LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing GE HealthCare Datalogue

Version 1.3

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced GE HealthCare Datalogue (DL) environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any DL configuration changes that are required to enable load balancing.

1.1. Acronyms Used in the Guide

Acronym	Description
EA	Enterprise Archive
MPI	Master Patient Index
ATR	Audit Trail Repository
ZFP	Zero Footprint
ZFP-PT	Zero Footprint Viewer Patient Timeline
XDS	Cross Document Sharing
DL	Datalogue
MM	Media Manager
ADT	Admission, Discharge and Transfer
PIX	Patient Identifier Cross-referencing
PDQ	Patient Demographics Query

2. Prerequisites

1. Have access to the VMware Hypervisor environment to enable the Loadbalancer.org Virtual Appliance (VA) to be deployed and configured.
2. Have sufficient available Hypervisor CPU and memory resources to allocate to the VA based on the required throughput - for details refer to Virtual Hardware Resource Requirements.
3. Ensure that firewalls and other network devices are configured to allow management and other required access to the VA - for details of all ports used refer to Ports Used by the Appliance.
4. Ensure that firewalls and other network devices are configured to allow client/test access to all Virtual Services (VIPs).
5. Ensure that firewalls and other network devices are configured to allow load balancer access to all DL servers.
6. Have IP addresses for the VA and all required Virtual Services.
7. Have access to the DL servers to enable the ARP problem to be solved for Layer 4 DR mode VIPs - for details refer to Configuring DL for Load Balancing.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.0 & later

3.2. GE HealthCare DL

- All versions

4. Load Balancing DL

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

4.1. Virtual Service (VIP) Requirements

To provide load balancing and HA for DL, the following VIPs maybe required depending on which components the customer requires:

Reference	VIP Name	Mode	Port(s)	Persistence Mode	Health Check
VIP 1	EA_HL7	L4 DR	2575	Source IP	HTTPS (GET)
VIP 2	EA_DICOM_TLS	L4 DR	2762	Source IP	HTTPS (GET)
VIP 3	EA_XDS	L4 DR	443	Source IP	HTTPS (GET)
VIP 4	EA_Console	L4 DR	80	Source IP	HTTPS (GET)
VIP 5	EA_DICOM	L4 DR	104	Source IP	HTTP (GET)
VIP 6	MM	L4 DR	443	Source IP	HTTPS (GET)
VIP 7	MM_DICOM	L4 DR	104	Source IP	HTTPS (GET)
VIP 8	ATR_WEB	L4 DR	8443	Source IP	HTTPS (GET)
VIP 9	ATR_SYSLOG	L4 DR	2514	Source IP	HTTPS (GET)
VIP 10	REG_XDS	L4 DR	8443	Source IP	HTTPS (GET)
VIP 11	REG_HL7_ADT	L4 DR	3800	Source IP	HTTPS (GET)
VIP 12	MPI_HL7_ADT	L4 DR	3700	Source IP	HTTPS (GET)
VIP 13	MPI_HL7_PIX	L4 DR	3710	Source IP	HTTPS (GET)
VIP 14	MPI_HL7_PDQ	L4 DR	3750	Source IP	HTTPS (GET)
VIP 15	MPI_WEB	L4 DR	8444	Source IP	HTTPS (GET)
VIP 16	ZFP	L7 SNAT	443	Source IP	HTTPS (GET)

> **Note** VIP 7 (**MM_DICOM**) is only required when Media Manager is configured to be a DICOM source.

> **Note** Whilst testing VIP 16 (**ZFP**), a performance issue was encountered when using Layer 4 DR

where the connection was taking around 12 seconds to complete. Therefore the decision was made to move the ZFP service to Layer 7.

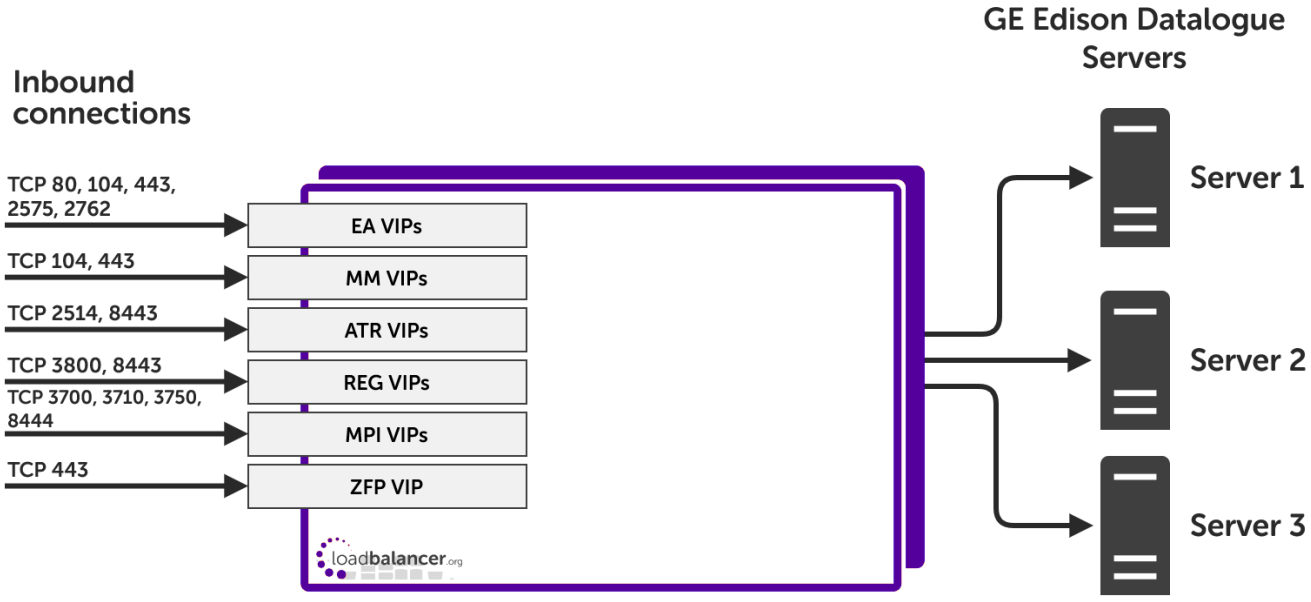
5. Ports Used by the Appliance

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.

6. Deployment Concept



VIP = **V**irtual **IP** Address

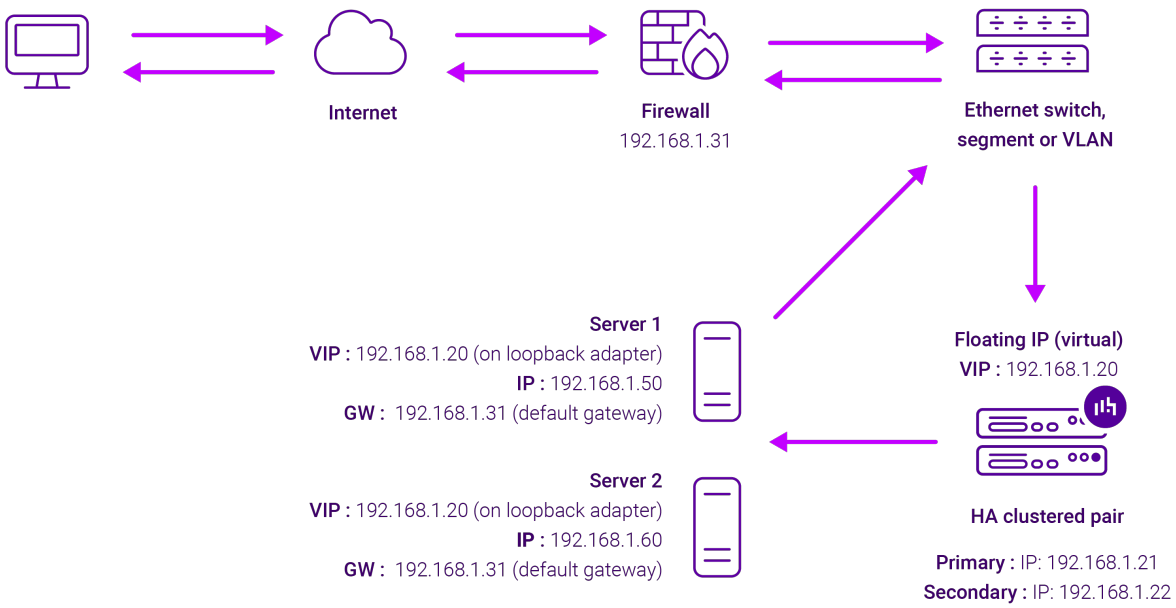
7. Load Balancer Deployment Methods

For GE HealthCare DL, layer 4 DR mode and layer 7 SNAT mode are used. These modes are described below are 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

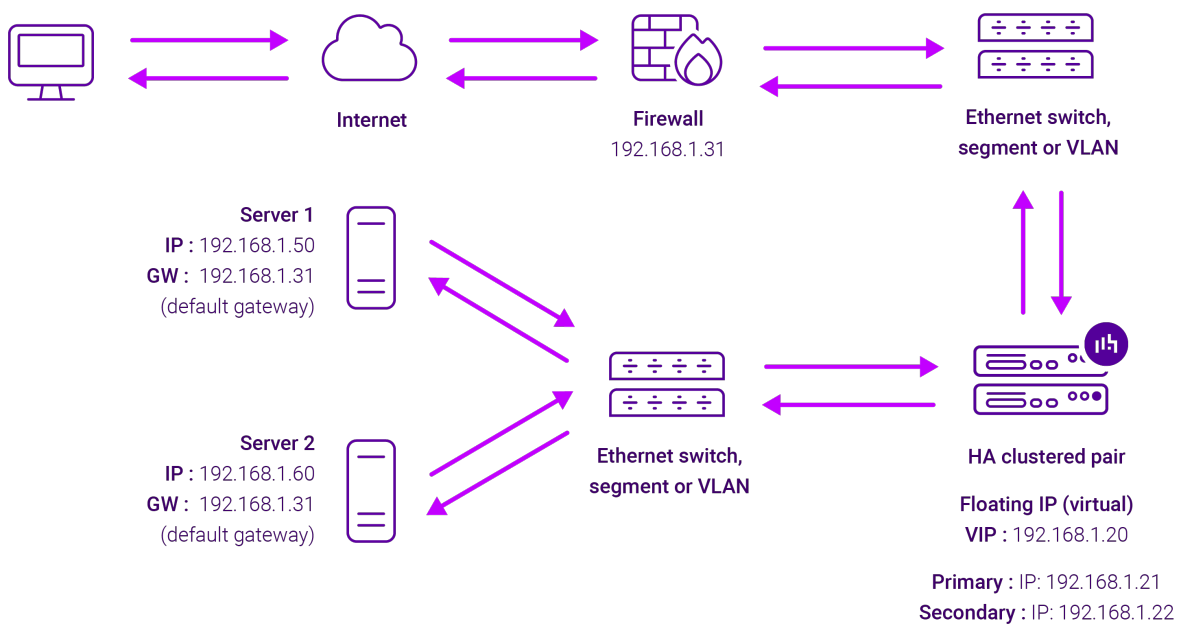
load balancer has an interface in that subnet.

- 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.

> **Note** For additional information on how the MAC address is modified in relation to the traffic flow between the load balancer, the load balanced backend servers and the Modality, please refer DR Mode Packet Manipulation in the appendix.

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 DL for Load Balancing

8.1. Layer 7 SNAT Mode

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

8.2. Layer 4 DR Mode

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

Detailed steps on solving the "ARP problem" for Windows 2012 and later are presented below.

8.3. Windows Server 2012 & Later

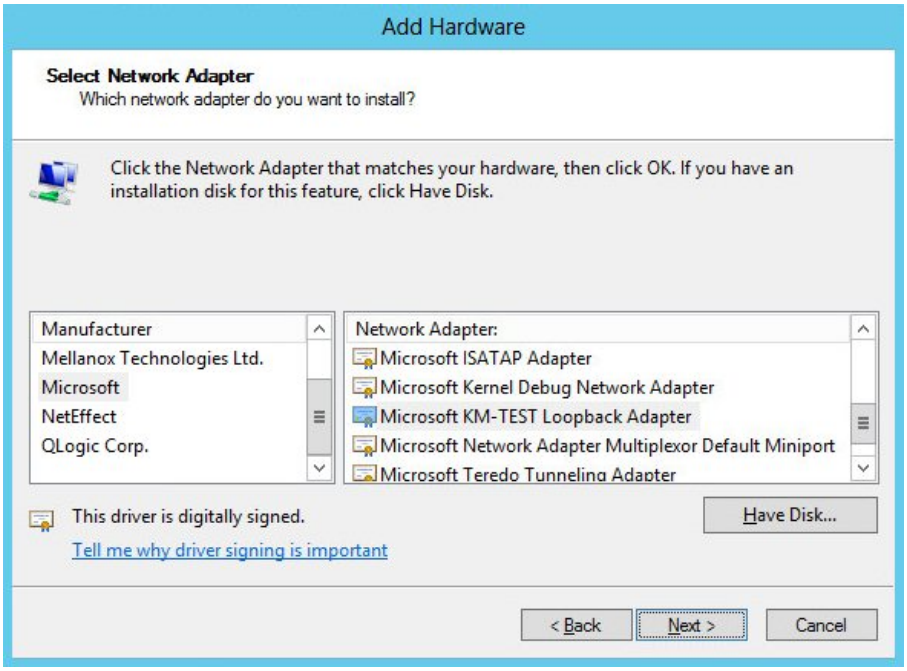
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables 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.

8.3.1. Step 1 of 3: Install the Microsoft Loopback Adapter

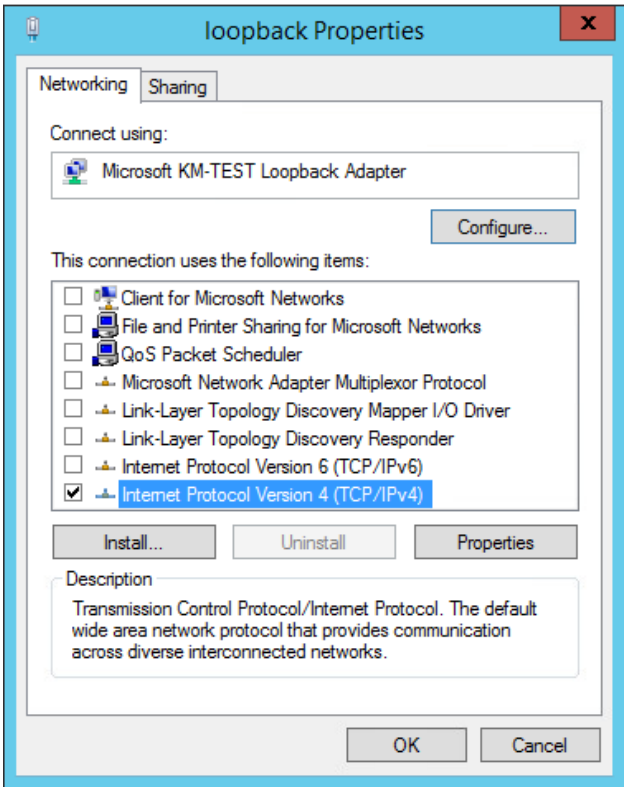
1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. Once the Wizard has started, click **Next**.
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.
4. Select **Network adapters**, click **Next**.



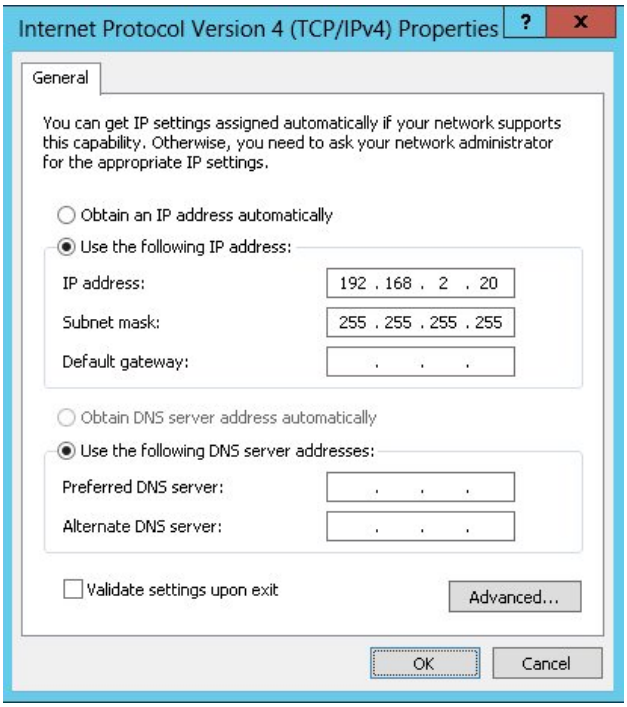
5. Select **Microsoft** & **Microsoft KM-Test Loopback Adapter**, click **Next**.
6. Click **Next** to start the installation, when complete click **Finish**.

8.3.2. 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**.
4. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below:



5. 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.

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

8.3.3. 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:

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

Option 2 - Using PowerShell Cmdlets

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

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

9. Appliance Installation & Configuration for DL

9.1. Overview

For DL deployments, 2 load balancer appliances must be installed and configured and then paired to create an active/passive HA clustered pair.

The following is an overview of the installation and configuration process:

1. Deploy 2 Virtual Appliances - refer to Section 9.2
2. Configure the management IP address and other network settings on **both** appliances - refer to Section 9.3
3. Run a software update check on **both** appliances - refer to Section 9.5
4. Configure the appliance security mode on **both** appliances - refer to Section 9.6
5. Verify network connections and configure any additional settings on **both** appliances - refer to Section 9.7
6. Configure the required load balanced services on the **Primary** appliance - refer to Section 9.8
7. Verify that everything is working as expected on the **Primary** appliance - refer to Section 10
8. Configure the HA Pair on the **Primary** appliance - this will replicate all load balanced services to the Secondary appliance, once configured the Secondary appliance will be kept in-sync automatically - refer to Section 11
9. Configure any required optional settings on **both** appliances - refer to Section 12

9.2. Virtual Appliance Installation

9.2.1. Download & Extract the Appliance

1. Download the Virtual Appliance.
2. Unzip the contents of the file to your chosen location.

9.2.2. Virtual Hardware Resource Requirements

The resource requirements depend on the particular virtual appliance used. The following GE HealthCare VAs are available:

- **v1000** - 2 vCPUs, 4GB RAM, 20GB Drive
- **v4000** - 4 vCPUs, 8GB RAM, 20GB Drive
- **vUltimate** - 8 vCPUs, 16GB RAM, 20GB Drive

Please refer to the technical documentation for the site to determine which appliance to use and obtain the download link.

9.2.3. VMware vSphere Client

The steps below apply to VMware ESX/ESXi & vSphere Client v6.7 and later.

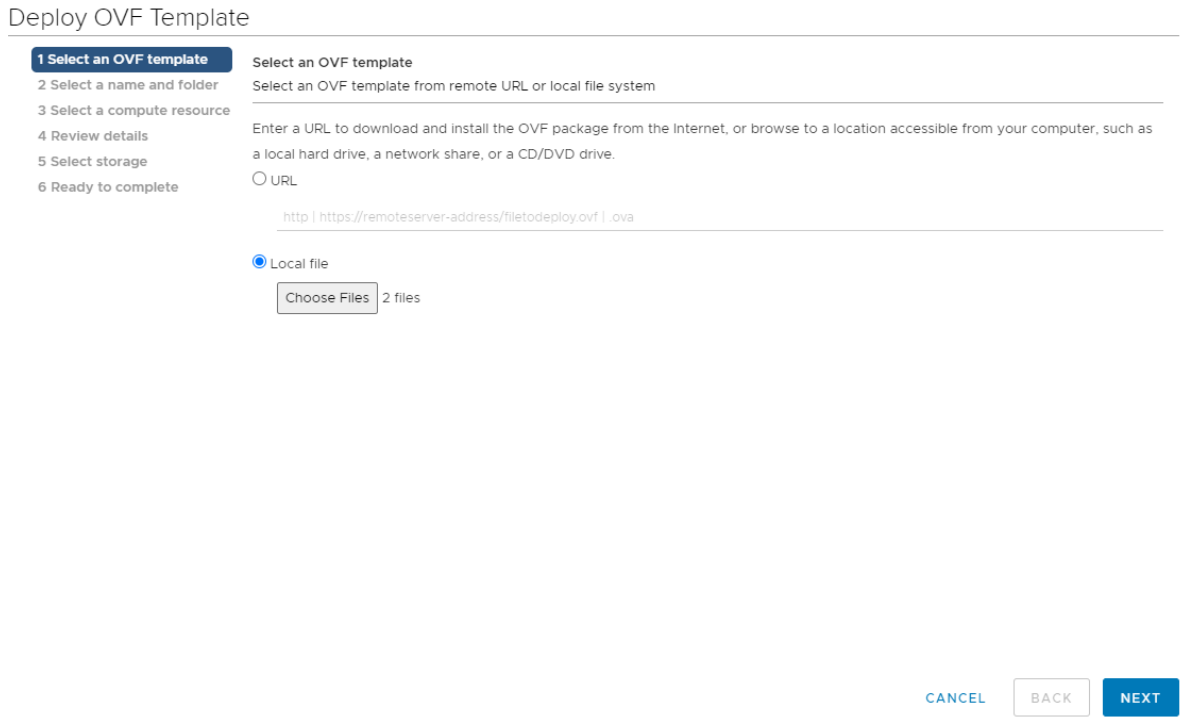
9.2.3.1. Upgrading to the latest Hardware Version

When the appliance is deployed, the virtual hardware version is set to 11. This enables compatibility with ESX version 6.0 and later. You can upgrade to a later hardware version if required.

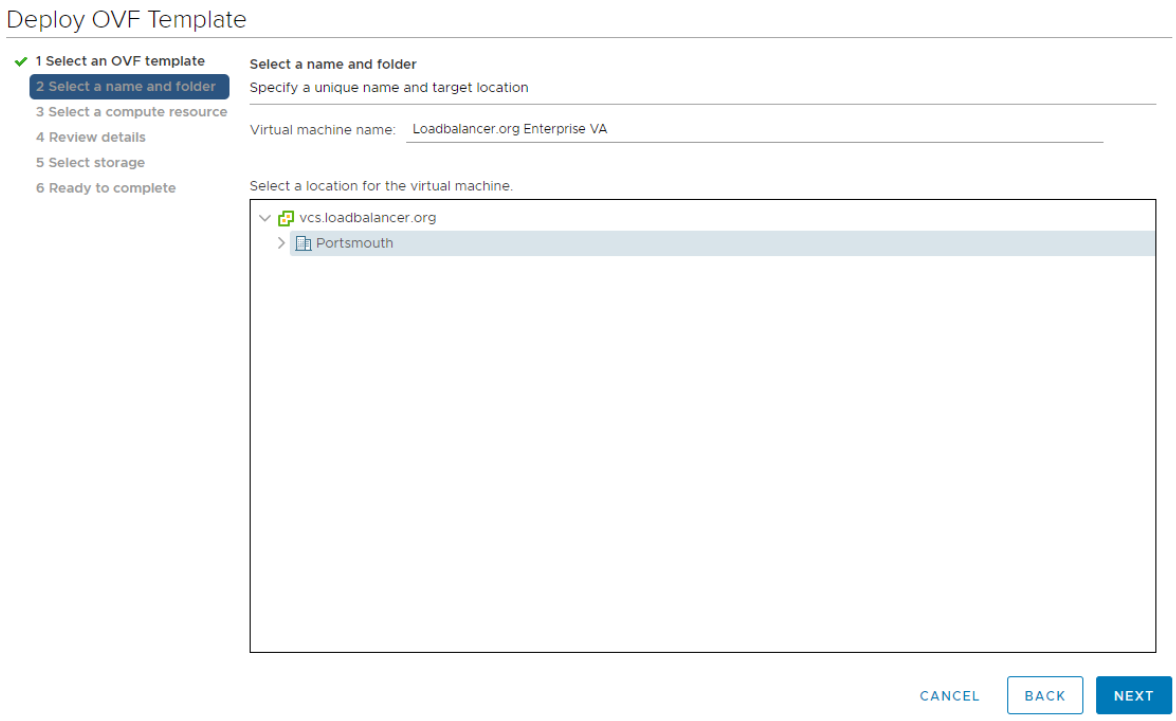
> **Note** Create a snapshot or backup of the virtual machine first before upgrading.

9.2.3.2. Installing the Appliance using vSphere Client

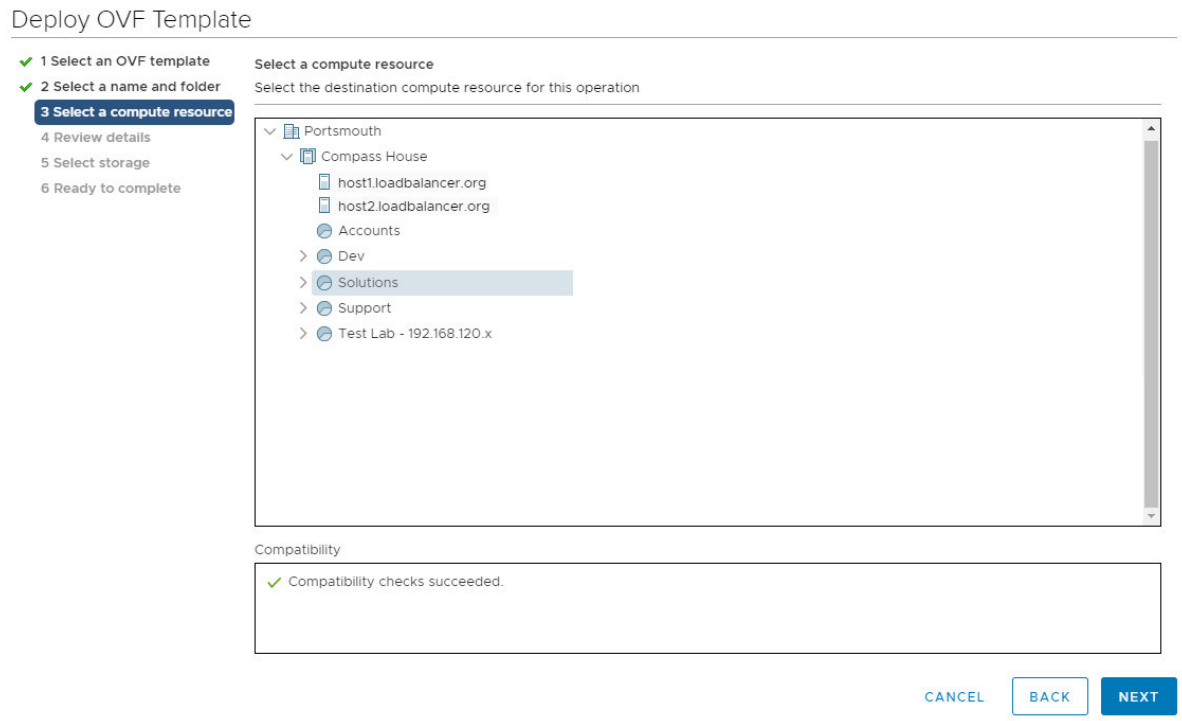
1. Right-click the inventory object where the appliance is to be located and select **Deploy OVF Template**.
2. In the **Select an OVF Template** screen, select the **Local File** option, click **Browse**, navigate to the download location, select the **.ova** file and click **Next**.



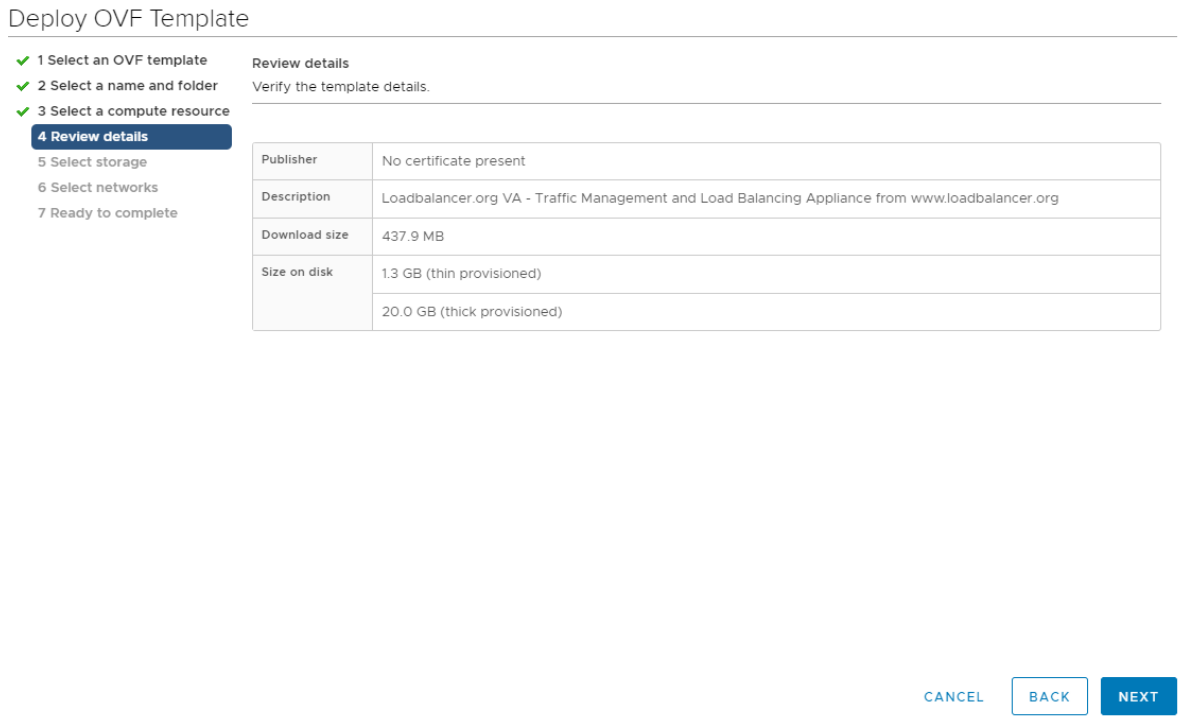
3. In the **Select a name and folder** screen, type a suitable name for the appliance - this can be up to 80 characters in length.
4. Select the required location for the appliance - by default this will be the location of the inventory object from where the wizard was started and click **Next**.



5. In the **Select a compute resource** screen, select the required compute resource for the appliance - by default this will be the inventory object from where the wizard was started and click **Next**.

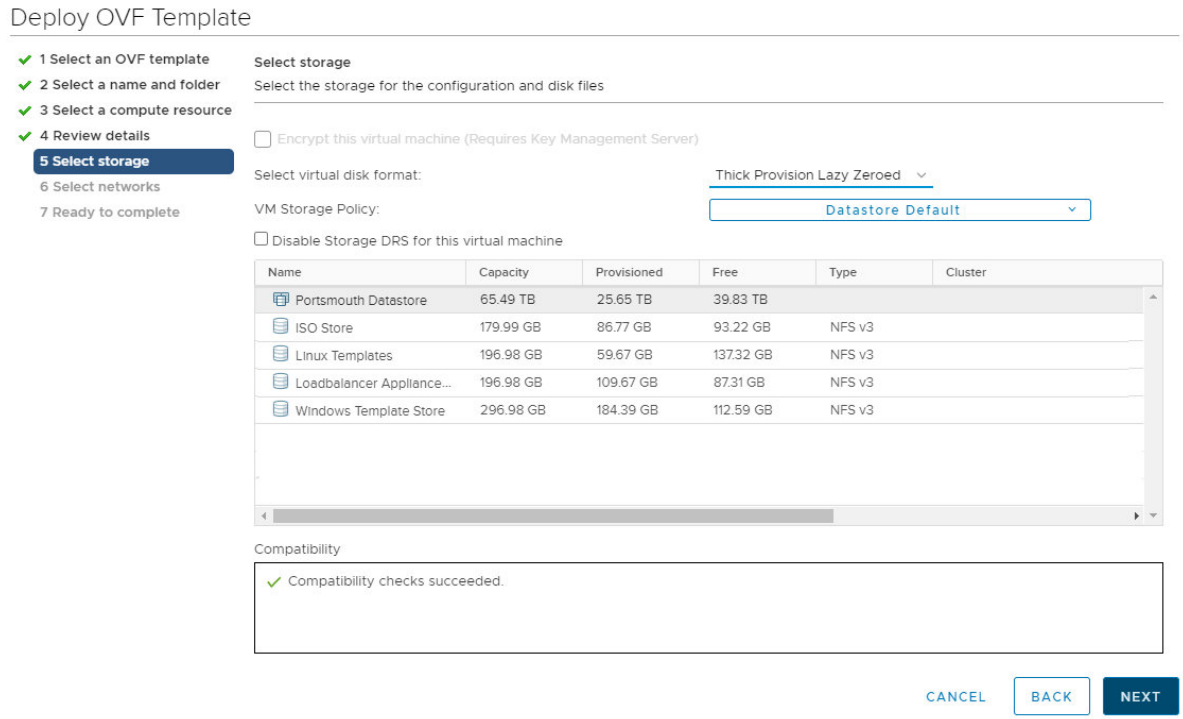


6. In the **Review details** screen, verify the template details and click **Next**.

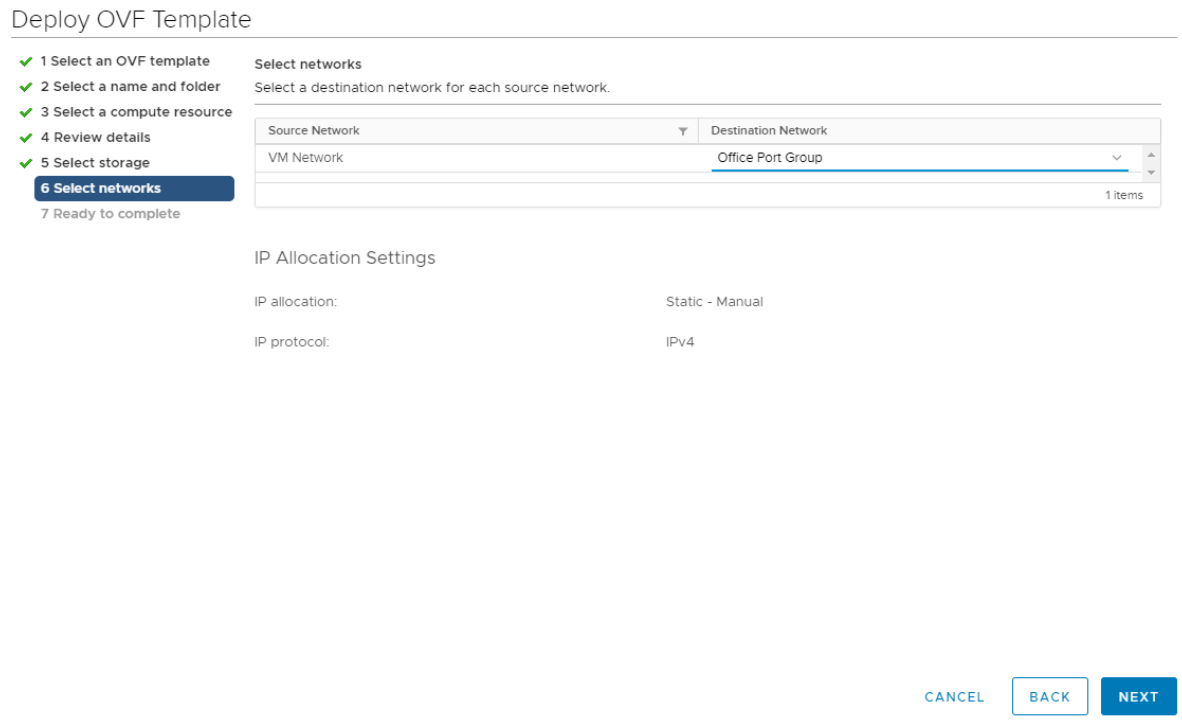


7. In the **Select Storage** screen, first select the required storage location for the appliance.
8. Now select the required disk format and click **Next**.

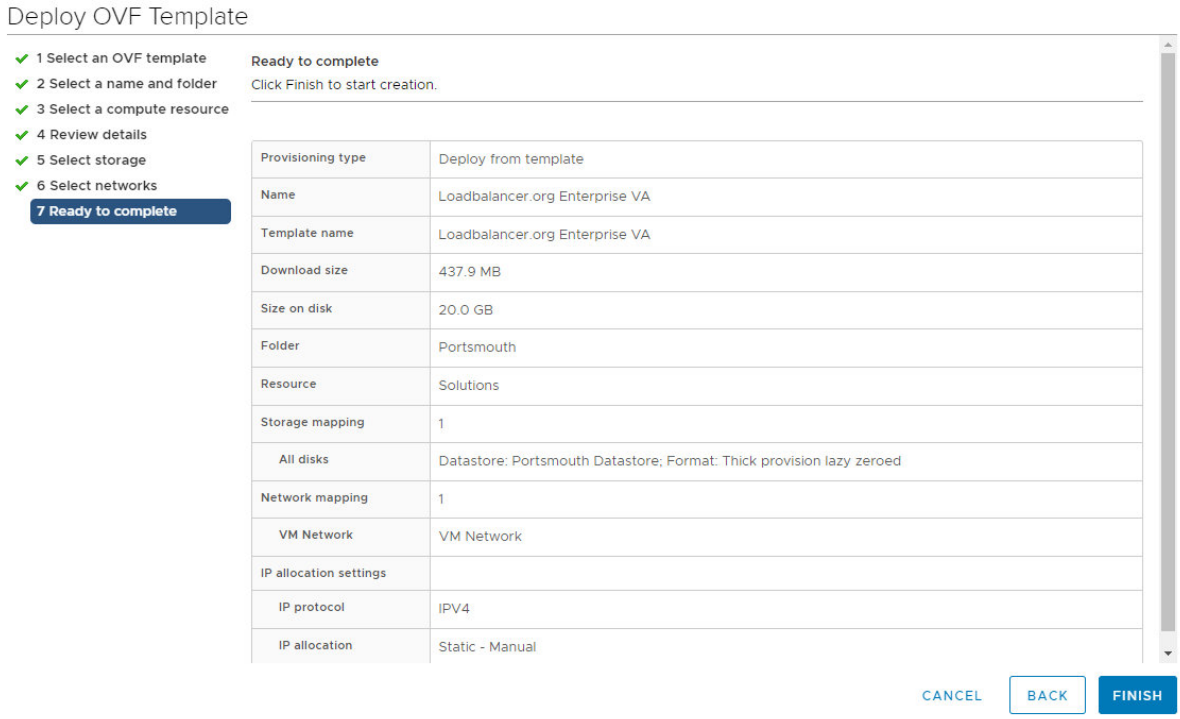
> **Note** Loadbalancer.org recommends selecting a thick provision format. By default the appliance disk is 20GB.



9. In the **Select Networks** screen, select the required destination network using the drop-down next to **VM Network** and click **Next**.



10. In the **Ready to complete** screen, review the settings and click **Finish** to create the virtual appliance. To change a setting, use the **Back** button to navigate back through the screens as required.



9.2.3.3. Configure Network Adapters

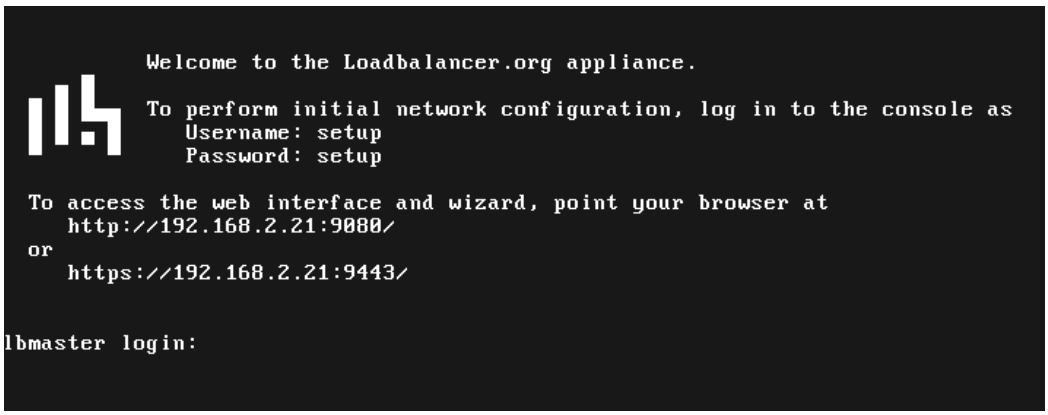
The appliance has 4 network adapters. By default only the first adapter is connected which is the requirement for GE HealthCare deployments. This will be **eth0** when viewed in the appliance WebUI.

9.2.3.4. Start the Appliance

Now power up the appliance.

9.3. Configuring Initial Network Settings

After power up, the following startup message is displayed on the appliance console:



As mentioned in the text, to perform initial network configuration, login as the "setup" user at the appliance console.

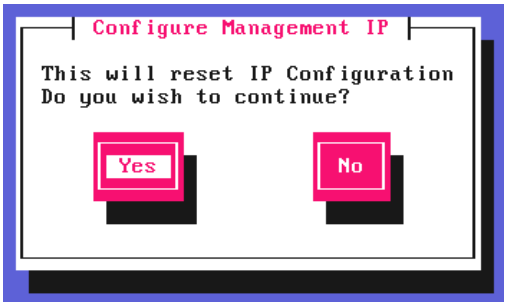
Once logged in, the Network Setup Wizard will start automatically. This will enable you to configure the management IP address and other network settings for the appliance.

login to the console:

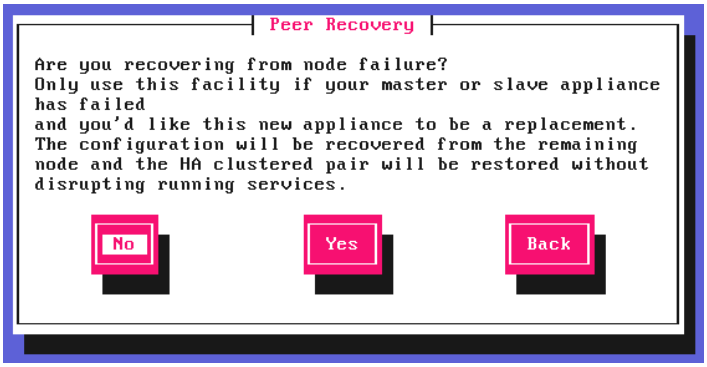
Username: setup
Password: setup

A series of screens will be displayed that allow network settings to be configured:

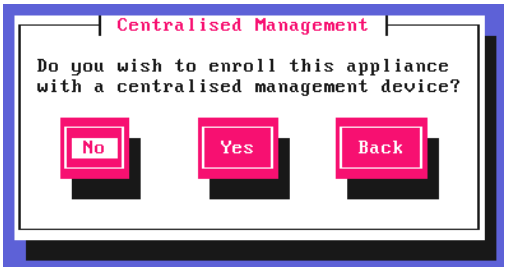
In the **Configure Management IP** screen, leave **Yes** selected and hit <ENTER> to continue.



In the **Peer Recovery** screen, leave **No** selected and hit <ENTER> to continue.

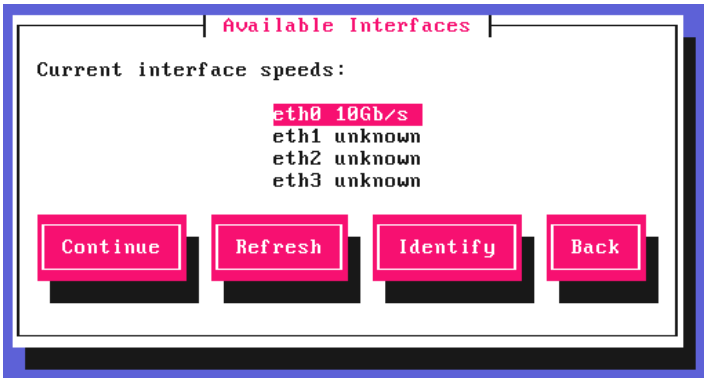


In the **Centralized Management** screen, if you have been provided with Management Server details select **Yes**, otherwise leave **No** selected, then hit <ENTER> to continue.

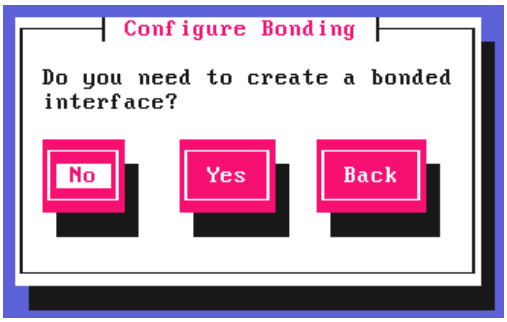


> **Note** For information on how to modify Centralized Management settings via the WebUI, please refer to Portal Management & Appliance Adoption.

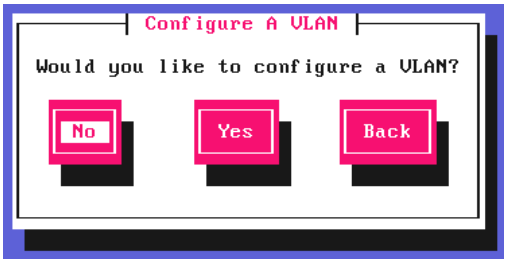
In the **Available Interfaces** screen, a list of available interfaces will be displayed, hit <ENTER> to continue.



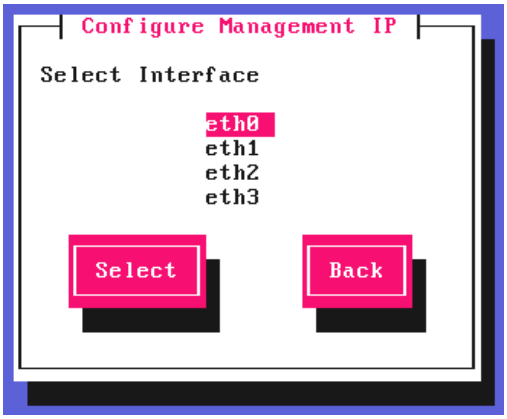
In the **Configure Bonding** screen, leave **No** selected, then hit <ENTER> to continue.



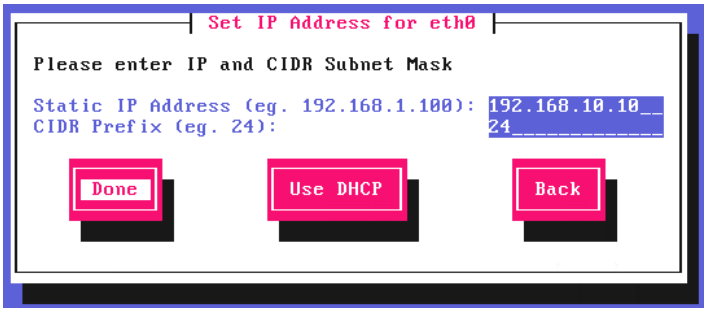
In the **Configure a VLAN** screen, leave **No** selected, then hit <ENTER> to continue.



In the **Configure Management IP** screen, select **eth0** and hit <ENTER> to continue.

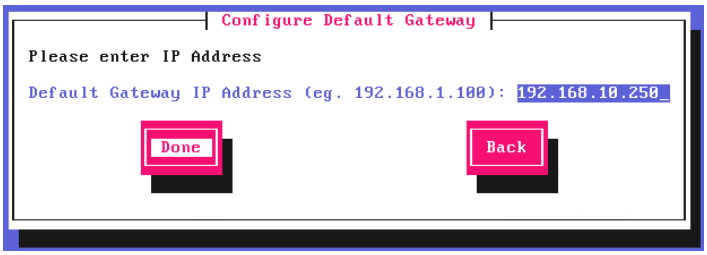


In the **Set IP address** screen, specify the required management address in the *Static IP Address* & *CIDR Prefix* fields, select **Done** and hit <ENTER> to continue.

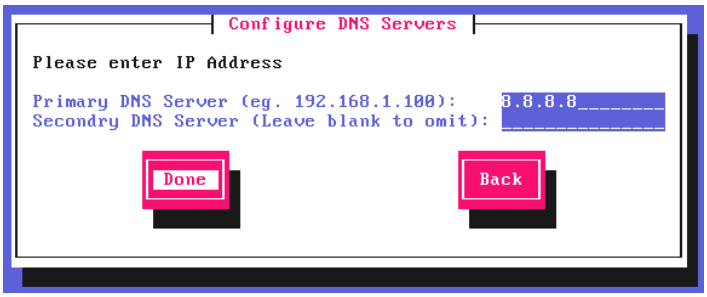


> **Note** A subnet mask such as 255.255.255.0 is not valid, in this case enter 24 instead.

In the **Configure Default Gateway** screen, enter the required *Default Gateway IP Address*, select **Done** and hit <ENTER> to continue.

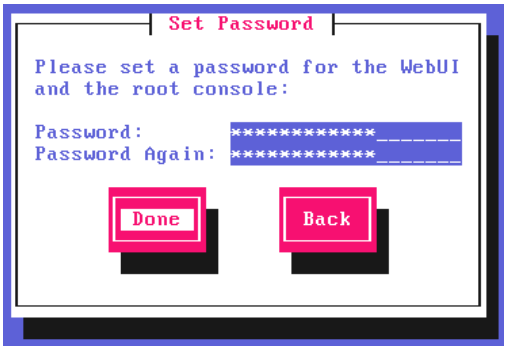


In the **Configure DNS Servers** screen, configure the required DNS server(s), select **Done** and hit <ENTER> to continue.

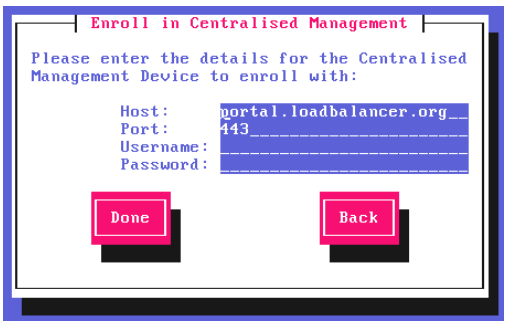


In the **Set Password** screen, hit <ENTER> to continue.

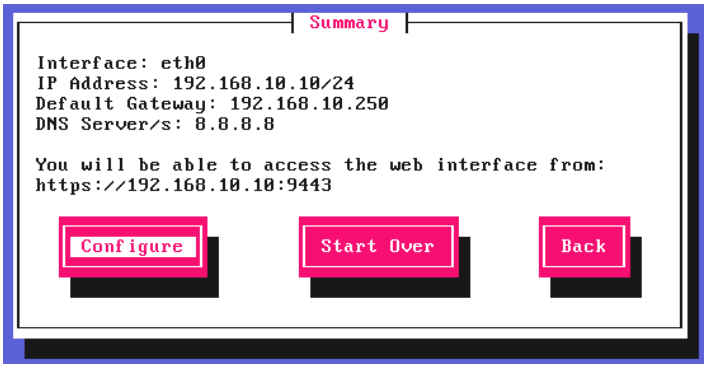
Enter the *Password* you'd like to use for the **loadbalancer** WebUI user account and the **root** Linux user account. Repeat the password, select **Done** and hit <ENTER> to continue.



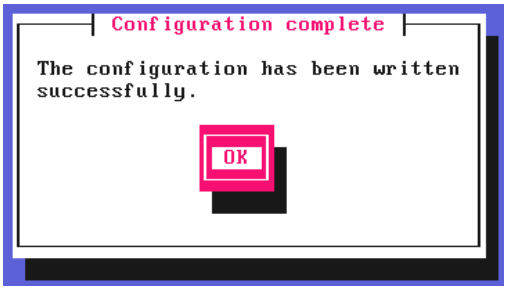
If you selected **Yes** when asked if you want to enroll for Centralized Management, you'll now be prompted for the details. Default values for the *Host* and *Port* are set and can be changed if required. Enter the *Username* and *Password* for the management server account you'd like the appliance to be associated with, select **Done** and hit <ENTER> to continue.



In the **Summary** screen, check all settings. If everything is correct, leave **Configure** selected and hit <ENTER> to continue. All settings will be applied. If you need to change a setting, use the **Back** button.



Once the configuration has been written, the **Configuration Complete** screen and message will be displayed. Click **OK** to exit the wizard and return to the command prompt.



9.4. 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.

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.

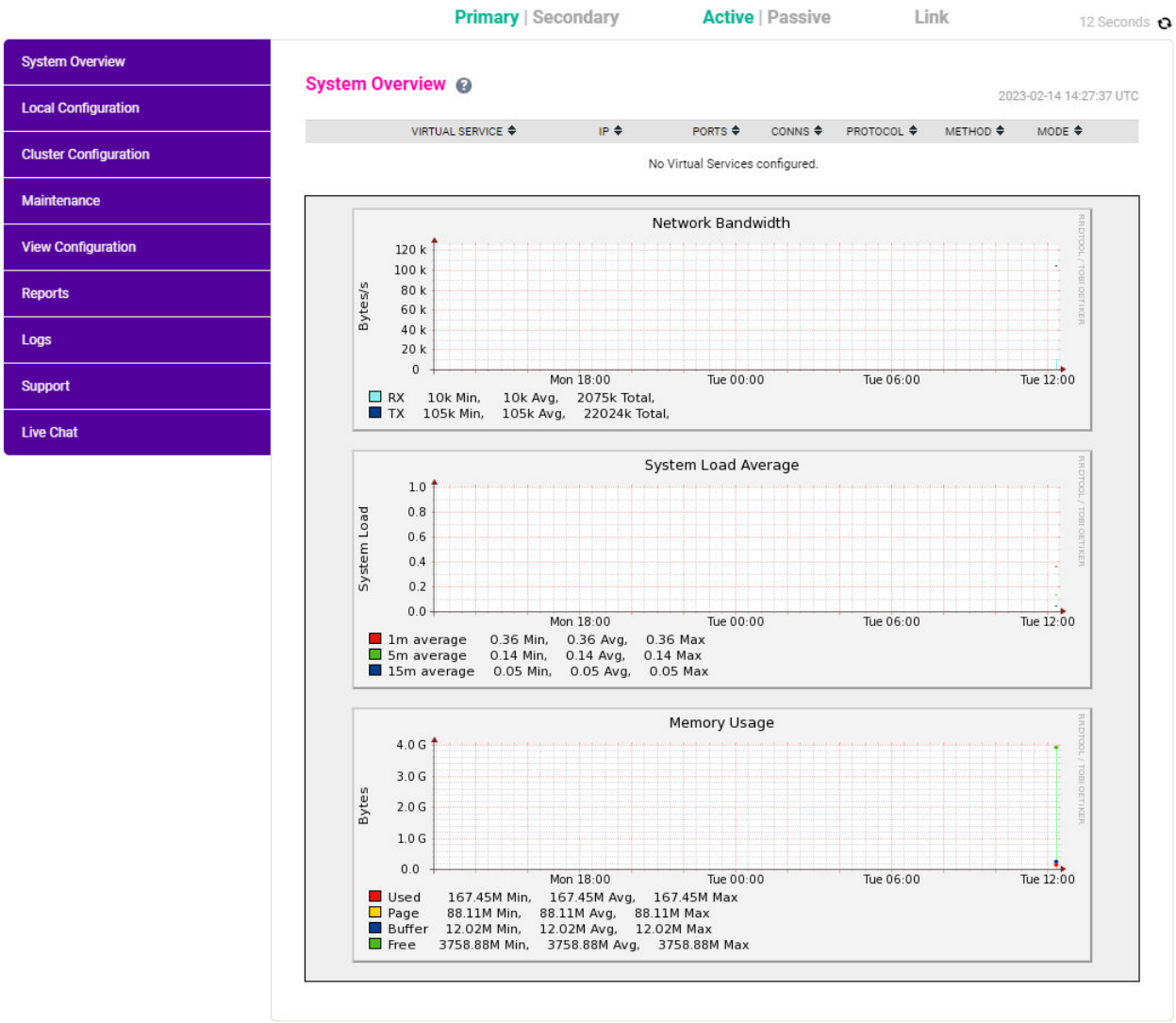
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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:



9.4.1. 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

9.5. Appliance Software Update

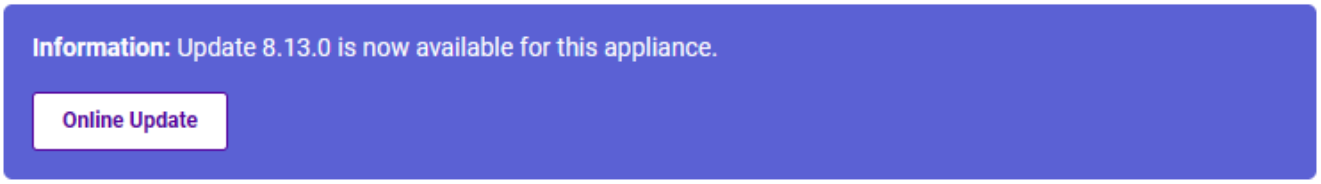
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **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.

9.5.1. Online Update

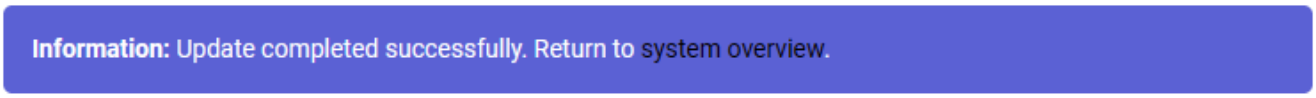
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



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.

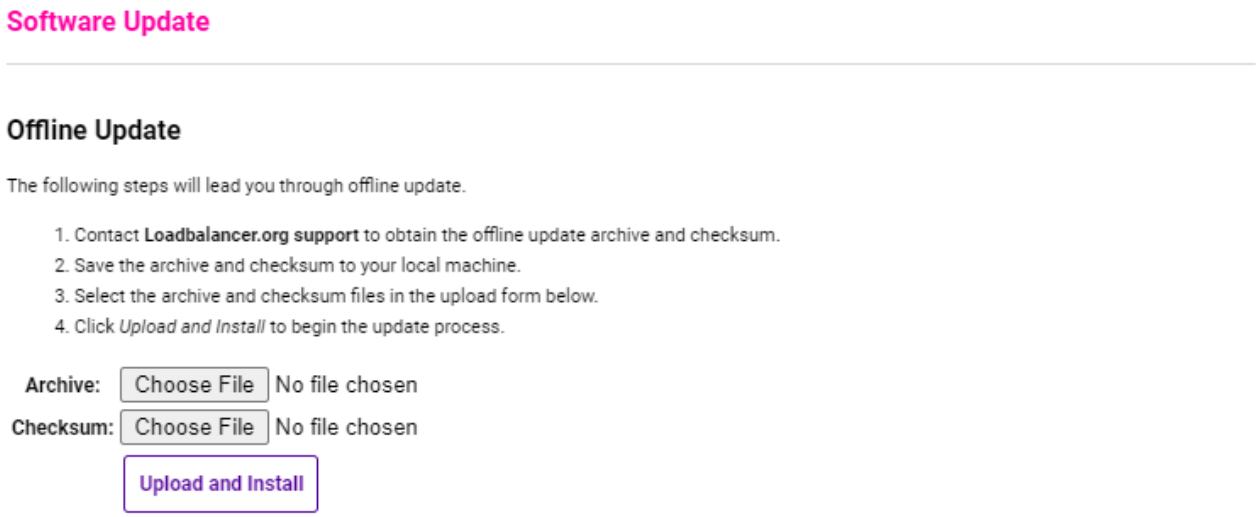
9.5.2. Offline Update

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.

9.6. Configuring the Appliance Security Mode

To enable shell commands to be run from the WebUI, the appliance Security Mode must be configured:

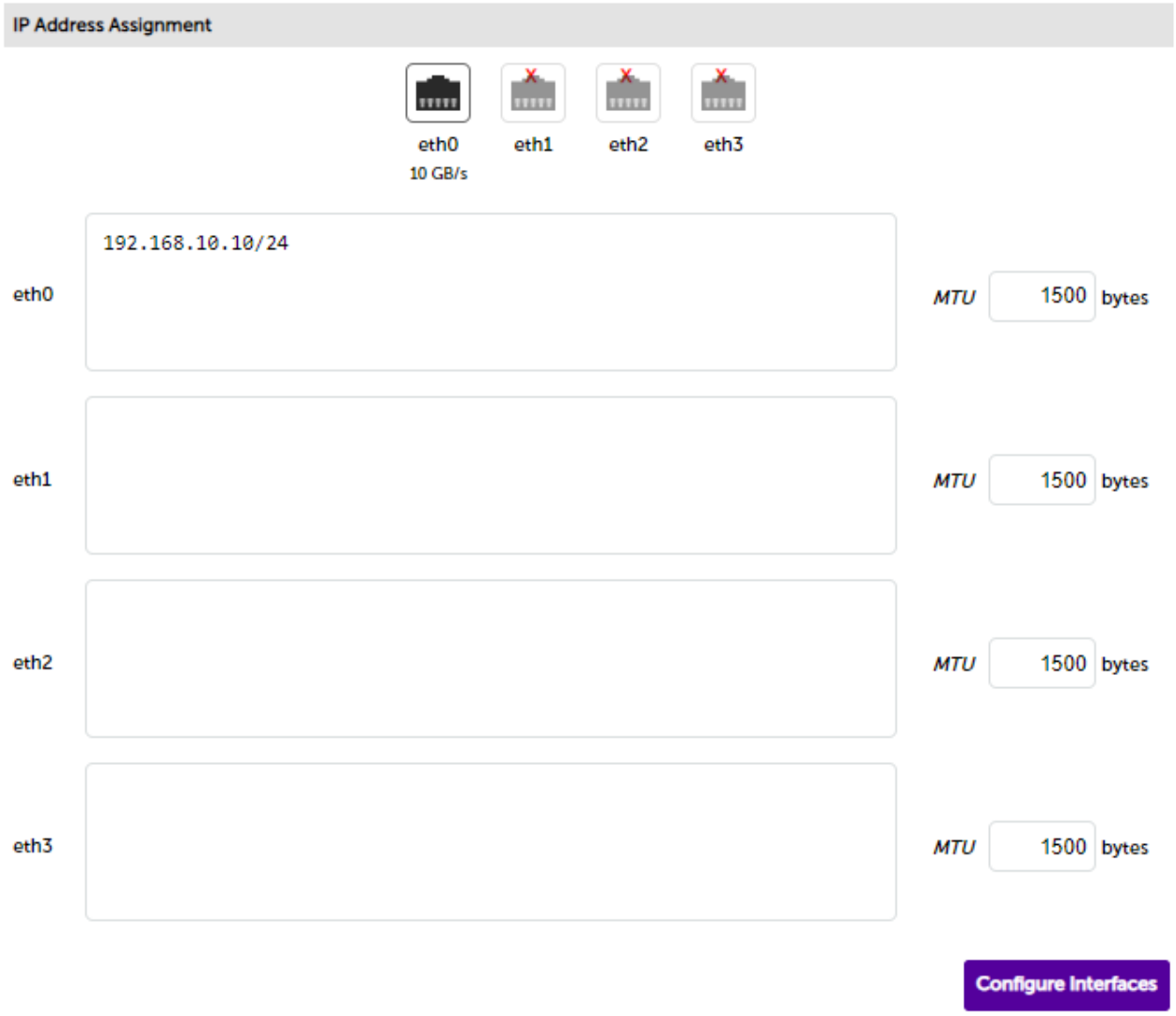
1. Using the WebUI, navigate to: *Local Configuration > Security*.
2. Set *Appliance Security Mode* to **Custom**.
3. Click **Update**.

9.7. Appliance Network Configuration

The standard DL network configuration requires 1 network adapter.

9.7.1. Verify Network Connections

1. Verify that the adapter is connected to the appropriate virtual switch/network using the Hypervisor management tool.
2. Using the appliance WebUI navigate to: *Local Configuration > Network Interface Configuration*.



3. Verify that the network is configured as required.

> **Note** The IP address/CIDR prefix for **eth0** was set during the Network Setup Wizard and will be shown here, e.g. **192.168.10.10/24**.

9.7.2. Configuring Hostname & DNS

1. Using the WebUI, navigate to: *Local Configuration > Hostname & DNS*.
2. Set the required *Hostname* and *Domain Name*.
3. Configure additional DNS servers if required.
4. Click **Update**.

9.7.3. Configuring NTP

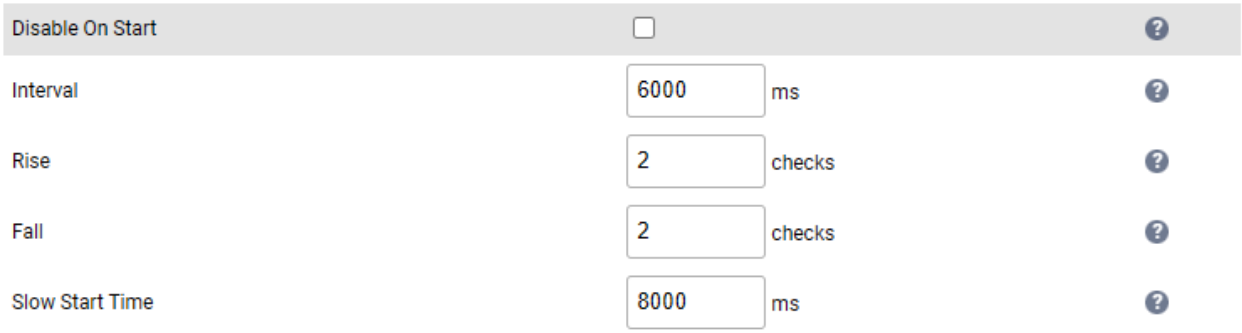
1. Using the WebUI, navigate to: *Local Configuration > System Date & Time*.
2. Select the required *System Timezone*.
3. Define the required NTP servers.

4. Click **Set Timezone & NTP**.

9.8. Configuring Load Balanced Services

9.8.1. Layer 7 Global Settings

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 - Advanced Configuration*.
2. Set the health check *Interval* to **6000** (ms) as shown below.

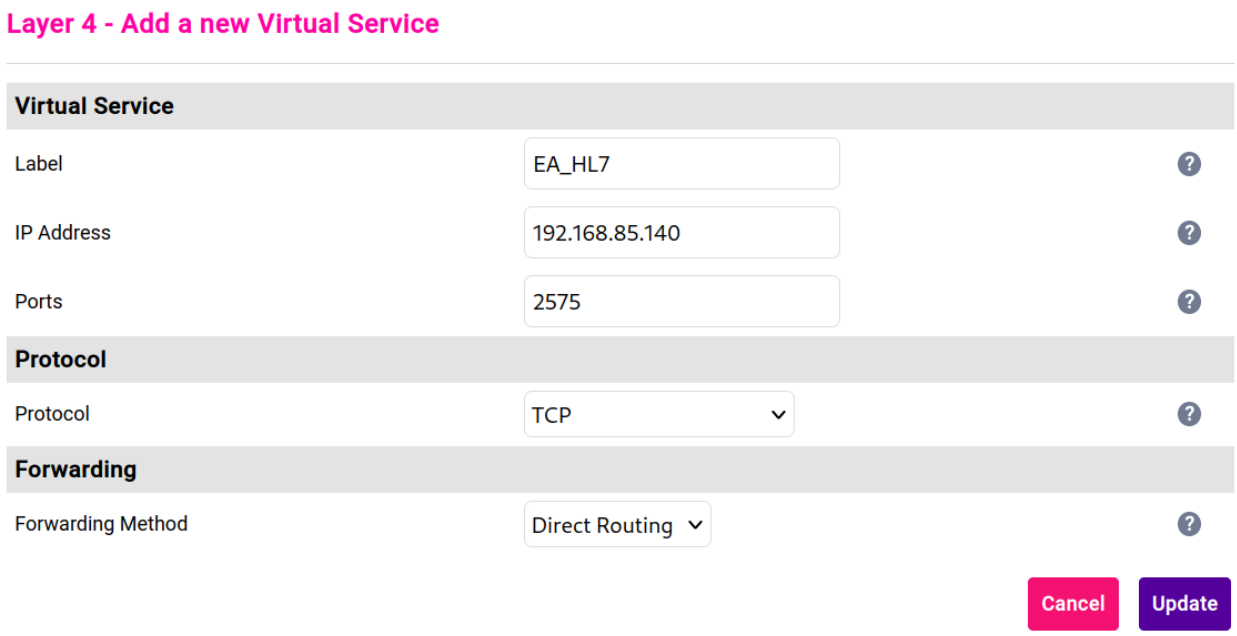


3. Scroll to the bottom of the page and click **Update**.

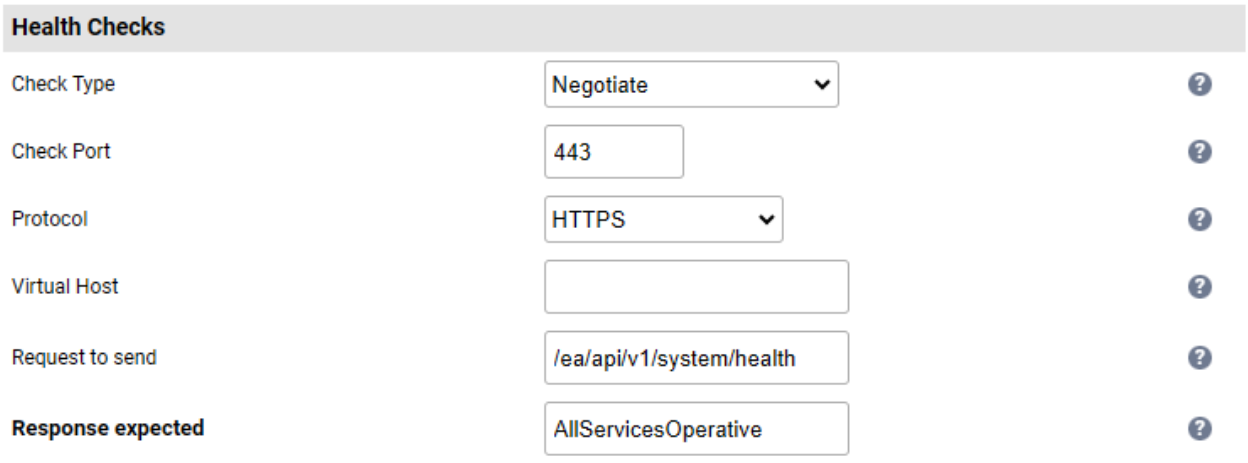
9.8.2. VIP 1 - EA_HL7

9.8.2.1. 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. **EA_HL7**.
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 **2575**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Persistence Timeout* to **1980** seconds.
11. Set the *Health Checks Check Type* to **Negotiate**.
12. Set the *Check Port* to **443**.
13. Set the *Protocol* to **HTTPS**.
14. Set the *Request to send* to **/ea/api/v1/system/health**
15. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.



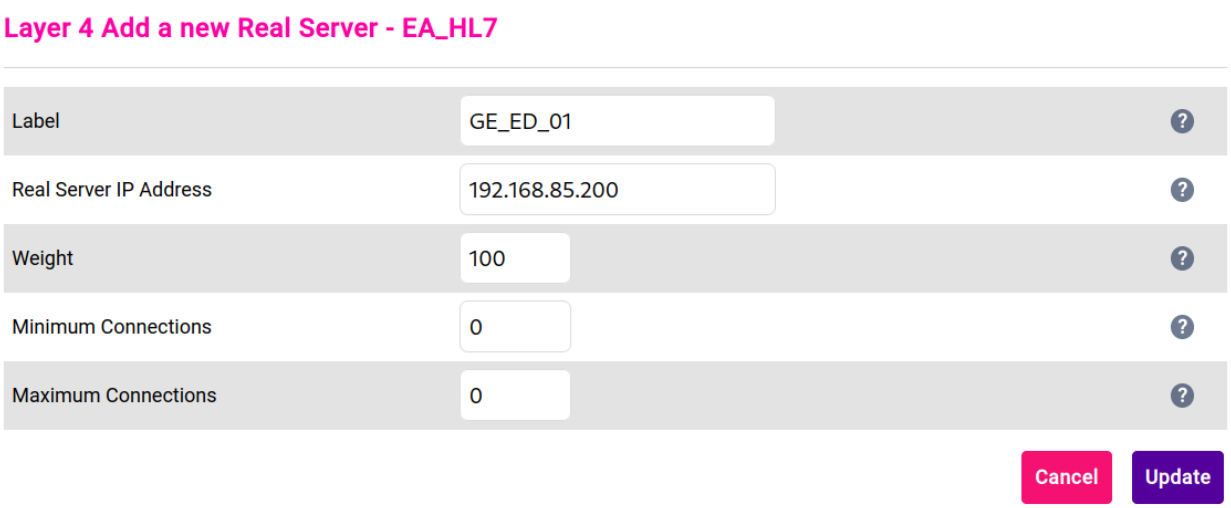
16. Leave all other settings at their default value.
17. Click **Update**.

9.8.2.2. 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.

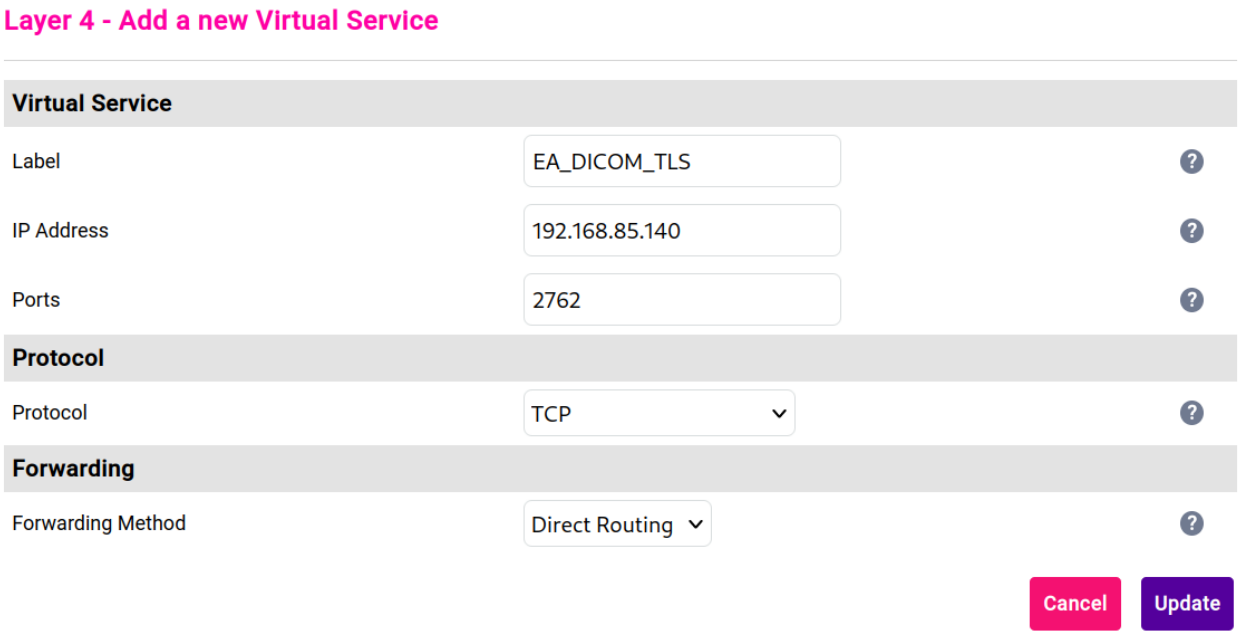
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



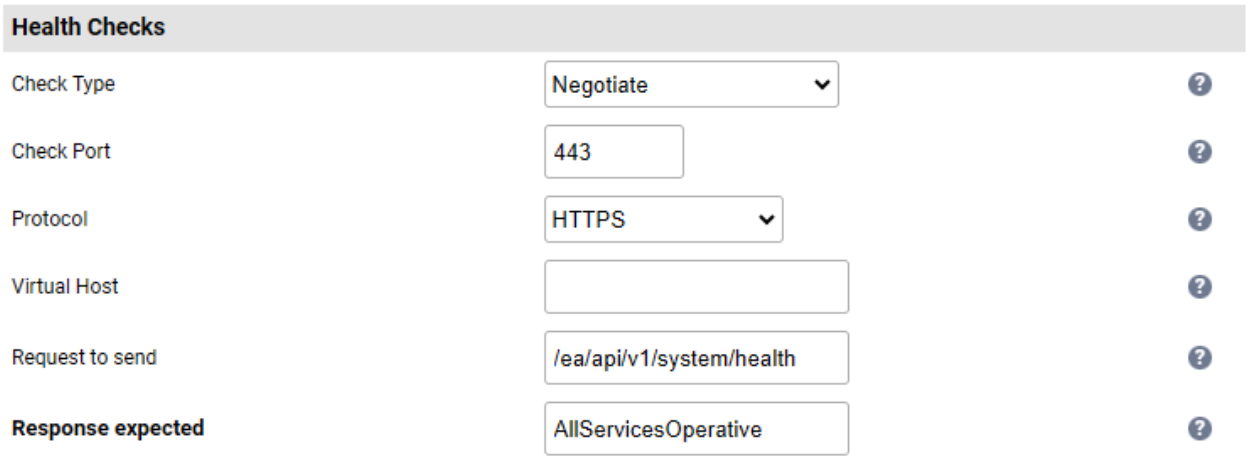
9.8.3. VIP 2 - EA_DICOM_TLS

9.8.3.1. 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. **EA_DICOM_TLS**.
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 **2762**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Persistence Timeout* to **1980** seconds.
11. Set the *Health Checks Check Type* to **Negotiate**.
12. Set the *Check Port* to **443**.
13. Set the *Protocol* to **HTTPS**.
14. Set the *Request to send* to **/ea/api/v1/system/health**
15. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.



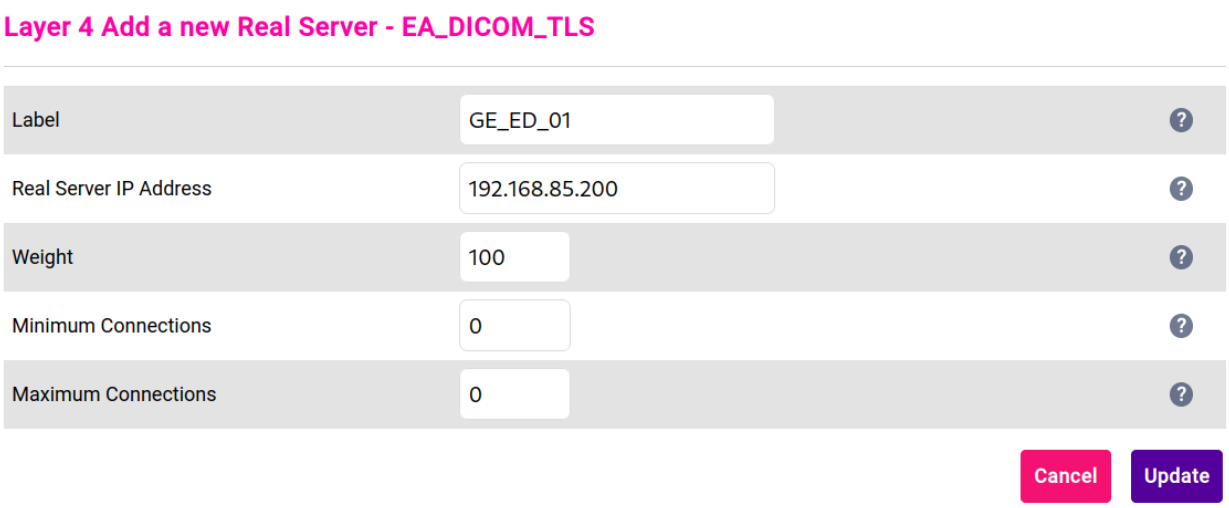
16. Leave all other settings at their default value.
17. Click **Update**.

9.8.3.2. 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.

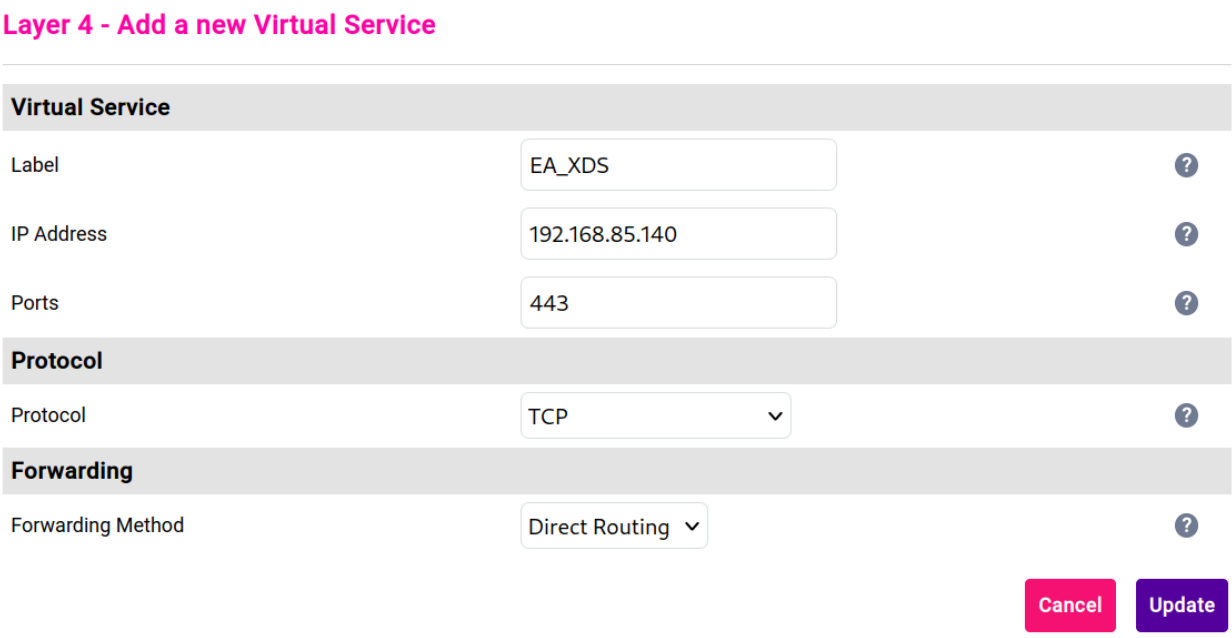
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



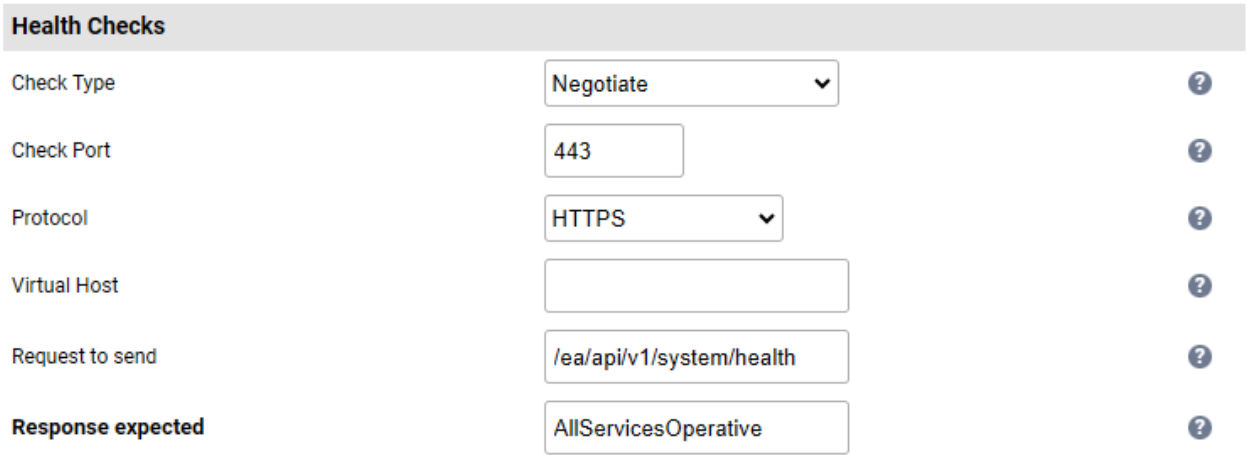
9.8.4. VIP 3 - EA_XDS

9.8.4.1. 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. **EA_XDS**.
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 **443**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



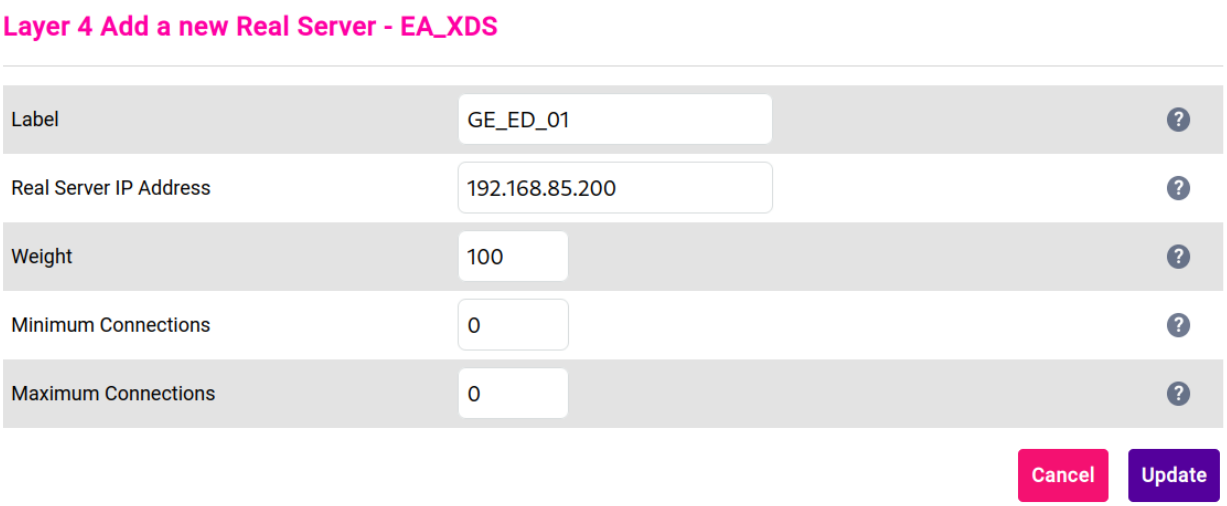
8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Persistence Timeout* to **1980** seconds.
11. Set the *Health Checks Check Type* to **Negotiate**.
12. Set the *Check Port* to **443**.
13. Set the *Protocol* to **HTTPS**.
14. Set the *Request to send* to **/ea/api/v1/system/health**
15. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.



16. Leave all other settings at their default value.
17. Click **Update**.

9.8.4.2. Defining the Real Servers (RIPs)

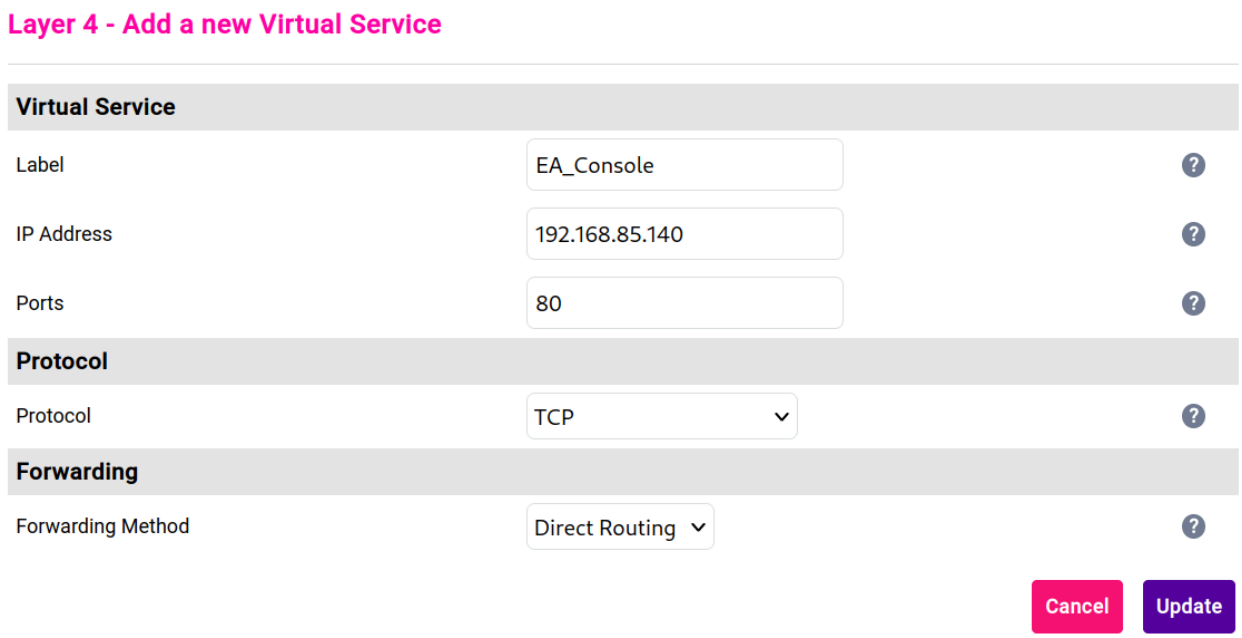
1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



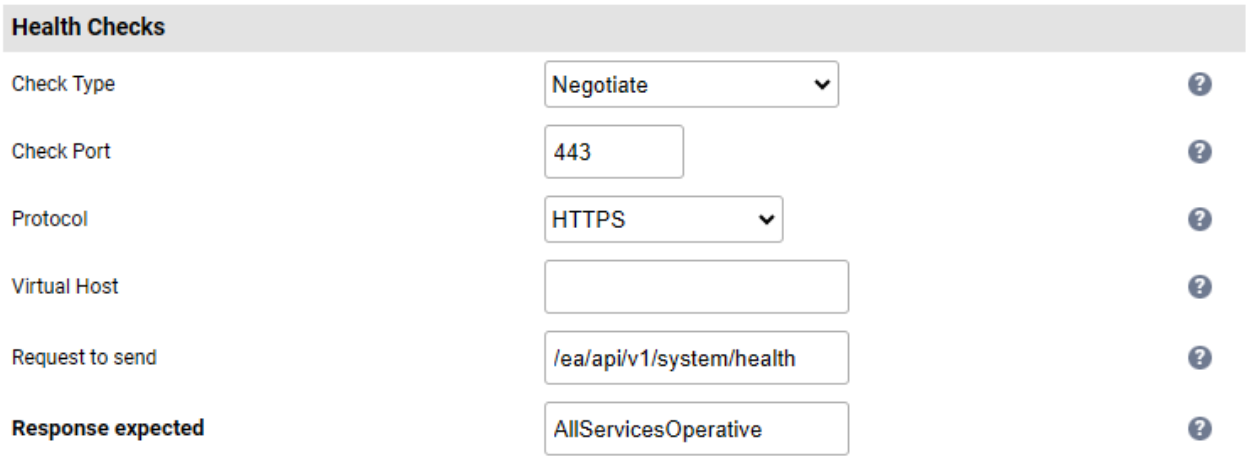
9.8.5. VIP 4 - EA_Console

9.8.5.1. 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. **EA_Console**.
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 **80**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



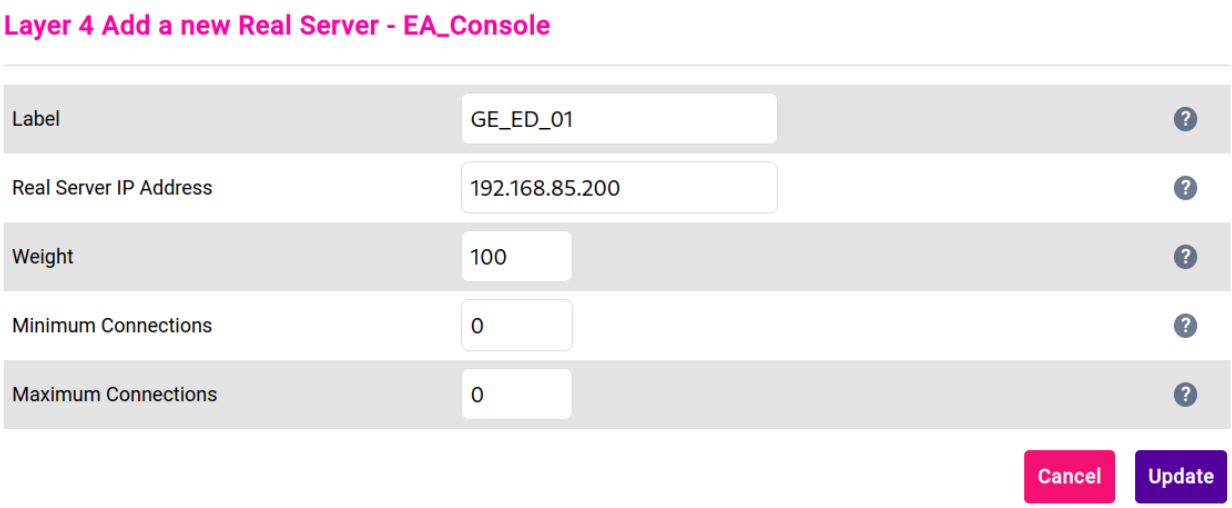
8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Persistence Timeout* to **1980** seconds.
11. Set the *Health Checks Check Type* to **Negotiate**.
12. Set the *Check Port* to **443**.
13. Set the *Protocol* to **HTTPS**.
14. Set the *Request to send* to **/ea/api/v1/system/health**
15. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.



16. Leave all other settings at their default value.
17. Click **Update**.

9.8.5.2. Defining the Real Servers (RIPs)

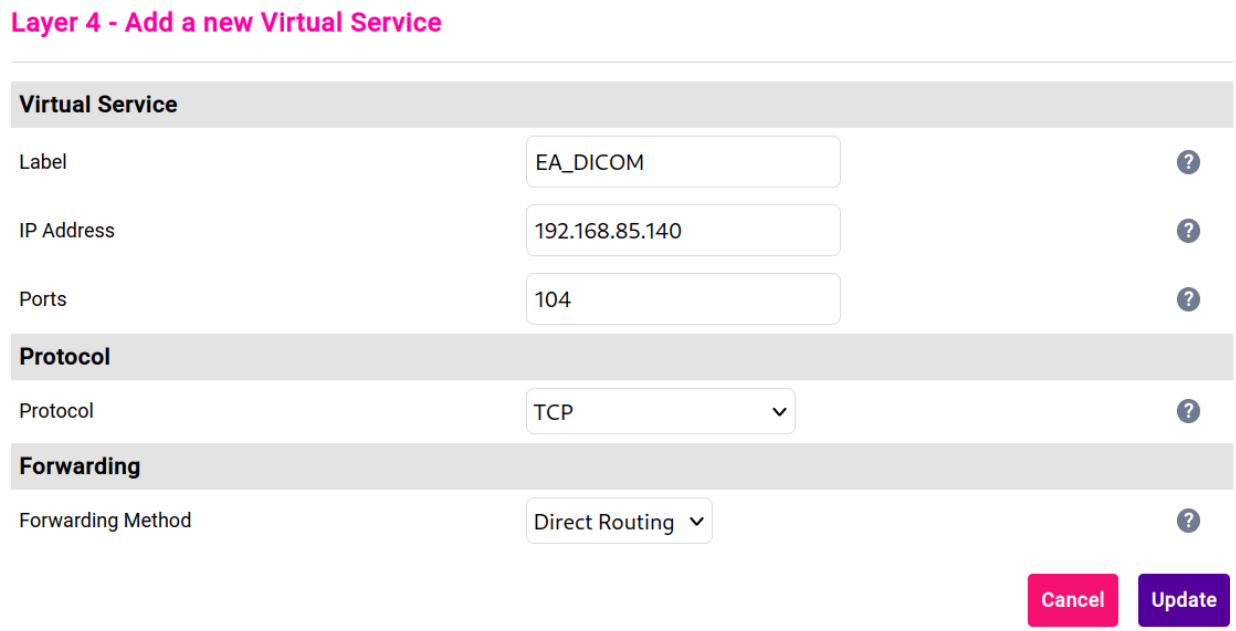
1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



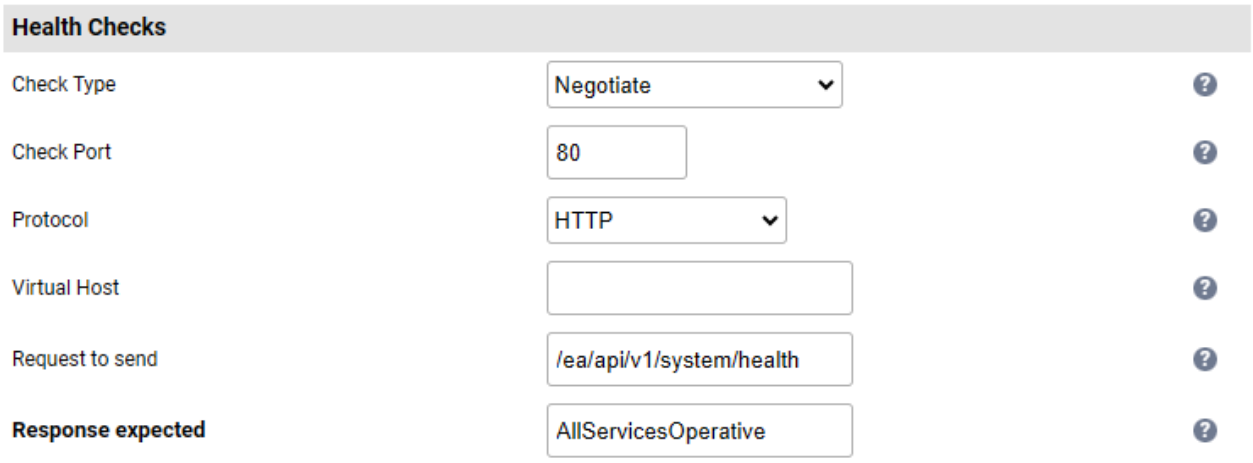
9.8.6. VIP 5 - EA_DICOM

9.8.6.1. 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. **EA_DICOM**.
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 **104**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **80**.
12. Set the *Protocol* to **HTTP**.
13. Set the *Request to send* to **/ea/api/v1/system/health**
14. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.

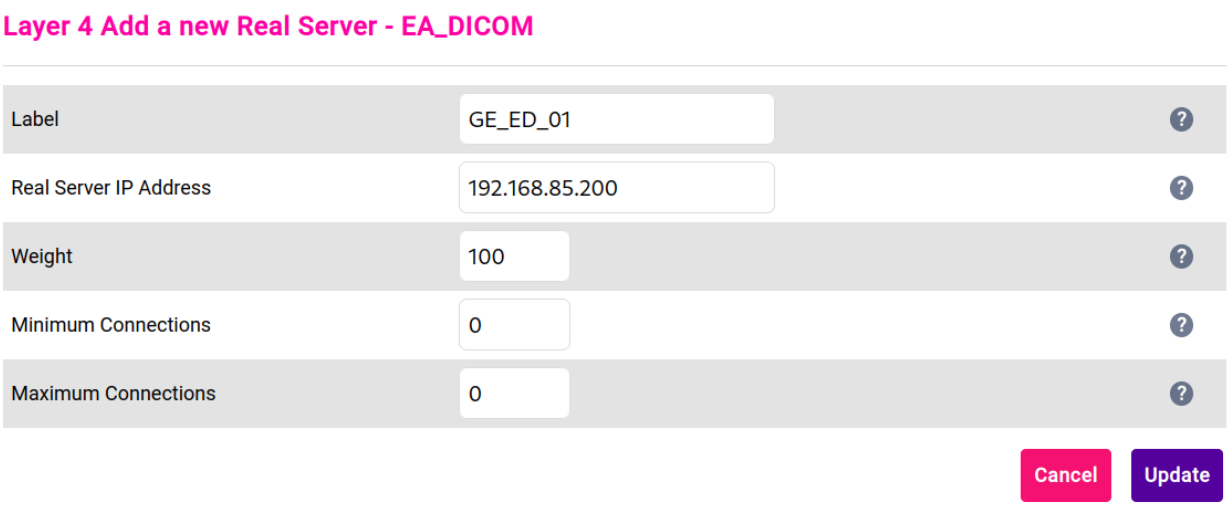


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.6.2. 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.

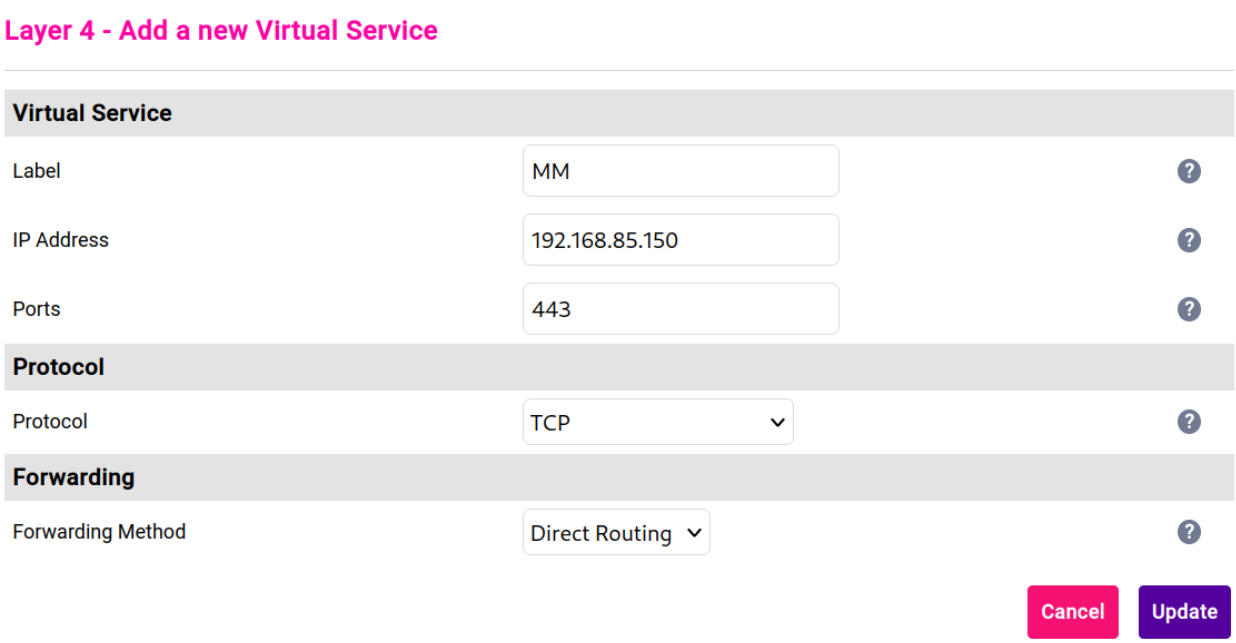
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



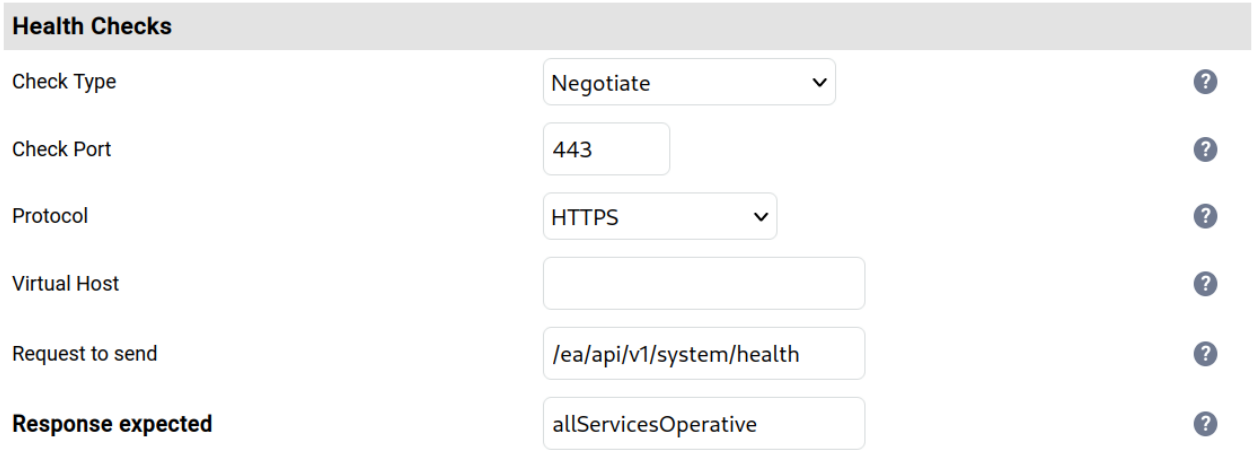
9.8.7. VIP 6 - MM

9.8.7.1. 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. **MM**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.150**.
4. Set the *Ports* field to **443**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **443**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/ea/api/v1/system/health**
14. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.

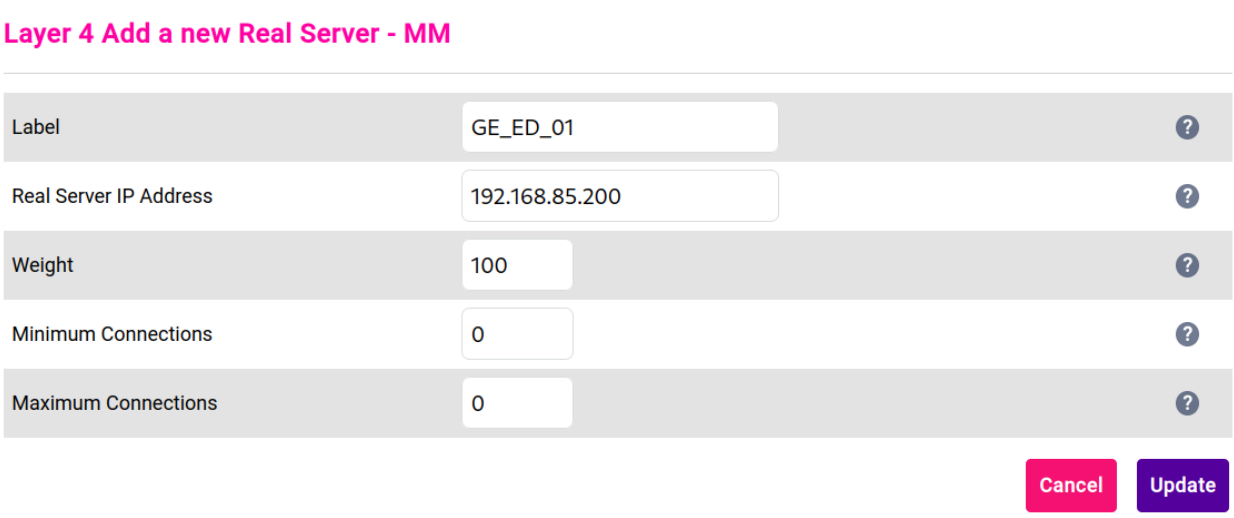


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.7.2. 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.

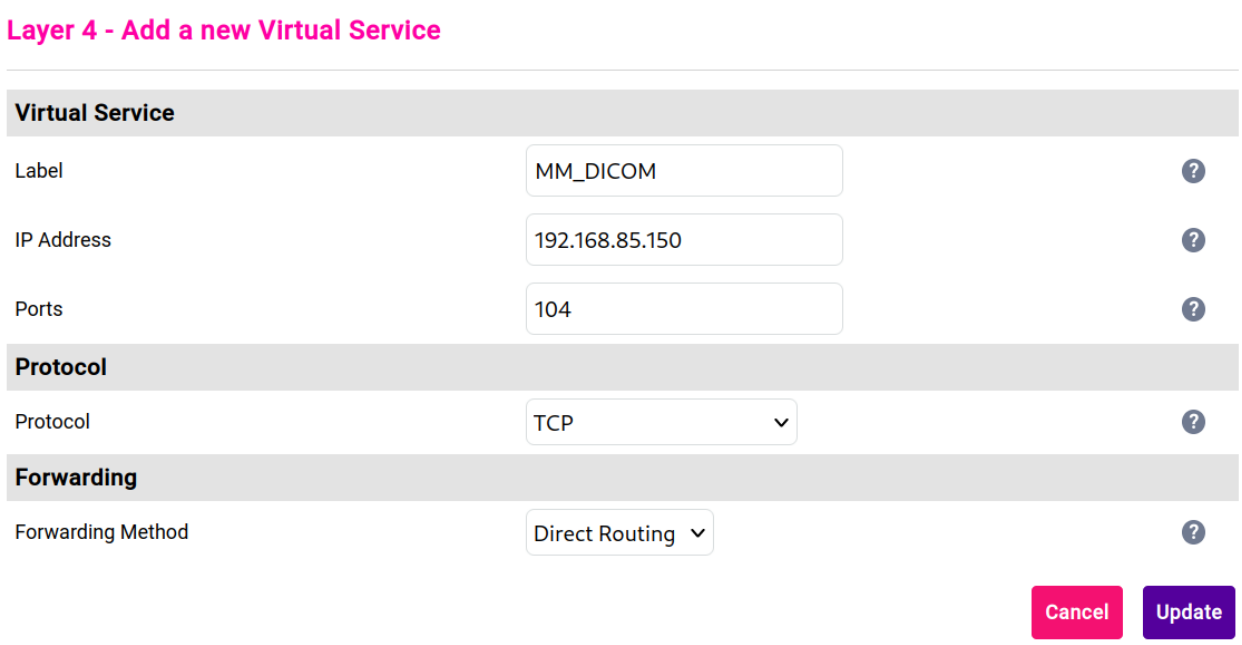
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



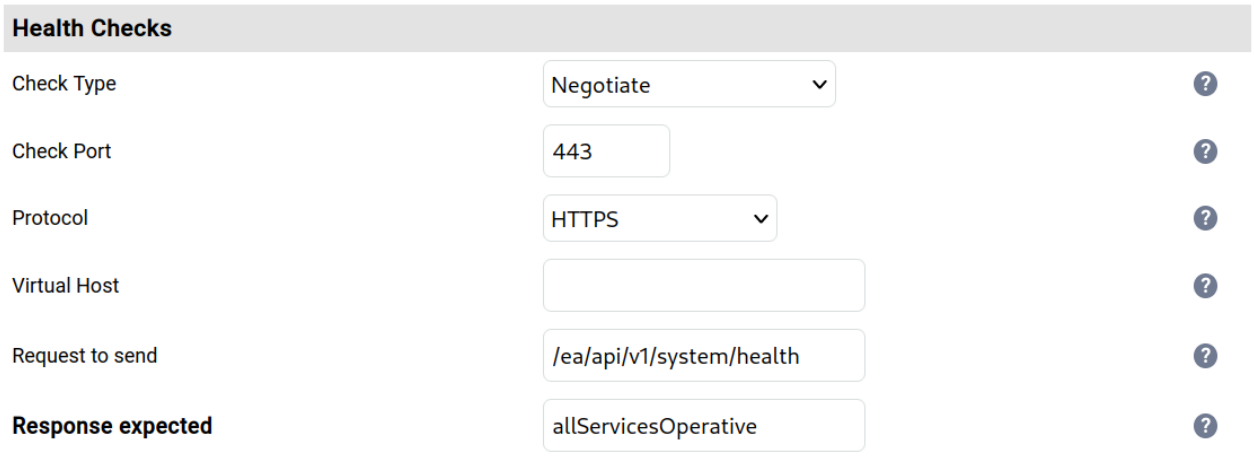
9.8.8. VIP 7 - MM_DICOM

9.8.8.1. 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. **MM_DICOM**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.150**.
4. Set the *Ports* field to **104**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **443**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/ea/api/v1/system/health**
14. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.

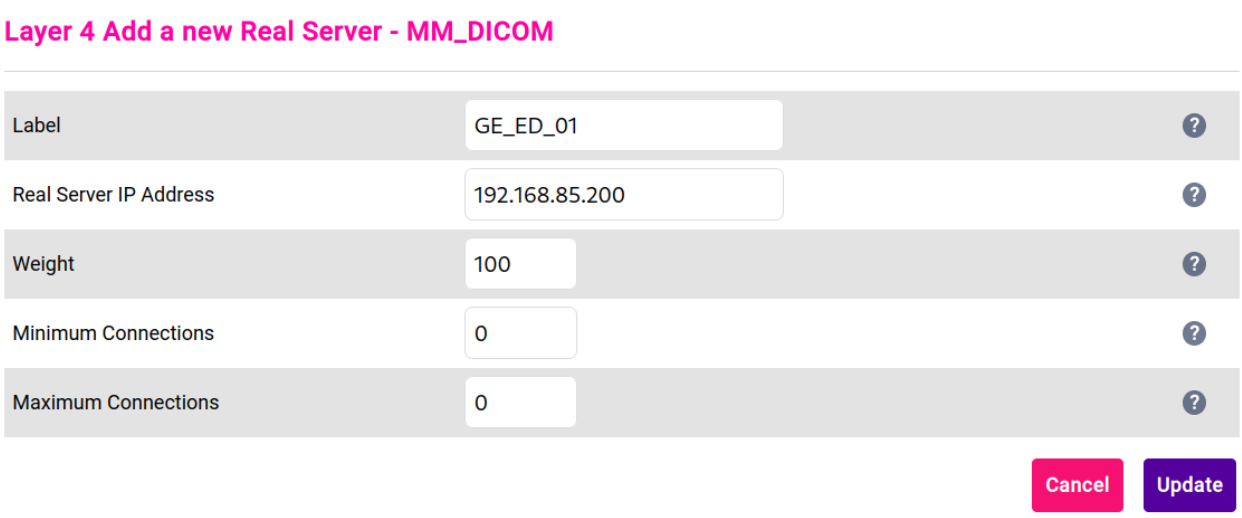


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.8.2. 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.

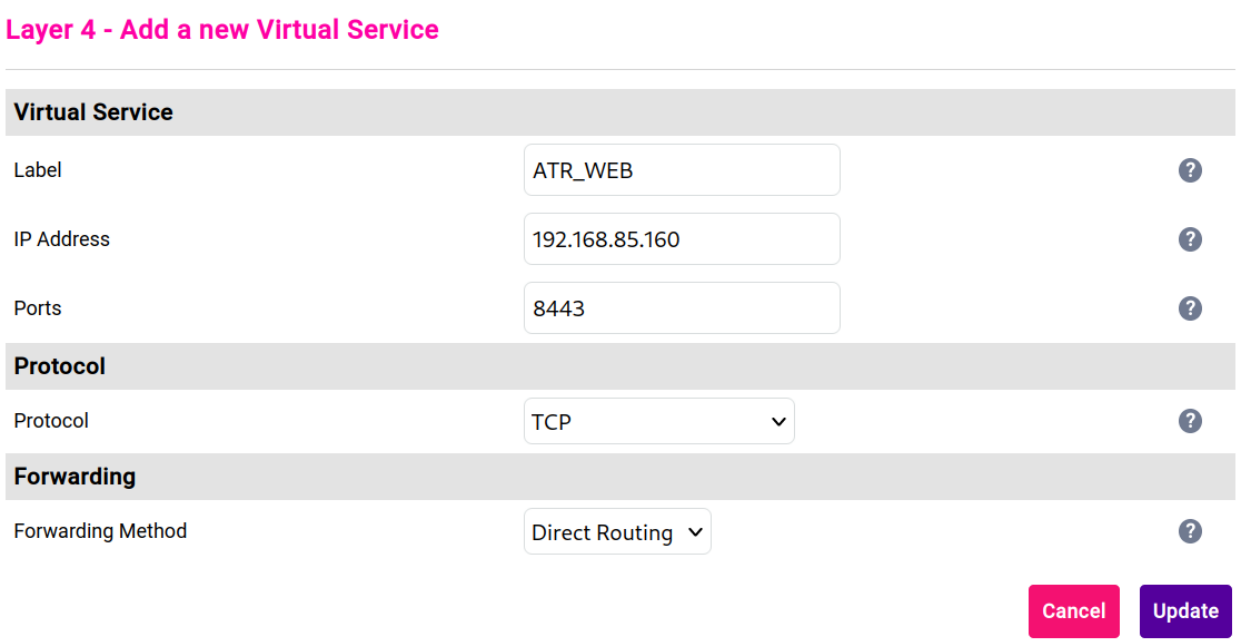
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



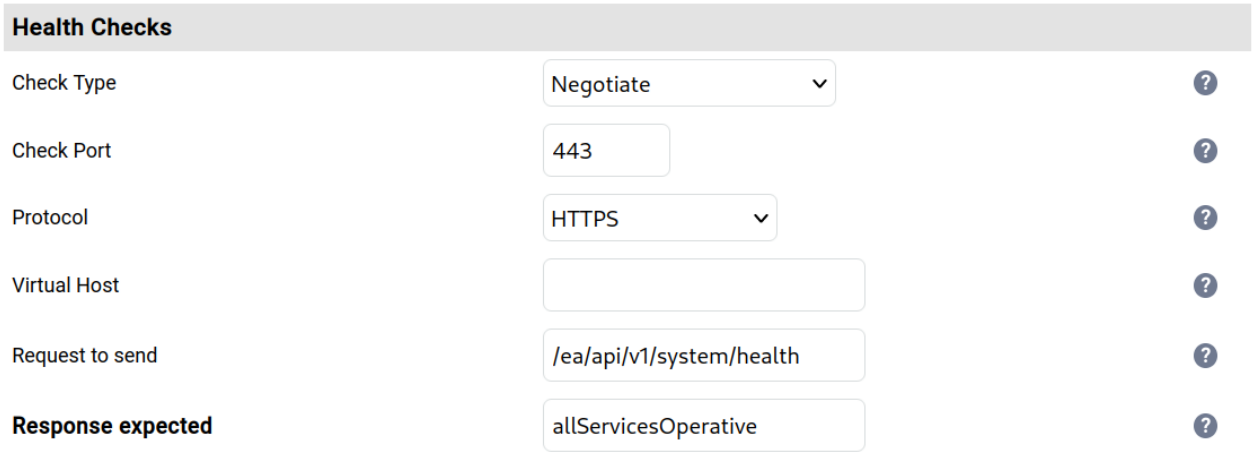
9.8.9. VIP 8 - ATR_WEB

9.8.9.1. 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. **ATR_WEB**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.160**.
4. Set the *Ports* field to **8443**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **443**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/ea/api/v1/system/health**
14. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.

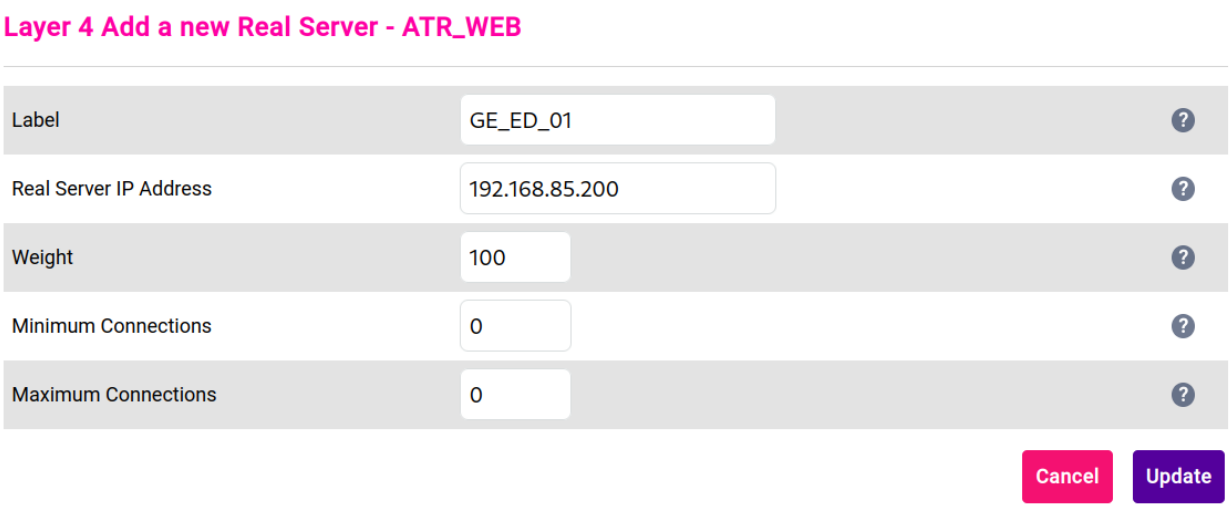


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.9.2. 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.

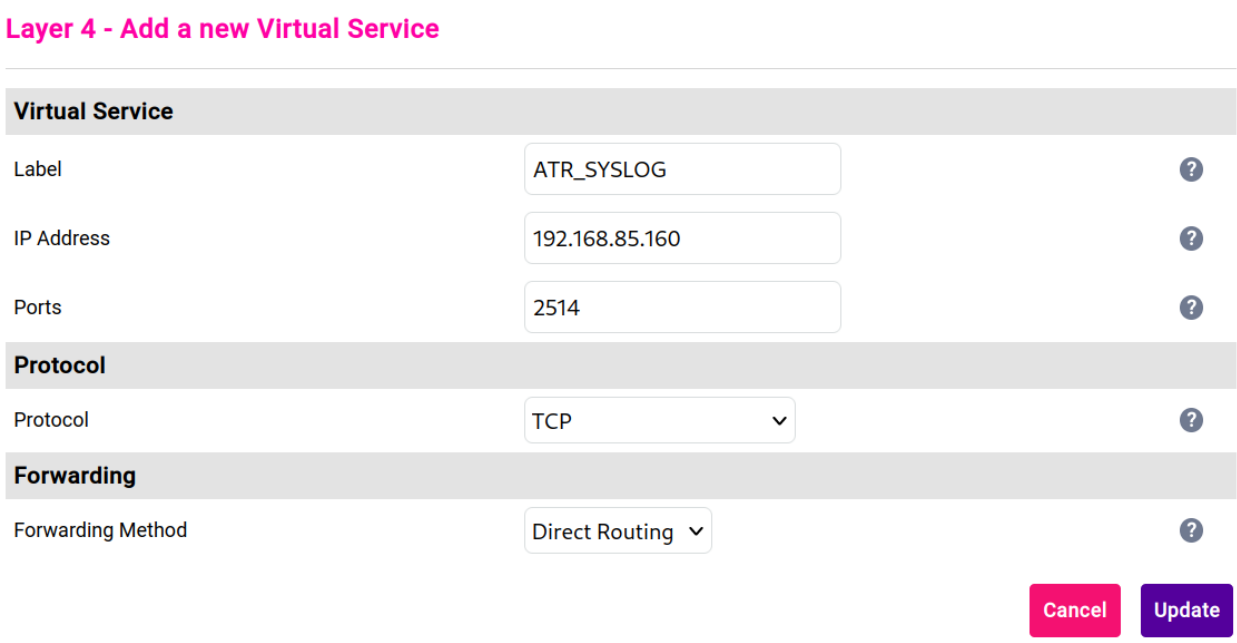
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



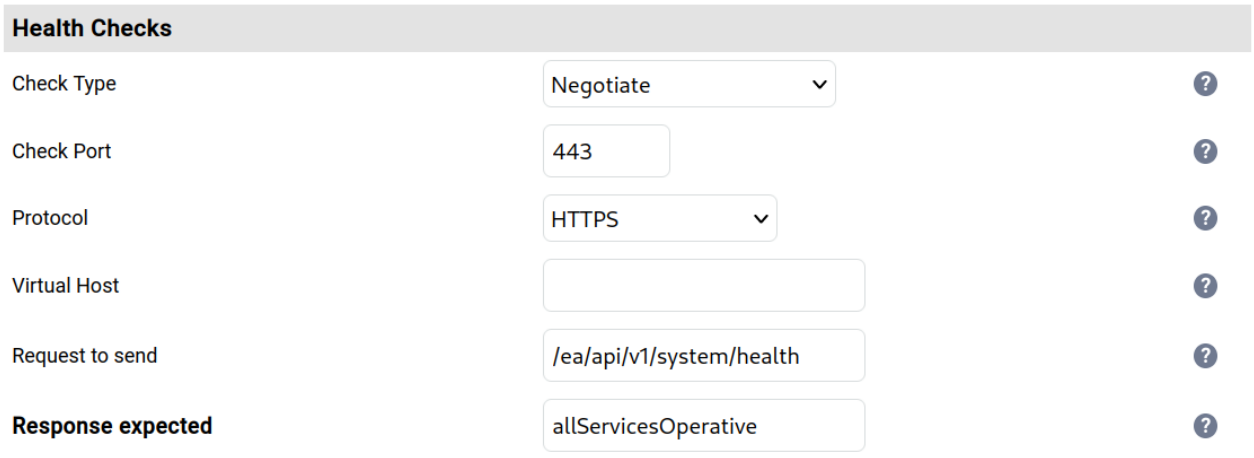
9.8.10. VIP 9 - ATR_SYSLOG

9.8.10.1. 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. **ATR_SYSLOG**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.160**.
4. Set the *Ports* field to **2514**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **443**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/ea/api/v1/system/health**
14. Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.

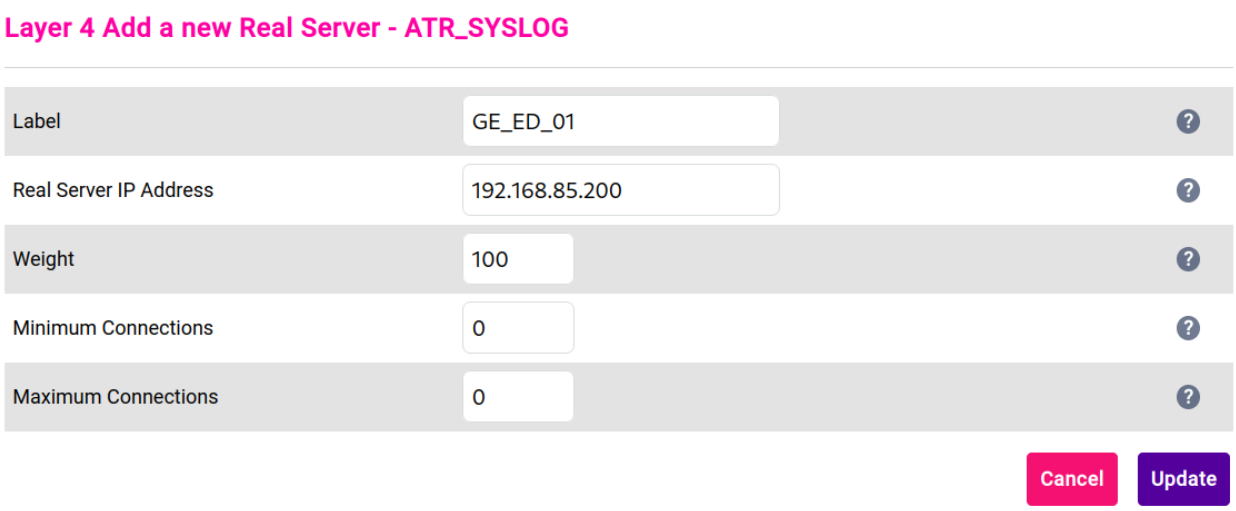


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.10.2. 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.

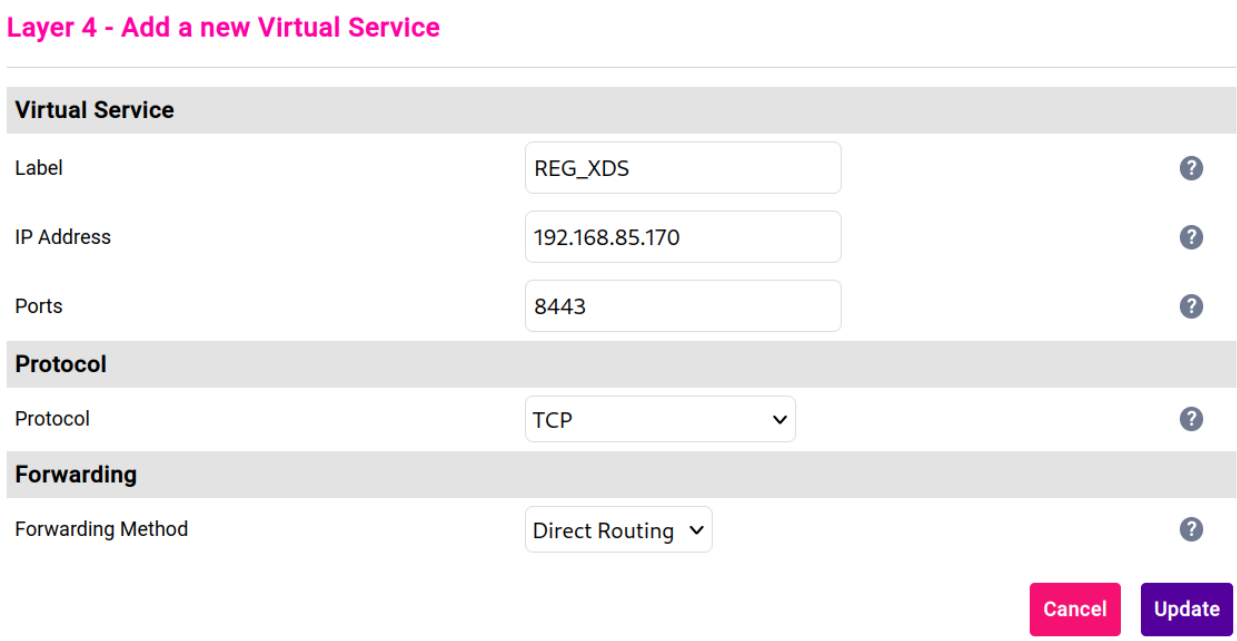
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



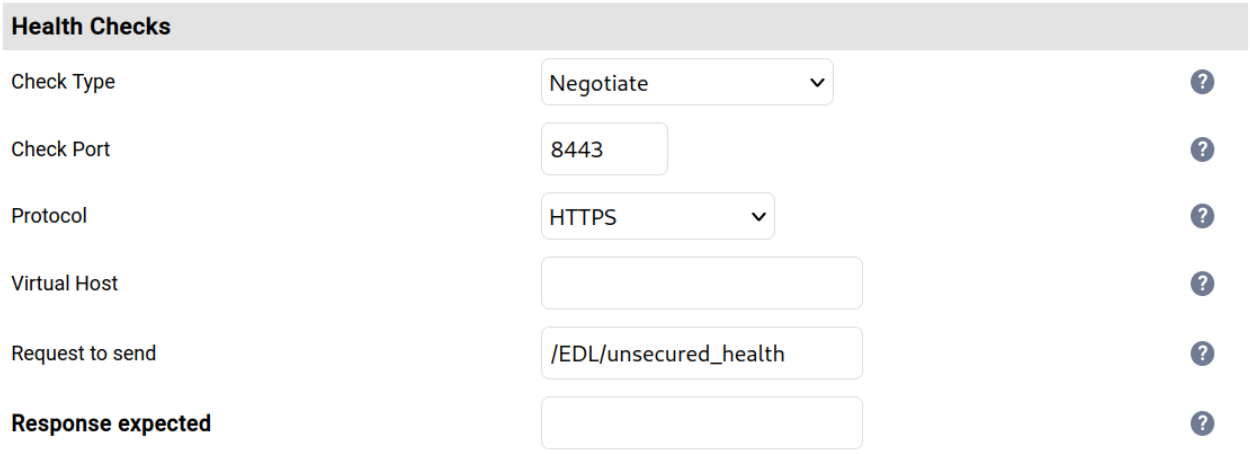
9.8.11. VIP 10 - REG_XDS

9.8.11.1. 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. **REG_XDS**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.170**.
4. Set the *Ports* field to **8443**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **8443**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/EDL/unsecured_health**
14. Ensure that the *Response expected* field is left empty.

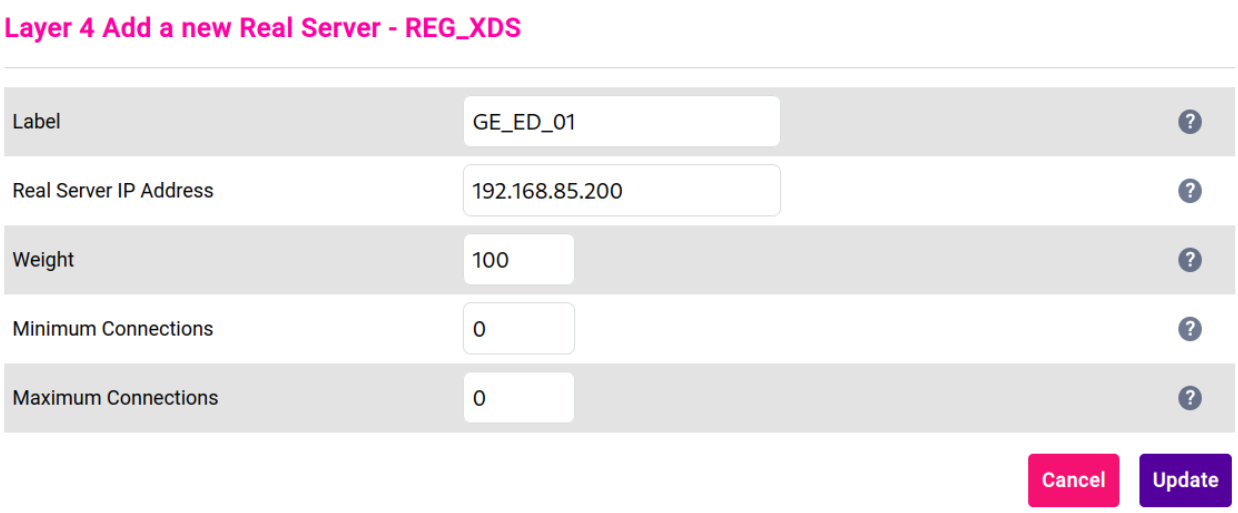


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.11.2. 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.

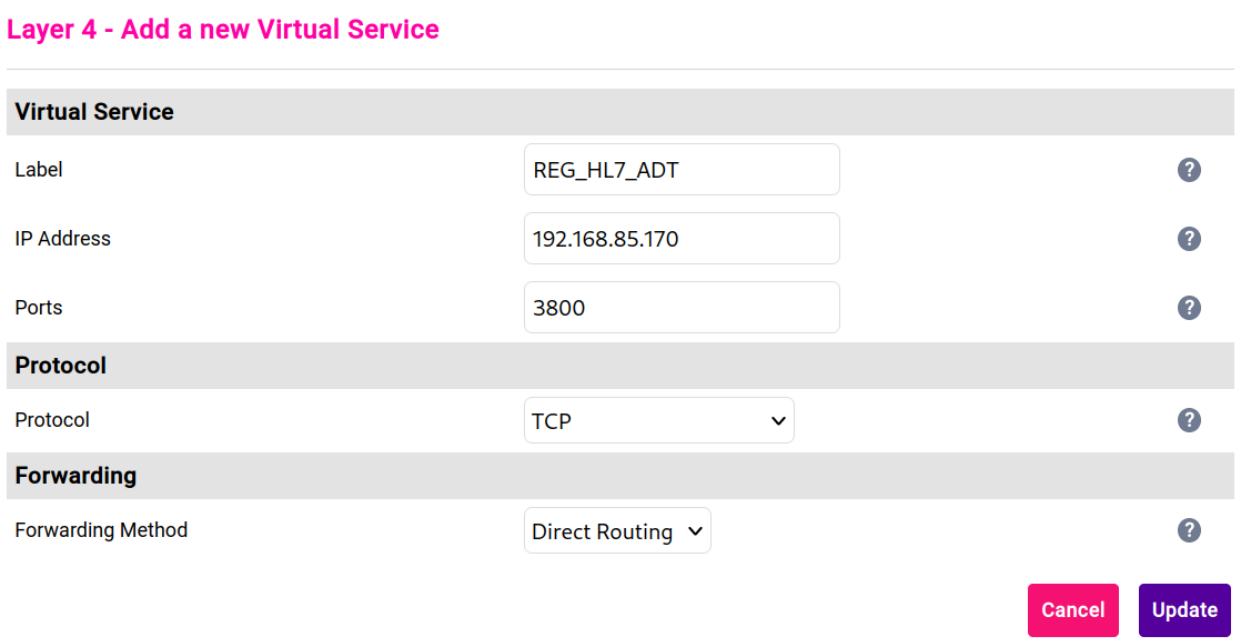
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



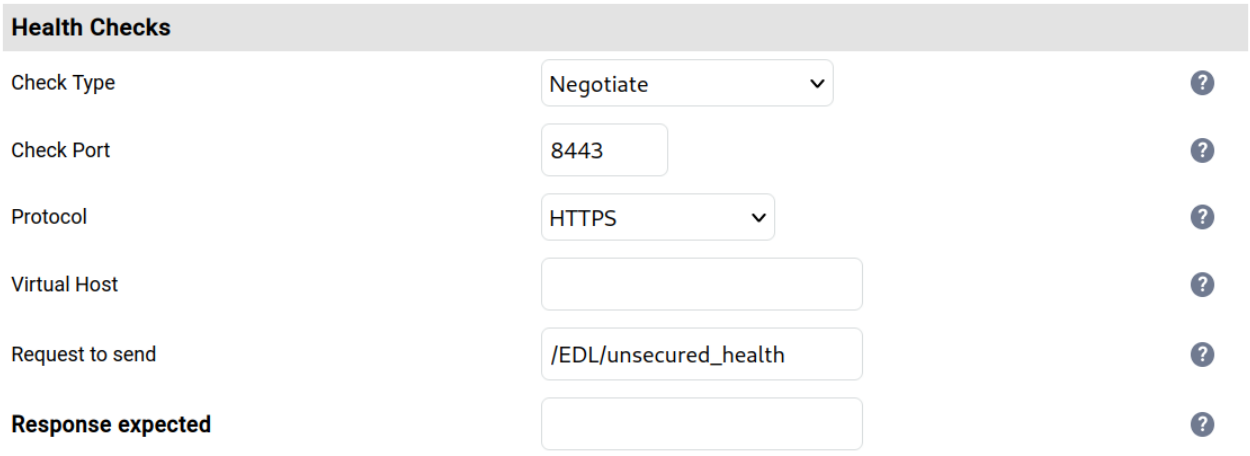
9.8.12. VIP 11 - REG_HL7_ADT

9.8.12.1. 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. **REG_HL7_ADT**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.170**.
4. Set the *Ports* field to **3800**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **8443**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/EDL/unsecured_health**
14. Ensure that the *Response expected* field is left empty.

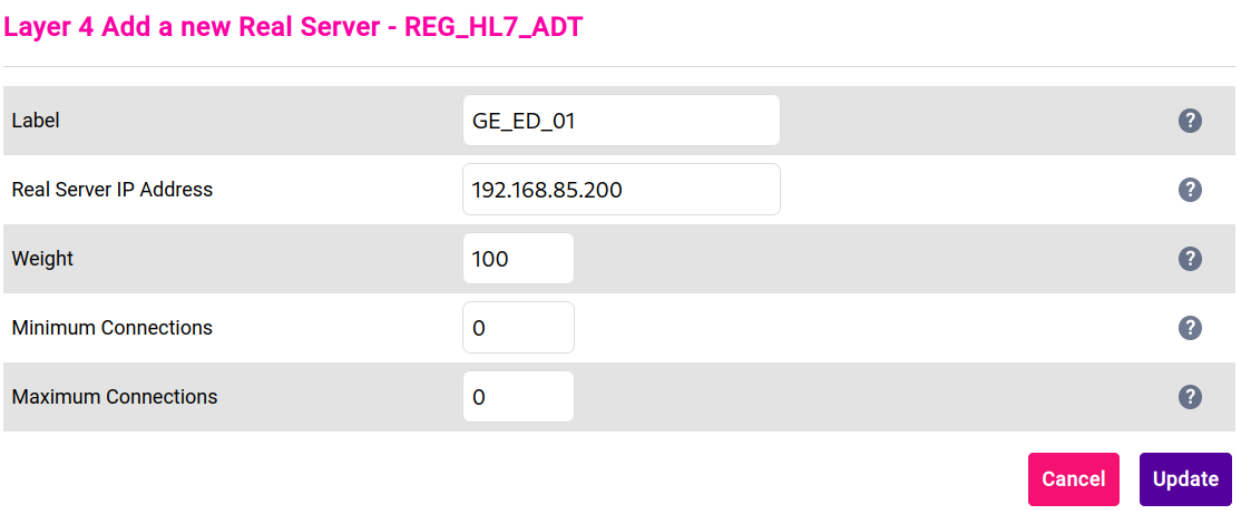


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.12.2. 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.

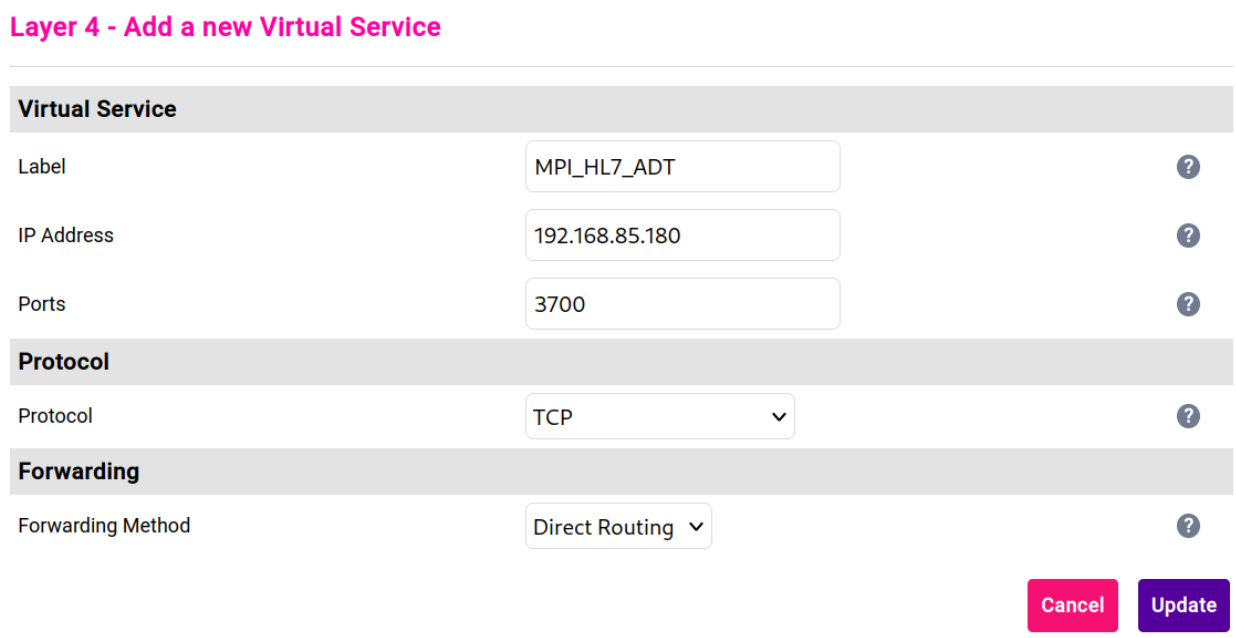
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



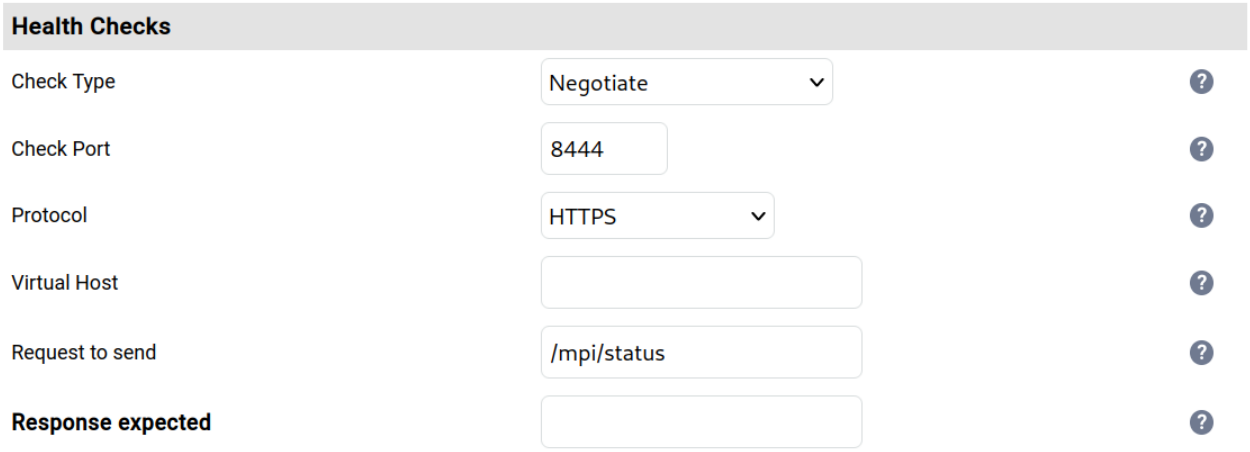
9.8.13. VIP 12 - MPI_HL7_ADT

9.8.13.1. 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. **MPI_HL7_ADT**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.180**.
4. Set the *Ports* field to **3700**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **8444**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/mpi/status**
14. Ensure that the *Response expected* field is left empty.

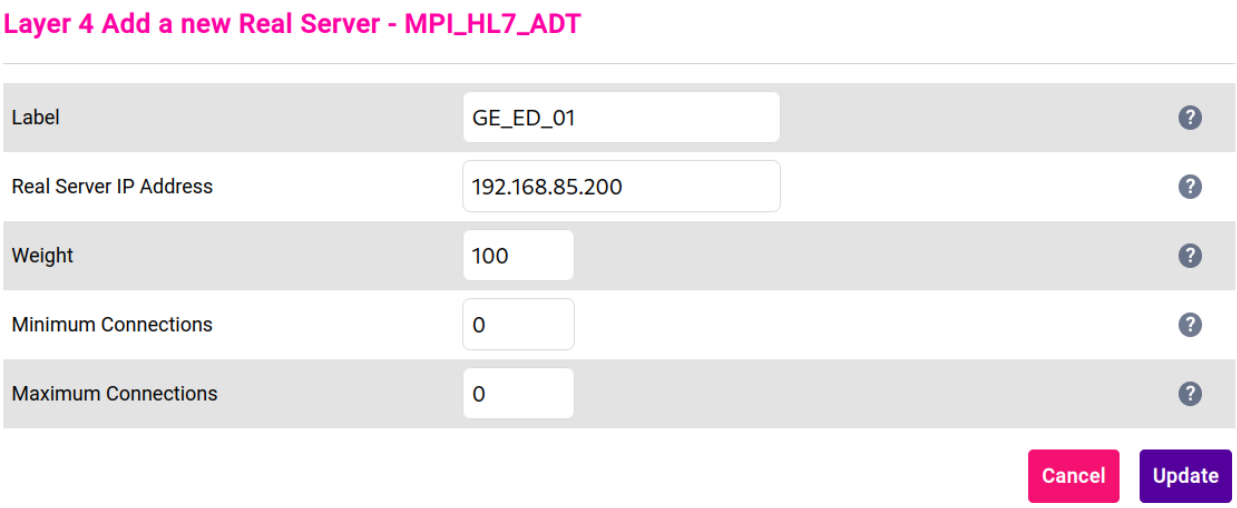


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.13.2. 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.

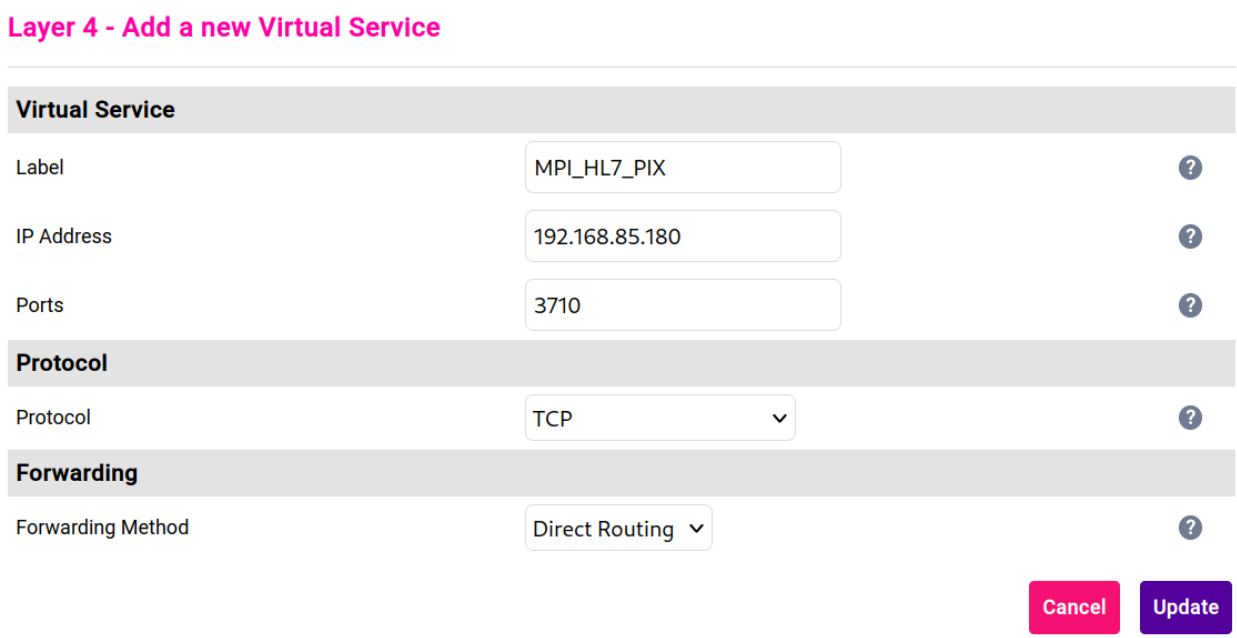
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



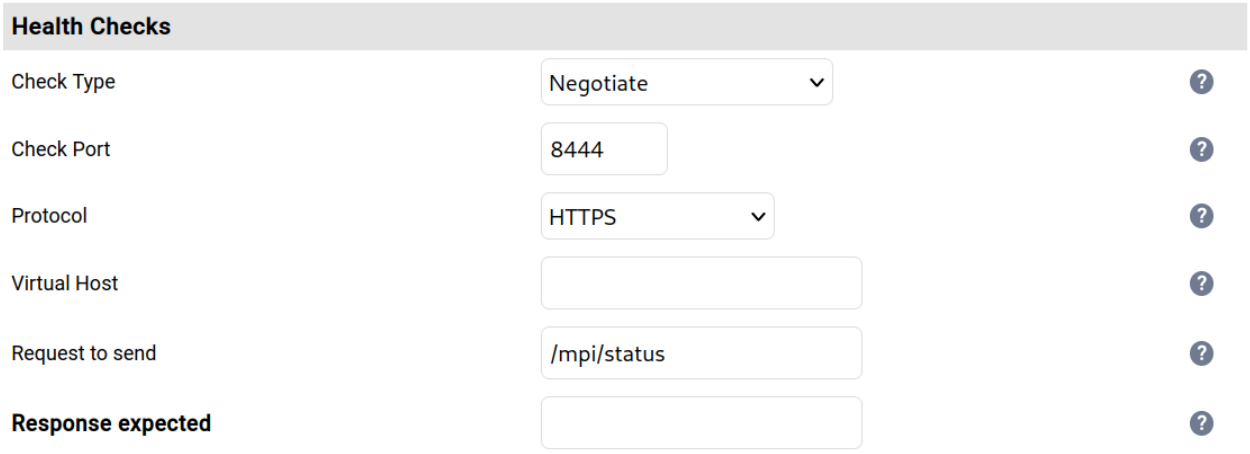
9.8.14. VIP 13 - MPI_HL7_PIX

9.8.14.1. 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. **MPI_HL7_PIX**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.180**.
4. Set the *Ports* field to **3710**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **8444**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/mpi/status**
14. Ensure that the *Response expected* field is left empty.

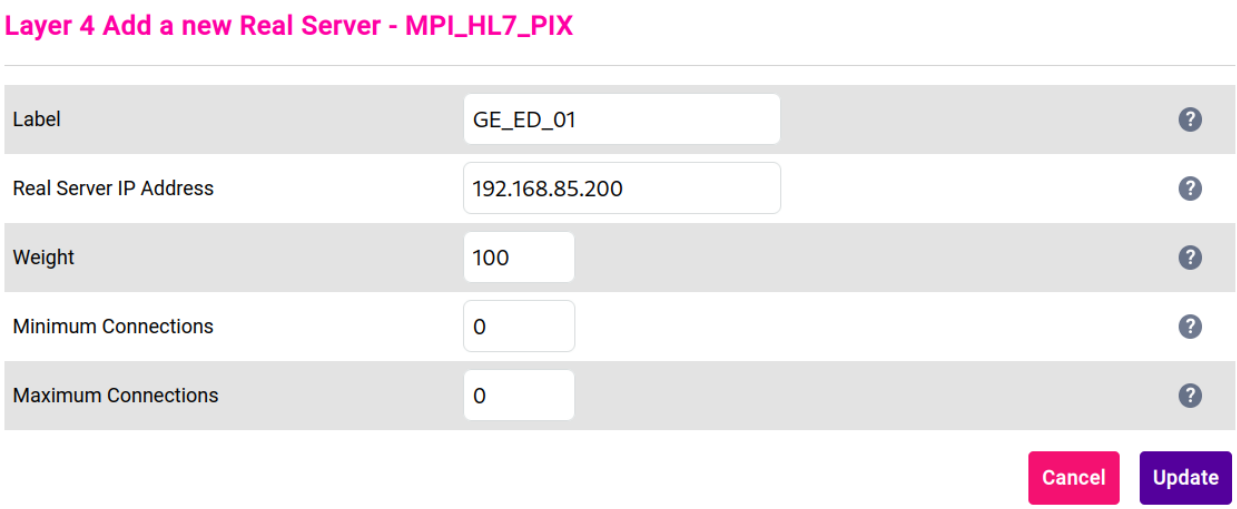


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.14.2. 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.

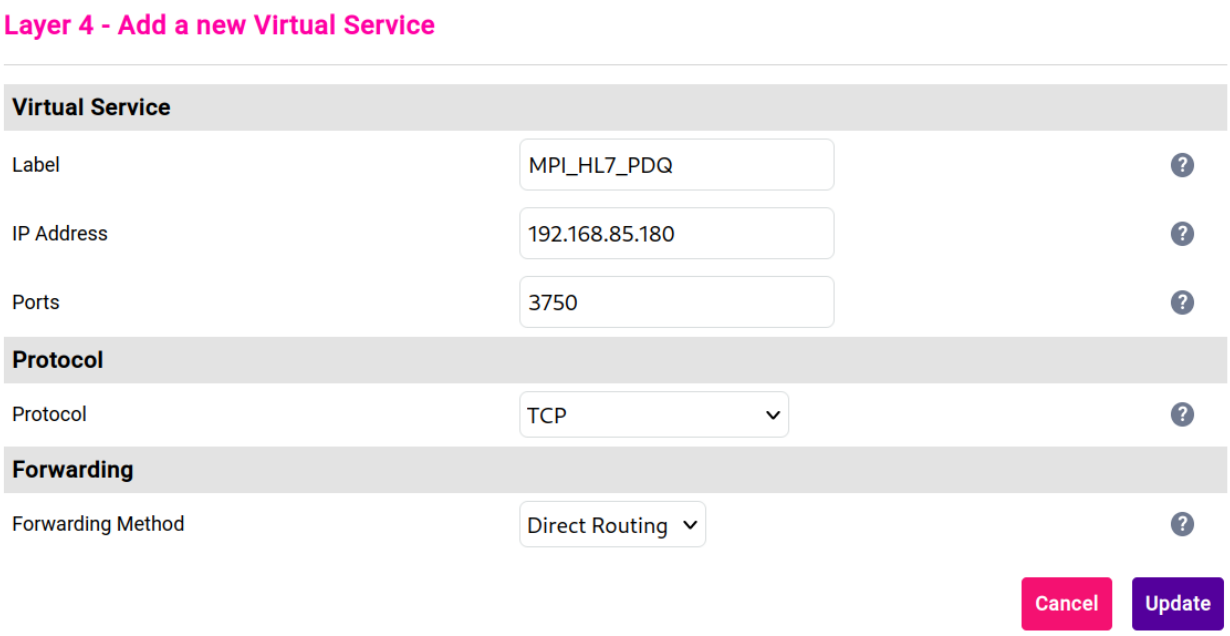
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



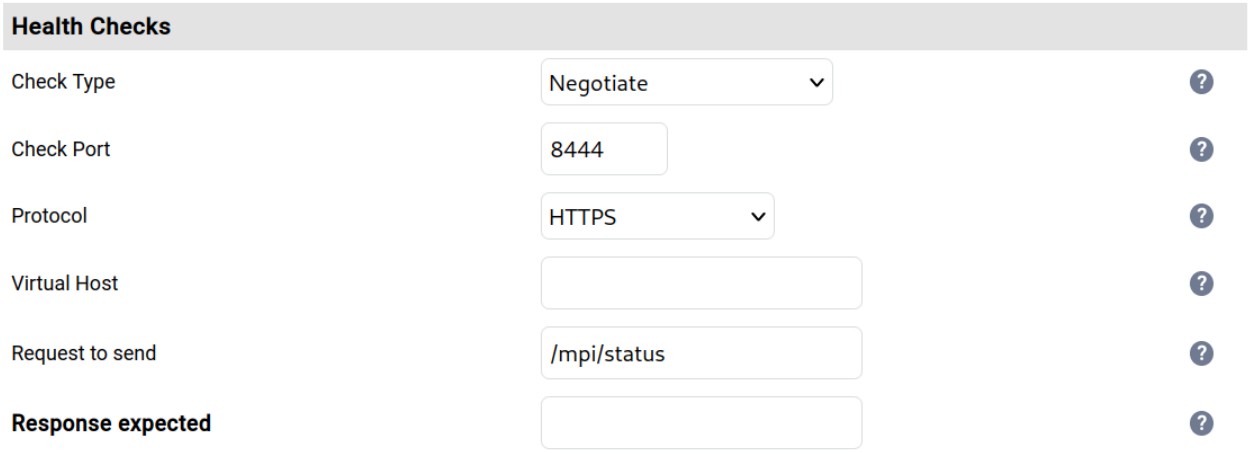
9.8.15. VIP 14 - MPI_HL7_PDQ

9.8.15.1. 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. **MPI_HL7_PDQ**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.180**.
4. Set the *Ports* field to **3750**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **8444**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/mpi/status**
14. Ensure that the *Response expected* field is left empty.

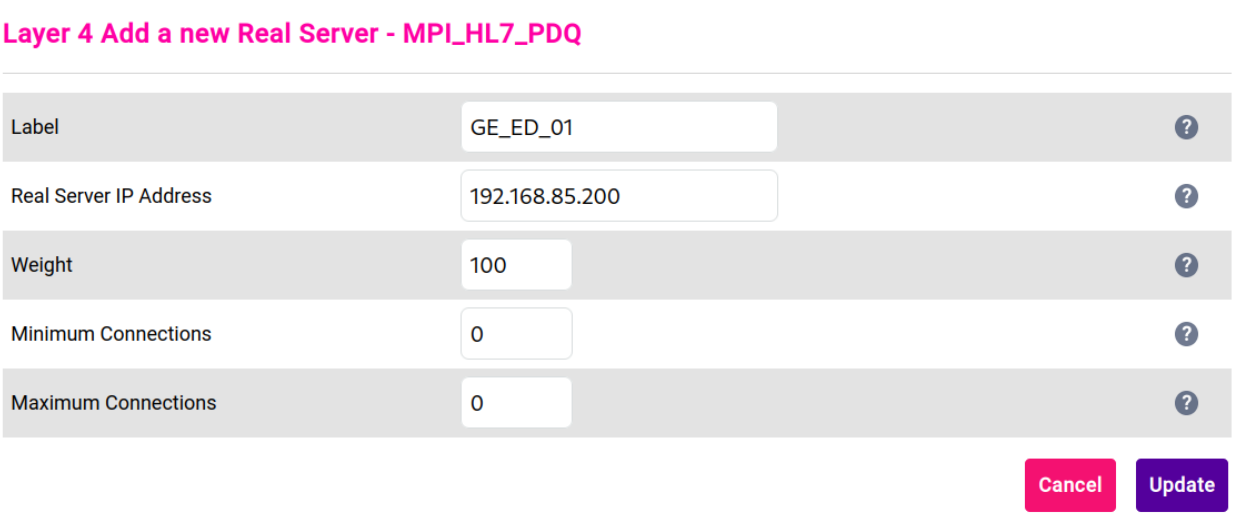


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.15.2. 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.

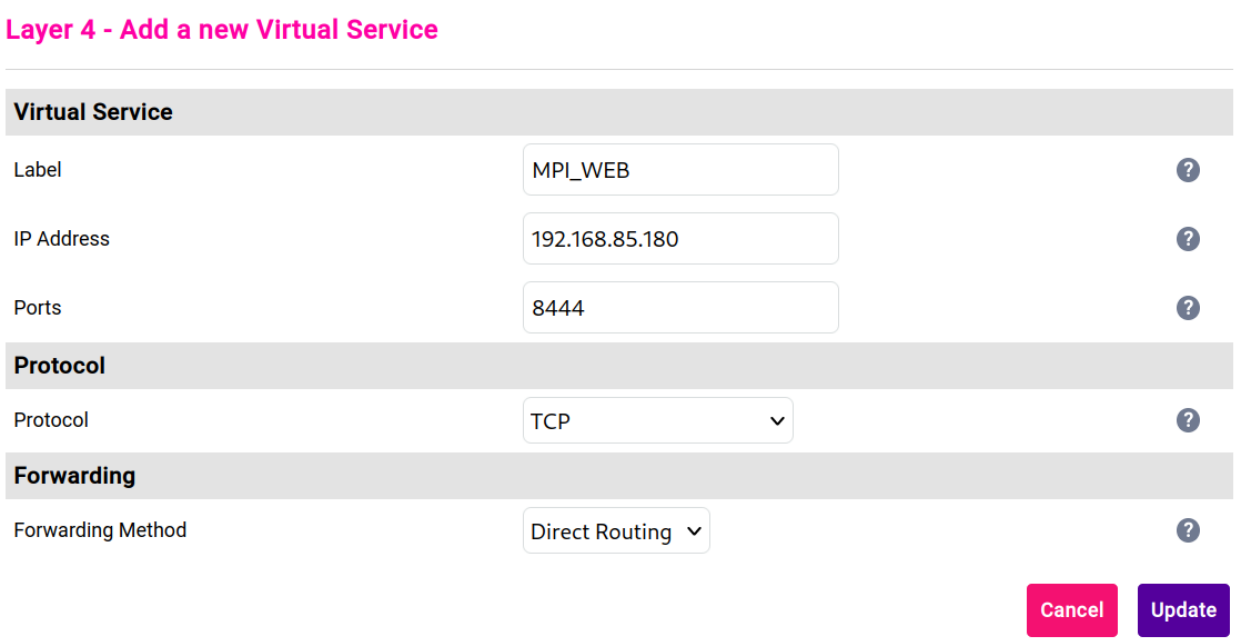
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



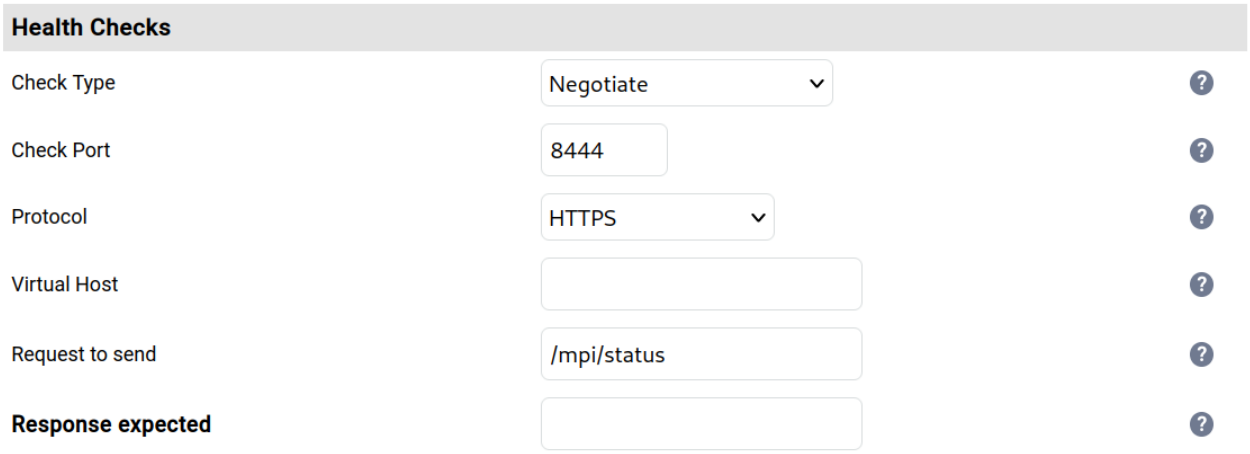
9.8.16. VIP 15 - MPI_WEB

9.8.16.1. 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. **MPI_WEB**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.180**.
4. Set the *Ports* field to **8444**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the Virtual Service.



8. Click **Modify** next to the newly created VIP.
9. Set the *Balance Mode* to **Weighted Round Robin**.
10. Set the *Health Checks Check Type* to **Negotiate**.
11. Set the *Check Port* to **8444**.
12. Set the *Protocol* to **HTTPS**.
13. Set the *Request to send* to **/mpi/status**
14. Ensure that the *Response expected* field is left empty.

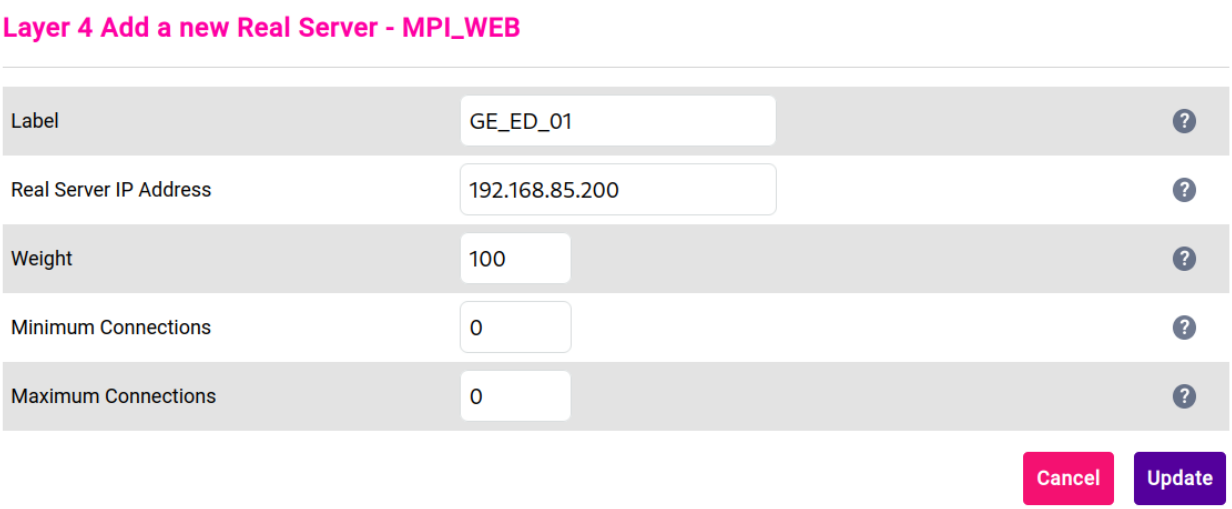


15. Leave all other settings at their default value.
16. Click **Update**.

9.8.16.2. 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.

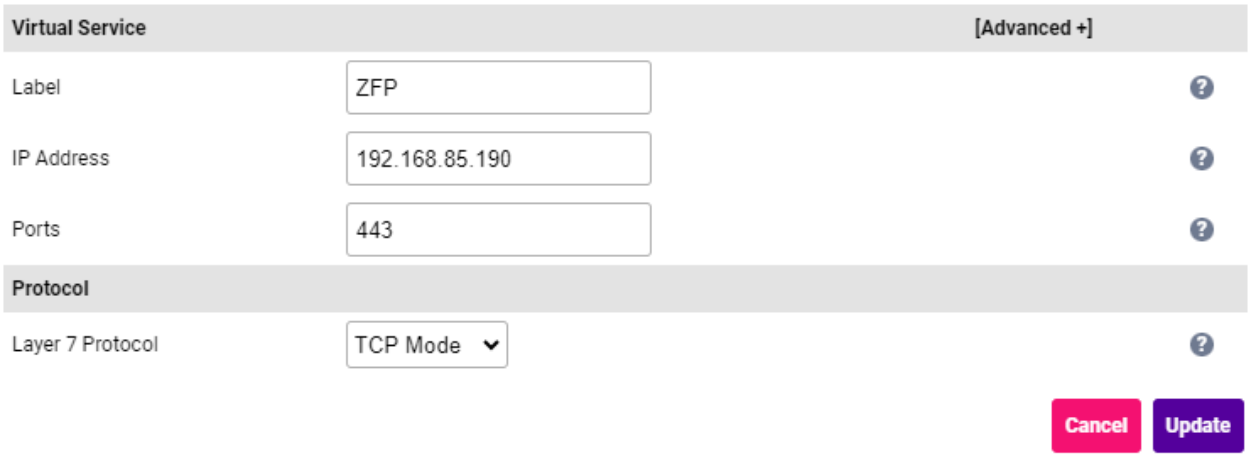
2. Define the *Label* for the Real Server as required, e.g. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Servers as required.



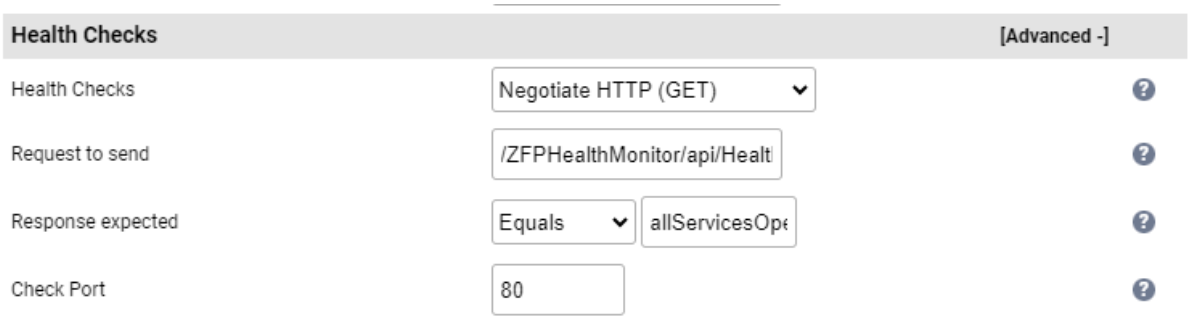
9.8.17. VIP 16 - ZFP

9.8.17.1. Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the Virtual Service as required, e.g. **ZFP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.190**.
4. Set the *Ports* field to **443**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the Virtual Service.



7. Click **Modify** next to the newly created VIP.
8. Set the *Balance Mode* to **Weighted Round Robin**.
9. Scroll to the *Persistence* section and click **[Advanced]**.
    - Set the *Persistence Timeout* to **33**, i.e. 33 minutes.
10. Scroll to the *Health Checks* section and click **[Advanced]**.
    - Set the *Health Checks Check Type* to **Negotiate HTTPS (GET)**.
    - Set *Request to send* to **/ZFPHealthMonitor/api/HealthCheck**.
    - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
    - Set the *Check Port* to **443**.

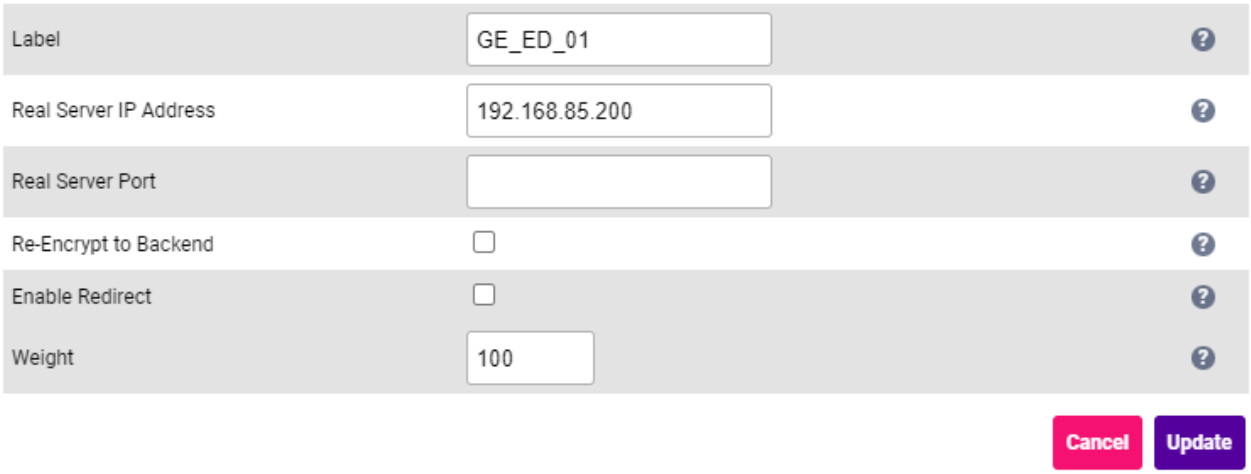


11. Leave all other settings at their default value.
12. Click **Update**.

> **Note** VIP 16 - ZFP also requires the layer 7 health check interval to be changed from 4 to 6 seconds. To change this setting, please refer to Layer 7 Global Settings.

9.8.17.2. Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – 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. **GE_ED_01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Leave the *Real Server Port* field blank.
5. Leave all other settings at their default value.
6. Click **Update**.
7. Repeat these steps to add additional Real Servers as required.



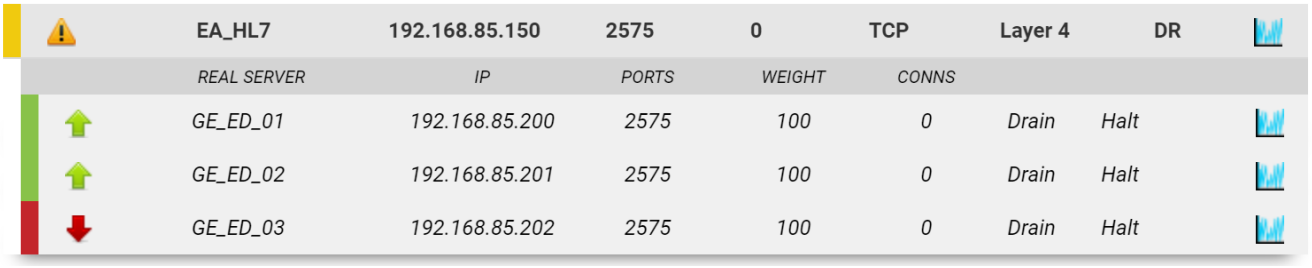
10. Testing & Verification

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

10.1. Using System Overview

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

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:



If the services are up (green) verify that clients can connect to the VIPs and access all services.

> **Note** Make sure that DNS points at the VIP rather than individual servers.

Once you have completed the verification process, continue to the next section and add a Secondary appliance to form the HA (active/passive) clustered pair.

11. 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.

11.1. 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:

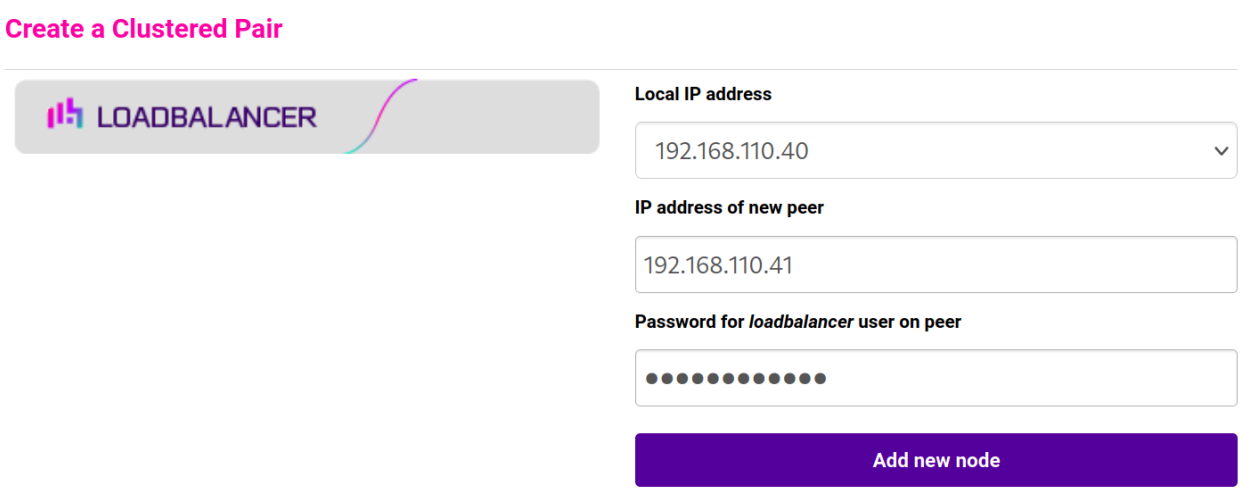
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration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

WebUI Main Menu Option	Sub Menu Option	Description
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

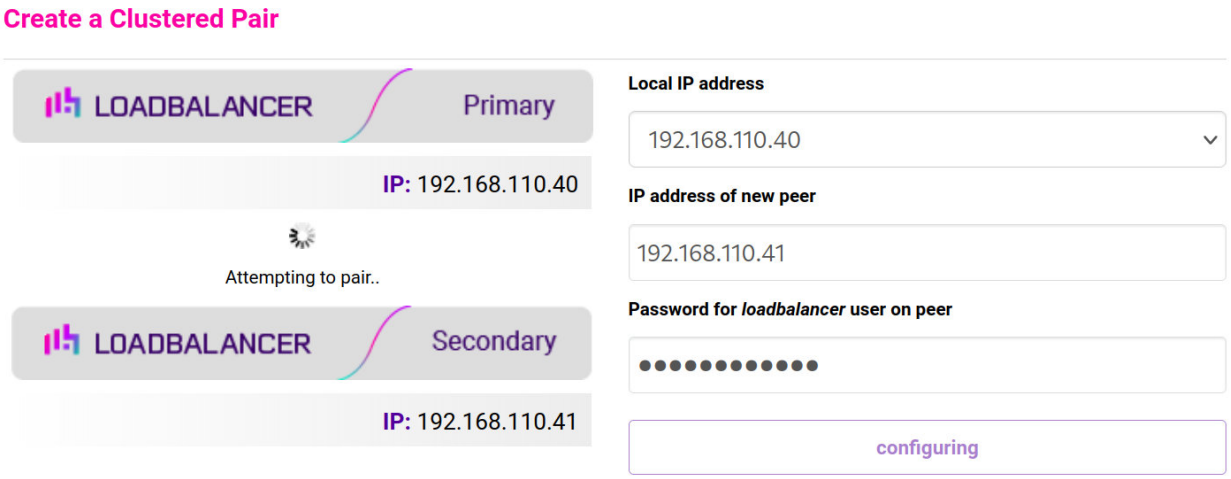
> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

11.2. Configuring the HA Clustered Pair

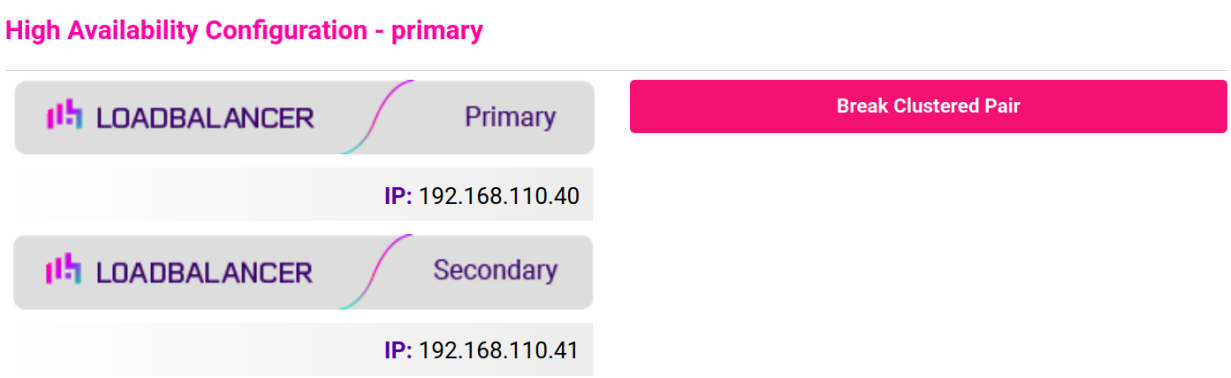
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



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.

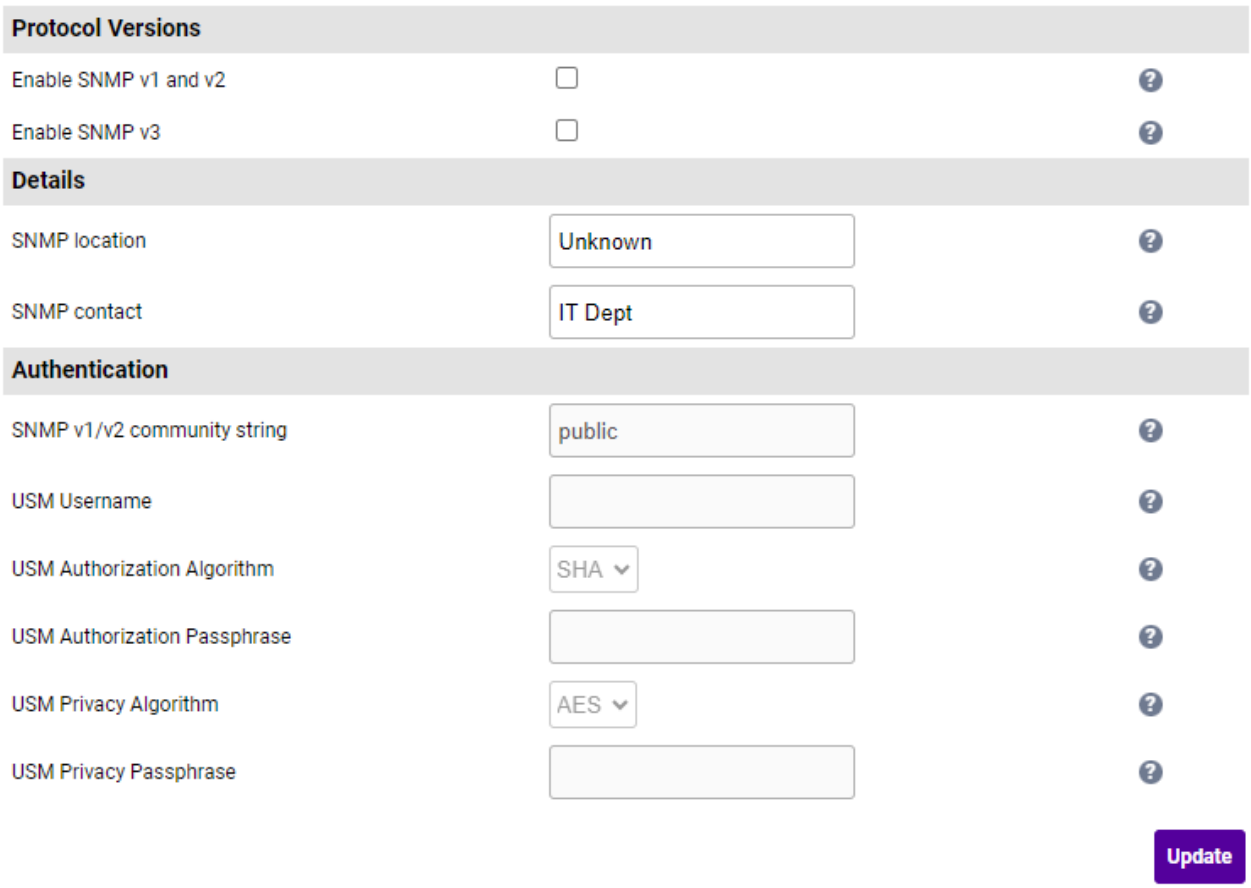
12. Optional Appliance Configuration

12.1. SNMP Configuration

The appliance supports SNMP v1, v2 and v3.

To configure SNMP:

1. Using the WebUI, navigate to: *Local Configuration > SNMP Configuration*.



2. Enable the required SNMP version(s).
3. Enter the required *SNMP location* and *SNMP contact*.
4. For SNMP v1 & v2:
   - Enter the required *SNMP v1/v2 community string*.
5. For SNMP v3:
   - Specify the *USM Username*.
   - Select the required *USM Authorization Algorithm*.
   - Specify the *USM Authorization Passphrase*, it should be at least 8 characters.
   - Select the required *USM Privacy Algorithm*.
   - Specify *USM Privacy Passphrase*, it should be at least 8 characters.
6. Click **Update**.
7. Restart SNMPD using the **Restart SNMPD** button at the top of the screen.

> **Note** Valid characters for the *Community string*, *USM Username*, *USM Authorization Passphrase* and *USM Privacy Passphrase* fields are: **a-z A-Z 0-9 [ ] # ~ _ * ! = - $ % ? { } @ : ; ^**

> **Note** For more information about the various OIDs and associated MIBs supported by the appliance, please refer to SNMP Reporting.

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

12.2. Configuring Email Alerts for Virtual Services

Email alerts can be configured for layer 4 and layer 7 Virtual Services. This enables emails to be sent when one or more of the associated Real Servers fail their health check and also when they subsequently start to pass their health check.

12.2.1. Layer 4

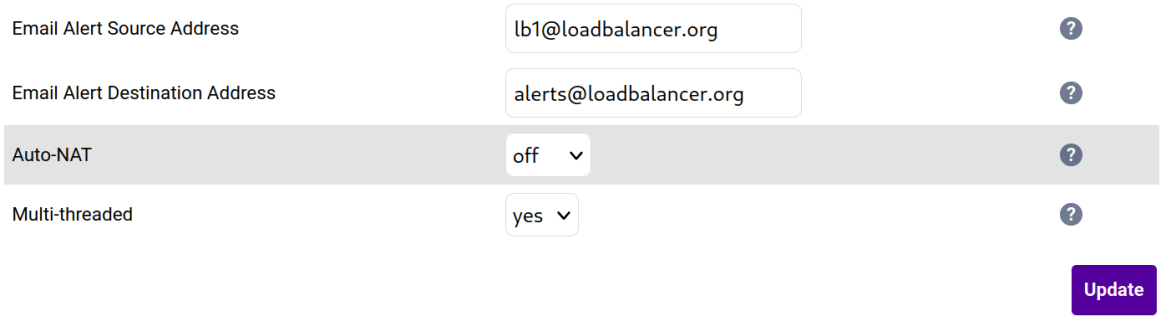
For layer 4 Virtual Services, settings can be configured globally for all VIPs or individually per VIP.

12.2.1.1. Global Layer 4 Email Settings

Once configured, these settings apply to all layer 4 VIPs by default.

To configure global email alert settings for layer 4 services:

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



2. Enter an appropriate email address in the *Email Alert Source Address* field.

```
e.g. lb1@loadbalancer.org
```

3. Enter an appropriate email address in the *Email Alert Destination Address* field.

```
e.g. alerts@loadbalancer.org
```

4. Click **Update**.

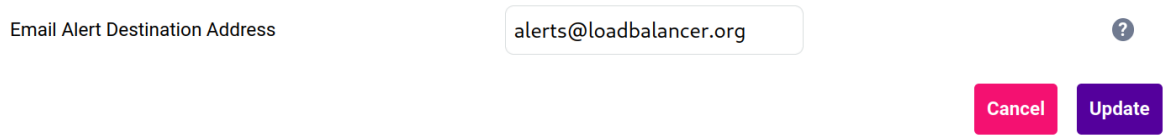
12.2.1.2. VIP Level Settings

> **Note** VIP level settings override the global settings.

Once configured, these settings apply to the individual VIP.

To configure VIP level email alerts:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 Virtual Service* and click **Modify** next to the VIP to be configured.
2. Scroll down to the *Fallback Server* section.



3. Enter an appropriate email address in the *Email Alert Destination Address* field.

```
e.g. alerts@loadbalancer.org
```

4. Click **Update**.

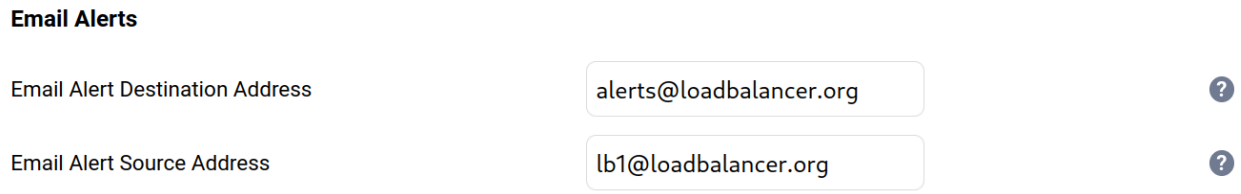
> **Note** You can set the *Email Alert Source Address* field as explained above if required to configure a default source address.

12.3. Configuring Email Alerts for Heartbeat

Email alerts can be setup for heartbeat once a clustered pair has been configured. This enables alerts to be sent when the primary/secondary communication state has changed. This can occur when the secondary appliance takes over from the primary, when the primary takes over from the secondary and also when there is a communication issue between the 2 appliances.

To configure email alert settings for Heartbeat:

1. Using the WebUI, navigate to: *Cluster Configuration > Heartbeat Configuration*.
2. Scroll down to the **Email Alerts** section.



3. Enter an appropriate email address in the *Email Alert Destination Address* field.
4. Enter an appropriate email address in the *Email Alert Source Address* field.
5. Click **Modify Heartbeat Configuration**.

12.4. Configuring a Smart Host (SMTP relay)

For Heartbeat (and layer 4 services), email alerts are sent from the load balancer directly to the mail server defined in the destination domain's DNS MX record by default. Alternatively, a custom smart host (mail relay server) can be specified. A smart host is an email server through which approved devices can send emails. Where possible, we recommend that you use a smart host for email alerts as this often helps improve the deliverability of emails.

To configure a Smart Host:

1. Using the WebUI, navigate to: *Local Configuration > Physical - Advanced Configuration*.
2. Scroll down to the *SMTP Relay* section.
3. Specify the FQDN or IP address of the *Smart Host*.
4. Click **Update**.

> **Note** By default the *Smart Host* is set as the destination email domain's DNS MX record when the *Email Alert Destination Address* is configured. It must either be left at its default setting or a custom smart host must be configured to enable email alerts to be sent.

13. Technical Support

If you require any assistance please contact support@loadbalancer.org.

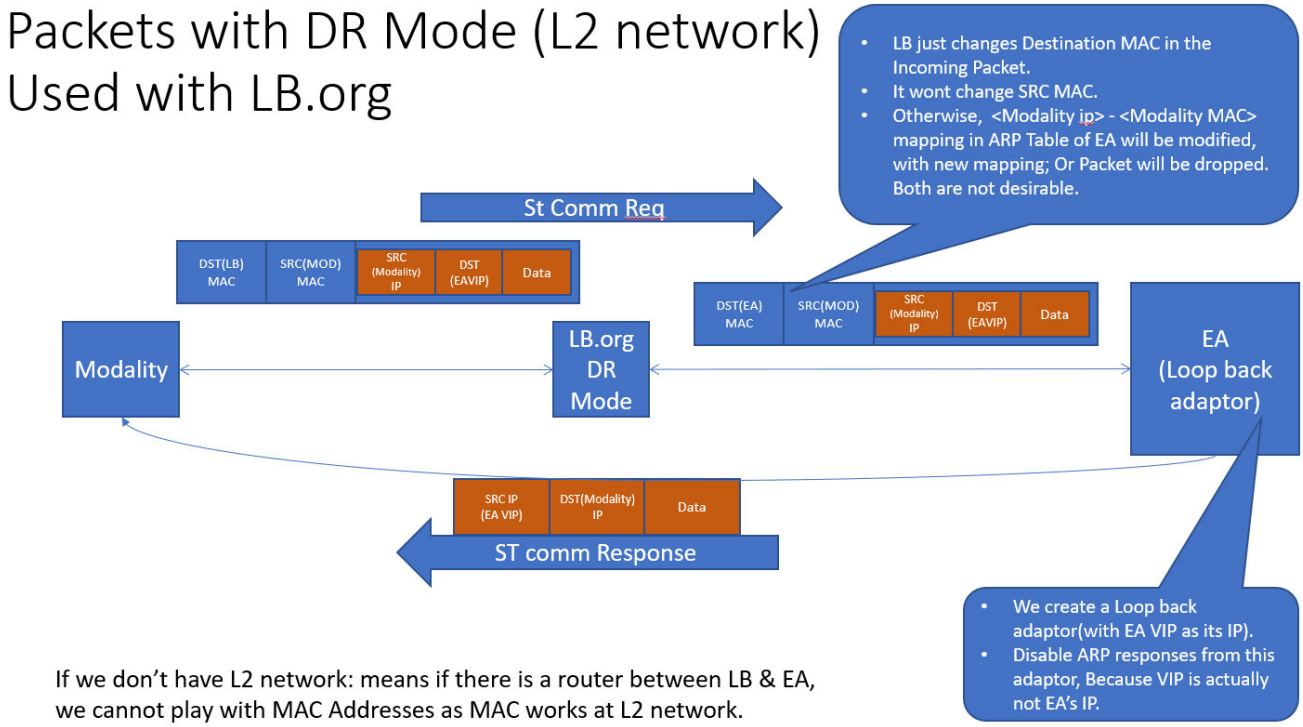
14. Further Documentation

For additional information, please refer to the Administration Manual.

15. Appendix

15.1. DR Mode Packet Manipulation

The following diagram shows the traffic flow between the load balancer, the load balanced backend servers and the Modality and how the destination MAC address is modified.



16. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0	18 July 2024	Initial version		RJC
1.1	11 September 2024	Added new section "Layer 7 Global Settings" to enable the health check interval to be changed from 4 to 6 seconds	Required by VIP 16 - ZFP	RJC
1.2	25 March 2025	Updated the "Virtual Hardware Resource Requirements" section to list the GE HealthCare virtual appliances that are available and the resource requirements for each Removed the Configuration screen step from the "Installing the Appliance using vSphere Client" section since this does not apply to GE HealthCare VAs	Technical accuracy	RJC
1.3	8 April 2025	Updated VIPs to ensure that all have the Balance Mode set to Weighted Round Robin	Technical requirement	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.