LOADBALANCER

QUICK GUIDE

Load Balancing NGINX Web Servers with OWASP Top 10 WAF in AWS

Version 1.3.0

Table of Contents

1. About this Guide . . . 3
2. Software Versions Supported . . . 3
    2.1. Loadbalancer.org Appliance . . . 3
    2.2. Nginx Server . . . 3
3. Related Documentation . . . 3
4. Load Balanced Ports / Services . . . 3
5. VPC Security Group inbound rules . . . 3
6. Appliance Configuration Overview . . . 3
    6.1. Operation Mode . . . 3
    6.2. SSL Termination / Re-encryption . . . 4
    6.3. Web Server Health-check . . . 4
    6.4. Deployment Concept . . . 4
7. Deploying & Accessing the Appliance . . . 4
    7.1. Deployment . . . 4
    7.2. Accessing the Appliance WebUI . . . 4
        7.2.1. WebUI Menu Options . . . 6
8. Appliance Configuration . . . 6
    8.1. Configure the Virtual Service (VIP) . . . 7
    8.2. Define the Real (Nginx) Servers . . . 7
    8.3. Upload the Public SSL Certificate . . . 8
    8.4. Configure the STunnel Virtual Service (VIP) . . . 9
    8.5. Configure the WAF . . . 9
    8.6. Apply the New Settings . . . 10
    8.7. Associate the VIP with an Elastic IP Address . . . 10
9. Testing . . . 10
10. Logging Client Source IP Addresses in Nginx . . . 10
11. Loadbalancer.org Technical Support . . . 11
12. Document Revision History . . . 12

1. About this Guide

This document provides a quick reference guide on how to load balance Nginx Web Servers and configure a WAF using the Enterprise AWS Loadbalancer.org Amazon cloud appliance.

- The WAF addresses the OWASP Top 10 vulnerabilities and is very quick and simple to deploy.
- SSL offload is handled by STunnel, HAProxy handles back-end server re-encryption.

2. Software Versions Supported

2.1. 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.

2.2. Nginx Server

- All versions

3. Related Documentation

For additional information, please refer to the Administration Manual and the AWS Quickstart Configuration Guide.

4. Load Balanced Ports / Services

Port	Use	Transport Layer Protocol
80	HTTP	TCP
443	HTTPS	TCP

5. VPC Security Group inbound rules

The following inbound rules must be configured in your Security Group:

- For Management: TCP 9443 (Appliance WebUI)
- For access to the load balanced Web Services: TCP 80 (HTTP), TCP 443 (HTTPS)

6. Appliance Configuration Overview

6.1. Operation Mode

The load balancer is configured using layer 7 SNAT mode. This mode does not require any mode specific configuration changes to the load balanced Real Servers.

6.2. SSL Termination / Re-encryption

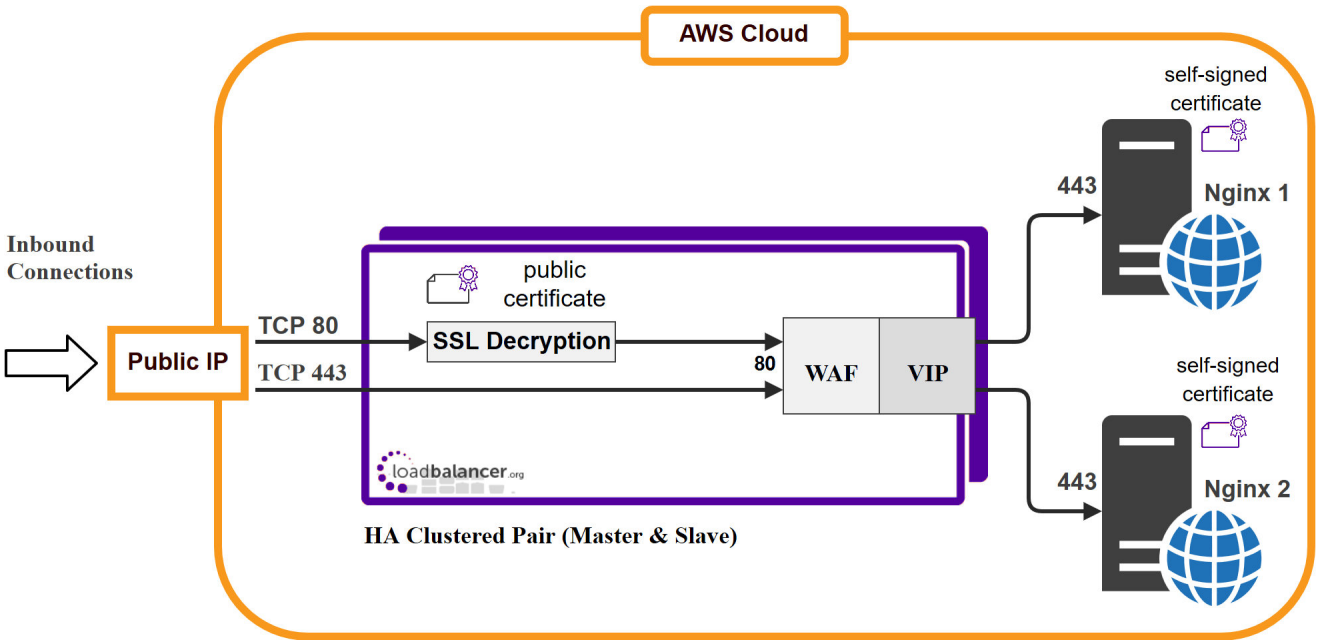
SSL Termination is configured on the load balancer. This provides a corresponding HTTPS Virtual Service on port 443. Decrypted traffic is then passed to the WAF for inspection and then to the Layer VIP for load balancing and re-encryption to the Nginx Servers.

6.3. Web Server Health-check

A HTTPS negotiate health-check is used to verify that each Nginx Server is available.

6.4. Deployment Concept

The diagram below shows how the system is configured.



7. Deploying & Accessing the Appliance

7.1. Deployment

Deploy the Loadbalancer.org appliance as described in the AWS Quickstart Configuration Guide.

7.2. Accessing the Appliance WebUI

Using a browser, navigate to the public IP address or public DNS name on port 9443:

https://<Public IP address>:9443

or

https://<Public DNS name>:9443

> **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.

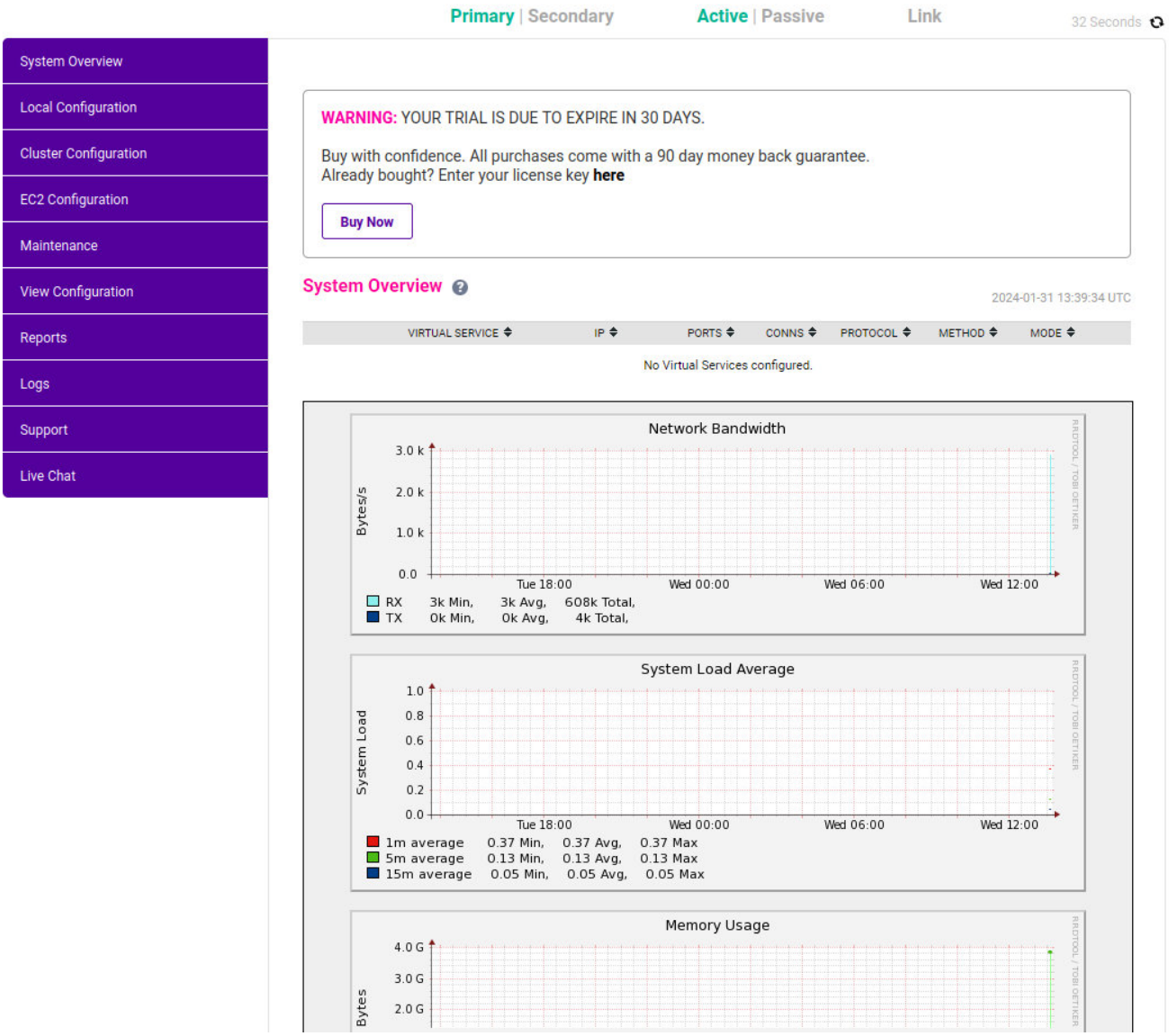
> **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

Log in to the WebUI using the following default credentials:

Username: loadbalancer
Password: <EC2 Instance-ID>

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

Once logged in, the WebUI is displayed:



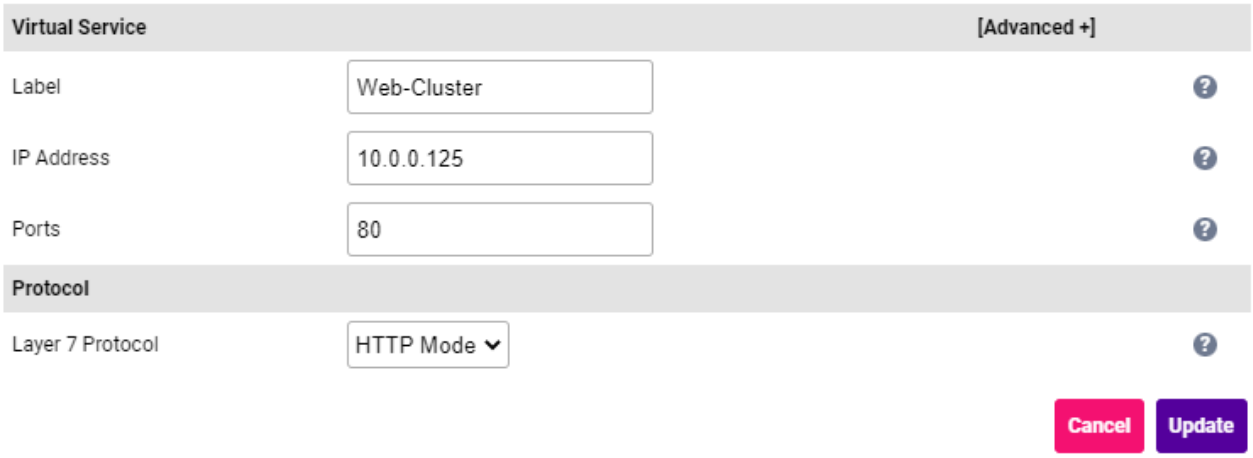
7.2.1. WebUI Menu Options

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
EC2 Configuration - Configure AWS specific settings
Maintenance - Perform maintenance tasks such as service restarts and taking backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links
Live Chat - Start a Live Chat session with one of our Support Engineers

8. Appliance Configuration

8.1. Configure the Virtual Service (VIP)

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 the required *Label* (name) for the VIP, e.g. **Web-Cluster**.
4. Set the *Virtual Service IP Address* field to an appropriate value, e.g. **10.0.0.125**.
5. Set the *Virtual Service Ports* field to the required port, e.g. **443**.
6. Leave *Layer 7 Protocol* set to **HTTP Mode**.
7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Scroll to the *Health Checks* section.
   - Set *Health Checks* to **Negotiate HTTPS (GET)**.
   - Leave *Request to Send* blank.

> **Note** Leaving *Request to Send* blank will send the health check request to the Web Server's root directory. Change this if needed.

   - Leave *Response Expected* blank.

> **Note** Leaving *Response Expected* blank will mean that all HTTP 2xx (usually HTTP 200) and HTTP 3xx responses will be considered as valid and the server will be marked as up.

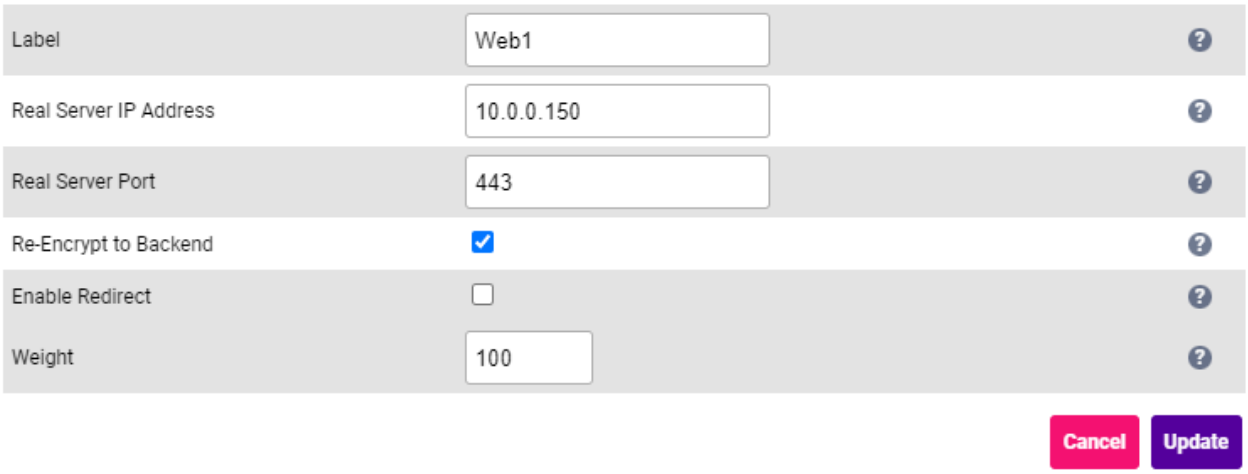
10. Click **Update**.

8.2. Define the Real (Nginx) 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.

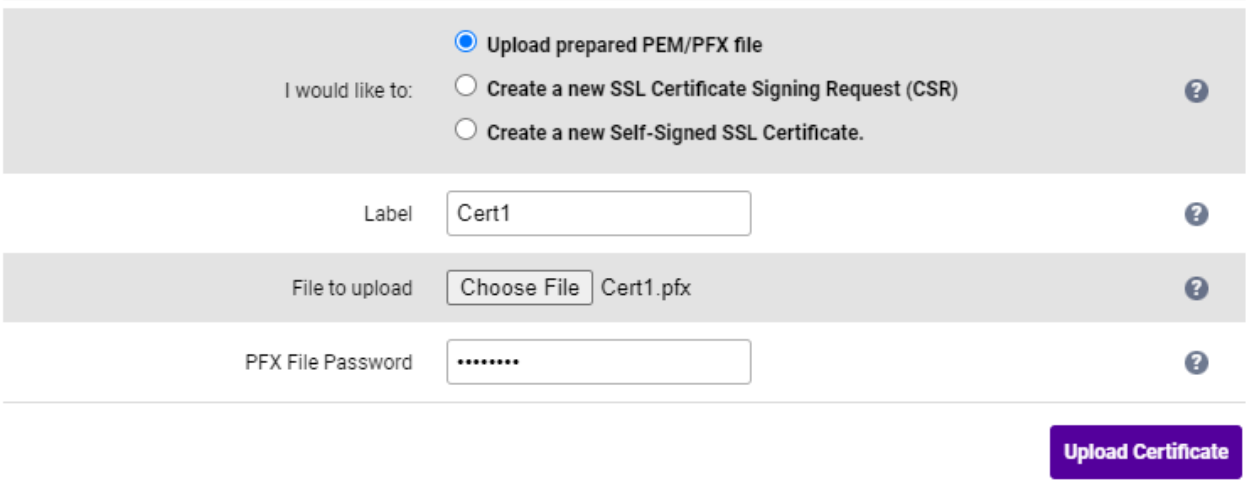
2. Enter the following details:



3. Enter an appropriate label for the Real Server , e.g. **Web1**.
4. Set the *Real Server IP Address* field to the required address, e.g. **10.0.0.150**.
5. Set the *Real Server Port* to **443**.
6. Enable (check) **Re-Encrypt to Backend**.
7. Click **Update**.
8. Repeat the above steps to add your other Nginx Server(s).

8.3. Upload the Public SSL Certificate

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificate* and click **Add a New SSL Certificate**.
2. Select **Upload prepared PEM/PFX file**.
3. Enter the following details:



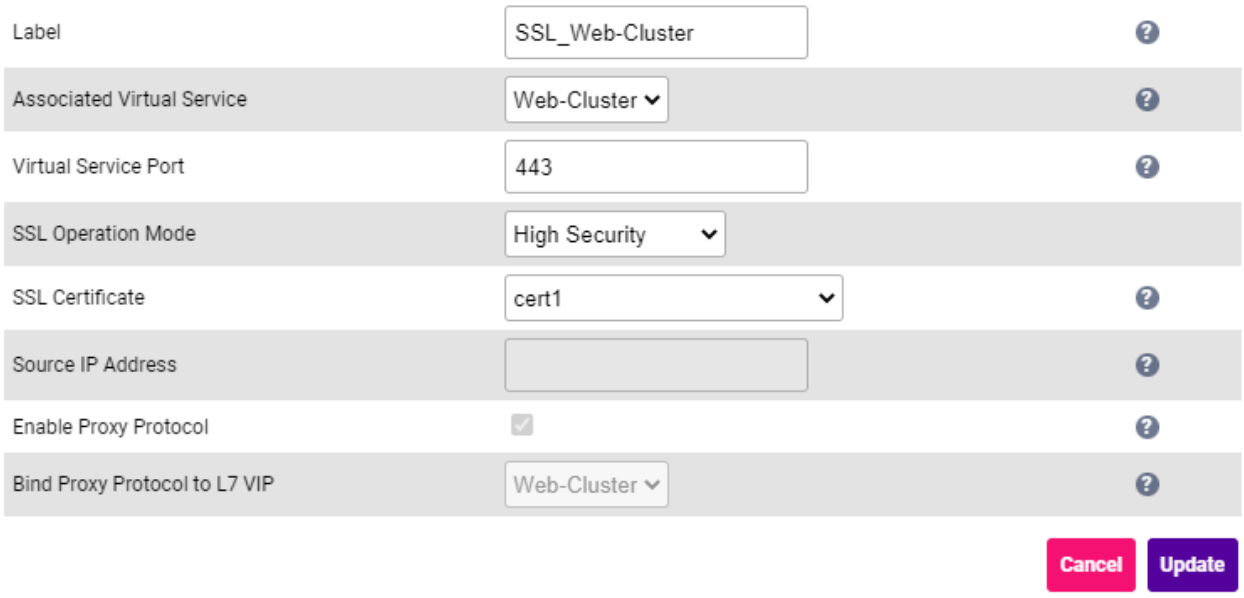
4. Specify and Label (name) for the certificate, e.g. **Cert1**.

5. Click **Choose File** and browse to and select the relevant PFX or PEM file.
6. Enter the *PFX file Password*.
7. Click **Upload Certificate**.

8.4. Configure the STunnel Virtual Service (VIP)

STunnel is used to terminate SSL on the load balancer.

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



3. Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **Web-Cluster**.

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

4. Ensure that the *Virtual Service Port* is set to **443**.
5. Leave *SSL Operation Mode* set to **High Security**.
6. Select the *SSL Certificate* uploaded previously.
7. Click **Update**.

8.5. Configure the WAF

1. Using the WebUI, navigate to: *Cluster Configuration > WAF – Gateway* and click **Add a New WAF Gateway**.
2. Enter the following details:

3. Select the VIP created previously, e.g. **Web-Cluster**.

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

4. Click **Update**.

> **Note** By default the WAF setting *Rule Engine Traffic Blocking* is disabled when the WAF is created. While disabled this option ensures that the ModSecurity Rule Engine logs any critical errors but does not block any requests. You should leave the WAF in this mode until you are confident that the error logs are not showing false positives. Once you are confident it can be enabled and the WAF will start blocking any malicious requests with a 403 Forbidden response. To enable this setting, click **Modify** next to the WAF gateway, check the *Rule Engine Traffic Blocking* option and click **Update**.

8.6. Apply the New Settings

To apply the new settings, HAProxy, STunnel and the WAF must be reloaded. This can be done using the button 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**.
4. Click **Reload WAF**.

8.7. Associate the VIP with an Elastic IP Address

1. Using the EC2 Management Console, allocate a new Elastic IP address.
2. Now associate this address with the VIP, in this case **10.0.0.150**.

9. Testing

The load balanced Nginx Web Servers should now be accessible on ports 80 & 443 using the EIP address or corresponding public DNS name.

10. Logging Client Source IP Addresses in Nginx

Nginx can be configured to store the value of X-Forwarded-For headers for incoming web traffic. These headers are added by default by the load balancer. This allows upstream servers and network devices to see the real source IP addresses of clients, even though the load balancer is acting as a proxy.

For full details on how to configure Nginx for this, see our blog post:

https://www.loadbalancer.org/blog/nginx-and-x-forwarded-for-header/

11. Loadbalancer.org 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.

12. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.1.0	4 November 2019	Styling and layout	General styling updates	AH
1.1.1	27 August 2020	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH
1.2.0	1 September 2022	Converted the document to AsciiDoc Updated links and instructions where necessary	Move to new documentation system Required updates	AH
1.2.1	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.2.2	5 January 2023	Added one level of section numbering	Housekeeping across all documentation	AH
1.2.3	2 February 2023	Updated screenshots	Branding update	AH
1.2.4	23 March 2023	Improved document structure Updated various configuration steps	Document standardization Product feature updates	RJC
1.3.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

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.