Load Balancing SIP – Quick Reference Guide v1.3.1

About this Guide
This guide provides a quick reference for setting up SIP load balancing using Loadbalancer.org appliances.

SIP Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>UDP &amp; TCP</td>
</tr>
<tr>
<td>5061</td>
<td>UDP &amp; TCP</td>
</tr>
</tbody>
</table>

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

Load Balancer Configuration

N.B. the steps and screen shots are specific to v7.6 although they can also be used as a guideline for other versions of the appliance.

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 (Virtual Server), 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, see the section ‘Solving the ARP Problem’ later in this guide.
Virtual Service (VIP) Setup
Create a new VIP as described below – this is the IP address that clients will connect to. 'Firewall Marks' is used which enables the VIP to simultaneously support both TCP and UDP.

- Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Services and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>SIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>1</td>
</tr>
<tr>
<td>Ports</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Firewall Marks</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. **SIP**
- Change the Virtual Service IP Address field to a suitable reference for the Firewall Mark, e.g. **1**
- Leave the Virtual Service Ports field blank
• Set Protocol to Firewall Marks
• Leave the Forwarding Method set to Direct Routing
• Click Update
• Now click [Modify] next to the newly created VIP
• Ensure Persistence is enabled
• Change Check Type to Negotiate
• Set the Check Port to 5060 or 5061 as required
• Ensure that Protocol is set to SIP
• Click Update

Real Server (RIP) Setup
Real Servers (RIPs), i.e. the SIP Servers must now be defined for the Virtual Service already created.

• Using the WUI, go to Cluster Configuration > Layer 4 – Real Servers and click [Add a new Real Server] next to the newly created VIP
• 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>

  • Enter an appropriate label for the RIP, e.g. SIP1
  • Change the Real Server IP Address field to the required address, e.g. 192.168.10.20
  • Click Update
  • Repeat the above steps to add your other SIP server(s)
**Firewall Mark Setup**

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

VIP1="192.168.10.10"

```bash
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:

- Using the WUI, go to **Maintenance > Firewall Script**
- Scroll down to the Firewall Marks section
- Edit the example entries as shown below:

```
# Example: Associate HTTP and HTTPS with Firewall Mark 1:
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

# A Virtual Service may then be created in the web interface, using 1 as the
# service address.

# Packet Filtering

# You should always use a network perimeter firewall to lock down all
# external access to the load balancer except the required Virtual Services
# and the required services from your admin machine / network (SSH & HTTPS)

# Allow unlimited traffic on the loopback interface:
#iptables -A INPUT -i lo -j ACCEPT
#iptables -A OUTPUT -o lo -j ACCEPT
```

- Click **Update**
**Floating IP Address**

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

- Using the WUI, go to *Cluster Configuration > Floating IPs*
- Enter the required IP address, e.g. **192.168.10.10**

![Floating IP Configuration](image)

- Click *Add Floating IP*

**Solving the ARP Problem**

The steps required depend on the particular OS being used. For detailed steps on solving the ARP problem, please refer to the *administration manual*.

and search for “Solving the ARP Problem”.

**Testing & Verification**

Now test the load balancer by connecting clients to the VIP address (192.168.10.10 in this example configuration) instead of connecting users directly to the SIP servers.

**Loadbalancer.org Technical Support**

Don't hesitate to contact our support team if you need further assistance: [support@loadbalancer.org](mailto:support@loadbalancer.org)