial of Service and Distributed Denial of Service attacks
  - RTP Session hijacking
  - Injection of inauthentic RTP packets into existing RTP flows
  - Voice Spam
  - Packet level intrusion
  - Session hijacking and redirection
  - Vmail bombing
  - SIP Spam

- Supports SNMP for integration with network frameworks (HP OpenView, IBM Tivoli, CA UniCenter, BMC Patrol)

- Integrates with F5 Networks Big-IP

3.2 Optional Functions

Ingate offers several optional functions. All modules are separately priced.

- **Remote SIP Connectivity (RSC)**
  The Remote SIP Connectivity module enables employees or customers to work from behind a NATting device and make and receive SIP calls using the PBX located at the corporate headquarters. This module includes:

  - STUN server on board to support STUN clients, if available
  - Far-End Nat Traversal which is used when a STUN client is not available, or if the remote user is behind a symmetric NAT. With the RSC enabled, the Ingate unit negotiates through the far-end NAT device and keeps a pinhole alive as long as the client is registered.

- **Advanced SIP Routing (ASR)**
  This module enables the product to provide even greater functionality for control of the enterprise, including:

  - Matching on various header information

- Options to rewrite the Request URI on forwarding
- ENUM lookup
- Defined parameters by user
- Common blacklists

- **VOIP Survival**
  The VoIP Survival Module allows an enterprise that is using a CENTREX or hosted PBX solution to fail over to the Ingate device at their site to enable internal calls, and re-direction of outside calls to a local PSTN gateway.

- **Quality of Service**
  This module allows the enterprise to tag certain packets and then to prioritize the delivery of those packets. This is useful to ensure good voice quality.

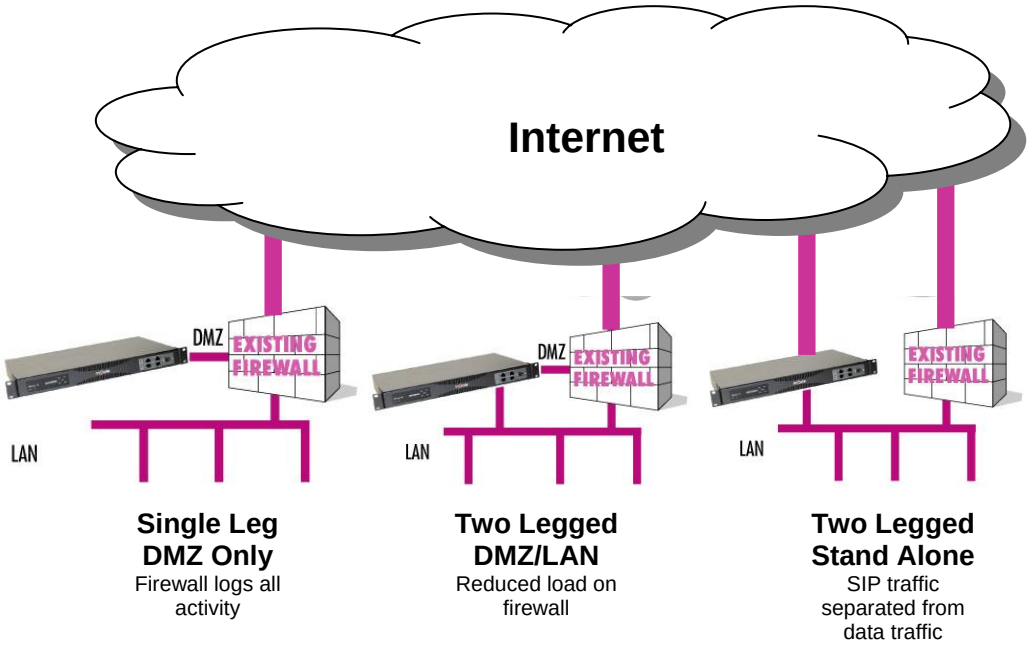
4 About Ingate® Systems

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 inherent in 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.

Appendix 1. SIParator Configurations

SIParator Network Configurations

The SIParator has been designed to work in parallel with an existing firewall to give the enterprise maximum flexibility in the adoption of SIP and solving the NAT traversal issues. Typically the SIParator is installed in one of the following three ways:



SIParator in the DMZ mode (scenario 1 and 2)

In either of the first two scenarios, the SIParator performs its function in the DMZ of the existing firewall. This provides several benefits for security:

- One physical entry point into the network
- The existing firewall continues to log all traffic, including the SIP traffic
- All networks connected to ANY of the firewall's interfaces can be SIP-enabled

Using this configuration, the SIParator is located on the DMZ of the firewall, and connected to it with only one interface. This is the safest configuration, since all traffic goes through both the firewall and the SIParator. It is also the most flexible, since all networks connected to any of the firewall's interfaces can be SIP-enabled. On the firewall, the SIP port (normally UDP port 5060) and a range of UDP ports for RTP traffic must be opened between the SIParator and the Internet as well as between the SIParator and the internal networks. The SIP traffic finds its way to the SIParator using DNS or by setting the SIParator as an outbound proxy on the clients. The firewall must not use NAT for the traffic between the SIParator and the internal networks OR for the traffic between the SIParator and the Internet. However, the SIParator can itself use NAT for traffic to the Internet.

The DMZ of the existing firewall must be a "true" DMZ with abilities to set the configuration parameters that are described above. Some vendors are offering "virtual DMZ's." Some of these have a physical port, but the IP address of this port is "shared" with the IP address of the

outside/WAN port. With these types of DMZ's, most do not have the ability to turn off NATing from the DMZ to the LAN, which is a requirement. The firewalls CANNOT do the NATing to the LAN. This means they need be to be able to support the following:

- SIParator in DMZ must have public (non-NATed) IP address
- Firewall cannot NAT traffic from SIParator to LAN
- Must be able to write rules for traffic between Internet and SIParator and for the SIParator and LAN

SIParator in the Stand-Alone Mode (scenario 3)

The third configuration offers the alternate method of installation in the event that the DMZ does not support the requirements for supporting the SIParator or if the enterprise does not want to add the SIP traffic as an additional burden on the limited bandwidth of the existing firewall.

Although in this case the existing firewall does not process any of the SIP packets, the SIParator is based on an ICSA-certified firewall architecture. In the SIParator configuration, all other protocols are stopped. All data traffic is processed by the existing firewall, but all SIP traffic is processed on the SIParator.

All of the capabilities regarding SIP inspection, routing, authentication, encryption and filtering are fully available to the enterprise to ensure that the security of the network is not compromised.