Ingate Firewall/SIParator®
SIP Security Best Practice

02 September 2008

Table of Contents

Tested versions: Ingate Firewall and SIParator - Version 4.6.2
Startup Tool - Version 2.4.0

Revision History:

Revision	Date	Author	Comments
	2008-09-02	Scott Beer	1st draft

1 Technology Introduction and Challenges

1.1 SIP Protocol

Session Initiation Protocol is an Application Layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, multimedia conferences, and presence. The SIP Protocol is defined as part of IETF RFCs starting with RFC 3261, and more, all located at www.ieft.org.

SIP invitations are used to create sessions that carry session descriptions, which allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features for users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols, such as UDP, TCP and TLS.

The SIP requests and responses are written in plain text within the datagram of the IP Header. SIP is not implicitly secure and is communicated clear over the Internet. Contained in the SIP requests and responses are the addresses of the source and the destination of the participants. These addresses are SIP URI's, which have a UserInfo and Host Address, and this host address can either be an IP address or a domain name, for example a SIP URI can look like "sip:scott@ingate.com" or "sip:6139630933@207.112.18.164". Confidential IP Addresses and SIP URI addresses are in plain text for anyone to read and possibility intrude upon.

1.2 Network Address Translation (NAT)

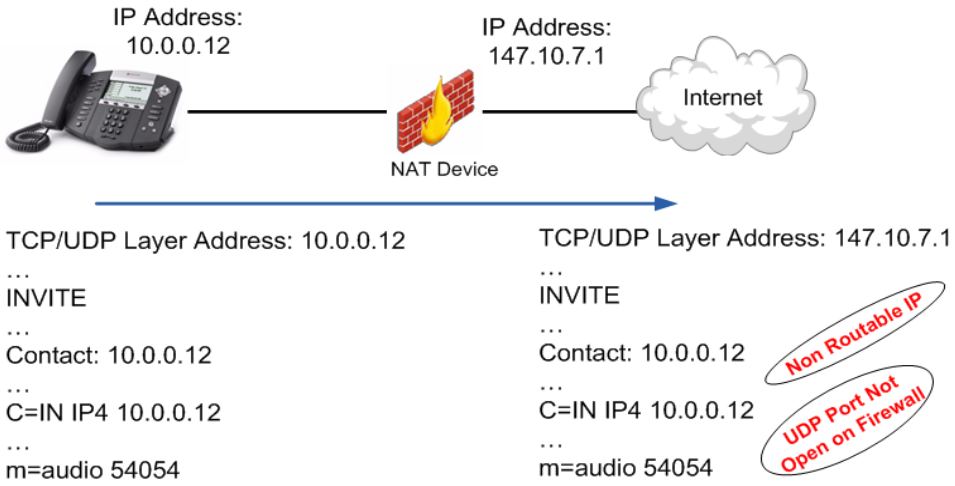
Network Address Translation (NAT) provides the translation between a single public IP address on the WAN and multiple private IP addresses for all of the workstations, Servers and other IP equipment within the LAN. The router running NAT should never advertise the LAN network addresses to the WAN network backbone. Only the networks with global addresses may be known outside the router. However, global information that NAT receives from the border router can be advertised in the LAN network the usual way. Typical or traditional firewalls apply NAT to the TCP/IP protocol at the Transport and Network layers.

The network addresses inside a private domain can be reused by any other private domain. For instance, a single Class A address could be used by many private domains. At each exit point between a private domain and the public WAN backbone, NAT is installed. If there is more than one exit point it is of great importance that each NAT has the same translation table.

As the addressing and routing of SIP Protocol are done at the Application Layer, the biggest problem the SIP Protocol now has is the disconnect between the IPv4 addressing and routing at the Application Layer versus the IPv4 addressing and routing at the Transport and Network layers. NAT further impedes the SIP Protocol as NAT works to hide IPv4 addressing and routing at the Transport and Network layers, as SIP communication traffic through a NAT device will completely disconnect the two addressing schemes.

OSI Model				
	Data unit	**Layer**	**Function**	**Protocol**
Host Layers	Data	7. Application	Network process to application	SIP Protocol Addressing
		6. Presentation	Data representation and encryption	
		5. Session	Interhost communication	
	Segment/Datagram	4. Transport	End-to-end connections and reliability (TCP)	NAT Addressing
Media Layers	Packet	3. Network	Path determination and logical addressing (IP)	
	Frame	2. Data Link	Physical addressing (MAC & LLC)	
	Bit	1. Physical	Media, signal and binary transmission	

The general rule is "NAT Breaks SIP".

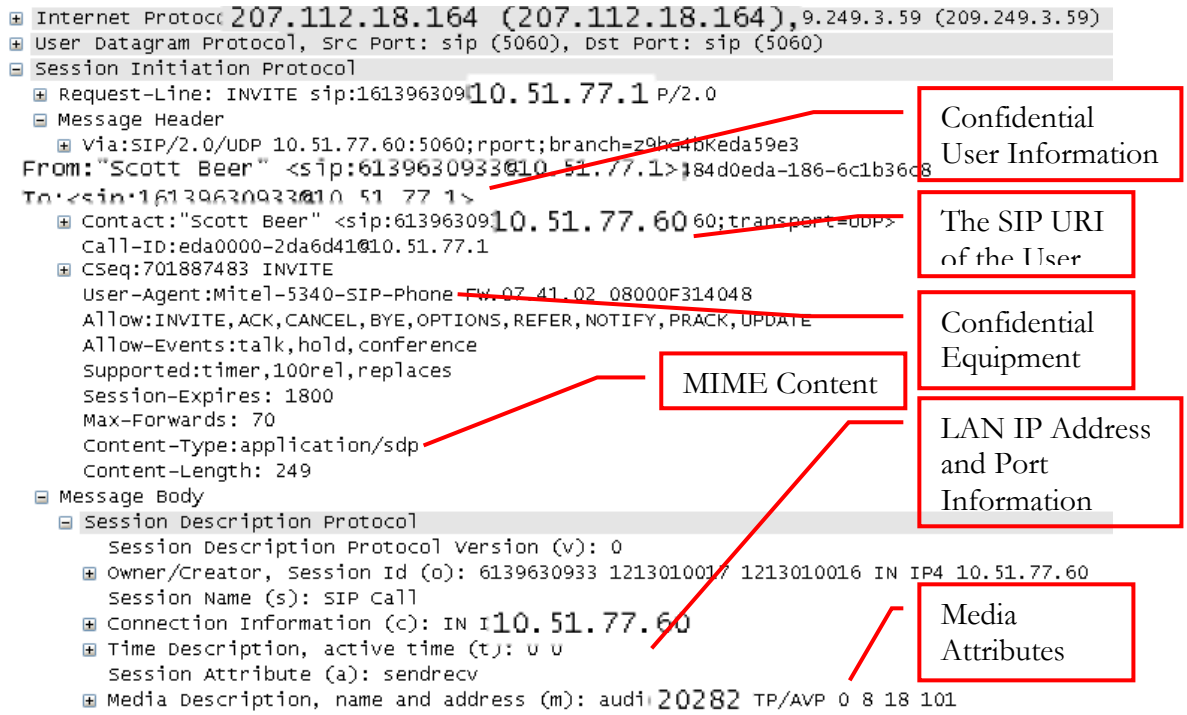


1.3 Network and SIP Communication Security

1.3.1 SIP Protocol Vulnerabilities

The SIP Protocol resides in the Application Layer; it is written in clear text within the datagram of a UDP or TCP Transport. Because the SIP Protocol is in clear text, it is readily readable to any malicious efforts to compromise your VoIP or Data traffic. Sensitive IP address information, Port Address information, contact addresses, usernames, SIP compliance capabilities, media stream attributes and more are all contained in the SIP Protocol. When SIP is sent out over the Internet, the enterprises sensitive networking and VoIP information becomes available for everyone to see. This could result in compromises on several fronts.

Here is an example of a open text seen in a SIP Request over the public Internet, showing where SIP can compromise an Enterprise environment.



Here are some of the vulnerabilities exposed.

LAN IP Address Scheme

Sensitive LAN IP Addresses are provided; this provides hackers and malicious software insight into the LAN network topology. This sensitive information can be helpful for any malicious attempts to gain access to the LAN Network.

Calling and Called Party Information

The Users Name and Phone Number along with the called party's number are provided. This compromises the user privacy to their phone activity; by knowing who, where and when users made calls too.

SIP URI

A SIP URI is the addressing scheme in the SIP Protocol. The Contact Header provides the exact SIP URI (SIP Address) to send all SIP responses too. This gives hackers and malicious attacks the precise address to send an attack too. For example, giving your email address for all to see, this time instead of SPAM email, which can easily be deleted, malicious activities can range from be DoS Attacks or attempts to Intrude on SIP Services (ex. Toll Fraud).

Port Address Allocation

Port addresses are just as important as IP address, giving hackers and malicious attacks key port information of the device. Knowing exactly what ports are used and in turn attempting to comprise this open port.

Media Attributes

The Media Stream encoding information is provided; giving Hackers and malicious activity knowledge of the format of the media stream. This can allow them to decode the media for playback and listen to your conversation.

Vendor Equipment

Knowledge of vendor equipment can be exploited, having knowledge of the equipment hacker and malicious attack can target any known vulnerabilities of the vendor.

MIME Content Type

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of e-mail. However, MIME has grown beyond describing the content of e-mail to describing content type in general. In SIP Protocol it is used to describe additional applications, audio and video streams, images, text (IM) and more. A typical application is SDP (Session Description Protocol) where Media Codecs and addressing are negotiated. But there are others, like Message Waiting (simple-message-summary), Instant Messaging (dialog-info+xml). The risk is the use of the SIP Protocol to receive MIME content that is not wanted. Allowing the possibility of receiving an SPAM Instant Message could occur. The concern might be; what data could be transported in the MIME content of a SIP message.

Given that SIP is a relatively new protocol for VoIP deployment, and is not yet a widespread deployment, there have been very few malicious SIP attacks. But as the popularity grows, and SIP becomes more widespread the possibility of a malicious attack grows. Given the ease at which SIP Traffic can be opened and viewed by anyone, it's a sure thing that someone will try to discover a weakness in an Enterprise SIP communications platform. Toll Fraud, Intrusion of SIP Services, and Denial of Service, to name a few, are just some of the things that malicious people could consider. It would be naïve to think someone won't try to take advantage of the SIP communications and security weaknesses.

The IP-PBX as the controller for all of the VoIP Phone and applications should be deemed a "Mission Critical" server. Any service outage or degradation would result in the loss of communication and ultimately the loss of business revenue. With SIP exposing IP addresses in clear, it becomes obvious that security needs to be considered as another focus in a SIP trunk deployment scenario.

1.3.2 Media Stream Vulnerabilities

In addition, the VoIP media stream is also unencrypted, common media streams such as G711, G723, G729 and others are open for malicious efforts to record conversations over the Internet. Sensitive voice conversations over the Internet with lawyers, brokers and more can be maliciously recorded. As the SIP Protocol provides all of the connection information for the Media Stream, hackers and malicious activities have all the knowledge they need to intercept and record the audio conversation.

1.3.3 Network Vulnerabilities

The Internet (WAN)

The Internet is a network like any other, every device connected to the Internet is accessible from all other devices connected to the Internet. This is a public space for all to use and abuse, a great environment for information sharing and enterprises, but a hazardous environment without control. From a security perspective the Internet is an "Untrusted Network". SPAM/SPIT issues are a constant concern; hackers and malicious software are constantly attempting attack networks, computers and devices with Service Intrusion attacks, Denial of Service attacks, and a host of other fraudulent activities.

The Local Area Network (LAN)

Protecting an Enterprise Network is always the highest priority. NAT devices, such as Firewalls are the solution to most all network security. NAT provides the translation between a single public IP address on the WAN and multiple private IP addresses for all of the workstations, Servers and other IP equipment within the LAN. This is an effective way to hide private network IP addresses.

But NAT and SIP do not work together, sending SIP communications out a NAT device will effectively fail. In an attempt to overcome NAT issues, many IP-PBX and ITSP vendors will recommend to "Port Forward" or "Tunnel" all UDP and TCP traffic on Port 5060 (SIP Signaling Port) and a range of thousands of Media Ports on the NAT Firewall to the IP-PBX. As you may know Port Forwarding creates a Hole in your firewall, now forwarding ALL UDP or TCP traffic to the IP-PBX. This UDP/TCP traffic may not only be legitimate SIP Protocol messages, but also malicious hacker traffic attempting to gain access to your network, on what could be thousands of ports.

Other Foreign Networks

There are a large number of scenarios in connecting networks together; Networks from Remote Offices, Service Providers, Inter-Businesses, LAN Extensions, and many other sources of networks. They can be connected using various types of connectivity, T1, MPLS, WAN Ethernet, and many others. The vulnerability comes in the level of trust you place between an Enterprise LAN network and the other networks being connected to it. Leaving access open between foreign networks and the Enterprise network can leave your network open their vulnerabilities and open to hackers and malicious software located on the foreign network. These foreign networks connected to the local enterprise network should be labeled an "Untrusted Network". Ultimately a security control point needs to be created between the local enterprise network and any foreign network connected to it.

2 SIP Security Solution: Ingate SIParator/Firewall

2.1 Resolving the SIP thru NAT Issue

In the first section the SIP Protocol and NAT was discussed, and we learned that the SIP protocol resides in the Application Layer. The SIP addresses are formed as SIP URI's, with a Userinfo@host, where the host can be an IPv4 IP address or domain name. Thus SIP requests, responses and routing are controlled at the Application layer. NAT provided an address translation between private LAN addresses and public WAN addresses. This translation was done at the Transport and Network layer within the Internet Protocol Header. The general rule is "NAT Breaks SIP".

Typical firewalls do not apply NAT to the Application Layer. As SIP is an Application Layer protocol, the IPv4 addresses and domain resolution are not translated for Application Layer routing through a NAT device. SIP traffic cannot effectively traverse these traditional enterprise firewalls and NAT devices, and as a result, the firewall/NAT device incorrectly routes all SIP traffic, which includes VoIP. Thus when a SIP phone call attempts to traverse a typical firewall, although the TCP/IP addressing NAT is correct, the IP addresses within the SIP protocol information are not corrected properly. As a result, when a far end WAN device receives a SIP request the SIP addresses are the private IP addresses of the SIP device behind the typical firewall. These private IP addresses are not routable back to the original source.

Ingate SIParator/Firewalls contain functionalities such as SIP Proxy, SIP B2BUA, SIP Media Relay, and a SIP Registrar that are above the typical firewall NAT capabilities. These SIP functional components allow the traversal of the IP addresses within the SIP protocol at the Application Layer. This capability within the Ingate SIParator/Firewall will inspect each SIP packet, and substitute the private IP addresses with the public IP address.

The Ingate SIParator/Firewall will allow the network traversal of SIP Trunking calls to various ITSPs from the IP-PBX. The Ingate controls both incoming and outgoing SIP communications and routes the SIP communication to the intended users and devices. The advantage of the Ingate Firewall is that it will allow all voice traffic as well as data traffic to traverse the enterprise firewall/NAT/ALG. NAT firewall with ALGs enables enterprises to utilize SIP trunks to ITSPs while continuing to manage data traffic.

Ingate SIParator/Firewalls monitor the SIP signaling port (5060) and apply routing rules and process policies to only the SIP Protocol traffic, where all other UDP/TCP traffic will be discarded and not forwarded to the IP-PBX. In addition, the Ingate SIParator/Firewall will dynamically open and close media ports based on the negotiated SIP Traffic, by carefully monitoring the Media Ports negotiated and responding and routing media accordingly.

This functionality brings the security capabilities to the Ingate product, there is no longer a requirement to "Port Forward" thousands of ports to an IP-PBX, a "mission critical" application. In addition, allows the Ingate to take responsibility of SIP Security away from the IP-PBX and put it on the network edge, keeping the LAN Network and SIP communications safe

2.2 Addressing the SIP Communication Security

The IP-PBX is the controller for all of the VoIP Phones and applications; it should be deemed a "Mission Critical" server. Any service outage or degradation would result in the loss of communication and ultimately the loss of business revenue. Without compromises, the IP-PBX should be protected from the Internet and foreign or unknown networks.

In an attempt to overcome NAT issues, many IP-PBX and ITSP vendors will recommend to Port Forward all UDP and TCP traffic on Port 5060 (SIP Signaling Port) and a range of thousands of Media Ports on the NAT Firewall to the IP-PBX. As you may know Port Forwarding creates a Hole in your firewall, now forwarding ALL UDP or TCP traffic to the IP-PBX. This UDP/TCP traffic may not only be legitimate SIP Protocol messages, but also malicious hacker traffic attempting to gain access to your network.

2.2.1 Deep Packet Inspection

Deep packet inspection (DPI) is a form of computer network packet filtering that examines the data (datagram) and UDP/TCP header part of a packet as it passes our SIParator/Firewall. The Ingate SIParator/Firewall is searching for non-protocol compliance, SPIT, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information. This is in contrast to shallow packet inspection (usually called just packet inspection) which just checks the UDP/TCP header portion of a packet, commonly found in most NAT Firewall devices.

With Deep Packet Inspection capability, the Ingate SIParator and Firewall have the ability to look at Layer 2 through Layer 7 of the OSI model. As the SIP Protocol resides at the Application Layer (Layer 7) in the OSI Model, the Ingate products have a unique ability to look at both 1) the SIP Protocol packets and provide non-protocol compliance rules, routing rules and statistical information and 2) Provide IDS/IPS security features for an effective against defense against overflow attacks, denial of service (DoS) attacks, and sophisticated intrusions which could occur at this level. This includes headers and SIP protocol structures as well as the actual payload of the message. The DPI will identify and classify the SIP traffic based on a signature database that includes information extracted from the data part of a UDP/TCP packet, allowing the most precise control of any SIP traffic, finer than any classification based only on header information only.

2.2.2 SIP Protocol Security

As the SIP Protocol is an Application Layer (Layer 7) in the OSI Model, the Ingate products have a unique ability to look at the SIP Protocol packets and provide non-protocol compliance rules, routing rules and security policies.

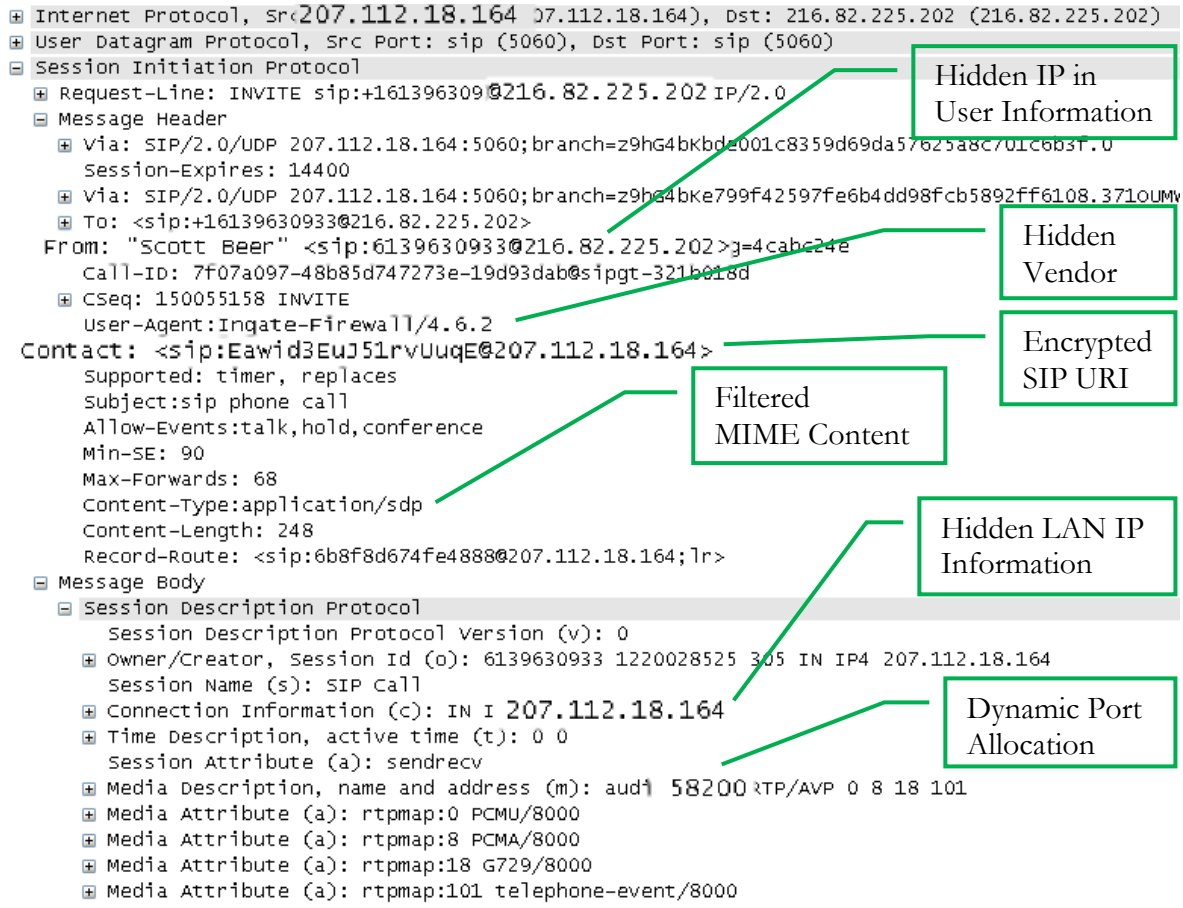
SIP Protocol Compliancy

The Ingate focusing on the SIP Protocol is looking for SIP Protocol compliancy, depending on the nature of the failure to adhere to the SIP Protocol, the Ingate can invoke a denial of service, or can correct the non-conformance if possible. The Ingate can use SIP components such as its SIP Proxy and SIP B2BUA to correct or discard SIP traffic to resolve compliancy issues. The Ingate can apply policies to correct SIP non-conformances in various applications such as; Removal of VIA headers, SIP Offer/Answer call flow, URI Encoding, Username Checks, UDP Packet Size, 180 Response Removal, SIP Method Processing Rules, Escaped Whitespaces Rules, Session Timers, Limitation of Media Streams, Limitation of RTP Codecs, MIME Content Filtering, SIP Method Authentication and so much more.

The Ingate products are SIP Connect Compliant. SIP Connect (www.sipforum.org) is the governing body overseeing SIP Trunking and other SIP deployments. Here are some of the SIP components and features within the Ingate to ensure SIP Protocol compliancy.

SIP Feature	Description
SIP Proxy	• Dynamic routing of SIP Traffic • SIP Security of ensuring of specific SIP Traffic is allowed • Stateful Proxy, monitoring all SIP Transactions, opening and closing ports on every call • Application Layer Gateway functionality for IP Address and Media Port traversal • Independent SIP Session handling
SIP B2BUA	• Everything in SIP Proxy • Separation into two Call Halves for dynamic handling of SIP Protocol. • Customizable SIP Header manipulation • Media Relay B2BUA, ensure media is directed to Ingate
SIP Media Relay	• Direct Media to Ingate to ensure NAT/PAT traversal • Dynamically opening a closing Media ports to allow media in and out of the LAN/WAN • Apply Codec rules and restrictions

Here are some of the vulnerabilities solved by Ingate, even when in clear text over the Internet. In addition, once TLS Transport is used, all clear text is encrypted.



Hidden LAN IP Address Scheme

Sensitive LAN IP Addresses are rewritten to Public WAN IP addresses to ensure all SIP communications are only on the Public side of the Ingate; this ensures hackers and malicious software no view into the LAN network topology and also ensures all subsequent SIP communications are directed back to the Ingate for security control.

Calling and Called Party IP Information

Although Phone numbers persist, LAN IP address information is hidden. Compete security of these numbers can only be provided over the TLS Transport.

Encrypted SIP URI

The most important SIP Header that gives away an Enterprise's SIP address contact information is encrypted. Dynamically on every call the Ingate changes the corresponding SIP URI contact address, ensuring that once the call is complete no further hacker or malicious attack can be directed to the internal SIP User/IP-PBX. For example, the Ingate is denying the ability of giving your SIP URI address for all to see, thus denying malicious activities such as DoS Attacks or Intrusion of Services.

Dynamic Port Address Allocation

The Ingate dynamically changes every Media Port address on every call. Not allowing hackers and malicious attacks an entry into the LAN network. In addition with DPI, only allowing RTP media through these ports while temporally open.

Rename Vendor Equipment

Changing the vendor information ensures the vendor equipment cannot be exploited. The hacker knowing that they must overcome a Security device rather than an IP-PBX may prove to be a deterrent.

Filter MIME Content Type

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of e-mail. However, MIME has grown beyond describing the content of e-mail to describing content type in general. Filtering MIME content ensures the content of a SIP messages are defined, and only the content expressed is allowed to reach the internal LAN and IP-PBX.

TLS and SRTP

In addition, the Ingate Firewall/SIParator offers the ability to encrypt the SIP Protocol signaling by changing the transport from UDP/TCP to TLS (Transport Layer Security). Ingate also includes support for SRTP (Secure Real-time Transport Protocol). Together, this powerful SRTP-TLS combination protects media from being overheard by unauthorized persons, providing a high level of security for live data with advanced encryption, confidentiality, message authentication, and replay protection. Using TLS and SRTP to encrypt signaling and media traversing the Internet effectively stops eavesdroppers, hackers and spoofers.

The Ingate Firewall/SIParator can decrypt the signaling and media and deliver them "in the clear" to devices on the Local Area Network (LAN), or pass the encrypted packets on to the server or phone fully encrypted all the way to the user. This flexibility permits the network administrator to tailor the use of encryption to the needs of the organization and the capabilities of the other SIP equipment in the network.

The integrity of such call is in this case much stronger than ever delivered over PSTN.

2.2.3 SIP Security using Routing Rules and Policies

The Deep Packet Inspection capability of the Ingate SIParator and Firewalls give the ability to apply Routing and Dial Plan rules to all incoming SIP Traffic. As the Ingate product has the ability to look at Layer 2 through Layer 7 of the OSI model, Routing and Dial Plan rules can be combine the use of several layers at once. Combining such things as the TCP/IP (Transport Layer) with the SIP Protocol (Application Layer) to ensure only predefined SIP Traffic is processed.

Routing Rules

The Ingate Dial Plan has three main attributes:

1. Match From Header, where the Ingate can match on the From Header SIP URI, which of course is who is making the call, in addition we can separate the Transport whether UDP, TCP or TLS, and even more we can specify what IP address or range of IP addresses in the Network that we can accept calls from.

2. Matching Request URI, the Request URI Header is a routable header of any SIP Request. Here we have the ability to Match & Remove a Prefix, Match any specific Alpha/Numeric characters or even range of characters. This also includes Domain matching.
3. Forward To, the forward to section defines where to 'actually' send the call. Here the Ingate can send it to a predefined account, with Registration and/or Header Replacement requirements/behavior, or send the call to a IP address or Domain, can change the call request to a different Transport and port if required, and even dynamically assign the use of our B2BUA if needed.

The actual Ingate Dial Plan then combines these three attributes to give the ultimate in flexibility and security in defining accepting where the call is coming from to defining where the call is going to. If the SIP Traffic is not predefined the SIP traffic will be denied.

This also gives the ability to have multiple different IP-PBX vendors and multiple different ITSP accounts. N+1 ITSPs to N+1 IP-PBXs. There is no limit to the customization of call routing in the Ingate.

Policies

Policies related to SIP concern allowing or disallowing SIP traffic based on SIP Methods, SIP Mime Content, SIP Domains and other higher level rules. A SIP Method policy can be implemented to ensure incoming SIP packets are matched on the particular SIP Method and Traffic to specified domains. If required, Authentication can be applied for processing the packet.

Further policies can be applied to filter MIME Content types, to ensure the type of SIP Traffic is allowed. MIME has grown beyond describing the content of e-mail to describing content type in general, as in SIP Protocol it is used to describe additional applications such as audio and video streams, images, text (IM) and more. The Ingate can filter out any SIP messages that will not be supported. Such as sending Message Waiting, and Instant Messages to devices that will not support these types of messages.

Ingate also have other Routing Rules and Policies can be applied to allow for SIP Domain forwarding, Static SIP URI forwarding, SIP Registrar Authentication, and more.

2.2.4 IDS/IPS Security

With deep packet inspection functionality the Ingate can provide intrusion detection system (IDS) and intrusion prevention system (IPS) features with our traditional stateful SIP Session Border Controller functionality in our Firewall/SIParator. This combination makes it possible to detect certain attacks that neither the IDS/IPS nor the stateful firewall can catch on their own. DPI can be effective against buffer overflow attacks, denial of service (DoS) attacks, sophisticated intrusions, and a small percentage of worms that fit within a single packet.

The IDS/IPS in the Enhanced Security Module enables the Ingate Firewall/SIParator to detect DoS attacks based on the SIP protocol, and to block malicious SIP signaling packets designed to attack certain SIP phones, servers or other devices on the enterprise

LAN. This secures the enterprise network as the edge device – the Firewall or the SIParator – handles the attacks while the servers and other SIP devices in the network can still be used.

For DoS attack detection, the administrator specifies what should be regarded as an attack. This offers the administrator flexibility to set the criteria for the number of requests/responses per time frame as environments and functions vary, and must thus be defined individually. The rules may also be written to limit requests/responses from specific IP addresses or domains within a time period, or to block all requests/responses from an IP address or domain if the administrator determines that the attack is being launched from that site. All logs can be exported for analysis and, based on the findings; the administrator can refine the rules to minimize attacks and intrusions, while also allowing normal communications to continue.

Ingate's Enhanced Security Module can also protect the network against malicious SIP packet attacks: attacks where the SIP packets look correct, but a combination of headers can make a SIP phone or server reboot (or become temporarily unusable). For these intrusion scenarios, Ingate provides rule packs to upload to the Firewall/SIParator. Ingate will provide rule packs for the detection of known attacks as reported by industry watch groups, or by customers. These rule packs may then be installed on the Ingate Firewall/SIParator, so that if there is an attack launched against the customer's network, the Ingate products can detect and block that SIP packets instead of forwarding it to the SIP client, protecting the SIP client from being compromised. The same rule packs can be applied to monitor outbound traffic to detect if the network has been compromised and the malicious packets are being added to outbound headers. In this case the transmissions will be blocked to avoid delivering the packets to other networks and the administrator will be alerted so that steps can be taken to eliminate the problem.

A SIP packet can be redirected, marked/tagged (see Ingate's Quality of Service Module), blocked, rate limited, and of course reported to a reporting agent in the network. In this way, SIP errors of different classifications may be identified and forwarded for analysis. The Ingate SIParator/Firewall can identify packet flows (rather than packet-by-packet analysis), allowing control actions based on accumulated flow information.

2.2.5 Network Security: NAT and PAT Rules

The Ingate SIParator/Firewall natively provides Network Address Translation (NAT) as well as Port Address Translation (PAT), which is essential to any security solution. NAT is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. PAT is a feature of a network device that translates TCP or UDP communications made between hosts on a private network and hosts on a public network. It allows a single public IP address to be used by many hosts on a private network, which is usually a Local Area Network (LAN).

The Ingate SIParator/Firewall can provide multi-network security control. Not just security from the Internet, but security between Foreign and "Untrusted Networks". The Ingate with multiple interfaces can connect to and provide security on multiple networks allowing for a secure solution for connecting networks as well as SIP communications all in one package.

3 Summary

SIP Trunking solutions are quickly being adopted by enterprises worldwide as the communications method of choice. It is cost efficient, as VoIP and especially SIP trunks can save businesses significant communications costs. Even though the VoIP traffic (as other data traffic) is sent over the public Internet, your network and the communication must still be secured against attacks from hackers and eavesdroppers. Ingate's SIP architecture grants fully secure traversal of the SIP traffic over NAT. The ports for the media streams are only opened between the specific parties of a call and only for the duration of the call. The SIP proxy inspects the SIP packets before sending them on.

Ingate has proven interoperability with several leading ITSP vendors. It is designed to be the demarcation point of the enterprise network and to work seamlessly in conjunction with IP-PBX installed on the enterprise LAN to allow for the IP-PBX to be connected to an ITSP. Ingate provides a range of features to integrate into any SIP trunking deployment, overcoming obstacles and difference between vendors due to vendors' interpretation of the open standard, thus creating inconsistencies between the implementations.

The IDS/IPS in the Enhanced Security Module enables the Ingate Firewall/SIParator to detect DoS attacks based on the SIP protocol, and to block malicious SIP signaling packets designed to attack certain SIP phones, servers or other devices on the enterprise LAN. This secures the enterprise network as the edge device – the Firewall or the SIParator – handles the attacks while the servers and other SIP devices in the network can still be used. TLS and SRTP encryption ensures privacy, making call eavesdropping, call hijacking and call spoofing harder to do.

For enterprises wanting to make full use of their installed IP-PBX and provide a secure network and SIP communications solution, the Ingate offers an easy and smooth transition to a modern, future-proofed, security focused SIP solution.