

# 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:

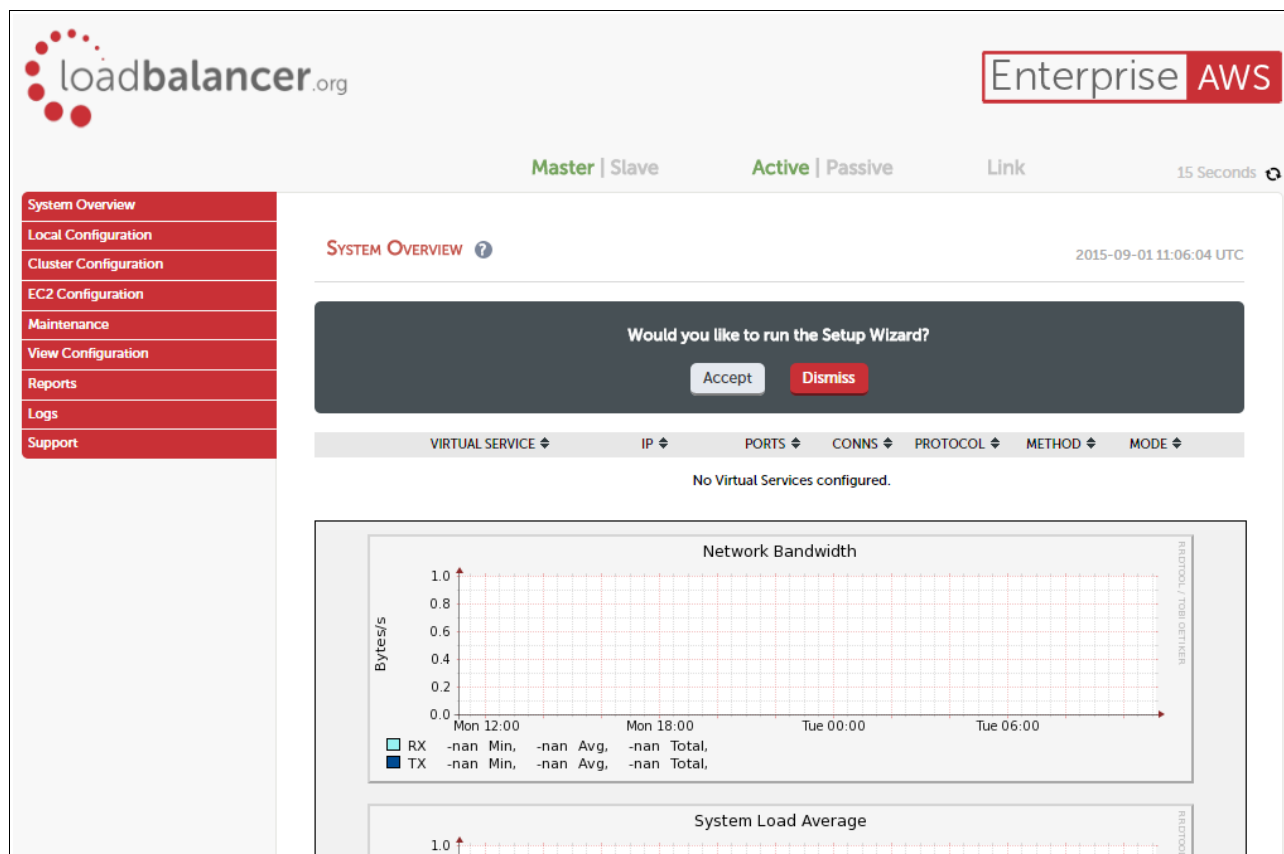
**Username:** loadbalancer

**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.

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

Label	<input type="text" value="FreePBX"/>	?
Virtual Service	IP Address <input type="text" value="1"/>	?
	Ports <input type="text" value="80"/>	?
Protocol	<input type="text" value="Firewall Marks"/>	?
Forwarding Method	<input type="text" value="NAT"/>	?

- Define the required *Label* (name) for the VIP, e.g. **FreePBX**
- 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
- Set *Protocol* to **Firewall Marks** – at this point the *Virtual Service Ports* field will be grayed out
- Click **Update**
- Click **Modify** next to the newly created VIP
- Set *Check Port* to **80**
- Click **Update**

## DEFINE THE REAL (FREE-PBX) SERVERS

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

Label	<input type="text" value="PBX1"/>	?
Real Server IP Address	<input type="text" value="192.168.1.110"/>	?
Real Server Port	<input type="text"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

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

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

## FIREWALL MARK SETUP

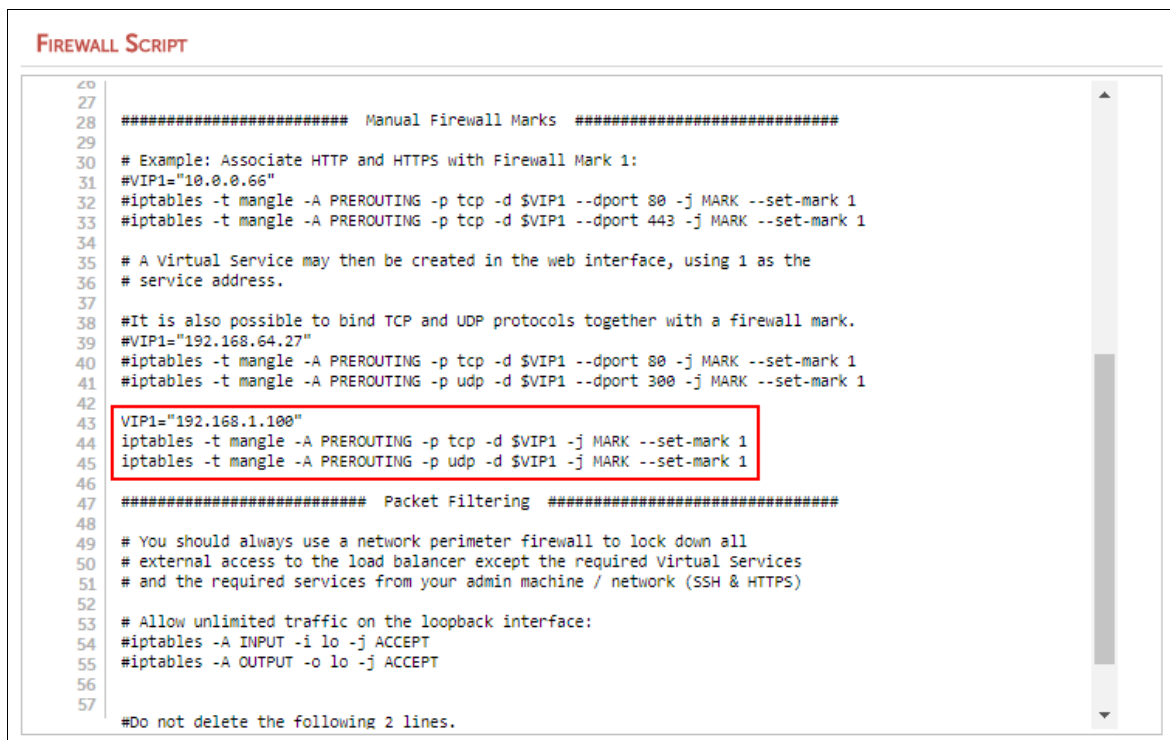
To enable the Firewall Mark the following lines must be added to the firewall script:

```
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:



```
FIREWALL SCRIPT
26
27
28 ##### Manual Firewall Marks #####
29
30 # Example: Associate HTTP and HTTPS with Firewall Mark 1:
31 #VIP1="10.0.0.66"
32 #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
33 #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1
34
35 # A Virtual Service may then be created in the web interface, using 1 as the
36 # service address.
37
38 #It is also possible to bind TCP and UDP protocols together with a firewall mark.
39 #VIP1="192.168.64.27"
40 #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
41 #iptables -t mangle -A PREROUTING -p udp -d $VIP1 --dport 300 -j MARK --set-mark 1
42
43 VIP1="192.168.1.100"
44 iptables -t mangle -A PREROUTING -p tcp -d $VIP1 -j MARK --set-mark 1
45 iptables -t mangle -A PREROUTING -p udp -d $VIP1 -j MARK --set-mark 1
46
47 ##### Packet Filtering #####
48
49 # You should always use a network perimeter firewall to lock down all
50 # external access to the load balancer except the required Virtual Services
51 # and the required services from your admin machine / network (SSH & HTTPS)
52
53 # Allow unlimited traffic on the loopback interface:
54 #iptables -A INPUT -i lo -j ACCEPT
55 #iptables -A OUTPUT -o lo -j ACCEPT
56
57 #Do not delete the following 2 lines.
```

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**

**FLOATING IPs**

---

New Floating IP

[Add Floating IP](#)

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

**EC2 NETWORK CONFIGURATION**

---

**Associated Elastic IP's** ?

Elastic IP	→	Private IP	<input type="checkbox"/>	Use with AZ HA
<input style="width: 100%;" type="text" value="34.240.200.162"/>	→	<input style="width: 100%;" type="text" value="192.168.1.100"/>	<input type="checkbox"/>	<a href="#" style="border: 1px solid #ccc; padding: 2px 5px;">[ Associate ]</a>

---

**Available Elastic IP's**

34.240.200.162	eipalloc-0a90a430	<a href="#" style="border: 1px solid #ccc; padding: 2px 5px;">[ Delete ]</a>
192.168.1.100	<a href="#" style="border: 1px solid #ccc; padding: 2px 5px;">Allocate New Elastic IP</a> <span style="font-size: 0.8em;">?</span>	

This association is then displayed as shown below:

**EC2 NETWORK CONFIGURATION**

---

**Associated Elastic IP's** ?

Elastic IP	→	Private IP	<input type="checkbox"/>	Use with AZ HA
34.240.200.162	→	192.168.1.100	<input type="checkbox"/>	<a href="#" style="border: 1px solid #ccc; padding: 2px 5px;">[ Disassociate ]</a>

---

**Available Elastic IP's**

[Allocate New Elastic IP](#) ?

---

## 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](mailto:support@loadbalancer.org)