AWS WEB-APPLICATION FIREWALL ON THE APPLICATION LOAD BALANCER

1) Create a VPC with multiple Public subnet.

2) Connect Internet Gateway to the VPC.

3) Create Route Table and attach to the VPC.

4) Deploy EC2 Instance in the VPC.

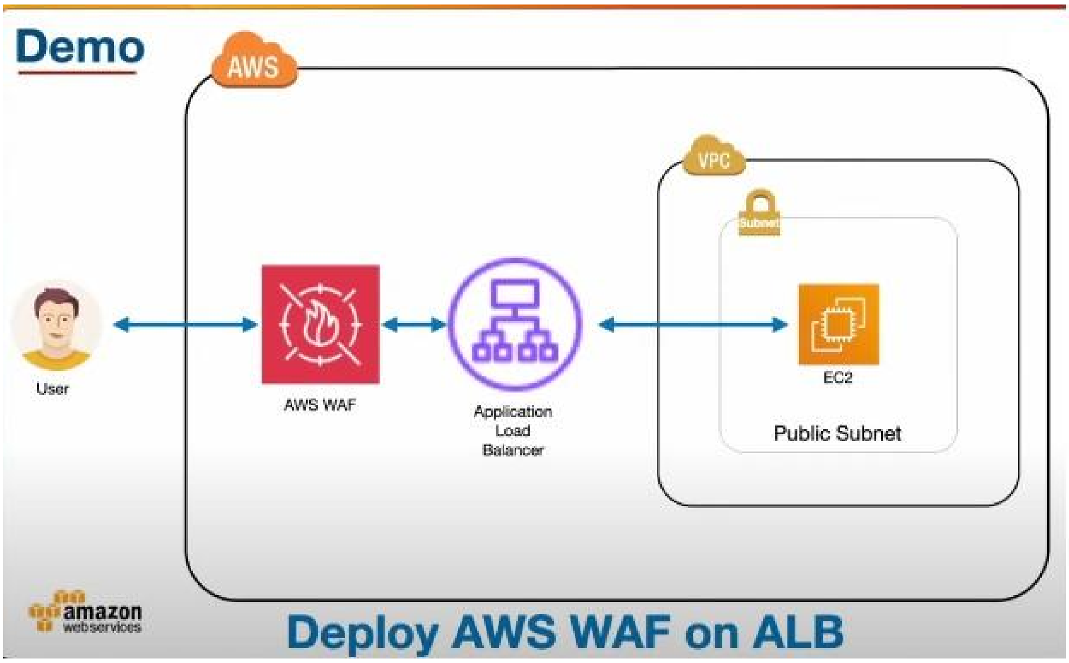
5) Create a Target Group to Attach the Application Load Balancer..

6) Deploy Application Load Balancer.

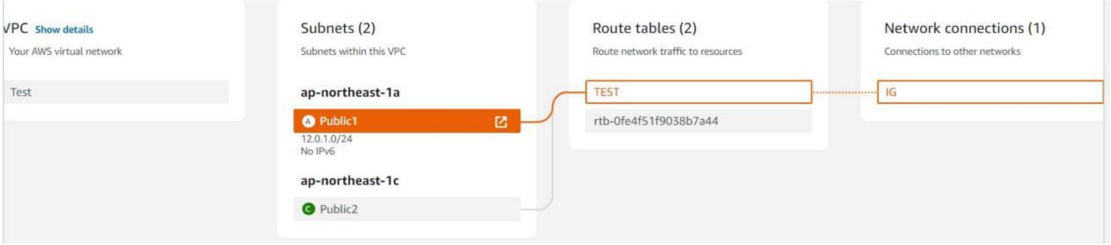
7) Create Web ACLs

8) Test

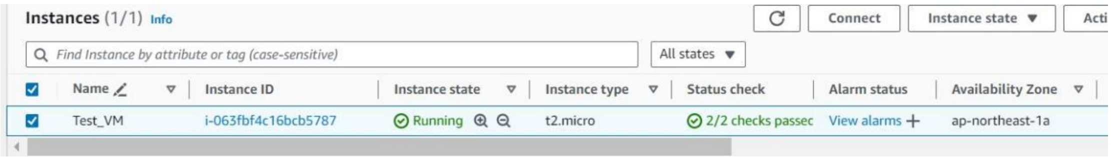
9) Monitor



STEP 1 :- Setup the VPC and Internet Gateway

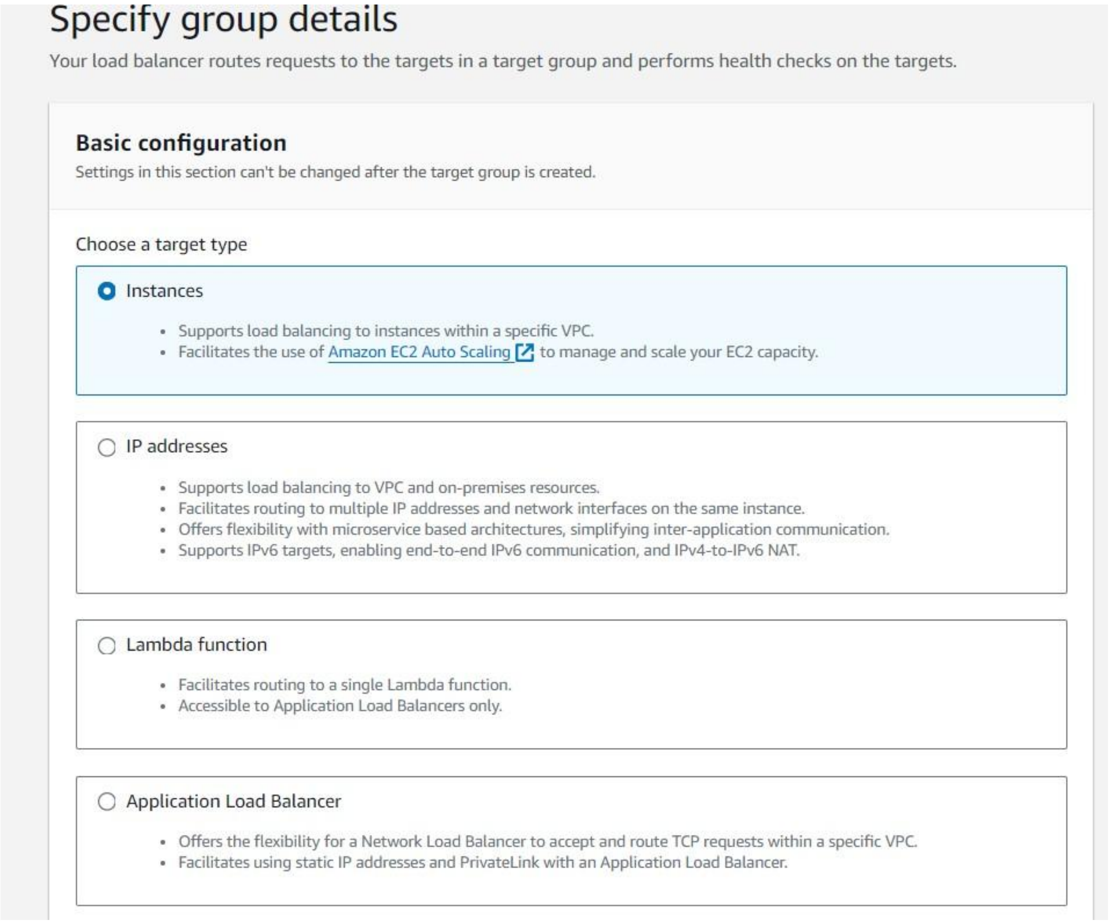


STEP 2 :- Deployed the Instance.



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☑	Test_VM	i-063fbf4c16bcb5787	Running	t2.micro	2/2 checks passec	View alarms +	ap-northeast-1a

STEP 3 :- Creating Target Group for Application Load Balancer.



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.

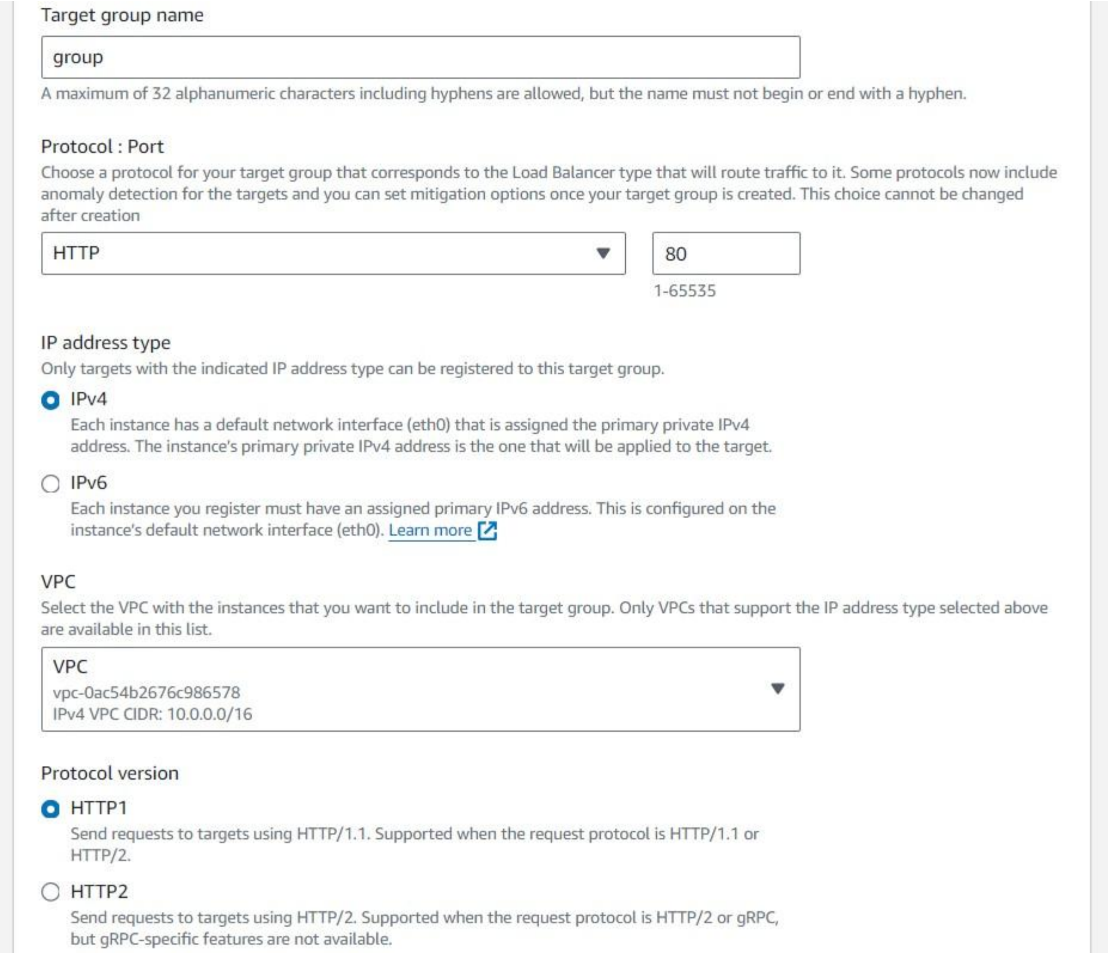
○ Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

○ Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

]



Target group name

group

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

HTTP ▼ | 80

1-65535

IP address type

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

● IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

○ IPv6

Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

VPC
vpc-0ac54b2676c986578
IPv4 VPC CIDR: 10.0.0.0/16 ▼

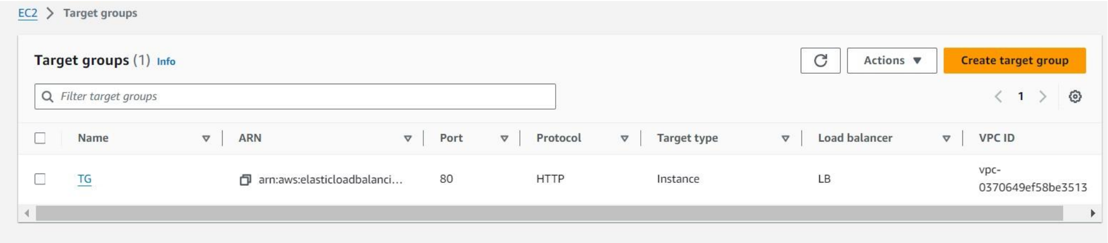
Protocol version

● HTTP1

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

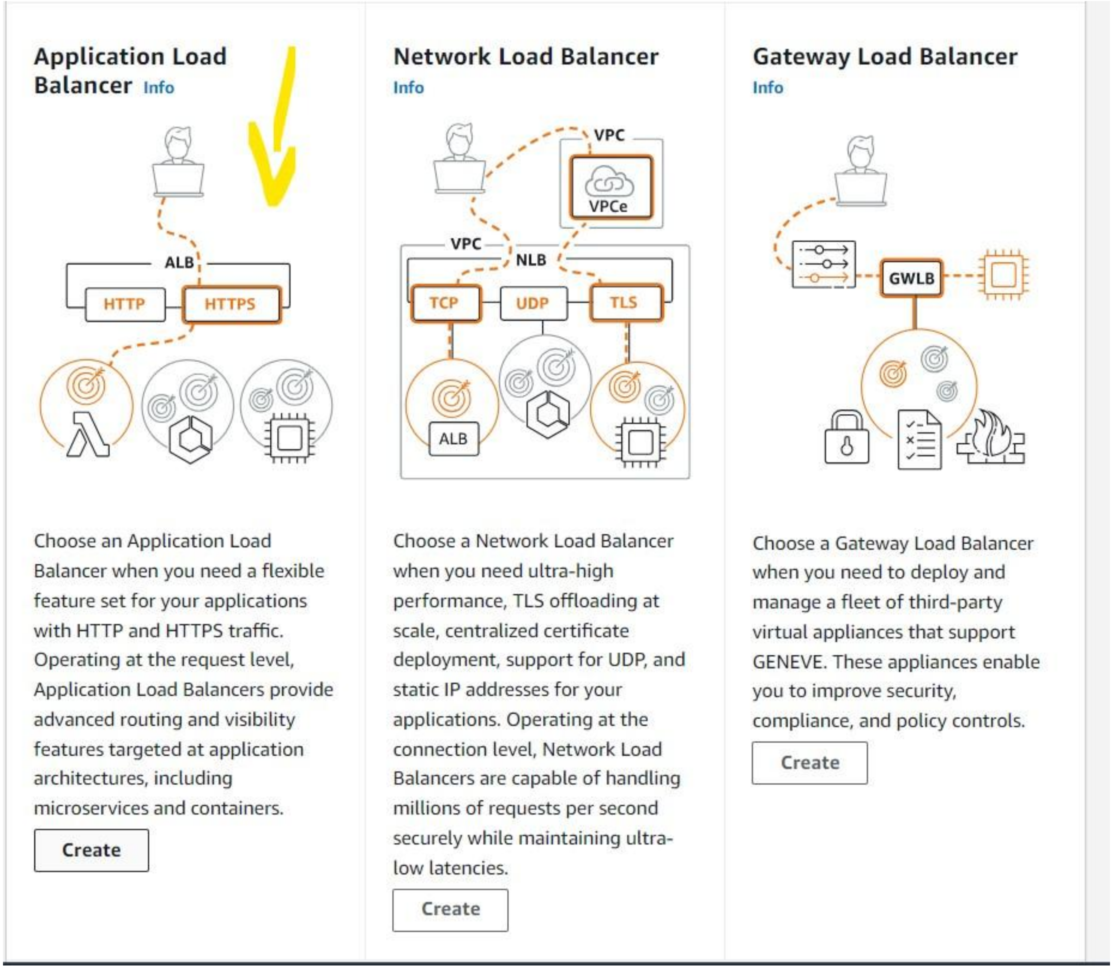
○ HTTP2

Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.



□	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
□	TG	arn:aws:elasticloadbalanci...	80	HTTP	Instance	LB	vpc-0370649ef58be3513

STEP 4 :- Creating Application Load Balancer



Application Load Balancer Info

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

Network Load Balancer Info

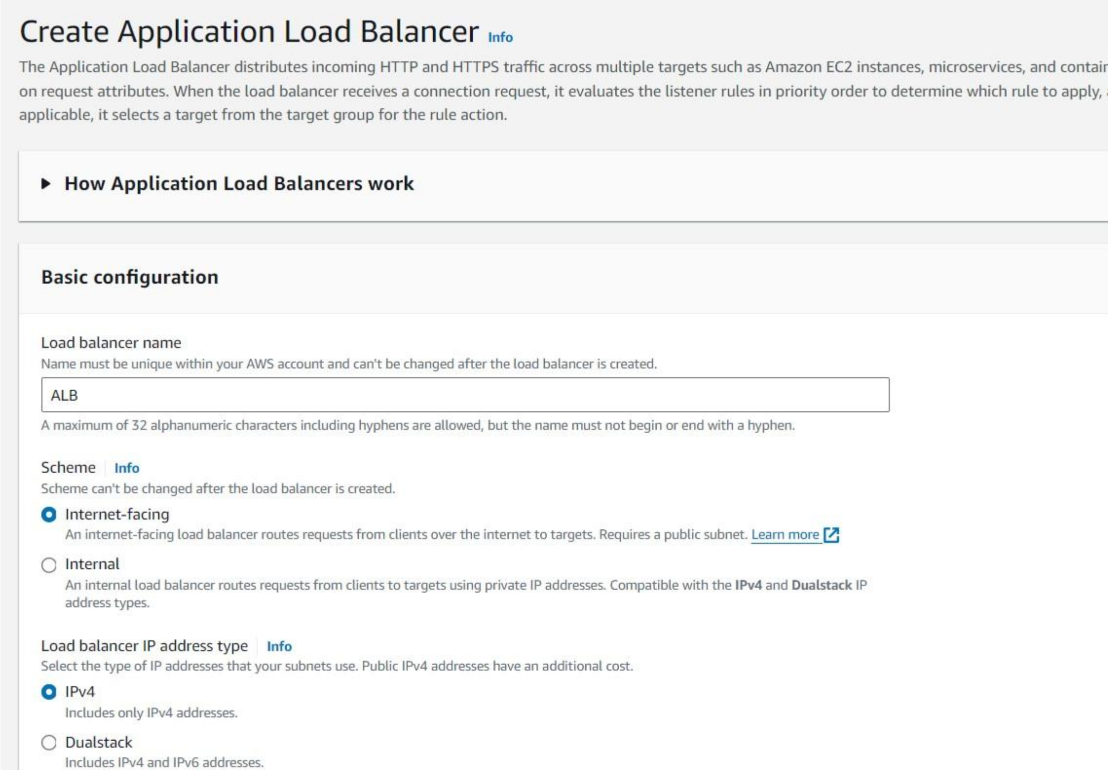
Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per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

Create

Gateway Load Balancer Info

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and contair on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, applicable, it selects a target from the target group for the rule action.

▸ **How Application Load Balancers work**

Basic configuration

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

ALB

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.

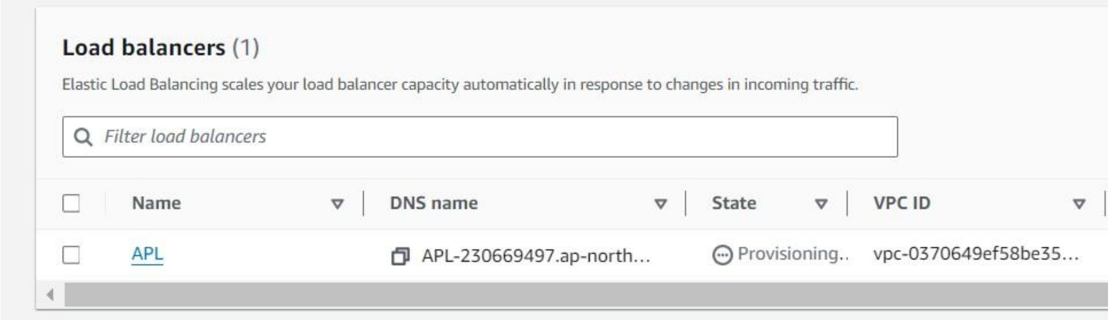
● Internet-facing
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more

○ Internal
An internal load balancer routes requests from clients to targets using private IP addresses. Compatible with the **IPv4** and **Dualstack** IP address types.

Load balancer IP address type Info
Select the type of IP addresses that your subnets use. Public IPv4 addresses have an additional cost.

● IPv4
Includes only IPv4 addresses.

○ Dualstack
Includes IPv4 and IPv6 addresses.



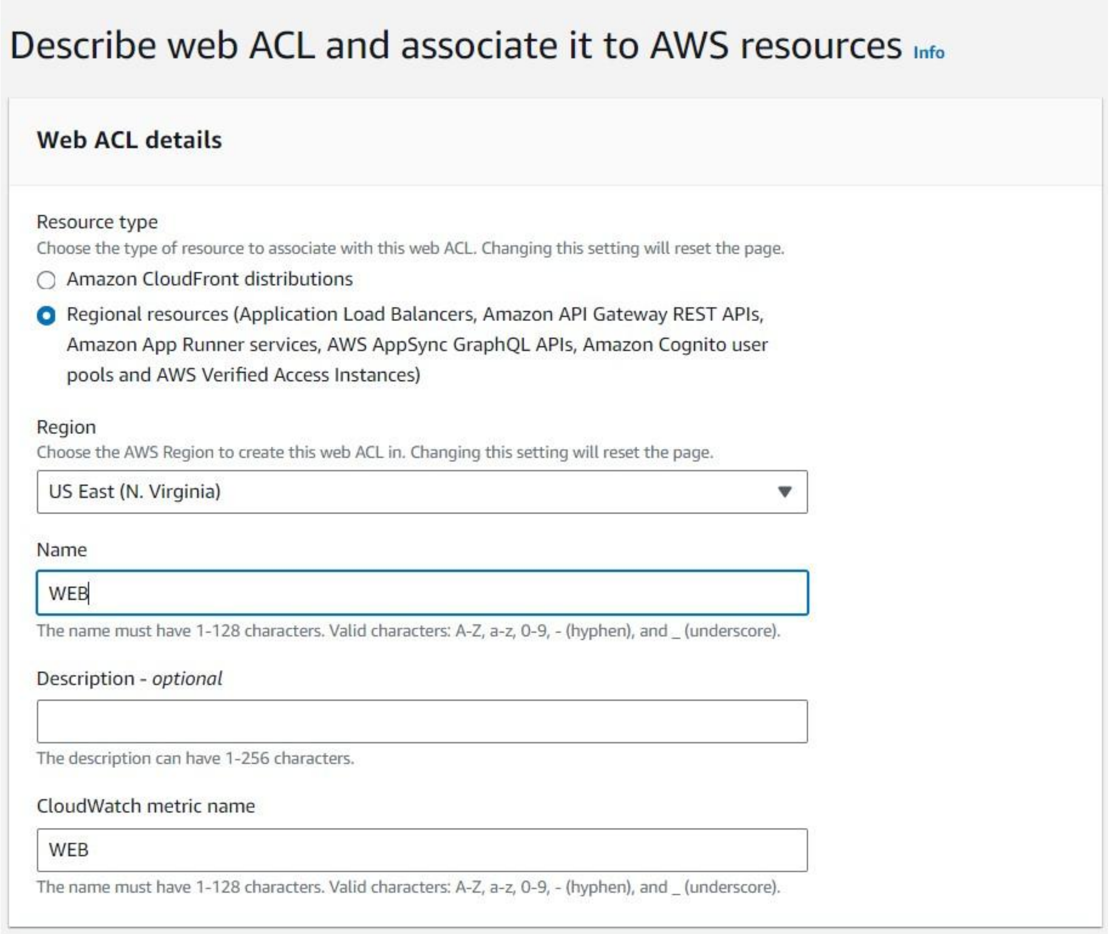
Load balancers (1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Filter load balancers

□	Name	DNS name	State	VPC ID
□	APL	APL-230669497.ap-north...	Provisioning..	vpc-0370649ef58be35...

STEP 5 :- Creating Web Application Firewall



Describe web ACL and associate it to AWS resources

Web ACL details

Resource type

Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

○ Amazon CloudFront distributions

● Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync GraphQL APIs, Amazon Cognito user pools and AWS Verified Access Instances)

Region

Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

US East (N. Virginia) ▼

Name

WEB

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

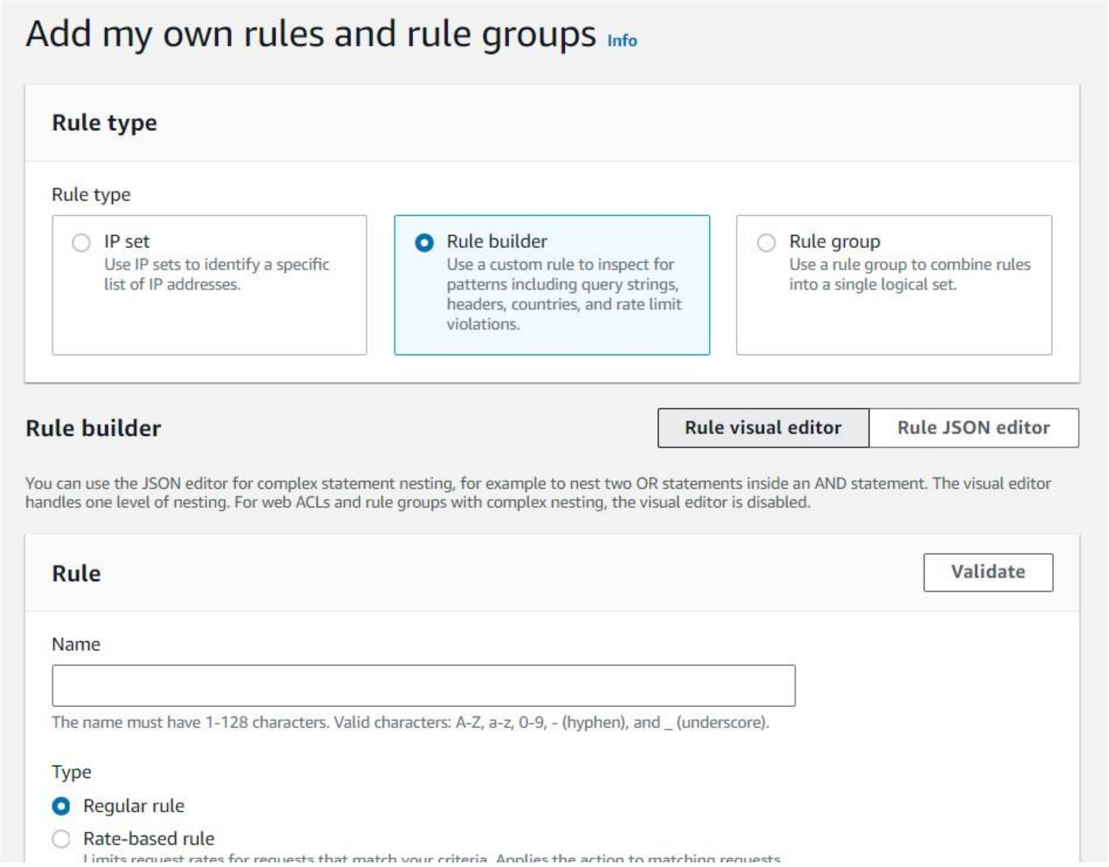
Description - *optional*

The description can have 1-256 characters.

CloudWatch metric name

WEB

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).



Add my own rules and rule groups Info

Rule type

Rule type

○ IP set
Use IP sets to identify a specific list of IP addresses.

● Rule builder
Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.

○ Rule group
Use a rule group to combine rules into a single logical set.

Rule builder

You can use the JSON editor for complex statement nesting, for example to nest two OR statements inside an AND statement. The visual editor handles one level of nesting. For web ACLs and rule groups with complex nesting, the visual editor is disabled.

Rule

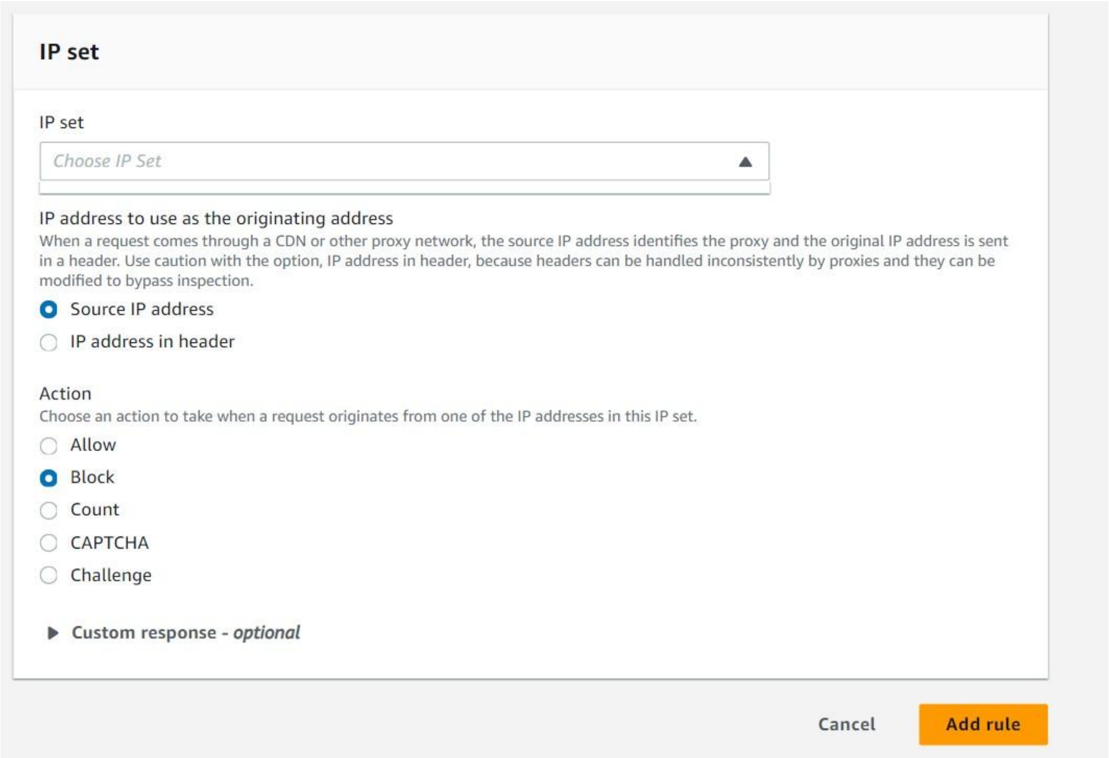
Name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Type

● Regular rule

○ Rate-based rule
Limits request rates for requests that match your criteria. Applies the action to matching requests



IP set

IP set

Choose IP Set ▲

IP address to use as the originating address
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with the option, IP address in header, because headers can be handled inconsistently by proxies and they can be modified to bypass inspection.

● Source IP address

○ IP address in header

Action
Choose an action to take when a request originates from one of the IP addresses in this IP set.

○ Allow

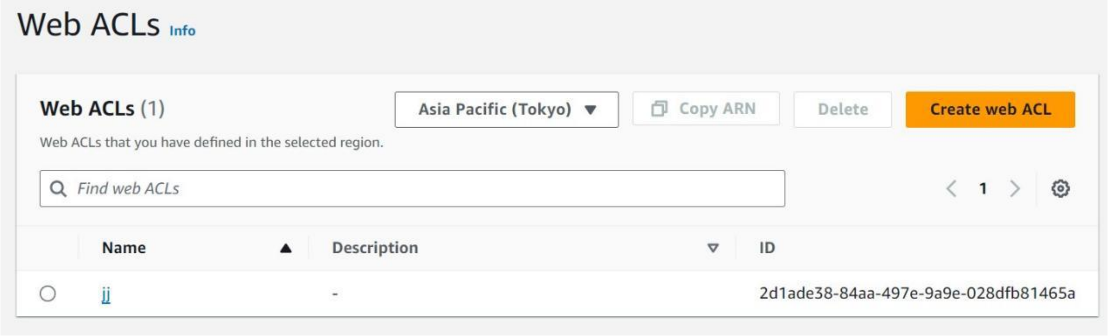
● Block

○ Count

○ CAPTCHA

○ Challenge

▶ Custom response - *optional*

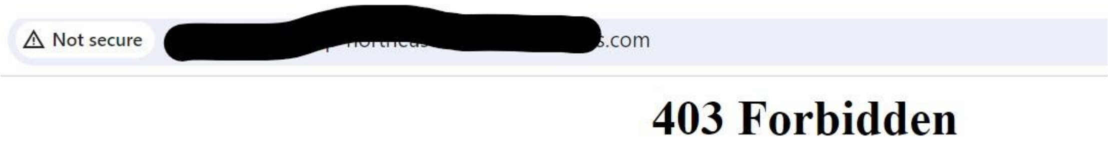


Web ACLs (1)

Web ACLs that you have defined in the selected region.

	Name	Description	ID
○	jj	-	2d1ade38-84aa-497e-9a9e-028dfb81465a

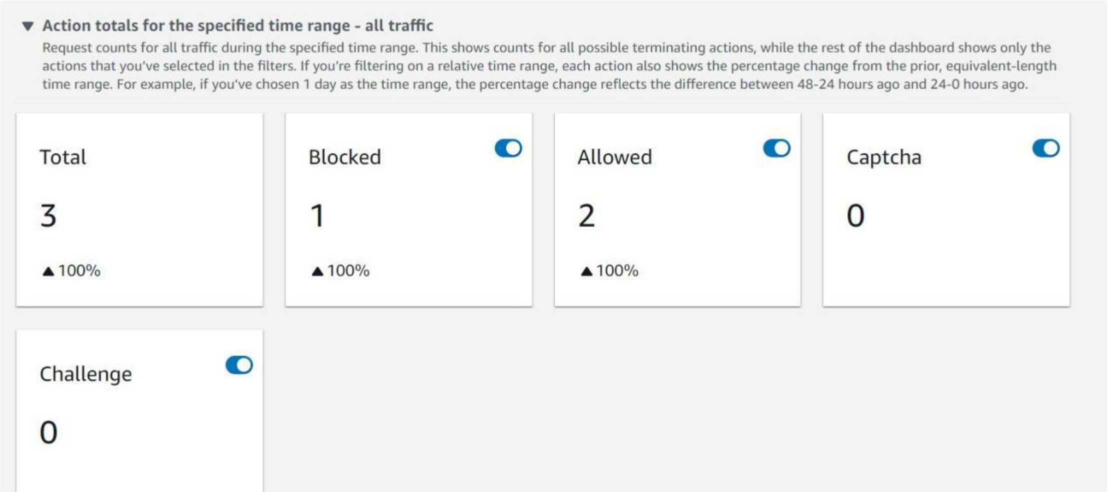
STEP 6 :- TEST



[redacted]

403 Forbidden

STEP 7 :- Monitoring



▼ Action totals for the specified time range - all traffic

Request counts for all traffic during the specified time range. This shows counts for all possible terminating actions, while the rest of the dashboard shows only the actions that you've selected in the filters. If you're filtering on a relative time range, each action also shows the percentage change from the prior, equivalent-length time range. For example, if you've chosen 1 day as the time range, the percentage change reflects the difference between 48-24 hours ago and 24-0 hours ago.

Total	Blocked	Allowed	Captcha	Challenge
3	1	2	0	0
▲100%	▲100%	▲100%		