LOADBALANCER

DEPLOYMENT GUIDE

# Load Balancing Smoothwall Secure Web Gateway

Version 1.6.0

# Table of Contents

# 1. About this Guide

This guide details the steps required to configure a load balanced Smoothwall Secure Web Gateway environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Smoothwall Secure Web Gateway configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

# 2. Loadbalancer.org Appliances Supported

All our products can be used with Smoothwall Secure Web Gateway. For full specifications of available models please refer to https://www.loadbalancer.org/products.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

# 3. Software Versions Supported

## 3.1. Loadbalancer.org Appliance

- V8.9.1 and later

> **Note** The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

## 3.2. Smoothwall Web Gateway

- All versions

# 4. 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.

# 5. Benefits of Implementing a Load Balancer

Implementing Loadbalancer.org appliances enables multiple Smoothwall Web Gateways to be deployed in a cluster. This provides the following key benefits:

- **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

# 6. Load Balancer Configuration Options

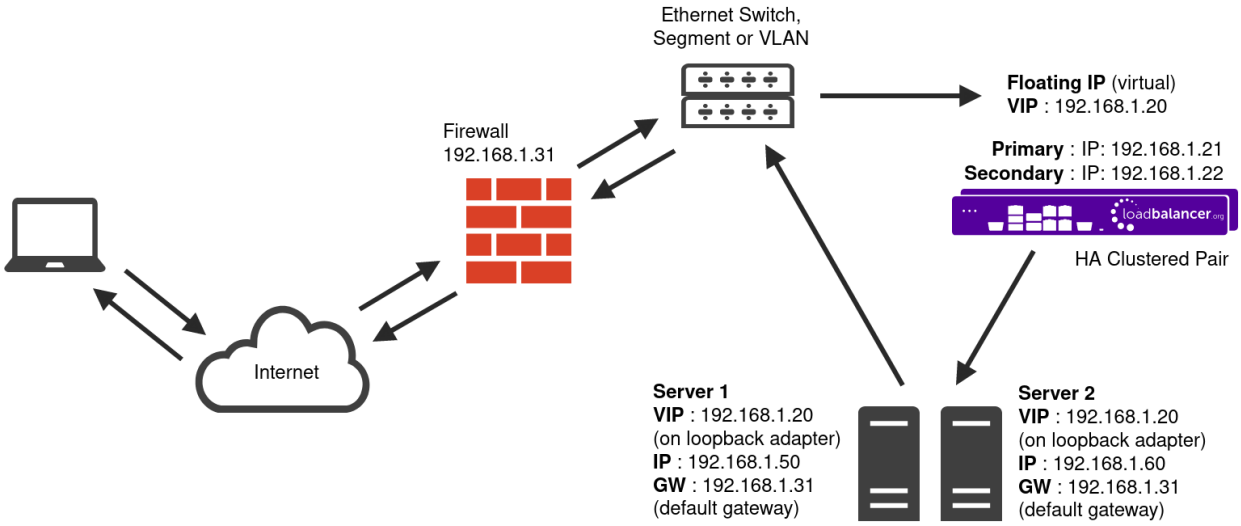
The following sections describe the various load balancer deployment modes and persistence options that are used when load balancing Smoothwall Web Gateways.

## 6.1. Deployment Modes

### Layer 4 DR Mode

Layer 4 DR (Direct Routing) mode is a very high performance solution that requires little change to your existing infrastructure.

> **Note** Kemp, Brocade, Barracuda & A10 Networks call this ***Direct Server Return*** and F5 call it ***nPath***.

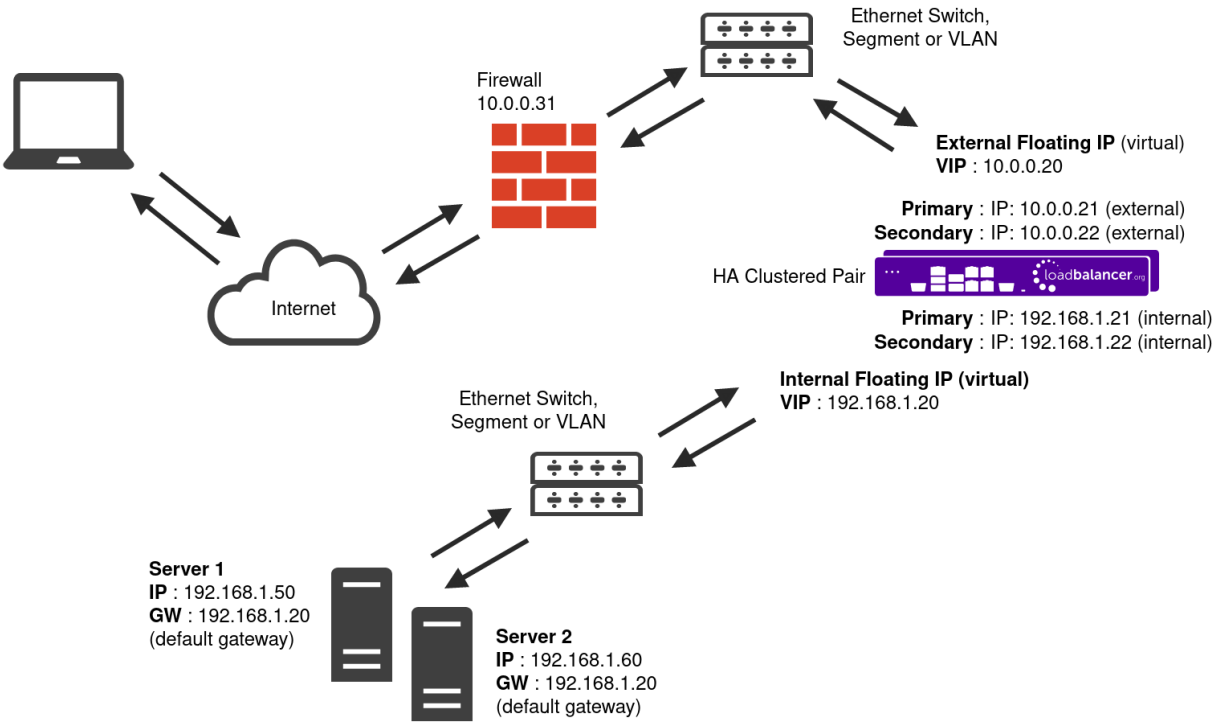



- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the load balanced application) must respond to both the Real Server's own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Server in this way is referred to as "Solving the ARP Problem". For more information please refer to DR Mode Considerations.
- On average, DR mode is 8 times quicker than NAT mode for HTTP and much faster for other applications such as Remote Desktop Services, streaming media and FTP.
- The load balancer must have an interface in the same subnet as the Real Servers to ensure layer 2 connectivity which is required for DR mode to operate.
- The VIP can be brought up on the same subnet as the Real Servers or on a different subnet provided that the load balancer has an interface in that subnet.
- Port translation is not possible with DR mode, e.g. VIP:80 → RIP:8080 is not supported.

- DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

## Layer 4 NAT Mode

Layer 4 NAT mode is a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode.




- The load balancer translates all requests from the Virtual Service to the Real Servers.
- NAT mode can be deployed in the following ways:
  - **Two-arm (using 2 Interfaces)** (as shown above) - Here, 2 subnets are used. The VIP is located in one subnet and the load balanced Real Servers are located in the other. The load balancer requires 2 interfaces, one in each subnet.

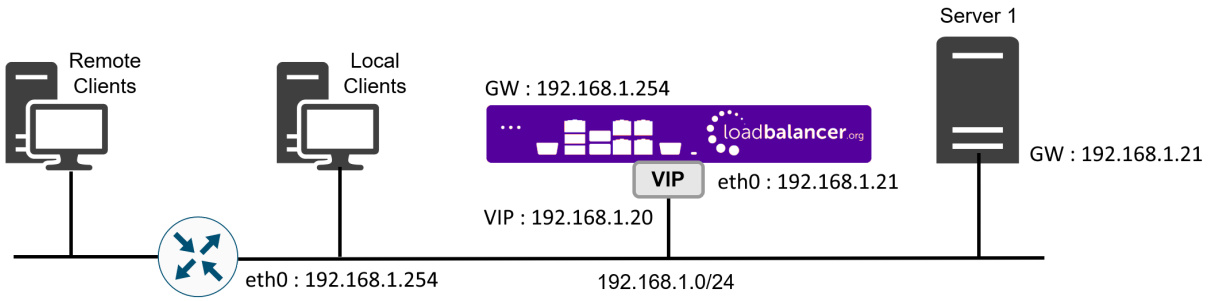
> **Note** This can be achieved by using two network adapters, or by creating VLANs on a single adapter.

    - Normally **eth0** is used for the internal network and **eth1** is used for the external network although this is optional. Any interface can be used for any purpose.
    - If the Real Servers require Internet access, *Auto-NAT* should be enabled using the WebUI menu option: *Cluster Configuration > Layer 4 - Advanced Configuration*, the external interface should be selected.
    - The default gateway on the Real Servers must be set to be an IP address on the load balancer.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

- Clients can be located in the same subnet as the VIP or any remote subnet provided they can route to the VIP.

- **One-arm (using 1 Interface)** - Here, the VIP is brought up in the same subnet as the Real Servers.




  - To support remote clients, the default gateway on the Real Servers must be an IP address on the load balancer and routing on the load balancer must be configured so that return traffic is routed back via the router.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

  - To support local clients, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer. For more information please refer to One-Arm (Single Subnet) NAT Mode.

- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this.
- Port translation is possible with Layer 4 NAT mode, e.g. VIP:80 → RIP:8080 is supported.
- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.

### NAT Mode Packet re-Writing

In NAT mode, the inbound destination IP address is changed by the load balancer from the Virtual Service IP address (VIP) to the Real Server. For outbound replies the load balancer changes the source IP address of the Real Server to be the Virtual Services IP address.

**The following table shows an example NAT mode setup:**

| Protocol | VIP | Port | RIP | Port |
|---|---|---|---|---|
| TCP | 10.0.0.20 | 80 | 192.168.1.50 | 80 |

In this simple example all traffic destined for IP address 10.0.0.20 on port 80 is load-balanced to the real IP address 192.168.1.50 on port 80.

**Packet rewriting works as follows:**

1) The incoming packet for the web server has source and destination addresses as:

| | | | |
|---|---|---|---|
| **Source** | x.x.x.x:34567 | **Destination** | 10.0.0.20:80 |

2) The packet is rewritten and forwarded to the backend server as:

| | | | |
|---|---|---|---|
| **Source** | x.x.x.x:34567 | **Destination** | 192.168.1.50:80 |

3) Replies return to the load balancer as:

| | | | |
|---|---|---|---|
| **Source** | 192.168.1.50:80 | **Destination** | x.x.x.x:34567 |

4) The packet is written back to the VIP address and returned to the client as:

| | | | |
|---|---|---|---|
| **Source** | 10.0.0.20:80 | **Destination** | x.x.x.x:34567 |

## 6.2. Persistence / 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 default option for Layer 4 services. When set, clients connecting from the same source IP address within the persistence timeout period (the default is 5 minutes) 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 Web Gateway 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 the Web Gateways.

# 7. Web Gateway Deployment Modes

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

## 7.1. 1 – Explicit Proxy Mode (Recommended)

This mode requires the load balancer's 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 Gateways.

Smoothwall refer to this as "Non-Transparent Mode". Please refer to the section Option 1 – Explicit Proxy Mode (Recommended) for configuration details.

### 7.2. 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. Smoothwall refer to this as "Transparent Mode". Please refer to the section Option 2 - Transparent Routed Proxy Mode for configuration details.

## 8. Summary of Deployment Options

| Option | Web Gateway Mode | Load Balancer Mode | Notes |
|---|---|---|---|
| Option 1A<br><br>(Recommended) | Non-Transparent Mode | DR Mode | The Web Gateways must be configured to accept traffic for the VIP.<br><br>Please refer to Option 1 – Explicit Proxy Mode (Recommended) for configuration details. |
| Option 1B | Non-Transparent Mode | NAT Mode | The load balancer must be set as the default gateway for the Web Gateways.<br><br>Please refer to Option 1B – Using NAT Mode for configuration details. |
| Option 1C | Non-Transparent Mode | NAT Mode | A static route must be configured on the Web Gateways to send client return traffic back via the load balancer.<br><br>Please refer to Option 1C – Using NAT Mode (Preferred NAT Topology) for configuration details. |

| Option | Web Gateway Mode | Load Balancer Mode | Notes |
|---|---|---|---|
| Option 2 | Transparent Mode | DR Mode | Firewall rules must be added to the load balancer to transparently send traffic to the Web Gateways.<br><br>Please refer to Option 2 - Transparent Routed Proxy Mode for configuration details. |

# 9. Loadbalancer.org Appliance – the Basics

## 9.1. Virtual Appliance

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.

> **Note** The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

> **Note** Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

> **Note** The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

## 9.2. Initial Network Configuration

After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS servers and other network and administrative settings.

> **Important** Be sure to set a secure password for the load balancer, when prompted during the setup routine.

## 9.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

> **Note** There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

1. Using a browser, navigate to the following URL:

   **https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/**

   > **Note** You'll receive a warning about the WebUI's SSL certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

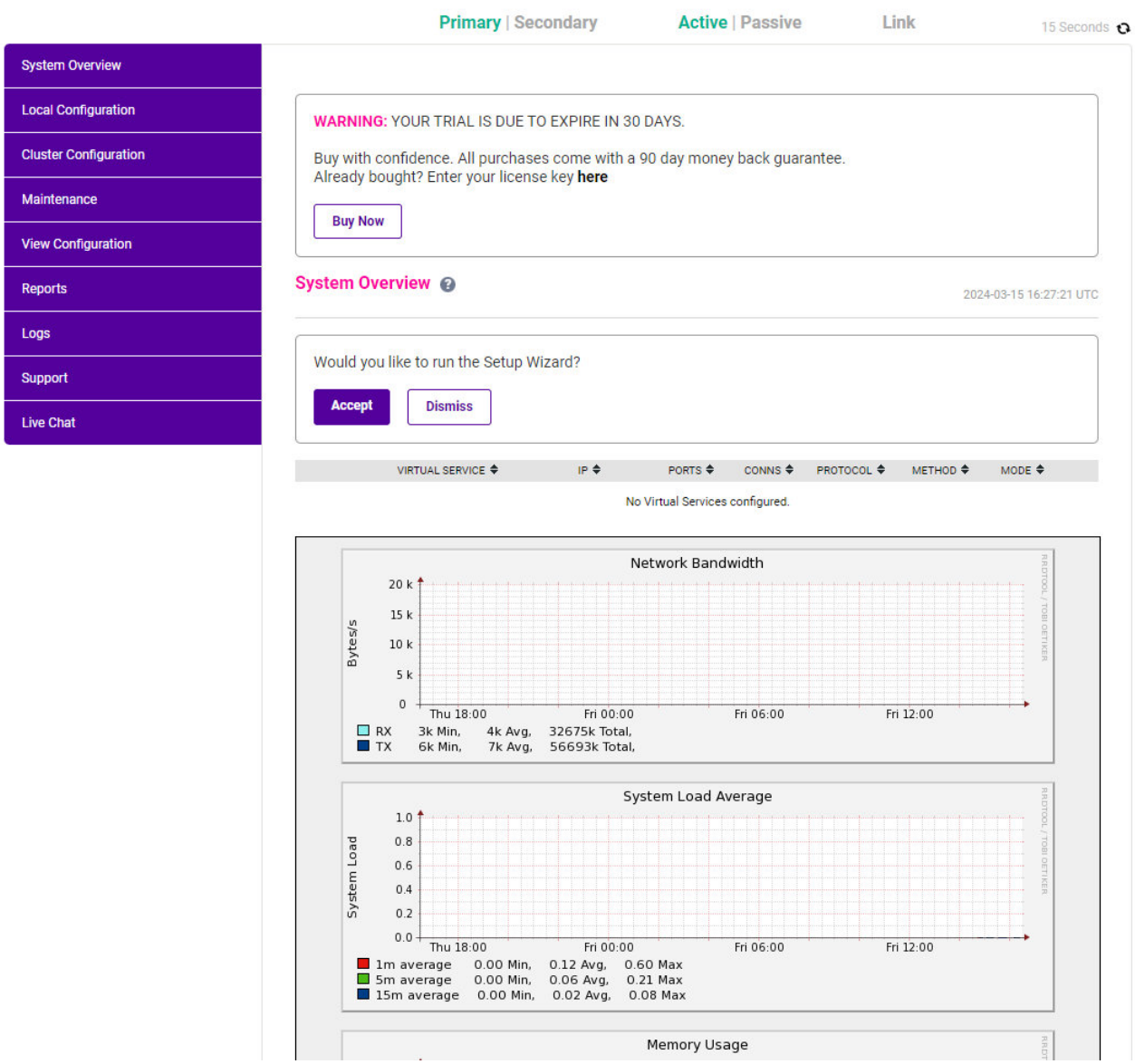
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

2. Log in to the WebUI using the following credentials:

   **Username**: loadbalancer
   **Password**: <configured-during-network-setup-wizard>

   > **Note** To change the password, use the WebUI menu option: ***Maintenance > Passwords.***

   Once logged in, the WebUI will be displayed as shown below:




3. You'll be asked if you want to run the Setup Wizard which can be used to configure layer 7 services. Click **Dismiss** if you're following a guide or want to configure the appliance manually or click **Accept** to start the wizard.

## Main Menu Options

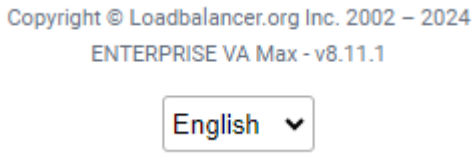
**System Overview** - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
**Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.
**Cluster Configuration** - Configure load balanced services such as VIPs & RIPs
**Maintenance** - Perform maintenance tasks such as service restarts and taking backups
**View Configuration** - Display the saved appliance configuration settings
**Reports** - View various appliance reports & graphs
**Logs** - View various appliance logs
**Support** - Create a support download, contact the support team & access useful links
**Live Chat** - Start a live chat session with one of our Support Engineers

## 9.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

### Determining the Current Software Version

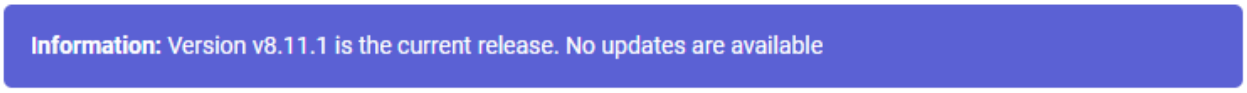
The software version is displayed at the bottom of the WebUI as shown in the example below:




### Checking for Updates using Online Update

> **Note** By default, the appliance periodically contacts the Loadbalancer.org update server and checks for updates. An update check can also be manually triggered as detailed below.

1. Using the WebUI, navigate to: ***Maintenance > Software Update***.
2. Select **Online Update**.
3. If the latest version is already installed, a message similar to the following will be displayed:




4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click **Online Update** to start the update process.

> **Note** Do not navigate away whilst the update is ongoing, this may cause the update to fail.

6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:


7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

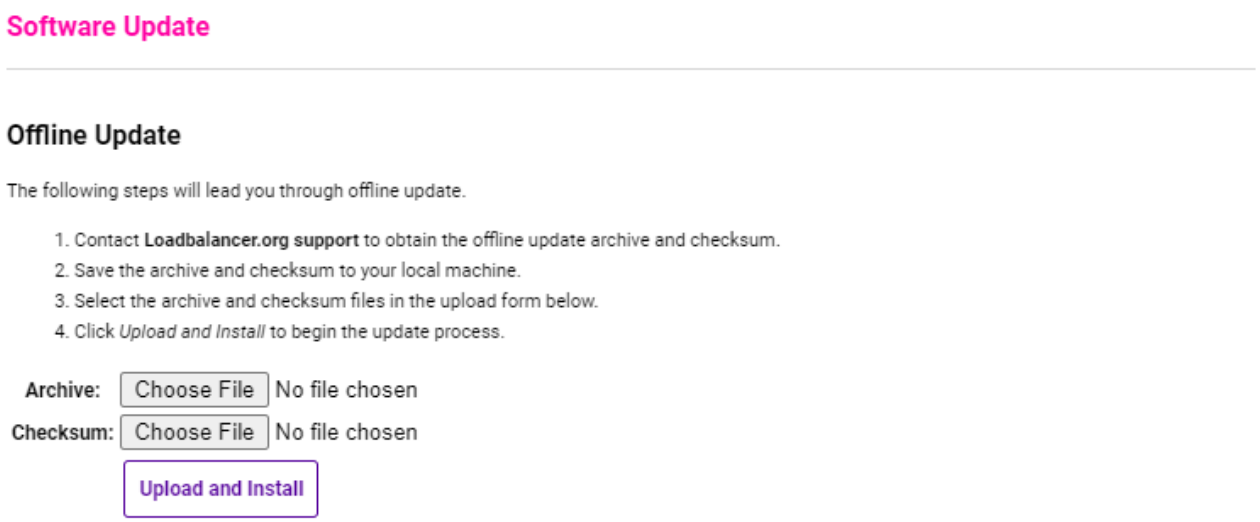
### Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.

> **Note** Please contact support@loadbalancer.org to check if an update is available and obtain the latest offline update files.

To perform an offline update:

1. Using the WebUI, navigate to: *Maintenance > Software Update*.
2. Select **Offline Update**.
3. The following screen will be displayed:




4. Select the *Archive* and *Checksum* files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

## 9.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

| Protocol | Port | Purpose |
|---|---|---|
| TCP | 22 * | SSH |
| TCP & UDP | 53 * | DNS / GSLB |
| TCP & UDP | 123 | NTP |
| TCP & UDP | 161 * | SNMP |
| UDP | 6694 | Heartbeat between Primary & Secondary appliances in HA mode |
| TCP | 7778 | HAProxy persistence table replication |
| TCP | 9000 * | Gateway service (Centralized/Portal Management) |
| TCP | 9080 * | WebUI - HTTP (disabled by default) |
| TCP | 9081 * | Nginx fallback page |

| Protocol | Port | Purpose |
|---|---|---|
| TCP | 9443 * | WebUI - HTTPS |
| TCP | 25565 * | Shuttle service (Centralized/Portal Management) |

> **Note** The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket Addresses.

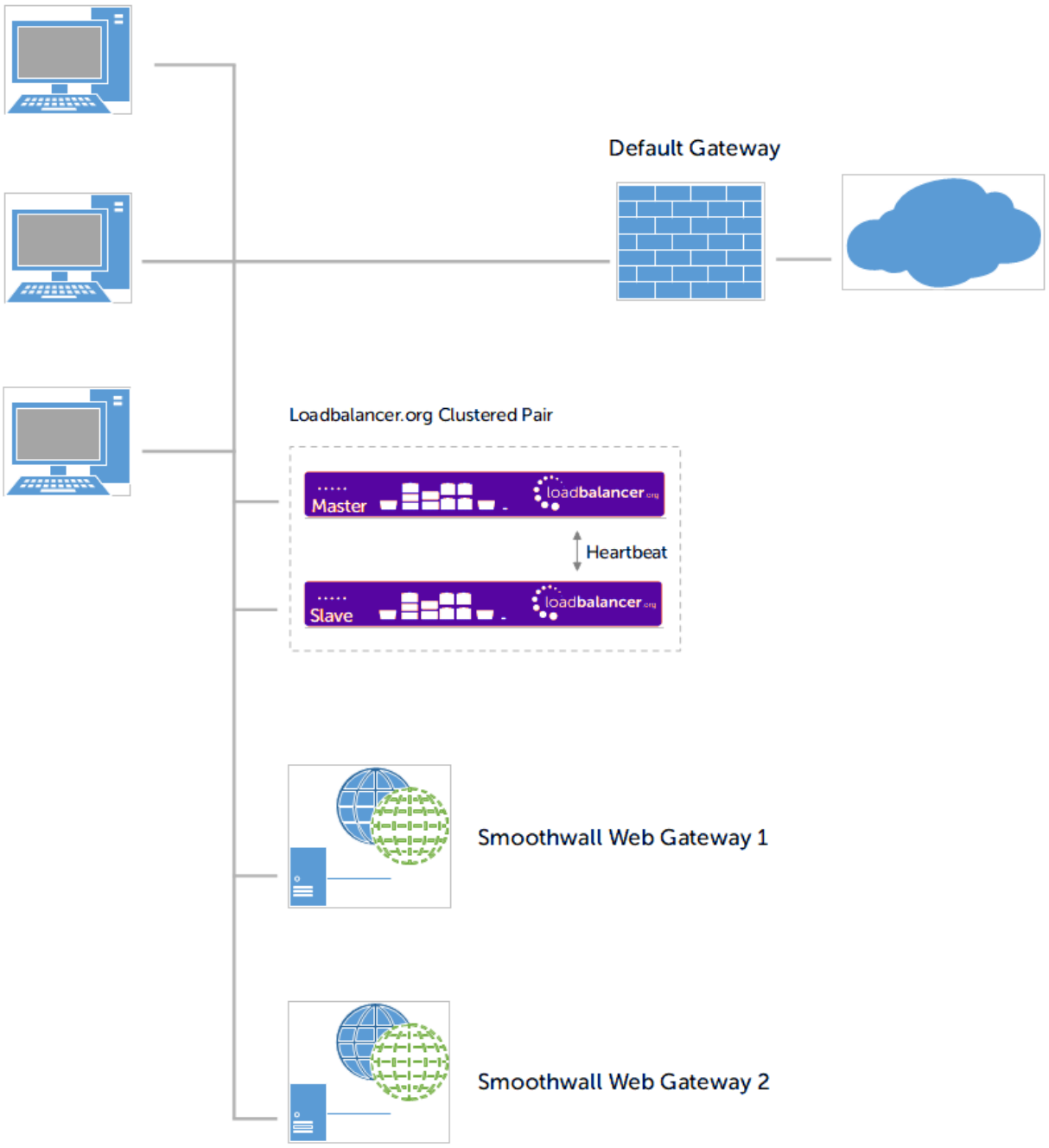
## 9.6. HA Clustered Pair Configuration

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 unit is covered in Configuring HA - Adding a Secondary Appliance.

# 10. Option 1 – Explicit Proxy Mode (Recommended)

## 10.1. Option 1A – Using DR (Direct Return) Mode (Recommended)

### Deployment Architecture



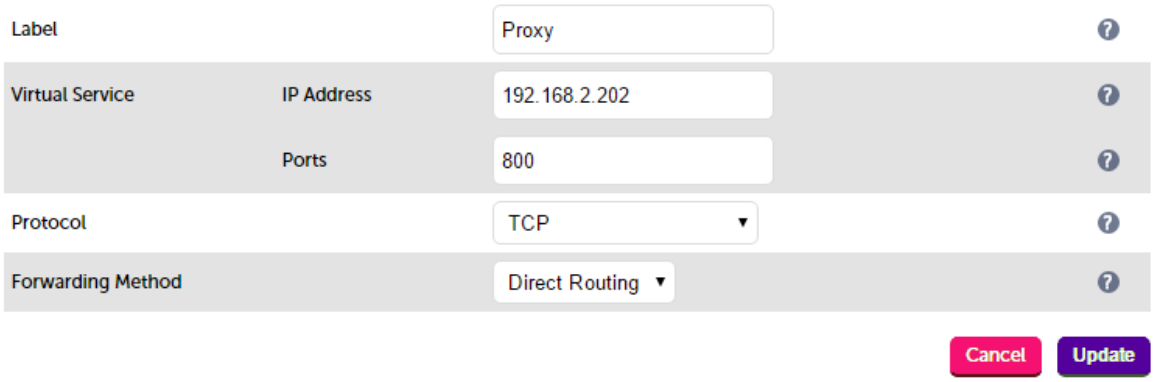

### Notes

- Browser settings on client PC's must be changed to point at the Virtual Service (VIP) on the load balancer (see Client Configuration)
- The load balancers are configured in one-arm Layer 4 DR mode
- The Smoothwall Web Gateways must be configured to accept traffic for the VIP (see Web Gateway 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 unit is covered in Configuring HA - Adding a Secondary Appliance

## Load Balancer Configuration

## Create the Virtual Service (VIP)

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




4. Enter an appropriate label (name) for the VIP, e.g. **Proxy**.
5. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.202**.
6. Set the *Virtual Service Ports* field to the required port, e.g. **800**.

> **Note**
>
> It's possible to use * in the *Ports* field instead of a specific port or list/range of ports.
>
> Using * allows the virtual service to load balance traffic on all ports, which can be useful if the service uses many different ports. It also removes the need to make changes on the load balancer if additional ports are added to the Smoothwall servers in the future.

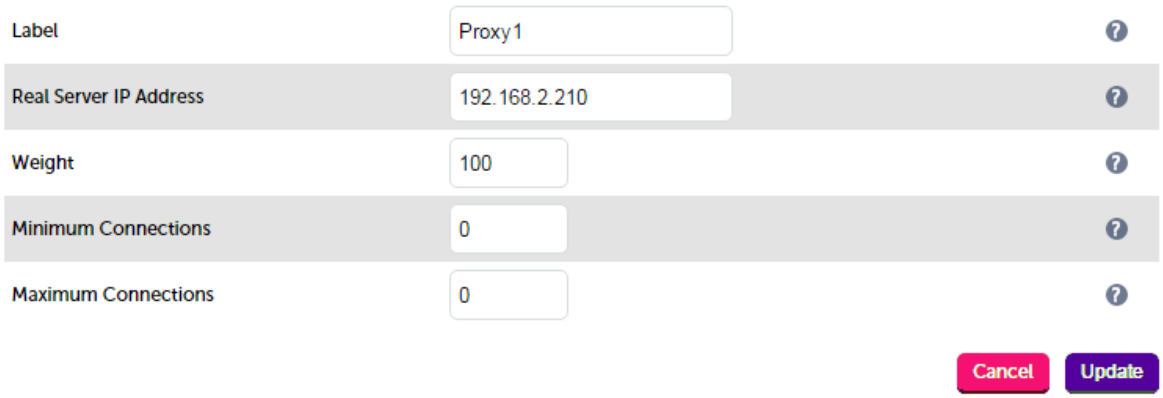
7. Ensure that *Protocol* is set to **TCP**.
8. Ensure that *Forwarding Method* is set to **Direct Routing**.
9. Click **Update**.
10. Now click **Modify** next to the newly created VIP.
11. Ensure *Persistence* s enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour).

> **Note**
>
> It's **optionally** possible to define the parent node of the Smoothwall cluster as a fallback server for the new virtual service.
>
> Smoothwall parent nodes do not ordinarily process client traffic and are designed to handle logging and cluster configuration only. It may be desirable, however, for the load balancer to direct client traffic to the parent node in the event that **all** real servers, i.e. all Smoothwall child nodes, fail health checking and are marked as offline.
>
> To implement this, enter the IP address of the parent node in the *IP Address* field under the *Fallback Server* section, and leave the *Port* field under the *Fallback Server* section empty.

12. Click **Update**.

### Define the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration* > *Layer 4 – Real Servers*.
2. Click **Add a new Real Server** next to the newly created VIP.
3. Enter the following details:




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

## Web Gateway Configuration

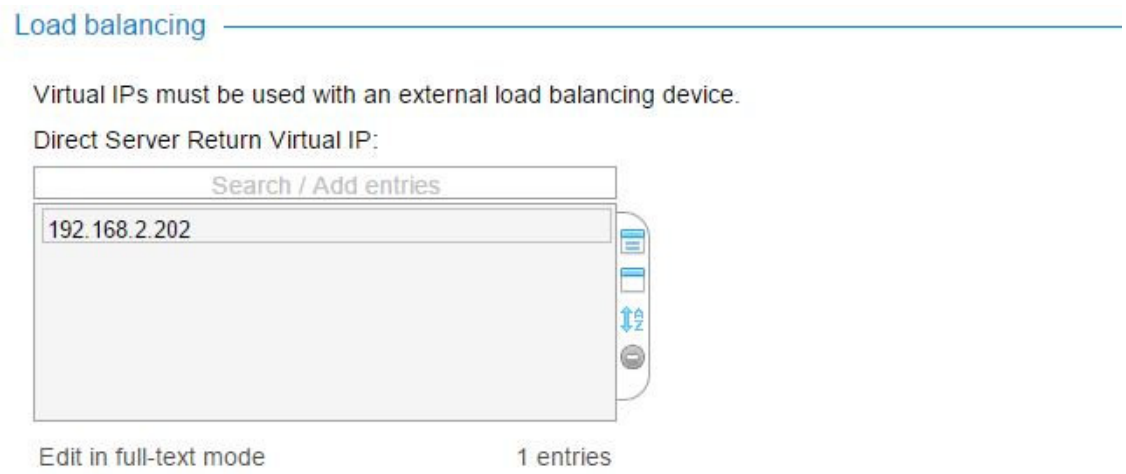
### Modify the Web Gateways to accept traffic for the VIP

#### 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 WebUI

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

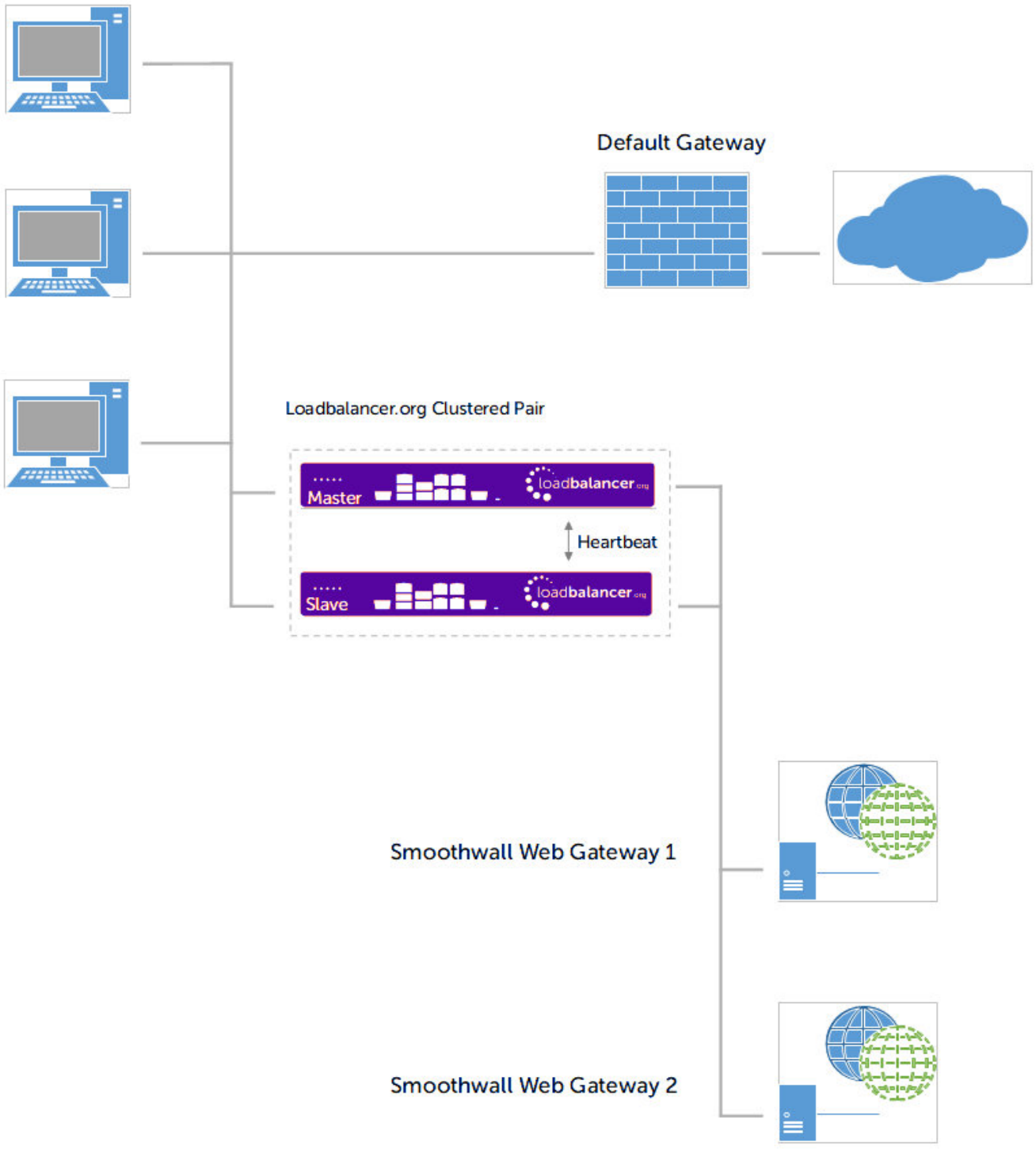



### Finalize Settings

Now refer to the section Configuration Settings Common to Options 1A, 1B & 1C to finalize Web Gateway settings and configure client browser settings.

## 10.2. Option 1B – Using NAT Mode

### Deployment Architecture




### Notes

- Browser settings on client PC's must be changed to point at the Virtual Service (VIP) on the load balancer (see Client Configuration)
- The load balancer is configured in two-arm Layer 4 NAT mode
- Return traffic MUST pass back via the load balancer. To enable this, the default gateway for the Web Gateways is configured to be the load balancer. For an HA pair, a floating IP address must be configured to allow the gateway to move between Primary and Secondary in the event of a failover (see Define a Floating IP to be used as the Default Gateway for the Web Gateways)

- 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 unit is covered in Configuring HA - Adding a Secondary Appliance

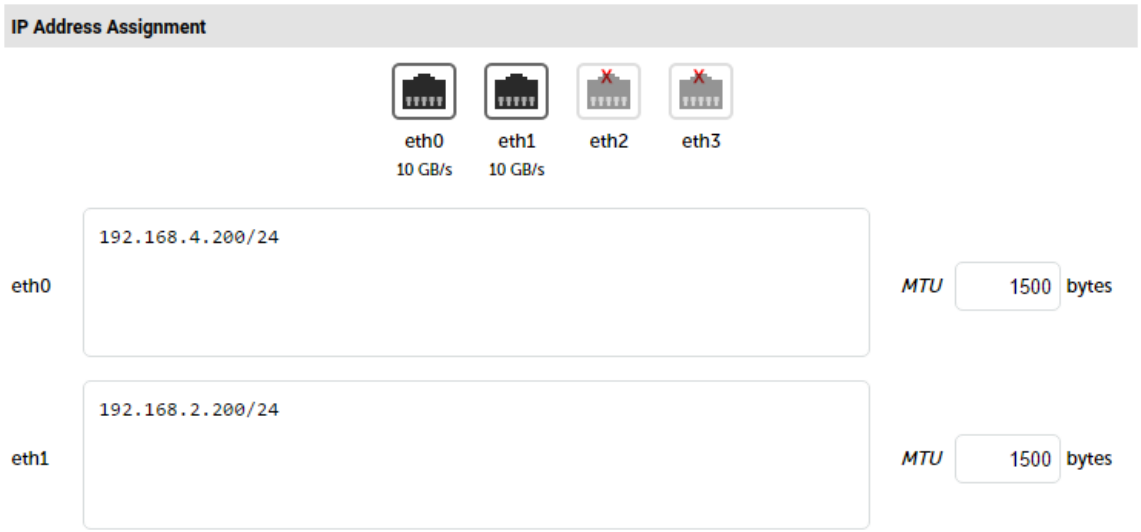
## Load Balancer Configuration

### Configure Network Settings

Two interfaces are required. Typically **eth0** is used for the internal (Web Gateway) subnet and **eth1** is used for the external (client & VIP) subnet, although this is not mandatory since interfaces can be used as required / preferred.

*To configure network settings on the load balancer:*

1. Ensure that the required cables are plugged in (hardware) or virtual NICs are connected (virtual).
2. Using the WebUI, navigate to: *Local Configuration > Network Interface Configuration*.
3. Define the required IP addresses and subnet mask:



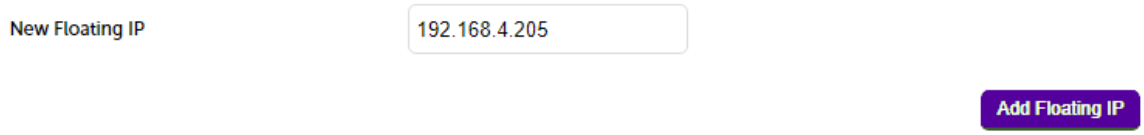

4. Configure the required IP address for **eth0**, e.g. **192.168.4.200/24**.
5. Configure the required IP address for **eth1**, e.g. **192.168.2.200/24**.
6. Click **Configure Interfaces**.

### Define a Floating IP to be used as the Default Gateway for the Web Gateways

As mentioned, when using a clustered pair of load balancers for HA (our recommended configuration), a floating IP must be used as the default gateway for the Web Gateways. This will "float" between the Primary and Secondary units in the event of a failover or failback. This ensures that the Web Gateways always have a consistent return path via the load balancer – whether the Primary or Secondary is active.

*To configure a Floating IP:*

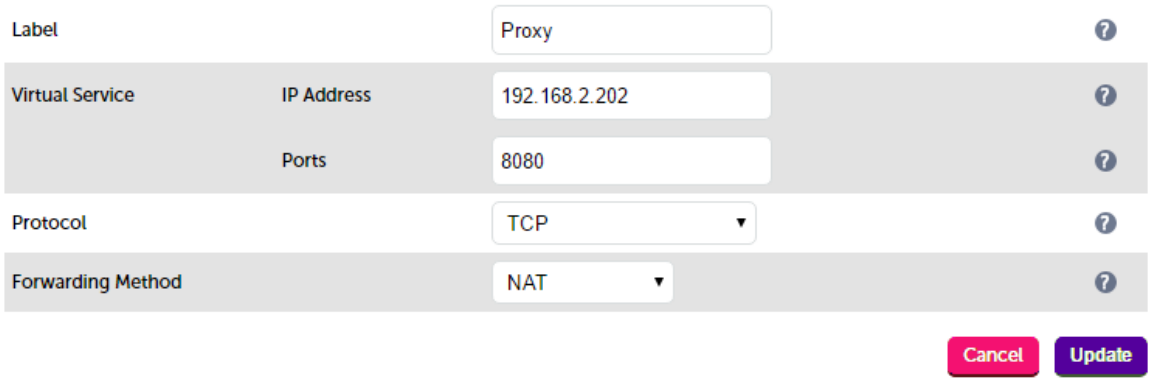
1. Using the WebUI, navigate to: *Cluster Configuration > Floating IP's*.




2. Define a suitable IP address for the default gateway , e.g. **192.168.4.205**.
3. Click **Add Floating IP**.

## Create the Virtual Service (VIP)

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




4. Enter an appropriate label (name) for the VIP, e.g. **Proxy**.
5. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.202**.
6. Set the *Virtual Service Ports* field to the required port, e.g. **8080**.

> **Note**
>
> It's possible to use * in the *Ports* field instead of a specific port or list/range of ports.
>
> Using * allows the virtual service to load balance traffic on all ports, which can be useful if the service uses many different ports. It also removes the need to make changes on the load balancer if additional ports are added to the Smoothwall servers in the future.

7. Ensure that *Protocol* is set to **TCP**.
8. Ensure that *Forwarding Method* is set to **NAT**.
9. Click **Update**.
10. Now click **Modify** next to the newly created VIP.
11. Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour).

> **Note**
>
> It's **optionally** possible to define the parent node of the Smoothwall cluster as a fallback server for the new virtual service.

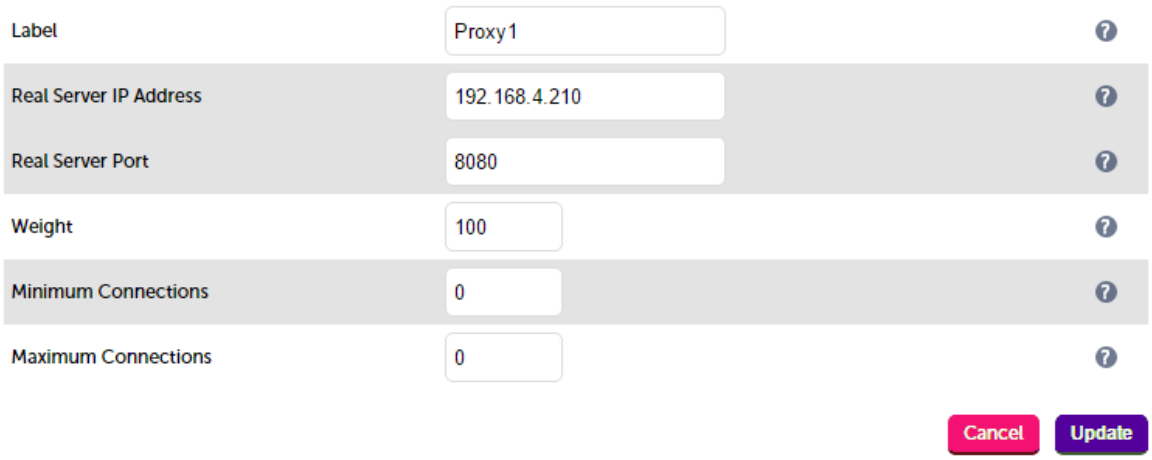
Smoothwall parent nodes do not ordinarily process client traffic and are designed to handle logging and cluster configuration only. It may be desirable, however, for the load balancer to direct client traffic to the parent node in the event that **all** real servers, i.e. all Smoothwall child nodes, fail health checking and are marked as offline.

To implement this, enter the IP address of the parent node in the *IP Address* field under the *Fallback Server* section, and set the *Port* field under the *Fallback Server* section to the required port (if *multiple* ports must be supported, set the *Port* field value to 0).

12. Click **Update**.

## Define the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration* > *Layer 4 – Real Servers*.
2. Click **Add a new Real Server** next to the newly created VIP.
3. Enter the following details:




4. Enter an appropriate label (name) for the first Web Gateway, e.g. **Proxy1**.
5. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.4.210**.
6. Set the *Real Server Port* field to the required port, e.g. **8080**.
7. Click **Update**.
8. Repeat the above steps to add your other Web Gateway(s).

## Enable Auto-NAT

By default, servers behind the load balancer in a NAT configuration will not have access to the outside network. By enabling Auto-NAT, servers (i.e. the Web Gateways) will have their requests automatically mapped to the load balancer's external IP address. The default configuration is to map all requests originating from internal network **eth0** to the external IP on **eth1**. A different interface can be selected if required.

*To enable Auto-NAT on the load balancer:*

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Advanced configuration*.


2. Set the Auto-NAT field to the external interface. As mentioned the default configuration is to use **eth1** and the external interface and **eth0** as the internal interface, but can be set to suit your needs.
3. Click **Update**.

### Web Gateway Configuration

#### Configure the Default Gateway

As mentioned, Option 1B requires the default gateway on the Web Gateway to be the load balancer. When using an HA pair of load balancers, the gateway on the load balancer must be a Floating IP to provide a consistent return path via the load balancer – whether the Primary or Secondary is active. Define a Floating IP to be used as the Default Gateway for the Web Gateways details how to create the Floating IP.

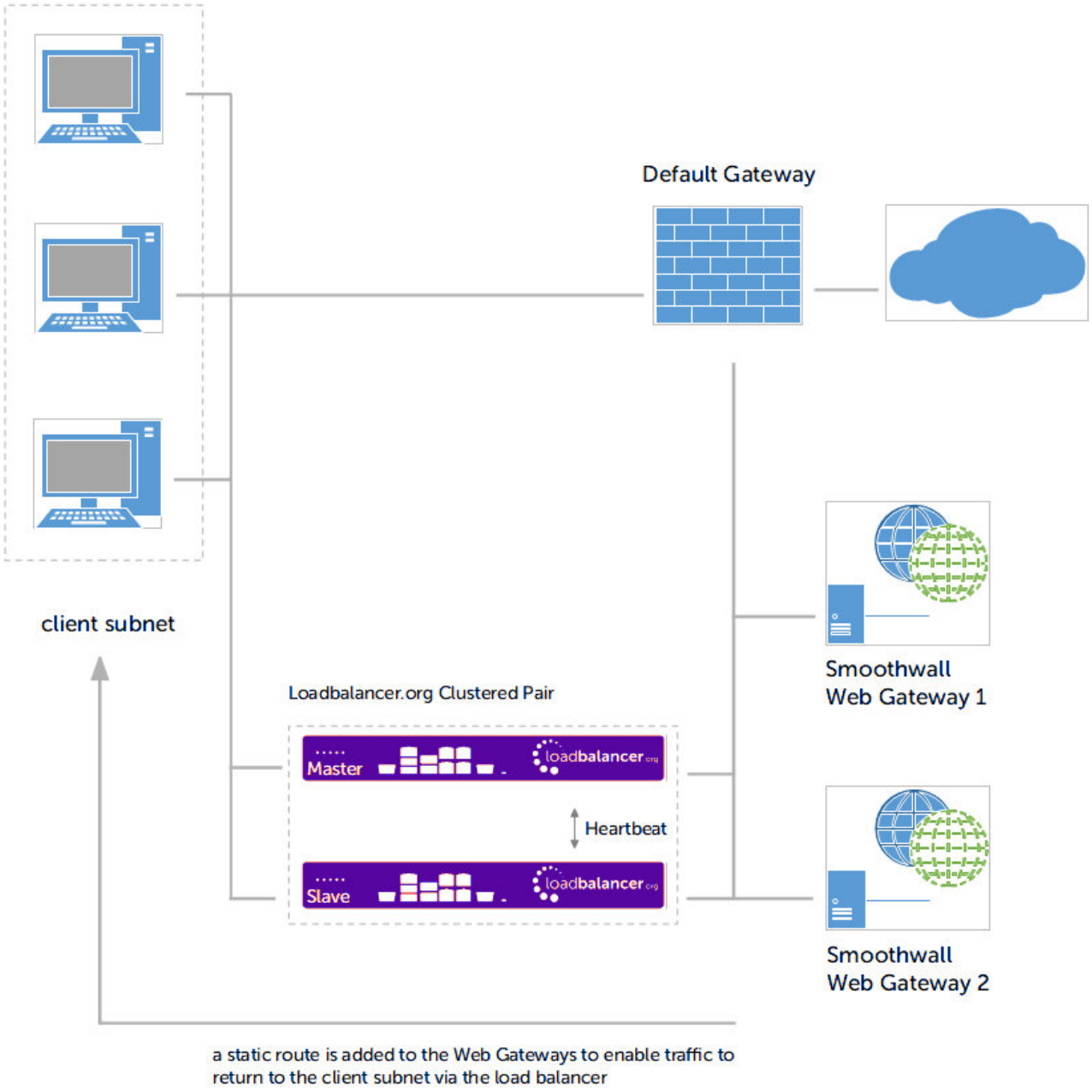
> **Note** Please refer to the Smoothwall Web Gateway documentation for instructions on setting the default gateway. This should be done on all Web Gateways.

### Finalize Settings

Now refer to the section Configuration Settings Common to Options 1A, 1B & 1C to finalize Web Gateway settings and configure client browser settings.

## 10.3. Option 1C – Using NAT Mode (Preferred NAT Topology)

### Deployment Architecture




### Notes

- Browser settings on client PC's must be changed to point at the Virtual Service (VIP) on the load balancer (see Client Configuration)
- The load balancers are configured in two-arm Layer 4 NAT mode
- Return traffic MUST pass back via the load balancer. To enable this, a static route is configured on the Web Gateways to send return traffic back via the load balancer. For an HA pair, a floating IP address must be configured to allow the gateway to move between Primary and Secondary in the event of a failover (see Define a Floating IP to be used as the gateway for the Static Route on the Web Gateways)
- This method is more efficient & faster than Option 1B since the Web Gateways can access the Internet directly rather than going via the load balancer
- 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 unit is covered in Configuring HA - Adding a

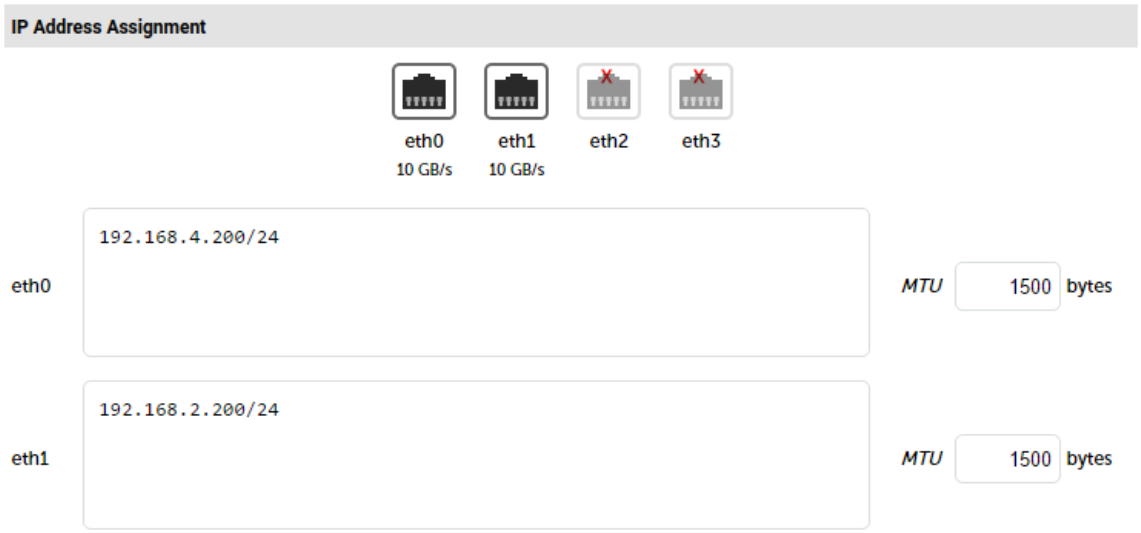
# Load Balancer Configuration

## Configure Network Settings

Two interfaces are required. Typically **eth0** is used for the internal (Web Gateway) subnet and **eth1** is used for the external (client & VIP) subnet, although this is not mandatory since interfaces can be used as required / preferred.

To configure network settings on the load balancer:

1. Ensure that the required cables are plugged in (hardware) or virtual NICs are connected (virtual).
2. Using the WebUI, navigate to: *Local Configuration > Network Interface Configuration*.
3. Define the required IP addresses and subnet mask:



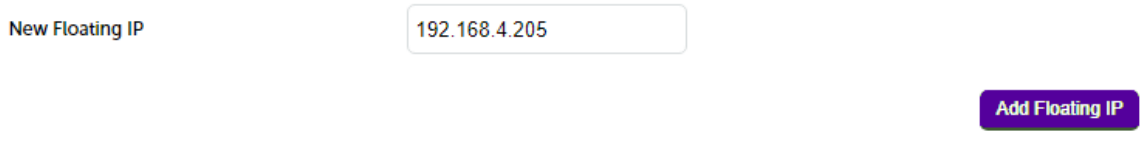

4. Configure the required IP address for **eth0**, e.g. **192.168.4.200/24**.
5. Configure the required IP address for **eth1**, e.g. **192.168.2.200/24**.
6. Click **Configure Interfaces**.

## Define a Floating IP to be used as the gateway for the Static Route on the Web Gateways

As mentioned, when using a clustered pair of load balancers for HA (our recommended configuration), a floating IP must be used as the gateway for the static route on the Web Gateways. This will "float" between the Primary and Secondary units in the event of a failover or failback. This ensures that the Web Gateways always have a consistent return path via the load balancer – whether the Primary or Secondary is active.

*To configure a Floating IP:*

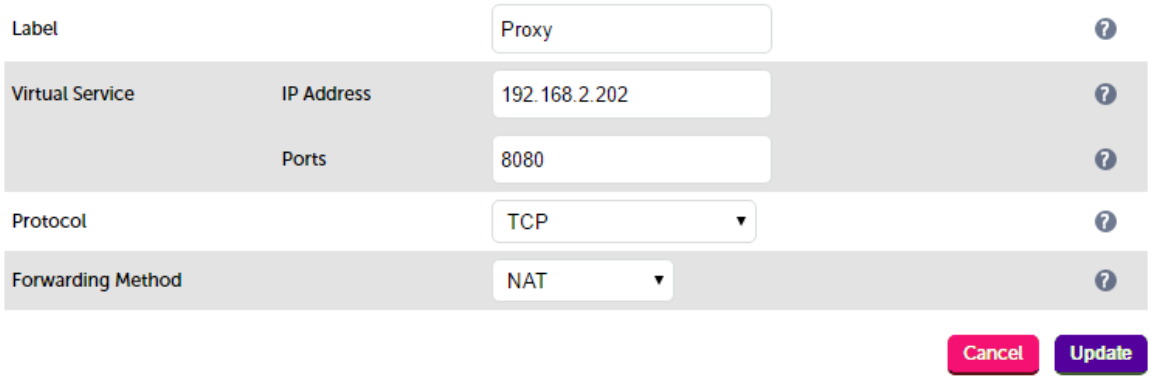
1. Using the WebUI, navigate to: *Cluster Configuration > Floating IP's*.



2. Define a suitable IP address for the default gateway , e.g. **192.168.4.205**.
3. Click **Add Floating IP**.

## Create the Virtual Service (VIP)

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




4. Enter an appropriate label (name) for the VIP, e.g. **Proxy**.
5. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.202**.
6. Set the *Virtual Service Ports* field to the required port, e.g. **8080**.

> **Note**
>
> It's possible to use * in the *Ports* field instead of a specific port or list/range of ports.
>
> Using * allows the virtual service to load balance traffic on all ports, which can be useful if the service uses many different ports. It also removes the need to make changes on the load balancer if additional ports are added to the Smoothwall servers in the future.

7. Ensure that *Protocol* is set to **TCP**.
8. Ensure that *Forwarding Method* is set to **NAT**.
9. Click **Update**.
10. Now click **Modify** next to the newly created VIP.
11. Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour).

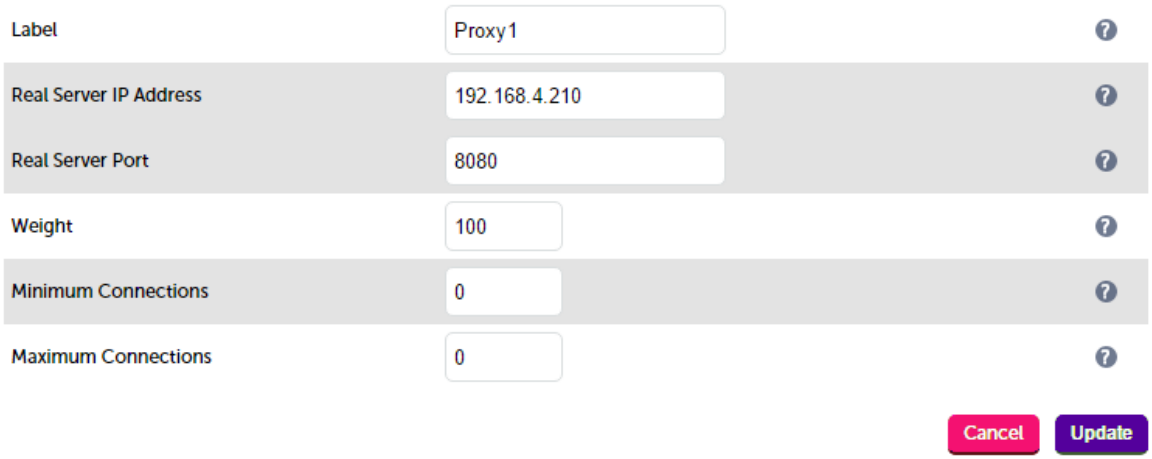
> **Note**
>
> It's **optionally** possible to define the parent node of the Smoothwall cluster as a fallback server for the new virtual service.
>
> Smoothwall parent nodes do not ordinarily process client traffic and are designed to handle logging and cluster configuration only. It may be desirable, however, for the load balancer to direct client traffic to the parent node in the event that **all** real servers, i.e. all Smoothwall child nodes, fail health checking and are marked as offline.
>
> To implement this, enter the IP address of the parent node in the *IP Address* field under the

*Fallback Server* section, and set the *Port* field under the *Fallback Server* section to the required port (if ***multiple*** ports must be supported, set the *Port* field value to 0).

12. Click **Update**.

### Define the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers*.
2. Click **Add a new Real Server** next to the newly created VIP.
3. Enter the following details:




4. Enter an appropriate label (name) for the first Web Gateway, e.g. **Proxy1**.
5. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.4.210**.
6. Set the *Real Server Port* field to the required port, e.g. **8080**.
7. Click **Update**.
8. Repeat the above steps to add your other Web Gateway(s).

## Web Gateway Configuration

### Configure a Static Route

As mentioned, Option 1C requires a Static Route to be defined on the Web Gateway that forces client return traffic to pass back via the load balancer. When using an HA pair of load balancers, the gateway for the static route must be a Floating IP to provide a consistent return path via the load balancer – whether the Primary or Secondary is active. Define a Floating IP to be used as the gateway for the Static Route on the Web Gateways details how to create the Floating IP.

> **Note** Please refer to the Smoothwall Web Gateway documentation for instructions on configuring a Static Route. This should be done on all Web Gateways.

## Finalize Settings

Now refer to the section Configuration Settings Common to Options 1A, 1B & 1C to finalize Web Gateway and client browser settings.

## 10.4. Configuration Settings Common to Options 1A, 1B & 1C

The steps in the following 3 sub sections must be followed for options 1A, 1B & 1C.

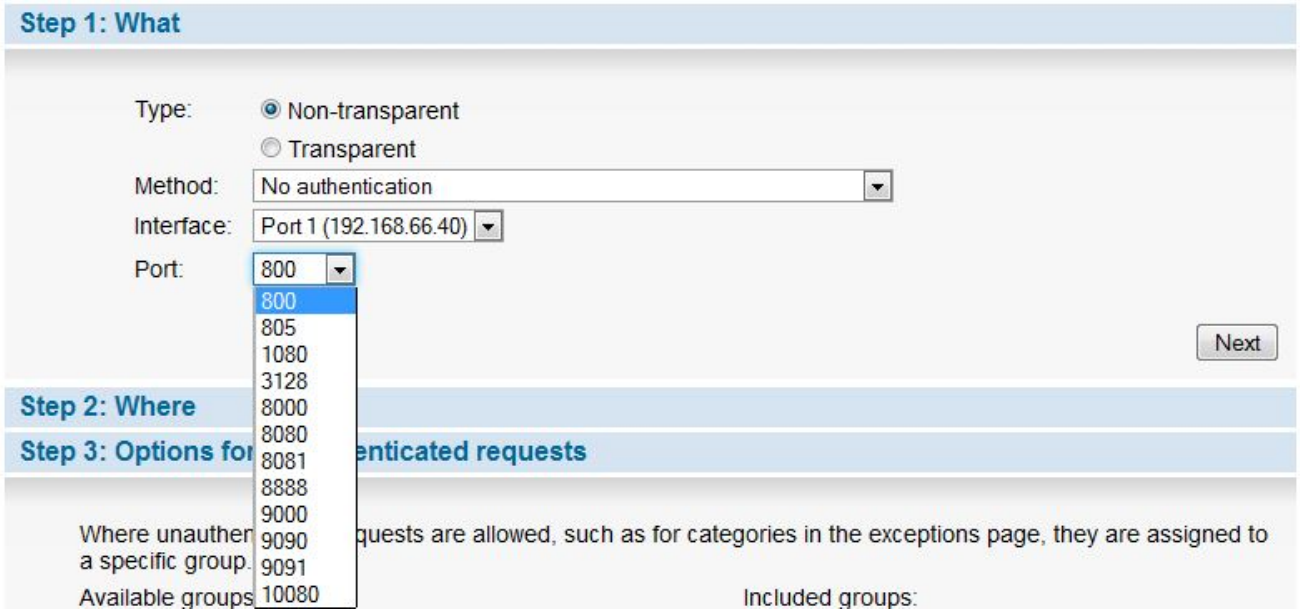
### Web Gateway Operating Mode

The Smoothwall Web Gateway can easily be configured for client configured Explicit Proxy Mode using the policy wizard. Use the WebUI option: ***Web Proxy > Authentication > Policy Wizard*** and select "Non-transparent" as shown below:


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 WebUI 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.

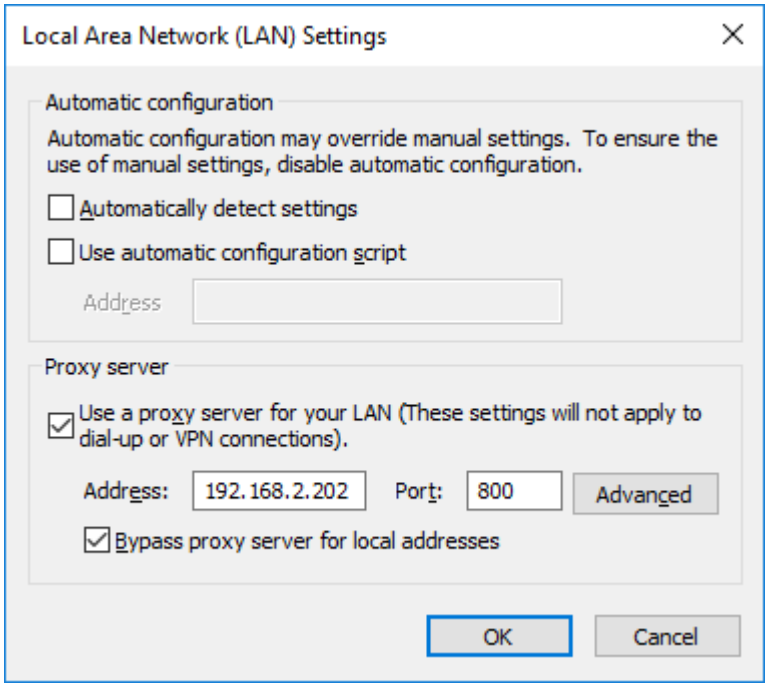
> **Note** The default proxy port for Smoothwall Web Gateway is 800.

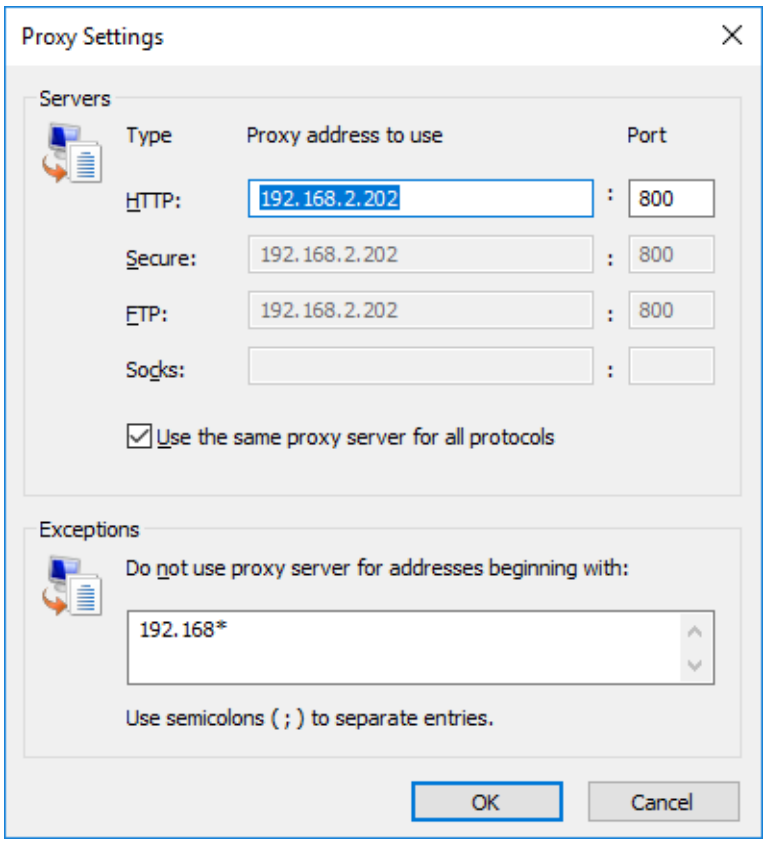
## Client Configuration

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.

> **Note** Depending on your requirements, it may be necessary to use an FQDN rather than an IP address for the Proxy server address. If you use an FQDN, make sure you have a valid DNS configuration that correctly resolves the hostname.

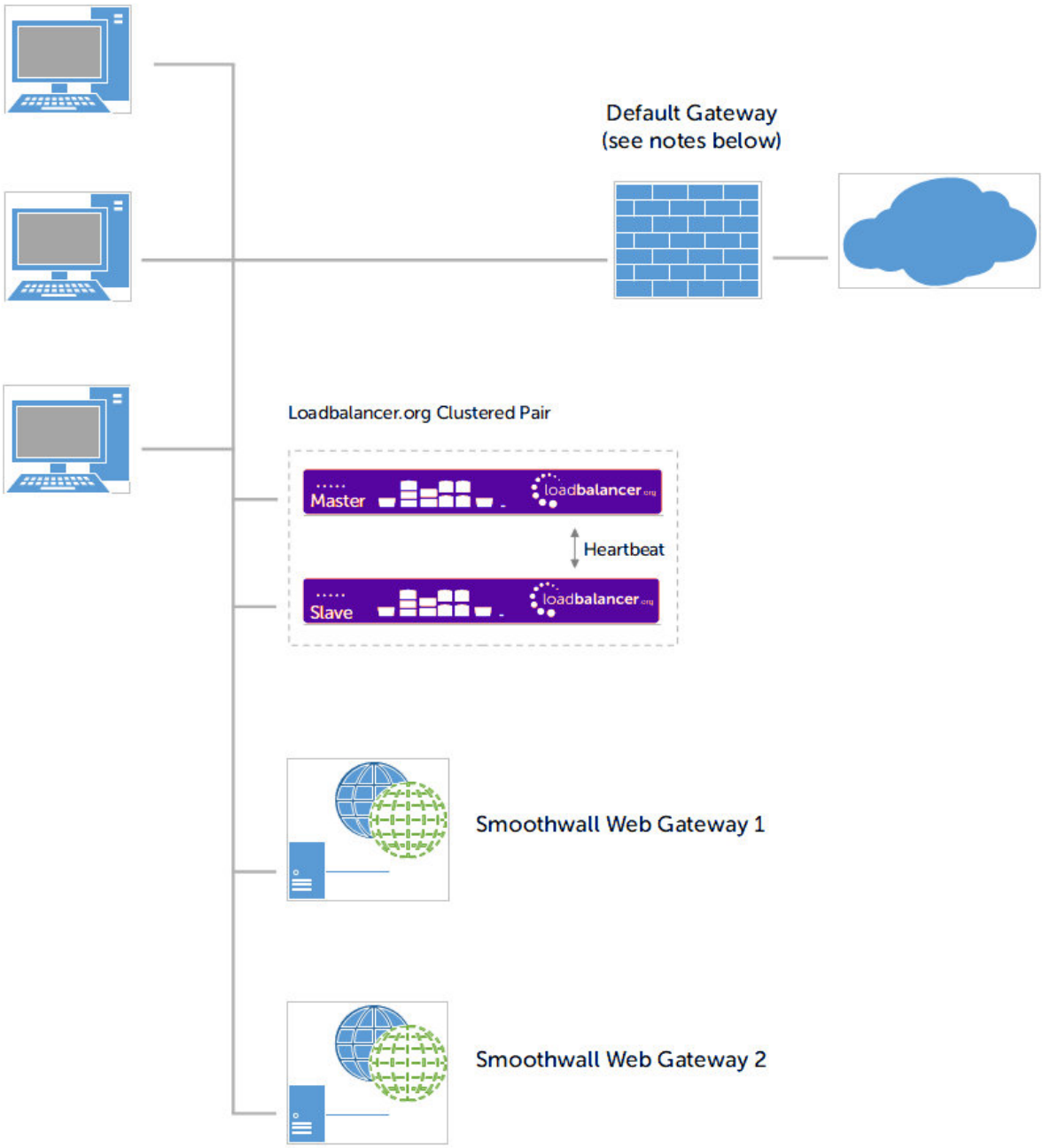
Browser Network Settings:






# 11. Option 2 - Transparent Routed Proxy Mode

## 11.1. Deployment Architecture



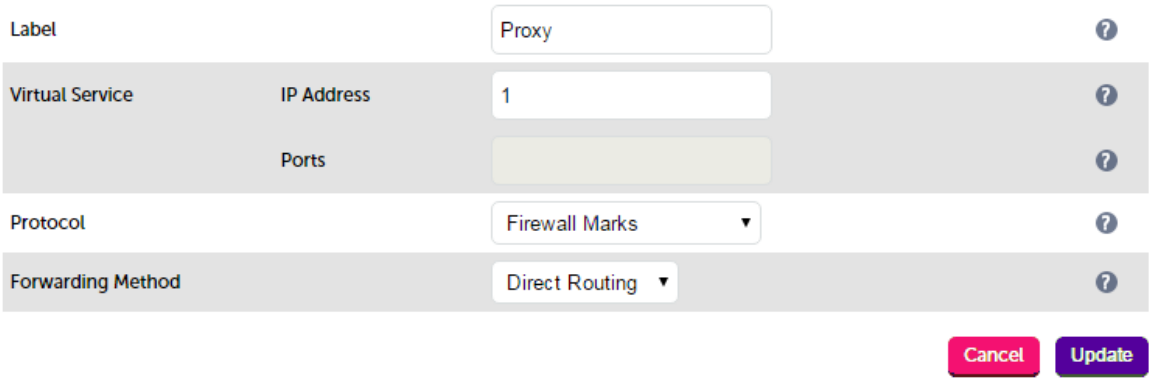

**Notes**

- Rules must be added to the router/firewall so that the required traffic (typically HTTP & HTTPS on port 80 & 443) is sent transparently to the load balancer, please see Router/Default Gateway Configuration for example rules for a Linux router
- As with Explicit Proxy 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 Configure Firewall Rules)
- 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 unit is covered in Configuring HA - Adding a Secondary Appliance

## 11.2. Load Balancer Configuration

## Create the Virtual Service (VIP)

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




4. Enter an appropriate label (name) for the VIP, e.g. **Proxy**.
5. Change the *Virtual Service IP address* field to **1**.

> **Note** This is the reference number for the 'Firewall Mark' . The same reference number is used when configuring the firewall rules – please see Configure Firewall Rules for more details.

6. Clear the *Virtual Service Ports* field, the ports are defined in the firewall rules in Configure Firewall Rules.
7. Ensure that *Protocol* is set to **Firewall Marks**.

> **Note** The ports field will be disabled when this is done.

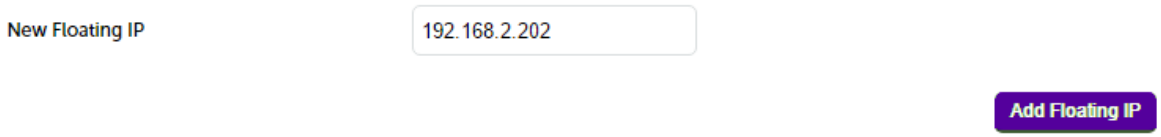
8. Ensure that *Forwarding Method* is set to **Direct Routing**.
9. Click **Update**.
10. Now click **Modify** next to the newly created VIP.
11. Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour).

> **Note**
>
> It's **optionally** possible to define the parent node of the Smoothwall cluster as a fallback server for the new virtual service.
>
> Smoothwall parent nodes do not ordinarily process client traffic and are designed to handle logging and cluster configuration only. It may be desirable, however, for the load balancer to direct client traffic to the parent node in the event that **all** real servers, i.e. all Smoothwall child nodes, fail health checking and are marked as offline.
>
> To implement this, enter the IP address of the parent node in the *IP Address* field under the *Fallback Server* section, and leave the *Port* field under the *Fallback Server* section empty.

12. Under the *Health Checks* section change *Check Type* to **Ping Server**.
13. Click **Update**.

## Add the Floating IP

1. Using the WebUI, navigate to: *Cluster Configuration > Floating IPs*.




2. Enter an appropriate IP address for the Virtual Service, e.g. **192.168.2.202**.
3. Click **Add Floating IP**.

## Configure Firewall Rules

> **Note**
>
> The *Firewall Script* page is *locked* by default on newer Loadbalancer.org appliances as part of "Secure Mode", which makes applying the changes described below impossible.
>
> To enable editing of the firewall script, navigate to *Local Configuration > Security*, set *Appliance Security Mode* to **Custom**, and click the **Update** button to apply the change. Editing the *Firewall Script* page will then be possible.

1. Using the WebUI, navigate to: *Maintenance > Firewall Script*.
2. Scroll down to the Firewall Marks section.
3. Add the following lines to this section as shown in the screen shot below:

```
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
```

> **Note**
>
> Please see Modified Transparent Mode Firewall Rules if you intend to forward ALL traffic to the Web Gateways.

**Firewall Script**

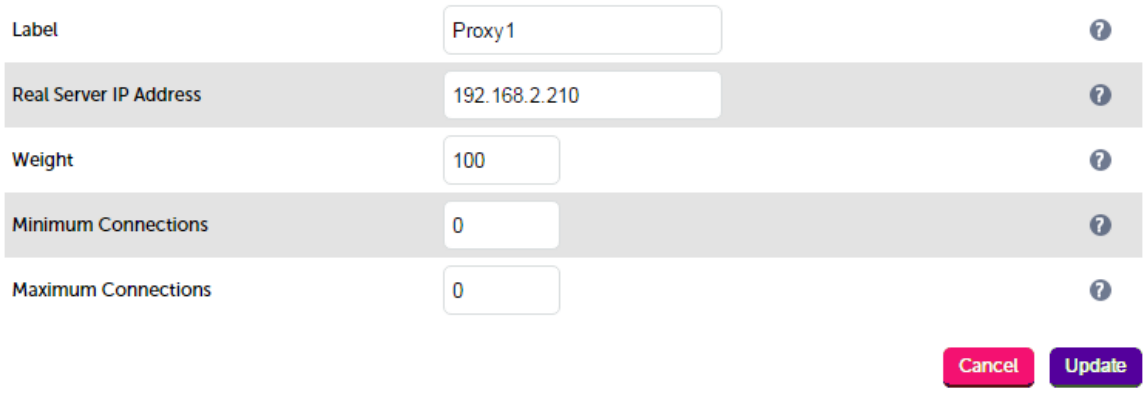
```
#!/bin/sh
# $Id$

#
# User firewall script for Loadbalancer.org appliance.
#



# Please note:
#               Most configurations will not require any changes to be made to
#               this script.
#
#               Administrators will only need to modify this script if their
#               needs are not met by the lock-down wizard, auto-NAT, and
#               automatic firewall mark functions of the web interface.



##########################  One-arm NAT Mode  ##############################
# For one-arm NAT, ICMP re-directs will need to be disabled.
# (1 = on, 0 = off)
#echo "0" >/proc/sys/net/ipv4/conf/all/send_redirects
#echo "0" >/proc/sys/net/ipv4/conf/default/send_redirects



########################  Manual Firewall Marks  ############################
```

Update

4. Click **Update**.

## Define the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers*.
2. Click **Add a New Real Server** next to the newly created VIP.
3. Enter the following details:



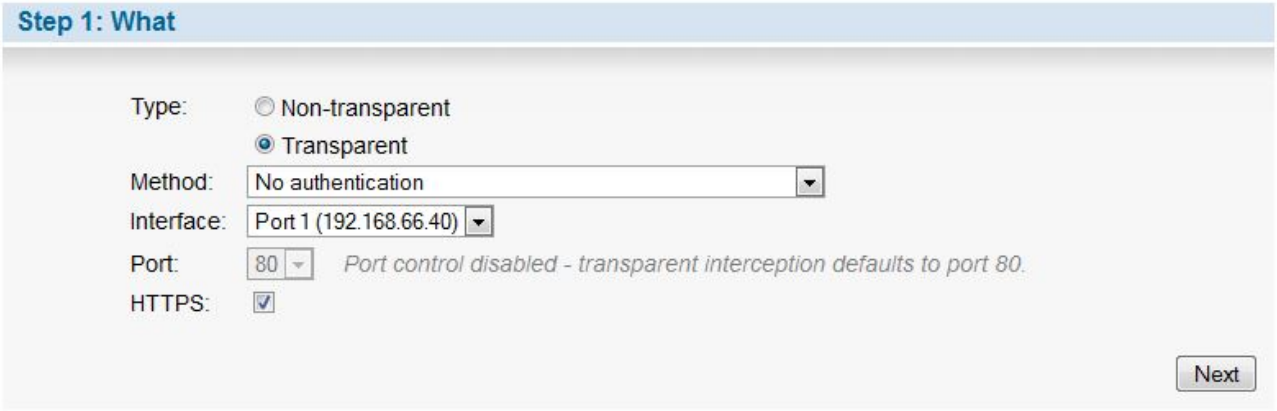

4. Enter an appropriate label (name) for the first Web Gateway, e.g. **Proxy1**.
5. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.210**.
6. Click **Update**.
7. Repeat the above steps to add your other Web Gateway(s).

## 11.3. Web Gateway Configuration

### Web Gateway Operating Mode

The Smoothwall Web Gateway can easily be configured for transparent mode using the policy wizard.

Use the WebUI option: ***Web Proxy > Authentication > Policy Wizard*** and select "Transparent" 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 Explicit Proxy Mode. However, it's still recommended to configure this so both modes are catered for from the start.

## 11.4. 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 Gateways. The example shown below is for a Linux based router:

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 $SUBNET -p tcp -m tcp --dport 80 -j MARK --set-mark $FWMARK
iptables -t mangle -A PREROUTING -s $SUBNET -p tcp -m 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 Web Gateway, i.e. all packets on port 80 & 443. 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 Gateway.

> **Note** This is required when no changes have been made to the clients default gateway settings.

## 11.5. 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.

# 12. Testing & Verification

> **Note** For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

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

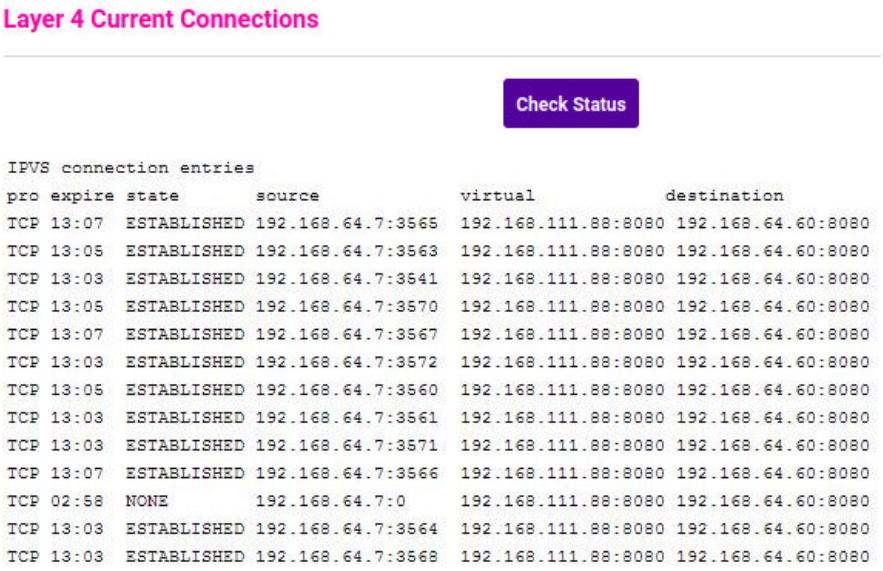
1. System Overview
2. Reports > Layer 4 Status
3. Reports > Layer 4 Current Connections

Several reporting and dashboard options are also available on the Web Gateway, for more details please refer to the Smoothwall Web Gateway documentation.

## 12.1. Layer 4 – Current Connections

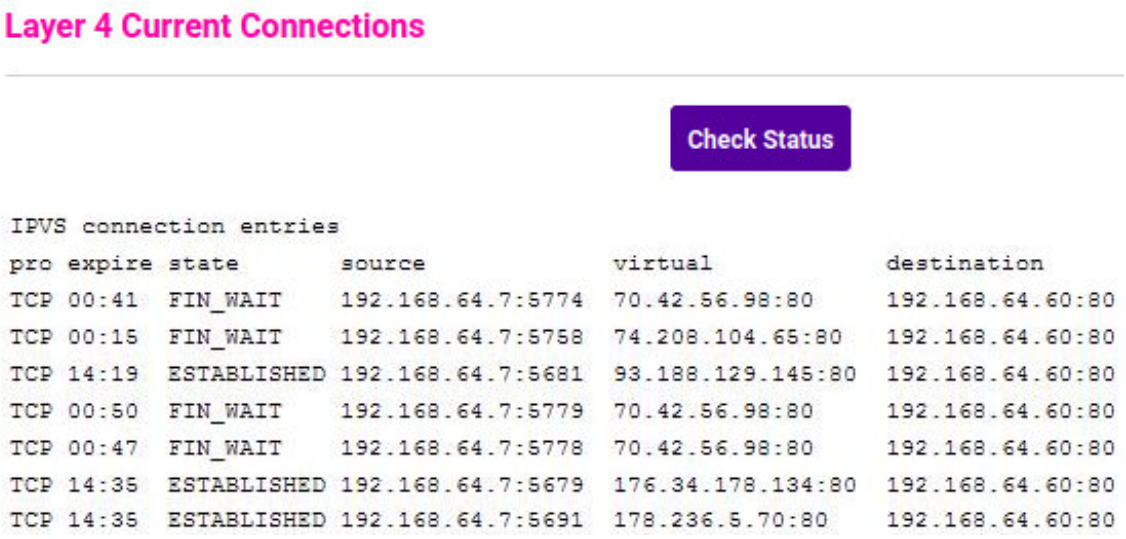
### Explicit Proxy Mode

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).




### Transparent Mode

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




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.

# 13. 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.

# 14. Further Documentation

For additional information, please refer to the Administration Manual.

# 15. Appendix

## 15.1. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution. We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

> **Note** For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

### Non-Replicated Settings

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

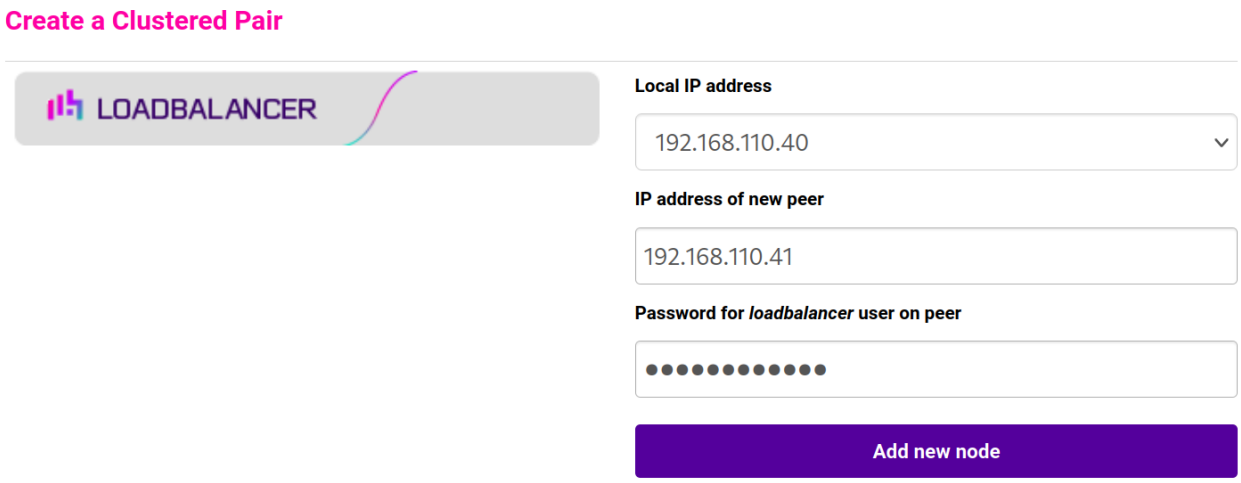
| WebUI Main Menu Option | Sub Menu Option | Description |
|---|---|---|
| Local Configuration | Hostname & DNS | Hostname and DNS settings |
| Local Configuration | Network Interface Configuration | Interface IP addresses, bonding configuration and VLANs |
| Local Configuration | Routing | Default gateways and static routes |
| Local Configuration | System Date & time | Time and date related settings |
| Local Configuration | Physical – Advanced Configuration | Various appliance settings |
| Local Configuration | Portal Management | Portal management settings |
| Local Configuration | Security | Security settings |
| Local Configuration | SNMP Configuration | SNMP settings |
| Local Configuration | Graphing | Graphing settings |
| Local Configuration | License Key | Appliance licensing |
| Maintenance | Backup & Restore | Local XML backups |
| Maintenance | Software Updates | Appliance software updates |
| Maintenance | Fallback Page | Fallback page configuration |
| Maintenance | Firewall Script | Firewall (iptables) configuration |
| Maintenance | Firewall Lockdown Wizard | Appliance management lockdown settings |

> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

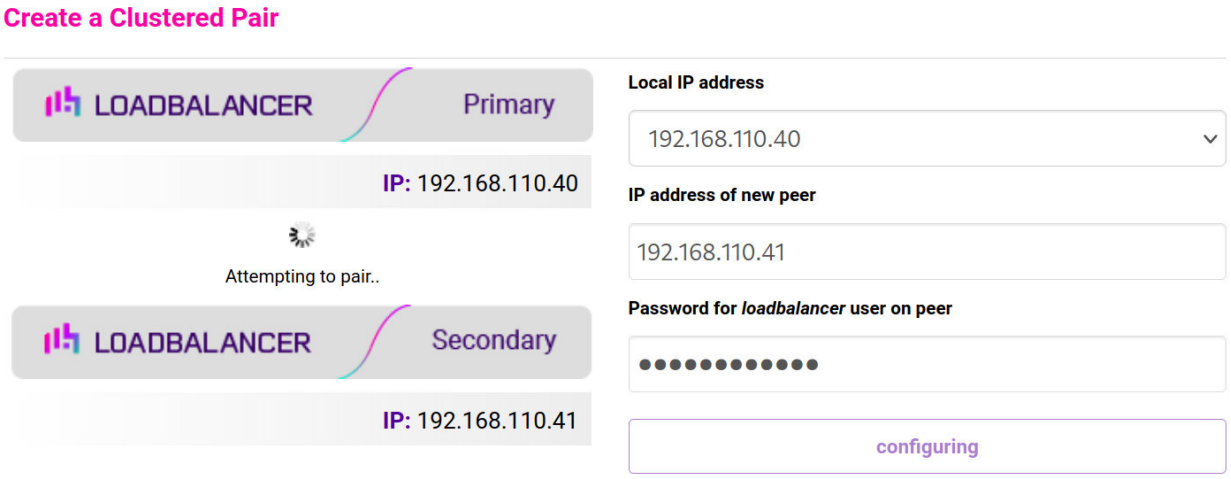
## Configuring the HA Clustered Pair

> **Note** If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

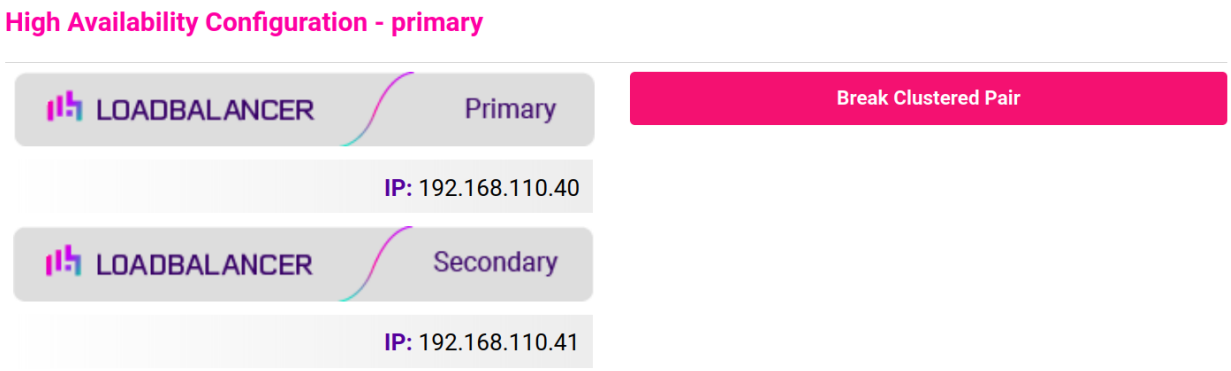
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.




3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:




6. Once complete, the following will be displayed on the Primary appliance:




7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

> **Note** Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

> **Note** For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.

> **Note** For details on testing and verifying HA, please refer to Clustered Pair Diagnostics.

## 15.2. Modified Transparent Mode Firewall Rules

If ALL traffic is to be forwarded to the Web Gateways, the firewall rules below should be used rather than the rules in Configure Firewall Rules:

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.

# 16. Document Revision History

| Version | Date | Change | Reason for Change | Changed By |
|---|---|---|---|---|
| 1.4.0 | 6 August 2019 | Styling and layout<br><br>Added notes explaining how * can be used in virtual service port fields<br><br>Added note explaining how to disable "Secure Mode" to unlock the firewall script page | General styling updates<br><br>Required updates | AH |
| 1.4.1 | 29 August 2019 | Added note sections on how to optionally define a parent Smoothwall node as a fallback server | Additional option documented based on discussions with Smoothwall | AH |
| 1.4.2 | 5 June 2020 | New title page<br><br>Updated Canadian contact details | Branding update<br><br>Change to Canadian contact details | AH |
| 1.5.0 | 1 October 2021 | Converted the document to AsciiDoc | Move to new documentation system | AH,RJC,ZAC |
| 1.5.1 | 5 January 2023 | Combined software version information into one section<br><br>Added one level of section numbering<br><br>Added software update instructions<br><br>Added table of ports used by the appliance<br><br>Reworded 'Further Documentation' section | Housekeeping across all documentation | AH |
| 1.5.2 | 2 February 2023 | Updated screenshots | Branding update | AH |
| 1.5.3 | 7 March 2023 | Removed conclusion section | Updates across all documentation | AH |
| 1.6.0 | 24 March 2023 | New document theme<br><br>Modified diagram colours | Branding update | AH |

LOADBALANCER

**Visit us:** www.loadbalancer.org

**Phone us:** +44 (0)330 380 1064

**Phone us:** +1 833 274 2566

**Email us:** info@loadbalancer.org

**Follow us:** @loadbalancer.org

## About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.