LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Canon Enterprise Imaging Suite

Version 1.0.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced Canon Enterprise Imaging Suite environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Canon Enterprise Imaging Suite 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 Canon Enterprise Imaging Suite. 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. Canon Enterprise Imaging Suite

- v7.1.4 and later

4. Canon Enterprise Imaging Suite

Canon Enterprise Imaging Suite is made up of Vitrea View, Vitrea Connection and Vitrea Intelligence, which together provide a full end-to-end PACS and image analytics solution. The suite provides vendor-neutral archive (VNA) viewing options, image and data sharing in addition to analytics and informatics tools.

5. Load Balancing Canon Enterprise Imaging Suite

> **Note** It's highly recommended that you have a working Canon Enterprise Imaging Suite environment first before implementing the load balancer.

5.1. Load Balancing & HA Requirements

The applications that form the Canon Enterprise Imaging Suite require load balancing in order to provide high

availability (HA) across multiple Real Servers, and to distribute application traffic between them to provide sufficient capacity for the intended deployment environment.

5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Canon Enterprise Imaging Suite, the following VIPs are required:

Ref.	VIP Name	Mode	Port(s)	Persistence Mode	Health Check
VIP 1	DicomRouting	L4 DR	TCP/11112	Source IP	Connect to Port
VIP 2	DicomInternal	L4 DR	TCP/11112	Source IP	Connect to Port
VIP 3	HL7Live	L4 DR	TCP/2398	Source IP	Connect to Port
VIP 4	HL7Migrate	L4 DR	TCP/2988	Source IP	Connect to Port
VIP 5	MWL	L4 DR	TCP/4106	Source IP	Connect to Port
VIP 6	VPWorklistHL7Live	L4 DR	TCP/19001	Source IP	Connect to Port
VIP 7	VPWorklistHL7Migrate	L4 DR	TCP/19002	Source IP	Connect to Port
VIP 8	MINT	L4 DR	TCP/8080	Source IP	Connect to Port
VIP 9	WorklistHL7Draft	L4 DR	TCP/19011	Source IP	Connect to Port
VIP 10	WorklistHL7Prelim	L4 DR	TCP/19012	Source IP	Connect to Port
VIP 11	WorklistHL7Signed	L4 DR	TCP/19013	Source IP	Connect to Port
VIP 12	VC_AdminTools	L7 SNAT	TCP/8238	HTTP Cookie	Connect to Port
VIP 13	AuthM	L7 SNAT	TCP/8236	HTTP Cookie	Connect to Port
VIP 14	VitreaRead	L7 SNAT	TCP/8237	HTTP Cookie	Connect to Port
VIP 15	Worklist	L7 SNAT	TCP/8089	HTTP Cookie	Connect to Port
VIP 16	VPSmartReporting	L7 SNAT	TCP/8994	HTTP Cookie	Connect to Port

5.3. TLS/SSL Termination

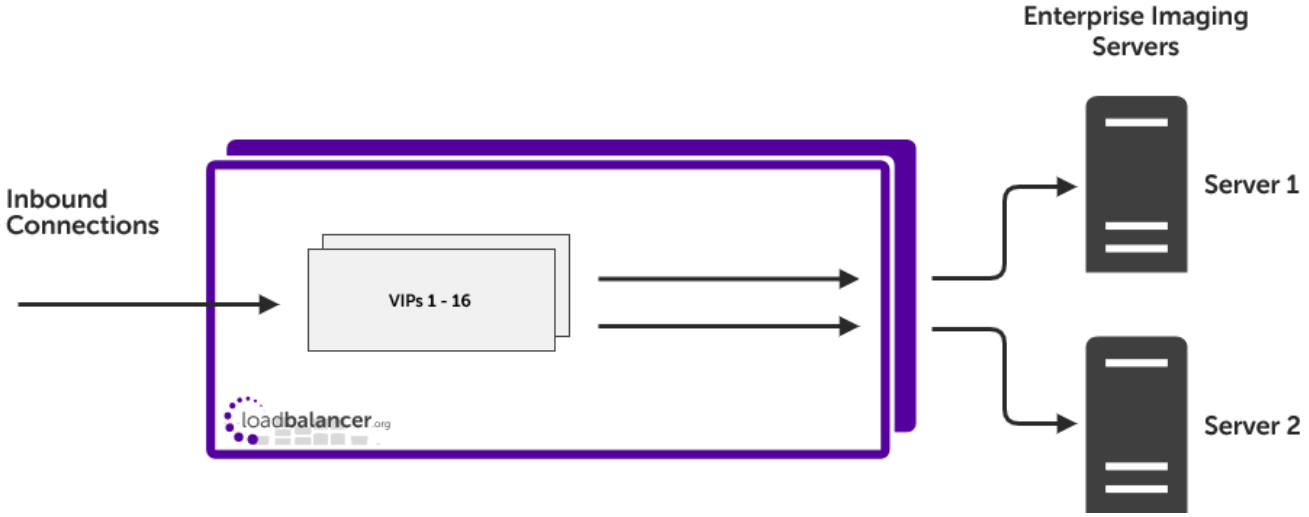
SSL Termination is configured on the load balancer for the following VIPs:

- VIP12 - **VC_AdminTools**
- VIP13 - **AuthM**
- VIP14 - **VitreaRead**
- VIP15 - **Worklist**
- VIP16 - **VPSmartReporting**

This provides a corresponding HTTPS Virtual Service for these VIPs. Certificates in PEM or PFX format can be uploaded to the load balancer.

6. Deployment Concept

Once the load balancer is deployed, clients connect to the Virtual Services (VIPs) rather than connecting directly to one of the Canon Enterprise Imaging Suite servers. These connections are then load balanced across the Canon Enterprise Imaging Suite servers to distribute the load according to the load balancing algorithm selected.



> **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. Load Balancer Deployment Methods

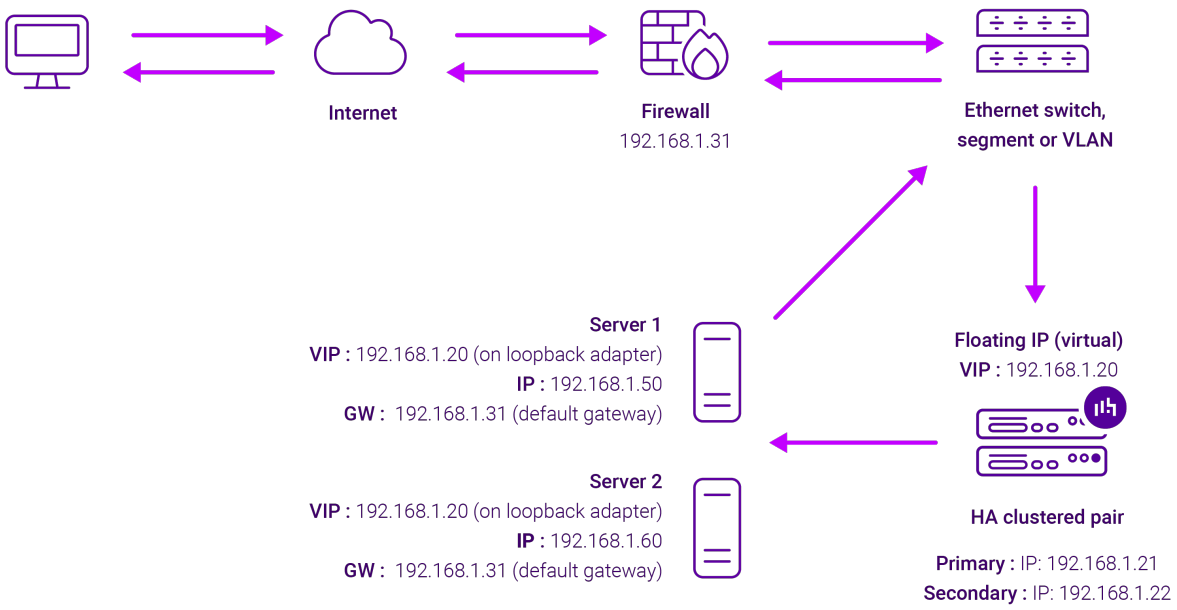
The load balancer can be deployed in 4 fundamental ways: ***Layer 4 DR mode***, ***Layer 4 NAT mode***, ***Layer 4 SNAT mode***, and ***Layer 7 SNAT mode***.

For Canon Enterprise Imaging Suite, both layer 4 DR mode and layer 7 SNAT mode are used. These modes are described below and are used for the configurations presented in this guide.

7.1. Layer 4 DR Mode

Layer 4 DR (Direct Routing) mode is a very high performance solution that requires little change to your existing infrastructure. The image below shows an example network diagram for this mode.

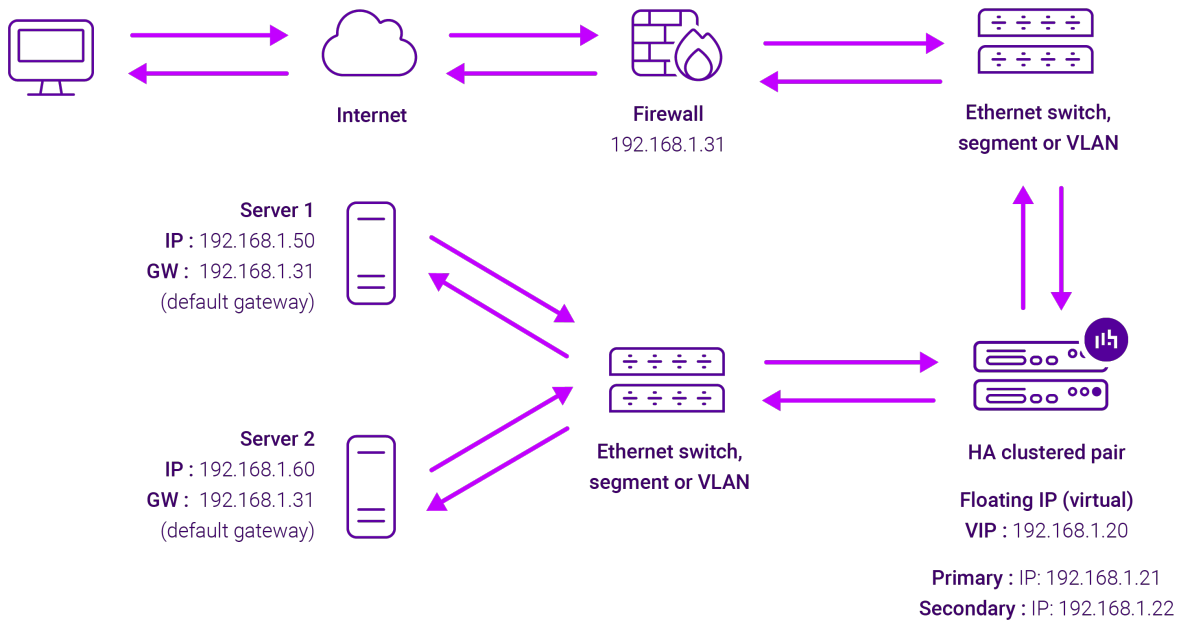
> **Note** Kemp, Brocade, Barracuda & A10 Networks call this ***Direct Server Return*** and F5 call it ***nPath***.



- 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.

7.2. Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer and HAProxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods. The image below shows an example network diagram for this mode.



- Because layer 7 SNAT mode is a full proxy, Real Servers in the cluster can be on any accessible network including across the Internet or WAN.
- Layer 7 SNAT mode is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancer's own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address). This can be configured per layer 7 VIP. If required, the load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client's source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to Transparency at Layer 7.
- Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, **eth1** is typically used for client side connections and **eth0** is used for Real Server connections, although this is not mandatory since any interface can be used for any purpose.
- Requires no mode-specific configuration changes to the load balanced Real Servers.
- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.
- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

8. Configuring Canon Enterprise Imaging Suite for Load Balancing

8.1. When using Layer 7 SNAT Mode

Layer 7 SNAT mode VIPs do not require any mode specific configuration changes to the load balanced Real Servers (Enterprise Imaging Servers).

8.2. When using Layer 4 DR Mode

Layer 4 DR mode VIPs require the "ARP problem" to be solved on each load balanced Real Server. This enables DR mode to work correctly.

Detailed steps on solving the "ARP problem" for Windows 2012 & later are presented below. These steps must be followed on each Real Server.

8.2.1. Windows Server 2012 & Later

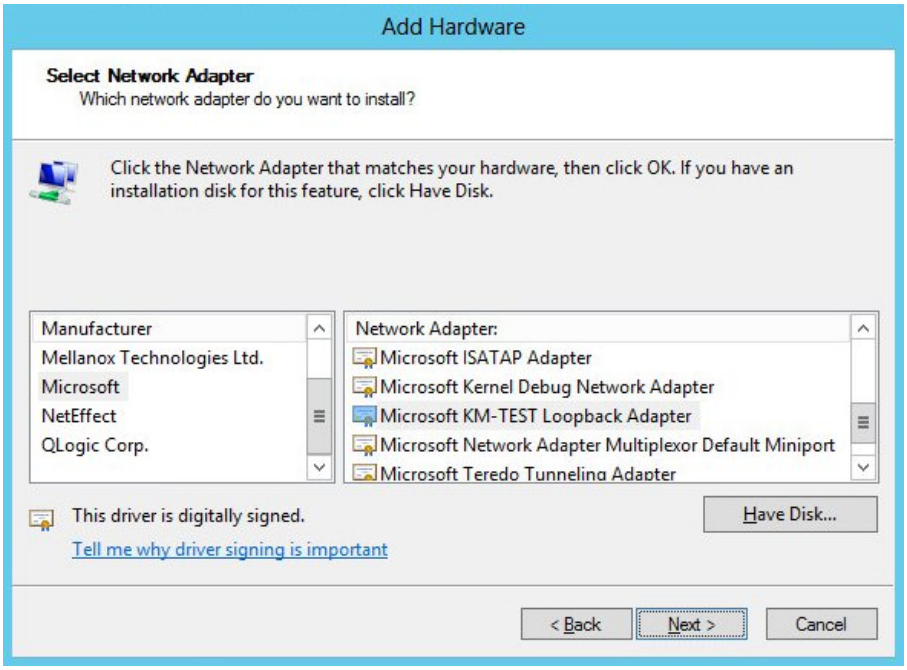
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables the server to receive packets that have their destination set as the VIP address. If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

In addition, the strong/weak host behavior must be configured on each Real Server. The weak host model allows packets with any IP to be sent or received via an interface. The strong host model only allows packets with an IP belonging to the interface to be sent or received.

> **Important** The following 3 steps must be completed on ***all*** Real Servers associated with the VIP.

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. Once the Wizard has started, click **Next**.
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.
4. Select **Network adapters**, click **Next**.



5. Select **Microsoft** & **Microsoft KM-Test Loopback Adapter**, click **Next**.
6. Click **Next** to start the installation, when complete click **Finish**.

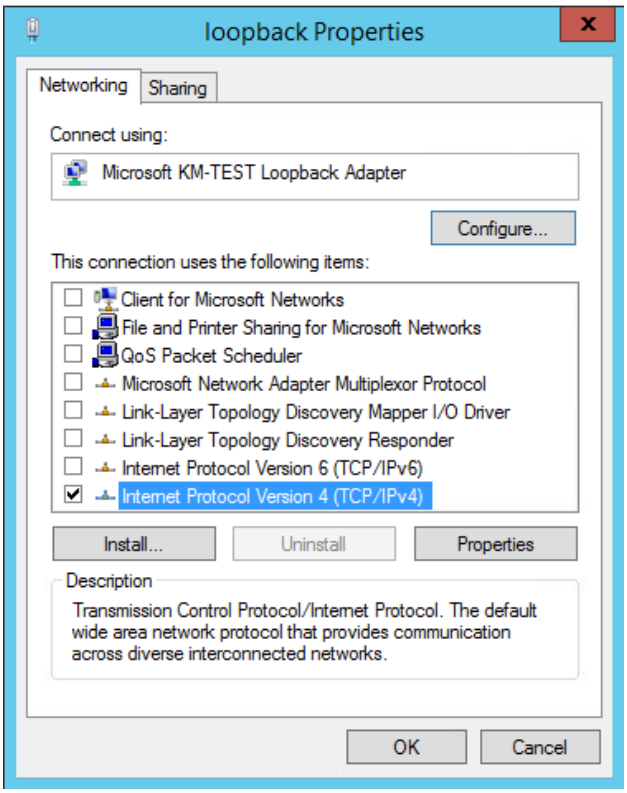
Step 2 of 3: Configure the Loopback Adapter

1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the new Loopback Adapter and select **Properties**.

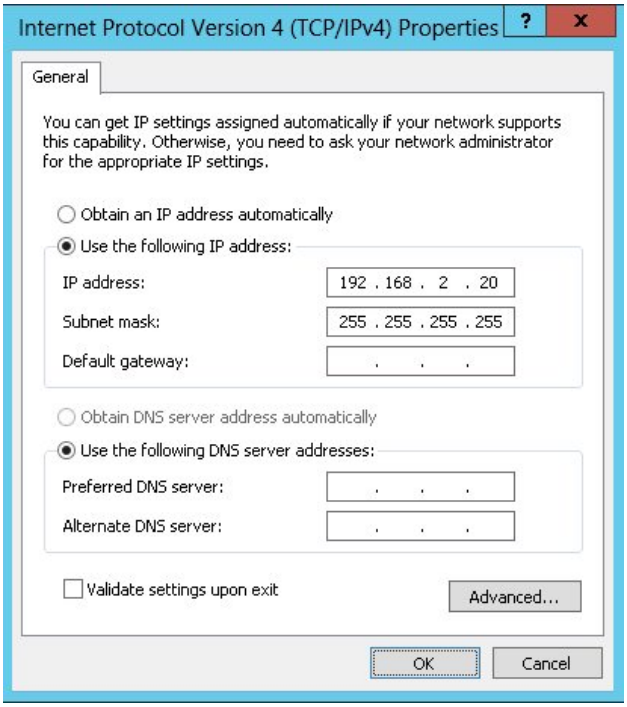
> **Note** You can configure IPv4 or IPv6 addresses or both depending on your requirements.

IPv4 Addresses

1. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below:



2. Ensure that **Internet Protocol Version (TCP/IPv4)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service address (VIP) with a subnet mask of **255.255.255.255**, e.g. **192.168.2.20/255.255.255.255** as shown below:



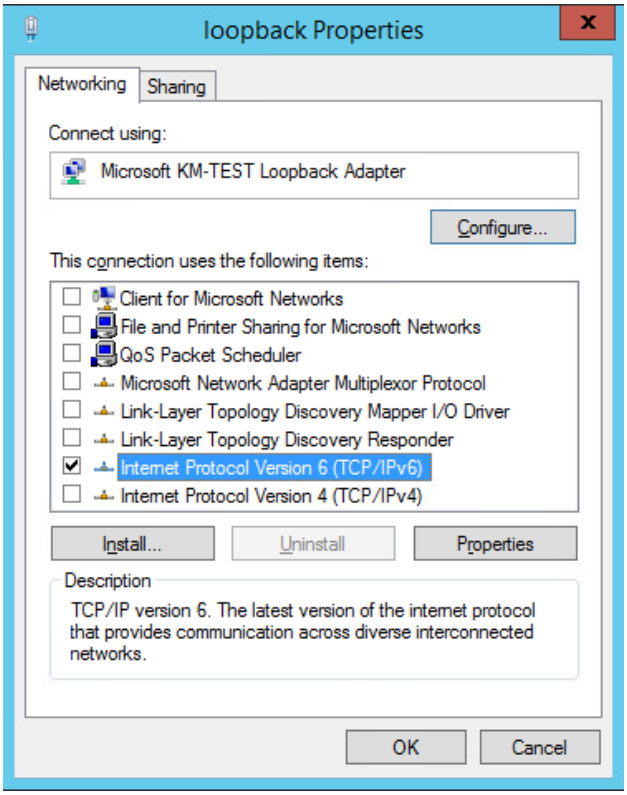
> **Note** **192.168.2.20** is an example, make sure you specify the correct VIP address.

> **Note** If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

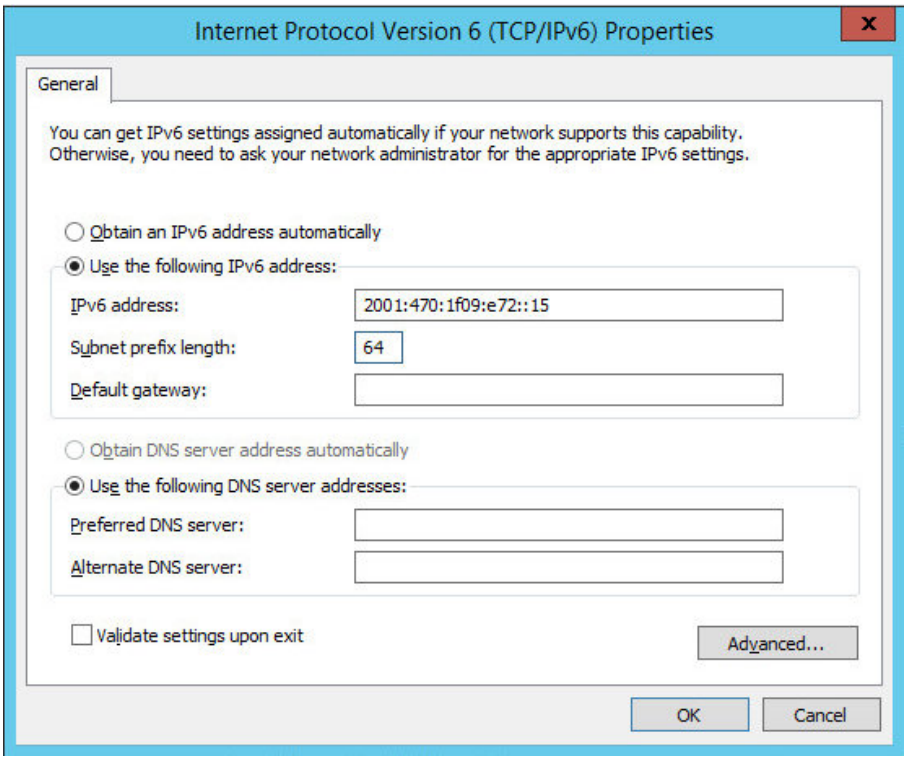
3. Click **OK** then click **Close** to save and apply the new settings.

IPv6 Addresses

1. Uncheck all items except **Internet Protocol Version 6 (TCP/IPv6)** as shown below:



2. Ensure that **Internet Protocol Version (TCP/IPv6)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) and set the ***Subnet Prefix Length*** to be the same as your network setting, e.g. **2001:470:1f09:e72::15/64** as shown below:



> **Note** **2001:470:1f09:e72::15/64** is an example, make sure you specify the correct VIP address.

> **Note** If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be

added to the Loopback Adapter.

3. Click **OK** then click **Close** to save and apply the new settings.

Step 3 of 3: Configure the strong/weak host behavior

The strong/weak host behavior can be configured using either of the following 2 methods:

- Option 1 - Using network shell (netsh) commands
- Option 2 - Using PowerShell cmdlets

The commands in this section assume that the LAN Adapter is named "**net**" and the Loopback Adapter is named "**loopback**" as shown in the example below:

> **Important** Either adjust the commands to use the names allocated to your LAN and loopback adapters, or rename the adapters before running the commands. Names are case sensitive so make sure that the interface names used in the commands match the adapter names exactly.

Option 1 - Using Network Shell (netsh) Commands

To configure the correct strong/weak host behavior run the following commands:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

Option 2 - Using PowerShell Cmdlets

For IPv4 addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv4
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4
```

For IPv6 Addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv6
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6
```

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.

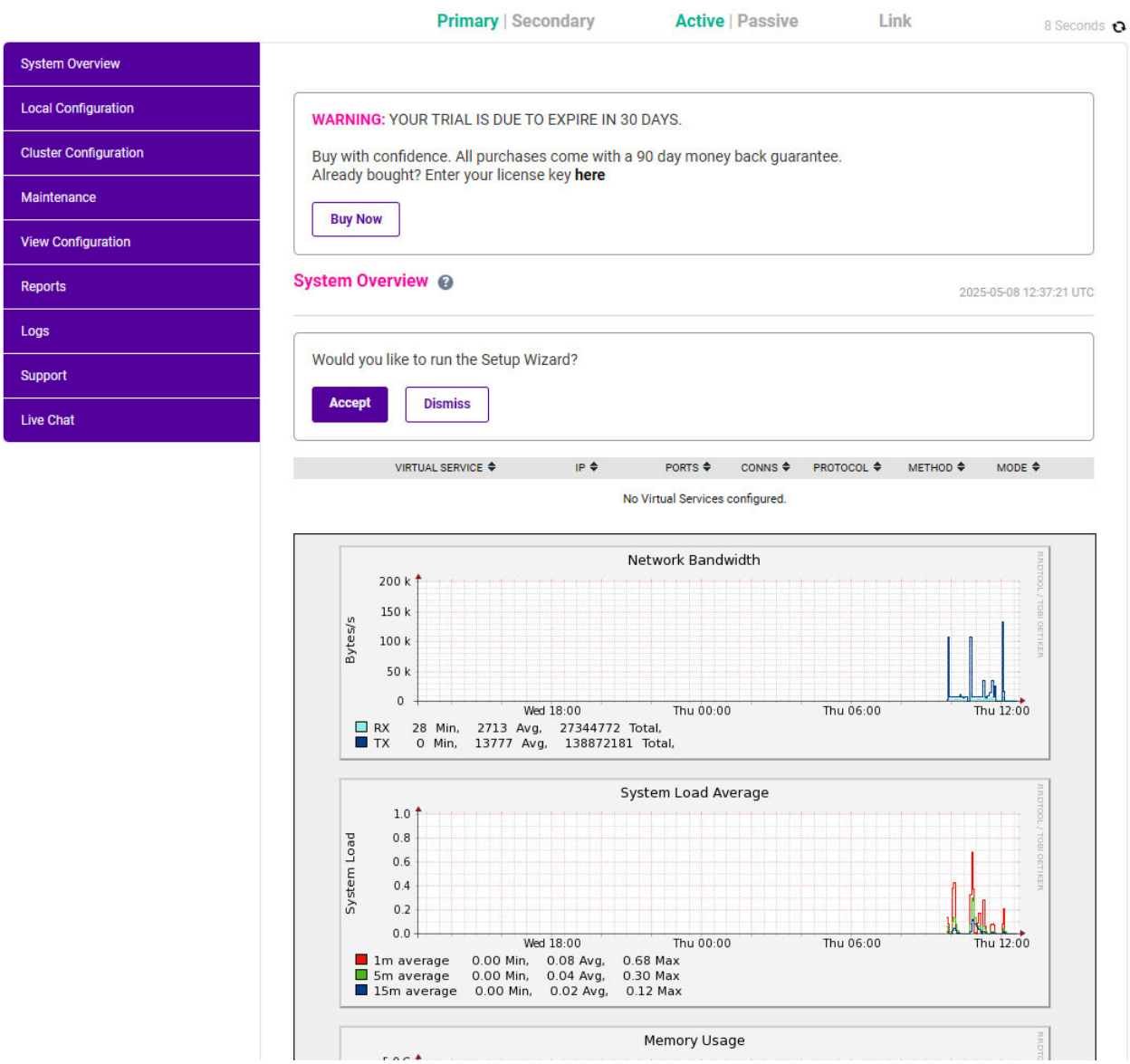
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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. 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.

9.3.1. 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

9.4. Appliance Software Update

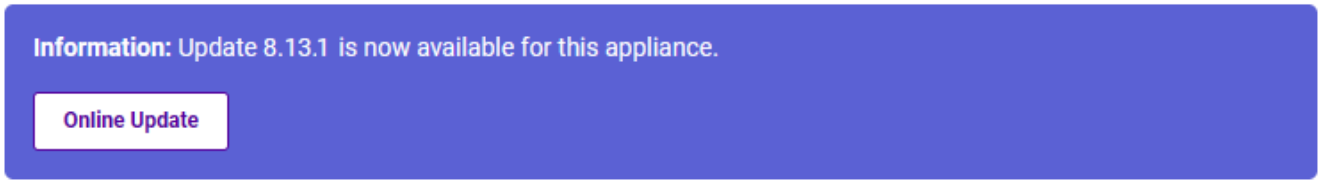
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **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.

9.4.1. Online Update

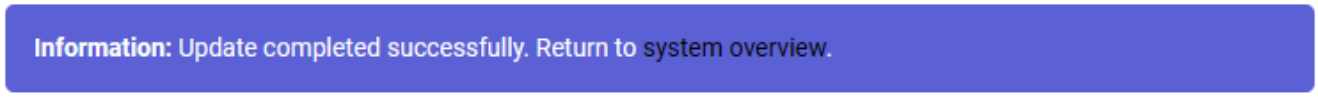
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



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.

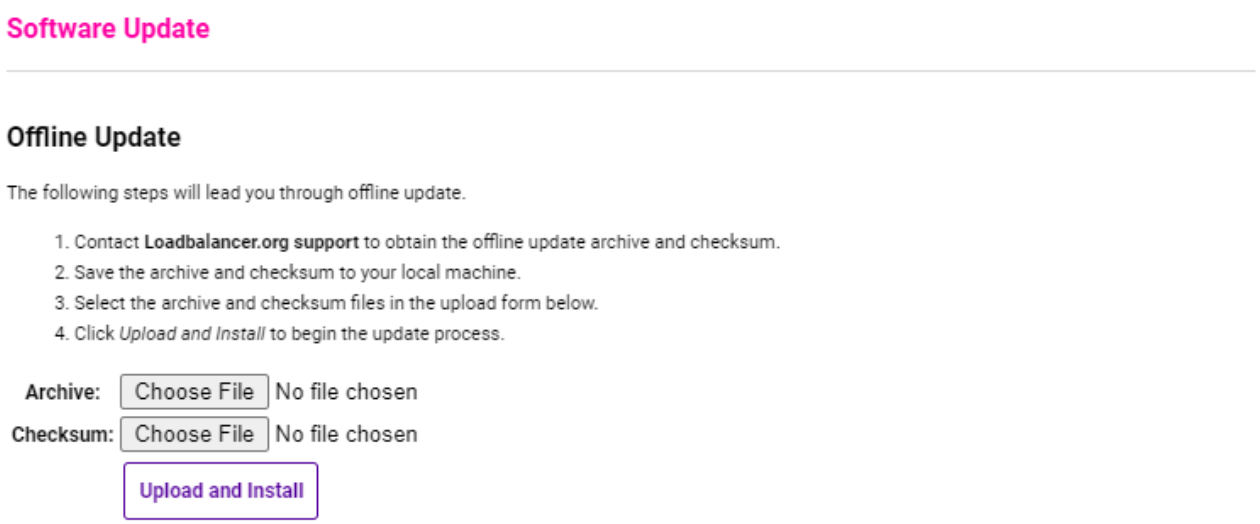
9.4.2. Offline Update

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.

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
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

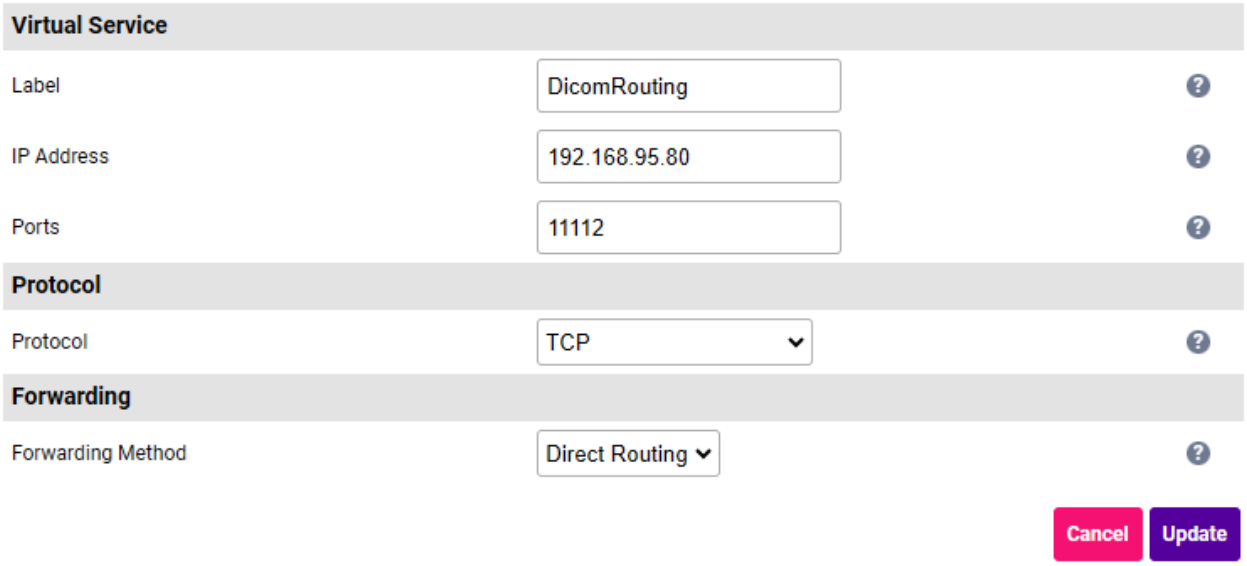
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in the section Configuring HA - Adding a Secondary Appliance of the appendix.

10. Appliance Configuration for Canon Enterprise Imaging Suite

10.1. VIP 1 - DicomRouting

10.1.1. Virtual Service (VIP) Configuration

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



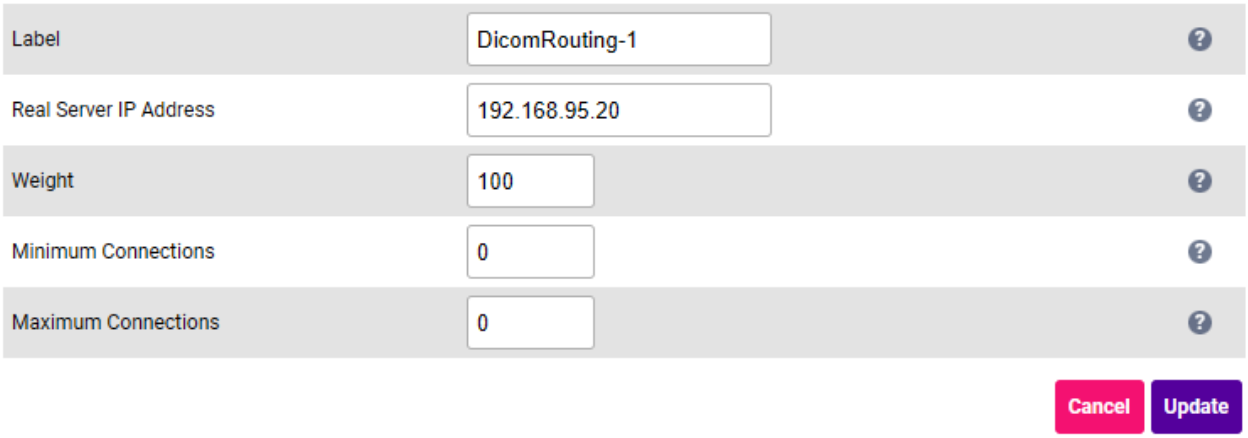
   - Specify an appropriate *Label* for the Virtual Service, e.g. **DicomRouting**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.80**.
   - Set the *Ports* field to **11112**.
   - Leave the *Protocol* set to **TCP**.
   - Leave the *Forwarding Method* set to **Direct Routing**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.

- Set the *Balance Mode* to **Weighted Round Robin**.

6. Leave all other settings at their default value.
7. Click **Update**.

10.1.2. Define the Associated Real Servers (RIPs)

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



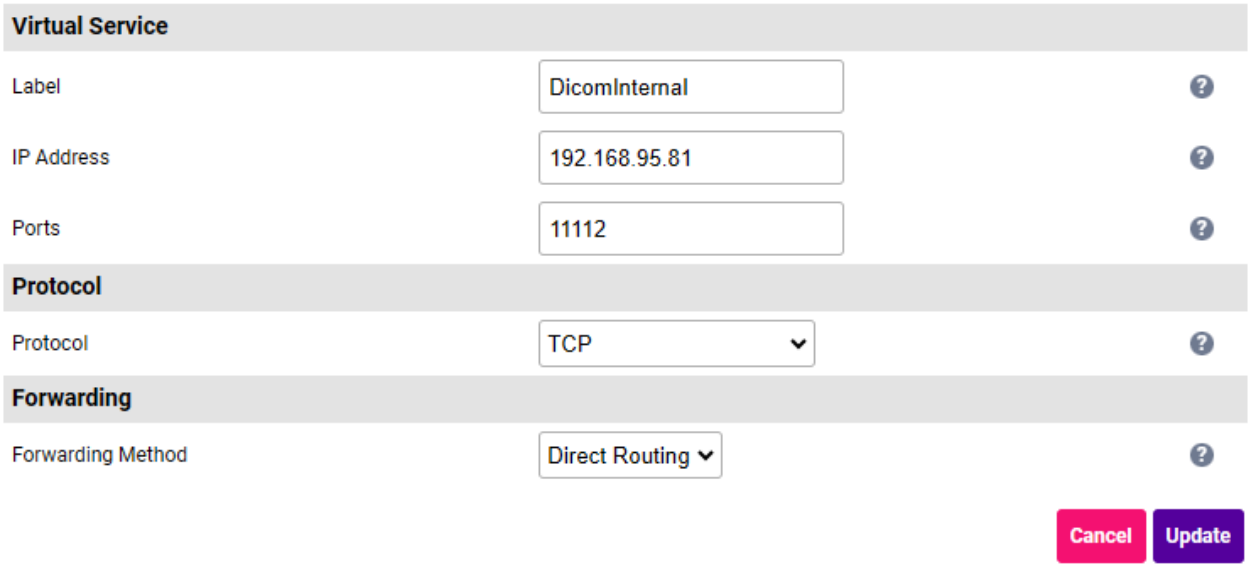
- Specify an appropriate *Label* for the RIP, e.g. **DicomRouting-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.2. VIP 2 - DicomInternal

10.2.1. Virtual Service (VIP) Configuration

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

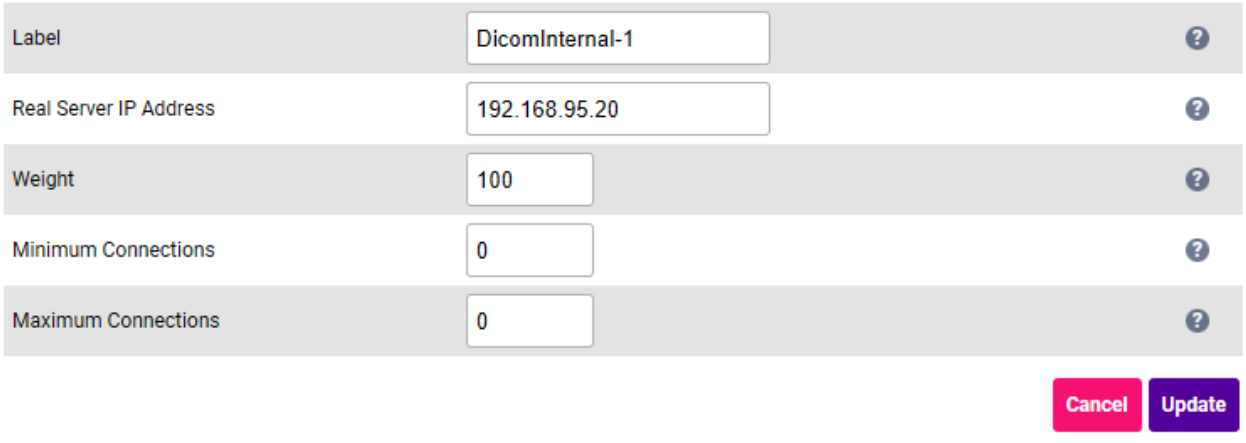


- Specify an appropriate *Label* for the Virtual Service, e.g. **DicomInternal**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.81**.
- Set the *Ports* field to **11112**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.

10.2.2. Define the Associated Real Servers (RIPs)

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



- Specify an appropriate *Label* for the RIP, e.g. **DicomInternal-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

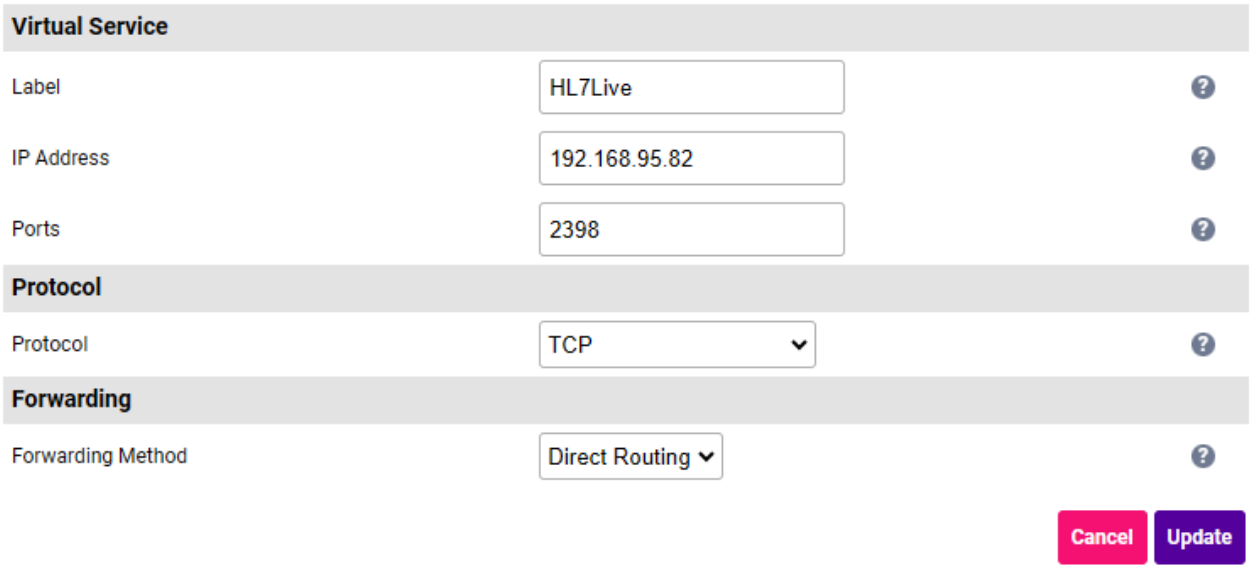
3. Leave all other settings at their default value.

4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.3. VIP 3 - HL7Live

10.3.1. Virtual Service (VIP) Configuration

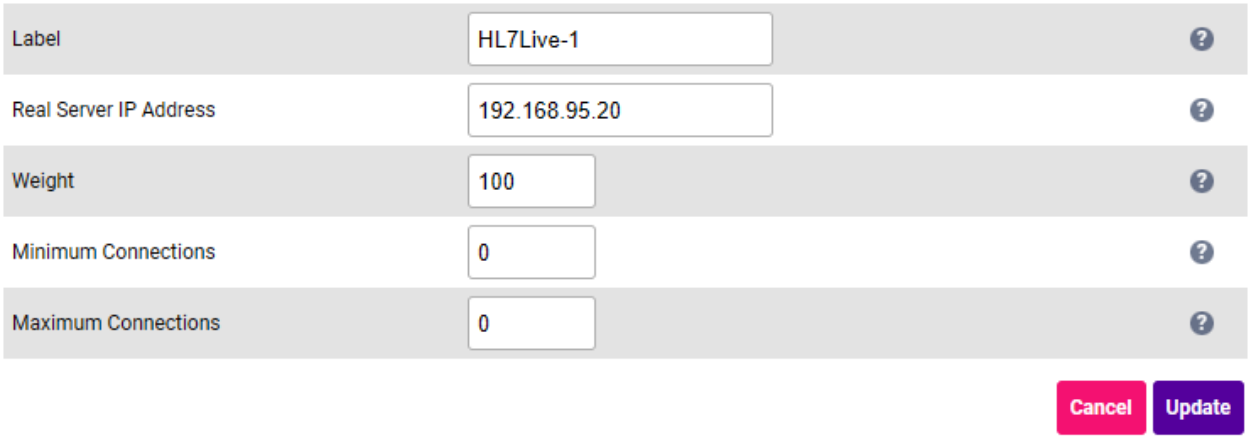
1. Using the WebUI, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:



   - Specify an appropriate *Label* for the Virtual Service, e.g. **HL7Live**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.82**.
   - Set the *Ports* field to **2398**.
   - Leave the *Protocol* set to **TCP**.
   - Leave the *Forwarding Method* set to **Direct Routing**.
3. Click **Update** to create the Virtual Service.

10.3.2. Define the Associated Real Servers (RIPs)

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



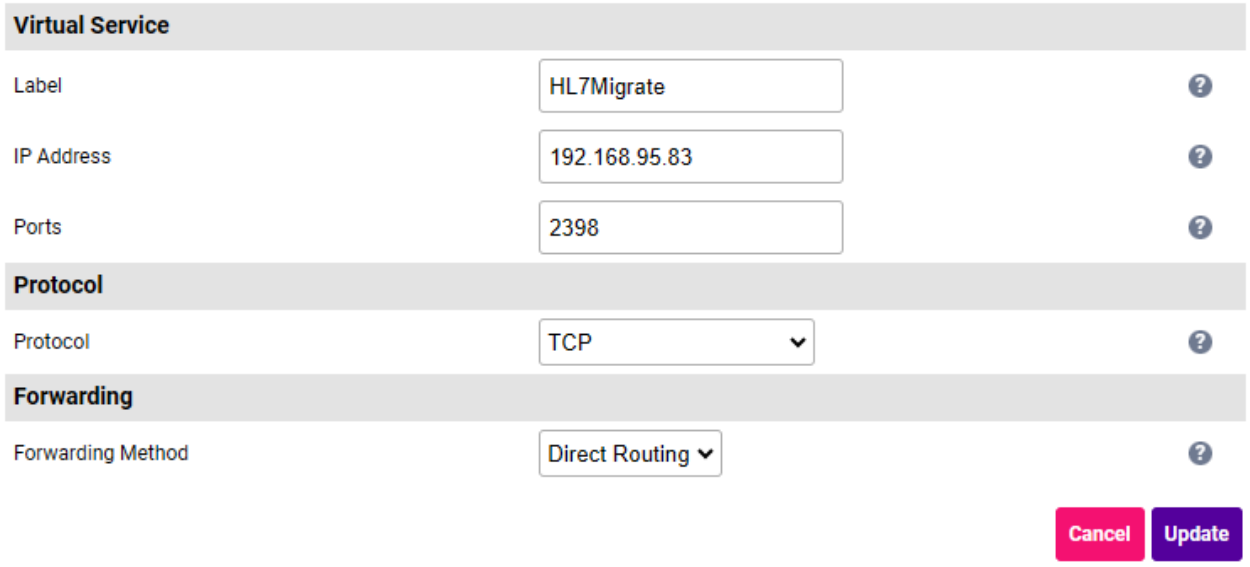
- Specify an appropriate *Label* for the RIP, e.g. **HL7Live-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.4. VIP 4 - HL7Migrate

10.4.1. Virtual Service (VIP) Configuration

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



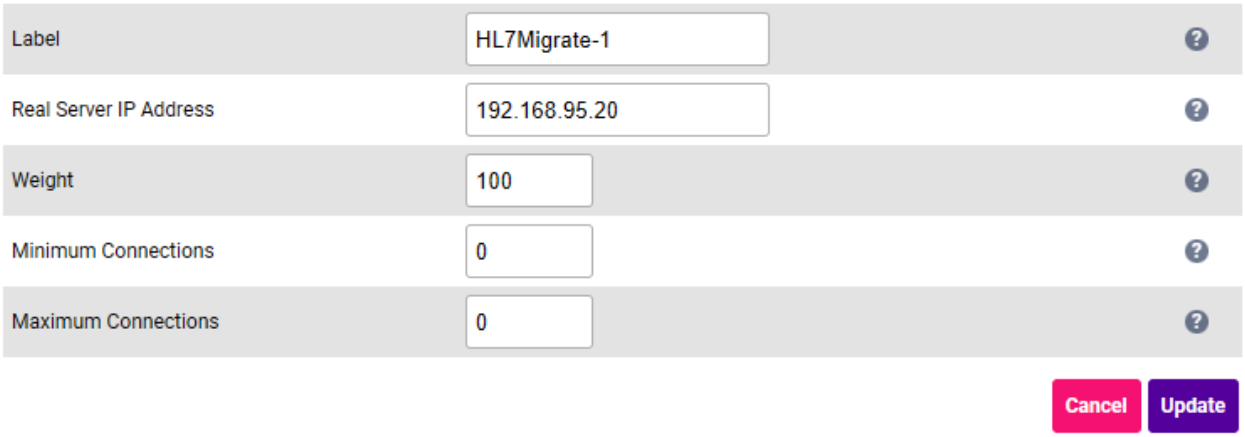
- Specify an appropriate *Label* for the Virtual Service, e.g. **HL7Migrate**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.83**.
- Set the *Ports* field to **2988**.

- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.

10.4.2. Define the Associated Real Servers (RIPs)

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



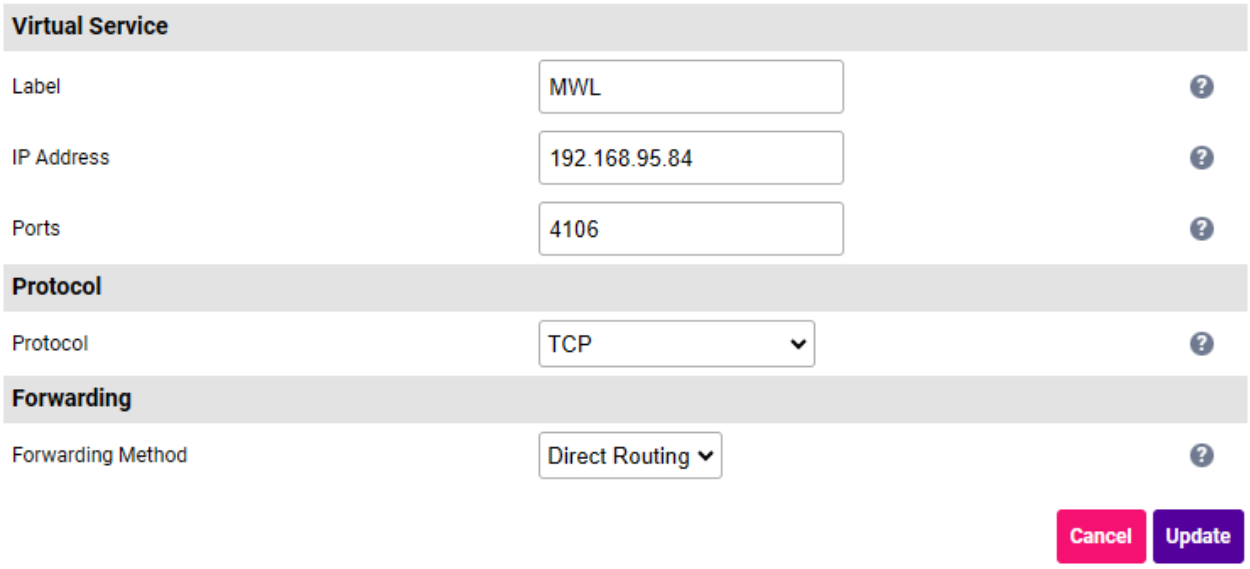
- Specify an appropriate *Label* for the RIP, e.g. **HL7Migrate-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.5. VIP 5 - MWL

10.5.1. Virtual Service (VIP) Configuration

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

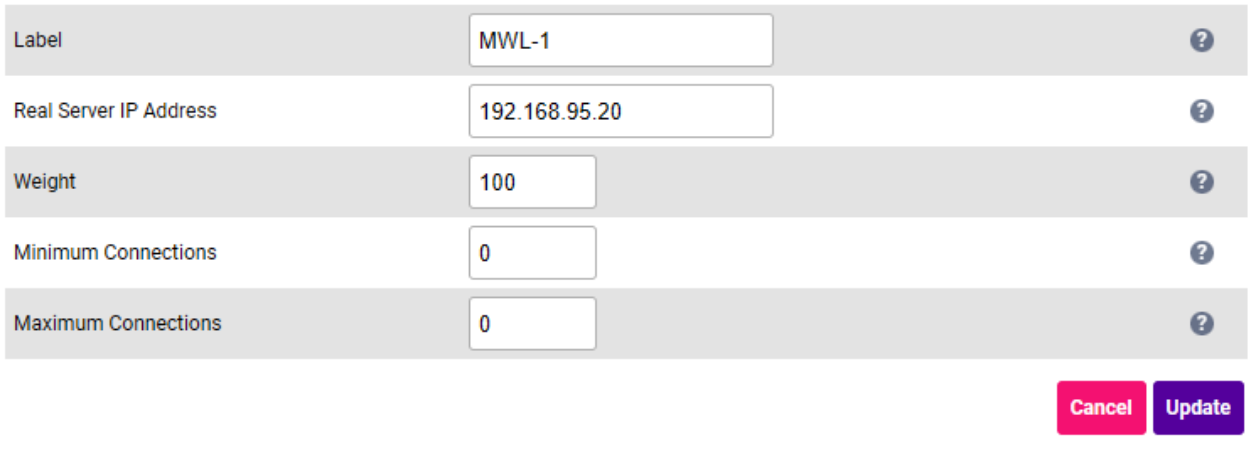


- Specify an appropriate *Label* for the Virtual Service, e.g. **MWL**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.84**.
- Set the *Ports* field to **4106**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.

10.5.2. Define the Associated Real Servers (RIPs)

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



- Specify an appropriate *Label* for the RIP, e.g. **MWL-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

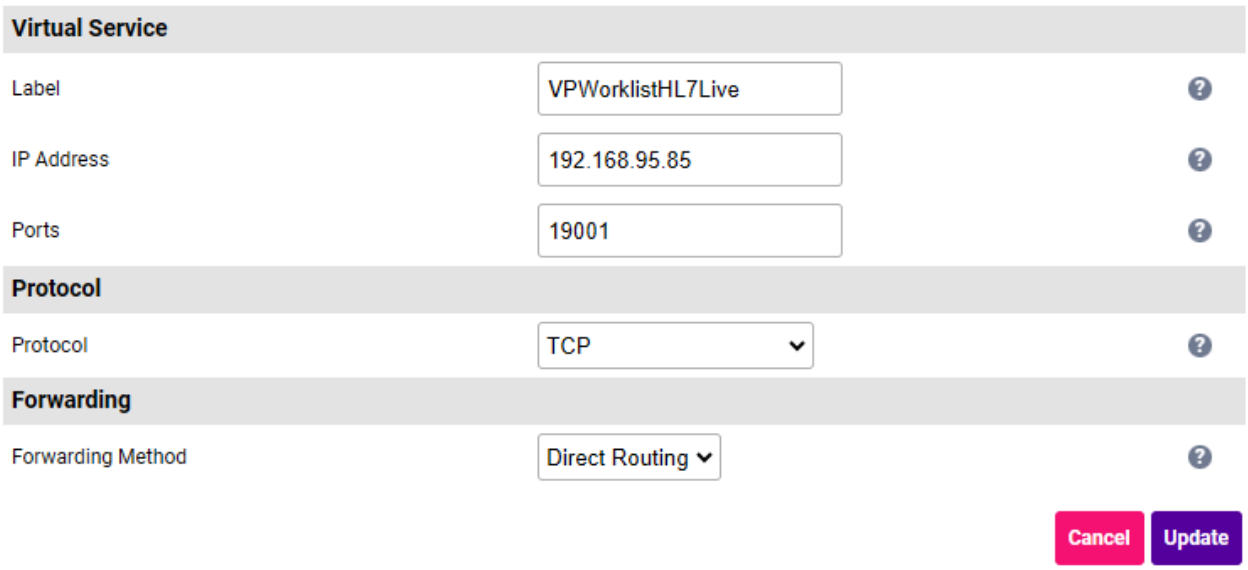
3. Leave all other settings at their default value.

4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.6. VIP 6 - VPWorklistHL7Live

10.6.1. Virtual Service (VIP) Configuration

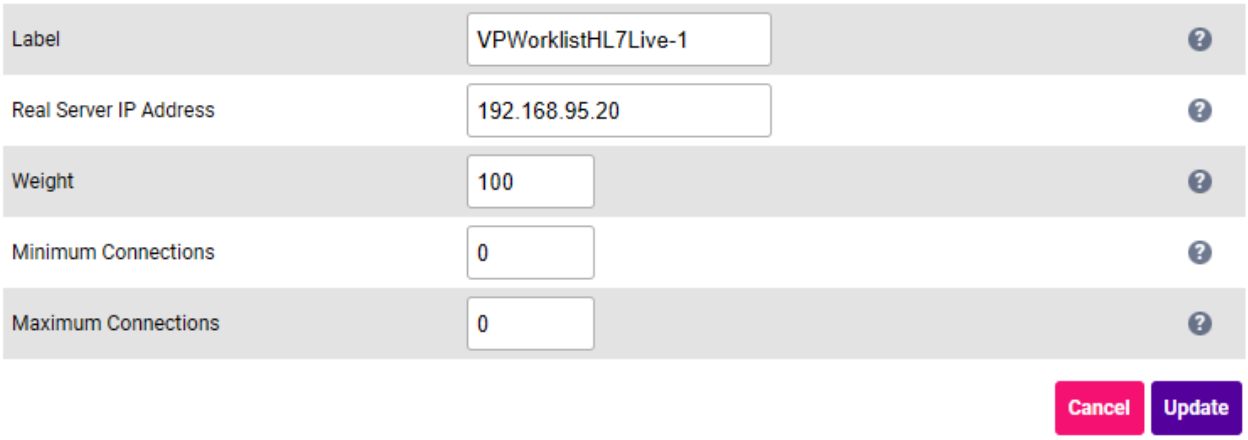
1. Using the WebUI, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:



   - Specify an appropriate *Label* for the Virtual Service, e.g. **VPWorklistHL7Live**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.85**.
   - Set the *Ports* field to **19001**.
   - Leave the *Protocol* set to **TCP**.
   - Leave the *Forwarding Method* set to **Direct Routing**.
3. Click **Update** to create the Virtual Service.

10.6.2. Define the Associated Real Servers (RIPs)

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



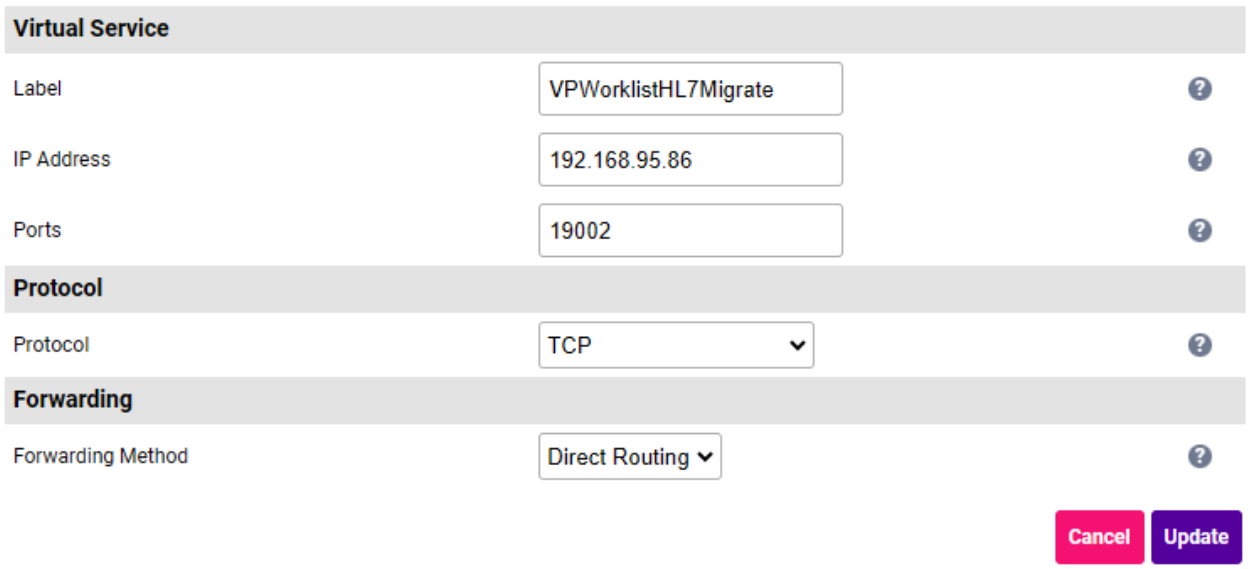
- Specify an appropriate *Label* for the RIP, e.g. **VPWorklistHL7Live-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.7. VIP 7 - VPWorklistHL7Migrate

10.7.1. Virtual Service (VIP) Configuration

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



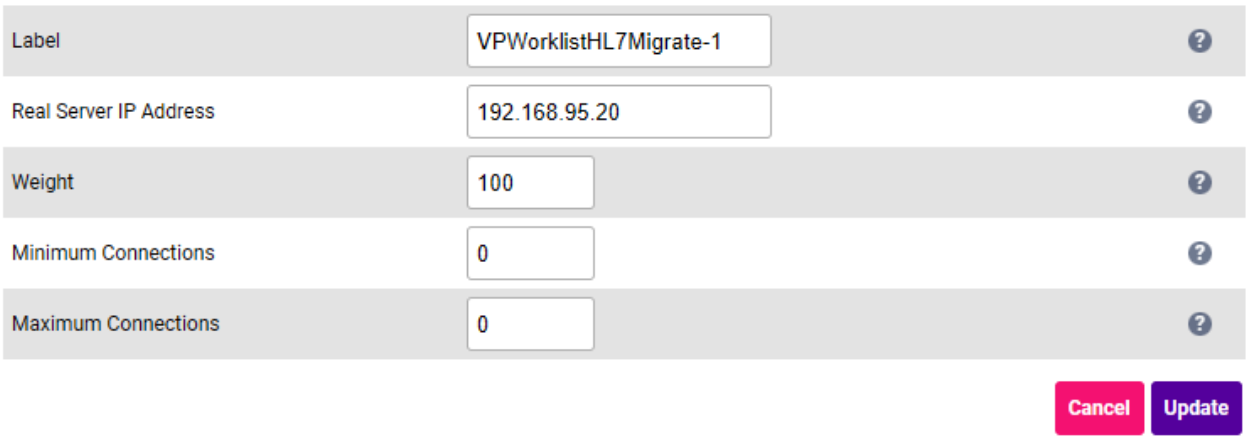
- Specify an appropriate *Label* for the Virtual Service, e.g. **VPWorklistHL7Migrate**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.86**.
- Set the *Ports* field to **19002**.

- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.

10.7.2. Define the Associated Real Servers (RIPs)

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



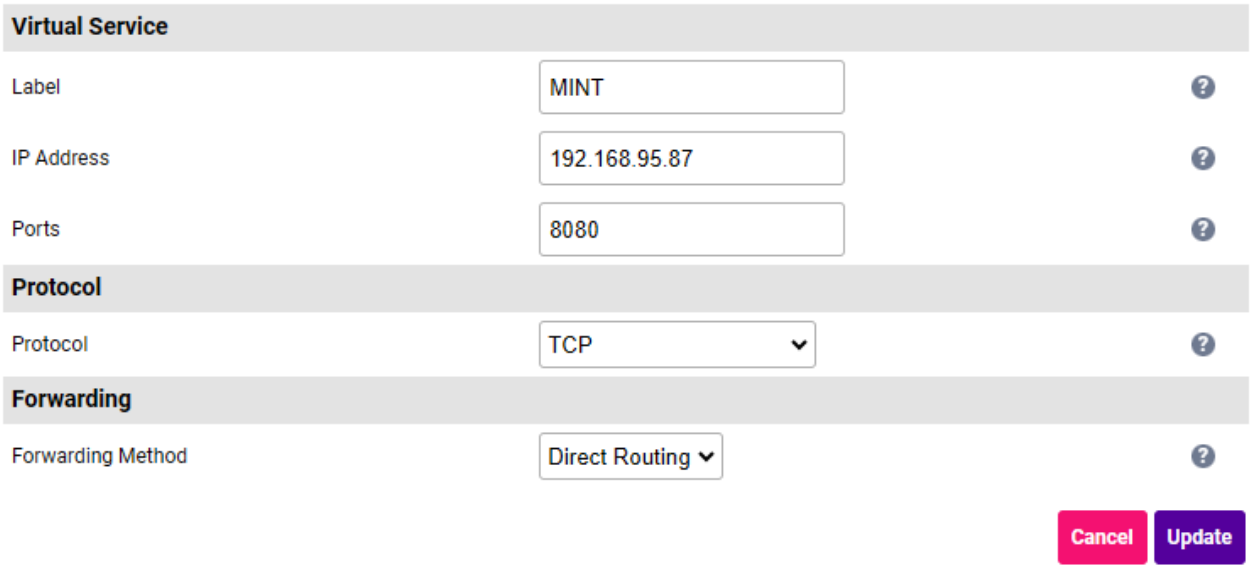
- Specify an appropriate *Label* for the RIP, e.g. **VPWorklistHL7Migrate-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.8. VIP 8 - MINT

10.8.1. Virtual Service (VIP) Configuration

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

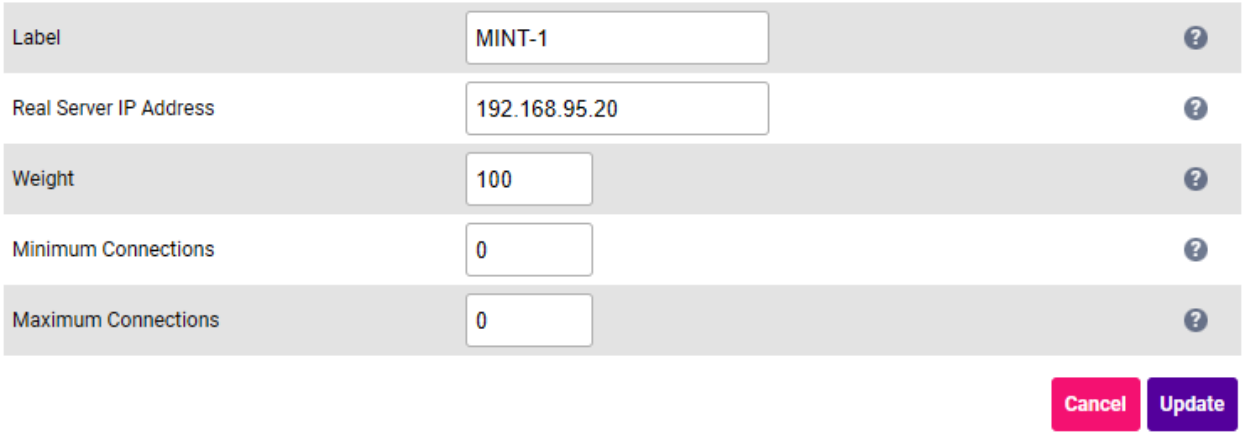


- Specify an appropriate *Label* for the Virtual Service, e.g. **MINT**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.87**.
- Set the *Ports* field to **8080**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.

10.8.2. Define the Associated Real Servers (RIPs)

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



- Specify an appropriate *Label* for the RIP, e.g. **MINT-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

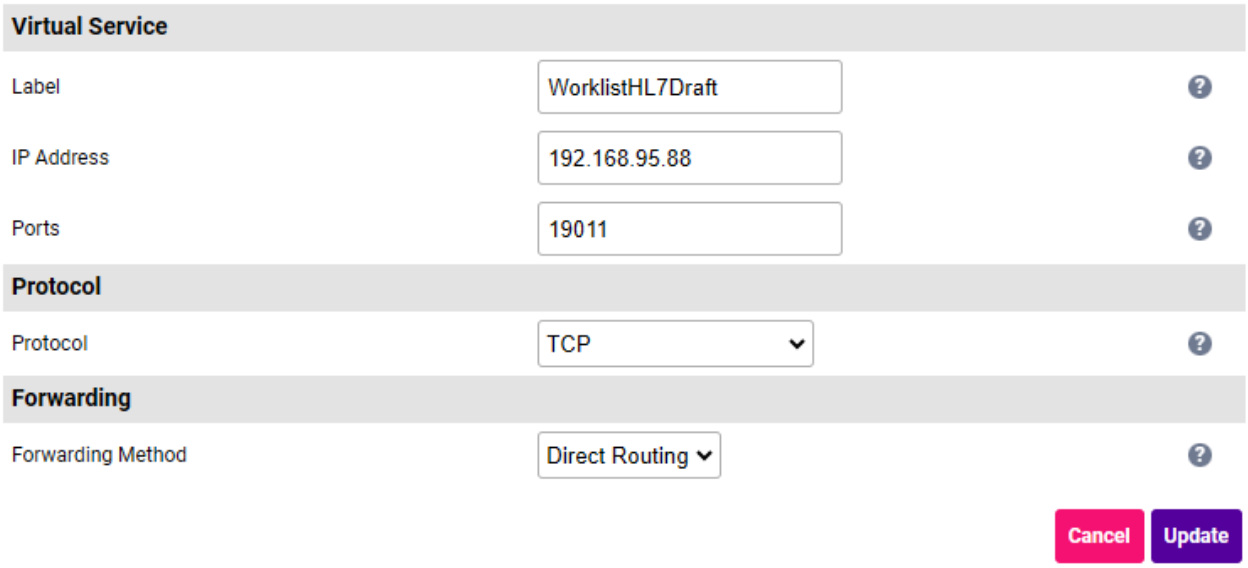
3. Leave all other settings at their default value.

4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.9. VIP 9 - WorklistHL7Draft

10.9.1. Virtual Service (VIP) Configuration

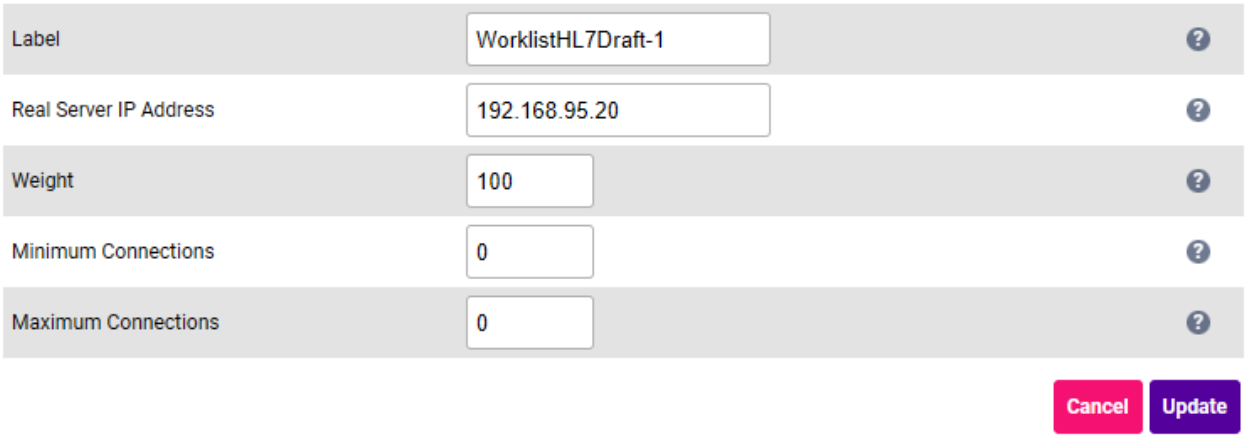
1. Using the WebUI, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:



   - Specify an appropriate *Label* for the Virtual Service, e.g. **WorklistHL7Draft**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.88**.
   - Set the *Ports* field to **19011**.
   - Leave the *Protocol* set to **TCP**.
   - Leave the *Forwarding Method* set to **Direct Routing**.
3. Click **Update** to create the Virtual Service.

10.9.2. Define the Associated Real Servers (RIPs)

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



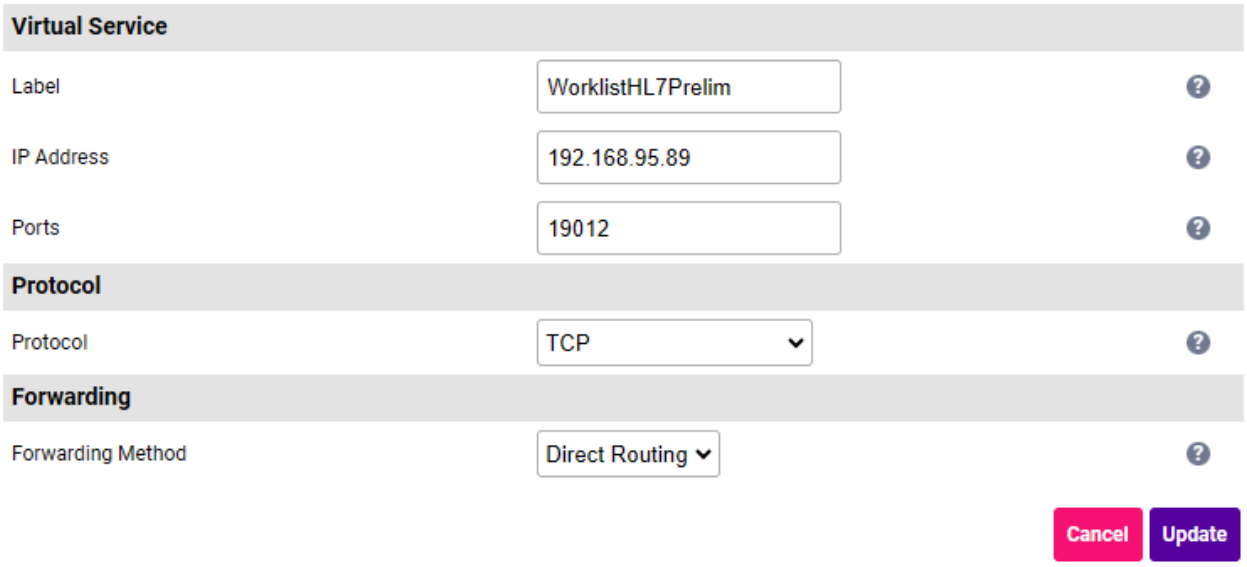
- Specify an appropriate *Label* for the RIP, e.g. **WorklistHL7Draft-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.10. VIP 10 - WorklistHL7Prelim

10.10.1. Virtual Service (VIP) Configuration

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



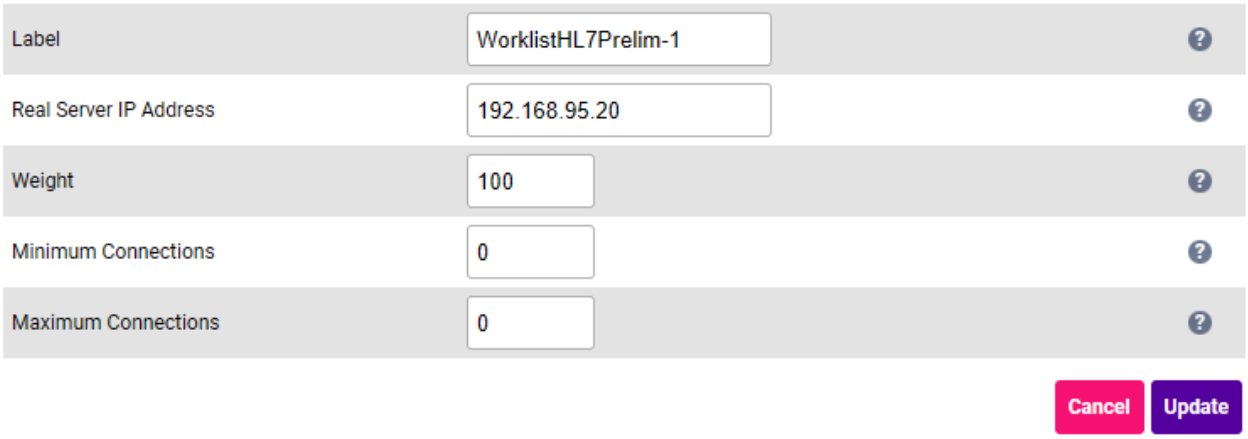
- Specify an appropriate *Label* for the Virtual Service, e.g. **WorklistHL7Prelim**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.89**.
- Set the *Ports* field to **19012**.

- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.

10.10.2. Define the Associated Real Servers (RIPs)

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



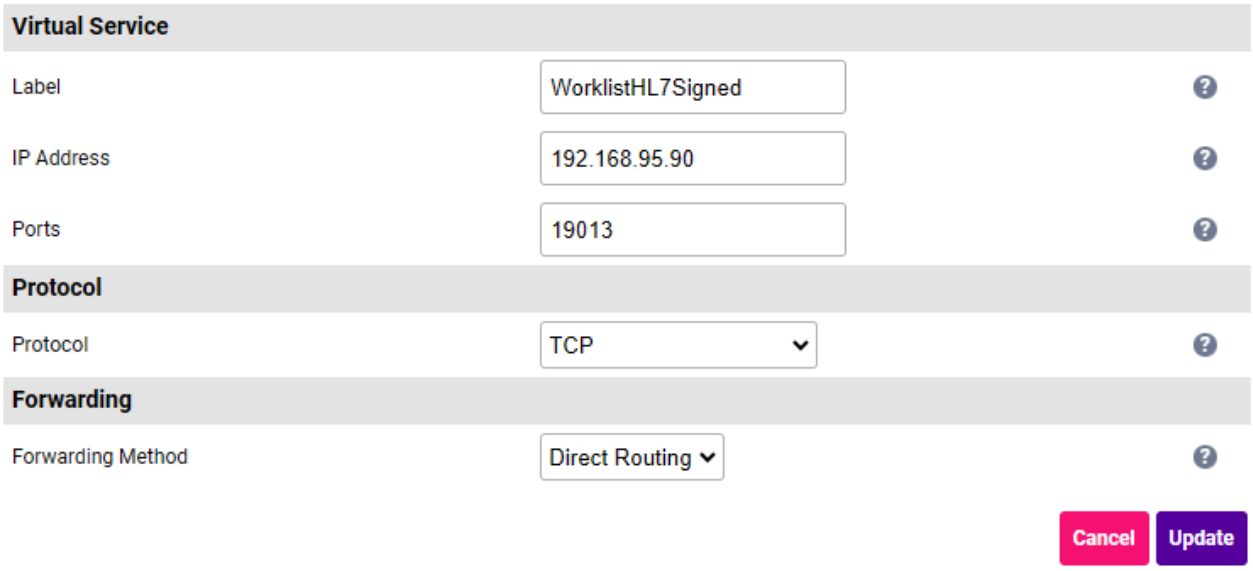
- Specify an appropriate *Label* for the RIP, e.g. **WorklistHL7Prelim-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.11. VIP 11 - WorklistHL7Signed

10.11.1. Virtual Service (VIP) Configuration

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

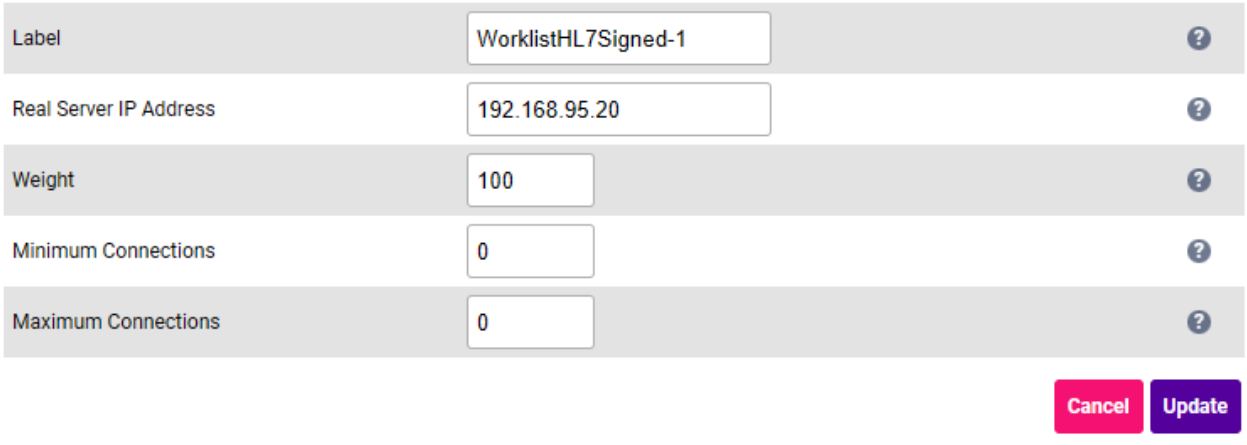


- Specify an appropriate *Label* for the Virtual Service, e.g. **WorklistHL7Signed**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.90**.
- Set the *Ports* field to **19013**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.

10.11.2. Define the Associated Real Servers (RIPs)

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



- Specify an appropriate *Label* for the RIP, e.g. **WorklistHL7Signed-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.

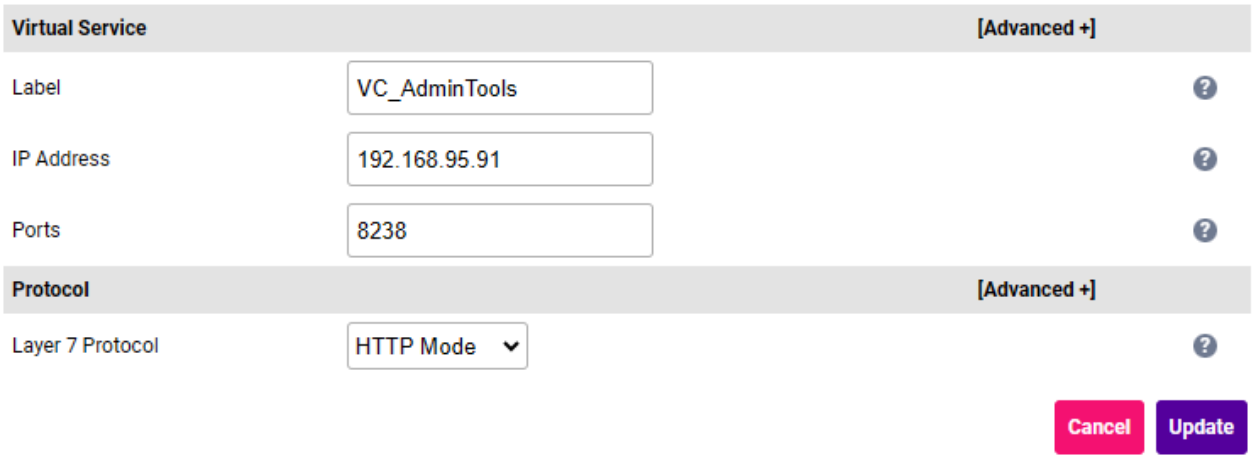
3. Leave all other settings at their default value.

4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.12. VIP 12 - VC_AdminTools

10.12.1. Virtual Service (VIP) Configuration

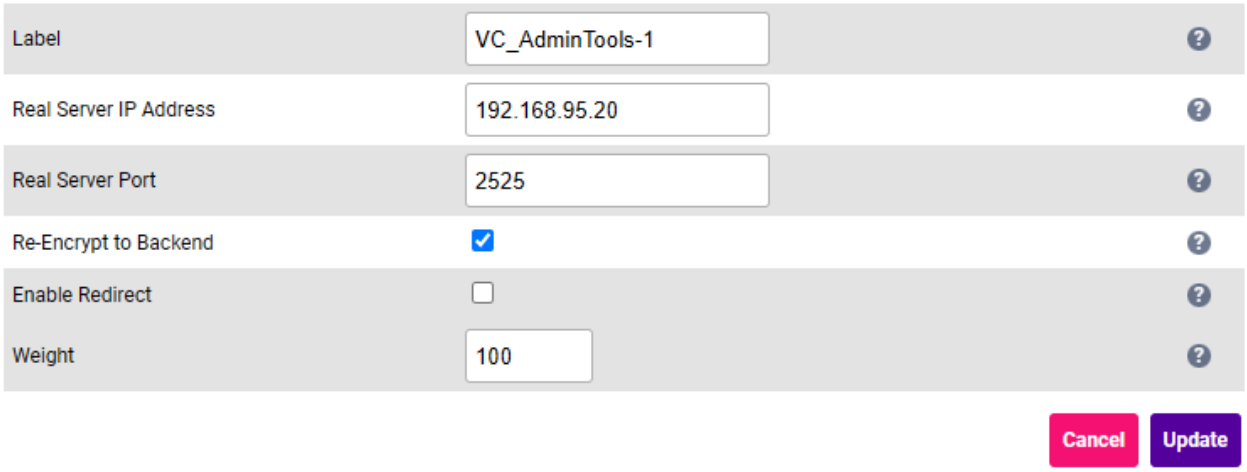
1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:



   - Specify an appropriate *Label* for the Virtual Service, e.g. **VC_AdminTools**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.91**.
   - Set the *Ports* field to **8238**.
   - Set the *Layer 7 Protocol* to **HTTP Mode**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *SSL* section.
   - Enable (check) the *Enable Backend Encryption* checkbox.
6. Scroll to the *Other* section.
   - Click the **[Advanced]** option and disable (un-check) *Set X-Forward-For header*.
7. Leave all other settings at their default value.
8. Click **Update**.

10.12.2. Define the Associated Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.
2. Enter the following details:

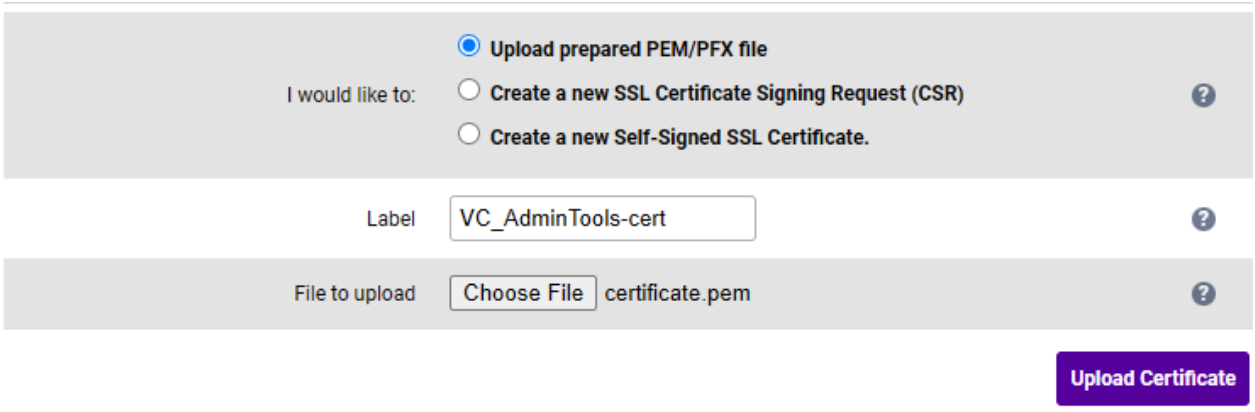


- Specify an appropriate *Label* for the RIP, e.g. **WorklistHL7Signed-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.
- Set the *Real Server Port* field to **2525**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.12.3. Upload the SSL Certificate

1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:

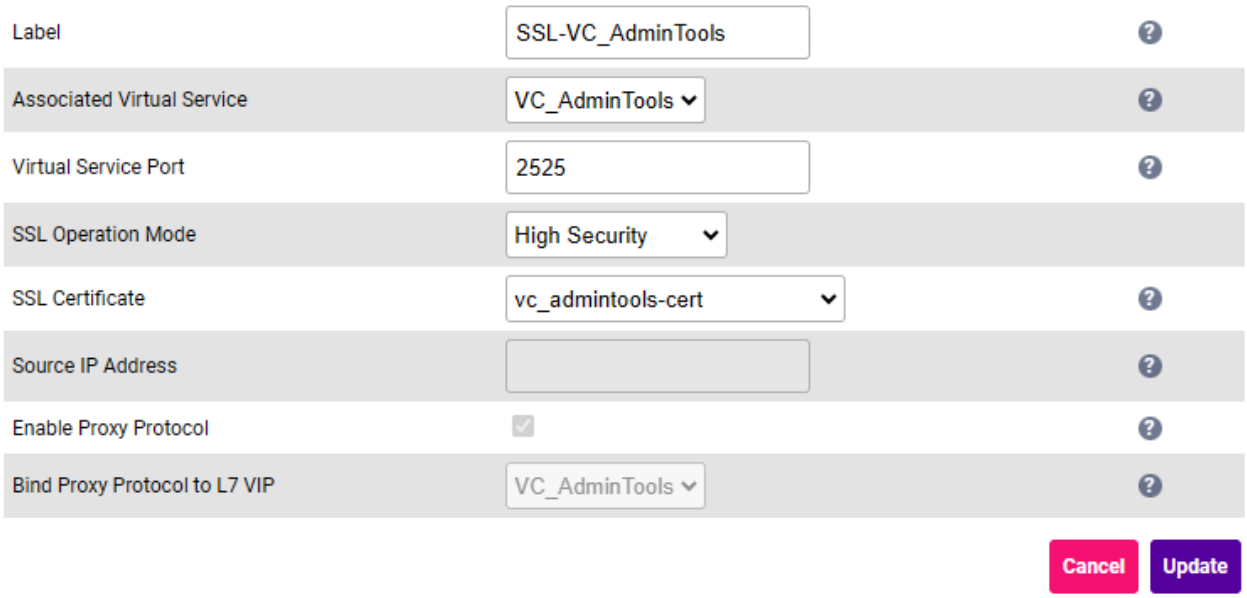


- Specify an appropriate *Label*, e.g. **VC_AdminTools-cert**.
- Click **Choose File**.
- Browse to and select the relevant PEM or PFX file.
- For PFX files specify the password if required.

4. Click **Upload Certificate**.

10.12.4. Configure SSL Termination

1. Using the WebUI, navigate to *Cluster Configuration > SSL Termination* and click **Add a new Virtual Service**.
2. Enter the following details:



   - Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **VC_AdminTools**.

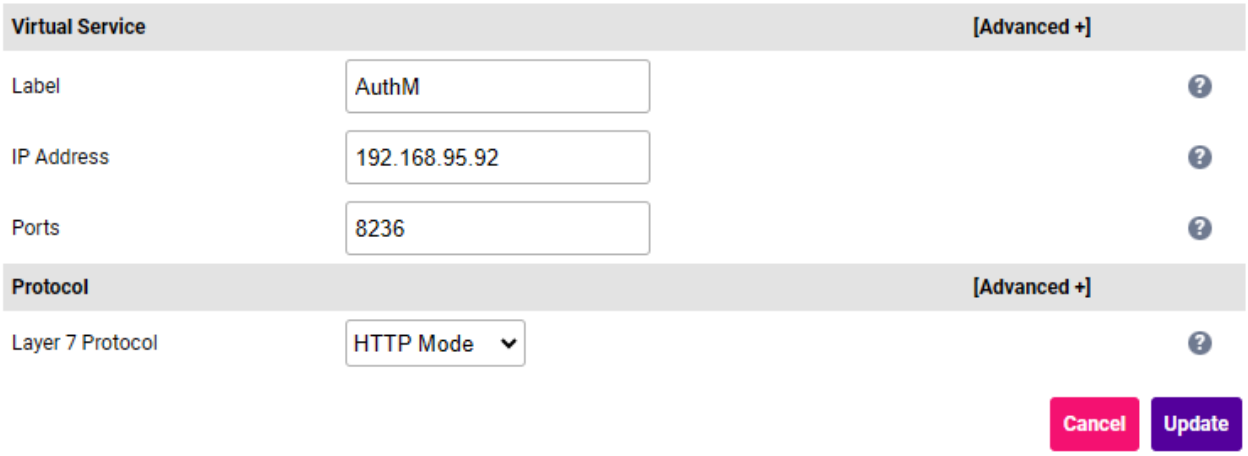
> **Note** Once the VIP is selected, the *Label* field will be auto-populated with **SSL-VC_AdminTools**. This can be changed if preferred.

   - Ensure that the *Virtual Service Port* is set to **2525**.
   - Leave *SSL Operation Mode* set to **High Security**.
   - Select the required *SSL Certificate*.
3. Leave all other settings at their default value.
4. Click **Update**.

10.13. VIP 13 - AuthM

10.13.1. Virtual Service (VIP) Configuration

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:

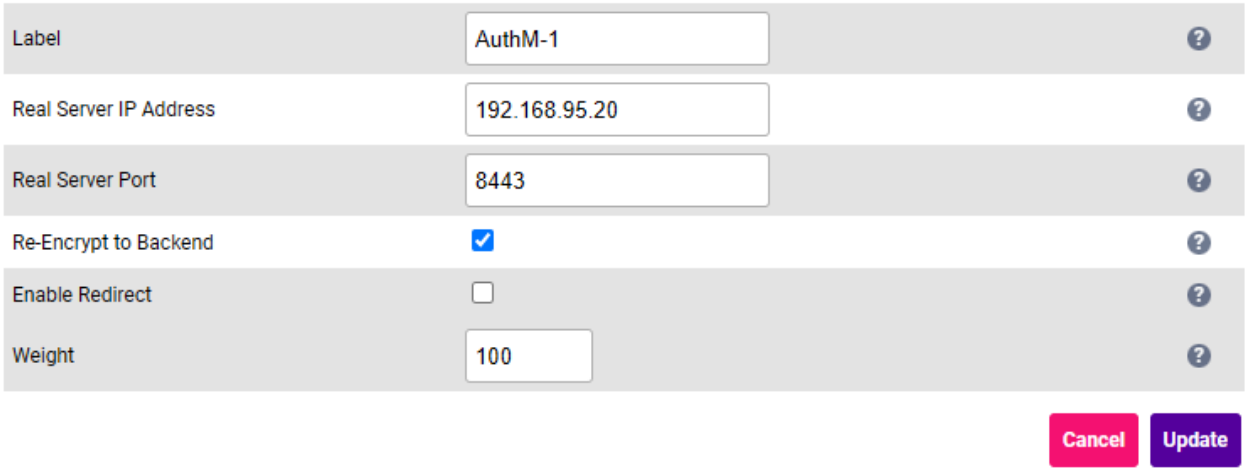


- Specify an appropriate *Label* for the Virtual Service, e.g. **AuthM**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.92**.
- Set the *Ports* field to **8236**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *SSL* section.
   - Enable (check) the *Enable Backend Encryption* checkbox.
6. Scroll to the *Other* section.
   - Click the **[Advanced]** option and disable (un-check) *Set X-Forward-For header*.
7. Leave all other settings at their default value.
8. Click **Update**.

10.13.2. Define the Associated Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.
2. Enter the following details:



- Specify an appropriate *Label* for the RIP, e.g. **AuthM-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.
- Set the *Real Server Port* field to **8443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.13.3. Customize the Configuration

The VIP must be converted to manual mode to enable the SNI directives that are included by default in the Real Server definition lines to be removed.

1. Using the WebUI, navigate to *View Configuration > Layer 7*.
2. Scroll down to the section that starts with "**listen AuthM**".
3. Copy the complete configuration for the VIP - this is from the **listen <VIP name>** line up to and including the last **server <RIP name> ...** line as per the example below:

```
listen AuthM
    bind 192.168.95.92:8236 transparent
    default-server on-marked-up shutdown-backup-sessions
    id 169466519
    mode http
    balance leastconn
    cookie "SERVERID" insert attr "SameSite=None" nocache indirect maxidle 30m maxlife 12h
    server backup 127.0.0.1:9081 backup  non-stick
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    timeout tunnel 1h
    option redispatch
    option abortonclose
    maxconn 40000
    server AuthM-1 192.168.95.20:8443 id 2  weight 100  cookie AuthM-1  check  inter 4000  rise
```

```
2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl verify
none sni req.hdr(host) sni req.hdr(host)
    server AuthM-2 192.168.95.21:8443 id 2  weight 100  cookie AuthM-1  check  inter 4000  rise
2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl verify
none sni req.hdr(host) sni req.hdr(host)
```

4. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services*.
5. Click **Modify** next to the **AuthM** VIP.
6. In the *Virtual Service* section at the top of the page, click **[Advanced]** and enable (check) the *Manual Configuration* checkbox.
7. Click **Update**.
8. Using the WebUI, navigate to *Cluster Configuration > Layer 7 - Manual Configuration*.
9. Paste the VIP's configuration into the edit window as shown in the example below:

HAProxy Manual Configuration

```
#    Configuration > Layer 7 - Virtual Services, ensuring that the Manual
#    Configuration checkbox is ticked.
#
# 2) Define the required layer 7 real servers using the menu option: Cluster
#    Configuration > Layer 7 - Real Servers.
#
# 3) Use this edit window to manually define the virtual service and real
#    servers using the same names, IP addresses and ports used in steps 1 & 2.
#
# MANUALLY DEFINE YOUR VIPS BELOW THIS LINE:

listen AuthM
    bind 192.168.95.92:8236 transparent
    default-server on-marked-up shutdown-backup-sessions
    id 169466519
    mode http
    balance leastconn
    cookie "SERVERID" insert attr "SameSite=None" nocache indirect maxidle 30m maxlife 12h
    server backup 127.0.0.1:9081 backup  non-stick
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    timeout tunnel 1h
    option redispatch
    option abortonclose
    maxconn 40000
    server AuthM-1 192.168.95.20:8443 id 2  weight 100  cookie AuthM-1  check  inter 4000  rise 2  fall 2
    server AuthM-2 192.168.95.21:8443 id 2  weight 100  cookie AuthM-1  check  inter 4000  rise 2  fall 2
```

Update

10. Now scroll to the right and remove the sni directives **sni req.hdr(host) sni req.hdr(host)** from the end of the last 2 lines so they appear as follows:

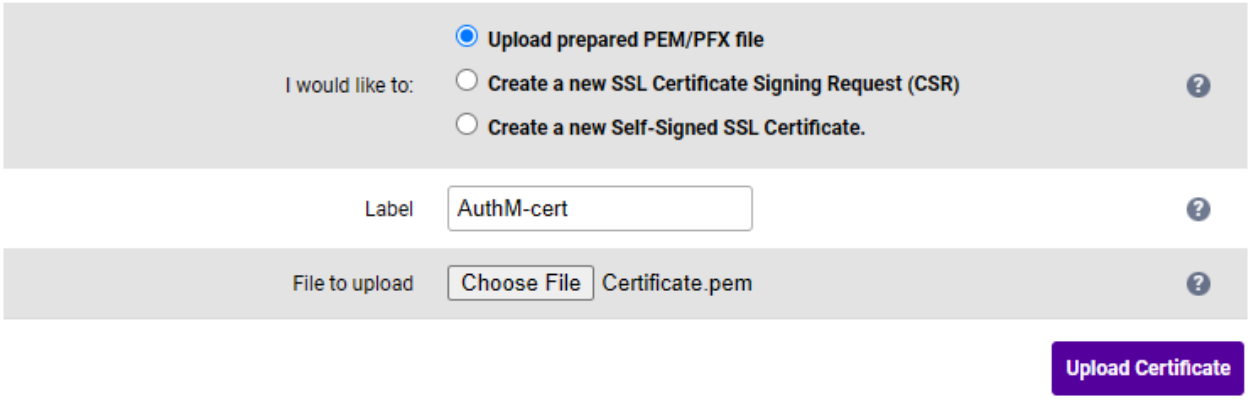
```
000  rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl verify none
000  rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl verify none
```

Update

11. Click **Update**.

10.13.4. Upload the SSL Certificate

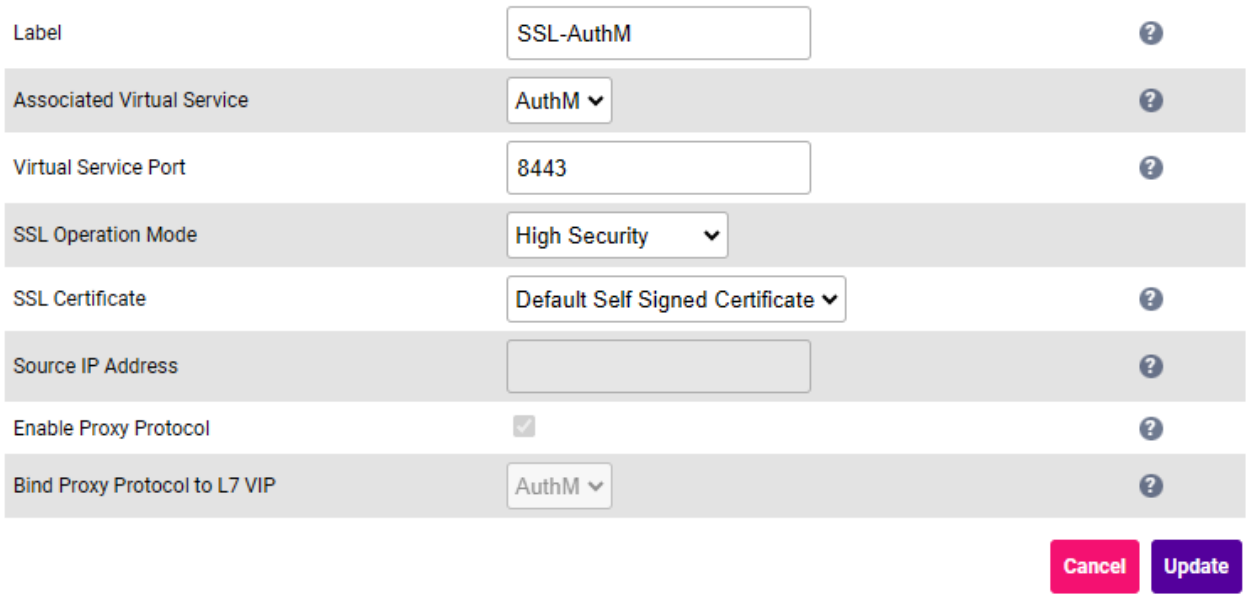
1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:



   - Specify an appropriate *Label*, e.g. **AuthM-cert**.
   - Click **Choose File**.
   - Browse to and select the relevant PEM or PFX file.
   - For PFX files specify the password if required.
4. Click **Upload Certificate**.

10.13.5. Configure SSL Termination

1. Using the WebUI, navigate to *Cluster Configuration > SSL Termination* and click **Add a new Virtual Service**.
2. Enter the following details:



- Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **AuthM**.

> **Note** Once the VIP is selected, the *Label* field will be auto-populated with **SSL-AuthM**. This can be changed if preferred.

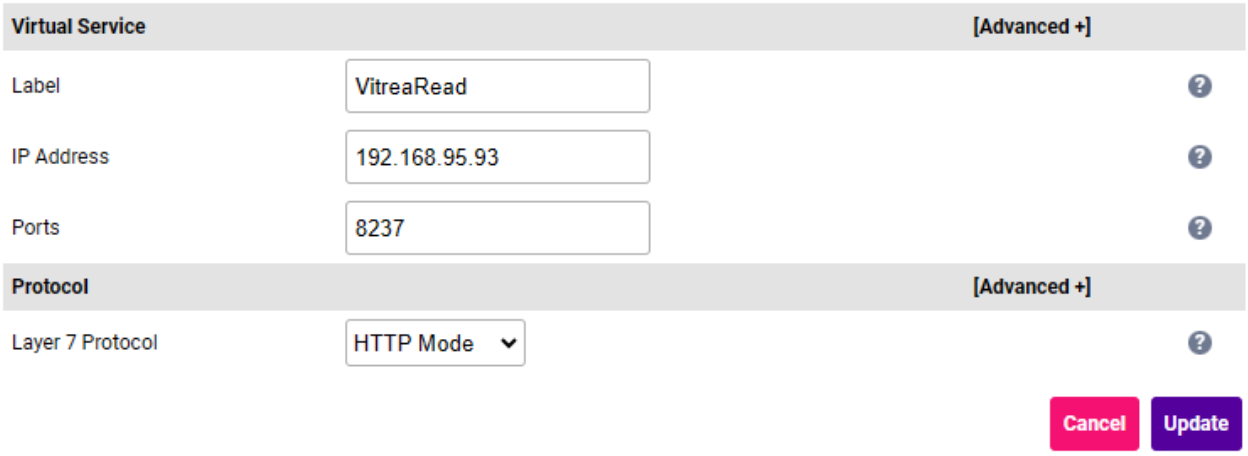
- Ensure that the *Virtual Service Port* is set to **8443**.
- Leave *SSL Operation Mode* set to **High Security**.
- Select the required *SSL Certificate*.

3. Leave all other settings at their default value.
4. Click **Update**.

10.14. VIP 14 - VitreaRead

10.14.1. Virtual Service (VIP) Configuration

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:



- Specify an appropriate *Label* for the Virtual Service, e.g. **VitreaRead**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.93**.
- Set the *Ports* field to **8237**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

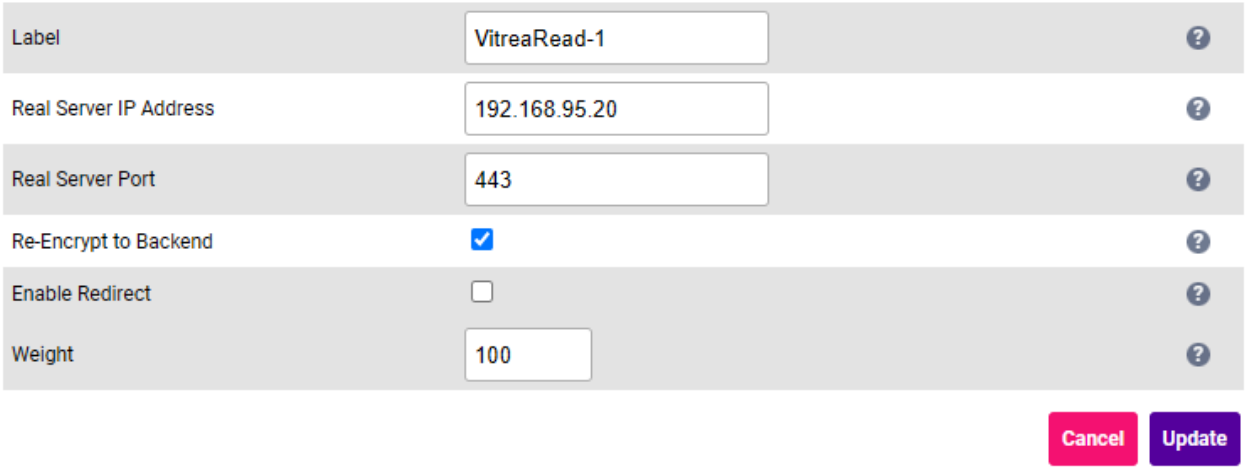
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *SSL* section.
   - Enable (check) the *Enable Backend Encryption* checkbox.
6. Scroll to the *Other* section.

- Click the **[Advanced]** option and disable (un-check) *Set X-Forward-For header*.

7. Leave all other settings at their default value.
8. Click **Update**.

10.14.2. Define the Associated Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.
2. Enter the following details:



- Specify an appropriate *Label* for the RIP, e.g. **VitreaRead-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.14.3. Customize the Configuration

The VIP must be converted to manual mode to enable the SNI directives that are included by default in the Real Server definition lines to be removed.

1. Using the WebUI, navigate to *View Configuration > Layer 7*.
2. Scroll down to the section that starts with "**listen VitreaRead**".
3. Copy the complete configuration for the VIP - this is from the **listen <VIP name>** line up to and including the last **server <RIP name> …** line as per the example below:

```
listen VitreaRead
    bind 192.168.95.93:8237 transparent
    default-server on-marked-up shutdown-backup-sessions
```

```
    id 286216545
    mode http
    balance leastconn
    cookie "SERVERID" insert attr "SameSite=None" nocache indirect maxidle 30m maxlife 12h
    server backup 127.0.0.1:9081 backup  non-stick
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    timeout tunnel 1h
    option redispatch
    option abortonclose
    maxconn 40000
    server VitreaRead-1 192.168.95.20:443 id 2  weight 100  cookie AuthM-1  check  inter 4000
rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl
verify none sni req.hdr(host) sni req.hdr(host)
    server VitreaRead-2 192.168.95.21:443 id 2  weight 100  cookie AuthM-1  check  inter 4000
rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl
verify none sni req.hdr(host) sni req.hdr(host)
```

4. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services*.
5. Click **Modify** next to the **AuthM** VIP.
6. In the *Virtual Service* section at the top of the page, click **[Advanced]** and enable (check) the *Manual Configuration* checkbox.
7. Click **Update**.
8. Using the WebUI, navigate to *Cluster Configuration > Layer 7 - Manual Configuration*.
9. Paste the VIP's configuration into the edit window as shown in the example below:

HAProxy Manual Configuration

```
    cookie "SERVERID" insert attr "SameSite=None" nocache indirect maxidle 30m maxlife 12h
    server backup 127.0.0.1:9081 backup  non-stick
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    timeout tunnel 1h
    option redispatch
    option abortonclose
    maxconn 40000
    server AuthM-1 192.168.95.20:8443 id 2  weight 100  cookie AuthM-1  check  inter 4000  rise 2  fall 2
    server AuthM-2 192.168.95.21:8443 id 2  weight 100  cookie AuthM-1  check  inter 4000  rise 2  fall 2

listen VitreaRead
    bind 192.168.95.93:8237 transparent
    default-server on-marked-up shutdown-backup-sessions
    id 286216545
    mode http
    balance leastconn
    cookie "SERVERID" insert attr "SameSite=None" nocache indirect maxidle 30m maxlife 12h
    server backup 127.0.0.1:9081 backup  non-stick
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    timeout tunnel 1h
    option redispatch
    option abortonclose
    maxconn 40000
    server VitreaRead-1 192.168.95.20:443 id 2  weight 100  cookie AuthM-1  check  inter 4000  rise 2  fall
    server VitreaRead-2 192.168.95.21:443 id 2  weight 100  cookie AuthM-1  check  inter 4000  rise 2  fall
```

Update

10. Now scroll to the right and remove the sni directives **sni req.hdr(host) sni req.hdr(host)** from the end of the last 2 lines so they appear as follows:

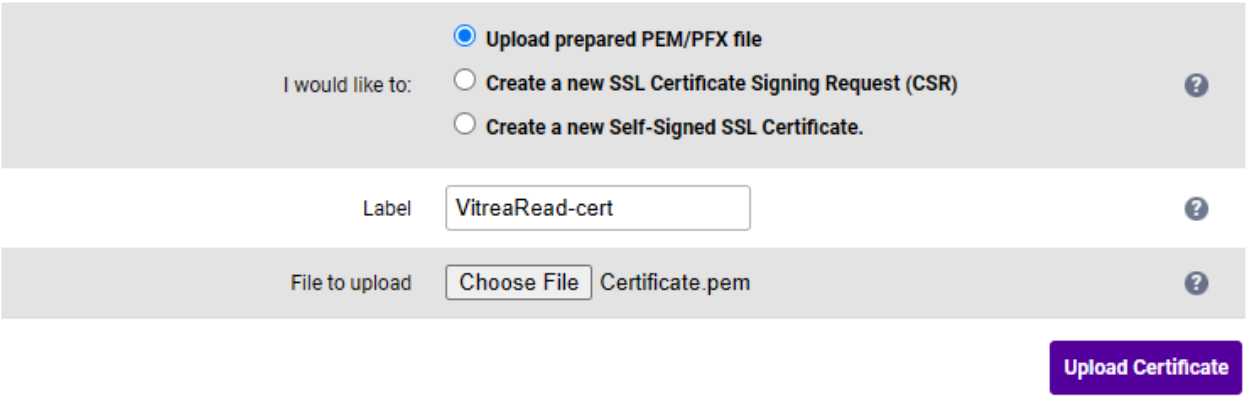
```
000  rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl verify none
000  rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl verify none
```

Update

11. Click **Update**.

10.14.4. Upload the SSL Certificate

1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:

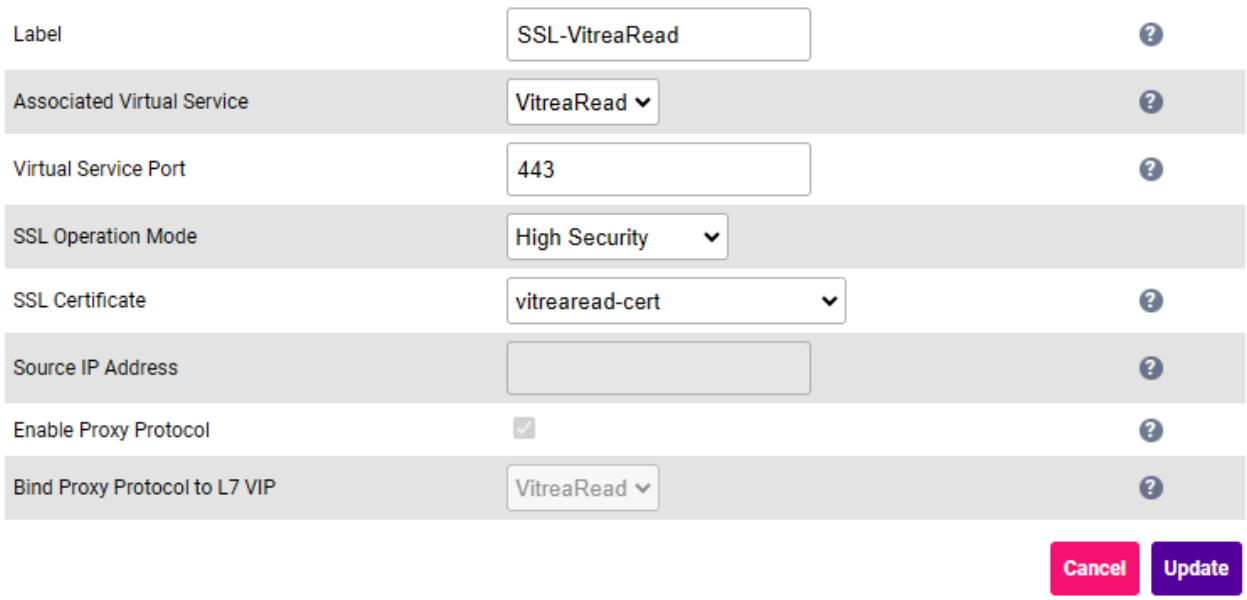


- Specify an appropriate *Label*, e.g. **VitreaRead-cert**.
- Click **Choose File**.
- Browse to and select the relevant PEM or PFX file.
- For PFX files specify the password if required.

4. Click **Upload Certificate**.

10.14.5. Configure SSL Termination

1. Using the WebUI, navigate to *Cluster Configuration > SSL Termination* and click **Add a new Virtual Service**.
2. Enter the following details:



- Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **VitreaRead**.

> **Note** Once the VIP is selected, the *Label* field will be auto-populated with **SSL-VitreaRead**. This can be changed if preferred.

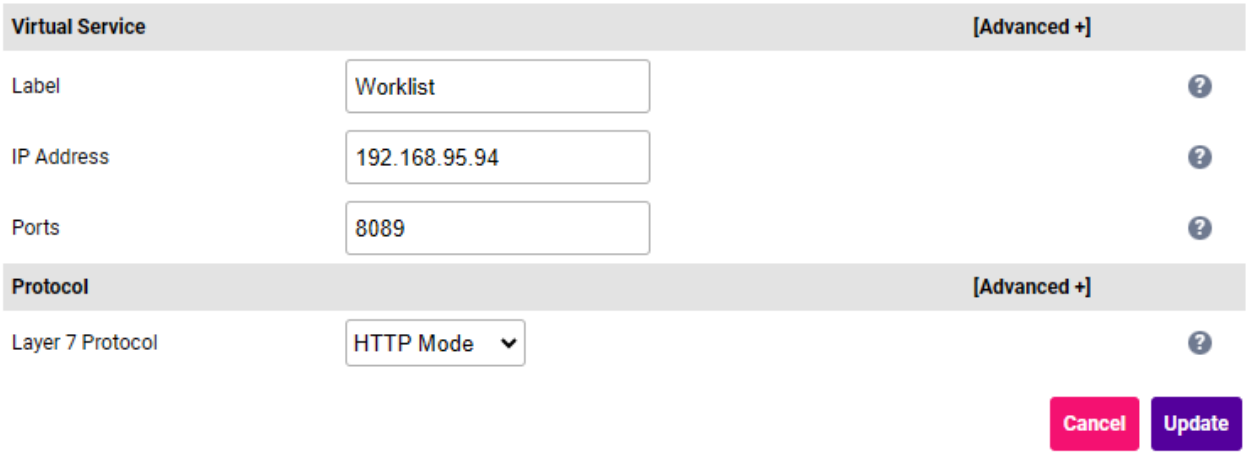
- Ensure that the *Virtual Service Port* is set to **443**.
- Leave *SSL Operation Mode* set to **High Security**.
- Select the required *SSL Certificate*.

3. Leave all other settings at their default value.
4. Click **Update**.

10.15. VIP 15 - Worklist

10.15.1. Virtual Service (VIP) Configuration

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:

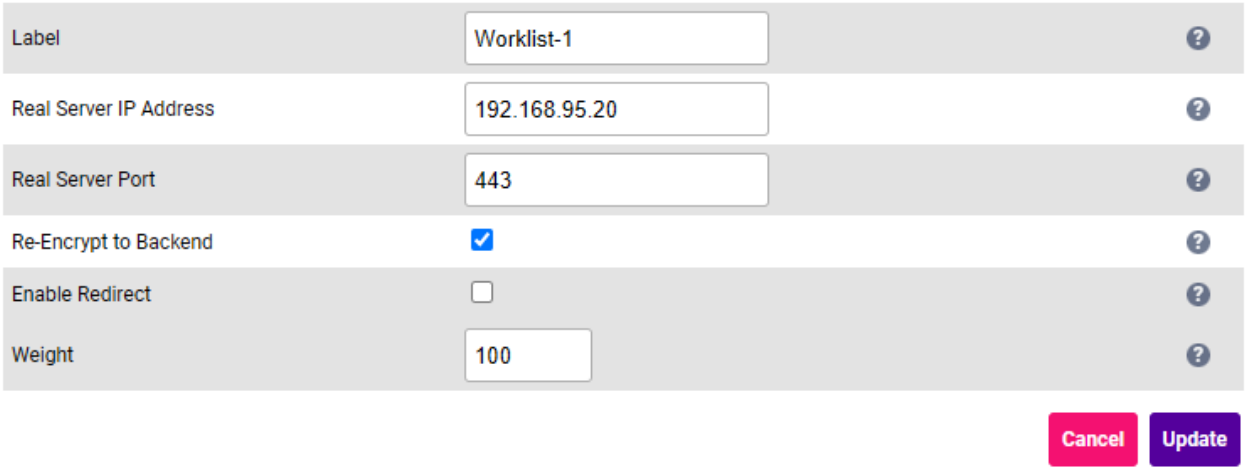


- Specify an appropriate *Label* for the Virtual Service, e.g. **Worklist**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.94**.
- Set the *Ports* field to **8089**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *SSL* section.
   - Enable (check) the *Enable Backend Encryption* checkbox.
6. Scroll to the *Other* section.
   - Click the **[Advanced]** option and disable (un-check) *Set X-Forward-For header*.
7. Leave all other settings at their default value.
8. Click **Update**.

10.15.2. Define the Associated Real Servers (RIPs)

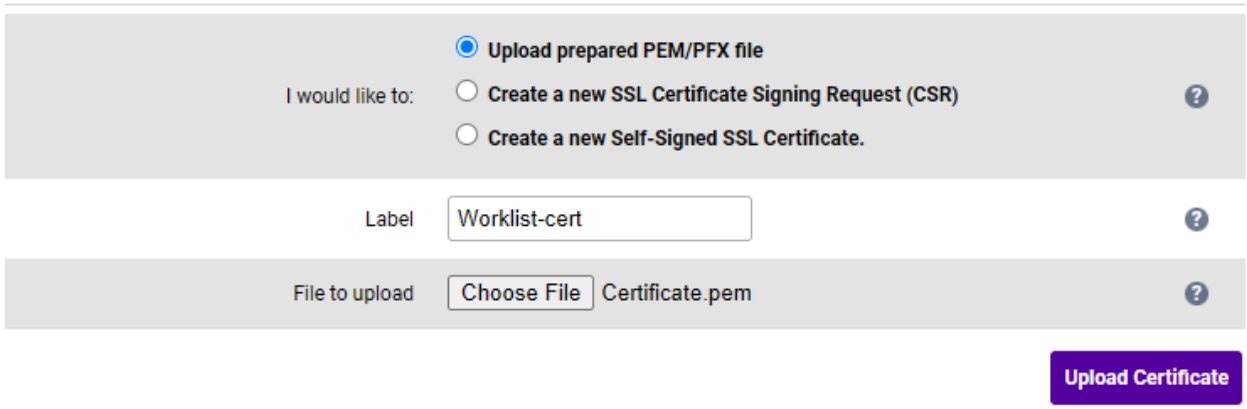
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.
2. Enter the following details:



   - Specify an appropriate *Label* for the RIP, e.g. **Worklist-1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.
   - Set the *Real Server Port* field to **443**.
   - Ensure that *Re-Encrypt to Backend* is enabled (checked).
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.15.3. Upload the SSL Certificate

1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:



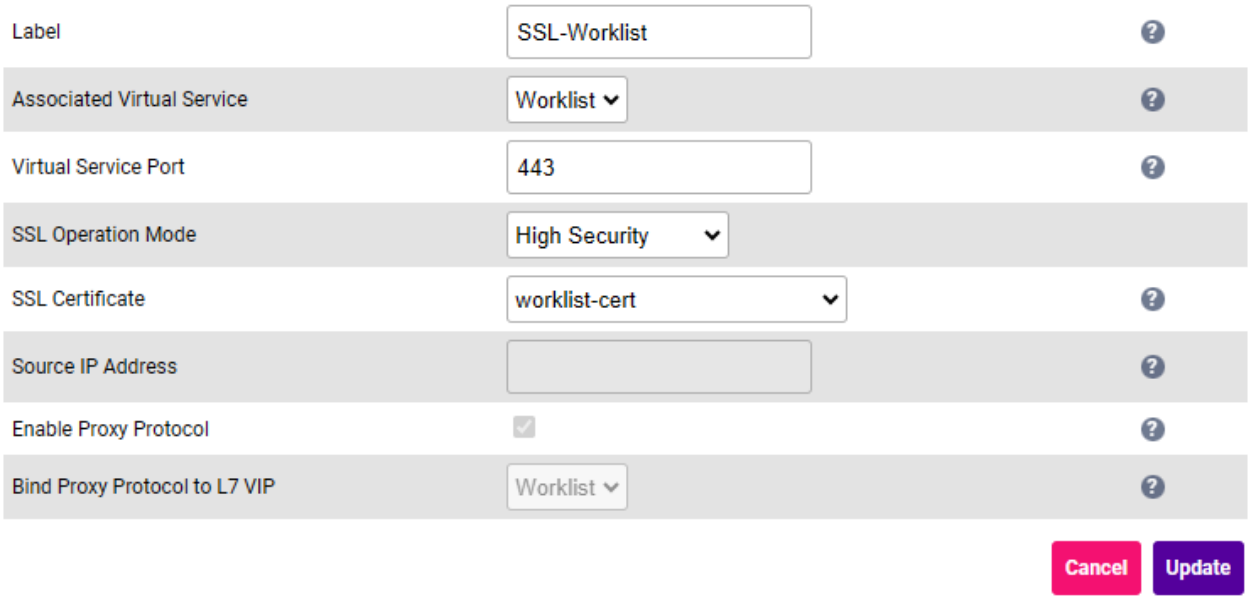
   - Specify an appropriate *Label*, e.g. **Worklist-cert**.

- Click **Choose File**.
- Browse to and select the relevant PEM or PFX file.
- For PFX files specify the password if required.

4. Click **Upload Certificate**.

10.15.4. Configure SSL Termination

1. Using the WebUI, navigate to *Cluster Configuration > SSL Termination* and click **Add a new Virtual Service**.
2. Enter the following details:



- Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **Worklist**.

> **Note** Once the VIP is selected, the *Label* field will be auto-populated with **SSL-Worklist**. This can be changed if preferred.

- Ensure that the *Virtual Service Port* is set to **443**.
- Leave *SSL Operation Mode* set to **High Security**.
- Select the required *SSL Certificate*.

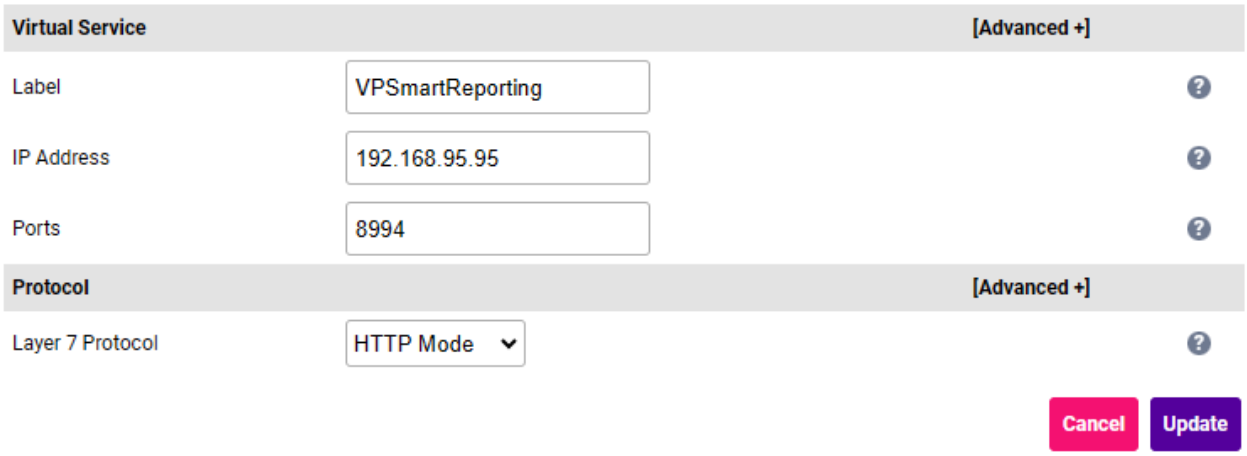
3. Leave all other settings at their default value.
4. Click **Update**.

10.16. VIP 16 - VPSmartReporting

10.16.1. Virtual Service (VIP) Configuration

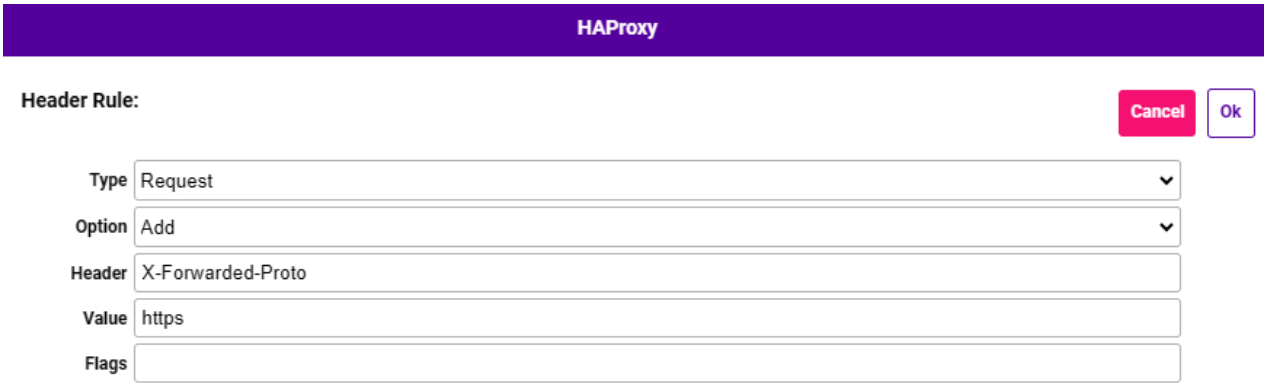
1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.

2. Enter the following details:



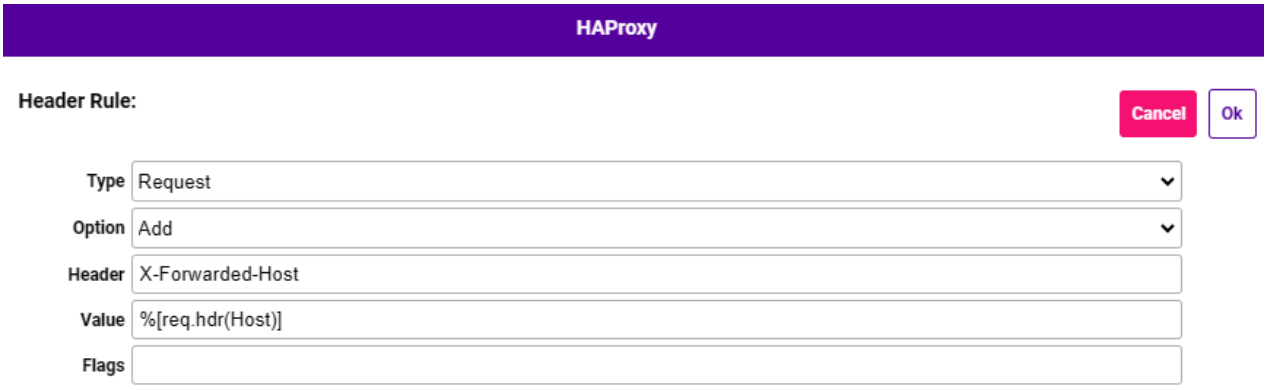
- Specify an appropriate *Label* for the Virtual Service, e.g. **VPSmartReporting**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.95.95**.
- Set the *Ports* field to **8994**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Header Rules* section and click **Add Rule**.



- Set the *Type* to **Request**.
- Set the *Option* to **Add**.
- Set the *Header* to **X-Forwarded-Proto**.
- Set the *Value* to **https**.

6. Click **Ok** and then click **Add Rule** again.

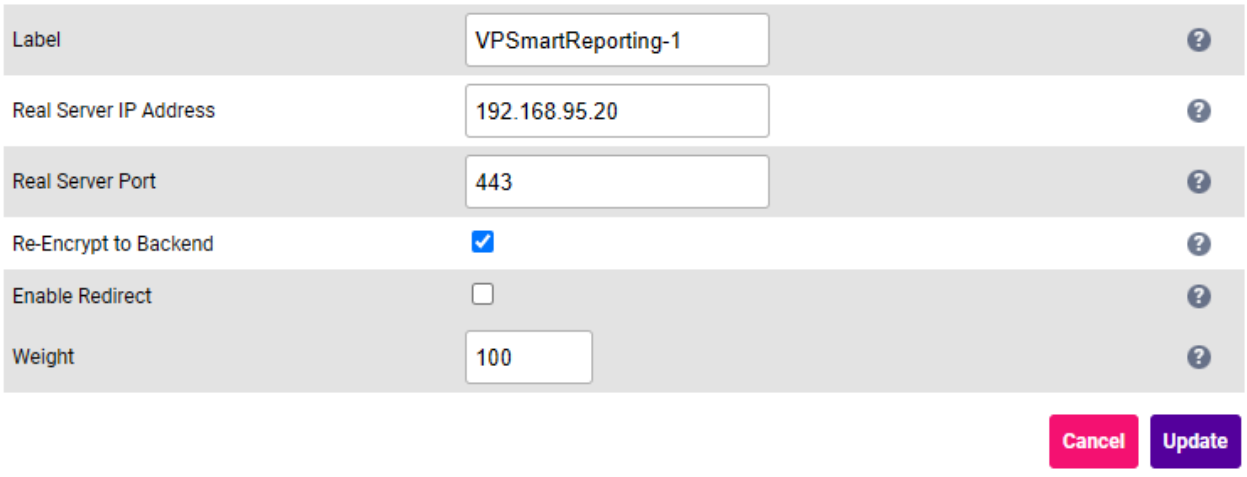


- Set the *Type* to **Request**.
- Set the *Option* to **Add**.
- Set the *Header* to **X-Forwarded-Host**.
- Set the *Value* to **%[req.hdr(Host)]**.

7. Click **Ok**.
8. Scroll to the *SSL* section.
   - Enable (check) the *Enable Backend Encryption* checkbox.
9. Scroll to the *Other* section.
   - Click the **[Advanced]** option and disable (un-check) *Set X-Forward-For header*.
10. Leave all other settings at their default value.
11. Click **Update**.

10.16.2. Define the Associated Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.
2. Enter the following details:



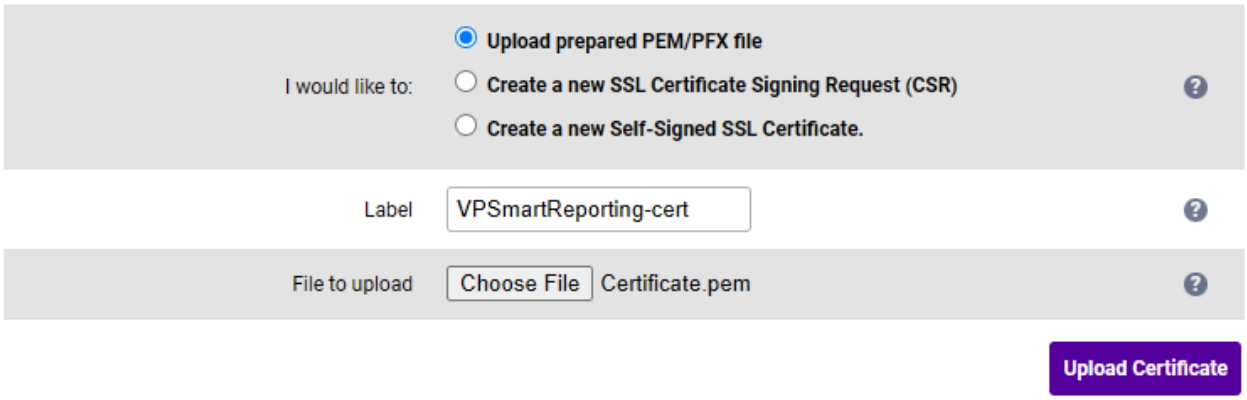
- Specify an appropriate *Label* for the RIP, e.g. **VPSmartReporting-1**.

- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.95.20**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

10.16.3. Upload the SSL Certificate

1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:

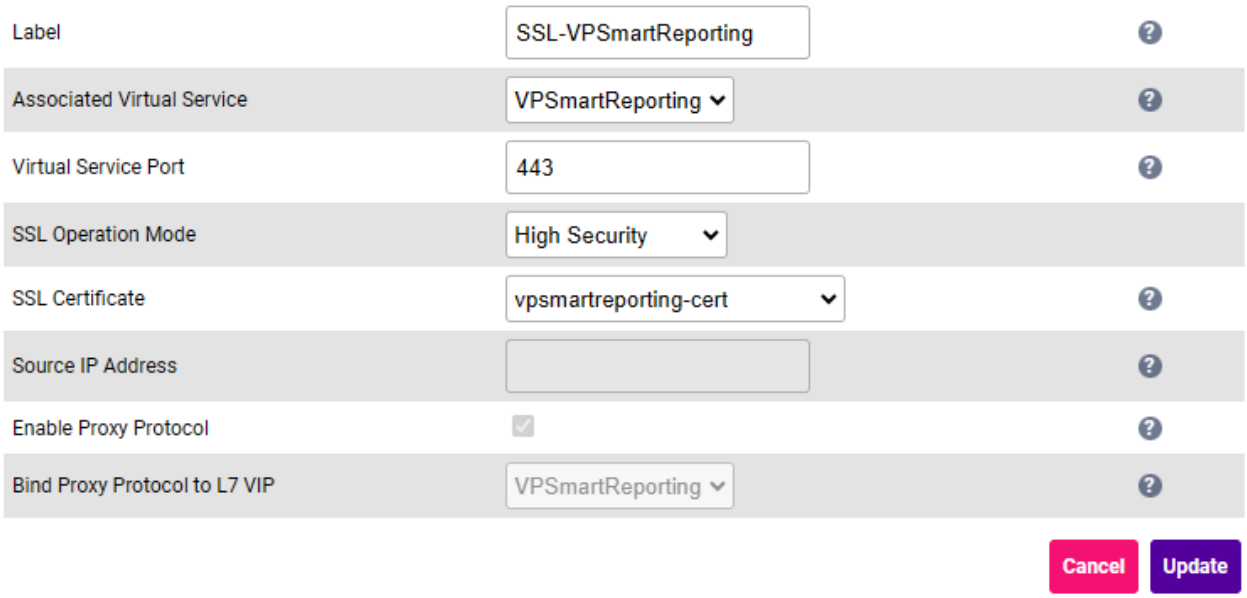


- Specify an appropriate *Label*, e.g. **VPSmartReporting-cert**.
- Click **Choose File**.
- Browse to and select the relevant PEM or PFX file.
- For PFX files specify the password if required.

4. Click **Upload Certificate**.

10.16.4. Configure SSL Termination

1. Using the WebUI, navigate to *Cluster Configuration > SSL Termination* and click **Add a new Virtual Service**.
2. Enter the following details:



- Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **VPSmartReporting**.

> **Note** Once the VIP is selected, the *Label* field will be auto-populated with **SSL-VPSmartReporting**. This can be changed if preferred.

- Ensure that the *Virtual Service Port* is set to **443**.
- Leave *SSL Operation Mode* set to **High Security**.
- Select the required *SSL Certificate*.

3. Leave all other settings at their default value.
4. Click **Update**.

10.17. Finalizing the Configuration

To apply the new settings, HAProxy and STunnel must be reloaded. This can be done using the button in the "Commit changes" box at the top of the screen or by using the Restart Services menu option:

1. Using the WebUI, navigate to: *Maintenance > Restart Services*.
2. Click **Reload HAProxy**.
3. Click **Reload STunnel**.

11. Testing & Verification

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

11.1. Accessing Canon Enterprise Imaging Suite via the Load Balancer

Verify that you're able to successfully access all load balanced applications and services via the Virtual Services on the load balancer.

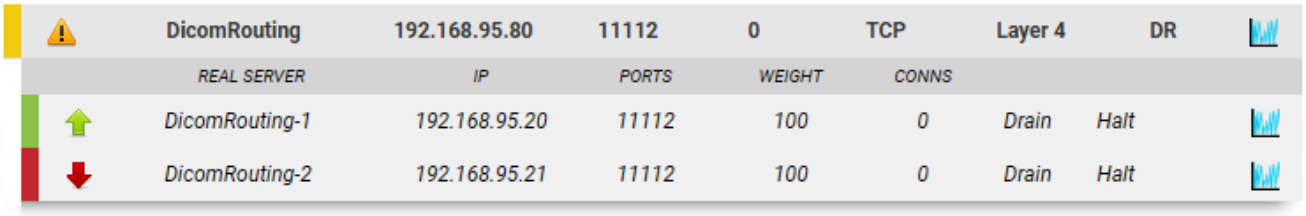
> **Note** Make sure that DNS is updated so that any FQDNs used point to the VIPs rather than individual servers.

11.2. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all Virtual Services & the associated Real Servers (i.e. the Canon Enterprise Imaging servers) and shows the state/health of each server as well as the overall state of each cluster. The example below shows that all servers are healthy (green) and available to accept connections:

VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE
DicomRouting	192.168.95.80	11112	0	TCP	Layer 4	DR
DicomInternal	192.168.95.81	11112	0	TCP	Layer 4	DR
HL7Live	192.168.95.82	2398	0	TCP	Layer 4	DR
HL7Migrate	192.168.95.83	2988	0	TCP	Layer 4	DR
MWL	192.168.95.84	4106	0	TCP	Layer 4	DR
WorklistHL7Live	192.168.95.85	19001	0	TCP	Layer 4	DR
WorklistHL7Migra..	192.168.95.86	19002	0	TCP	Layer 4	DR
MINT	192.168.95.87	8080	0	TCP	Layer 4	DR
WorklistHL7Draft..	192.168.95.88	19011	0	TCP	Layer 4	DR
WorklistHL7Preli..	192.168.95.89	19012	0	TCP	Layer 4	DR
WorklistHL7Signe..	192.168.95.90	19013	0	TCP	Layer 4	DR
VC_AdminTools	192.168.95.91	8238	0	HTTP	Layer 7	Proxy
AuthM	192.168.95.92	8236	0	HTTP	Layer 7	Proxy

If one of the servers within a cluster fails its health check, that server will be colored red and the cluster will be colored yellow as shown below:



	DicomRouting	192.168.95.80	11112	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
	DicomRouting-1	192.168.95.20	11112	100	0	Drain	Halt	
	DicomRouting-2	192.168.95.21	11112	100	0	Drain	Halt	

12. 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.

13. Further Documentation

For additional information, please refer to the Administration Manual.

14. Appendix

14.1. 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.

14.1.1. 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:

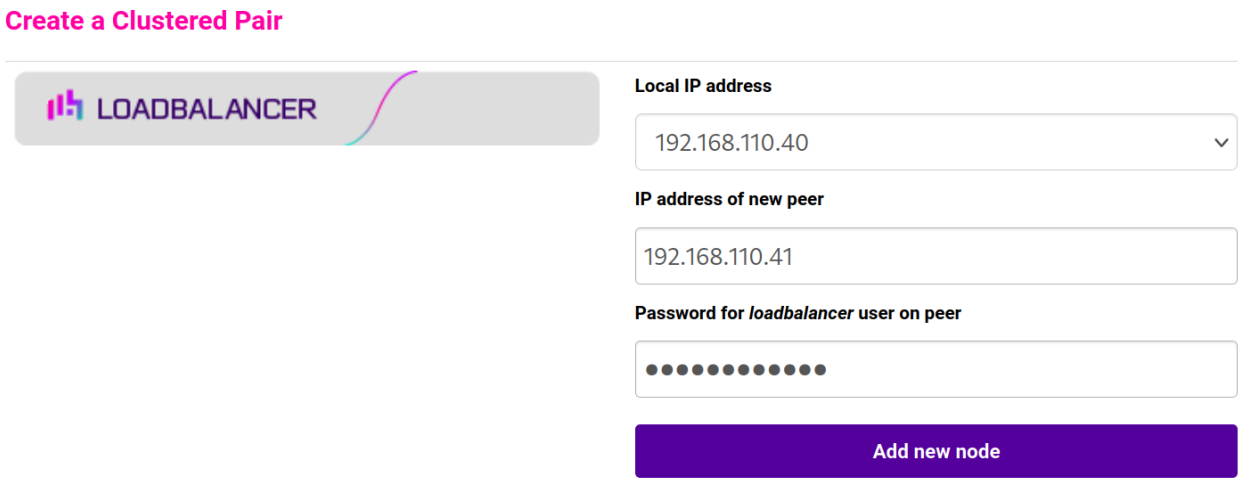
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration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

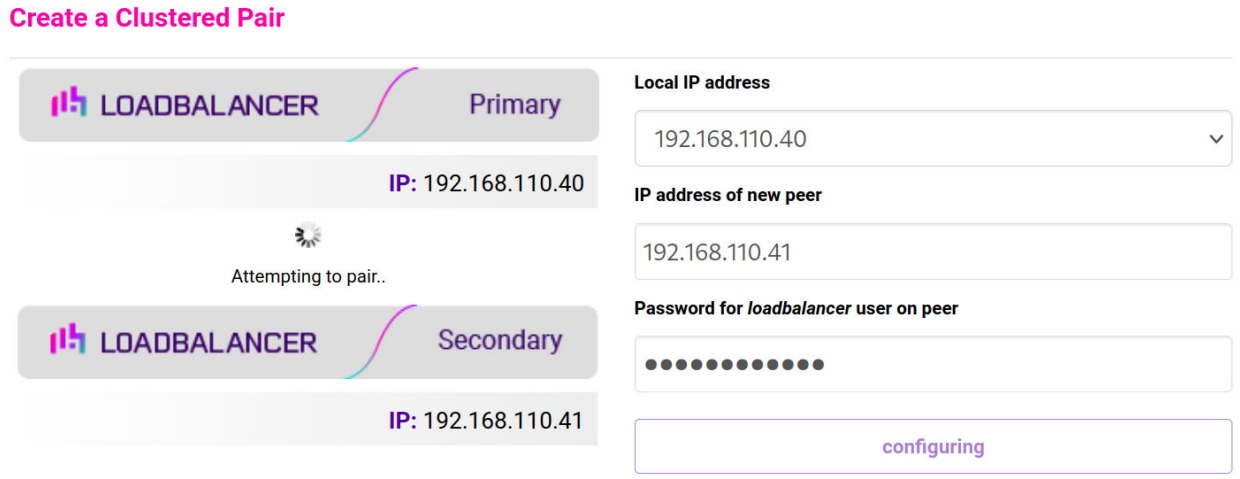
14.1.2. Configuring the HA Clustered Pair

> **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.

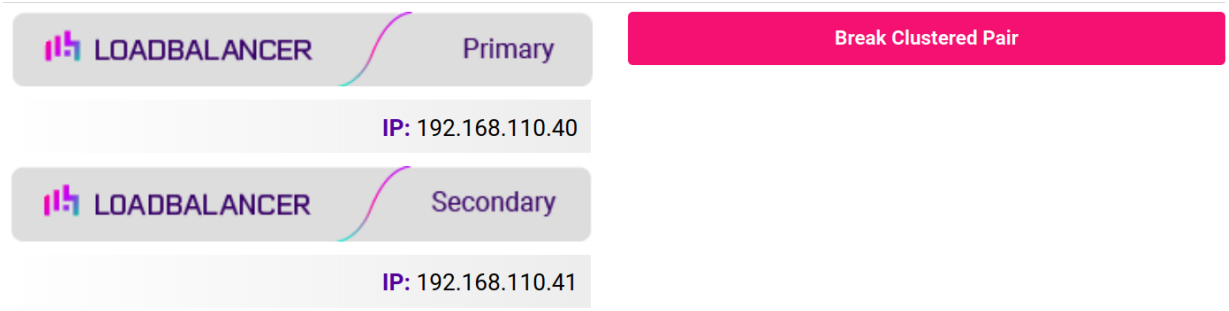
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



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.

15. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	05 December 2024	Initial version		RJC

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.