

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]

1	INTR	ODUCTION	4
	1.1 DE	TAILED USE CASE	5
	1.2 Ass	UMPTIONS BEFORE STARTING	7
	1.3 INC	GATE SIPARATOR®/FIREWALL® SUPPORTED	7
	1.3.1	Ingate SIParator®/Firewall® S21	7
	1.3.2	Ingate SIParator®/Firewall® S52	7
	1.3.3	Ingate SIParator®/Firewall® S95/S97/S98	7
	1.3.4	Ingate Software SIParator®/Firewall®	8
2	SSL C	ERTIFICATES CREATION	9
	2.1 USI	NG SIMPLE AUTHORITY	9
	2.2 INS	TALLING SIMPLE AUTHORITY FOR WINDOWS	.10
	2.3 SEI	TING UP CA CERTIFICATE ON THE SIDADATOD	12
	2.4 INS 2.5 CRI	TALLING CA CERTIFICATE ON THE STFARATOR	. 12
	2.5 CK		. 13
3	INGA	TE DATA CENTER NODE CONFIGURATION	. 19
	3.1 BAS	SIC CONFIGURATION	. 19
	3.1.1	Access Control	. 20
	3.1.2	SIParator Type	. 21
	3.2 NE	TWORK CONFIGURATION	. 21
	3.2.1	Networks and Computers	. 21
	3.2.2	Defining Outside Interface:	. 23
	3.2.3	Defining Inside Interface:	. 24
	3.2.4	Configuring NAT	. 25
	3.3 INS	TALLING CERTIFICATE ON INGATE DATA CENTER	.26
	3.4 FIR	EWALL CONFIGURATION - KULES AND RELAYS	.27
	3.5 SIP	Besie een Germatien	.30
	3.5.1	Basic configuration	.30 22
	3.5.2	Media Encryption	. 32
	354	Remote SIP Connectivity	. 33 34
	355	VoIP Survival	. 35
	3.6 SIP	TRUNKS	.36
	3.7 SIP	TRAFFIC	.40
	3.7.1	Allowed SIP Methods	.41
	3.7.2	Filtering	.42
	3.7.3	Routing	. 45
	3.7.4	Dial Plan	.46
4	INGA	TE REMOTE OFFICE NODE CONFIGURATION	47
т			
	4.1 RO	BASIC CONFIGURATION	.47
	4.1.1	DHCP Server	.49
	4.1.2	SIParator Type	.49
	4.2 KO	Networks and Computers	.50
	4.2.1	Networks and Computers	. 50 50
	4.2.2	TALLING CEPTIEICATE ON INCATE REMOTE OFFICE	50
	4.5 INS	FIREWALL CONFIGURATION - RULES AND RELAYS	.50
	4.5 RO	SIP SERVICES	.51
	4.5.1	Basic configuration	.51
	4.5.2	Signaling Encryption	.53
	4.5.3	Media Encryption	. 54
	4.5.4	Remote SIP Connectivity	. 54
	4.5.5	VoIP Survival	. 55
	4.6 RO	SIP TRAFFIC	. 56

	4.6.1 RO Routing	4.6.1	
58	ADDITIONAL INFORMATION	ADD	5
	5.1 ENDPOINT CONFIGURATION EXAMPLES	5.1 En	

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:

1

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 • 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

SimpleAuthority - InGate Systems CA									
File View T	ools Help								
Active -	Certificate Details		Namo						
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 SIP SIP SIP Traffic Trunks Failover Virtual Private Quality of Service Administration Configuration									
Changes have been made to the prelin	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 Certificates (Help)								
Name	CA Certificate	CA CRL	Information					
InGate CA	Change/View	Change/View	Subject: /C=US/O=Pre-Sales Engineering/OU=Certification /CN=InGate Systems CA Issuer: /C=US/O=Pre-Sales Engineering/OU=Certification /CN=InGate Systems CA MD5 Fingerprint: SHA1 Fingerprint: Valid from: 2017-08-09 15:45:48 Valid to: 2027-08-10 15:46:01 Subject Key ID: Authority Key ID:	on Authority n Authority D:55:06 0F 2497 8001 3:F9:5E:51:84				

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 Acc Configuration Cor	cess ntrol RADIUS	SNMP	Dynamic DNS Update	Certificates	TLS Ad	vanced	IParator Type		
Private Cer	Private Certificates (Help)								
Name			Certific	cate				Information	
No certificate	No certificate exists.								
No value giv TLS Voice Sign	ren. Crea ned	ate New	Import	View/Do	ownload	No c	urrent c	ertificate	

Figure 9

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

Create Certificate or C	Certificate Reques	st				
Fill in the certificate data for	r "TLS Voice Signed	ed" below, then create either a certificate or a certificate reque	est.			
After generating a certificate	e request, and having	ng it signed by a signing authority, the certificate must be impo	orte			
Expire in (days): Co * 365 U: Common Name (CN): St * ingate-siparator.lo Email address Lo ernesto@ingate.co	ountry code (C): S tate/province (ST): L ocality/town (L):	Organization (O): Ingate Organizational Unit (OU): Support				
SubjectAltName Exten	sion					
Enter the alternative names to request. Multiple values can Email: ernesto@ingate.com URI: DNS: ingate-siparator.losca IP: 52.7.99.1	that you want to add t be added by using c asas.co	d to a certificate or a certificate comma separation.				
Key Length and Signat	ture 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 numbers.						
Serial number:						
* 3 Fields marked with "*" are mandatory.						
Create a self-signed X.509 ca	ertificate Create a	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.

 Certificate request created: Subject: /C=US/ST=FL/O=Ingate/OU=Support/CN=ingate-siparator.loscasas.com/emailAddress=ernesto@ingate. SubjectAltName: email:ernesto@ingate.com, DNS:ingate-siparator.loscasas.com, IP Address:52.7.99.1 									
Basic Configuration	Basic Access Dynamic Dynamic Configuration Control RADIUS SNMP DNS Update Certificates TLS Advanced Type								
Private C	Certifi	cates	<u>(Help)</u>						
Nan	1e			Certific	ate				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 SubjectAltName: email:ernesto@ingate.com SubjectAltName: email:ernesto@ingate.com SubjectAltName: email:ernesto@ingate.com DNS:ingate-siparator.loscasas.com Import									

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=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
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).

👺 SimpleAuthority - InGate Systems CA											
File View	File View Tools Help										
S S I (Certificate Details										
Active	CA Certificate Details		Name								
	Log File	•	ingate-siparator.losc								
	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 certificat	te.		
Certificate Type:		General	Purpose	\checkmark
Certificate Validity:		365	days	
• Use Subject DN from	request			
E=ernesto@ingate.cor	n,CN=ingate-s	siparato	or.loscasas.c	com,OU=Support,O=Ingate,ST=FL,C=US
OUse custom settings f	or Subject DN	l		
Common Name	ingate-sipara	tor.losc	asas.com	
Email Address	ernesto@inga	ate.com	1	
🖂 Organisational Unit	Support			
Organisation	Ingate			
Country	United States	5		
⊡ Include extension req	uests from CS	R		
		Car	ncel OK	
		Figu	re 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	Certificate Type:	General Purpo	ose 🗸	
✓ Ingate-siparator.ioscas	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	<u>(Help)</u>						
Na	me			Certifi	cate				Information
TLS Voice	Signed	Crea	ite Nev		View/Do	ownle	oad Sub sipa Sub sipa	ject: /C=U rator.loscas: jectAltNan rator.loscas:	S/ST=FL/O=Ingate/OU=Support/CN=ingate- as.com/emailAddress=ernesto@ingate.com ae: 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 Configuration Control	RADIUS SNMP	Dynamic DNS Update	Certificates TLS Adv	anced SIParator Type							
Private Certific	Private Certificates (Help)										
Name		Certifica	ate	Information							
TLS Voice Signed	Create Nev	/ 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:45 SHA1 Fingerprint: E7C 73EI Valid from: 2017-08-09 17:55:11 Valid for: 2018-08-09 17:55:12 SubjectAltName: 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.

Administration Basic	Basic Configuration Netw	vork Rules and Relays DHCP DHCI	SIP SIP SIP Si Traffic Tru P DHCP	IP nks Failover Virtua Net Router Dynamic	l Private works	Quality of Service	Loggi and To	ing pols Aba	ator		
Configuration	Control RADIUS SN	MP Options Serve	er Server Status Adv	ertisement DNŚ Updo	te Certific	ates TLS #	Advance	ed Typ	e		
Configu	iration Allowed	Via Interface	(Help)								
Add new	ce or Tunnel Allow (eth0) Yes eth1) Yes rows 1	red Delete Rom		Phy Inter	sica face	l s					
Configu	iration Transpor	t <u>(Help)</u>						_			
Protoc	ol IP Addre	ss Port	Cert	TLS		Delete R	low				
НТТР	eth0 (10.0.0.14	80	-	× -	~		_		Ma	anagem	ent
HTTPS	× -	× 443	httpsconfig	V TLSv1.x	~		_		F	Protocol	s
SSH	×	22	l	×	~						
Add new	rows 1 rows.										
User A	uthentication Fo	r Web Interfa	ce Access (Help	<u>)</u>	_						_
• Loca	l users					Orig	gina	ating	g Net	tworks	
⊖ RAE	IUS database					allo	we	d to	acco	ess for	
🔿 Loca	l users or RADIUS	database					ma	ana	geme	ent	
Web In	terface Access Se	ettings (Help)					<hr/>				
Login tim	eout: 28800 sec	onds									
Configu	aration Compute	rs <u>(Help)</u>							4		
No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IP:	sec Peer	SSH	нттр	HTTPS	Log Class	Delete Row
1	10.0.0	10.0.0.0	16	10.0.0.0 -	-	~				-	-
2	192.168.200.0	192.168.200.0	24	192.168.200.0 -	-	~				-	
2		0.0.0.0	0	192.168.200.255							
3	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	sic vration	Network	Rules a Relay	ind rs Sei	SIP rvices Traffic	SIP Trunks Failov	ver Virtual P Netwo	rivate Qua orks Sei	lity of vice	Logging and Tool	About
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 SIPara e SIPar four dif	ator ator ferent ty	pes of	SIPara	tors. Pl	ease choose	the one that f	fits your ne	eds.			
Firewall	Mode	(Help)									
To switch t Chang Save Ur	o SIPar e Opera ndo	ator mo ational r	de and node:	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:

Administration Bas Configu Networks and Default Computers Gateway Networks and O	ic ration Network All rs Interfaces NAT Computers	Rules and Relays Services VLAN EthO Eth1	SIP Traffic Trunks Faile	over Virtual Private Networks els Topology	Quality of Logging Service and Tools	About
News	C. L.	Lower	Limit	Upper (for IP	· Limit ranges)	Later for a CVT A N
Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/ v LAIN
• ІРРВХ	- ~	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] - 🔍	1.00.000	110 110 1 40	1 m 1 m 1 m	110 110 1 40	- · ·
	- ~	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	- ~	Forth, Progilies carrie	102129-063	Forth, Proglin, card	182 179 46.3	Outside (eth0 untagged) >
+ Sipstation2	- ~	transfer transfer and	162 213 134 142		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:

Administration	Basic Configura	tion Network	Rules and Relays	SIP Services	SIP Traffic Trunks	Failover	Virtual Private Networks	Quality of Service	Logging and Tools Al	tuod	
Networks and Computers	Default Gateways	All Interfaces NA	T VLAN EI	h0 Eth1 1	iterface Status PPPoE	Tunnels To	opology				
General											
Physical de	evice: eth	10									
This int <mark>erf</mark>	ace is: 🔇	Active 🔿	Inactive								
Interfac <mark>e</mark> n	ame: Ou	tside									
Directly	Connec	ted Networ	ks <u>(Help</u>)							
Ner		Address	DNS	Name	IP	Notes	asla / Dita	Network	Broadcast	VLAN	VLAN
Ivar	пе	Туре	or IP	Address	Address	Neur	IASK / DIUS	Address	Address	Id	Name
eth0		Static 🗸	10.0.0.14	7	10.0.0.14	7 24		10.0.0.0	10.0.0.255		-
Add new ro	ows 1	fows.									
Alias (H	(alp)										
Below are t	the range	s from which	you can s	elect alias	es.						
10.0.0.1-1	0.0.0.254	1	-								
	DNS Nor										
Name or	IP Add	ress IP Add	ress Delet	e Row							
Add new ro	ows 1	fows.									
Proxy A	RP (He	<u>lp)</u>									
			Prox	y ARPed	Network						
Get Netw	ork Fro	m DNS Na Network	me or Address	Network	Address Ne	tmask / B	its VLAN Id	I VLAN N	ame Delete	Row	
Add new ro	ows 1	fows.									
Static Ro	outing	(Help)									
		Routed	Network				Rou	iter			
DNS I Network	Name or k Addres	ss Network	Address	Netma	ısk / Bits	Dynamic	DNS N or IP Ad	ame Idress	IP Address	Delete R	ow
0.0.0.0		0.0.0.0		0		- ~	10.0.0.1		10.0.0.1		
Add new ro	ows 1	fows.									
Save Un	ido Loc	k up all IP add	resses aga	ain							

- 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:

Administration	Basic Configurat	ion Network	Rules and Relays	SIP Services	SIP Iraffic	SIP Trunks	Failover	Virtual Pi Netwo	rivate rks	Quality ol Service	Loggir and To	ng ols Ab	out	
Networks and Computers	Default Gateways	All Interfaces NA	T VLAN EthO	D Eth1 S	terface Status	PPPoE	Tunnels	lopology						
General Physical de This interf Interface n Directly	evice: eth: ace is: name: Insi Connect	1) Active () de red Networ	Inactive											
Nar	ne	Address	DNS I	Name		IP	Net	nask / B	lits	Networ	k Broa	dcast	VLAN	VLAN
eth1		Static V	10.0.1.147	udress	10.0	0.1.147	24			10.0.1.0) 10.0.	1.255		-
Alias (H) Below are to 10.0.1.1-10 Name I or Add new ro	Lelp) the ranges 0.0.1.254 ONS Nam IP Addre ows 1 RP (Helt	from which te ess IP Addr frows.	you can sel	lect aliase Row	es.									
Get Netw	ork Fron	DNS Na Network	Proxy me or Address N	ARPed	Netwo Addres	ork ss Neti	mask / H	Bits	AN Id	VLAN	Name]	Delete	Row	
Static Ro	outing (Help)												
	1	Routed Netv	vork		-		R	outer		_				
DNS Na Network	ame or Address	Network A	ddress Net	tmask / H	Bits D	ynamio	DNS or IP	Name Address	IP Ad	ldress	Delete R	low		
Add new ro	ows 1 do Look	rows.	resses agair	n										

- 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 Netwo	rk Rules Rela	and 1ys	SIP Services	SIP Traffic	SIP Trunks	Failover	Virtual Pri Networ
Networks and Computers	Default Gateways	All Interfaces	NAT VLA	N EthO) Eth1	Interface Status	PPPoE	Tunnels	Topology
Main De	efault IPv	v4 Gatew	vays <u>(I</u>	<u>Ielp)</u>					
Priority	Dynamic	DNS	S Name		IP		Interf	200	Delete
110110	Dynamic	or IP	Addres	s	Addr	ess	Intera	a.c	Row
	- ~	10.0.0.1			10.0.0.	1 Ou	tside (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 S ervices Tre	SIP SI Iraffic Tru	IP nks Failover ^{Vi}	rtual Private Qu Networks S	vality of La iervice an	gging d Tools About				
letworks and Computers	Default All Gateways Interfaces	NAT VLAN EthO	Eth1 Sto	terface status PPI	PoE Tunnels Top	ology						
NAT												
Select if pa	ckets that originate	from a unit beh	ind the F	From int	orface should b	a MAT of mine	m there are	cont to a unit behind	the To int	orface Ontionally a	ou can also select spe	
networks to	o be NAT:ed, as we	l as the address	to use.		enace should t	e IVAL ed wile	in uley are	sent to a unit dennik	Tule IO III	errace. Optionally j		ecific
networks to	o be NAT:ed, as we	l as the address	to use.		enace should b	e IVAL ed whe	in mey are	To		errace. Optionally j		Bula
networks to No.	o be NAT:ed, as we	l as the address	to use. rom Networ	ork (optio	onal)	e IVAL ed whe	in they are	To Net	work (optio	onal)	NAT As (optional)	Dele
networks to No.	o be NAT:ed, as we Interface	as the address F	to use. rom Networ	ork (optio	onal) Netmask / B	its Inte	erface	To Netv DNS Name or	work (optic	onal) Netmask / Bits	NAT As (optional)	Dele Rov
No.	o be NAT:ed, as we Interface	as the address F DNS Name Network Ad	to use. rom Networ e or Ne dress A	ork (optio Vetwork Address	mal) Netmask/B	its Inte	erface	To Netv DNS Name or Network Address	work (optio Network Address	onal) Netmask / Bits	NAT As (optional)	Dele Rov
No.	o be NAT:ed, as we Interface	l as the address F DNS Name Network Ad	to use. rom Networ e or No dress A	ork (optio Network Address	onal) Netmask / B	its Outside (erface (eth0) >	To Network Address	work (option Network	onal) Netmask / Bits	NAT As (optional)	Dele Rov

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	sic vration	Rules and Relays Se	SIP SIP ervices Traffic	SIP Trunks Failover Virtual Private Quality of Logging About Service and Tools About								
Basic Access Configuration Control	RADIUS SNMP	DHCP DHCP Options Server	DHCP Server Status	Router Dynamic Idvertisement DNS Update Certificates TLS Advanced SIParator Type								
Private Certifi	Private Certificates (Help)											
Name		Certificat	te	Information								
CA Signed TLS	Create New	/ Import	View/Downloa	 Subject: //C=US/ST=FL/L=Coral Springs: O=ingste/CN=ingste- siparator.loscass.com/emailAddress=emesto@ingste.com Issuer: //C=US/O=Presales Engineering/OU=Certification Authority /CN=ingste Systems MD5 Fingerprint: SHAI Fingerprint: I Valid from: 2017-08-07 14:47:39 Valid fro: 2027-08-05 14:47:25 SubjectAlrName: email.emesto@ingste.com, DN5:ingste- siparator.loscass.com, IP Address:52.7.99.1 Subject Kev ID: i Authority Kev 								

Figure 27

CA Certificate:

Name	CA Certificate	CACRL	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-	
			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:

Administration	Ba: 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					
Rules Relays	DHCP Relay	Services Protocols	Time Classes									
Rule No.	Activ	e Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	t Delete Row
1	Yes	access ~	- ~	PrivateLan 💙	[Indeterminate interface -> Indeterminate interface	icmp/udp/tcp 💛	Allow ~	24/7 ~	- ~		
2	Yes	PrivateLan \vee	•	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 agrees shows ports pagesery for IDPRV related agrees

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	is	how	this	is	included	in	SIParator	config	iration
I ICIC	10	110 W	uno	10	menuaca	***	orr arator	comg	<i>i</i> rau011

Relays (Help)							
Listen '	Го	Rela	ay 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.

Administration Basic Network Rules and SIP SIP Services Traffic Trunks Failover Virtual Private Networks	Quality of Logging About and Tools	
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 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 debi messages: messages:	ug
Yes V 5061 TLS V Yes 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: 🖲 Yes 🔿 No	
Public IP Address for NATed firewall (Help)	SIP Servers To Monitor (Help)	
DNS Name DNS Name IP Address	Server Port Transport Row	ie r
or Ir Address	trunk1.freepbx.co	4
	trunk2.freepbx.co	
	10.0.1.149	
	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 Ti	SIP runks	Failover Virtu Ne	al Private tworks	Qualit Servi
Basic Signaling Media Encryption Encryption	Interoperability and M	ions Ren Aedia Con	note SIP nectivity S	VoIP urvival	VoIP Survival Status		
SIP Transport (Hell) Enable signaling en Disable signaling en	eryption cryption						
TLS CA Certificat	es <u>(Help)</u>	Chec	k Serve	r Don	nain Match	(<u>Help)</u>	
CA Ingate CA Certificate Add new rows 1	Delete Row	Check i certific: Ye	if the serv ate: is () No	ver do	main matche	s the	
TLS Connections C	On Different IP A	ddress	es <u>(Help</u>)			
IP Address	Own Certificate	Use CN FQDN	Require Client Cert	e	TLS	De	elete low
eth0 (10.0.0.147) 🗸	CA Signed TLS 🖂	No 🖂	No 🗸	TLS	v1.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 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 Services	SIP SIP Traffic Trunks Failov	er Virtual Priva Networks
Basic Signalir	ng <mark>Media</mark> on <mark>Encryption</mark> Inte	roperability Sessions Ro	emote SIP VoIP VoIP nnectivity Survival S	Survival tatus
Media E	ncryption (He	<u>lp)</u>		
Enable	media encryption	n		
O Disable	e media encryptic	n		
SIP Mee	dia Encryption	Policy (Help)		
No.	Media	Suite Requiremen	ts Allow	Delete
1	Internet	SPTP		Kow
2	Privatel an	Cleartext	Yes V	
Add new r	ows 1 rows Encryption Po	blicy <u>(Help)</u>		
Suite requ	irements:	Allow transcoding:		
Cleartext	~	◉ Yes ○ No		
-				_
Require	TLS (Help)			
Requir	re TLS for all cry	ptos but cleartext		
• Do no	t require 1LS			
RTP Pr	o file <u>(Help)</u>			
○ Prefer	RTP/SAVP (sde	scriptions)		
Prefer	RTP/AVP (clear	text and legacy encryp	tions)	
() 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.

Administration Basic Configuration Network Rules ar Relays	nd SIP SIP SIP SIP Failover Virtual Pri Services Traffic Trunks Failover Networ
Basic Encryption Media Interoperability and	essions Remote SIP VoIP VoIP Survival ad Media Connectivity Survival Status
STUN Server (Help) Enable STUN server Disable STUN server	
Remote NAT Traversal (Help) 	
IP address 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:	
Unconditional NAT Traversal (E) O Always use Remote NAT Traversal Image: Image: Only use Remote NAT Traversal with the second secon	Ielp) hen client looks NATed

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 Med Encryption Encryp	ia tion Interoperabilit	Sessions y and Media	Remote SIP Connectivity	VolP Survival	VoIP Survival Status	
VoIP Survival (Enable VoIP Sur Disable VoIP Survival Disable VoIP Survival Disable VoIP Survival	<u>Help)</u> rvival rvival					
Server Check I	interval I mds I	Domains T Domain Na ngate-sipara dd new rows	o Monitor me Me tor Display	thod name ×	Delete Row	
Registrations Re-REGISTER int 30 seco	erval during surv mds	vival mode:	Time to st	tore subs	criber data: 's	
PSTN Gateway	/S <u>(Help)</u>	PSTN I	Numbers	(Help)		
Domain/IP Address Add new rows 1	Delete Row rows.	Local are Maximun (not inclu	a code: 1 length of l ding area co digits	local pho ode):	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 Rules and SIP Relays Service	es Traffic SIP Trunks Failover Virtual Private Networks	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		
Carries name:	Color I	(Things description would
Service name.	30.6	(Conque descriptive rame)
Partrict to calls from:		(L' = No restriction)
Outbound Prosv		(FODN or IP address)
Use alias IP address:	L	(Forces this source address from our side)
Outbound Gateway:		('-' = Use Default Gateway)
Signaling Transport:		('-' = Automatic)
Port number:		(
From header domain:	Provider domain	
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:	. v	('-' = Don't use TGP)
Preserve Max-Forwards:	No V	
Relay media:	No Y	
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 \vee	
SIP 3xx redirection to caller domain:	No \vee	
Route incoming based on:	To header 🗸 🗸	
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)								
	Des		Outgoing	g Calls		Authe	ntication	Incoming	g Calls	
NO.	Reg	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)								
	PBX Lines (Help)									
			Outgoing	g Calls		Authe	entication	Incomi	ng Calls	Data
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.	Reg No ~	From PBX Number/User	Outgoing Display Name	g Calls User Name	Identity	Authe User ID	entication Password Change Password	Incomi Incoming Trunk Match 0291	ng Calls Forward to PBX Account 0291	Delete Row
No. 6 7	Reg No ~ No ~	From PBX Number/User	Outgoing Display Name	g Calls User Name	Identity Inbound DID rounting. Destination in the PBX	Authe User ID	Password Change Password Change Password	Incomi Incoming Trunk Match 0291 0292	ng Calls Forward to PBX Account 0291 0292	Delete 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	IPP from	IPPBX can be defined here, or you can choose from an existing IPPBX defined in another Trunk Page							
PBX Name: IPPBX	(Uni	ique descriptive name,							
Use alias IP address: - 🗸	(For	rces this source addres	s from our side)						
	Auth	entication	PBX IP A	ddress					
PBX Registration SIP Address	User ID	Password	DNS Name or IP Address	IP Address	PBX Domain Name				
		Change Password	10.0.1.149	10.0.1.149					
(At least one of PBX Registration, IP ad	ddress or Doma	in Name is required to	locate the PBX)						
PBX Network: Signaling transport: Port number:	IPPBX UDP ~ 5060	✓]	('-' = Aut	omatic)	IPPBX IP Address located in the Private subnet				
Match From Number/User in field:	From UF	য	~						
Common User Name suffix:				_					
To header field:	ame a:	s Request-URI 🖂			Adjust Parameters				
Forward incoming REFER:	No			IF	PPBX requirements				
Remote Trunk Group Parameters u	sage: -		('-' = Dor	ı't use TGP)					
Local Trunk Group Parameters usa	ge: -		✓ ('-' = Dor	ı'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.

l	Administra	tion Cor	Basic nfiguration	Network Rul R	es and elays Se	SIP ervices	SIP Traffic	SIP Trunks	Failove	r Virt N
L	ogged in	ı as adm	nin (Full A	Access) using	local pa	sswoi	r d .			
	SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	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 $\!$	No 🗠	
REFER	Both ~	Yes 🗠	No 🗠	
REGISTER	Both ~	Yes 🗵	Yes $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $	
SERVICE	Both ~	Yes 🗠	No ~	
SUBSCRIBE	Both ~	Yes 🖂	No 🗠	
	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).

ministration	Basic Configuration	Network Rule Re	is and lays So	SIP ervices	SIP Traffic	SIP Trunks	Failove	er Virtua Net	l Priva works	te Quality Servio
SIP Aethods Filte	Local ring Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Status
Sender I	P Filter Ru	les <u>(Help)</u>								
No.	From Network	Action	Del Ro	ete w	Def	ault F	olicy F	for SIP	Req	luests
1	IPPBX	Process all	<u> </u>		OL	local o	l only			
2	PrivateLan	Process all	<u>~</u> 🗆		• R	leject a	all			
3	SipTrunk	Process all	<u> </u>							
4	ingate	Process all	<u> </u>							
5	Office	Process all	<u> </u>							
Add new ro	ows 1 ro	WS.								

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 NAT	ed Networks (Help)	
Allow SIP traffic directly	to NATed networks	
Block SIP traffic directly to the second	to NATed Networks	
Policy for Signaling and I	Madia on different No	tworks (Holp)
Allow Signaling and Med	in on different Networks	works <u>(rieip)</u>
Reject Signaling and Med	lia on different Networks	
<u> </u>		
Content Type Filter Rule	es (<u>Help)</u>	
Content Type Allowed Do	elete 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.		
Add new rows 1 rows.		
To/From Header Filter R	Rules (<u>Help)</u>	
No. From Header To Head	der Action Delete Row	Default Header Filter Policy
Add new rows 1 rows		Process
nuo new lows 1 lows.		⊖ 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	tion Con	Basic figuration	Network Rule	es and elays	SIP Services	SIP Traffic	SIP Trunks	Failove	r Virtu Ne	al Priva tworks	te	Quality 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/IP: Status	5 SIP Test	S Test	SIP Status		
DNS	Overri	de For	SIP Reques	ts <u>(He</u> l	<u>lp)</u>									
								Relay I	Ĩo					
	Domain	1	DNS Nar or IP Add	ne ress	IF Addi	ress	Port	Trans	sport	Priori	ity	Weigh	t 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	g Order	(Help)	Clas	s 3xx	Messa	ige Pro	cessing	g <u>(He</u>	<u>lp)</u>				
N	o. R	outing I	Function	• F	orward	all								
1	D	NS Ove	rride	O Fe	ollow 1	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.

se Dial Plan	n <u>(Help)</u>	Emer	gency N	umber (Help)									
0 On		911											
) Fallback													
fatching Fi	rom Hea	der (Help)											
		Use This		Or This									
Name	User	name D	omain	Reg Expr	Transp	ort Netwo	rk 1	Delete Row					
PPBX	•	10.0.	1.149		UDP	IPPBX	~						
dd new rows	1 ro	ows.											
fatching R	equest_I	R (Help)						_					
	equest e	and the first						0.71					
Name	Dava	6. I	Head	Use I his	Min. Tail	Domain		Or This	Delete Roy	x			
Dutbound Too	90		lieau	0.9. + #. *		10.0.1.147		Ceg LAPI		-			
baland Fra	0.					10.0.1.147				-			
Jutbound_Sips	91			09, +, -, #, *	<u> </u>	10.0.1.147							
				-									
Dutbound_Sot	92			09, +, -, #, *	<u> </u>	10.0.1.147							
Outbound_Sot	92			09, +, -, #, *	× []	10.0.1.147							
dd new rows	92 1 ro	ows.		09, +, -, #, *	 ✓ ✓ 	10.0.1.147							
outbound_Sot	92 1 rc (<u>Help)</u>	ows.		09, +, -, #, *	× []	10.0.1.147							
dd new rows	92 1 rc (Help)	ows. Use This		09, +, -, #, * Or Th	vis	<u>10.0.1.147</u>	115		Or This				
outbound_Sot dd new rows orward To Name	92 1 rc (Help) No.	Use This Account	Replaces	09, +, -, #, * Or Th ment Domain	iis Port Transpor	10.0.1.147	nis pr		Or This Trunk	U	se Alias IP	Delete Row	r
dd new rows orward To Name	92 1 rc (Help) No.	Use This Account	Replace	09, +, -, #, * Or Th ment Domain	is Port Transpot	10.0.1.147	nis pr	SIP Trunk	Or This Trunk 1: Sipstation1:I	U.	se Alias IP	Delete Row	F
dd new rows orward To Name F Sipstation	92 1 rc (Help) No. 1	Use This Account	Replace	0.9, +, -, #, *	iis Port Transpor	10.0.1.147	nis pr) SIP Trunk	Or This Trunk 1: Sipstation1;I 2: Sipstation2;I	U PPBX Y PPBX Y	se Alias IP	Delete Row	r
dd new rows orward To Name Sipstation	92 (Help) No. 1 2	Use This Account	Replaces	09, +, -, #, *	iis Port Transpor	10.0.1.147	nis pr	SIP Trunk	Or This Trunk 1: Sipstation1;1 2: Sipstation2;1 3: ingate:1PPB3	PPBX > - PPBX > -	se Alias IP	Delete Row	F
dd new rows orward To Name Sipstation	(Help) No. 1 2	Use This Account	Replaces	09, +, -, #, *	sis Port Transpor - ~ ~	10.0.1.147	nis pr	SIP Trunk SIP Trunk SIP Trunk	Or This Trunk 1: Sipstation1;1 2: Sipstation2;1 3: ingate;1PPB3 4: Samel/DPPY	PPBX >] - PPBX >] - PPBX >] -	se Alias IP	Delete Row	F
dd new rows orward To Name Sipstation	(Help) No. 1 1	Use This Account - ~ - ~ - ~	Replaces	09, +, -, #, * Or Th meat Domain	is Port Transpor - ~ ~ - ~ ~	10.0.1.147	nis pr	SIP Trunk SIP Trunk SIP Trunk	Or This Trunk 1: Sipstation1:1 2: Sipstation2:1 3: ingate:1PPB3 4: Sotel:1PPBX	PPBX →] - (→] - (→] -	se Alias IP	Delete Row	
dd new rows orward To Name * Sipstation * ingate * sotel dd new rows	(Help) No. 1 1 1 1 1 1 1 1 1 1 1 1 1	Use This Account	Replace	09, +, -, #, *	is Port Transpor	10.0.1.147	nis pr	SIP Trunk SIP Trunk SIP Trunk	Or This Trunk 1: Sipstation1;1 2: Sipstation2;1 3: ingate;1PPB3 4: Sotel;1PPB3	PPBX → (→) = (→) =	se Alias IP	Delete Row	
dd new rows orward Io Name Sipstation Ingate Sotel dd new rows	(Help) No. 1 1 1 1 1 1 1 1 1	Use This Account	Replaces	Or Th Or Th meat Domsin 	iis Port Transpor C ~ ~ C ~ ~ C ~ ~	10.0.1.147	nis pr	SIP Trunk SIP Trunk SIP Trunk	Or This Trunk 1: Sipstation1;1 2: Sipstation2;1 3: ingate;1PPBX 4: Sotel;1PPBX	PPBX →] [- (→) [- (→) [- (→)] [-	se Alias IP	Delete Row	
dd new rows orward To Name F Sipstation F ingate f sotel dd new rows bial Plan g	(Help) (Help) 1 1 1 1 1 1 1 1	Use This Account > > > > > >	Replaces	Or The ment Domain	is Port Transpor C ~ ~ C ~ ~ C ~ ~	ID.0.1.147	nis pr	SIP Trunk SIP Trunk SIP Trunk	Or This Truak 1: Sipstation1:1 2: Sipstation2:1 3: ingate:1PPB3 4: Sotel;1PPB3	PPEX V PPEX V C V C V C	se Alias IP	Delete Row	
dd new rows orward To Name Sipstation Ingate Sotel dd new rows Sial Plan g	(Help) (Help) 1 1 1 1 1 1 1 1 1 1 1 1 1	Use This Account 	Replaces	09, +, -, #, #	iii Port Transpor	10.0.1.147	niz pr	SIP Trunk SIP Trunk SIP Trunk SIP Trunk Add Pr	Or This Trunk 1: Sipstation1:T 2: Sipstation2:T 3: ingate:1PPB: 4: Sotel:1PPBX	PPEX V PPEX V C PPEX V C	se Alias IP	Delete Row	
dd new rows orward To Name \$ Sipstation \$ ingate \$ sotel dd new rows Dial Plan g No. F	(192 (Help) No. 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Use This Account 	Replaces	Or The meet Domain er group.	ini Port Transpor	iii.o.i.147	nis pr	SIP Trunk SIP Trunk SIP Trunk SIP Trunk	Or This Trunk Sipstation2:1 Sipstation2:1 Sipstation2:1 Sipstation2:1 Sipstation2:1 Sotel:IPPEX efix ENUM	PPBX Y = PPBX Y = Y = Y = ENUM Rot	se Alias IP	Delete Row	
dd new rows orward To Name # Sipstation # ingate # socel dd new rows bial Plan g No. F F H. IPS	(192 (Help) No. 1 2 1 1 1 1 1 1 1 1 1 1 2 2 1 1 2 2 2 1 1 2 2 2 1 1 2 2 1 1 2 2 2 1 1 2 2 2 1 1 2	Vie This Account	Replace rows p	o.g., +, -, #, *	sia Port Transpo - ~ ~ - ~ ~	10.0.1.147		SIP Trunk	Or This Truak 1: Systation1:1 2: Systation2:1 3: Ingate:1PPB3 4: Sotel:1PPBX 4: Sotel:1PPBX	PPEX > = PPEX > = C > = C > = ENUM Root	se Alias IP	Delete Row	r I
dd new rows orward To Name F Sipstation F ingate Sotel dd new rows Mal Plan P H 1 [PP: 1 [PP:	(Help) (Help) No. 1 2 1 1 1 1 5 7 7 7 7 7 7 7 7 7 7 7 7 7	Use This Account	Replace rows p -URI tel ~	6.9. +. , #, # Or Th next Domain er group	is Port Transpor	10.0.1.147		SIP Trunk SIP Trunk SIP Trunk SIP Trunk	Or This Trunk 1: Sipptation1:1 2: Sipptation2:1 3: ingate:1PPB: 4: Socel:1PPBX effx ENUM	PPEX 2 PPEX 2 C C C C C C C C C C C C C	se Alias IP	Delete Row	v t



- 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:

iterface Over	view	TLAN CINU D	2011 2002	z cina sidios ri	roc tonners topology						
General											
Physical Device	Interface Nam	e Active	Spee	d and Duplex							
eth0	inside	Yes 🗸	Autoneg	gotiation 🗸 🗸							
eth1	outside	Yes 🗸	Autoneg	gotiation \vee							
eth2	Ethernet2	No 🗸	Autoneg	gotiation 🗸 🗸							
eth3	Ethernet3	No 🗸	Autoneg	gotiation \sim							
Directly Conne Name	ected Networks Address Type	S <u>(Help)</u> DNS Na or IP Add	me Iress	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel	VLAN Id	VLAN Name	Dele Roy
inside	Static V 19	92.168.200.3	254	192.168.200.254	255.255.255.0	192.168.200.0	192.168.200.255	inside (eth0) 🗸 🗸		-	
				*		1.	-	outside (eth1)		-	

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.

Basic Acc Configuration Con	ess trol RADIUS	SNMP	DHCP Options	DHCP Server Ser	DHCP ver Status	Router Advertisement	Dynamic DNS Update	Certificates	TLS	Advanced 1	arator ype			
DHCP serve Enable DF Disable D Domain	er (Help) ICP server HCP server Cli Defa	ent La mum	ease Tin 60 43200	ne (Help secon secon	হ) .ds .ds									
IP Ranges	Max <u>(Help)</u>	imum	86400	secon	ds									
Lis	ten To		DN or I	IP Rang NS Name <mark>P Addres</mark>	e (lower	limit) IP Address	II DNS or IP	P Range (u S Name Address	ıppe	r limit) IP Address		Gate DNS Name or IP Address	eway IP Address	Options
Add new rows	untagged) s 1 rc rs <u>(Help)</u>	vws.	192.168	3.200.210	19	2.168.200.21	0 192.168.2	200.250	19	92.168.200.2	50 19	2. 168. 200. 254	192.168.200.254	- ~
Assign DNS s	servers: 1 sign	vlanua	DNS Se	ervers										
Manual		N	o. D	ynamic	DN or I	IS Name P Address	IP Addre	ss Delete	Row					
O Don't ass	sign	1 2	OL -	utside 🖂	8.8.8.8		*							
		3	-	~	8.8.4.4		8.8.4.4							
	[Add n	ew rows	1 ro	ows.									

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

Administration Configura	tion Network Rules Relat	and SIP SIP ys Services Traffic Tr	SIP unks Failover Virt N	ual Private Letworks Service a	ogging nd Tools		
Networks and Computers Gateways	All Interfaces NAT VLAN	I EthO Eth1 Eth2 Eth3	Interface Status PPPoE Tu	innels Topology			
Networks and C	omputers						
Nama	C. L.	Lower]	Limit	Upper (for IP r	Limit anges)	T- t- F- AT AN	Delete
Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/VLAIN	Row
1 LAN	- · ·	192.168.200.0	192.168.200.0	192.168.200.255	192.168.200.255	inside (eth0 untagged)	- -
🛨 рвх	- v	fragmentation income	12.149.0]	-	
1 WAN	- ×	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	$\overline{}$

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:

Networks and Computers Default Gateways All Interfaces VLAN Etho Eth Eth Interface PPPoE funnels Topology NAT Select 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 b as well as the address to use. To To No. Interface Network (optional) Interface Network (optional) NAT As (optional) Interface DNS Name or Network Network Netmask / Bits Interface Network Address Netmask / Bits	ion Basic Configuratio	n Network	Rules and SIP Relays Services Tr	SIP SIP affic Trunks	Failover Virtual Private Networks	Quality of Logging Service and Tools	bout				
NAT Select 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 b as well as the address to use. From To No. Interface Network (optional) DNS Name or Network Network Norwork Address Network Address Network Address No. Interface Network (optional) DNS Name or Network Network Network Address Network Address Network Address Network Address	and Default rs Gateways Ir	All nterfaces NAT	VLAN EthO Eth1 Eth2	Interfo 2 Eth3 Statu	ace Js PPPoE Tunnels Top	ology					
Select 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 b as well as the address to use. Select 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 b as well as the address to use. To NAT As (optional) No. Interface Network (optional) Interface NAT As (optional) DNS Name or Network Network Address Network Address Network Address Network Address											
To To No. Network (optional) Network (optional) Network (optional) NAT As (optional) DNS Name or Network Network Address Address Network Network Address Network Address Network Network Address Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network	i packets that or as the address t	riginate fro to use.	m a unit behind the F	rom interfac	ce should be NAT:ed	when they are sent to a	unit behind the To in	iterface. Opt	tionally you can also	select specific networks to	be N
No. Interface Network (optional) Network (optional) NAT As (optional) DNS Name or Network Address Network Address			From				То				
Interface DNS Name or Network Address Address Address Address Outside (eth.) Vetwork Address Network Address Outside (eth.) Vetwork Outside (eth.) Vet			Ne	twork (optio	onal)		Net	work (optio	onal)	NAT As (optional)	1
1 inside (eth0) v inside (eth1) v inside (eth1	. Inte	erface	DNS Name or Network Address	Network Address	Netmask / Bits	Interface	DNS Name or Network Address	Network Address	Netmask / Bits	rom no (optional)	
	inside (et	h0) 🗸				outside (eth1) 🛛 🗸]		-	~

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

Admin	istration	Basic Configurati	on Network Ru	iles a Relay:	d SIP SIP Services Traffic Tr	SIP unks Failover Virtu N	ual Private letworks Service	Logging and Tools About					
Rules	BHCP International International International International Internation												
R	Rules												
F	Rule No.	Active	Client		From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment
1		Yes 🗸	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 Configuration Network Rules and SIP Relays Services Traffic Trunks Failover Virtual Private	e 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.	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 local Local Local Local Local Local Log class for SIP media Log class for SIP debug messages: messages:
Yes Standard TLS port Add new rows 1	Local Log class for SIP IDS/IPS: 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 IP Address	Ingate-siparator.lo 5061 TLS

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 Configuration	Network Rules and Relays	SIP Services Traffic	SIP Trunks Failover Virtual Netv	Private Qualit vorks Servi				
Basic Signaling Media Encryption Encryption	Interoperability and M	ions Remote SIP Media Connectivity	VoIP VoIP Survival Survival Status					
SIP Transport (Help) Enable signaling encryption Disable signaling encryption								
TLS CA Certificat	es <u>(Help)</u>	Check Serve	er Domain Match	(Help)				
CA Ingate CA Certificate Add new rows 1	Delete Row rows.	Check if the set certificate: Yes O N	rver domain matches	the				
TLS Connections (On Different IP A	ddresses (Hel	<u>p)</u>					
IP Address	Own Certificate	Use Requir CN Clien FQDN Cert	re t TLS	Delete Row				
eth0 (10.0.0.147) 🖂	CA Signed TLS \vee	No 🗸 No 🗸	TLSv1.x & SSLv3.0					
Add new rows 1 rows.								
Making TLS Connections (Help)								
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	Media Encryption Intero	perability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Sur Statu	vival Is	
Media Encryption (Help)								
Enable n	Enable media encryption							
O Disable r	○ Disable media encryption							
SIP Media Encryption Policy (Help)								
			(IICIP)					
N	Media		the Descript		Al	low	Delete	
No.	Media Network	Su	iit e Re qui	rements	Al Trans	low <mark>co</mark> ding	Delete Row	
No.	Media Network	SRTP	iite Requi	rements ~	All Trans	low coding	Delete Row	
No.	Media Network PBX ~ LAN ~	SRTP Cleart	iite Requi	rements ~ ~	All Trans Yes	low coding	Delete Row	

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	Sessions and Media	Remote SIP Connectivity	VolP Survival	VoIP Survival Status			
ST	STUN Server (Help)									
0	 Enable STUN server Disable STUN server 									
Re	emote NA	T Trave	rsal <u>(Help)</u>							
0	O Enable Remote NAT Traversal									
۲	Oisable Remote NAT 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	Interoperabil	Sessions ty and Media	Remote SIP Connectivity	VolP Survival	VoIP Survival Status		
Va O	VoIP Survival (Help) Enable VoIP Survival Disable VoIP Survival								
S	erver Ch	eck Inte	rval 1	Domains T	o Monitor	r			
4	40 seconds Domain Name Method Delete Row ingate-siparator Display name								
R	egistrati	ons							
Re	-REGISTI	ER interva	l during sur	vival mode:	Time to st	tore subs	criber data:		
3()	seconds			14	day	s		
P	PSTN Gateways (Help) PSTN Numbers (Help)								
	Domain Addre	n/IP ess	Delete Row	Local area	a code:				
A	dd new row	/s 1 1	rows.	Maximun (not inclu	n length of l ding area co	local pho ode):	ne numbers		
					digits				

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.

Ingate System

SII Meth	o ods Filteri	Local ing Registrar	Authentication and Accounting	SIP Accounts	Dial Plan <mark>Ro</mark>	SIP Status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Status			
D	DNS Override For SIP Requests (Help)												
							Relay To						
	Domain		DNS Nan or IP <u>Add</u>	1e 1ess	IP Address	Port	Transp	ort Pi	iorit	y Weight	Auth	Modify RURI	Row
÷	+ ingate-siparator.lo ingate-sip				99.	1 5061	TLS 🕓				No 🖂	No 🖂	
Ad	d new ro	ws 1 g	roups with 1	fows	per gro	up.							
S	SIP Routing Order (Help) Class 3xx Message Processing (Help)												
17	No. Douting Expection			• Fo	rward al	1	-	,	-				
1	I DNS Override 2 Local Registrar 3 Dial Plan		O Follow redirects										
5													
3													

- 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:	(?
Ringtone:	Ringer 1 🛛 🗸 🕐
Custom Melody URL:	•
Display text for idle screen:	(?
XML Idle Screen URL:	(?
Ring After Delay (sec):	(?
Record Missed Calls:	●on ○off ?
Record Dialed Calls:	●on Ooff ?
Record Received Calls:	Oon Ooff ?
Identity is hidden:	Oon Ooff 🕐
Apply Re-Register Play Ringer	
Remove Identity Remove All Identities	

- 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 ③

Grandstream GXV3240

Status	Account Advanced Settings	Maintenance
	Account 1 Account 2 Accoun	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
Chalma		
Status	Account Advanced Setting	s Maintenance
	Account 1 Account 2 Account	It 3 Account 4 Account 5 Account 6
	Outbound Proxy :	192.168.200.254
	Secondary Outbound Proxy :	
	DNS Mode :	A Record
	NAT Traversal	
	Drom Doquire :	
-	PTOXV-Reduire :	

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 ③

Sangoma S500

OUDP OTCP OTLS 3	
	0
192.168.200.254	0
®No OYes 🕜	
	0
	0
ingate-siparator.loscasas.com	0
ONo ©Yes	
Registered	
	Registered ONo OYes Ingate-siparator.loscasas.com No OYes P 192.168.200.254 UDP OTCP OTLS P

- 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 ③

