Load Balancing Philips IntelliSpace PACS

Version 1.2.0
# Table of 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 ..................................................... 4  
6. Load Balancing Philips IntelliSpace PACS ................................ 4  
   - Persistence (aka Server Affinity) ........................................ 4  
   - Virtual Service (VIP) Requirements .................................... 4  
   - Port Requirements ..................................................... 5  
   - Health Checks .......................................................... 5  
   - Specifying Traffic Source Address / SNAT Options ............... 5  
7. Deployment Concept ........................................................ 6  
8. Loadbalancer.org Appliance – the Basics .................................. 6  
   - Virtual Appliance ....................................................... 6  
   - Initial Network Configuration ....................................... 7  
   - Accessing the WebUI .................................................. 7  
   - Main Menu Options ................................................... 8  
   - HA Clustered Pair Configuration ................................... 9  
9. Appliance Configuration for Philips IntelliSpace PACS – Using Layer 7 SNAT Mode .................................................. 9  
   - Configuring VIP 1 – DICOM ........................................... 9  
     - Configuring the Virtual Service (VIP) ............................. 9  
     - Defining the Real Servers (RIPs) ................................. 9  
   - Configuring VIP 2 – DICOM Secure .................................. 10  
     - Configuring the Virtual Service (VIP) ............................. 10  
     - Defining the Real Servers (RIPs) ................................. 11  
   - Configuring VIP 3 – DMWL ............................................ 11  
     - Configuring the Virtual Service (VIP) ............................. 11  
     - Defining the Real Servers (RIPs) ................................. 12  
   - Configuring VIP 4 – DMWL Secure .................................. 13  
     - Configuring the Virtual Service (VIP) ............................. 13  
     - Defining the Real Servers (RIPs) ................................. 13  
   - Configuring VIP 5 – SQL ............................................... 14  
     - Configuring the Virtual Service (VIP) ............................. 14  
     - Defining the Real Servers (RIPs) ................................. 15  
   - Configuring VIP 6 – LDAP ............................................. 15  
     - Configuring the Virtual Service (VIP) ............................. 15  
     - Defining the Real Servers (RIPs) ................................. 16  
   - Configuring VIP 6 – LDAP Secure (LDAPS) ......................... 17  
     - Configuring the Virtual Service (VIP) ............................. 17  
     - Defining the Real Servers (RIPs) ................................. 17  
   - Configuring VIP 7 – QRSCP ........................................... 18  
     - Configuring the Virtual Service (VIP) ............................. 18  
     - Defining the Real Servers (RIPs) ................................. 19  
   - Configuring VIP 8 – QRSCP Secure ................................ 19  
     - Configuring the Virtual Service (VIP) ............................. 19  
     - Defining the Real Servers (RIPs) ................................. 20  
Finalizing the Configuration .................................................. 21  
10. Testing & Verification ..................................................... 21  
   Using System Overview .................................................. 21
## 11. Technical Support

### 12. Further Documentation

### 13. Conclusion

### 14. Appendix

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

- Example SNAT rule
- Example SNAT rule using multiple IP addresses
- Source IP Transparency at Layer 7 Using TPROXY
- Configuring HA - Adding a Secondary Appliance

### 15. Document Revision History
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. Loadbalancer.org Software Versions Supported

- V8.3.8 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>2762</td>
<td>TCP/TLS/DICOM</td>
<td>DICOM traffic over TLS, &quot;DICOM secure&quot;</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, &quot;DMWL secure&quot;</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, &quot;QRSCP secure&quot;</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/

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

8. Loadbalancer.org Appliance – the Basics

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 The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Note
For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.
Initial Network Configuration
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway, DNS and other network settings.

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

Accessing the WebUI
The WebUI is accessed using a web browser. By default, user authentication is based on local Apache .htaccess files. User administration tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

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

Note If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

1. Using a browser, access the WebUI using the following URL:


2. Log in to the WebUI:

   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:
The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

3. You’ll be asked if you want to run the Setup Wizard. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click **Dismiss**.

**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
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.

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.

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>Server1</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>

---

**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.

---

**Layer 7 - Add a new Virtual Service**

<table>
<thead>
<tr>
<th>Virtual Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Configuration</td>
</tr>
<tr>
<td>Label</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Ports</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
</tr>
</tbody>
</table>
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 (R IPs)**
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.

---

**Layer 7 Add a new Real Server - DICOM-Secure**

<table>
<thead>
<tr>
<th>Label</th>
<th>Server1</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>2762</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

---

**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 (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.
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.

```
Layer 7 - Add a new Virtual Service

Virtual Service

Manual Configuration

Label
DMWL-Secure

IP Address
192.168.85.5

Ports
10104

Protocol

Layer 7 Protocol
TCP Mode
```

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**

<table>
<thead>
<tr>
<th>Label</th>
<th>Server1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.0.52.20</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>10104</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

7. Click **Update** to create the virtual service.

**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**.
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.

---

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

<table>
<thead>
<tr>
<th>Label</th>
<th>Server1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.0.52.30</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>1433</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

---

**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.
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.
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.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.

---

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

<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

Note For additional general guidance please also refer to Testing Load Balanced Services.

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.

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.
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.

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 Secondary 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.
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 should be configured first, 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.

Note

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:

<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface Configuration</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced Configuration</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
</tbody>
</table>
To add a Secondary node - i.e. create a highly available 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 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:

![High Availability Configuration - primary interface](image)

7. 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 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.
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 &quot;Finalizing the Configuration&quot; 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>
<tr>
<td>1.2.0</td>
<td>1 January 2022</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</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.