



Load Balancing VMware Horizon View

v1.4.2

Deployment Guide

NOTE: This guide has been archived and is no longer being maintained. While the content is still valid for the particular software versions mentioned, it may refer to outdated software that has now reached end-of-life. For more information please contact support@loadbalancer.org.



Contents

1. About this Guide.....	4
2. Loadbalancer.org Appliances Supported.....	4
3. Loadbalancer.org Software Versions Supported.....	4
4. VMware Horizon View Versions Supported.....	5
5. VMware Horizon View.....	5
6. Horizon View Servers to Load Balance.....	5
7. Load Balancing VMware View.....	5
<i>Load Balancing & HA Requirements.....</i>	<i>5</i>
<i>Persistence (aka Server Affinity).....</i>	<i>5</i>
<i>SSL Offload.....</i>	<i>6</i>
<i>Port Requirements.....</i>	<i>6</i>
<i>Load Balancer Deployment.....</i>	<i>6</i>
<i>Load Balancer Deployment Modes.....</i>	<i>7</i>
8. Load Balancer Deployment Options.....	7
<i>View Client Connection Process (2 Phase).....</i>	<i>7</i>
<i>External Clients.....</i>	<i>7</i>
Method 1 – Fully load balanced Phase 1 & 2 (Using Source IP Persistence).....	7
Method 2 – Load Balanced Phase 1 (Using Source IP Persistence).....	8
Method 3 – Load Balanced Phase 1 (Using Application Cookie Persistence).....	9
External Clients - Helping you Choose the most appropriate Method.....	11
<i>Internal Clients.....</i>	<i>11</i>
Method 1 – Load Balanced Phase 1 (Using Source IP Persistence).....	11
Method 2 – Load Balanced Phase 1 (Using Application cookie Persistence).....	12
Internal Clients – Helping you Choose the most appropriate Method.....	13
9. Loadbalancer.org Appliance – the Basics.....	14
<i>Virtual Appliance Download & Deployment.....</i>	<i>14</i>
<i>Initial Network Configuration.....</i>	<i>14</i>
<i>Accessing the Web User Interface (WebUI).....</i>	<i>14</i>
<i>HA Clustered Pair Configuration.....</i>	<i>16</i>
10. Configuring for Horizon View External Clients.....	16
<i>Method 1 – Fully load balanced Phase 1 & 2 (Using Source IP Persistence).....</i>	<i>16</i>
View Server Configuration.....	16
Appliance Configuration.....	17
<i>Method 2 – Load Balanced Phase 1 (Using Source IP Persistence).....</i>	<i>21</i>
View Server Configuration.....	21
Appliance Configuration.....	23
<i>Method 3 – Load Balanced Phase 1 (Using Application Cookie Persistence).....</i>	<i>25</i>
View Server Configuration.....	25
Appliance Configuration.....	26
11. Configuring for Horizon View Internal Clients.....	30
<i>Method 1 – Load Balanced Phase 1 (Using Source IP Persistence).....</i>	<i>30</i>
Connection Server Configuration.....	31
Appliance Configuration.....	31

<i>Method 2 – Load Balanced Phase 1 (Using Application cookie Persistence)</i>	33
Connection Server Configuration.....	33
Appliance Configuration.....	34
12. Testing & Verification.....	38
<i>Using System Overview</i>	38
<i>Layer 4 Current Connections Report</i>	39
<i>Layer 4 Status Report</i>	39
<i>Layer 7 Statistics Report</i>	40
<i>Appliance Logs</i>	40
13. Technical Support.....	40
14. Further Documentation.....	41
15. Conclusion.....	41
16. Appendix.....	42
1 – <i>Configuring an HTTP to HTTPS redirect</i>	42
2 – <i>Clustered Pair Configuration – Adding a Slave Unit</i>	42
17. Document Revision History.....	45

1. About this Guide

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

Note: If you want to load balance VMware Horizon v6.2 & later (with Access Point / Universal Access Gateway), please refer to [this guide](#).

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

- [v7 Administration Manual](#)
- [v8 Administration Manual](#)

2. Loadbalancer.org Appliances Supported

All our products can be used with Horizon View. The complete list of models is shown below:

Discontinued Models	Current Models *
Enterprise R16	Enterprise R20
Enterprise VA R16	Enterprise MAX
Enterprise VA	Enterprise 10G
Enterprise R320	Enterprise 40G
	Enterprise Ultra
	Enterprise VA R20
	Enterprise VA MAX
	Enterprise AWS **
	Enterprise AZURE **
	Enterprise GCP **

* For full specifications of these models please refer to: <http://www.loadbalancer.org/products/hardware>

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

3. Loadbalancer.org Software Versions Supported

- v7.6.4 and later

4. VMware Horizon View Versions Supported

- v5.2 to v6.1

Note: VMware Horizon View was renamed VMware Horizon in v6.1.

5. VMware Horizon View

VMware Horizon View (formerly VMware View) is a virtual desktop infrastructure solution that simplifies desktop management and provides users with access when needed, whatever their location.

6. Horizon View Servers to Load Balance

Server	Purpose
Connection Server	View Connection Server acts as a broker for client connections. It authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical or blade PC, or Windows Terminal Services server.
Security Server	A Security Server is a special instance of View Connection Server that runs a subset of View Connection Server functions. A Security Server is used to provide an additional layer of security between the Internet and the internal network. A Security Server resides within a DMZ and acts as a proxy host for connections inside the trusted network. Each Security Server is paired with an instance of View Connection Server and forwards all traffic to that instance.

7. Load Balancing VMware View

Note: It's highly recommended that you have a working VMware Horizon View environment first before implementing the load balancer.

Load Balancing & HA Requirements

For high availability and scalability, VMware recommends that multiple Connection Servers and multiple Security Servers are deployed in load balanced clusters.

Persistence (aka Server Affinity)

It's important that client requests are forwarded to the same View server for the duration of their session. This can be achieved using either source IP persistence or application cookie (JSESSIONID) persistence.

SSL Offload

The load balancer can be configured to terminate SSL if required. However, this is only recommended when JSESSIONID application cookie persistence is used.

Port Requirements

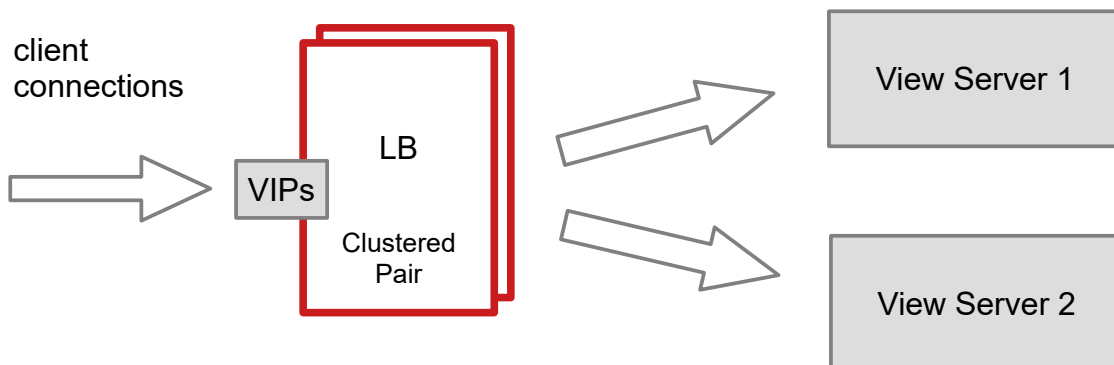
The following table shows the ports that are load balanced:

Port	Protocol	Uses
443	TCP	HTTPS
4172	TCP	PCoIP
4172	UDP	PCoIP
8443	TCP	Blast

Note: The exact ports to be load balanced depends on how the View Security/Connection Servers are load balanced. This is covered in later sections of this guide.

Load Balancer Deployment

A Virtual Services (VIP) is configured on the load balancer that acts as a connection point for clients. Clients then connect to the VIP on the load balancer rather than connecting directly to a one of the View Servers. These connections are then load balanced across the back-end servers (i.e. the View Servers) to distribute the load according to the load balancing algorithm selected.



VIPs = Virtual IP Addresses

Note: The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to section 2 in the appendix on page [42](#) for

more details on configuring a clustered pair.

Load Balancer Deployment Modes

Layer 4 NAT mode and layer 7 SNAT mode (HAProxy) are used for the configurations presented in this guide. Layer 4 DR mode can also be used if preferred. For DR mode you'll need to solve the ARP problem on each VMware View server (please see the Administration Manual and search for "DR mode considerations").

8. Load Balancer Deployment Options

The load balancer can be configured in various ways to support internal and external clients as detailed in the following sections.

View Client Connection Process (2 Phase)

View clients connect in 2 phases, these are:

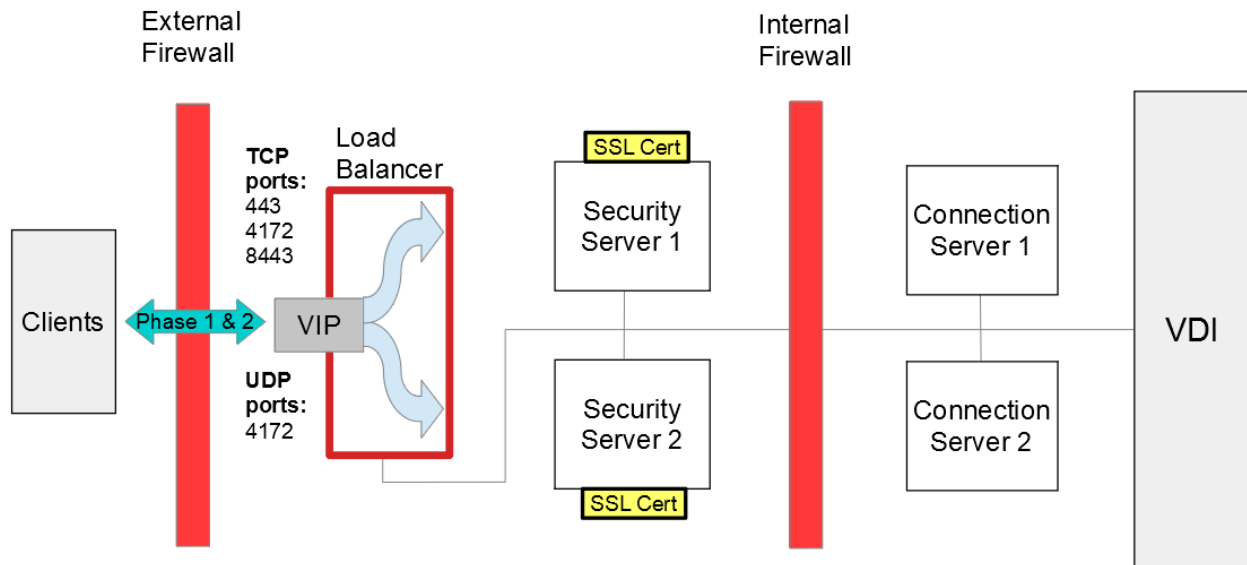
- **Phase 1** - Initial connection establishment, authentication, entitlement etc.
- **Phase 2** - Client to Virtual Desktop connection

External Clients

External clients connect to the Security Servers located in the DMZ. Each Security Server must be paired with a corresponding Connection Server. The PCoIP and Blast gateways on each Security Server must be enabled and correctly configured to ensure that clients can successfully connect.

Method 1 – Fully Load Balanced Phase 1 & 2 (Using Source IP Persistence)

In this scenario **ALL** client traffic passes via the load balancer. This option has the advantage that only one public IP address is required. Source IP address persistence is used which may result in an unbalanced distribution of connections for external clients due to inline NAT/proxy devices. This can happen because under these circumstances multiple clients can appear to come from the same IP address and therefore the load balancer will forward all these connections to the same Security Server rather than distributing them equally between the servers.



Notes:

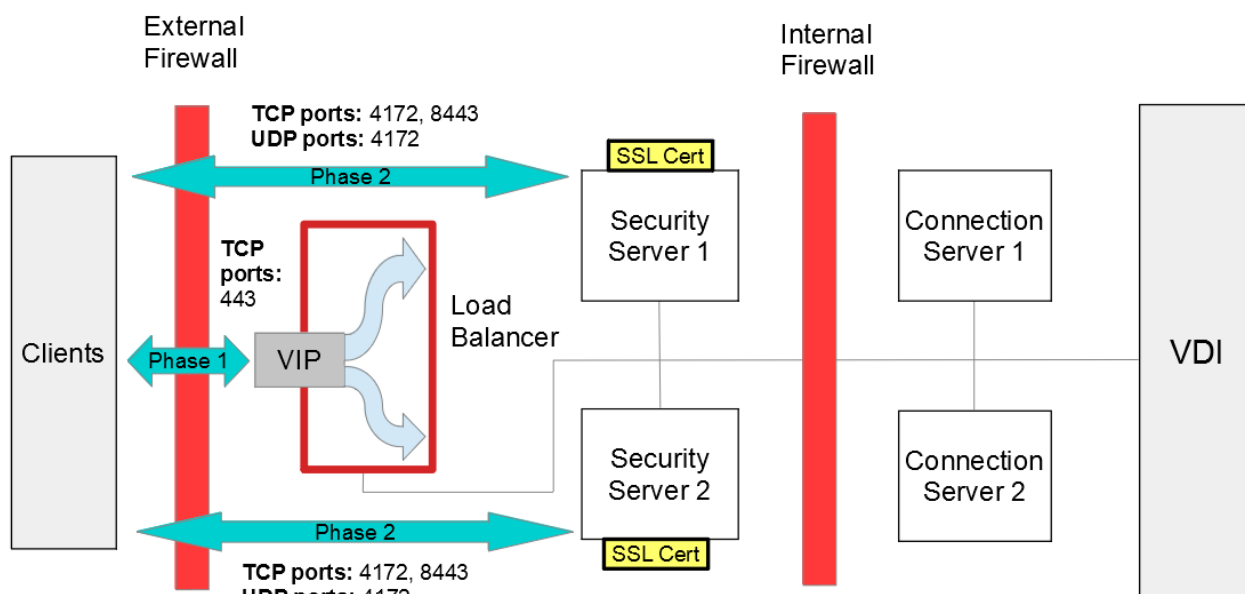
- The load balancer requires a single interface
- The VIP is configured in Layer 4 NAT mode
- The VIP is used to load balance both phase 1 and phase 2 of the connection process and must listen on TCP ports 443, 4172 & 8443 and UDP port 4172
- The default gateway of the Security Servers must be the load balancer. For a clustered pair of load balancers (master & slave) this should be a floating IP address to allow failover
- The default gateway of the load balancer must be the external firewall
- The paired Connection Servers must be configured to gateway the connections. Clients then connect to the desktops via the load balancer and the Security Servers
- Source IP address persistence may result in non balanced connections due to inline NAT/proxy devices
- See the steps starting on page [16](#) for appliance and server configuration guidance

Note: In this scenario the load balancer only requires a single network interface for NAT mode to work. This is because clients are located on the Internet, the default gateway of the Security Servers is the load balancer and the default gateway of the load balancer is the external firewall. This ensures that return traffic from the Security Servers to the clients passes back via the load balancer which is a requirement for layer 4 NAT mode.

Method 2 – Load Balanced Phase 1 (Using Source IP Persistence)

In this scenario, only Phase 1 is handled by the load balancer. A single VIP in layer 7 SNAT mode is used and is configured to use source IP address persistence to ensure that clients connect to the same Security Server for the duration of the Phase. Once Phase 1 negotiation is complete, Phase 2 connections are direct from the client to the

Security Servers. For this to work, each Security Server must be externally accessible from the Internet.

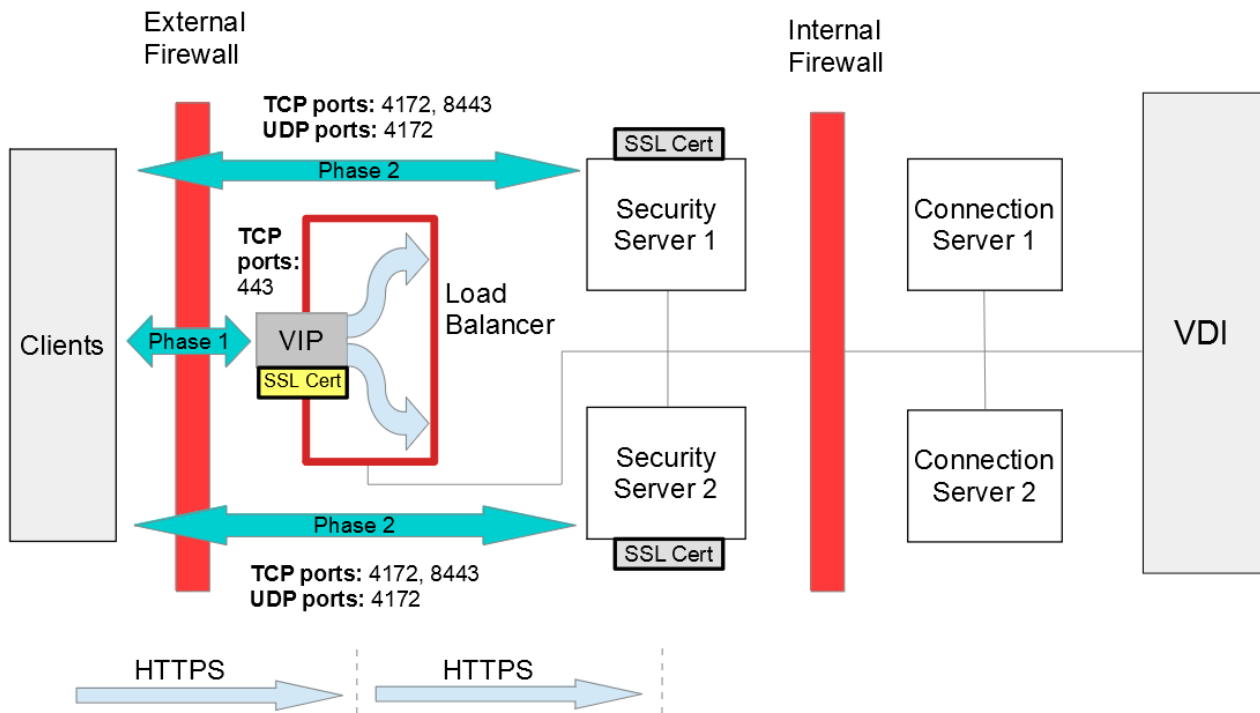


Notes:

- The load balancer requires a single interface
- The VIP is configured in Layer 7 SNAT mode
- The VIP is used to load balance phase 1 of the connection process and must listen on TCP port 443
- The paired Connection Servers must be configured to gateway the connections. Clients then connect to the desktops via the Security Servers bypassing the load balancer
- The Security Servers must be accessible externally for Phase 2 connections
- Source IP address persistence may result in non balanced connections due to inline NAT/proxy devices
- See the steps starting on page [21](#) for appliance and server configuration guidance

Method 3 – Load Balanced Phase 1 (Using Application Cookie Persistence)

In this scenario, only Phase 1 is handled by the load balancer. A single VIP in layer 7 SNAT mode is used and is configured to use application cookie (JSESSIONID) persistence to ensure that clients connect to the same Security Server for the duration of the Phase. Once Phase 1 negotiation is complete, Phase 2 connections are direct from the client to the Security Servers. For this to work, each Security Server must also be externally accessible from the Internet.



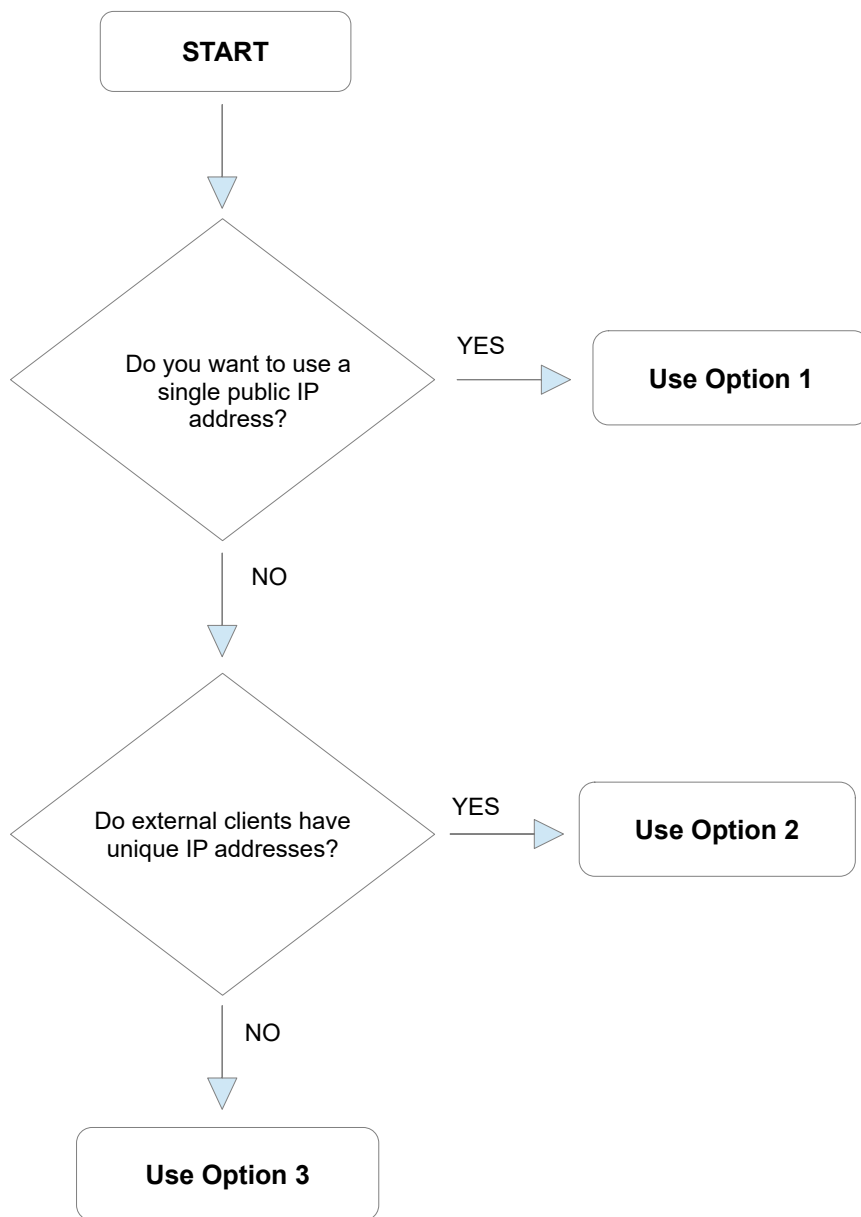
Notes:

- The load balancer requires a single interface
- The VIP is configured in Layer 7 SNAT mode
- The VIP is used to load balance phase 1 of the connection process and must listen on TCP port 443
- Inbound HTTPS connections are terminated on the load balancer to enable the JSESSIONID cookie to be read. Connections are then re-encrypted from load balancer to Security Server. This can be achieved using self signed SSL certs (colored grey above)

Note: SSL offload is not supported for smart-card authentication.

- The paired Connection Servers must be configured to gateway the connections. Clients then connect to the desktops via the Security Servers bypassing the load balancer
- The Security Servers must be accessible externally for Phase 2 connections
- See the steps starting on page [25](#) for appliance and server configuration guidance

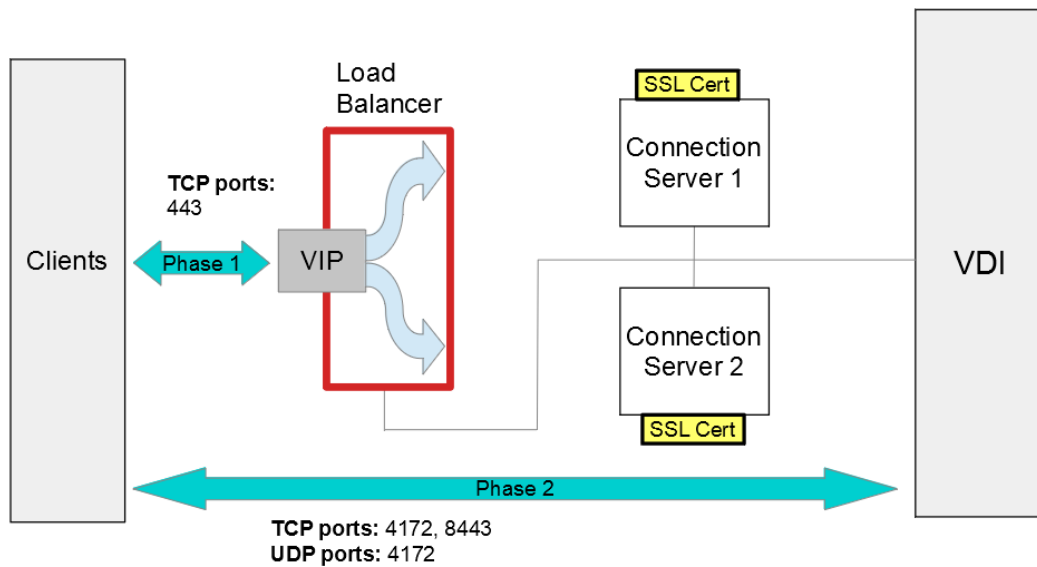
External Clients - Helping You Choose The Most Appropriate Method



Internal Clients

Internal clients connect directly to the Connection Servers located on the LAN. The gateway must be disabled so that clients can connect directly to the desktops rather than passing via the load balancer or gateway.

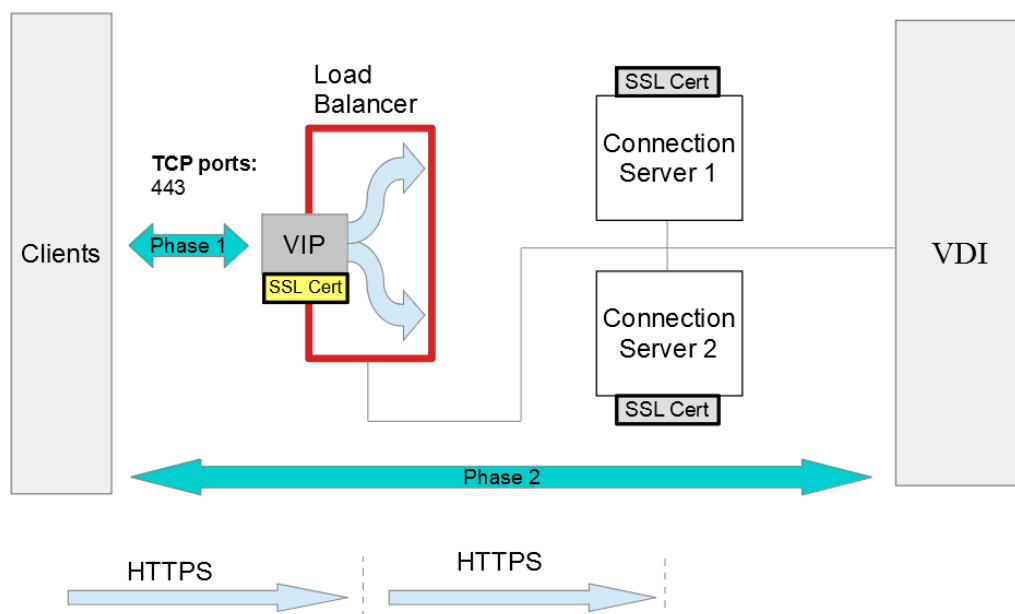
Method 1 – Load Balanced Phase 1 (Using Source IP Persistence)



Notes:

- The load balancer requires a single interface
- The VIP is configured in Layer 7 SNAT mode
- A single VIP is used to load balance phase 1 of the connection process and must listen on TCP port 443
- The Connection Servers must NOT be configured to gateway the connections. Clients are then able to connect directly to the desktops
- Source IP address persistence may result in non balanced connections due to inline NAT/proxy devices
- See the steps starting on page [30](#) for appliance and server configuration guidance

Method 2 – Load Balanced Phase 1 (Using Application Cookie Persistence)



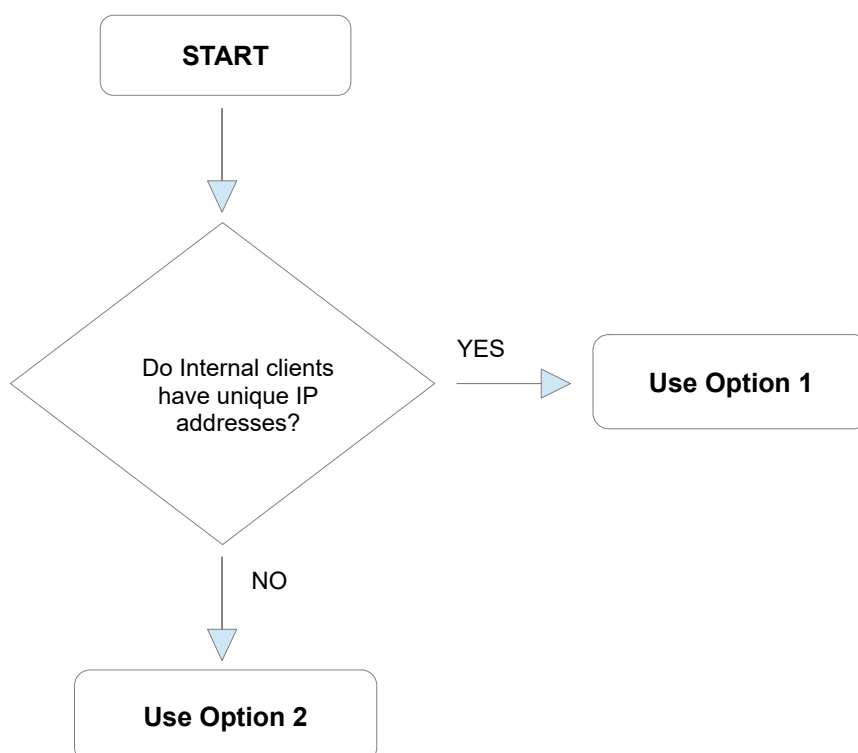
Notes:

- The load balancer requires a single interface
- The VIP is configured in Layer 7 SNAT mode
- A single VIP is used to load balance phase 1 of the connection process and must listen on TCP port 443
- Inbound SSL connections are terminated on the load balancer to enable the JSESSIONID cookie to be read. Connections are then re-encrypted from load balancer to connection Server. This can be achieved using self signed SSL certs (colored grey above)

Note: SSL offload is **not** supported for smart-card authentication.

- The Connection Servers must NOT be configured to gateway the connections. Clients are then able to connect directly to the desktops
- Persistence is based on the JSESSIONID cookie that is inserted by the Connection Servers
- See the steps starting on page [33](#) for appliance and server configuration guidance

Internal Clients – Helping You Choose The Most Appropriate Method



9. Loadbalancer.org Appliance – the Basics

Virtual Appliance Download & Deployment

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk. The Virtual Appliance can be downloaded [here](#).

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

Note: Please refer to the [Administration Manual](#) and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Initial Network Configuration

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

Method 1 - Using the Network Setup Wizard at the console

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

Method 2 - Using the WebUI

Using a browser, connect to the WebUI on the default IP address/port: **https://192.168.2.21:9443**

To set the IP address & subnet mask, use: *Local Configuration > Network Interface Configuration*

To set the default gateway, use: *Local Configuration > Routing*

To configure DNS settings, use: *Local Configuration > Hostname & DNS*

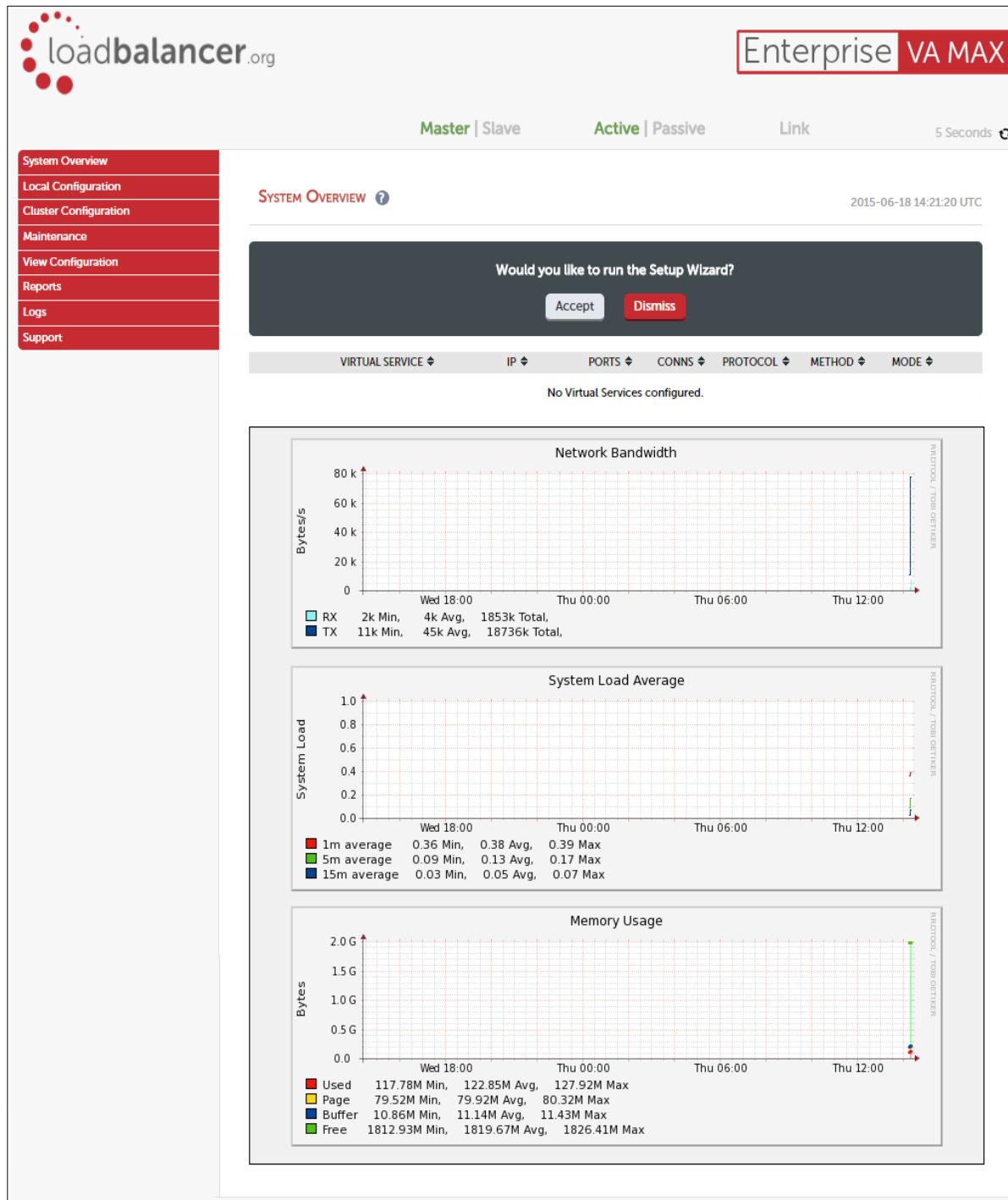
Accessing the Web User Interface (WebUI)

1. Browse to the following URL: **https://192.168.2.21:9443/lbadmin/**
(replace with your IP address if it's been changed)
* Note the port number → **9443**
2. Login to the WebUI:
Username: loadbalancer

Password: loadbalancer

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

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



HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 2 of the Appendix on page [42](#).

10. Configuring for Horizon View External Clients

External clients connect to View Security Servers. This section covers the various methods for load balancing Security Servers.

Method 1 – Fully load balanced Phase 1 & 2 (Using Source IP Persistence)

This method uses a Firewall Mark configuration which enables a single VIP to support both TCP and UDP.

View Server Configuration

The following sections illustrate how the Connection/Security Servers must be configured for external clients.

Paired Connection Server Settings

For each Connection Server leave the servers own IP address/DNS FQDN and ensure all check boxes are enabled:

The screenshot shows the 'Edit View Connection Server Settings' dialog box with the 'General' tab selected. The dialog has four tabs: General, Local Mode, Authentication, and Backup. The 'General' tab contains the following settings:

- Tags:** A text field for tags, with a note: 'Tags can be used to restrict which pools can be accessed through this Connection Server.' and a separator instruction: 'Separate tags with ; or ,'. The field is currently empty.
- HTTP(S) Secure Tunnel:** A checkbox labeled 'Use Secure Tunnel connection to desktop' is checked. Below it is an 'External URL' field containing 'https://192.168.120.101:443' and an example: 'Example: https://myserver.com:443'.
- PCoIP Secure Gateway:** A checkbox labeled 'Use PCoIP Secure Gateway for PCoIP connections to desktop' is checked. Below it is a 'PCoIP External URL' field containing '192.168.120.101:4172' and an example: 'Example: 10.0.0.1:4172'.
- Blast Secure Gateway:** A checkbox labeled 'Use Blast Secure Gateway for HTML access to desktop' is checked. Below it is a 'Blast External URL' field containing 'https://192.168.120.101:8443' and an example: 'Example: https://myserver.com:8443'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Paired Security Server Settings

For each Security Server set the IP addresses/DNS FQDN's to be the external address of the VIP , e.g.:

Server name: VM-SEC1

HTTP(S) Secure Tunnel

External URL: https://10.100.120.10:443
Example: https://myserver.com:443 ?

PCoIP Secure Gateway

PCoIP External URL: 10.100.120.10:4172
Example: 10.0.0.1:4172 ?

Blast Secure Gateway

Blast External URL: https://10.100.120.10:8443
Example: https://myserver.com:8443 ?

OK Cancel

Note: In this example 10.100.120.10 is used. In production environments, publicly accessible IP addresses would be required. In this test lab example the external firewall NATs 10.100.120.10 to the VIP address 192.168.120.50.

Appliance Configuration

Port Requirements

The following table shows the ports that must be load balanced.

Port	Protocol	Uses
443	TCP	HTTPS
4172	TCP	PCoIP
4172	UDP	PCoIP
8443	TCP	Blast

Configure the Virtual Service & Real Servers

a) Setting up 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:

Label	<input type="text" value="Cluster-1"/>	?	
Virtual Service	IP Address	<input type="text" value="1"/>	?
	Ports	<input type="text" value="80"/>	?
Protocol	<input type="text" value="Firewall Marks"/>	▼	?
Forwarding Method	<input type="text" value="NAT"/>	▼	?
<div><input type="button" value="Cancel"/> <input type="button" value="Update"/></div>			

3. Define the required *Label* (name) for the VIP, e.g. **Cluster-1**
4. Instead of entering an IP address, enter a numeric value, e.g. **1** – this is the numeric reference for the Firewall Mark, this reference is used in step c) below when defining the firewall rules
5. The *Virtual Service Ports* field does not need to be changed as it is not relevant in this case - the actual port(s) used are defined in the firewall script in step c) below
6. Set *Protocol* to **Firewall Marks** – at this point the *Virtual Service Ports* field will be grayed out
7. Set *Forwarding Method* to **NAT**
8. **Click Update**
9. Now click **Modify** next to the newly created VIP
10. Change *Persistent Time* to **36000** (i.e. 10 hours)

Note: The value set should match the "Forcibly disconnect users" setting under View's Global Settings. (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 **/**
15. Set *Response expected* to **vmware**
16. Click **Update**

b) Setting up 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:

Label	<input type="text" value="Security1"/>	?
Real Server IP Address	<input type="text" value="192.168.120.100"/>	?
Real Server Port	<input type="text"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

3. Enter an appropriate label for the RIP, e.g. **Security1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.120.100**
5. Leave the *Real Server Port* field blank
6. Click **Update**
7. Repeat the above steps to add your other Security Server(s)

Configure the Firewall Rules

Note: The *Firewall Script* page is locked by default on newer Loadbalancer.org appliances as part of "Secure Mode", which makes applying the changes described below impossible. To enable editing of the firewall script, navigate to *Local Configuration > Security*, set *Appliance Security Mode* to **Custom**, and click the **Update** button to apply the change. Editing the *Firewall Script* page will then be possible.

1. Using the WebUI, navigate to: *Maintenance > Firewall Script*
2. Scroll down to the Manual Firewall Marks section and add the following lines as shown below:

```
VIP1="192.168.120.50"
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j
MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 4172 -j
MARK --set-mark 1
iptables -t mangle -A PREROUTING -p udp -d $VIP1 --dport 4172 -j
MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 8443 -j
```

MARK --set-mark 1

Note: Set 'VIP1' above to the required IP address, e.g. 192.168.120.50.

FIREWALL SCRIPT

```
27
28 ##### Manual Firewall Marks #####
29
30 # Example: Associate HTTP and HTTPS with Firewall Mark 1:
31 #VIP1="10.0.0.66"
32 #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
33 #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1
34
35 # A Virtual Service may then be created in the web interface, using 1 as the
36 # service address.
37
38 #It is also possible to bind TCP and UDP protocols together with a firewall mark.
39 #VIP1="192.168.64.27"
40 #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
41 #iptables -t mangle -A PREROUTING -p udp -d $VIP1 --dport 300 -j MARK --set-mark 1
42
43 VIP1="192.168.120.50"
44 iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1
45 iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 4172 -j MARK --set-mark 1
46 iptables -t mangle -A PREROUTING -p udp -d $VIP1 --dport 4172 -j MARK --set-mark 1
47 iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 8443 -j MARK --set-mark 1
48
49 ##### Packet Filtering #####
50
51 # You should always use a network perimeter firewall to lock down all
52 # external access to the load balancer except the required Virtual Services
53 # and the required services from your admin machine / network (SSH & HTTPS)
54
55 # Allow unlimited traffic on the loopback interface:
56 #iptables -A INPUT -i lo -j ACCEPT
57 #iptables -A OUTPUT -o lo -j ACCEPT
58
```

Update

3. Click **Update**

Add a Floating IP Address to be used as the Default Gateway for the Security Servers

1. Using the WebUI, navigate to: *Cluster Configuration > Floating IP's*
2. Enter the IP address for the default gateway, e.g. **192.168.120.253**
3. Click **Add Floating IP**

Configure the default gateway on the Security Servers

1. Set the default gateway on each Security Server to be the floating IP address added in the previous step (e.g. 192.168.120.253)

Configure the default gateway on the load balancer

1. Using the WebUI option: *Local Configuration > Routing* set the default gateway to be the internal interface of the external firewall (e.g. 192.168.120.254)

Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect VMware Blast users who attempt to connect to **http://<URL to access VIEW>** to **https://<URL to access VIEW>**. For details on configuring this, please refer to section 1 in the Appendix on page [42](#).

Note: In this scenario the load balancer only requires a single network interface for NAT mode to work. This is because clients are located on the Internet, the default gateway of the Security Servers is the load balancer and the default gateway of the load balancer is the external firewall. This ensures that return traffic from the Security Servers to the clients passes back via the load balancer which is a requirement for layer 4 NAT mode.

Method 2 – Load Balanced Phase 1 (Using Source IP Persistence)

View Server Configuration

The following sections illustrate how the Connection/Security Servers must be configured for external clients.

Paired Connection Server Settings

For each Connection Server leave the servers own IP address/DNS FQDN and ensure all check boxes are enabled as shown below:

Edit View Connection Server Settings

General
Local Mode
Authentication
Backup

Tags
Tags can be used to restrict which pools can be accessed through this Connection Server.
Tags: Separate tags with ; or ,

HTTP(S) Secure Tunnel
☒ Use Secure Tunnel connection to desktop
External URL: Example: https://myserver.com:443 ?

PCoIP Secure Gateway
☒ Use PCoIP Secure Gateway for PCoIP connections to desktop
PCoIP External URL: Example: 10.0.0.1:4172 ?

Blast Secure Gateway
☒ Use Blast Secure Gateway for HTML access to desktop ?
Blast External URL: Example: https://myserver.com:8443 ?

OK Cancel

Paired Security Server Settings

For each Security Server set the IP addresses/DNS FQDN's to be the external address for that Security Server , e.g.:

Edit Security Server - VM-SEC1

Server name:

HTTP(S) Secure Tunnel
External URL:
Example: https://myserver.com:443 ?

PCoIP Secure Gateway
PCoIP External URL:
Example: 10.0.0.1:4172 ?

Blast Secure Gateway
Blast External URL:
Example: https://myserver.com:8443 ?

OK Cancel

Note: In this example 10.100.100.100 used. In production, publicly accessible IP addresses would be required. In this example the external firewall NATs 10.100.100.100 to the Security Servers own address 192.168.100.100. This must be done for each load balanced Security Server.

Appliance Configuration

Port Requirements

The following table shows the ports that must be load balanced.

Port	Protocol	Uses
443	TCP	HTTPS

Configure Layer 7 Global Settings

The Client Timeout and Server Timeout values should be changed from their default values of 43 seconds and 45 seconds respectively to 5 minutes. To do this follow the steps below:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*

Lock HAProxy Configuration (Deprecated)	<input type="checkbox"/>	?
Logging	Off ▼	?
Redispatch	<input checked="" type="checkbox"/>	?
Connection Timeout	4000 ms	?
Client Timeout	300000 ms	?
Real Server Timeout	300000 ms	?

2. Change *Client Timeout* to **300000** as shown above (i.e. 5 minutes)
*N.B. You can also enter **5m** rather than 300000*
3. Change *Real Server Timeout* to **300000** as shown above (i.e. 5 minutes)
*N.B. You can also enter **5m** rather than 300000*
4. Click the **Update** button to save the settings

Configure the Virtual Service & Real Servers

a) Setting up 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:

Label	<input type="text" value="ViewExternal"/>	?
Virtual Service	IP Address <input type="text" value="192.168.100.10"/>	?
	Ports <input type="text" value="443"/>	?
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?
Manual Configuration	<input type="checkbox"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

3. Enter an appropriate label for the VIP, e.g. **ViewExternal**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.100.10**
5. Set the *Virtual Service Ports* field to **443**
6. Ensure *Layer 7 Protocol* is set to **TCP Mode**
7. Click **Update**

b) Setting up 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:

Label	<input type="text" value="Security1"/>	?
Real Server IP Address	<input type="text" value="192.168.100.100"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

3. Enter an appropriate label for the RIP, e.g. **Security1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.100**
5. Change the *Real Server Port* field to **443**
6. Click **Update**
7. Repeat the above steps to add your other Security Server(s)

Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect VMware Blast users who attempt to connect to **http://<URL to access VIEW>** to **https://<URL to access VIEW>**. For details on configuring this, please refer to section 1 in the Appendix on page [42](#).

Finalizing the Configuration

To apply the new settings, reload HAProxy using the **Reload** button in the blue commit changes box at the top of the screen.

Method 3 – Load Balanced Phase 1 (Using Application Cookie Persistence)

View Server Configuration

The following sections illustrate how the Connection/Security Servers must be configured for external clients.

Paired Connection Server Settings

For each Connection Server leave the servers own IP address/DNS FQDN and ensure all check boxes are enabled:

Edit View Connection Server Settings

General Local Mode Authentication Backup

Tags
Tags can be used to restrict which pools can be accessed through this Connection Server.
Tags: Separate tags with ; or ,

HTTP(S) Secure Tunnel
☒ Use Secure Tunnel connection to desktop
External URL: Example: https://myserver.com:443 ?

PCoIP Secure Gateway
☒ Use PCoIP Secure Gateway for PCoIP connections to desktop
PCoIP External URL: Example: 10.0.0.1:4172 ?

Blast Secure Gateway
☒ Use Blast Secure Gateway for HTML access to desktop ?
Blast External URL: Example: https://myserver.com:8443 ?

OK Cancel

Paired Security Server Settings

For each Security Server set the IP addresses/DNS FQDN's to be the external address for that Security Server , e.g.:

Server name:

HTTP(S) Secure Tunnel

External URL:
Example: https://myserver.com:443 ?

PCoIP Secure Gateway

PCoIP External URL:
Example: 10.0.0.1:4172 ?

Blast Secure Gateway

Blast External URL:
Example: https://myserver.com:8443 ?

OK Cancel

Note: In this example 10.100.100.100 used. In production, publicly accessible IP addresses would be required. In this example the external firewall NATs 10.100.100.100 to the Security Servers own address 192.168.100.100. This must be done for each load balanced Security Server.

Reading the Application Cookie

It's possible to configure each Security Server to listen on port 80 for HTTP connections using the `serverProtocol=http` directive in the **locked.properties** file, then terminate SSL on the load balancer and pass unencrypted HTTP connections to the Security Servers. However, to avoid making this change to each Security Server it's possible to configure the load balancer to re-encrypt the data using the default self-signed cert on each server so that connections are made using HTTPS which is the default.

Appliance Configuration

Port Requirements

The following table shows the ports that must be load balanced.

Port	Protocol	Uses
443	TCP	HTTPS

Configure Layer 7 Global Settings

The Client Timeout and Server Timeout values should be changed from their default values of 43 seconds and 45 seconds respectively to 5 minutes. To do this follow the steps below:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*

Lock HAProxy Configuration (Deprecated)	<input type="checkbox"/>	?
Logging	Off ▼	?
Redispatch	<input checked="" type="checkbox"/>	?
Connection Timeout	4000 ms	?
Client Timeout	300000 ms	?
Real Server Timeout	300000 ms	?

2. Change *Client Timeout* to **300000** as shown above (i.e. 5 minutes)
*N.B. You can also enter **5m** rather than 300000*
3. Change *Real Server Timeout* to **300000** as shown above (i.e. 5 minutes)
*N.B. You can also enter **5m** rather than 300000*
4. Click the **Update** button to save the settings

Configure the Virtual Service & Real Servers

a) Setting up 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:

Label	ViewExternal	?	
Virtual Service	IP Address	192.168.100.10	?
	Ports	80	?
Layer 7 Protocol	HTTP Mode ▼	?	
Manual Configuration	<input type="checkbox"/>	?	

Cancel Update

3. Enter an appropriate label for the VIP, e.g. **ViewExternal**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.100.10**
5. Set the *Virtual Service Ports* field to **80**
6. Ensure *Layer 7 Protocol* is set to **HTTP Mode**
7. Click **Update**

8. Now click **Modify** next to the newly created VIP
9. Set *Persistence Mode* to **Application Cookie**
10. Set *Application Cookie Name* to **JSESSIONID**
11. Set *Application Persistence Timeout* to **5** (i.e. 5 minutes)
12. Click **Update**

b) Setting up 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:

Label	<input type="text" value="Security1"/>	?
Real Server IP Address	<input type="text" value="192.168.100.100"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

3. Enter an appropriate label for the RIP, e.g. **Security1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.100**
5. Change the *Real Server Port* field to **443**
6. Enable the *Encrypted Backend* checkbox
7. Click **Update**
8. Repeat the above steps to add your other Security Server(s)

Export the certificate from a Security Server

First, export the SSL Certificate from one of your Security Servers – note the following points when exporting the certificate from Windows:

- Make sure that the private key is included
- Tick the option '*Include all certificates in the certification path if possible*'

Next, import the SSL Certificate to the Load Balancer:

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**
2. Select the *Upload prepared PEM/PFX file* option

ADD A NEW SSL CERTIFICATE

I would like to:
☒ Upload prepared PEM/PFX file
☐ Create A New SSL Certificate (CSR)

Label

File to upload
 ViewSecurity1.pfx

PFX File Password

Add Certificate

- Enter an appropriate *label* (name), e.g. **ViewSecurity**
- Browse to and select the relevant .pfx file
- Enter the relevant password if the certificate file is password protected
- Click **Add Certificate**

Configure SSL Termination

- Using the WUI, navigate to: *Cluster Configuration > SSL Termination*
- Click **Add a new Virtual Service**

for v8.3.2 and earlier:

- Enter the following details:

Label	<input type="text" value="ViewExternalSSL"/>	?
SSL Certificate	<input type="text" value="ViewSecurity"/>	?
Virtual Service IP Address	<input type="text" value="192.168.100.10"/>	?
Virtual Service Port	<input type="text" value="443"/>	?
Backend Virtual Service IP Address	<input type="text" value="192.168.100.10"/>	?
Backend Virtual Service Port	<input type="text" value="80"/>	?
Ciphers to use	<input type="text" value="ECDHE-RSA-AES256-SHA384:ECDHE-"/>	?
SSL Terminator	<input type="radio"/> Pound <input checked="" type="radio"/> STunnel	?

- Enter an appropriate label for the VIP, e.g. **ViewExternalSSL**
- Select the SSL certificate just uploaded
- Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.100.10**
- Set the *Virtual Service Ports* field to **443**
- Set the *Backend Virtual Service IP Address* field to same IP address, e.g. **192.168.100.10**

7. Set the *Backend Virtual Service Port* field to **80**
8. Leave other fields at their default values
9. Click **Update**

for v8.3.3 and later:

1. Enter the following details:

Label	<input type="text" value="ViewExternalSSL"/>	?
Associated Virtual Service	<input type="text" value="ViewExternal"/>	?
Virtual Service Port	<input type="text" value="443"/>	?
SSL Operation Mode	<input type="text" value="High Security"/>	?
SSL Certificate	<input type="text" value="ViewSecurity"/>	?

2. Enter a suitable Label (name) for the VIP, e.g. **ViewExternalSSL**
3. Set *Associated Virtual Service* to the Layer 7 VIP created earlier, e.g. **ViewExternal**
4. Leave *Virtual Service Port* set to **443**
5. Leave *SSL Operation Mode* set to **High Security**
6. Select the SSL certificate uploaded previously using the *SSL Certificate* drop-down
7. Click **Update**

Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect VMware Blast users who attempt to connect to **http://<URL to access VIEW>** to **https://<URL to access VIEW>**. For details on configuring this, please refer to section 1 in the Appendix on page [42](#).

Finalizing the Configuration

To apply the new settings, reload HAProxy and STunnel using the **Reload** buttons in the blue commit changes box at the top of the screen.

11. Configuring for Horizon View Internal Clients

Internal clients connect to View Connection Servers. This section covers the various methods for load balancing Connection Servers.

Method 1 – Load Balanced Phase 1 (Using Source IP Persistence)

Connection Server Configuration

For each Connection Server leave the servers own IP address/DNS FQDN and un-check all checkboxes as shown below:

Edit View Connection Server Settings

General Local Mode Authentication Backup

Tags

Tags can be used to restrict which pools can be accessed through this Connection Server.

Tags: Separate tags with ; or ,

HTTP(S) Secure Tunnel

☐ Use Secure Tunnel connection to desktop

External URL: Example: https://myserver.com:443 ?

PCoIP Secure Gateway

☐ Use PCoIP Secure Gateway for PCoIP connections to desktop

PCoIP External URL: Example: 10.0.0.1:4172 ?

Blast Secure Gateway

☐ Use Blast Secure Gateway for HTML access to desktop ?

Blast External URL: Example: https://myserver.com:8443 ?

OK Cancel

Appliance Configuration

Port Requirements

The following table shows the ports that must be load balanced.

Port	Protocol	Uses
443	TCP	HTTPS

Configure Layer 7 Global Settings

The Client Timeout and Server Timeout values should be changed from their default values of 43 seconds and 45 seconds respectively to 5 minutes. To do this follow the steps below:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*

Lock HAProxy Configuration (Deprecated)	<input type="checkbox"/>	?
Logging	Off	?
Redispatch	<input checked="" type="checkbox"/>	?
Connection Timeout	4000 ms	?
Client Timeout	300000 ms	?
Real Server Timeout	300000 ms	?

- Change *Client Timeout* to **300000** as shown above (i.e. 5 minutes)
*N.B. You can also enter **5m** rather than 300000*
- Change *Real Server Timeout* to **300000** as shown above (i.e. 5 minutes)
*N.B. You can also enter **5m** rather than 300000*
- Click the **Update** button to save the settings

Configure the Virtual Service & Real Servers

a) Setting up the Virtual Service

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

Label	ViewInternal	?
Virtual Service	IP Address	192.168.100.10
	Ports	443
Layer 7 Protocol	TCP Mode	?
Manual Configuration	<input type="checkbox"/>	?

- Enter an appropriate label for the VIP, e.g. **ViewInternal**
- Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.100.10**
- Set the *Virtual Service Ports* field to **443**
- Set the *Layer 7 Protocol* to **TCP Mode**
- Click **Update**

b) Setting up 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:

Label	<input type="text" value="Connection1"/>	?
Real Server IP Address	<input type="text" value="192.168.100.101"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

3. Enter an appropriate label for the RIP, e.g. **Connection1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.101**
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 HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect VMware Blast users who attempt to connect to **http://<URL to access VIEW>** to **https://<URL to access VIEW>**. For details on configuring this, please refer to section 1 in the Appendix on page [42](#).

Finalizing the Configuration

To apply the new settings, reload HAProxy using the **Reload** button in the blue commit changes box at the top of the screen.

Method 2 – Load Balanced Phase 1 (Using Application cookie Persistence)

Connection Server Configuration

For each Connection Server leave the servers own IP address/DNS FQDN and uncheck all checkboxes as shown below:

Edit View Connection Server Settings

General
Local Mode
Authentication
Backup

Tags
Tags can be used to restrict which pools can be accessed through this Connection Server.
Tags: Separate tags with ; or ,

HTTP(S) Secure Tunnel
☐ Use Secure Tunnel connection to desktop
External URL: Example: https://myserver.com:443 ?

PCoIP Secure Gateway
☐ Use PCoIP Secure Gateway for PCoIP connections to desktop
PCoIP External URL: Example: 10.0.0.1:4172 ?

Blast Secure Gateway
☐ Use Blast Secure Gateway for HTML access to desktop ?
Blast External URL: Example: https://myserver.com:8443 ?

OK Cancel

Reading the Application Cookie

It is possible to configure each Connection Server to listen on port 80 for HTTP connections using the `serverProtocol=http` directive in the `locked.properties` file, then terminate SSL on the load balancer and pass unencrypted HTTP connections to the Connection Servers. However, to avoid making this change to each Connection Server it's possible to configure the load balancer to re-encrypt the data using the default self-signed cert on each server so that connections are made using HTTPS which is the default.

Appliance Configuration

Port Requirements

The following table shows the ports that must be load balanced.

Port	Protocol	Uses
443	TCP	HTTPS

Configure Layer 7 Global Settings

The Client Timeout and Server Timeout values should be changed from their default values of 43 seconds and 45 seconds respectively to 5 minutes. To do this follow the steps below:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*

Lock HAProxy Configuration (Deprecated)	<input type="checkbox"/>	?
Logging	Off ▾	?
Redispatch	<input checked="" type="checkbox"/>	?
Connection Timeout	4000 ms	?
Client Timeout	300000 ms	?
Real Server Timeout	300000 ms	?

2. Change *Client Timeout* to **300000** as shown above (i.e. 5 minutes)
*N.B. You can also enter **5m** rather than 300000*
3. Change *Real Server Timeout* to **300000** as shown above (i.e. 5 minutes)
*N.B. You can also enter **5m** rather than 300000*
4. Click the **Update** button to save the settings

Configure the Virtual Service & Real Servers

a) Setting up 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:

Label	ViewInternal	?	
Virtual Service	IP Address	192.168.100.10	?
	Ports	80	?
Layer 7 Protocol	HTTP Mode ▾	?	
Manual Configuration	<input type="checkbox"/>	?	
		Cancel Update	

3. Enter an appropriate label for the VIP, e.g. **ViewInternal**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.100.10**
5. Set the *Virtual Service Ports* field to **80**

6. Click **Update**
7. Now click **Modify** next to the newly created VIP
8. Set *Persistence Mode* to **Application Cookie**
9. Set *Application Cookie Name* to **JSESSIONID**
10. Set *Application Persistence Timeout* to **5** (i.e. 5 minutes)
11. Click **Update**

b) Setting up 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:

Label	<input type="text" value="Connection1"/>	?
Real Server IP Address	<input type="text" value="192.168.100.101"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

3. Enter an appropriate label for the RIP, e.g. **Connection1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.101**
5. Change the *Real Server Port* field to **443**
6. Enable the *Encrypted Backend* checkbox
7. Click **Update**
8. Repeat the above steps to add your other Connection Server(s)

Export the certificate from a Connection Server

First, export the SSL Certificate from one of your Connection Servers – note the following points when exporting the certificate from Windows:

- Make sure that the private key is included
- Tick the option '*Include all certificates in the certification path if possible*'

Next, import the SSL Certificate to the Load Balancer:

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**
2. Select the *Upload prepared PEM/PFX file* option

ADD A NEW SSL CERTIFICATE

I would like to:
☒ Upload prepared PEM/PFX file
☐ Create A New SSL Certificate (CSR)

Label

File to upload
 ViewConnection1.pfx

PFX File Password

Add Certificate

- Enter an appropriate *label* (name), e.g. **ViewConnection**
- Browse to and select the relevant .pfx file
- Enter the relevant password if the certificate file is password protected
- Click **Add Certificate**

Configure SSL Termination

- Using the WUI, navigate to: *Cluster Configuration > SSL Termination*
- Click **Add a new Virtual Service**

for v8.3.2 and earlier:

- Using the WebUI, navigate to: *Cluster Configuration > SSL Termination* and click **Add a New Virtual Service**
- Enter the following details:

Label	<input type="text" value="ViewInternalSSL"/>	?
SSL Certificate	<input type="text" value="ViewConnection"/>	?
Virtual Service IP Address	<input type="text" value="192.168.100.10"/>	?
Virtual Service Port	<input type="text" value="443"/>	?
Backend Virtual Service IP Address	<input type="text" value="192.168.100.10"/>	?
Backend Virtual Service Port	<input type="text" value="80"/>	?
Ciphers to use	<input type="text" value="ECDHE-RSA-AES256-SHA384:ECDHE-"/>	?
SSL Terminator	<input type="radio"/> Pound <input checked="" type="radio"/> STunnel	?

- Enter an appropriate label for the VIP, e.g. **ViewInternalSSL**
- Select the SSL certificate just uploaded
- Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.100.10**

6. Set the *Virtual Service Ports* field to **443**
7. Set the *Backend Virtual Service IP Address* field to same IP address, e.g. **192.168.100.10**
8. Set the *Backend Virtual Service Port* field to **80**
9. Leave other fields at their default values
10. Click **Update**

for v8.3.3 and later:

1. Enter the following details:

Label	<input type="text" value="ViewInternalSSL"/>	?
Associated Virtual Service	<input type="text" value="ViewInternal"/>	?
Virtual Service Port	<input type="text" value="443"/>	?
SSL Operation Mode	<input type="text" value="High Security"/>	?
SSL Certificate	<input type="text" value="ViewConnection"/>	?

2. Enter a suitable Label (name) for the VIP, e.g. **ViewInternalSSL**
3. Set *Associated Virtual Service* to the Layer 7 VIP created earlier, e.g. **ViewInternal**
4. Leave *Virtual Service Port* set to **443**
5. Leave *SSL Operation Mode* set to **High Security**
6. Select the SSL certificate uploaded previously using the *SSL Certificate* drop-down
7. Click **Update**

Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect VMware Blast users who attempt to connect to **http://<URL to access VIEW>** to **https://<URL to access VIEW>**. For details on configuring this, please refer to section 1 in the Appendix on page [42](#).

Finalizing the Configuration

To apply the new settings, reload HAProxy and STunnel using the **Reload** buttons in the blue commit changes box at the top of the screen.

12. Testing & Verification

Using System Overview

The System Overview is accessed using the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the View 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 Connection Servers are healthy and available to accept connections.

Virtual Service	IP	Ports	Protocol	Method	Mode	
ViewInternal	192.168.100.10	443	OTHER TCP	Layer 7	Proxy	
Real Server	IP	Ports	Weight			
Connection1	192.168.100.101	443	1	Drain	Halt	
Connection2	192.168.100.102	443	1	Drain	Halt	

Key: Cluster healthy Cluster needs attention Cluster is down Real Server taken offline

The example below shows that the server 'Connection1' has been put in halt mode, in this situation all connections will be sent to Connection2. Connection1 can be put back online by clicking the 'Online' link.

Virtual Service	IP	Ports	Protocol	Method	Mode	
ViewInternal	192.168.100.10	443	OTHER TCP	Layer 7	Proxy	
Real Server	IP	Ports	Weight			
Connection1	192.168.110.101	443	0	Online		
Connection2	192.168.100.102	443	1	Drain	Halt	

Layer 4 Current Connections Report

The Layer 4 Current Connection report shows all current layer 4 connects 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 View Client is connected via a layer 4 VIP (Method 1).

LAYER 4 CURRENT CONNECTIONS					
Check Status					
IPVS connection entries					
pro	expire	state	source	virtual	destination
TCP	01:36	FIN_WAIT	10.100.1.85:49887	192.168.110.68:443	192.168.110.101:443
TCP	01:16	TIME_WAIT	10.100.1.85:49891	192.168.110.68:4172	192.168.110.101:4172
TCP	01:32	FIN_WAIT	10.100.1.85:49885	192.168.110.68:443	192.168.110.101:443
TCP	01:39	FIN_WAIT	10.100.1.85:49888	192.168.110.68:443	192.168.110.101:443
UDP	05:00	UDP	10.100.1.85:50002	192.168.110.68:4172	192.168.110.101:4172
TCP	14:43	ESTABLISHED	10.100.1.85:49886	192.168.110.68:443	192.168.110.101:443
TCP	00:16	TIME_WAIT	10.100.1.85:49883	192.168.110.68:443	192.168.110.101:443
IP	04:16	NONE	10.100.1.85:0	0.0.0.1:0	192.168.110.101:0

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*.

LAYER 4 STATUS

Check Status

Virtual Service Real Server Forwarding Method Weight Active Connections Inactive Connections

ViewExternal

port /fwm

Connection1
192.168.120.101
port 443

Masq

1

0

0

Connection2
192.168.120.102
port 443

Masq

1

0

0

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 2611

> General process information

pid = 2611 (process #1, nbproc = 1)
uptime = 0d 0h22m58s
system limits: memmax = unlimited; ulimit-n = 81000
maxsock = 80033; maxconn = 40000; maxpipes = 0
current conns = 2; current pipes = 0/0; conn rate = 2/sec
Running tasks: 1/11; idle = 100 %

active UP
active UP, going down
active DOWN, going up
active or backup DOWN
active or backup DOWN for maintenance (MAINT)
backup UP
backup UP, going down
backup DOWN, going up
not checked

Display option:

- [Hide 'DOWN' servers](#)
- [Refresh now](#)
- [CSV export](#)

External resources:

- [Primary site](#)
- [Updates \(v1.5\)](#)
- [Online manual](#)

Note: UP with load-balancing disabled is reported as "NOLB".

ViewInternal

	Queue			Session rate			Sessions			Bytes		Denied		Errors		Warnings		Server												
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle	
Frontend				0	0	-	0	0	0	40 000	0	0	0	0	0	0	0	0	0	0	0	OPEN								
backup	0	0	-	0	0	0	0	0	-	0	0	0	0	0	0	0	0	0	0	0			1	-	Y					-
Connection1	0	0	-	0	0	0	0	0	-	0	0	0	0	0	0	0	0	0	0	0	2s UP	L4OK in 0ms	1	Y	-	0	1	19m18s	-	
Connection2	0	0	-	0	0	0	0	0	-	0	0	0	0	0	0	0	0	0	0	0	22m58s UP	L4OK in 0ms	1	Y	-	0	0	0	0s	-
Backend	0	0	0	0	0	0	0	0	4 000	0	0	0	0	0	0	0	0	0	0	0	22m58s UP		2	2	1		0	0	0s	

stats

	Queue		Session rate		Sessions				Bytes		Denied		Errors		Warnings		Server									
	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend			2	2	-	2	2 000	5	1 406	28 486	0	0	0	0	0	0	0	OPEN								
Backend	0	0	0	0	0	0	200	0	1 406	28 486	0	0	0	0	0	0	0	22m58s UP		0	0	0		0		

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 its 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*.

13. 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.

14. Further Documentation

The Administration Manual contains much more information about configuring and deploying the appliance. It's available here: <http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf>

15. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced VMware Horizon View environments.

16. Appendix

1 – Configuring an HTTP to HTTPS redirect

An additional later 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://view.robstest.com> should be redirected to <https://view.robstest.com>

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**

2 – Clustered Pair Configuration – Adding a Slave Unit

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

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

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs

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

Version 7:


Please refer to **Chapter 8 – Appliance Clustering for HA** in the [v7 Administration Manual](#).

Version 8:

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

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: *Cluster Configuration > High-Availability Configuration*

CREATE A CLUSTERED PAIR



Local IP address

192.168.1.20 ▼

IP address of new peer

192.168.1.21


Password for *loadbalancer* user on peer

.....


Add new node

- Specify the IP address and the *loadbalancer* users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above
- Click **Add new node**
- The pairing process now commences as shown below:

CREATE A CLUSTERED PAIR



192.168.120
loadbalancer.org



192.168.121
loadbalancer.org

Attempting to pair..

Local IP address

192.168.120

IP address of new peer

192.168.121


Password for loadbalancer user on peer

.....


configuring

- Once complete, the following will be displayed:

HIGH AVAILABILITY CONFIGURATION - MASTER



192.168.120
loadbalancer.org



192.168.121
loadbalancer.org

Break Clustered Pair

- To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen

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

Note: Please refer to chapter 9 – Appliance Clustering for HA in the [Administration Manual](#) for more detailed information on configuring HA with 2 appliances.

17. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.4.0	14 August 2019	Styling and layout	General styling updates	RJC
1.4.1	17 January 2020	Added note explaining how to disable "Secure Mode" to unlock the firewall script page	Required update	RJC
1.4.2	21 July 2020	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH

About Loadbalancer.org

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



United Kingdom

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

United States

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

Canada

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

Germany

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