LOADBALANCER

DEPLOYMENT GUIDE

# Load Balancing Netsweeper

Version 1.2.0

# Table of Contents

# 1. About this Guide

This guide details the steps required to configure a load balanced Netsweeper environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Netsweeper 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 Netsweeper. For full specifications of available models please refer to https://www.loadbalancer.org/products/enterprise.

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. Netsweeper

- All versions

# 4. Netsweeper

Netsweeper is a Linux-based web filtering software developed by the Netsweeper corporation. It provides functions for filtering malicious and inappropriate web content, which can help with meeting compliance and regulatory requirements.

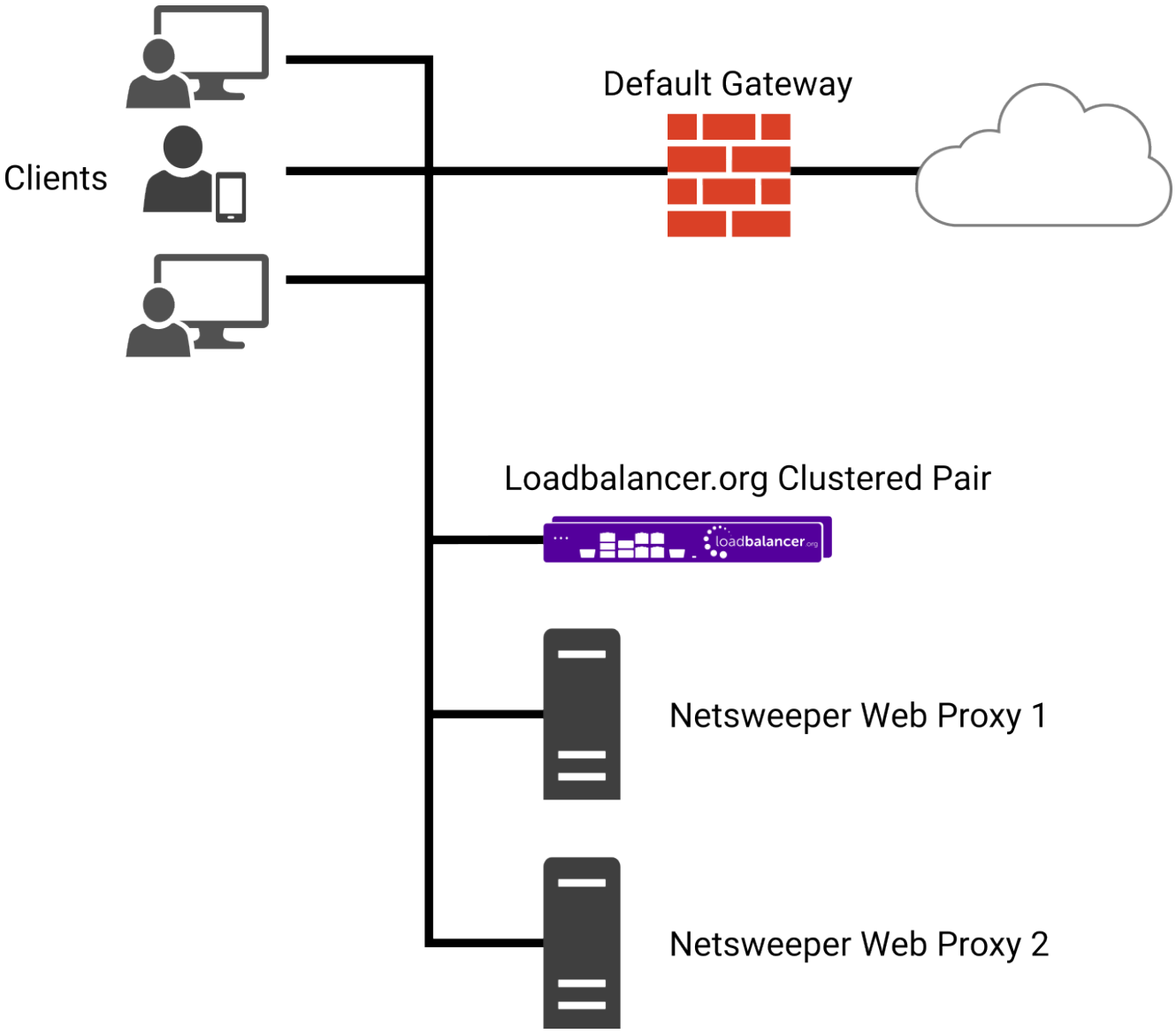
The Netsweeper software comes as both a virtual and hardware product, both of which can be effectively load balanced using Loadbalancer.org appliances. Load balancing a Netsweeper installation makes it highly available to avoid service interruption, easily scalable to meet changing levels of service demand, and simple to maintain by allowing Netsweepers to be gracefully removed from service ahead of disruptive maintenance tasks like reboots.

# 5. Netsweeper Deployment Modes

Three modes of Netsweeper operation are officially supported with Loadbalancer.org appliances:

- **Explicit Mode:** Proxy settings are explicitly set on each client device. Browser settings on client PCs must be changed to point to the virtual service (VIP) on the load balancer. *(Explicit Mode setup instructions.)*
- **Transparent Mode:** Policy based routing (PBR) is used at the router/firewall that handles client traffic. These rules at the router/firewall ensure that the required traffic (typically HTTP & HTTPS traffic on ports 80 and 443) is sent transparently to the load balancer. *(Transparent Mode setup instructions.)*
- **Non-Transparent Mode:** Proxy settings are explicitly set on each client device. Browser settings on client PCs must be changed to point at the virtual service (VIP) on the load balancer. *(Non-Transparent Mode setup instructions.)*

# 6. Deployment Concept




For a Netsweeper deployment, the load balancer is deployed using ***Layer 4 DR Mode*** (direct routing, aka DSR / direct server return). This is a very high performance solution which is well suited to web filters and proxies.

> **Note** The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

# 7. Configuring Netsweeper for Load Balancing

The following instructions apply to **all options/modes** of operation for load balancing Netsweeper, and **must** be carried out on *every deployment*.

## 7.1. Firewall Configuration

Netsweeper uses several different network ports to function. Any firewalls that handle Netsweeper traffic should have the following network port rules configured so that Netsweeper works correctly:

- Open inbound ports: 80, 8080, 8081, 3431, 3432
- Open outbound ports: 25, 53, 80, 443, 3436

## 7.2. DR Mode Considerations

### 7.2.1. The ARP problem

DR mode works by changing the MAC addresses of inbound packets to match the Netsweeper server selected by the load balancing algorithm. To enable DR mode to operate:

- Each Netsweeper server must be configured to accept packets destined for both the VIP address ***and*** the Netsweeper server's IP address (RIP). This is because in DR mode the destination address of load balanced packets is the VIP address, while for all other traffic, such as health checks, administration traffic, etc., the destination address is the Netsweeper server's own IP address (the RIP). The Netsweeper service must also respond to both addresses.
- Each Netsweeper server must be configured so that it does not respond to ARP requests for the VIP address: only the load balancer should do this.

Configuring the Netsweeper servers in this way is referred to as "Solving the ARP problem". The steps presented below detail the Netsweeper-recommended solution to the ARP problem.

### 7.2.2. Solving the ARP Problem

iptables can be used on each Netsweeper server to identify incoming packets that are addressed to a virtual IP address (VIP) and redirect those packets to the server itself. This is achieved using the **REDIRECT** target in iptables, which performs the necessary NAT to make this possible. This allows a Netsweeper to accept packets addressed to a VIP without the Netsweeper owning the VIP.

Execute the following command to put the necessary iptables rule in place to redirect traffic for a single IPv4 VIP address. Note that iptables rules added in this way ***will not persist across reboots***. To make such a rule permanent, either add the rule to an iptables firewall script, if one is provided with the Linux distribution in question, or add the command to an appropriate startup script such as `/etc/rc.local` on each Netsweeper.

```
iptables -t nat -A PREROUTING -d <IPv4-VIP> -j REDIRECT
```

The VIP address should be changed to match the virtual service in question, for example:

```
iptables -t nat -A PREROUTING -d 10.0.0.21 -j REDIRECT
```

The example above will redirect any incoming packets destined for 10.0.0.21 (the virtual service) locally, i.e. to the primary address of the incoming interface on the Netsweeper.

If a real server is responsible for serving ***multiple*** VIPs then additional iptables rules should be added to cover each VIP.

# 8. Loadbalancer.org Appliance – the Basics

## 8.1. 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. |

## 8.2. 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. |

## 8.3. 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.

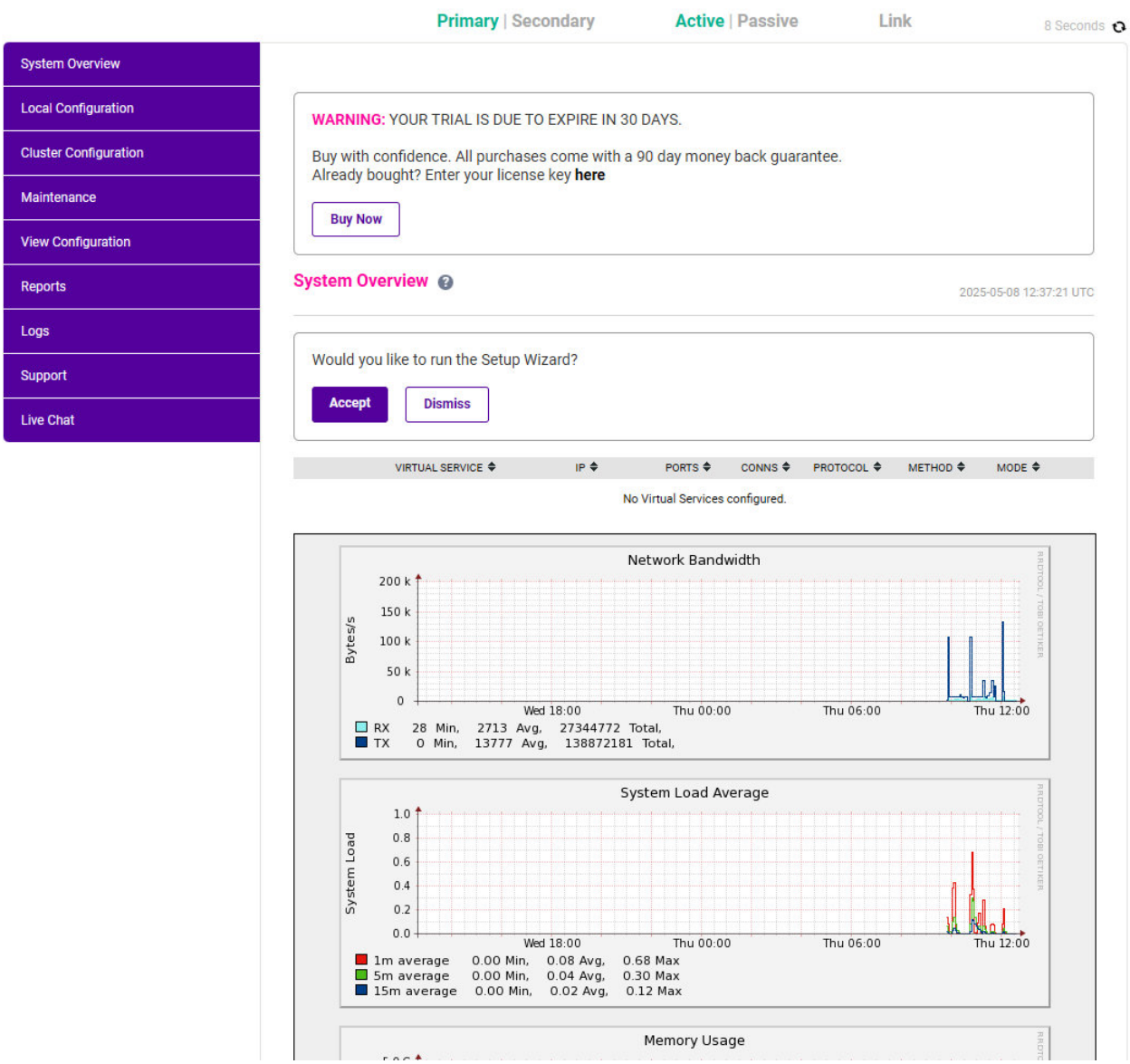
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.

> **Note** The Setup Wizard can only be used to configure Layer 7 services.

## 8.3.1. 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 creating 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

## 8.4. Appliance Software Update

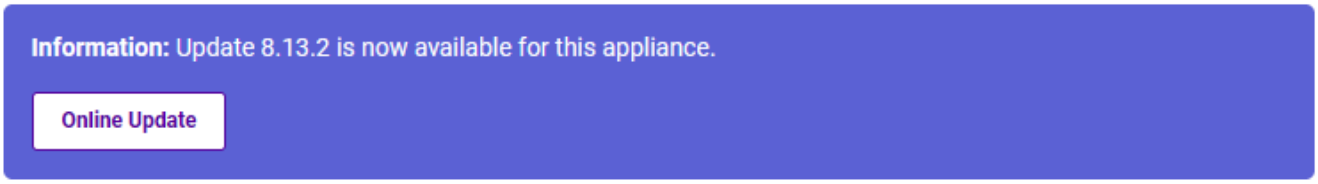
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **Note** For full details, please refer to Appliance Software Update in the Administration Manual.

> **Note** Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

### 8.4.1. Online Update

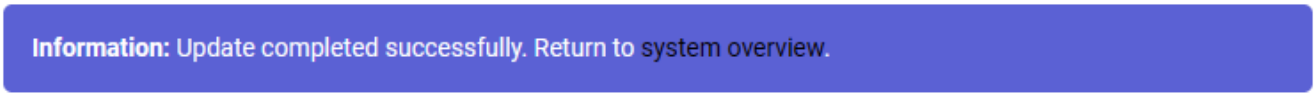
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:




Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

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

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




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

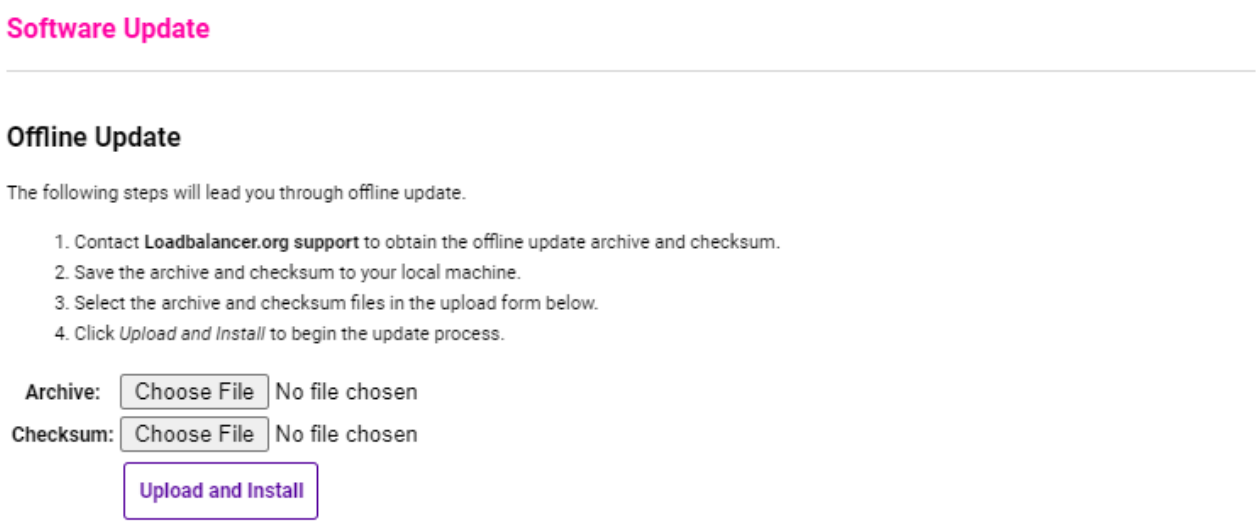
### 8.4.2. Offline Update

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

To check for the latest version, please refer to our product roadmap page available here. To obtain the latest offline update files contact support@loadbalancer.org.

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.

## 8.5. 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 |
| 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.

## 8.6. 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 the section Configuring HA - Adding a Secondary Appliance of the appendix.

# 9. Option 1 – Explicit Mode

## 9.1. Netsweeper Network Alias Configuration

The following steps should be carried out on the Netsweeper software instances to configure them for load balancing using layer 4 DR mode.

These instructions will create a network alias for the eth0 network interface so that it can be assigned an additional IP address. This is required for layer 4 DR mode operation.

1. Establish an SSH session with the Netsweeper software.
2. Login to the ***admin*** account using the appropriate credentials.
3. Change to the network-scripts directory by executing the following command:

```
cd /etc/sysconfig/network-scripts
```

4. Execute the following command to create the configuration file for the eth0 network interface alias:

```
cp ifcfg-eth0 ifcfg-eth0:0
```

5. Open the newly-created configuration file for editing, by executing the command:

```
nano ifcfg-eth0:0
```

6. Edit the following lines in the configuration file to make it read like so:

```
DEVICE=eth0:0
ONBOOT=YES
BOOTPROTO=static
IPADDR=<Insert Virtual IP Address>
NETMASK=<Insert Subnet Mask For Network>
GATEWAY=<Insert Default Gateway Address>
NAME=Ethernet
```

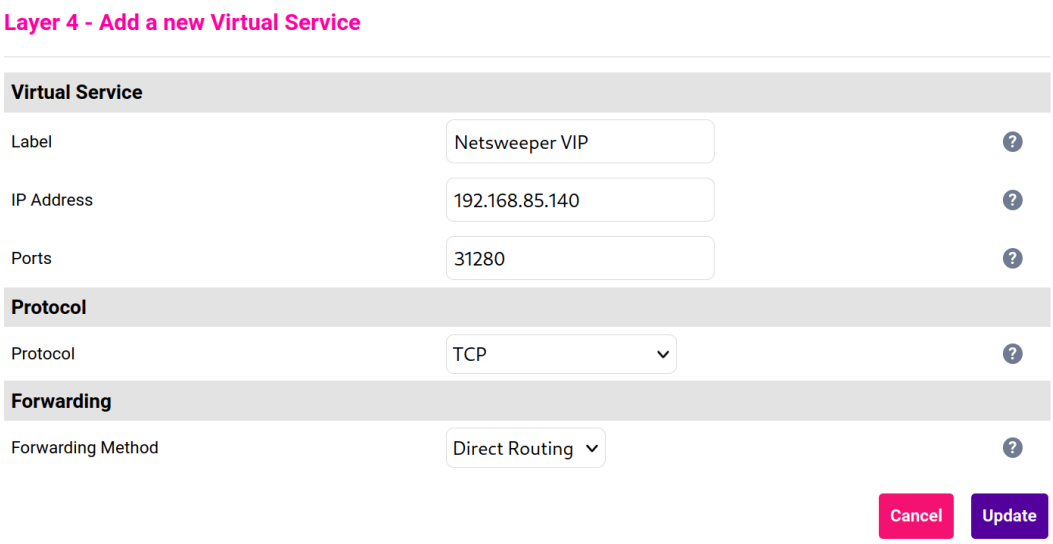
7. Press **Control+X** to prompt to exit the text editor, then press **Y** and hit the **Enter** key to save the changes.
8. Bring up the newly added eth0 network interface alias by executing the command:

```
service network restart
```

## 9.2. Loadbalancer Appliance Configuration

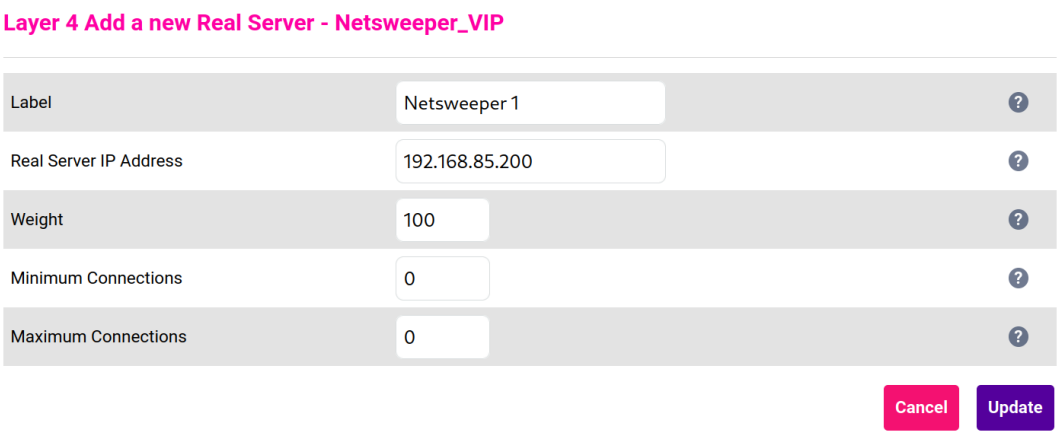
### 9.2.1. Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **Netsweeper VIP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.140**.
4. Set the *Ports* field to **31280**.
5. Set the *Protocol* to **TCP**.
6. Set the *Forwarding Method* to **Direct Routing**.
7. Click **Update** to create the virtual service.




### 9.2.2. Defining the Real Servers (RIPs)

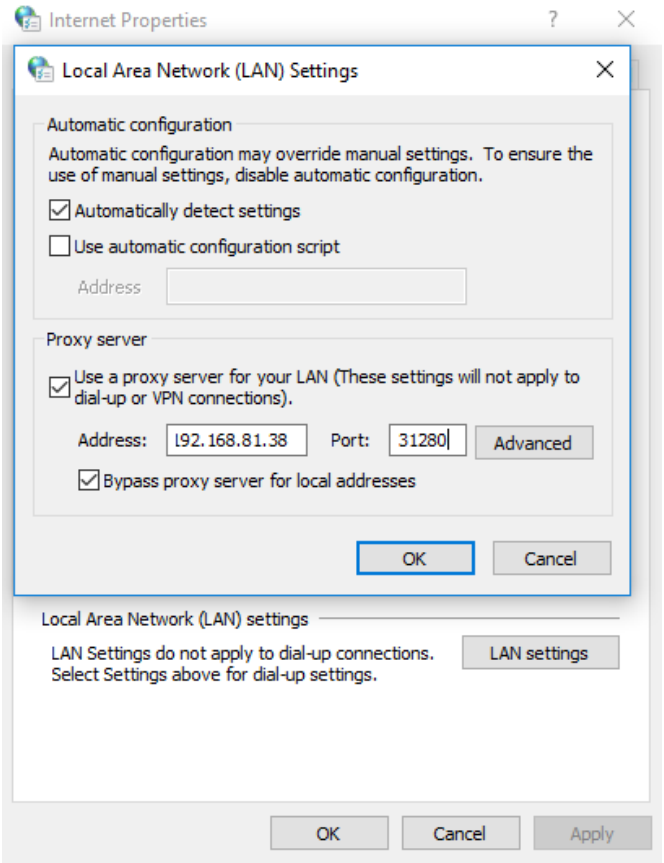
1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Netsweeper 1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Click **Update**.
5. Repeat these steps to add additional Netsweepers as real servers as required.




## 9.3. Client Browser Configuration

On every client machine, the web browsers' proxy settings should be changed to use the VIP address of the new load balanced service on port 31280.

Presented below is an example in the Chrome browser using a VIP address of 192.168.81.38:




Once this is done, the proxy and filter setup can be tested on a client machine as follows:

1. Close all running instances of the web browser.
2. Re-open the web browser, which should now be using the explicit proxy settings.
3. Try to access a website which should be blocked by Netsweeper.

This can be verified by checking the Netsweeper logs, under ***Netsweeper Web Appliance > Logs > Request Log***

*Files*. There should be a new log entry for the blocked web page used in the browser test.

# 10. Option 2 – Transparent Mode

## 10.1. Netsweeper Network Alias Configuration

The following steps should be carried out on Netsweeper software instances to configure them for load balancing using layer 4 DR mode.

These instructions will create a network alias for the loopback adaptor so that it can be assigned an additional IP address. This is required for layer 4 DR mode operation.

1. Establish an SSH session with the Netsweeper software.
2. Login to the ***admin*** account using the appropriate credentials.
3. Change to the network-scripts directory by executing the following command:

```
cd /etc/sysconfig/network-scripts
```

4. Execute the following command to create the configuration file for the loopback adaptor alias:

```
cp ifcfg-lo ifcfg-lo:0
```

5. Open the newly-created configuration file for editing, by executing the command:

```
nano ifcfg-lo:0
```

6. Edit the following lines in the configuration file to make it read like so:

```
DEVICE=lo:0
ONBOOT=YES
BOOTPROTO=static
IPADDR=<Insert Virtual IP Address>
NETMASK=255.255.255.255
GATEWAY=<Insert Default Gateway Address>
NAME=loopback
```

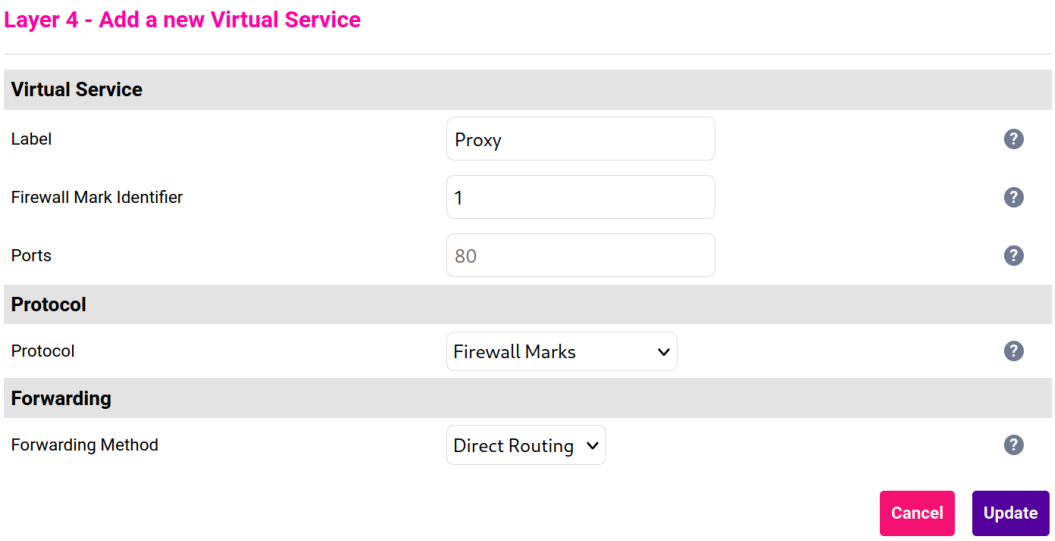
7. Press **Control+X** to prompt to exit the text editor, then press **Y** and hit the **Enter** key to save the changes.
8. Bring up the newly added loopback adaptor alias by executing the command:

```
service network restart
```

## 10.2. Loadbalancer Appliance Configuration

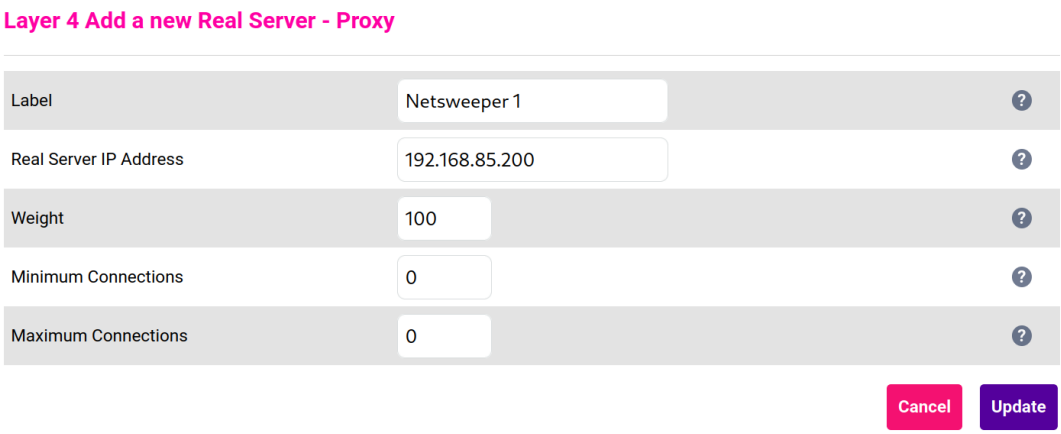
### 10.2.1. Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **Proxy**.
3. Set the *Protocol* to **Firewall Marks**.
4. Set the *Firewall Mark Identifier* to **1**.
5. Ignore the greyed-out *Ports* field as this is not used.
6. Set the *Forwarding Method* to **Direct Routing**.
7. Click **Update** to create the virtual service.




### 10.2.2. Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Netsweeper 1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Click **Update**.
5. Repeat these steps to add additional Netsweepers as real servers as required.




### 10.2.3. Firewall Script Configuration

Making transparent mode work requires making changes to the load balancer's firewall script. The following instructions should be followed to make the necessary changes.

> **Note**
>
> The *Firewall Script* page is **locked** by default on 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 web user interface, navigate to *Maintenance > Firewall Script*.
2. Under the "Manual Firewall Marks" section, uncomment the following three lines and change the value of "VIP1" to the IP address that the virtual service should listen on:

```
VIP1="10.0.0.1"
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1
```

3. Press the *Update* button to apply the changes.

## 10.3. Additional Netsweeper Configuration

Further configuration changes need to be made on the Netsweeper software.

The following steps should be followed to make the necessary changes.

1. Establish an SSH session with the Netsweeper software.
2. Login to the *admin* account using the appropriate credentials.
3. Change to the netsweeper/etc directory by executing the following command:

```
cd /usr/local/netsweeper/etc
```

4. Open the Netsweeper port mapping configuration file for editing, by executing the command:

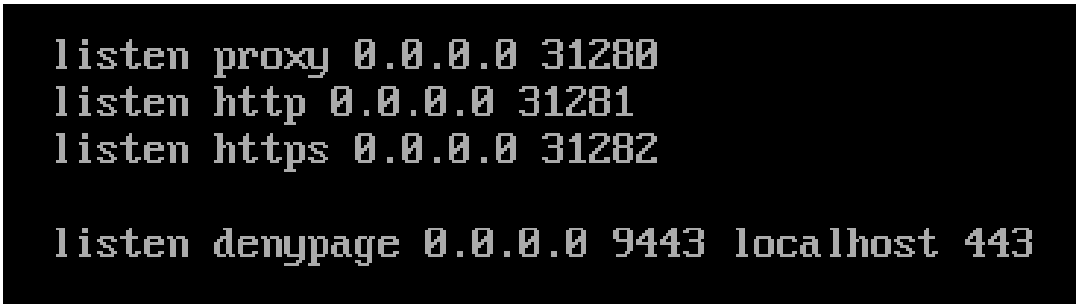
```
nano nsportmap.conf
```

5. Add the following two lines of text so that the file looks like so:


6. Press **Control+X** to prompt to exit the text editor, then press **Y** and hit the **Enter** key to save the changes.
7. Open the Netsweeper proxy configuration file for editing, by executing the command:

```
nano nsproxy.conf
```

8. Locate the section above *Access control settings* and add the following lines:




9. Press **Control+X** to prompt to exit the text editor, then press **Y** and hit the **Enter** key to save the changes.
10. Restart the port mapping service by executing the command

```
service nsportmapctl restart
```

11. Restart the proxy service by executing the command

```
service nsproxyctl restart
```

12. *Start* the port mapping service by executing the command

```
service nsportmapctl start
```

After making these changes, the Netsweeper software should now work in a transparent mode-style deployment.

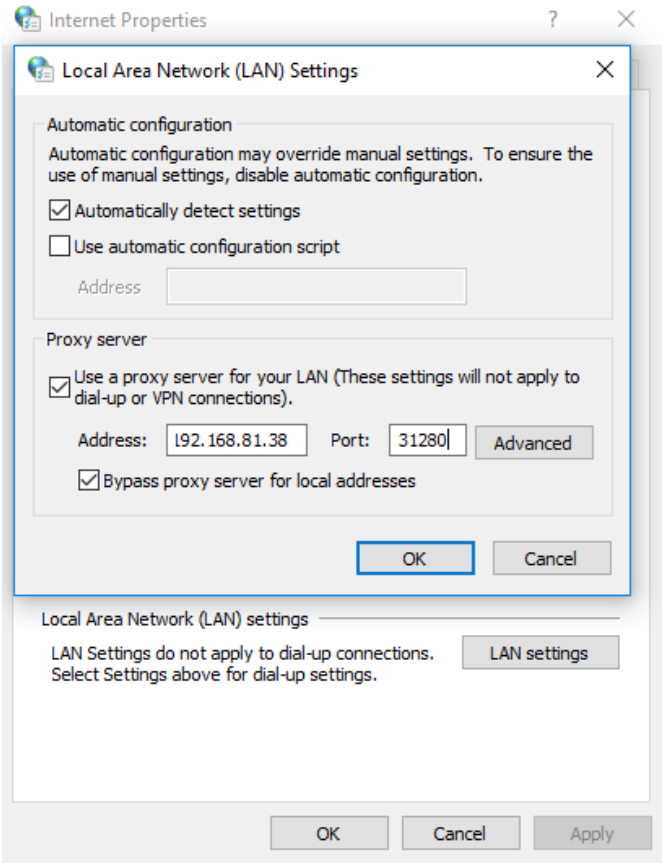
# 11. Option 3 – Non-Transparent Mode

## 11.1. Client Browser Configuration

For a non-transparent deployment, first follow through **all** of the instructions for Option 2 – Transparent Mode.

An additional step is needed to turn a transparent deployment into a non-transparent deployment. On every client machine, the web browsers' proxy settings should be changed to use the VIP address of the new load balanced service on port 31280.

Presented below is an example in the Chrome browser using a VIP address of 192.168.81.38:

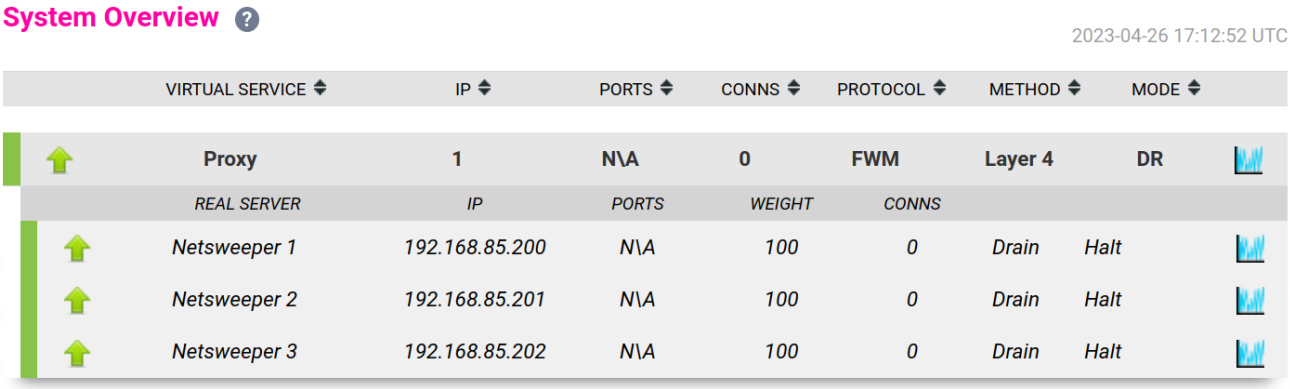



# 12. Testing & Verification

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

## 12.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Netsweepers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows a transparent mode deployment where all three Netsweepers are healthy and available to accept connections:




# 13. Technical Support

For more details about configuring the appliance and assistance with designing your deployment please don't hesitate to contact the support team using the following email address: 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.

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.

### 15.1.1. 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:

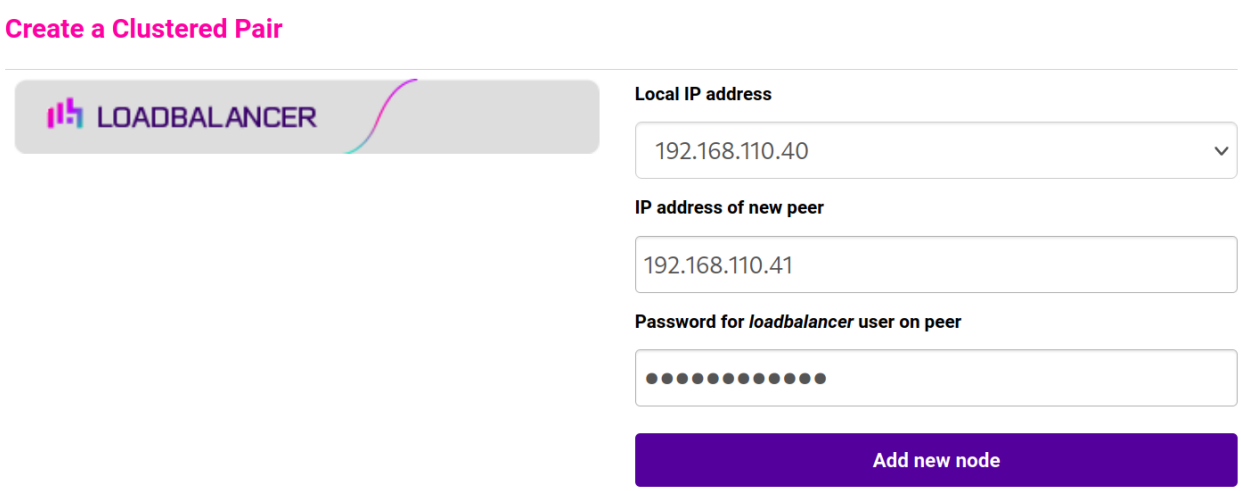
| WebUI Main Menu Option | Sub Menu Option | Description |
|---|---|---|
| Local Configuration | Hostname & DNS | Hostname and DNS settings |
| Local Configuration | Network Interface Configuration | Interface IP addresses, bonding configuration and VLANs |
| Local Configuration | Routing | Default gateways 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 | 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.

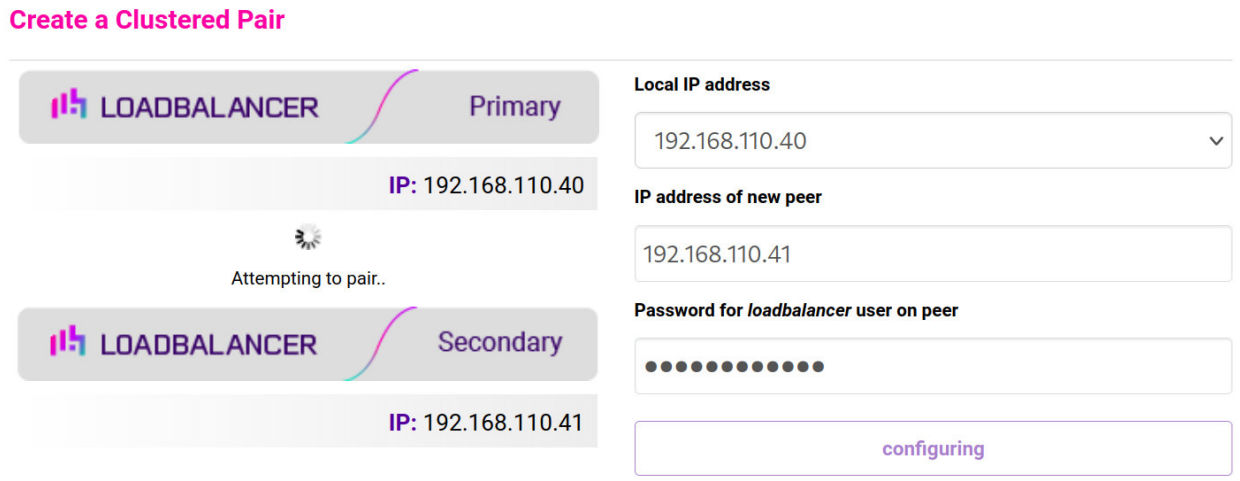
### 15.1.2. Configuring the HA Clustered Pair

> **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.

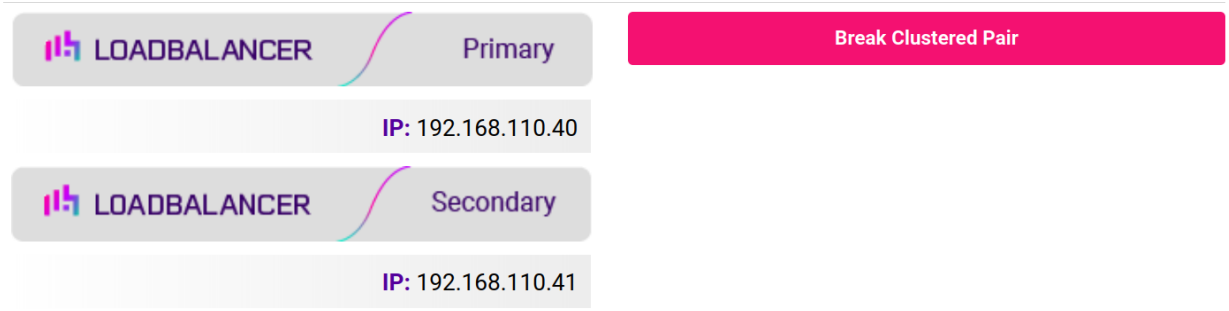
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.




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.

# 16. Document Revision History

| Version | Date | Change | Reason for Change | Changed By |
|---|---|---|---|---|
| 1.0.0 | 3 March 2018 | Initial version | | AH |
| 1.0.1 | 27 March 2018 | Change of 'ARP problem' solution to use iptables method, based on feedback from Netsweeper | Required updates | AH |
| 1.0.2 | 21 May 2018 | Terminology change at the request of Netsweeper | Required updates | AH |
| 1.0.3 | 6 December 2018 | Added the new "Company Contact Information" page | Required updates | AH |
| 1.1.0 | 9 December 2019 | Styling and layout | General styling updates | AH |
| 1.1.1 | 17 January 2020 | Added note explaining how to disable "Secure Mode" to unlock the firewall script page | Required update | RJC |
| 1.1.2 | 26 August 2020 | New title page<br><br>Updated Canadian contact details | Branding update<br><br>Change to Canadian contact details | AH |
| 1.2.0 | 26 April 2023 | Converted the document to AsciiDoc<br><br>Significant updates to bring the document into line with current documentation format<br><br>New document theme<br><br>Modified diagram colours | Document updates required moving it to the new documentation system<br><br>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.