LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Philips IntelliSpace PACS

Version 1.3.0

Table of Contents

1. About this Guide

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

Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.3.8 and later

> **Note** The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If using an older software version, note that the screenshots presented here may not match the WebUI exactly.

3.2. Philips IntelliSpace PACS

- All versions

4. Philips IntelliSpace PACS

Philips IntelliSpace PACS is an enterprise medical imaging solution and workflow. It gives clinicians rapid access to the images needed throughout the whole patient care cycle. It is based on open standards, allowing for interoperability with other systems.

The system processes and presents patient data in an intelligent way, combining data from multiple sources into a single comprehensive view for analysis. It is designed to be secure and to respect patient confidentiality through the appropriate handling of data.

5. Load Balancing Philips IntelliSpace PACS

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

5.1. Persistence (aka Server Affinity)

Source IP address persistence is used for every virtual service involved in load balancing Philips IntelliSpace PACS. This ensures that a client connects to the same back end real server for their entire session.

5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Philips IntelliSpace PACS, the following VIPs are required:

- DICOM
- DICOM Secure
- DMWL
- DMWL Secure
- SQL
- LDAP
- LDAP Secure
- QRSCP
- QRSCP Secure

5.3. Port Requirements

The following table shows the ports that are load balanced:

Port	Protocols	Use
104	TCP/DICOM	DICOM traffic
2762	TCP/TLS/DICOM	DICOM traffic over TLS, "DICOM secure"
8104	TCP/DICOM	DMWL traffic (DICOM Modality Worklists) traffic
10104	TCP/TLS/DICOM	DMWL traffic over TLS, "DMWL secure"
1433	TCP/SQL	MS SQL service
3890	TCP/LDAP	LDAP service
6360	TCP/LDAPS	Secure LDAP service
107	TCP/DICOM	QRSCP service (Query/Retrieve Service Class Provider)
2765	TCP/TLS/DICOM	QRSCP service over TLS, "QRSCP secure"

5.4. Health Checks

Load balancing a Philips IntelliSpace deployment requires using three different health checks.

Most virtual services use the default ***Connect to port*** health check. The exceptions are the DMWL and QRSCP virtual services, which use ping based checks, and the SQL virtual service, which uses a proprietary MS SQL health check.

The Microsoft SQL health check requires the Microsoft ODBC Driver. Because it is not free and open source software, this driver cannot be redistributed with our load balancer.

We have a blog post on our website which walks through how to set up and use this health check. This blog post is available here: https://www.loadbalancer.org/blog/ms-sql-health-check/

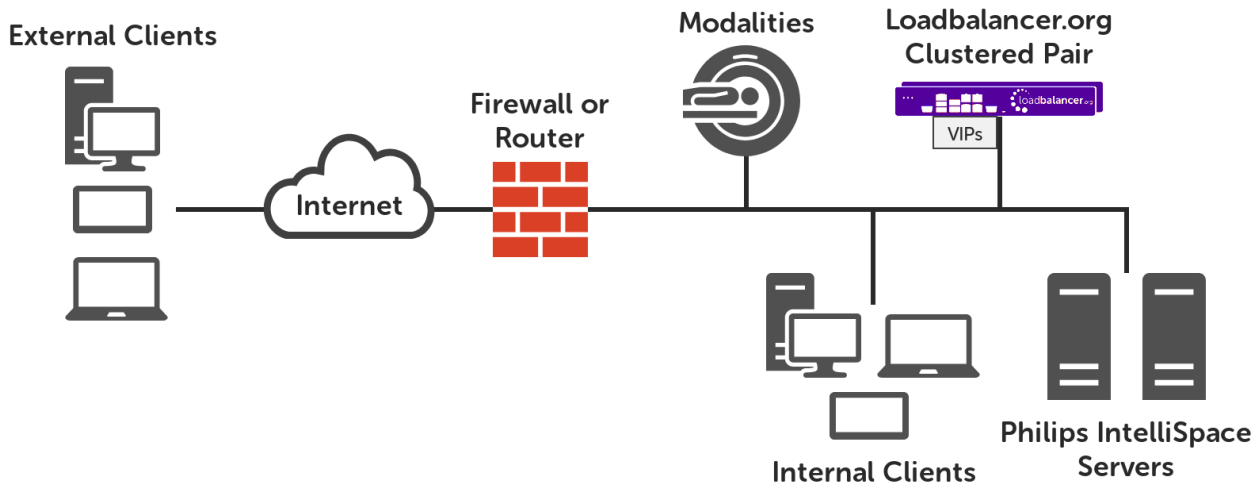
5.5. Specifying Traffic Source Address / SNAT Options

This guide contains references to using the *Set Source Address* option. This option may be required to successfully implement load balancing in a Philips IntelliSpace deployment.

For a given virtual service, the *Set Source Address* option makes outgoing traffic leave the load balancer from a specified IP address that it owns. When using a pair of load balancers, an IP address specified in this way should be a floating IP address so that it can 'float' between and function correctly on either appliance when active . Such an address can be defined through the WebUI under *Cluster Configuration > Floating IPs*.

Using the *Set Source Address* option is useful when the back end real servers that the load balancer is querying require incoming traffic to originate from a specific, possibly trusted or whitelisted, IP address.

6. Deployment Concept



VIPs = **V**irtual **IP** Addresses

> **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 Configuring HA - Adding a Secondary Appliance for more details on configuring a clustered pair.

7. Loadbalancer.org Appliance – the Basics

7.1. 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.

7.2. Initial Network Configuration

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

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

7.3. 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.

> **Note** A number of compatibility issues have been found with various versions of Microsoft Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

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

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

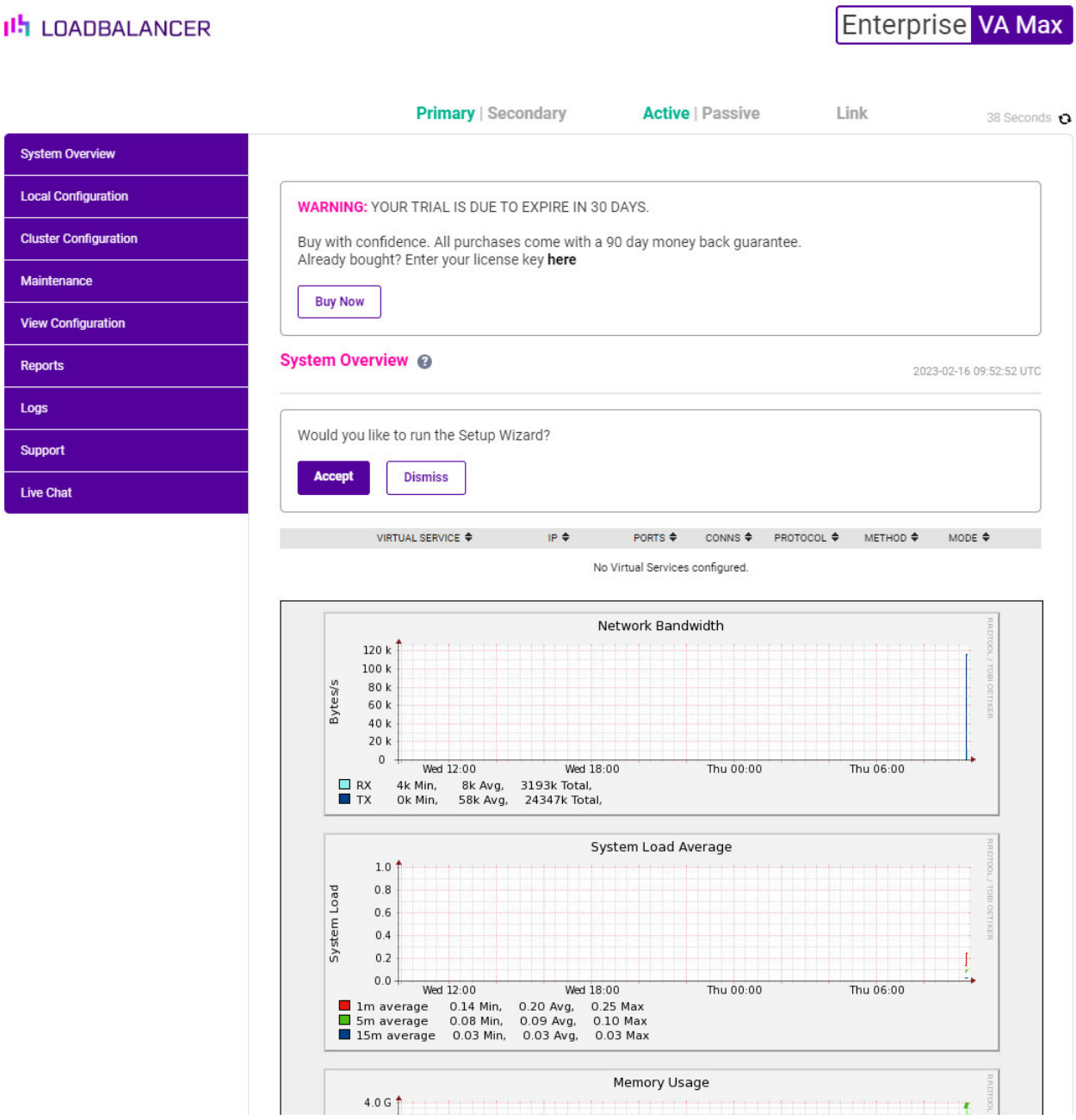
   > **Note** You'll receive a warning about the WebUI's certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

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.

Main Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs

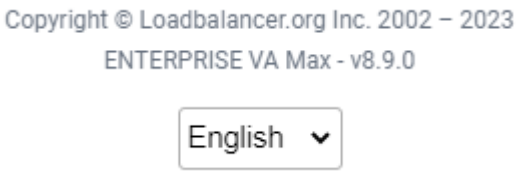
Maintenance - Perform maintenance tasks such as service restarts and taking backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links
Live Chat - Start a live chat session with one of our Support Engineers

7.4. Appliance Software Update

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

Determining the Current Software Version

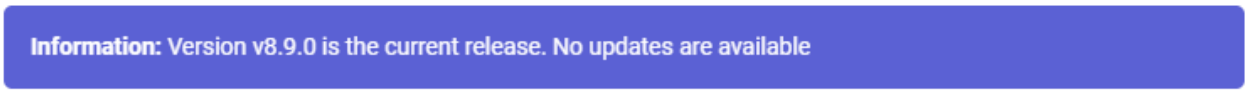
The software version is displayed at the bottom of the WebUI as shown in the example below:



Checking for Updates using Online Update

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

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



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

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

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

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

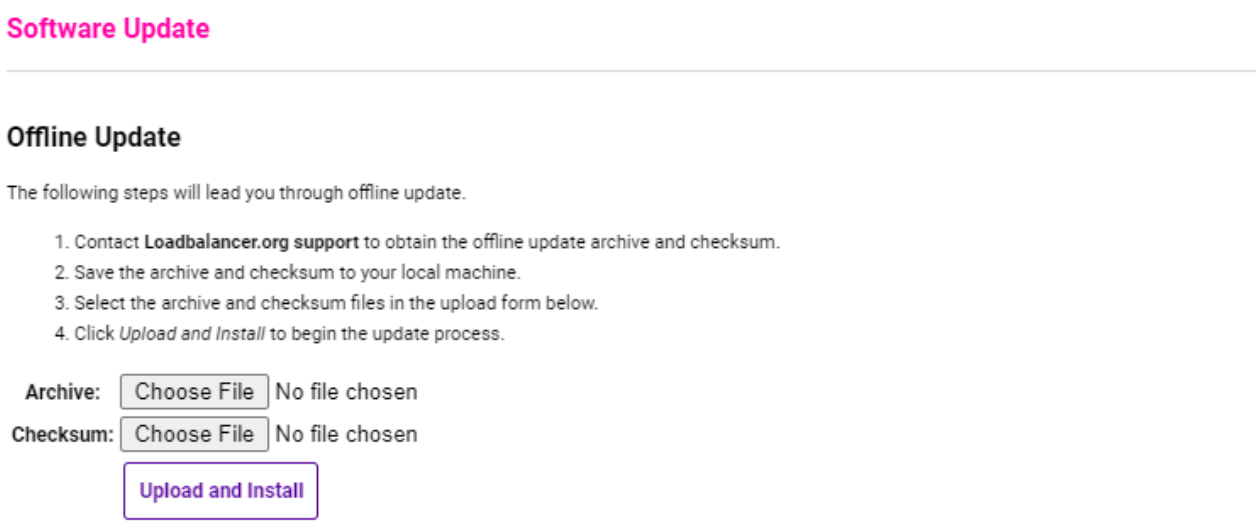
Using Offline Update

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

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

To perform an offline update:

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



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

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
TCP & UDP	123	NTP
TCP & UDP	161	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode

Protocol	Port	Purpose
TCP	7778	HAProxy persistence table replication
TCP	9080	WebUI - HTTP (disabled by default)
TCP	9081	Nginx fallback page
TCP	9443	WebUI - HTTPS

7.6. HA Clustered Pair Configuration

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

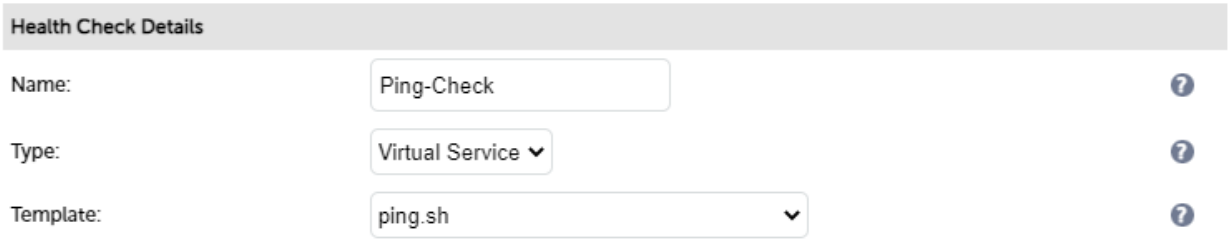
8. Appliance Configuration for Philips IntelliSpace PACS – Using Layer 7 SNAT Mode

8.1. Configuring the External Health Check Scripts

Once configured, these health checks will be available when configuring the VIPs.

Ping Check

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.

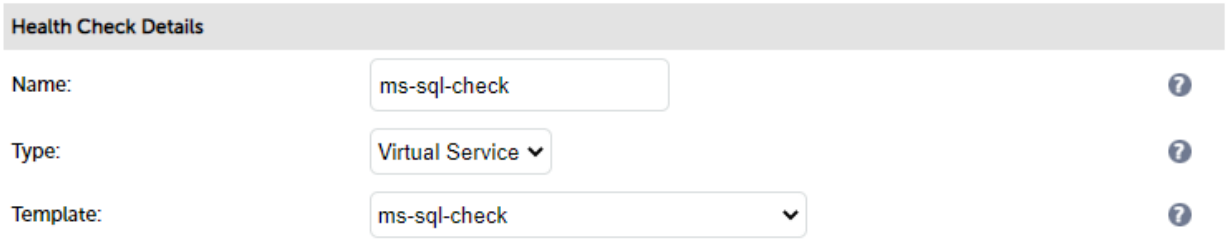


2. Specify an appropriate *Name* for the health check, e.g. **Ping-Check**.
3. Set *Type* to **Virtual Service**.
4. Set *Template* to **ping.sh**.
5. Click **Update**.

MS-SQL Check

The Microsoft SQL health check requires the Microsoft ODBC Driver. Because it is not free and open source software, this driver cannot be redistributed with our load balancer. We have a blog post on our website which walks through how to set up and use this health check. This blog post is available here: https://www.loadbalancer.org/blog/ms-sql-health-check/. Once this has been completed, follow the steps below to complete the process.

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.

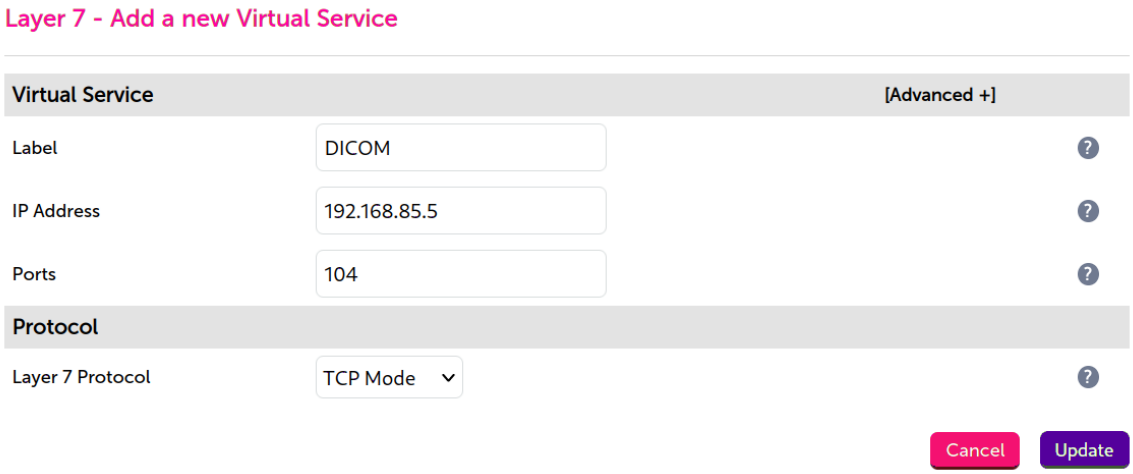


2. Specify an appropriate *Name* for the health check, e.g. **ms-sql-check**.
3. Set *Type* to **Virtual Service**.
4. Set *Template* to **ms-sql-check**.
5. Click **Update**.

8.2. Configuring VIP 1 – DICOM

Configuring the Virtual Service (VIP)

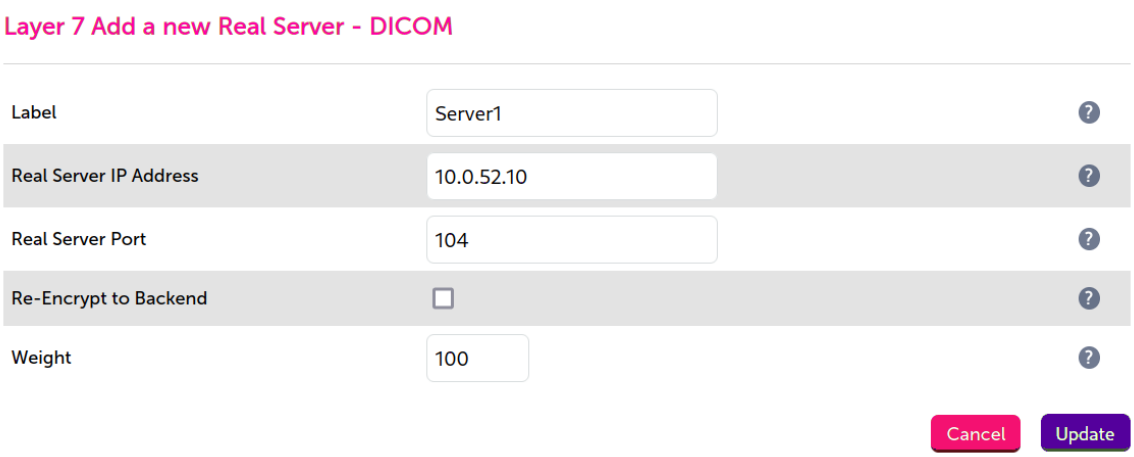
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **DICOM**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **104**.
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. In the *Other* section, click **Advanced** to show more options.
9. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
10. Click **Update**.

Defining the Real Servers (RIPs)

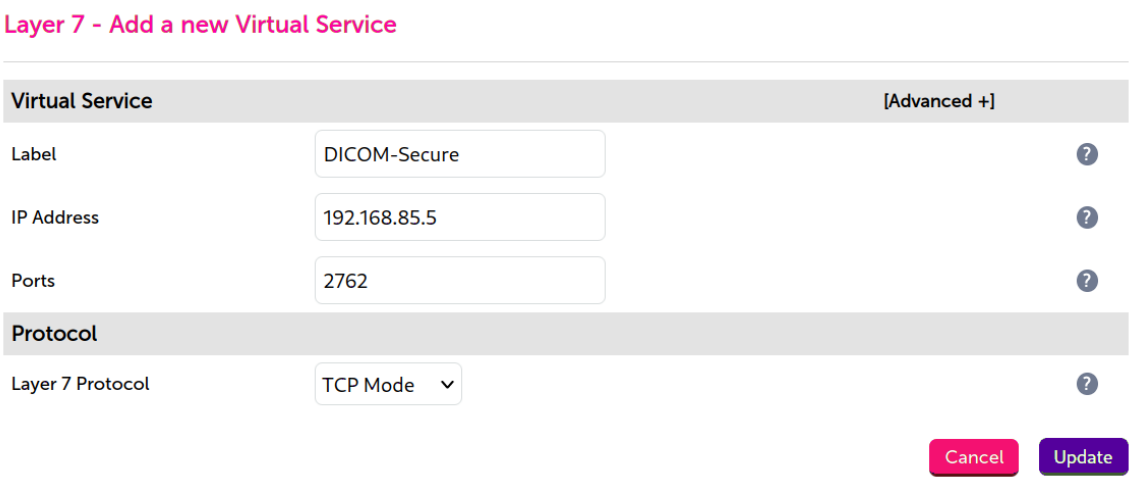
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.10**.
4. Set the *Real Server Port* field to **104**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.3. Configuring VIP 2 – DICOM Secure

Configuring the Virtual Service (VIP)

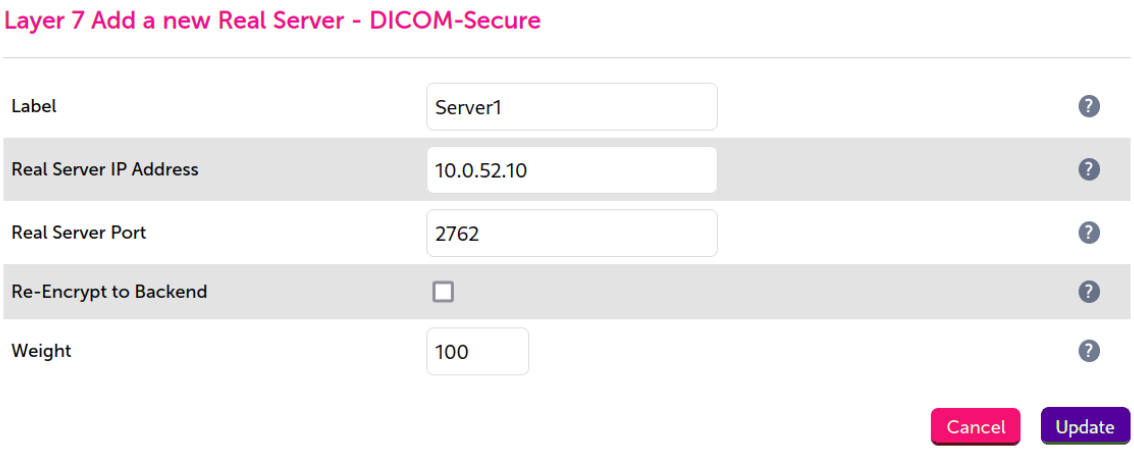
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **DICOM-Secure**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **2762**.
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. In the *Other* section, click **Advanced** to show more options.
9. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
10. Click **Update**.

Defining the Real Servers (RIPs)

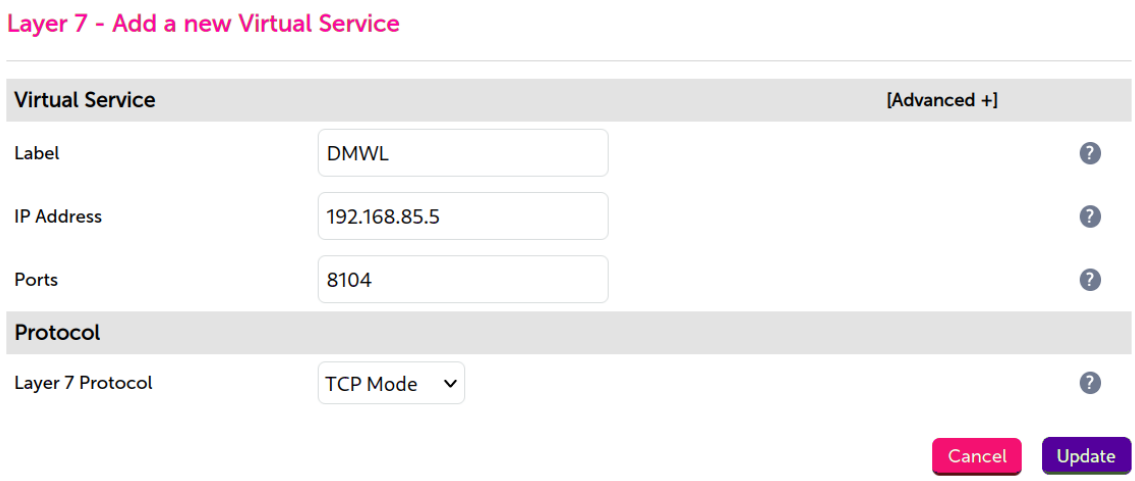
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.10**.
4. Set the *Real Server Port* field to **2762**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.4. Configuring VIP 3 – DMWL

Configuring the Virtual Service (VIP)

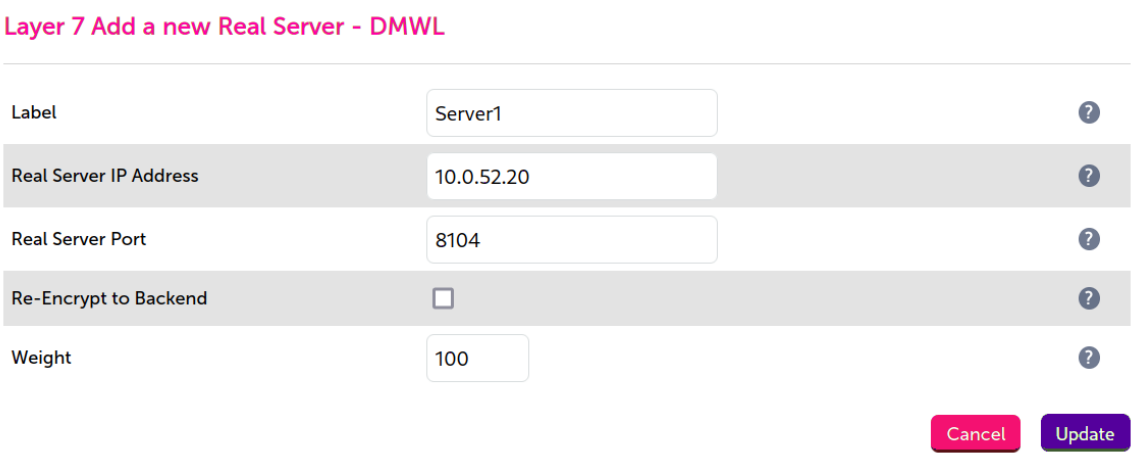
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **DMWL**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **8104**.
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. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **60**.
10. Set *Health Checks* to **External script**.
11. Set *Check Script* to **Ping-Check**.
12. In the *Other* section, click **Advanced** to show more options.
13. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

Defining the Real Servers (RIPs)

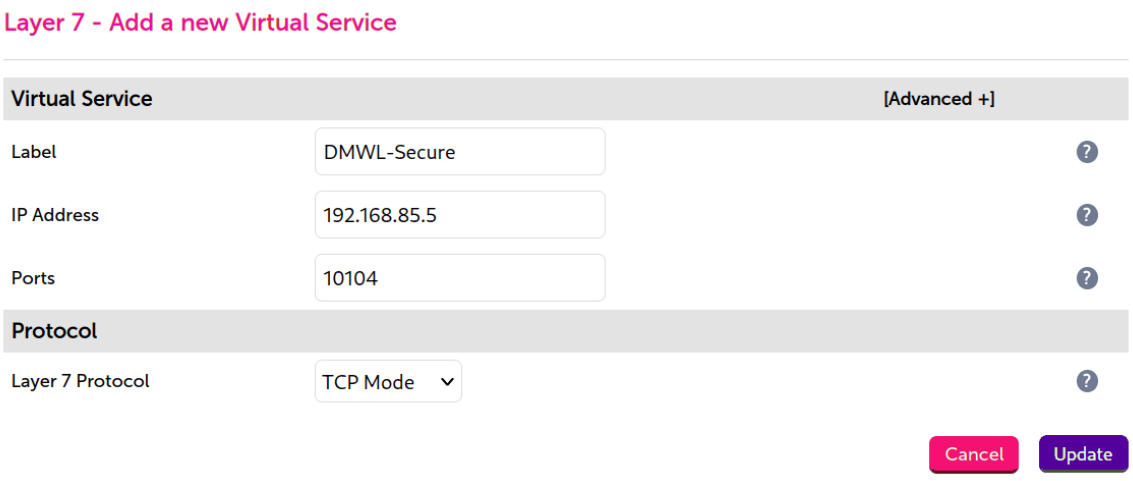
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.20**.
4. Set the *Real Server Port* field to **8104**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.5. Configuring VIP 4 – DMWL Secure

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. **DMWL-Secure**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **10104**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.

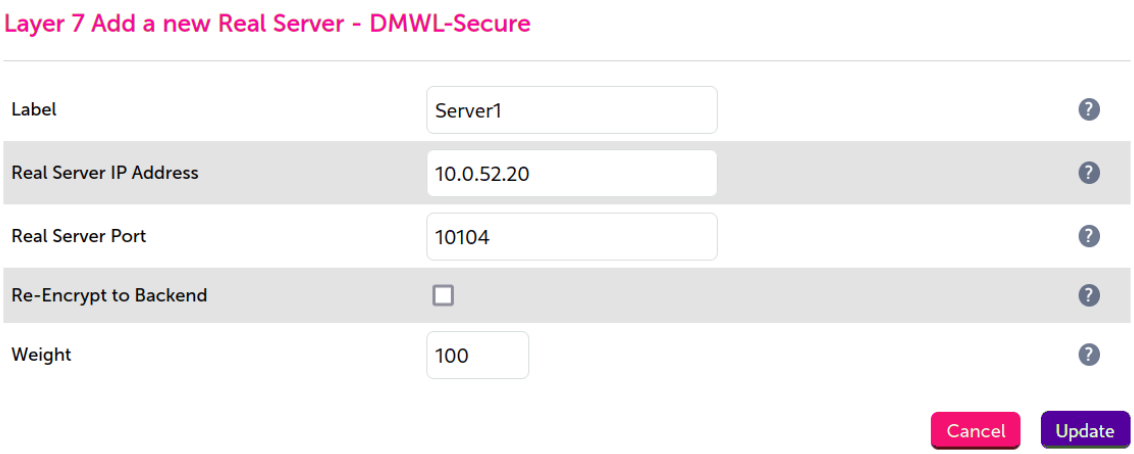


7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **60**.
10. Set *Health Checks* to **External script**.
11. Set *Check Script* to **Ping-check**.

12. In the *Other* section, click **Advanced** to show more options.
13. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

Defining the Real Servers (RIPs)

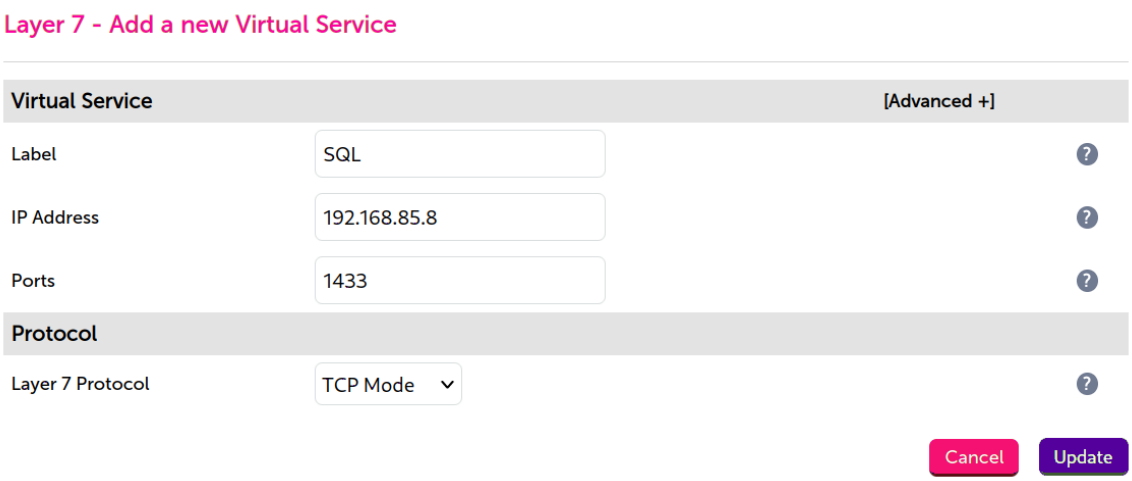
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.20**.
4. Set the *Real Server Port* field to **10104**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.6. Configuring VIP 5 – SQL

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. **SQL**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.8**.
4. Set the *Ports* field to **1433**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.



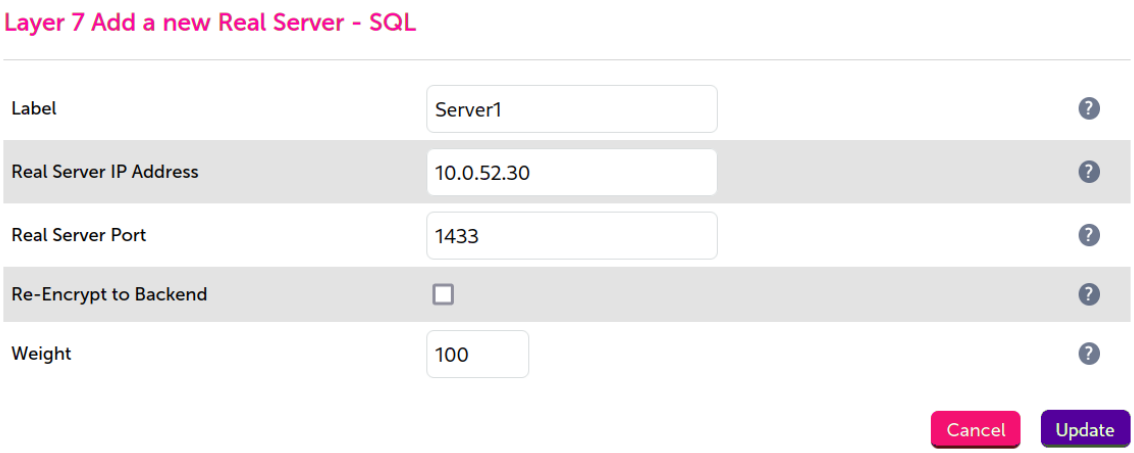
7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **2**.
10. Set *Health Checks* to **External script**.
11. Set *Check Script* to **ms-sql-check**.

> **Note**
>
> The Microsoft SQL health check requires the Microsoft ODBC Driver. Because it is not free and open source software, this driver cannot be redistributed with our load balancer.
>
> We have a blog post on our website which walks through how to set up and use this health check. This blog post is available here: https://www.loadbalancer.org/blog/ms-sql-health-check/. These steps must be completed first before the SQL check is available for selection in the WebUI.

12. In the *Other* section, click **Advanced** to show more options.
13. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

Defining the Real Servers (RIPs)

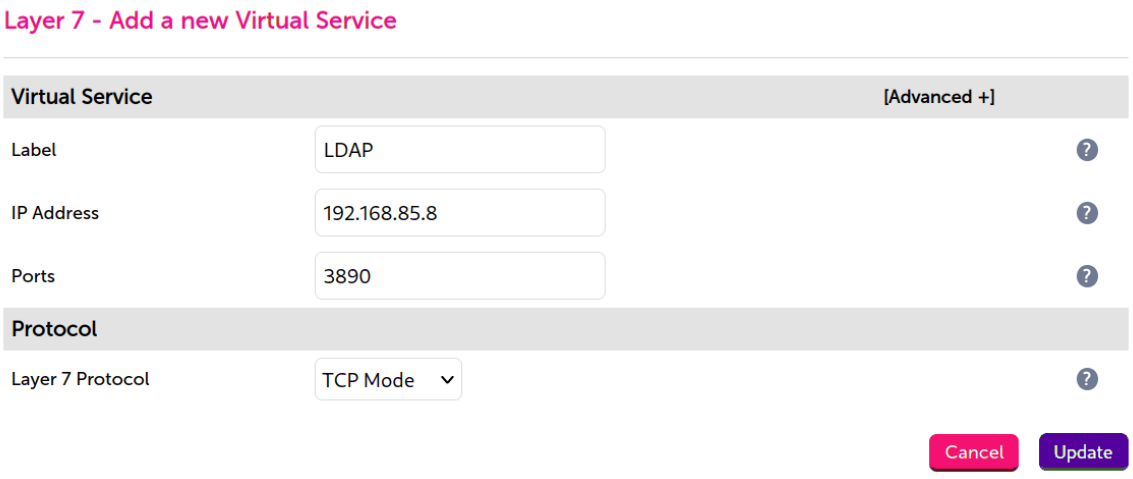
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.30**.
4. Set the *Real Server Port* field to **1433**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.7. Configuring VIP 6 – LDAP

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. **LDAP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.8**.
4. Set the *Ports* field to **3890**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.

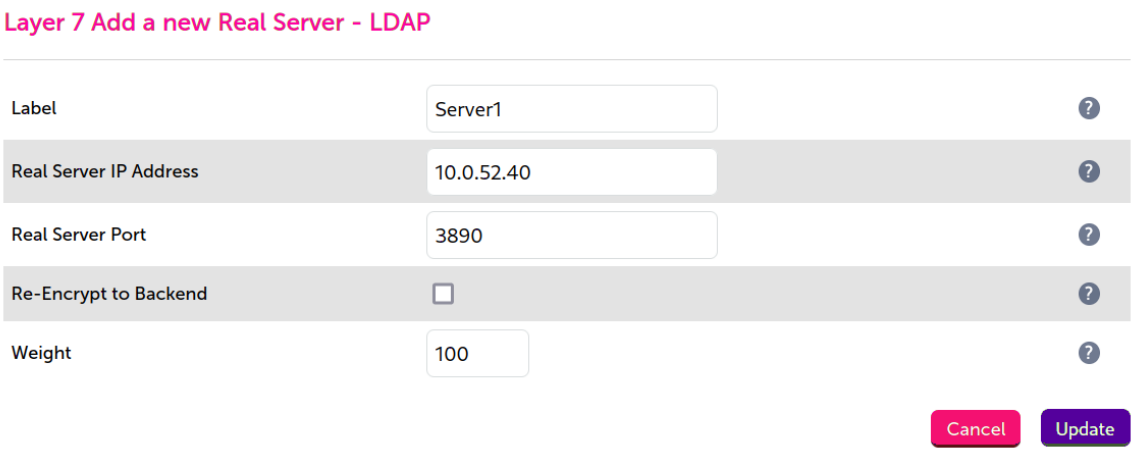


7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **2**.
10. In the *Other* section, click **Advanced** to show more options.
11. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.

12. Click **Update**.

Defining the Real Servers (RIPs)

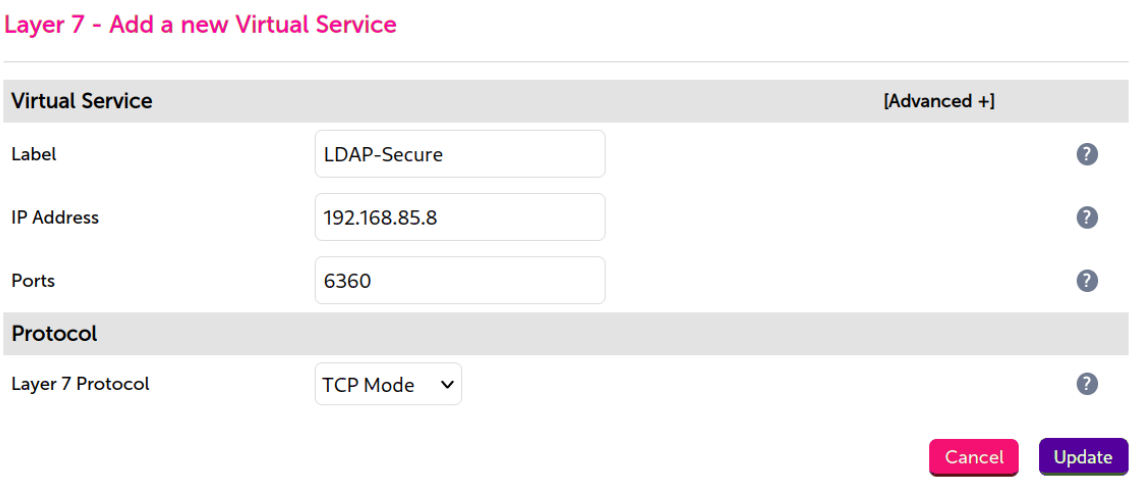
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.40**.
4. Set the *Real Server Port* field to **3890**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.8. Configuring VIP 6 – LDAP Secure (LDAPS)

Configuring the Virtual Service (VIP)

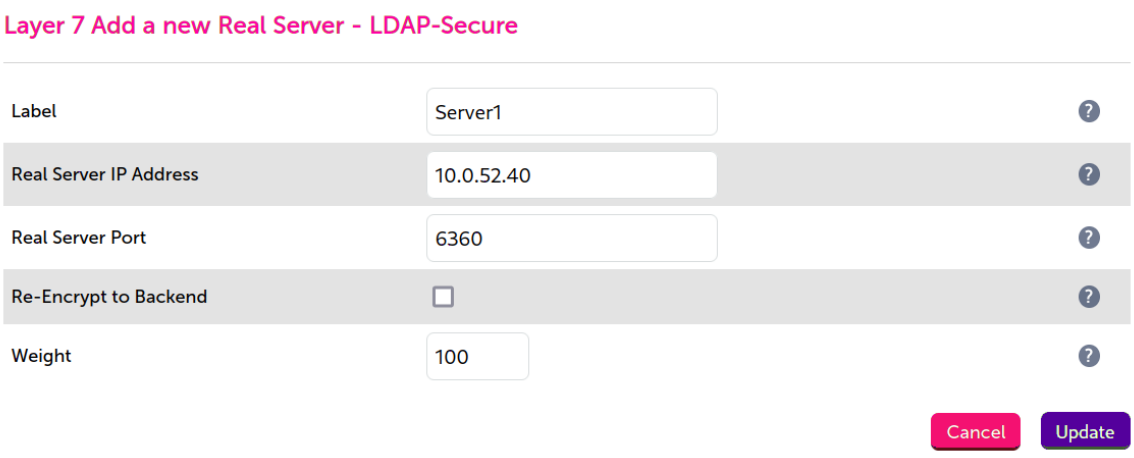
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **LDAP-Secure**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.8**.
4. Set the *Ports* field to **6360**.
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. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **2**.
10. In the *Other* section, click **Advanced** to show more options.
11. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
12. Click **Update**.

Defining the Real Servers (RIPs)

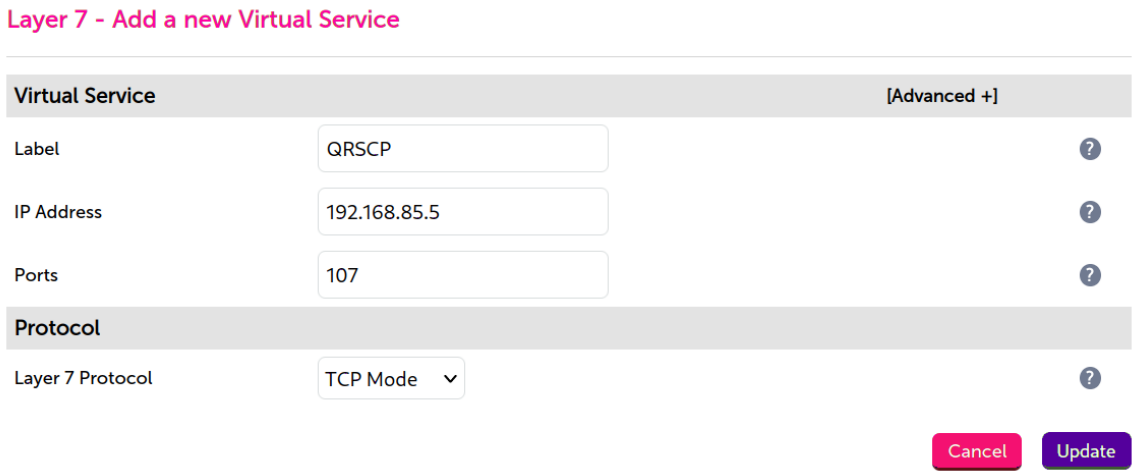
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.40**.
4. Set the *Real Server Port* field to **6360**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.9. Configuring VIP 7 – QRSCP

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. **QRSCP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **107**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.

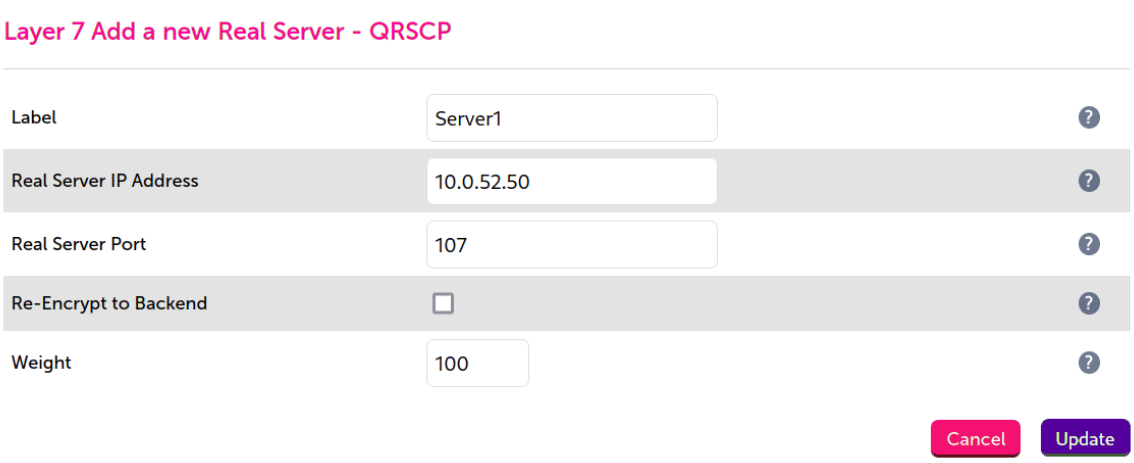


7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **2**.
10. Set *Health Checks* to **External script**.
11. Set *Check Script* to **Ping-Check**.
12. In the *Other* section, click **Advanced** to show more options.
13. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

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. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.50**.
4. Set the *Real Server Port* field to **107**.

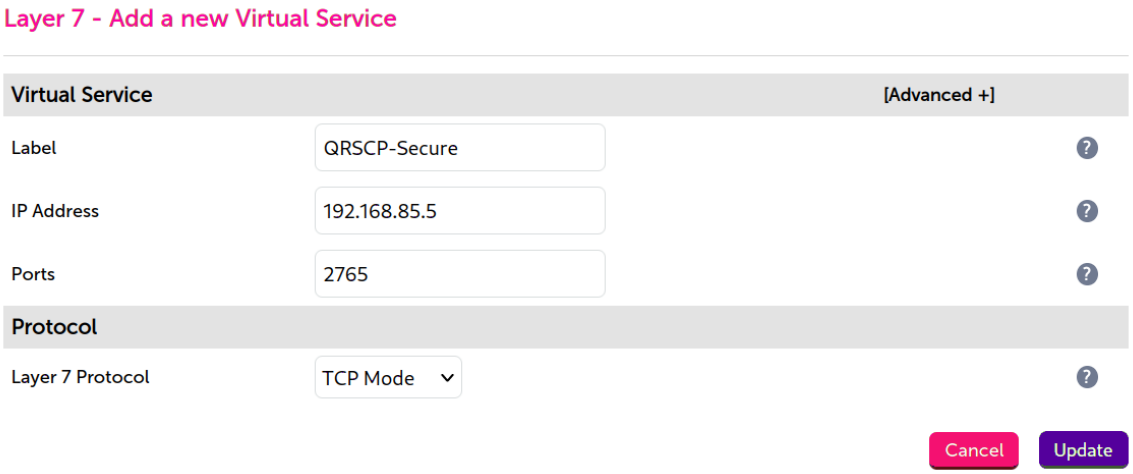
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.10. Configuring VIP 8 – QRSCP Secure

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. **QRSCP-Secure**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **2765**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.

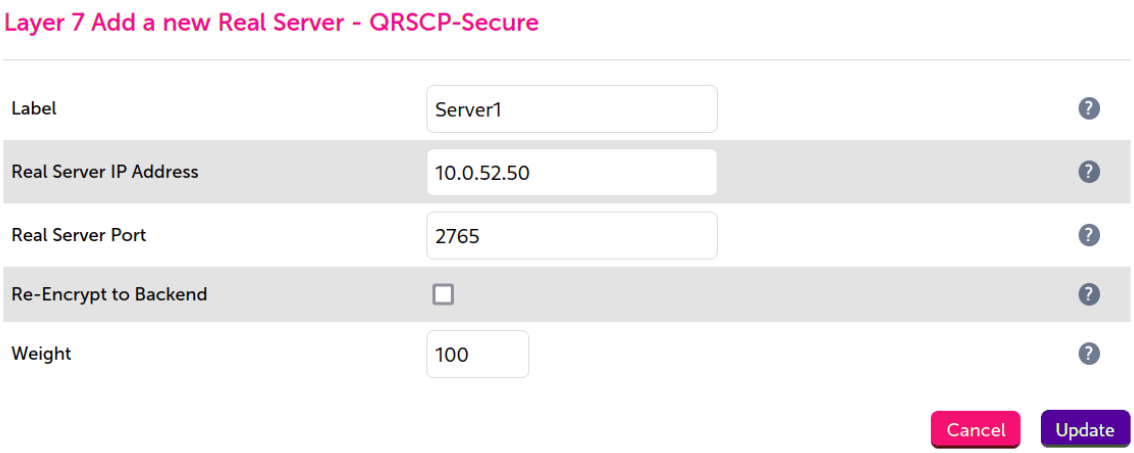


7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **2**.

10. Set *Health Checks* to **External script**.
11. Set *Check Script* to **Ping-Check**.
12. In the *Other* section, click **Advanced** to show more options.
13. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

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. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.50**.
4. Set the *Real Server Port* field to **2765**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



8.11. Finalizing the Configuration

To apply the new settings, HAProxy 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:

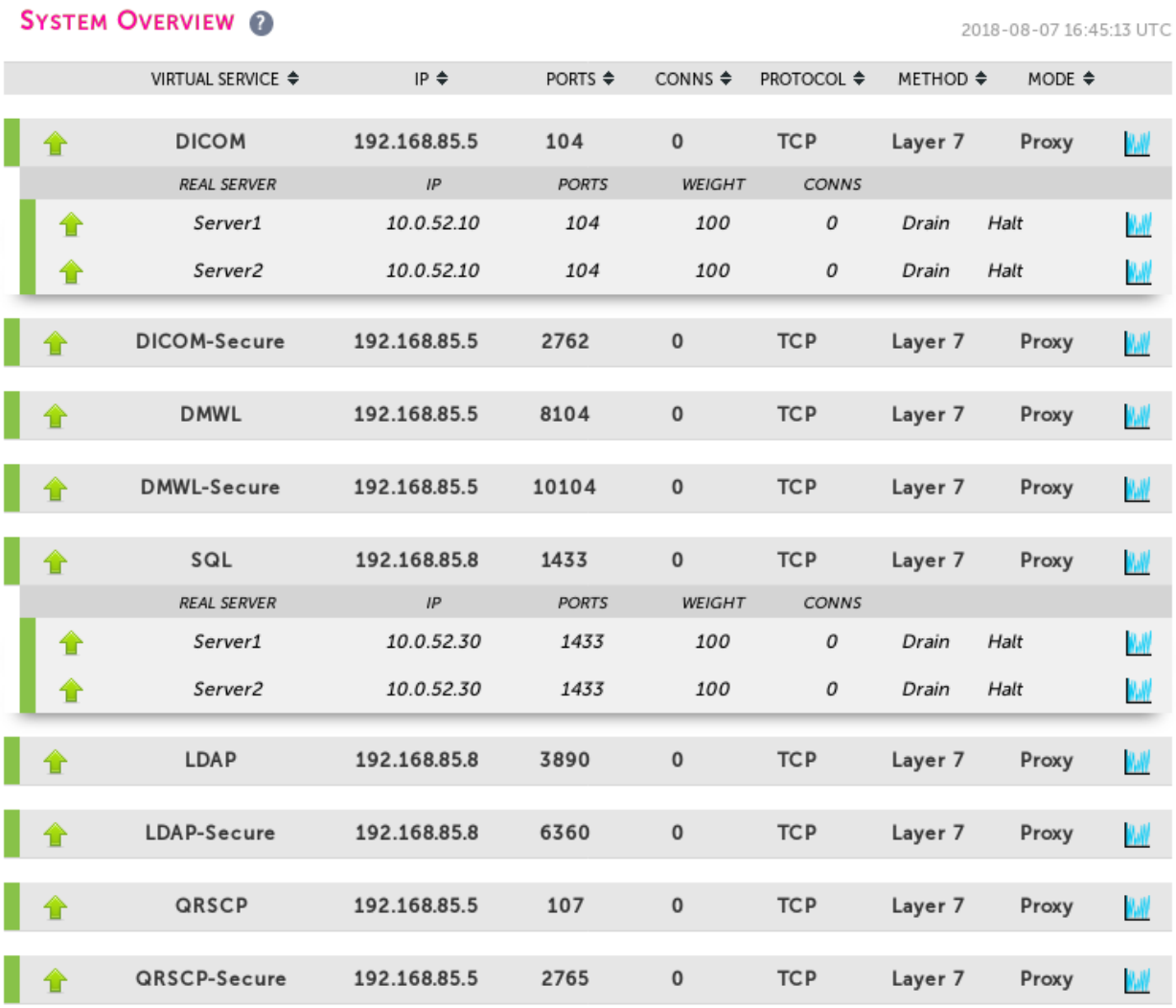
1. Using the WebUI, navigate to: *Maintenance > Restart Services*.
2. Click **Reload HAProxy**.

9. Testing & Verification

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

9.1. Using System Overview

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



10. 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.

11. Further Documentation

For additional information, please refer to the Administration Manual.

12. Appendix

12.1. Configuring Outbound SNAT Rules for DICOM Services (iExport and iQuery)

iptables SNAT rules can be used to SNAT traffic coming from the real servers that is destined to specific ports. To make sure that these rules do not affect other traffic, the rules should be restricted so that they only apply to traffic that has a source IP address matching a real server that requires this configuration.

It is important to note that **the real servers in question must use the load balancer as their default gateway** in order for SNAT rules as described here to function.

It is recommended to put the SNAT rules in the load balancer's firewall script. This can be edited from the WebUI under ***Maintenance > Firewall Script***. Any changes made here must also be made on the Secondary load balancer, if present, as these changes are manual and are not synchronised automatically.

Example SNAT rule

```
iptables -t nat -A POSTROUTING -p tcp -s <real server IP address> -m multiport --dports 104,11112
-j SNAT --to-source <SNAT IP address>
```

Example SNAT rule using multiple IP addresses

```
iptables -t nat -A POSTROUTING -p tcp -s 10.10.5.59,10.10.5.60,10.10.5.113 -m multiport --dports
104,11112 -j SNAT --to-source 10.10.5.100
```

> **Note** The SNAT rules need to be adjusted to accommodate the customer configured destination TCP port for each iExport and iQuery destination.

12.2. Source IP Transparency at Layer 7 Using TPROXY

Layer 7 is the recommended load balancing method for Philips IntelliSpace PACS. Load balancing at layer 7 uses the HAProxy service. HAProxy is a proxy which means that a new connection is established from the proxy out to the backend server in response to an inbound client connection to the proxy. This means that the source IP address of the packet reaching the server will be the proxy's address. By default this is the IP address assigned to the load balancer's Ethernet interface.

The TProxy (Transparent Proxy) kernel option can be used alongside HAProxy to enable IP address transparency, i.e. maintain the actual source IP address of the client. When enabling TProxy, it is important to be aware of the topology requirements for it to work correctly.

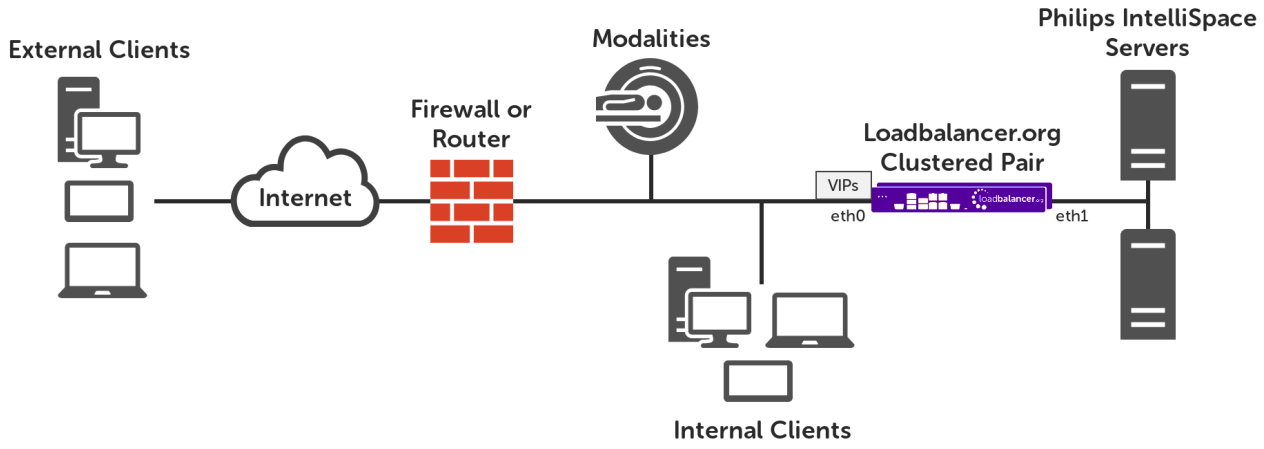
Layer 7 SNAT mode with TProxy is typically used in a 2-arm configuration where the VIP is located in one subnet and the load balanced Real Servers are located in another. This can be achieved by using two network adapters, or by creating VLAN's on a single adapter. Single arm configuration is also supported under certain conditions - for more information please refer to Transparency at Layer 7.

The default gateway on the Real Servers must be an IP address on the load balancer - for a clustered pair, this

should be a floating IP to allow it to move between appliances when needed.

Using a 2-arm Topology:

The diagram below is an overview of a network layout where the Philips IntelliSpace servers sit in their own separate subnet.



12.3. 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 configured first and then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.

> **Note** For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it's active on the Primary and one for the VIP when it's active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

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

Non-Replicated Settings

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

WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	All network settings including IP address(es), bonding configuration and VLANs

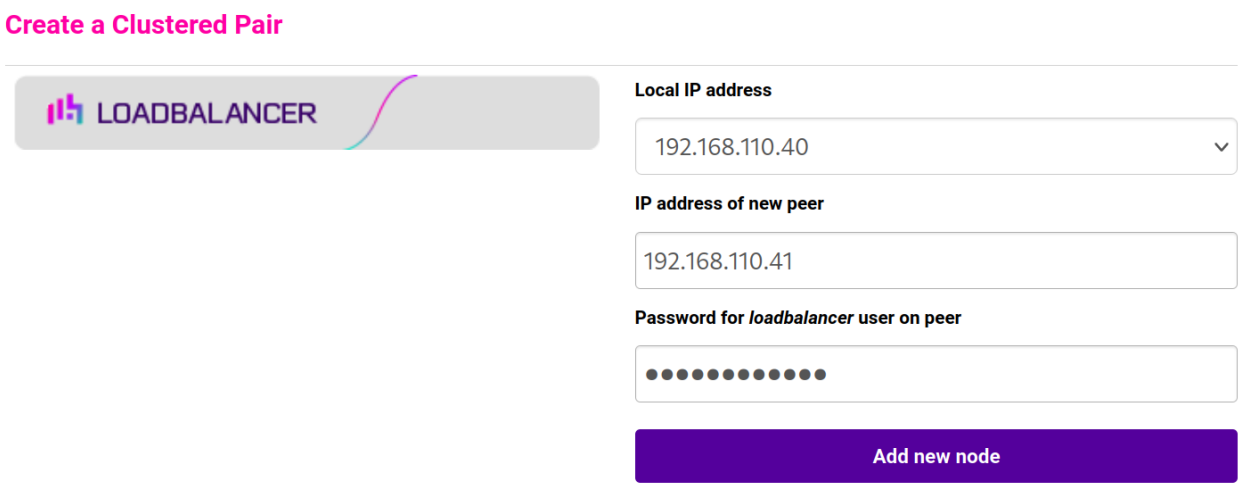
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Routing	Routing configuration including default gateways and static routes
Local Configuration	System Date & time	All time and date related settings
Local Configuration	Physical – Advanced Configuration	Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server
Local Configuration	Security	Appliance security settings
Local Configuration	SNMP Configuration	Appliance SNMP settings
Local Configuration	Graphing	Appliance graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Software Updates	Appliance software update management
Maintenance	Firewall Script	Appliance firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

Important Make sure that if these settings/updates have been configured on the Primary appliance, they're also configured on the Secondary appliance.

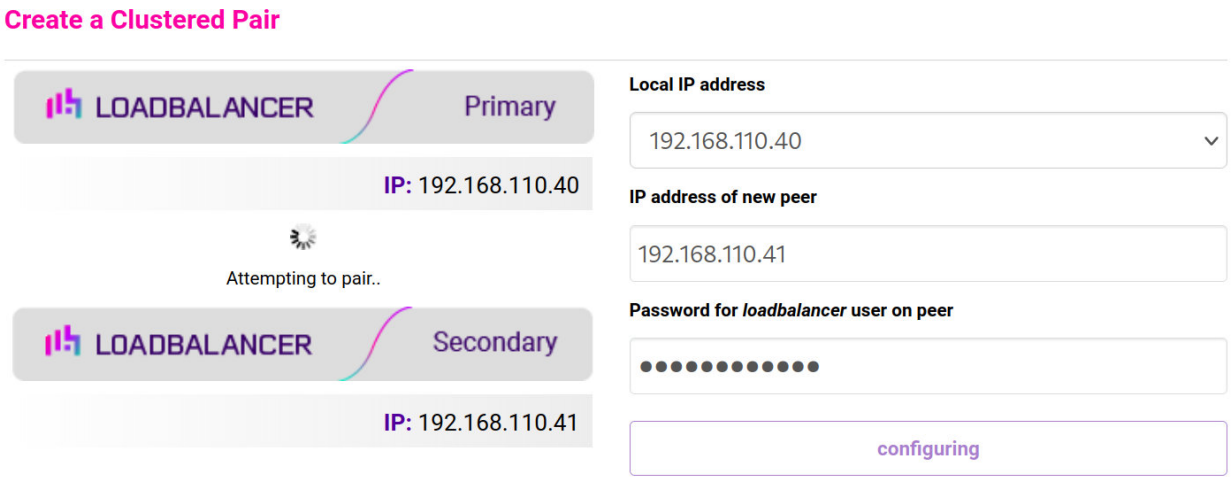
Adding a Secondary Appliance - Create an HA Clustered Pair

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.

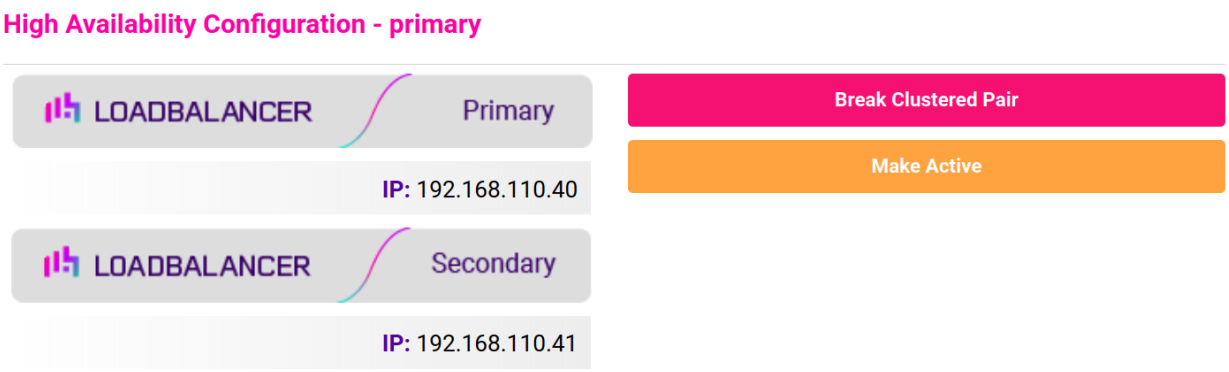
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



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.

13. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	16 August 2018	Initial version		AH
1.0.1	6 December 2018	Added the new "Company Contact Information" page	Required updates	AH
1.1.0	10 December 2019	Styling and layout	General styling updates	AH
1.1.1	18 December 2019	Added the section "Finalizing the Configuration" to ensure HAProxy is explicitly reloaded	Provided clarity for reloading HAProxy post-configuration	AH
1.1.2	21 August 2020	New title page Updated Canadian contact details New screenshots for creating layer 7 VIPs Amended instructions for configuring persistence timeouts and the layer 7 source address	Branding update Change to Canadian contact details Changes to the appliance WebUI	AH
1.2.0	1 January 2022	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.2.1	12 May 2022	Updated external health check related content to reflect latest software version	New software release	RJC
1.2.2	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.2.3	5 January 2023	Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section Removed references to the colour of certain UI elements	Housekeeping across all documentation	AH

Version	Date	Change	Reason for Change	Changed By
1.2.4	2 February 2023	Updated screenshots	Branding update	AH
1.2.5	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.3.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

LOADBALANCER

Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @loadbalancer.org

About Loadbalancer.org

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