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

[May 15th, 2019]

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 Reference Guide) 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.

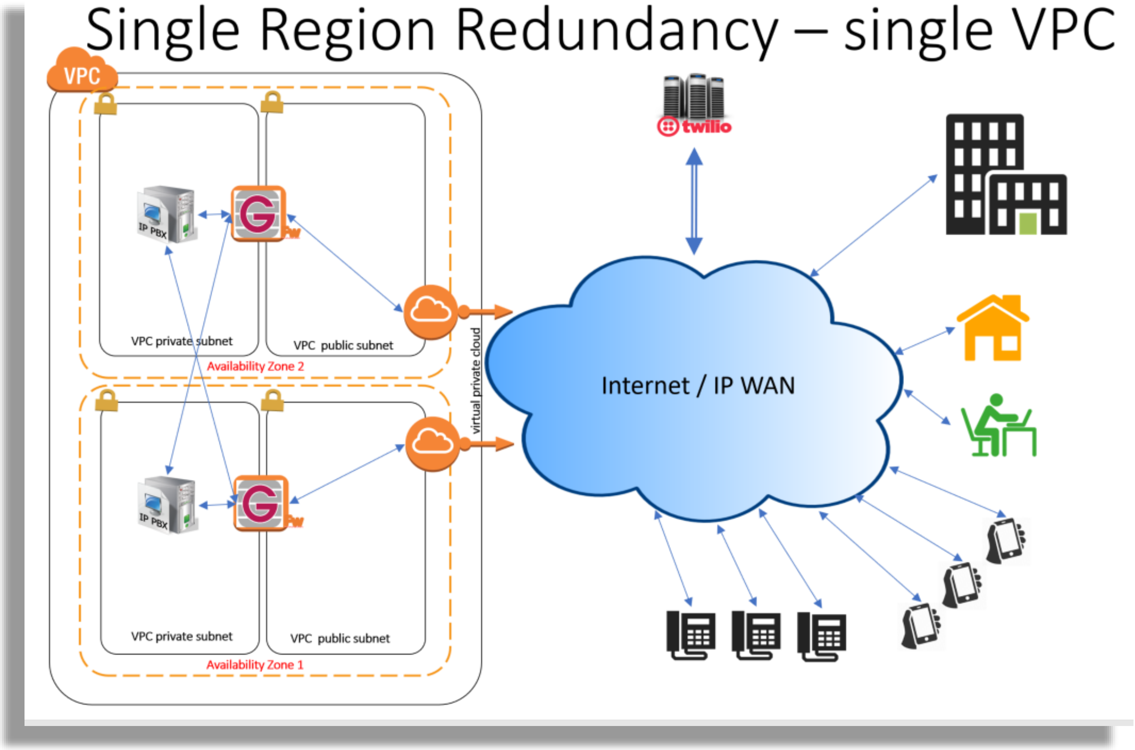
A resilient implementation will be the one that provides minimum down time to both scenarios, users remotely connected willing to use Telephony Services and PSTN access

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 (Failover) 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.



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:

1) 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;

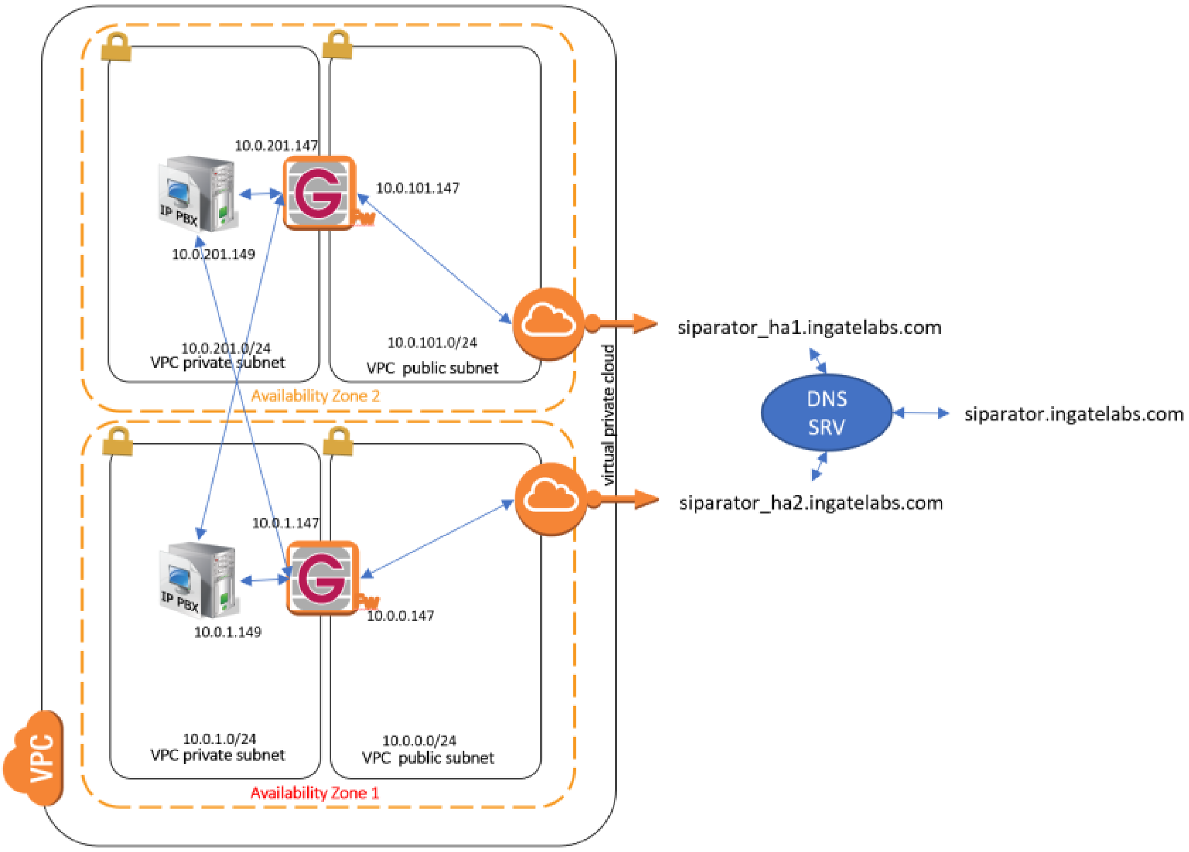
    a. Full support of DNS SRV records, so they will send traffic to an FQDN and SRV records will define the failover strategy,

    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.

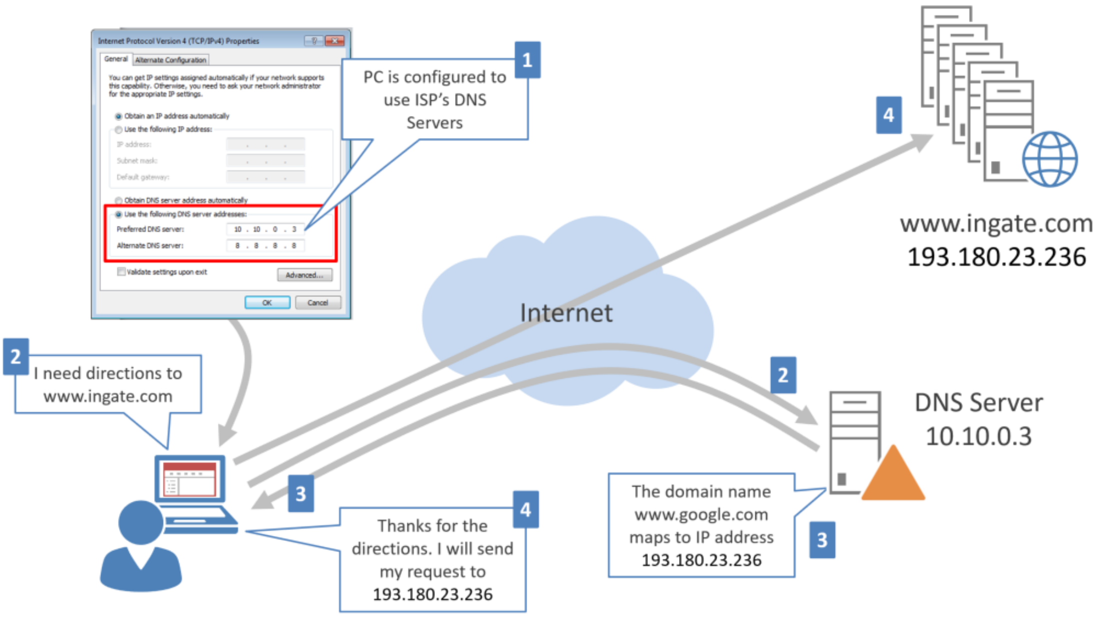
2) Both SBCs will be able to process inbound traffic. If one SBC becomes unreachable to the ITSP, the second SBC will be tried. (this failover is provided by the ITSP)

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 www.ingate.com and instead is interpreted as the IP address 193.180.23.236
- DNS Infrastructure is a hierarchy of databases distributed across the internet (https://en.wikipedia.org/wiki/Domain_Name_System)

4.2 DNS Illustrated.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 0 . 3
Alternate DNS server: 8 . 8 . 8 . 8

□ Validate settings upon exit

Advanced...
OK
Cancel
1
PC is configured to use ISP's DNS Servers
2
I need directions to www.ingate.com
Internet
4
www.ingate.com
193.180.23.236
2
DNS Server
10.10.0.3
3
The domain name www.google.com maps to IP address 193.180.23.236
3
4
Thanks for the directions. I will send my request to 193.180.23.236

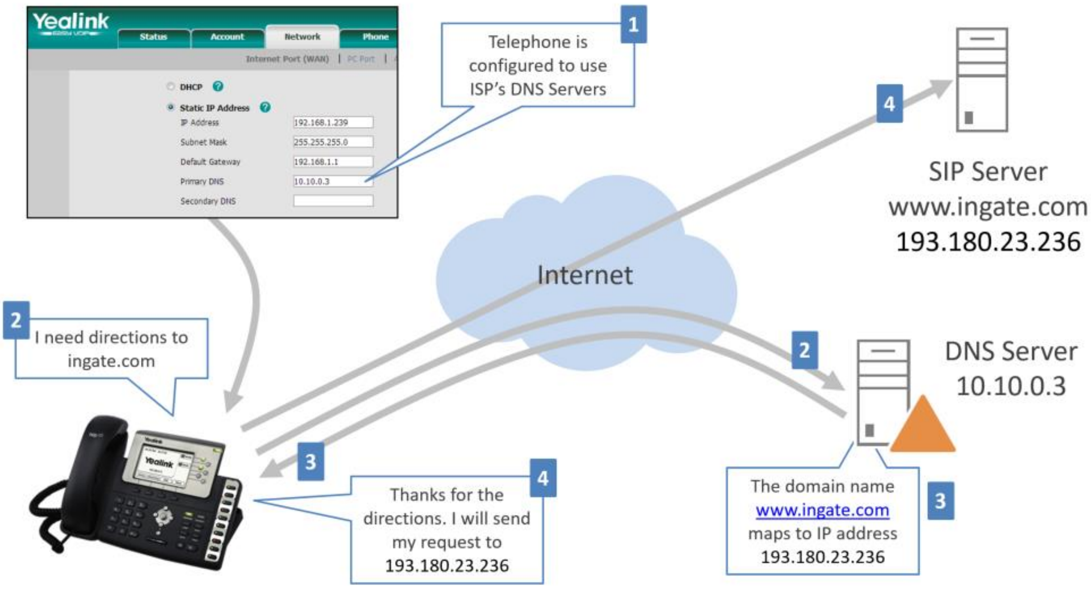
1) A Client device is configured to use a specific DNS Server (10.10.0.3)
2) The Client device seeks to access www.ingate.com, and asks the DNS Server
3) The DNS Server responds to the client with the IP address where www.ingate.com is located
4) Now the Client sends the same request to the discovered 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:



○ DHCP

● Static IP Address

IP Address: 192.168.1.239

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Primary DNS: 10.10.0.3

Secondary DNS:

1 Telephone is configured to use ISP's DNS Servers

2 I need directions to ingate.com

3 The domain name www.ingate.com maps to IP address 193.180.23.236

4 Thanks for the directions. I will send my request to 193.180.23.236

- 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

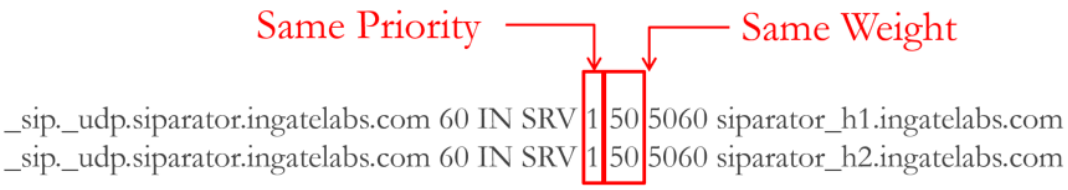
*_sip._udp.**siparator.ingatelabs.com** 60 IN SRV 1 50 5060 siparator_h1.ingatelabs.com*
*_sip._udp.**siparator.ingatelabs.com** 60 IN SRV 2 50 5060 siparator_h2.ingatelabs.com*

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:



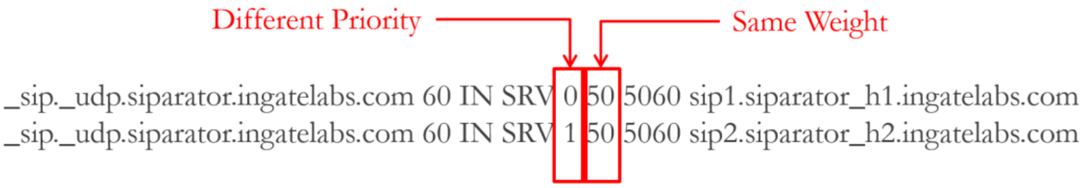
```
_sip._udp.siparator.ingatelabs.com 60 IN SRV 1 50 5060 siparator_h1.ingatelabs.com
_sip._udp.siparator.ingatelabs.com 60 IN SRV 1 50 5060 siparator_h2.ingatelabs.com
```

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:



```
_sip._udp.siparator.ingatelabs.com 60 IN SRV 0 50 5060 sip1.siparator_h1.ingatelabs.com
_sip._udp.siparator.ingatelabs.com 60 IN SRV 1 50 5060 sip2.siparator_h2.ingatelabs.com
```

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

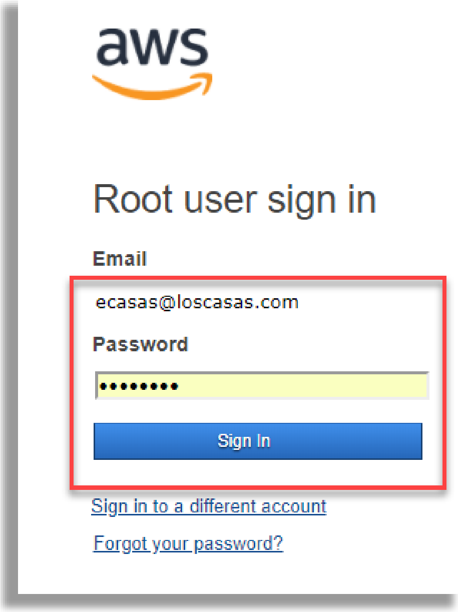
AWS provides its own DNS Services known as ***"Route 53"***.

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)



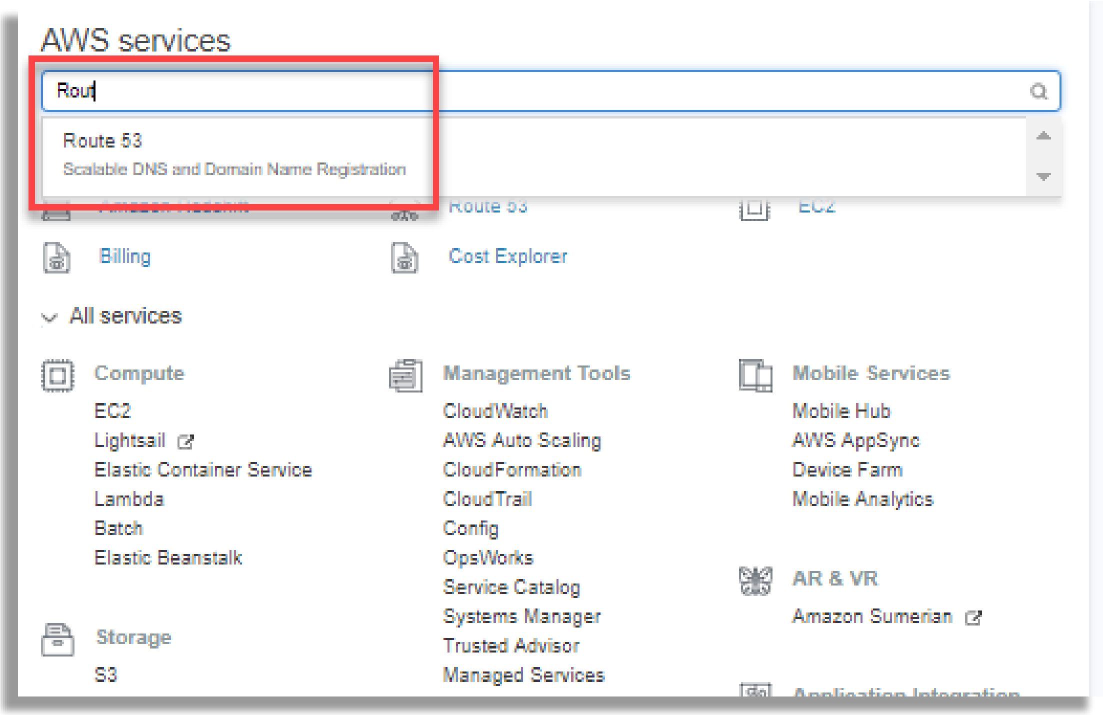
Root user sign in

Email

ecasas@loscasas.com

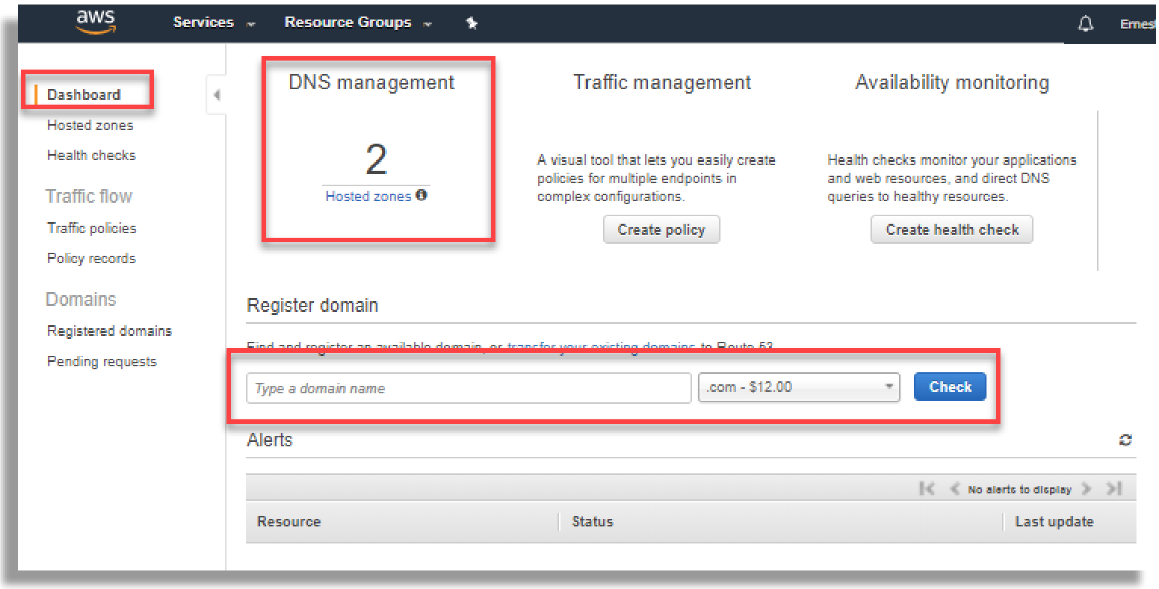
Password

••••••••



Scalable DNS and Domain Name Registration

Route 53 dashboard should look like this:



A visual tool that lets you easily create policies for multiple endpoints in complex configurations.

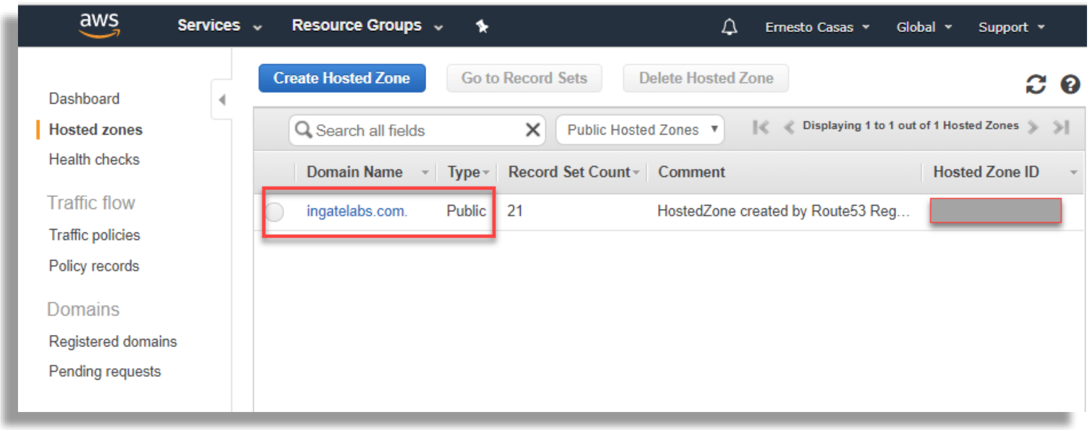
Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.

Find and register an available domain, or transfer your existing domains to Route 53

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.

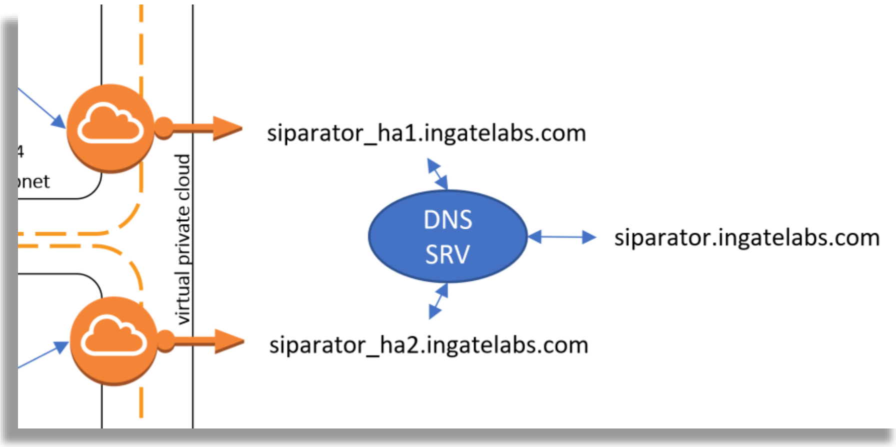
In our example we have already created and own a public domain "ingatelabs.com"



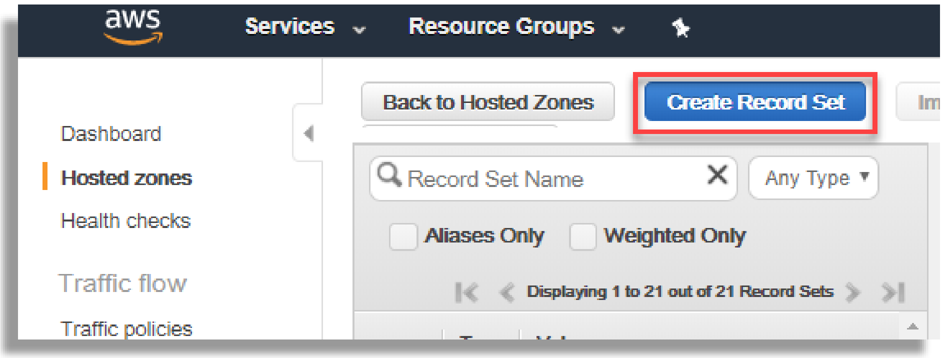
Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
ingatelabs.com.	Public	21	HostedZone created by Route53 Reg...	[redacted]

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

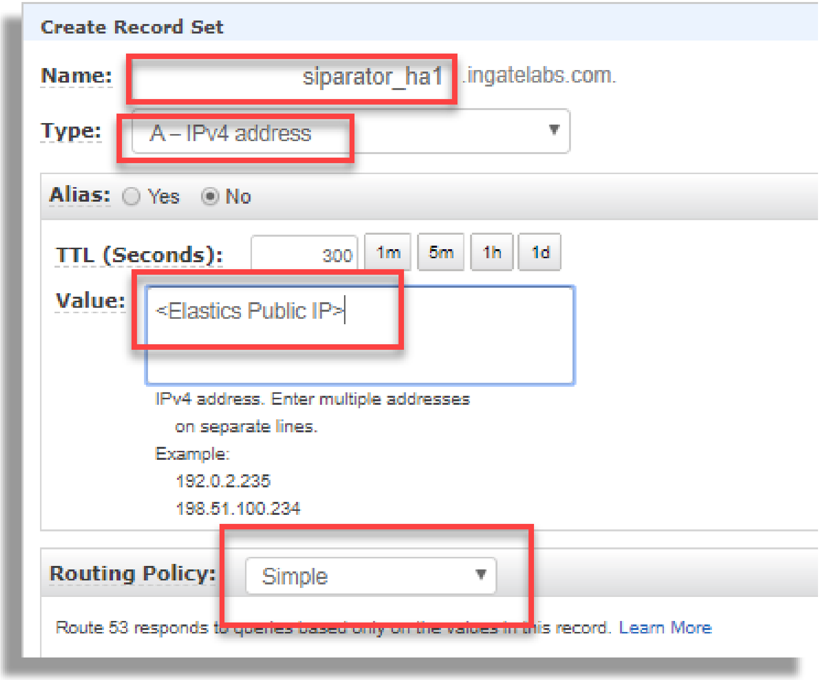
Based in our diagram:



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



Select the hosted zone and press on “Create Record Set”



Create Record Set

Name: siparator_ha1 .ingatelabs.com.

Type: A – IPv4 address

Alias: ○ Yes ● No

TTL (Seconds): 300

Value: <Elastics Public IP>

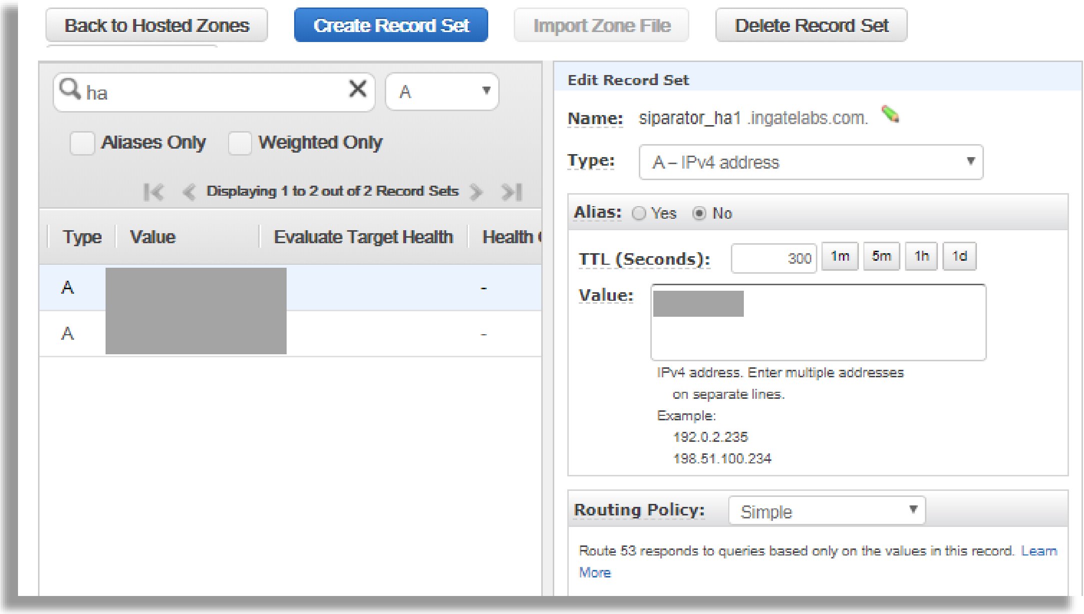
IPv4 address. Enter multiple addresses on separate lines.
Example:
192.0.2.235
198.51.100.234

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. Learn More

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:



Search: ha

Type filter: A

□ Aliases Only □ Weighted Only

Displaying 1 to 2 out of 2 Record Sets

Type	Value	Evaluate Target Health	Health
A	[redacted]	-	
A	[redacted]	-	

Edit Record Set

Name: siparator_ha1 .ingatelabs.com.

Type: A – IPv4 address

Alias: ○ Yes ● No

TTL (Seconds): 300

Value: [redacted]

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

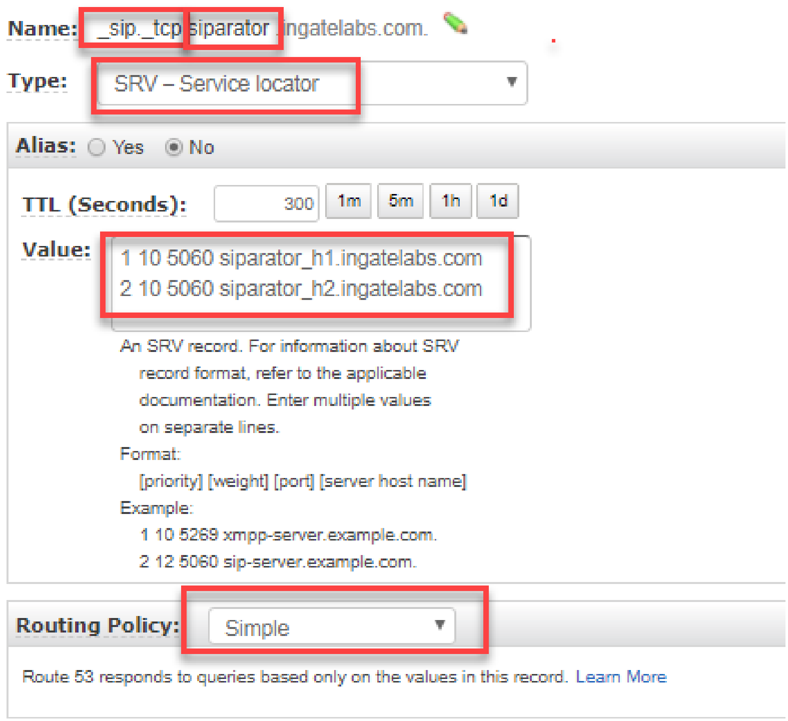
Now we have two new FQDN, each one resolving to one of the corresponding public IP addresses.

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: _sip._tcp.siparator.ingatelabs.com.

Type: SRV – Service locator

Alias: ○ Yes ● No

TTL (Seconds): 300

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

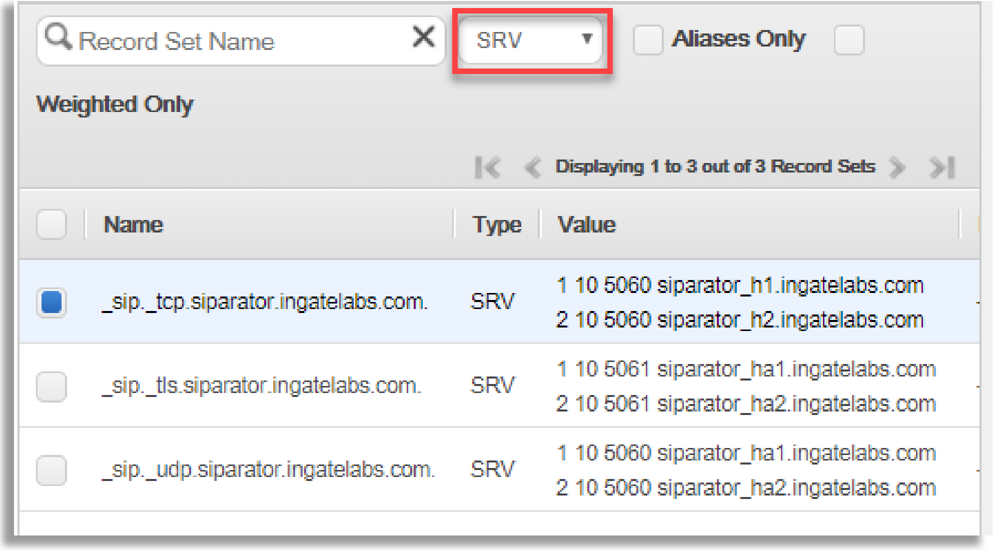
1) Note that Protocol and transport are part of the domain prefix (_sip._tcp),
2) The FQDN that will be referred to resolve is siparator.ingatelabs.com
3) Siparator_h1 will be the primary for failover (lowest priority)
4) _h1 and _h2 have same weight
5) Routing Policy will be kept by default.

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:



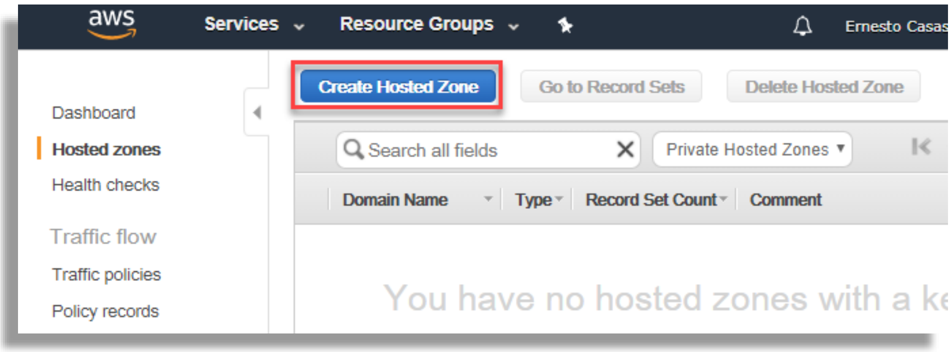
Name	Type	Value
_sip._tcp.siparator.ingatelabs.com.	SRV	1 10 5060 siparator_h1.ingatelabs.com 2 10 5060 siparator_h2.ingatelabs.com
_sip._tls.siparator.ingatelabs.com.	SRV	1 10 5061 siparator_ha1.ingatelabs.com 2 10 5061 siparator_ha2.ingatelabs.com
_sip._udp.siparator.ingatelabs.com.	SRV	1 10 5060 siparator_ha1.ingatelabs.com 2 10 5060 siparator_ha2.ingatelabs.com

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

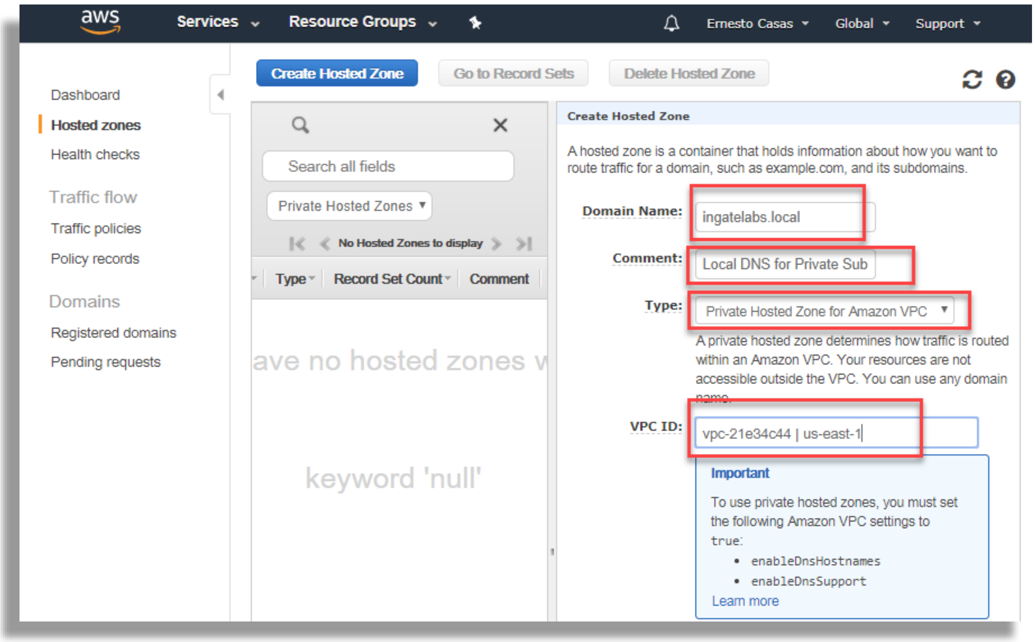
Later we will show 2 methods to implement Failover for the PBX. One of them is also based on SRV records but used to resolve IPs in the private network. To do so we will create a private hosted zone for the private network using a private domain named “ingatelabs.local”.

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



You have no hosted zones with a ke

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



Create Hosted Zone

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain Name: ingatelabs.local

Comment: Local DNS for Private Sub

Type: Private Hosted Zone for Amazon VPC

A private hosted zone determines how traffic is routed within an Amazon VPC. Your resources are not accessible outside the VPC. You can use any domain name.

VPC ID: vpc-21e34c44 | us-east-1

Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

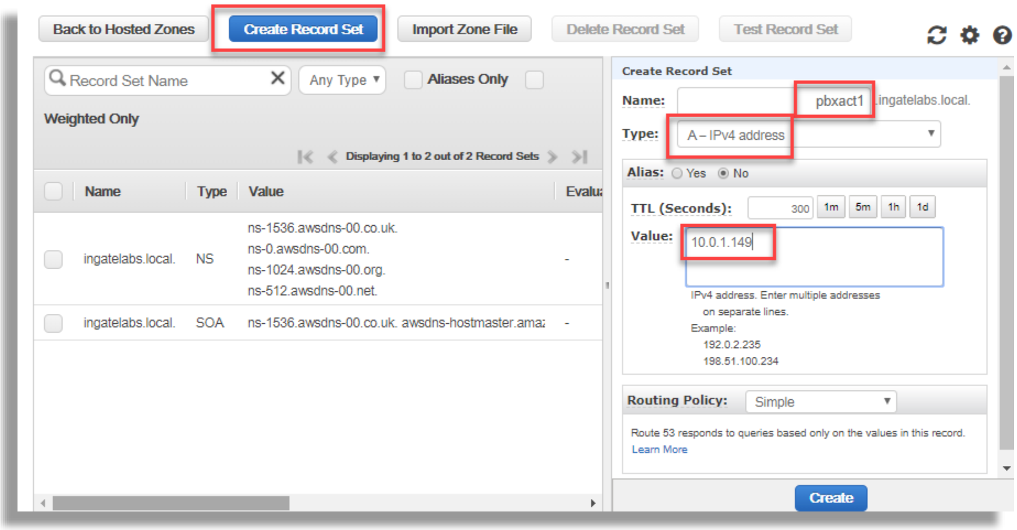
- `enableDnsHostnames`
- `enableDnsSupport`

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: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html

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



Name	Type	Value	Evalu
ingatelabs.local.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	-
ingatelabs.local.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz	-

Create Record Set

Name: pbxact1 .ingatelabs.local.

Type: A – IPv4 address

Alias: ○ Yes ● No

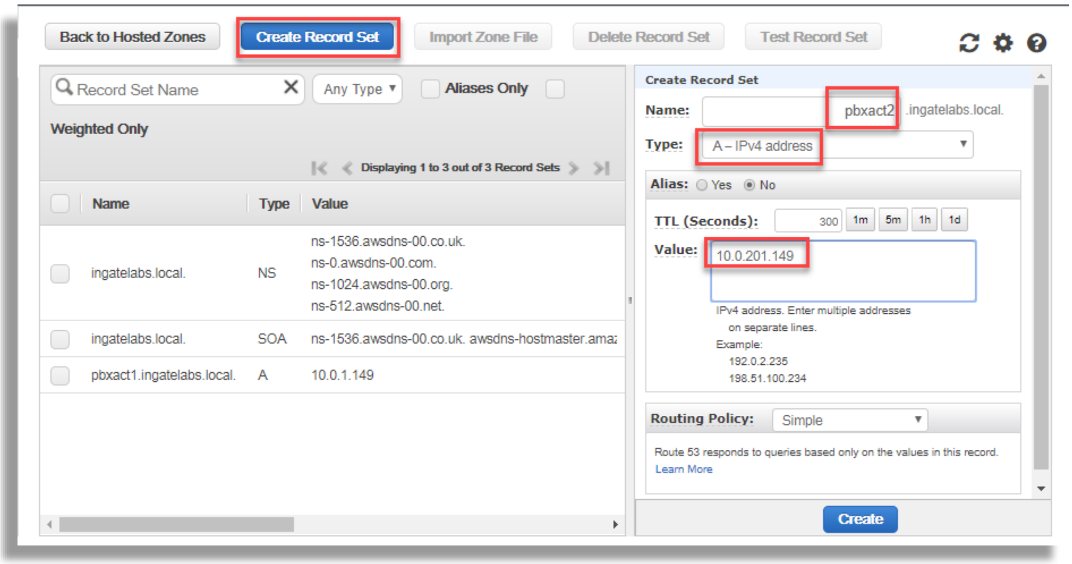
TTL (Seconds): 300 1m 5m 1h 1d

Value: 10.0.1.149

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



Name	Type	Value
ingatelabs.local.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
ingatelabs.local.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.ama:
pbxact1.ingatelabs.local.	A	10.0.1.149

Create Record Set

Name: pbxact2 .ingatelabs.local.

Type: A – IPv4 address

Alias: ○ Yes ● No

TTL (Seconds): 300

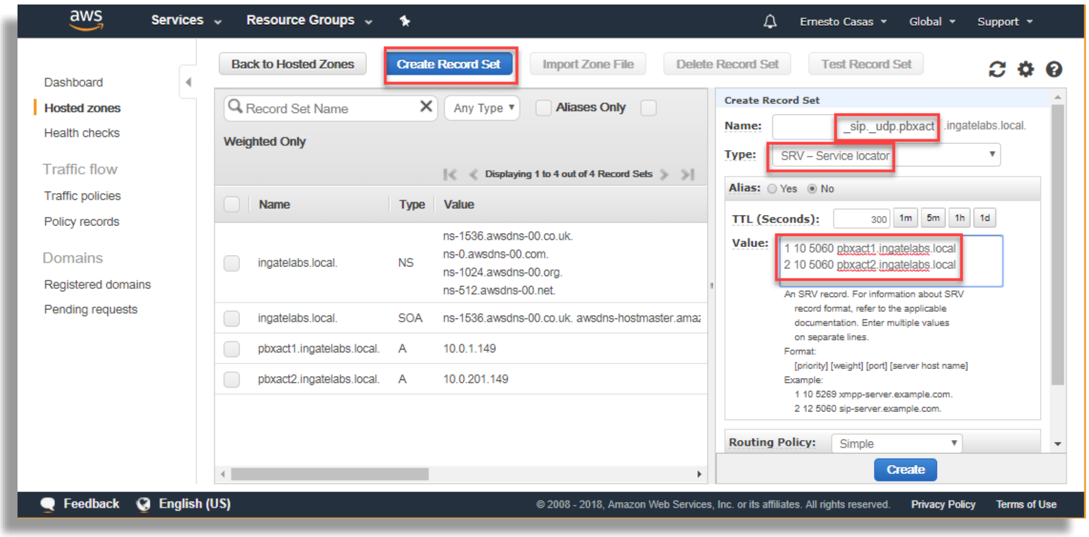
Value: 10.0.201.149

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

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



Name	Type	Value
ingatelabs.local.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
ingatelabs.local.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.ama:
pbxact1.ingatelabs.local.	A	10.0.1.149
pbxact2.ingatelabs.local.	A	10.0.201.149

Create Record Set

Name: _sip._udp.pbxact .ingatelabs.local.

Type: SRV – Service locator

Alias: ○ Yes ● No

TTL (Seconds): 300

Value:
1 10 5060 pbxact1.ingatelabs.local
2 10 5060 pbxact2.ingatelabs.local

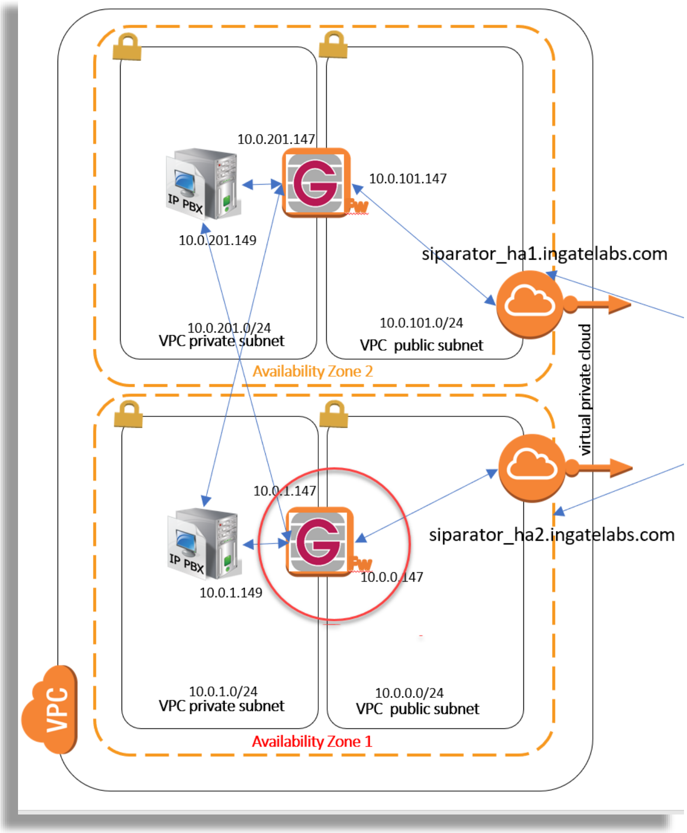
An SRV record. For information about SRV record format, refer to the applicable documentation. Enter multiple values on separate lines.
Format:
[priority] [weight] [port] [server host name]
Example:
1 10 5269 xmpp-server.example.com.
2 12 5060 sip-server.example.com.

Routing Policy: Simple

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.

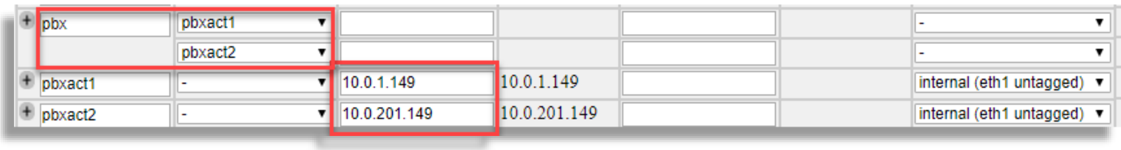


Let's first focus on configuring one of the SIParators

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.

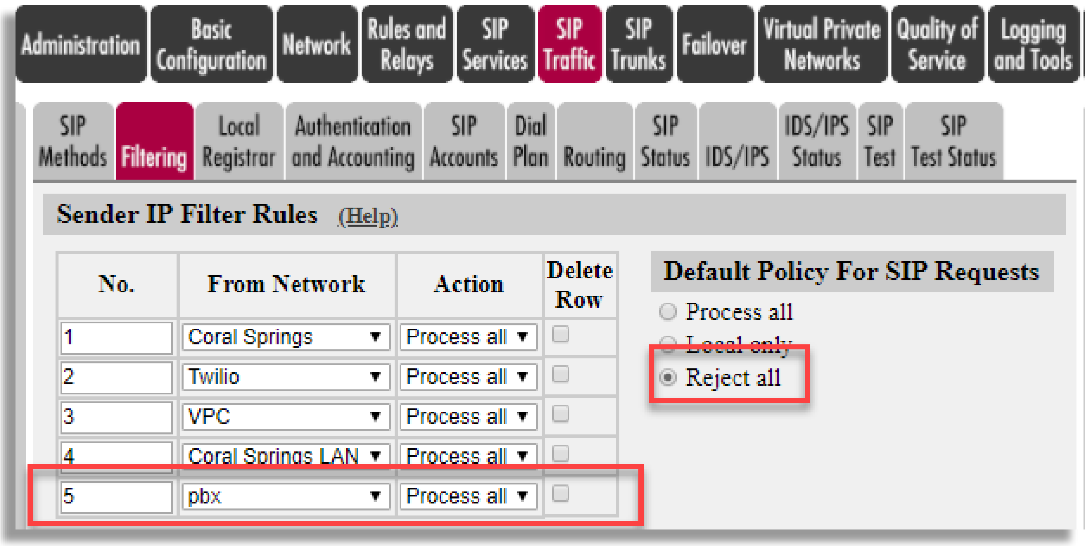
1) As shown in the diagram we will provide failover inbound calls to 2 IP-PBXes, and, we will allow traffic coming from any of them. So, we will need in the "Networks and Computers" Section under "Network":



pbx	pbxact1					-
	pbxact2					-
pbxact1	-	10.0.1.149	10.0.1.149			internal (eth1 untagged)
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



Sender IP Filter Rules (Help)

No.	From Network	Action	Delete Row
1	Coral Springs ▾	Process all ▾	□
2	Twilio ▾	Process all ▾	□
3	VPC ▾	Process all ▾	□
4	Coral Springs LAN ▾	Process all ▾	□
5	pbx ▾	Process all ▾	□

Default Policy For SIP Requests

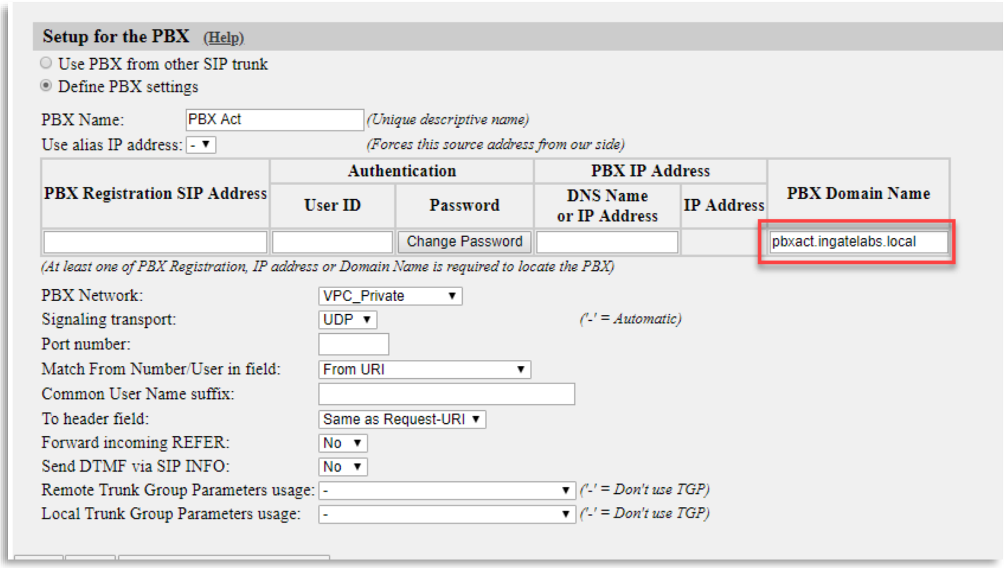
○ Process all
○ Local only
● Reject all

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



Setup for the PBX (Help)

○ Use PBX from other SIP trunk
● Define PBX settings

PBX Name: PBX Act *(Unique descriptive name)*
Use alias IP address: - ▾ *(Forces this source address from our side)*

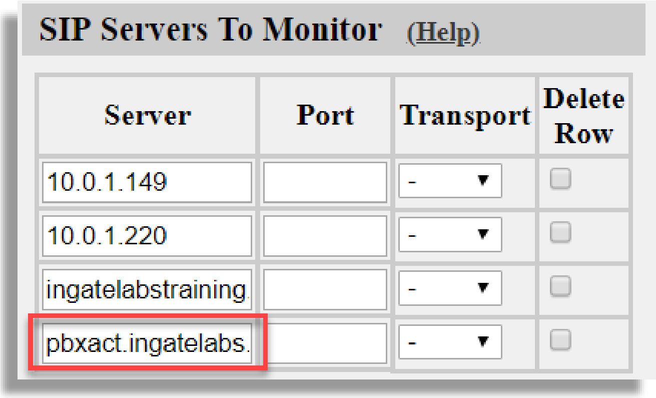
PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
	User ID	Password	DNS Name or IP Address	IP Address	
		Change Password			pbxact.ingatelabs.local

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

PBX Network: VPC_Private ▾
Signaling transport: UDP ▾ *('-' = Automatic)*
Port number:
Match From Number/User in field: From URI ▾
Common User Name suffix:
To header field: Same as Request-URI ▾
Forward incoming REFER: No ▾
Send DTMF via SIP INFO: No ▾
Remote Trunk Group Parameters usage: - ▾ *('-' = Don't use TGP)*
Local Trunk Group Parameters usage: - ▾ *('-' = 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

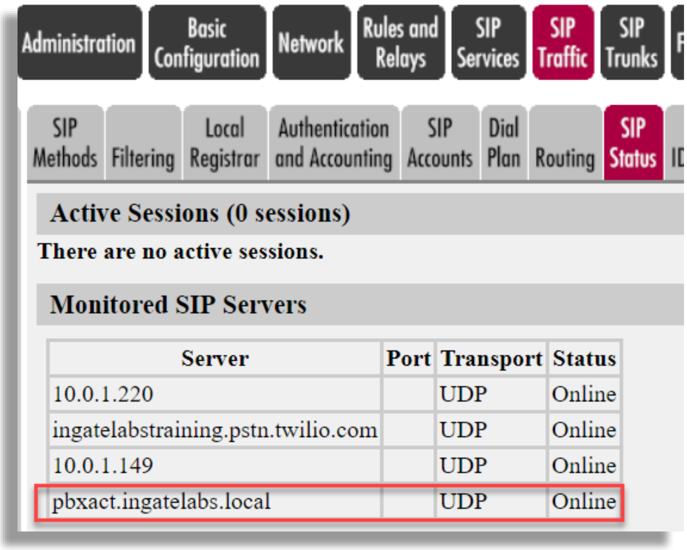
We will add also monitoring to the PBX Domain (pbxact.ingatelabs.local) in the SIP Services Section, Basic Configuration:



SIP Servers To Monitor (Help)

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"



Active Sessions (0 sessions)

There are no active sessions.

Monitored SIP Servers

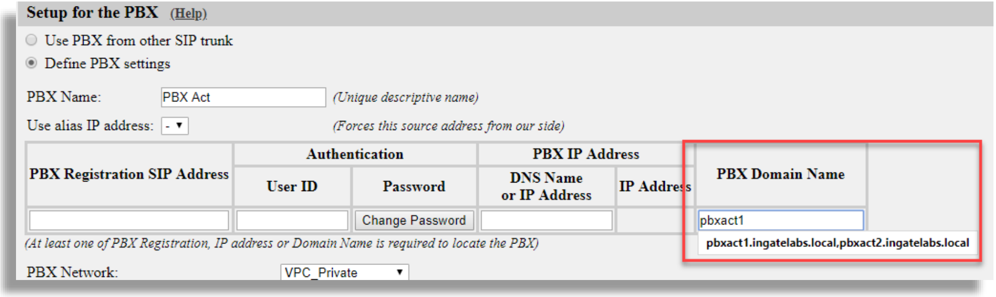
Server	Port	Transport	Status
10.0.1.220		UDP	Online
ingatelabstraining.pstn.twilio.com		UDP	Online
10.0.1.149		UDP	Online
pbxact.ingatelabs.local		UDP	Online

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 comma-separated 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)

○ Use PBX from other SIP trunk
● Define PBX settings

PBX Name: PBX Act *(Unique descriptive name)*

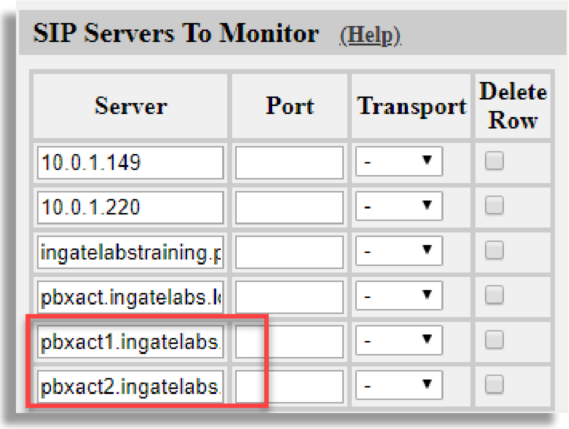
Use alias IP address: - *(Forces this source address from our side)*

PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
	User ID	Password	DNS Name or IP Address	IP Address	
		Change Password			pbxact1 pbxact1.ingatelabs.local,pbxact2.ingatelabs.local

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

PBX Network: VPC_Private

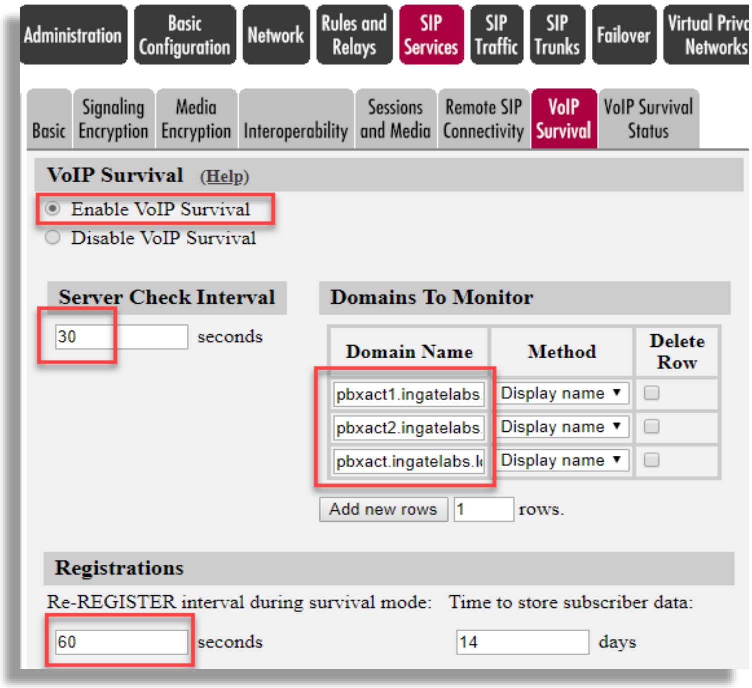
Adding the two domains to SIP Monitor:



SIP Servers To Monitor (Help)

Server	Port	Transport	Delete Row
10.0.1.149		-	□
10.0.1.220		-	□
ingatelabstraining.p		-	□
pbxact.ingatelabs.l		-	□
pbxact1.ingatelabs.		-	□
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.



VoIP Survival (Help)

● Enable VoIP Survival
○ Disable VoIP Survival

Server Check Interval

30 seconds

Domains To Monitor

Domain Name	Method	Delete Row
pbxact1.ingatelabs	Display name	□
pbxact2.ingatelabs	Display name	□
pbxact.ingatelabs.l	Display name	□

Add new rows 1 rows.

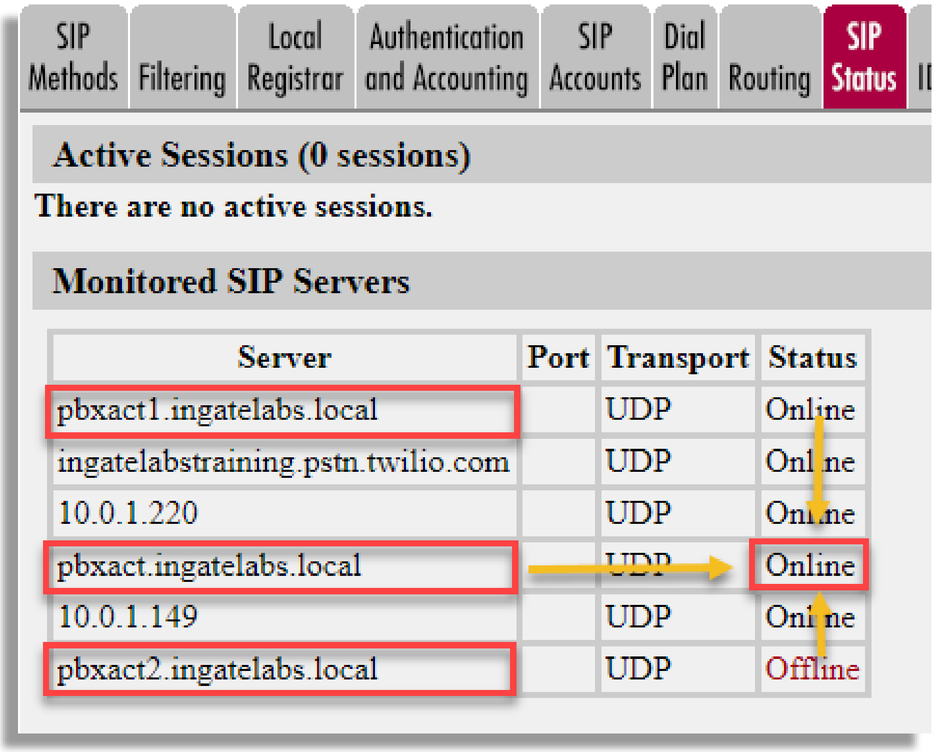
Registrations

Re-REGISTER interval during survival mode: 60 seconds

Time to store subscriber data: 14 days

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.



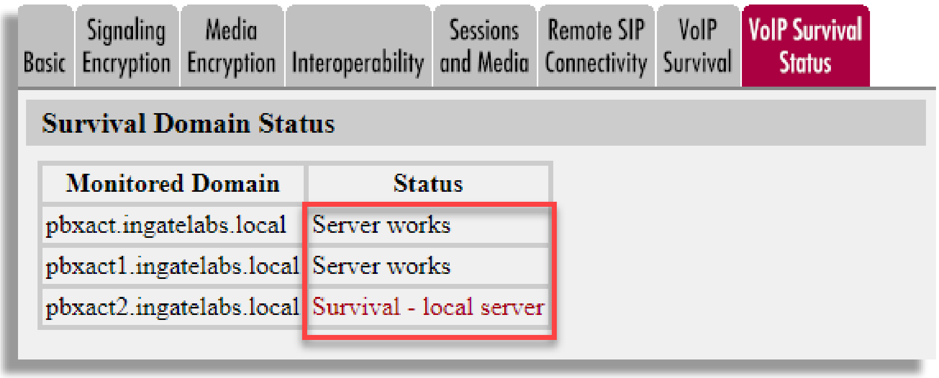
Active Sessions (0 sessions)

There are no active sessions.

Monitored SIP Servers

Server	Port	Transport	Status
pbxact1.ingatelabs.local		UDP	Online
ingatelabstraining.pstn.twilio.com		UDP	Online
10.0.1.220		UDP	Online
pbxact.ingatelabs.local		UDP	Online
10.0.1.149		UDP	Online
pbxact2.ingatelabs.local		UDP	Offline

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



Survival Domain Status

Monitored Domain	Status
pbxact.ingatelabs.local	Server works
pbxact1.ingatelabs.local	Server works
pbxact2.ingatelabs.local	Survival - local server

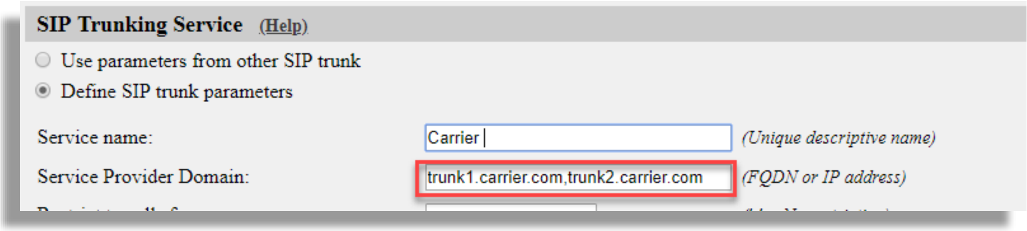
5.3.4 SIP Trunks Failover.

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)

○ Use parameters from other SIP trunk

● Define SIP trunk parameters

Service name: Carrier (Unique descriptive name)

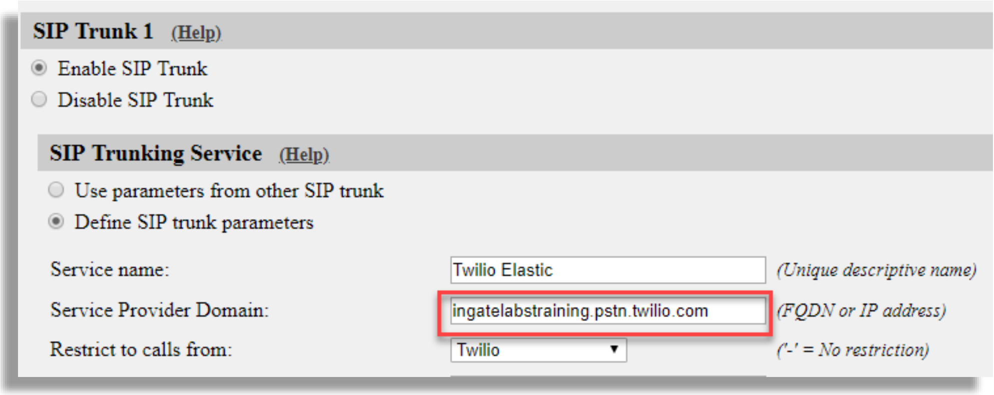
Service Provider Domain: trunk1.carrier.com,trunk2.carrier.com (FQDN or IP address)

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)

● Enable SIP Trunk
○ Disable SIP Trunk

SIP Trunking Service (Help)

○ 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)

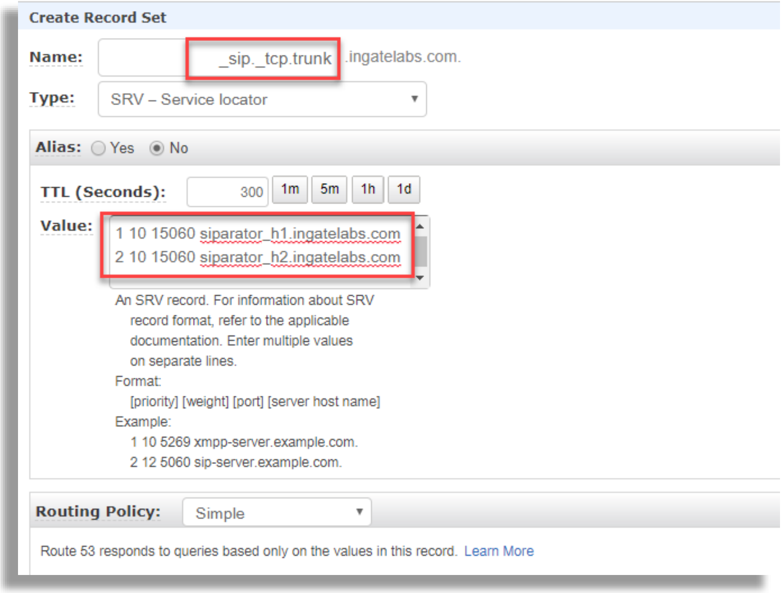
Notice the domain used is an FQDN resolved using SRV records, where the carrier Failover strategy will be implemented.

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



Create Record Set

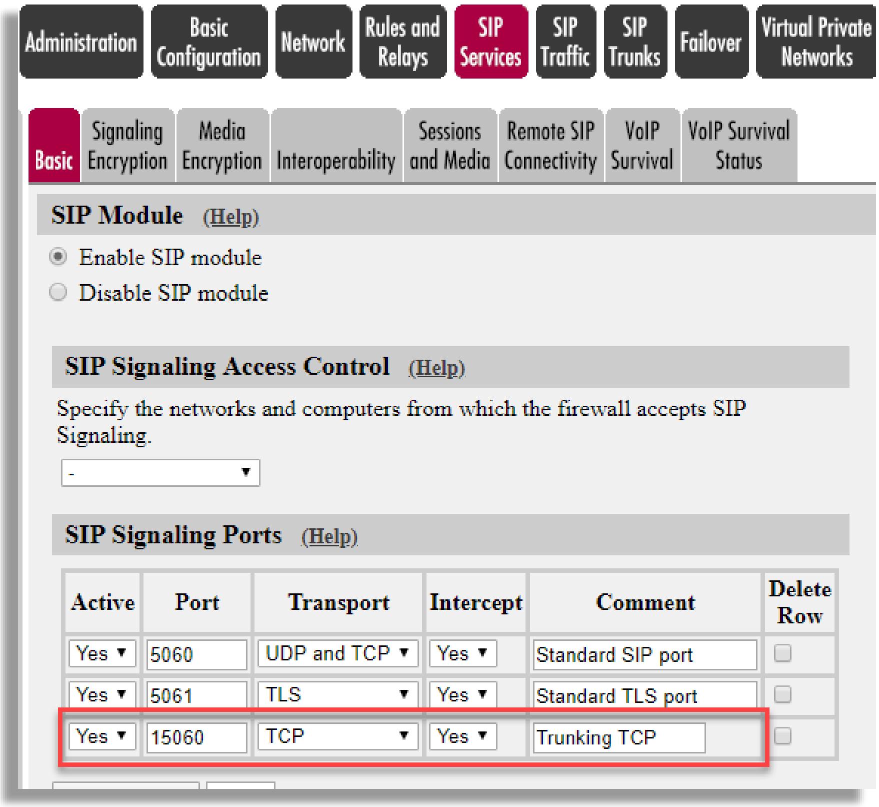
Name: _sip._tcp.trunk .ingatelabs.com.
Type: SRV – Service locator
Alias: ○ Yes ● No
TTL (Seconds): 300 1m 5m 1h 1d
Value:
```
1 10 15060 siparator_h1.ingatelabs.com
2 10 15060 siparator_h2.ingatelabs.com
```

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

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



SIP Module (Help)

● Enable SIP module

○ Disable SIP module

SIP Signaling Access Control (Help)

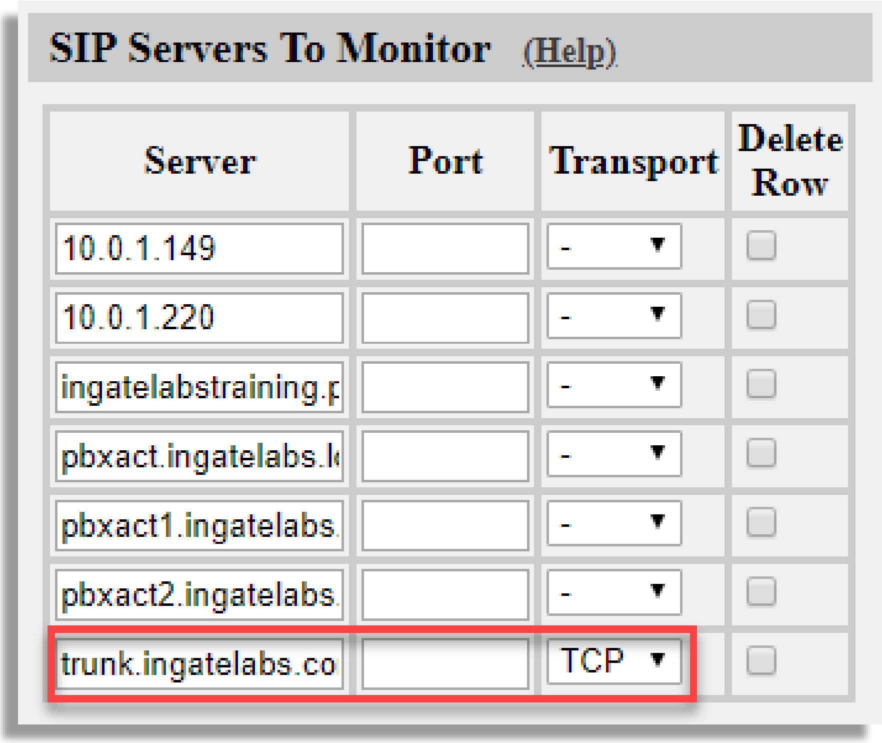
Specify the networks and computers from which the firewall accepts SIP Signaling.

- ▾

SIP Signaling Ports (Help)

Active	Port	Transport	Intercept	Comment	Delete Row
Yes ▾	5060	UDP and TCP ▾	Yes ▾	Standard SIP port	□
Yes ▾	5061	TLS ▾	Yes ▾	Standard TLS port	□
Yes ▾	15060	TCP ▾	Yes ▾	Trunking TCP	□

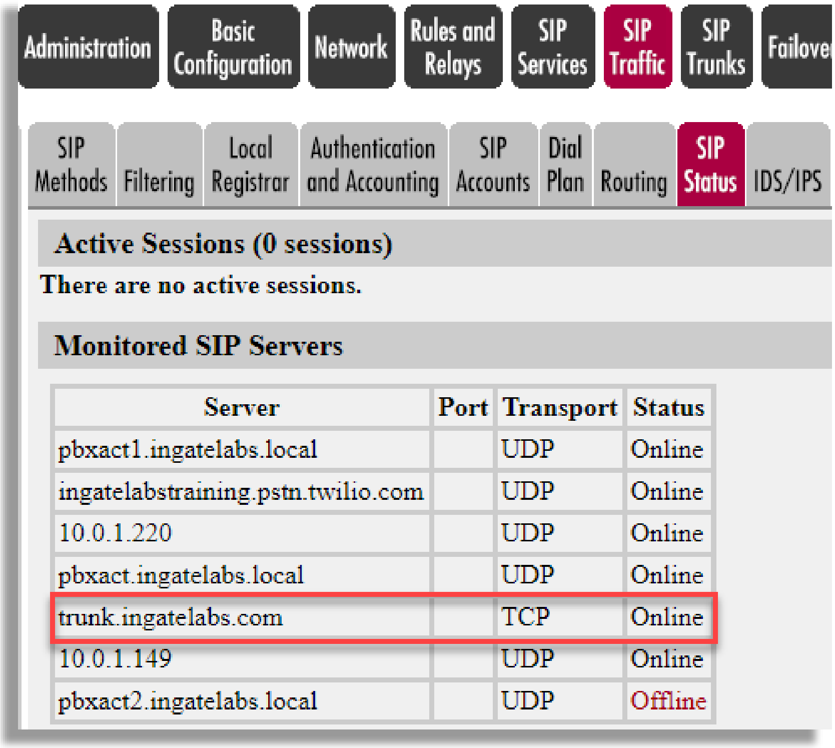
3) Add SIP Monitor for trunk.ingatelabs.com



SIP Servers To Monitor (Help)

Server	Port	Transport	Delete Row
10.0.1.149		- ▾	□
10.0.1.220		- ▾	□
ingatelabstraining.p		- ▾	□
pbxact.ingatelabs.l		- ▾	□
pbxact1.ingatelabs.		- ▾	□
pbxact2.ingatelabs.		- ▾	□
trunk.ingatelabs.co		TCP ▾	□

SIP Monitor will show the status for the Trunk Domain



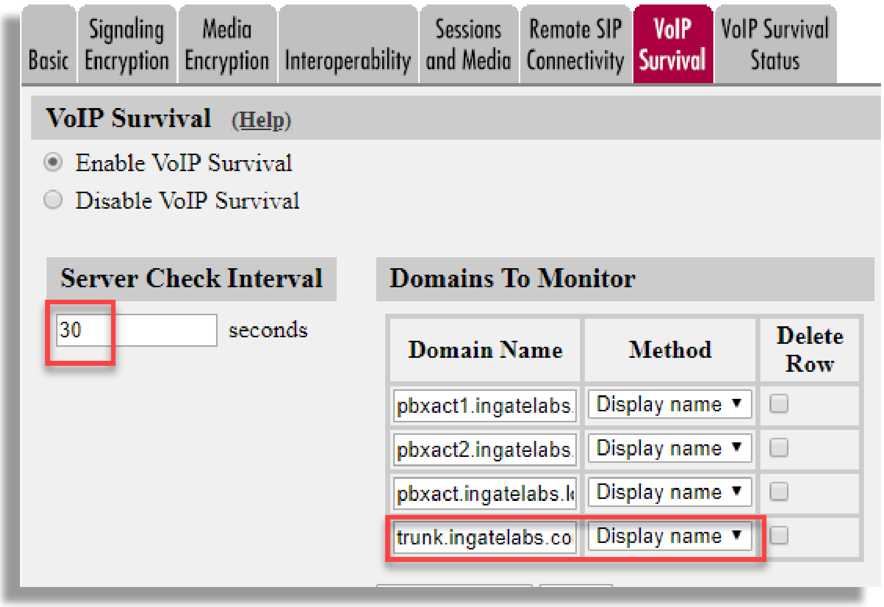
Active Sessions (0 sessions)

There are no active sessions.

Monitored SIP Servers

Server	Port	Transport	Status
pbxact1.ingatelabs.local		UDP	Online
ingatelabstraining.pstn.twilio.com		UDP	Online
10.0.1.220		UDP	Online
pbxact.ingatelabs.local		UDP	Online
trunk.ingatelabs.com		TCP	Online
10.0.1.149		UDP	Online
pbxact2.ingatelabs.local		UDP	Offline

4) Add VoIP Survival for trunk.ingatelabs.com



VoIP Survival (Help)

● Enable VoIP Survival

○ Disable VoIP Survival

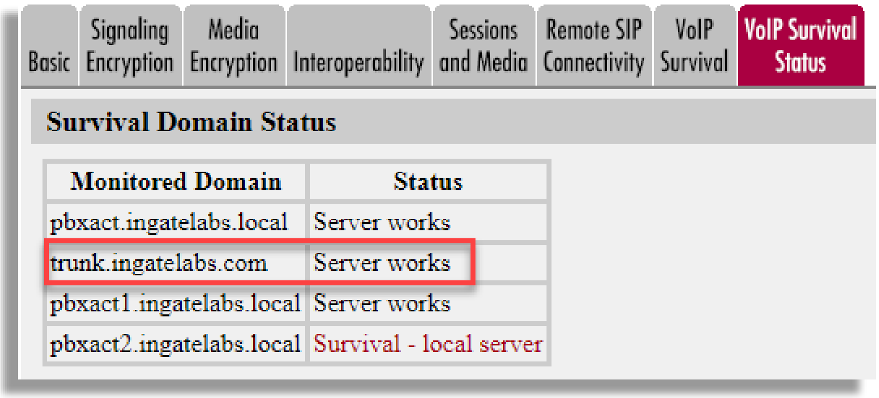
Server Check Interval

30 seconds

Domains To Monitor

Domain Name	Method	Delete Row
pbxact1.ingatelabs.	Display name ▼	□
pbxact2.ingatelabs.	Display name ▼	□
pbxact.ingatelabs.l	Display name ▼	□
trunk.ingatelabs.co	Display name ▼	□

VoIP Survival Status will show:



Survival Domain Status

Monitored Domain	Status
pbxact.ingatelabs.local	Server works
trunk.ingatelabs.com	Server works
pbxact1.ingatelabs.local	Server works
pbxact2.ingatelabs.local	Survival - local server

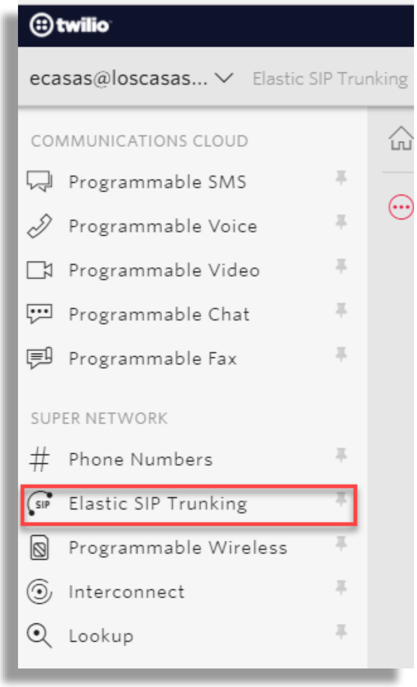
5.3.8 Twilio Redundancy Options

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

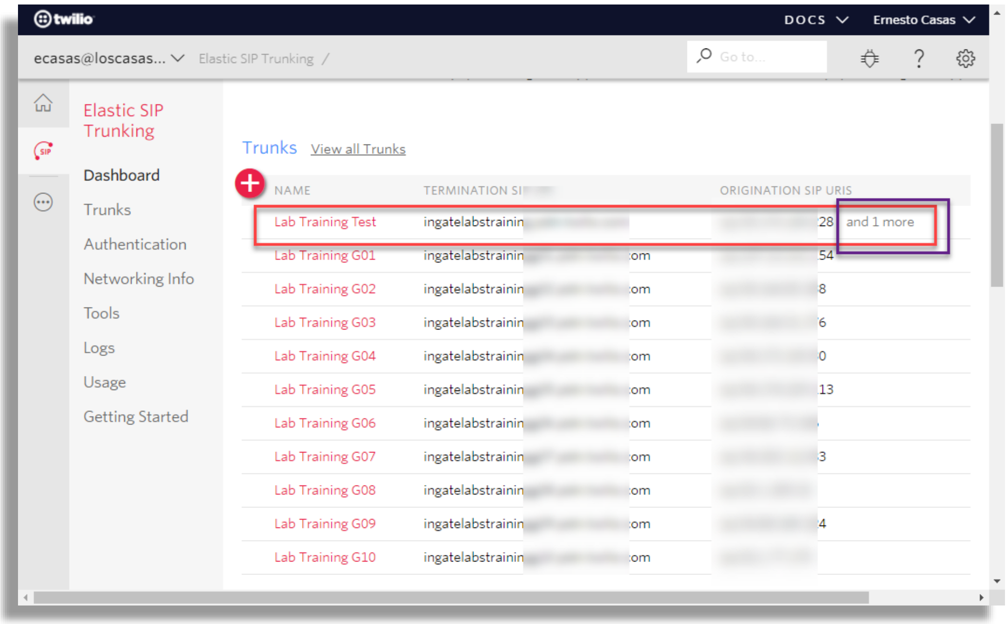
When designing a Highly Available solution, it is very important to review not only features and capabilities provided by your own infrastructure but also related functionalities on the Service Provider side.

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 → Elastic SIP Trunking

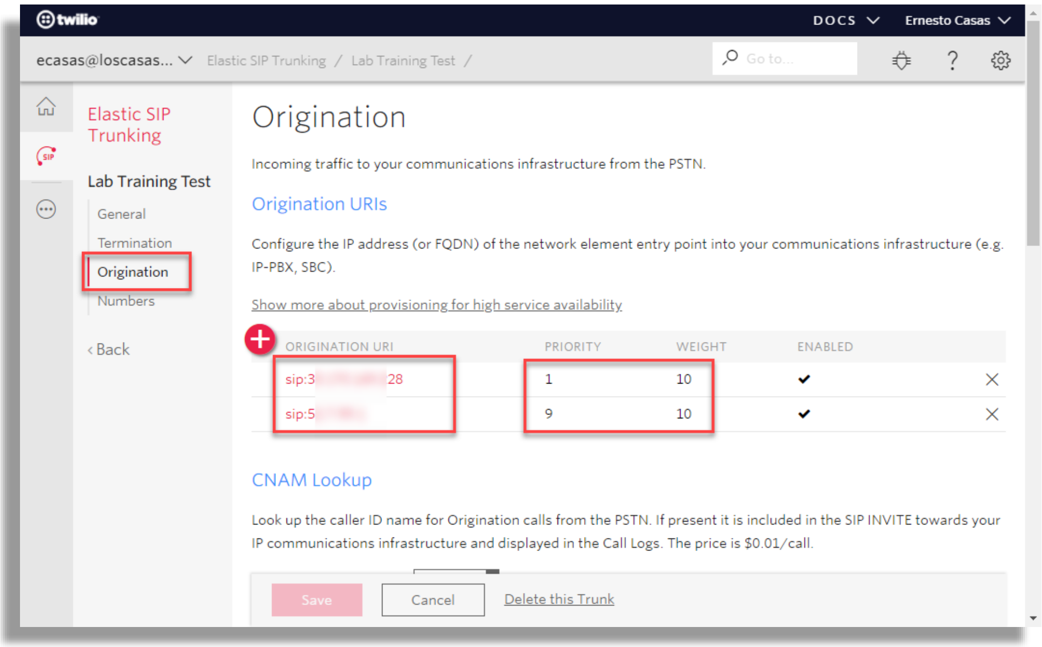


For this document, we set up the Lab Training Test SIP Trunk to be configured in such a way that calls can be routed to any of the 2 SBCs using a failover strategy.



NAME	TERMINATION SI[redacted]	ORIGINATION SIP URIS
Lab Training Test	ingatelabstrainin[redacted]	[redacted]28 and 1 more
Lab Training G01	ingatelabstrainin[redacted]om	[redacted]54
Lab Training G02	ingatelabstrainin[redacted]om	[redacted]8
Lab Training G03	ingatelabstrainin[redacted]om	[redacted]6
Lab Training G04	ingatelabstrainin[redacted]om	[redacted]0
Lab Training G05	ingatelabstrainin[redacted]om	[redacted]13
Lab Training G06	ingatelabstrainin[redacted]om	[redacted]
Lab Training G07	ingatelabstrainin[redacted]om	[redacted]3
Lab Training G08	ingatelabstrainin[redacted]om	[redacted]
Lab Training G09	ingatelabstrainin[redacted]om	[redacted]4
Lab Training G10	ingatelabstrainin[redacted]om	[redacted]

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.



Origination

Incoming traffic to your communications infrastructure from the PSTN.

Origination URIs

Configure the IP address (or FQDN) of the network element entry point into your communications infrastructure (e.g. IP-PBX, SBC).

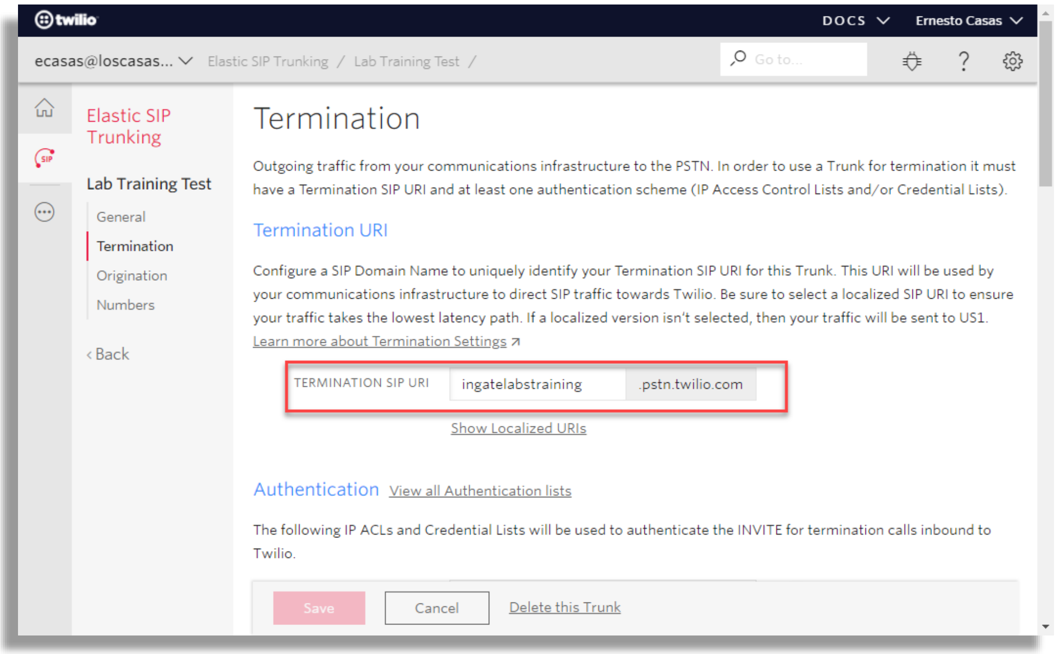
Show more about provisioning for high service availability

ORIGINATION URI	PRIORITY	WEIGHT	ENABLED	
sip:3[redacted]28	1	10	✓	×
sip:5[redacted]	9	10	✓	×

CNAM Lookup

Look up the caller ID name for Origination calls from the PSTN. If present it is included in the SIP INVITE towards your IP communications infrastructure and displayed in the Call Logs. The price is $0.01/call.

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



Termination

Outgoing traffic from your communications infrastructure to the PSTN. In order to use a Trunk for termination it must have a Termination SIP URI and at least one authentication scheme (IP Access Control Lists and/or Credential Lists).

Termination URI

Configure a SIP Domain Name to uniquely identify your Termination SIP URI for this Trunk. This URI will be used by your communications infrastructure to direct SIP traffic towards Twilio. Be sure to select a localized SIP URI to ensure your traffic takes the lowest latency path. If a localized version isn't selected, then your traffic will be sent to US1.
Learn more about Termination Settings ↗

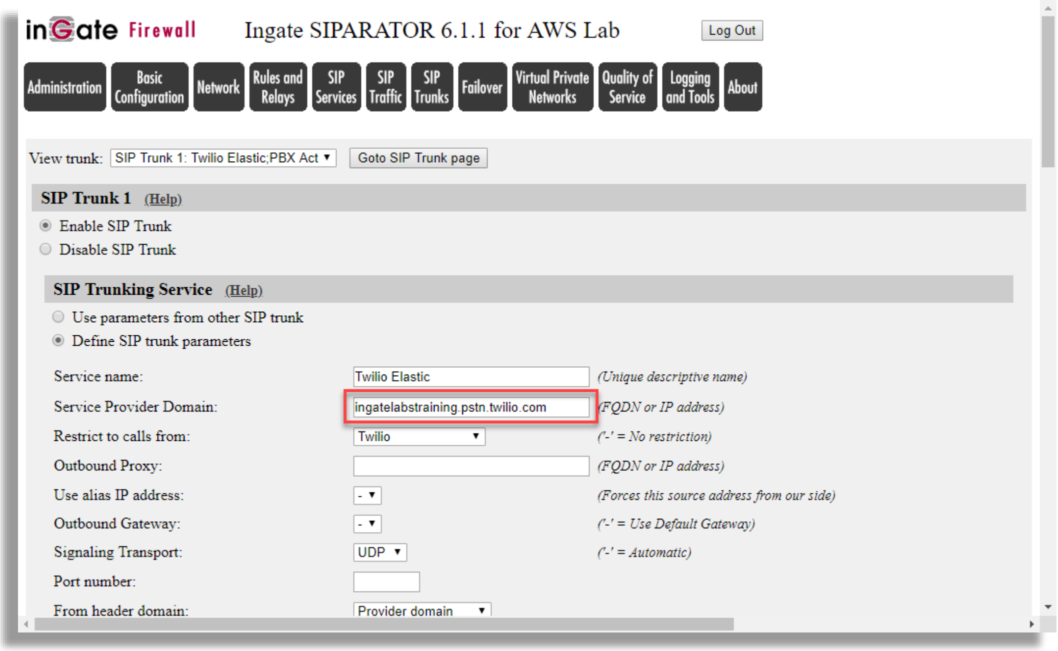
TERMINATION SIP URI: ingatelabstraining .pstn.twilio.com

Show Localized URIs

Authentication View all Authentication lists

The following IP ACLs and Credential Lists will be used to authenticate the INVITE for termination calls inbound to Twilio.

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



Ingate SIPARATOR 6.1.1 for AWS Lab

View trunk: SIP Trunk 1: Twilio Elastic;PBX Act

SIP Trunk 1 (Help)

● Enable SIP Trunk
○ Disable SIP Trunk

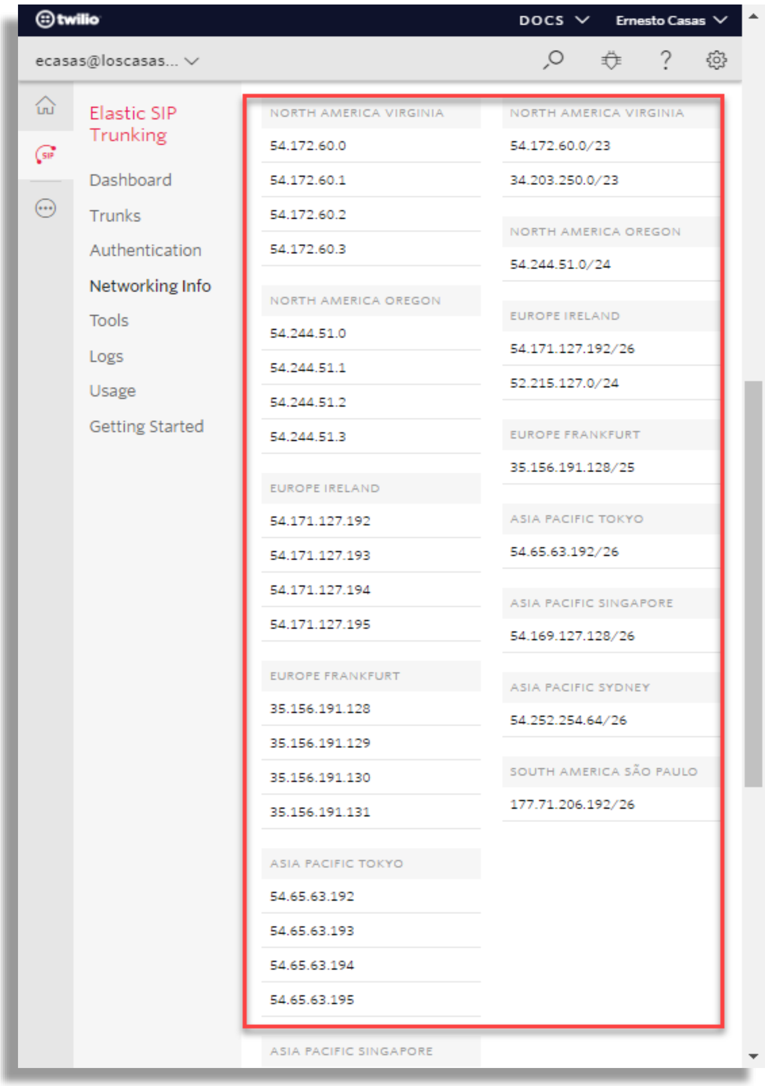
SIP Trunking Service (Help)

○ 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:	-	('-' = Use Default Gateway)
Signaling Transport:	UDP	('-' = Automatic)
Port number:		
From header domain:	Provider domain	

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 → Elastics Sip trunks → 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



NORTH AMERICA VIRGINIA
54.172.60.0
54.172.60.1
54.172.60.2
54.172.60.3

NORTH AMERICA OREGON
54.244.51.0
54.244.51.1
54.244.51.2
54.244.51.3

EUROPE IRELAND
54.171.127.192
54.171.127.193
54.171.127.194
54.171.127.195

EUROPE FRANKFURT
35.156.191.128
35.156.191.129
35.156.191.130
35.156.191.131

ASIA PACIFIC TOKYO
54.65.63.192
54.65.63.193
54.65.63.194
54.65.63.195

ASIA PACIFIC SINGAPORE

NORTH AMERICA VIRGINIA
54.172.60.0/23
34.203.250.0/23

NORTH AMERICA OREGON
54.244.51.0/24

EUROPE IRELAND
54.171.127.192/26
52.215.127.0/24

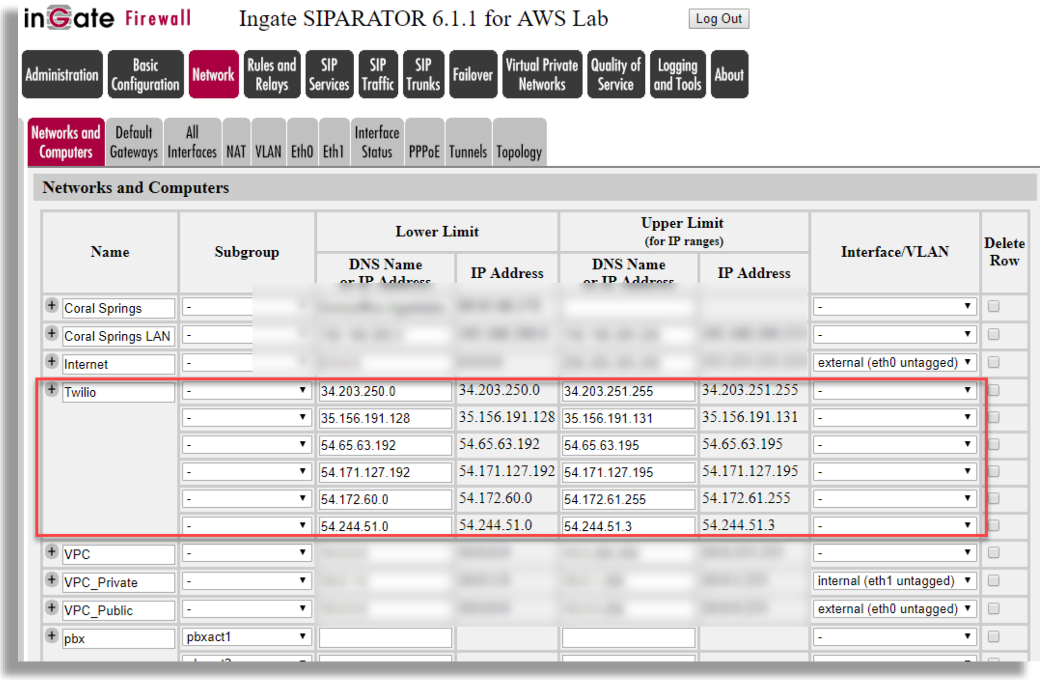
EUROPE FRANKFURT
35.156.191.128/25

ASIA PACIFIC TOKYO
54.65.63.192/26

ASIA PACIFIC SINGAPORE
54.169.127.128/26

ASIA PACIFIC SYDNEY
54.252.254.64/26

SOUTH AMERICA SÃO PAULO
177.71.206.192/26

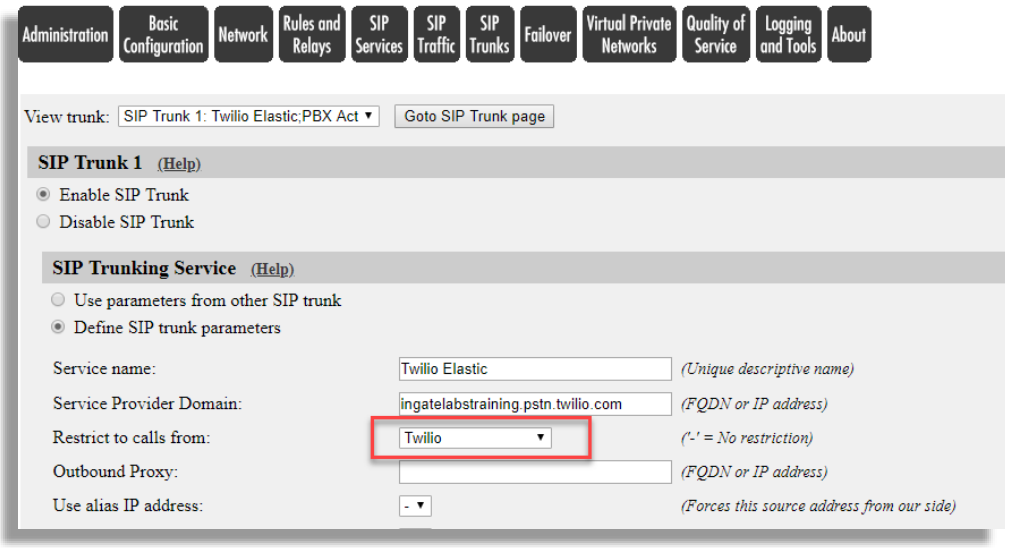


Ingate SIPARATOR 6.1.1 for AWS Lab

Networks and Computers

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
Coral Springs	-	[redacted]	[redacted]			-	□
Coral Springs LAN	-	[redacted]	[redacted]	[redacted]	[redacted]	-	□
Internet	-	[redacted]	[redacted]	[redacted]	[redacted]	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	-	[redacted]	[redacted]	[redacted]	[redacted]	-	□
VPC_Private	-	[redacted]	[redacted]	[redacted]	[redacted]	internal (eth1 untagged)	□
VPC_Public	-	[redacted]	[redacted]	[redacted]	[redacted]	external (eth0 untagged)	□
pbx	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.



View trunk: SIP Trunk 1: Twilio Elastic;PBX Act

SIP Trunk 1 (Help)

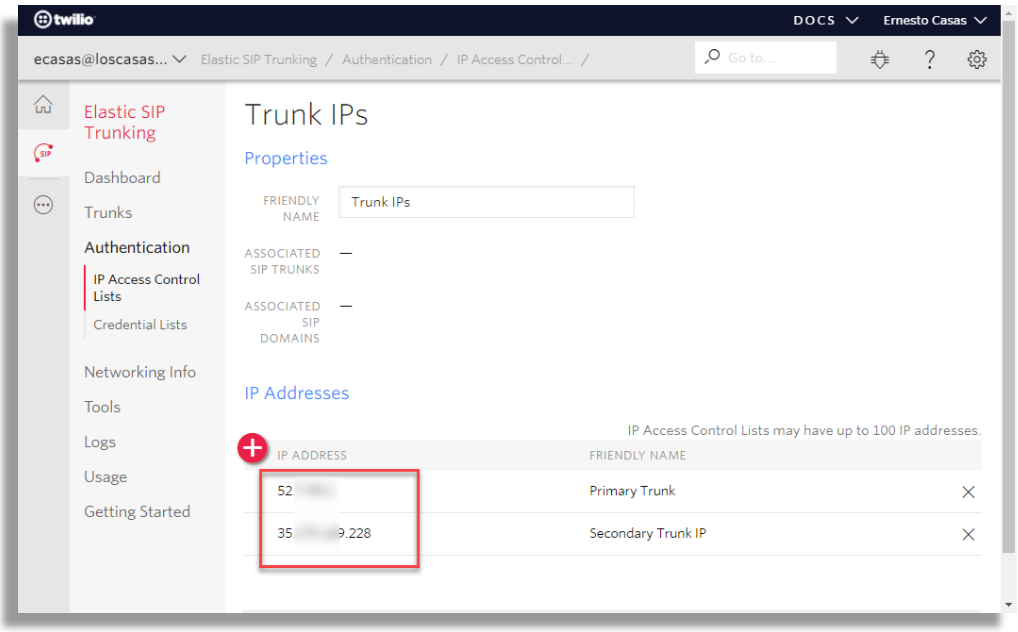
● Enable SIP Trunk
○ Disable SIP Trunk

SIP Trunking Service (Help)

○ 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.



Trunk IPs

Properties

FRIENDLY NAME: Trunk IPs

ASSOCIATED SIP TRUNKS: —

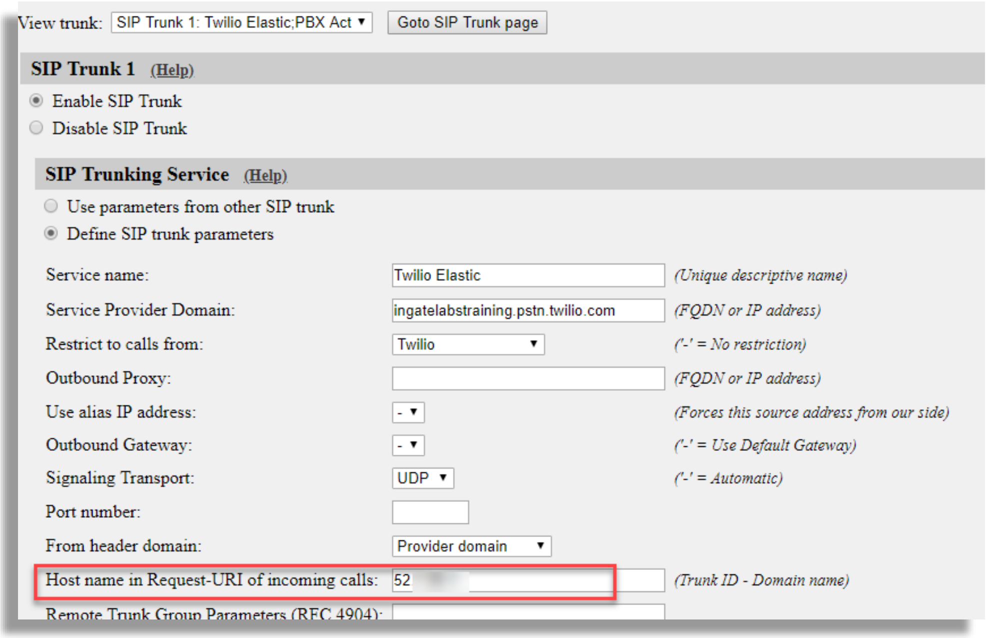
ASSOCIATED SIP DOMAINS: —

IP Addresses

IP Access Control Lists may have up to 100 IP addresses.

IP ADDRESS	FRIENDLY NAME
52[redacted]	Primary Trunk
35[redacted]9.228	Secondary Trunk IP

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:



View 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 trunk

● Define SIP trunk parameters

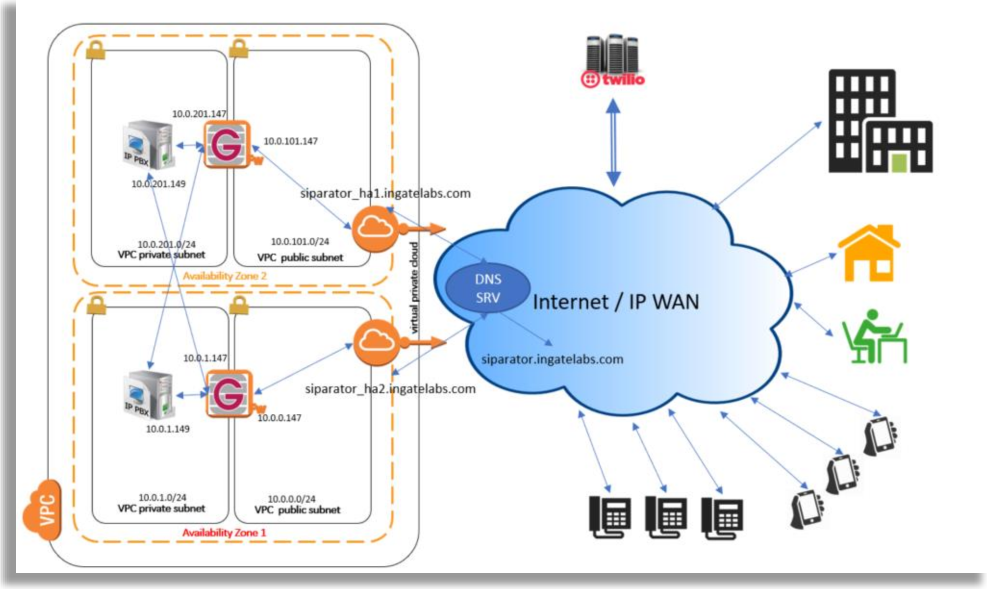
Service name:	Twilio Elastic	*(Unique descriptive name)*
Service Provider Domain:	ingatelabstraining.pstn.twilio.com	*(FQDN or IP address)*
Restrict to calls from:	Twilio ▾	*('-' = No restriction)*
Outbound Proxy:		*(FQDN or IP address)*
Use alias IP address:	- ▾	*(Forces this source address from our side)*
Outbound Gateway:	- ▾	*('-' = Use Default Gateway)*
Signaling Transport:	UDP ▾	*('-' = Automatic)*
Port number:		
From header domain:	Provider domain ▾	
Host name in Request-URI of incoming calls:	52[redacted]	*(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

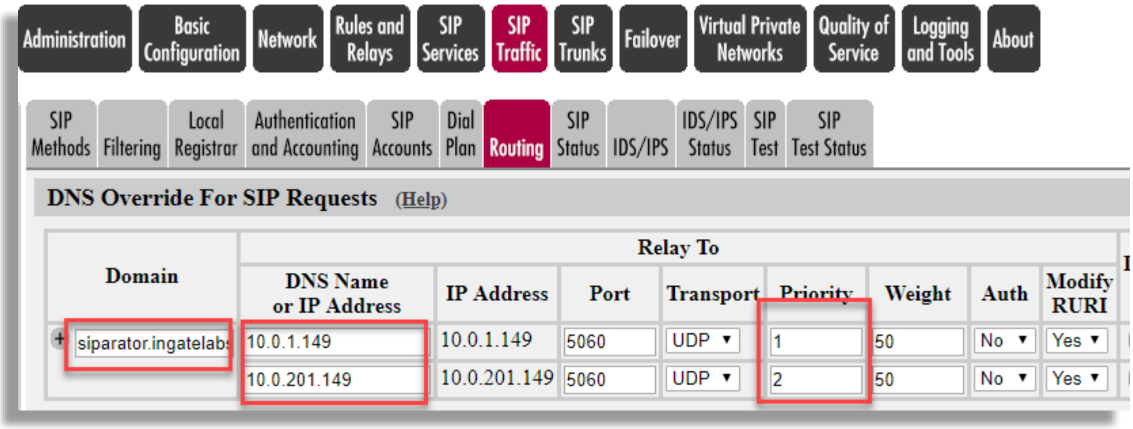


We can create a new SRV record for a different domain name and use the SRV we created in 5.1 as siparator.ingatelabs.com, which we know resolves using Failover or Load Balance Strategy to siparator_ha1.ingatelabs.com and siparator_ha2.ingatelabs.com.

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.

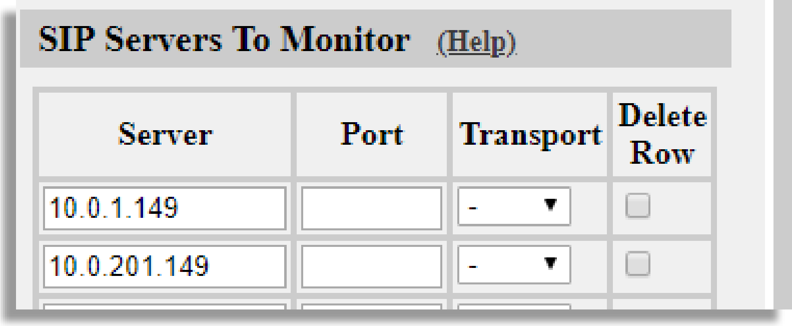
Here is how it looks when using the SIParator to manage PBX Failover strategy. Note we are assigning lower priority to 10.0.1.149, which means that this will be the primary PBX, and only when it's unavailable will the request be sent to the second PBX.



DNS Override For SIP Requests (Help)

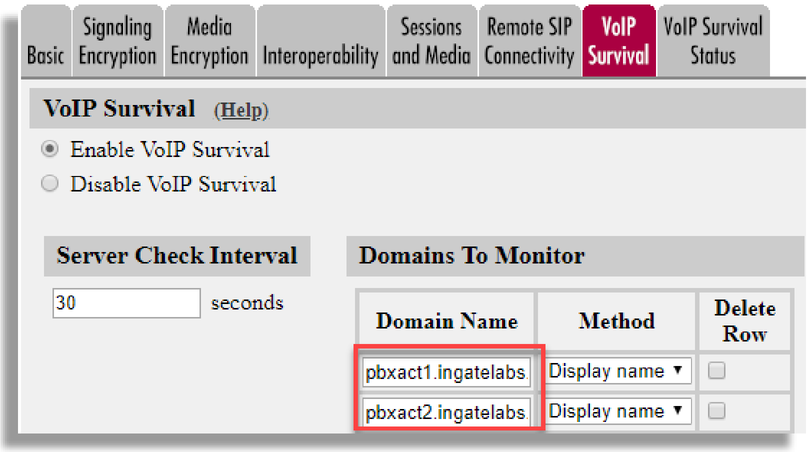
Domain	Relay To								I
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	
siparator.ingatelab	10.0.1.149	10.0.1.149	5060	UDP	1	50	No	Yes	
	10.0.201.149	10.0.201.149	5060	UDP	2	50	No	Yes	

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 Monitor (Help)

Server	Port	Transport	Delete Row
10.0.1.149		-	☐
10.0.201.149		-	☐



VoIP Survival (Help)

● Enable VoIP Survival
○ Disable VoIP Survival

Server Check Interval

30 seconds

Domains To Monitor

Domain Name	Method	Delete Row
pbxact1.ingatelabs	Display name ▾	□
pbxact2.ingatelabs	Display name ▾	□

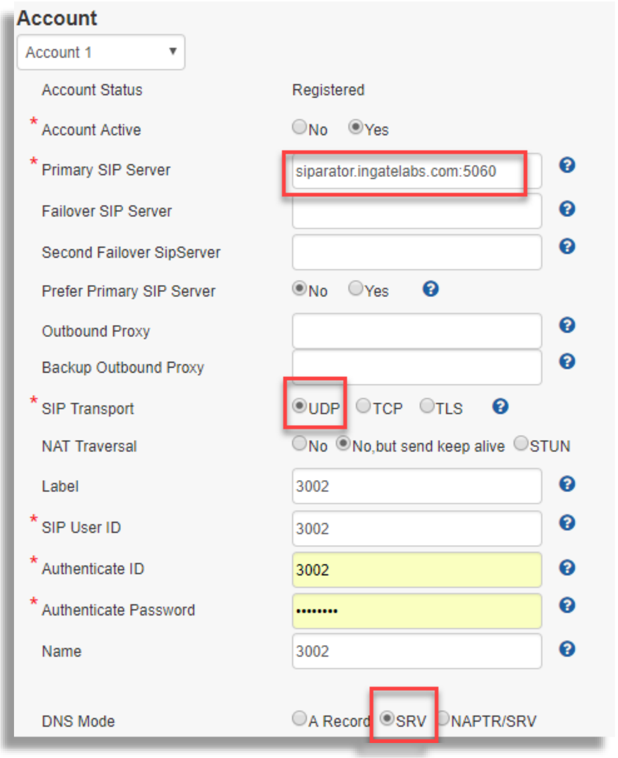
As we have also DNS A Records for a hosted private zone, we can use pbxact1.ingatelabs.local and pbxact2.ingatelabs.local as defined in section 5.2, either on SIP DNS Override, SIP Servers Monitor and VoIP Survival Tables

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:

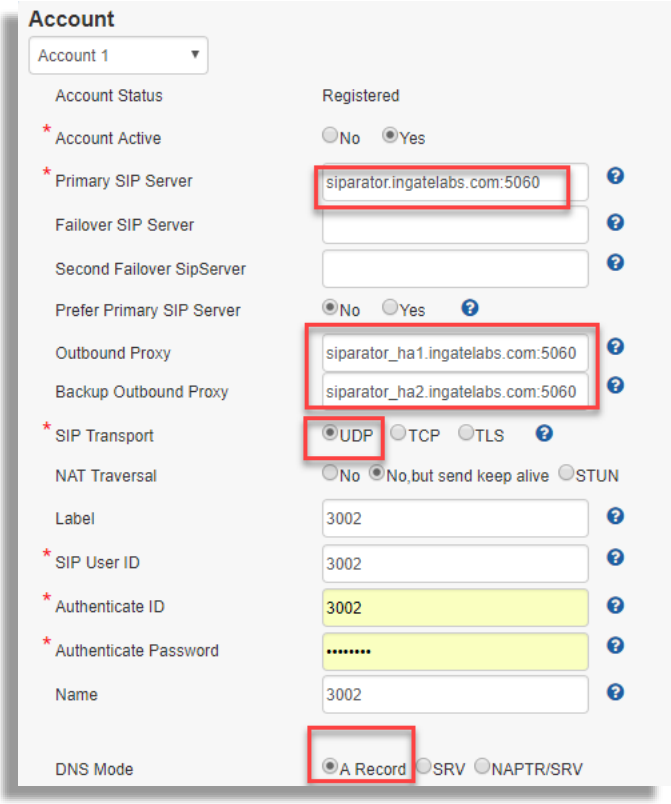


Account

Account 1 ▾

Account Status	Registered
* Account Active	○ No ● Yes
* Primary SIP Server	siparator.ingatelabs.com:5060
Failover SIP Server	
Second Failover SipServer	
Prefer Primary SIP Server	● No ○ Yes
Outbound Proxy	
Backup Outbound Proxy	
* SIP Transport	● UDP ○ TCP ○ TLS
NAT Traversal	○ No ● No,but send keep alive ○ STUN
Label	3002
* SIP User ID	3002
* Authenticate ID	3002
* Authenticate Password	••••••••
Name	3002
DNS Mode	○ A Record ● SRV ○ NAPTR/SRV

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

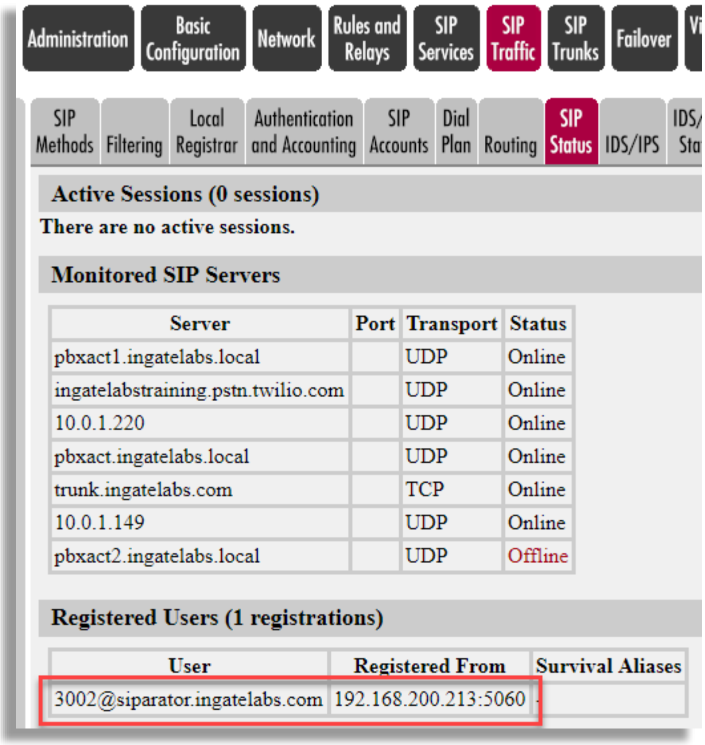


Account

Account 1 ▾

Account Status	Registered
* Account Active	○ No ● Yes
* Primary SIP Server	siparator.ingatelabs.com:5060
Failover SIP Server	
Second Failover SipServer	
Prefer Primary SIP Server	● No ○ Yes
Outbound Proxy	siparator_ha1.ingatelabs.com:5060
Backup Outbound Proxy	siparator_ha2.ingatelabs.com:5060
* SIP Transport	● UDP ○ TCP ○ TLS
NAT Traversal	○ No ● No,but send keep alive ○ STUN
Label	3002
* SIP User ID	3002
* Authenticate ID	3002
* Authenticate Password	••••••••
Name	3002
DNS Mode	● A Record ○ SRV ○ NAPTR/SRV

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



Active Sessions (0 sessions)

There are no active sessions.

Monitored SIP Servers

Server	Port	Transport	Status
pbxact1.ingatelabs.local		UDP	Online
ingatelabstraining.pstn.twilio.com		UDP	Online
10.0.1.220		UDP	Online
pbxact.ingatelabs.local		UDP	Online
trunk.ingatelabs.com		TCP	Online
10.0.1.149		UDP	Online
pbxact2.ingatelabs.local		UDP	Offline

Registered Users (1 registrations)

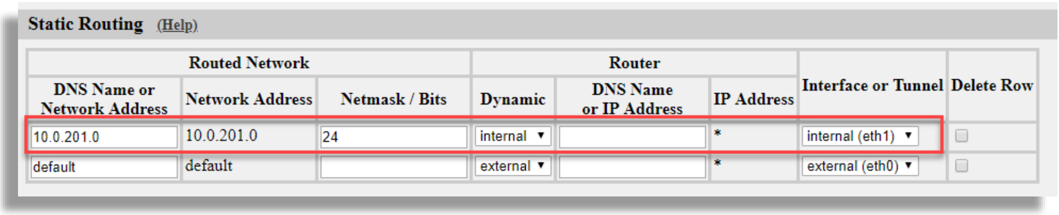
User	Registered From	Survival Aliases
3002@siparator.ingatelabs.com	192.168.200.213:5060	-

5.5 PBX cross connection with SIParators

One potential scenario when a SIParator only goes offline, or a PBX only goes off line 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 ←→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.



Static Routing (Help)

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	internal ▾		*	internal (eth1) ▾	□
default	default		external ▾		*	external (eth0) ▾	□

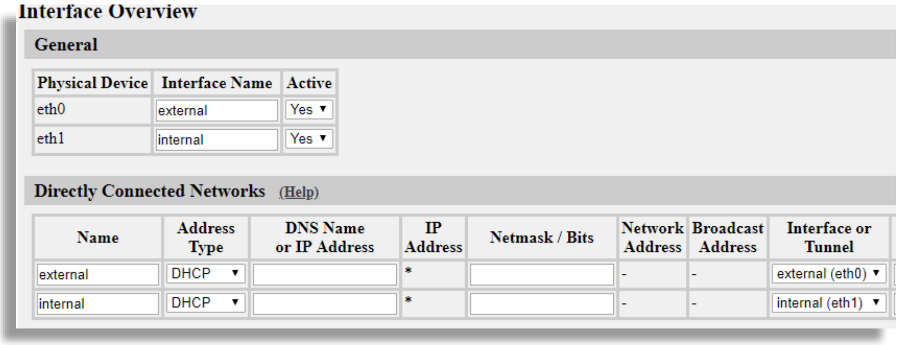
We are saying in order to reach 10.0.201.0 (Private subnet in the failover area), to use the dynamic gateway provided by DHCP on the Internal Interface and route using eth1.

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



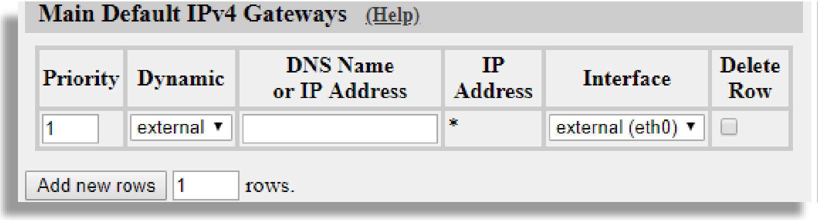
Interface Overview

General

Physical Device	Interface Name	Active
eth0	external	Yes ▾
eth1	internal	Yes ▾

Directly Connected Networks (Help)

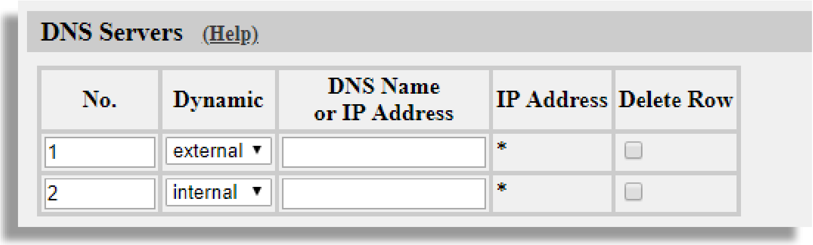
Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel
external	DHCP ▾		*		-	-	external (eth0) ▾
internal	DHCP ▾		*		-	-	internal (eth1) ▾



Main Default IPv4 Gateways (Help)

Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
1	external ▼		*	external (eth0) ▼	☐

Add new rows 1 rows.



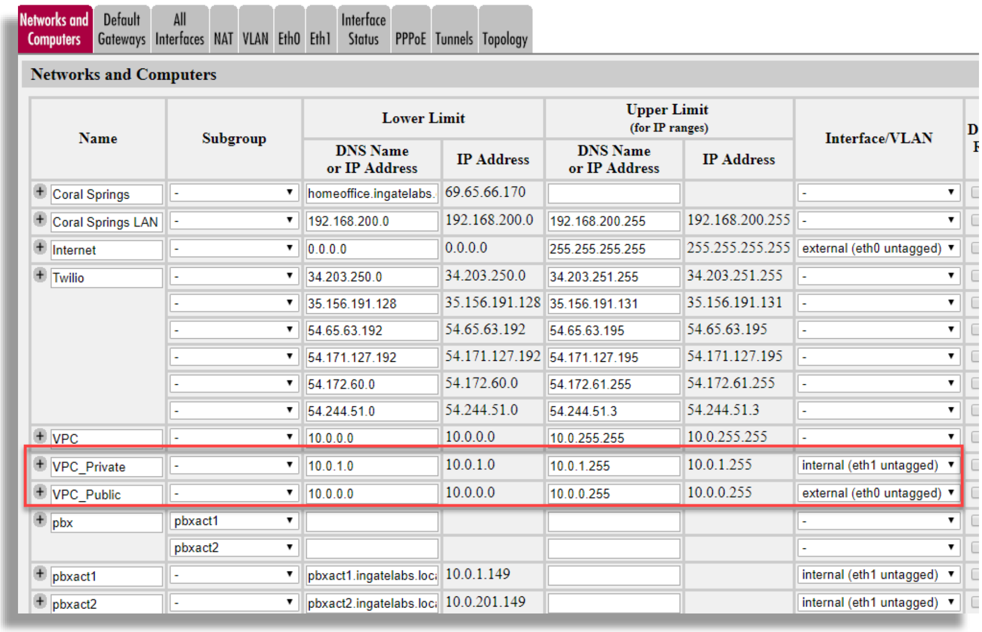
DNS Servers (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	external ▼		*	☐
2	internal ▼		*	☐

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 → 10.0.10.0/24

   b. 10.0.1.0/24 → 10.0.201.0/24

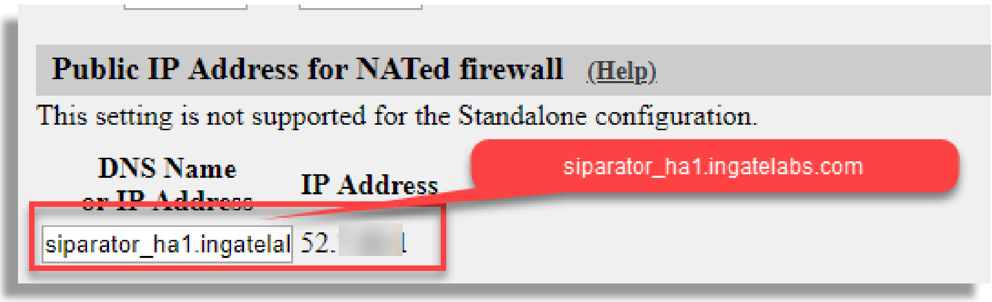


Networks and Computers

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	D
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
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	- ▼	☐
VPC_Private	- ▼	10.0.1.0	10.0.1.0	10.0.1.255	10.0.1.255	internal (eth1 untagged) ▼	☐
VPC_Public	- ▼	10.0.0.0	10.0.0.0	10.0.0.255	10.0.0.255	external (eth0 untagged) ▼	☐
pbx	pbxact1 ▼					- ▼	☐
	pbxact2 ▼					- ▼	☐
pbxact1	- ▼	pbxact1.ingatelabs.loc	10.0.1.149			internal (eth1 untagged) ▼	☐
pbxact2	- ▼	pbxact2.ingatelabs.loc	10.0.201.149			internal (eth1 untagged) ▼	☐

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



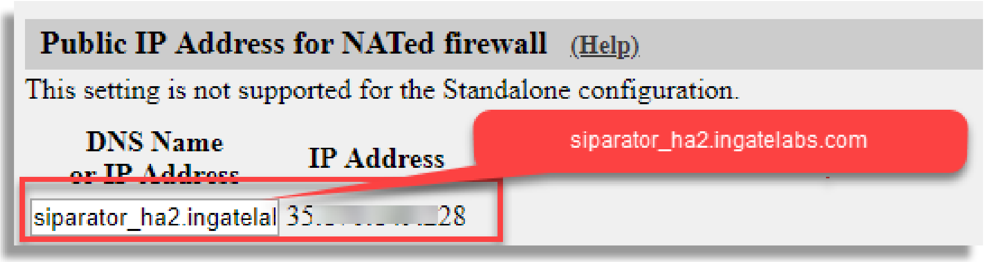
Public IP Address for NATed firewall (Help)

This setting is not supported for the Standalone configuration.

DNS Name or IP Address	IP Address
siparator_ha1.ingatelal	52.[redacted]1

siparator_ha1.ingatelabs.com

SIPARATOR 2



Public IP Address for NATed firewall (Help)

This setting is not supported for the Standalone configuration.

DNS Name or IP Address	IP Address
siparator_ha2.ingatelal	35.[redacted]28

siparator_ha2.ingatelabs.com

6.1 How to synchronize Configuration.

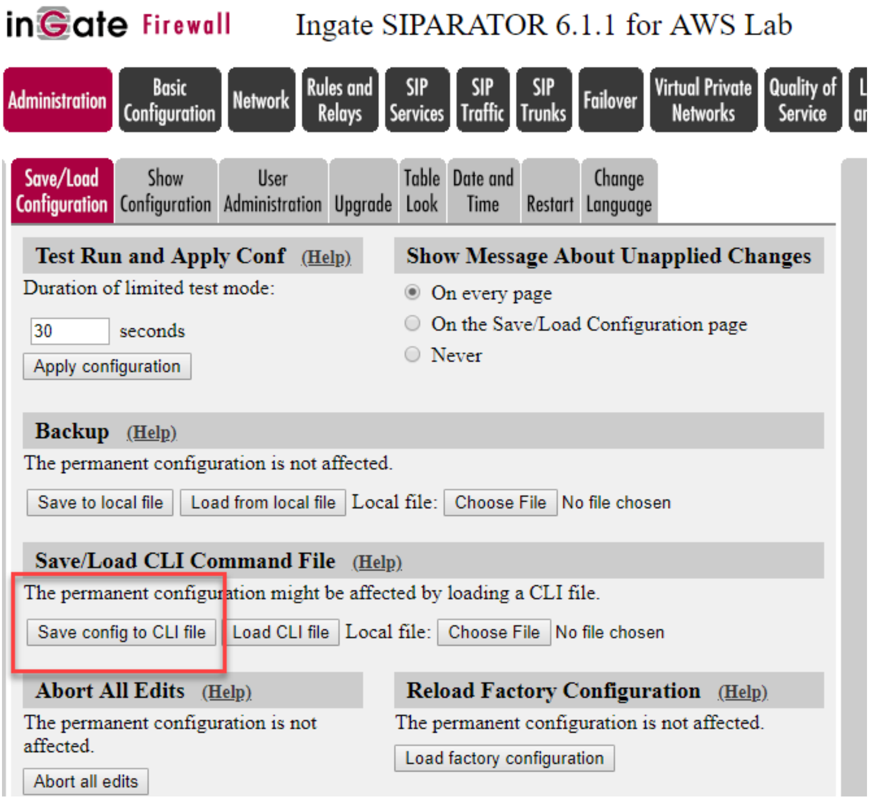
There are two ways we can create and apply the configuration needed and adjusted for the Failover SIParator. Both use the CLI saved file form the Main SIParator.

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



Test Run and Apply Conf (Help)

Duration of limited test mode:

30 seconds

Apply configuration

Show Message About Unapplied Changes

● On every page
○ On the Save/Load Configuration page
○ Never

Backup (Help)

The permanent configuration is not affected.

Save to local file | Load from local file | Local file: Choose File No file chosen

Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Save config to CLI file | Load CLI file | Local file: Choose File No file chosen

Abort All Edits (Help)

The permanent configuration is not affected.

Abort all edits

Reload Factory Configuration (Help)

The permanent configuration is not affected.

Load factory configuration

The file name will be like:

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

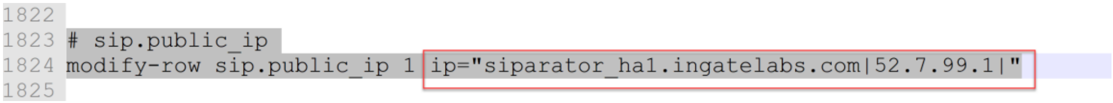
6.1.2 Manually modify CLI File:

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:

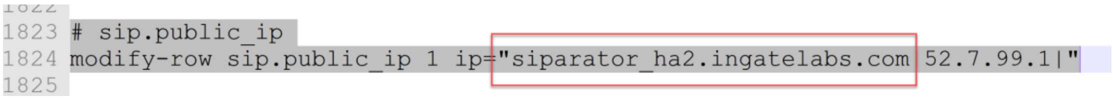
  Seach for **”# sip.public_ip”**

  You will find something like this:



```
# sip.public_ip
modify-row sip.public_ip 1 ip="siparator_ha1.ingatelabs.com|52.7.99.1|"
```

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:

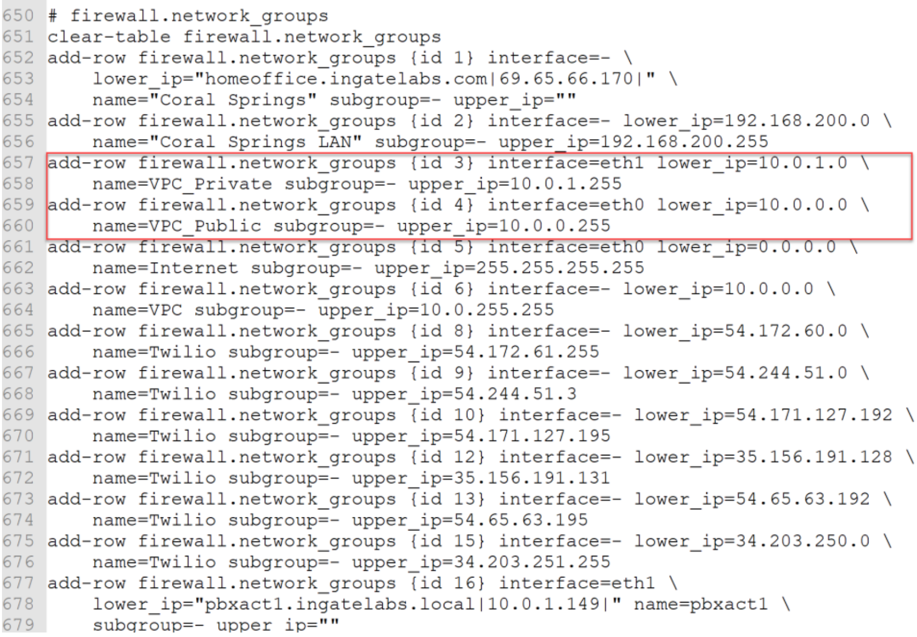


```
# sip.public_ip
modify-row sip.public_ip 1 ip="siparator_ha2.ingatelabs.com|52.7.99.1|"
```

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

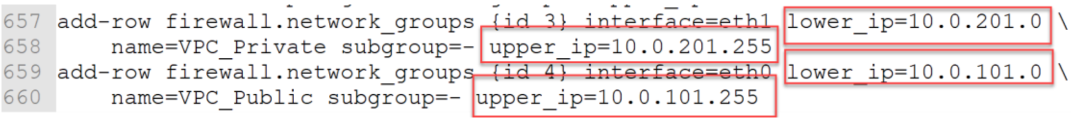
  Search for **"# firewall.network_groups"**

  You will find something like this:



```
# firewall.network_groups
clear-table firewall.network_groups
add-row firewall.network_groups {id 1} interface=- \
    lower_ip="homeoffice.ingatelabs.com|69.65.66.170|" \
    name="Coral Springs" subgroup=- upper_ip=""
add-row firewall.network_groups {id 2} interface=- lower_ip=192.168.200.0 \
    name="Coral Springs LAN" subgroup=- upper_ip=192.168.200.255
add-row firewall.network_groups {id 3} interface=eth1 lower_ip=10.0.1.0 \
    name=VPC_Private subgroup=- upper_ip=10.0.1.255
add-row firewall.network_groups {id 4} interface=eth0 lower_ip=10.0.0.0 \
    name=VPC_Public subgroup=- upper_ip=10.0.0.255
add-row firewall.network_groups {id 5} interface=eth0 lower_ip=0.0.0.0 \
    name=Internet subgroup=- upper_ip=255.255.255.255
add-row firewall.network_groups {id 6} interface=- lower_ip=10.0.0.0 \
    name=VPC subgroup=- upper_ip=10.0.255.255
add-row firewall.network_groups {id 8} interface=- lower_ip=54.172.60.0 \
    name=Twilio subgroup=- upper_ip=54.172.61.255
add-row firewall.network_groups {id 9} interface=- lower_ip=54.244.51.0 \
    name=Twilio subgroup=- upper_ip=54.244.51.3
add-row firewall.network_groups {id 10} interface=- lower_ip=54.171.127.192 \
    name=Twilio subgroup=- upper_ip=54.171.127.195
add-row firewall.network_groups {id 12} interface=- lower_ip=35.156.191.128 \
    name=Twilio subgroup=- upper_ip=35.156.191.131
add-row firewall.network_groups {id 13} interface=- lower_ip=54.65.63.192 \
    name=Twilio subgroup=- upper_ip=54.65.63.195
add-row firewall.network_groups {id 15} interface=- lower_ip=34.203.250.0 \
    name=Twilio subgroup=- upper_ip=34.203.251.255
add-row firewall.network_groups {id 16} interface=eth1 \
    lower_ip="pbxact1.ingatelabs.local|10.0.1.149|" name=pbxact1 \
    subgroup=- upper_ip=""
```

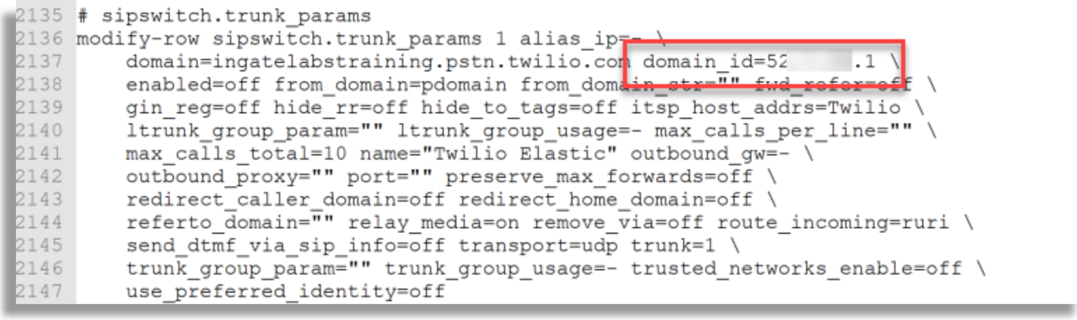
  Change the Upper and Lower IPs to match the new subnet in the second SIParator. It should then look like this:



```
add-row firewall.network_groups {id 3} interface=eth1 lower_ip=10.0.201.0 \
    name=VPC_Private subgroup=- upper_ip=10.0.201.255
add-row firewall.network_groups {id 4} interface=eth0 lower_ip=10.0.101.0 \
    name=VPC_Public subgroup=- upper_ip=10.0.101.255
```

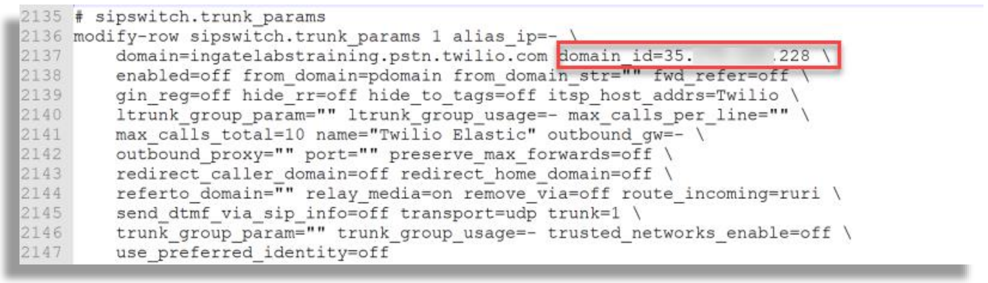
- As we are using Twilio, we will change the Host name in Request URI to the Public IP address of the Secondary SIParator

  Search for **"domain_id"**



```
# sipswitch.trunk_params
modify-row sipswitch.trunk_params 1 alias_ip=- \
    domain=ingatelabstraining.pstn.twilio.com domain_id=52[redacted].1 \
    enabled=off from_domain=pdomain from_domain_str="" fwd_refer=off \
    gin_reg=off hide_rr=off hide_to_tags=off itsp_host_addrs=Twilio \
    ltrunk_group_param="" ltrunk_group_usage=- max_calls_per_line="" \
    max_calls_total=10 name="Twilio Elastic" outbound_gw=- \
    outbound_proxy="" port="" preserve_max_forwards=off \
    redirect_caller_domain=off redirect_home_domain=off \
    referto_domain="" relay_media=on remove_via=off route_incoming=ruri \
    send_dtmf_via_sip_info=off transport=udp trunk=1 \
    trunk_group_param="" trunk_group_usage=- trusted_networks_enable=off \
    use_preferred_identity=off
```

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

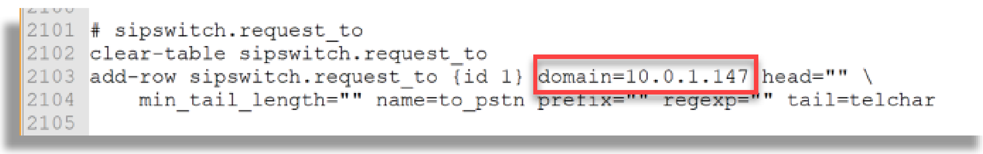


```
# sipswitch.trunk_params
modify-row sipswitch.trunk_params 1 alias_ip=- \
    domain=ingatelabstraining.pstn.twilio.com domain_id=35.[redacted].228 \
    enabled=off from_domain=pdomain from_domain_str="" fwd_refer=off \
    gin_reg=off hide_rr=off hide_to_tags=off itsp_host_addrs=Twilio \
    ltrunk_group_param="" ltrunk_group_usage=- max_calls_per_line="" \
    max_calls_total=10 name="Twilio Elastic" outbound_gw=- \
    outbound_proxy="" port="" preserve_max_forwards=off \
    redirect_caller_domain=off redirect_home_domain=off \
    referto_domain="" relay_media=on remove_via=off route_incoming=ruri \
    send_dtmf_via_sip_info=off transport=udp trunk=1 \
    trunk_group_param="" trunk_group_usage=- trusted_networks_enable=off \
    use_preferred_identity=off
```

- Need to adjust Dial Plan for Matching Request-URI

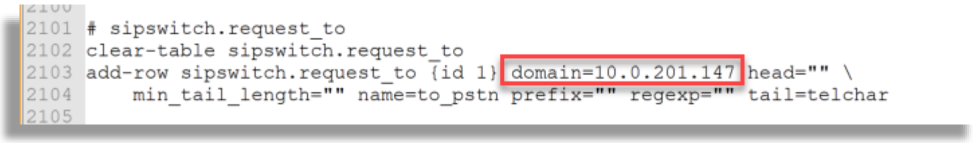
  In case you are matching the internal IP address in the Request URI in the dial plan you might need to consider this change in the file to be synchronized.

  Seach for **"# sipswitch.request_to"**



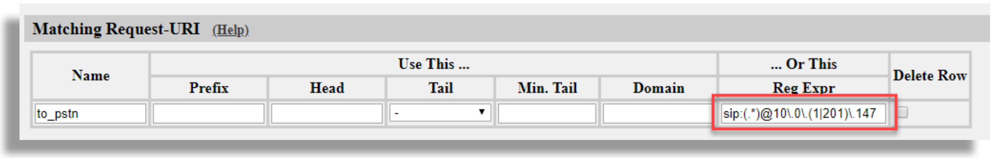
```
# sipswitch.request_to
clear-table sipswitch.request_to
add-row sipswitch.request_to {id 1} domain=10.0.1.147 head="" \
    min_tail_length="" name=to_pstn prefix="" regexp="" tail=telchar
```

Replace the IP with the Failover internal IP address:



```
# sipswitch.request_to
clear-table sipswitch.request_to
add-row sipswitch.request_to {id 1} domain=10.0.201.147 head="" \
    min_tail_length="" name=to_pstn prefix="" regexp="" tail=telchar
```

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:

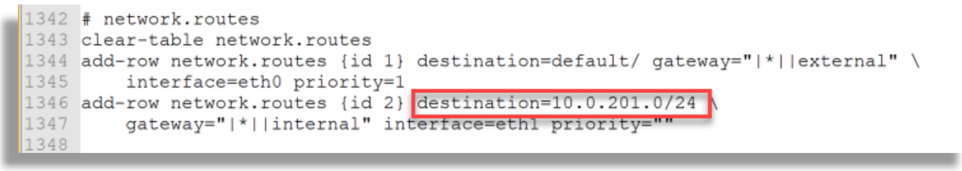


Matching Request-URI (Help)

Name	Use This ...					... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
to_pstn			-			sip:(.*)@10\.0\.(1|201)\.147	□

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

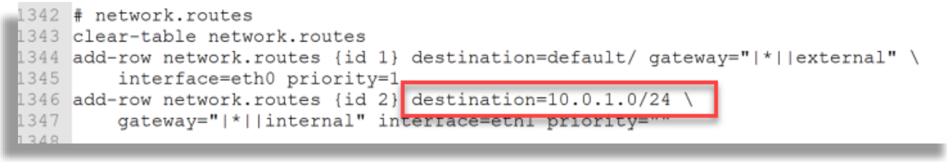
  Search for **"# network.routes"**



```
# network.routes
clear-table network.routes
add-row network.routes {id 1} destination=default/ gateway="|*||external" \
    interface=eth0 priority=1
add-row network.routes {id 2} destination=10.0.201.0/24 \
    gateway="|*||internal" interface=eth1 priority=""
```

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:

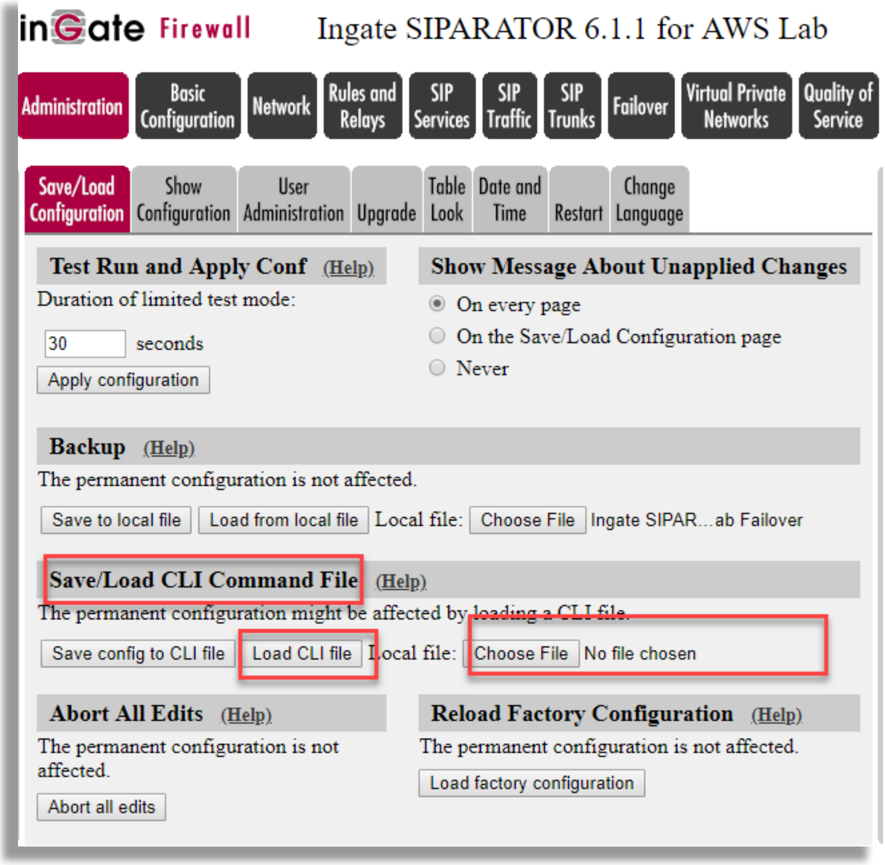


```
# network.routes
clear-table network.routes
add-row network.routes {id 1} destination=default/ gateway="|*||external" \
    interface=eth0 priority=1
add-row network.routes {id 2} destination=10.0.1.0/24 \
    gateway="|*||internal" interface=eth1 priority=""
```

- 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 → Save/Load Configuration and load the CLI file you modified in the previous step.



Test Run and Apply Conf (Help)

Duration of limited test mode:

30 seconds

Show Message About Unapplied Changes

● On every page

○ On the Save/Load Configuration page

○ Never

Backup (Help)

The permanent configuration is not affected.

Local file: Choose File Ingate SIPAR...ab Failover

Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Local file: Choose File No file chosen

Abort All Edits (Help)

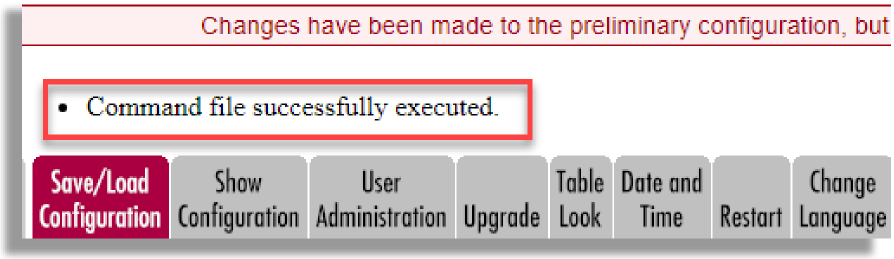
The permanent configuration is not affected.

Reload Factory Configuration (Help)

The permanent configuration is not affected.

- Chose the file
- Load CLI File

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

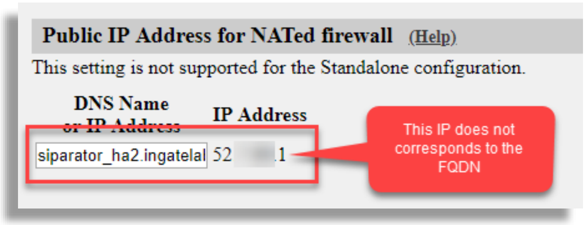


Changes have been made to the preliminary configuration, but

- Command file successfully executed.

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

It looks like:



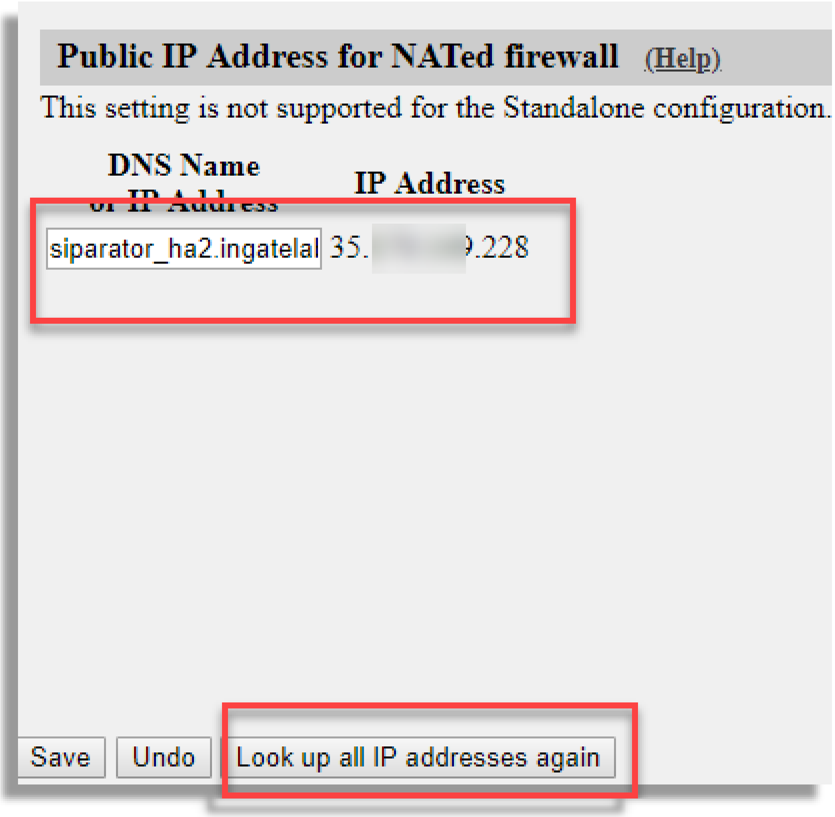
Public IP Address for NATed firewall (Help)

This setting is not supported for the Standalone configuration.

DNS Name or IP Address	IP Address
siparator_ha2.ingatelal	52 [redacted] 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.

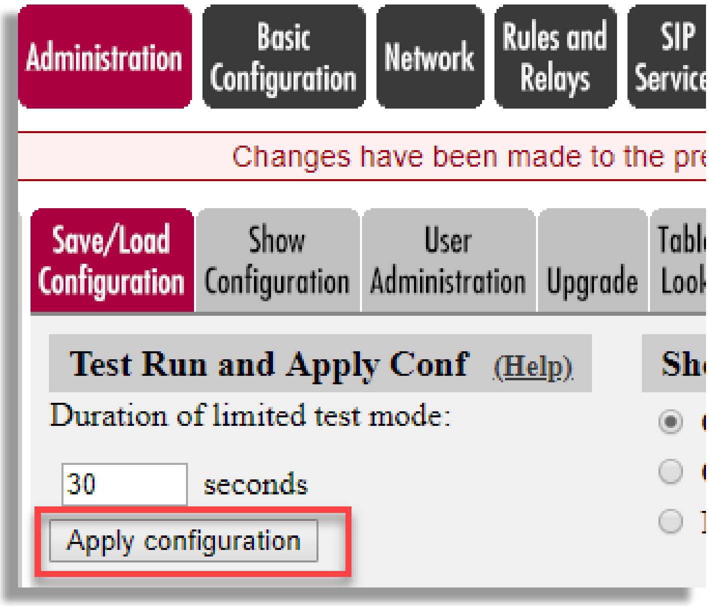


Public IP Address for NATed firewall (Help)

This setting is not supported for the Standalone configuration.

DNS Name or IP Address	IP Address
siparator_ha2.ingatelal	35.[redacted].228

Next step is just to Apply all changes and save.

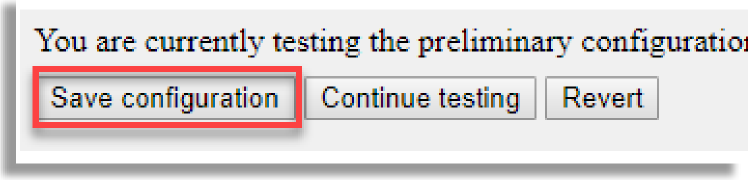


Changes have been made to the pre

Test Run and Apply Conf (Help)

Duration of limited test mode:

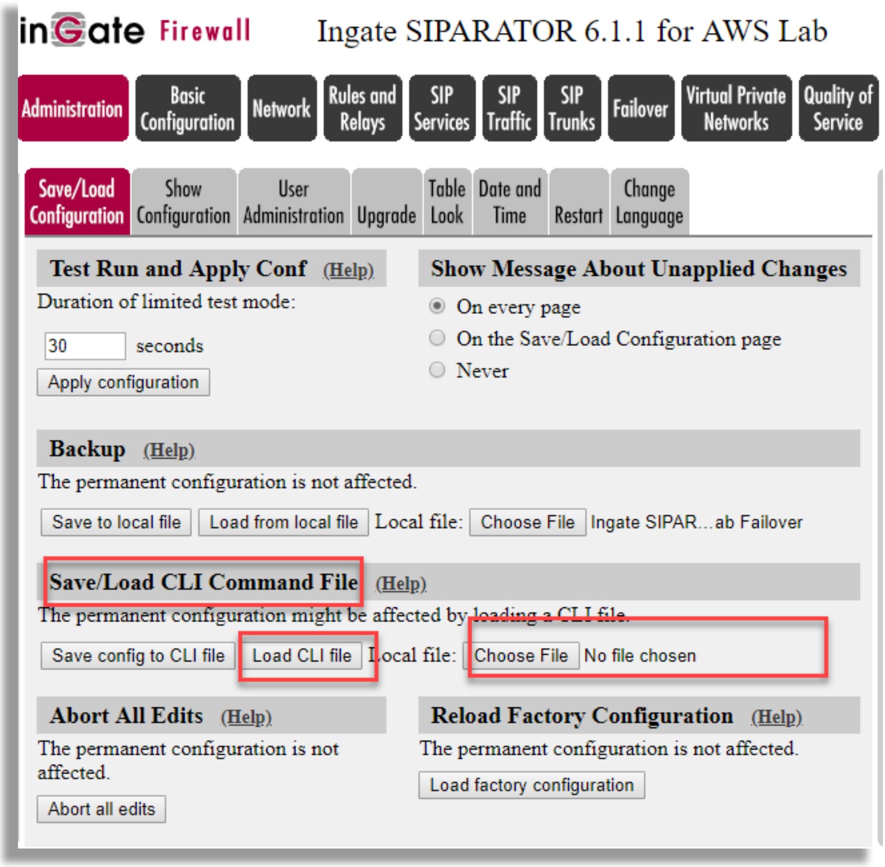
30 seconds



You are currently testing the preliminary configuratio

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 → Save/Load Configuration and load the CLI file you downloaded from the Main SIParator.



Ingate SIPARATOR 6.1.1 for AWS Lab

Test Run and Apply Conf (Help)

Duration of limited test mode:

30 seconds

Apply configuration

Show Message About Unapplied Changes

● On every page

○ On the Save/Load Configuration page

○ Never

Backup (Help)

The permanent configuration is not affected.

Save to local file | Load from local file | Local file: Choose File Ingate SIPAR...ab Failover

Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Save config to CLI file | Load CLI file | Local file: Choose File No file chosen

Abort All Edits (Help)

The permanent configuration is not affected.

Abort all edits

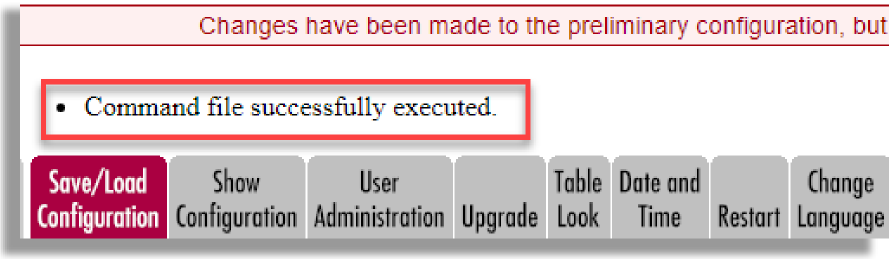
Reload Factory Configuration (Help)

The permanent configuration is not affected.

Load factory configuration

- Chose the file
- Load CLI File

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



Changes have been made to the preliminary configuration, but

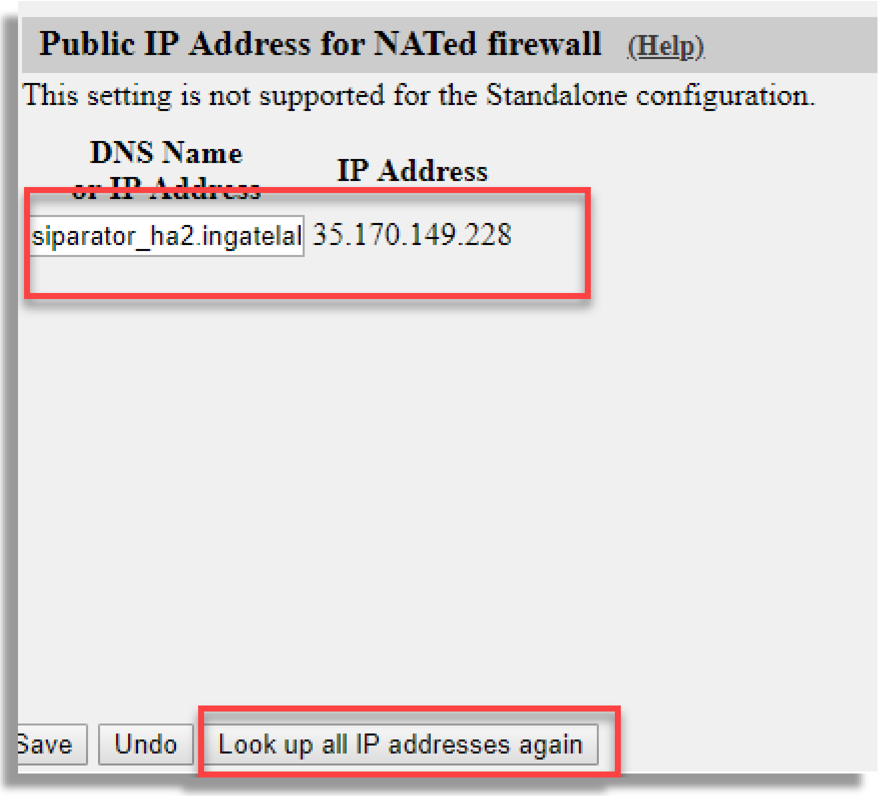
- Command file successfully executed.

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:

SIP Services → Basic



Public IP Address for NATed firewall (Help)

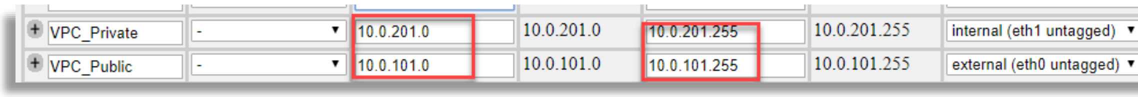
This setting is not supported for the Standalone configuration.

DNS Name or IP Address	IP Address
siparator_ha2.ingatelal	35.170.149.228

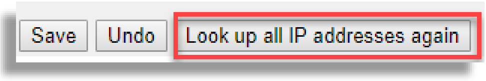
Change the FQDN to the one associated to the Public IP address of the Failover SIParator. Then press "Look up IP addresses again" to discover the new IP address

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

Networks → Networks and Computers



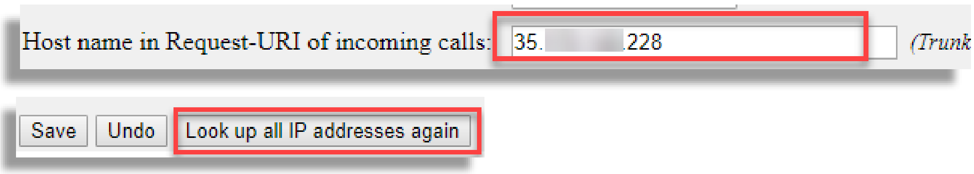
VPC_Private	-	10.0.201.0	10.0.201.0	10.0.201.255	10.0.201.255	internal (eth1 untagged)
VPC_Public	-	10.0.101.0	10.0.101.0	10.0.101.255	10.0.101.255	external (eth0 untagged)



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 → Go to SIP Trunk



Host name in Request-URI of incoming calls: 35.[redacted].228 (Trunk

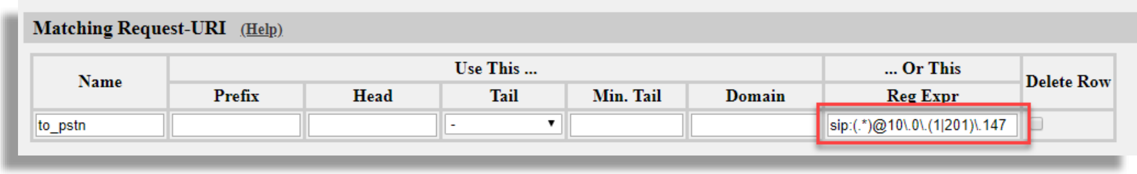
- Need to adjust Dial Plan for Matching Request-URI

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 Request-URI (Help)

Name	Use This ...					... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
to_pstn			- ▾			sip:(.*)@10\.0\.(1|201)\.147	□

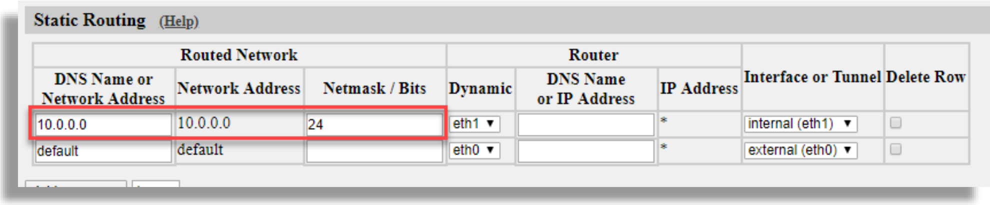
- Replicate static route to consider Failover and non-failover cross connection

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:

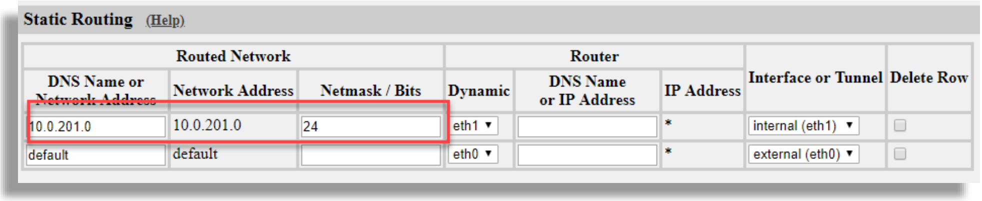
Failover Static Routes:



Static Routing (Help)

Routed Network			Router			Interface or Tunnel	Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address		
10.0.0.0	10.0.0.0	24	eth1 ▾		*	internal (eth1) ▾	□
default	default		eth0 ▾		*	external (eth0) ▾	□

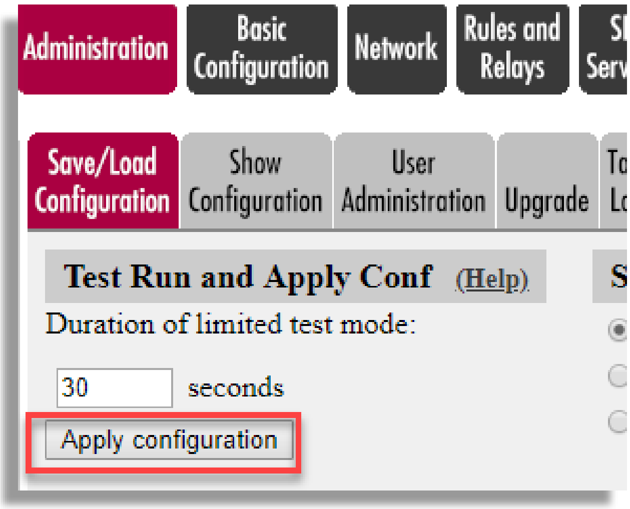
Main Static Route



Static Routing (Help)

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

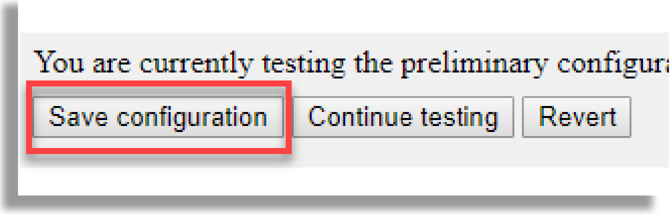
- Save all and apply changes



Test Run and Apply Conf (Help)

Duration of limited test mode:

30 seconds



You are currently testing the preliminary configur

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.

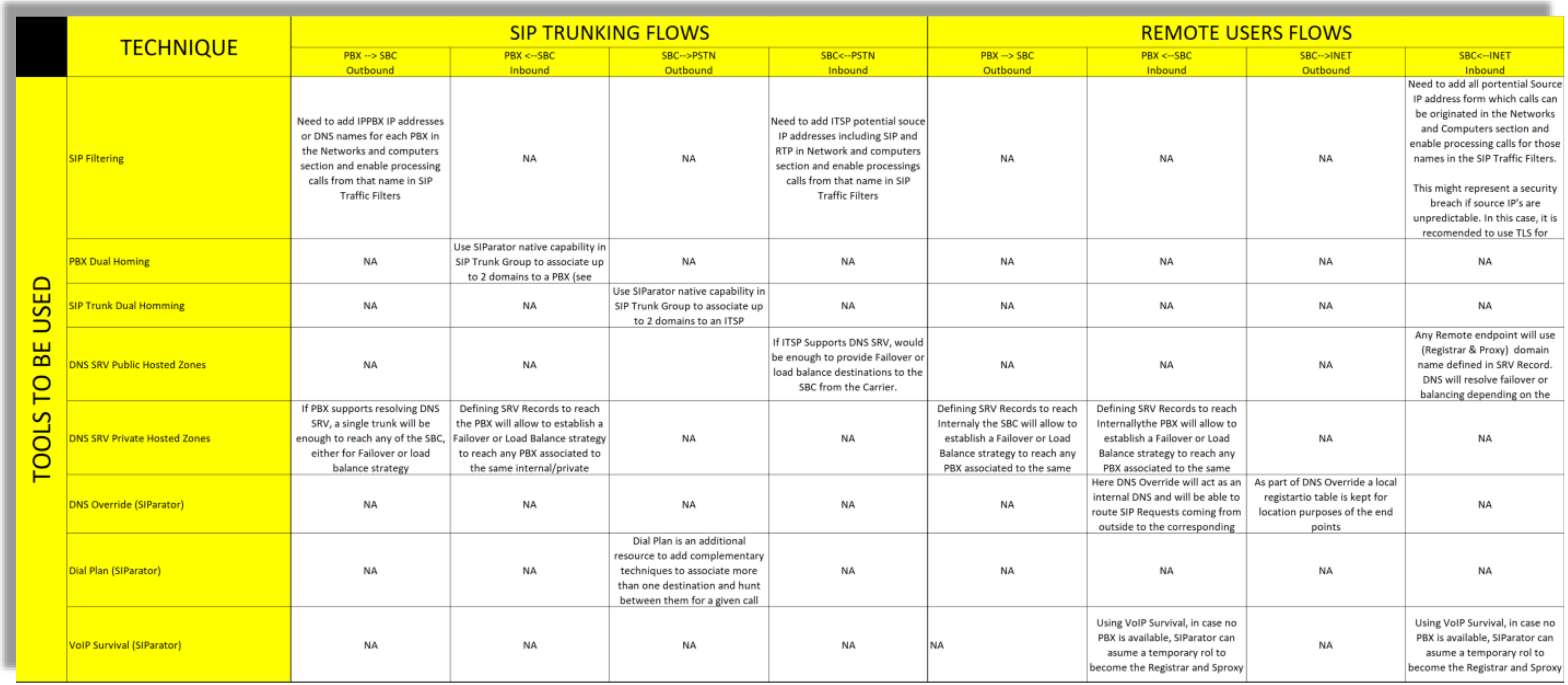
With minor adjustments it can be extrapolated to other scenarios, such as:

- 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.html

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.



	TECHNIQUE	SIP TRUNKING FLOWS				REMOTE USERS FLOWS			
		PBX --> SBC Outbound	PBX <--SBC Inbound	SBC-->PSTN Outbound	SBC<--PSTN Inbound	PBX --> SBC Outbound	PBX <--SBC Inbound	SBC-->INET Outbound	SBC<--INET Inbound
TOOLS TO BE USED	SIP Filtering	Need to add IPPBX IP addresses or DNS names for each PBX in the Networks and computers section and enable processing 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 Traffic Filters	NA	NA	NA	Need to add all portential Source IP address form which calls can be originated in the Networks and Computers section and enable processing calls for those names in the SIP Traffic Filters. This might represent a security breach if source IP's are unpredictable. In this case, it is recomended to use TLS 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
	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
	DNS SRV Public Hosted Zones	NA	NA		If ITSP Supports DNS SRV, would be enough to provide Failover 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
	DNS SRV Private Hosted Zones	If PBX supports resolving DNS SRV, a single trunk will be enough to reach any of the SBC, either for Failover or load balance strategy	Defining SRV Records to reach the PBX will allow to establish a Failover 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 Failover or Load Balance strategy to reach any PBX associated to the same	Defining SRV Records to reach Internallythe PBX will allow to establish a Failover or Load Balance strategy to reach any PBX associated to the same	NA	NA
	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
	VoIP Survival (SIParator)	NA	NA	NA	NA	NA	Using VoIP Survival, in case no PBX is available, SIParator can asume a temporary rol to become the Registrar and Sproxy	NA	Using VoIP Survival, in case no PBX is available, SIParator can asume a temporary rol to become the Registrar and Sproxy