Load Balancing SIP

Quick Reference Guide

v1.4.5

ABOUT THIS GUIDE
This guide provides a quick reference for setting up SIP load balancing using Loadbalancer.org appliances.

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

• Quick Start Guide
• Administration Manual

LOAD BALANCED PORTS

<table>
<thead>
<tr>
<th>Port</th>
<th>Use</th>
<th>Transport Layer Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>non-encrypted SIP</td>
<td>UDP &amp; TCP</td>
</tr>
<tr>
<td>5061</td>
<td>encrypted SIP</td>
<td>UDP &amp; TCP</td>
</tr>
</tbody>
</table>

Note:
The exact port requirements depend on how the VoIP system is configured. This guide includes both TCP & UDP ports 5060 and 5061 for completeness.

LOAD BALANCER CONFIGURATION

OPERATION MODE
The load balancer is configured in single-arm layer 4 DR (Direct Return) mode. This mode offers very high performance since return traffic passes directly from the SIP Servers back to the clients by-passing the load balancer. DR mode works by changing the MAC address on the fly to match the relevant SIP Server. Since packets will still have the IP address of the VIP, the SIP Servers must be configured to accept this traffic, but must also be configured to not reply to ARP requests for this address. For more details, please refer to the section ‘Solving the ARP Problem’ on page 5.
DEPLOY THE LOADBALANCER.ORG APPLIANCE
Deploy the Loadbalancer.org appliance as detailed in the Quick Start Guide.

ACCESSING THE APPLIANCE WEBUI
Using a browser, navigate to the appliance's IP address on HTTP port 9080 or HTTPS port 9443, i.e.

http://<IP-Address>:9080
or
https://<IP-Address>:9443

Note:
For HTTPS connections you’ll receive a warning about the certificate as it’s a self signed cert not related to an Internet based CA.

Use the following default credentials to login:

Username: loadbalancer
Password: loadbalancer

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

Once logged in, the WebUI is displayed:
CONFIGURATION STEPS

STEP 1 – CREATE THE VIRTUAL SERVICE (VIP)
Create a new VIP as described below – this is the IP address that clients will connect to. A 'Firewall Mark' is used which enables the VIP to support both TCP and UDP on ports 5060 and 5061.

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

<table>
<thead>
<tr>
<th>Label</th>
<th>SIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td>IP Address</td>
</tr>
<tr>
<td>Ports</td>
<td>80</td>
</tr>
<tr>
<td>Protocol</td>
<td>Firewall Marks</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
</tbody>
</table>

4. Define the required Label (name) for the VIP, e.g. SIP
5. 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
6. The Virtual Service Ports field does not need to be set as it is not relevant in this case - the actual port(s) used are defined in the Firewall Mark Setup section below when defining the firewall rules.

7. Set Protocol to Firewall Marks – at this point the Virtual Service Ports field will be grayed out.

8. Leave the Forwarding Method set to Direct Routing.

9. Click Update.

10. Click Modify next to the newly created VIP.

11. Set Check Port to 5060 or 5061 to suit your requirements.

Note:
If your SIP server only supports SIP over UDP, the standard port connect check won’t work. For UDP only SIP servers, set the check type to ping server.

12. Click Update.

**STEP 2 – DEFINE THE REAL SERVERS (RIPS)**
The Real Servers (i.e. the SIP servers) must now be associated with the VIP.

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:

<table>
<thead>
<tr>
<th>Label</th>
<th>SIP1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.10.20</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. SIP1.

4. Change the Real Server IP Address field to the required address, e.g. 192.168.10.20.

5. Click Update.

6. Repeat the above steps to add your other SIP server(s).

**STEP 3 – CONFIGURE FIREWALL MARKS**
To enable the Firewall Mark the following lines must be added to the firewall script:

```
VIP1="192.168.10.10"
iptables -t mangle -A PREROUTING -d $VIP1 --dport 5060 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -d $VIP1 --dport 5061 -j MARK --set-mark 1
```

This enables Firewall Mark ‘1’ to support both TCP & UDP on ports 5060 & 5061.
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](image)

   ![Firewall Script](image)

   ![Firewall Script](image)

4. Click **Update**

**STEP 4 – ADD THE FLOATING IP ADDRESS**

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. **192.168.10.10**

   ![Floating IPs](image)

3. Click **Add Floating IP**

**STEP 5 – SOLVE THE ARP PROBLEM**

As mentioned previously, DR mode works by changing the MAC address of the inbound packets to match the Real Server selected by the load balancing algorithm. To enable DR mode to operate:

- Each Real Server must be configured to accept packets destined for both the VIP address and the
Real Servers IP address (RIP). This is because in DR mode the destination address of load balanced packets is the VIP address, whilst for other traffic such as health-checks, administration traffic etc. it's the Real Server’s own IP address (the RIP). The service/process (e.g. IIS) must also respond to both addresses.

- Each Real Server must be configured so that it does not respond to ARP requests for the VIP address – only the load balancer should do this.

Configuring the Real Servers in this way is referred to as ‘Solving the ARP problem”. The exact steps required depend on the particular OS being used. For full details, please refer to the Administration Manual and search for “Solving the ARP Problem”.

TESTING & VERIFICATION

Check Server State
Using the System Overview in the WebUI, verify that the VIP and associated RIPs are up (green) as shown in the example below:

![System Overview](image)

Check Connectivity
Now test the load balancer by connecting clients to the VIP address (192.168.10.10 in this example configuration) rather than connecting users directly to the SIP servers.

RELATED QUICK REFERENCE GUIDES
The following guide may also be useful:

- Load Balancing Asterix in AWS

LOADBALANCER.ORG TECHNICAL SUPPORT
If you have any questions regarding the appliance or would like assistance designing your deployment, please don’t hesitate to contact our support team: support@loadbalancer.org.