

Configuration Guide Ingate SIParator/Firewall High Available Deployments with Amazon Web Services (AWS)

A how-to Guide For the Ingate SIParator®/Firewalls using software release 6.2.1 or later



1	INTROD	DUCTION	3
2	GENER	AL OVERVIEW	4
3	PROPOS	SED SOLUTION OVERVIEW	5
л			7
4	WHAT		/
	4.1 DNS	TECHNOLOGY	7
	4.2 DNS	SDV records Structure	/
	4.5 DNS	Load Balancing	o
	432	Failover	9 9
_	001510		
5	CONFIG	URING DNS SRV ON AWS	10
	5.1 Con	FIGURING DNS SRV FOR PUBLIC HOSTED ZONES	10
	5.2 DNS	SRV AS AN ADDITIONAL OPTION FOR FAILOVER IN THE PRIVATE SUBNET	15
	5.3 SIPAF	RATOR CONFIGURATION FOR FAILOVER USING DNS SRV AND OTHER FEATURES (SIP TRUNKING USE CAS	SE)
	531	IP-PBX Failover	18
	5.3.2	PBX Failover using DNS SRV for SIP Trunks	19
	5.3.3	PBX Failover using Dual Homing for PBX Domain in the Trunk Group	20
	5.3.4	SIP Trunks Failover.	22
	5.3.5	Dual/Multi homed Carrier	23
	5.3.6	DNS SRV SIP Trunk (Carrier Side)	24
	5.3.7	DNS SRV SIP Trunk (SIParator Side).	24
	5.3.8	Twilio Redundancy Options	27
	5.4 SIPA	RATOR CONFIGURATION FOR FAILOVER USING DINS SKV AND OTHER FEATURES (KEMO DRODUTS USE CASE)	ле ор
	5 4 1	Using DNS SRV to become the SIP Proxy and Registrar with a Failover with 2 SIParato	
	5.1.1	32	10
	5.5 PBX	CROSS CONNECTION WITH SIPARATORS	36
6	REPLICA	ATING AND SYNCHRONIZING SIPARATOR CONFIGURATIONS ACROSS ALL INSTANCES	3 6
	6.1 How	7 TO SYNCHRONIZE CONFIGURATION	38
	6.1.1	Obtaining CLI file from the main SIParator	38
	6.1.2	Manually modify CLI File:	39
	6.1.3	Loading CLI file and use the GUI to make all needed adjustments	45
7	FINAL T	IPS AND RECOMMENDATIONS	48
8	ADDITIO	DNAL HELP OR SUPPORT	51

Version:

Ingate SIParator/Firewall version 6.X



1 Introduction

This document aims to provide step by step guidance to design and deploy Highly Available Ingate SIParator instances in AWS/VPC. It leverages existing AWS VPC functionalities and Services which facilitate the goal of keeping operational continuity of your infrastructure.

Operational continuity will not be reachable by only applying these concepts to the SIParator, but also to the remaining infrastructure (IP-PBX, Soft switch, Routing gear, etc..) as they will need to be considered in the design. These considerations fall outside the scope of this guide.

SIParator appliances provide a way to implement High Availability by enabling Ingate's own SIParator Fail Over feature, pairing two identical Appliances into a cluster (see the Failover chapter in the <u>Reference Guide</u>) using one logical IP address. This functionality is not used in this document, as it is not available yet for AWS.

When configuring on AWS, the best way to proceed is by using DNS SRV records and some additional failover capabilities that will be shown in this document.

The two most common use cases when configuring SIParator are:

- 1) Provide remote access to users/endpoints to Telephony resources thru an SBC
- 2) Provide PSTN connectivity thru Service Providers by mediating SIP Trunks between the IPPBX and the Carrier.

A resilient implementation will be the one that provides minimum down time to both scenarios, users remotely connected willing to use Telephony Services and PSTN access

You will learn about the following topics:

- 1) How to use DNS Override (SIParator included feature) for remote extensions, and how it fits for redundant PBXes
- 2) How to use dual homing/domain support on SIParator Trunk Groups either facing the carrier, or facing the IP-PBX
- 3) How to use Route53 Service from AWS to build your DNS SRV records. (You can use your own managed DNS services)
- 4) How to use a Service Provider that already offers redundancy, accepts redundancy or supports DNS SRV



2 General Overview

In our case, we are going to implement a Redundant pair whereby each SIParator instance is in different AZ (Availability Zone) in the same VPC (Virtual Private Cloud). As each availability zone represents a physical data centre, we are protecting the solution not only against a potential Instance Failure, but also a full isolation of one of the data canters.

Note: this use case is totally different of "**SIParator Failover Pair**" feature explained in "**Ingate Reference Guide**" Chapter 13. Failover Pair feature uses heart beat between the 2 units using layer 2 protocols that are possible to implement in cloud environments such as AWS.



As shown in the figure, our two SIParators are located each one in a different AZ (separated Data Centers). Also, each one of them will have one interface in a Public Subnet (to face the Internet) and a second interface in a private subnet (to face the IP-PBX),

The interface facing the public subnet will have an Elastic IP (Public IP associated) for each SIParator.

One PBX will be located on the private subnet for each AZ (assuming they are configured in a failover fashion). And each SIParator will be able to reach any PBX. In this case, it is important to understand that All VPC subnets are always reachable from any other subnet as all of them belong to the same VPC.



As illustrated, we have the most common use cases represented here. We have PSTN connectivity using in our case TWILIO as the service provider and we have remote users in all possible fashions, including Remote Phones, Offices, Home Office, Softphones, etc.

Our goal in this case is to provide users with service continuity in the event one of the SIParators or PBX goes down.

DNS SRV, configured using Route53 (as explained in a later section)

3 Proposed Solution Overview

Here are the specific actions we will take to deploy a solution:

- For remote users, we will use an FQDN (Fully Qualified Domain Name) on the public side of the SIParators, and such FQDN will be resolved using SRV Records in a Domain Server (Route53) to include Corresponding Elastics IPs of each SIParator. This will create a failover strategy to reach any of the SIParators
- 2) As our Domain Name Service to resolve external FQDN, we will use Route53 from AWS
- 3) We will use DNS Override feature in SIParator to route SIP Requests internally to one of the IPPBX with a similar approach to how DNS SRV is used
- 4) For SIP Trunks (PSTN), we will leverage Twilio's failover capabilities. For inbound (from PSTN to SBC). They provide two different options;
 - a. Full support of DNS SRV records, so they will send traffic to an FQDN and SRV records will define the failover strategy,
 - b. To define more than one IP Address, to send traffic to, and failover from one to the other. This is useful when DNS SRV is not easy to implement.
- 5) Inbound traffic (Originated from PSTN) to be sent to IPPBX will be implemented by using redundant PBX domains supported in the Trunk Group Page
- 6) Outbound PSTN traffic from any of the two IPPBX to SBC can be implemented by accepting calls from any of the two IPPBX and routing to the appropriate SIP Trunk Group (Which already has a failover strategy as defined in 7)
- 7) For Outbound (From SBC to PSTN), Twilio Provides a unique FQDN for each trunk and it is resolved using DNS SRV. Here, Twilio already provides a failover strategy by default. It is important to know that in case the carrier does not have DNS SVR FQDN, but they can provide more than one IP for



failover, we can use the Dual Domain Feature for SIP Trunk configuration in the Ingate SIP Trunk Group.



What we are enabling here are the following failover strategies:

For Remote Users (Access use case)

- 1) Any remote user/extension uses a single registrar/proxy domain (siparator.ingatelabs.com), and via SRV records in case one SBC becomes unreachable, the other will take over operations. (siparator_ha1 and separator_ha2)
- 2) No matter which SBC is active, if any of the PBXs fails, the second PBX will be used instead.

For PSTN (trunking use case)

1) Traffic to the ITSP will be accepted from any of the SBCs. So, in case one fails, the second SBC will be capable of routing outbound calls.



2) Both SBCs will be able to process inbound traffic. If one SBC becomes unreachable to the ITSP, the second SBC will be tried. (this failover is provided by the ITSP)

4 What is DNS SRV and how does it work?

4.1 DNS Technology

- DNS means Domain Name Service
- Is Used as a phonebook for the internet
- Internet works on IP addresses
- DNS Infrastructure allows you to remember something like <u>www.ingate.com</u> and instead is interpreted as the IP address 193.180.23.236
- DNS Infrastructure is a hierarchy of databases distributed across the internet (<u>https://en.wikipedia.org/wiki/Domain_Name_System</u>)

4.2 DNS Illustrated.



- 1) A Client device is configured to use a specific DNS Server (10.10.0.3)
- 2) The Client device seeks to access <u>www.ingate.com</u>, and asks the DNS Server
- 3) The DNS Server responds to the client with the IP address where <u>www.ingate.com</u> is located



4) Now the Client sends the same request to the discovered IP address indicated by the DNS Server.

In SIP it is very similar. If I'm making a call the destination address might look something like this:

15554018146@ingate.com

For the call to proceed, the device needs to find where ingate.com is located. It could be for instance a PBX, or a Soft switch, or even a proxy-server or SBC.

In a SIP call looks like:



- As mentioned, DNS is a massively distributed database, which is comprised of many records
- Database look ups and IP resolution take just a few milliseconds
- It is very reliable, as it is the foundation of the Internet
- DNS records are divided into types:
 - A Type: maps a single domain name to an IP address (1:1)
 - SRV Type: Service records. Useful for locating specific services (i.e. SIP) and multiple servers
 - Many others (MX, AAAA, etc....)

4.3 DNS SRV records Structure

An SRV record follows this structure:



_Service._Proto.Name TTL Class SVR Priority Weight Port Target

Where:

- Service: the symbolic name of the desired service.
- Proto: the protocol of the desired service; this is usually either TCP or UDP.
- Name: the domain name for which this record is valid.
- TTL: standard DNS time to live field
- Class: standard DNS class field (this is always IN)
- Priority: the priority of the target host, lower value means more preferred
- Weight: A relative weight for records with the same priority
- Port: the TCP or UDP port on which the service is to be found
- Target: the canonical hostname of the machine providing the service

As an example, a query to siparator.ingatelabx.com would yield

_sip._udp.siparator.ingatelabs.com 60 IN SRV 1 50 5060 siparator_h1.ingatelabs.com _sip._udp.siparator.ingatelabs.com 60 IN SRV 2 50 5060 siparator_h2.ingatelabs.com

4.3.1 Load Balancing

All SRV Records with the same Priority form a load balancing group

Weight is used for distribution in terms of what proportion of traffic will be sent to each destination

For instance, an even distribution between 2 servers might look like this:



4.3.2 Failover

SRV records with a lower ordinal priority are always tried first

Records with higher ordinal priorities are only tried if all records with lower ordinal priority are tried considered unreachable

For instance, failover between 2 servers might look like this:





In this case, all sip requests to siparator_h1 are always tried first, and only when it is unavailable, to siparator_h2

5 Configuring DNS SRV on AWS

AWS provides its own DNS Services known as "Route 53".

Amazon Route 53 (Route 53) is a scalable and highly available Domain Name System (DNS). It is part of Amazon.com's cloud computing platform, Amazon Web Services (AWS). The name is a reference to TCP or UDP port 53, where DNS server requests are addressed. Route 53's servers are distributed throughout the world.

5.1 Configuring DNS SRV for Public Hosted Zones

Here we will show all you need to do to create your DNS SRV records in Route53, including the initial setup of your domain.

You need of course, to have an AWS account and you will need to log in to your AWS Console. (http://console.aws.com)

aws
Root user sign in
Eman
ecasas@loscasas.com
Password
•••••
Sign In
 Sign in to a different account
Forgot your password?



AW	'S services					
Rou	đ					Q
Ro	ute 53 slable DNS and Domain Name Registra	tion				* •
=		otto	Route 53		EGZ	
B	Billing	Ð	Cost Explorer			
,~ Al	Il services					
	Compute	ē	Management Tools		Mobile Services	
	EC2		CloudWatch		Mobile Hub	
	Lightsail 🕑		AWS Auto Scaling		AWS AppSync	
	Elastic Container Service		CloudFormation		Device Farm	
	Lambda		CloudTrail		Mobile Analytics	
	Batch		Config			
	Elastic Beanstalk		OpsWorks	912	AR & VR	
			Service Catalog	689	America Cumulan et	
P	Storage		Systems manager		Amazon Sumenan 🕑	
	63		Managed Services			
			Manageu Services	da	Application Integration	

Route 53 dashboard should look like this:

Jervic	æs 👻 Resource Groups 👻 🛠		۵
Dashboard	DNS management	Traffic management	Availability monitoring
Hosted zones			
Health checks	2	A visual tool that lets you easily create	Health checks monitor your applications
Traffic flow	Hosted zones 0	policies for multiple endpoints in complex configurations.	and web resources, and direct DNS queries to healthy resources.
Traffic policies		Create policy	Create health check
Policy records			
Domains	Register domain		
	-		
Registered domains			
Registered domains Pending requests	Find and register an available domain o Type a domain name	er tracefor your existing domains to Boute 52 .com - \$12.00	Check
Registered domains Pending requests	Find and engister an available domain of Type a domain name Alerts	se transfor your evicting domains to Boute 52	* Check
Registered domains Pending requests	Find and register an available domain o Type a domain name Alerts	com - \$12.00	Check Check K No alerts to display

- 1) Among other options, the dashboard gives you access to manage the service and hosted zones
- 2) Allows you to create and own a domain in case you need it. This has a cost associated depending on the domain.

A hosted zone is a collection of records for a specified domain. You create a hosted zone for a domain (such as example.com), and then create records to tell the Domain Name System how you want traffic to be routed for that domain.

In our example we have already created and own a public domain "ingatelabs.com"



aws	Services	✓ Resource Groups ✓ ★	pport 👻
Dashboard Hosted zones	•	Create Hosted Zone Go to Record Sets Delete Hosted Zone Q Search all fields X Public Hosted Zones K < Displaying 1 to 1 out of 1 Hosted Zone	€ 0 mes > >
Health checks		Domain Name v Type Record Set Count V Comment	one ID 🔹 👻
Traffic flow Traffic policies Policy records		ingatelabs.com. Public 21 HostedZone created by Route53 Reg	
Domains Registered domain Pending requests	s		

Based on what we have discussed in previous sections we will define all A and SRV records needed to build a failover FQDN using DNS SRV

Based in our diagram:



First, we will create an A record for each SIParator and associate them to the corresponding Elastic IP Address

aws	Services	 Resource Groups 	*
Dashboard	•	Back to Hosted Zones	Create Record Set
Hosted zones		Record Set Name	X Any Type 🔻
Health checks		Aliases Only W	eighted Only
Traffic flow		🛛 🐇 🐇 Displaying 1	to 21 out of 21 Record Sets 🔌
Traffic policies		- v.	A

Select the hosted zone and press on "Create Record Set"



Create R	ecord Set
Name:	siparator_ha1 .ingatelabs.com.
Type:	A – IPv4 address
Alias:	Yes No
TTL (S	econds): 300 1m 5m 1h 1d
Value:	<elastics ip="" public=""></elastics>
	IPv4 address. Enter multiple addresses
	on separate lines.
	Example:
	192.0.2.235
	186.01.100.234
Routing	Policy: Simple V
Route 53	responds to queries based only on the values in this record. Learn More

- 1) Create the record selecting Type A-IPv4 Address
- 2) Enter the Elastic IP address in the Value Field
- 3) Keep the default Policy on Simple.
- 4) Press "Create"
- 5) Repeat the process for siparator_ha2.ingatelabs.com

Once created you can verify everything is as expected:

Back to Hosted Zones Create Record Set	port Zone File Delete Record Set
Back to Hosted Zones Create Record Set Aliases Only Weighted Only K Displaying 1 to 2 out of 2 Record Sets Type Value Evaluate Target Health Health A	Edit Record Set Name: siparator_ha1.ingatelabs.com. Type: A-IPv4 address Alias: Yes Ves No TTL (Seconds): 300 Im Im Im Im Value: Im IPv4 address. Enter multiple addresses on separate lines. Example: 192.0.2.235 198.51.100.234
	Routing Policy: Simple Route 53 responds to queries based only on the values in this record. Learn More

Now we have two new FQDN, each one resolving to one of the corresponding public IP addresses.

Now we will create SRV records for SIP UDP, SIP TCP and SIP TLS.



Three SRV records will be needed (One per transport protocol, UDP, TCP and TLS)

As we want to create a Failover strategy we will use different Priorities and same weights.

Each record should look like this:

Name: _siptcp siparator ngatelabs.com. 💊
Type: SRV – Service locator
Alias: O Yes No
TTL (Seconds): 300 1m 5m 1h 1d
Value: 1 10 5060 siparator_h1.ingatelabs.com 2 10 5060 siparator_h2.ingatelabs.com
An SRV record. For information about SRV record format, refer to the applicable documentation. Enter multiple values on separate lines.
Format: [priority] [weight] [port] [server host name] Example: 1 10 5269 xmpp-server.example.com. 2 12 5060 sip-server.example.com.
Routing Policy: Simple
Route 53 responds to queries based only on the values in this record. Learn More

- 1) Note that Protocol and transport are part of the domain prefix (_sip._tcp),
- 2) The FQDN that will be referred to resolve is siparator.ingatelabs.com
- 3) Siparator_h1 will be the primary for failover (lowest priority)
- 4) _h1 and _h2 have same weight
- 5) Routing Policy will be kept by default.

You will need to repeat this for UDP (port 5060) and TLS (port 5061) to complete our 3 SRV records.

In Route 53 an SRV record Value element consists of four space-separated values. The first three values are decimal numbers representing priority, weight, and port. The fourth value is a domain name.

Note, other typical parameters as explained in 4.3 are included as part of the domain name (i.e. _sip._udp.siparator), or the TTL parameter that can be setup in the same screen.

As a summary you can verify the SRV records you recently created and should look like these:



Record Set Name	SRV Aliases Only	
Weighted Only		
	K Displaying 1 to 3 out of 3 Record Sets	>1
Name	Type Value	
siptcp.siparator.ingatelabs.com.	SRV 1 10 5060 siparator_h1.ingatelabs.com 2 10 5060 siparator_h2.ingatelabs.com	
siptls.siparator.ingatelabs.com.	SRV 1 10 5061 siparator_ha1.ingatelabs.com 2 10 5061 siparator_ha2.ingatelabs.com	1 1
sipudp.siparator.ingatelabs.com.	SRV 1 10 5060 siparator_ha1.ingatelabs.com 2 10 5060 siparator_ha2.ingatelabs.com	1

This concludes what needs to be done to create your SRV records with Failover strategy.

5.2 DNS SRV as an additional option for Failover in the private subnet

Later we will show 2 methods to implement Failover for the PBX. One of them is also based on SRV records but used to resolve IPs in the private network. To do so we will create a private hosted zone for the private network using a private domain named "ingatelabs.local".

1) First, we need to create a private Hosted Zone





2) Assign the Domain Name (ingatelabs.local), Select Private Hosted Zone for VPC, and press "create"

aws services	s 🗸 Resource Groups 🗸 🛧	🗘 Ernesto Casas 👻 Global 👻 Support 👻	
Dashboard	Create Hosted Zone Go to Record S	Sets Delete Hosted Zone	8
Hosted zones	Q X	Create Hosted Zone	
Health checks	Search all fields	A hosted zone is a container that holds information about how you want route traffic for a domain, such as example.com, and its subdomains.	to
Traffic flow	Private Hosted Zones V	Domain Name: ingatelabs.local	
Policy records	I ✓ No Hosted Zones to display	Comment: Local DNS for Private Sub	
Domains	* Type * Record Set Count * Comment	Type: Private Hosted Zone for Amazon VPC V	
Registered domains Pending requests	ave no hosted zones v	A private hosted zone determines how traffic is ro within an Amazon VPC. Your resources are not accessible outside the VPC. You can use any don name.	uted main
		VPC ID: vpc-21e34c44 us-east-1	
	keyword 'null'	Important	
		to use private hosted zones, you must set the following Amazon VPC settings to true: enableDnsHostnames enableDnsSupport Learn more	

Make sure you associate this domain to the VPC you are using to deploy the solution

You can add more VPCs as needed in case your SIParators or PBXs are installed in more than one VPC. For more detailed information you can refer to: <u>https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-</u> <u>zones-private.html</u>

3) Create A records for each PBX. Based on the diagram they are located at 10.0.1.149 and 10.0.201.149.





Back to Hosted Zones Create Record Set Test Record Set Test Record Set Record Set Name Any Type Aliases Only Weighted Only Import Zone File Delete Record Set Test Record Set Name Type Value Import Zone File Delete Record Set Name Type Value Import Zone File Delete Record Set Ingatelabs.local. NS ns-1536.awsdns-00.co.uk. ns-1024.awsdns-00.org. ns-512.awsdns-00.co.uk. awsdns-hostmaster.ama: Displaying 1 to 3 out of 3 Record Sets Import Zone File Ingatelabs.local. SOA ns-1536.awsdns-00.co.uk. awsdns-hostmaster.ama: Displaying 1 to 3 out of 3 Record Set Test Record Set Ingatelabs.local. SOA ns-1536.awsdns-00.co.uk. awsdns-hostmaster.ama: Displaying 1 to 3 out of 3 Record Set Test Record Set Ipvia address. Enter multiple addresses on separate lines. Example: 192.0.2.235 198.51.100.234 Ipvia doress Simple Routing Policy: Simple Routing Policy: Simple Routing Policy: Simple Routing Policy: Simple Routing Nore						
Weig	phted Only				Name: pbxact2 .ingatelabs.local. Type: A-IPv4 address	
	Name	Туре	Value		Alias: Yes No TTL (Seconds): 200 1m 5m 1h 1d	
	ingatelabs.local.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	8	Value: 10.0201.149	
	ingatelabs.local.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz		on separate lines. Example:	
	pbxact1.ingatelabs.local.	А	10.0.1.149		192.0.2.235 198.51.100.234	
					Routing Policy: Simple v Route 53 responds to queries based only on the values in this record. Learn More	

4) Create SRV Record for Failover strategy between the two PBXes

Destational	Back to Hosted Zones	Create	Record Set Import Zone File Delet	te Record Set Test Record Set 2 🌣		
Hosted zones	Record Set Name	×	Any Type Aliases Only	Create Record Set		
Health checks	Weighted Only			Name:		
Traffic flow			 K Displaying 1 to 4 out of 4 Record Sets			
Traffic policies	Name	Туре	Value	Allas: Yes No TTI (Seconds): 300 1m 5m 1h 1d		
Domains	ingatelabs.local.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org.	Value: 1 10 5060 <u>pbxact1 ingatelabs</u> local 2 10 5060 <u>pbxact2 ingatelabs</u> local		
Registered domains Pending requests	ingatelabs.local.	SOA	ns-512.awsdns-00.net. ns-1536.awsdns-00.co.uk. awsdns-hostmaster.ama;	An SRV record. For information about SRV record format, refer to the applicable documentation. Enter multiple values		
	pbxact1.ingatelabs.local.	A	10.0.1.149	on separate lines. Format:		
	pbxact2.ingatelabs.local.	A	10.0.201.149	Example: Example: 1 10 5269 xmpp-server.example.com. 2 12 5060 sip-server.example.com.		
				Routing Policy: Simple T		

You can repeat this step if you need to add TCP and TLS as additional transport options.

5.3 SIParator configuration for Failover using DNS SRV and other features (SIP Trunking use case)

First, we need to understand that we will setup 2 SIParators with almost identical configuration. Just a few elements will be different between them which we explain in detail later.





Let's first focus on configuring one of the SIParators

5.3.1 IP-PBX Failover

We are not going to present the details of all the required configuration but will describe the ones that are related to some type of failover functionality.

1) As shown in the diagram we will provide failover inbound calls to 2 IP-PBXes, and, we will allow traffic coming from any of them. So, we will need in the "Networks and Computers" Section under "Network":

Ī	t	pbx	pbxact1 🔻				- •
	L		pbxact2 🔻				- •
1	Ð	pbxact1	- •	10.0.1.149	10.0.1.149		internal (eth1 untagged) 🔻
6	Ð	pbxact2	- •	10.0.201.149	10.0.201.149		internal (eth1 untagged) 🔻

Here with a single name "pbx" we are including any of the two PBXes shown in the diagram.

2) In "Filtering" under SIP Traffic we are adding "pbx" as a valid source to process SIP requests



Administration	Basic onfiguration	Rules and Relays	d SIP Services	SIP Traffic Tr	SIP runks Fo	ilover V	irtual Priv Network	rate s	Quality of Service	Logging and Tools
SIP Methods Filteri Sender IE	Local Authen ng Registrar and Acc	tication counting A	SIP Di accounts Pla	al an Routing	SIP Status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Statu	s
No.	From Networ	k A	Action	Delete Row	De O P	fault P	olicy F	or S	IP Requ	iests
1	Coral Springs	▼ Pro	cess all 🔻		e I	ocal on	17			
2	Twilio	▼ Pro	cess all 🔻		• R	leject al	1			
3	VPC	▼ Pro	cess all 🔻		_		_			
4	Coral Springs LAN	V ▼ Pro	cess all 🔻							
5	pbx	▼ Pro	cess all 🔻							

Here, as we are using "pbx" network name, the 2 IP-PBXes has been included as a valid source.

3) Inbound failover for PSTN calls. In this case, we configure how to failover to a secondary pbx (pbxact2) in case the primary does not respond to inbound calls coming from PSTN.

There are 2 methods we can use, the first one is based on DNS SRV Records for Private Hosted Zone (See section 5.2). In this case we will use pbxact.ingatelabs.local as the PBX domain.

5.3.2 PBX Failover using DNS SRV for SIP Trunks

	ther SIP trunk						
Define PBX setti	ings						
PBX Name:	PBX Act	(Un	uque descriptive name)				
Use alias IP addres	s: - 🔻	(Fo	rces this source address	from our side)			
		Authe	entication	PBX IP Ad	dress		
PBX Registration SIP Address		User ID	Password	DNS Name or IP Address	IP Address	PBX Domain Name	
			Change Password			pbxact.ingatelabs.local	
(At least one of PBX I	Registration, IP	address or Domain	Name is required to loc	ate the PBX)			
PBX Network:		VPC_Priva	ate 🔻				
Signaling transport	:	UDP V	UDP V		c)		
Port number:							
Match From Numb	er/User in field	I: From URI	•				
Common User Nan	ne suffix:						
To header field:		Same as F	Request-URI 🔻				
Forward incoming	REFER:	No 🔻					
Send DTMF via SI	P INFO:	No 🔻					
Remote Trunk Gro	up Parameters	usage: -		▼ ('-' = Don't use	TGP)		
Logal Trants Course	Parameters us	age: -		\checkmark $C_{-}' = Don't use$	TGP)		

As shown, we are using the DNS name as the PBX Domain associates to an SRV Record. Failover between the two PBXes will be managed by DNS Services based on the Strategy created in Section 5.2



We will add also monitoring to the PBX Domain (pbxact.ingatelabs.local) in the SIP Services Section, Basic Configuration:

SIP Servers To Monitor (<u>Help</u>)								
Server	Port	Transport	Delete Row					
10.0.1.149		- •						
10.0.1.220		- •						
ingatelabstraining		- •						
pbxact.ingatelabs.		- •						

You can also confirm that the domain is properly resolved using DNS SRV and the PBX is declared as Online. Looking at the "SIP Traffic" section, "SIP Status"

ľ	Administra	ition Con	Basic Ifiguration	Network	tules Rela	and iys	Ser	ilP vices	SIP Traffic	SIP Trunks
	SIP Methods	Filtering	Local Registrar	Authenticati and Account	on ing	SI Acco	P unts	Dial Plan	Routing	SIP Status I
	Active Sessions (0 sessions)									
	There are no active sessions.									
	Mon	itored S	SIP Serv	vers						
l			Server		Po	ort	Trai	ıspor	t Statı	15
l	10.0.	1.220				1	UDF	•	Onlin	ne
l	ingatelabstraining.pstn.twilio.com			ı	1	UDP Onl		Onlin	ne	
	10.0.	10.0.1.149				1	UDF)	Onlin	ne
	pbxac	ct.ingate	labs.local	l			UDF)	Onlin	ne

5.3.3 PBX Failover using Dual Homing for PBX Domain in the Trunk Group

As a second option, we can take advantage of dual domain (two domains commaseparated in the trunk Group PBX configuration). In this case, we can directly use PBX IP addresses or domain names created with A Records as explained in section 5.2.

PBX Domain Name - Optional SIP domain name of the PBX in case the PBX wants incoming calls to be addressed to sip:number@domain instead of sip:number@ip-address. *You shall also use this field if you have two redundant PBXes. Then add the IP address or FQDN of both PBXes in this field, separated by comma.* (Do not fill in the PBX IP Address field then.) If the first PBX is out of service, the second will be tried. You should also enter these



PBXes for monitoring at the SIP Services > VoIP Survival page to speed up failover.

Setup for the PBX (Help)							
O Use PBX from other SIP trunk							
Oefine PBX settings							
PBX Name: PBX Act	(L	Unique descriptive name)					
Use alias IP address: - 🔻							
	Authe	thentication PBX IP Address					
PBX Registration SIP Address	User ID	Password	DNS Name or IP Address	IP Address	PBX Domain Name		
		Change Password			pbxact1		
(At least one of PBX Registration, IP a	ddress or Domain l	Change Password Name is required to locate	e the PBX)		pbxact1 pbxact1.ingatelabs.local.pbxa	ct2.ingatelabs.local	

Adding the two domains to SIP Monitor:

SIP Servers To Monitor (Help)								
Server		Port	Tra	nsport	Delete Row			
10.0.1.149			-	T				
10.0.1.220			-	T				
ingatelabstraining.p			-	T				
pbxact.ingatelabs.k			-	T				
pbxact1.ingatelabs.			-	T				
pbxact2.ingatelabs.			-	•				

And, we can speed up the Failure detection by enabling the VoIP Survival feature and adding both domains (A Records). We can also include an SRV record to illustrate that it also works for the DNS SRV case.

Administration Basic Configuration	Network Rules Rel	s and SIF ays Servi	ces Tra	IP SIP Iffic Trunks	Failove	r Virtual Privo Networks					
Signaling Media Basic Encryption Encryption In	nteroperability	Sessions and Media	Remote Connect	e SIP VolP livity Surviva	VolP St	Survival atus					
VoIP Survival (Help) Enable VoIP Survival Disable VoIP Survival Server Check Interval Domains To Monitor											
30 second	is I	Domain Na	ame	Metho	d	Delete Row					
	pb	xact1.ingat	elabs.	Display nar	ne 🔻						
	pb	xact2.ingat	elabs.	Display nar	ne 🔻						
	pb	xact.ingate	labs.k	Display nar	ne 🔻						
	Add new rows 1 rows.										
Registrations											
Re-REGISTER interval	during surviv ls	val mode:	Time 14	to store sub	oscribe days	r data:					



Note the field Server Check Interval. This value in seconds defines how many seconds a new check (SIP OPTIONS) will be sent. The interval must be shorter than the SIP blacklist interval on the Sessions and Media page.

Here is how the SIP Status screen will look, in this case, one of the two IPPBX shows as down, and having at least one available shows the SRV Domain as online.

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SI Acco	P unts	Dial Plan	Ro	uting	SIF Stat	o US	
Activ	Active Sessions (0 sessions)										
There	There are no active sessions.										
Monitored SIP Servers											
	Server					Transport		Stat	us		
pbxa	ct1.ingat	elabs.loc	al		UD	Р		Onli	ne		
ingat	elabstrai	ning.pstn	.twilio.com		UD	Р		Onl	ne		
10.0.	1.220				UD	Р		Oni.	ne		
pbxa	pbxact.ingatelabs.local					P		Onli	ne		
10.0.	10.0.1.149					Р		Oni	ne		
pbxa	pbxact2.ingatelabs.local					Р		Offl	ine		

As we are using VoIP Survival, the same behavior is expected:

Basic	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status	
St	urvival D	omain St	atus					
Monitored Domain		Sta	tus	1				
pb	xact.ingat	elabs.local	Server work	Server works				
pb	pbxact1.ingatelabs.local Server works							
pb	pbxact2.ingatelabs.local		1 Survival - 1	Survival - local server				
			-					

5.3.4 SIP Trunks Failover.

PSTN connectivity is another of the important components of the service to consider when designing a highly available service. In our case, we will mention the most common techniques to provide a failover strategy. In some cases, to have a



highly available solution for PSTN connections depends on how the ITSP offers their service.

- 1) **Dual/Multi Homed Carrier**. In this case the ITSP provides more than one IP Address or FQDN and the SBC should be able to allocate them associated to the same trunk
- 2) DNS SRV SIP Trunk (Carrier Side). In this case the carrier will provide an FQDN that resolves using SRV records pointing to more than one destination. The resilience strategy is managed using DNS SRV, including Failover and Load Balance Strategies
- **3) DNS SRV SIP Trunk (SIParator Side).** The other side of the coin could be to provide the carrier an FQDN for inbound traffic, and such an FQDN is resolved using DNS SRV Records. Is short, the ITSP must support DNS SRV resolution for customer trunk destinations
- **4) Multi IP Hunting (Carrier side).** In this case, The ITSP must be able to hunt, failover or load balance between the IPs or FQDN (A records) pointing to the SIParators
- 5) Twilio Redundancy options. Twilio is a good example of an ITSP which provides more than one option for resilience. First, they provide each customer SIP trunk a unique FQDN with SRV records, solving the outbound failover case. Second, they provide DNS SRV support for the customer to provide an FQDN with SRV records for inbound failover. They also provide inbound traffic a way to assign multiple FQDNs or IP addresses to send inbound traffic using a Failover or balancing strategy.

5.3.5 Dual/Multi homed Carrier.

In this case, we will take advantage of Dual Domains supported in SIP Trunk configuration under the Trunk Group Pages

SIP Trunking Service (Help)		
O Use parameters from other SIP trunk		
 Define SIP trunk parameters 		
Service name:	Carrier	(Unique descriptive name)
Service Provider Domain:	trunk1.carrier.com,trunk2.carrier.com	(FQDN or IP address)
Destant H C	·	a

Service Provider Domain - The FQDN or IP address of the ITSP SIP server. This domain name will be used in the Request-URI and To header field for outgoing SIP requests. *If there are two redundant SIP Servers, enter both here, separated by comma. (Do not enter both SIP Servers if these instead are addressed by DNS SRV records for the Outbound Proxy.)* If the first SIP Server is out of service, the second will be tried. You should also add these SIP Servers to the table "SIP Services" > Basic > "SIP Servers to Monitor" to accelerate failover.



5.3.6 DNS SRV SIP Trunk (Carrier Side)

In this case the carrier provides a SIP Trunk Domain (FQDN) with DNS SRV Records. This helps to have a failover strategy on outbound traffic to PSTN

This is the case of Twilio and other advanced SIP Trunk Providers.

SIP Trunk 1 (Help)		
Inable SIP Trunk		
O Disable SIP Trunk		
SIP Trunking Service (<u>Help</u>)		
O Use parameters from other SIP trunk		
 Define SIP trunk parameters 		
Service name:	Twilio Elastic	(Unique descriptive name)
Service Provider Domain:	ingatelabstraining.pstn.twilio.com	(FQDN or IP address)
Restrict to calls from:	Twilio	('-' = No restriction)

Notice the domain used is an FQDN resolved using SRV records, where the carrier Failover strategy will be implemented.

5.3.7 DNS SRV SIP Trunk (SIParator Side).

In this case, as explained in section 5.1, the SIParator is reachable via an FQDN using SRV records. We can reuse the same siparator.ingatelabs.com or we can create additional FQDN specifically for SIP Trunking.

For instance, let's think how to implement a specific trunk using a new FQDN (trunk.ingatelabs.com) and let's use port 15060 and TCP to failover to siparator_ha1.ingatelabs.com and siparator_ha2.ingatelabs.com

1) Create a Record Set in the Hosted Public Zone ingatelabs.com

Name: Type: SRV -	_siptcp.trunk .ingatelabs.com.
Type: SRV -	
	- Service locator
Alias: O Yes	No
TTL (Seconds): 300 1m 5m 1h 1d
Value: 1 10 1 2 10 1	15060 siparator h1.ingatelabs.com
An SR reco docu	V record. For information about SRV ord format, refer to the applicable umentation. Enter multiple values separate lines.
Forma [prio Examp	t. http://weight] [port] [server host name] ple:
1 10 2 12) 5269 xmpp-server.example.com. } 5060 sip-server.example.com.
Routing Policy	: Simple •
Route 53 responds	to queries based only on the values in this record. Learn More



2) Add 15060 on TCP as a valid SIP listening port

Administration	Basic Configuration	Network	Rules a Relay	nd Si s Servi	P ices	SIP Traffic	SIP Trunks	Failover	Virtual Private Networks
Basic Signalin	ng Media on Encryption	Interopera	sility a	Sessions nd Media	Rer Con	note SIP nectivity	VoIP Survival	VoIP Sur State	rvival us
SIP Mod	ule (<u>Help)</u>								
 Enable Disable SIP Sign Specify the Simulation 	 Enable SIP module Disable SIP module SIP Signaling Access Control (Help) Specify the networks and computers from which the firewall accepts SIP 								
- Signaling.	• naling Por	ts (Help)	1						
Active	Port	Transp	ort	Interco	ept	(Comme	nt	Delete Row
Yes ▼	5060	UDP and ⁻	ГСР 🔻	Yes •		Standa	rd SIP p	ort	
Yes ▼	5061	TLS	•	Yes v		Standa	rd TLS p	ort	
Yes 🔻	15060	ТСР	۲	Yes ▼		Trunkin	g TCP		

3) Add SIP Monitor for trunk.ingatelabs.com

SIP Servers To Monitor (<u>Help</u>)					
Port	Transport	Delete Row			
	- •				
	- •				
	- •				
	- •				
	- •				
	- •				
	TCP 🔻				
	Ionitor (Port	Ionitor (Help) Port Transport - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -			



SIP Monitor will show the status for the Trunk Domain

Administra	^{ition} Con	Basic figuration	Network Ru	iles and Relays	Se	SIP rvices	S Tra	IP Iffic	SIP Trunk	s Failove
SIP Methods	Filtering	Local Registrar	Authentication and Accountin	n Sl g Acco	P unts	Dial Plan	Rou	ting	SIP Status	IDS/IPS
Activ	e Sessi	ons (0 s	essions)							
There	are no a	ctive ses	sions.							
Mon	itored S	SIP Serv	vers							
		Server		Port	Tra	nspo	rt	Stat	tus	
pbxa	ct1.ingat	elabs.loc	al		UD	Р	(Onli	ine	
ingate	elabstrai	ning.pstn	.twilio.com		UD	Р		Onli	ine	
10.0.	1.220				UD	Р	(Onli	ine	
pbxa	pbxact.ingatelabs.local				UD	Р	(Onli	ine	
trunk	trunk.ingatelabs.com				TC	Р	(Onli	ine	
10.0.	10.0.1.149				UD	Р	(Onli	ine	
pbxa	ct2.ingat	elabs.loc	al		UD	Р	(Offl	ine	

4) Add VoIP Survival for trunk.ingatelabs.com

Basic	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VolP Survival	VoIP Survival Status			
Vo	VoIP Survival (Help)									
•	 Enable VoIP Survival Disable VoIP Survival 									
S	erver Ch	eck Inte	rval De	omains T	o Monito	r				
30		seco	nds I	Domain N	ame	Method	Delete Row			
			pt	xact1.ingat	elabs. Dis	play nam	e 🔻 🗌			
			pt	xact2.ingat	elabs. Dis	play nam	e 🔻 🗌			
			pt	xact.ingate	labs.k Dis	play nam	e 🔻 🗌			
			tru	unk.ingatela	ibs.co Dis	play nam	e 🔻 🗌			
			_				_			



VoIP Survival Status will show:

Basic	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
Survival Domain Sta			itus				
]	Monitored	l Domain	Sta	tus]		
pb	xact.ingate	elabs.local	Server work	ks			
tru	ınk.ingatel	abs.com	Server work	ks			
pb	xact1.inga	telabs.loca	1 Server worl	ks			
pb	xact2.inga	telabs.loca	1 Survival - 1	ocal serve	r		

5.3.8 Twilio Redundancy Options

Twilio, among several SIP and SMS APIs and Services, also provides very advanced SIP Trunking Options.

When designing a Highly Available solution, it is very important to review not only features and capabilities provided by your own infrastructure but also related functionalities on the Service Provider side.

In this section we will use Twilio as the Service Provider for their Failover capabilities. Many other ITSPs in the market offer extensive HA features and you should consider them when designing your platform.

Lets first access Twilio Account Dashboard \rightarrow Elastic SIP Trunking





For this document, we set up the Lab Training Test SIP Trunk to be configured in such a way that calls can be routed to any of the 2 SBCs using a failover strategy.

casa	as@loscasas∨ Elast	ic SIP Trunking /		,O G	o to €	€?
	Elastic SIP Trunking	Trunks Viewall Trunk				
51F	Dashboard		TERMINATION SI	01	IGINATION SIP LIRIS	
••	Trunks	Lab Training Test	ingatelabstrainin		28 and	1 more
	Authentication	Lab Training G01	ingatelabstrainin	om	54	
	Networking Info	Lab Training G02	ingatelabstrainin	om	8	
	Tools	Lab Training G03	ingatelabstrainin	om	6	
	Logs	Lab Training G04	ingatelabstrainin	om	0	
	Usage	Lab Training G05	ingatelabstrainin	om	13	
	Getting Started	Lab Training G06	ingatelabstrainin	om		
		Lab Training G07	ingatelabstrainin	om	3	
		Lab Training G08	ingatelabstrainin	om		
		Lab Training G09	ingatelabstrainin	om	4	
		Lab Training G10	ingatelabstrainin	om		

Now we can associate one or more origination IP addresses or FQDN. Notice that when using 2 or more, you have the tools to assign priority and weight and they work exactly how DNS SRV records work. You can have a Failover or even a Load Balance Strategy.

(i) tv	vilio					DOCS	∽ Erne	esto Cas	ias 🗸
ecas	as@loscasas∨ Elas	tic SIP Trunking / Lab Training Test	t /		<u>م</u>		÷	?	ŝ
▲	Elastic SIP Trunking Lab Training Test General Termination Origination Numbers	Origination Incoming traffic to your commu Origination URIS Configure the IP address (or FQ IP-PBX, SBC). Show more about provisioning.	nications in DN) of the <u>for high ser</u>	nfrastructure fron network element <u>vice availability</u>	n the PSTN. entry point into yo	our communicatic	ons infrastr	ructure	(e.g.
	< Back	ORIGINATION URI sip:3 28 sip:5		PRIORITY 1 9	WEIGHT 10 10	ENABLED			× ×
		CNAM Lookup Look up the caller ID name for C IP communications infrastructu Save Cance	Drigination re and disp	calls from the PST layed in the Call L lete this Trunk	™. If present it is i .ogs. The price is \$	ncluded in the SIF 0.01/call.	P INVITE to	wards y	<i>y</i> our

Regarding origination, Twilio will allow you to define a URI for each SIP Trunk that you will use in your SIParator Trunk Group configuration.





The URI defined above "ingatelabs.pstn.twilio.com" will be the one used in SIParator Trunk Group Page configuration, as shown here:

in@ate Firewall Ingate SIP	ARATOR 6.1.1 for AWS I	Lab Log Out	^
Administration Basic Configuration Network Rules and SIF Relays Servi	ces SIP SIP Failover Virtual Private Traffic Trunks Failover Networks	Quality of Logging About and Tools	l
View trunk: SIP Trunk 1: Twilio Elastic;PBX Act v	Goto SIP Trunk page		ł
SIP Trunk 1 (<u>Help</u>)			
Enable SIP Trunk			
O Disable SIP Trunk			
SIP Trunking Service (Help)			
\odot Use parameters from other SIP trunk			
 Define SIP trunk parameters 			
Service name:	Twilio Elastic	(Unique descriptive name)	
Service Provider Domain:	ingatelabstraining.pstn.twilio.com	(FQDN or IP address)	
Restrict to calls from:	Twilio	('-' = No restriction)	
Outbound Proxy:		(FQDN or IP address)	
Use alias IP address:	- 🔻	(Forces this source address from our side)	
Outbound Gateway:	- T	('-' = Use Default Gateway)	
Signaling Transport:	UDP •	('-' = Automatic)	
Port number:			
From header domain:	Provider domain 🔹		Ŧ

The domain ingatelabstraining.pstn.twilio.com resolves to multiple addresses predefined by Twilio and they do what's needed to ensure availability of any of them. Those IPs are listed per region in your dashboard \rightarrow Elastics Sip trunks \rightarrow Networking Information and are used in a round-robin fashion in the region you have your Instances deployed.

These IP addresses should be added to your Networks & Computers section in SIParator configuration



<u> </u>	niio		DOCS 🗸 Ernesto Casas 🗸
ecasa	as@loscasas∨		,⊂ \$? \$
<u>ل</u> ر	Elastic SIP	NORTH AMERICA VIRGINIA	NORTH AMERICA VIRGINIA
a	Trunking	54.172.60.0	54.172.60.0/23
	Dashboard	54.172.60.1	34.203.250.0/23
	Trunks	54.172.60.2	
	Authentication	54.172.60.3	NORTH AMERICA OREGON
	Networking Info		54.244.51.0/24
	Tools	NORTH AMERICA OREGON	EUROPE IRELAND
	Logs	54.244.51.0	54.171.127.192/26
	Usage	54.244.51.1	52.215.127.0/24
	Getting Started	54.244.51.2	
		54.244.51.3	EUROPE FRANKFURT
		EUROPE IRELAND	35.156.191.128/25
		54.171.127.192	ASIA PACIFIC TOKYO
		54.171.127.193	54.65.63.192/26
		54.171.127.194	
		54.171.127.195	54 169 127 128/26
			54.107.117.1107.10
		EUROPE FRANKFURT	ASIA PACIFIC SYDNEY
		35.156.191.128	54.252.254.64/26
		35.156.191.129	SOUTH AMERICA SÃO PAULO
		35.156.191.130	177.71.206.192/26
		35.156.191.131	
		ASIA PACIFIC TOKYO	
		54.65.63.192	
		54.65.63.193	
		54.65.63.194	
		54.65.63.195	
			-

inGate Firewall Ingate SIPARATOR 6.1.1 for AWS Lab Log Out Basic Administration Abou Relays Con Services Traffic Net Ser Networks and Computers Default All VLAN Eth0 Eth1 Interface PPPoE Tunnels Topology Networks and Computers Upper Limit Lower Limit (for IP ranges) Delete Subgroup Interface/VLAN Name DNS Name DNS Name or IP Address Row IP Address IP Address + Coral Springs Coral Springs LAN . + Internet external (eth0 untagged) 🔻 🗌 34.203.250.0 34.203.251.255 34.203.251.255 + Twilio ▼ 34.203.250.0 ۳ 35.156.191.128 35.156.191.131 35.156.191.131 ۲ 35.156.191.128 54.65.63.192 54.65.63.195 • 54.65.63.192 54.65.63.195 54.171.127.192 54.171.127.195 54.171.127.195 • • 54.171.127.192 ▼ 54.172.60.0 54.172.60.0 54.172.61.255 54.172.61.255 • 54.244.51.0 54.244.51.3 ▼ 54.244.51.0 54.244.51.3 • + VPC ۲ • VPC_Private ۲ internal (eth1 untagged) 🔻 + VPC_Public • external (eth0 untagged) 🔻 + pbx v ٠ pbxact1



Having Twilio defined as a Network group name will allow you to refer to those addresses by name. For instance, to limit from where SIP trunk traffic is accepted.

Administration Basic Configuration Network Rules and SIF Relays Servi	P SIP SIP Failover Virtual Private Traffic Trunks Failover Networks	Quality of Logging Service and Tools About
View trunk: SIP Trunk 1: Twilio Elastic;PBX Act 🔻	Goto SIP Trunk page	
SIP Trunk 1 (Help)		
Inable SIP Trunk		
O Disable SIP Trunk		
SIP Trunking Service (Help)		
O Use parameters from other SIP trunk		
 Define SIP trunk parameters 		
Service name:	Twilio Elastic	(Unique descriptive name)
Service Provider Domain:	ingatelabstraining.pstn.twilio.com	(FQDN or IP address)
Restrict to calls from:	Twilio	('-' = No restriction)
Outbound Proxy:		(FQDN or IP address)
Use alias IP address:	- •	(Forces this source address from our side)

It is also required to have an access control list (ACL) to control which IP addresses are included as potential originator of traffic in this trunk from the Twilio point of view. It must be the Public IP addresses assigned to each one of our SIParators.

ecas	as@loscasas∨ Elas	tic SIP Trunking / Authentication /	IP Access Control /	🔎 Go to	Ö	?	<u></u>
S S S	Elastic SIP Trunking Dashboard Trunks Authentication IP Access Control Lists Credential Lists Networking Info	Trunk IPs Properties FRIENDLY NAME ASSOCIATED ASSOCIATED SIP DOMAINS					
	Tools Logs Usage Getting Started	IP Addresses	IP Ac FRIENDLY N Primary Tru Secondary	cess Control Lists may have u AME nk Irunk IP	p to 100 IP	addres •	×

Finally, Twilio will use those IP address in the host Request URI and it is used to match inbound traffic to the SIParator. It should be included here:



Tiew trunk: SIP Trunk 1: Twilio Elastic;PBX Act ▼	Goto SIP Trunk page	
SIP Trunk 1 (Help)		
 Enable SIP Trunk Disable SIP Trunk 		
SIP Trunking Service (Help)		
Use parameters from other SIP trunkDefine SIP trunk parameters		
Service name:	Twilio Elastic	(Unique descriptive name)
Service Provider Domain:	ingatelabstraining.pstn.twilio.com	(FQDN or IP address)
Restrict to calls from:	Twilio 🔻	('-' = No restriction)
Outbound Proxy:		(FQDN or IP address)
Use alias IP address:	- •	(Forces this source address from our side)
Outbound Gateway:	- •	('-' = Use Default Gateway)
Signaling Transport:	UDP •	('-' = Automatic)
Port number:		
From header domain:	Provider domain •	
Host name in Request-URI of incoming calls:	52	(Trunk ID - Domain name)
Remote Trunk Group Parameters (RFC 4904)		

5.4 SIParator configuration for Failover using DNS SRV and other features (Remote Users/Endpoints use case)

In this section, we explain another use case, Remote Users or Endpoints.

The SIParator is the immediate point of contact for any remote SIP device addressable through the Internet. It acts as registrar and proxy, but, it forwards all SIP requests using its built in DNS Override feature.

5.4.1 Using DNS SRV to become the SIP Proxy and Registrar with a Failover with 2 SIParators





We can create a new SRV record for a different domain name and use the SRV we created in 5.1 as siparator.ingatelabs.com, which we know resolves using Failover or Load Balance Strategy to siparator_ha1.ingatelabs.com and siparator_ha2.ingatelabs.com.

In this way, any SIP request from remote points will be sent to any of the SIParators based on the selected strategy.

Once the request reaches one of the SIParators, it will use DNS Override to decide which PBX will process the request.

Here is how it looks when using the SIParator to manage PBX Failover strategy. Note we are assigning lower priority to 10.0.1.149, which means that this will be the primary PBX, and only when it's unavailable will the request be sent to the second PBX.

Administra	tion Conf	Basic iguration	Network Rule Re	es and lays Se	SIP prvices T	SIP raffic	SIP Trunks	Failove	r Virtua Net	l Privo works	te Quality Servic	of Logging e and Tools	About	
SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan <mark>R</mark> o	uting S	SIP status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Status			
DNS	Overrio	de For	SIP Request	ts (<u>Hel</u> ı	<u>?)</u>			Rela	ıy To					
	Domain	۱ 	DNS Nat or IP Add	me ress	IP Add	lress	Po	rt I	ranspo	rt	Priority	Weight	Auth	Modify RURI
+ sip	parator.ing	atelab	10.0.1.149		10.0.1.1	49	5060		JDP 🔻	1		50	No 🔻	Yes •
			10.0.201.149		10.0.20	1.149	5060		JDP 🔻	2		50	No 🔻	Yes •

As recommended before we can speed up the detection by adding PBX addresses to the SIP Monitor Server list and including them in the VoIP Survival Table.

SIP Servers To N	Monitor	(<u>Help)</u>	
Server	Port	Transport	Delete Row
10.0.1.149		- •	
10.0.201.149		- •	



Basi	Signaling c Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VolP Survival	VoIP Survival Status				
٦	'oIP Survi	val <u>(Helj</u>	<u>))</u>								
۲	Enable VoIP Survival										
C	Disable V	oIP Surviv	ral								
	Server Cł	eck Inte	rval Do	omains T	o Monito	r					
[30	secon	nds	Domain N	ame	Method	Delet Row	e			
			pt	xact1.inga	telabs. Dis	play name	•				
			pt	xact2.inga	telabs. Dis	play name	•				

As we have also DNS A Records for a hosted private zone, we can use pbxact1.ingatelabs.local and pbxact2.ingatelabs.local as defined in section 5.2, either on SIP DNS Override, SIP Servers Monitor and VoIP Survival Tables

Your remote users/endpoints will refer then to siparator.ingatelabs.com as Proxy and registrar. You need to make sure the endpoint device supports DNS SRV resolution.

In case the endpoint doesn't support DNS SRV resolution but supports secondary Proxy/Registrar you can use siparator_ha1.ingatelabs.com as the primary and siparator_ha2.ingatelabs.com as the secondary or backup.

Here a few examples:

1) Using DNS SRV:

Account 1	
Account Status	Registered
* Account Active	
* Primary SIP Sonver	
Phinary SIP Server	siparator.ingateiabs.com:5060
Failover SIP Server	
Second Failover SipServer	
Prefer Primary SIP Server	●No ○Yes 😯
Outbound Proxy	
Backup Outbound Proxy	6
* SIP Transport	●UDP OTCP OTLS 🔮
NAT Traversal	ONo ●No,but send keep alive OSTUN
Label	3002
* SIP User ID	3002
* Authenticate ID	3002
* Authenticate Password	
Name	3002
DNS Mode	



2) Using DNS, A Records (Note the destination for SIP requests is managed by the outbound proxy. The domain is still siparator.ingatelabs.com

Account	
Account 1	
Account Status	Registered
* Account Active	⊖No ®Yes
* Primary SIP Server	siparator.ingatelabs.com:5060
Failover SIP Server	0
Second Failover SipServer	0
Prefer Primary SIP Server	●No ○Yes 🚱
Outbound Proxy	siparator_ha1.ingatelabs.com:5060
Backup Outbound Proxy	siparator_ha2.ingatelabs.com:5060
* SIP Transport	●UDP OTCP OTLS 2
NAT Traversal	○No ●No,but send keep alive ○STUN
Label	3002
* SIP User ID	3002
* Authenticate ID	3002
* Authenticate Password	
Name	3002
DNS Mode	

Finally, you can visually check registrations in the SIP Status Page on each SIParator:

dministrati	ion Con	Basic Ifiguration	Network	Rule Re	s and lays	Se	SIP rvices	SIP Traffic	SIP Trunk	Failove	r
SIP Methods F	Filtering	Local Registrar	Authenticat and Accoun	tion ting	SI Acco	P unts	Dial Plan	Routing	SIP Status	IDS/IPS	ID S
Active	e Sessi	ons (0 s	essions)								
There a	re no a	ctive ses	sions.								
Monit	tored S	SIP Serv	vers								
		Server		I	Port	Tra	nspo	rt Sta	itus		
pbxact	1.ingat	elabs.loc	al			UD	Р	On	line		
ingatel	labstrai	ning.pstn	.twilio.co	m		UD	Р	On	line		
10.0.1	.220					UD	Р	On	line		
pbxact	ingate	labs.local	1			UD	Р	On	line		
trunk.i	ngatela	lbs.com				TC	Р	On	line		
10.0.1	.149					UD	Р	On	line		
pbxact	2.ingat	elabs.loc	al			UD	Р	Of	line		
Regist	tered l	Users (1	registra	tion	ıs)		1.5		G	1.41	
3002/7	deinara	User tor ingate	labs com	107	cegis	200	od Fro	5060	Surviv	val Alias	es
3002@	ysipara	tor.mgate	aus.com	192		.200		5000			



5.5 PBX cross connection with SIParators

One potential scenario when a SIParator only goes offline, or a PBX only goes offline is that sip trunk traffic will go from a Main SIParator to a Failover PBX. In other words will go across in our case subnet $10.0.1.0/24 \leftarrow 10.0.201.0/24$. This case needs to have extra considerations as none of the SIParators are directly connected to both subnets and we want the traffic between PBX and SIParators always to happen on the Internal Interface.

In this scenario we need to consider adding static routes to each SIParator to make sure the traffic goes from the SIParator internal interface to the appropriate PBX subnet.

On the Main SIParator we will need then to add a static routo to define how to reach the PBX that is on the Failover subnet and not directly connected to it.

Routed Network				Router			
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	Interface or Tunnel	Delete Roy
10.0.201.0	10.0.201.0	24	internal 🔻		*	internal (eth1) •	
default	default		external •		*	external (eth0) T	

We are saying in order to reach 10.0.201.0 (Private subnet in the failover area), to use the dynamic gateway provided by DHCP on the Internal Interface and route using eth1.

6 Replicating and synchronizing SIParator configurations across all instances

Once you have one of the 2 SIParators fully configured we will need to replicate and synchronize with the secondary/failover configuration.

Some points to clarify:

1) Network Interface configuration is provided via DHCP by AWS VPC

terrace Over							
General							
Physical Device	Interface Name	Active					
eth0	external	Yes 🔻					
eth1	internal	Yes 🔻					
eth1	internal	Yes V					
eth1 Directly Connec	internal cted Networks	Yes ▼ (<u>Help)</u>					
eth1 Directly Conner Name	internal cted Networks Address Type	Yes ▼ (Help) DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface o Tunnel
eth1 Directly Connec Name external	internal cted Networks Address Type DHCP V	Yes V (Help) DNS Name or IP Address	IP Address *	Netmask / Bits	Network Address	Broadcast Address	Interface o Tunnel external (eth0



Priority	Dynamic	DI or I	NS Name P Address	IP Address	Int	erface	Delete Row
1	external •			*	externa	al (eth0) 🔻	
DNC C-			_	_	-	_	-
DNS Se	rvers <u>(He</u>	<u>lp)</u>					
DNS Se No.	rvers (<u>He</u> Dynan	l <u>p)</u> nic	DNS Nam or IP Addr	e IP	Address	Delete R	.ow
DNS Se No.	rvers (He Dynan externa	l <u>p)</u> nic	DNS Nam or IP Addr	ess IP	Address	Delete R	ow

- 2) Networks and Computers will be very similar in both SIParators. Only VPC_Private and VPC_Public differ from one SIParator to the other
 - a. $10.0.0.0/24 \rightarrow 10.0.10.0/24$
 - b. 10.0.1.0/24 → 10.0.201.0/24

Networks and Co	mputers						
Nama	Salaman	Lower L	imit	Upper (for IP 1	Limit ranges)	Interfere All AN	D
Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/vLAN	
+ Coral Springs] [•	homeoffice.ingatelabs.	69.65.66.170			- •	
+ Coral Springs LAN	· ·	192.168.200.0	192.168.200.0	192.168.200.255	192.168.200.255	- •	
+ Internet		0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	external (eth0 untagged) 🔻	
+ Twilio		34.203.250.0	34.203.250.0	34.203.251.255	34.203.251.255	- •	
	-	35.156.191.128	35.156.191.128	35.156.191.131	35.156.191.131	. .	
	-	54.65.63.192	54.65.63.192	54.65.63.195	54.65.63.195	- •	
	-	54.171.127.192	54.171.127.192	54.171.127.195	54.171.127.195	- •	
	-	54.172.60.0	54.172.60.0	54.172.61.255	54.172.61.255	- •	
	-	54.244.51.0	54.244.51.0	54.244.51.3	54.244.51.3	- •	
+ VPC		10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	- •	10
+ VPC_Private	-	10.0.1.0	10.0.1.0	10.0.1.255	10.0.1.255	internal (eth1 untagged) 🔻	i i
+ VPC_Public	-	10.0.0.0	10.0.0.0	10.0.0.255	10.0.0.255	external (eth0 untagged) 🔻	1 e
+ pbx	pbxact1					- •] (
	pbxact2					- •	
+ pbxact1		pbxact1.ingatelabs.loca	10.0.1.149			internal (eth1 untagged) 🔻	
+ pbxact2	1 - •	pbxact2.ingatelabs.loca	10.0.201.149			internal (eth1 untagged) 🔻	10

3) To manage Near End Nat Traversal, and because AWS VPC manages Elastic Public IPs as a NAT IP to an interface, we will need to properly assign the Public IP address in SIP Services → Basics. We can use the Domain name for each Specific SIParator as shown here for the Main SIParator in our pair:

SIPARATOR 1



6.1 How to synchronize Configuration.

There are two ways we can create and apply the configuration needed and adjusted for the Failover SIParator. Both use the CLI saved file form the Main SIParator.

We can edit even manually (using and editor) or automate using some scripting application the needed changes to be used in the Failover SIParator, or we can just directly load a CLI file in the Failover for the one downloaded from the main unit and do the modifications using the GUI in the second unit.

6.1.1 Obtaining CLI file from the main SIParator

We will manually save a CLI configuration file and use it to load the configuration into the failover unit.

1) Saving the CLI Backup



in@ate Firewall Ingate S	SIPARATOR 6.1.1 for AWS Lab
Administration Basic Configuration Network Rules and Relays	SIP SIP SIP Failover Virtual Private Quality of L Services Traffic Trunks Failover Networks Service ar
Save/Load Show User Configuration Configuration Upgrade	Table Date and Change Look Time Restart Language
Test Run and Apply Conf (Help)	Show Message About Unapplied Changes
Duration of limited test mode:	On every page
30 seconds	On the Save/Load Configuration page
Apply configuration	○ Never
Backup (<u>Help</u>)	
The permanent configuration is not affected	
Save to local file Load from local file Loca	al file: Choose File No file chosen
Save/Load CLI Command File (Hel	<u>p)</u>
The permanent configuration might be affec	eted by loading a CLI file.
Save config to CLI file Load CLI file Local	1 file: Choose File No file chosen
Abort All Edits (<u>Help)</u>	Reload Factory Configuration (<u>Help</u>)
The permanent configuration is not affected	The permanent configuration is not affected.
Abort all adita	Load factory configuration
Abort all edits	

The file name will be like:

"Ingate SIPARATOR 6.1.1 for AWS Lab_2018-04-27T003837.cli"

6.1.2 Manually modify CLI File:

Using a text editor such as notepad++, make the following changes:

• Modify the Public IP Address for the NATed firewall with the FQDN and IP of the second SIParator:

Seach for "# sip.public_ip"

You will find something like this:

```
1822
1823 # sip.public_ip
1824 modify-row sip.public_ip 1 ip="siparator_hal.ingatelabs.com|52.7.99.1|"
1825
```

Replace this with the FQDN of the second SIParator. No need to change the IP as it will be resolved on the second SIParator once the new configuration is loaded and saved. It should look like this:

```
1823 # sip.public_ip
1824 modify-row sip.public_ip 1 ip="siparator_ha2.ingatelabs.com" 52.7.99.1|"
1825
```



• Now we are going to change Private and Public VPC subnets

Search for "# firewall.network_groups"

You will find something like this:

650	# firewall.network groups
651	clear-table firewall.network groups
652	add-row firewall.network groups {id 1} interface=- \
653	lower_ip="homeoffice.ingatelabs.com 69.65.66.170 " \
654	name="Coral Springs" subgroup=- upper ip=""
655	add-row firewall.network groups {id 2} interface=- lower ip=192.168.200.0 \
656	name="Coral Springs LAN" subgroup=- upper_ip=192.168.200.255
657	add-row firewall.network_groups {id 3} interface=eth1 lower_ip=10.0.1.0 \
658	name=VPC_Private subgroup=- upper_ip=10.0.1.255
659	add-row firewall.network_groups {id 4} interface=eth0 lower_ip=10.0.0.0 \
660	name=VPC_Public subgroup=- upper_ip=10.0.0.255
661	add-row firewall.network_groups {id 5} interface=eth0 lower_ip=0.0.0.0 \
662	name=Internet subgroup=- upper_ip=255.255.255.255
663	add-row firewall.network_groups {id 6} interface=- lower_ip=10.0.0.0 \
664	name=VPC subgroup=- upper_ip=10.0.255.255
665	add-row firewall.network_groups {id 8} interface=- lower_ip=54.172.60.0 \
666	name=Twilio subgroup=- upper_ip=54.172.61.255
667	add-row firewall.network_groups {id 9} interface=- lower_ip=54.244.51.0 \
668	name=Twilio subgroup=- upper_ip=54.244.51.3
669	add-row firewall.network_groups {id 10} interface=- lower_ip=54.171.127.192 \
670	name=Twilio subgroup=- upper_ip=54.171.127.195
671	add-row firewall.network_groups {id 12} interface=- lower_ip=35.156.191.128 \
672	name=Twilio subgroup=- upper_ip=35.156.191.131
673	add-row firewall.network_groups {id 13} interface=- lower_ip=54.65.63.192 \
674	name=Twilio subgroup=- upper_ip=54.65.63.195
675	add-row firewall.network_groups {id 15} interface=- lower_ip=34.203.250.0 \
676	name=Twilio subgroup=- upper_ip=34.203.251.255
677	add-row firewall.network_groups {id 16} interface=eth1 \
678	lower_ip="pbxactl.ingatelabs.local 10.0.1.149 " name=pbxact1 \
679	subgroup=- upper ip=""

Change the Upper and Lower IPs to match the new subnet in the second SIParator. It should then look like this:

		· · · · ·	
657	add-row firewall.network_groups	{id 3} interface=eth1	lower_ip=10.0.201.0 \
658	name=VPC_Private subgroup=-	upper_ip=10.0.201.255	
659	add-row firewall.network groups	{id 4} interface=eth0	lower ip=10.0.101.0 \
660	name=VPC_Public subgroup=- u	pper_ip=10.0.101.255	

• As we are using Twilio, we will change the Host name in Request URI to the Public IP address of the Secondary SIParator

Search for "domain_id"

2135	# sipswitch.trunk_params
2136	modify-row sipswitch.trunk params 1 alias_ip
2137	domain=ingatelabstraining.pstn.twilio.con domain_id=52 .1 \
2138	enabled=off from_domain=pdomain from_domain_str=""_fwd_refer=off \
2139	gin_reg=off hide_rr=off hide_to_tags=off itsp_host_addrs=Twilio \
2140	ltrunk_group_param="" ltrunk_group_usage=- max_calls_per_line="" \
2141	max_calls_total=10 name="Twilio Elastic" outbound_gw=- \
2142	outbound_proxy="" port="" preserve_max_forwards=off \
2143	redirect_caller_domain=off redirect_home_domain=off \
2144	referto_domain="" relay_media=on remove_via=off route_incoming=ruri \
2145	send_dtmf_via_sip_info=off transport=udp trunk=1 \
2146	trunk_group_param="" trunk_group_usage=- trusted_networks_enable=off \
2147	use_preferred_identity=off

Change the value for domain_id to the public IP address of the destination SIParator. It should look like this:



2135	# sipswitch.trunk_params
2136	modify-row sipswitch.trunk_params 1 alias_ip=\
2137	domain=ingatelabstraining.pstn.twilio.com domain id=35
2138	enabled=off from domain=pdomain from domain str="" fwd refer=off \
2139	gin_reg=off hide_rr=off hide_to_tags=off itsp_host_addrs=Twilio \
2140	ltrunk group param="" ltrunk group usage=- max calls per line="" \
2141	max calls total=10 name="Twilio Elastic" outbound gw=- \
2142	outbound_proxy="" port="" preserve max_forwards=off \
2143	redirect_caller_domain=off redirect_home_domain=off \
2144	referto_domain="" relay_media=on remove_via=off route_incoming=ruri \
2145	<pre>send_dtmf_via_sip_info=off transport=udp trunk=1 \</pre>
2146	trunk_group_param="" trunk_group_usage=- trusted_networks_enable=off \
2147	use_preferred_identity=off

• Need to adjust Dial Plan for Matching Request-URI

In case you are matching the internal IP address in the Request URI in the dial plan you might need to consider this change in the file to be synchronized.

Seach for "# sipswitch.request_to"



Replace the IP with the Failover internal IP address:

2100	
2101	# sipswitch.request_to
2102	clear-table sipswitch.request to
2103	add-row sipswitch.request to {id 1} domain=10.0.201.147 head="" \
2104	min tail length="" name=to pstn prefix="" regexp="" tail=telchar
2105	

In order to avoid this change you can build the Rules in the dial plan using regular expressions to match ip addresses of all SIParators used in failover. You can use something similar to this rule in the Match Request-URI:

Matching Request-URI (Help)							
Name	Use This					Or This	Delete Barr
Ivame	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	Delete Kow
to_pstn			- •			sip:(.*)@10\.0\.(1 201)\.147	

• Replicate static route to consider Failover and non-failover cross connection

Search for "# network.routes"





Notice The Primary SIParator has a static route to the subnet where the failover PBX is located.

We will need to put on the failover SIParator a static route to the subnet where the main PBX is located. Like this:

1342	# network.routes
1343	clear-table network.routes
1344	add-row network.routes {id 1} destination=default/ gateway=" * external" \
1345	interface=eth0 priority=1
1346	add-row network.routes {id 2} destination=10.0.1.0/24 \
1347	gateway=" * internal" internace=ethi priority=""
1348	

- Save your changes to the file
- 2) Load the Modified CLI File.

Once you have logged in to the Failover SIParator go to the Administration \rightarrow Save/Load Configuration and load the CLI file you modified in the previous step.

in © ate	Firewa	ll Ing	gate S	IPA	RATO	OR 6.	1.1 fo	r AWS I	Lab
Administration	Basic Configuration	Network Ru R	les and elays S	SIP ervices	SIP Traffic	SIP Trunks	Failover	Virtual Private Networks	Quality of Service
Save/Load Configuration	Show onfiguration	User Administration	Upgrade	Table Look	Date and Time	Restart	Change Language		
Test Run	and Appl	y Conf (He	<u>elp)</u>	Show	v Mess	age Ab	out Una	applied Cl	ianges
Duration of 1 30 se Apply config	imited test econds uration	mode:		 Or Or Or No 	n every j n the Sav ever	page ve/Load	l Configu	ration page	
Backup ((<u>Help)</u>								
The permane	nt configu	ration is not a	affected.						
Save to loca	I file Loa	d from local fi	e Local	file:	Choose	File In	gate SIPA	Rab Failov	er
Save/Load	l CLI Co	mmand Fil	e <u>(Help</u>	<u>)</u>					
The permane	nt configu	ration might	be affect	ed by	loading	2 CLI fi	<u>le.</u>		
Save config	to CLI file	Load CLI file	e I.ocal	file:	Choose F	File No	file chose	n	
Abort All	Edits (H	<u>lelp)</u>		Relo	ad Fac	tory C	onfigur	ation <u>(Hel</u>	<u>p)</u>
The permane affected. Abort all edit	ent configu s	ration is not	[The pe Load	rmanent factory co	t config onfigurat	uration is tion	not affecte	d.



- Chose the file
- Load CLI File

Once the file is loaded you'll get a confirmation message like this:



Now, go to SIP Services \rightarrow Basic and let's refresh the Public IP address associated to the FQDN we entered in the CLI file.

It looks like:

Public IP Address for NATed firew	all <u>(Help)</u>
This setting is not supported for the Standa	alone configuration.
DNS Name or IP Address siparator_ha2.ingatelal 52 .1	This IP does not corresponds to the FQDN

Using the "Look up All IP addresses again" button it will be resolved again and updated correctly.



This setting is not supported for the Standalone configuration DNS Name IP Address or IP Address siparator_ha2.ingatelal 35. 0.228
DNS Name IP Address or IP Address siparator_ha2.ingatelal 35. 0.228
siparator_ha2.ingatelal 35.).228
siparator_naz.ingateiai 55. 7.220
Save Undo Look up all IP addresses again

Next step is just to Apply all changes and save.

Administration	Basic Configuration	Network	Rules and Relays	SIP Service
	Changes	have beer	n made t	o the pre
Save/Load Configuration	Show Configuration	User Administrat	ion Upgr	Table ade Look
Test Ru	n and Appl	y Conf	<u>(Help)</u>	Sh
Duration o	f limited test	mode:		۲
30	seconds			\bigcirc
Apply conf	figuration			01
You are curr Save config	ently testing uration Cor	the prelin	ninary co ng Rev	onfiguration vert



6.1.3 Loading CLI file and use the GUI to make all needed adjustments

Once you have logged in to the Failover SIParator go to the Administration \rightarrow Save/Load Configuration and load the CLI file you downloaded from the Main SIParator.

inGate Firewall Inga	ate SIPA	RATOR 6	.1.1 for	AWS L	ab
Administration Basic Configuration Network Rela	and SIP ays Services	SIP SIP Traffic Trunks	Failover	/irtual Private Networks	Quality of Service
Save/Load Show User Configuration Configuration Administration U	pgrade Table	Date and Time Restart	Change Language		
Test Run and Apply Conf (Help Duration of limited test mode: 30 seconds Apply configuration). Sho • O • O • N	w Message A n every page n the Save/Loa ever	bout Una d Configur	pplied Characteristics	anges
Backup (Help) The permanent configuration is not aff Save to local file Load from local file	ècted. Local file: [Choose File Ir	ngate SIPAF	Rab Failove	r
Save/Load CLI Command File The permanent configuration might be Save config to CLI file	(<u>Help)</u> affected by Local file: [loading a CLL Choose File No	51e. o file choser	1	
Abort All Edits (Help)	Relo	ad Factory (Configura	tion <u>(Help</u>).
The permanent configuration is not affected. Abort all edits	The period	ermanent config factory configura	guration is ation	not affected	

- Chose the file
- Load CLI File

Once the file is loaded you'll get a confirmation message like this:

At this point you have exactly the same configuration you have on the Main unit, loaded in the Failover unit, but it hasn't been applied yet.

Before applying the configuration, we will modify all the parameter needed.



• Modify the Public IP Address for the NATed firewall with the FQDN and IP of the second SIParator:





Change the FQDN to the one associated to the Public IP address of the Failover SIParator. Then press "Look up IP addresses again" to discover the new IP address

• Now we are going to change Private and Public VPC subnets

Networks → Networks and Computers



Change the Upper and Lower IPs to match the new subnet in the second SIParator. Then press "Look up IP addresses again" to discover the new IP address



• As we are using Twilio, we will change the Host name in Request URI to the Public IP address of the Secondary SIParator

SIP Trunks \rightarrow Go to SIP Trunk

Host name in F	Request-URI of incoming calls:	35.	.228	(Trunk
Save Undo	Look up all IP addresses again			

• Need to adjust Dial Plan for Matching Request-URI

In case you are matching the internal IP address in the Matching Request URI in the dial plan you might need to consider this change in the file to be synchronized.

SIP Traffic →Dial Plan

Replace the IP with the Failover internal IP address:

Here we can build the Rules in the dial plan using regular expressions to match ip addresses of all SIParators used in failover with a single rule. You can use something similar to this rule in the Match Request-URI:

Matching Reque	est-URI (<u>Help</u>)						
Name			Use This			Or This	Delete Dem
Ivame	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	Delete Kow
to_pstn			- •			sip:(.*)@10\.0\.(1 201)\.147	

• Replicate static route to consider Failover and non-failover cross connection

Network → All Interfaces

Notice The Primary SIParator has a static route to the subnet where the failover PBX is located.

We will need to put on the failover SIParator a static route to the subnet where the main PBX is located. Like this:

Failover Static Routes:

	Routed Network			Router			
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	Interface or Tunnel	Delete Rov
10.0.0.0	10.0.0.0	24	eth1 🔻		*	internal (eth1) V	
default	default		eth0 v		*	external (eth0) V	



Main Static Route

	Routed Network			Router			
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	Interface or Tunnel	Delete Row
10.0.201.0	10.0.201.0	24	eth1 ▼		*	internal (eth1) <	
default	default		eth0 🔻		*	external (eth0) T	

• Save all and apply changes

Administration	Basic Configuration	Network Ru	les and SI Relays Serv
Save/Load Configuration	Show Configuration	User Administration	Ta Upgrade La
Test Ru	n and Appl	y Conf <u>(H</u>	<u>elp)</u> S
Duration o	f limited test	mode:	۲
30	seconds		C
Apply conf	iguration		С
-			_

You are currently te	sting the prelimina	ıry configur
Save configuration	Continue testing	Revert

7 Final Tips and recommendations

There is not a "one size fits all" solution when talking about High Availability (HA) deployments in AWS, but the structure presented here is a good template to start and build variations on top of it.

What is presented here considers 2 SIParators in Failover or Load Balance, inside the same VPC but in separated Availability zones. This is a typical case when we want to prevent not only Instance failures but Data Center Isolations.

With minor adjustments it can be extrapolated to other scenarios, such as:



- Two SIParators in separated VPCs. In this case, some additional modifications will be needed in the CLI Migration file, specifically in the Networks and Computers section. Also, you will need to enable peer connection between VPCs using native services from AWS, and some additional Route53 Hosted Private Zone and SRV records.
- Two SIParators in separated regions. This case is very similar to Separated VPCs in the same region

One recommended reading about VPC Peering can be found here:

https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/Welcome.ht ml

The following table can help identify how HA can be implemented depending on the scenarios and what we want, in order to prevent specific call flow interruptions. (see next page)



			SIP TRUNK	ING FLOWS			REMOTE US	ERS FLOWS	
	IECHINIQUE	PBX> SBC Outbound	PBX <sbc Inbound</sbc 	SBC>PSTN Outbound	SBC <pstn Inbound</pstn 	PBX> SBC Outbound	PBX <sbc Inbound</sbc 	SBC>INET Outbound	SBC <inet Inbound</inet
	SIP Filtering	Need to add IPPBX IP addresses or DNS names for each PBX in the Networks and computers section and has had concesting calls from that name in SIP Traffic Filters	NA	NA	Need to add ITSP potential souce IP addresses including SIP and RTP in Network and computers section and enable processings calls from that name in SIP Taffic Filters	NA	NA	NA	Need to add all portential Source the address from which calls can be originated in the Networks and Computers section and enable processing calls for those names in the SPT ratific Filters. This might represent a security breach if source F's are urperdictable to use f. Is recommended to use f. Is for recommended to use f. Is for
(PBX Dual Homing	NA	Use SIParator native capability in SIP Trunk Group to associate up to 2 domains to a PBX (see	NA	NA	NA	NA	NA	NA
ISE	SIP Trunk Dual Homming	NA	NA	Use SIParator native capability in SIP Trunk Group to associate up to 2 domains to an ITSP	NA	NA	NA	NA	NA
LO BE (DNS SRV Public Hosted Zones	NA	NA		If ITSP Supports DNS SRV, would be enough to provide Fallover or load balance destinations to the SBC from the Carrier.	NA	NA	NA	Any Remote endpoint will use (Registrar & Proxy) domain name defined in SRV Record. DNS will resolve failover or balancing depending on the
. \$700.	DNS SRV Private Hosted Zones	If PBX supports resolving DNS SRV, a single trunk will be enough to reach any of the SBC, i either for Failower or load balance strategy	Defining SRV Records to reach the PBX will allow to establish a Fallover or Load Balance strategy to reach any PBX associated to the same internal/private	NA	NA	Defining SRV Records to reach Internaly the SBC will allow to establish a Fallover or Load Balance strategy to reach any PBX associated to the same	Defining SRV Records to reach Internallythe PBX will allow to establish a Fallover or Load Balance strategy to reach any PBX associated to the same	NA	NA
L	DNS Override (SiParator)	NA	NA	NA	NA	NA	Here DNS Override will act as an internal DNS and will be able to route SIP Requests coming from outside to the corresponding	As part of DNS Override a local registartio table is kept for location purposes of the end points	NA
	Dial Plan (SIParator)	NA	NA	Dial Plan is an additional resource to add complementary techniques to associate more than one destination and hunt between them for a given call	NA	NA	NA	NA	NA
	VolP Survival (SiParator)	NA	NA	NA	AN	٩٨	Using VoIP Survival, in case no PBX is available, SiParator can asume a temporary rol to become the Registrar and Sproxy	NA	Using VolP Survival, in case no PBX is available, SiParator can asume a temporary rol to become the Registrar and Sproxy



8 Additional help or support

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

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

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

