# Table of Contents

About this Guide.................................................................................................................. 3
Loadbalancer.org Appliances Supported............................................................................. 3
Loadbalancer.org Software Versions Supported................................................................. 3
Smoothwall Web Gateway Appliances Supported............................................................... 3
Loadbalancer.org & Smoothwall........................................................................................... 4
Benefits of Implementing a Load Balancer.......................................................................... 4
Load Balancer Configuration Options................................................................................ 4
Layer 4.................................................................................................................................. 4
  DR Mode - Direct Server Return Mode (Recommended).................................................. 4
  NAT Mode - Network Address Translation Mode............................................................ 4
Persistence - aka Server Affinity.......................................................................................... 4
  Source IP Address (Recommended)................................................................................ 5
  Destination Hash............................................................................................................. 5
Web Gateway Deployment Modes....................................................................................... 5
  1 – Non Transparent Proxy Mode (Recommended).......................................................... 5
  2 – Transparent Routed Proxy Mode.............................................................................. 5
Loadbalancer.org Appliance – the Basics......................................................................... 6
Initial Network Configuration.............................................................................................. 6
Accessing the Web User Interface (WUI)........................................................................... 7
Clustered Pair Configuration............................................................................................... 8
Option 1 - Proxy Mode (Recommended)............................................................................ 9
Deployment Architecture.................................................................................................. 9
Load Balancer Configuration.............................................................................................. 10
  Create the Virtual Service (VIP).................................................................................... 10
  Define the Real Servers (RIPs)..................................................................................... 11
Web Gateway Configuration.............................................................................................. 12
  Modify the Web Gateways to accept traffic for the VIP.............................................. 12
  Using the Smoothwall WUI......................................................................................... 12
  Web Gateway Operating Mode..................................................................................... 12
  Proxy Port Configuration............................................................................................... 13
Client Configuration.......................................................................................................... 13
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 Gateway Configuration.............................................................................................. 19
  Web Gateway Operating Mode..................................................................................... 19
  Router / Default Gateway Configuration.................................................................... 20
Client Configuration.......................................................................................................... 20
Testing & Validation............................................................................................................ 21
Layer 4 – Current Connections......................................................................................... 21
Technical Support............................................................................................................. 22
Conclusion.......................................................................................................................... 22
Appendix............................................................................................................................. 23
  1 – Clustered Pair Configuration – Adding a Slave Unit........................................... 23
  2 – Modified Transparent Mode Firewall Rules......................................................... 23
  3 – Loadbalancer.org Company Contact Information.............................................. 24
  4 – Smoothwall Company Contact Information....................................................... 25
About this Guide

This guide details the configuration of Loadbalancer.org appliances for deployment with Smoothwall’s range of Web Gateway products. It includes recommended deployment topologies and also steps on how to configure the appliances.

For an introduction on setting up the load balancer as well as more technical information, please also refer to the 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 Smoothwall Web Gateway. 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
** 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

Smoothwall Web Gateway Appliances Supported

- All versions
Loadbalancer.org & Smoothwall
Loadbalancer.org and Smoothwall have partnered to provide high performance, robust and highly available Web Filtering solutions that enable customers to deploy with confidence.

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 Gateway devices to be deployed in a load balanced and highly available cluster. Benefits include:

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

Load Balancer Configuration Options
The following sections describe the various load balancer configuration methods that are possible when load balancing Smoothwall Web Gateways.

**Layer 4**

**DR Mode - Direct Server Return Mode (Recommended)**
In this mode, traffic from the client to the Web Gateway 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 Web Gateway 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 Gateways) must have their default gateway configured to be the load balancer. It offers high performance and like DR mode is transparent by default.

**Persistence - aka Server Affinity**
Persistence may or may not be required and depends on the specific Web Gateway 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 Gateway. It’s recommended that this should be set to 1 hour minimum.

**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 Gateway servers.

**Web Gateway Deployment Modes**

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

1 – **Non Transparent 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 / Web Gateway 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.
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.
route 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:  \texttt{http://192.168.2.21:9080/lbadmin}

* 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)

\begin{itemize}
  \item \textbf{Username:} loadbalancer
  \item \textbf{Password:} loadbalancer
\end{itemize}

Once you have entered the logon credentials the Loadbalancer.org Web User Interface will be displayed as shown below:
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 Gateway environment first before implementing the load balancer.
Option 1 - Proxy Mode (Recommended)

**Deployment Architecture**

- **Client PC 1**
- **Client PC 2**
- **Client PC n**
- **Default Gateway**
- **Router**
- **Firewall**
- **Internet**
- **Load Balancer 1 (master)**
- **Load Balancer 2 (slave)**
- **Smoothwall Web Filter 1**
- **Smoothwall Web Filter 2**

**Notes**

- Browser settings on client PC’s must be changed to point at the Virtual Service (VIP) on the load balancer
- The load balancer(s) must be configured in Layer 4 DR mode
- The Smoothwall Web Gateways must be configured to accept traffic for the VIP (see page 12)
- 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>192.168.2.202</td>
</tr>
<tr>
<td>Ports</td>
<td>8080</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</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**
- 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:

<table>
<thead>
<tr>
<th>Label</th>
<th>Proxy1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.2.210</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 (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 Web Gateway(s)
Web Gateway Configuration

Modify the Web Gateways to accept traffic for the VIP

Concept
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 Gateways. 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.

Using the Smoothwall WUI
To configure the Smoothwall appliance for load balancing use the WUI option: Web Proxy > Settings > Advanced, then enter the required Virtual Service (VIP) IP address as shown below:

Web Gateway Operating Mode
The Smoothwall Web Gateway can easily be configured for client configured proxy mode using the policy wizard.
Use the WUI option: Web Proxy > Authentication > Policy Wizard

Now click next to run through the wizard and configure the remaining settings and apply the policy
Proxy Port Configuration

The required proxy port can be set using the WUI option: Web Proxy > Authentication > Policy Wizard as shown below:

Now click **next** to run through the wizard and configure the remaining settings and apply the policy.

*N.B. The default proxy port for Smoothwall Web Gateway is 800*

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.

It's recommended that a FQDN is used to define the proxy server rather than an IP address.
Option 2 - Transparent (Routed) Proxy Mode

**Deployment Architecture**

- Client PC 1
- Client PC 2
- Client PC n
- Default Gateway *(see notes below)*
  - Router
  - Firewall
  - Internet
  - Load Balancer 1 *(master)*
  - Load Balancer 2 *(slave)*
  - Heartbeat
  - Smoothwall Web Filter 1
  - Smoothwall Web Filter 2

**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 20 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 Web Gateways *(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</td>
<td></td>
</tr>
<tr>
<td>Firewall Mark identifier</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*
- The **Virtual Service Ports** field does not need to be completed in this case and is therefore disabled
- Ensure that **Protocol** is set to **Firewall Marks**
- 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*
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:

<table>
<thead>
<tr>
<th>Label</th>
<th>Proxy1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.2.210</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 (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 Web Gateway(s)
Web Gateway Configuration

Web Gateway Operating Mode

The Smoothwall Web Gateway can easily be configured for transparent mode using the policy wizard. Use the WUI option: Web Proxy > Authentication > Policy Wizard as shown below:

Now click next to run through the wizard and configure the remaining settings and apply the policy.

NOTE: When using transparent routed mode, it's not necessary to modify the Web Gateway to accept traffic destined for the VIP, this is only required when using proxy mode. However, it's still recommended to configure this so both modes are catered for from the start.
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:

```
SUBNET="192.168.2.0/24"
FWMARK="5"
TABLE="10"
LOADBALANCER ="192.168.2.202"
iptables -t mangle -A PREROUTING -s $CLIENT -p tcp --dport 80 -j MARK --set-mark $FWMARK
iptables -t mangle -A PREROUTING -s $CLIENT -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 Gateway (192.168.64.60).

```
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
| Source                          | Virtual Address                 | Destination                     | Prostate                        |
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
| 192.168.64.7:3565               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3563               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3541               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3570               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3567               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3572               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3560               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3561               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3571               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3566               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3569               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
| 192.168.64.7:3569               | 192.168.111.88:8080             | 192.168.64.60:8080              | ESTABLISHED                     |
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
Transparent Mode

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

<table>
<thead>
<tr>
<th>Layer 4 Current Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Status</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPVS connection entries</th>
<th>source</th>
<th>virtual</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 00:41 FIN_WAIT</td>
<td>192.168.64.7:5774</td>
<td>70.42.56.98:80</td>
<td>192.168.64.60:80</td>
</tr>
<tr>
<td>TCP 00:15 FIN_WAIT</td>
<td>192.168.64.7:5758</td>
<td>74.208.104.65:80</td>
<td>192.168.64.60:80</td>
</tr>
<tr>
<td>TCP 14:19 ESTABLISHED</td>
<td>192.168.64.7:5681</td>
<td>98.188.129.145:80</td>
<td>192.168.64.60:80</td>
</tr>
<tr>
<td>TCP 00:50 FIN_WAIT</td>
<td>192.168.64.7:5779</td>
<td>70.42.56.98:80</td>
<td>192.168.64.60:80</td>
</tr>
<tr>
<td>TCP 00:47 FIN_WAIT</td>
<td>192.168.64.7:5770</td>
<td>70.42.56.98:80</td>
<td>192.168.64.60:80</td>
</tr>
<tr>
<td>TCP 14:35 ESTABLISHED</td>
<td>192.168.64.7:5679</td>
<td>176.34.178.134:80</td>
<td>192.168.64.60:80</td>
</tr>
<tr>
<td>TCP 14:35 ESTABLISHED</td>
<td>192.168.64.7:5691</td>
<td>178.136.8.70:80</td>
<td>192.168.64.60:80</td>
</tr>
</tbody>
</table>

Many reporting and dashboard options are also available in the Smoothwall Web Gateway user interface. For more details please refer to the appropriate Smoothwall documentation available at the following link: http://www.smoothwall.net/get-support/product-manuals/swg-manuals

Technical Support

Loadbalancer.org support: support@loadbalancer.org
Smoothwall support: support@smoothwall.net

Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Smoothwall Web Gateway 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
<table>
<thead>
<tr>
<th>Region</th>
<th>Address</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Website</strong></td>
<td>URL: <a href="http://www.loadbalancer.org">www.loadbalancer.org</a></td>
<td></td>
</tr>
</tbody>
</table>
| **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 Dusseldorf  
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 |                                                   |
### Smoothwall Company Contact Information

<table>
<thead>
<tr>
<th>Website</th>
<th>URL: <a href="http://www.smoothwall.net">www.smoothwall.net</a></th>
</tr>
</thead>
</table>
| **UK & International** | Tel (sales): +44 (0) 870 1 999 500  
Email (sales): sales@smoothwall.net  
Tel (support): +44 (0) 800 5 999 041  
Email (support): support@smoothwall.net |
| **USA** | Tel (sales): 1-800-959-3760  
Email (sales): sales@smoothwall.net  
Tel (support): 1-800-959-1261  
Email (support): support@smoothwall.net |