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

v1.1.1

Quick Reference Guide
# Contents

- **About this Guide**: 3
- **Related Documentation**: 3
- **Load Balanced Ports**: 3
- **VPC Security Group inbound rules**: 3
- **Load Balancer Configuration**: 3
  - Deploy the Loadbalancer.org AWS Appliance: 3
  - Accessing The Appliance WebUI: 3
  - Configuration Diagram: 5
  - Configure the Virtual Service (VIP): 5
  - Define the Real (Nginx) Servers: 6
  - Upload the Public SSL Certificate: 6
  - Configure the STunnel Virtual Service (VIP): 7
  - Configure the WAF: 7
  - Apply the New Settings: 8
  - Associate an EIP with the Virtual Services: 8
- **Testing**: 9
- **Logging client source IP addresses IN Nginx**: 9
- **Loadbalancer.org Technical Support**: 10
- **Document Revision History**: 11
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

Related Documentation

For additional information about the Loadbalancer.org AWS Appliance, please also refer to the following documents:

- Administration Manual
- AWS Quick Start Guide

Load Balanced Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Use</th>
<th>Transport Layer Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>HTTP</td>
<td>TCP</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>TCP</td>
</tr>
</tbody>
</table>

VPC Security Group inbound rules

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

- For Management: TCP 22 (SSH), TCP 9443 (Appliance WebUI), 7777 (HAProxy Stats page)
- For Nginx services: TCP 80 (HTTP), TCP 443 (HTTPS)

Load Balancer Configuration

Deploy The Loadbalancer.org AWS Appliance

1. Deploy an AWS Loadbalancer.org appliance as detailed in the Quick Start Guide

Accessing The Appliance WebUI

Using a browser, navigate to the Public DNS name or Public IP address on port 9443, i.e. https://<Public IP address>:9443

You’ll receive a warning about the certificate as it’s a self signed cert not related to an Internet based CA. Confirm you want to continue and a login prompt will be displayed. Use the following default credentials:

Username: loadbalancer
Password: <EC2 Instance-ID>
Note: To change the password for the 'loadbalancer' account, use the WebUI option: Maintenance > Passwords.

Once logged in, the WebUI is displayed:
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:

<table>
<thead>
<tr>
<th>Label</th>
<th>Web1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>10.0.0.125</td>
</tr>
<tr>
<td>Ports</td>
<td>80</td>
</tr>
</tbody>
</table>

3. Enter the required Label (name) for the VIP, e.g. **Web1**
4. Set the Virtual Service IP address field to the required IP address, e.g. **10.0.0.125**
5. Set the Virtual Service Ports field to the required port, e.g. **80**
6. Leave Layer 7 Protocol set to **HTTP Mode**
7. Click **Update**
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:

<table>
<thead>
<tr>
<th>Label</th>
<th>Nginx1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.0.0.150</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>✓</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the Real Server, e.g. Nginx1
4. Set the Real Server IP Address field to the required address, e.g. 10.0.0.150
5. Leave the Real Server Port field blank
6. Enable (check) Re-Encrypt to Backend
7. Click Update
8. Repeat the above steps to add your other Nginx server(s)

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:

<table>
<thead>
<tr>
<th>Label</th>
<th>Cert1</th>
</tr>
</thead>
<tbody>
<tr>
<td>File to upload</td>
<td>Choose file cert1.pfx</td>
</tr>
<tr>
<td>PFX File Password</td>
<td>*********</td>
</tr>
</tbody>
</table>

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 **Add Certificate**

**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:

   ![Virtual Service Configuration](image)

   3. Enter the required *Label* (name) for the Virtual Service, e.g. **SSL1**
   4. Select the required certificate in the *SSL Certificate* drop-down
   5. Set the *Virtual Service IP address* to be the same as the VIP created previously, e.g. **10.0.0.125**
   6. Set the *Virtual Service Port* field to **443**
   7. Set the *Backend Virtual Service IP address* to be the same as the VIP created previously, e.g. **10.0.0.125**
   8. Set the *Backend Virtual Service Port* field to **80**
   9. The other settings can typically be left at their default values
   10. Click **Update**

**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. Web1
4. Specify a suitable WAF label (name), e.g. WAF1
5. Leave Rule Engine Traffic Blocking unchecked for now

Note: While disabled, this option ensures that the ModSecurity Rule Engine logs any critical errors. 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 you can enable this mode and the WAF will start blocking any malicious requests with a 403 Forbidden response.

6. Click Update

**Apply The New Settings**

1. Once the configuration is complete, use the Reload HAProxy, Restart STunnel and Reload WAF buttons at the top of the screen to commit the changes.

**Associate An EIP With The Virtual Services**

An EIP is added and associated with the VIP to provide a public IP address for client connections.

1. Using the WebUI, navigate to: EC2 > EC2 Network Configuration
2. Click Allocate New Elastic IP, this will request an EIP from Amazon using API calls
3. Click [Associate] to associate the EIP to the Virtual Service private IP address
This association is then displayed as shown below:

This association is then displayed as shown below:

**Testing**

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

**Logging client source IP addresses IN Nginx**

The Nginx service on a web server can be configured to store the value of X-Forwaded-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/

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.
## Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.0</td>
<td>4 November 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>27 August 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
</tbody>
</table>
About Loadbalancer.org
Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.

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

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

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

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

© Copyright Loadbalancer.org • www.loadbalancer.org