Elastix with Twilio Elastic SIP Trunking
Interconnection Guide

Introduction

This document is a walk-through of how to connect your office VoIP phone system, here represented as a VoIP Softphone to the Elastix IP-PBX and consequently Twilio Elastic SIP Trunking. At the end of the setup you will be able to make and receive low-priced phone calls between your office phone and any phone worldwide. No lead-time! No contracts! No provisioning cap! Thanks to Twilio’s unique offer.

The Elastix system will be running in an AMAZON EC2 instance. Your VoIP phone system is typically in your office environment but, for the purposes of this introduction, we’ll be using a softphone on your laptop. Twilio Elastic SIP Trunking will be used to interface with the Public Switched Telephony Network (PSTN); globally if you want. We do make no assumptions about your skill level or experience and instead walk you through how to do the following, step-by-step.

Setup Twilio Elastic SIP Trunk
Build the Elastix IP-PBX
   Provision an Amazon EC2 server
   Access and Update your CentOS instance
   Install Elastix on your CentOS instance
Install Zoiper Softphone
Configure the Elastix IP-PBX
   Configure Elastix for outgoing calls
   Configure Zoiper as an extension
   Configure Elastix for incoming calls
Summary and next Steps

The emphasis in this document is not on terminology, but on getting you up and running in the shortest amount of time.
Note: The charges you will incur following this tutorial are Amazon EC2 charges and possibly Twilio charges. This is true if you exceeded your free allotment. All software components are free of charge for demo purposes.

Setup Twilio Elastic SIP Trunk

We assume you have already setup your Elastic SIP Trunks with Twilio in the Elastic SIP Trunking section. If not Twilio provides very concise and clear instructions on this page.

In a nutshell here are the steps you need to do:

1. Go to the Elastic SIP Trunking section and configure a Trunk
2. Go to the termination section and configure the username/password or Access Control List (ACL). The ACL is the egress/public IP address of your IP PBX or SBC system that sends traffic to Twilio. Here it should be the public IP address of your Elastix server. If you haven’t set up your Elastix PBX yet, please do revisit this section after doing so.
3. In the Origination section provide the IP address for the ingress of your IP PBX/SBC. Again if you follow our document this should be the IP address of your Elastix server. Also configure a Twilio number so that calls to this Twilio phone number get forwarded to the SIP URI you configured.

Take note of the information you configured in the Twilio portal, particularly username/password, SIP URI and IP addresses you configured. All of this is explained in some detail in the Getting Started section in the Twilio portal.

Build the Elastix IP-PBX

Provision an Amazon EC2 server

We assume you already have an Amazon EC2 account. If not, please use publicly available Amazon documentation to create an account. Once you have an account, login to the EC2 Management Console. Mine looks like this (see figure 1):
What we are going to do here is launch a CentOS image and configure it for use with Elastix. Again Amazon provides excellent documentation and we will only concentrate on minimalistic instructions.

1. Go to Launch Instance and Select Community AMI’s and checkbox the CentOS filter. I am going to pick the first 64bit CentOS, which I used successfully in the past. The AMI image is ami-0053dd30
2. Select that image and pick a micro instance in the next screen.
3. Go through the “Next” screens until you hit STEP 5 where you are going to name your instance. Pick a descriptive name, like ElastixTwilioSIPTrunkServer.
4. The next step, STEP 6: Configure Security Group, is very important. Essentially every Amazon server has a built-in firewall (IP tables) but we want the server to let our VoIP and administrative traffic (like ssh) pass. So we have to do the correct configuration. There are a couple of ports we need to open (see figure 2):
   - HTTPS – TCP – port 443 – anywhere : Elastix GUI
   - HTTP – TCP – port 80 – anywhere : Elastix GUI
   - SSH – TCP – port 22 - – anywhere : console login
   - Custom UDP Rule – UDP – port 4569 - anywhere : SIP REGISTER ( mind you Twilio does not yet support SIP REGISTER but we are building for the future )
   - Custom TCP Rule – TCP – port 5060 – anywhere : SIP SIGNALING
   - Custom UDP Rule – UDP – port 5060 – anywhere : SIP SIGNALING ( signaling at Twilio can be TCP or UDP )
   - Custom UDP Rule – UDP – port range 10,000-20,000 – anywhere : RTP ( audio streams )
5. Press Review and Launch and check that you configured everything correctly

6. Next you need to select a keypair. This keypair is used to login directly to your Amazon EC2 server from a terminal, which we will do shortly. The private key will be stored on your disk. Ensure you set permissions for the saved private key file so that ssh can use it. On a Linux system, you would do this with the command $chmod 600 privatekeyfilename$. I already have keys so I just select one of my existing ones.
7. Now Launch Instances and watch how the server proceeds through the different stages in your EC2 console. It's pure magic happening here.

Access and Update your CentOS instance

Once your servers “status checks” shows the green checkmark the server is up and running.

IMPORTANT NOTE: Amazon servers have their own firewalls (IP-tables) and have a private and public IP address. The private IP address is only routable within the Amazon network. For remote access and to send SIP traffic we need to use the public IP address. In my case the private IP is 172.31.30.245 and the public IP is ec2-52-26-140-183.us-west-2.compute.amazonaws.com/52.26.140.183 (see figure 3)

NOTE: When you restart a server the public IP won’t change. However when you stop and start or terminate and relaunch a server it may change. Amazon gives you public IP’s you can permanently assign to your machine image. You can do this at this stage to make rebooting easier. Descriptions are here. I won’t do this.
Let's now connect to our instance. If you right click your server instance (Ctrl-click on Mac) Amazon will tell you exactly how to connect to this instance. This is how it looks for me.
So I am opening a terminal on my Apple MAC and go to the folder where I downloads my access key from the previous step (~Downloads for me) and issue the command to connect to my instance. For me this is $ssh -i ralfelastix.pem root@52.26.140.183 Your IP address and your filename for the keyfile will be different.

Amazing! The prompt shows me that I am now on my EC2 CentOS server with internal IP address 172.31.30.245. Magic! Let’s update this CentOS image to the latest packages.
On the command line, issue a "$yum –y update", which will update your system. If you are asked to “yes” any actions, please do so. There are quite a few packages to update. For me it’s close to 1GB to download. This should take no more than about 10 minutes to finish.

Install Elastix on your CentOS instance

After the upgrade has finished we are finally going to install Elastix. In a nutshell we will have to download Elastix as iso (CD image), transfer it to our server, make the CD accessible and install Elastix. Here we go.

I am using Elastix-2.5.0-Stable-x86_64-bin-21oct2014.iso. Other versions may work, but this is the latest at the time of writing this document.

1. Head over to [http://www.elastix.com/en/downloads/](http://www.elastix.com/en/downloads/) where you can find the Elastix downloads. I picked the 64 bit version, though this shouldn’t matter much. Note: you could probably download it with wget to the EC2 instance directly. I liked the graphical selection GUI instead of a hard link, which may change as this document ages. Once you have downloaded the iso image we need to transfer it to the EC2 server.

2. Open another terminal on your local machine and cd to the downloads directory where you downloaded the iso. Let’s transfer it now to the EC2 instance.

3. The command for me is

```
scp -i ralfelastix.pem Elastix-2.5.0-Stable-x86_64-bin-21oct2014.iso root@52.26.140.183:~/
```

   - you still need your private key file even with SCP

   - your username and EC2 server

   - the home directory for the root user. We will find the binary there.

4. Let’s go back to our terminal where we are logged-in to our EC2 instance. Here are the commands you should issue:

   a. $cd – brings you to your home directory where you should see the iso ( check with $ls * )

   b. $mkdir /mnt/iso – to create a directory in which we are going to mount the iso

   c. $mount –o loop Elastix-2.5.0-Stable-x86_64-bin-21oct2014.iso /mnt/iso
5. Now we need to make our yum repository aware that it should also check for the local disk when we do an install. The way to do that is to add our mounted iso image to the yum repositories.
   a. $vi /etc/yum.repos.d/CentOS-Base.repo – this is the config file yum consults to check to update packages
   b. At the end of the file add the following
      
      [elastix]
      name=Elastix
      baseurl=file:///mnt/elastix/
      pgcheck=0
      enabled=1

      There is no need to disable the other repositories. In fact it would cause issues with PHP during the Elastix install.
We now need to clear the yum cache with $yum clean all and check that your repolist has the new file repository included by issuing a $yum repolist. See how there are references to Elastix. Just what we want.

```
[root@ip-172-31-38-245 ~]# yum clean all
Cleaning up Everything
Cleaning up list of fastest mirrors
[root@ip-172-31-38-245 ~]# yum repolist
Loaded plugins: fastestmirror
 Determining fastest mirrors
  * base: mirror.chpe.utah.edu
  * extras: mirror.keystealth.org
  * updates: mirrors.cat.pdn.edu
base | 1.1 kB | 00:00
base/pri | 1.3 MB | 00:00
base | 3657/3657
elastix | 1.1 kB | 00:00
elastix/pri | 215 kB | 00:00
elastix | 477/477
extras | 2.1 kB | 00:00
extras/pri | 173 kB | 00:00
updates | 2.0 kB | 00:00
updates/pri | 410 kB | 00:00
repo id repo name status
base | CentOS-5 - Base | 5,857
elastix | Elastix | 477
extras | CentOS-5 - Extras | 366
updates | CentOS-5 - Updates | 306
repolist: 4,796
[root@ip-172-31-38-245 ~]#
```

Figure 7 Yum installer check to see that it picked up the Elastix Repo
d. Finally we are ready to install Elastix. In the terminal do a `yum --nogpgcheck install elastix`

e. There are two more things involved. Start the mysql database and configure the GUI with a password
   i. `sbin/service mysqld start`
   ii. `#/etc/rc3.d/S66elastix-firstboot start`
Install Zoiper Softphone

1. **IMPORTANT**: Before we configure our softphone there is a very important step to do. And it cannot be done in the Elastix GUI. We need to tell Elastix what it’s internal and what it’s external IP address is. The Elastix server itself only sees its own internal IP address. In the EC2 console this is called the private IP and usually starts with 172.x.x.x. We don’t want Elastix to send the private IP in any connection identifiers, as Twilio would not be able to reach it. Remember that all Amazon EC2 servers have an external, public IP, as well as an internal, private IP. We need to tell Elastix to differentiate between the two and send the right one. This can only be done in a file, not the GUI. In the Mac terminal connected your Elastix server do the following:
   a. `$ vi /etc/asterisk/sip_nat.conf`
      ;add the following
      
      nat=yes
      externip=52.26.140.183
      fromdomain=ec2-52-26-140-183.us-west-2.compute.amazonaws.com
      localnet=172.0.0.0/8
      
      externip is the public IP address that the EC2 console shows you. Remember this may change with stopping and starting the server
      fromdomain is the Public DNS from EC2
      localnet – make sure your private IP starts with 172
   b. restart the server, either via the ec2 console or since you are in a terminal already you can do a $shutdown –r now

   **If you do NOT do this step you will experience one way audio and the phone hanging up after being connected for about 15s later. Do it now!**

2. While the server is rebooting let’s install and configure the Zoiper SIP softphone on your local computer. Once you downloaded zoiper from [http://www.zoiper.com/en/voip-softphone/download/zoiper3](http://www.zoiper.com/en/voip-softphone/download/zoiper3) you must launch and configure it. I am using the 3.3 version. Any other version will work just as well. Make sure that in your Twilio account you have whitelisted the IP address of your Elastix
server. Otherwise you will get a 503 error in Zoiper Since Twilio will be rejecting your call.

a. After you launch Zoiper for the first time go to the Settings->Accounts tab
b. In the accounts Tab configure a new account
c. In the account settings provide the following
   i. Domain – this is the public DNS name of your Elastix Server as you see it in the Amazon EC2 console. Mine is ec2-52-26-140-183.us-west-2.compute.amazonaws.com
   ii. Username : 100 ( as configured in Elastix )
   iii. Auth Username: 100
   iv. Password : What you configured in Elastix. We used yourtwiliosecret1234 earlier
d. Once you click register it Zoiper should change the status for this account to registered.

Figure 15 Zoiper First Launch
Figure 16 Accounts Tab
Figure 17 Fill in your Elastix details, the domain name is the Publix DNS address of your Elastix server, username is 100 and password is the one we configured in Elastix

Configure the Elastix IP-PBX
It is time to configure your Elastix server for Twilio SIP Trunking. We will do this in 3 easy steps. First we configure the SIP Termination trunk, which let’s you place calls to any PSTN phone globally (watch your Twilio geographic account permissions), then we configure it to use the Zoiper softphone, which represents your office phone system, and, finally, we will configure the system to receive SIP calls from Twilio and send it to the Zoiper phone. Let’s do it!

**Configure Elastix for outgoing calls**

3. If you haven’t configured your Twilio SIP Trunks yet, now is a good time to catch-up. Instructions are at the head of this document.
   First let’s log on to the Elastix GUI. You can do this by launching Firefox and typing as URL https://publicipaddressofyourserver. In my case this would be https://ec2-52-26-140-183.us-west-2.compute.amazonaws.com/
   There may be a security exception, since this Elastix server doesn’t have an officially signed SSL certificate installed. Just accept the exception. You should now see the Elastix GUI in your browser.
   Use the username=admin and the password you configured earlier to log in to your Elastix instance.
   Remember? The one you set in the blue config screen.
Figure 10 Elastix Login Screen
4. Let’s dive right in. Go to the PBX-tab and then on the left side menu select Trunks. On the right side menu you will find a preconfigured trunk Channel go (dahdi). Select this channel by clicking the link and then delete it. It has caused me pain and trouble in the past and it is not used for SIP anyways.
Figure 12 Initial Loading of Trunk Screens
5. Once we have this clean slate to work from add your Twilio Termination SIP trunk. Select “Add Trunk” on the right side and configure your Twilio Termination SIP Trunk as follows:
   a. Trunk name: twilioterminationtrunk
   b. Outbound CallerID: set to the phone number you configured for your SIP trunk in the Twilio portal or any other number you want to display as CallerID when you place calls. Twilio will allow any CallerID as long as it adheres to the E.164 format. In the US, this is a +1 followed by the number.
   c. Outgoing settings: Name the trunk again twilioterminationtrunk
   d. In the Peer Settings field add the following freeform settings
      
      ```
      type=peer
      host=yourtwilioconfiguredsipdomain.pstn.twilio.com
      dtmfmode=rfc2833
      canreinvite=no
      ```
disallow=all
allow=ulaw
insecure=port,invite

You only have to change the hostname to what you had configured earlier in the Twilio account portal to be your SIP domain and inherit the other settings. The Twilio domains all go like whateveryouchose.pstn.twilio.com and represent the endpoint where Elastix sends the INVITE to, to connect with Twilio.
Edit SIP Trunk

Delete Trunk twillterminationtrunk

In use by 1 route

General Settings

Trunk Name: twillterminationtrunk
Outbound CallerID: +16502156517
CID Options: Allow Any CID
Maximum Channels:

Asterisk Trunk Dial Options:
Continue if Busy: Do not check this box to always try next trunk
Disable Trunk: 

Dialed Number Manipulation Rules:

(prepend ) + prefix | match pattern

Add More Dial Pattern Fields
Clear all Fields

Dial Rules Wizard:
(pick one)
Outbound Dial Prefix:

Outgoing Settings

Trunk Name: twilltermination

PEER Details:
type= Sangoma
host= elastix.getn.twilio.com
dialmode=rfc3329
disable=all
allow=all
insecure=port,invite

Incoming Settings

USER Context:
USER Details:

Registration

Register String:

Submit Changes  Duplicate Trunk
6. Now “Submit Changes” followed by “Apply Config”. If you have not set the CallerID you can ignore the warning about the CallerID but you may find some strange CallerID during your first call.

7. Next let’s configure an Outbound Route to make use of this trunk. In the left menu select “Outbound Routes”. You can use and modify the 9_outside pre-configured route or create one from scratch. If you create a new Route make sure the Route Position is before the default 9_outside route. We will reuse and modify the existing route.

   a. In the Dial Pattern that will use this route add +1 as prepend field. Remember that Twilio wants all numbers in full E.164 format, which means for US dialing Twilio needs the +1 in front of the NPANXXXXXX. Leave the 9 in the prefix, because that’s how we want users to dial a number to get an outside line. And for the match pattern insert NXXNXXXXXX. So in Zoiper a user would dial 94151231234 and Elastix will send the request to Twilio as +14151231234, just what we need.

   b. In the Trunk Sequence for Matched Routes select your previously configured twilioterminationtrunk.

   c. Press “Submit Changes” and “Apply Config” to make these changes real.

Configure Zoiper as an extension

8. Now we need to configure an extension in the Elastix GUI, which represents our Zoiper phone to make use of the new outbound dialing functionality. Select Extensions in the left hand menu. On the screen insert the following fields:

   a. Generic SIP Device and Submit
   b. Add Extension: Set all 4 fields to 100
   c. Secret: yourtwiliosecret1234—this is your password that you must use in the Zoiper Account Settings later
   d. Leave dtmfmode as RFC2833
   e. Set nat to yes
f. Enable voicemail and set a password
9. Now make your first call with Twilio Elastic SIP Trunking. In the Zoiper status line type 9 followed by your US number like 94151231234 and press the Green Call button. You should ring through to that number. Have both callers speak so you can assure audio is flowing in both directions.

![Zoiper](image)

*Figure 18 Dialing in Zoiper via Elastix and Twilio Elastic SIP Trunking*

**Configure Elastix for incoming calls**

We are about 90% there. Let’s quickly recap what we have achieved so far: We installed Elastix and configured an office extension (Zoiper) and gave it the ability to dial out to any PSTN phone. What is left is to configure Elastix so Twilio can send it calls when the Twilio number for the SIP trunk is dialed. This is both easy and fairly tedious in the GUI. The tedious part comes in since Twilio will be configured as peer and Twilio is currently not able to send username/passwords. So we need to identify Twilio based on the IP address and there are 4 of
them. In other words, in addition to the existing trunk we will have to set 4 more Twilio trunks. The 4 configurations are equal but the IP addresses will change for every trunk. The 4 IP addresses are 54.172.60.0, 54.172.60.1, 54.172.60.2, 54.172.60.3. These may change as this document ages, so please check at the Twilio website.

Select the PBX tab in the Elastix GUI and in the left-hand menu Trunks. Let’s configure our 4 additional Twilio trunks.

1. Click Add Trunk followed by Add SIP Trunk  
2. Trunkname: twilioorigination0  
3. Outgoing Settings  
   a. Trunk Name: twilioorigination0  
   b. PEER Details:  
      i. type=peer  
      ii. host=54.172.60.0  
      iii. dtmfmode=rfc2833  
      iv. canreinvite=no  
      v. disallow=all  
      vi. allow=ulaw  
      vii. insecure=port,invite  

4. Submit your changes. You can ignore the warning about the CallerID as these are Origination trunks.  
5. Do the above 3 more times for 3 more trunks. Move the names through twilioorigination0-3 and the IP addresses in the Peer details through 54.172.60.0-3
Figure 19 TwilioOriginationTrunk. You need 4 of these with varying IP addresses

6. "Submit Changes" for each trunk and when you are done with all 4 do the "Apply Config"
7. Almost done!!!! We only need to tell Elastix that when these trunks receive a call from Twilio to route it to Zoiper. This is done with an Inbound Route, which you can select in the left-hand menu.

8. Fill in the Description. I use fromtwiliotrunk

9. Down in the page for "Set Destination" select the Extensions and <100> 100

10. Submit and Apply Config

![Figure 20 Incoming Route Config (Origination)](image-url)
11. Make sure that your Twilio Account Portal’s Elastic SIP Trunk in the Origination section points to your Elastix server. For me this means that my Origination Settings show sip:ec2-52-26-140-183.us-west-2.compute.amazonaws.com

12. Place a call to the number configured in the Twilio portal and Zoiper should ring. Pick it up and talk to yourself. Make sure audio flows in both directions.

Summary and next Steps

This is awesome. We went through a full configuration of Elastix and can now make and receive phone calls via Twilio’s Elastic SIP Trunking product. As next steps you can try to make international dialing work, change the CallerID for calls you place and develop elaborate hunt group rules in Elastix. the only limit is your imagination and, Twilio will be by your side, with help and guidance, the whole way.