Load Balancing FreePBX / Asterisk in AWS

Quick Reference Guide

V1.0.1

ABOUT THIS GUIDE

This document provides a quick reference guide on how to load balance FreePBX / Asterisk servers using the Enterprise AWS Loadbalancer.org Amazon cloud appliance.

RELATED DOCUMENTATION

For additional information about the Loadbalancer.org AWS appliance, please also refer to the following documents:

- Administration Manual
- AWS Quick Start Guide

LOAD BALANCED PORTS

Port	Use	Transport Layer Protocol
5060	Non-encrypted Session Initiation Protocol (SIP)	UDP & TCP
5061	Encrypted Session Initiation Protocol (SIP)	UDP & TCP
4569	Inter Asterisk eXchange (IAX)	UDP
10000 – 20000	Real Time Transport Protocol (RTP)	UDP
10000 – 20000	Real Time Transport Control Protocol (RTCP)	UDP

VPC SECURITY GROUP INBOUND RULES

The following inbound rules must be configured in your Security Group:

- For management: TCP 22 (SSH), TCP 80 (Web), TCP 9001 (WebMin), TCP 9443 (Appliance WebUI), 7777 (HAProxy Stats page)
- For VoIP services: UDP 5060 & 5061 (SIP), UDP 10000-20000 (RTP & RTCP) and UDP 4569 (IAX)

LOAD BALANCER CONFIGURATION

DEPLOY THE LOADBALANCER.ORG AWS APPLIANCE

1. Deploy an AWS Loadbalancer.org appliance as detailed in the Quick Start Guide

ACCESSING THE APPLIANCE WEBUI

Using a browser, navigate to the Public DNS name or Public IP address on port 9443 , i.e.

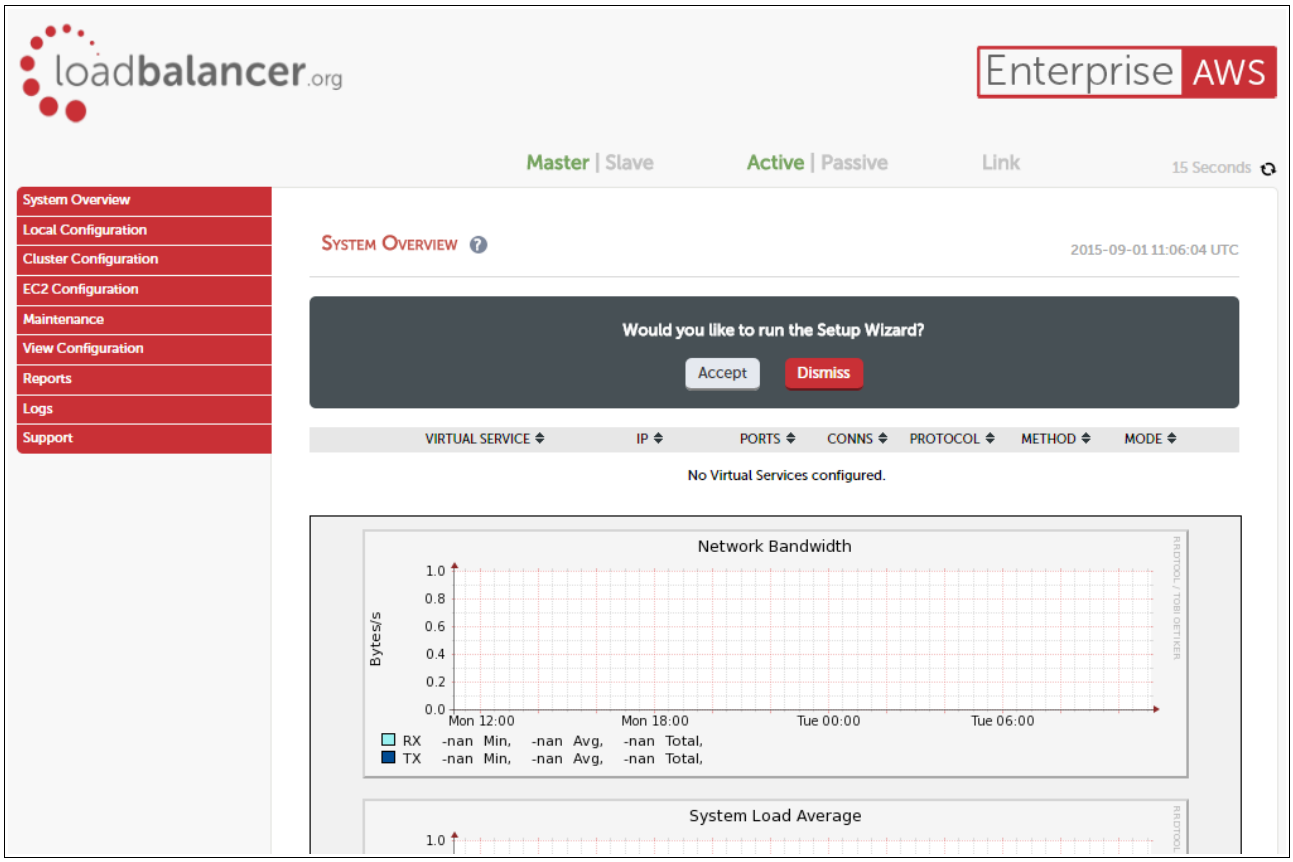
https://<Public DNS name>:9443
or
https://<Public IP address>:9443

You'll receive a warning about the certificate as it's a self signed cert not related to an Internet based CA. Confirm you want to continue and a login prompt will be displayed. Use the following default credentials:

Username: loadbalancer
Password: <EC2 Instance-ID>

> Note:
>
> To change the password for the 'loadbalancer' account, use the WebUI option: *Maintenance > Passwords*.

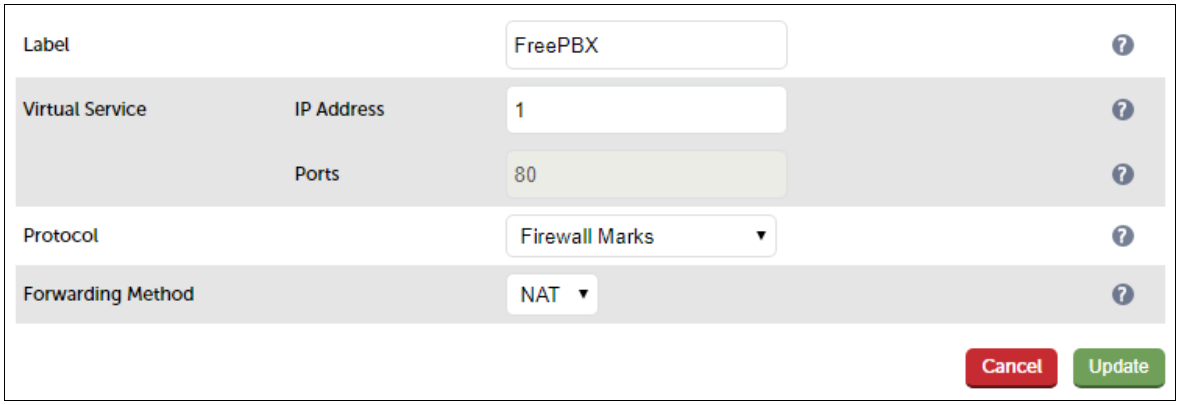
Once logged in, the WebUI is displayed:



CONFIGURE THE VIRTUAL SERVICE

Create a new VIP as described below. A 'Firewall Mark' configuration is used which enables the VIP to support both TCP and UDP on all required ports.

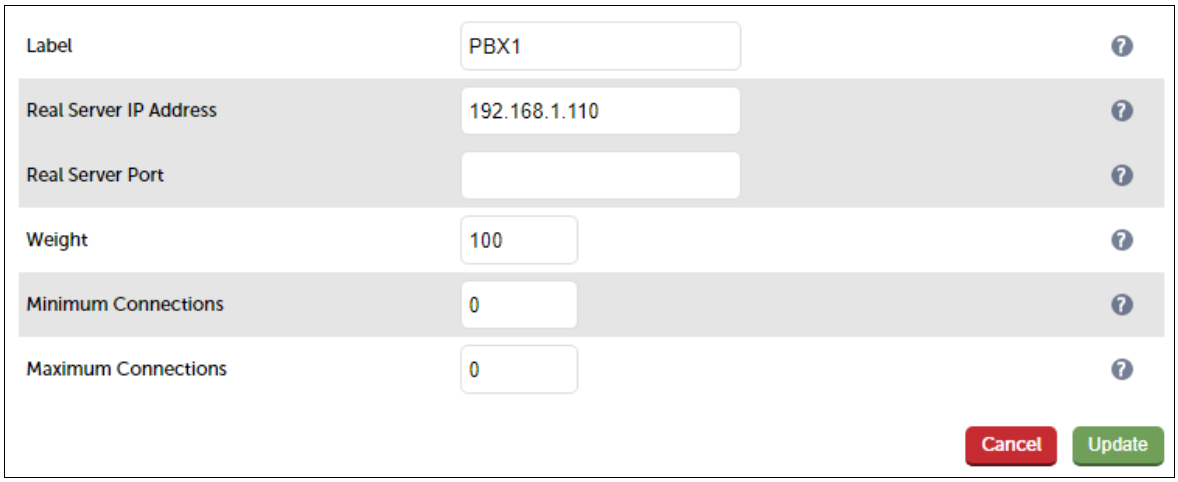
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



3. Define the required *Label* (name) for the VIP, e.g. **FreePBX**
4. Instead of entering an IP address, enter a numeric value, e.g. **1 –** this is the numeric reference for the Firewall Mark, this reference is used in the Firewall Mark Setup section below when defining the firewall rules
5. Set *Protocol* to **Firewall Marks –** at this point the *Virtual Service Ports* field will be grayed out
6. Click **Update**
7. Click **Modify** next to the newly created VIP
8. Set *Check Port* to **80**
9. Click **Update**

DEFINE THE REAL (FREE-PBX) SERVERS

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created VIP
2. Enter the following details:



3. Enter an appropriate label for the Real Server , e.g. **PBX1**
4. Change the *Real Server IP Address* field to the required address, e.g. **192.168.1.110**
5. Leave the *Real Server Port* field blank
6. Click **Update**

7. Repeat the above steps to add your other FreePBX server(s)

FIREWALL MARK SETUP

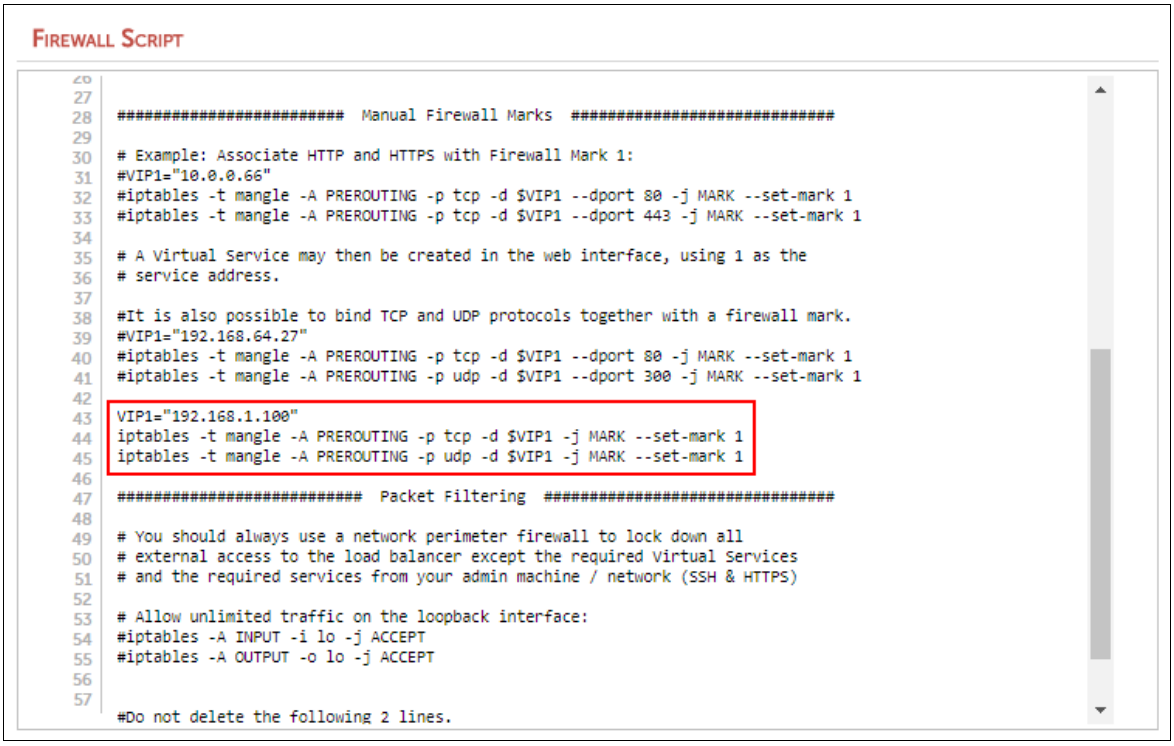
To enable the Firewall Mark the following lines must be added to the firewall script:

```
VIP1="192.168.1.100"
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p udp -d $VIP1 -j MARK --set-mark 1
```

This enables Firewall Mark '1' to support both TCP & UDP on all ports.

To configure this, follow the steps below:

1. Using the WebUI, navigate to: *Maintenance > Firewall Script*
2. Scroll down to the Firewall Marks section
3. Add the additional lines as shown below:

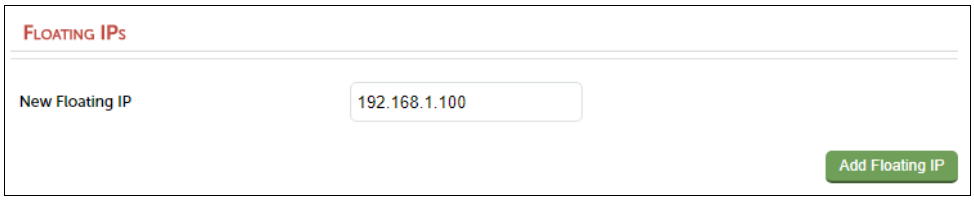


4. Click **Update**

ADD A FLOATING IP

A floating IP must be added that corresponds to the Firewall Mark.

1. Using the WebUI, navigate to: *Cluster Configuration > Floating IPs*
2. Enter the required IP address, e.g. **192.168.1.100**

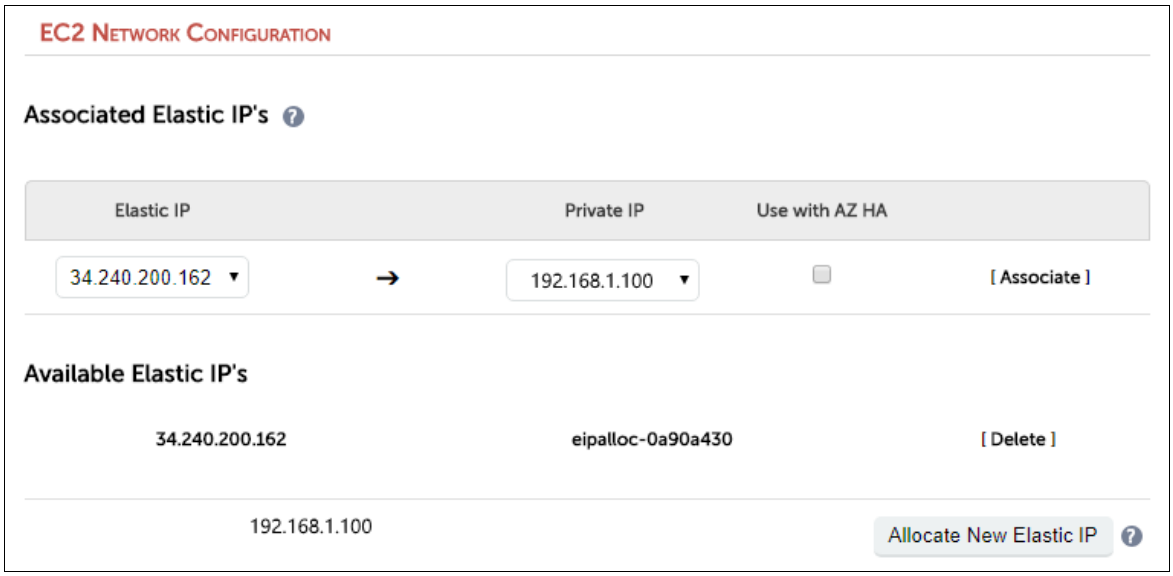


3. Click **Add Floating IP**

ASSOCIATE AN EIP WITH THE FLOATING IP

An EIP is added and associated with the VIP to provide a public IP address for client connections.

1. Using the WebUI, navigate to: *EC2 > EC2 Network Configuration*
2. Click **Allocate New Elastic IP** , this will request an EIP from Amazon using API calls
3. Click **[Associate]** to associate the EIP to the Floating IP private IP address



This association is then displayed as shown below:

CONFIGURE THE SOURCE/DEST. CHECK

1. Using the EC2 Management Console, right click the Loadbalancer.org Appliance, select: *Networking > Change Source/Dest. Check* and click **Yes, Disable**

FREE-PBX SERVER CONFIGURATION

CONFIGURE THE EXTERNAL IP ADDRESS

1. Using the PBX GUI, navigate to: *Settings > Asterisk SIP Settings* and set the *External Address* to the EIP associated with the Floating IP address, in this example **34.240.200.162**

CONFIGURING USERS

- When configuring extensions, ensure that NAT is set to Yes.

CONFIGURE THE DEFAULT GATEWAY

1. SSH to each PBX and as root run the following command:

   ```
   ip route change default via 192.168.1.100
   ```

   replace 192.168.1.100 with your floating IP address

   At this point you will loose access to the PBX and will need to connect again through the EIP.

TESTING

You should now be able to configure your soft client to register against the PBX EIP **sip:extn@EIP** and make calls across extensions.

LOADBALANCER.ORG TECHNICAL SUPPORT

Don't hesitate to contact our support team if you need further assistance: support@loadbalancer.org