Table of Contents

1. About this Guide .......................................................... 4
2. Loadbalancer.org Appliances Supported ................................ 4
3. Loadbalancer.org Software Versions Supported ....................... 4
4. Leostream Software Versions Supported ............................... 4
5. Leostream ................................................................. 4
6. Leostream Platform Components ....................................... 4
7. Load Balancing Leostream ............................................... 5
   Load Balancing & HA Requirements .................................. 5
   Persistence (aka Server Affinity) .................................... 5
   Virtual Service (VIP) Requirements ................................ 5
   Port Requirements ....................................................... 5
8. Deployment Concept ...................................................... 6
   Multiple Leostream Gateways Connecting to a Single Leostream Connection Broker .................. 6
   Multiple Leostream Gateways Connecting to a Cluster of Leostream Connection Brokers .......... 7
9. Load Balancer Deployment Methods ................................... 8
   Layer 4 DR Mode ......................................................... 8
   Layer 4 NAT Mode ....................................................... 9
   Our Recommendation .................................................... 12
   Leostream Gateway Configuration ................................... 12
   Leostream Connection Broker Configuration .......................... 12
   Leostream Agent Configuration ....................................... 16
   Leostream Connect Client Configuration ............................. 17
      Windows Clients ....................................................... 17
      Java Clients .......................................................... 18
10. Loadbalancer.org Appliance – the Basics ............................. 18
    Virtual Appliance ......................................................... 18
    Initial Network Configuration ....................................... 18
    Accessing the WebUI .................................................... 18
       Main Menu Options ................................................... 20
    HA Clustered Pair Configuration ................................... 20
11. Appliance Configuration for Leostream - Using Layer 4 DR Mode .... 20
    Configuring VIP 1 - Leostream Gateway Service .................... 20
       Configuring the Virtual Service (VIP) ........................... 20
       Defining the Real Servers (RIPs) .................................. 21
    Configuring VIP 2 - Leostream Connection Broker Service .......... 22
       Configuring the Virtual Service (VIP) ........................... 22
       Defining the Real Servers (RIPs) .................................. 23
    Configure the Load Balancer’s Network Interfaces .................. 24
    Configuring VIP 1 - Leostream Gateway Service .................... 25
       Configuring the Virtual Service (VIP) ........................... 25
       Defining the Real Servers (RIPs) .................................. 26
    Configuring VIP 2 - Leostream Connection Broker Service .......... 26
       Configuring the Virtual Service (VIP) ........................... 26
       Defining the Real Servers (RIPs) .................................. 28
    Create a Floating IP to Use for the Leostream Servers' Default Gateway .................. 28
       To Create a Floating IP Address on the Load Balancer .............. 28
    Leostream Server Configuration ...................................... 29
    Default Gateway ......................................................... 29
1. About this Guide

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

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Leostream. 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

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.

4. Leostream Software Versions Supported

- Leostream Connection Broker – 9.0 and later
- Leostream Gateway – 2.0 and later

5. Leostream

Leostream provides the critical remote desktop connection management technology required for organizations to build successful large-scale remote access solutions for physical, virtual, and cloud-hosted desktops. The Leostream Platform is the industry’s most widely deployed vendor-independent remote desktop connection management solution, enabling enterprises to integrate the complex array of clients, hosting platforms, guest operating systems, and display protocols required for successful VDI, hosted desktop, and application deployments.

6. Leostream Platform Components

- **Connection Broker**: The main application that manages the hosted desktop environment. The Connection Broker is the central management layer for configuring your deployment, including inventorying and provisioning desktops, assigning and connecting users to these desktops, and defining the end-user experience. The Connection Broker also includes a web portal for users to access their hosted resources.

- **Leostream Gateway**: An optional application that provides HTML5-based clientless remote access for users connecting to their remote desktop. The Leostream Gateway also provides gateway functionality for protocols such as RDP, HP ZCentral Remote Boost, NICE DCV, and Mechdyne TGX, to connect users to desktops that are hosted in a network that is isolated from the user’s client device.
Leostream Agent: When installed on the remote desktop, the Leostream Agent provides the Connection Broker with insight into the connection status of remote users, including when they log out, disconnect, or are idle on their desktop. The Agent also manages enhancements such as USB device passthrough and network printer redirection. The Leostream Agent is available for Microsoft Windows, Linux, and macOS operating systems.

Leostream Connect: A software client provided by Leostream that allows users to log into your Leostream environment and access their hosted resources from fat or thin clients. Using Leostream Connect, you can repurpose existing desktops and laptops as client devices, lowering the cost of VDI deployments. Some thin clients provide built-in Leostream Connect clients.

The Leostream Connection Broker and Gateway are deployed onto Linux hosts.

The Leostream Client and Agent can be deployed onto Windows, Linux, and Mac hosts.

7. Load Balancing Leostream

Note: It’s highly recommended that you have a working Leostream environment first before implementing the load balancer.

Load Balancing & HA Requirements
For high availability and scalability, it is recommended that multiple Leostream Gateway servers and multiple Connection Broker servers are deployed in load balanced clusters.

Persistence (aka Server Affinity)
Source IP address based persistence is required to successfully load balance a Leostream deployment. This is true for load balancing Leostream gateway servers and for load balancing connection brokers.

Virtual Service (VIP) Requirements
To provide load balancing and HA for Leostream, the following VIP is required:

- Leostream Gateway Service

Optionally, an additional VIP may be required as follows:

- Leostream Connection Broker Service

Port Requirements
For the purposes of this guide, the focus will be on the RDP, PCoIP, and HP ZCentral remote protocols. Leostream is also compatible with a plethora of other different remote connection protocols, however. Refer to the official Leostream documentation for further details.

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>80</td>
<td>TCP/HTTP</td>
<td>HTTP Logon to Leostream Service</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>HTTPS Logon to Leostream Service</td>
</tr>
<tr>
<td>3389</td>
<td>TCP/UDP/RDP</td>
<td>(Optional) Connection to RDP Hosts</td>
</tr>
<tr>
<td>Port</td>
<td>Protocols</td>
<td>Use</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>42966</td>
<td>TCP/UDP/HP RGS</td>
<td>(Optional) ZCentral Remote Boost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Formerly HP Remote Graphics Software)</td>
</tr>
<tr>
<td>4172</td>
<td>TCP/UDP/PCoIP</td>
<td>(Optional) PC-over-IP Remote Display</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol</td>
</tr>
<tr>
<td>50001</td>
<td>TCP/PCoIP</td>
<td>(Optional) PC-over-IP Remote Display</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol</td>
</tr>
<tr>
<td>50002</td>
<td>TCP/PCoIP</td>
<td>(Optional) PC-over-IP Remote Display</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol</td>
</tr>
</tbody>
</table>

**Note** | Optional protocols are dependent on the remote desktop protocol in use for client connections.

8. Deployment Concept

Leostream can be deployed in two different ways that can be load balanced.

**Multiple Leostream Gateways Connecting to a Single Leostream Connection Broker**

---

**Step 1: Authentication**

(Reprinted from Leostream 6 documentation)

**Diagram:**

- **End Users**
- **Internet**
- **VIP GW_VIP_L4**
- **Leostream Gateway 1**
- **Leostream Gateway 2**
- **Leostream Connection Broker**
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 the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

Multiple Leostream Gateways Connecting to a Cluster of Leostream Connection Brokers

Step 1: Authentication (Clustered Leostream Connection Brokers)

End Users

Step 2: Remote Connection (Single Leostream Connection Broker)
9. Load Balancer Deployment Methods

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

For Leostream, using layer 4 DR mode is recommended. It is also possible to use layer 4 NAT mode, however the performance of this set up is not as great as layer 4 DR mode. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode please refer to Section 11, “Appliance Configuration for Leostream - Using Layer 4 DR Mode”, and for configuring using layer 4 NAT mode refer to Section 12, “Appliance & Server Configuration for Leostream - Using Layer 4 NAT Mode”.

Layer 4 DR Mode

One-arm direct routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

Note: Kemp, Brocade, Barracuda & A10 Networks call this Direct Server Return and F5 call it N-Path.
- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.

- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Server’s own IP address and the VIP.

- The Real Servers should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as **Solving the ARP Problem**. For more information please refer to [DR Mode Considerations](#).

- On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP.

- The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work.

- The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet.

- Port translation is not possible with DR mode, e.g. VIP:80 → RIP:8080 is not supported.

- DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

**Layer 4 NAT Mode**

Layer 4 NAT mode is a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode.
The load balancer translates all requests from the Virtual Service to the Real Servers.

NAT mode can be deployed in the following ways:

- **Two-arm (using 2 Interfaces)** (as shown above) - Here, 2 subnets are used. The VIP is located in one subnet and the load balanced Real Servers are located in the other. The load balancer requires 2 interfaces, one in each subnet.

  **Note** This can be achieved by using two network adapters, or by creating VLANs on a single adapter.

  - Normally eth0 is used for the internal network and eth1 is used for the external network although this is not mandatory. If the Real Servers require Internet access, *Autonat* should be enabled using the WebUI menu option: *Cluster Configuration > Layer 4 - Advanced Configuration*, the external interface should be selected.

  - The default gateway on the Real Servers must be set to be an IP address on the load balancer.

  - Clients can be located in the same subnet as the VIP or any remote subnet provided they can route to the VIP.

- **One-arm (using 1 Interface)** - Here, the VIP is brought up in the same subnet as the Real Servers.

  - To support remote clients, the default gateway on the Real Servers must be an IP address on the load balancer and routing on the load balancer must be configured so that return traffic is routed
back via the router.

Note

For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server’s default gateway. This ensures that the IP address can ‘float’ (move) between Primary and Secondary appliances.

- To support local clients, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer. For more information please refer to One-Arm (Single Subnet) NAT Mode.

- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. SMTP or RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this.

- Port translation is possible with Layer 4 NAT mode, e.g. VIP:80 → RIP:8080 is supported.

- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.

NAT Mode Packet re-Writing

In NAT mode, the inbound destination IP address is changed by the load balancer from the Virtual Service IP address (VIP) to the Real Server. For outbound replies the load balancer changes the source IP address of the Real Server to be the Virtual Services IP address.

The following table shows an example NAT mode setup:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>VIP</th>
<th>Port</th>
<th>RIP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>10.0.0.20</td>
<td>80</td>
<td>192.168.1.50</td>
<td>80</td>
</tr>
</tbody>
</table>

In this simple example all traffic destined for IP address 10.0.0.20 on port 80 is load-balanced to the real IP address 192.168.1.50 on port 80.

Packet rewriting works as follows:

1) The incoming packet for the web server has source and destination addresses as:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>10.0.0.20:80</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.x.x.x:34567</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2) The packet is rewritten and forwarded to the backend server as:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>192.168.1.50:80</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.x.x.x:34567</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3) Replies return to the load balancer as:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>x.x.x.x:34567</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.50:80</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4) The packet is written back to the VIP address and returned to the client as:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>x.x.x.x:34567</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.20:80</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Our Recommendation**

Where possible, we recommend that Layer 4 Direct Routing (DR) mode is used. This mode offers the best possible performance since replies go directly from the Real Servers to the client, not via the load balancer. It’s also relatively simple to implement. Ultimately, the final choice does depend on your specific requirements and infrastructure.

If DR mode cannot be used, for example if the real servers are located in remote routed networks, then NAT mode is recommended.

**Leostream Gateway Configuration**

Carry out the following instructions on each gateway server:

1. **If deploying using DR mode**: Change the ARP behaviour of the server by following the instructions in the section [Solving the ARP Problem for Linux](#) of the appendix.

2. Open an SSH connection to the Leostream Gateway host.

3. Run the command `leostream-gateway --broker <BROKER_VIP_L4>`
   
   - **Non-clustered connection broker deployment**: Use the IP address / FQDN of the connection broker server.
   
   - **Clustered connection broker deployment**: Use the VIP address of the connection broker virtual service.

```
[root@localhost ~]# leostream-gateway --broker 192.168.98.237
Connection Broker forwarding is enabled
```

4. Run the command `leostream-gateway --info` to confirm that the connection broker has been added to the configuration.

```
[root@localhost ~]# leostream-gateway --info
OS is CentOS 7
Port range is 20001-23000
Gateway version is 2.0.0.18
The VPN is OFF
Connection Broker forwarding is ON to 192.168.98.237
Azure Broker forwarding is OFF
Guacamole is ENABLED
This Gateway is attached to a Connection Broker
```

**Leostream Connection Broker Configuration**

If load balancing multiple connection brokers (this is optional), carry out the following instructions on each connection broker server:

1. **If deploying using DR mode**: Change the ARP behaviour of the server by following the instructions in the section [Solving the ARP Problem for Linux](#) of the appendix.

2. Connect to the connection broker server via browser and login as an admin user.

3. From the left hand menu, expand Setup, navigate to Gateways, and click on **Add Gateway Cluster** as the top of the main window.
4. Set the name of the cluster.

5. Choose the option **All Gateways in this cluster**.

6. In the text box **Public IP address or FQDN of the external load balancer**, put in the VIP address of the connection broker virtual service.

7. Set **Method for routing display protocol traffic through this Leostream gateway** to **From random gateway port to protocol-specific desktop port**.

8. Click **Save** to commit the changes.

10. Select the gateway cluster created in the previous step from the drop-down list.

11. Set Public IP address or FQDN for use in Protocol Plans as the VIP address of the gateway virtual service.

12. Set IP address or FQDN used for Connection Broker communications to this Gateway as real server's own IP address / FQDN.
13. Click **Save** to commit the changes.

14. Repeat the *Add Gateway* process to add additional Leostream Gateways as required.

15. From the left hand menu, navigate to **Configuration > Protocol Plans**.

16. Click on **Edit** next to the *Default* plan.
17. For each protocol in use, set the Gateway to the gateway cluster created previously.

![Edit Protocol Plan](image1)

18. Save the changes.

**Leostream Agent Configuration**

For each Leostream agent installed, the agent should be configured with either the connection broker VIP address or the (solo) connection broker’s IP address / FQDN in a non-clustered environment. This should be set as the Trusted Connection Broker Address, like so:

![Leostream Agent Configuration](image2)
Leostream Connect Client Configuration

Leostream Connect clients must be configured as described below, depending on the specific platform in use.

Windows Clients

1. Open the Leostream Connect client.

2. Right-click on the Leostream icon in the Windows taskbar and click on Options...

3. Click on the Broker tab and set the Address to the VIP address of the gateway service.
Java Clients

1. Navigate to the location of (directory that contains) the LeostreamConnect.jar file.

2. Create or edit a file named lc.conf that contains the following minimum contents:

   ```
   trace_level=ERROR,WARN,INFO,TRACE,DIAG
   rdp_path=/usr/bin/remmina
   connection_broker_auto_discovery=false
   recent_brokers=192.168.98.231
   connection_broker_address=<GW_VIP_L4>
   ```

   where GW_VIP_L4 is the VIP address of the gateway service.

   **Note** Set the rdp_path variable to the location of the preferred RDP client.

10. 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 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.

**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.

**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
- **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

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

11. Appliance Configuration for Leostream - Using Layer 4 DR Mode

Configuring VIP 1 - Leostream Gateway Service

Configuring the Virtual Service (VIP)
1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service.
2. Define the Label for the virtual service as required, e.g. GW_VIP_L4.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.98.238.
4. Set the Ports field to cover the remote desktop protocols in use, e.g. 80,443,3389,4172,42966,50001,50002.
5. Set the Protocol to TCP/UDP.
7. Click Update to create the virtual service.
8. Click **Modify** next to the newly created VIP.
9. Ensure that the **Persistence Enable** checkbox is checked.
10. Set the **Health Checks Check Type** to **Negotiate**.
11. Set the **Check Port** to **443**.
12. Set the **Protocol** to **HTTPS**.
13. Set the **Request to send** to **/app/system/ping**
14. Set the **Response expected** to **OK**
15. Click **Update**.

### Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **GW01**.

3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.98.231**.

4. Click **Update**.

5. Repeat these steps to add additional Leostream Gateways as real servers as required.

### Configuring VIP 2 - Leostream Connection Broker Service

**Important**

This virtual service should **only** be configured in a deployment with multiple, clustered Leostream Connection Brokers. If operating with a **single** Leostream Connection Broker then skip setting up this service.

#### Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**.

2. Define the *Label* for the virtual service as required, e.g. **BROKER_VIP_L4**.

3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.98.237**.

4. Set the *Ports* field to **80,443**.

5. Set the *Protocol* to **TCP**.

6. Set the *Forwarding Method* to **Direct Routing**.

7. Click **Update** to create the virtual service.
8. Click **Modify** next to the newly created VIP.
9. Ensure that the **Persistence Enable** checkbox is checked.
10. Set the **Health Checks Check Type** to **Negotiate**.
11. Set the **Check Port** to **443**.
12. Set the **Protocol** to **HTTPS**.
13. Set the **Request to send** to `/index.pl?action=cb_status`
14. Set the **Response expected** to **CB_IS_OK**
15. Click **Update**.

**Defining the Real Servers (RIPs)**

1. Using the web user interface, navigate to **Cluster Configuration > Layer 4 – Real Servers** and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **BRK01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.98.230**.
4. Click **Update**.
5. Repeat these steps to add additional Leostream Connection Brokers as real servers as required.

![Layer 4 Add a new Real Server - BROKER_VIP_L4](image)

**Layer 4 Add a new Real Server - BROKER_VIP_L4**

<table>
<thead>
<tr>
<th>Label</th>
<th>BRK01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.98.230</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

12. **Appliance & Server Configuration for Leostream - Using Layer 4 NAT Mode**

**Configure the Load Balancer's Network Interfaces**

Layer 4 NAT mode 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 VLANs on a single adapter. Single arm configuration is also supported under certain conditions - for more information please refer to **Layer 4 NAT Mode**.

**To configure an additional network interface for a 2-arm configuration:**

1. Using the WebUI, navigate to **Local Configuration > Network Interface Configuration**.
2. Scroll to the **IP Address Assignment** section.

![IP Address Assignment](image)

- **eth0**: 192.168.85.100/24
- **eth1**: 192.168.98.1/24

**MTU**: 1500 bytes

[Configure Interfaces]
3. Specify an appropriate IP address for eth1 in CIDR format as shown above.
4. Click Configure Interfaces.

Note: There are no restrictions on which interface is used for each requirement.

Configuring VIP 1 - Leostream Gateway Service

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service.
2. Define the Label for the virtual service as required, e.g. GW_VIP_L4.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.140.
4. Set the Ports field to cover the remote desktop protocols in use, e.g. 80,443,3389,4172,42966,50001,50002.
5. Set the Protocol to TCP/UDP.
6. Leave the Forwarding Method set to NAT.
7. Click Update to create the virtual service.

8. Click Modify next to the newly created VIP.
9. Ensure that the Persistence Enable checkbox is checked.
10. Set the Health Checks Check Type to Negotiate.
11. Set the Check Port to 443.
12. Set the Protocol to HTTPS.
13. Set the Request to send to /app/system/ping
14. Set the Response expected to OK
15. Click Update.
Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Real Servers and click on Add a new Real Server next to the newly created VIP.

2. Define the Label for the real server as required, e.g. GW01.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.98.231.

4. Click Update.

5. Repeat these steps to add additional Leostream Gateways as real servers as required.

Configuring VIP 2 - Leostream Connection Broker Service

**Important**
This virtual service should only be configured in a deployment with multiple, clustered Leostream Connection Brokers. If operating with a single Leostream Connection Broker then skip setting up this service.

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service.

2. Define the Label for the virtual service as required, e.g. BROKER_VIP_L4.
3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.85.141**.

4. Set the **Ports** field to **80,443**.

5. Set the **Protocol** to **TCP**.

6. Set the **Forwarding Method** to **NAT**.

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

```
Layer 4 - Add a new Virtual Service

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>BROKER_VIP_14</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.85.141</td>
</tr>
<tr>
<td>Ports</td>
<td>80,443</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>NAT</td>
</tr>
</tbody>
</table>
```

8. Click **Modify** next to the newly created VIP.

9. Ensure that the **Persistence Enable** checkbox is checked.

10. Set the **Health Checks Check Type** to **Negotiate**.

11. Set the **Check Port** to **443**.

12. Set the **Protocol** to **HTTPS**.

13. Set the **Request to send** to `/index.pl?action=cb_status`

14. Set the **Response expected** to **CB_IS_OK**

15. Click **Update**.
Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Real Servers and click on Add a new Real Server next to the newly created VIP.

2. Define the Label for the real server as required, e.g. BRK01.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.98.230.

4. Click Update.

5. Repeat these steps to add additional Leostream Connection Brokers as real servers as required.

Create a Floating IP to Use for the Leostream Servers' Default Gateway

The default gateway on each Leostream server must be configured to be an IP address on the load balancer. It's possible to use the IP address assigned to the internal facing interface (eth1 in this example) for the default gateway, although it's recommended that an additional floating IP is created for this purpose. This is required if two load balancers (our recommended configuration) are used. In this scenario if the primary unit fails, the floating IP will be brought up on the secondary.

To Create a Floating IP Address on the Load Balancer

1. Using the WebUI, navigate to: Cluster Configuration > Floating IPs.

2. Enter the required IP address to be used for the default gateway, e.g. 192.168.98.100.
3. Click Add Floating IP.

Once added, there will be multiple floating IPs: one for each virtual service (192.168.85.140 and 192.168.85.141, in the example presented here) and one for the default gateway (e.g. 192.168.98.100) as shown below:

<table>
<thead>
<tr>
<th>Floating IPs</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.85.140</td>
<td></td>
</tr>
<tr>
<td>192.168.85.141</td>
<td></td>
</tr>
<tr>
<td>192.168.98.100</td>
<td></td>
</tr>
</tbody>
</table>

Leostream Server Configuration

Default Gateway
To ensure that return traffic passes back to the client via the load balancer, set the default gateway of each Leostream server (gateways and, if being load balanced, connection brokers) to be the floating IP address added in the previous step, in this example 192.168.98.100.

Warning | The default gateway changes must be permanent, otherwise the changes will be lost on reboot and the virtual service(s) will cease to function.

Note | For more information about NAT mode, please refer to Layer 4 NAT Mode.

13. Testing & Verification

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

Testing the Load Balanced Gateway Service
The load balanced Leostream gateway service can be tested by using it.

1. Use SSH to connect to both Leostream gateway hosts as the root user.
2. Execute the command leostream --conn to view current connections.
3. Use a web browser to connect to the Leostream gateway virtual service and log in using appropriate authorised credentials.
4. Select a client to connect to.

5. Open the downloaded file in an RDP client and enter appropriate credentials (if SSO isn’t enabled).

6. A connection should be successfully established to the remote client, via the gateway virtual service configured on the load balancer.
7. On the Leostream gateway hosts, re-execute the command `leostream --conn` and the active connection should be listed.

```
[root@localhost ~]# leostream-gateway --conn
Desktop Port Dport Source address Key
192.168.98.235 3389 3389 192.168.65.185 de8e9319ea66b1dc85ec285f17bb4
```

8. Use a web browser to connect to the Leostream connection broker service (if configured).

9. In the menu on the left, navigate to Resources > Desktops.

10. A Release option should be visible next to the client that has been connected to.

11. Repeat these tests using Leostream connection clients, if applicable.

**Using System Overview**

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the web servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows a DR mode deployment where both Leostream servers are healthy and available to accept connections:
14. 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.

15. Further Documentation


16. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Leostream environments.
17. Appendix

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.

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:

<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</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</td>
<td>Various settings including Internet Proxy, Management Gateway,</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>Firewall connection tracking table size, NIC offloading, SMTP relay,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown</td>
<td>Appliance management lockdown settings</td>
</tr>
<tr>
<td></td>
<td>Wizard</td>
<td></td>
</tr>
</tbody>
</table>

Important

Make sure that if these settings(updates) have been configured on the Primary appliance, they’re also configured on the Secondary appliance.

To add a Secondary node - i.e. create a highly available clustered pair:
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 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 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.

**Note** For details on testing and verifying HA, please refer to Clustered Pair Diagnostics.

### Solving the ARP Problem for Linux

**Method 1 (using iptables)**

You can use iptables (netfilter) on each Real Server to re-direct incoming packets destined for the Virtual Service IP address. To make this permanent, simply add the following command to an appropriate start-up script such as `/etc/rc.local` on each of your Real Servers. If Real Servers are serving multiple VIPs, add additional iptables rules for each VIP.

```
iptables -t nat -A PREROUTING -d <VIP> -j REDIRECT
```

**e.g.**

```
iptables -t nat -A PREROUTING -d 10.0.0.21 -j REDIRECT
```

**Note** Change the IP address to be the same as your Virtual Service.

This means redirect any incoming packets destined for 10.0.0.21 (the Virtual Service) locally, i.e. to the primary address of the incoming interface on the Real Server.

**Note** Method 1 may not always be appropriate if you’re using IP-based virtual hosting on your web server. This is because the iptables rule above redirects incoming packets to the primary address of the incoming interface on the web server rather than any of the virtual hosts that are configured. Where this is an issue, use method 2 below instead.

**Note** Method 1 does not work with IPv6 Virtual Services, use method 2 below instead.

**Method 2 (using arp_ignore sysctl values)**

This is the preferred method as it supports both IPv4 and IPv6. Each Real Server needs the loopback adapter to be configured with the Virtual Services IP address. This address must not respond to ARP requests and the web server
also needs to be configured to respond to this address. To set this up follow steps 1-4 below on each Real Server.

**Step 1 of 4: re-configure ARP on the Real Servers (this step can be skipped for IPv6 Virtual Services)**

To do this add the following lines to /etc/sysctl.conf:

```plaintext
net.ipv4.conf.all.arp_ignore=1
net.ipv4.conf.eth0.arp_ignore=1
net.ipv4.conf.eth1.arp_ignore=1
net.ipv4.conf.all.arp_announce=2
net.ipv4.conf.eth0.arp_announce=2
net.ipv4.conf.eth1.arp_announce=2
```

*Note* | Adjust the commands shown above to suit the network configuration of your servers.

**Step 2 of 4: re-configure DAD on the Real Servers (this step can be skipped for IPv4 Virtual Services)**

To do this add the following lines to /etc/sysctl.conf:

```plaintext
net.ipv6.conf.lo.dad_transmits=0
net.ipv6.conf.lo.accept_dad=0
```

**Step 3 of 4: apply these settings**

Either reboot the Real Server or run the following command to apply these settings:

```
/sbin/sysctl -p
```

**Step 4 of 4: add the Virtual Services IP address to the loopback adapter**

Run the following command for each VIP. To make this permanent, simply add the command to an appropriate startup script such as /etc/rc.local.

```
ip addr add dev lo <IPv4-VIP>/32
```

_for IPv6 addresses use:_

```
ip addr add dev lo <IPv6-VIP>/128
```

*Note* | You can check if this command added the VIP successfully using the command:

```
ip addr ls
```

You can remove the VIP from the loopback adapter using the command:

```
ip addr del dev lo <IPv4-VIP>/32
```
Steps 1, 2 & 3 can be replaced by writing directly to the required files using the following commands (run as root at the command line), this is temporary until the next reboot:

Note

```
echo 1 > /proc/sys/net/ipv4/conf/all/arp_ignore
echo 1 > /proc/sys/net/ipv4/conf/eth0/arp_ignore
echo 1 > /proc/sys/net/ipv4/conf/eth1/arp_ignore
echo 2 > /proc/sys/net/ipv4/conf/all/arp_announce
echo 2 > /proc/sys/net/ipv4/conf/eth0/arp_announce
echo 2 > /proc/sys/net/ipv4/conf/eth1/arp_announce
echo 0 > /proc/sys/net/ipv6/conf/lo/dad_transmits
echo 0 > /proc/sys/net/ipv6/conf/lo/accept_dad
```

Method 3 (using firewalld)

In some newer versions of Linux, iptables is being deprecated in favour of firewalld. The following command can be used on each Real Server to resolve the ARP issue using firewalld:

```
firewall-cmd --permanent --direct --add-rule ipv4 nat PREROUTING 0 -d <VIP> -j REDIRECT
```

E.g.

```
firewall-cmd --permanent --direct --add-rule ipv4 nat PREROUTING 0 -d 10.0.0.50 -j REDIRECT
```

Note | Change the IP address to be the same as your Virtual Service.

To apply the new configuration, reload the firewall rules:

```
firewall-cmd --reload
```

The current permanent configuration will become the new firewalld runtime configuration as well as the configuration at the next system start.
## 18. 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>1 Jan 2021</td>
<td>Initial version</td>
<td></td>
<td>DT, AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>26 May 2022</td>
<td>Added NAT mode deployment method</td>
<td>NAT mode validated as a working deployment method</td>
<td>AH</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.