LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Omnissa Horizon

Version 1.0.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load-balanced Omnissa Horizon (formerly VMware Horizon) environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Omnissa Horizon 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 Omnissa Horizon. For full specifications of available models please refer to https://www.loadbalancer.org/products/enterprise.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

> **Note** The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Omnissa Horizon

- v8 and later

4. Omnissa Horizon

Omnissa Horizon is a virtual desktop infrastructure (VDI) solution that simplifies desktop management and provides users with access to these desktops when needed, from virtually any device, whatever their location.

5. Omnissa Horizon Servers to be Load Balanced

Server	Purpose
Connection Server	Acts as a broker for client connections in Omnissa Horizon 8 environments. Horizon Connection Server authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical PC, or Microsoft RDS host.
Unified Access Gateway (UAG)	Enables secure remote access from an external network.

6. Omnissa Horizon Protocols

When an Omnissa Horizon Client user connects to a Horizon environment, several different protocols are used. The first connection is always the primary XML-API protocol over HTTPS. Following successful authentication, one or more secondary protocols are also made.

6.1. Primary Horizon Protocol (Phase 1)

The user enters a hostname at the Horizon Client and this starts the primary Horizon protocol. This is a control protocol for authentication, authorization and session management. It uses XML structured messages over HTTPS. This protocol is sometimes known as the Horizon XML-API control protocol. In a load balanced environment, the load balancer distributes client connections across the available set of UAGs.

6.2. Secondary Horizon Protocols (Phase 2)

After the Horizon Client has established secure communication to one of the UAG appliances, the user authenticates. If this authentication attempt is successful, then one or more secondary connections are made from the Horizon client. These secondary connections can include:

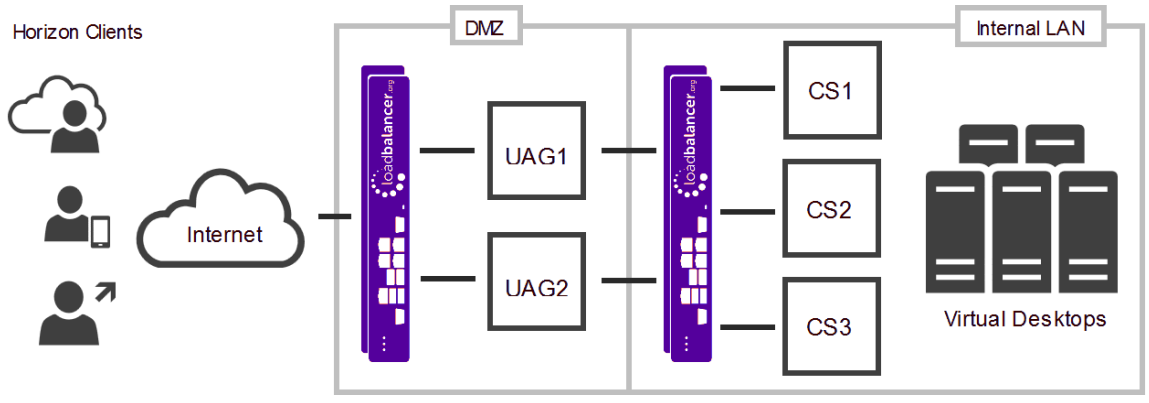
- HTTPS Tunnel used for encapsulating TCP protocols such as RDP, MMR/CDR and the client framework channel (TCP 443)
- Blast display protocol (TCP/UDP 443 & TCP/UDP 8443)
- PCoIP display protocol (TCP/UDP 4172)

These secondary Horizon protocols must be routed to the same UAG appliance to which the primary Horizon protocol was routed. The reason for this is so that UAG can authorize the secondary protocols based on the authenticated user session. If the secondary protocols were to be misrouted to a different UAG appliance to the primary protocol one, they would not be authorized and would therefore be dropped in the DMZ and the connection would fail.

7. Load Balancing Omnissa Horizon

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

The diagram below illustrates where the load balancers are positioned in a typical deployment.



> **Note** We recommend that a clustered pair of load balancers is deployed rather than a single appliance to avoid introducing a single point of failure.

7.1. Port Requirements

The following table shows the ports that are load balanced:

Port	Transport Protocol	Use
443	TCP	Primary Horizon Protocol / HTTPS Tunnel
443	TCP & UDP	Blast
4172	TCP & UDP	PCoIP
8443	TCP & UDP	Blast

> **Note** Some of the above ports may not be used in all scenarios. For simplicity when configuring the load balancer and to ensure all scenarios are covered, all ports are included.

7.2. Persistence (aka Server Affinity)

7.2.1. External Clients

Source IP address or cookie based persistence can be used to ensure all primary protocol connections are handled by the same UAG. For simplicity, source IP address persistence is recommended where possible. Typically, the only time source IP persistence is not appropriate is when clients are located behind a NAT device that hides their IP addresses. Secondary protocol connections must be handled by the same UAG to which the primary protocol was routed. This can be achieved in various ways as described in Load Balancer Deployment Options: External Clients.

7.2.2. Internal Clients

Source IP address or cookie based persistence can be used to ensure all primary protocol connections are handled by the same Connection Server. For simplicity, source IP address persistence is recommended where possible. Typically, the only time source IP persistence is not appropriate is when clients are located behind a NAT device that hides their IP addresses. Secondary protocol connections are direct from client to Connection Server.

7.3. SSL Certificates

Wildcard certificates and SAN based certificates are supported for Omnissa Horizon. In this guide, the SSL certificate was obtained from an internal CA. The certificate should include the FQDNs used by clients and by the Horizon components, for example the external VIP FQDN, internal VIP FQDN, Connection Server FQDN, and UAG FQDNs.

In the lab used to create this guide, a wildcard certificate for ***.ohlab.local** was issued by OHLAB-CA and used for the load balancer, Connection Server, and UAGs.

7.4. SSL Offload

Terminating SSL on the load balancer is only necessary when using cookie based persistence for the primary protocol connections. Cookie based persistence is only needed when source IP address persistence cannot be used due to inline NAT/proxy devices hiding client source IP addresses. If SSL offload is used, the load balancer and the UAGs ***must*** have the same certificate.

7.5. Load Balancer Deployment Modes

The primary protocol is TCP/HTTPS based, so either layer 7 or layer 4 methods can be used. The secondary protocols use both TCP & UDP so only layer 4 methods are supported. Layer 4 NAT mode and layer 7 SNAT mode are used for the configurations presented in this guide.

> **Note** Layer 4 DR mode is not supported for UAG. This is because UAG is a hardened appliance based on Linux which has been locked down by Omnissa. This means that modifying the UAGs to solve the ARP issue becomes more complex and may cause unforeseen issues.

7.6. Server Health Checks

The load balancer is configured to check the health of each Connection Server and UAG by periodically sending an HTTPS **GET /favicon.ico** request. It will perform this HTTPS GET and expect a "**200 OK**" response. If it receives a response other than "**200 OK**" or doesn't get any response, that server will be marked as down and will not attempt to route client requests to it. It will continue to poll so that it can detect when it is available again.

8. Load Balancer Deployment Options

The load balancer can be configured in various ways to support internal and external clients.

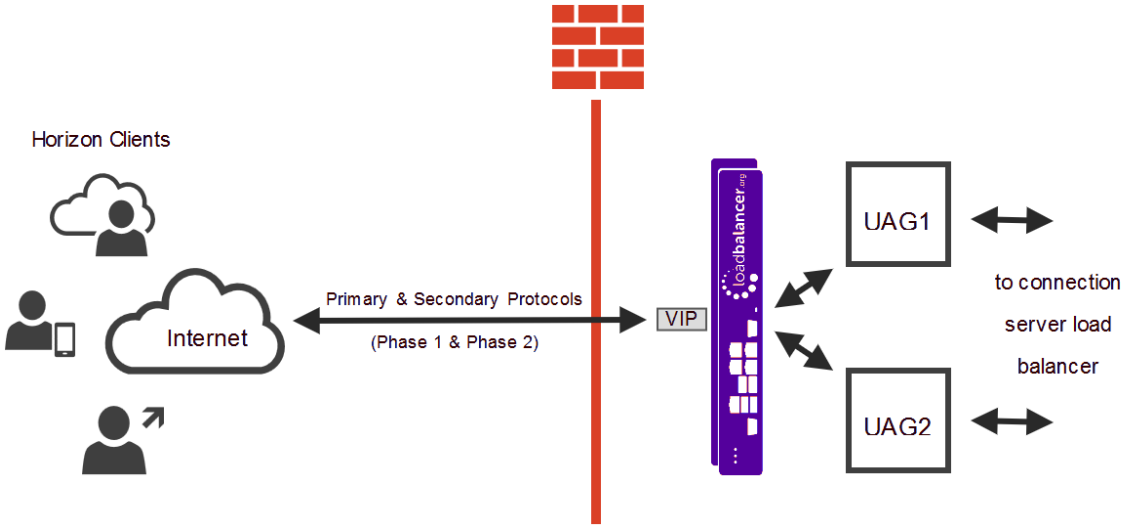
8.1. External Clients

As explained in Secondary Horizon Protocols (Phase 2) the key requirement for external clients is that the secondary protocols must be sent to the same UAG as the primary protocol. This guide presents 3 options to achieve this. These are explained below.

8.1.1. External Clients – Option 1

The load balancer uses a single VIP configured with source IP address persistence to load balance the primary protocol to one of the UAGs. The client connection URLs on each UAG (Option 1: UAG Configuration) are configured so that secondary protocols are also sent to the VIP for load balancing to the same UAG.

This option is recommended for all environments where source IP address persistence is possible. Where it's not possible (typically due to in-line NAT devices hiding client source IP addresses), then either option 2 or option 3 should be used.



Key Points

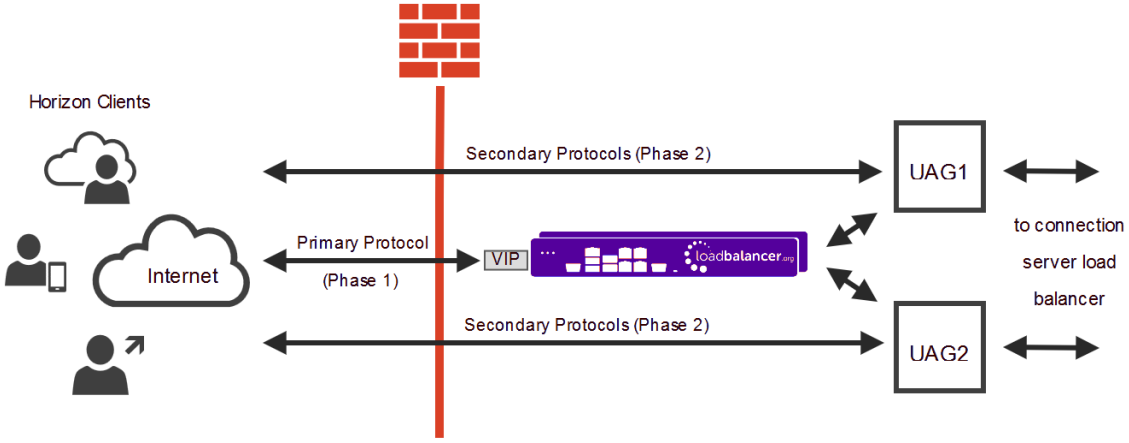
- Requires a single public IP address.
- All traffic passes via the load balancer.

Notes

1. The load balancer requires one network interface.
2. The UAGs are configured with 2 NICs.
3. The VIP is configured in Layer 4 NAT mode using source IP persistence.
4. Return traffic must pass back via the load balancer for layer 4 NAT mode to operate. Set the default gateway on each UAG to an address on the load balancer. For a clustered pair, this should be a Floating IP address to allow failover.
5. The default gateway of the load balancer is the external firewall.
6. Please refer to Configuring for External Clients: Option 1 for UAG and load balancer configuration guidance.

8.1.2. External Clients – Option 2

The load balancer uses a single VIP configured with either source IP address or cookie persistence to load balance the primary protocol to one of the UAGs. The client connection URLs on each UAG (Option 2: UAG Configuration) are configured so that secondary protocols are sent directly to the same UAG, bypassing the load balancer.



Key Points

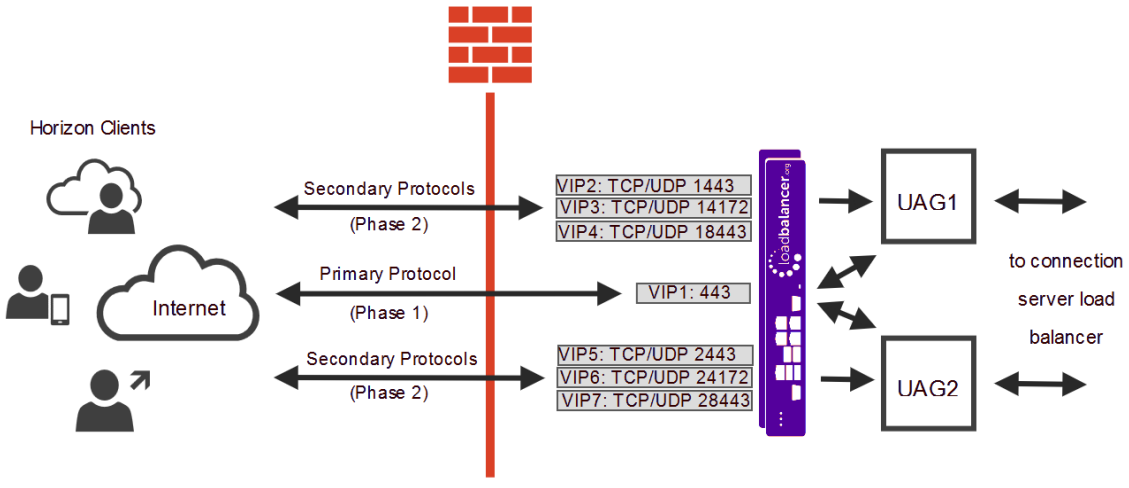
- Requires multiple public IP addresses – one for the VIP, one for each UAG.
- Only the primary protocol is load balanced, secondary protocols go direct to the UAGs.

Notes

1. The load balancer requires one network interface.
2. The UAGs are configured with 2 NICs.
3. The VIP is configured in Layer 7 SNAT mode using either source IP address or cookie based persistence.
4. The default gateway of the UAGs is the external firewall.
5. The default gateway of the load balancer is the external firewall.
6. Please refer to Configuring for External Clients: Option 2 for UAG and load balancer configuration guidance.

8.1.3. External Clients – Option 3

The load balancer uses one VIP configured with either source IP address or cookie persistence to load balance the primary protocol to one of the UAGs. The client connection URLs on each UAG (Option 3: UAG Configuration) are configured so that secondary protocols are sent to the same UAG via additional VIPs on unique port numbers.



Key Points

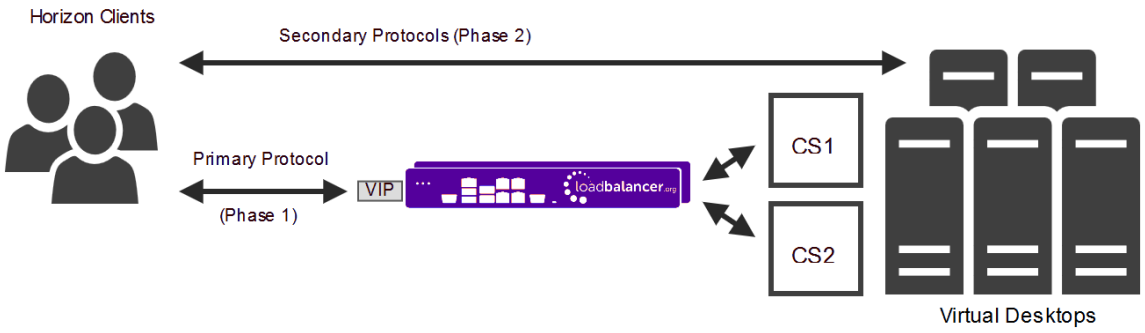
- Requires a single public IP address (VIP1 – VIP7 use the same IP address).
- All traffic passes via the load balancer.
- Uses non standard ports for external client connections (example ports are shown, any appropriate ports can be used).

Notes

1. The load balancer requires one network interface.
2. The UAGs are configured with 2 NICs.
3. VIP1 is configured in Layer 7 SNAT mode using either source IP address or cookie based persistence.
4. VIPs 2 to 7 are configured in Layer 4 NAT mode.
5. The default gateway of the UAGs must be the load balancer, for a clustered pair of load balancers (Primary & Secondary) this should be a floating IP address to allow failover.
6. The default gateway of the load balancer is the external firewall.
7. Please refer to Configuring for External Clients: Option 3 for UAG and load balancer configuration guidance.

8.2. Internal Clients

Internal clients connect to the Connection Server VIP on the LAN. Secondary protocols go direct to the virtual desktops unless Connection Server gateways are explicitly enabled.



Key Points

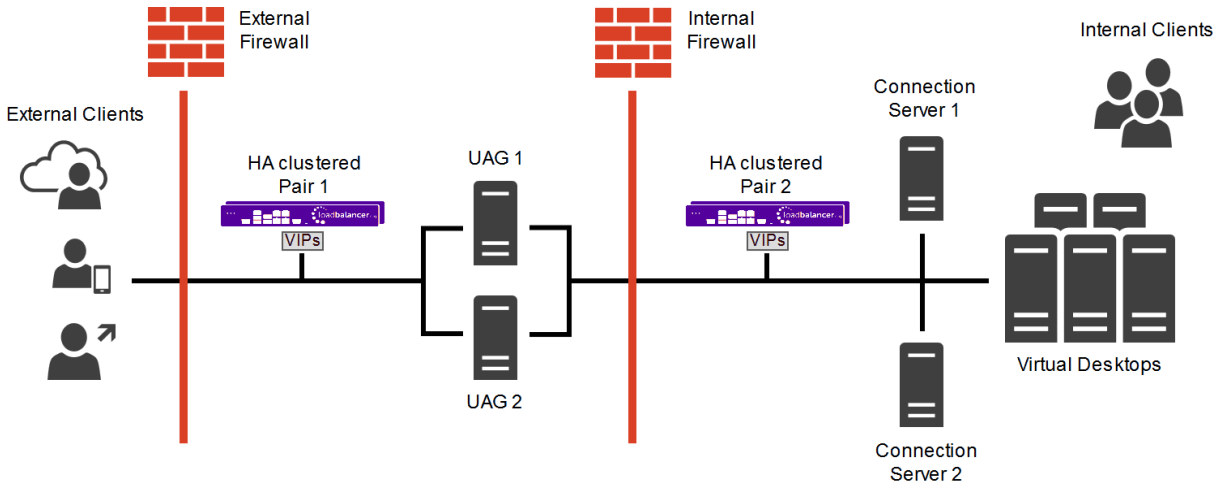
- Only the primary protocol is load balanced, secondary protocols go direct to the virtual desktops.

Notes

1. The load balancer requires one network interface.
2. The VIP is configured in Layer 7 SNAT mode using either source IP address or cookie based persistence.
3. Please refer to Configuring for Internal Clients for server and load balancer configuration guidance.

9. Network Topology Used for this Guide

The diagram below shows the network topology used for this deployment guide. Clustered Pair 1 in the DMZ is used to load balance external clients connecting to the UAGs, and clustered Pair 2 on the LAN is used to load balance internal clients connecting to the Connection Servers.



10. Loadbalancer.org Appliance – the Basics

10.1. Virtual Appliance

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.

Note	The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

Note	Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

Note	The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

10.2. Initial Network Configuration

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

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

10.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

> **Note** There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

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

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

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

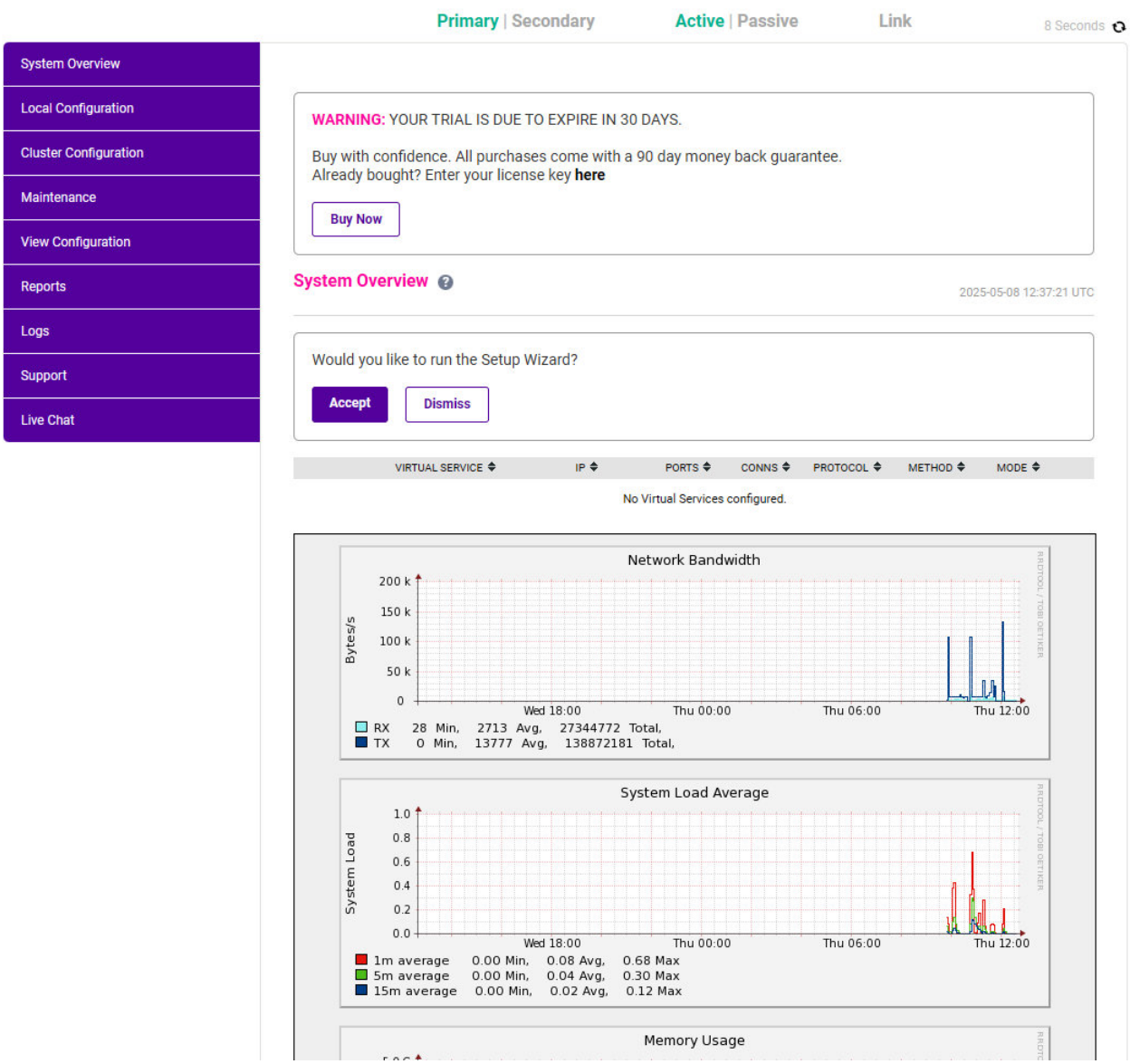
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

2. Log in to the WebUI using the following credentials:

   Username: loadbalancer
   Password: <configured-during-network-setup-wizard>

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

   Once logged in, the WebUI will be displayed as shown below:



3. You'll be asked if you want to run the Setup Wizard. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.

> **Note** The Setup Wizard can only be used to configure Layer 7 services.

10.3.1. Main Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs
Maintenance - Perform maintenance tasks such as service restarts and creating backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links

Live Chat - Start a live chat session with one of our Support Engineers

10.4. Appliance Software Update

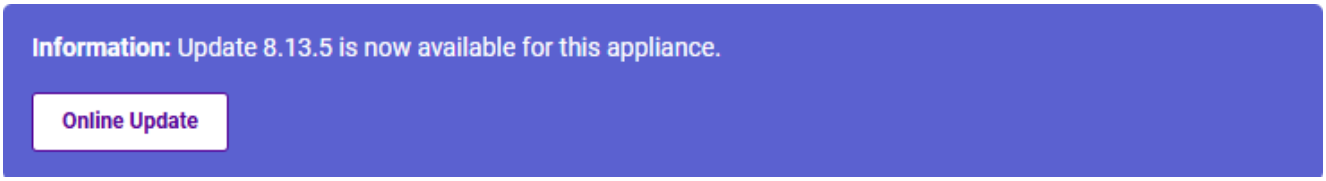
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **Note** For full details, please refer to Appliance Software Update in the Administration Manual.

> **Note** Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

10.4.1. Online Update

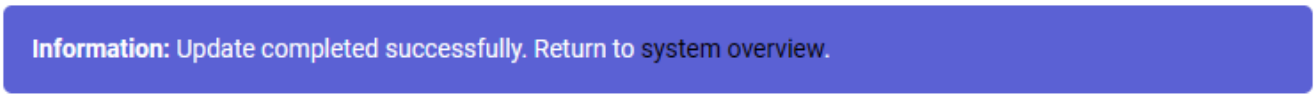
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

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

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



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

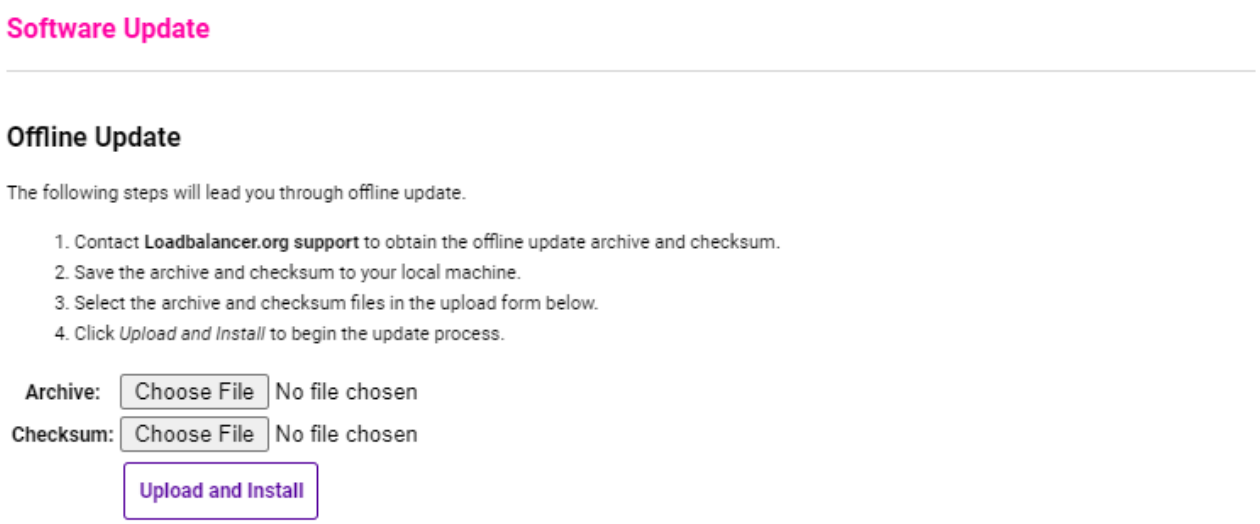
10.4.2. Offline Update

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

To check for the latest version, please refer to our product roadmap page available here. To obtain the latest offline update files contact support@loadbalancer.org.

To perform an offline update:

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



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

10.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

Protocol	Port	Purpose
TCP	22	SSH
TCP & UDP	53	GSLB
TCP & UDP	123	NTP
TCP & UDP	161	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9000	Gateway service for ADC Portal comms
TCP	9080	WebUI - HTTP (disabled by default)
TCP	9081	Nginx fallback server
TCP	9443	WebUI - HTTPS
TCP	25565	Shuttle service for ADC Portal comms

> **Note** All ports listed above except port 123 (NTP) can be changed if required.

- To change the port used for heartbeat, refer to Configuring High Availability
- To change the port used for HAProxy replication, refer to Layer 7 - Advanced Configuration
- To change other ports, refer to Service Socket Addresses

10.6. HA Clustered Pair Configuration

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

11. Configuring for External Clients

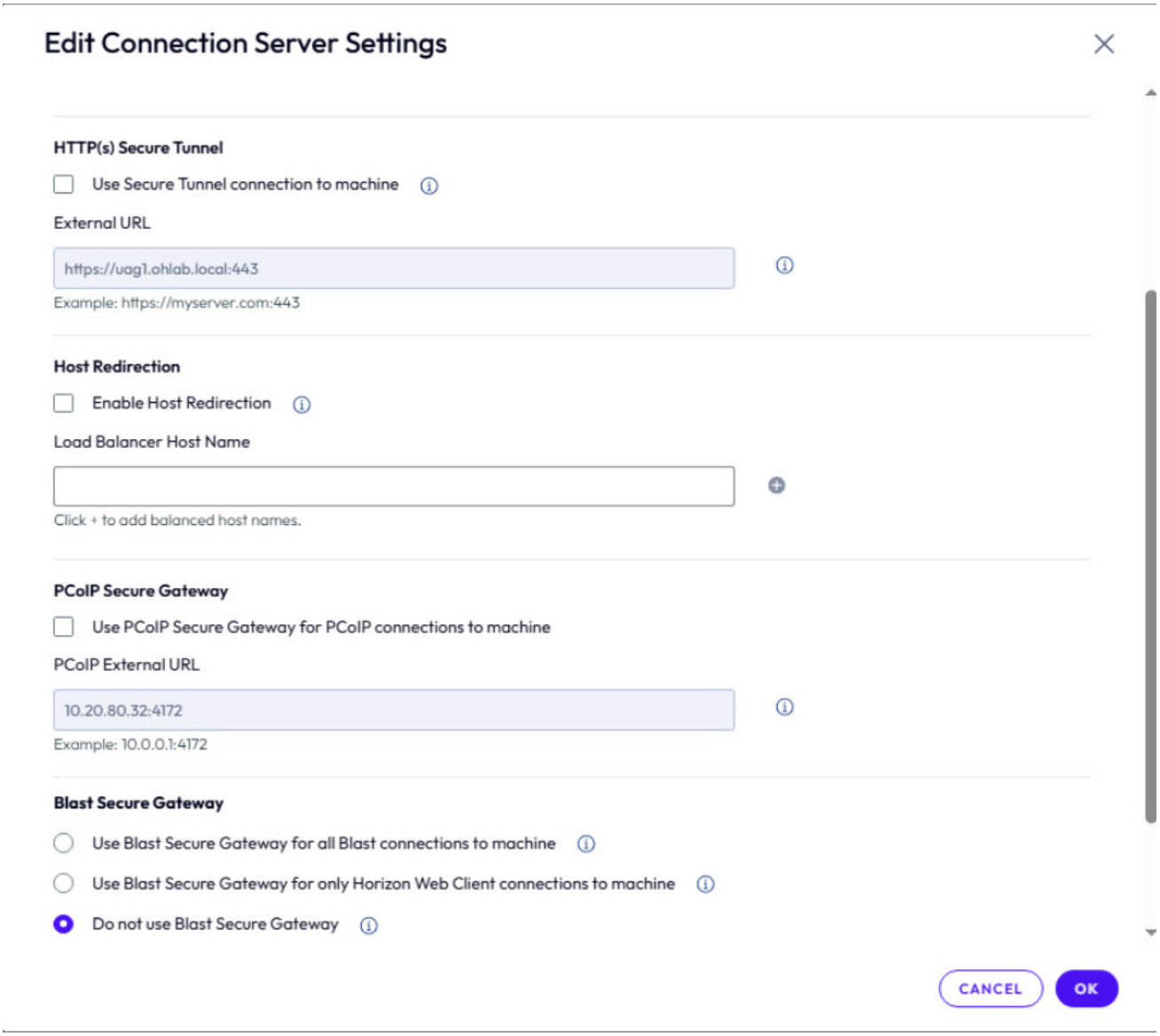
11.1. Option 1

The configuration presented in this section relates to the topology described in External Clients – Option 1.

11.1.1. Connection Server Configuration

For each Connection Server, complete steps 1 & 2:

Step 1 – Configure General Settings



Un-check the 3 boxes as shown above. These options are not required when using UAG. These options only need to be set when a legacy Security Server is paired with the Connection Server.

Step 2 - Enable HTML Access via the Load Balancer

Connection Servers that are directly behind a load balancer or load-balanced gateway must know the address by which browsers will connect to the load balancer when users use HTML Access. On each Connection Server complete the following steps:

1. Create or edit the **locked.properties** file in the SSL gateway configuration folder:

   ```
   C:\Program Files\Omnissa\Horizon\Server\sslgateway\conf\locked.properties
   ```

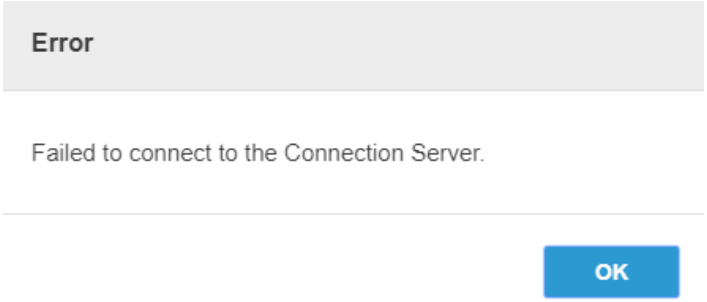
2. Add the **balancedHost** property and set it to the address that users type for HTML Access. For example, if users type **https://horizon.example.com**, add the following entry to the file:

   `balancedHost=horizon.example.com` (Note: "balancedHost" is case sensitive!)

3. Save the **locked.properties** file and restart the Connection Server service to apply the changes.

> **Note** It's recommended that connection origin checks should be enabled for production environments. Adding `allowUnexpectedHost=true` to `locked.properties` should be reserved for temporary testing only.

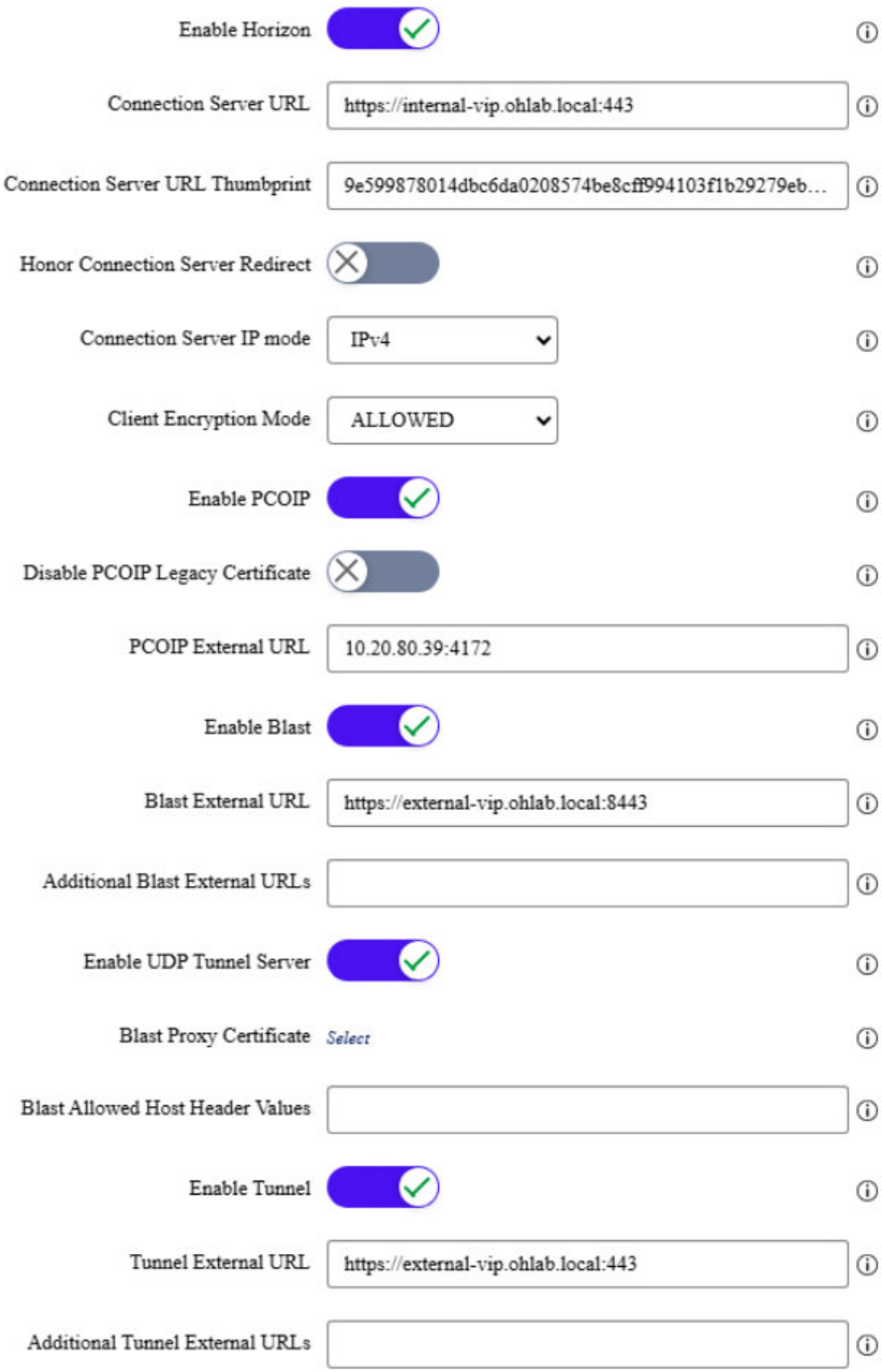
If the above steps are not completed, you'll receive the following error when connecting via a browser:



11.1.2. UAG Configuration

For each UAG, complete steps 1 & 2:

Step 1 – Configure URLs



The various URLs must be configured as shown above.

To access the UAG Web Interface use: **https://<uag-ip>:9443/admin**.

1. Configure the Connection Server URL to be the VIP address of the load balanced Connection Servers on the internal load balancer, in this guide **https://internal-vip.ohlab.local:443**.
2. Configure the ***PCoIP External URL*** to be the public IP address of the VIP on the load balancer, in this guide **10.20.80.39:4172**.
3. Configure the ***Blast External URL*** to be the FQDN that external clients use to connect, in this guide

https://external-vip.ohlab.local:8443. This should resolve to the public IP address of the VIP on the load balancer.

4. Configure the *Tunnel External URL* to be the FQDN that external clients use to connect, in this guide **https://external-vip.ohlab.local:443**. This should resolve to the public IP address of the VIP on the load balancer.

> **Note** Steps 2 – 4 above illustrate that clients connect via the load balancer for all secondary protocols.

Step 2 - Configure the Default Gateway on the UAGs

> **Note** Return traffic MUST pass back via the load balancer for layer 4 NAT mode to operate.

Either:

1. Set the default gateway on each UAG to be an address on the load balancer. This address should be a floating IP address to enable failover when using a clustered pair as described in the *Load Balancer Configuration* section (Step 2) below.
2. If the UAG's default route must remain as the firewall, add static routes on each UAG with next hop = the floating IP, so return traffic still passes via the load balancer.

> **Note** The default gateway can be set at UAG deployment, or later by using the UAG's Admin UI as mentioned here.

11.1.3. Load Balancer Configuration

The load balancer is used for both the primary and secondary protocols.

Port Requirements

The following table shows the ports that are load balanced:

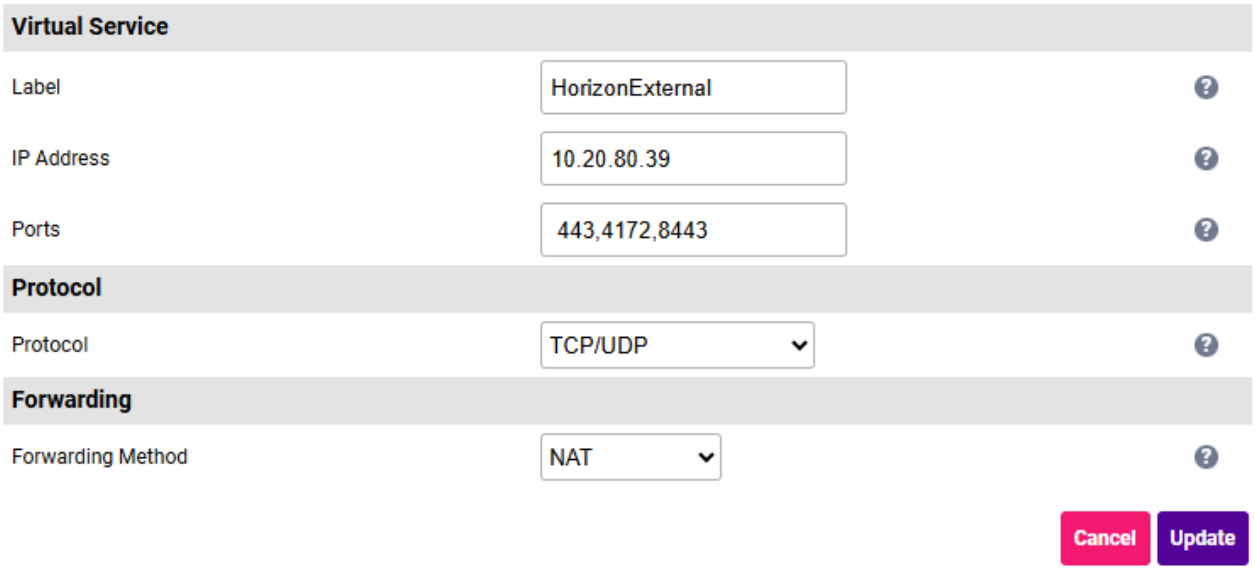
Port	Transport Protocol	Use
443	TCP	Primary Horizon Protocol / HTTPS Tunnel
443	TCP & UDP	Blast
4172	TCP & UDP	PCoIP
8443	TCP & UDP	Blast

Step 1 - Configure the Virtual Service (VIP) & Real Servers (RIPs)

Configure the Virtual Service:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Service* and click **Add a New Virtual Service**.

2. Enter the following details:



3. Enter an appropriate label (name) for the VIP, e.g. **HorizonExternal**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **10.20.80.39**.
5. Set the *Virtual Service Ports* field to **443,4172,8443**.
6. Set the *Protocol* to **TCP/UDP**.
7. Set the *Forwarding Method* to **NAT**.
8. Click **Update**.
9. Now click **Modify** next to the newly created VIP.
10. Ensure *Persistence* is enabled and set *Persistence Timeout* to **36000** (i.e. 10 hour).

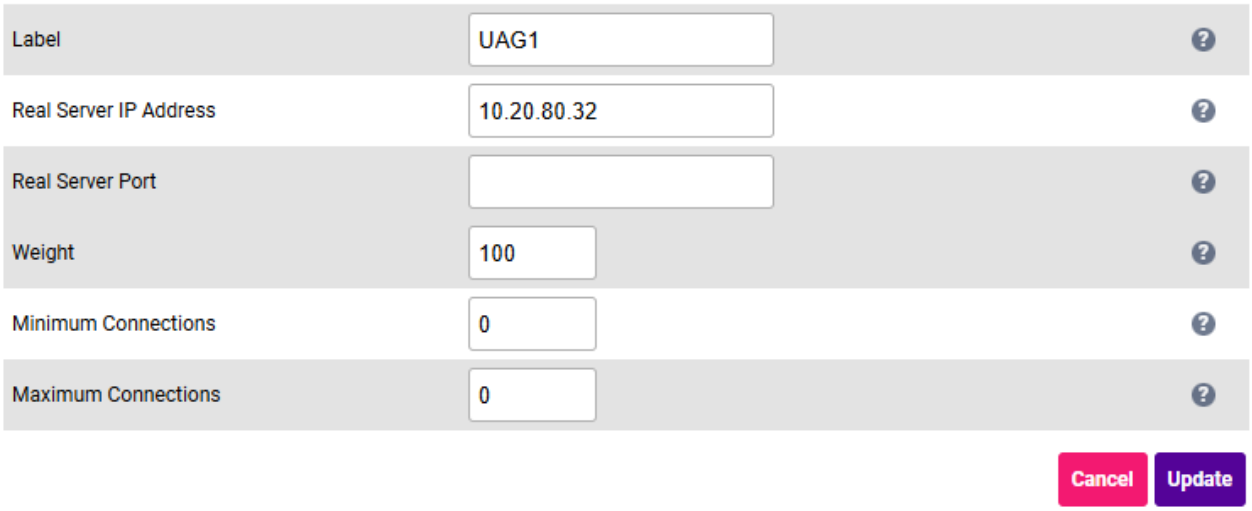
> **Note** The value set should match the *Forcibly disconnect users* setting under Global Settings for the Connection Server (the default value for this is 10 hours).

11. Set *Check Type* to **Negotiate**.
12. Set *Check Port* to **443**.
13. Set *Protocol* to **HTTPS**.
14. Set *Request to send* to **/favicon.ico**.
15. Leave *Response expected* blank.
16. Click **Update**.

Configure the Real Servers:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a New Real Server** next to the newly created VIP.

2. Enter the following details:



3. Enter an appropriate label for the RIP, e.g. **UAG1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **10.20.80.32**.
5. Leave the *Real Server Port* field blank.
6. Click **Update**.
7. Repeat the above steps to add your other UAG(s).

Step 2 - Add a Floating IP Address to the Load Balancer to be used as the UAGs Default Gateway

Using the WebUI option: *Cluster Configuration > Floating IPs* add a Floating IP that can be used as the default gateway for the UAGs. Using a floating IP will ensure that the IP address is available when a clustered pair is used, and a failover to the Secondary has occurred. This floating IP should be an additional IP address that is dedicated to this purpose.

Step 3 - Configure the Default Gateway on the Load Balancer

Using the WebUI option: *Local Configuration > Routing* set the default gateway to be the internal interface of the external firewall, e.g. **10.20.80.254**.

Step 4 - Configure HTTP to HTTPS Redirection

If required, the load balancer can be configured to automatically redirect clients who attempt to connect to **http://<Horizon URL>** to **https://<Horizon URL>.**

When SSL is terminated on the real servers, a separate VIP is required to handle this. For details on setting this up, please refer to Configuring an HTTP to HTTPS redirect.

11.2. Option 2

The configuration presented in this section relates to the topology described in External Clients – Option 2.

11.2.1. Connection Server Configuration

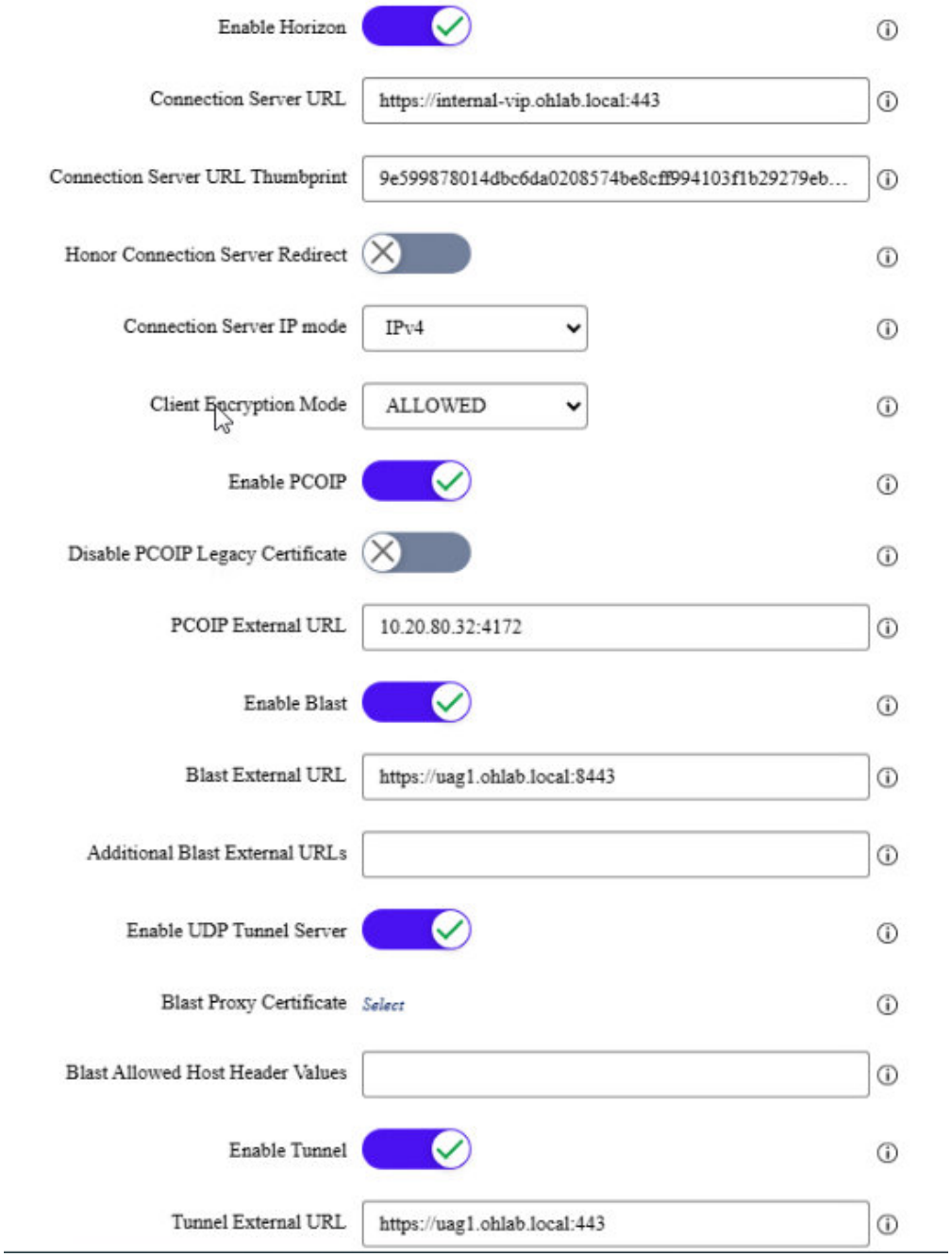
Follow the same Connection Server configuration steps as per option 1 - see Option 1 - Connection Server

Configuration.

11.2.2. UAG Configuration

For each UAG, complete steps 1 & 2:

Step 1 – Configure URLs



The various URLs must be configured as shown above.

To access the UAG Web Interface use: **https://<uag-ip>:9443/admin**.

1. Configure the *Connection Server URL* to be the VIP FQDN (or IP) of the load balanced Connection Servers on the internal load balancer, in this guide **https://internal-vip.ohlab.local:443**.

2. Configure the *PCoIP External URL* to be the public IP address of the UAG, in this guide **10.20.80.32:4172**.
3. Configure the *Blast External URL* to be the FQDN of the UAG, in this guide **https://uag1.ohlab.local:8443**. This should resolve to the public IP address of the UAG.
4. Configure the *Tunnel External URL* to be the FQDN of the UAG, in this guide **https://uag1.ohlab.local:443**. This should resolve to the public IP address of the UAG.

> **Note** Steps 2 – 4 above illustrate that clients connect directly to the UAGs for all secondary protocols, bypassing the load balancer. Using FQDNs for steps 3 & 4 rather than IP addresses avoids certificate related errors. For a SAN certificate, ensure that you include the FQDN of each UAG.

Step 2 - Configure the default gateway on the UAGs

1. Set the default gateway on each UAG to be the external firewall.

> **Note** The default gateway can be set at UAG deployment, or later by using the UAG's Admin UI.

11.2.3. Load Balancer Configuration

The load balancer is used for the primary protocol only, secondary protocols pass directly from client to the UAGs.

Port Requirements

The following table shows the ports that are load balanced:

Port	Transport Protocol	Use
443	TCP	Primary Horizon Protocol / HTTPS Tunnel

Step 1 - Configure the Virtual Service (VIP) & Real Servers (RIPs)

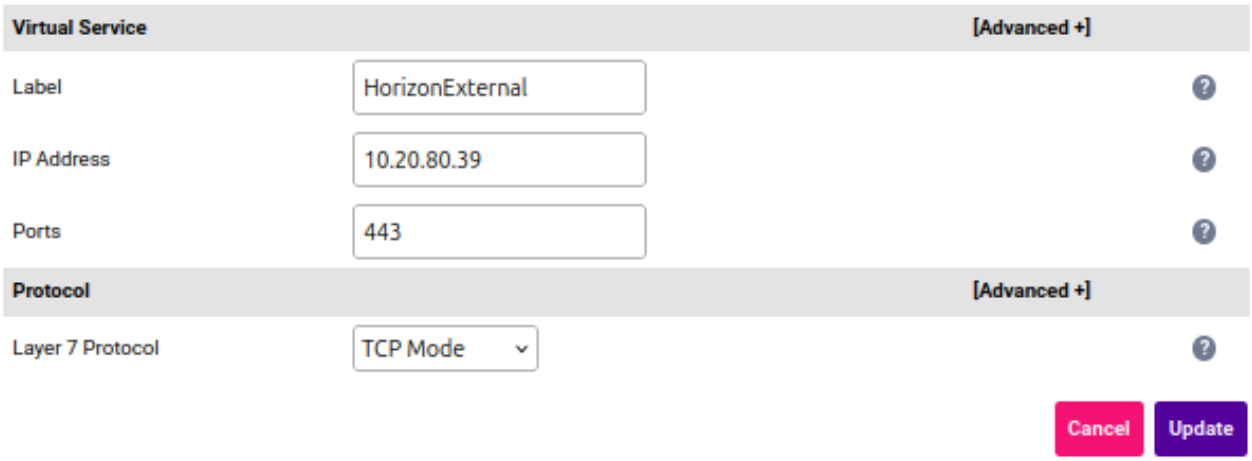
Source IP address persistence is recommended if there are no inline NAT devices between the clients and the VIP. To configure the load balancer using source IP persistence, follow the steps in Using Source IP Persistence (External Clients).

If there are inline NAT devices, cookie based persistence can be used. To configure the load balancer using cookie persistence, follow the steps in Using Cookie Persistence (External Clients).

Using Source IP Persistence (External Clients)

Configure the Virtual Service:

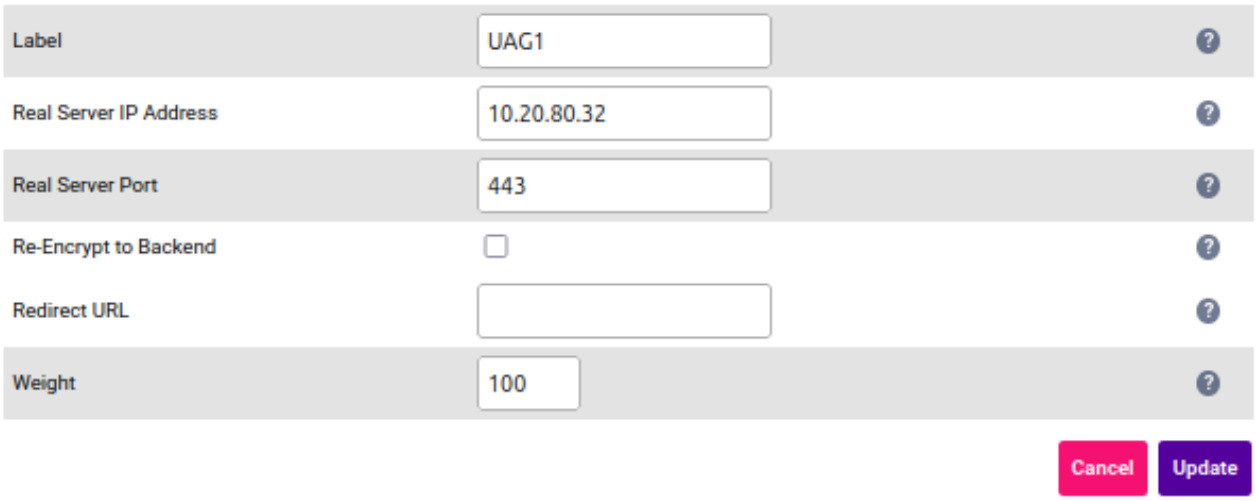
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**.
2. Enter the following details:



3. Enter an appropriate label for the VIP, e.g. **HorizonExternal**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **10.20.80.39**.
5. Set the *Virtual Service Ports* field to **443**.
6. Set *Layer 7 Protocol* to **TCP Mode**.
7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Set *Health Checks* to **Negotiate HTTPS (GET)**.
10. Set *Check Port* to **443**.
11. Set *Request to send* to **/favicon.ico**.
12. Leave *Response expected* blank.
13. Click **Update**.

Configure the Real Servers:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a New Real Server** next to the newly created VIP.
2. Enter the following details:

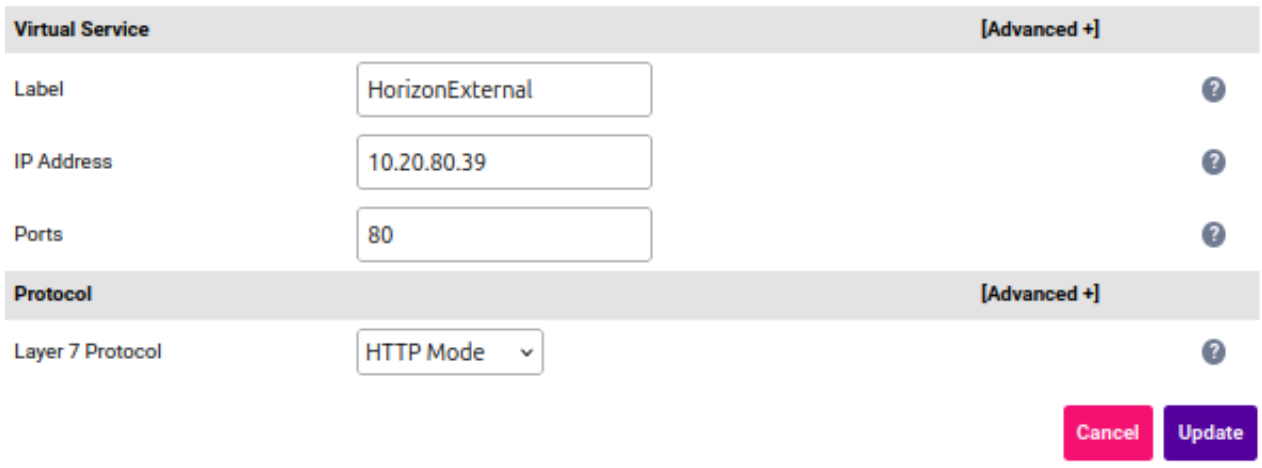


3. Enter an appropriate label for the RIP, e.g. **UAG1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **10.20.80.32**.
5. Change the *Real Server Port* field to **443**.
6. Click **Update**.
7. Repeat the above steps to add your other UAG(s).

Using Cookie Persistence (External Clients)

Configure the Virtual Service:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**.
2. Enter the following details:

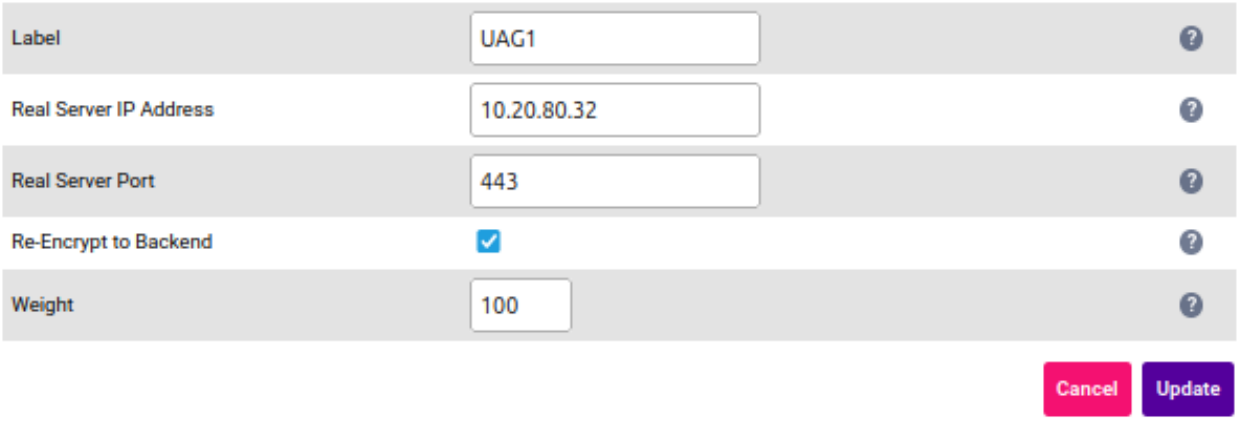


3. Enter an appropriate label for the VIP, e.g. **HorizonExternal**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **10.20.80.39**.
5. Set the *Virtual Service Ports* field to **80**.
6. Leave *Layer 7 Protocol* set to **HTTP Mode**.

7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Set *Health Checks* to **Negotiate HTTP (GET)**.
10. Set *Check Port* to **80**.
11. Set *Request to send* to **/favicon.ico**.
12. Leave *Response expected* blank.
13. Click **Update**.

Configure the Real Servers:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a New Real Server** next to the newly created VIP.
2. Enter the following details:



3. Enter an appropriate label for the RIP, e.g. **UAG1**.
4. Set the *Real Server IP Address* field to the required IP address, e.g. **10.20.80.32**.
5. Set the *Real Server Port* field to **443**.
6. Enable (check) *Re-Encrypt to Backend*.
7. Click **Update**.
8. Repeat the above steps to add your other UAG(s).

Configure SSL Termination – Upload the SSL certificate:

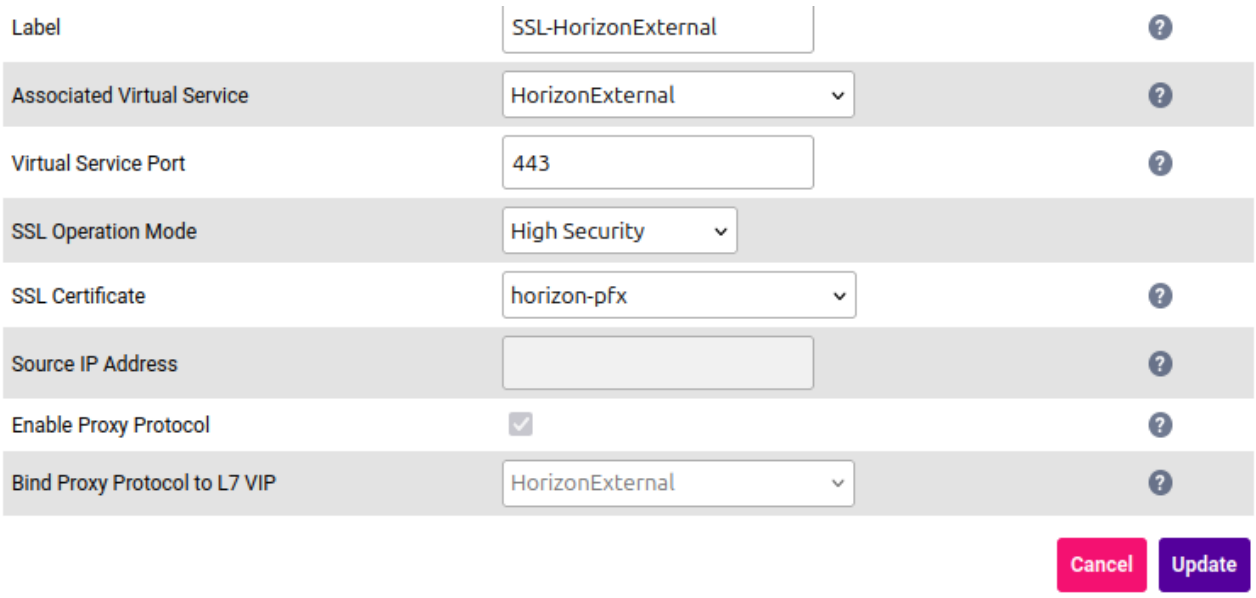
1. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificate*.
2. Click **Add a new SSL Certificate**.
3. Select *Upload prepared PEM/PFX file*.
4. Enter a suitable label (name) for the certificate, e.g. **Horizon**.
5. Browse to the relevant Horizon PFX certificate file.

> **Note** When SSL re-encryption (SSL bridging) is used, the UAG & load balancer ***must*** have the same SSL certificate.

6. Enter the relevant *PFX File Password*.
7. Click **Add Certificate**.

Configure SSL Termination – Create the SSL Virtual Service:

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Termination* and click **Add a new Virtual Service**.



2. Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **HorizonExternal**.

> **Note** Once the VIP is selected, the *Label* field will be auto-populated with **SSL-HorizonExternal**. This can be changed if preferred.

3. Leave *Virtual Service Port* set to **443**.
4. Leave *SSL Operation Mode* set to **High Security**.
5. Select the SSL certificate uploaded previously using the *SSL Certificate* drop-down
6. Click **Update**.

Step 2 - Configure HTTP to HTTPS Redirection

If required, the load balancer can be configured to automatically redirect clients who attempt to connect to **http://<Horizon URL>** to **https://<Horizon URL>**.

- When using cookie based persistence (SSL is terminated on the load balancer), this can be configured by modifying the *HorizonExternal* VIP and enabling the *Force to HTTPS* option.
- When using source IP persistence (SSL is terminated on the real servers), a separate VIP is required to handle this. For details on setting this up, please refer to Configuring an HTTP to HTTPS redirect.

Step 3 - Configure the Default Gateway on the Load Balancer

Using the WebUI option: ***Local Configuration > Routing*** set the default gateway to be the internal interface of the external firewall, e.g. **10.20.80.254**.

Step 4 – Reload Services

To apply the new settings, HAProxy and STunnel (if using SSL offload) must both be reloaded. This can be done using the buttons in the "Commit changes" box at the top of the screen or by using the ***Restart Services*** menu option:

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

11.3. Option 3

The configuration presented in this section relates to the topology described in External Clients – Option 3.

11.3.1. Connection Server Configuration

Follow the same Connection Server configuration steps as per option 1 - see Option 1 - Connection Server Configuration.

11.3.2. UAG Configuration

For each UAG, complete steps 1,2 & 3:

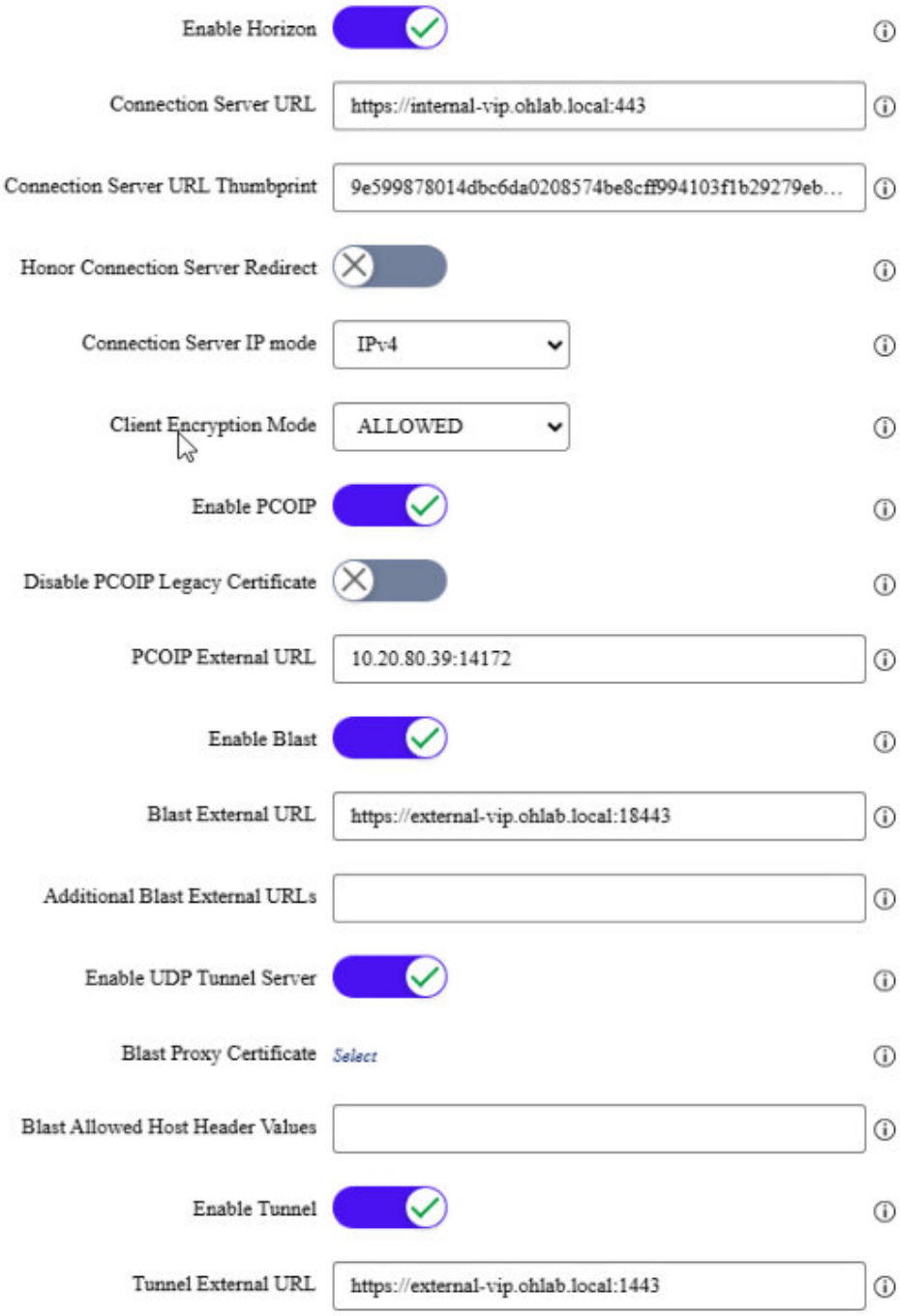
Step 1 - Decide on the External Ports for the VIPs

The table below shows one possible option for the external ports for the VIPs used for the secondary protocols.

VIP/External Port	Primary/Secondary	Protocol	VIP Name	Real Server IP/Port
UAG 1 & 2 – Primary Protocol				
10.20.80.39:443	Primary	TCP	HorizonExternal	10.20.80.32:443 10.20.80.33:443
UAG1 – Secondary Protocols				
10.20.80.39:1443	Secondary	TCP/UDP	UAG1-443	10.20.80.32:443
10.20.80.39:14172	Secondary	TCP/UDP	UAG1-PCoIP	10.20.80.32:4172
10.20.80.39:18443	Secondary	TCP/UDP	UAG1-Blast	10.20.80.32:8443
UAG2 – Secondary Protocols				
10.20.80.39:2443	Secondary	TCP/UDP	UAG2-443	10.20.80.33:443
10.20.80.39:24172	Secondary	TCP/UDP	UAG2-PCoIP	10.20.80.33:4172

VIP/External Port	Primary/Secondary	Protocol	VIP Name	Real Server IP/Port
10.20.80.39:28443	Secondary	TCP/UDP	UAG2-Blast	10.20.80.33:8443

Step 2 – Configure URLs



The various URLs must be configured as shown above.

To access the UAG Web Interface use: **https://<uag-ip>:9443/admin**.

1. Configure the Connection Server URL to be the VIP address of the load balanced Connection Servers on the internal load balancer, in this guide **https://internal-vip.ohlab.local:443**.
2. Configure the *PCoIP External URL* to be the public IP address of the VIP on the load balancer, in this guide **10.20.80.39:14172**.

3. Configure the *Blast External URL* to be the FQDN that external clients use to connect, in this guide **https://external-vip.ohlab.local:18443**. This should resolve to the public IP address of the VIP on the load balancer.
4. Configure the *Tunnel External URL* to be the FQDN that external clients use to connect, in this guide **https://external-vip.ohlab.local:1443**. This should resolve to the public IP address of the VIP on the load balancer.

> **Note** Steps 2 – 4 above illustrate that clients connect to the VIP on the load balancer for all secondary protocols.

Step 3 - Configure the default gateway on the UAGs

> **Note** Return traffic MUST pass back via the load balancer for layer 4 NAT mode to operate.

1. Set the default gateway on each UAG to be an address on the load balancer. This address should be a floating IP address to enable failover when using a clustered pair as described in Step 3 below.

> **Note** The default gateway can be set at UAG deployment, or later by using the UAG's admin UI.

11.3.3. Load Balancer Configuration

The load balancer is used for both the primary & secondary protocols.

Step 1 - Configure the Virtual Service (VIP) & Real Servers (RIPs) for the Primary Protocol

Source IP address persistence is recommended if there are no inline NAT devices between the clients and the VIP. To configure the load balancer using source IP persistence, follow the same configuration steps as per option 2 - see Using Source IP Persistence (External Clients).

If there are inline NAT devices, cookie based persistence can be used. To configure the load balancer using cookie persistence, follow the same configuration steps as per option 2 - see Using Cookie Persistence (External Clients).

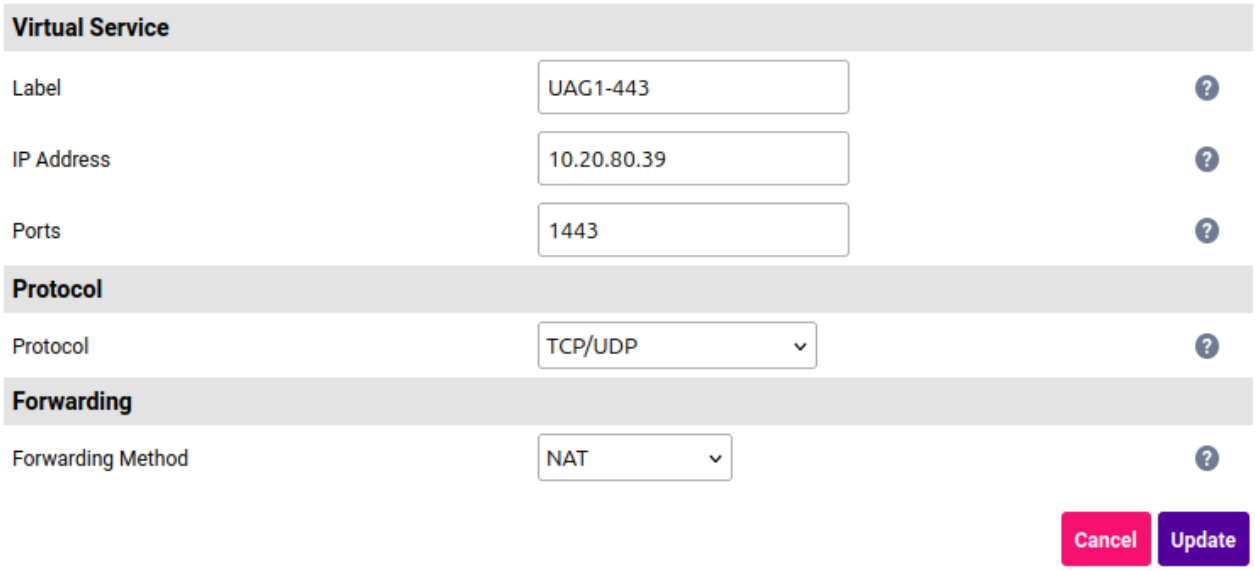
Step 2 - Configure the Virtual Service (VIP) & Real Servers (RIPs) for the Secondary Protocols

The 6 secondary protocol VIPs (3 for UAG1, 3 for UAG2) are listed in Option 3: UAG Configuration.

The configuration for the first VIP, **UAG1-HTTPS** is shown below:

Configure the Virtual Service:

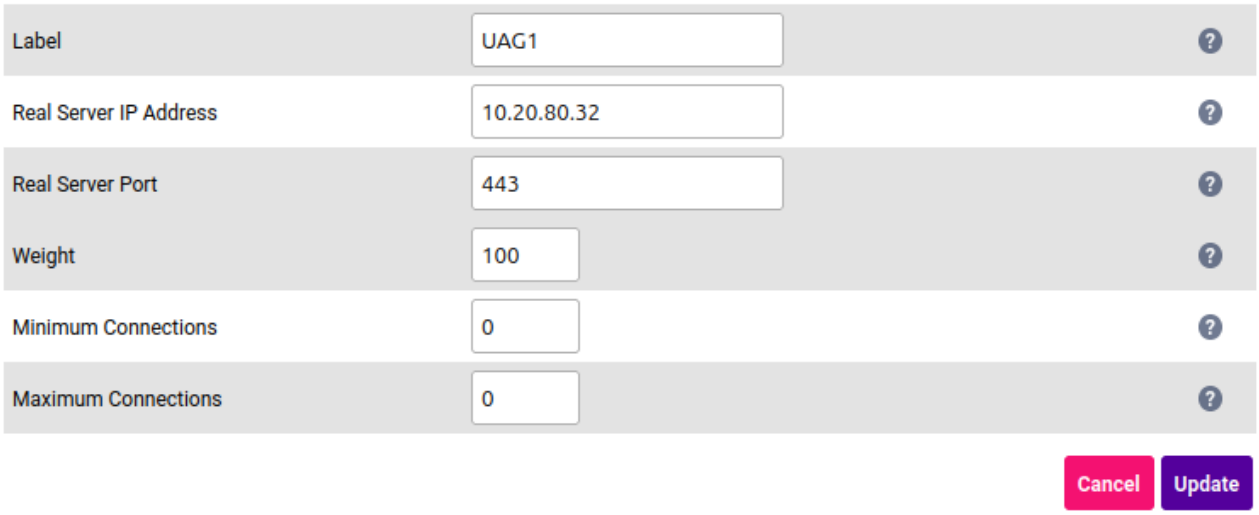
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Service* and click **Add a New Virtual Service**.
2. Enter the following details:



3. Enter an appropriate label (name) for the VIP, e.g. **UAG1-443**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **10.20.80.39**.
5. Set the *Virtual Service Ports* field to **1443**.
6. Set the *Protocol* to **TCP/UDP**.
7. Set the *Forwarding Method* to **NAT**.
8. Click **Update**.
9. Now click **Modify** next to the newly created VIP.
10. Set *Check Type* to **Negotiate**.
11. Set *Check Port* to **443**.
12. Set *Protocol* to **HTTPS**.
13. Set *Request to send* to **/favicon.ico**.
14. Leave *Response expected* blank.
15. Click **Update**.

Configure the Real Servers:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a New Real Server** next to the newly created VIP.
2. Enter the following details:



3. Enter an appropriate label for the RIP, e.g. **UAG1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **10.20.80.32**.
5. Set the port to the **443**.
6. Click **Update**.
7. Repeat the above steps to add your other UAG(s).

Now continue and create the 5 remaining secondary protocol VIPs (UAG1-PCoIP, UAG1-Blast, UAG2-443, UAG2-PCoIP & UAG2-Blast) & associated RIPs listed in the table. Ensure that you:

- Configure all VIPs using layer 4 NAT mode.
- Set the *Virtual Service Port* and the *Real Server Port* according to column 1 & 5 respectively in the table.
- Set the *Protocol* according to column 3 in the table.
- Configure the same health check settings:
  - Set *Check Type* to **Negotiate**.
  - Set *Check Port* to **443**.
  - Set *Protocol* to **HTTPS**.
  - Set *Request to send* to **/favicon.ico**.
  - Leave *Response expected* blank.

Step 3 - Add a Floating IP Address to the Load Balancer to be used as the UAG's Default Gateway

Using the WebUI option: *Cluster Configuration > Floating IPs* add a Floating IP that can be used as the default gateway for the UAGs. Using a floating IP will ensure that the IP address is available when a clustered pair is used, and a failover to the Secondary has occurred. This floating IP should be an additional IP address that is dedicated to this purpose.

Step 4 - Configure the Default Gateway on the Load Balancer

Using the WebUI option: *Local Configuration > Routing* set the default gateway to be the internal interface of the external firewall, e.g. **10.20.80.254**.

Step 5 - Configure HTTP to HTTPS Redirection

If required, the load balancer can be configured to automatically redirect clients who attempt to connect to **http://<Horizon URL>** to **https://<Horizon URL>**.

- When using cookie based persistence (SSL is terminated on the load balancer), this can be configured by modifying the *HorizonExternal* VIP and enabling the *Force to HTTPS* option.
- When using source IP persistence (SSL is terminated on the real servers), a separate VIP is required to handle this. For details on setting this up, please refer to Configuring an HTTP to HTTPS redirect.

Step 6 – Reload Services

To apply the new settings, HAProxy and STunnel (if using SSL offload) must both be reloaded. This can be done using the buttons in the "Commit changes" box at the top of the screen or by using the *Restart Services* menu option:

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

12. Configuring for Internal Clients

The configuration presented in this section relates to the topology described in Internal Clients.

12.1. Connection Server Configuration

Follow the same Connection Server configuration steps as per option 1 - see Option 1 - Connection Server Configuration.

12.2. Load Balancer Configuration

The load balancer is used for the primary protocol only, secondary protocols pass directly from client to virtual desktop.

12.2.1. Port Requirements

The following table shows the ports that are load balanced:

Port	Transport Protocol	Use
443	TCP	Primary Horizon Protocol / HTTPS Tunnel

12.2.2. Step 1 - Configure the Virtual Service (VIP) & Real Servers (RIPs)

Source IP address persistence is recommended if there are no inline NAT devices between the clients and the VIP. To configure the load balancer using source IP persistence, follow the steps in Using Source IP Persistence (Internal Clients).

If there are inline NAT devices, cookie based persistence can be used. To configure the load balancer using cookie persistence, follow the steps in Using Cookie Persistence (Internal Clients).

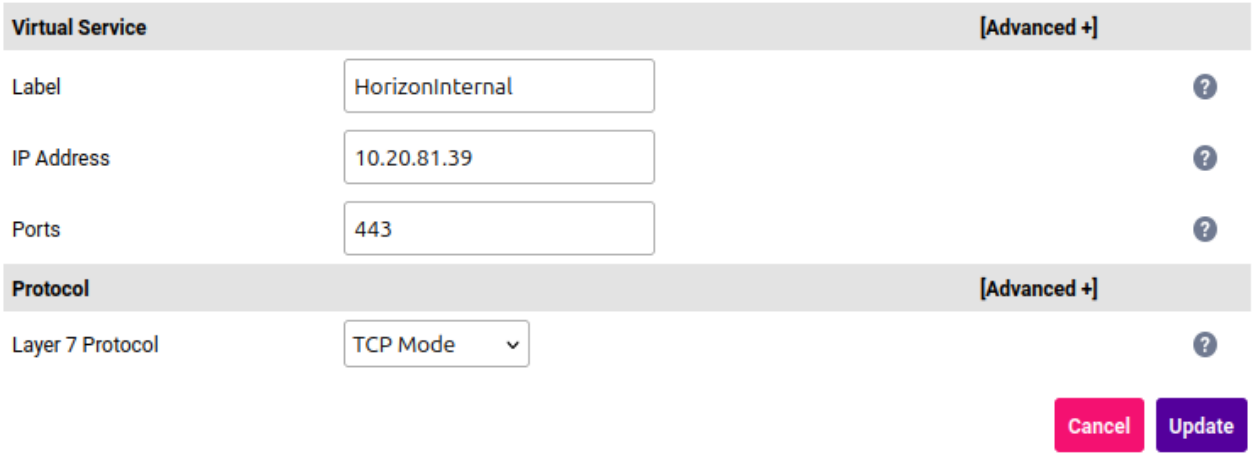
> **Note**
>
> If you want the actual client IP addresses to be represented in X-Forwarded-For (XFF) headers which the Connection Servers can use, follow the steps in Using Cookie Persistence (Internal Clients) and in addition to the configuration steps mentioned there, enable (check) the option ***Set X-Forward-For header*** when configuring the layer 7 VIP "HorizonInternal".

For more information on enabling layer 7 transparency using inserted headers, Transparency at Layer 7.

Using Source IP Persistence (Internal Clients)

Configure the Virtual Service:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**.
2. Enter the following details:

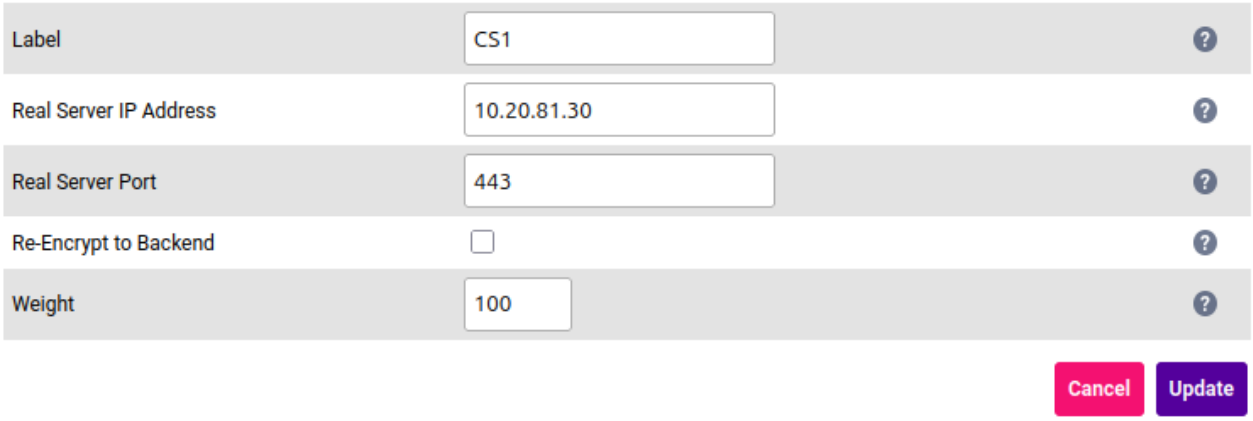


3. Enter an appropriate label for the VIP, e.g. **HorizonInternal**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **10.20.81.39**.
5. Set the *Virtual Service Ports* field to **443**.
6. Set *Layer 7 Protocol* to **TCP Mode**.
7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Set *Health Checks* to **Negotiate HTTPS (GET)**.
10. Set *Check Port* to **443**.
11. Set *Request to send* to **/favicon.ico**.
12. Leave *Response expected* blank.
13. Click **Update**.

Configure the Real Servers:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a New Real Server** next to the newly created VIP.

2. Enter the following details:

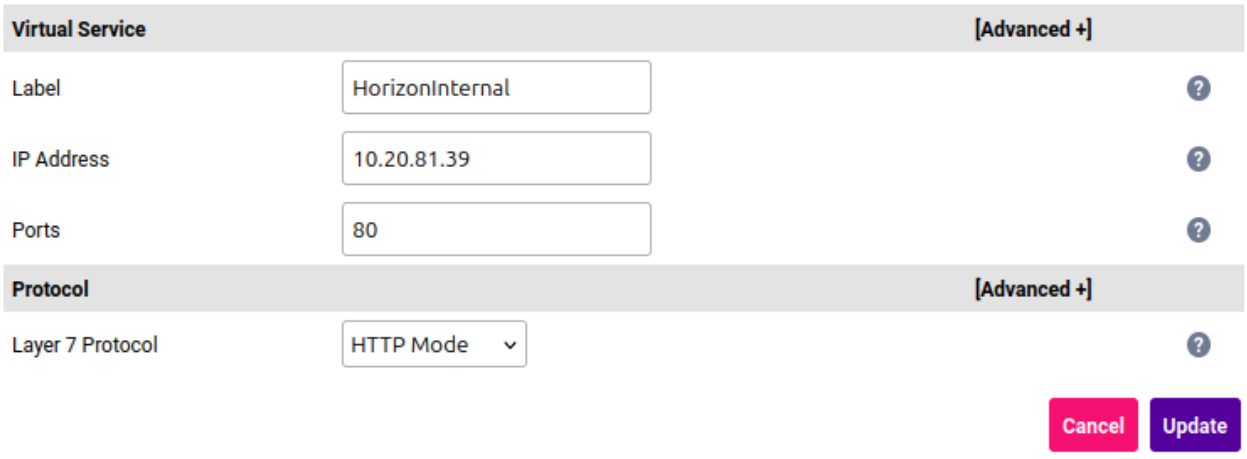


3. Enter an appropriate label for the RIP, e.g. **CS1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **10.20.81.30**.
5. Change the *Real Server Port* field to **443**.
6. Click **Update**.
7. Repeat the above steps to add your other Connection Server(s).

Using Cookie Persistence (Internal Clients)

Configure the Virtual Service:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**.
2. Enter the following details:

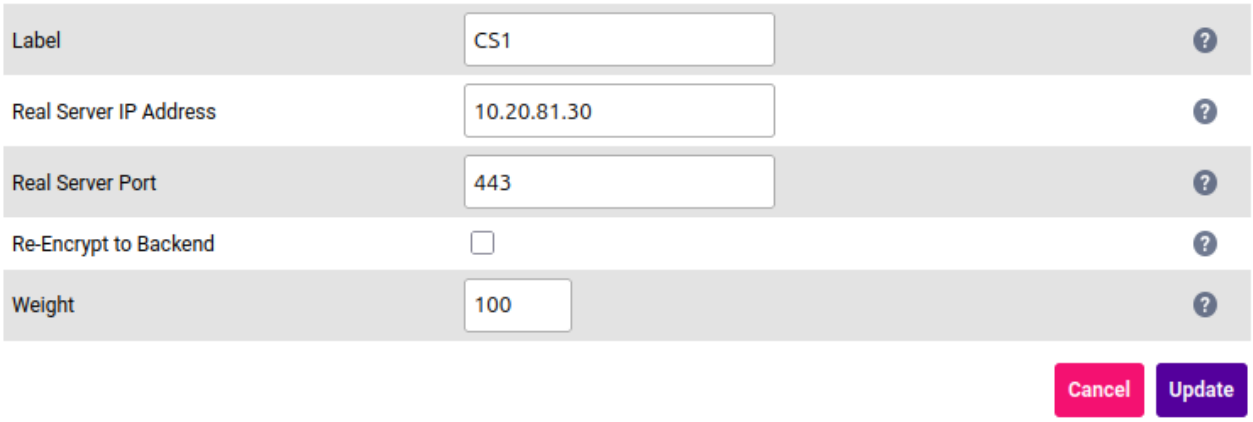


3. Enter an appropriate label for the VIP, e.g. **HorizonInternal**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **10.20.81.39**.
5. Set the *Virtual Service Ports* field to **80**.
6. Leave *Layer 7 Protocol* set to **HTTP Mode**.

7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Set *Health Checks* to **Negotiate HTTP (GET)**.
10. Set *Check Port* to **80**.
11. Set *Request to send* to **/favicon.ico**.
12. Leave *Response expected* blank.
13. Click **Update**.

Configure the Real Servers:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a New Real Server** next to the newly created VIP.
2. Enter the following details:



3. Enter an appropriate label for the RIP, e.g. **CS1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **10.20.81.30**.
5. Change the *Real Server Port* field to **443**.
6. Click **Update**.
7. Repeat the above steps to add your other Connection Server(s).

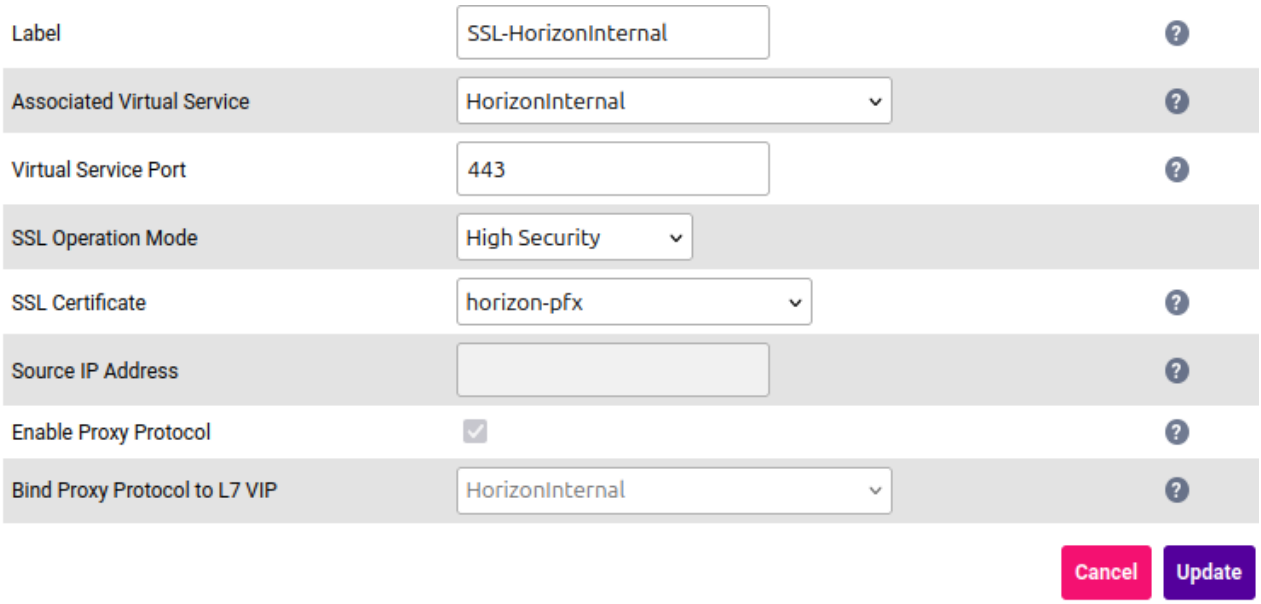
Configure SSL Termination – Upload the SSL certificate:

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificate*.
2. Click **Add a new SSL Certificate**.
3. Select *Upload prepared PEM/PFX file*.
4. Enter a suitable label (name) for the certificate, e.g. **Horizon**.
5. Browse to the relevant Horizon PFX certificate file.
6. Enter the relevant *PFX File Password*.

7. Click **Add Certificate**.

Configure SSL Termination – Create the SSL Virtual Service:

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Termination* and click **Add a new Virtual Service**.



2. Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **HorizonInternal**.

> **Note** Once the VIP is selected, the *Label* field will be auto-populated with **SSL-HorizonInternal**. This can be changed if preferred.

3. Leave *Virtual Service Port* set to **443**.
4. Leave *SSL Operation Mode* set to **High Security**.
5. Select the SSL certificate uploaded previously using the *SSL Certificate* drop-down
6. Click **Update**.

12.2.3. Step 2 - Configure HTTP to HTTPS Redirection

If required, the load balancer can be configured to automatically redirect clients who attempt to connect to **http://<Horizon URL>** to **https://<Horizon URL>**.

- When using cookie based persistence (SSL is terminated on the load balancer), this can be configured by modifying the *HorizonInternal* VIP and enabling the *Force to HTTPS* option.
- When using source IP persistence (SSL is terminated on the real servers), a separate VIP is required to handle this. For details on setting this up, please refer to Configuring an HTTP to HTTPS redirect.

12.2.4. Step 3 – Reload Services

To apply the new settings, HAProxy and STunnel (if using SSL offload) must both be reloaded. This can be done using the buttons in the "Commit changes" box at the top of the screen or by using the *Restart Services* menu

option:

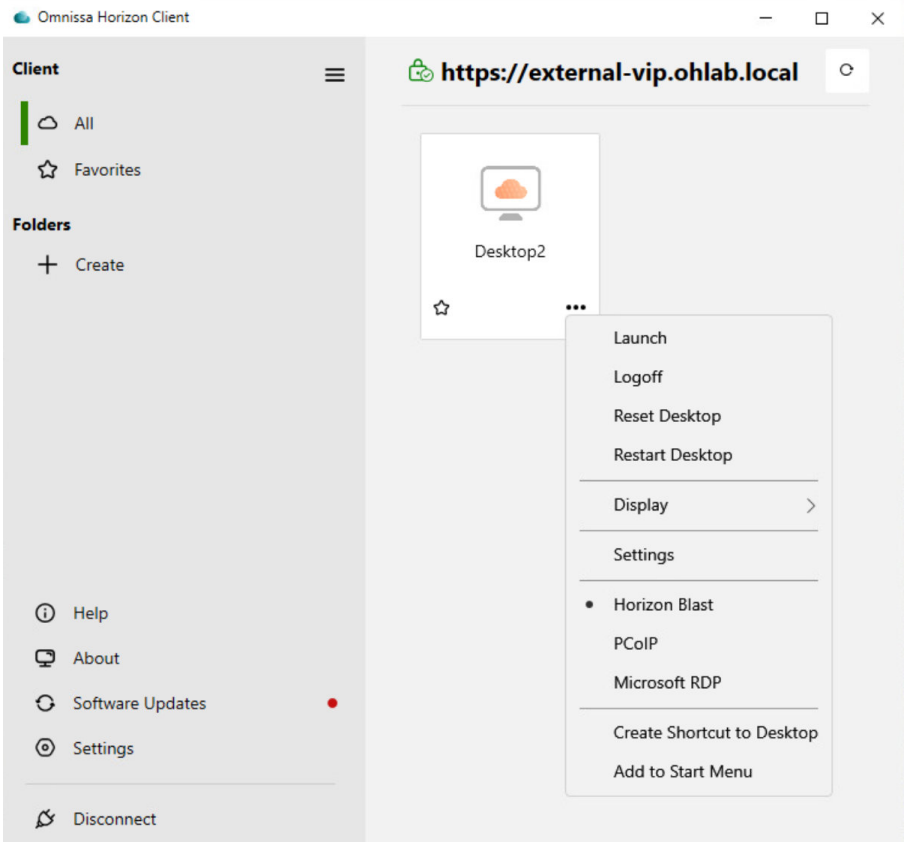
1. Using the WebUI, navigate to: *Maintenance > Restart Services*.
2. Click **Reload HAProxy**.
3. Click **Reload STunnel**.

13. Testing & Verification

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

13.1. Client Protocol Testing

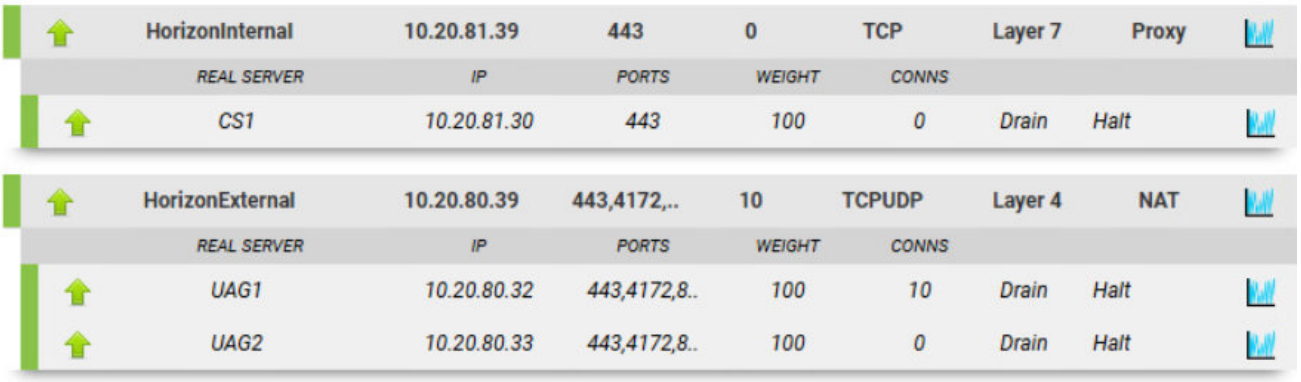
To ensure that all required client protocols are configured correctly, the Horizon client should be configured to each of the configured protocols using the right-click menu as shown below for both internal and external clients.



HTML Access should also be verified for internal and external clients using a browser.

13.2. Using System Overview

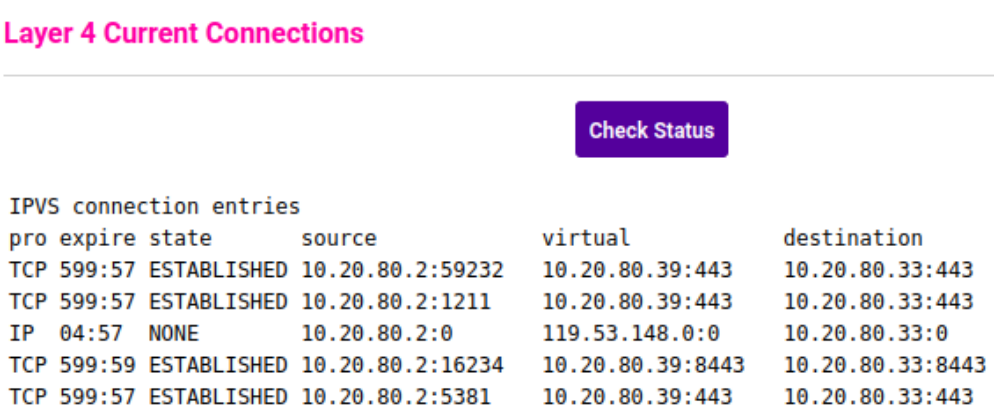
The System Overview shows a graphical view of all VIPs & RIPs (i.e. the Horizon Servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows that both UAGs are healthy and available to accept connections.



HorizonInternal	10.20.81.39	443	0	TCP	Layer 7	Proxy	
REAL SERVER	IP	PORTS	WEIGHT	CONNS			
CS1	10.20.81.30	443	100	0	Drain	Halt	
HorizonExternal	10.20.80.39	443,4172,..	10	TCPUDP	Layer 4	NAT	
REAL SERVER	IP	PORTS	WEIGHT	CONNS			
UAG1	10.20.80.32	443,4172,8..	100	10	Drain	Halt	
UAG2	10.20.80.33	443,4172,8..	100	0	Drain	Halt	

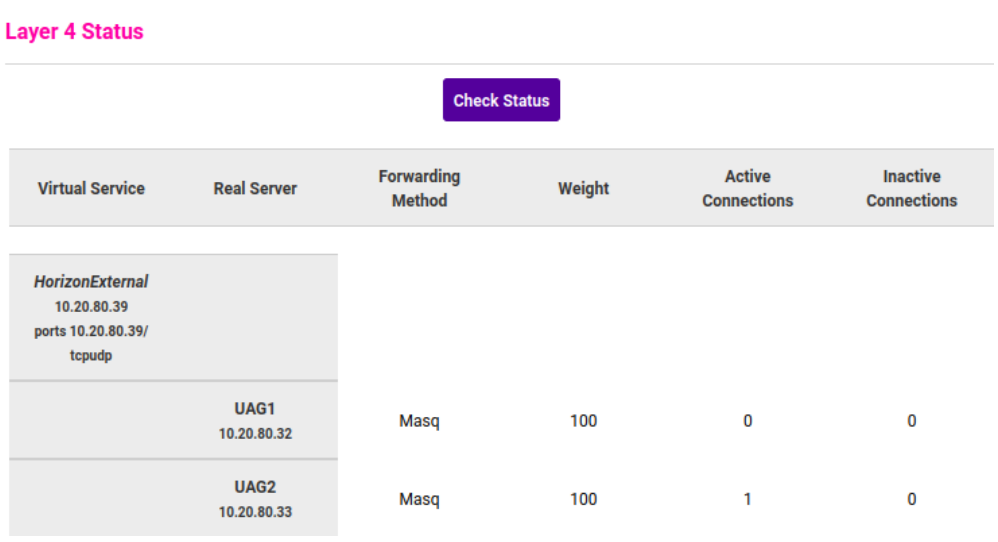
13.3. Layer 4 Current Connections Report

The Layer 4 Current Connection report shows all current layer 4 connections and their status. This can be accessed in the WebUI using the option: *Reports > Layer 4 Current Connections*. The example below shows the report whilst an External Horizon Client is connected via a layer 4 VIP.



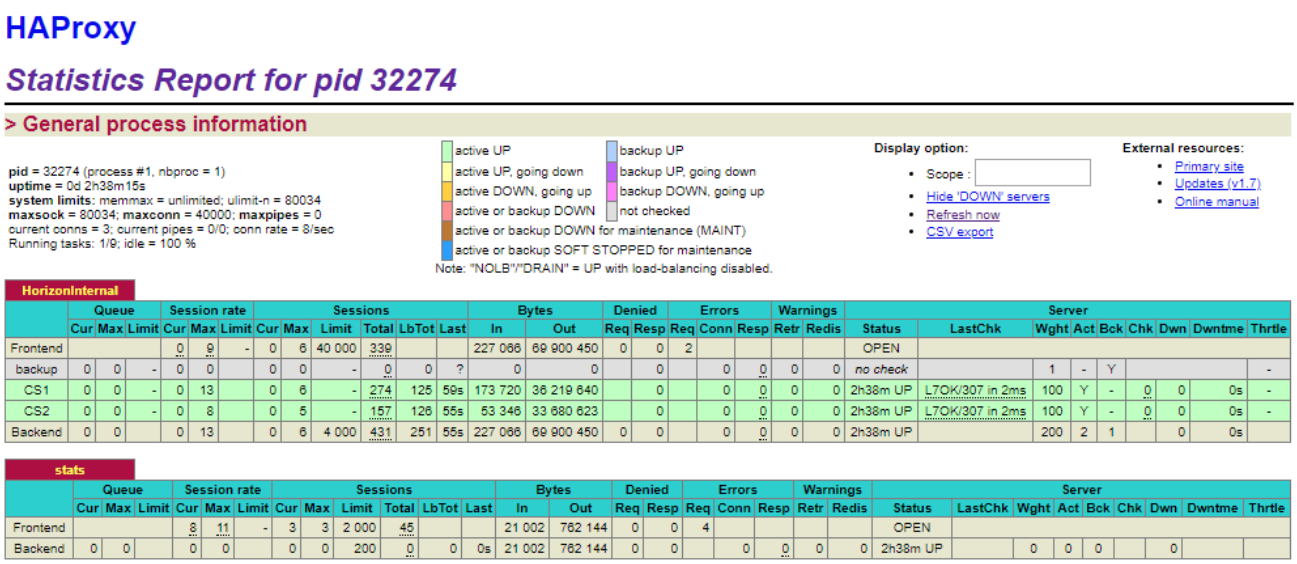
13.4. Layer 4 Status Report

The Layer 4 Status report gives a summary of layer 4 configuration and running stats as shown below. This can be accessed in the WebUI using the option: *Reports > Layer 4 Status*.



13.5. Layer 7 Statistics Report

The Layer 7 Statistics report gives a summary of all layer 7 configuration and running stats as shown below. This can be accessed in the WebUI using the option: ***Reports > Layer 7 Status.***



HAProxy

Statistics Report for pid 32274

> General process information

pid = 32274 (process #1, nbproc = 1)
uptime = 0d 2h38m15s
system limits: memmax = unlimited; ulimit-n = 80034
maxsock = 80034; maxconn = 40000; maxpipes = 0
current conns = 3; current pipes = 0/0; conn rate = 8/sec
Running tasks: 1/9; idle = 100 %

active UP
active UP, going down
active DOWN, going up
active or backup DOWN
active or backup DOWN for maintenance (MAINT)
active or backup SOFT STOPPED for maintenance
backup UP
backup UP, going down
backup DOWN, going up
not checked
Note: "NOLB"/"DRAIN" = UP with load-balancing disabled.

Display option:
- Scope :
- Hide 'DOWN' servers
- Refresh now
- CSV export

External resources:
- Primary site
- Updates (v1.7)
- Online manual

HorizonInternal

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server								
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				0	9	-	0	6	40 000	339			227 066	69 900 450	0	0	2					OPEN								
backup	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	*no check*		1	-	Y				-
CS1	0	0	-	0	13		0	6	-	274	125	59s	173 720	36 219 640		0		0	0	0	0	2h38m UP	L7OK/307 in 2ms	100	Y	-	0	0	0s	-
CS2	0	0	-	0	8		0	5	-	157	126	55s	53 346	33 680 623		0		0	0	0	0	2h38m UP	L7OK/307 in 2ms	100	Y	-	0	0	0s	-
Backend	0	0		0	13		0	6	4 000	431	251	55s	227 066	69 900 450	0	0		0	0	0	0	2h38m UP		200	2	1		0	0s	

stats

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server								
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				8	11	-	3	3	2 000	45			21 002	762 144	0	0	4					OPEN								
Backend	0	0		0	0		0	0	200	0	0	0s	21 002	762 144	0	0		0	0	0	0	2h38m UP		0	0	0		0		

13.6. Appliance Logs

Logs are available for both layer 4 and layer 7 services and can be very useful when trying to diagnose issues. Layer 4 logs are active by default and can be accessed using the WebUI option: ***Logs > Layer 4***. Layer 7 logging is not enabled by default (because it's extremely verbose) and can be enabled using the WebUI option: ***Cluster Configuration > Layer 7 – Advanced Configuration***, and then viewed using the option: ***Logs > Layer 7***.

14. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don't hesitate to contact our support team: support@loadbalancer.org.

15. Further Documentation

For additional information, please refer to the Administration Manual.

16. Appendix

16.1. Configuring an HTTP to HTTPS redirect

An additional layer 7 VIP is required that listens on HTTP port 80 on the same IP address. The VIP is then configured to redirect connections to HTTPS port 443.

e.g. **http://external-vip.ohlab.local** should be redirected to **https://external-vip.ohlab.local**.

The steps:

1) Create another Layer 7 VIP with the following settings:

- *Label*: **HTTP-redirect**.
- Virtual Service IP Address: **<same as the VIP that's listening on port 443>**.
- Virtual Service Ports: **80**.
- *Layer 7 Protocol*: **HTTP Mode**.
- Persistence Mode: **None**.
- Force to HTTPS: **Yes**.

> **Note** This additional VIP will be shown purple/green to indicate that it's being used for HTTP to HTTPS redirection.

2) Apply the new settings – to apply the new settings, HAProxy must be restarted:

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

16.2. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution. We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

> **Note** For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

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.

16.2.1. Non-Replicated Settings

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

WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

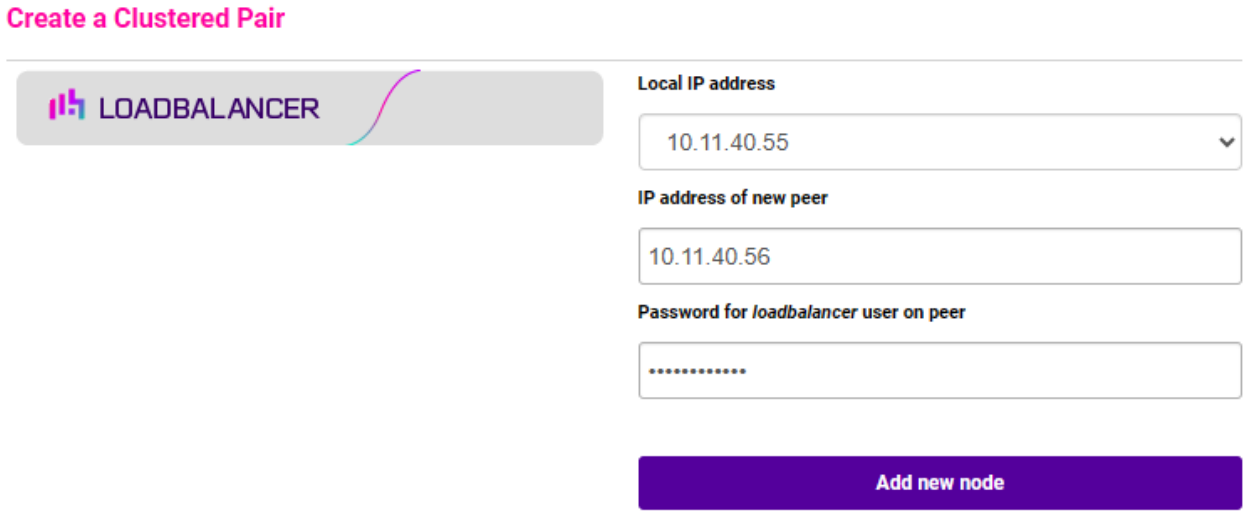
Important Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

16.2.2. Configuring the HA Clustered Pair

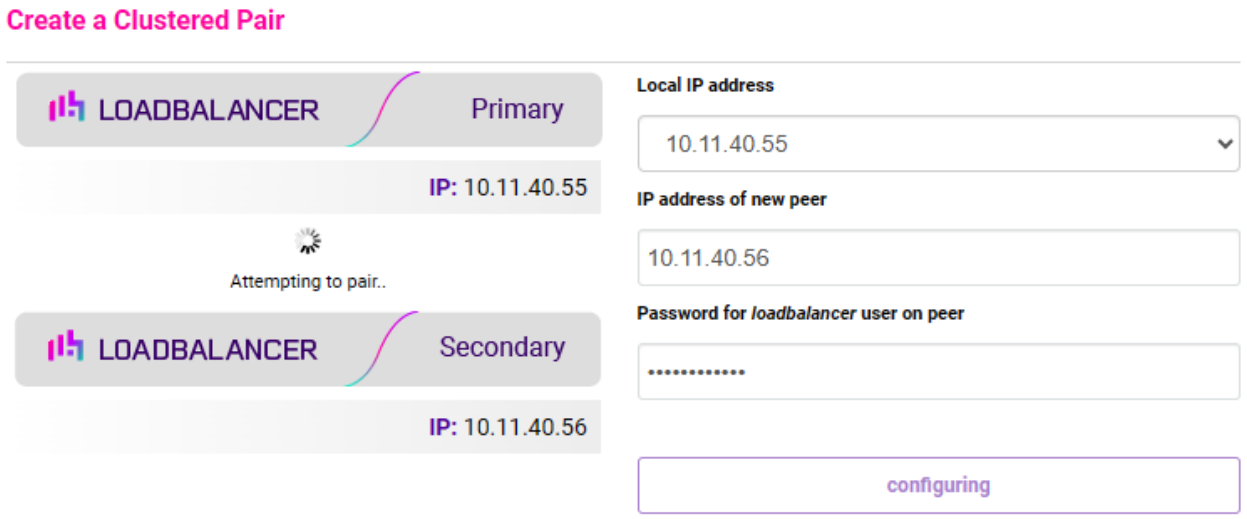
Important During HA pairing, all WebUI users and passwords are synchronized from the Primary to the Secondary. After clustering completes (you will be logged out of the Secondary when this occurs), the Primary's credentials should be used to login to both nodes.

Note If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

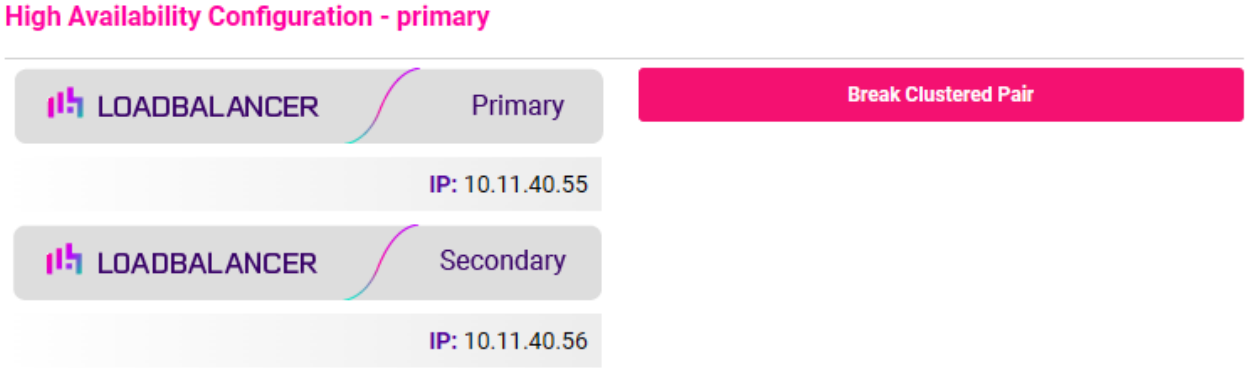
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: ***Cluster Configuration > High-Availability Configuration***.



3. Specify the IP address and the ***loadbalancer*** user's password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:



6. Once complete, the following will be displayed on the Primary appliance:



7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

> **Note** Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

> **Note** For more details on configuring HA with 2 appliances, please refer to Configuring High Availability.

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

17. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	29 April 2026	Initial Version		RJC

LOADBALANCER

Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @loadbalancer.org

About Loadbalancer.org

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