

# 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.

<b>Q</b> Search	[Alt+S]	D ¢	Ireland ▲
Console Home Info		US East (N. Virginia)	us-east-1
		US East (Ohio)	us-east-2
Recently visited Info		US West (N. California)	us-west-1
		US West (Oregon)	us-west-2
	$\bigcirc$	Asia Pacific (Mumbai)	ap-south-1
		Asia Pacific (Osaka)	ap-northeast-3
	No recently visited services	Asia Pacific (Seoul)	ap-northeast-2
E	inless one of these commonly vicited AWS convices	Asia Pacific (Singapore)	ap-southeast-1
EX.	IAM EC2 S3 RDS Lambda	Asia Pacific (Sydney)	ap-southeast-2
		Asia Pacific (Tokyo)	ap-northeast-1
		Canada (Central)	ca-central-1
	View all services	Europe (Frankfurt)	eu-central-1
		Europe (Ireland)	eu-west-1
# AWS Health Info	E Cost and usage Info	Europe (London)	eu-west-2



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

10	aws	Services	Q ec2	×	D
	Savings Reserve	Plans d Instances		Search results for 'ec2'	
	Dedicate	ed Hosts	Services (12)	Services Ser	e all 12 results 🕨 🔺
	Schedul	ed Instances	Features (51)		
	Capacity	Reservation	Resources New	EC2 ☆ Virtual Sequence in the Cloud	
	Images		Blogs (1,885)		
	AMIs		Documentation (127,530)	🔞 EC2 Image Builder 😭	
	AMI Cat	alog	Knowledge Articles (30)	A managed service to automate build, customize and deploy OS images	
_	El colto E		Tutorials (20)		
	Elastic E	Slock Store	Events (28)	🍭 Amazon Inspector 🕁	
	Volume	5	Marketplace (1,898)	Continual vulnerability management at scale	
	Snapsho	Managan			
	Litecycle	e Manager		AWS Firewall Manager ☆     Control manager affirmult rules	
•	Networl	« & Security		Central management of frewalt rules	

- 4. In the left menu, expand Load Balancing and select Load Balancers.
- 5. The Load balancers window opens. Click Create load balancer.

EC2 > Load balancers		
Load balancers (22) Elastic Load Balancing scales your load balancer capacity autom	atically in response to changes in incoming traffic.	C Actions V Create load balancer
Q Filter by property or value		< 1 > 🕲
Name		

6. Under Network Load Balancer click Create.



# Network Load Balancer



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 ultralow latencies.

- 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.

# Barracuda CloudGen Firewall



Load balancer name Name must be unique within your AWS account and ca	an't be changed after the load balancer is created.
External_LoadBalancer	
A maximum of 32 alphanumeric characters including h	yphens are allowed, but the name must not begin or end with a hyphen.
Scheme	
Internet-facing     An internet facing	eated.
Internal     An internal load balancer routes requests from clie	ents 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.	
<ul> <li>Dualstack</li> <li>Includes IPv4 and IPv6 addresses.</li> </ul>	
The load balancer routes traffic to targets in the select VPC Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for yo	ed subnets, and in accordance with your IP address settings. or you can <u>create a new VPC [2]</u> . Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be chang ur targets, view your <u>target groups [2]</u> .
The load balancer routes traffic to targets in the select VPC Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for yo -vpc vpc-0787e83abb6291ac3 IPv4: 10.0.0.0/24 Mappings Select at least one duril billing Zone and one subset for	red subnets, and in accordance with your IP address settings.
The load balancer routes traffic to targets in the select  VPC Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for yo  -vpc vpc-0787e83abb6291ac3 IPv4: 10.0.0./24  Mappings Select at least one Availability Zone and one subnet fo Availability Zones. Zones that are not supported by the	read subnets, and in accordance with your IP address settings.
The load balancer routes traffic to targets in the select VPC Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for your -vpc vpc-0787e83abb6291ac3 IPv4: 10.0.0.0/24 Mappings Select at least one Availability Zone and one subnet fo Availability Zones. Zones that are not supported by the ✓ eu-west-1a (euw1-az1) Cuba ct	red subnets, and in accordance with your IP address settings.
Wetwork mapping into         The load balancer routes traffic to targets in the select         VPC         Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for your or the VPC fo	red subnets, and in accordance with your IP address settings.
Wetwork mapping into         The load balancer routes traffic to targets in the select         VPC         Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the VPC for your target	eed subnets, and in accordance with your IP address settings.  or you can create a new VPC [2]. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be change un targets, view your target groups [2].  or each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the s e load balancer or VPC can't be selected. Subnets can be added, but not removed, once a load balancer is created.  Lab033-WKoeck-VPC-subnet-public1-eu-west-1a ▼
Network mapping into         The load balancer routes traffic to targets in the select         VPC         Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for your targets of the load balancer is created. To confirm the VPC for your targets of the virtual private cloud (VPC) for your targets of the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for your targets of the virtual private cloud (VPC) for your targets of the	red subnets, and in accordance with your IP address settings.
The load balancer routes traffic to targets in the select  VPC Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for yo  -vpc vpc-0787e83abb6291ac3 IPv4: 10.0.0.0/24  Mappings Select at least one Availability Zone and one subnet fo Availability Zones. Zones that are not supported by the u-west-1a (euw1-az1) Subnet subnet-0b4594a727cefd5eb Iect one or more Security Security groups Info A security group is a set of firewall rules that control th	eed subnets, and in accordance with your IP address settings.  or you can create a new VPC [2]. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be change on targets, view your target groups [2].  r each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected balancer or VPC can't be selected. Subnets can be added, but not removed, once a load balancer is created.  Lab033-WKoeck-VPC-subnet-public1-eu-west-1a ▼ / groups for your load balancer.  he traffic to your load balancer. Select an existing security group, or you can create a new security group [2].
The load balancer routes traffic to targets in the select The load balancer routes traffic to targets in the select VPC Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for your -vpc vpc-0787e83abb6291ac3 IPv4: 10.0.0.0/24 Mappings Select at least one Availability Zone and one subnet fo Availability Zones. Zones that are not supported by the eu-west-1a (euw1-az1) Subnet subnet-0b4594a727cefd5eb Cecurity groups Info A security groups a set of firewall rules that control the Security groups - recommended Security groups - recommended Security groups support on Network Load Balancers can for your load balancer must allow it to communicate wa are enforced on PrivateLink traffic; however, you can the	eed subnets, and in accordance with your IP address settings.  or you can create a new VPC [2]. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be change urr targets, view your target groups [2].  I C I C I C I C I C I C I C I C I C I
The load balancer routes traffic to targets in the select VPC Select the virtual private cloud (VPC) for your targets of the load balancer is created. To confirm the VPC for your -vpc vpc-0787e83abb6291ac3 IPv4: 10.0.0.0/24 Mappings Select at least one Availability Zone and one subnet fo Availability Zones. Zones that are not supported by the eu-west-1a (euw1-az1) Subnet Subnet Subnet-Ob4594a727cefd5eb ICCT ONE OF MORE Security Security groups Info A security groups is a set of firewall rules that control th Security groups - recommended Security groups support on Network Load Balancers ca for your load balancer must allow it to communicate w are enforced on PrivateLink traffic; however, you can the Select up to 5 security groups	eed subnets, and in accordance with your IP address settings.  or you can create a new VPC [2]. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be change ur targets, view your target groups [2].  I a c c c c c c c c c c c c c c c c c c

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.

	Thewait for your instance	to control inbound and outb	ound traffic. To create a new	security group, complete the fields	below.	
Basic details						
ecurity group name Info						
CGF-ELB-SG						
ame cannot be edited after creati	tion.					
escription Info						
Security group for the firewa	all elastic load balancer					
PC Info						
Q vpc-043f10892f33de3b	d		×			
nbound rules Info						
nbound rules Info	Protocol	Port range	Source		Description - optional	
nbound rules info Type Custom TCP	Protocol	Port range	Source	<b>▼</b> Q	Description - optional	Delete
nbound rules info Type Custom TCP	Protocol TCP	Port range	Source	▼ Q 0.0.0.0/0 X	Description - optional	Delete
nbound rules info Type Custom TCP HTTPS	Protocol TCP	Port range 691	Source Anywhe	• Q 0.0.0.0/0 X	Description - optional	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 TCP ▼ : 807 1-65535	Default action Info Forward to Select a target group ▼ C Create target group 2					

- 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.)



Step 1	Specify group details
Specify group details	Your load balancer routes requests to the targets in a target group and performs health checks on the targets.
Step 2	
Register targets	Basic configuration Settings in this section can't be changed after the target group is created.
	Choose a target type
	○ Instances
	<ul> <li>Supports load balancing to instances within a specific VPC.</li> <li>Facilitates the use of <u>Amazon EC2 Auto Scaling</u> <sup>1</sup> to manage and scale your EC2 capacity.</li> </ul>
	• IP addresses
	<ul> <li>Supports load balancing to VPC and on-premises resources.</li> <li>Facilitates routing to multiple IP addresses and network interfaces on the same instance.</li> </ul>
	<ul> <li>Others the table to the table of tabl</li></ul>
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must ( (SSH) as a targe	oup name, for example: FWAdmin I : Port list, select TCP 807. provide the same service as the listening port. Do NOT select port et when using port 807 as listener for the network load balancer.
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must ( (SSH) as a target Target group name	oup name, for example: FWAdmin I : Port list, select TCP 807. provide the same service as the listening port. Do NOT select port et when using port 807 as listener for the network load balancer.
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must ( (SSH) as a target Target group name FWAdmin	oup name, for example: FWAdmin I : Port list, select TCP 807. provide the same service as the listening port. Do NOT select port et when using port 807 as listener for the network load balancer.
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must r (SSH) as a targe Target group name FWAdmin A maximum of 32 alphanur	oup name, for example: FWAdmin I : Port list, select TCP 807. Drovide the same service as the listening port. Do NOT select port et when using port 807 as listener for the network load balancer.
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must ( (SSH) as a target Target group name FWAdmin A maximum of 32 alphanur Protocol : Port	oup name, for example: FWAdmin I : Port list, select TCP 807. provide the same service as the listening port. Do NOT select port et when using port 807 as listener for the network load balancer.
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must r (SSH) as a targe Target group name FWAdmin A maximum of 32 alphanur Protocol : Port Choose a protocol for your	<pre>oup name, for example: FWAdmin I : Port list, select TCP 807. provide the same service as the listening port. Do NOT select port et when using port 807 as listener for the network load balancer. neric characters including hyphens are allowed, but the name must not begin or end with a hyphen. target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now are not and use on art mitigation entions are user to are user to protect and use are not be character.</pre>
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must r (SSH) as a targe Target group name <b>FWAdmin</b> A maximum of 32 alphanur <b>Protocol : Port</b> Choose a protocol for your anomaly detection for the t after creation	oup name, for example: FWAdmin         I: Port list, select TCP 807.         provide the same service as the listening port. Do NOT select port         et when using port 807 as listener for the network load balancer.         neric characters including hyphens are allowed, but the name must not begin or end with a hyphen.         target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now argets and you can set mitigation options once your target group is created. This choice cannot be changed
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must r (SSH) as a target Target group name FWAdmin A maximum of 32 alphanur Protocol : Port Choose a protocol for your anomaly detection for the t after creation	oup name, for example: FWAdmin         I: Port list, select TCP 807.         provide the same service as the listening port. Do NOT select port et when using port 807 as listener for the network load balancer.         neric characters including hyphens are allowed, but the name must not begin or end with a hyphen.         target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now argets and you can set mitigation options once your target group is created. This choice cannot be changed
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must r (SSH) as a targe Target group name FWAdmin A maximum of 32 alphanur Protocol : Port Choose a protocol for your anomaly detection for the t after creation	<pre>oup name, for example: FWAdmin I: Port list, select TCP 807. provide the same service as the listening port. Do NOT select port at when using port 807 as listener for the network load balancer. neric characters including hyphens are allowed, but the name must not begin or end with a hyphen. target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now argets and you can set mitigation options once your target group is created. This choice cannot be change</pre>
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must r (SSH) as a target Target group name FWAdmin A maximum of 32 alphanur Protocol : Port Choose a protocol for your anomaly detection for the t after creation	<pre>oup name, for example: FWAdmin I: Port list, select TCP 807. provide the same service as the listening port. Do NOT select port at when using port 807 as listener for the network load balancer. neric characters including hyphens are allowed, but the name must not begin or end with a hyphen. target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now argets and you can set mitigation options once your target group is created. This choice cannot be change</pre>
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must r (SSH) as a targe Target group name FWAdmin A maximum of 32 alphanur Protocol : Port Choose a protocol for your anomaly detection for the t after creation TCP	oup name, for example: FWAdmin I: Port list, select TCP 807. provide the same service as the listening port. Do NOT select port at when using port 807 as listener for the network load balancer. neric characters including hyphens are allowed, but the name must not begin or end with a hyphen. target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now argets and you can set mitigation options once your target group is created. This choice cannot be changed 1-65535
Enter a <b>Target gr</b> From the <b>Protoco</b> This port must p (SSH) as a target Target group name FWAdmin A maximum of 32 alphanur Protocol : Port Choose a protocol for your anomaly detection for the t after creation TCP	oup name, for example: FWAdmin         1: Port list, select TCP 807.         provide the same service as the listening port. Do NOT select port set when using port 807 as listener for the network load balancer.         neric characters including hyphens are allowed, but the name must not begin or end with a hyphen.         target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now argets and you can set mitigation options once your target group is created. This choice cannot be changed and you can set mitigation options once your target group is created. This choice cannot be changed and you can set mitigation options once your target group is created. This choice cannot be changed and you can set mitigation options once your target group is created. This choice cannot be changed and you can set mitigation options once your target group is created. This choice cannot be changed and you can set mitigation options once your target group is created. This choice cannot be changed and you can set mitigate the this target group.         tet IP address type can be registered to this target group.

- 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 tes	t their status.
Health check protocol	
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 group's traffic port. However, you can specify a different port as an override.	the same as the target
<ul> <li>Override</li> <li>691</li> <li>1-65535</li> </ul>	

- 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 10.0.0/24 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.

addresses	
Step 1: Choose a netwo You can add IP addresses from the targets from multiple network sour	ork VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of rces by returning to this step and choosing another network.
Network	
<b>-vpc</b> vpc-0787e83abb6291ac3 IPv4: 10.0.0.0/24	▼
rou can manually enter if addresse	es nom the selected network.
Enter an IPv4 address from a	VPC subnet.
Enter an IPv4 address from a $\sqrt{10.0.0}$ X	VPC subnet.
Enter an IPv4 address from a V 10.0.0. X Add IPv4 address	VPC subnet.
Enter an IPv4 address from a V 10.0.0. X Add IPv4 address You can add up to 4 more IP address	VPC subnet. Remove
Enter an IPv4 address from a V 10.0.0. X Add IPv4 address You can add up to 4 more IP addres	VPC subnet.  Sses.  Ports Dests for resulting to this target
Enter an IPv4 address from a 10.0.0. X Add IPv4 address You can add up to 4 more IP addres	VPC subnet.  Seeses.  Ports Ports for routing to this target.  807
Enter an IPv4 address from a 1 10.0.0. X Add IPv4 address fou can add up to 4 more IP addres	VPC subnet.  Sees.  Ports Ports Ports for routing to this target.  807 1-65535 (separate multiple ports with commas)

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*.

<b>Q</b> 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.



rget type	Protocol :	Port	VPC	IP addres	s type
stance	TCP: 807		vpc-0787e83abb6291	ac3 🖸 IPv4	
ad balancer <u>-ELB</u>	<b>Z</b> Healthy	Unhealthy	Unused	Initial	Draining
Total largets					

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.

Targe	ts Monitoring	g Health checks	Attribu	ites	Гадs			
Regi	stered targets	(2)				C	Deregister	egister targets
Q F	Filter targets							< 1 > ©
	Instanc 🔻	Name	▼	Port	▽	Zone 🗸	Health s 🔻	Health status det
	<u>i-033c7a7</u>	CGF-AW	S	807		eu-west-1a	🛞 Unhealthy	Health checks faile
	<u>i-0ea1d41</u>	CGF-AW	S	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.

Q Search [Alt+5]	ג א פֿע איז
Console Home Info	▲ US East (N. Virginia) us-east-1
	US East (Ohio) us-east-2
Recently visited Info	US West (N. California) us-west-1
	US West (Oregon) us-west-2
	Asia Pacific (Mumbai) ap-south-1
	Asia Pacific (Osaka) ap-northeast-3
No recently visited services	Asia Pacific (Seoul) ap-northeast-2
	Asia Pacific (Singapore) ap-southeast-1
Explore one of these commonly visited AWS services.	Asia Pacific (Sydney) ap-southeast-2
	Asia Pacific (Tokyo) ap-northeast-1
	Canada (Central) ca-central-1
View all services	Europe (Frankfurt) eu-central-1
	Europe (Ireland) eu-west-1
AWS Health Info E Cost and usage Info	Europe (London) eu-west-2

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

aws Servic	es Q ec2	×	
Savings Plans		Search results for 'ec2'	
Dedicated Hosts	Services (12)	Services	See all 12 results ►
Scheduled Instan Capacity Reserva	iens Features (51) ions Resources New	🛃 EC2 ☆ Virtual Servers in the Cloud	
<ul> <li>Images</li> <li>AMIs</li> <li>AMI Catalog</li> </ul>	Blogs (1,885) Documentation (127,530) Knowledge Articles (30)	BEC2 Image Builder ☆ A managed service to automate build	l, customize and deploy OS images
<ul> <li>Elastic Block Stor</li> <li>Volumes</li> <li>Spanshots</li> </ul>	Tutorials (20) Events (28) Marketplace (1,898)	<b>&amp; Amazon Inspector</b> な Continual vulnerability management	at scale
Lifecycle Manage	ity	AWS Firewall Manager ☆     Central management of firewall rules	3

- 4. In the left menu, expand **Load Balancing** and select **Load Balancers**. The **Load balancers** window opens.
- 5. Click Create load balancer.



Load balancers (2	2)			G	Actions 🔻	Create load balancer
C Filter by property	scales your load balancer capacity auto	omatically in response to cha	anges in incoming traffic.		-	< 1 > @

6. Expand Classic Load Balancer and click Create.

Classic Load Balancer - previous generation

Classic Load Balancer Info



- 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.

# Barracuda CloudGen Firewall



Load balancer name Name must be unique wit	n your AWS account and can't be changed after the load balancer is created.
Firewall-Load-Balan	r
A maximum of 32 alphan	neric characters including hyphens are allowed, but the name must not begin or end with a hyphen.
Scheme Info Scheme can't be changed	ter the load balancer is created.
<ul> <li>Internet-facing</li> <li>An internet-facing lost</li> </ul>	balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more 🔀
<ul> <li>Internal An internal load bala</li> </ul>	er routes requests from clients to targets using private IP addresses.
Network mappin The load balancer routes VPC Info Select the victual private	Info ffic to targets in the selected subnets, and in accordance with your network settings.
Network mappin The load balancer routes VPC Info Select the virtual private toad balancer, ensure eac - vpc-043f10892f33de3b IPv4: 172.31.0.0/16	Info ffic to targets in the selected subnets, and in accordance with your network settings. ud (VPC) for your targets or you can create a new VPC 2. The selected VPC cannot be changed after the load balancer is created. When selecting a VPC for ubnet has a CIDR block with at least a /27 bitmask and at least 8 free IP addresses. Learn more 2 C
Network mappin The load balancer routes VPC Info Select the virtual private load balancer, ensure eac - vpc-043f10892f33de3b IPv4: 172.31.0.0/16 Mappings Select at least one Availal Availability Zones. Availal	Info ffic to targets in the selected subnets, and in accordance with your network settings. ud (VPC) for your targets or you can create a new VPC 2. The selected VPC cannot be changed after the load balancer is created. When selecting a VPC for ubnet has a CIDR block with at least a /27 bitmask and at least 8 free IP addresses. Learn more 2 v ty 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 select ty 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 select ty Zones that are not supported by the load balancer or the VPC are not available for selection.
Network mappin The load balancer routes VPC Info Select the virtual private load balancer, ensure eac - vpc-043f10892f33de3t IPv4: 172.31.0.0/16 Mappings Select at least one Availa Availability Zones. Availal eu-west-1a (euw Subnet	Info ffic to targets in the selected subnets, and in accordance with your network settings. ud (VPC) for your targets or you can create a new VPC [2]. The selected VPC cannot be changed after the load balancer is created. When selecting a VPC for ubnet has a CIDR block with at least a /27 bitmask and at least 8 free IP addresses. Learn more [2] v ty 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 select ty Zones that are not supported by the load balancer or the VPC are not available for selection. -az1)

- 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.



Basic details						
Security group name Info	fo					
CGF-ELB-SG						
Name cannot be edited after	er creation.					
Description Info						
Security group for the	firewall elastic load balancer					
VPC Info						
vi e into						
Q vpc-043f10892f33	3de3bd		×			
Q vpc-043f10892f33	3de3bd		×			
Q vpc-043f10892f33	3de3bd		×			
Q vpc-043f10892f33	3de3bd		×			
Q vpc-043f10892f33	8de3bd Protocol	Port range	Source		Description - optional	
Q vpc-043f10892f33	Bde3bd Protocol	Port range	Source	Q	Description - optional	
Q vpc-043f10892f33 Inbound rules info Type Custom TCP	Sde3bd Protocol TCP	Port range	Source	] ]	Description - optional	
Q vpc-043f10892f33 Inbound rules info Type Custom TCP	Sde3bd Protocol TCP	Port range	Source	Q 0000/0 X	Description - optional	
Q vpc-043f10892f33 Inbound rules info Type Custom TCP HTTPS	Protocol TCP TCP	Port range 691	Source	Q 0.0.0.0/0 X	Description - optional	

- 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 conf its registered targets.	igure. The settings you define for a listener determine how the load balanc	er routes requests to
Listener TCP:691	Instance TCP:691	Remove
▼ Listener HTTPS:443	Instance HTTP:443	Remove
Listener protocol Listener port HTTPS ▼ : 443 1-65535	Instance protocol Instance port HTTP  I: 443 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.
- $\circ~$  Interval Enter the number of seconds between two probes.
- **Unhealthy threshold** Enter the number of failed heath 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 registers the health check.	ed instances. Traffic is only routed to healthy instances, which is determined on their response to
Ping target         The health check ping is sent using the protocol and port you specify. If using HTTP/HTTPS pr         Ping protocol       Ping port         TCP       ▼         1-65535	otocol, you must also provide the destination path.
Advanced health check settings	Restore defaults
Response timeout	Interval
Time to wait for EC2 instances to respond to health checks.	Amount of time between health checks sent to EC2 instances.
5 seconds	30 seconds
2-60 seconds. Must be less than the health check interval.	5-300 seconds. Must be greater than the health check response timeout.
Unhealthy threshold	Healthy threshold
Number of consecutive health check failures before declaring an EC2 instance unhealthy.	Number of consecutive health check successes before declaring an EC2 instance healthy.           10 <ul> <li>Instance health check successes before declaring an EC2 instance healthy.</li> </ul>

- 12. (optional) If the firewall EC2 instances are already deployed, select the EC2 instances. To add EC2 instances, click **Add instances**.
- 13. 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: <strong>1-3600</strong> (integers only)

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

# Barracuda CloudGen Firewall



Basic configuration <sup>Edit</sup>	Network mapping Edit	Security groups Edit	Listeners and routing Edit
Firewall-Load-Balancer • Internal	VPC vpc-043f10892f33de3bd 🕻 • eu-west-1a subnet-0aea00cafc730bdf4 🕻	<ul> <li>Barracuda CloudGen Firewall Control Center - BYOL-8-0-3- 0137-20200421- AutogenByAWSMP- sg-039cd3e8213473414 2</li> <li>default sg-0b67f717f8c857e36 2</li> </ul>	<ul> <li>TCP:691</li> <li>HTTPS:443</li> <li>Secure listener settings</li> <li>ELBSecurityPolicy-TLS-1-2-2017-01</li> <li>qa2020.cudaops.com From IAM</li> </ul>
Health checks <sup>Edit</sup> 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 <sup>Edit</sup> Ib-9784598internalLB

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

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

Filter	r: 🔍 Firewall-Load-Balanc	cei	×						
	Name	•	DNS name	Ŧ	State≖	VPC ID -	Availability Zones	+	Туре 👻
	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.