Load Balancing Philips IntelliSpace PACS
v1.1.2
Contents

1. About this Guide................................................................................................................................................. 4
2. Loadbalancer.org Appliances Supported........................................................................................................... 4
3. Loadbalancer.org Software Versions Supported................................................................................................ 4
4. Philips IntelliSpace PACS Software Versions Supported..................................................................................... 4
5. Philips IntelliSpace PACS................................................................................................................................... 5
6. Load Balancing Philips IntelliSpace PACS........................................................................................................... 5
   Persistence (aka Server Affinity).......................................................................................................................... 5
   Virtual Service (VIP) Requirements.................................................................................................................... 5
   Port Requirements.............................................................................................................................................. 5
   Health Checks.................................................................................................................................................. 6
   Specifying Traffic Source Address / SNAT Options............................................................................................ 6
7. Deployment Concept............................................................................................................................................ 7
8. Loadbalancer.org Appliance – the Basics............................................................................................................... 8
   Virtual Appliance Download & Deployment..................................................................................................... 8
   Initial Network Configuration.............................................................................................................................. 8
   Accessing the Web User Interface (WebUI)........................................................................................................ 8
   HA Clustered Pair Configuration......................................................................................................................... 10
9. Appliance Configuration for Philips IntelliSpace PACS – Using Layer 7 SNAT Mode........................................... 11
   Configuring VIP 1 – DICOM............................................................................................................................... 11
      Configuring the Virtual Service (VIP)............................................................................................................ 11
      Defining the Real Servers (RIPS).................................................................................................................. 11
   Configuring VIP 2 – DICOM Secure.................................................................................................................. 12
      Configuring the Virtual Service (VIP)............................................................................................................ 12
      Defining the Real Servers (RIPS).................................................................................................................. 12
   Configuring VIP 3 – DMWL............................................................................................................................... 14
      Configuring the Virtual Service (VIP)............................................................................................................ 14
      Defining the Real Servers (RIPS).................................................................................................................. 14
   Configuring VIP 4 – DMWL Secure.................................................................................................................... 16
      Configuring the Virtual Service (VIP)............................................................................................................ 16
      Defining the Real Servers (RIPS).................................................................................................................. 16
   Configuring VIP 5 – SQL..................................................................................................................................... 17
      Configuring the Virtual Service (VIP)............................................................................................................ 17
      Defining the Real Servers (RIPS).................................................................................................................. 17
   Configuring VIP 6 – LDAP.................................................................................................................................... 19
      Configuring the Virtual Service (VIP)............................................................................................................ 19
      Defining the Real Servers (RIPS).................................................................................................................. 19
   Configuring VIP 6 – LDAP Secure (LDAPS)...................................................................................................... 20
      Configuring the Virtual Service (VIP)............................................................................................................ 20
      Defining the Real Servers (RIPS).................................................................................................................. 20
   Configuring VIP 7 – QRSCP............................................................................................................................... 22
      Configuring the Virtual Service (VIP)............................................................................................................ 22
      Defining the Real Servers (RIPS).................................................................................................................. 22
   Configuring VIP 8 – QRSCP Secure.................................................................................................................... 23
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 relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Philips IntelliSpace PACS. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
<tr>
<td></td>
<td>Enterprise GCP **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products/hardware](http://www.loadbalancer.org/products/hardware)

** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- V76.4 and later

4. Philips IntelliSpace PACS Software Versions Supported

- Philips IntelliSpace PACS – all versions
5. 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.

6. 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.

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.

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

Port Requirements

The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>104</td>
<td>TCP/DICOM</td>
<td>DICOM traffic</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol/Service</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>2762</td>
<td>TCP/TLS/DICOM</td>
<td>DICOM traffic over TLS, “DICOM secure”</td>
</tr>
<tr>
<td>8104</td>
<td>TCP/DICOM</td>
<td>DMWL traffic (DICOM Modality Worklists) traffic</td>
</tr>
<tr>
<td>10104</td>
<td>TCP/TLS/DICOM</td>
<td>DMWL traffic over TLS, “DMWL secure”</td>
</tr>
<tr>
<td>1433</td>
<td>TCP/SQL</td>
<td>MS SQL service</td>
</tr>
<tr>
<td>3890</td>
<td>TCP/LDAP</td>
<td>LDAP service</td>
</tr>
<tr>
<td>6360</td>
<td>TCP/LDAPS</td>
<td>Secure LDAP service</td>
</tr>
<tr>
<td>107</td>
<td>TCP/DICOM</td>
<td>QRSCP service (Query/Retrieve Service Class Provider)</td>
</tr>
<tr>
<td>2765</td>
<td>TCP/TLS/DICOM</td>
<td>QRSCP service over TLS, “QRSCP secure”</td>
</tr>
</tbody>
</table>

**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/](https://www.loadbalancer.org/blog/ms-sql-health-check/)

**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.
7. Deployment Concept

VIPs = Virtual 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 section 3 in the appendix on page 30 for more details on configuring a clustered pair.
8. Loadbalancer.org Appliance – the Basics

Virtual Appliance Download & Deployment
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 and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB 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.

Initial Network Configuration
The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

Method 1 - Using the Network Setup Wizard at the console
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Method 2 - Using the WebUI
Using a browser, connect to the WebUI on the default IP address/port: https://192.168.2.21:9443
To set the IP address & subnet mask, use: Local Configuration > Network Interface Configuration
To set the default gateway, use: Local Configuration > Routing
To configure DNS settings, use: Local Configuration > Hostname & DNS

Accessing the Web User Interface (WebUI)
The WebUI can be accessed via HTTPS at the following URL: https://192.168.2.21:9443/lbadmin
* Note the port number → 9443

(replace 192.168.2.21 with the IP address of your load balancer if it’s been changed from the default)

Login using the following credentials:
Username: loadbalancer
Password: loadbalancer

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

Once logged in, the WebUI will be displayed as shown on the following page:
(shows v8.2.x)

**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 slave unit is covered in section 3 of the appendix on page 30.
9. Appliance Configuration for Philips IntelliSpace PACS – Using Layer 7 SNAT Mode

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

![Layer 7 - Add a new Virtual Service](image)

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

**Layer 7 Add a new Real Server – DICOM**

<table>
<thead>
<tr>
<th>Label</th>
<th>Server 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.0.52.10</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>104</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

7. Click **Modify** next to the newly created VIP
8. In the **Other** section, click **Advanced** to show more options

**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
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

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.sh**
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 (RPs)**

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
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.sh`
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

![Layer 7 Add a new Real Server - DMWL-Secure](image)

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/](https://www.loadbalancer.org/blog/ms-sql-health-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. **10.0.52.30**
4. Set the **Real Server Port** field to **1433**
5. Click **Update**
6. Repeat these steps to add additional real servers as required
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

---

**Layer 7 Add a new Real Server - LDAP**

<table>
<thead>
<tr>
<th>Label</th>
<th>Server1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.0.52.40</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>3890</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>
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

![Layer 7 - Add a new Virtual Service](image)

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

![Layer 7 Add a New Real Server - LDAP-Secure](image)

**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

![Layer 7 - Add a new Virtual Service](image)

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.sh
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

<table>
<thead>
<tr>
<th>Label</th>
<th>Server1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.0.52.50</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>107</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

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.sh**
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
Finalizing the Configuration
To apply the new settings, HAProxy must be reloaded as follows:

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

10. Testing & Verification

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.
<table>
<thead>
<tr>
<th>Virtual Service</th>
<th>IP</th>
<th>Ports</th>
<th>ConnS</th>
<th>Protocol</th>
<th>Layer</th>
<th>Method</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DICOM</td>
<td>192.168.85.5</td>
<td>104</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>Server1</td>
<td>10.0.52.10</td>
<td>104</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
<td></td>
</tr>
<tr>
<td>Server2</td>
<td>10.0.52.10</td>
<td>104</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
<td></td>
</tr>
<tr>
<td>DICOM-Secure</td>
<td>192.168.85.5</td>
<td>2762</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>DMWL</td>
<td>192.168.85.5</td>
<td>8104</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>DMWL-Secure</td>
<td>192.168.85.5</td>
<td>10104</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>SQL</td>
<td>192.168.85.8</td>
<td>1433</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>Server1</td>
<td>10.0.52.30</td>
<td>1433</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
<td></td>
</tr>
<tr>
<td>Server2</td>
<td>10.0.52.30</td>
<td>1433</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>192.168.85.8</td>
<td>3890</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>LDAP-Secure</td>
<td>192.168.85.8</td>
<td>6360</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>QRSCP</td>
<td>192.168.85.5</td>
<td>107</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>QRSCP-Secure</td>
<td>192.168.85.5</td>
<td>2765</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
</tbody>
</table>
11. 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.

12. Further Documentation

13. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Philips IntelliSpace PACS environments.
14. Appendix

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 slave 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.
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. When using TPROXY, for a given load balanced virtual service, the real servers must be in a different subnet to the virtual IP address. On the real servers, the default gateway must be configured to be an IP address on the load balancer. When using an HA pair of load balancers, this should be a floating IP address so that it can fail over to the slave appliance when needed. These network topology restrictions are caused by the need to ensure that the real servers cannot directly reply to client traffic; reply traffic must flow back via the load balancer.

The below diagram is an overview of a network layout where the Philips IntelliSpace servers sit in their own separate subnet, to allow TPROXY to be used successfully.
3 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
- Software updates

Version 7:

Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8:

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration
• Specify the IP address and the loadbalancer users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above

• Click Add new node

• The pairing process now commences as shown below:

• Once complete, the following will be displayed:
To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen.

Note: Clicking the Restart Heartbeat button on the master appliance will also automatically restart heartbeat on the slave appliance.

Note: Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
## 15. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>16 August 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>6 December 2018</td>
<td>Added the new &quot;Company Contact Information&quot; page</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>10 December 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>18 December 2019</td>
<td>Added the section “Finalizing the Configuration” to ensure HAProxy is explicitly reloaded</td>
<td>Provided clarity for reloading HAProxy post-configuration</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.2</td>
<td>21 August 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>New screenshots for creating layer 7 VIPs</td>
<td>Changes to the appliance WebUI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amended instructions for configuring persistence timeouts and the layer 7 source address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

United Kingdom
Loadbalancer.org Ltd.
Compass House, North Harbour Business Park, Portsmouth, PO6 4PS
UK:+44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver, BC, V6B 2Z4, Canada
TEL:+1 866 998 0508
sales@loadbalancer.org
support@loadbalancer.org

United States
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany
Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org