

Configuration Guide

Secure VoIP Implementation for Remote Users Use case

How to design and deploy a secure IP Telephony/UC using unique Ingate SIParator/Firewall features

Contents

| 1 | INT | RODUCTION | 4 |
|---|----------------|---|-----|
| | 1.1 D | ETAILED USE CASE | 5 |
| | 1.2 A | SSUMPTIONS BEFORE STARTING | 7 |
| | 1.3 In | GATE SIPARATOR [®] /Firewall [®] Supported | 7 |
| | 1.3.3 | Ingate SIParator [®] /Firewall [®] S21 | 7 |
| | 1.3.2 | | |
| | 1.3.3 | | |
| | 1.3.4 | | |
| | 1.3. | Ingate Software SIParator [®] /Firewall [®] for AWS | 8 |
| 2 | SSL | CERTIFICATES CREATION | 9 |
| - | | | |
| | | SING SIMPLE AUTHORITY. | |
| | | STALLING SIMPLE AUTHORITY FOR WINDOWS | - |
| | | TTING UP CA CERTIFICATE | |
| | | STALLING CA CERTIFICATE ON THE SIPARATOR | |
| | 2.5 C | REATING AND INSTALLING SERVER CERTIFICATES FOR SIPARATOR | .13 |
| 3 | INC | ATE DATA CENTER NODE CONFIGURATION | 19 |
| | 3.1 B | ASIC CONFIGURATION | 10 |
| | 3.1. | | |
| | 3.1.2 | | |
| | | ETWORK CONFIGURATION | |
| | 3.2.1 | | |
| | 3.2.2 | • | |
| | 3.2.3 | | |
| | 3.2.4 | 0 | |
| | 3.3 In | STALLING CERTIFICATE ON INGATE DATA CENTER | 26 |
| | 3.4 F | REWALL CONFIGURATION - RULES AND RELAYS | 27 |
| | 3.5 S | P SERVICES | 30 |
| | 3.5.2 | Basic configuration | .30 |
| | 3.5.2 | Signaling Encryption | 32 |
| | 3.5.3 | | |
| | 3.5.4 | | |
| | 3.5. | | |
| | | P Trunks | |
| | | P TRAFFIC | |
| | 3.7.2 | | |
| | 3.7.2 | | |
| | 3.7.3 3.7.4 | | |
| | 5.7.4 | | .40 |
| 4 | INC | ATE REMOTE OFFICE NODE CONFIGURATION | 47 |
| | 4.1 R | O BASIC CONFIGURATION | 47 |
| | 4.1.3 | | |
| | 4.1.2 | | - |
| | | O NETWORK CONFIGURATION | |
| | 4.2.2 | Networks and Computers | 50 |
| | 4.2.2 | | |
| | 4.3 In | STALLING CERTIFICATE ON INGATE REMOTE OFFICE | |
| | | D FIREWALL CONFIGURATION - RULES AND RELAYS | |
| | 4.5 R | O SIP Services | 51 |
| | 4.5.2 | Basic configuration | 51 |
| | 4.5.2 | | |
| | 4.5.3 | Media Encryption | .54 |
| | | | |

| | 4.5.4 | Remote SIP Connectivity | 54 |
|---|----------|-----------------------------|----|
| | | VoIP Survival | |
| | 4.6 ROS | IP TRAFFIC | 56 |
| | | RO Routing | |
| 5 | ADDIT | 'IONAL INFORMATION | 58 |
| | 5.1 ENDP | OINT CONFIGURATION EXAMPLES | 58 |
| 6 | ADDITIC | DNAL HELP OR SUPPORT | 61 |

1 Introduction

This guide is a step by step guide that walks you thru the process to deploy a strong, resilient and secure platform taking advantage of unique features and functionalities included in SIParator/Firewall platforms.

The unique values inherit by the only solution in the market that combines Full SIP Compliance, SIP Connect Compliance, SIP Proxy, B2BUA and advanced firewall features, provides Solutions Engineers with the tools and capabilities to implement strong, resilient and secure VoIP Infrastructure.

The use case associated to this guide covers remote user access with the following functionalities:

- 1) Focus on Remote Branch office
- 2) Remote Phone Provisioning
- 3) TLS secure connection when crossing public network (Internet)
- 4) SRTP media secured.
- 5) Double tier survivability (When IPPBX goes down, and also in case Internet connection goes down.

This diagram summarizes the use case we are about to explain along this document:

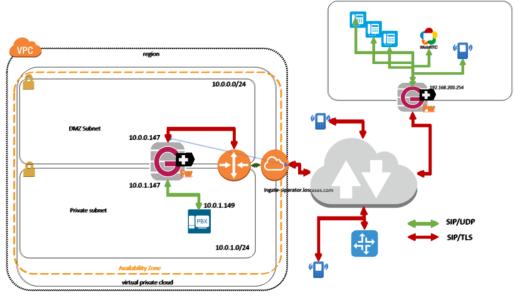
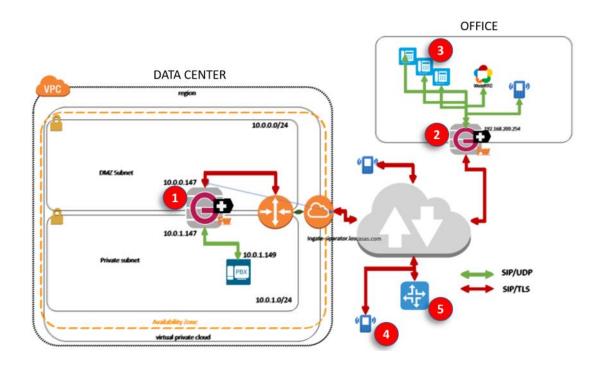


Figure 1

1.1 Detailed use case

We have selected a specific layout that covers most of the typical situations in Enterprise deployments. We assume:

- 1) IPPBX is centrally located in a Data Center
- 2) We use one Remote Office to represent HQ or any typical Branch Office.
- 3) Data center IPPBX will be sitting behind a SIParator/Firewall
- 4) Ingate SIParator/Firewall will be setup as a DMZ/LAN in the Data Center.



Here more details:

Ingat

Ingate at Data Center. We use a SIParator/Firewall in front of the IPPBX/UC system using DMZ/LAN Topology. It will:

- Act as a NAT Gateway to the Internet for data traffic other than SIP and Media.
- Provide Rules and Policies for traffic flow and port forwarding for other non-SIP/Media traffic
- Convert all SIP sessions between SIP/UDP and SIP/TLS
- Provide survivability to remote endpoints in case IPPBX becomes unreachable
- Provide RTP ←→ SRTP conversion for media going to or coming from the Internet
- The PBX will not be penalized with any load consequence of TLS Session Management or RTP/SRTP transcoding



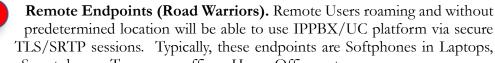
Ingate at Remote Office. To be able to show all potential and unique capabilities when using SIParator/Firewall, we add one Ingate at the remote site. This will enable the following:

- Eliminate any NAT Traversal challenge.
- Convert all SIP sessions between SIP/UDP and SIP/TLS, removing the need to have TLS and SRTP Support on every single endpoint.
- Provide a secondary Survival device for all local endpoints. In case connectivity to Internet is lost, or even the IPPBX in the Data Center becomes unreachable, the Ingate will provide local Telephony and basic inbound/outbound call routing.



Remote Endpoints (Branch Office). Users in Branch or remote offices use endpoints registered to the UC/IPPBX platform located in the Data Center. All features and functionalities must be preserved as though the user were local to the IPPBX/UC platform.

- - Phones will be provisioned via the functionalities provided by the IPPBX/UC Vendor
- Phones will use standard SIP and RTP (No encryption necessary at the phone ٠ level)
- Phones will see local Ingate as its Outbound Proxy for SIP
- Phones will see local Ingate as the default gateway to the Internet
- Phones will be able to use any expanded feature from the Vendor, such as Presence, BLF, RestAPI, etc..



Tablet's or Smartphones. Temporary offices, Home Offices, etc.

- Endpoint Device or softphone will be configured with TLS/SRTP
- They will be able to connect to services regardless of where they are located (LTE, 3g/4g, wifi, etc..)



ITSP and PSTN connection. The use case includes PSTN access and considers.

As TLS/SRTP is becoming more a key component to diminish risks, attacks and misuse, ITSPs today offer Secure SIP Trunks as an optional feature on their service.

1.2 Assumptions before starting

This use case has been tested and is viable with any SIParator/Firewall hardware models, as well as SIParator VM and SIParator for AWS.

Software version used in SIParator/Firewall is 6.2.1

As this document show case uses AWS, it assumes you have already done the Installation and licensing for the SIParator needed. In case you need to do so, you can refer to this documentation:

→ Orientation and How to Install SIParator on AWS

1.3 Ingate SIParator®/Firewall® Supported

1.3.1 Ingate SIParator®/Firewall® S21

The S21 is a powerful tool that offers small businesses, branch offices and home workers complete support for IP communications based on SIP. With the SIParator 21, these businesses can leverage the same productivity and cost-savings benefits of Voice over IP and other IP-based communications as large corporations. It manages up to 400 concurrent RTP sessions.

1.3.2 Ingate SIParator®/Firewall® S52



The Ingate SIParator®/Firewall® S52 is a powerful tool for businesses wanting to step up to the next level of using Voice over IP and other IP-based realtime communications,

and to do so not only within the company, but outside the enterprise as well. It manages up to 2000 concurrent RTP sessions.

1.3.3 Ingate SIParator®/Firewall® S95/S97/S98



The Ingate SIParator®/Firewall® S95/S97/S98 are E-SBCs that offers large enterprises a controlled and secured migration to Voice over IP and other live

communications, based on SIP. With the Ingate SIParator, E-SBC even the largest of businesses, with branch offices around the world and remote workers, can easily harness the productivity and cost-saving benefits of VoIP and other IP-based communications while maintaining current investments in security technology.

The Ingate SIParator® 95/97/98 are high capacity, high performance E-SBCs designed for large enterprises, call centers and service providers, and can handle up to 20,000 RTP sessions.

1.3.4 Ingate Software SIParator®/Firewall®



Ingate's Software SIParator®/Firewall® is the software version of Ingate's E-SBCs, - the solution for enterprises that want to deploy Ingate's award-winning E-SBCs on your own hardware platform. Like all Ingate E-SBCs the Software SIParator®/Firewall® makes secure SIP-based communications – including VoIP, SIP trunking and UC – possible. The Software SIParator®/Firewall® come with the option to

choose the number of sessions, to meet the needs of the entire enterprise market, regardless if it's used by small enterprises e.g. branch offices, home workers, or midrange/large enterprises.

1.3.5 Ingate Software SIParator®/Firewall® for AWS

awsmarketplace Ingate Software SIParator®/Firewall® is also available thru AWS Marketplace. It is the same product we have for VM environments as well as any of the appliances explained before. If you have an AWS account, you can directly provision one SIParator instance using this link:

→ <u>Get it from AWS Marketplace</u>

The following sections show step by step how to deploy this use case.

2 SSL Certificates creation

In our case we use SSL certificates as a component of TLS deployment. To understand in a simplified diagram, all VoIP traffic traversing the Internet between endpoints and SIParator will be encrypted and secured using TLS for signaling and SRTP for media.

In real implementations, it is recommended to use Commercial Certification Authorities (Trusted) to issue and sign certificates. In our case, to make it easy to understand the concept, we illustrate how to generate your own CA and sign your own certificates. This is not recommended for real production environments but is a very easy way to build your PoC or Labs.

2.1 Using Simple Authority.

SimpleAuthority is a fully functional Certification Authority, or Certificate Authority (CA), that is designed to be very easy to use. It generates and manages keys and certificates that provide cryptographic digital identities for people and/or computer servers. These identities are designed to be used in other applications such as for:

- secure two factor authentications using a technology like KeyVault for controlling access to Web resources
- secure email for digital signing and encryption of email
- document signing including PDF, Word and OpenOffice documents
- VPN access to provide a much higher level of security than username/password access
- client SSL authentication to control access to an online service such as a subversion repository or wiki
- server SSL authentication to authenticate a Web server to people within a known community
- code signing including Java archives, Windows executables, etc.

SimpleAuthority supports Windows, Mac OS-X and Linux platforms.

Unlike most CA products, SimpleAuthority does not require specialist <u>PKI knowledge</u> or supporting components like an external database. It is built on <u>The Legion of the Bouncy</u> <u>Castle</u> cryptographic library.

2.2 Installing Simple Authority for Windows

First you will need to download the application from here:

https://simpleauthority.com/download.html

Select the platform which fits your case. We will use Windows 64 bits option.

Make sure you have Java Runtime version 8 at least.

2.3 Setting up CA Certificate

After Install is completed, and on first time run, you will be requested to create your CA. This will be your own Certification Authority that will be used to Generate Signed Server/Client certificates as well as Sign Certification Requests generated by third parties.

| 🎬 New self-signed CA | × | | | | | | |
|-----------------------|-------------------------|--|--|--|--|--|--|
| Common Name: | InGate Systems CA | | | | | | |
| Organisational Unit: | Certification Authority | | | | | | |
| Organisation: | Pre-Sales Engineering | | | | | | |
| Country: | United States | | | | | | |
| Certificate Validity: | 10 years | | | | | | |
| Advanced Settings | | | | | | | |
| Help | Cancel OK | | | | | | |

Figure 2

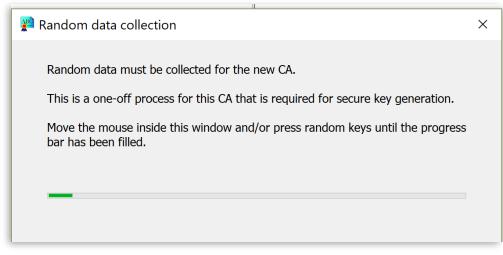


Figure 3

After the key is generated, a password will be requested to be assigned to the CA



Now to export and install the CA Certificate to each SIParator, for each one of them to be able to trust certificates signed by this authority

| 🕎 Simple/ | Authority - InGate Systems | CA | |
|-------------|---|----------------------------|------------------------|
| File View T | ools Help | | |
| Active ⊽ | Certificate Details CA Certificate Details | | Name |
| Active | Log File | • | ingate-siparator.losca |
| | Import > | • | No Name |
| | Export > | Latest Certificates | Ctrl+E |
| | BER Parse | CA Certificate | |
| | Options | Selected Certificate | |
| | | Export certificate | for InGate $	imes$ |
| | | iCa Export certificate to: | File (PEM format) |
| | _ | Cancel | Export |

Figure 5

- Select Tools→Export→CA Certificate
- Select PEM Format

2.4 Installing CA certificate on the SIParator

Import CA Certificate on each SIParator. In the SIParator GUI, Basic Configuration \rightarrow Certificates, add a new row in the CA Certificates section:

| CA Certificates (Help) | | | | | | | | |
|------------------------------|--------------------------------|-------------|------------------------|------------|--|--|--|--|
| Name | CA Certificate | CA CRL | Information | Delete Row | | | | |
| No value given. InGate CA | No value given. Change/View | Change/View | No current certificate | | | | | |
| Add new rows 1 | fows. | | | | | | | |

Figure 6

- Assign a Name for this certificate
- Press "Change/View" Option to proceed to create/download

| Administration Basic Configuration Network Services Traff | ic Trunks Failover Virtual Private Quality of Service and Tools About |
|---|--|
| Changes have been made to the prelim | ninary configuration, but have not been applied. |
| Current CA Certificate | Upload CA Certificate |
| No current certificate. Download current CA certificate (DER format) Download current CA certificate (PEM format) | Specify the local file, in PEM (.pem) or DER (.cer) format, containing the CA certificate for "InGate CA" below, then press the import button. Local file containing CA certificate: Browse Ingate Systems_cert_CA.pem Import CA certificate Abort |

Figure 7

- Browse and select the recently exported CA Certificate
- Press "Import CA certificate"

After Importing you will see a confirmation message with the details, and also you will be able to see the certificate already loaded in the CA Certificates section:

| | CA | | | |
|-----------|-------------|-------------|--|---|
| Name | Certificate | CA CRL | Information | |
| InGate CA | Change/View | Change/View | Subject: /C=US/O=Pre-Sales Engineering/OU=Certificati | on Authority |
| | | | /CN=InGate Systems CA | |
| | | | Issuer: /C=US/O=Pre-Sales Engineering/OU=Certification | 1 Authority |
| | | | /CN=InGate Systems CA | |
| | | | MD5 Fingerprint: | D:55:06 |
| | | | SHA1 Fingerprint: | 0F 2497 8001 |
| | | | Valid from: 2017-08-09 15:45:48 | |
| | | | Valid to: 2027-08-10 15:46:01 | |
| | | | Subject Key ID: | 3:F9:5E:51:84 |
| | | | Authority Key | |
| | | | ID: | and the second se |

Figure 8

2.5 Creating and Installing Server Certificates for SIParator

We will now create a Certificate Request (CR) in the SIParator GUI and send it to our CA Authority to be signed, returned and updated.

Creating the Request (CR)

| Basic Configuration | Access Control | RADIUS | SNMP | Dynamic DNS Update | Certificates | TLS | Advanced | SIParator Type | |
|-------------------------------------|-----------------------------|--------|-------------|-----------------------|--------------|-------|----------|-------------------|-------------|
| Private C | Private Certificates (Help) | | | | | | | | |
| Nan | Name | | Certificate | | | | | | Information |
| No certific | No certificate exists. | | | | | | | | |
| No value given. TLS Voice Signed | | Crea | te Nev | Import | View/Do | ownlo | No | current c | ertificate |

Figure 9

- Assign a name to the certificate
- Press "Create New" button.

| Create Certificate or Certificate Request | |
|--|------|
| Fill in the certificate data for "TLS Voice Signed" below, then create either a certificate or a certificate reque | est. |
| After generating a certificate request, and having it signed by a signing authority, the certificate must be imp | orte |
| Expire in (days): Country code (C): Organization (O): * 365 US Ingate Common Name (CN): State/province (ST): Organizational Unit (OU): * ingate-siparator.lo FL Support Email address Locality/town (L): ernesto@ingate.cd | |
| SubjectAltName Extension | |
| Enter the alternative names that you want to add to a certificate or a certificate request. Multiple values can be added by using comma separation. Email: ernesto@ingate.com URI: DNS: ingate-siparator.loscasas.co IP: 52.7.99.1 | |
| Key Length and Signature Algorithm | |
| Select the key length and the signature algorithm that you want to use when creating a certificate or a certificate request. Key length (bits): 2048 Signature algorithm: SHA-256 | |
| If you generate several certificates with identical data you should make sure they have different serial numb | ers. |
| Serial number: | |
| * 3 Fields marked with "*" are mandatory. | |
| Create a self-signed X.509 certificate Create an X.509 certificate request Abort | |

Figure 10

- Complete all information relevant, and the mandatory field CN (Common Name) is the FQDN or exposed IP address of the device where the certificate is going to be installed
- Use the Button "Create an X.509 certificate request". Otherwise you will be creating a self-signed certificate which won't work in TLS between SIParators.
- Save and Apply changes

You will be able to see the recent CR in the GUI.

| | bject: /c | =US/ST=FL/ | | | | | or.loscasas.com/emailAddress=erne ator.loscasas.com, IP Address:52 | | |
|---------------|------------------------------|------------|-----------------------|------------------|-----------------|--|---|--|--|
| | _ | | Dynamic DNS Update | Certificates TLS | | lParator Type | | | |
| Name | Name Certificate Information | | | | | | | | |
| TLS Voice Sig | gned | Create New | Import | View/Downlo | sipara Subje | Subject: /C=US/ST=FL/O=Ingate/OU=Support/CN=ingate- siparator.loscasas.com/emailAddress=ernesto@ingate.com SubjectAltName: email:ernesto@ingate.com, DNS:ingate- siparator.loscasas.com, IP Address:52.7.99.1 | | | |

Figure 11

Now you will need to send (Export) this CR to be signed by the CA.

Press on the "View/Download"

| Current Private Certificate for "TLS Voice Signed" |
|--|
| Current certificate request: |
| Subject: /C=U3/8T=FL/O=Ingate/OU=Support/CN=ingate-siparator.loscasas.com/emailAddress=ernesto@ingate.com SubjectAltName: email:ernesto@ingate.com, DNS:ingate-siparator.loscasas.com, IP Address:52.7.99.1 |
| Download certificate/certificate request (DER format) Download certificate/certificate request (PEM format) |
| Return to certificate page |

Figure 12

• Download the CR to your local folder

Sign the Certificate with Simple Authority CA

There is initially a default user created. For Simple Authority each user represents one user or device to which one or more certificates can be associated.

In our case we have 2 users, one for each SIParator. But will show here only the first one. You can repeat the process for the second SIParator (RO).

| 👺 Simple | eAuthority - InGate Systems | CA | |
|-----------|-----------------------------|------------------------|------------------------|
| File View | Tools Help | | |
| S 🚨 (| Certificate Details | | |
| Active | CA Certificate Details | | Name |
| | Log File | • | ingate-siparator.losca |
| | Import > | Certificate from File | |
| | Export > | Identity from File | |
| | BER Parse | Users from LDIF | |
| | Options | Users from vCard | |
| | | Certificate Signing Re | quest |
| | | | |
| | | | |

Figure 13

- Having the user selected, go to Tools \rightarrow Import \rightarrow Certificate signing request
- Select and import the CR you exported from the SIParator GUI.

| | | | | × |
|----------------------------|---------------|-----------|---------------|------------------------------------|
| Enter the settings for the | new certifica | te. | | |
| Certificate Type: | | General | Purpose | \checkmark |
| Certificate Validity: | | 365 | days | |
| • Use Subject DN from | request | | | |
| E=ernesto@ingate.cor | n,CN=ingate- | siparato | or.loscasas.c | com,OU=Support,O=Ingate,ST=FL,C=US |
| OUse custom settings f | or Subject DN | I | | |
| Common Name | ingate-sipara | ator.losc | asas.com | |
| 🖂 Email Address | ernesto@ing | ate.com | 1 | |
| 🖂 Organisational Unit | Support | | | |
| Organisation | Ingate | | | |
| Country | United States | S | | |
| ⊡ Include extension req | uests from CS | SR | | |
| | | Car | ncel OK | |
| | | Figu | ıre 14 | |

- At this point you can leave or modify settings for this certificate
- Once you press OK the new certificate, already signed is created.

A New Certificate is generated and can be seen in the tool:

| Status Name Days to Expiry | ingate-siparator.loscasas.com | | | Clear |
|---|-------------------------------|---------------|-------------|-----------|
| Active Status Name Days to Expiry | ingate-siparator.loscasas.com | | | Ciedi |
| | | | | |
| ✓ ingate-siparator.loscas 364 ✓ ingate-siparator.loscas | Certificate Type: | General Purpo | ose 🗸 | |
| ingate-siparator.loscas | Email Address | ernesto@inga | te.com | |
| | Organisational Unit | Support | | |
| | Organisation | Ingate | | |
| | Country | United States | | |
| | Certificate Validity: | 365 days | | |
| | Edit User | | | |
| s s | Status Identity Is | sued | Expires | Days Left |
| | • | Aug 9, 2017 | Aug 9, 2018 | 364 |

Figure 15

Now we will export the Signed Certificate to be loaded in SIParator.

Right click on the Certificate and select Export Certificate

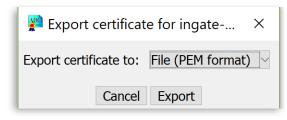


Figure 16

- Select PEM Format
- Press "Export"
- Save the Signed certificate in your folder

| Basic Configuration | Access Control | RADIUS | SNMP | Dynamic DNS Update | Certificates | TLS | Advanced | SIParator Type | |
|------------------------|-------------------|--------|---------|-----------------------|--------------|-------|-------------|-----------------------------|---|
| Private (| Certifi | cates | (Help) | | | | | | |
| Nar | ne | | | Certifi | cate | | | | Information |
| TLS Voice | Signed | Crea | ate Nev | Import | View/Do | ownle | sipa Sub | rator.loscas: jectAltNan | 5/ST=FL/O=Ingate/OU=Support/CN=ingate- as.com/emailAddress=ernesto@ingate.com ne: email:ernesto@ingate.com, DNS:ingate- as.com, IP Address:52.7.99.1 |

Figure 17

• Use the Import button under the CR we generated before.



Figure 18

• Select the file and press "Import signed certificate"

Now you will see the signed certificate already in the Table:

| Basic Access onfiguration Control | | Dynamic IS Update | Certificates TLS Adva | SIParator Inced Type |
|--------------------------------------|---------------------|----------------------|-----------------------|---|
| Private Certific | ates (<u>Help)</u> | | | |
| Name | | Certifica | ite | Information |
| TLS Voice Signed | Create New | Import | View/Download | Subject: /C=US/ST=FL/O=Ingate/OU=Support/CN=ingate- siparator.loscasas.com/emailAddress=ernesto@ingate.com Issuer: /C=US/O=Pre-Sales Engineering/OU=Certification Authority /CN=InGate Systems CA MD5 Fingerprint: AB:2F:4 SHA1 Fingerprint: B7C 73: Valid from: 2017-08-09 17:55:11 Valid from: 2017-08-09 17:55:12 SubjectAlfName: email:ernesto@ingate.com, DNS:ingate- siparator.loscasas.com, IP Address:52.7.99.1 Subject Key ID: I:: BC:79 Authority Key ID: F9:5E:51:84 |

You can now repeat the sequence of steps for the second SIParator.

3 Ingate Data Center Node Configuration

Going Back to our original Layout:

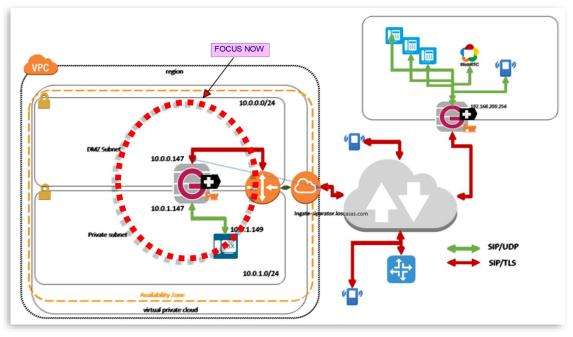


Figure 19

We are going to explain the steps necessary to have a fully configured SIParator at the Data center side. This SIParator will accomplish the following main functionalities:

- Isolate IPPBX from being SIP/Telephony exposed to the Internet.
- Hide internal topology
- Provide Endpoints access to IPPBX telephony resources only via a secure protocol (TLS in this case), without the need of TLS support at the IPPBX
- Enable controlled and policy-based data traffic between endpoints and IPPBX for specialized (NON-Voice related) capabilities (i.e. Provisioning, collaboration, etc...)
- Provide Endpoints Communications between them or with the IPPBX with Secure Media Encryption (SRTP)
- Provide survivability features for remote endpoints in case IPPBX becomes unreachable.
- Provide ITSP (PSTN) connectivity to the IPPBX
- Protect against brute force attacks
- Prevent Intrusion access
- Resolve Near and Far End NAT (FENT) traversal.
- Maximize media flow efficiency and QoS where possible.

3.1 Basic Configuration

We will not go over all potential options that can be configured. We assume most of the default configuration values are in place and show only what is needed and not default.

3.1.1 Access Control

We have 2 Physical Interfaces. One (eth0) will be used for connecting to "Outside" and will be located in a Subnet (DMX type) with 1-1 NAT to a dedicated public IP address. The second Interface (eth1) will be assigned to "Inside" and will be connected to a LAN Subnet with no direct access to the Internet.

| Adı | ministration | Basic Configuration | rork Rules and Relays | SIP SIP SIP SIP SIP SIP SIP SIP SIP SIP | | l Private works | Quality of Service | Loggi and To | ~ Abo | but | | |
|-----|---|-----------------------------------|------------------------------|--|---------------------------------------|--------------------|-----------------------|-----------------|------------------|-------|---------------------|---------------|
| 6 | Basic onfiguration | Access Control RADIUS SN | DHCP DHC MP Options Serve | | Router Dynamic ertisement DNS Upda | | cates TLS / | Advance | SIPara ed Typ | | | |
| lī | Configu | ration Allowed | Via Interface | (Help) | | _ | | | | | | |
| | Interface Outside (Inside (et Add new r | h1) V Yes | red Delete Row | | Phy Inter | | | | | | | |
| Ļ | Configu | ration Transpor | t (Help) | | | | | | | | | |
| l | Protoco | | | Cert | TLS | | Delete F | low | | | | |
| | HTTPS | | × 443 | | TLSv1.x | - - | | - | | | anageme Protocol | |
| | | - - | × 22 | | < | ~ | | | | | 1010001 | 5 |
| ļ | Add new r | ows 1 rows. | | | | | | | | | | |
| Ľ | | | | | | | | | | | | |
| Ľ | User Au Local | | r Web Interfa | ce Access (Help | <u>)</u> | - 1 | Orio | nin | atin | | tworks | |
| | 0 | users US database | | | | | | | | | ess for | |
| | O Local | users or RADIUS | database | | | | ano | | | geme | | |
| | Web Int | erface Access Se | ettings (Help) | | | | | <hr/> | | | | |
| I | Login time | out: 28800 sec | onds | | | | | | | | | |
| L | Configu | ration Compute | rs <u>(Help)</u> | | | | | | 2 | 4 | | |
| | No. | DNS Name or Network Address | Network Address | Netmask / Bits | Range | Via II | sec Peer | SSH | HTTP | HTTPS | Log Class | Delete Row |
| | 1 | 10.0.0.0 | 10.0.0.0 | 16 | 10.0.0.0 - 10.0.255.255 | - | ~ | | | | - | |
| | 2 | 192.168.200.0 | 192.168.200.0 | 24 | 192.168.200.0 - 192.168.200.255 | - | ~ | | | | - | |
| | 3 | 0.0.0.0 | 0.0.0.0 | 0 | 0.0.0.0 - 255.255.255.255 | - | ~ | | | | - `` | |

Figure 20

3.1.2 SIParator Type

Here we make sure SIParator in "SIParator Type in Firewall Mode" is enabled, type is DMZ/LAN and Firewall mode is active.

This guide fully applies also when the device is in SIParator mode (non-Firewall) with minor adjustments. Refer to the Product Manual or contact our Support team if you need additional details.

| Administration | Ba: Configu | | Network | Rules a Relay | ind rs Sei | SIP rvices Traffic | SIP Trunks Failov | ver Virtual P Netwo | | lity of vice | Logging and Tool | ADOUT |
|--|-------------------|-----------------------|---------|------------------|----------------|-----------------------|-------------------------|------------------------|--------------|-----------------|---------------------|-------------------|
| Basic Configuration | Access Control | RADIUS | SNMP | DHCP Options | DHCP Server | DHCP Server Status | Router Advertisement | Dynamic DNS Update | Certificates | TLS | Advanced | SIParator Type |
| SIParate | or Typ | <mark>e in F</mark> i | rewal | l Mode | (Hel | <u>p)</u> | | | | | | |
| Enable Disable Disable Disable DMZ/LAN | e SIPar | ator | pes of | SIPara | tors. Pl | ease choose | the one that f | fits your ne | eds. | | | |
| Firewall | Mode | (Help |) | | | | | | | | | |
| | | ator mo ational r | | l reboot | enabl | e checkbox t | hen press but | ton | | | | |

Figure 21

- Make sure SIParator is enabled
- Select DMZ/LAN option
- Make sure the device is working in Firewall Mode. If not it will show the "SIParator" logo in the top of the GUI and you will need to "change operational mode"

3.2 Network configuration

In this section, we review and complete each one of the interfaces IP addressing, DNS and Default gateway. We also name (Networks & Computers) specific IP addresses, subnets or groups of subnets to easy referring to them in other sections.

3.2.1 Networks and Computers

Here we will name Devices (IPs), Subnets and Groups of subnets to be used later in the configuration:

| works and Defa | ays Interfaces NAT | | nterface | Networks nels Topology | Service and Tools | - |
|----------------|--------------------|---------------------------|-----------------|---------------------------|--------------------|-------------------------|
| N. | | Lower | Limit | | · Limit ranges) | |
| Name | Subgroup | DNS Name or IP Address | IP Address | DNS Name or IP Address | IP Address | Interface/VLAN |
| + IPPBX | | 10.0.1.149 | 10.0.1.149 | 10.0.1.149 | 10.0.1.149 | - |
| • Internet | - ~ | 0.0.0.0 | 0.0.0.0 | 255.255.255.255 | 255.255.255.255 | Outside (eth0 untagged) |
| + Office | | | 100 100 140 | in the second | 100 100 140 | - |
| | - ~ | 192.168.200.0 | 192.168.200.0 | 192.168.200.255 | 192.168.200.255 | - |
| + PrivateLan | - ~ | 10.0.1.0 | 10.0.1.0 | 10.0.1.255 | 10.0.1.255 | - |
| • PublicLan | - ~ | 10.0.0.0 | 10.0.0.0 | 10.0.255 | 10.0.255 | - |
| • SipTrunk | Sipstation1 × | | | | | - |
| | Sipstation2 | | | | | - |
| • Sipstation1 | | Partic Progles and | 101119-063 | Forth, Pauglin, cort | 182 179-66.3 | Outside (eth0 untagged) |
| • Sipstation2 | - ~ | States in such as an | 162 213 234 242 | Intelligible and | 162 213 134 142 | Outside (eth0 untagged) |
| + access | Internet 🗸 | | | | | - |
| | Office | | | | | - |

- IPPBX associated to IPPBX IP address in the Private LAN
- Internet to group all IP address
- Office combining Public IP address of the remote office and internal private subnet
- PrivateLan to associate Private Subnet in the Data Center where the IPPB is located and where SIParator has eth1 connected
- PublicLan to associate Public Subnet in the Data Center where connectivity to Internet and the Outside is located and where SIParator has eth0 connected
- SIPTrunk, combines two SIPTrunk destinations (Used here combined as they belong to the same provider in Failover setup)
- Access, combining Internet and Office under the same name.

3.2.2 Defining Outside Interface:

| | t ation Network | Rules and Si Relays Serv | | SIP Trunks | Failover | Virtual Private Networks | Quality of Service | Logging and Tools | bout | |
|--|---|---|-------------------------|---------------|----------------------|--------------------------------|-----------------------|----------------------|----------|-----|
| letworks and Default Computers Gateways | All Interfaces NA | AT VLAN <mark>Etho</mark> e | Interface th1 Status | | Tunnels To | opology | | | | |
| General | | | | | | | | | | |
| Physical device: eth | h0 | | | | | | | | | |
| This int <mark>erface is:</mark> (| 🖲 Active 🔿 | Inactive | | | | | | | | |
| Interfac <mark>e name:</mark> Ou | utside | | | | | | | | | |
| Directly Connec | ted Networ | ks (Help) | | | | | | | | |
| | Address | DNS Nat | ne | IP | | 1 / 1914 | Network | Broadcast | VLAN | VLA |
| Name | Туре | or IP Add | | ddress | | ask / Bits | Address | | Id | Nam |
| eth0 | Static 🗸 | 10.0.0.147 | 10 | 0.0.0.147 | 24 | | 10.0.0.0 | 10.0.0.255 | | - |
| Add new rows | fows. | | | | | | | | | |
| | | | | | | | | | | |
| Alias (Help) | | | | | | | | | | |
| Below are the range | s from which | i you can select | aliases. | | | | | | | |
| 10.0.0.1-10.0.0.254 | i | | | | | | | | | |
| DNS Nar | me | | | | | | | | | |
| at Dino Ital | | | | | | | | | | |
| Name or IP Add | | ress Delete Ro |)W | | | | | | | |
| | | ress Delete Ro | ow | | | | | | | |
| Add new rows 1 | ress IP Addi | ress Delete Ro |)W | | | | | | | |
| Name or IP Add | ress IP Addi | ress Delete Ro |)W | | | | | | | |
| Name or IP Add Add new rows 1 Proxy ARP (He | ress IP Addi | Proxy Al | w RPed Netw | vork | | | | | | |
| Add new rows 1 | ress IP Addi | Proxy Al | | | mask / Bi | ts VLAN Id | VLAN N | vame Delete | Row | |
| Name or IP Add Add new rows 1 Proxy ARP (He | ress IP Addi rows. | Proxy Al | RPed Netw | | nask / Bi | ts VLAN Id | VLAN N | iame Delete | Row | |
| Name or IP Add Add new rows 1 Proxy ARP (He Get Network Fro | ress IP Addi rows. | Proxy Al | RPed Netw | | mask / Bi | ts VLAN Id | VLAN N | vame Delete | Row | |
| Name or IP Add Add new rows 1 Proxy ARP (He Get Network Fro Add new rows 1 | ress IP Addi rows. | Proxy Al | RPed Netw | | nask / Bi | ts VLAN Id | | iame Delete | Row | |
| Name or IP Add Add new rows 1 Proxy ARP (He Get Network Fro Add new rows 1 | ress IP Addi rows. | Proxy Al ame or Address Netw Address | RPed Netw | ress Neti | mask / Bi Dynamic | Rou | tter ame | iame Delete | e Row | Row |
| Name or IP Add Add new rows 1 Proxy ARP (He Get Network Fro Add new rows 1 Static Routing DNS Name or | ress IP Addi rows. | Proxy Al ame or Address Netw Address | RPed Netw | ress Netr | | its Rou DNS N | tter ame Idress | | | tow |
| Name or IP Add Add new rows 1 Proxy ARP He Get Network Fro Add new rows 1 Static Routing DNS Name or Network Addres | ress IP Addi rows. m DNS Na Network. (Help) css Network 0.0.0.0 | Proxy Al ame or Address Netw Network | RPed Netw | ress Netr | Dynamic | ts Rou DNS N or IP Ad | tter ame Idress | IP Address | Delete F | Low |

- Remember eth0 interfaces DMZ subnet and maps 1-1 to a Public IP address
- Make eth0 active
- Name eth0 "Outside" for a better identification
- IP address has been assigned as documented in the Solution layout (Figure 19)
- Default gateway (See Static Route) points to 10.0.0.1, which is the gateway provided by the Cloud Service Provider.

3.2.3 Defining Inside Interface:

| Iministration Configure | | Rules and S Relays Serv | IP SIP vices Traffic | SIP Trunks | | ial Private etworks | Quality of Service | Logging and Tools | About | |
|---|----------------------|----------------------------|-------------------------|---------------|-----------------------|------------------------|-----------------------|-------------------------|--------|------------|
| Vetworks and Default Computers Gateways | All Interfaces NA | T VLAN EthO E | th1 Status | | Tunnels Topolo | ogy | | | | |
| General Physical device: eth This interface is: () Interface name: Ins | Active 🔾 | Inactive | | | | | | | | |
| Directly Connec | | ks <u>(Help)</u> | | | | | | | | |
| Name | Address Type | DNS Nat or IP Add | | IP Address | Netmask | . / Bits | Networ Addres | k Broadcas s Address | | VLA Nam |
| eth1 | Static 💛 | 10.0.1.147 | 10 | 0.0.1.147 | 24 | | 10.0.1.0 | 10.0.1.25 | 5 |]- |
| Name DNS Nar or IP Addr Add new rows 1 Proxy ARP (He | fows. | ress Delete Ro |)W | | | | | | | |
| Get Network Fro | m DNS Na Network | ame or Note | RPed Netv vork Addr | | nask / Bits | VLAN Id | I VLAN | Name Dele | te Row | |
| Add new rows 1 | fows. | | | | | | | | | |
| Static Routing | (Help) | | | | | | | | | |
| | Routed Net | work | | | Route | r | | | | |
| DNS Name or Network Address | Network A | ddress Netma | ask / Bits | Dynamic | DNS Nan or IP Addr | | Iddress | Delete Row | | |
| Add new rows 1 | fows. | | | | | | | | | |

- Remember eth1 interfaces the LAN the IPPBX
- Make eth1 active
- Name eth1 "Inside" for a better identification
- IP address has been assigned as documented in the Solution layout (Figure 19)
- No default gateway defined here.

After configuring both interfaces you will be able to confirm proper configuration of Default gateway for the system.

| dministration | Basic Configurat | ion Network | Rules an Relays | d]s | SIP ervices | SIP Traffic | SIP Trunks | Failove | Virtual P Netwo |
|---------------------------|---------------------|---------------------|--------------------------|-----------|----------------|---------------------|---------------|---------|--------------------|
| Networks and Computers | | All Interfaces N | IAT VLAN | Eth0 | Eth1 | Interface Status | | Tunnels | Topology |
| | | 4 Gatewa DNS | ays <u>(He</u> l Name | <u>(q</u> | IP | | _ | | Delete |
| Priority | Dynamic | or IP / | Address | 2 | Addre | ess | Interf | ace | Row |
| | - ~ | 10.0.0.1 | | 1 | 0.0.0. | 1 Out | side (et | th0) 🖂 | |

Figure 25

• Default Gateway is automatically populated as a consequence of the static route defined in eth0.

3.2.4 Configuring NAT

As the Ingate will be the default gateway for any device on the Inside (LAN), we will need to enable NATing in the Network section.

| dministration | Basic Configuration | rk Rules and Relays Se | SIP SI ervices Tro | SIP SI raffic Tru | IP nks Failover | Virtual Pri Networl | ivate Quality of Li rks Service an | About About | | | | |
|---------------------------|---|---------------------------|---------------------------|----------------------|--------------------|------------------------|---------------------------------------|-----------------------|-------------|----------------------|------------------------|-------------|
| Networks and Computers | Default All Gateways Interfaces | NAT VLAN EthO | | erface tatus PPA | PoE Tunnels To | opology | | | | | | |
| NAT | | | | | | | | | | | | |
| - | ckets that originate o be NAT:ed, as wel | | | From int | erface should | be NAT | Fied when they are | sent to a unit behind | the To int | erface. Optionally y | ou can also select spe | cific |
| Inerworks to | o de IVAL ed, as wel | | rom | | | | | То | | | | |
| | b be INAL.ed, as we | | rom | rk (optio | onal) | | | | vork (optic | onal) | NAT As (aptional) | Dele |
| No. | Interface | F DNS Name | rom Networl e or Ne | ietwork | • | Bits | Interface | Network DNS Name or | Network | | NAT As (optional) | |
| | Interface | F | rom Networl e or Ne | ietwork | | | | Net | Network | | | Dele Rot |
| | | F DNS Name | rom Networl e or Ne | ietwork | | | Interface Outside (ethi) 🗸 | Network DNS Name or | Network | | NAT As (optional) | |

Figure 26

3.3 Installing Certificate on Ingate Data Center

This section is already covered in section 2.1.3 (*Installing CA certificate on the* SIParator) and 2.1.4 (*Creating and Installing Server Certificates for SIParator*)

Certificates installed should look like this:

Server Signed Certificate:

| dministration Configu | | Rules and Relays Se | SIP SIP ervices Traffic | SIP Trunks Failo | ver Virtual P Netwo | | | ADOUT |
|---------------------------------------|--------------|-----------------------------|----------------------------|---|---|----------------|---|--------------------------|
| Basic Access Configuration Control | RADIUS SNMP | DHCP DHCP Options Server | | Router Advertisement | Dynamic DNS Update | Certificates T | LS Advanced | SIParator Type |
| Private Certifi | cates (Help) | | | | | | | |
| Name | | Certificat | te | 1 | | Inform | nation | |
| CA Signed TLS | Create New | Import | View/Downloz | siparator. Issuer: A /CN=Ing MD5 Fin SHA1 Fingerpu Valid fro Valid to: Subject? | loscasas.com/e C=US/O=Press ate System* gerprint: int: I m: 2017-08-0 2027-08-05 1- il(Name: email loscasas.com, Kev | 7 14:47:39 | rmesto@ingatu g/OU=Certific tte.com, DNS: | e.com ation Authority |

Figure 27

CA Certificate:

| Name | CA Certificate | CA CRL | Information | De R |
|---------------------|-------------------|-------------|--|---------|
| Ingate CA Certifica | Change/View | Change/View | Subject: /C=US/O=Presales Engineering/OU=Certification Authority /CN=Ingate Systems | |
| | | | Issuer: /C=US/O=Presales Engineering/OU=Certification Authority | |
| | | | /CN=Ingate System | |
| | | | MD5 Fingerprint: :A7 | |
| | | | SHA1 Fingerprint 14 C9B9 | |
| | | | Valid from: 2017-0 | |
| | | | Valid to: 2027-08- | |
| | | | Subject Key | |
| | | | ID: 6D:AE:2C:BD E | |
| | | | Authority Key | |
| | | | ID: 6D:AE:2C:BD E | |

Figure 28

3.4 Firewall Configuration - Rules and Relays

As we are using the Ingate SIParator in Firewall mode, a new tab in the GUI shows "Rules and Relays".

We configure not only basic Policies, but also Port Mapping, Relay and routing based on specific needs of the IPPBX platform.

Relay Rules depend on which IPPBX platform is adopted. In our case we use an Open Source platform for illustration purposes.

The following screenshots are specific to this IPPBX and explain what the reason for each relay Rule is.

Here we also use the names we defined in the Network section to point to a device, a subnet, or a group of subnets

Let's see first policy Rules:

| ministration | Bas Configu | ic ration Network | Rules and SIP Relays Services | SIP SIP Traffic Trunks | Failover Virtual Netw | Private Quality of Logging vorks Service and Tools | About | | | | | |
|----------------------|----------------|----------------------|----------------------------------|---------------------------|--------------------------|---|----------------|---------|---------------|-----------|---------|----------------|
| Jles Relays Rules | DHCP Relay | Services Protocols | Time Classes | | | | | | | | | |
| Rule No. | Active | Client | From IPsec Peer | Server | To IPsec Peer | Direction | Service | Action | Time Class | Log Class | Comment | t Delet Row |
| 1 | Yes Y | access ~ | - ~ | PrivateLan \vee | - ~ | Indeterminate interface -> Indeterminate interface | icmp/udp/tcp ~ | Allow 🗸 | 24/7 ~ | - ~ | | |
| 2 | Yes Y | PrivateLan 🗡 | • • | access | • ~ | Indeterminate interface -> Indeterminate interface (NAT:ed) | icmp/udp/tcp ~ | Allow ~ | 24/7 ∨ | - ~ | | |

Figure 29

- In this case, for simplicity, we permit flow between access network and the Inside (PrivateLan), for any ports (icmp/udp/tcp), (see *Networks and Computers*)
- Here you can be more specific and restrictive, limiting specific services, or even Time ranges.

Here we define relay Rules. The SIParator is a Full SIP Connect SIP Proxy and can detect and manage Signaling and Media according to the associated standards (i.e. RFC's, etc..). Also, all the firewall added features allows to manage and control any other traffic beyond VoIP. This is useful when other services are located behind the SIParator, not only as extended services in the IPPBX (Such as Collaboration Tools, Management, Provisioning, etc..), but also other services not associated to VoIP (Such as Web Services, ERP's, SQL, etc...).

In our case SIParator/Firewall will be the only NAT gateway available to the Private Lan, so we can limit inbound access and control outbound.

This screen shows ports necessary for IPPBX related services.

| Web Management | TCP Port: 80 |
|-------------------------|----------------------------------|
| Web Management (Secure) | TCP Port: 443 |
| UCP | TCP Ports: 81, 4443, 8001, 8003 |
| SIP Protocol | UDP Port: 5061 |
| CHAN_SIP Protocol | UDP Port: 5060 TCP Port: 5061 |
| IAX Protocol | UDP Port: 4569 |
| WebRTC | TCP Ports: 8088, 8089 |
| Extra Services | |
| Zulu UC | TCP Port: 8002 |
| XactView | TCP Ports: 58080, 55050 |
| HTTP Provisioning | TCP Port: 83 |
| HTTPS Provisioning | TCP Port: 1443 |
| OpenVPN Server | UDP Port: 1194 |
| REST Apps (HTTP) | TCP Port: 84 |
| REST Apps (HTTPS) | TCP Port: 3443 |
| ХМРР | TCP Port: 5222 |
| FTP | TCP Port: 21 |
| TFTP | UDP Port: 69 |

- We do not explain details about all these services.
- This is a list of needed ports as per the IPPBX specs and configuration
- Some are related to Provisioning such as TFTP and FTP, XMPP for instant messaging, etc..

| Here | 15 | how | this | 15 | included | in | SIParator | configuration |
|-------|----|--------|-------|----|----------|-----|------------|---------------|
| 11010 | 10 | 110 11 | criio | 10 | meradea | 111 | OII aracor | comgaration |

| Relays <u>(Help)</u> | | | | | | | | |
|----------------------|-----------|---------------------------|---------------|-------|---------------------|---------|------------|----------|
| Listen | To | Rela | ıy To | | | | Allow Acc | ess From |
| IP Address | Port | DNS Name or IP Address | IP Address | Port | Relay Type | Network | IPsec Peer | |
| eth0 (10.0.0.147) 🗸 | 21 | 10.0.1.149 | 10.0.1.149 | 21 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) ~ | 25 | 10.0.1.149 | 10.0.1.149 | 25 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) ~ | 69 | 10.0.1.149 | 10.0.1.149 | 69 | UDP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🗠 | 81 | 10.0.1.149 | 10.0.1.149 | 81 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🖂 | 83 | 10.0.1.149 | 10.0.1.149 | 83 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🗠 | 84 | 10.0.1.149 | 10.0.1.149 | 84 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🗠 | 1443 | 10.0.1.149 | 10.0.1.149 | 1443 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🗠 | 2001 | 10.0.1.149 | 10.0.1.149 | 2001 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🗸 | 3443 | 10.0.1.149 | 10.0.1.149 | 3443 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🖂 | 4343 | 10.0.1.149 | 10.0.1.149 | 443 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🖂 | 4443 | 10.0.1.149 | 10.0.1.149 | 4443 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🖂 | 5006 | 10.0.1.149 | 10.0.1.149 | 5006 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🖂 | 5007 | 10.0.1.149 | 10.0.1.149 | 5007 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🖂 | 5222 | 10.0.1.149 | 10.0.1.149 | 5222 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🖂 | 8001-8003 | 10.0.1.149 | 10.0.1.149 | | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) 🖂 | 8080 | 10.0.1.149 | 10.0.1.149 | 80 | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) < | 8088-8089 | 10.0.1.149 | 10.0.1.149 | | TCP port forwarding | ~ | access ~ | - |
| eth0 (10.0.0.147) ~ | 55050 | 10.0.1.149 | 10.0.1.149 | 55050 | TCP port forwarding | ~ | access | - |

- Here specific ports as per IPPBX specs are mapped from the Outside (10.0.0.147) to the IPPBX in the Inside (10.0.1.149).
- Note two ports that are mapped and changed from the origin (4343 \rightarrow 443, 8080 \rightarrow 80), this is to avoid conflict with ports already in use by the SIParator.
- Also, here we are allowing the mapping when originated from the Network named "access"; you can be restrictive and reduce the originator scope, however.

3.5 Sip Services

In this section we show configuration needed to accomplish our original goals. Let's review a simplified layout:

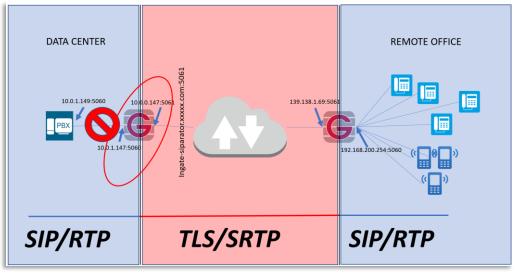


Figure 32

- Data Centre (DC) SIParator is represented on the left side
- Remote Office (RO) SIParator is on the right side
- All VoIP Traffic between IPPBX and DC SIParator, as well as between RO SIParator and endpoints will be SIP/RTP
- VoIP traffic crossing Internet is TLS/SRTP
- We use a domain (Ingate-SIParator.xxxxxx.com) for all registrations, and resolving to the Public IP on the DC SIParator

3.5.1 Basic configuration

Here follows basic information such as Transport Protocols, Ports, SIP destinations to monitor, etc.

Ensure the SIP Module is enabled, assign ports associated to SIP/UDP and SIP/TLS.

| | Quality of Logging About | |
|---|---|---|
| Signaling Media Sessions Remote SIP VolP VolP Survival Basic Encryption Interoperability and Media Connectivity Survival Status | | |
| SIP Module (Help) | | |
| Enable SIP module Disable SIP module | | |
| SIP Signaling Access Control (Help) | SIP Logging (Help) | |
| Specify the networks and computers from which the firewall accepts SIP Signaling. | Log class for SIP Log class for SIP signaling: packets: | |
| SIP Signaling Ports (Help) | Local V Log class for SIP Log class for SIP | |
| Delete | license messages: errors: | |
| Active Port Transport Intercept Comment Row | Local V Local V | |
| Yes 5060 UDP Yes Standard SIP port | Log class for SIP media Log class for SIP debu messages: messages: | g |
| Yes V 5061 TLS V Yes V Non Standard TLS port | Local V Local V | |
| Add new rows 1 rows. | Log class for SIP IDS/IPS: | |
| SIP Media Port Range (Help) | Local ~ | |
| Ports: 58024 - 60999 | Hide sensitive data: $\textcircled{\label{eq:sensitive}}$ Yes \bigcirc No | |
| Public IP Address for NATed firewall (Help) | SIP Servers To Monitor (Help) | |
| This setting is not supported for the Standalone configuration. DNS Name or IP Address IP Address | Server Port Transport Delete Row | |
| or IP Address | trunk1.freepbx.co | |
| | trunk2.freepbx.co(5060 UDP > | |
| | 10.0.1.149 UDP ~ | |
| | ingate.com | |
| | Add new rows 1 rows. | |

- Enable the SIP module to be able to configure all SIP associated attributes. In some cases, you might want to use Ingate as a Firewall only.
- In SIP Signaling access control you can limit SIP to specific networks. Here you can use Network Group Names defined previously.
- We will use 5060 and 5061 ports for SIP over UDP and TLS respectively.
- SIP Servers to monitor is an easy way to establish a permanent SIP ping (SIP OPTIONS packet) to confirm destinations are listening SIP. SIP Status tab will show the result of this monitoring.
- In our case, as SIParator is in the DMZ, with a dedicated Public IP address NAT 1-1, we need to manually add the FQDN or IP address. This will help in proper manipulation of headers when traversing the Firewall.

3.5.2 Signaling Encryption

As shown previously (see *Figure 32*) we will use TLS encryption for all signaling traffic crossing the Internet.

Here we show what needs to be setup. Notice we will use TLS certificates already created (See *Installing CA certificate on the* SIParator and *Creating and Installing Server Certificates for SIParator*).

| Administration Basic Configuration | Network Rules and Relays | SIP Services | SIP Traffic Tr | SIP runks | | al Private tworks | Qualit Servi | | | | |
|--|---|-------------------|---------------------------|-----------------|-------------------------|----------------------|-----------------|--|--|--|--|
| Basic Signaling Media Encryption Encryption | Interoperability and M | | | VoIP urvival | VoIP Survival Status | | | | | | |
| SIP Transport (Help) Enable signaling encryption Disable signaling encryption | | | | | | | | | | | |
| TLS CA Certificat | TLS CA Certificates (Help) Check Server Domain Match (Help) | | | | | | | | | | |
| CA Delete Row Check if the server domain matches the certificate: Ingate CA Certificate Image: Check if the server domain matches the certificate: Add new rows 1 | | | | | | | | | | | |
| TLS Connections C | On Different IP A | ddress | es <u>(Help</u> | 2 | | | | | | | |
| IP Address | Own Certificate | Use CN FQDN | Require Client Cert | • | TLS | | lete ow | | | | |
| eth0 (10.0.0.147) 🗸 | CA Signed TLS 🖂 | No 🖂 | No 🗸 | TLS | /1.x & SSLv3.(| | | | | | |
| Add new rows 1 rows. | | | | | | | | | | | |
| Making TLS Conn | Making TLS Connections (Help) | | | | | | | | | | |
| Default own certificate | | 3.0 🗸 | | | | | | | | | |

Figure 34

- Make sure Signaling Encryption is enabled
- Add to the TLS CA certificates Table, the CA Certificate we created before.
- Associate the Signed Certificate we created before to the Outside the Interface (eth0)
- Select TLS Protocol including TLSv1.x. SSLv3.0 adds additional backward compatibility with certain clients, although this is considered a security compromise as this protocol is broken (not recommended)
- Default own certificate can be left blank, or just use the same for any TLS connection in other IP addresses.

• Check Server domain match can be enabled if you want extra validation that Domain Matches with Certificate.

3.5.3 Media Encryption

As shown in the simplified diagram (see *Figure 32*), we enforce SRTP (Secure RTP) in media crossing the Internet.

| Administration | Basic Configuration | work Rules and SIP Relays Service | SIP SIP Traffic Trunks Failov | ver Virtual Priva Networks | | | | | | | |
|----------------|---|--------------------------------------|----------------------------------|-------------------------------|--|--|--|--|--|--|--|
| | Signaling Basic Media Encryption Media Interoperability Sessions and Media Remote SIP Connectivity VolP Survival Status | | | | | | | | | | |
| Media E | ncryption (He | <u>lp)</u> | | | | | | | | | |
| Enable | media encryptio | n | | | | | | | | | |
| O Disable | e media encryptic | n | | | | | | | | | |
| SIP Mee | dia Encryption | Policy (Help) | | | | | | | | | |
| No. | Media Network | Suite Requiremen | Allow | Delete Row | | | | | | | |
| 1 | Internet | SRTP | Yes V | Kow | | | | | | | |
| 2 | PrivateLan V | Cleartext | V Yes V | | | | | | | | |
| Add new r | ows 1 rows Encryption Po | | | | | | | | | | |
| Suite requ | irements: | Allow transcoding: | | | | | | | | | |
| Cleartext | ~ | ◉ Yes ○ No | | | | | | | | | |
| - | | | | | | | | | | | |
| | TLS (Help) | | | | | | | | | | |
| • | - | ptos but cleartext | | | | | | | | | |
| © D0 10 | Do not require TLS | | | | | | | | | | |
| RTP Pro | o file <u>(Help)</u> | | | | | | | | | | |
| ○ Prefer | ○ Prefer RTP/SAVP (sdescriptions) | | | | | | | | | | |
| | - | text and legacy encryp | | | | | | | | | |
| () Prefer | RTP/AVP (toget | her with sdescriptions |) | | | | | | | | |

- Enable media Encryption
- All traffic on the Internet will use SRTP and allow transcoding. It is important to consider the case when SIP trunks don't support SRTP and they are connected via the Internet you need to be specify destination networks where SRTP is not support and avoid overlapping.
- All traffic going to the PBX or Private Lan will be unencrypted (cleartext) and transcoding is allowed

• All remaining parameters can be left default.

3.5.4 Remote SIP Connectivity

Here we add all needed setup to enable remote endpoints to register and connect with SIParator and then the IPPBX.

Here we will adjust anything needed to prevent problems generated by NAT in the far end.

| dministration Basic Network Rules and Configuration Network Relays | H SIP SIP SIP SIP SIP Failover Virtual Pr Services Traffic Trunks Failover Networ |
|---|---|
| Signaling Media Basic Encryption Encryption Interoperability and | sssions Remote SIP VoIP VoIP Survival I Media <mark>Connectivity</mark> Survival Status |
| STUN Server (Help) C Enable STUN server Disable STUN server | |
| Remote NAT Traversal (Help) | |
| IP address for remote clients: IP port for remote clients: | Forward signaling from IP address: |
| NAT keepalive method: Use OPTIONS Use short registration times Use both OPTIONS and short registration times Use neither OPTIONS nor short registration times | Media Route: Route media directly between clients behind the same NAT Always route media through the firewall |
| NAT timeout for UDP: 20 seconds NAT timeout for TCP: | |
| 150 seconds Unconditional NAT Traversal (<u>H</u>) Always use Remote NAT Traversal Only use Remote NAT Traversal wh | |

Figure 36

- In our case we will not use STUN for NAT traversal. In most scenarios it isn't needed, and more relates to traversing local NAT when interchanging UDP traffic with remote devices
- We will, however, enable Remote NAT Traversal.
- Optionally, but not in our case, you can associate a different Interface and Port to listen for SIP from remote endpoints. This separates SIP listening from the standard port defined in SIP Basic Configuration

- When Possible, the SIParator can identify calls between endpoints behind the same NAT. Unless the IPPBX enforces SIP relay thru its Media server, this will allow to keep media traffic local between endpoints.
- Unconditional NAT traversal we use it only when endpoints are NATed.

3.5.5 VoIP Survival

This is one of the most valuable features included in the SIParator/Firewall. We enable it in the DC SIParator to provide a first level of survival if the IPPBX behind becomes unreachable.

We later do the same in the RO SIParator to provide also autonomous local Survival at the remote office.

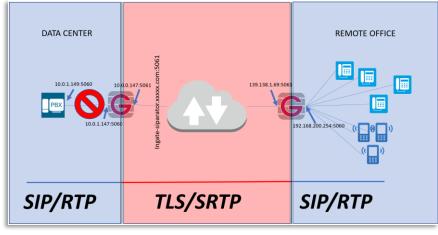


Figure 37

SIParator Survivability is unique compared with similar offerings in the market. Some of the reasons are:

- No extra configuration is needed in the endpoints. Other implementations require phones to use the SBC as a secondary Proxy/Registrar
- You control how and how long Authentication cache will be kept until IPPBX returns.
- You can route outbound calls from endpoints to failover devices (i.e. a Failover PSTN gateway)
- In the RO SIParator, you don't even need to configure any SIP additional features. Any SIP Traffic from registered endpoints traversing the SIParator/Firewall is automatically detected and logged to be able to manage any Proxy outage.
- You can define which Domains will be monitored and provided with Survival capabilities.
- More than one Domain can be managed at the same time in the same location. This is helpful in multitenant environments on Hosted PBX with more than one PBX.

| Basic | Signaling Encryption | Media Encryption | Interoperability | Sessions and Media | Remote SIP Connectivity | VolP Survival | VoIP Survival Status | | |
|-------|--|---------------------|------------------|-----------------------|----------------------------|------------------|-------------------------|--|--|
| ۲ | VoIP Survival (Help) Enable VoIP Survival Disable VoIP Survival | | | | | | | | |
| | Server Check Interval Domains To Monitor 40 seconds Domain Name Method Delete Row ingate-siparator Display name Image: Compared seconds Add new rows 1mm rows. | | | | | | | | |
| Re | Registrations Re-REGISTER interval during survival mode: Time to store subscriber data: 30 seconds 14 | | | | | | | | |
| P | STN Ga | teways | (Help) | | Numbers | (Help) | | | |
| Α | Domain Addre dd new row | ess | Delete Row | | | • | ne numbers | | |

Figure 38

- First enable VoIP Survival
- Define the check frequency (This value must be shorter than SIP Blacklist Interval in the Session and Media tab).
- Add the Domain name to check. You can add more domains if needed.
- Include registration frequency. This increases the registration frequency when in Survival mode. This helps to detect when service returns to normal operation quickly.
- Subscriber data can be kept for several days. This time should be decided based on your expectation of maximum time system could be down.
- The method to use in most cases is Display Name. This means that Subscriber data will be obtained from the Display Name in the SIP header.

3.6 SIP Trunks

In our exercise we have 3 ITSP's, wherein one of them has two destinations for failover.

We will use one of the most powerful and simplified features in Ingate SIParator/Firewall SIP Trunk pages.

A SIP Trunk Page defines a path that connects an ITSP with an IPPBX with specific configuration needs.

A single IPPBX could be the destination for several ITSP Trunks, and also the same ITSP Trunk can be used by more than one destination IPPBX (i.e. DID's define which IPPBX should receive the call).

Here we show only configuration for one of the SIP Trunks:

| inGate Firewall AWS In | gate 6.0.1GA 10.0.0.147 | Log Out |
|---|-------------------------|---|
| Administration Basic Configuration Network Relays Servic | - m - i Follover - i | Quality of Logging Service and Tools About |
| View trunk: SIP Trunk 1: Sipstation1; IPPBX 🗹 | Goto SIP Trunk page | |
| SIP Trunk 4 (Help) | | |
| Enable SIP Trunk | | |
| O Disable SIP Trunk | | |
| SIP Trunking Service (Help) | | |
| O Use parameters from other SIP trunk | | |
| Define SIP trunk parameters | | |
| Service name: | Sote | (Unique descriptive name) |
| Service Provider Domain: | | (FQDN or IP address) |
| Restrict to calls from: | . v | (-' = No restriction) |
| Outbound Proxy: | | (FQDN or IP address) |
| Use alias IP address: | | (Forces this source address from our side) |
| Outbound Gateway: | | ('-' = Use Default Gateway) |
| Signaling Transport: | | ('-' = Automatic) |
| Port number: | | ·, |
| From header domain: | Provider domain V | |
| Host name in Request-URI of incoming calls: | | (Trunk ID - Domain name) |
| Remote Trunk Group Parameters (RFC 4904): | | |
| Used as: | • V | ('-' = Don't use TGP) |
| Local Trunk Group Parameters (RFC 4904): | | |
| Used as: | • · | ('-' = Don't use TGP) |
| Preserve Max-Forwards: | No 🗸 | |
| Relay media: | No 🗠 | |
| Exactly one Via header: | No 🗸 | |
| 'gin' registration (RFC 6140): | No 🗸 | |
| Hide Record-Route: | No 🗸 | |
| Show only one To tag: | No 🗸 | |
| SIP 3xx redirection to provider domain: | No 🗸 | |
| SIP 3xx redirection to caller domain: | No | |
| Route incoming based on: | To header V | |
| Service Provider domain is trusted: | No 🗸 | (For P-Asserted-Identity) |
| Use P-Preferred-Identity: | No 🗸 | (Instead of P-Asserted-Identity) |
| Forward outgoing REFER: | No 🗸 | |
| Max simultaneous calls: | | (Call Admission Control) |
| Max simultaneous calls per Trunk Line: | | |

Figure 39

Previous figure corresponds only to the ITSP side of the Trunk Page.

• This Trunk Page associates a carrier trunk named "Sotel" with the IPPBX in the Private Subnet. Use the "help" link to get a full explanation for each parameter

- You should adjust parameters and interop attributes based on your ITSP requirements.
- You can control for example maximum simultaneous calls in the SIP trunk or limit per Trunk Line (A trunk Line in this case could be a DID)

Outgoing Calls are sent to a specific SIP Trunk page via Forward to in the Dial Plan. The from header in an outgoing call is searched for a match in the Dial Plan page Fromcolumns.

Incoming Calls from the ITSP are first scanned through the Incoming Trunk Match columns and only sent to the Dial Plan if no match is found.

Use "Help" links to obtain detailed information.

| Mai | n Trunl | k Line (Help) | | | | | | | | |
|-----|---------|----------------------|--------------------------|----------------------|-----------------------|------------------|------------------------|--------------------------------|---------------------------------------|---------------|
| | Reg | | Outgoing | g Calls | | Authe | ntication | Incoming | g Calls | |
| | Keg | Enable | Display Name | User Name | Identity | User ID | Password | Incoming Trunk Match | Forward to | |
| 1 | Yes ~ | registartion | | 0291 A | attributes | 0291 | Change Password | | | |
| _ | | | | | | | | - | | |
| PBX | Lines | (Help) | | | | | | | | |
| | | THEFT | | | | | | | | |
| | | | Outgoing | g Calls | | Authe | entication | Incomi | ng Calls | Date |
| No. | Reg | From PBX Number/User | Outgoing Display Name | g Calls User Name | Identity | Autho User ID | entication Password | Incomi Incoming Trunk Match | ng Calls Forward to PBX Account | Delete Row |
| No. | | | | , | Inbound DID rounting. | | | | Forward to PBX | |
| | Reg | | | , | | | Password | Incoming Trunk Match | Forward to PBX Account | Row |

Figure 40

- If the SIP Trunk requires implicit registration you need to enable it here
- You can load Authentication credentials that will be used for registration and call authentication challenges
- Incoming DID's can be routed to specific UA inside the IPPBX

| Setup for the PBX (Help) | | | | | |
|---|----------------------|--------------------------|---------------------------|--------------|--|
| Use PBX from other SIP trunk Define PBX settings PBX Name: | from | | defined in anoth age | | |
| | | nique descriptive name, | | | |
| Use alias IP address: | (Fe | orces this source addres | s from our side) | | |
| | Aut | hentication | PBX IP A | ddress | |
| PBX Registration SIP Address | Address User ID F | | DNS Name or IP Address | IP Addres | PBX Domain Name |
| | | Change Password | 10.0.1.149 | 10.0.1.149 | |
| (At least one of PBX Registration, IP a | ddress or Dom | ain Name is required to | locate the PBX) | | |
| PBX Network: Signaling transport: Port number: | IPPBX UDP 5060 | | ('-' = Auto | omatic) | IPPBX IP Address located in the Private subnet |
| Match From Number/User in field | : From (| JRI | ~ | | |
| Common User Name suffix: | | | | _ | |
| To header field: | A me | as Request-URI 🗸 | | | Adjust Parameters accordingly to the |
| Forward incoming REFER: | No ~ |] | | 1 | PPBX requirements |
| Remote Trunk Group Parameters v | usage: - | | | ı't use TGP) | |
| Local Trunk Group Parameters us | age: - | | ✓ ('-' = Dor | i't use TGP) | |

Figure 41

• Here you associate a new PBX to the Trunk Page or refer to an existing PBX.

- Configure the PBX IP address. In our case, 10.0.1.149 is located in the Private Subnet
- Complete the remaining parameters associated with the IPPBX. In our case, using an Open Source PBX, default values will be enough.

You can repeat similar steps for the remaining SIP Trunk pages.

For detailed explanation of SIP Trunking *see <u>Sip Trunking Configuration using the</u> <u>SIP Trunk Page</u>*

3.7 SIP Traffic

In this section, we address specifics related to Call Control and Call Flow.

SIP (Session Initiation Protocol) is a protocol for creating and terminating various media stream sessions over an IP network. It is for example used for Internet telephone calls and distribution of video streams.

SIP takes care of the initiation, modification and termination of a session with one or more participants. The protocol makes it possible for the participants to agree on what media types they should share. You can find more information in RFC 3261.

These SIP functions are configured in the SIP Traffic section:

- Allowed SIP methods
- Filtering of SIP signaling
- Local SIP domains
- SIP users
- SIP user authentication
- RADIUS accounting for SIP
- Routing of outgoing SIP requests
- Routing of incoming SIP requests
- SIP IDS/IPS

We address only the ones that define call behavior and add value to secure the service

3.7.1 Allowed SIP Methods

This section allows us to control, limit and restrict all SIP traffic to a specific set of Methods. In our case we leave it with default values.

Incoming SIP packets are matched on Method and Traffic to. Select in the "Allow" column whether the Firewall should process the packet.

Choose in the Auth column whether processing the packet should require authentication.

| Administratio | | | Network Ru R | | | _ | SIP Trunks | Failove | r Virt N |
|----------------|--------|--------------------|----------------------------------|----------|--------------|--------------|---------------|---------|-----------------|
| Logged in | as adm | in (Full A | Access) using | local pa | sswoi | r d . | | | |
| SIP Methods | | Local Registrar | Authentication and Accounting | | Dial Plan | | SIP Status | IDS/IPS | IDS/IF Statu |

SIP Methods (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated a SIP RFC.

| Method | Traffic To | Allow | Auth | Delete Row |
|-----------|------------|---|-------|------------|
| BYE | Both ~ | Yes $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $ | No 🗠 | |
| FEATURE | Both ~ | Yes ~ | No 🗠 | |
| INFO | Both ~ | Yes \vee | No 🗠 | |
| INVITE | Both ~ | Yes ~ | No ~ | |
| MESSAGE | Both ~ | Yes $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $ | No 🗠 | |
| NOTIFY | Both ~ | Yes ~ | No 🗠 | |
| OPTIONS | Both ~ | Yes \vee | No 🖂 | |
| PRACK | Both ~ | Yes ~ | No ~ | |
| PUBLISH | Both ~ | Yes $\scriptstyle{\scriptstyle \lor}$ | No 🗠 | |
| REFER | Both ~ | Yes 🗠 | No 🕑 | |
| REGISTER | Both ~ | Yes 🗵 | Yes 🗸 | |
| SERVICE | Both ~ | Yes ~ | No ~ | |
| SUBSCRIBE | Both ~ | Yes 🖂 | No 🗠 | |
| UPDATE | Both | Yes ~ | No 🕑 | |

Figure 42

3.7.2 Filtering

Under Filtering, you can filter out SIP requests based on various criteria. Filter based on sender IP address (Sender IP Filter Rules), sending and receiving SIP user (Header Filter Rules), or content type (Content Types).

| SIP ethods Filte | | Authentication and Accounting | SIP Accounts | Dial Plan | Routing | SIP Status | IDS/IPS | IDS/IPS Status | SIP Test | SIP Test Statu |
|---------------------|-----------------|----------------------------------|-----------------|--------------|---------|---------------|---------|-------------------|-------------|-------------------|
| Sender] | IP Filter Rul | es <u>(Help)</u> | | | | | | | | |
| No. | From Network | Action | Del Ro | | | ault P | • | or SIP | Rec | quests |
| 1 | ІРРВХ | Process all | <u> </u> | | | ocal o | | | | |
| 2 | PrivateLan ~ | Process all | <u>~</u> 🗆 | | | leject a | | | | |
| 3 | SipTrunk | Process all | <u> </u> | | | | | | | |
| 4 | ingate ~ | Process all | <u> </u> | | | | | | | |
| 5 | Office | Process all | <u> </u> | | | | | | | |
| Add new r | rows 1 roy | | | | | | | | | |

Figure 43

- Sender IP Filter allows to limit SIP traffic only from the networks listed. You can Allow or restrict based on the "Action". The choices are **Process all**, which handles all requests regardless of destination, **Local only**, which only handles requests to **Local SIP Domains** (entered on the **Local Registrar** page), and **Reject all**, which doesn't handle any requests at all.
- Define a Default policy that will apply to any traffic not covered by the rules. In our case we will reject any other traffic.

| Preloaded Route Rules (Help) | |
|------------------------------------|---|
| No. From Network Action Delete Row | Default Policy For Preloaded Routes |
| Add new rows 1 rows. | Reject Authenticate Remove Allow |

Figure 44

• By default, the unit rejects preloaded routes that do not point to itself. However, certain scenarios may require a preloaded route set.

| Block SIP Traffic to N | ATed Netwo | rks <u>(Help)</u> | |
|--|---------------------|-------------------|------------------------------|
| Allow SIP traffic direc | tly to NATed 1 | tworks | |
| Block SIP traffic direct | tly to NATed M | Vetworks | |
| Policy for Signaling an | d Modia on | different Net | vorks (Help) |
| Allow Signaling and M | | | WOLKS (Help) |
| Reject Signaling and N | | | |
| | | | |
| Content Type Filter R | ules (<u>Help)</u> | | |
| ~ * | Delete Row | | |
| */* Yes ~ | | | |
| application/SOAF No < | | | |
| application/adrl+: No 🗸 | | | |
| application/pidf+ No 🗸 | | | |
| application/vnd-r No 🗸 | | | |
| application/vnd-r No 🗸 | | | |
| application/vnd-r No 🗸 | | | |
| application/xml Yes > | | | |
| image/jpeg Yes 🗸 | | | |
| message/sipfrag No 🗸 | | | |
| text/html No 🗸 | | | |
| text/lpidf No 🗸 | | | |
| text/plain No 🗸 | | | |
| text/xml Yes 🗸 | | | |
| text/xml+msrtc., Yes 🗸 | | | |
| text/xml+msrtc.v Yes 🗸 | | | |
| Add new rows 1 row | s. | | |
| | | | |
| To/From Header Filte | r Rules (Hel | <u>b)</u> | |
| No. From Header To H | eader Action | Delete Row | Default Header Filter Policy |
| Add new rows 1 row | VS | | Process |
| 100 1010 1010 1 | | | ○ Reject |



- Our SIParator is in a DMZ and is NATed behind the Public IP. Traffic coming NATed not from the Public IP is considered suspicious.
- As some ITSPs may use separated OIP's for Signaling and Media we enable Signaling and Media from different IP's.
- Based on the content type header we are able to filter certain content type. Here, the firewall will only permit SIP packets that have one of the content types (MIME types) listed below. Please note that SIP packets with the content types "application/sdp", "application/xpidf+xml" and "text/xmsmsgsinvite" are always forwarded, as well as SIP packets without a body.
- The To/From header filter is useful if we want to be even more specific in restricting traffic to only those requests where we know From and/or To Header information or patterns. In our case we will not put any restriction here and make the default rule just to Allow

3.7.3 Routing

Here, you configure routing of the SIP signaling received by the unit. The options are: to forward all SIP requests to a server, regardless of what they concern (**Outbound Proxy**), to forward requests to a specific user to other users as well (**Static Registrations**), and to forward all requests addressed to a specific SIP domain to a SIP server (**DNS Override For SIP Requests**).

You can also:

- Configure how incoming calls for local SIP users should be processed. You can restrict allowed callers and send the calls on to a voice mail server.
- Select to process 3xx class messages in the unit or pass them on to the client.
- You can configure the order between some SIP routing functions. For most standard setups this is not needed, but special complicated scenarios may require a change of order.

| Administra | | Basic figuration | | es and elays | SIP Services | SIP Traffic | SIP Trunks | Failover | | al Priva tworks | | luality of Service | Logging and Tools | About |
|----------------|--|---------------------|-------------------------------|-----------------|-----------------|----------------|---------------|----------|-------------------|--------------------|-----|-----------------------|----------------------|----------------|
| SIP Methods | Filtering | Local Registrar | Authentication and Accounting | SIP Account | Dial s Plan | Routing | SIP Status | IDS/IPS | IDS/IPS Status | | - | IP Status | | |
| DNS | Overri | de For | SIP Reques | ts <u>(He</u> l | <u>lp)</u> | | | | | | | | | |
| | or IP Address Address Port Transport Priority Weight Auth RI | | | | | | | | | | | | | |
| | Domain | | | | | | Port | Trans | port | Priori | ity | Weight | Auth | Modify RURI |
| 🛨 ing | ate-sipar | ator.lo | 10.0.1.149 | | 10.0.1 | .149 5 | 060 | UDP | <u>~</u> [| | | | No 🗸 | Yes 🗸 |
| Add ne | ew rows | 1 gr | roups with 1 | fow | s per g | roup. | | | | | | | | |
| SIP | Routing | , Order | (Help) | Clas | s 3xx | Messa | ige Pro | cessing | g <u>(He</u> | <u>(ql</u> | | | | |
| N | o. R | outing I | Function | • F | orward | all | | | | | | | | |
| 1 | D | NS Ove | rride | O Fe | ollow r | edirect | s | | | | | | | |
| 2 | D | ial Plan | | | | | | | | | | | | |
| 3 | L | ocal Reg | gistrar | | | | | | | | | | | |



- DNS Override will be the key functionality to be able to route inbound requests from remotes using a specific domain and translate to the local SIP Proxy responsible. In our case any request to Ingate-SIParator.xxxxxx.com will be routed to the IPPBX in 10.0.1.149.
- Authentication will not be done by the SIParator, but delegated to the IPPBX
- Request-URI will be modified according to the forwarded destination
- We will also have an order on how SIP requests will be routed. First it will be checked if DNS Override has a destination for the Domain. Second the Dial Plan will be tried, and if no match is found it will be checked if the destination is locally registered.

For our case, we will leave the remaining parameters with default values.

3.7.4 Dial Plan

At this point it is important to understand:

- Inbound calls from ITSP's are routed automatically using the SIP Trunk Page Dial Plan for the corresponding Sip Trunk
- Calls from Remote extensions, will be routed to the PBX as per DNS Override
- Calls to Remote extensions, as Registrations authenticated by IPPBX are kept in SIParator, match the Local Registrar and are forwarded to the Known AOR
- Outbound calls to PSTN, from IPPB will be treated in the Dial Plan we present here

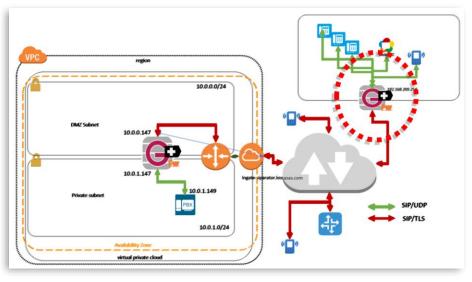
We expect to receive INVITES from the PBX with a prefix (90, 91, 92) to indicate which ITSP will be used.

|) On | | 911 | | | | | | | |
|--|-------------------------------------|----------------|---------------------|-----------|------------|-------------------|-----------------------|--------------|------------|
|) Off) Fallback | | | | | | | | | |
| - | | | | | | | | | |
| Matching Fro | | | 0.771 | | | | | | |
| Name | Username | This Domain | Or This Reg Expr | Transpo | rt Network | Delete Row | | | |
| IPPBX | * | 10.0.1.149 | | UDP | V IPPBX | | | | |
| | | | | | | | | | |
| Add new rows | 1 rows. | | | | | | | | |
| Matching Re | quest-URI | (Help) | | | | | | | |
| Name | | | Use This | | | Or This | Delete Row | | |
| | Prefix | Head | Tail | Min. Tail | Domain | Reg Expr | Delete Now | | |
| Outbound_Inga | | | 09, +, -, #, * ~ | | 10.0.1.147 | | | | |
| Outbound_Sips | 91 | | 09, +, -, #, * | | 10.0.1.147 | | | | |
| Outbound_Sote | 92 | | 09, +, -, #, * > | | 10.0.1.147 | | | | |
| Add new rows | | | | | | | | | |
| Rud new rows | I IOWS. | | | | | | | | |
| Forward To | (Help) | | | | | | | | |
| Name | No. Use | This | Or This | | Or This | | Or This | Use Alies IR | Delete Row |
| | A | | ement Domain P | | t Reg Expr | | Trunk | | |
| Sipstation | 1 - | | | - · | | | 1: Sipstation1; IPPBX | | |
| | 2 - | | | - × | | | 2: Sipstation2:IPPBX | | |
| | 1 | | | - ~ | | | 3: ingate;IPPBX | | |
| * ingate | | | | - V | | SIP Trunk | 4: Sotel;IPPBX | | |
| + ingate + sotel | | | | | | | | | |
| | | | per group. | | | | | | |
| * sotel | 1 - | | per group. | | | | | | |
| * sotel | 1 - | | per group. | | μ <u></u> | | | | |
| * sotel Add new rows Dial Plan (H | 1 groups | with 1 rows | | | Forward To | Add Pr | ENUX | f Root Time | |
| * <mark>sotel</mark> Add new rows Dial Plan (H No. Fr He | 1 groups elp) ader | with 1 rows | Ac | tion | Forward To | Add Pr Forward | ENUM | I Koot Class | |
| * <mark>sotel</mark> Add new rows Dial Plan (H No. Fr He | 1 groups elp) ader BX Outb | with 1 rows | Ac Forward | tion | sotel | | ENUX | | |



- First make sure Dial Plan is enabled
- There are 2 matching criteria that could be combined
 - Matching from header: match Network (IPPBX), Protocol (UDP) and domain (10.0.1.149)
 - Matching Request-URI: one match per prefix (90, 91 and 92) as well as the IP address (10.0.1.147)
- We created 3 main routing rules (Forward to), for each ITSP. Note one of the rules has 2 hunting rules, as this ITSP provides two destinations for fail over
- Finally, the dial plan table has one routing rule for each matching combination of "From Header" and "Request URI". Here is where the call is routed to the specific Trunk based on the dialed prefix.

This completes all that is needed in the Data Centre (DC) SIParator and in the next section we show what is needed in the remote office (RO SIParator)



4 Ingate Remote Office Node Configuration



Now we will focus on the Ingate Device (SIParator/Firewall) to be installed in the remote office where several endpoints will be used.

We assume the Ingate SIParator is the main router/firewall installed behind the Network access device (Carrier Modem). This is way, Topology for this device will be WAN (Public IP address will be in the Outside Interface). It can also be implemented in other topologies, but when used as WAN or any DMZ option, you will get several added value functionalities, and will simplify deployment.

In our case, SIParator/Firewall will also be the Default gateway for the remote office network (Or at least for all VoIP devices).

4.1 RO Basic Configuration

Here we show configuration relevant to this deployment. Sections not relevant for specific configuration are not shown.

For reference, we use eth0 as the Inside Interface and eth1 as the Outside.

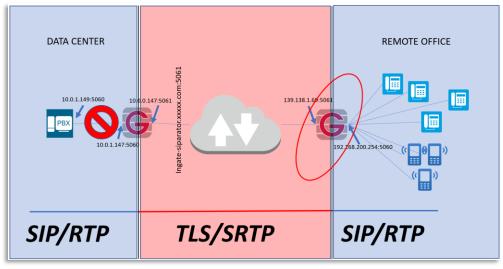


Figure 49

A summary on how the Network has been configured here:

| | rview | | | | | | | | | |
|-----------------|----------------|-----------------------------------|------------------|----------------|--------------------------|----------------------------|------------------------|------------|--------------|--|
| General | | | | | | | | | | |
| Physical Device | Interface Name | Active | Speed and Duplex | | | | | | | |
| eth0 | inside | Yes 🗸 | Autonegotiation | ~ | | | | | | |
| eth1 | outside | Yes 🗸 | Autonegotiation | \sim | | | | | | |
| eth2 | Ethernet2 | No 🗸 | Autonegotiation | \sim | | | | | | |
| eth3 | Ethernet3 | No 🗸 | Autonegotiation | <u> </u> | | | | | | |
| Directly Conne | cted Networks | (Help) | | | Network | Broadcast | Interface or Tunnel | VLAN Id | VLAN Name | |
| Name | Address | DNS Na or IP Add | TP Addres | Netmask / Bits | Address | Address | | | | |
| • | Туре | DNS Na or IP Add 2.168.200. | dress IP Address | Netmask / Bits | Address 192.168.200.0 | Address 192.168.200.255 | | | - | |

Figure 50

4.1.1 DHCP Server

As you use SIParator/Firewall as the Default gateway and the main router for the outside, you may also enable it as the DHCP Server for the network.

| Enable DHC | | | | | | | | |
|---|---|-----------------|---------------------------|--------------|------------|----------------|---------------------------|-----------------|
|) Disable DHC | | | | | | | | |
| Domain | main Client Lease Time (Help) | | | | | | | |
| | Minimum | | | | | | | |
| | | 43200 second | - | | | | | |
| | Maximum | 86400 second | s | | | | | |
| IP Ranges (I | Help) | | | | | | | |
| | | IP Range | (lower limit) | IP Ra | ange (uppe | er limit) | Gate | way |
| Listen | ı To | DNS Name | IP Address | DNS Na | | IP Address | DNS Name or IP Address | IP Address |
| inside (eth0 unt | agged) 🗸 | 192.168.200.210 | 192.168.200.210 | | | 92.168.200.250 | 192.168.200.254 | 192.168.200.254 |
| inside (euro diri | | | | | | | | |
| | | | | | | | | |
| Add new rows | 1 rows. | | | | | | | |
| | 1 rows. | | | | | | | |
| Add new rows | 1 rows. (<u>Help)</u> | DNS Servers | | | | _ | | |
| Add new rows | 1 rows. (Help) vers: Manual | | DNS Name or IP Address | IP Address 1 | Delete Rov | v | | |
| Add new rows DNS Servers Lssign DNS ser | 1 rows. (<u>Help</u>) vers: <u>Manual</u> n No | | | | Delete Row | v | | |
| Add new rows DNS Servers Lssign DNS ser Auto Assig Manual | 1 rows. (<u>Help)</u> vers: <u>Manual</u> n | Dynamic | | * | _ | r V | | |

Figure 51

- Make sure DHCP Server is enabled
- DHCP Requests will be listened for on the Inside, and a range of IP's are assigned.
- DNS will be used from the Carrier and Google DNS is additional.
- More advanced features can be used, including DHCP Options management, but it is not part of this material.

4.1.2 SIParator Type

In our case Firewall mode will be enabled and topology WAN.

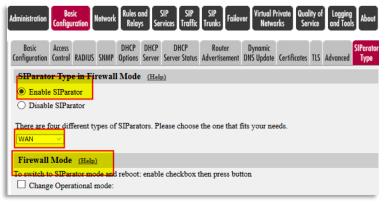


Figure 52

4.2 RO Network configuration

4.2.1 Networks and Computers

Besides the default LAN and WAN Networks we add one name which points to the domain that we use for our case ("Ingate-SIParator.xxxxxx.com); it is a FQDN resolving to the Public IP address of DC SIParator/Firewall

| ninistration Basic | ntion Network Rules Rela | | SIP runks Failover Virt N | ual Private Quality of l letworks Service a | agging nd Tools | | | | | |
|---|---|---------------------------|---------------------------------|--|--------------------|-------------------------|-----|--|--|--|
| etworks and Computers Gateways Networks and C | Amputers Gateways Interfaces NAT VLAN Eth0 Eth1 Eth2 Eth3 Status PPPoE Tunnels Topology | | | | | | | | | |
| Name | Calana | Lower | Limit | Upper (for IP r | | Interface/VLAN | Del | | | |
| Name | Subgroup | DNS Name or IP Address | IP Address | DNS Name or IP Address | IP Address | Interface/vLAIN | Ro | | | |
| 1 LAN | | 192.168.200.0 | 192.168.200.0 | 192.168.200.255 | 192.168.200.255 | inside (eth0 untagged) | ~ 🗆 | | | |
| 🛨 PBX | | | | | | | | | | |
| + WAN |] | 0.0.0.0 | 0.0.0.0 | 255,255,255,255 | 255.255.255.255 | outside (eth1 untagged) | | | | |

Figure 53

• Add PBX name using DC SIParator domain.

4.2.2 NAT configuration

As SIParator/Firewall will be the NAT device for this network we configure NATing:

| istration Configuration Network Rules and SIP SIP SIP Failover Virtual Private Quality of Logging About Service Configuration About | | | | | | | | | |
|---|---|--------------------------------|-----------------------------|--------------------|-------------------------|--------------------------------|-----------------------------|-----------------------|---|
| works and Default All Interfaces Interfaces Interfaces Interface PPPoE Tunnels Topology | | | | | | | | | |
| | | | | | | | | | |
| AT | AT ect if packets that originate from a unit behind the From interface should be NAT:ed when they are sent to a unit behind the To interface. Optionally you can also select specific networks to be | | | | | | | | |
| ect if pack | | n a unit behind the Fr | rom interfac | e should be NAT:ed | when they are sent to a | a unit behind the To ir | iterface. Op | tionally you can also | select specific networks to |
| ect if pack | kets that originate fror e address to use. | n a unit behind the Fr | rom interfac | e should be NAT:ed | when they are sent to a | a unit behind the To ir | iterface. Op | tionally you can also | select specific networks to |
| ect if pack | | n a unit behind the Fr From | rom interfac | e should be NAT:ed | when they are sent to a | a unit behind the To ir To | nterface. Op | tionally you can also | select specific networks to |
| lect if pack well as the | | From | rom interfac work (optio | | when they are sent to a | То | nterface. Op work (optio | | - |
| ect if pack | | From | work (optio Network | | when they are sent to a | То | • | | select specific networks to NAT As (optional) |

Figure 54

4.3 Installing Certificate on Ingate Remote Office

Here, as explained previously, we will need to have CA certificate loaded as well as a specific client certificate for this device.

Refer to the following sections to do this:

• Installing CA certificate on the SIParator

```
Educronix LLC
```

• Creating and Installing Server Certificates for SIParator

4.4 RO Firewall Configuration - Rules and Relays

We allow freely traffic WAN $\leftarrow \rightarrow$ LAN. It can be adjusted to specific needs depending on the real-world scenario.

| ninistration | Basic Configuratio | n Network Rules Rela | and SIP SIP SIP S ys Services Traffic Tru | IP Inks Failover Virtu Ne | al Private Quality of Log tworks Service and | aging Tools About | | | | | |
|--------------|-----------------------|-------------------------|--|---------------------------------|---|-------------------------------|-----------------|---------|---------------|-----------|---------|
| | OHCP Lelay Servi | ces Protocols Classe | | | | | | | | | |
| Rule No. | Active | Client | From IPsec Peer | Server | To IPsec Peer | Direction | Service | Action | Time Class | Log Class | Comment |
| 1 | Yes \vee | LAN ~ | • | WAN | | inside -> outside (NAT:ed) | icmp/udp/tcp <> | Allow 🗸 | 24/7 ∨ | - × | |
| 2 | Yes 🗸 | WAN ~ | - · · | LAN ~ | - ~ | outside -> inside | icmp/udp/tcp ~ | Allow ~ | 24/7 ~ | - ~ | |

Figure 55

4.5 RO SIP Services

4.5.1 Basic configuration

| Administration Basic Network Rules and SIP SIP SIP Traffic Failover Virtual Private Networks | Quality of Logging Service and Tools About |
|---|---|
| Signaling Media Sessions Remote SIP VolP VolP Survival Basic Encryption Interoperability and Media Connectivity Survival Status | |
| SIP Module (Help) Enable SIP module Disable SIP module | |
| SIP Signaling Access Control (Help) | SIP Logging (Help) |
| Specify the networks and computers from which the firewall accepts SIP Signaling. SIP Signaling Ports (Help) Active Port Transport Intercept Comment Row | Log class for SIP Log class for SIP signaling: packets: Local Local Log class for SIP Log class for SIP license messages: errors: Local Local Log class for SIP Log class for SIP license messages: errors: Local Local Log class for SIP media Log class for SIP debug |
| Yes 5060 UDP and TCP Yes Standard SIP port Yes 5061 TLS Yes Standard TLS port Add new rows 1 rows. | messages: messages: Local Log class for SIP IDS/IPS: Local Local Local |
| SIP Media Port Range (Help) | Hide sensitive data: Yes No |
| Ports: 58024 - 60999 Public IP Address for NATed firewall (Help) | SIP Servers To Monitor (Help) |
| This setting is not supported for the Standalone configuration. | Server Port Transport Row |
| DNS Name or IP Address | Add new rows 1 rows. |

Figure 56

- Make sure the SIP Module is enabled
- Make sure SIP/UDP and SIP/TLS are defined as valid signaling ports
- Add your domain as a SIP Server to monitor

4.5.2 Signaling Encryption

| Administration Basic Configuration | Network Rules and Relays | SIP Services Traffi | SIP Trunks Fa | ilover Virtual Privi Networks | |
|--|------------------------------|------------------------------|------------------|----------------------------------|---------------|
| Basic Signaling Media Encryption Encryption | Interoperability and M | | | oIP Survival Status | |
| SIP Transport (Hell Enable signaling en Disable signaling en | cryption | | | | |
| TLS CA Certificat | es <u>(Help)</u> | Check Se | rver Doma | in Match (H | <u>elp)</u> |
| CA Ingate CA Certificate Add new rows 1 | Delete Row | Check if the certificate: | | ain matches the | |
| TLS Connections (| On Different IP A | ddresses (1 | <u>Help)</u> | | |
| IP Address | Own Certificate | Use Req CN Cli FQDN Ce | ent | TLS | Delete Row |
| eth0 (10.0.0.147) 🗸 | CA Signed TLS 🖂 | No 🗸 No | TLSv1 | .x & SSLv3.0 🖂 | |
| Add new rows 1 | rows. | | | | |
| Making TLS Conn | ections <u>(Help)</u> | | | | |
| Default own certificate | : Use TLS: TLSv1.x & SSLv | 3.0 ~ | | | |

Figure 57

- Make sure Signaling Encryption is enabled
- Add to the TLS CA certificates Table, the CA Certificate we created before.
- Associate the Signed Certificate we created before to the Outside the Interface (eth1)
- Select TLS Protocol including TLSv1.x. SSLv3.0 will add additional backward compatibility with certain clients. (SSL is no longer recommended)
- Default own certificate can be left blank, or just use the same for any TLS connection in other IP addresses.
- Check Server domain match can be enabled if you want extra validation that Domain Matches with Certificate.

4.5.3 Media Encryption

As shown in the simplified diagram (see *Figure 32*), we will enforce SRTP (Secure RTP) for media crossing the Internet.

| Signaling Basic Encryption | | Sessions and Media | | | VoIP Sur Statu | | | | |
|-------------------------------|------------------------------------|-----------------------|--------------|-------|-------------------|--------|--|--|--|
| Media End | Media Encryption (Help) | | | | | | | | |
| Enable n | nedia encryption | | | | | | | | |
| O Disable r | media encryption | | | | | | | | |
| | | | | | | | | | |
| SIP Medi | SIP Media Encryption Policy (Help) | | | | | | | | |
| | •• | • | | | | | | | |
| N | Media | Contro Decord | | All | ow | Delete | | | |
| No. | Media Network | Suite Requi | rements | | ow coding | | | | |
| No. | | Suite Requi | rements ~ | | coding | | | | |
| No. | Network | - | | Trans | coding | | | | |

Figure 58

- Enable media Encryption
- All traffic via the Data Centre (IPPBX) uses SRTP and transcoding.
- All traffic going to the endpoints or LAN will be unencrypted (cleartext) and transcoding is allowed
- All remaining parameters can be left default.

4.5.4 Remote SIP Connectivity

As we don't need to provide remote access to local SIP services from the outside we disable everything here.

| Basic | Signaling Encryption | Media Encryption | Interoperability | the second s | VoIP Survival Status |
|-------|-------------------------|---------------------|--------------------|--|-------------------------|
| ST | UN Serv | er <u>(Help</u> |) | | |
| 0 | Enable SI | TUN serve | er 🔤 | | |
| ۲ | Disable S | TUN serv | er | | |
| Re | emote NA | T Trave | rsal <u>(Help)</u> | | |
| 0 | Enable R | emote NA | T Traversal | | |
| ۲ | Disable R | lemote NA | AT Traversal | | |
| Sav | e Undo |] | | | |

Figure 59

4.5.5 VoIP Survival

This is one of the most valuable features included with SIParator/Firewall. We enable it on the RO SIParator to provide a second level of survival if the Data Centre becomes unreachable

We previously did the same in the DC SIParator to provide an additional survival level.

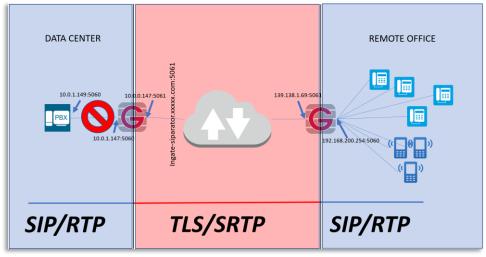


Figure 60

SIParator Survivability is unique compared with similar offerings in the market. Some of the reasons are:

- No extra configuration is needed in the endpoints. Other implementations require phones to use the SBC as a secondary Proxy/Registrar
- You can control how and how long Authentication cache is kept until IPPBX returns.
- You can route outbound calls from endpoints to failover devices (i.e. a Failover PSTN gateway)
- In the RO SIParator, you don't even need to configure any SIP additional features. Any SIP Traffic from registered endpoints traversing the SIParator/Firewall is automatically detected and recorded to be able to manage any Proxy outage.
- You can define which Domains will be monitored and provided with Survival capabilities.
- More than one Domain can be managed at the same time in the same location. This is helpful in multitenant environments on Hosted PBX with more than one PBX.

| Basic | Signaling Encryption | Media Encryption | Interoperability | Sessions and Media | Remote SIP Connectivity | VolP Survival | VoIP Survival Status |
|-------|---|---------------------|------------------|--|----------------------------|------------------|-------------------------|
| ۲ | o IP Survi Enable Vo Disable V | IP Surviv | al | | | | |
| S | erver Ch | eck Inte | rval D | omains T | o Monitor | • | |
| 4 | D | seconds | | omain Na gate-siparat d new rows | tor Display | | Delete Row |
| R | egistrati | ons | | | | | |
| Re | REGIST | ER interva | l during survi | v <mark>al mode</mark> : | Time to st | tore subs | criber data: |
| 3 | 0 | seconds | | | 14 | day | rs |
| F | STN Ga | teways | (Help) | PSTN I | Numbers | (Help) | |
| | Domaiı Addre | | Delete Row | Local area | | local pho | ne numbers |
| A | dd new row | /s 1 t | rows. | | ding area co | - | |

Figure 61

- First enable VoIP Survival
- Define the check frequency (This value must be shorter that SIP Blacklist Interval in the Session and Media tab).
- Add the Domain name to check. You can add more domains if needed.
- Include registration frequency. This increases registration frequency when in Survival mode. This helps to detect when service returns to normal operation quickly.
- Subscriber data can be kept for several days. This time should be decided based on your expectation of maximum time the system could be down.
- The method to use in most cases is Display Name. This means that Subscriber data will be obtained from the Display Name in the SIP header.

4.6 RO SIP Traffic

All we need from the VoIP perspective is to forward all SIP requests from local endpoints to the DC SIParator; we will use DNS Override to do so.

4.6.1 RO Routing

Remember that also this SIParator is the one doing the conversion UDP $\leftarrow \rightarrow$ TLS.

Educronix LLC

| SIP ethods | Filtering | Local Registrar | Authenticatio and Accountin | | Dial Is Plan <mark>Rou</mark> | SIP Status | | IPS SIP lus Test T | SIP est Status | | | |
|---------------|-------------------------------------|-------------------------------|--|-----------|--|------------------|--------------|-----------------------|-------------------|--------|----------------|--|
| DNS | NS Override For SIP Requests (Help) | | | | | | | | | | | |
| | | | Relay To | | | | | | | Delete | | |
| | Domai | n | DNS Na or IP Ad | | IP Address | Port | Transport | Priority | Weight | Auth | Modify RURI | |
| + ing | ate-sipa | rator lo | inanto sis | | 00.1 | 5061 | TRANS | | | No 🖂 | No | |
| | | | | _ | | | <u>⊓ls ∨</u> | | | | 140 * | |
| Add ne | ew rows | 1 g | roups with 1 | | vs per grou | ıp. | ocessing @ | Help) | | | | |
| Add ne | ew rows | 1 g g Order | roups with 1 | Clas | vs per grou | ep. essage Pr | | <u>Help)</u> | | | | |
| Add ne | ew rows Routin | 1 g g Order | roups with 1 (<u>Help)</u> Function | Clas F | vs per grou ss 3xx Me | essage Pr | | <u>Help)</u> | | | | |
| Add ne | ew rows Routin |] 1 g g Order Routing 1 | roups with 1 (<u>Help</u>) Function rride | Clas F | vs per grou ss 3xx Me forward all | essage Pr | | <u>Help)</u> | | | | |

- Figure 62
- Make sure the Domain is routed to the same domain (DC SIParator public IP) and signaling port is the one designated for TLS. This will automatically enforce conversion between SIP/UDP and SIP/TLS

5 Additional Information

5.1 Endpoint configuration examples

In our original case we have two types of remote users:

- Remote office behind Local SIParator/Firewall. In this case, Phones will be configured as standard as possible without using TLS/SRTP. All security will be managed at the Local SIParator.
- Roaming Users / Road warriors. This includes endpoints behind NAT not under management of the user or company. In this case, Phones use TLS/SRTP.

Examples of endpoint SIP configuration behind local SIParator, using our use case scenario.

SNOM 870 Phone:

| Login Features SIP NAT RTP | | |
|---------------------------------------|-------------------------------|----------|
| Login Information: | | |
| Identity active: | ◉on ○off ? | |
| Displayname: | 3008 |] ? |
| Account: | 3008 |] ? |
| Password: | | ? |
| Registrar: | ingate-siparator.loscasas.com | ? |
| Outbound Proxy: | 192.168.200.254 | ? |
| Failover Identity: | None 🗸 ? | |
| Authentication Username: | 3008 | ? |
| Mailbox: | | 0 |
| Ringtone: | Ringer 1 🗸 ? | _ |
| Custom Melody URL: | | ? |
| Display text for idle screen: | | ? |
| XML Idle Screen URL: | | 0 |
| Ring After Delay (sec): | | ? |
| Record Missed Calls: | ●on ○off ? | _ |
| Record Dialed Calls: | ◉on ○off ? | |
| Record Received Calls: | ●on ○off ? | |
| Identity is hidden: | Oon Ooff ? | |
| Apply Re-Register Play Ringer | | |
| Remove Identity Remove All Identities | | |

Figure 63

- Note we use the domain as the Registrar, and the outbound proxy is pointing to the local SIParator internal interface (Default Gateway)
- If Ingate SIParator is the LAN default gateway, you don't need to define the outbound proxy, just leave it blank 😇

Grandstream GXV3240

| Status | Account Advanced Settings | Maintenance |
|--------|-------------------------------|-----------------------------------|
| | Account 1 Account 2 Account | t 3 Account 4 Account 5 Account 6 |
| | | |
| | Account Active : | ⊠Yes |
| | Account Name : | 3007 |
| | SIP Server : | ingate-siparator.loscasas.com |
| | SIP User ID : | 3007 |
| | SIP Authentication ID : | 3007 |
| | SIP Authentication Password : | |
| | Voice Mail Access Number : | *97 |
| | Name : | 3007 |
| | Show Account Name Only : | ⊻Yes |
| | Tel URI : | User=Phone |
| | | |
| | | Save Cancel |
| | | |
| Status | Account Advanced Setting | s Maintenance |
| | Account 1 Account 2 Account | |
| | | |
| | | |
| | Outbound Proxy : | 192.168.200.254 |
| | Secondary Outbound Proxy : | |
| | DNS Mode : | A Record |
| | NAT Traversal : | NAT NO |
| | Proxv-Require : | |

Figure 64

- Note we use the domain as the Sip Server, and the outbound proxy is pointing to the local SIParator internal interface (Default Gateway)
- If Ingate SIParator is the LAN default gateway, you don't need to define the outbound proxy, just leave it blank 😇

Sangoma S500

| OUDP OTCP OTLS 😯 | |
|-------------------------------|---|
| | 0 |
| 192.168.200.254 | 0 |
| ®No OYes 😮 | |
| | 0 |
| | 0 |
| ingate-siparator.loscasas.com | 0 |
| ONo ©Yes | |
| Registered | |
| | ONo OYes Ingate-siparator.loscasas.com |

- Note we use the domain as the Sip Server, and the outbound proxy is pointing to the local SIParator internal interface (Default Gateway)
- If Ingate SIParator is the LAN default gateway, you don't need to define the outbound proxy, just leave it blank 😇

6 Additional help or support

If you have questions, suggestions and any other concern feel free to contact Educronix LLC

Web: <u>www.educronix.com</u> Email: <u>support@educronix.com</u> Toll-Free: +1 855 866 8854 Ph: +1 954 866 8884

We also provide consulting services as well as remote hands troubleshooting and configuration.

