

How to Configure an Elastic Load Balancer for CloudGen Firewalls in AWS

<https://campus.barracuda.com/doc/22674/>

The Elastic Load Balancer (ELB) is a managed layer 4 load balancer by AWS. The ELB can be deployed as a public-facing load balancer or internally in your VPC. Instances are added either manually or, if associated with an Auto Scaling group, automatically. The load balancer continuously checks the health of the instances and takes unhealthy instances out of rotation.

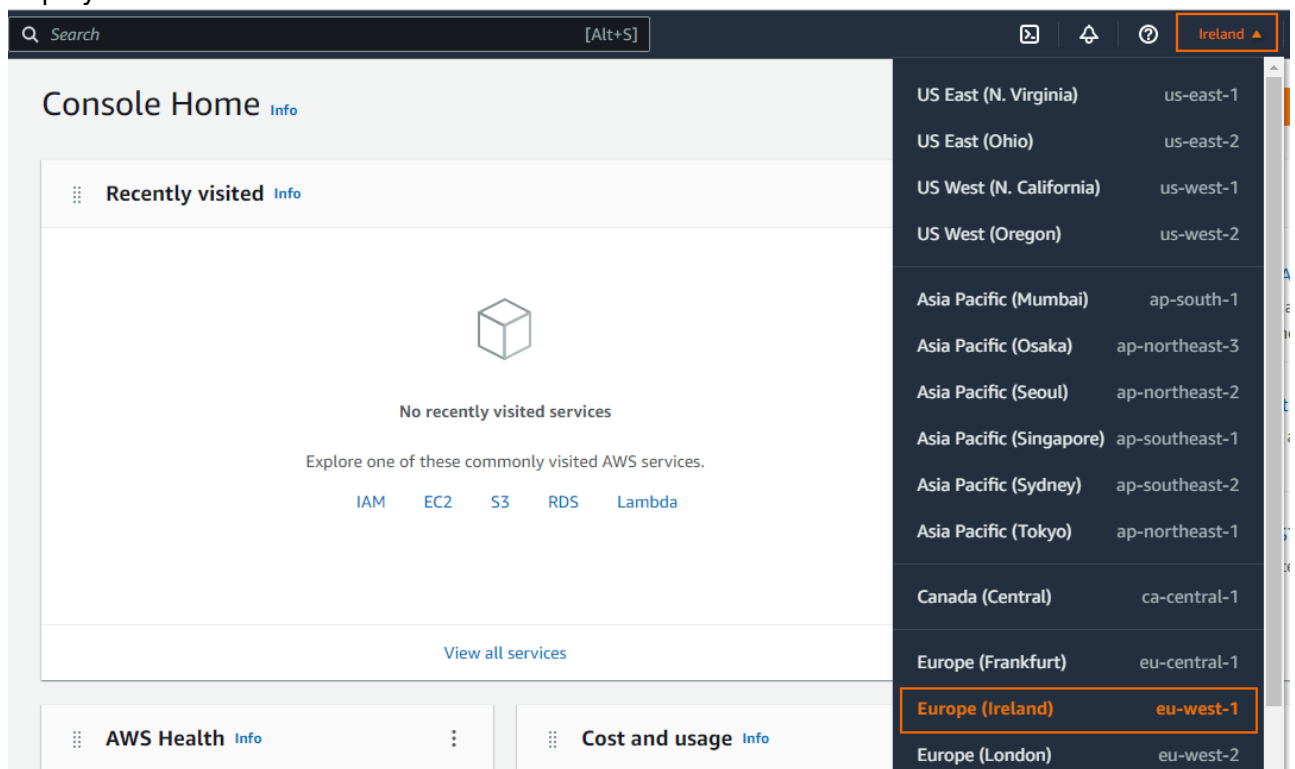
AWS Reference Architectures

This article is used in the following AWS reference architectures:

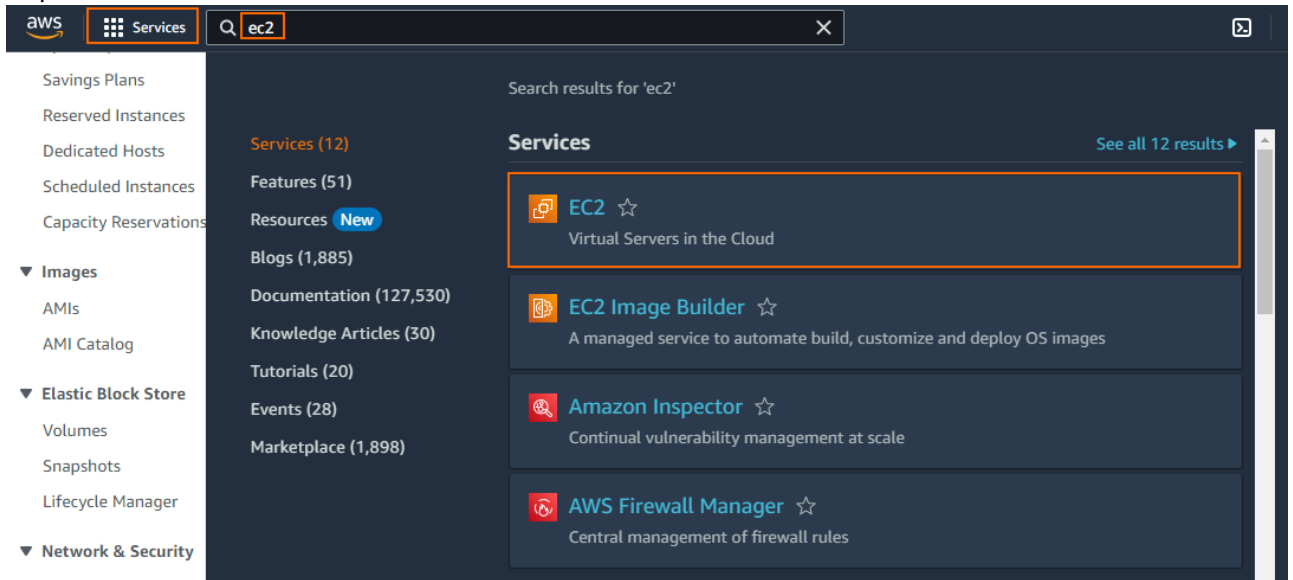
- [AWS Reference Architecture - CloudGen Firewall HA Cluster with Route Shifting](#)

Create an AWS Network Load Balancer

1. Log into the AWS console.
2. In the upper right, click on the datacenter location, and select the datacenter you want to deploy to from the list.

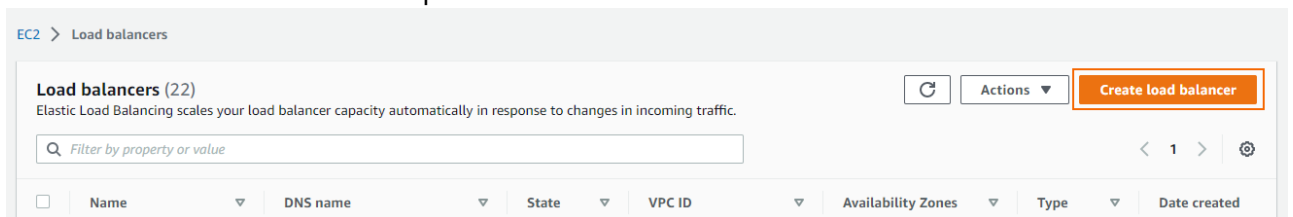


3. Expand **Services** and select **EC2**.



4. In the left menu, expand **Load Balancing** and select **Load Balancers**.

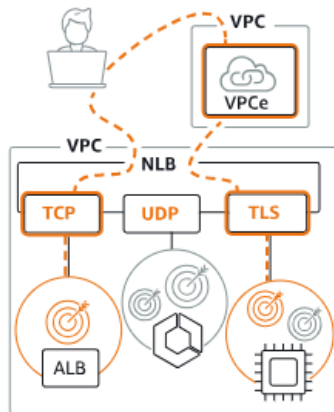
5. The **Load balancers** window opens. Click **Create load balancer**.



6. Under **Network Load Balancer** click **Create**.

Network Load Balancer

[Info](#)



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Create](#)

7. The **Basic configuration** window opens. Enter a unique **Load balancer name**.
8. Select a **Scheme** for your load balancer. For the external load balancer, select **Internet-Facing**.
9. Select the **VPC** the firewalls are deployed to from the list.
10. In the **Mappings** section, select one or more availability zones and define subnets for each zone from the **Subnet** selection menu.

Basic configuration**Load balancer name**

Name must be unique within your AWS account and can't be changed after the load balancer is created.

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme

Scheme can't be changed after the load balancer is created.

☒ **Internet-facing**

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☐ **Internal**

An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type [Info](#)

Select the type of IP addresses that your subnets use.

☒ **IPv4**

Recommended for internal load balancers.

☐ **Dualstack**

Includes IPv4 and IPv6 addresses.

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

vpc-0787e83abb6291ac3

IPv4: 10.0.0.0/24

**Mappings**

Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Zones that are not supported by the load balancer or VPC can't be selected. Subnets can be added, but not removed, once a load balancer is created.

☒ **eu-west-1a (euw1-az1)****Subnet**

Lab033-WKoeck-VPC-subnet-public1-eu-west-1a

11. Select one or more Security groups for your load balancer.**Security groups** [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups - recommended

Security groups support on Network Load Balancers can only be enabled at creation by including at least one security group. You can change security groups after creation. The security groups for your load balancer must allow it to communicate with registered targets on both the listener port and the health check port. For PrivateLink Network Load Balancers, security group rules are enforced on PrivateLink traffic; however, you can turn off inbound rule evaluation after creation within the load balancer's Security tab or using the API.

Select up to 5 security groups

sg-044a3a677822627bd VPC: vpc-0787e83abb6291ac3

If you wish to create a security group, click **create a new security group** and define the following settings:

1. Enter a **Security group name**.
2. Click **Add rule** for each additional security group rule required.
 - **Type / Protocol** – Select the protocol or type of traffic. E.g., **Custom TCP** for TCP, or **HTTPS** for TLS-encrypted web traffic.
 - **Port range** – Enter the port. E.g., 691 for TINA VPN
 - **Source** – Select the source of the traffic. For Internet traffic, select **Anywhere** and

enter 0.0.0.0/0.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
 CGF-ELB-SG
Name cannot be edited after creation.

Description [Info](#)
 Security group for the firewall elastic load balancer

VPC [Info](#)
 vpc-043f10892f33de3bd

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional	
Custom TCP	TCP	691	Anywhere...	0.0.0.0/0	Delete
HTTPS	TCP	443	Anywhere...	0.0.0.0/0	Delete

[Add rule](#)

3. Click **Create security group**.

12. In the **Listener and routing** section, select **TCP**, and enter 807 in the **Port** field. Port 807 is used for Firewall Admin access.

Ports for listening and health checks must provide the same service. When using port 807 as a listener, do NOT use another port, for example 22 (SSH), as target for health checks!

13. Click the **Create target group** link.

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener TCP:807 [Remove](#)

Protocol	Port	Default action	Info
TCP	807 1-65535	Forward to Select a target group	Create target group

14. The **Specify group details** window opens. Specify the following settings:

1. Select **IP addresses** as target type. (When selecting **Instances**, you must select instances as targets instead of IP addresses later.)

[EC2](#) > [Target groups](#) > Create target group

Step 1
Specify group details

Step 2
Register targets

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration
Settings in this section can't be changed after the target group is created.

Choose a target type

☐ Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

☒ IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

2. Enter a **Target group name**, for example: FWAdmin
3. From the **Protocol : Port** list, select **TCP 807**.

This port must provide the same service as the listening port. Do NOT select port 22 (SSH) as a target when using port 807 as listener for the network load balancer.

Target group name

FWAdmin

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

TCP

807

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

☒ IPv4

☐ IPv6

4. Select the **VPC** the firewalls are deployed to from the list.
15. In the **Health checks** section, expand **Advanced health check settings** and configure the following parameters:
 - **Health check protocol** – select **TCP**.
 - **Health check port** – select **Override** and enter 691. This is the VPN port on the firewall and will be used for probing.

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

TCP ▼

▼ Advanced health check settings

Restore defaults

Health check port

The port the load balancer uses when performing health checks on targets. By default, the health check port is the same as the target group's traffic port. However, you can specify a different port as an override.

☐ Traffic port

☒ Override

691 ▼
1-65535

- Leave the other settings as default.

16. Click **Next**.

17. The **Register targets** window opens. Specify the following settings:

- **Network** – Select the VPC the firewalls are deployed to from the list.
- Define subnet IP addresses that should be used as probing targets. For example, enter 10.0.0.6 and 10.0.0.8 for a 10.0.0.0/24 network. (If you have selected **Instances**, select the instances used as targets.)
- **Ports** – Enter the port used for probing. In this case, enter 807 for Firewall Admin.

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

IP addresses

Step 1: Choose a network

You can add IP addresses from the VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of targets from multiple network sources by returning to this step and choosing another network.

Network

Lab033-network-vpc
vpc-0787e83abb6291ac3
IPv4: 10.0.0.0/24

Step 2: Specify IPs and define ports

You can manually enter IP addresses from the selected network.

Enter an IPv4 address from a VPC subnet.

10.0.0.X

Remove

Add IPv4 address

You can add up to 4 more IP addresses.

Ports

Ports for routing to this target.

807

1-65535 (separate multiple ports with commas)

Include as pending below

18. Click **Include as pending below** to add your targets. IP addresses (or instances) and port are then listed in the lower section with **Health status** shown as *Pending*.

Filter targets					Show only pending	
					< 1 >	⚙
Remove IPv4 address	Health status	IP address	Port	Zone		
×	Pending	10.0.0.6	807	eu-west-1a		
×	Pending	10.0.0.8	807	eu-west-1a		

19. Review the targets and click **Create target group**.

The target group is now is now deployed with the network load balancer and ready for use.

Details

arn:aws:elasticloadbalancing:eu-west-1:573972924930:targetgroup/Lab033-WKoeck-CGF-FWAdmin/a983256ba3300bc7

Target type Instance	Protocol : Port TCP: 807	VPC vpc-0787e83abb6291ac3	IP address type IPv4
Load balancer Lab033-WKoeck-ELB			

Total targets 2	Healthy ✔ 1	Unhealthy ✘ 1	Unused ⊖ 0	Initial ⬇ 0	Draining ⊖ 0
--------------------	----------------	------------------	---------------	----------------	-----------------

► **Distribution of targets by Availability Zone (AZ)**
 Select values in this table to see corresponding filters applied to the Registered targets table below.

When a health check is performed in a HA setup, the active unit is reachable via probing and shown as healthy. As soon as a failover happens and the unit goes down, the secondary unit becomes reachable and shows up as healthy in the **Targets** list.

Targets | Monitoring | Health checks | Attributes | Tags

Registered targets (2)

< 1 >

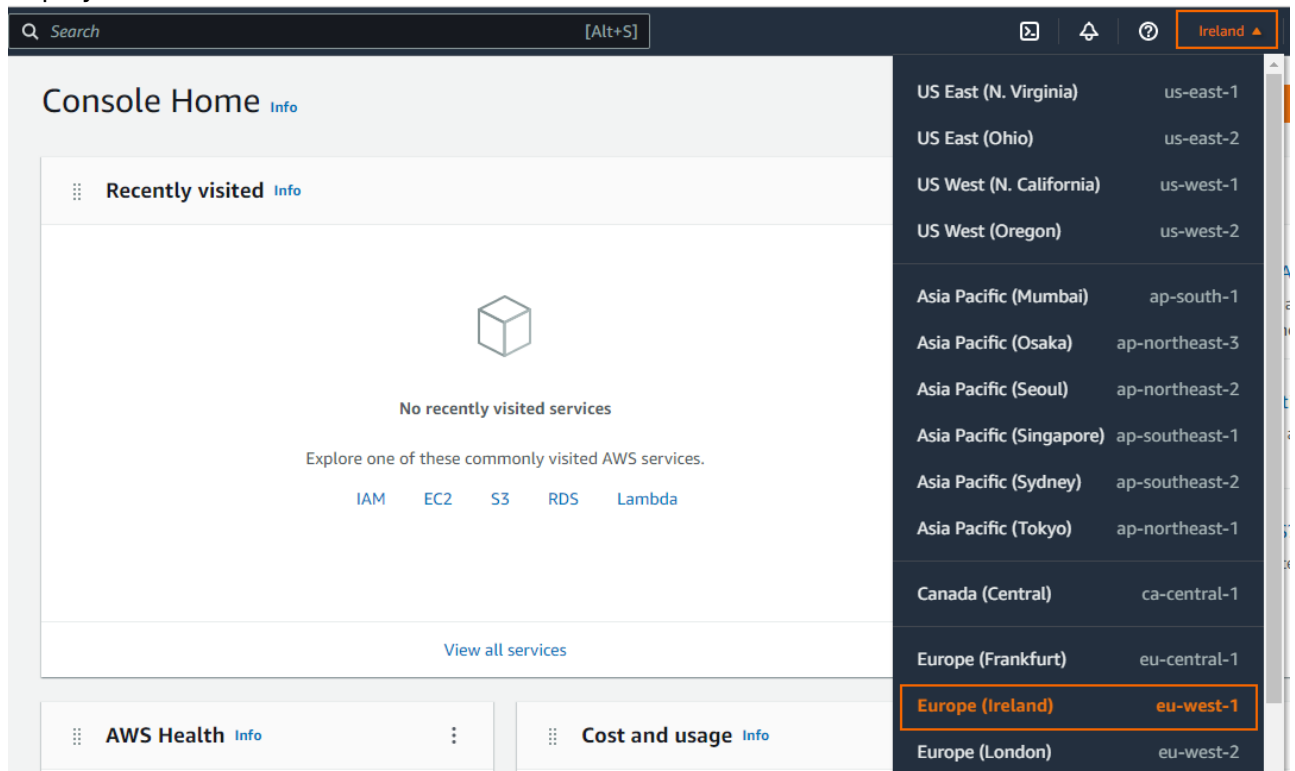
☐	Instanc... ▾	Name ▾	Port ▾	Zone ▾	Health s... ▾	Health status det..
☐	i-033c7a7...	Lab033-WKoeck CGF-AWS	807	eu-west-1a	✘ Unhealthy	Health checks failed
☐	i-0ea1d41...	Lab033-WKoeck CGF-AWS	807	eu-west-1a	✔ Healthy	

Create an AWS Classic Load Balancer

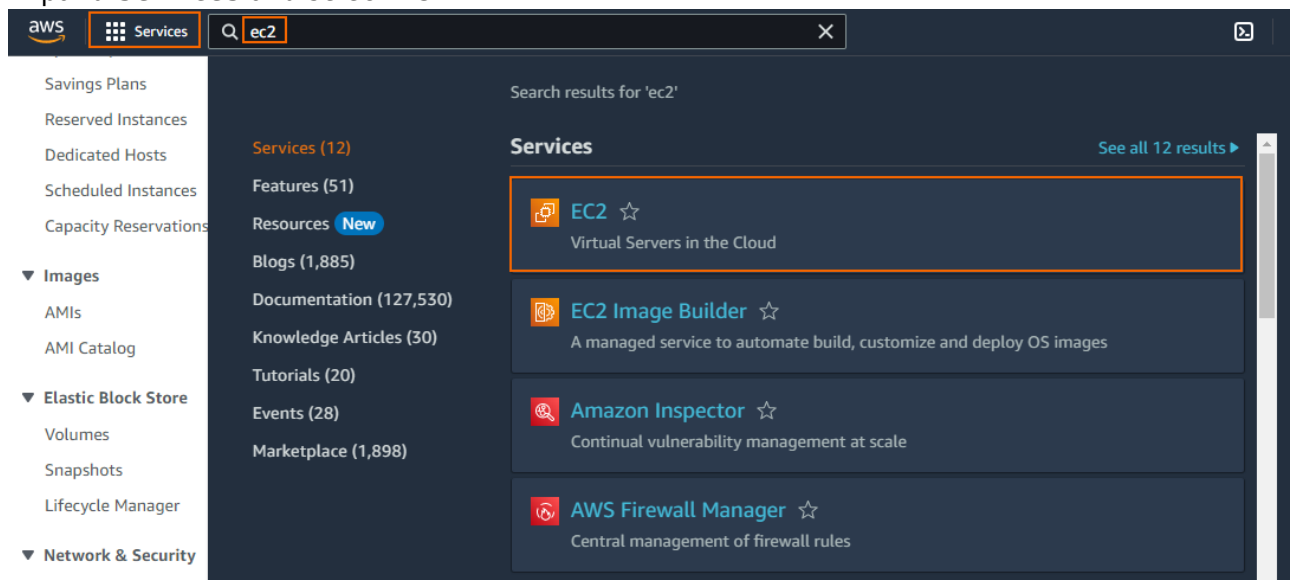
If your setup requires a legacy load balancer configuration, for example, when you have an existing application running in an EC2-Classic network, you can create a classic load balancer. The classic load balancer can be deployed as an external or internal load balancer. By enabling cross-zone loadbalancing, the load balancer spreads out the load evenly over multiple availability zones.

1. Log into the AWS console.
2. In the upper right, click on the datacenter location, and select the datacenter you want to

deploy to from the list.

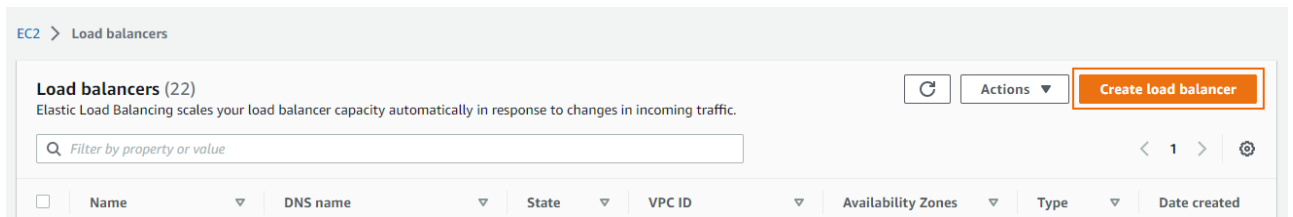


3. Expand **Services** and select **EC2**.



4. In the left menu, expand **Load Balancing** and select **Load Balancers**. The **Load balancers** window opens.

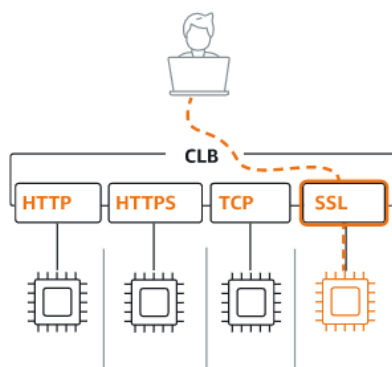
5. Click **Create load balancer**.



6. Expand **Classic Load Balancer** and click **Create**.

▼ Classic Load Balancer - previous generation

Classic Load Balancer [Info](#)



Choose a Classic Load Balancer when you have an existing application running in the EC2-Classical network.

Create

7. Enter the **Basic configuration** settings:

- **Load balancer name** – Enter name for the load balancer.
- Select a **Scheme** for your load balancer.

Internal load balancers are reachable from within the VPC and do not have a public IP address.

- **VPC** – Select the VPC the firewalls are deployed to from the list.
- Select one or more Availability Zones and define subnet for each zone from the **Subnet** selection menu.

Basic configuration**Load balancer name**

Name must be unique within your AWS account and can't be changed after the load balancer is created.

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme [Info](#)

Scheme can't be changed after the load balancer is created.

☐ Internet-facing

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☒ Internal

An internal load balancer routes requests from clients to targets using private IP addresses.

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your network settings.

VPC [Info](#)

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). The selected VPC cannot be changed after the load balancer is created. When selecting a VPC for your load balancer, ensure each subnet has a CIDR block with at least a /27 bitmask and at least 8 free IP addresses. [Learn more](#)

IPv4: 172.31.0.0/16**Mappings**

Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☒ eu-west-1a (euw1-az1)**Subnet**

8. in the **Security groups** section, select one or more security groups for your load balancer, or click **Create a new security group** to create a group:

1. Enter a **Security group name**.
2. Click **Add rule** for each additional security group rule required.
 - **Type / Protocol** – Select the protocol or type of traffic. E.g., **Custom TCP** for TCP, or **HTTPS** for TLS-encrypted web traffic.
 - **Port range** – Enter the port. E.g., 691 for TINA VPN
 - **Source** – Select the source of the traffic. For Internet traffic, select **Anywhere** and enter 0.0.0.0/0.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
 CGF-ELB-SG
Name cannot be edited after creation.

Description [Info](#)
 Security group for the firewall elastic load balancer

VPC [Info](#)
 vpc-043f10892f33de3bd

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional	
Custom TCP	TCP	691	Anywh...		Delete
HTTPS	TCP	443	Anywh...		Delete

[Add rule](#)

3. Click **Create security group**.

9. For each load balancer listener, click **Add listener** and enter:

- **Listener protocol** - Select the protocol from the list. Supported protocols: **HTTP, HTTPS, TCP, TLS (Secure TCP)**.
- **Listener port** - Enter the external port.
- **Instance protocol** - Enter the protocol. In most cases, this is the same protocol as the **Load Balancer Protocol**. To offload TLS encryption to the ELB, different protocols can be selected (e.g, HTTPS to HTTP).
- **Instance port** - Enter the port number of the service on the instance.

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the protocol and port you configure. The settings you define for a listener determine how the load balancer routes requests to its registered targets.

▶ Listener **TCP:691** Instance **TCP:691** [Remove](#)

▼ Listener **HTTPS:443** Instance **HTTP:443** [Remove](#)

Listener protocol	Listener port	Instance protocol	Instance port
HTTPS	443	HTTP	443
1-65535		1-65535	

[Add listener](#)

10. Define a **Security policy** for the load balancer listeners, create a **Rule**.

11. Configure the **Health checks**:

- **Ping protocol** - Select the protocol from the list. When using HTTP/HTTPS, enter a **Ping path** for the destination
- **Ping port** - Enter the port. E.g, 691 for TINA VPN, or 443 for HTTPS
- **Response Timeout** - Enter the number of seconds the probe waits for an answer.
- **Interval** - Enter the number of seconds between two probes.
- **Unhealthy threshold** - Enter the number of failed health checks for the instance to be considered unhealthy. Unhealthy health checks are taken out of rotation until healthy

again.

- **Healthy threshold** - Enter the the number of successful heath checks for the instance to be considered healthy.

Health checks [Info](#)

Your load balancer automatically performs health checks to test the availability of all registered instances. Traffic is only routed to healthy instances, which is determined on their response to the health check.

Ping target

The health check ping is sent using the protocol and port you specify. If using HTTP/HTTPS protocol, you must also provide the destination path.

Ping protocol

TCP

Ping port

691

1-65535

▼ Advanced health check settings

[Restore defaults](#)

Response timeout

Time to wait for EC2 instances to respond to health checks.

5 seconds

2-60 seconds. Must be less than the health check interval.

Interval

Amount of time between health checks sent to EC2 instances.

30 seconds

5-300 seconds. Must be greater than the health check response timeout.

Unhealthy threshold

Number of consecutive health check failures before declaring an EC2 instance unhealthy.

2

2-10

Healthy threshold

Number of consecutive health check successes before declaring an EC2 instance healthy.

10

2-10

- (optional) If the firewall EC2 instances are already deployed, select the EC2 instances. To add EC2 instances, click **Add instances**.
- Select **Enable Cross-Zone Load Balancing**.

Attributes

Creating your load balancer using the console gives you the opportunity specify additional features at launch. You can also find and adjust these settings in the load balancer's "Attributes" section after your load balancer is created.

☒ Enable cross-zone load balancing

With cross-zone load balancing, each load balancer node for your Classic Load Balancer distributes requests evenly across the registered instances in all enabled Availability Zones. If cross-zone load balancing is disabled, each load balancer node distributes requests evenly across the registered instances in its Availability Zone only. Classic Load Balancers created with the API or CLI have cross-zone load balancing disabled by default. After you create a Classic Load Balancer, you can enable or disable cross-zone load balancing at any time.

☒ Enable connection draining

Applicable to instances that are deregistering, this feature allows existing connections to complete (during a specified draining interval) before reporting the instance as deregistered.

[Learn more](#)

Timeout (draining interval)

The maximum time for the load balancer to allow existing connections to complete. When the maximum time limit is reached, the load balancer forcibly closes any remaining connections and reports the instance as deregistered.

300 seconds

Valid values: 1-3600 (integers only)

- (optional) Add **Key / Value** tags to the resource. Click **Create Add new tag** to add additional tags.
- Review your settings and click **Create load balancer**.

Summary

Review and confirm your configurations. [Estimate cost](#)

Basic configuration Edit Firewall-Load-Balancer Internal	Network mapping Edit VPC vpc-043f10892f33de3bd eu-west-1a subnet-0aea00cafc730bdf4	Security groups Edit - Barracuda CloudGen Firewall Control Center - BYOL-8-0-3-0137-20200421-AutogenByAWSMP-sg-039cd3e8213473414 - default sg-0b67f717f8c857e36	Listeners and routing Edit - TCP:691 - HTTPS:443 Secure listener settings - ELBSecurityPolicy-TLS-1-2-2017-01 - qa2020.cudaops.com From IAM
Health checks Edit TCP:691 - Timeout: 5 seconds - Interval: 30 seconds - Unhealthy threshold: 2 - Unhealthy threshold: 10	Instances Edit 2 instances added 2 instances in eu-west-1b	Attributes Edit - Cross-zone load balancing: On - Connection draining: On - Connection draining timeout: 300 seconds	Tags Edit lb-9784598 InternalLB

[Cancel](#) [Create load balancer](#)

16. Review the settings and click **Create load balancer**.

The classic load balancer is now deployed and ready for use.

Filter: Firewall-Load-Balancer						
☐	Name	DNS name	State	VPC ID	Availability Zones	Type
☐	Firewall-Load-Balancer	Firewall-Load-Balancer-2279...		vpc-0a84896f	eu-west-1c, eu-west-1a	classic

Figures

1. aws_nlb_01.png
2. aws_nlb_02.png
3. aws_nlb_03.png
4. aws_nlb_04.png
5. aws_nlb_05.png
6. aws_nlb_06.png
7. aws_nlb_07.png
8. aws_nlb_08.png
9. aws_nlb_09.png
10. aws_nlb_10.png
11. aws_nlb_11.png
12. aws_nlb_12.png
13. aws_nlb_13.png
14. aws_nlb_14.png
15. aws_nlb_15.png
16. aws_nlb_01.png
17. aws_nlb_02.png
18. aws_nlb_03.png
19. aws_clb_01.png
20. aws_clb_02.png
21. new_sg.png
22. aws_clb_03.png
23. aws_clb_04.png
24. aws_clb_05.png
25. aws_clb_06.png
26. aws_clb_07.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.