Ingate Firewall & SIParator
Product Training

SIP Trunking Focused
Common SIP Applications

SIP Trunking
Remote Desktop
Ingate Product Training
Common SIP Applications

- **SIP Trunking**
  - A SIP Trunk is a concurrent call that is routed over the IP backbone of a carrier (ITSP) using VoIP technology.
  - SIP Trunks are used in conjunction with an IP-PBX and are thought of as replacements for traditional PRI or analog circuits.
  - The popularity of SIP Trunks is due primarily to the cost savings; due to a true convergence of voice and data infrastructure, Increased ROI, the maximizing of bandwidth utilization, open source protocol standards, and more.
Ingate Product Training

Common SIP Applications

DNS Server:
Entry: ip-pbx.ingate.com
Resolves to: Public IP of Ingate
Entry: isp.serviceprovider.com
Resolves to: Public IP of ITSP

Ingate:
Public IP Address (or)
Domain: ip-pbx.ingate.com
Relay to: Private IP of IP-PBX

ITSP: ITSP IP Address or Domain

POTS

PSTN

Internet

LAN

IP-PBX

SIP Domain:
Domain: ip-pbx.ingate.com
VoIP Trunk: Relay to Phone or Application
Remote Desktop
- Extending SIP communications to Remote & Home Offices.
- Extension of IP-PBX services using Open Source standardized Protocol
- Use of off-the-self SIP Phones and Soft SIP Clients.
Ingate Product Training
Common SIP Applications

DNS Server:
Entry: ip-pbx.ingate.com
Resolves to: Public IP of Ingate

DNS Override for SIP Requests:
Domain: ip-pbx.ingate.com
Relay to: Private IP of Asterisk

SIP Phone:
Username: Extension Number
SIP Server: ip-pbx.ingate.com

SIP Domain:
Domain: ip-pbx.ingate.com
Common SIP Deployment Issues
Ingate Product Training
Common Deployment Issues

- **Problem #1 - “NAT BREAKS SIP”**
  - SIP Protocol is an Application Layer Protocol
  - Network Address Translation (NAT) resides at the Transport Layer (TCP/IP)
  - NAT will not change the SIP addressing within the TCP/UDP datagram
  - Firewalls are a NATing device and BLOCK all Incoming SIP Traffic to the LAN
  - Any NAT device, either Far End (remote) or Near End (on prem) can effect the call

```
TCP/UDP Layer Address: 10.0.0.12
....
INVITE
....
Contact: 10.0.0.12
....
C=IN IP4 10.0.0.12
....
m=audio 54054
```

```
TCP/UDP Layer Address: 147.10.7.1
....
INVITE
....
Contact: 10.0.0.12
....
C=IN IP4 10.0.0.12
....
m=audio 54054
```
Ingate Product Training

Common Deployment Issues

- Before NAT
  - TCP/IP Header is Private Space
  - SIP Headers are Private Space

```
| Internet Protocol, Sr: 10.51.77.60 | Dst: 10.51.77.1 |
| User Datagram Protocol, Src Port: sip (5060) | Dst Port: sip (5060) |
| Session Initiation Protocol |
| Request-Line: INVITE sip:161396309@10.51.77.1 P/2 0 |
| Message Header |
| Via: SIP/2.0/UDP 10.51.77.60:5060; rport; branch=z9hG4bKeds59a3 |
| From: "Scott Beer" <sip:6139630933@10.51.77.1; tag=4840eda-186-6c1b36c8 |
| To: <sip:16139630933@10.51.77.1> |
| Contact: "Scott Beer" <sip:6139630933@10.51.77.60:5060; transport=UDP> |
| Call-ID: eda0000-2da0a10101.51.77.1 |
| CSeq: 701887483 INVITE |
| User-Agent: Mitel-5340-SIP-Phone Fw.07.41.02 08000F314048 |
| Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, REFER, NOTIFY, PACT, UPDATE |
| Allow-Events: talk, hold, conference |
| Supported: timer,100rel, replaces |
| Session-Expires: 1800 |
| Max-Forwards: 70 |
| Content-Type: application/sdp |
| Content-Length: 249 |
| Message Body |
| Session Description Protocol |
| Session Description Protocol Version (v): 0 |
| Owner/Creator, Session Id (o): 6139630933 1213010017 1213010016 IN IP4 10.51.77.60 |
| Session Name (s): SIP Call |
| Connection Information (c): IN 10.51.77.60 |
| Time Description, active time (t): 0 0 |
| Session Attribute (a): sendrecv |
| Media Description, name and address (m): audio 20282 RTP/AVP 0 8 18 101 |
```
Ingate Product Training

Common Deployment Issues

- **After NAT**
  - TCP/IP Header is Public Space
  - SIP Headers are Private Space

```plaintext
Internet Protocol 207.112.18.164 (207.112.18.164), 9.249.3.59 (209.249.3.59)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
  - Request-Line: INVITE sip:161396309@10.51.77.1 P/2 0
  - Message Header
    - Via:SIP/2.0/UDP 10.51.77.60:5060; rport; branch=z9HG4bKeda59e8
    - From:"Scott Beer" <sip:6139630933010.51.77.1>; tag=484d0eda-186-6c1b36c8
    - To:<sip:16139630933@10.51.77.1>
    - Contact:"Scott Beer" <sip:6139630910.51.77.60:transport=UDP>
      Call-ID:eda0000-2da6d41010.51.77.1
    - CSeq:701887483 INVITE
      User-Agent:M1tel-5340-SIP-Phone FW.07.41.02 08000F314048
      Allow:INVITE,ACK,CANCEL,BYE,OPTIONS,REFER,NOTIFY,PRACK,UPDATE
      Allow-Events: talk, hold, conference
      Supported:timer,100rel, replaces
      Session-Expires: 1800
      Max-Forwards: 70
      Content-Type:application/sdp
      Content-Length: 249
  - Message Body
    - Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): 6139630933 1213010017 1213010016 IN IP4 10.51.77.60
      Session Name (s): SIP Call
      Connection Information (c): IN 10.51.77.60
      Time Description, active time (tj): u u
      Session Attribute (a): sendrecv
      Media Description, name and address (m): audio 20282 RTP/AVP 0 8 18 101
```
Resolution #1  - “NAT BREAKS SIP”

- SIP Protocol requires a SIP Proxy or Application Layer Gateway and NAT
- SIP Proxy (SIP-Aware Firewall) will correct IP Addresses and Port allocation in SIP Protocol from Private LAN addresses to Public WAN address.
- SIP Proxy monitors all SIP Traffic IN and OUT and can apply routing rules
Ingate Product Training

Common Deployment Issues

- After NAT & Ingate
  - TCP/IP Header is Public Space
  - SIP Headers are Private Space

<table>
<thead>
<tr>
<th>Internet Protocol</th>
<th>207.112.18.164 (207.112.18.164), 9.249.3.59 (209.249.3.59)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)</td>
<td></td>
</tr>
<tr>
<td>Session Initiation Protocol</td>
<td></td>
</tr>
<tr>
<td>Request-Line: INVITE sip:161396305209.249.3.59/2.0</td>
<td></td>
</tr>
<tr>
<td>Message Header</td>
<td></td>
</tr>
<tr>
<td>Via: SIP/2.0/UDP 207.112.18.164:5060;branch=z9hG4bkb42dfb3914946b8801d52bd5732dc849.0</td>
<td></td>
</tr>
<tr>
<td>Session-Expires: 14400</td>
<td></td>
</tr>
<tr>
<td>Via: SIP/2.0/UDP 207.112.18.164:5060;branch=z9hG4bk793e9c7e80e6185d673ce730c431ec1e.oshxzb9x7Bb3o-novQajpa__</td>
<td></td>
</tr>
<tr>
<td>To: <a href="">sip:16139630933@209.249.3.59</a></td>
<td></td>
</tr>
<tr>
<td>From: <a href="">sip:603764384@209.249.3.59</a>;tag=62b412e7</td>
<td></td>
</tr>
<tr>
<td>Call-ID: 30a1d9e8-484d471bd3fc8-2e238874@sipgt-46d4aeFa</td>
<td></td>
</tr>
<tr>
<td>CSeq: 1297043244 INVITE</td>
<td></td>
</tr>
<tr>
<td>Contact: &lt;sip:eSNg2VOMneyw5xKdKvXfP27no1z_TLY5Yx_i_JTyGvDcqx80_w4C25fKksdpE207.112.18.164</td>
<td></td>
</tr>
<tr>
<td>Supported: timer, replaces</td>
<td></td>
</tr>
<tr>
<td>Allow-Events: talk,hold,conference</td>
<td></td>
</tr>
<tr>
<td>Min-SE: 90</td>
<td></td>
</tr>
<tr>
<td>Max-Forwards: 68</td>
<td></td>
</tr>
<tr>
<td>Content-Type: application/sdp</td>
<td></td>
</tr>
<tr>
<td>Content-Length: 249</td>
<td></td>
</tr>
<tr>
<td>Record-Route: <a href="">sip:97a2b0734e1769@207.112.18.164;lr</a></td>
<td></td>
</tr>
</tbody>
</table>

- Session Description Protocol
  - Session Description Protocol Version (v): 0
  - Owner/Creator, Session Id (o): 6139630933 1213C10017 1552 IN IP4 207.112.18.164
  - Session Name (s): SIP Call
  - Connection Information (c): IN 207.112.18.164
  - Time Description, active time (u): u u
  - Session Attribute (a): sendrecv
  - Media Description, name and address (m): audio 58534 RTP/AVP 0 8 18 101
**Ingate Product Training**

**Common Deployment Issues**

- **Ingate Benefits - “NAT BREAKS SIP”**
  - Ingate products are ICSA Certified VoIP Firewalls
  - Ingate have a SIP Proxy, SIP B2BUA and NAT working together
  - Ingate SIParator can bring enhance the SIP capabilities and SIP security of an existing Firewall
  - Ingate can provide “Far End NAT Traversal” functionality

- **What Other IP-PBXs Vendors Do**
  - Most all IP-PBX vendors recommend the use of some sort of “SIP-Aware Firewall” for deployment
  - Other recommend the use of Port Forwarding, to forward Port 5060 and a thousand other Ports to the IP-PBX – **HUGE SECURITY RISK!!**
Problem #2 – SIP Interoperability

- Not all SIP is the same
  - One vendor’s implementation may not be the same as another
  - There are many SIP components and extensions that may be supported on one vendor’s equipment and not on another
  - SIP Protocol is an open standard and can be left to interpretation by each vendor

Examples

- Use of REFER Method is not typically supported by ITSP
- Use of INVITE with Replaces Header is not typically supported by ITSP
- Some ITSPs don’t like SDP with “a=Inactive” attribute
- ENUM SIP URI Delivery is supported by some and not by others
- Various TO and FROM Header conformances
- Alternate SIP Domain routing requirements
Resolution #2 – SIP Interoperability

- Testing and Development for each Vendor
  - Extensive Testing and Development time devoted to each vendor integration to ensure complete interoperability – a huge undertaking
  - Customization and Flexibility development for each Vendor integration

SIP Connect Compliance

- Adherence to SIP Forum – SIP Connect Compliance, governing body of SIP Trunking deployments an standards
Ingate Product Training

Common Deployment Issues

**Ingate Benefits – SIP Interoperability**

- In General,
  - Can rewrite headers commonly needing changed between vendors
  - Provide SIP Protocol error checking and fixes Protocol non-conformances
  - Routing Rules and Policies to direct traffic
  - Contains extensive list of features devoted to SIP non-conformances customization

- Ingate contains a B2BUA
  - Separates the call between the two parties, helping separate two different implementations of SIP
  - Provides Client or Server User Accounts for Registration and Authentication
  - Separate SIP Method Handling between two parties
Problem #3 – SIP Security

- SIP is written in clear text within the datagram of a UDP or TCP Transport.
- Confidential User/SIP URI Information
  - A SIP URI is like an Email Address, once someone has it, they who you are and where you are located.
  - The malicious person or software can send SIP Request after SIP Request to your SIP URI. Some malicious uses like DoS Attacks, SPIT Attacks, Intrusion of Services, Toll Fraud, Tele-markers and more.
- Called and Calling Party Number Information
- Private LAN Network Address Scheme
  - Giving away the confidential Private IP Address scheme of the internal LAN network, gives malicious attackers knowledge of the internal configuration of the Enterprise.
  - The Port being used on the device, gives malicious attackers where to direct traffic
- Media Attributes
  - Easy to see what Media is being negotiated and where its going
Why is SIP Insecure?

- Written in clear text within the datagram of a UDP or TCP Transport.
- Internet Protocol: 207.112.18.164 (207.112.18.164), 9.249.3.59 (209.249.3.59)
- User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol
  - Request-Line: INVITE sip:613963093@10.51.77.1 p/2.0
  - Message Header
    - Via: SIP/2.0/UDP 10.51.77.60:5060;branch=z9hG4bK9da59e3
    - From: "Scott Beer" <sip:613963093@10.51.77.1>;tag=8430eda-186-6c1b36c8
    - To: <sip:613963093@10.51.77.1>
    - Contact: "Scott Beer" <sip:613963093@10.51.77.60;transport=UDP>
    - Call-ID:eda0000-2da6d41010.51.77.1
    - CSeq:701887483 INVITE
      - User-Agent:Mitel-5340-SIP-Phone FW.07.41.02 0800E314048
      - Allow:INVITE,ACK,CANCEL,BYE,OPTIONS,REFER,NOTIFY,PRACK,UPDATE
      - Allow-Events:talk,hold,conference
      - Supported:timer,100rel,replaces
      - Session-Expires: 1800
      - Max-Forwards: 70
      - Content-Type:application/sdp
      - Content-Length: 249
  - Message Body
  - Session Description Protocol
    - Session Description Protocol Version (v): 0
    - Owner/Creator, Session Id (n): 6139630933 1213010017 1213010016 IN IP4 10.51.77.60
    - Session Name (s): SIP Call
    - Connection Information (c): IN :10.51.77.60
    - Time Description, active time (t): u v
      - Session Attribute (a): sendrecv
    - Media Description, name and address (m): auid:20282 TP/AVP 0 8 18 101

Confidential User Information
Confidential SIP URI of the User
Confidential Equipment
MIME Content
LAN IP Address and Port Information
Media Attributes
Common Deployment Issues

- **Common SIP Attacks**
  - Intrusion of Services
    - Devices attempting Register with a IP-PBX in an attempt to look like an IP-PBX extension and gain IP-PBX services
    - SPIT (SPAM over Internet Telephony)
  - Toll Fraud
    - A form of an Intrusion of Service, where malicious attempts to send INVITEs to an IP-PBX to gain access to PSTN Gateways and SIP Trunking to call the PSTN
  - Denial of Service
    - INVITE (or any SIP Request) Flood in an attempt to slow services or disrupt services
    - Or any UDP or TCP traffic directed at a SIP Service on SIP Ports
  - Indirect Security Breaches
    - Private LAN IP Address and infrastructure are now made public, and can be used in attacks to other non-SIP areas
Ingate Product Training
Common Deployment Issues

- **Resolution #3 – SIP Security**
  - Dynamic Encryption of SIP URI
    - Using the SIP Specification, enforce an Encrypted SIP URI where possible
  - Dynamic Port Allocation
    - Dynamically change ports on every call.
  - Hide LAN IP Address Scheme
    - Apply LAN to WAN Network Address Translation within the SIP Signaling
  - TLS and SRTP
    - TLS Transport provides complete encryption of SIP Signaling
    - SRTP provides encryption of RTP Media
  - IDS/IPS for SIP Protocol
    - SIP Protocol specific Intrusion Detection Systems and Intrusion Prevention Systems allow for monitoring and statistics of all SIP Traffic, and apply rules and policies based on the traffic
  - Traffic Routing Rules and Policies
    - IP Address Authentication, SIP URI Validation, and Routing Rules
Ingate Product Training
Common Deployment Issues

How to make SIP Secure

- Internet Protocol, src: 207.112.18.164:20712.18.164, dest: 216.82.223.202:216.82.223.202
- User Datagram Protocol, src: sip: (5060), dest: sip: (5060)
- Session Initiation Protocol

| Request-Line: INVITE sip:+1613963093@216.82.223.202 SIP/2.0 |
| Message-Header |
| Via: SIP/2.0/UDP 207.112.18.164:5060;branch=z9hG4bKd0U2Ic8359d9da67625a8c701c6b3F.0 |
| Session-Expires: 14400 |
| Via: SIP/2.0/UDP 207.112.18.164:5060;branch=z9hG4bKd0U2Ic8359d9da67625a8c701c6b3F.0 |
| To: <sip:+1613963093@216.82.223.202> |
| From: "SCOTT Beer" <sip:613963093@216.82.223.202;f=pcap> |
| Call-ID: 7f07a057-48b06d74727e-a13d36b0@216.82.223.202 |
| CSeq: 15665158 INVITE |
| User-Agent: Ingate-Firewall/1.6.2 |
| Contact: <sip:Eaweid3Eu13c2Vw1uoqG@207.112.18.164> |

- Hidden IP in User Information
- Hidden Internal Vendor
- Encrypted SIP URI
- Firewall Filters on MIME Content
- Hidden LAN IP Information
- Dynamic Port Allocation
- SRTP to Encrypt all RTP Media
- TLS to Encrypt all SIP Signaling
Ingate Product Training
Common Deployment Issues

- Ingate Benefits – SIP Security
  - Dynamic Encryption of SIP URI
  - Dynamic Port Allocation
  - Hide LAN IP Address Scheme
  - TLS and SRTP
  - IDS/IPS for SIP Protocol
  - Traffic Routing Rules and Policies

- Ingate products are ICSA Certified VoIP Firewall
- Ingate is focused on providing SIP Security
Introduction to Ingate Products
Ingate products

**Firewalls**

SIP-capable firewalls for computer security and communication

- New and replacement installations

**SIParator™**

SIParator™ - Add-on to existing firewalls to enable SIP communication

- Preserve firewall investment and keep established security policies
Extensive SIP Feature Set

- Encryption
- Authentication
- SIP Filtering
- Near-End Traversal
- Flexible Control
- SIP Proxy, ALG, B2BUA, Registrar
- Service Provider Compatibility
- ENUM Support
- QoS, Traffic Mgmt
- SIP Trunking
- SIP Trunking Tool Set
- Far-End NAT Traversal and STUN
- Sol. for Remote Workers
- SIP-ALG-only Firewalls can only do this much
The Ingate Product Family

- **Firewall® 1950 or SIParator® 95**
  - 1,800 Calls*
  - Better Capacity
  - Additional SIP Traversals

- **Firewall® 1650 or SIParator® 65**
  - 650 Calls*
  - Better Quality of Service
  - Enhanced Security

- **Firewall® 1550 or SIParator® 55**
  - 350 Calls*
  - Remote SIP Connectivity
  - VoIP Survival

- **Firewall® 1500 or SIParator® 50**
  - 300 Calls*
  - SIP Trunking
  - Enhanced Security

- **Firewall® 1190 or SIParator® 19**
  - 150 Calls*
  - Remote SIP Connectivity
  - VoIP Survival

Licenses

- Functional
  - SIP Trunking
  - Remote SIP Connectivity
  - Quality of Service
  - Advanced SIP Routing
  - VoIP Survival
  - Enhanced Security

- Capacity
  - Additional SIP Traversals

* Calls = Maximum Concurrent RTP Sessions = SIP Trunks
Connecting the Firewall

- Ingate Firewall
  - Handles All Data Traffic
  - Provides NAT
  - Protocol Service Rules
  - Data Traffic Relays
  - VPN (IPsec) Tunnels
  - PPTP Tunnels
  - DMZ Networks (multiple networks)
  - Default Gateway of the LAN
  - DHCP Server
  - SIP Session Border Controller
Connecting the Firewall

Network Address Translation (NAT)

Internet

Directly Connected Network

Default GW: 51.51.51.1

51.51.51.0/24

InGate IP: 51.51.51.254

10.51.77.1

10.51.77.0/24

Directly Connected Network

Firewall Two LAN Networks

Internet

Directly Connected Network

Default GW: 51.51.51.1

51.51.51.0/24

InGate IP: 51.51.51.254

10.51.77.1

10.51.77.0/24

Directly Connected Network

InGate IP: 10.51.10.1

10.51.10.0/24

Directly Connected Network

InGate IP: 10.51.77.1

10.51.77.0/24

Directly Connected Network
Connecting the Firewall

DMZ Networks

- Internet
- Default GW: 51.51.51.1
- Ingate IP: 10.51.10.1
- Directly Connected Network: 51.51.51.0/24
- LAN: 10.51.77.0/24
- Public or Private Network Address DMZ Networks

VLAN – Voice & Data Networks

- Internet
- Default GW: 51.51.51.1
- Ingate IP: 10.51.77.1
- Directly Connected Network
- Ingate IP: 10.51.10.1
- 10.51.77.0/24
- 10.51.10.0/24
- VLAN ID: 10
- Directly Connected Network
Connecting the Firewall
Connecting the Firewall

Firewall to other Routed Networks

Everything to do with SIP

Internet

Default GW: 51.51.51.1

InGate

InGate IP: 51.51.51.254

Routed Network

Router: 10.51.77.254

Directly Connected Network

Internet

Default GW: 51.51.51.1

InGate

InGate IP: 51.51.51.254

Routed Network

Router: 10.51.77.254

Directly Connected Network

Remote SIP Users

Remote Office

Road Warriors

ITSP

Hosted SIP Users

SIP Trunking

Hosted Service Provider

Everything SIP
Connecting the SIParator®

- Existing Firewall
  - Port Forward 5060
  - Port Forward Media Port range
Connecting the SIParator®

- NAT FW needs to Port FWD from Internet to DMZ and again from DMZ to LAN
- Increases number of Network hops
- Very Secure
- Ingate needs to know WAN IP address
Connecting the SIParator®

- NAT FW needs to Port FWD from Internet to DMZ
- Decreases Network hops
- Very Secure
- Ingate needs to know WAN IP address
Connecting the SIParator®

- NAT FW needs to Port FWD from Internet to LAN
- Decreases Network hops
- Least Secure
- Ingate needs to know WAN IP address
Connecting the SIParator®

- Ingate has its own Public IP address
- One Network hop
- Very Secure
- Reduces impact to NAT FW
- No NAT FW setup required
Connecting the SIParator®

- Ingate has its own Public IP address
- NAT FW has its own IP address
- Ingate adds QoS and Traffic Shaping
- Very Secure
- No NAT FW setup required
How Does It Work?

- **SIP Proxy**
  - Stateful Proxy redirects calls
  - NAT/PAT for UDP/TCP/TLS and SIP
- **SIP B2BUA**
  - Rewrites Request URIs, Domains, and other Headers
- **SIP Registrar / Client**
  - Can Register to ISTP, and provide a Registrar for SIP Clients
- **SIP Media Relay**
  - Can ensure media is directed in/out
  - Dynamically open and close ports for security
Ingate SIParator®

IngateSIParator™

LAN
Private IP Addresses

EXISTING FIREWALL

Internet
RTP traffic (UDP port interval)
SIP traffic (5060 UDP/TCP)

RTP Proxy
NAT/PAT Engine

SIP Proxy
SIP Registrar
Optional Modules

- The SIP functionality in Ingate Firewalls and SIParators has several software extension modules.
  - Remote SIP Connectivity
  - SIP Trunking
  - Advanced SIP Routing
  - VoIP Survival
  - Extended SIP Security
  - Quality of Service
Optional Modules

Remote SIP Connectivity

- Manages SIP clients behind NAT boxes which are not SIP-aware
- Solves far-end NAT traversal
- Includes a STUN server
Optional Modules

Remote SIP Connectivity
Far End NAT Traversal (FENT)

- All SIP addressing is in Home LAN Address space
- Not routable over Internet

- All SIP addressing is corrected and points back to Ingate IP
- Ingate changes behavior with far end SIP Client
- Works with FENT to ensure Media and SIP signaling back to SIP Client
Optional Modules

SIP Trunking

- Lets the administrator rewrite the entire or part of a SIP URI before the request is passed on
- Redirects requests based on From header, Request-URI and originating network
- Adding features to make the firewall register on behalf of clients
  - Local Registrar, B2BUA, Proxy, extensive Dial Plan & Routing features.
Optional Modules

SIP Trunking

- TDM Trunk replacement (T1, PRI, etc)
- Service Provider for DID
- IP-PBX to IP-PBX connectivity

- N+1 IP-PBX to N+1 ITSP call flow management
- Complete SIP SBC for the Enterprise
- SIP Proxy, B2BUA, Dial Plan, Routing, Registrar and more
- Normalizes SIP Traffic between all endpoints.
Optional Modules

VoIP Survival

- Monitors one or more remote SIP servers
- Useful for branch offices which uses a SIP server at the main office
- When the remote SIP server is down, the firewall:
  - Acts as registrar for the monitored SIP domain
  - Manages local calls
  - Redirects PSTN calls to a local PSTN gateway
  - Manages outgoing calls to other SIP domains
Optional Modules

Extended SIP Security

- Contains features such as:
  - **IDS/IPS**
    - Makes it possible to block SIP traffic due to various conditions
      - Traffic exceeds a given rate limit
      - Packets match specified criteria
  - **TLS and SRTP**

Advanced SIP Routing

- Create hunt groups, aliases and other user-based features
Break – 10 minutes
Ingate Startup Tool
Ingate Startup Tool

Startup Tool

- “Out of the Box” setup and commissioning of the Firewall and SIParator products
- Update current configuration
- Product Registration and unit Upgrades, including Software and Licenses.
- Automatic selection of ITSP and IP-PBX
- Backup of Startup Tool database
- Located at www.ingate.com FREE!
Ingate Startup Tool

Startup Tool - Product Type

- Select the Ingate Model
Ingate Startup Tool

Startup Tool Title Reference

- Configure the unit for the first time
- Change or update configuration
- Register the unit
- Backup the config

- IP/MAC Address
- Password
Ingate Startup Tool

**Startup Tool - Network Topology**

- Firewall or SIParator deployment type
- Inside (Eth0) - Private
- Outside (Eth1) - Public
- Default Gateway
- DNS Server
Ingate Startup Tool

Startup Tool – IP-PBX

- Select IP-PBX
- Provide IP Address
Ingate Startup Tool

Startup Tool – ITSP_1

- Select Trunking Provider
- Account Information
Ingate Startup Tool

Startup Tool – Upload Config

- Login to web GUI and apply settings
- Upload
Ingate Startup Tool

Startup Tool – Apply the Config

- The Startup Tool will launch a browser to have the installer apply the Configuration.
Ingate Startup Tool

Startup Tool – Register & Upgrade

- Enter Ingate Web Account
- Create Ingate Web Account
- Connect to www.ingate.com
- Install Modules & Licenses by entering 12-digit Purchase Key
- Upgrade the software of the unit
Exercise #1
Startup Tool
Exercise #1

Training Station #1

Ingate IP: 10.10.10.11
IP-PBX to Ingate
INVITE: 6135552222@10.10.10.11

Ingate IP: 12.34.56.11
Ingate to IP-PBX
INVITE: 6135551111@10.10.10.10

Ingate IP: 12.34.56.22
ITSP to Ingate Emulation
INVITE: 6135552222@12.34.56.22

Training Station #2

Ingate IP: 10.20.20.22
Ingate to IP-PBX
INVITE: 6135552222@10.20.20.20

Ingate to IP-PBX
INVITE: 6135551111@12.34.56.11

ITSP to Ingate Emulation
INVITE: 6135551111@10.20.20.22

IP-PBX to Ingate
INVITE: 6135551111@10.20.20.22
Break - Lunch
Recap

Ingate Products

- Ingate Firewall and Ingate SIParator
- Scale by appliance giving more traversals
- Number of purchasable Options Modules

Deployments

- Ingate Firewall and Ingate SIParator

Startup Tool

- “Out of the Box” setup and commissioning
- Select IP-PBX and ITSP
Programming GUI
Programming GUI

Web Configuration

- Web into the Ingate
- Major Categories and separate Tabs

### Networks and Computers

<table>
<thead>
<tr>
<th>Name</th>
<th>Subgroup</th>
<th>Lower Limit</th>
<th>Upper Limit (for IP ranges)</th>
<th>Interface/VLAN</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ ITSP_IP</td>
<td>-</td>
<td>DNS Name or IP Address: 0.0.0.0</td>
<td>IP Address: 0.0.0.0</td>
<td>DNS Name or IP Address: 255.255.255.255</td>
<td>IP Address: 255.255.255.255</td>
</tr>
<tr>
<td>+ LAN</td>
<td>-</td>
<td>DNS Name or IP Address: 10.51.77.0</td>
<td>IP Address: 10.51.77.0</td>
<td>DNS Name or IP Address: 10.51.77.255</td>
<td>IP Address: 10.51.77.255</td>
</tr>
<tr>
<td>+ PBX</td>
<td>-</td>
<td>DNS Name or IP Address: 10.51.77.20</td>
<td>IP Address: 10.51.77.20</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>+ WAN</td>
<td>-</td>
<td>DNS Name or IP Address: 0.0.0.0</td>
<td>IP Address: 0.0.0.0</td>
<td>DNS Name or IP Address: 127.0.0.0</td>
<td>IP Address: 127.0.0.0</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>DNS Name or IP Address: 127.0.0.2</td>
<td>IP Address: 127.0.0.2</td>
<td>DNS Name or IP Address: 255.255.255.255</td>
<td>IP Address: 255.255.255.255</td>
</tr>
</tbody>
</table>
Programming: Network
Programming: Network

Networks & Computers

- Provides a view of the Network connected on each interface as a Routing Table.
Programming: Network

Default Gateway

- The Default Gateway to the Internet, provided by the ISP.
Programming: Network

Eth0 Network Interface

- The IP Address/Mask of the NIC on the LAN.

- Static Routing – defines Router address for other network address on the LAN.
Programming: Network

Eth1 Network Interface

- The IP Address/Mask of the NIC on the WAN.

- PPPoE or DHCP IP address assignment are possible.
Programming: Basic Configuration
Programming: Basic Configuration

Basic Configuration

- Provides DNS Server addresses.

<table>
<thead>
<tr>
<th>No.</th>
<th>DNS Name or IP Address</th>
<th>IP Address</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>216.254.141.13</td>
<td>216.254.141.13</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>209.90.160.220</td>
<td>209.90.160.220</td>
<td></td>
</tr>
</tbody>
</table>
Programming: Basic Configuration

Access Control

- Provides configuration for HTTP and HTTPS access.
Programming: NAT & Rules and Relays

Firewall Only
Programming: NAT

NAT

- Define when to apply NAT rules. Typically, From LAN network to WAN network, NAT as WAN address.
Programming: Rules & Relays

Rules

- Define specific Service from Client to Server networks.
Programming: Rules & Relays

Relays

- Direct specific Traffic to specific locations

<table>
<thead>
<tr>
<th>Listen To ...</th>
<th>Relay To ...</th>
<th>Relay Type</th>
<th>Allow Access From ...</th>
<th>Certificate for TLS/SSL</th>
<th>Time Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>DNS Name or IP Address</td>
<td>IP Address</td>
<td>Port</td>
<td>Network</td>
<td>IPsec Peer</td>
</tr>
<tr>
<td>outside (eth1)</td>
<td>80</td>
<td>10.51.77.58</td>
<td>10.51.77.58</td>
<td>WAN</td>
<td>-</td>
</tr>
</tbody>
</table>
Programming: Quality of Service

Firewall Only
Programming: QoS

Quality of Service – Call Admission Control

- You can make the firewall reject SIP calls when there is not bandwidth enough left to get media streams through satisfactorily.

- Bandwidth for SIP Media - define BW Reservations

- Codec Bandwidth – define Codec BW
Programming: QoS

Quality of Service – QoS Classes

- Using Priority queues, you assign different priority to different types of traffic.
- Using Bandwidth allocation, you assign guaranteed bandwidth and bandwidth limits for different types of traffic.
Quality of Service – Most Restricted Interface

- You specify how packets belonging to different classes should be handled by the interface.
- The Priority field specifies in which priority queue to put the packets. Higher priority traffic will always be let through before lower priority traffic is allowed (but see also the Loose Priority setting).
Programming: QoS

Quality of Service – ToS Modification

- Modify the TOS octet of packets leaving the firewall. You can either specify a value for the (3 bit) TOS field (RFC 791), or you can specify a value for the (6 bit) Differentiated Services field (RFC 2474).
Programming: SIP Services
Programming: SIP Services

**Basic**

- Turn On SIP Module.
- Define Media Port Range.
Interoperability

- Common deviations from the standard
Programming: SIP Services

Remote SIP Connectivity

- Allows SIP client behind NAT boxes to use SIP.
Programming: SIP Traffic
Programming: SIP Traffic

SIP Methods

- Select which SIP methods the firewall should allow & authenticate
Filtering

- The **Proxy Rules and Default Policy For SIP Requests** settings control if sipfw should process requests, based on the sender IP address of the request.

- The **Content Type** table controls if sipfw should process requests, based on the content type of the request body.

  - `*/*` - Allows All
Programming: SIP Traffic

Local Registrar

- Define SIP Users that register to the Ingate (server registrar)
Programming: SIP Traffic

SIP Accounts

- Define SIP Users for Service Providers
- Select behavior of these SIP Users (Ingate as client)

### Registration Parameters

- Registration interval: 3600 seconds
- Retry registration after: 300 seconds

### SIP Accounts

<table>
<thead>
<tr>
<th>Username</th>
<th>Domain</th>
<th>Authentication Name</th>
<th>Display Name</th>
<th>P-Asserted-Identity</th>
<th>Password</th>
<th>Account Type</th>
<th>Delete Row</th>
</tr>
</thead>
<tbody>
<tr>
<td>6033240113</td>
<td>proxy1.bandtel</td>
<td>2036400002</td>
<td></td>
<td></td>
<td>Change Password</td>
<td>XF</td>
<td></td>
</tr>
<tr>
<td>6033240113</td>
<td>proxy2.bandtel</td>
<td>2036400002</td>
<td></td>
<td></td>
<td>Change Password</td>
<td>XF</td>
<td></td>
</tr>
<tr>
<td>2075800001</td>
<td>registrar.bandtel</td>
<td>2036400002</td>
<td></td>
<td></td>
<td>Change Password</td>
<td>XF/Register</td>
<td></td>
</tr>
</tbody>
</table>
Programming: SIP Traffic

User Database: Account Type Selections

- **Register:** With this Account type, the firewall registers the username with the SIP server associated with the domain. You may enter the address to send the request to in the User Routing table. This is useful when you have a SIP client which cannot register properly.

- **XF:** With this Account type, the firewall replaces the From header with the username and domain of this user. The request is then forwarded to the SIP server associated with the domain.

- **XF/Register:** With this Account type, the firewall replaces the From header as described above, then registers as described under Register above.
User Database: Account Type Selections

- **Domain:** This Account type can be used when sending requests to other domains where authentication is required. You must select this account in the Dial Plan when you forward requests to the domain in question. When that server requires authentication for its domain, the firewall sends the username and password configured here.

- **B2BUAWM:** With this Account type, the firewall replaces the From header as described under XF. It also changes the SDPs to the effect that media is always sent via the firewall.

- **B2BUAWM/Register:** With this Account type, the firewall acts as described under B2BUAWM above. It also registers the user as described under Register above.
Programming: SIP Traffic

Dial Plan

- On the **Dial Plan** page, you can perform advanced routing of SIP requests
Programming: SIP Traffic

Dial Plan “Matching FROM Header”

- Requests can be matched on From header, sender IP address, transport method and network.
Dial Plan “Matching Request URI”

- Requests can be matched on the Request-URI, which states where the request is bound.
Programming: SIP Traffic

Dial Plan “Forward To”

- Define destinations for the SIP requests
Dial Plan “Dial Plan”

- Combine the **From Header**, **Request-URI** and **Forward To** tables in the **Dial Plan** table.
Programming: SIP Traffic

How Does It Work?

- **Outgoing Call**
  - SIP Phone sends INVITE to 6135552000@IP_IP-PBX
  - IP-PBX sends INVITE to 6135552000@IP_Ingate
  - Ingate sends INVITE to 6135552000@IP_ITSP

- **Incoming Call**
  - ITSP sends INVITE to 6135554455@IP_Ingate
  - Ingate sends INVITE to 6135554455@IP_IP-PBX
  - IP-PBX sends INVITE to ExtNumber@IP_Phone
Programming: SIP Traffic

Dial Plan “Method in the Dial Plan”

- Select which methods should be processed by the Dial Plan.

The ACK, PRACK, CANCEL, BYE, NOTIFY, UPDATE and INFO methods cannot be handled by the Dial Plan.

**REGISTER in Dial Plan**
- Keep To headers for REGISTER requests passed through the Dial Plan
- Rewrite To headers for REGISTER requests passed through the Dial Plan
Programming: SIP Traffic

Routing “DNS Override for SIP Requests”

- Enter SIP domains to which traffic should be sent, but which for some reason cannot be looked up using DNS.
Routing “Class 3XX Processing & SIP Routing Order”

- Class 3xx Messages Processing concerns how to process redirect requests
- SIP Routing Order priorities which function to process first
Programming: SIP Traffic

Routing “Static Registrations”

- Statically forward the requests from one SIP URI to another.
Routing “Local REFER Handling”

- SIP Trunking Service Providers cannot handle a REFER Method. Many IP-PBX require to send REFERs for Transferring calls. This ensures the Ingate handles the REFER locally.
Programming: SIP Traffic

SIP Status

- Shows current SIP activity
Exercise #2
Dial Plan
Exercise #2

Training Station #1

Ingate IP: 10.10.10.11

IP-PBX to Ingate
INVITE:
6135552222@10.10.10.11

ITSP to Ingate Emulation
INVITE:
6135552222@12.34.56.22
FROM:
6135551111@12.34.56.11

Ingate to IP-PBX
INVITE:
6135551111@10.10.10.10

Training Station #2

Ingate IP: 12.34.56.11

Ingate IP: 12.34.56.22

Ingate IP: 10.20.20.22

ITSP to Ingate Emulation
INVITE:
6135552222@12.34.56.22
FROM:
6135551111@12.34.56.11

Ingate to IP-PBX
INVITE:
6135552222@10.20.20.20

IP-PBX to Ingate
INVITE:
6135552222@12.34.56.22
FROM:
6135551111@10.20.20.22

Internet
Exercise #3
SIP Security – Lock to Source IP
Overall Training Setup

Training Station #2
- Softphone: DID #: 6135552222, IP Address: 10.20.20.20
- Laptop: IP Address: 10.20.20.20
  - Mask: 255.255.255.0
  - Default GW: 10.10.10.1
  - DNS: 65.175.129.149
- Ingate SIParator 19
  - Username: admin
  - Password: admin
  - MAC Address: 00-D0-C9-A5-7F-15
  - Eth0 (Inside) IP Address: 10.20.20.22
    - Mask: 255.255.255.0
  - Eth1 (Outside) IP Address: 12.34.56.22
    - Mask: 255.255.255.0
  - Default GW: 12.34.56.1
  - DNS: 65.175.129.149

Training Station #3
- Softphone: DID #: 6135553333, IP Address: 10.30.30.30
- Laptop: IP Address: 10.30.30.30
  - Mask: 255.255.255.0
  - Default GW: 10.30.30.1
  - DNS: 65.175.129.149
- Ingate SIParator 19
  - Username: admin
  - Password: admin
  - MAC Address: 00-D0-C9-A5-81-63
  - Eth0 (Inside) IP Address: 10.30.30.33
    - Mask: 255.255.255.0
  - Eth1 (Outside) IP Address: 12.34.56.33
    - Mask: 255.255.255.0
  - Default GW: 12.34.56.1
  - DNS: 65.175.129.149

Training Station #1
- Softphone: DID #: 6135551111, IP Address: 10.10.10.10
- Laptop: IP Address: 10.10.10.10
  - Mask: 255.255.255.0
  - Default GW: 10.10.10.1
  - DNS: 65.175.129.149
- Ingate SIParator 19
  - Username: admin
  - Password: admin
  - MAC Address: 00-D0-C9-A5-81-39
  - Eth0 (Inside) IP Address: 10.10.10.11
    - Mask: 255.255.255.0
  - Eth1 (Outside) IP Address: 12.34.56.11
    - Mask: 255.255.255.0
  - Default GW: 12.34.56.1
  - DNS: 65.175.129.149

Training Station #4
- Softphone: DID #: 6135554444, IP Address: 10.40.40.40
- Laptop: IP Address: 10.40.40.40
  - Mask: 255.255.255.0
  - Default GW: 10.40.40.1
  - DNS: 55.175.129.149
- Ingate SIParator 19
  - Username: admin
  - Password: admin
  - MAC Address: 00-D0-C9-AD-B5-02
  - Eth0 (Inside) IP Address: 10.40.40.44
    - Mask: 255.255.255.0
  - Eth1 (Outside) IP Address: 12.34.56.44
    - Mask: 255.255.255.0
  - Default GW: 12.34.56.1
  - DNS: 65.175.129.149
Troubleshooting
Troubleshooting

Logging Configuration

- SIP Events will ensure SIP calls are logged.
Troubleshooting

Logging & Tools

- Display # Rows/Page
- Show Newest on Top
- Select SIP Log Attributes
- Select “Show internal SIP Signaling”
Troubleshooting

Packet Capture

- Creates a Wireshark PCAP network trace.
- Network Interface Selection – All Interfaces
- Start – Stop - Download
Exercise #4
Packet Capture
THE END
Training Station #1

**Softphone**
- DID #: 6135551111
- IP Address: 10.10.10.10

**Laptop**
- IP Address: 10.10.10.10
- Mask: 255.255.255.0
- Default GW: 10.10.10.1
- DNS: 65.175.129.149

**Ingate SIParator 19**
- Username: admin
- Password: admin
- MAC Address: 00-D0-C9-A5-81-39
- Eth0 (Inside) IP Address: 10.10.10.11
- Mask: 255.255.255.0
- Eth1 (Outside) IP Address: 12.34.56.11
- Mask: 255.255.255.0
- Default GW: 12.34.56.1
- DNS: 65.175.129.149

MAKE A CALL

Training Station #2
- IP Address: 123.123.123.22
- Softphone DID: 6135552222

Softphone
- Call Training Station #2: 6135552222@10.10.10.11
Training Station #3

**Softphone**
- DID #: 6135553333
- IP Address: 10.30.30.30

**Laptop**
- IP Address: 10.30.30.30
- Mask: 255.255.255.0
- Default GW: 10.30.30.1
- DNS: 65.175.129.149

**Ingate SIParator 18**
- Username: admin
- Password: admin
- MAC Address: 00-D0-C9-A5-81-63
- Eth0 (Inside) IP Address: 10.30.30.33
- Mask: 255.255.255.0
- Eth1 (Outside) IP Address: 12.34.56.33
- Mask: 255.255.255.0
- Default GW: 12.34.56.1
- DNS: 65.175.129.149

**MAKE A CALL**

**Softphone**
- Call Training Station #4:
  - 6135554444@10.30.30.33

**Training Station #4**
- IP Address: 12.34.56.44
- Softphone DID: 6135554444