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

For the Ingate SIParator®/Firewalls using software release 6.2.1 or later

[May 15th, 2019]

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:

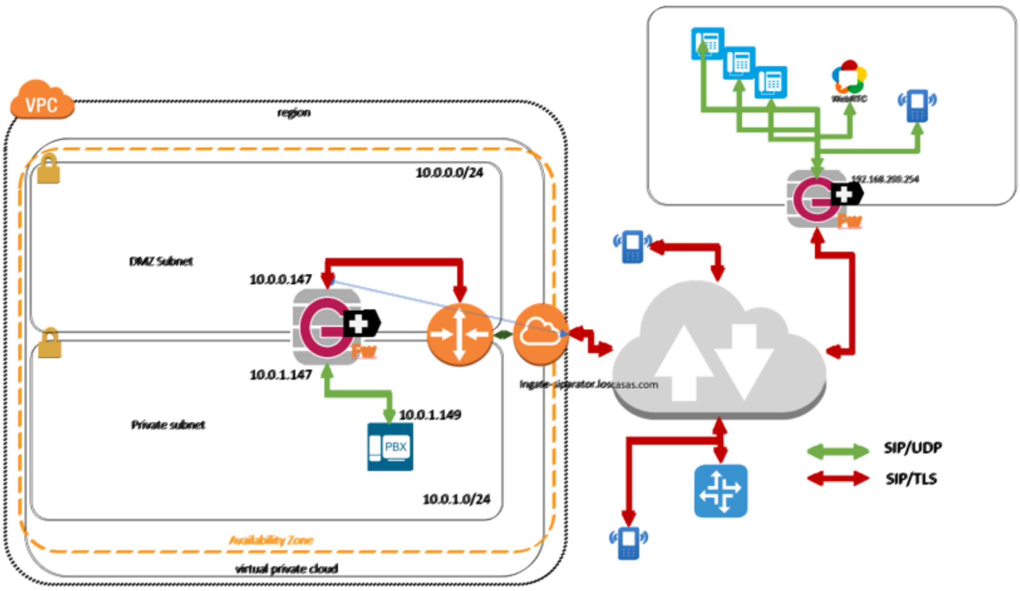
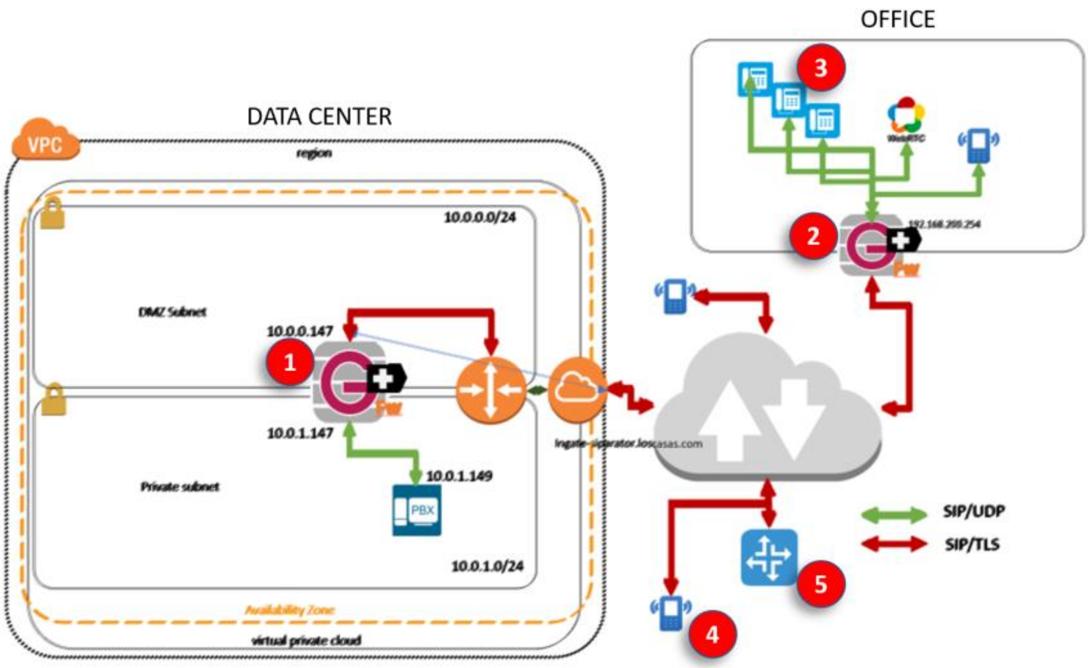


Figure 1

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:

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

2 **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.

3 **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 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..

4 **Remote Endpoints (Road Warriors).** Remote Users roaming and without predetermined location will be able to use IPPBX/UC platform via secure TLS/SRTP sessions. Typically, these endpoints are Softphones in Laptops, 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..)

5 **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

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:

➔ [Get it from AWS Marketplace]

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 PKI knowledge or supporting components like an external database. It is built on The Legion of the Bouncy Castle 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.

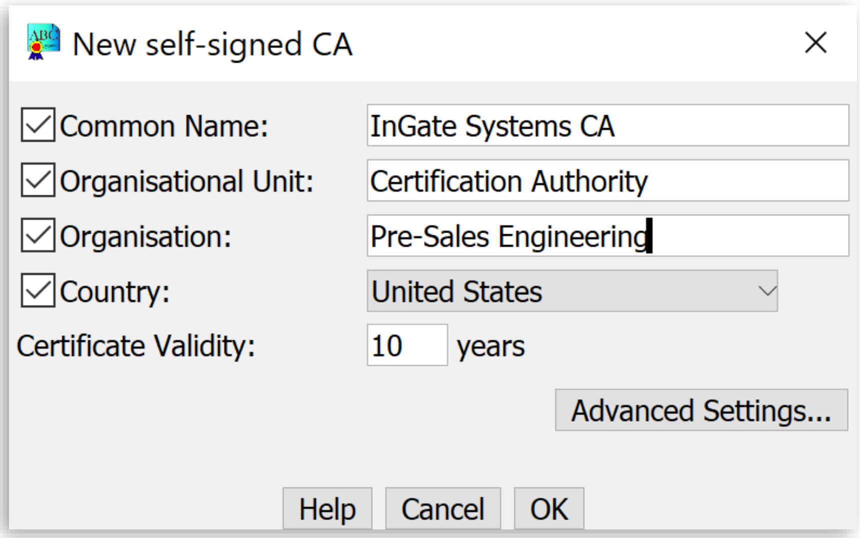


Figure 2

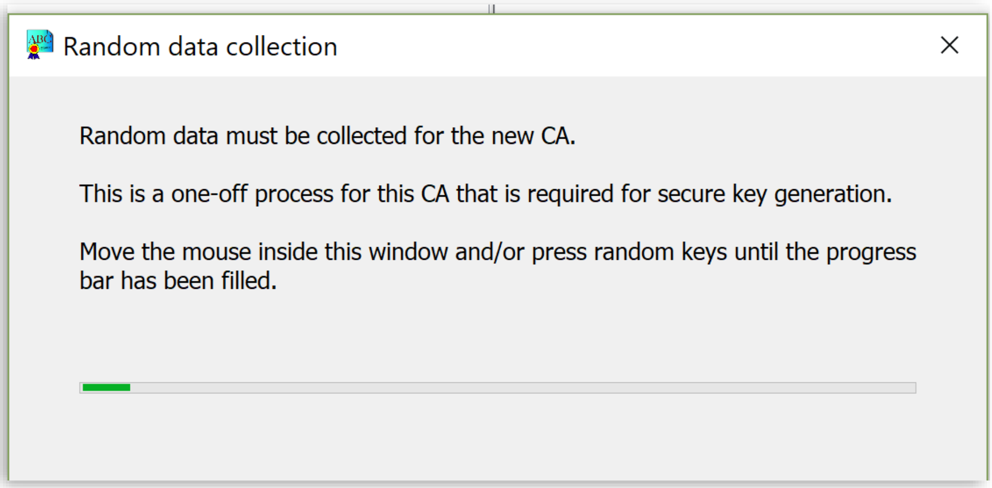


Figure 3

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

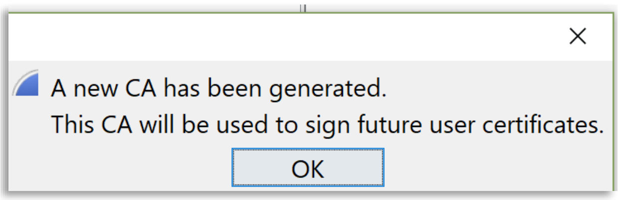


Figure 4

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

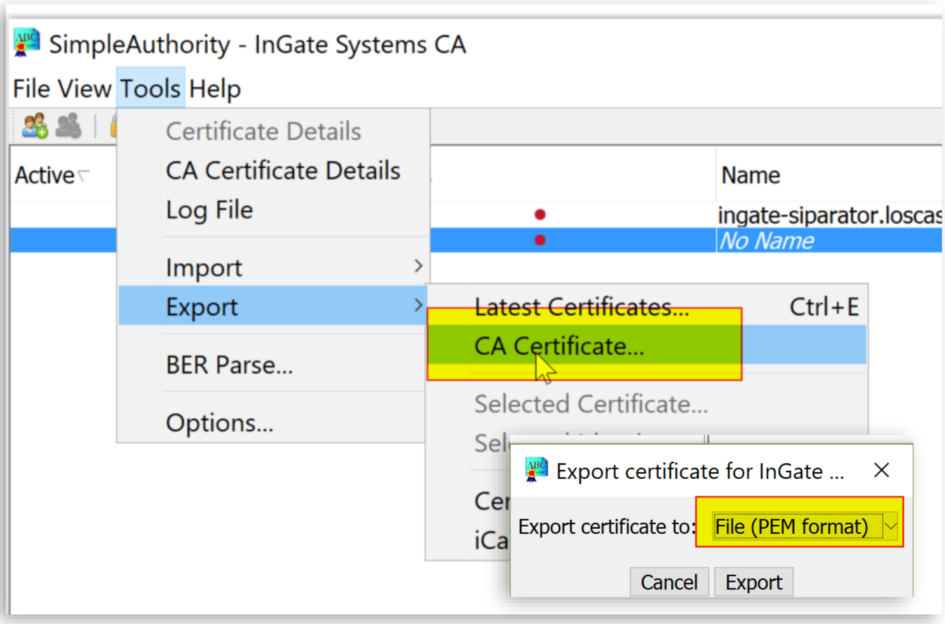


Figure 5

- 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 → Certificates, add a new row in the CA Certificates section:

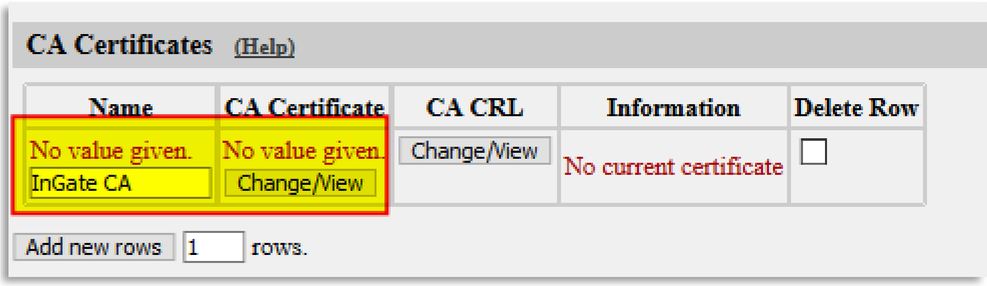


Figure 6

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

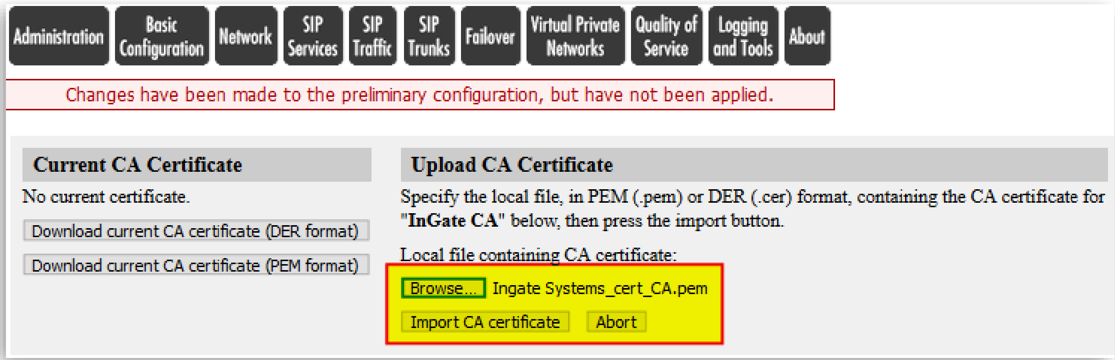


Figure 7

- 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:

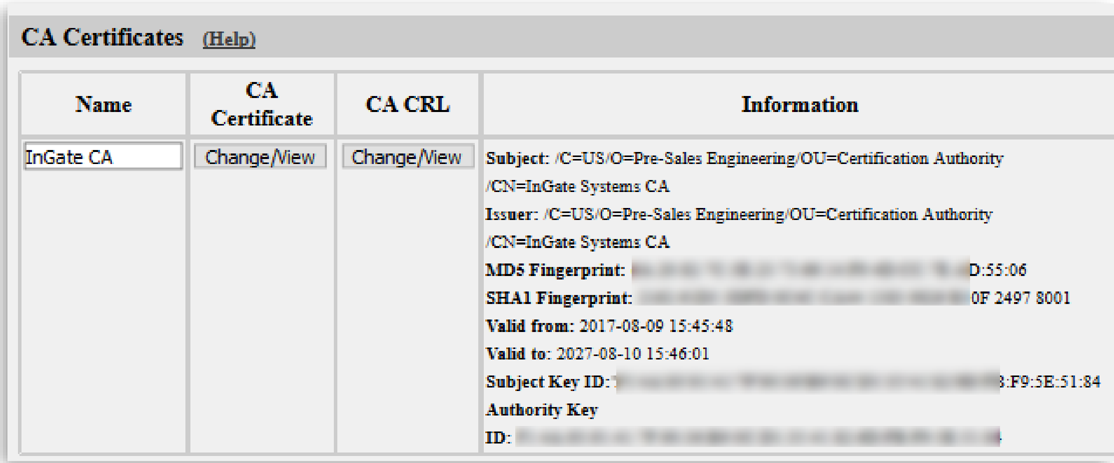


Figure 8

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)

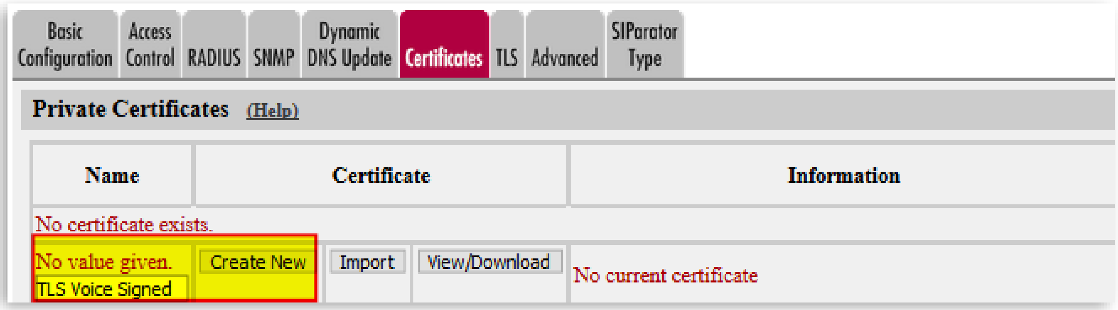


Figure 9

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

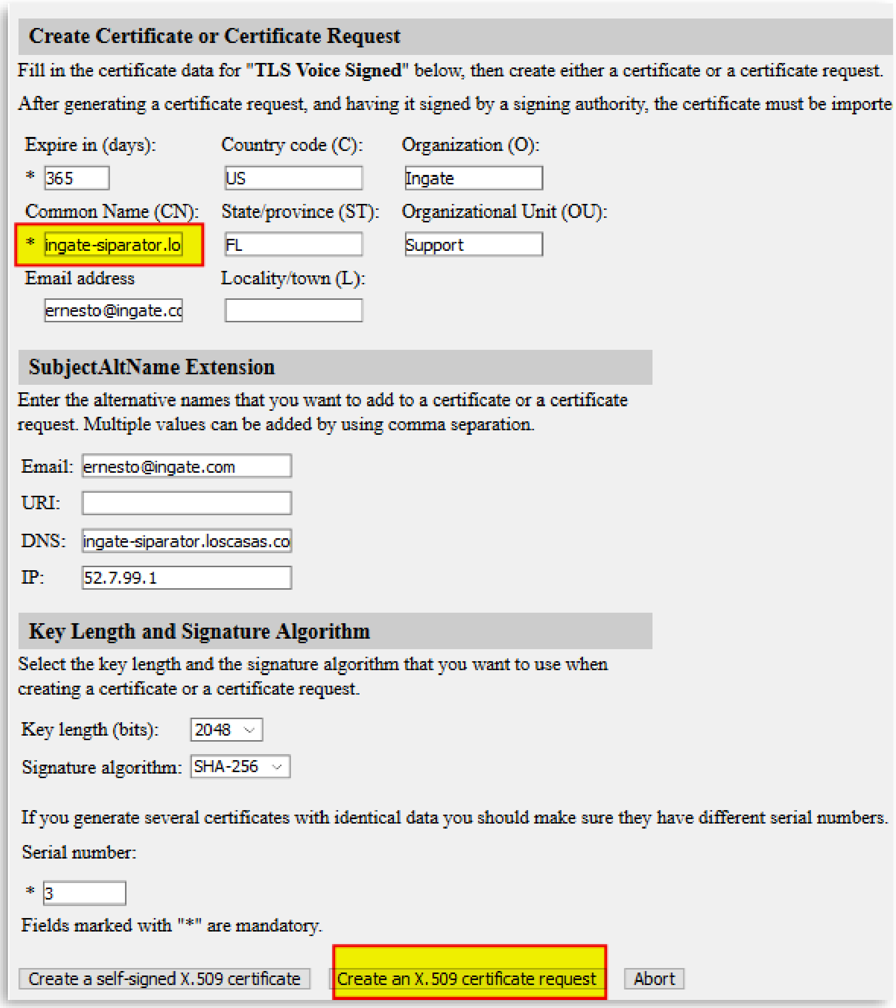


Figure 10

- 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.

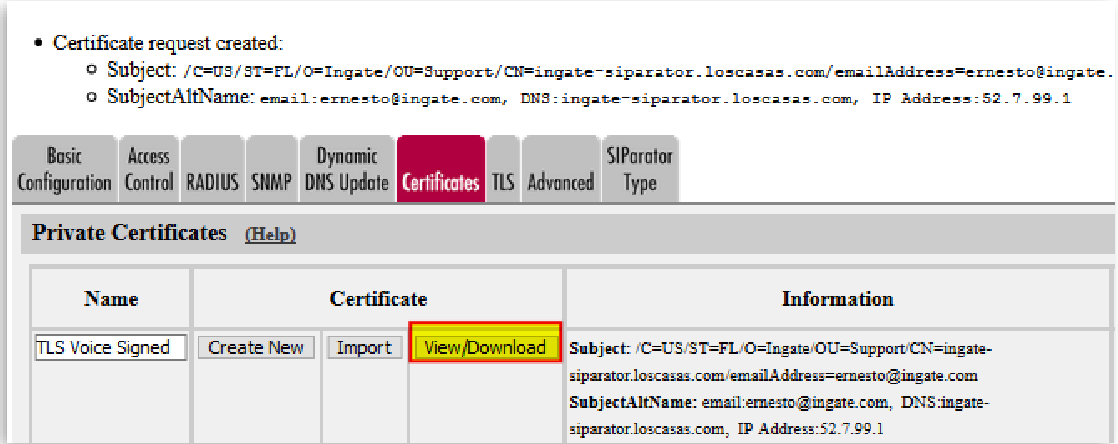


Figure 11

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

Press on the "View/Download"

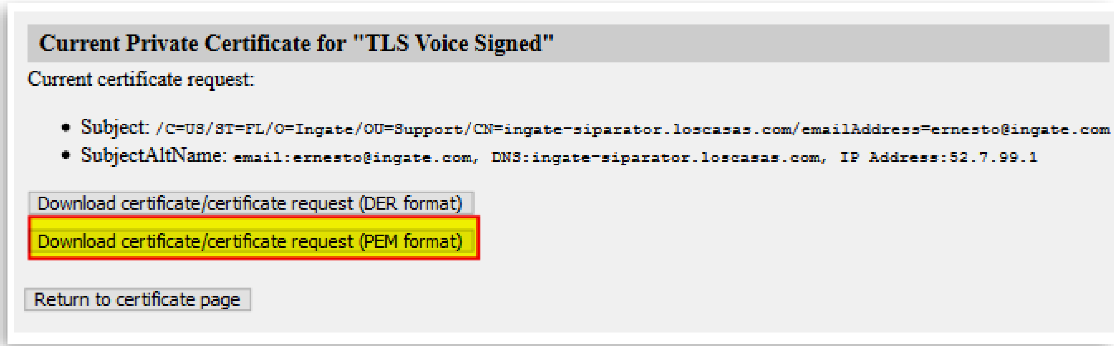


Figure 12

- 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).

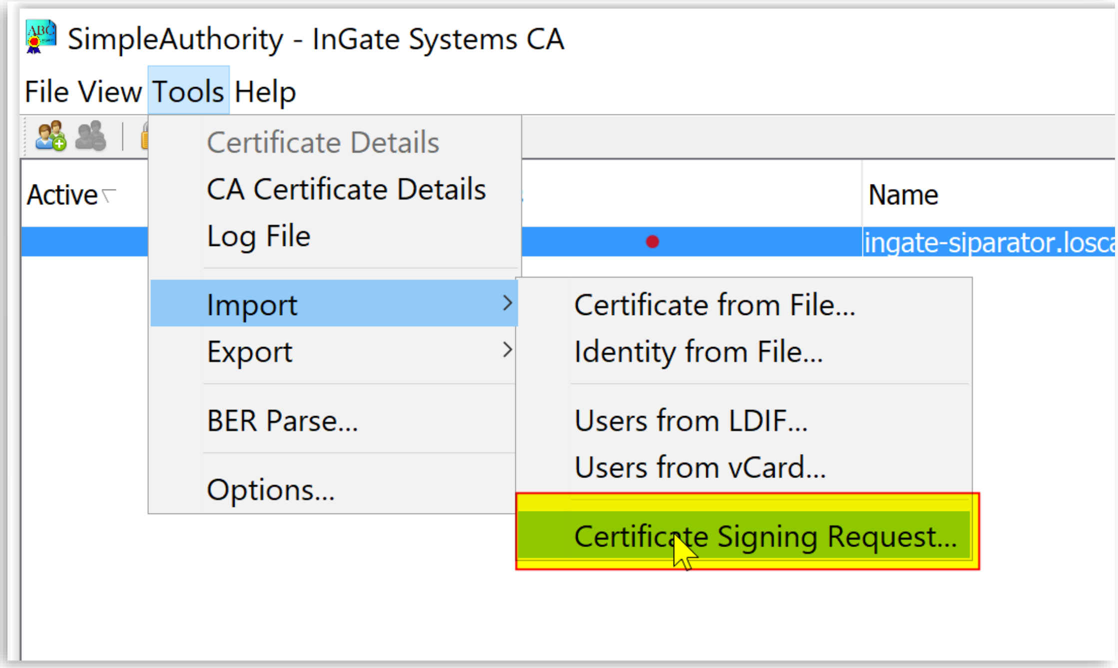


Figure 13

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

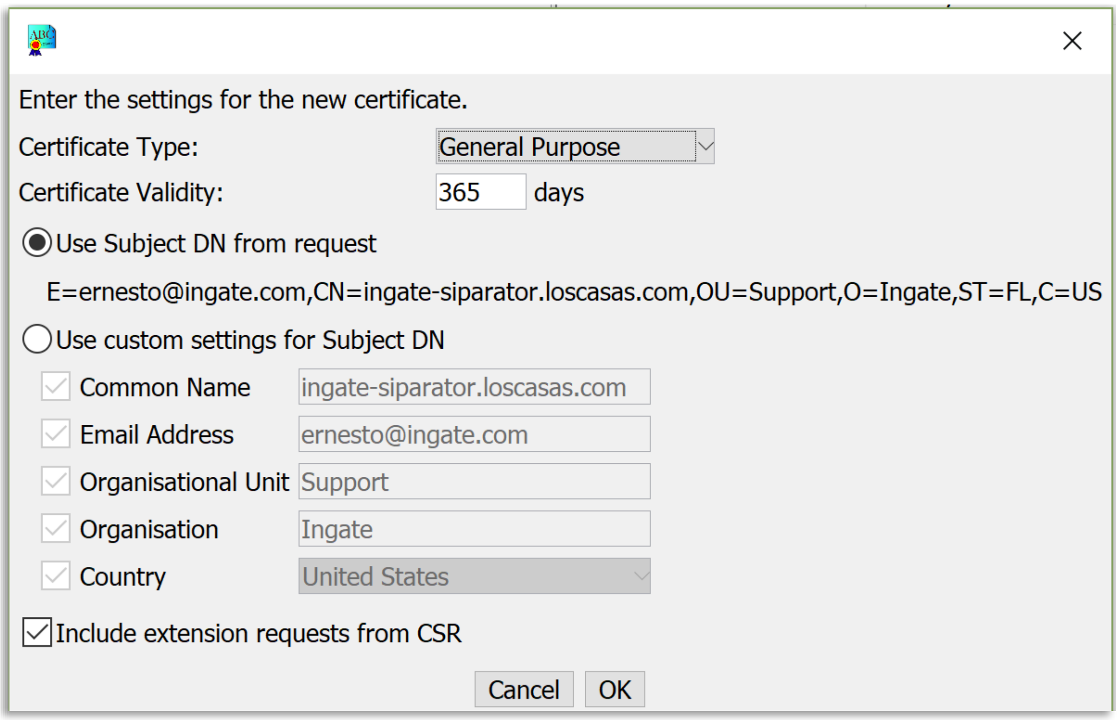


Figure 14

- 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:

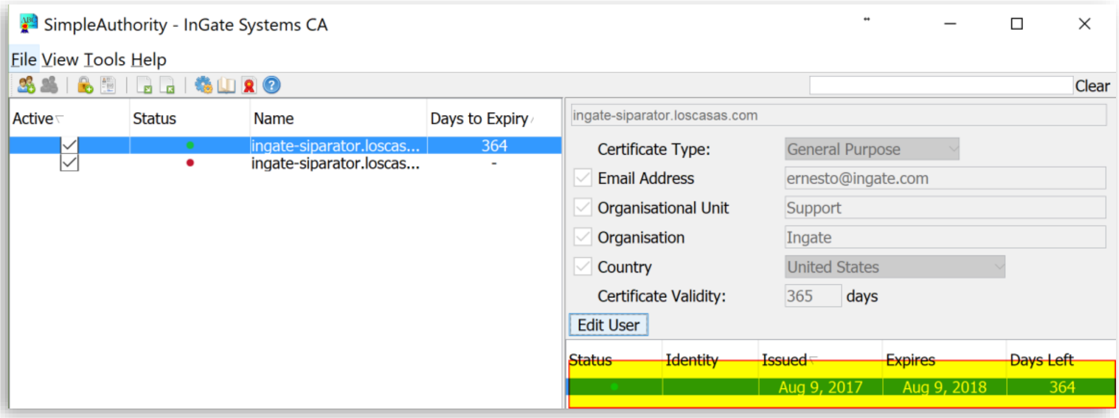


Figure 15

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

Right click on the Certificate and select Export Certificate

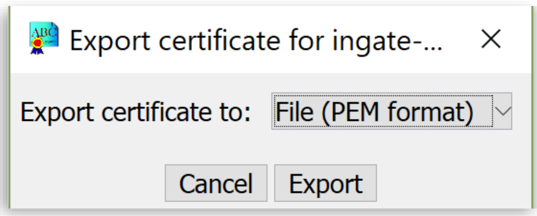


Figure 16

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

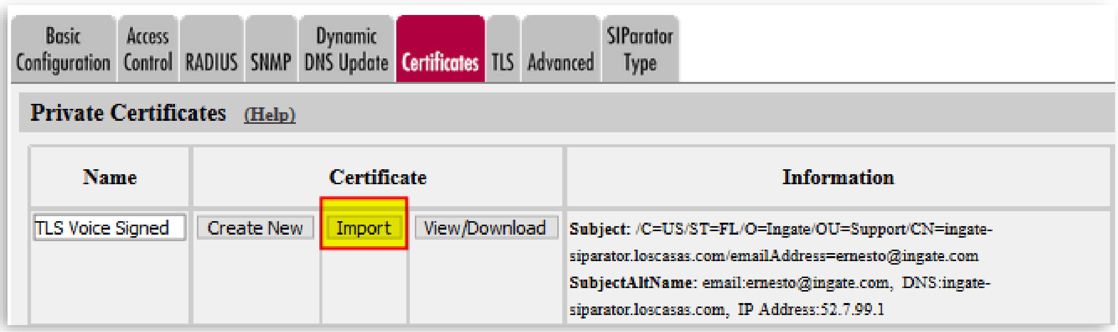


Figure 17

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

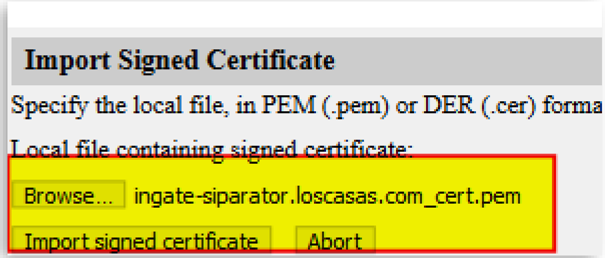
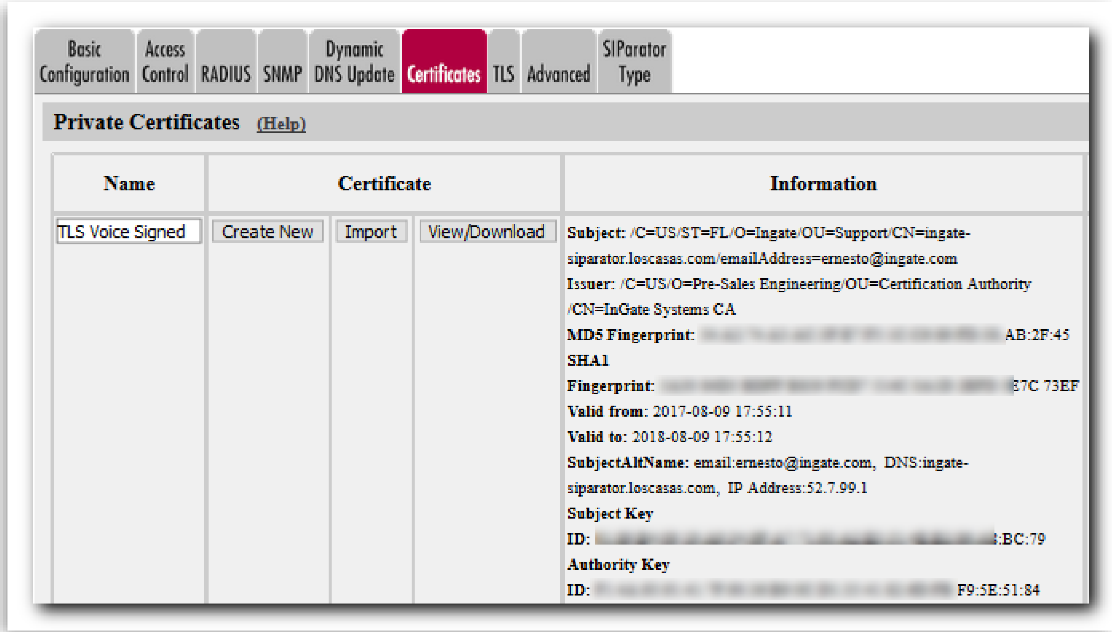


Figure 18

- Select the file and press "Import signed certificate"

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



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

3 Ingate Data Center Node Configuration

Going Back to our original Layout:

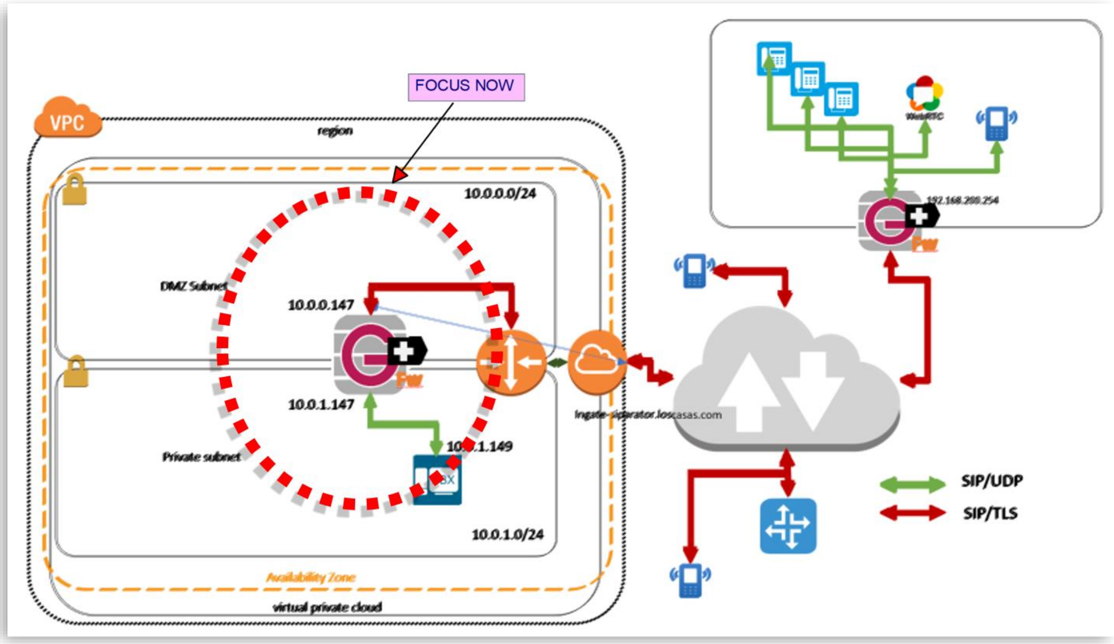


Figure 19

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.

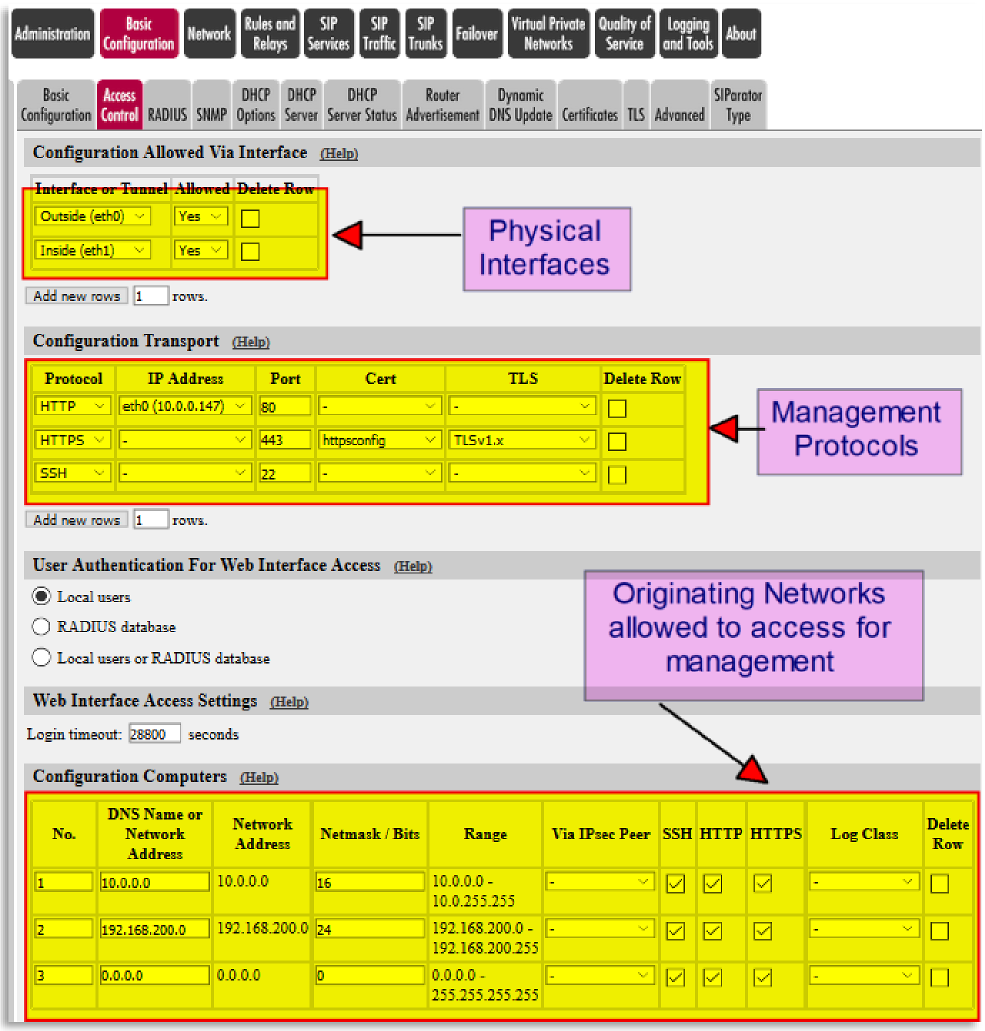


Figure 20

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.

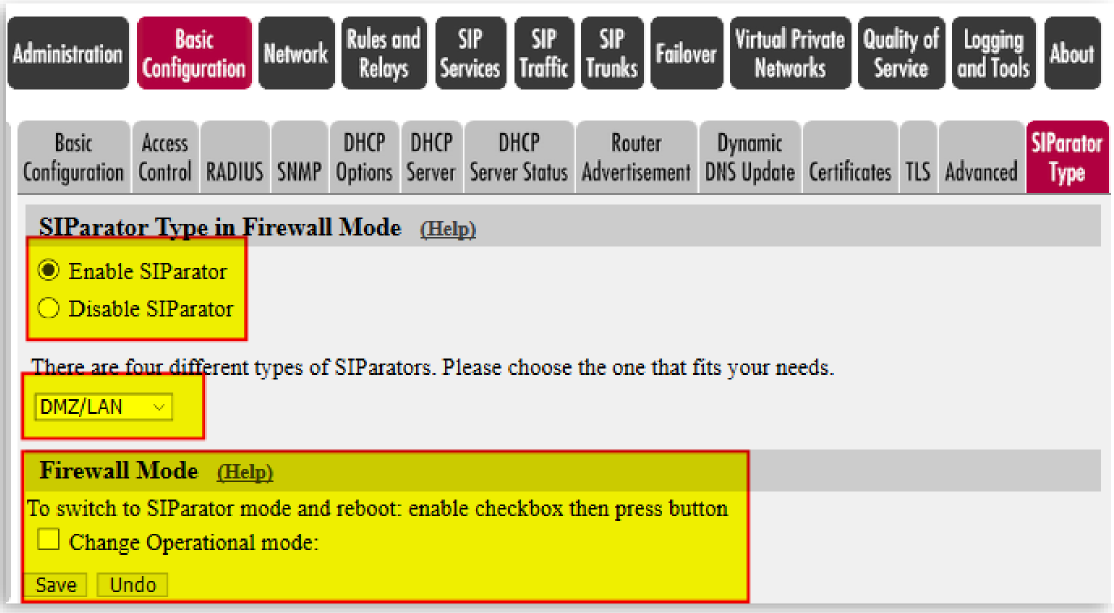


Figure 21

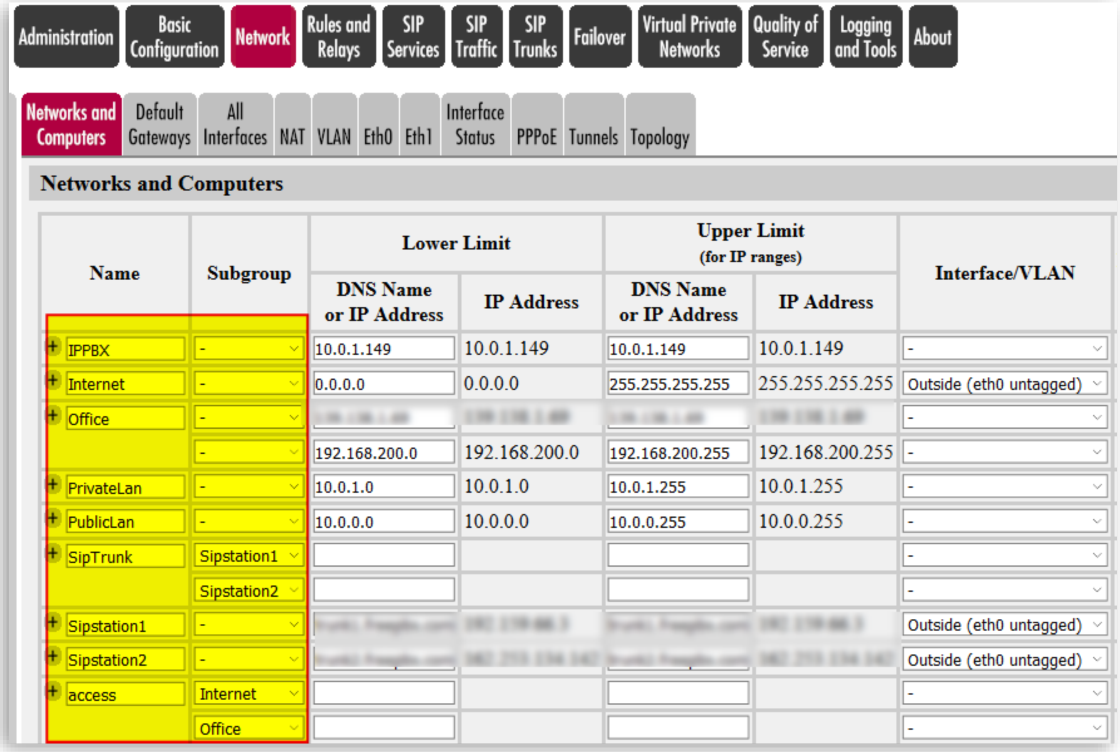
- Make sure SIParator is enabled
- Select DMZ/LAN option
- Make sure the device is working in Firewall Mode. If not it will show the "SIParator" logo in the top of the GUI and you will need to "change operational mode"

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:



Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	
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	-	[illegible]	[illegible]	[illegible]	[illegible]	-
	-	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	10.0.0.255	10.0.0.255	-
SipTrunk	Sipstation1					-
	Sipstation2					-
Sipstation1	-	[illegible]	[illegible]	[illegible]	[illegible]	Outside (eth0 untagged)
Sipstation2	-	[illegible]	[illegible]	[illegible]	[illegible]	Outside (eth0 untagged)
access	Internet					-
	Office					-

Figure 22

- 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:

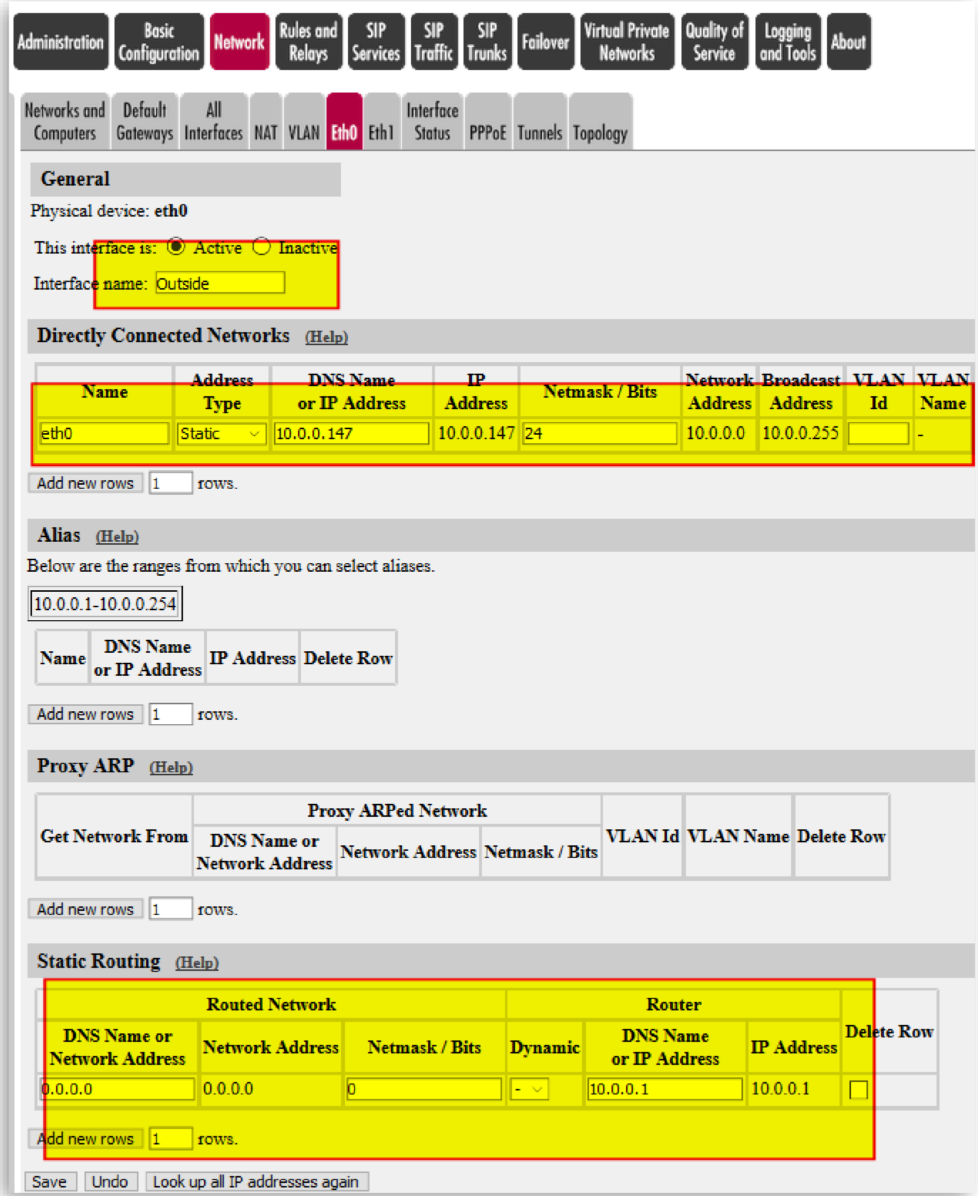


Figure 23

- 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:

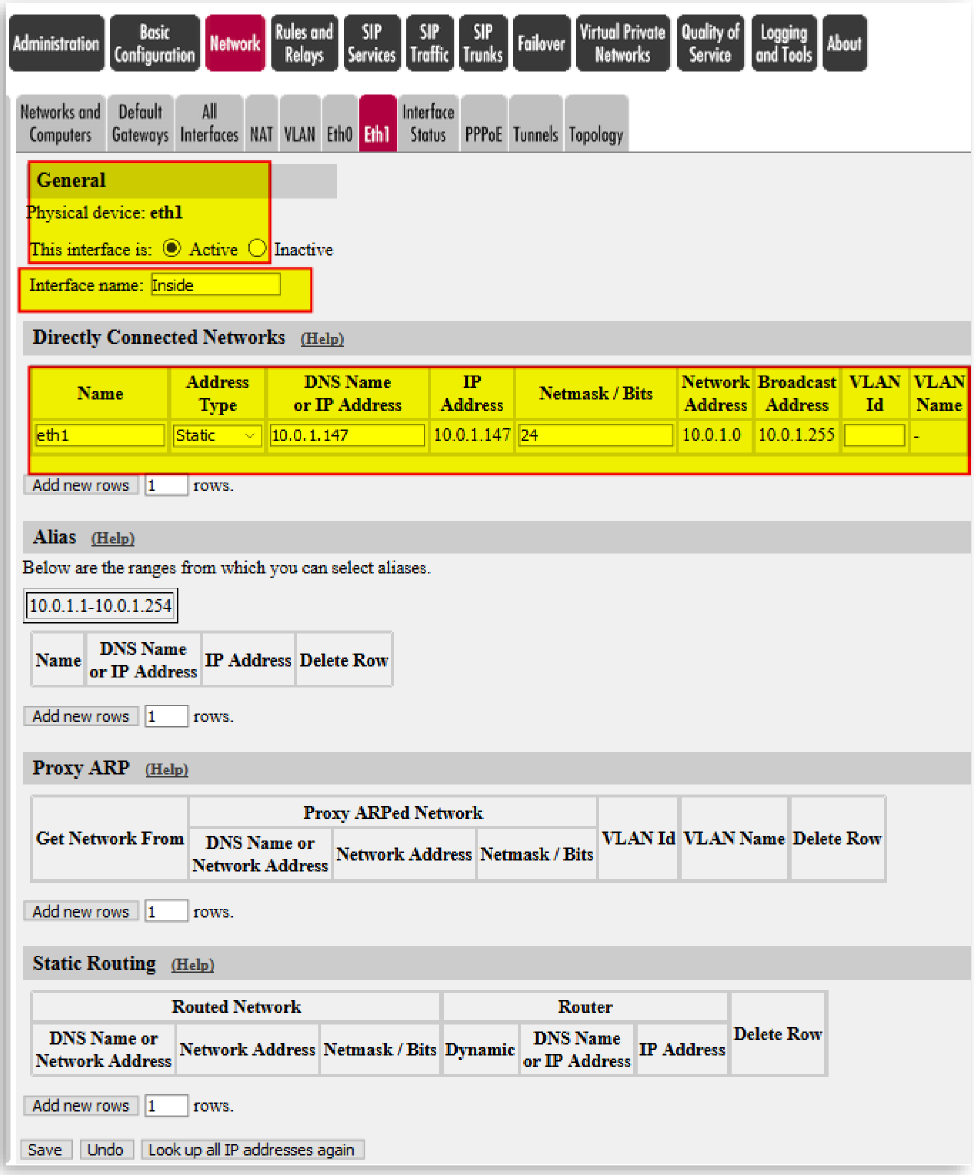


Figure 24

- 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.

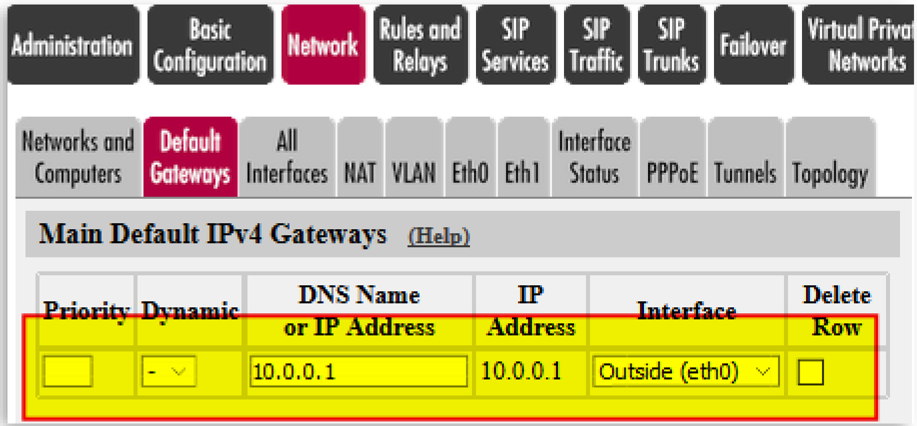


Figure 25

- 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.

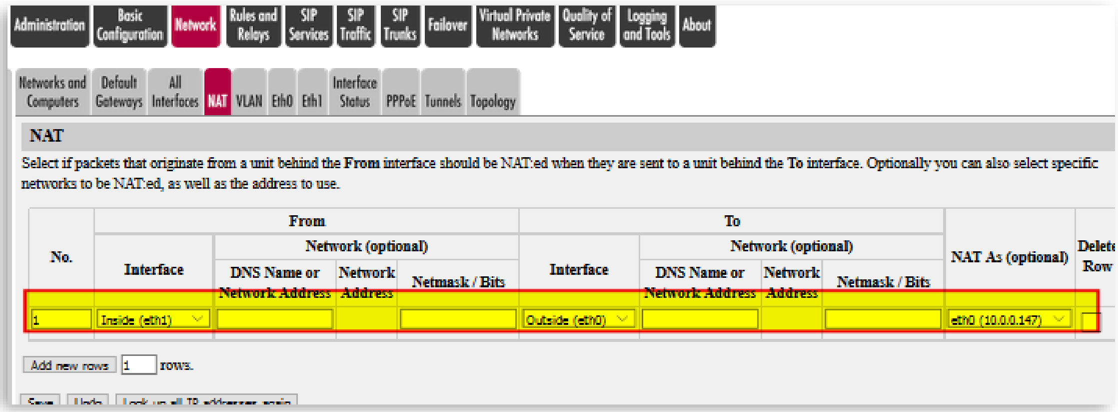


Figure 26

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:

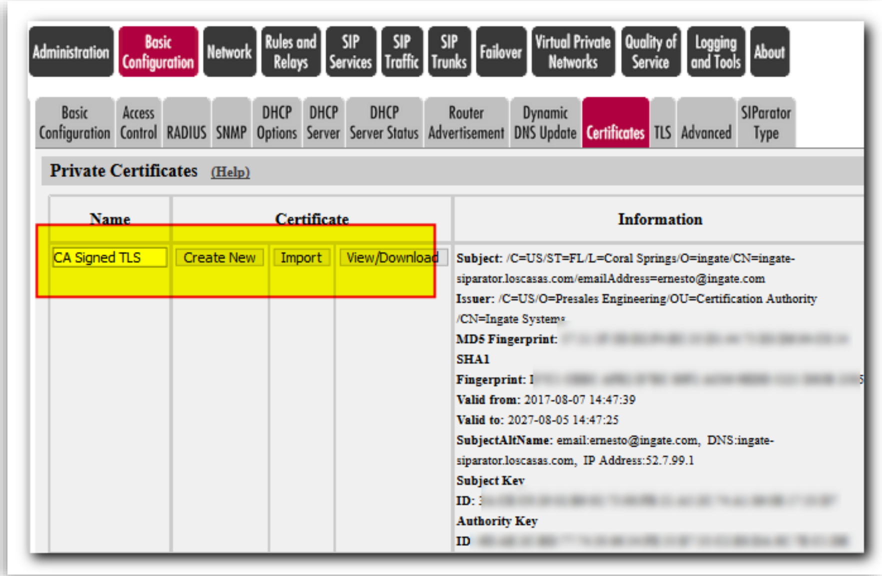


Figure 27

CA Certificate:

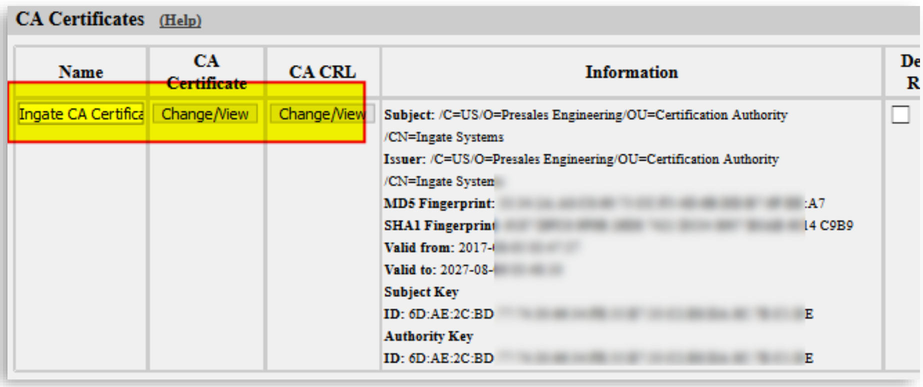


Figure 28

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:

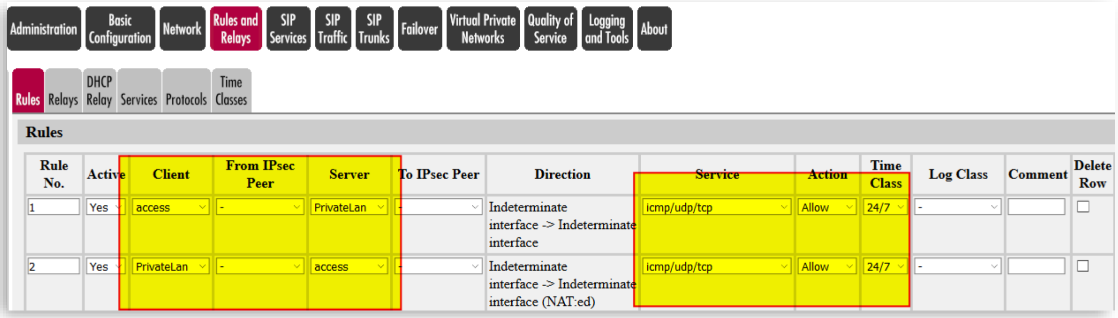


Figure 29

- 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
XMPP	TCP Port: 5222
FTP	TCP Port: 21
TFTP	UDP Port: 69

Figure 30

- 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 is how this is included in SIParator configuration

Rules | Relays | DHCP Relay | Services | Protocols | Time Classes

Relays (Help)

Listen To ...		Relay To ...			Relay Type	Allow Access From ...	
IP Address	Port	DNS Name or IP Address	IP Address	Port		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	-

Figure 31

- 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 →443, 8080→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:

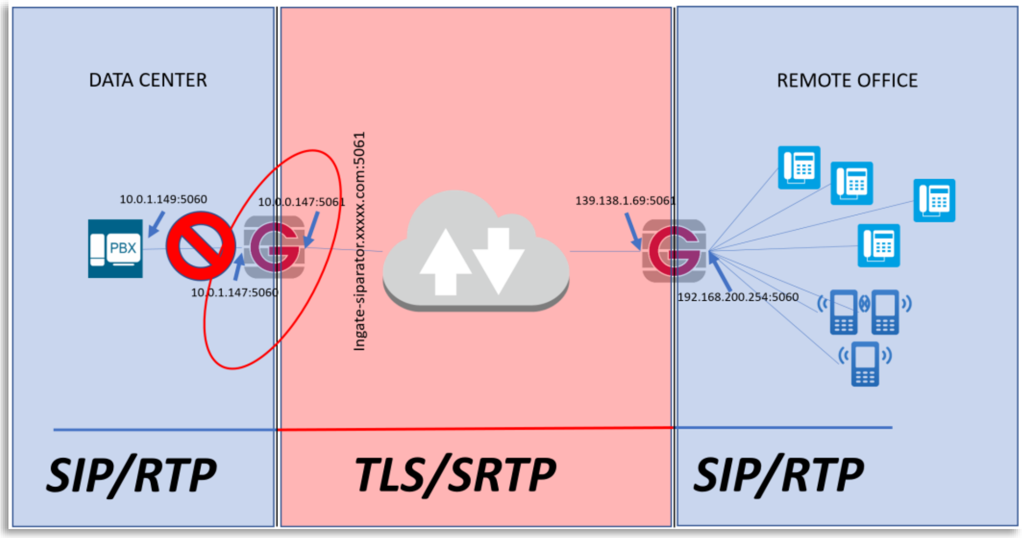


Figure 32

- 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.xxxxxxxxx.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.

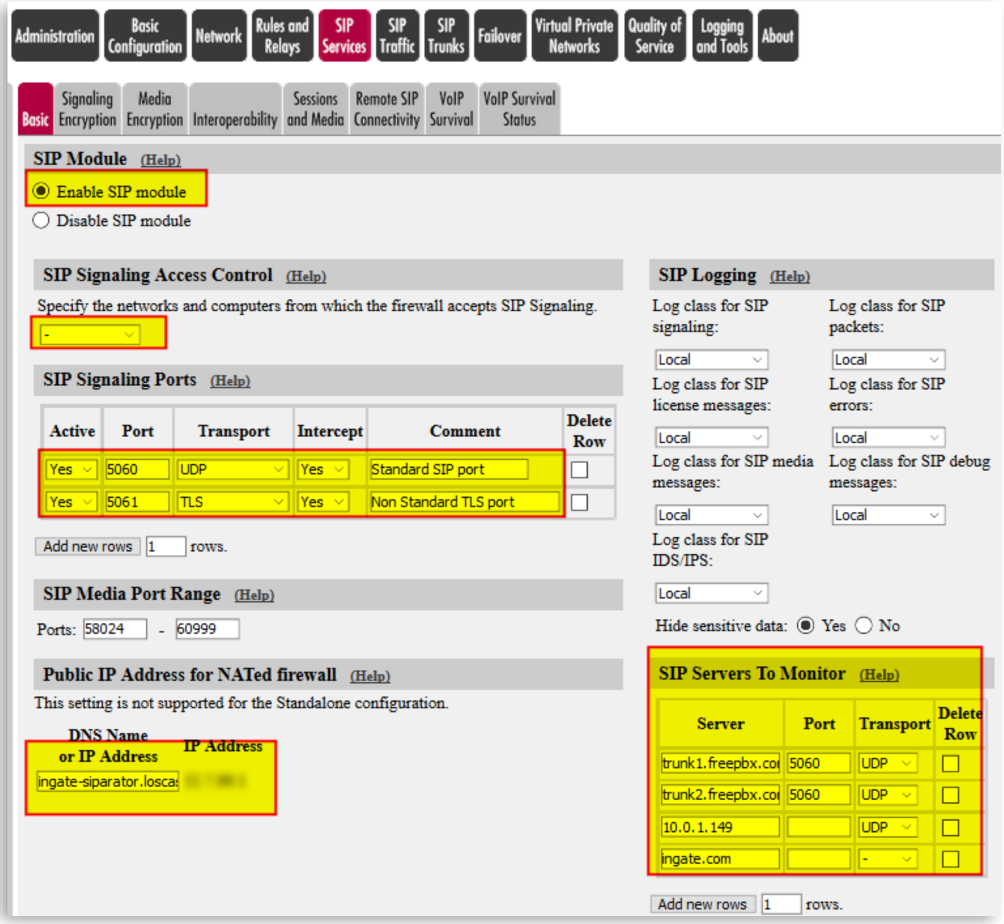


Figure 33

- 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***).

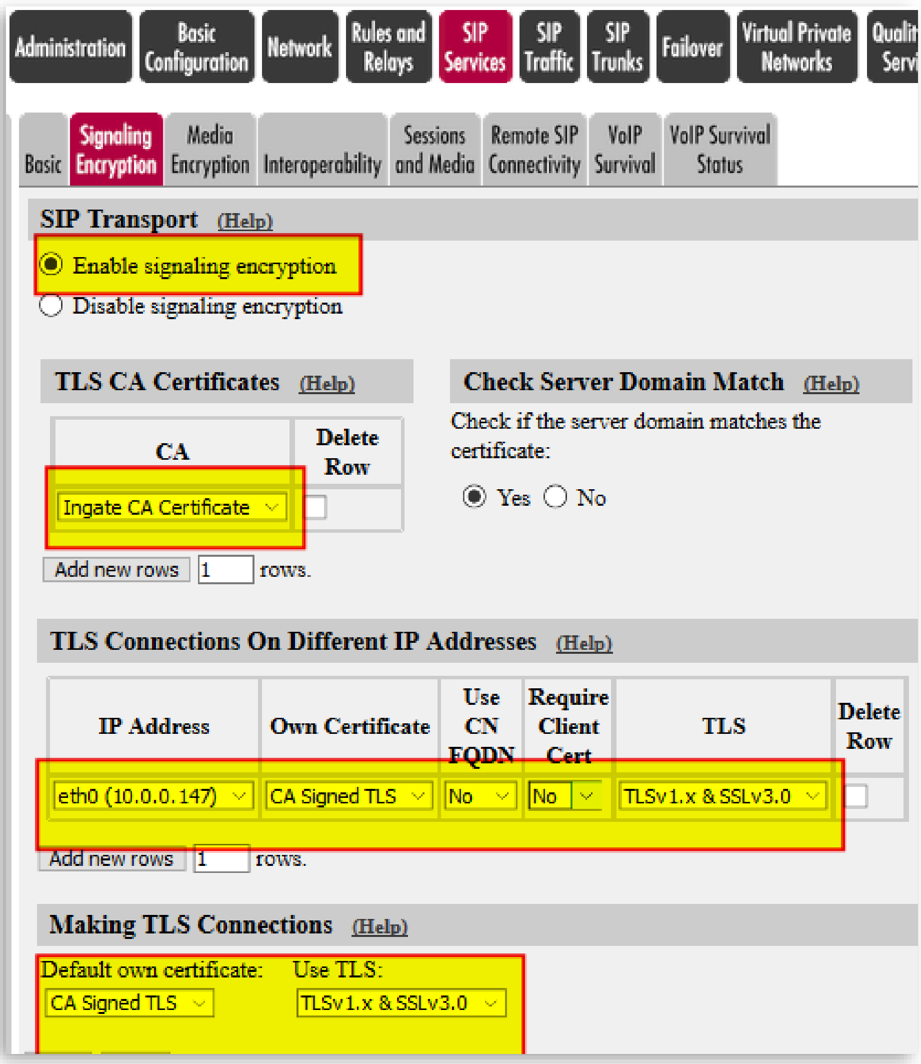


Figure 34

- 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.

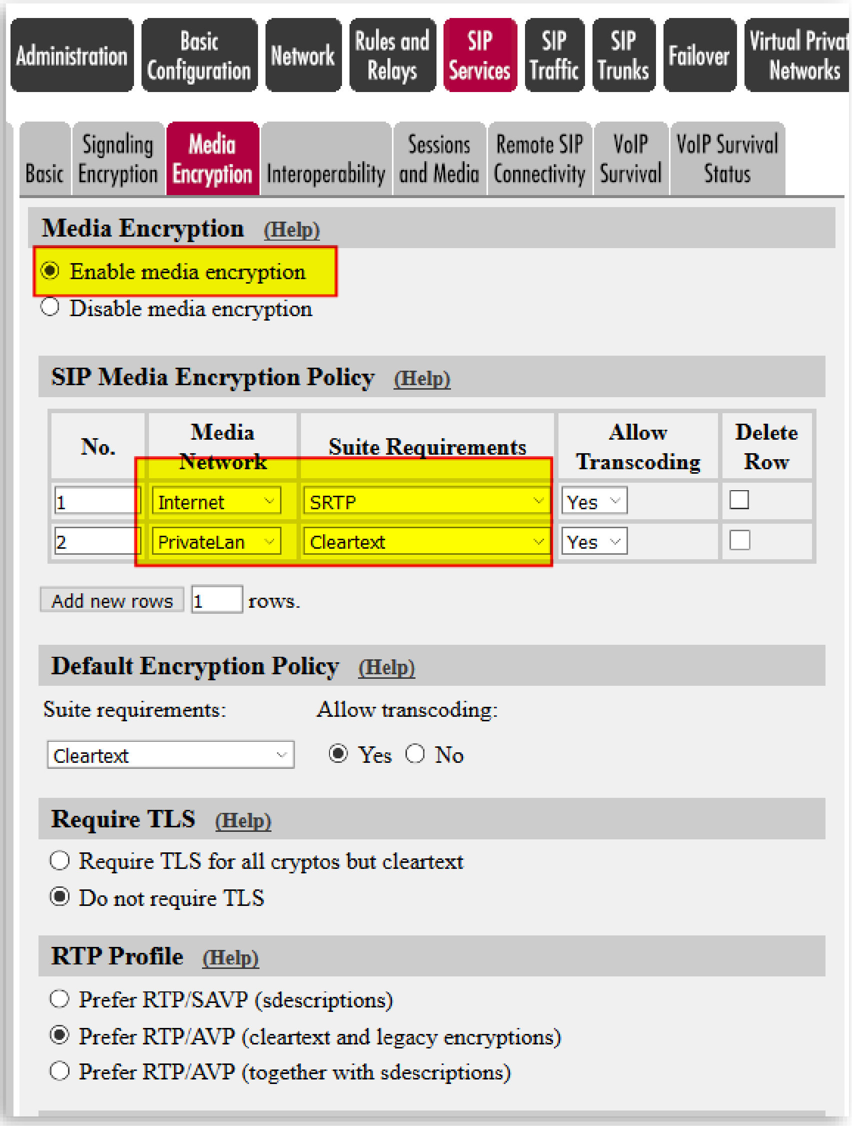


Figure 35

- 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.

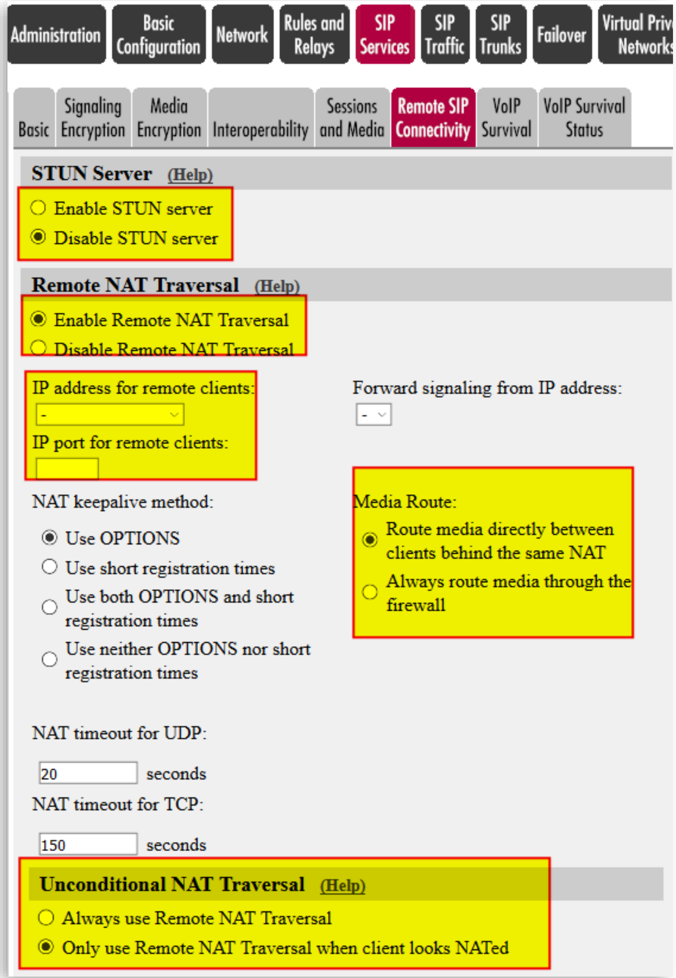


Figure 36

- 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.

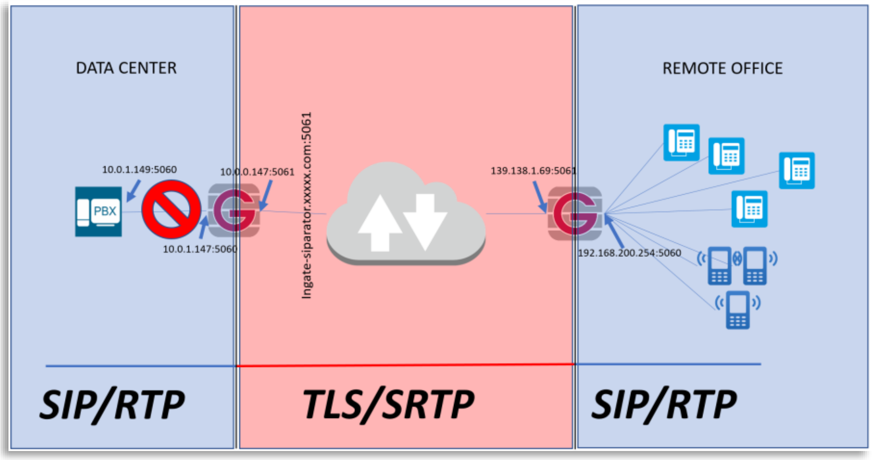


Figure 37

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.

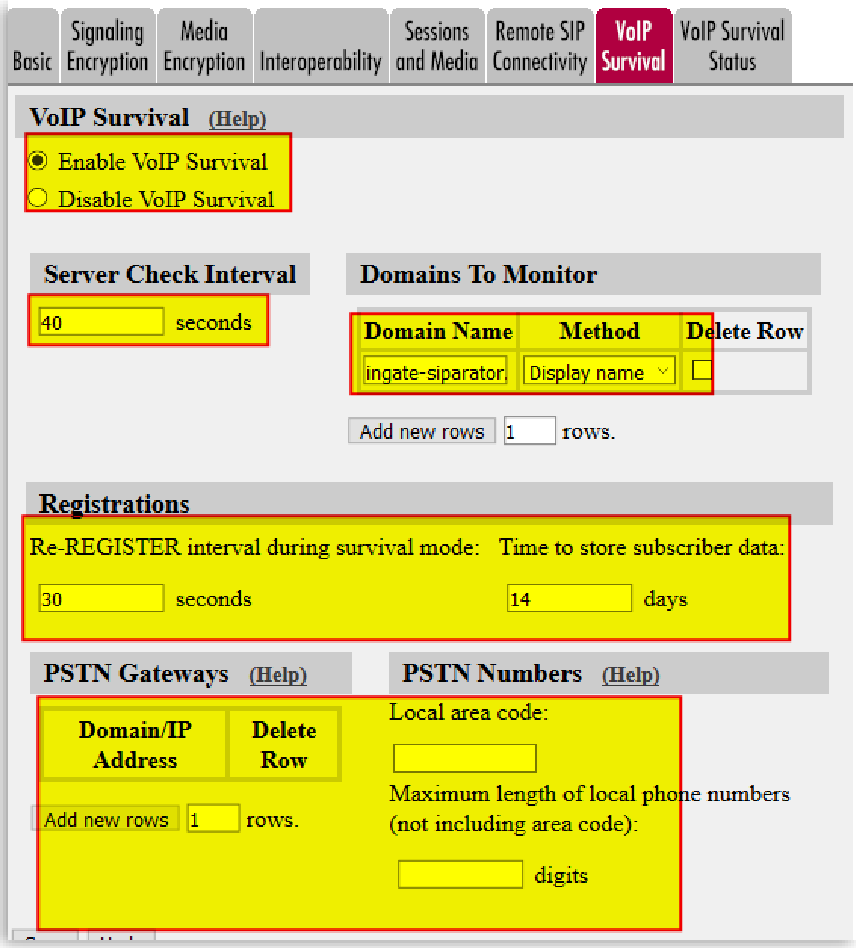


Figure 38

- 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:

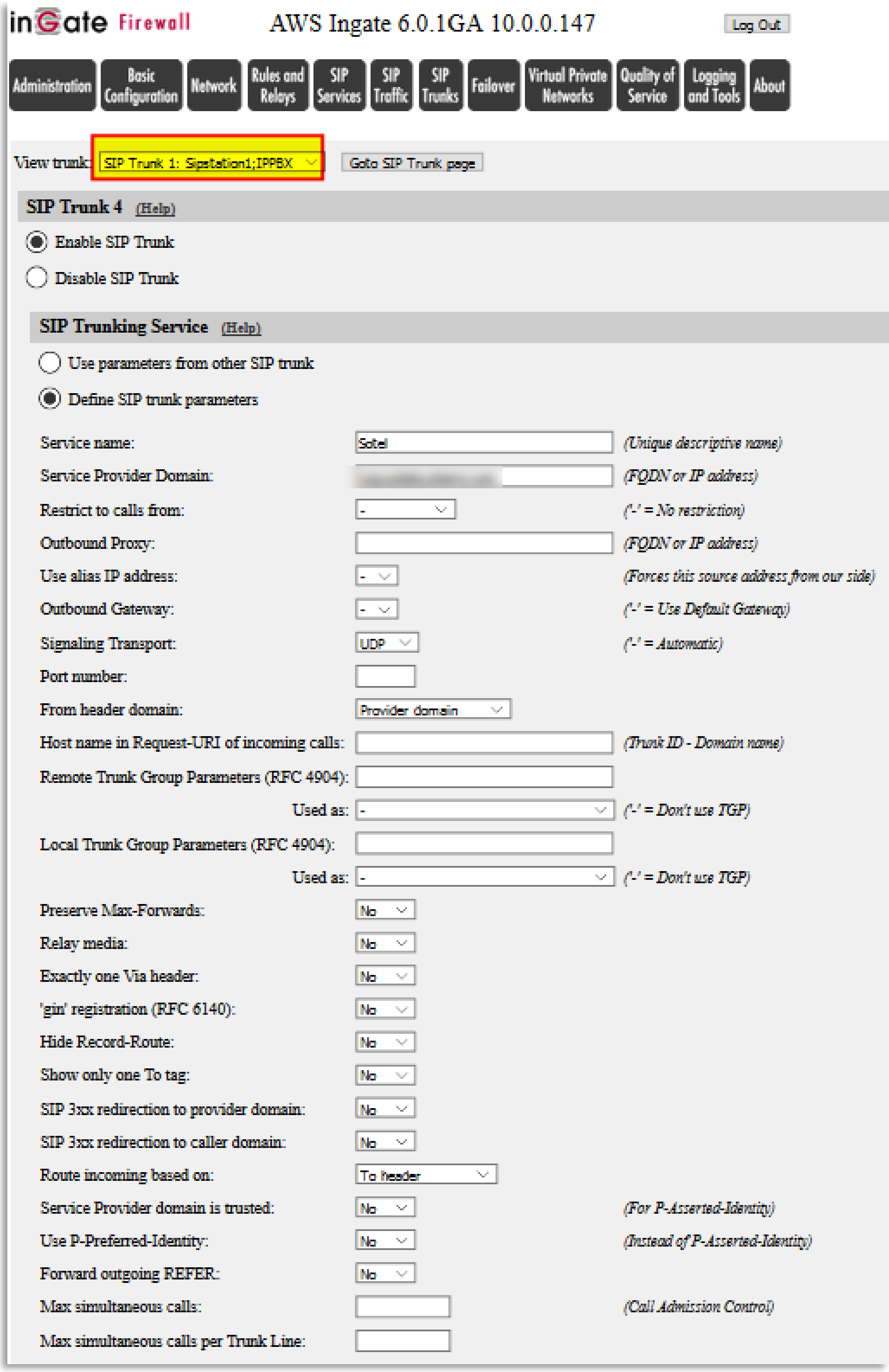


Figure 39

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 From-columns.

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.

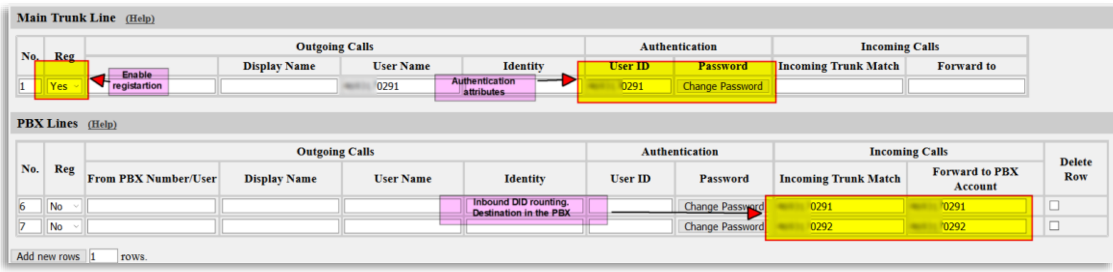


Figure 40

- 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

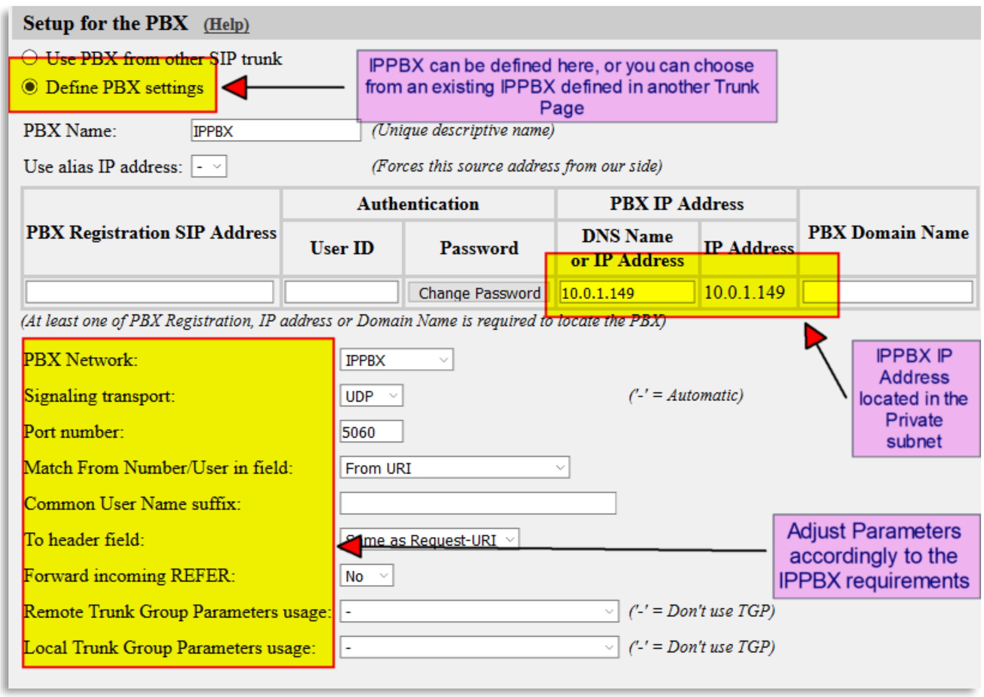


Figure 41

- 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*** ***Sip Trunking Configuration using the SIP Trunk Page***

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

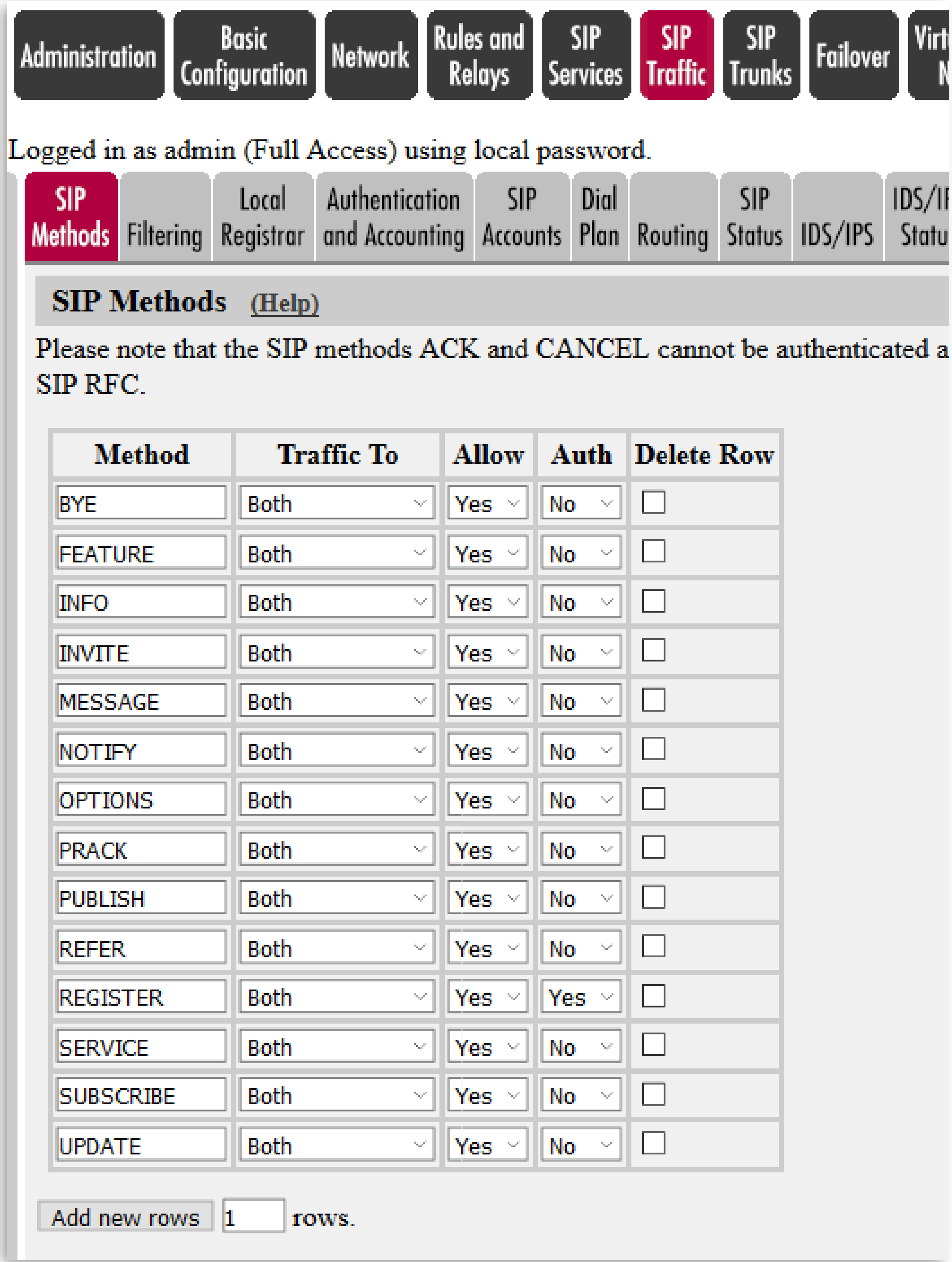
We address only the ones that define call behavior and add value to secure the service

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.



Method	Traffic To	Allow	Auth	Delete Row
BYE	Both	Yes	No	
FEATURE	Both	Yes	No	
INFO	Both	Yes	No	
INVITE	Both	Yes	No	
MESSAGE	Both	Yes	No	
NOTIFY	Both	Yes	No	
OPTIONS	Both	Yes	No	
PRACK	Both	Yes	No	
PUBLISH	Both	Yes	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).

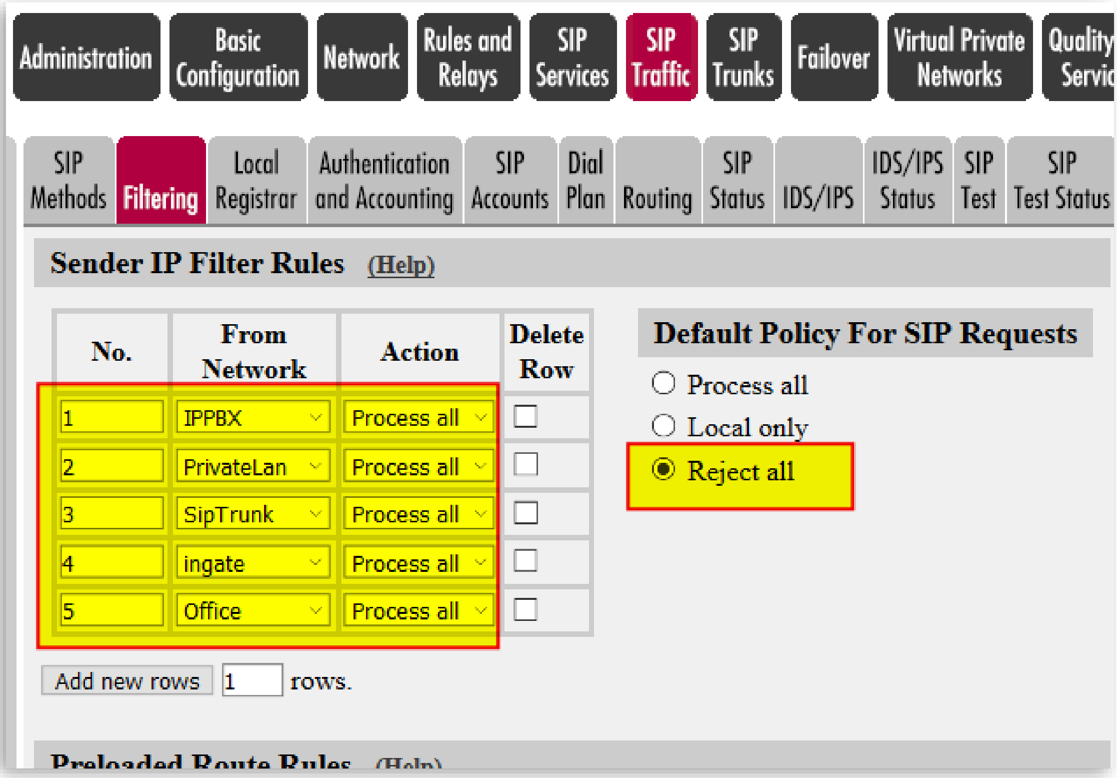


Figure 43

- 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.

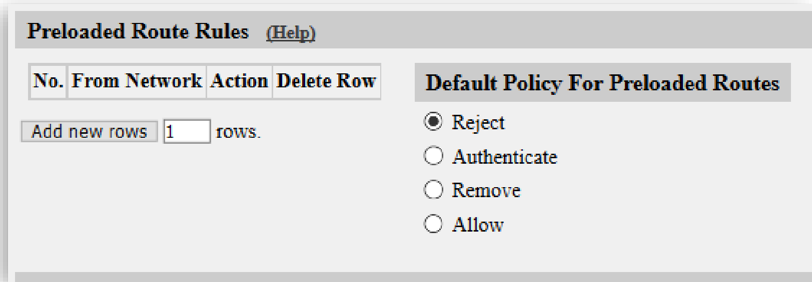


Figure 44

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

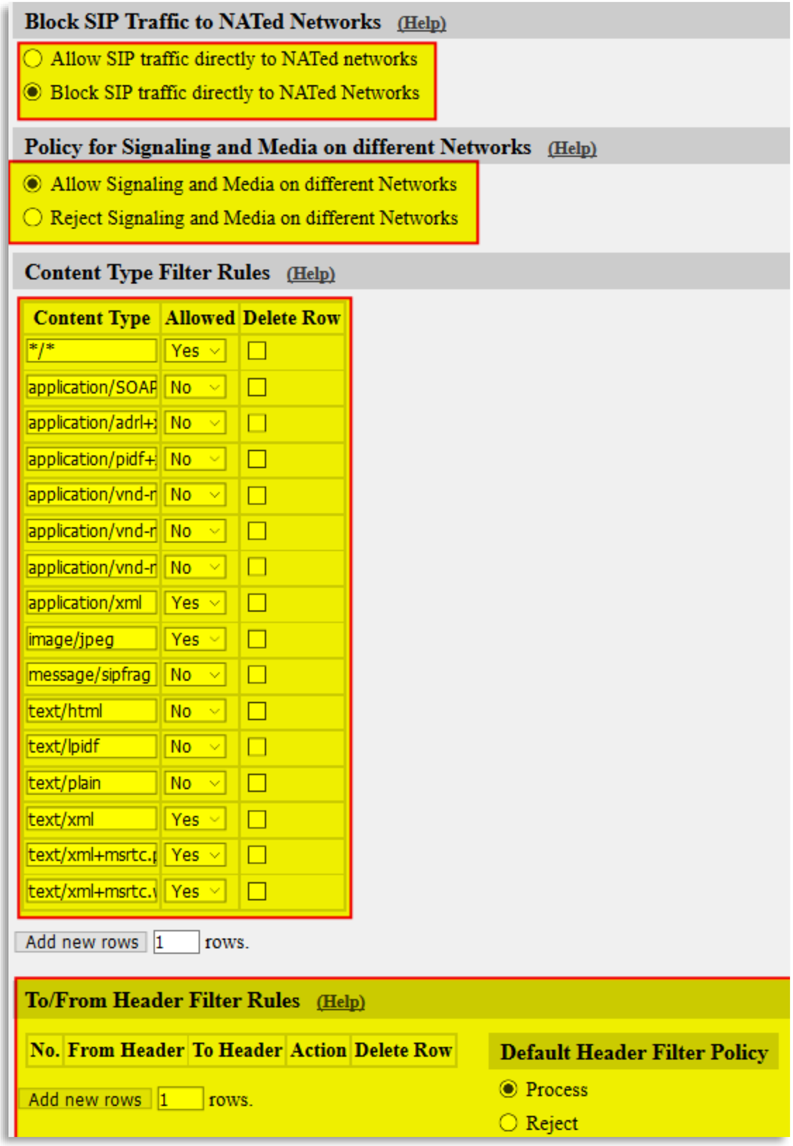


Figure 45

- 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/x-msmsgsinvite" 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.

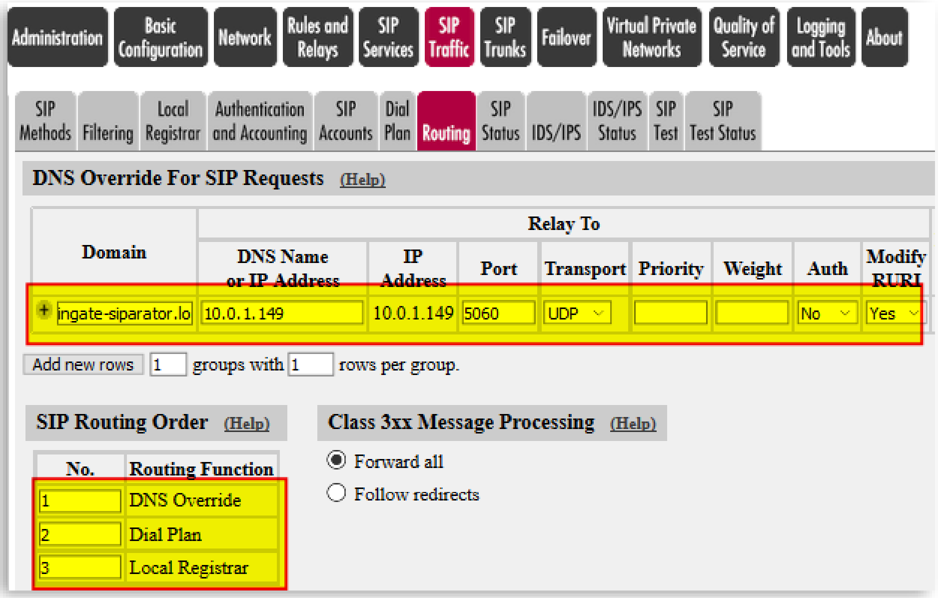


Figure 46

- 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.xxxxxxxx.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.

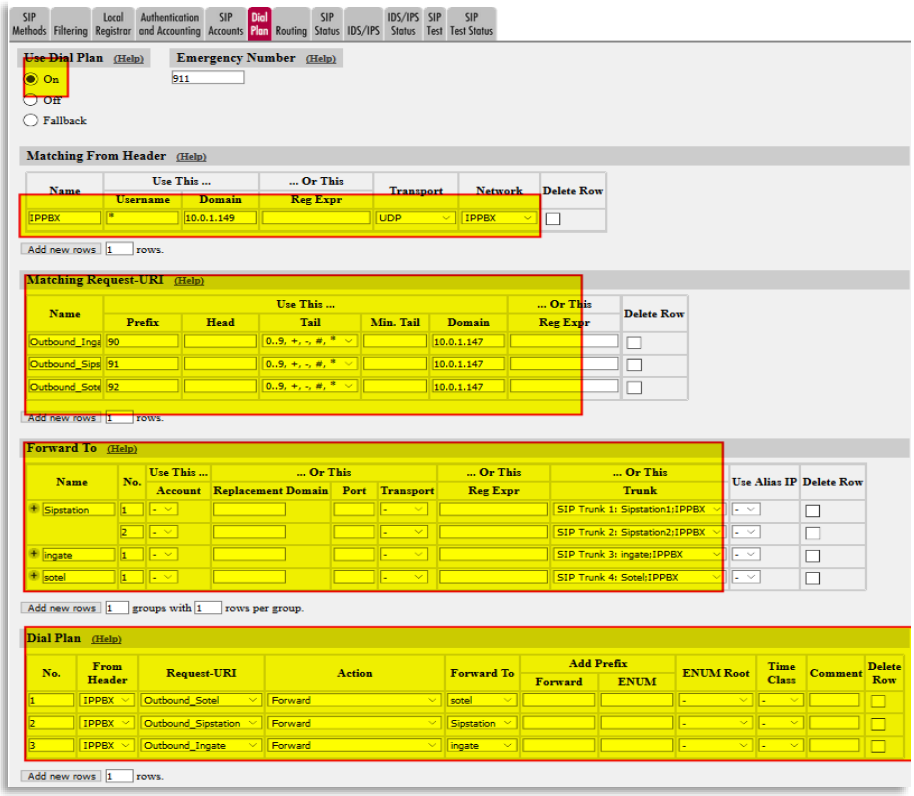


Figure 47

- 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

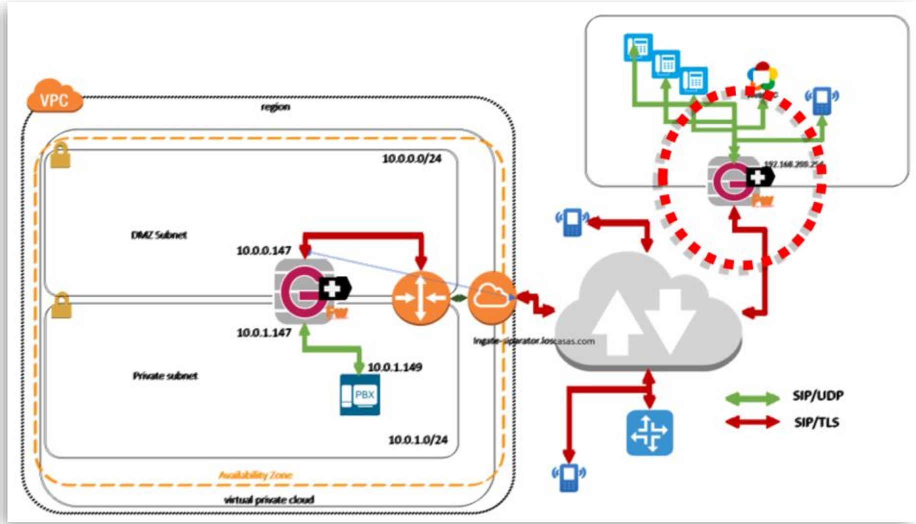


Figure 48

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.

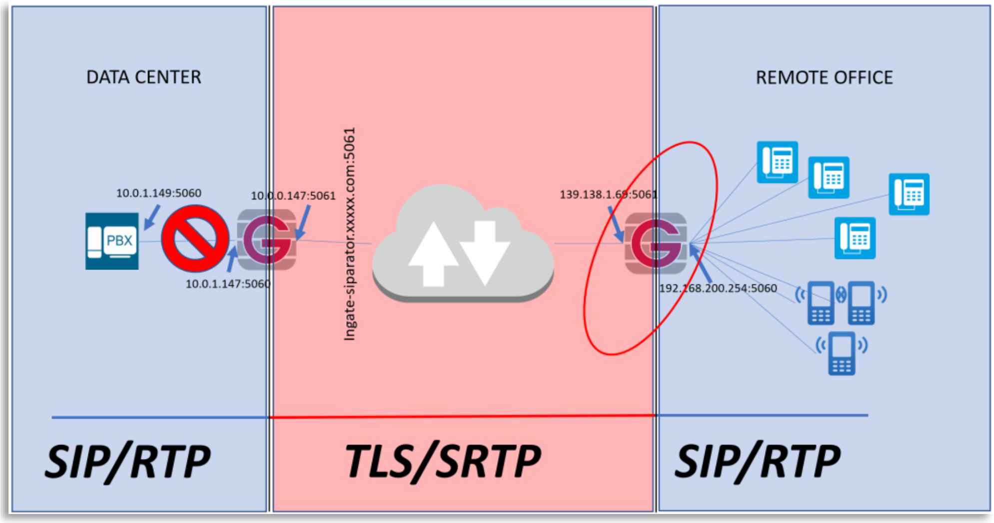
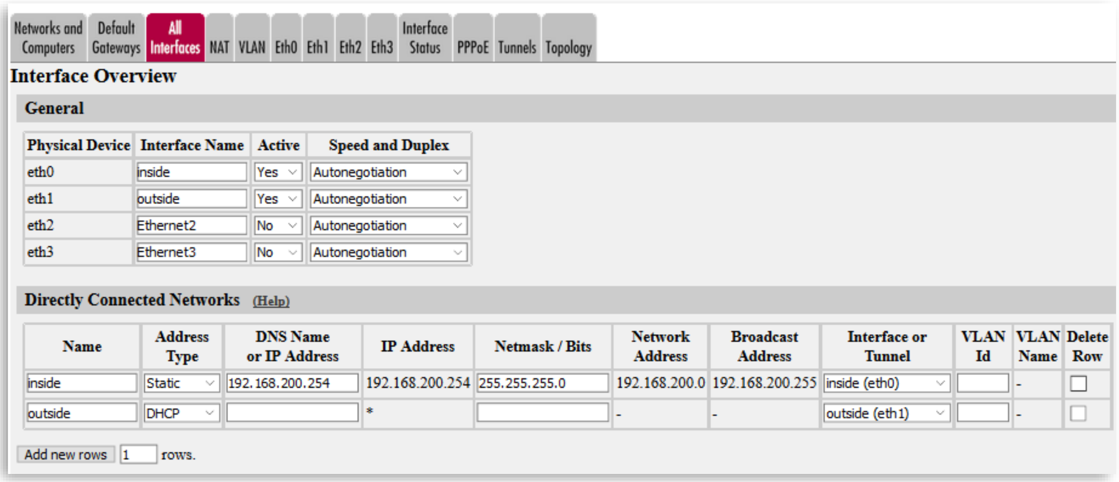


Figure 49

A summary on how the Network has been configured here:



Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Interface Status | PPPoE | Tunnels | Topology

Interface Overview

General

Physical Device	Interface Name	Active	Speed and Duplex
eth0	inside	Yes	Autonegotiation
eth1	outside	Yes	Autonegotiation
eth2	Ethernet2	No	Autonegotiation
eth3	Ethernet3	No	Autonegotiation

Directly Connected Networks (Help)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel	VLAN Id	VLAN Name	Delete Row
inside	Static	192.168.200.254	192.168.200.254	255.255.255.0	192.168.200.0	192.168.200.255	inside (eth0)		-	
outside	DHCP		*		-	-	outside (eth1)		-	

Add new rows 1 rows.

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.

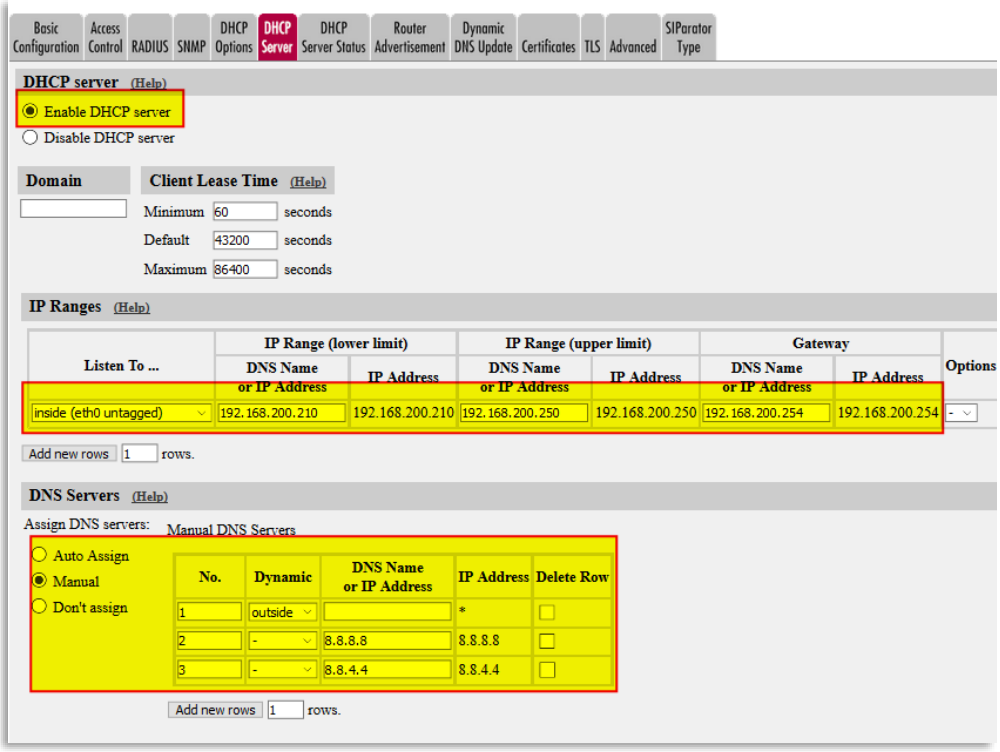


Figure 51

- 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.

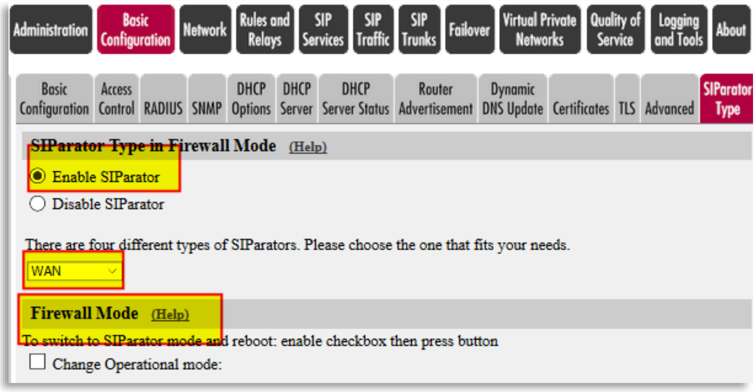


Figure 52

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.xxxxxxx.com); it is a FQDN resolving to the Public IP address of DC SIParator/Firewall

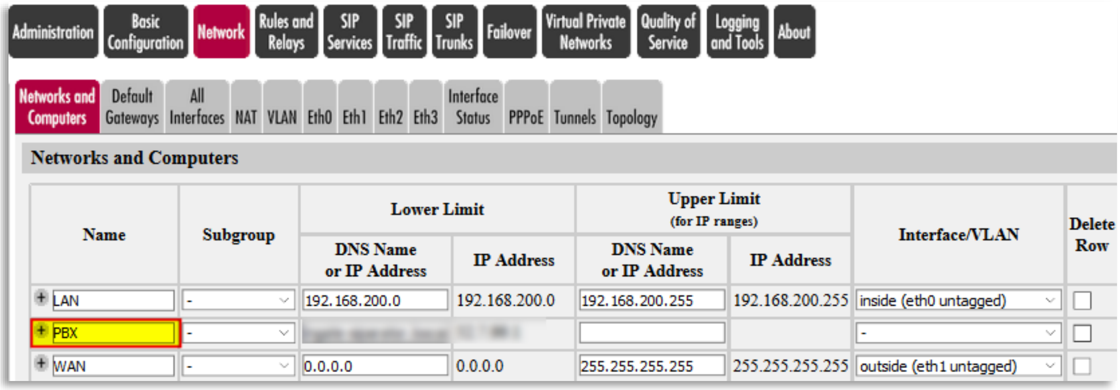


Figure 53

- 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:

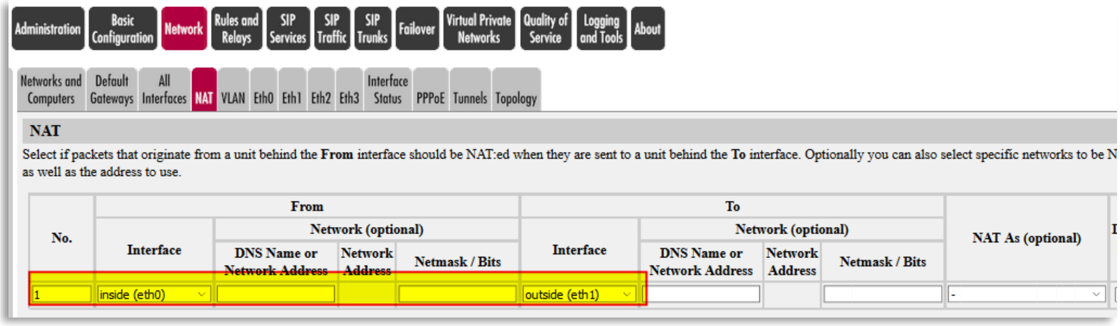


Figure 54

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***

- *Creating and Installing Server Certificates for SIParator*

4.4 RO Firewall Configuration - Rules and Relays

We allow freely traffic WAN ←→ LAN. It can be adjusted to specific needs depending on the real-world scenario.

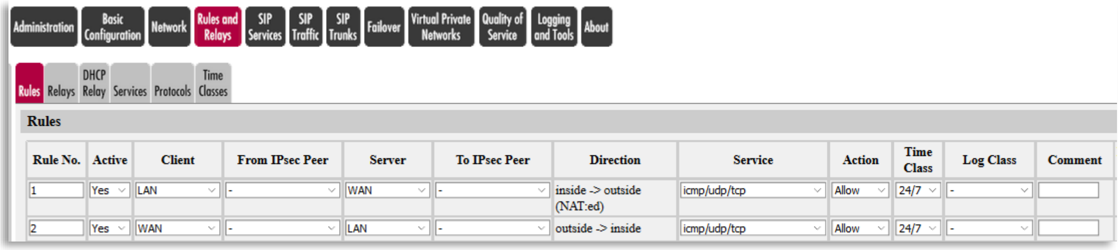


Figure 55

4.5 RO SIP Services

4.5.1 Basic configuration

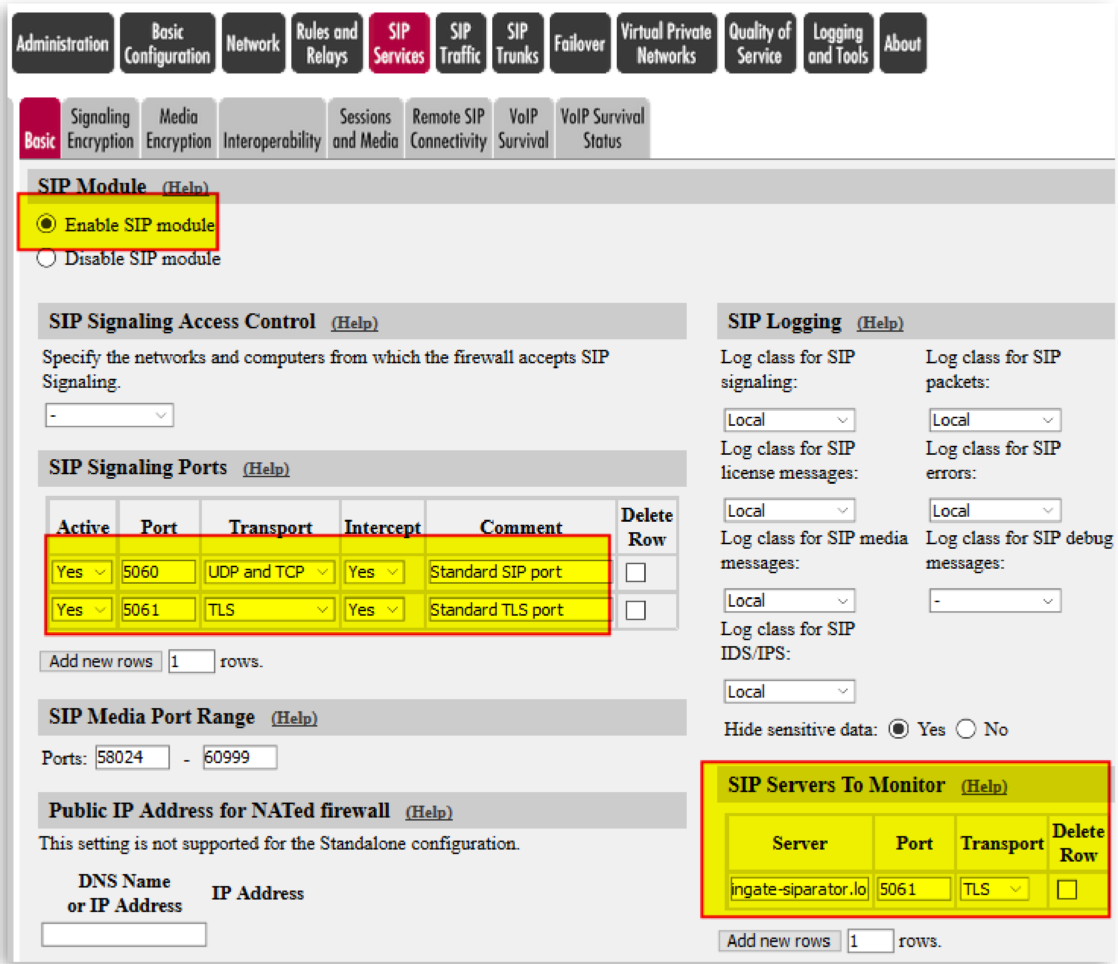


Figure 56

- 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

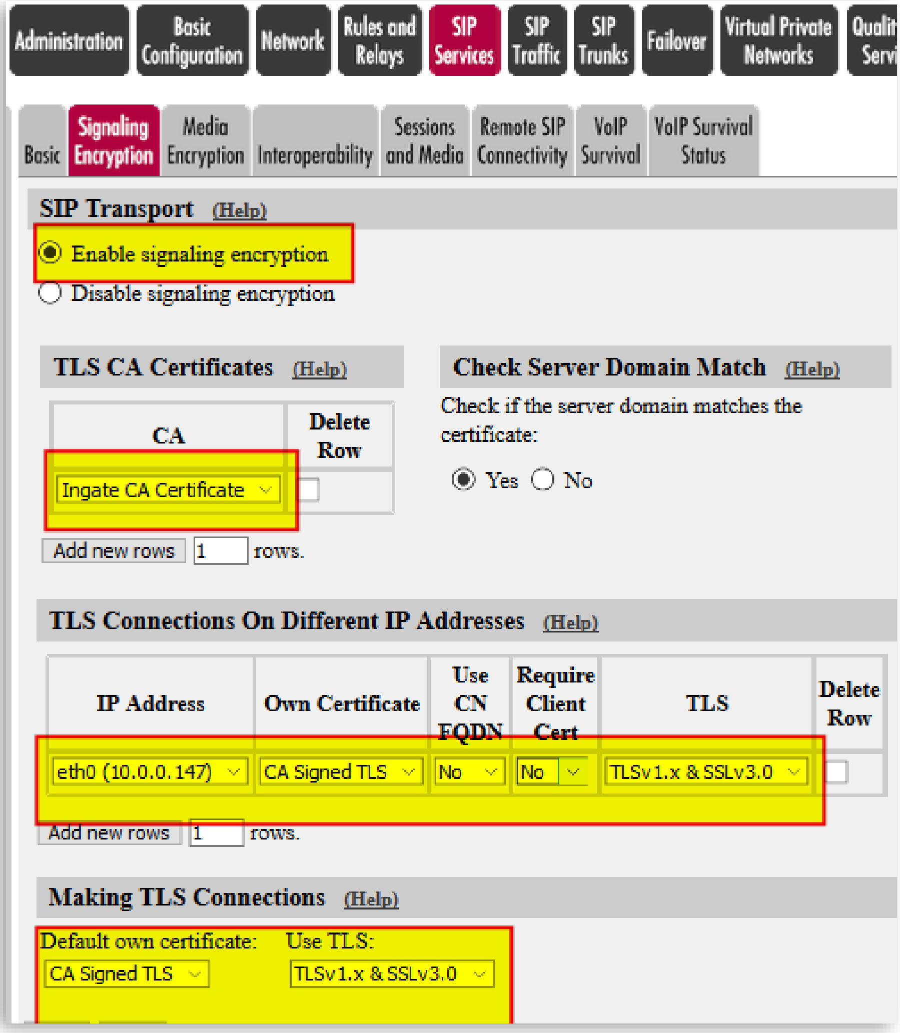


Figure 57

- 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.

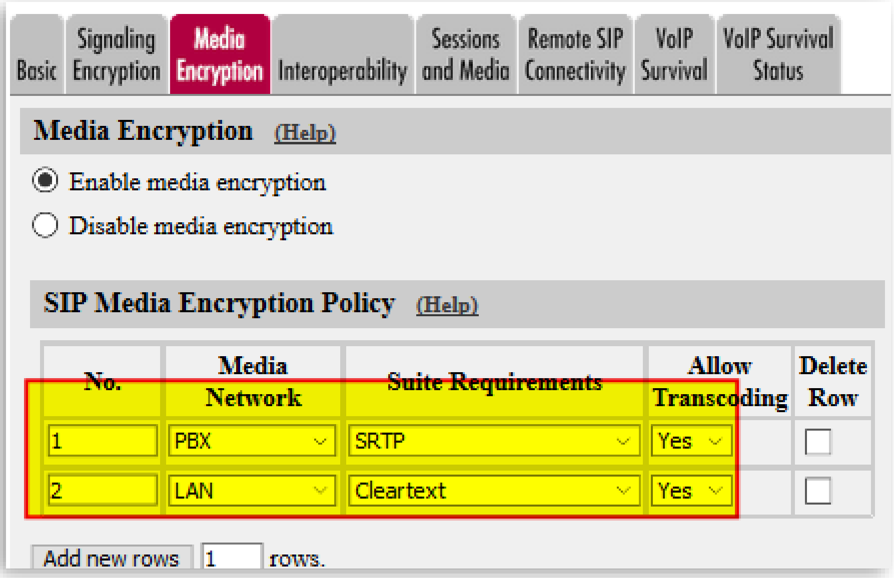


Figure 58

- 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.

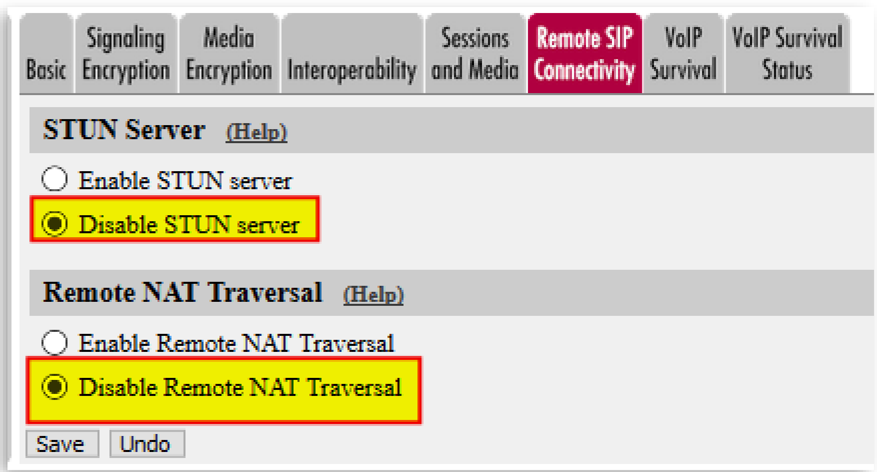


Figure 59

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.

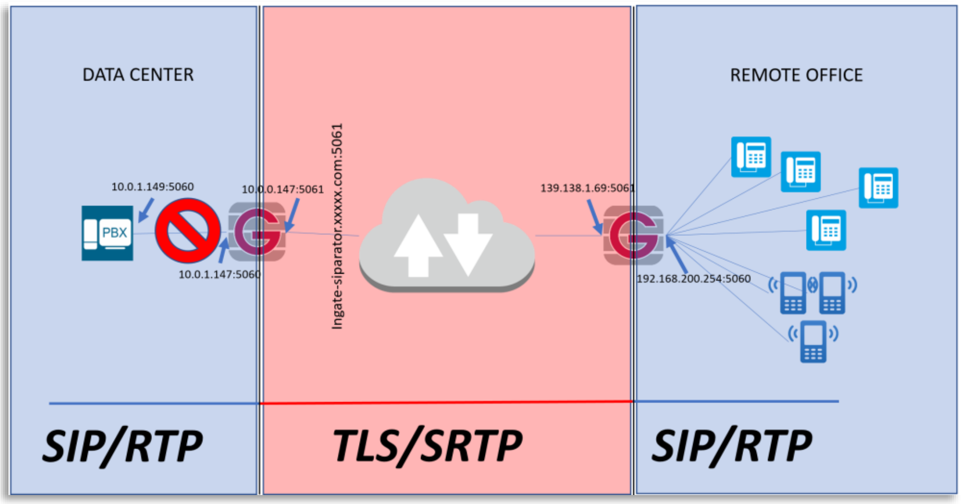


Figure 60

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.

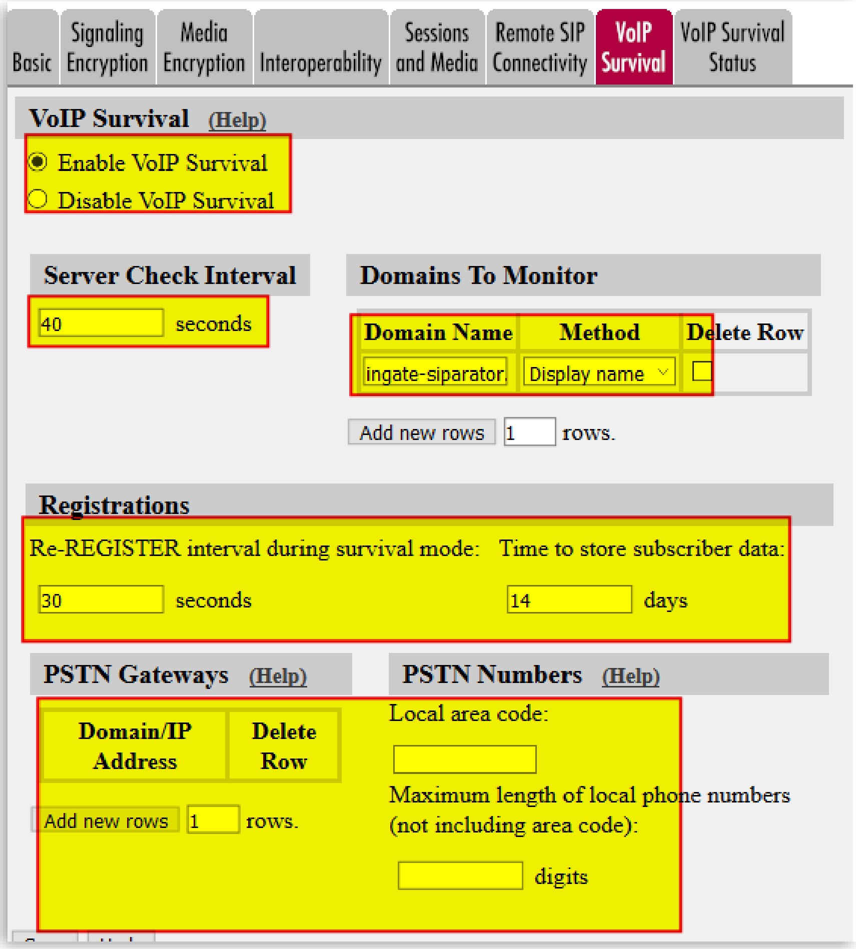


Figure 61

- 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 ←→ TLS.

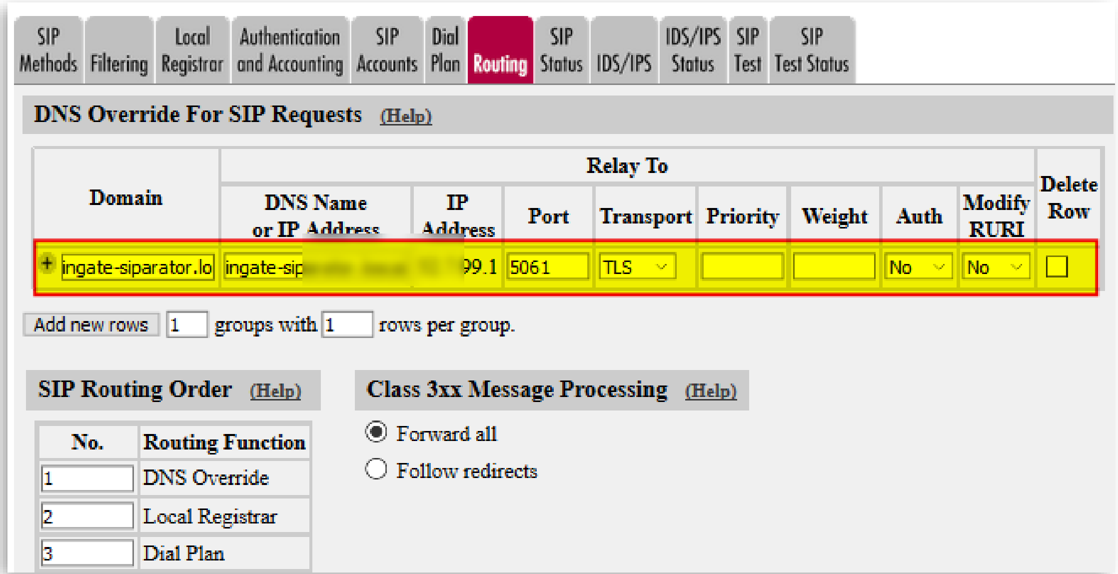


Figure 62

- 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:

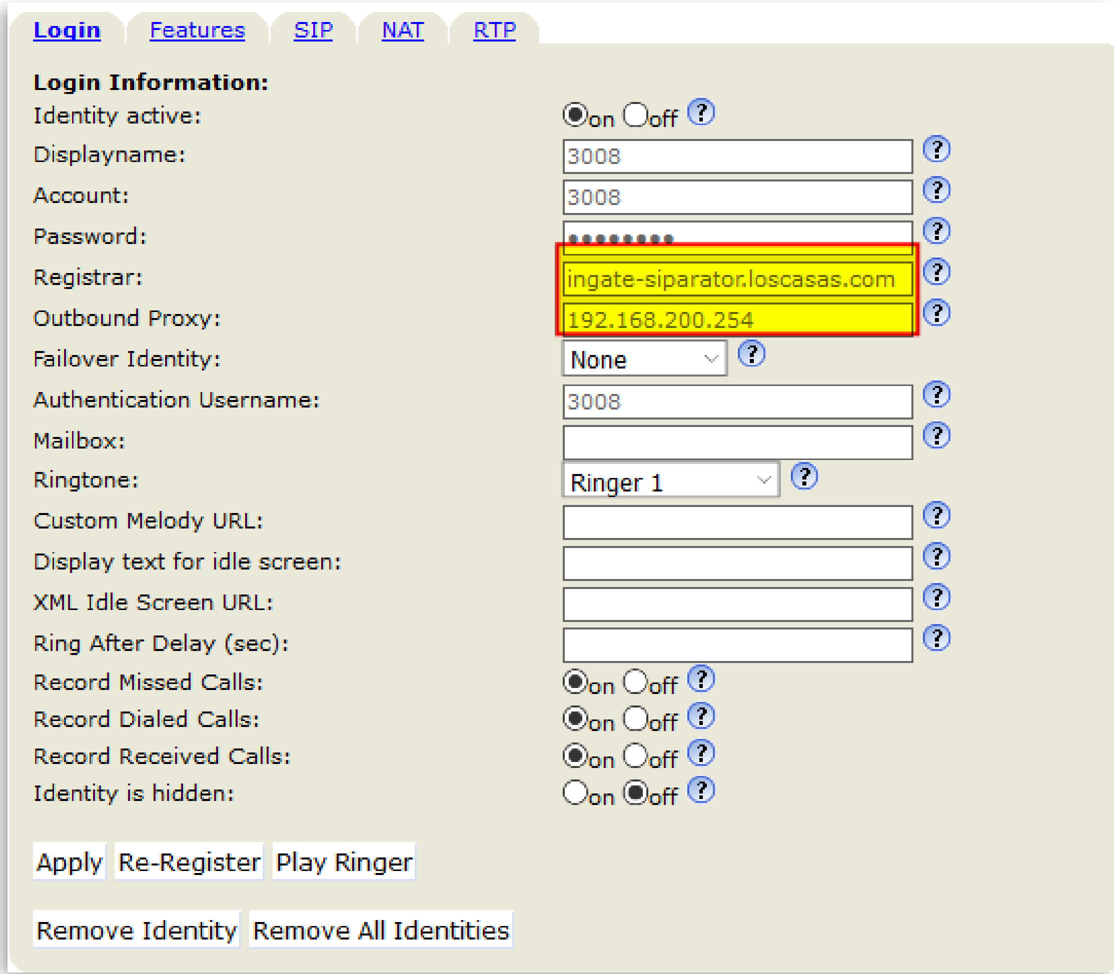
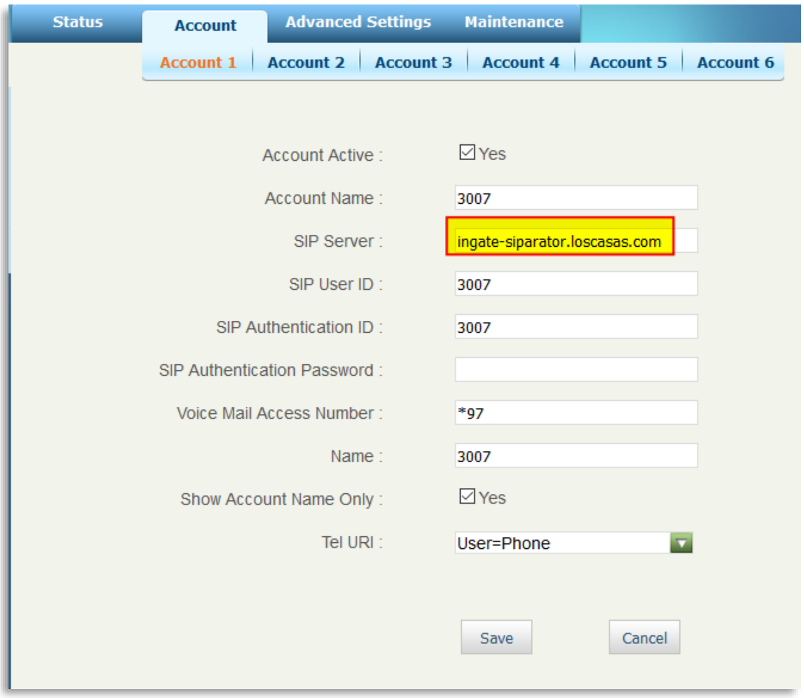


Figure 63

- 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



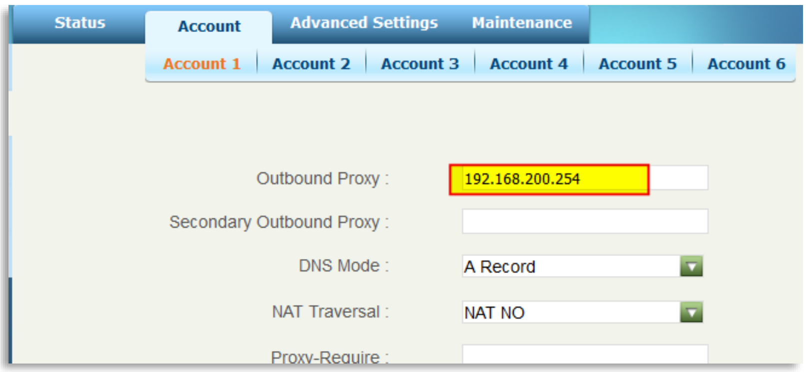


Figure 64

- 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

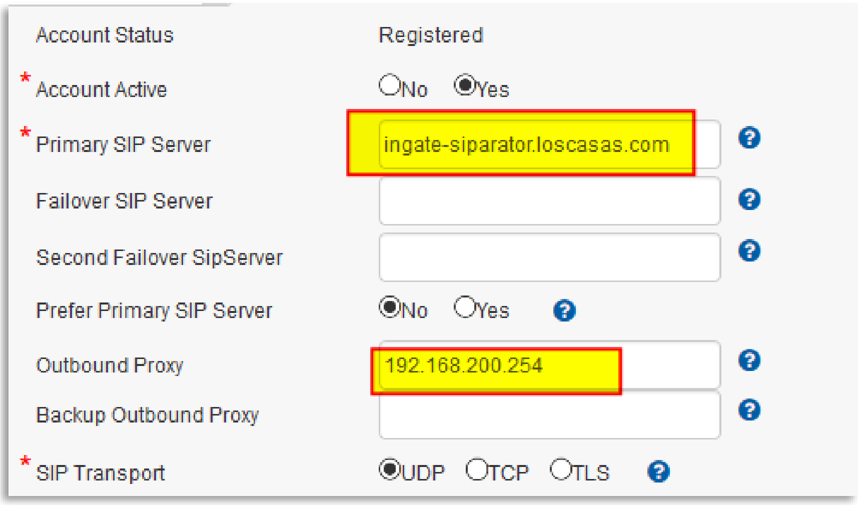


Figure 65

- 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 ☺**

---END---