Load Balancing Web Proxies
Load Balancing Web Filters
Load Balancing Web Gateways

Deployment Guide

rev. 1.5.4

Copyright © 2002 – 2016 Loadbalancer.org, Inc.
# Table of Contents

About this Guide................................................................................................................................................. 3
Loadbalancer.org Appliances Supported............................................................................................................. 3
Loadbalancer.org Software Versions Supported.................................................................................................... 3
Web Proxies / Filters................................................................................................................................................. 4
Benefits of Implementing a Load Balancer............................................................................................................. 4
Load Balancer Configuration Options..................................................................................................................... 4
  Layer 4 (Recommended)....................................................................................................................................... 4
    DR Mode - Direct Server Return Mode (Recommended)................................................................................... 4
    NAT Mode - Network Address Translation Mode............................................................................................. 4
  Layer 7 ................................................................................................................................................................... 5
    SNAT / HAPProxy Mode - Source Network Address Translation...................................................................... 5
Persistence - aka Server Affinity.................................................................................................................................. 5
  Source IP Address (Recommended)...................................................................................................................... 5
  Destination Hash.................................................................................................................................................... 5
Web Proxies / Filters Deployment Modes.................................................................................................................. 6
  1 – Proxy Mode (Recommended).......................................................................................................................... 6
  2 – Transparent Routed Proxy Mode..................................................................................................................... 6
Loadbalancer.org Appliance – the Basics.................................................................................................................... 7
  Initial Network Configuration.................................................................................................................................... 7
  Accessing the Web User Interface (WUI)............................................................................................................... 8
  Clustered Pair Configuration................................................................................................................................... 9
Option 1 - Proxy Mode (Recommended)................................................................................................................... 10
  Deployment Architecture......................................................................................................................................... 10
  Load Balancer Configuration................................................................................................................................... 11
    Create the Virtual Service (VIP)............................................................................................................................ 11
    Define the Real Servers (RIPs)............................................................................................................................. 12
  Web Proxy Appliance Configuration....................................................................................................................... 13
    Modify the Web Proxies to accept traffic for the VIP.............................................................................................. 13
    Web Proxy Operating Mode.................................................................................................................................... 13
  Client Configuration.................................................................................................................................................. 14
Option 2 - Transparent (Routed) Proxy Mode........................................................................................................... 15
  Deployment Architecture......................................................................................................................................... 15
  Load Balancer Configuration................................................................................................................................... 16
    Create the Virtual Service (VIP)............................................................................................................................ 16
    Add the Floating IP.................................................................................................................................................. 16
    Configure Appliance Firewall Rules.................................................................................................................... 17
    Define the Real Servers (RIPs)............................................................................................................................. 18
  Web Proxy Appliance Configuration....................................................................................................................... 19
    Web Proxy Operating Mode.................................................................................................................................... 19
  Router / Default Gateway Configuration............................................................................................................... 19
  Client Configuration.................................................................................................................................................. 19
Testing & Validation.................................................................................................................................................... 20
  Layer 4 – Current Connections.............................................................................................................................. 20
Technical Support..................................................................................................................................................... 21
Conclusion................................................................................................................................................................. 21
Appendix................................................................................................................................................................... 22
  1 – Clustered Pair Configuration – Adding a Slave Unit......................................................................................... 22
  2 – Modified Transparent Mode Firewall Rules..................................................................................................... 22
  3 – Company Contact Information....................................................................................................................... 23
About this Guide

This guide details the configuration of Loadbalancer.org appliances for deployment with Web Proxies / Filters. It includes typical topologies used and also steps on how to configure the appliances.

For an introduction on setting up the appliance as well as more technical information, please also refer to our quick-start guides and full administration manuals which are available at the following links:

**Version 7 Documentation**


**Version 8 Documentation**


Loadbalancer.org Appliances Supported

All our products can be used for load balancing Web Proxies / Filters. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td></td>
<td>Enterprise R320</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products](http://www.loadbalancer.org/products)

** Some features may not be supported, please check with Loadbalancer.org support

Loadbalancer.org Software Versions Supported

- V7.4.3 and later

*N.B. this guide includes configuration steps for v7.6 & later. For older versions of the appliance please contact Loadbalancer.org sales or support*
Web Proxies / Filters
Web Proxies / Filters provide a number of functions to permit organizations to control the way their staff access the Internet. These products are often appliance based and provide functionality including:

- Web Security & Control
- URL Filtering
- Content Caching
- Anti SPAM / Anti Malware / Anti Virus
- User Authentication
- High Availability

Benefits of Implementing a Load Balancer
Since secure, reliable and available Internet access is essential and not just a luxury, steps must be taken to ensure 100% up time. Loadbalancer.org appliances provide the perfect solution by allowing multiple Web Filter devices to be deployed in a load balanced and highly available cluster. Benefits include:

- **High-Availability** – If a Web Filter fails, service is not interrupted
- **Maintenance** – Web Filters can easily be taken out of the cluster for maintenance
- **Performance** – For additional performance simply add more Web Filters to the cluster

Load Balancer Configuration Options
The following sections describe the various load balancer configuration methods that are possible with web proxies.

Layer 4 (Recommended)

**DR Mode - Direct Server Return Mode (Recommended)**

In this mode, traffic from the client to the Web Proxy passes via the load balancer, return traffic passes directly back to the client which maximizes performance. Direct routing works by changing the destination MAC address of the incoming packet on the fly which is very fast. This mode is transparent by default meaning that the proxy sees the real client IP address and not the IP address of the load balancer.

Due to its speed, overall simplicity and effectiveness, Direct Routing (DR) mode with source IP persistence is our recommended method and can be used in both proxy mode & transparent (routed) proxy mode.

**NAT Mode - Network Address Translation Mode**

This mode requires the implementation of a two-arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works). The real servers (i.e. the Web Proxies) must have their default gateway configured to point at the load balancer. It offers high performance and like DR mode is transparent by default.
Layer 7

SNAT / HAProxy Mode - Source Network Address Translation

Using HAProxy in SNAT mode means that the load balancer is acting as a full proxy and therefore it doesn’t have the same raw throughput as the layer 4 methods. Also, this method is not transparent by default so the real servers will see the source address of each request as the load balancer’s IP address. This is generally not desirable although this can be resolved in two ways; either by reading the X-Forwarded-For header that’s included by default when using HAProxy, or by enabling Tproxy on the load balancer. The issues with using Proxy are that the default gateway on the real servers (i.e. the web proxies) must be changed to point as the load balancer and also it requires a two-arm infrastructure with two subnets which complicates the deployment.

SNAT mode does not have the raw throughput of the layer 4 solutions and is therefore not normally used for Web Filter / Proxy load balancing deployments.

Persistence - aka Server Affinity

Persistence may or may not be required and depends on the specific web proxy being used. Two possible methods are described in the following sections.

Source IP Address (Recommended)

Source IP persistence is the standard method and is appropriate for most requirements. When set, clients connecting from the same source IP address within the persistence timeout period (the default is 5 mins) will always be sent to the same web proxy.

Destination Hash

Another option at Layer 4 is to change the load balancing algorithm (i.e. the “scheduler”) to destination hash (DH). This causes the load balancer to select the proxy based on a hash of the destination IP address. This causes session requests to be directed at the same server based solely on the destination IP address of a packet which therefore makes client connections persistent for a particular Internet host.

Since this setting is a scheduler, the way connections are load balanced will also change. However it should still provide a well balanced distribution of client sessions between web proxy servers.
Web Proxy Deployment Modes

There are two implementation methods that are typically used – Proxy Mode & Transparent (Routed) Proxy Mode.

1 – Proxy Mode (Recommended)

This mode requires the load balancers VIP address to be defined in users browsers. This means that the load balancer will receive client requests and distribute these requests across the back-end web filters.

2 – Transparent Routed Proxy Mode

With this mode, client requests must be routed to the load balancer / proxy cluster. This can be achieved by either setting the default gateway on the client PCs to be the load balancer, or by adding rules to the default gateway device. Rules would typically be configured for HTTP & HTTPS traffic on ports 80 and 443.

NOTE: Various limitations relating to HTTPS inspection and client authentication may affect your particular web gateway appliance when deployed in transparent mode. Please check with your particular vendor to determine if this is the case and help choose the most appropriate deployment mode to use.
Loadbalancer.org Appliance – the Basics

Initial Network Configuration
The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

Method 1 - Using the Network Setup Wizard at the console
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Method 2 - Using the WUI:
Using a browser, connect to the WUI on the default IP address/port: **http://192.168.2.21:9080**
To set the IP address & subnet mask, use: **Local Configuration > Network Interface Configuration**
To set the default gateway, use: **Local Configuration > Routing**
To configure DNS settings, use: **Local Configuration > Hostname & DNS**

Method 3 - Using Linux commands:
At the console, set the initial IP address using the following command:

```
ip addr add <IP address>/<mask> dev eth0
e.g.
ip addr add 192.168.2.10/24 dev eth0
```

At the console, set the initial default gateway using the following command:

```
route add default gw <IP address> <interface>
e.g.
rout e add default gw 192.168.2.254 eth0
```

At the console, set the DNS server using the following command:

```
echo nameserver <IP address> >> /etc/resolv.conf
e.g.
echo nameserver 192.168.2.250 >> /etc/resolv.conf
```

N.B. If method 3 is used, you must also configure these settings using the WUI, otherwise the settings will be lost after a reboot
**Accessing the Web User Interface (WUI)**

The WUI can be accessed from a browser at:  

*Note the port number → 9080

(replace 192.168.2.21 with the IP address of your load balancer if its been changed from the default)

*Username:* loadbalancer  
*Password:* loadbalancer

Once you have entered the logon credentials the Loadbalancer.org Web User Interface will be displayed as shown below:
The screen shot below shows the v7.6 WUI once logged in:

**Clustered Pair Configuration**

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix.

**NOTE:** It's highly recommended that you have a working Web Proxy / Filter environment first before implementing the load balancer.
Option 1 - Proxy Mode (Recommended)

Deployment Architecture

- Browser settings on client PC’s must be changed to point at the Virtual Service (VIP) on the load balancer
- The load balancer is configured in Layer 4 DR mode
- The Web Proxies must be configured to accept traffic for the VIP (see page 13)
- Typically, two Loadbalancer.org appliances are deployed for resilience – this is our recommended configuration
Load Balancer Configuration

Create the Virtual Service (VIP)

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

  ![Virtual Service Configuration](image)

  - Enter an appropriate label (name) for the VIP, e.g. *Proxy*
  - Set the *Virtual Service IP address* field to the required IP address, e.g. *192.168.2.202*
  - Set the *Virtual Service Ports* field to the required port, e.g. *8080*
  - Ensure that *Protocol* is set to *TCP*
  - Ensure that *Forwarding Method* is set to *Direct Routing*
  - Click *Update*
  - Now click [*Modify*] next to the newly created VIP
  - Ensure *Persistence* is enabled and set *Persistence Timeout* to *3600* (i.e. 1 hour)
  - Click *Update*
Define the Real Servers (RIPs)

- Using the WUI go to *Cluster Configuration > Layer 4 – Real Servers*
- Click *[Add a new Real Server]* next to the newly created VIP
- Enter the following details:

  ![Real Server Configuration Form](image)

- Enter an appropriate label (name) for the first Proxy Server, e.g. *Proxy1*
- Change the *Real Server IP Address* field to the required IP address, e.g. *192.168.2.210*
- Click *Update*
- Repeat the above steps to add your other Proxy Server(s)
Web Proxy Appliance Configuration

Modify the Web Proxies to accept traffic for the VIP

As mentioned previously, DR mode is our recommended load balancer operating mode. To use this mode, changes are required to the real servers, i.e. the web proxies. The real servers must accept traffic for the VIP, but they must not respond to any ARP requests for that IP, only the VIP should do this.

To configure a Linux based web proxy appliance to accept traffic for the VIP the following line must be added to the rc.local startup script on each proxy:

```
iptables -t nat -A PREROUTING -p tcp -d <VIP address> -j REDIRECT
```

e.g.
```
iptables -t nat -A PREROUTING -p tcp -d 192.168.2.202 -j REDIRECT
```

i.e. Redirect any incoming packets destined for the VIP to the local address

N.B. For more information please to the administration manuals and search for ‘ARP Problem’

NOTE: Vendors such as Bloxx and Smoothwall have options in their Web User Interface that allow this to be easily configured, so command line entries are not required. Please consult your specific vendor or loadbalancer.org for more information.

Web Proxy Operating Mode

Typically there is setting on the web proxy to allow the selection of either client configured proxy or routed / transparent proxy. In this case, this should be set to Client Configured Proxy.

Please note the exact terminology does vary between vendors so please check your specific appliance.
Client Configuration

Client browser settings must be set so that browsers connect via the VIP. In a Microsoft based LAN environment, this is typically achieved using AD group policy.

![Local Area Network (LAN) Settings](image1)

![Proxy Settings](image2)

*Server Configuration*
**Option 2 - Transparent (Routed) Proxy Mode**

**Deployment Architecture**

![Deployment Architecture Diagram]

**Notes**

- Rules must be added to the router so that the required traffic (typically HTTP & HTTPS on port 80 & 443) is sent transparently to the load balancer, please see page 19 for example rules for a Linux router.
- As with non-transparent mode, the load balancer is configured in Layer 4 DR mode.
- Firewall rules must be added to the load balancer to transparently send traffic to the proxies (see page 17).
- Typically, two Loadbalancer.org appliances are deployed for resilience – this is our recommended configuration.
Load Balancer Configuration

Create the Virtual Service (VIP)

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

<table>
<thead>
<tr>
<th>Label</th>
<th>Proxy</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>Firewall Marks</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
</tbody>
</table>

- Enter an appropriate label (name) for the VIP, e.g. **Proxy**
- Change the Virtual Service IP address field to **1**
  - *N.B. This is the reference number for the ‘Firewall Mark’. The same reference number is used when configuring the firewall rules – please see page 17 for more details*
- Leave the Virtual Service Ports field blank, the ports are defined in the firewall rules on page 17
- Ensure that Protocol is set to **Firewall Marks**
  - *N.B. the ports field will be disabled when this is done*
- Ensure that Forwarding Method is set to **Direct Routing**
- Click Update
- Now click [Modify] next to the newly created VIP
- Ensure Persistence is enabled and set Persistence Timeout to **3600** (i.e. 1 hour)
- Under the Health Checks section change Check Type to **Ping Server**
- Click Update

Add the Floating IP

- Using the WUI, go to *Cluster Configuration > Floating IPs*
• Enter an appropriate IP address for the Virtual Service, e.g. **192.168.2.202**
• Click **Update**

**Configure Appliance Firewall Rules**

• Using the WUI, go to **Maintenance > Firewall Script**
• Scroll down to the Firewall Marks section
• Add the following lines to this section as shown in the screen shot below:

```bash
iptables -t mangle -A PREROUTING -p tcp --dport 80 --j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp --dport 443 --j MARK --set-mark 1
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100
```

_N.B. Please see section 2 in the Appendix if you intend to forward ALL traffic to the web proxies_
• Click Update

**Define the Real Servers (RIPs)**

• Using the WUI go to *Cluster Configuration > Layer 4 – Real Servers*
• Click [Add a new Real Server] next to the newly created VIP
• Enter the following details:

- Enter an appropriate label (name) for the first Proxy Server, e.g. *Proxy1*
- Change the *Real Server IP Address* field to the required IP address, e.g. *192.168.2.210*
- Click Update
- Repeat the above steps to add your other Proxy Server(s)
Web Proxy Appliance Configuration

Web Proxy Operating Mode

Typically there is a setting on the web proxy to allow the selection of either client configured proxy or routed / transparent proxy. In this case, this should be set to Routed / Transparent Proxy. Please note the exact terminology does vary between vendors so please check your specific appliance.

NOTE: When using transparent routed mode, it's not necessary to modify the Web Filter to accept traffic destined for the VIP, this is only required when using proxy mode.

Router / Default Gateway Configuration

Depending on your network configuration, rules must be added to the router/default gateway so that all required traffic (typically HTTP & HTTPS on port 80 & 443) is sent to the floating IP address on the load balancer. The load balancer then distributes this traffic between the web proxy servers.

Example iptables rules for a Linux based router:

```bash
SUBNET="192.168.2.0/24"
FWMARK="5"
TABLE="10"
LOADBALANCER ="192.168.2.202"
iptables -t mangle -A PREROUTING -s $SUBNET -p tcp --dport 80 -j MARK --set-mark $FWMARK
iptables -t mangle -A PREROUTING -s $SUBNET -p tcp --dport 443 -j MARK --set-mark $FWMARK
ip route add default via $LOADBALANCER dev eth3 table $TABLE
ip rule add fwmark $FWMARK table $TABLE
```

This example uses policy routing via firewall marks. This works by first selecting and marking the packets we want to be sent to the proxy, i.e. all packets on port 80. Then, when the kernel goes to make a routing decision, the marked packets aren't routed using the normal routing table, instead via table 10 in this case. Table 10 has only one entry: route packets to the web proxy.

N.B. This is required when no changes have been made to the clients gateway settings

Client Configuration

If rules are configured on the router as described in the section above, no client change are required. If such rules are not configured, then the default gateway on the client PCs must be modified to be the load balancer.
Testing & Validation

To verify that the traffic is passing through the load balancer correctly the following reporting options can be used:

System Overview

Reports > Layer 4 Status

Reports > Layer 4 Current Connections

Several reporting and dashboard options are also available on the web proxies, for this please refer to your specific vendors documentation.

Layer 4 – Current Connections

Proxy Mode

The example screen shot below illustrates that the test client (192.168.64.7) sends requests to the VIP (192.168.111.88), the load balancer then forwards the request onto the Web Filter / Gateway (192.168.64.60).

<table>
<thead>
<tr>
<th>IPVS connection entries</th>
<th>source</th>
<th>virtual</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 13:07</td>
<td>192.168.64.7:3565</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:05</td>
<td>192.168.64.7:3569</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:03</td>
<td>192.168.64.7:3541</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:05</td>
<td>192.168.64.7:3570</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:07</td>
<td>192.168.64.7:3567</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:03</td>
<td>192.168.64.7:3572</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:05</td>
<td>192.168.64.7:3560</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:03</td>
<td>192.168.64.7:3561</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:03</td>
<td>192.168.64.7:3571</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:07</td>
<td>192.168.64.7:3566</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 02:55</td>
<td>NONE</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:03</td>
<td>192.168.64.7:3564</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
<tr>
<td>TCP 13:03</td>
<td>192.168.64.7:3568</td>
<td>192.168.111.88:8080</td>
<td>192.168.64.60:8080</td>
</tr>
</tbody>
</table>
**Transparent Mode**

The example screen shot below illustrates the difference when running in transparent mode.

![Layer 4 Current Connections](image)

**Technical Support**

For more details or assistance with your deployment please don’t hesitate to contact the support team at the following email address: support@loadbalancer.org

**Conclusion**

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Web Proxy/Filter environments.
Appendix

1 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant document referenced below for more details:

Version 7
Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8
Please refer to Chapter 9 – Appliance Clustering for HA in the v8 Administration Manual.

2 – Modified Transparent Mode Firewall Rules

If ALL traffic is to be forwarded to the web proxies, the firewall rules below should be used rather than the rules on page 17, i.e.:

Replace:

```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp --dport 443 -j MARK --set-mark 1
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100
```

With:

```
iptables -t mangle -A PREROUTING -p tcp -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p udp -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp -d <LB-IP> -j MARK --set-mark 2
iptables -t mangle -A PREROUTING -p udp -d <LB-IP> -j MARK --set-mark 2
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100
```

Notes:

- `<LB-IP>` should be replaced with the base IP address of the load balancer (typically eth0), this is the address used by heartbeat and for administration purpose

- If these modified firewall rules are used, then either the default gateway for client PC’s should be changed to be the load balancer, or the rules on the router should be changed to forward all traffic to the load balancer

- This will only work for TCP and UDP traffic. So for example, ICMP and some VPN technologies will not work because the load balancer only supports TCP and UDP.

Don’t hesitate to contact our support team if you need further assistance: support@loadbalancer.org
### Website
URL: [www.loadbalancer.org](http://www.loadbalancer.org)

### North America (US)
Loadbalancer.org, Inc.
270 Presidential Drive
Wilmington,
DE 19807
USA
Tel: +1 888.867.9504 (24x7)
Fax: +1 302.213.0122
Email (sales): sales@loadbalancer.org
Email (support): support@loadbalancer.org

### North America (Canada)
Loadbalancer.org Ltd.
300–422 Richards Street
Vancouver, BC
V6B 2Z4
Canada
Tel: +1 855.681.6017 (24x7)
Fax: +1 302.213.0122
Email (sales): sales@loadbalancer.org
Email (support): support@loadbalancer.org

### Europe (UK)
Loadbalancer.org Ltd.
Portsmouth Technopole
Kingston Crescent
Portsmouth
PO2 8FA
England, UK
Tel: +44 (0)330 3801064 (24x7)
Fax: +44 (0)870 4327672
Email (sales): sales@loadbalancer.org
Email (support): support@loadbalancer.org

### Europe (Germany)
Loadbalancer.org GmbH
Alt Pempelfort 2
40211 Düsseldorf
Germany
Tel: +49 (0)30 920 383 6494
Fax: +49 (0)30 920 383 6495
Email (sales): vertrieb@loadbalancer.org
Email (support): support@loadbalancer.org