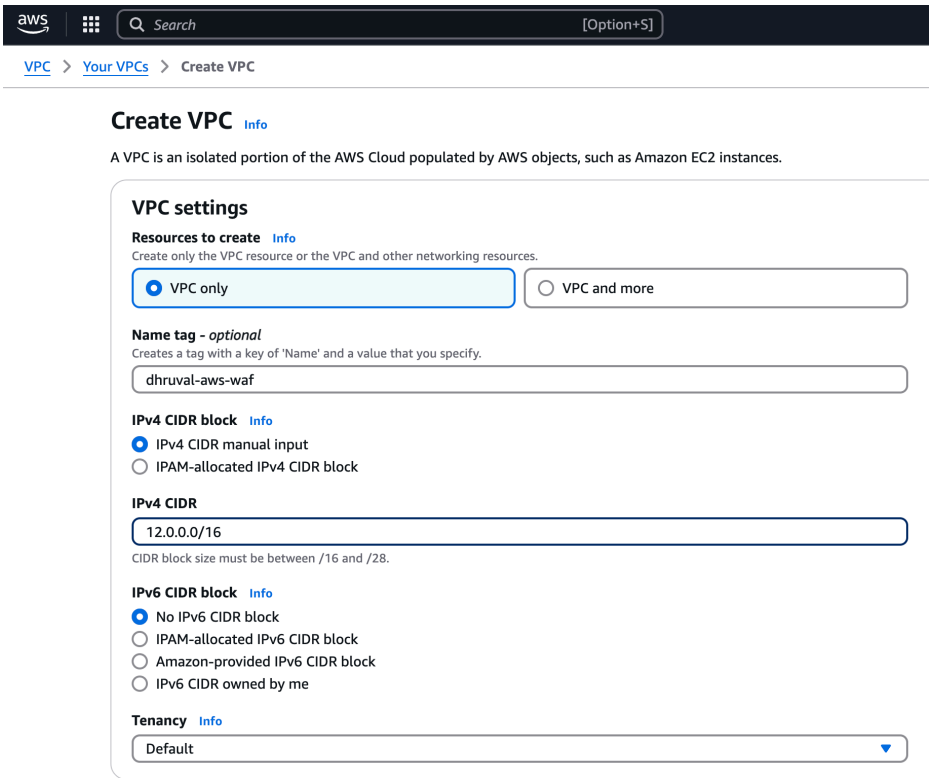
AWS WAF Project

In this project I will be configuring an AWS WAF with an Application Load Balancer to access an EC2 instance. I will demonstrate how to allow and deny traffic into the EC2 instance. I will start this project first by creating a VPC (Virtual Private Network), an internet gateway, and a subnet for the EC2 instance.

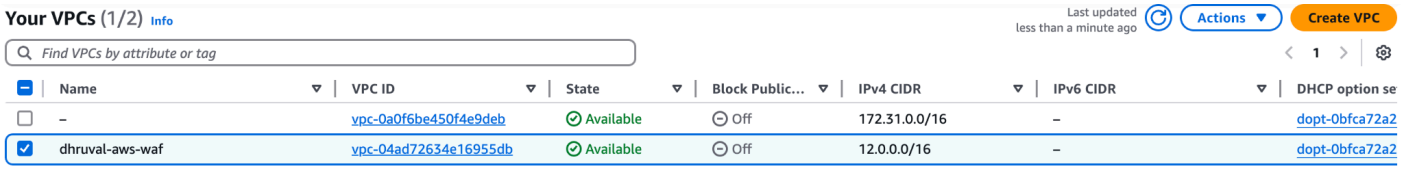
Note: Select the closest region to you for better performance.

Create a VPC:

1. Search for VPC on the AWS console and select it to open its dashboard.
2. Then click “create VPC”.
3. From VPC settings select VPC only, then name the VPC, insert the IPv4 CIDR, then leave all the other settings default and then click create VPC.



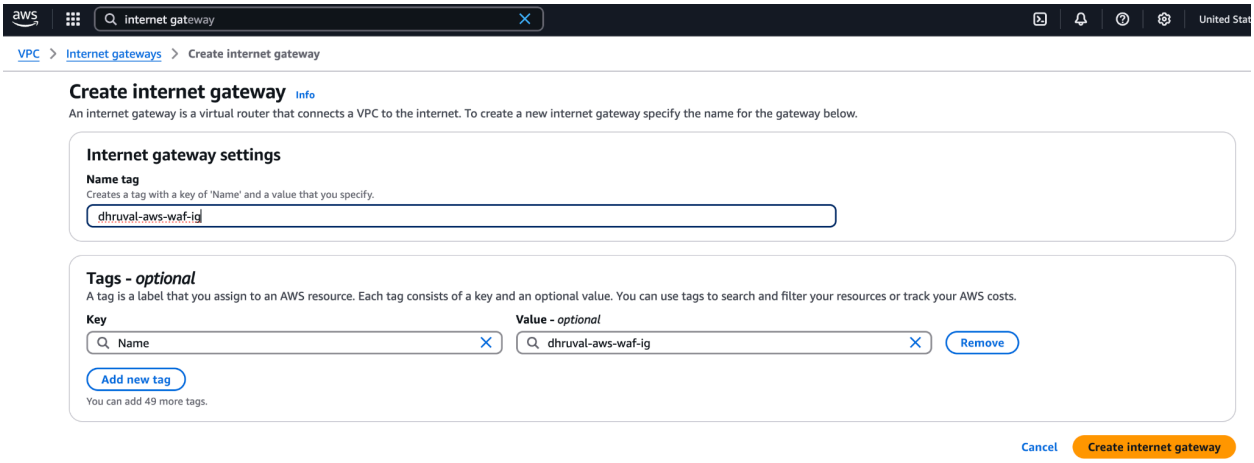
4. Then double check if the new VPC has been created.



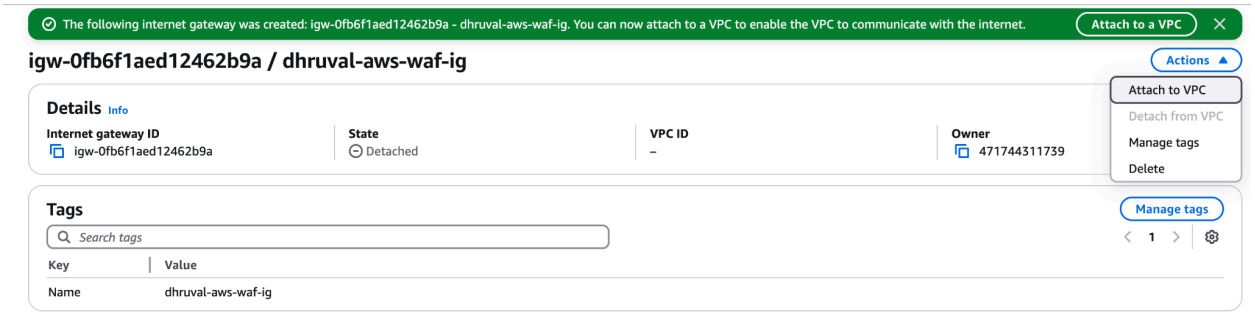
Create Internet Gateway:

Note: Internet Gateway is needed to have internet access to our VPC.

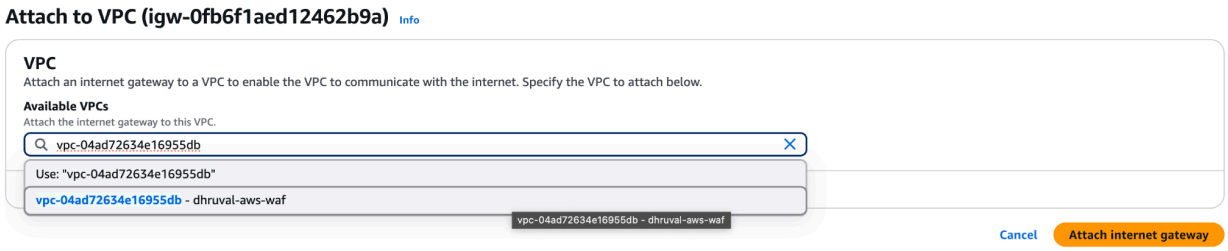
1. On the left side of the navigation bar in VPC, select Internet Gateway.
2. Then select create internet gateway on top right.
3. Name the internet gateway, leave everything else default and then select create internet gateway.



4. Once created, then attach it to the VPC that was created earlier.

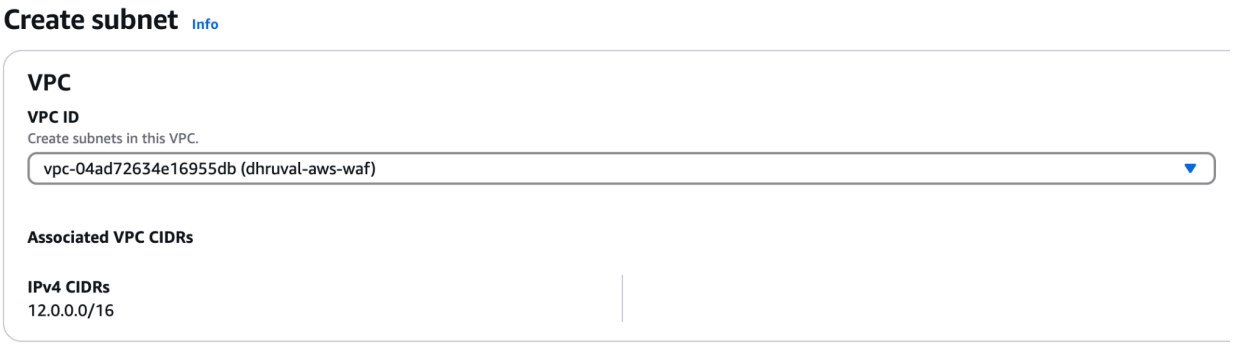


5. Select the VPC and then attach the internet gateway.

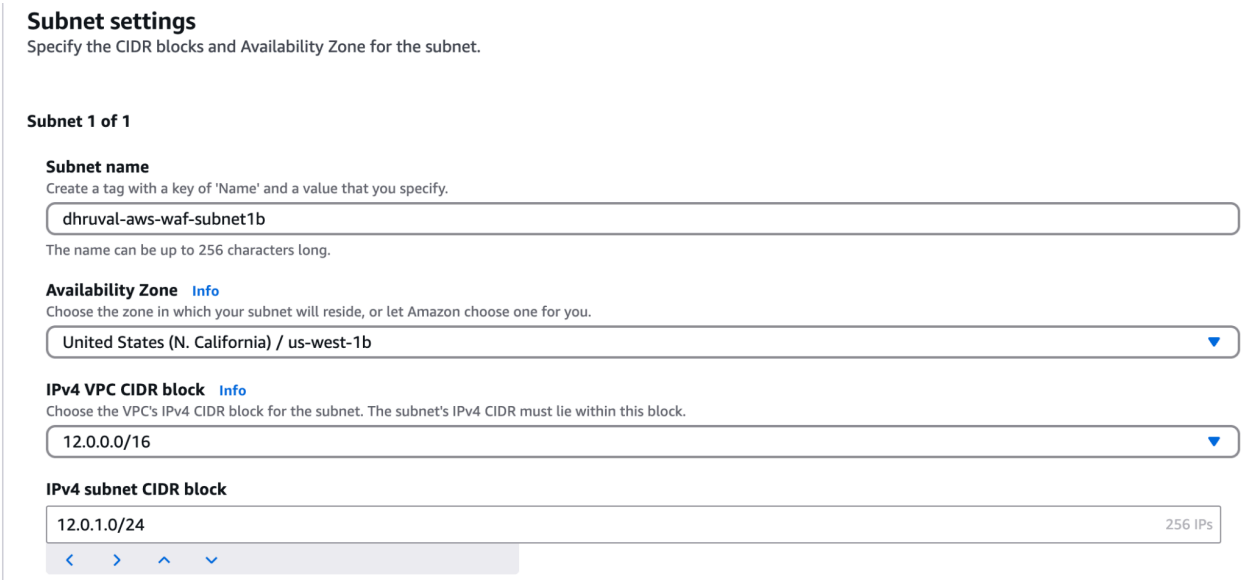


Create a subnet:

1. On the left side of the navigation bar in VPC, select Subnets and create subnet.
2. Select the created VPC.

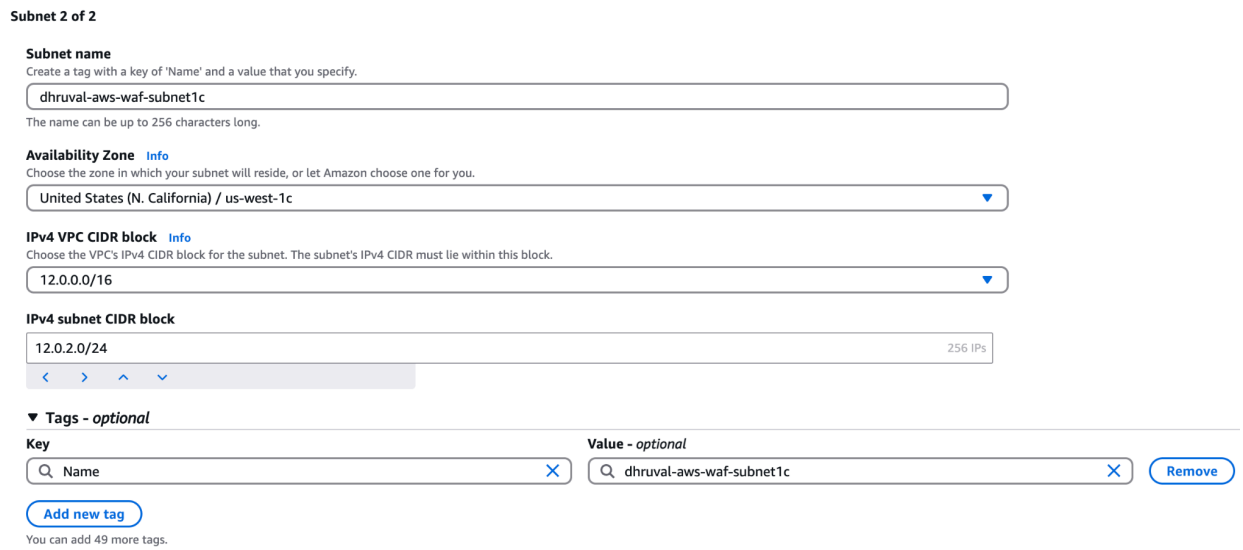


3. Create the first subnet with a unique name, availability zone, and IPv4 VPC / subnet CIDRs.

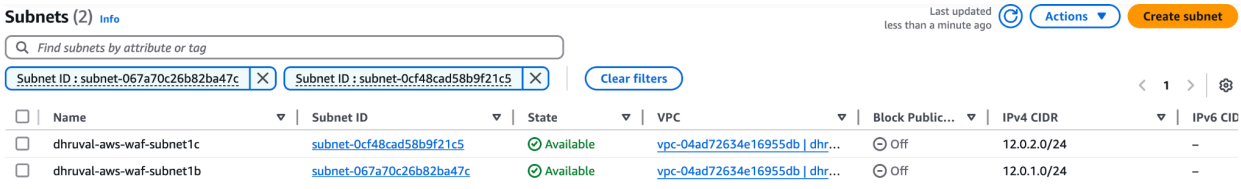


Note: need 2 subnets for different availability zones.

4. Create the second subnet with a unique name, different availability zone, and IPv4 VPC / subnet CIDRs. Then click create subnet.



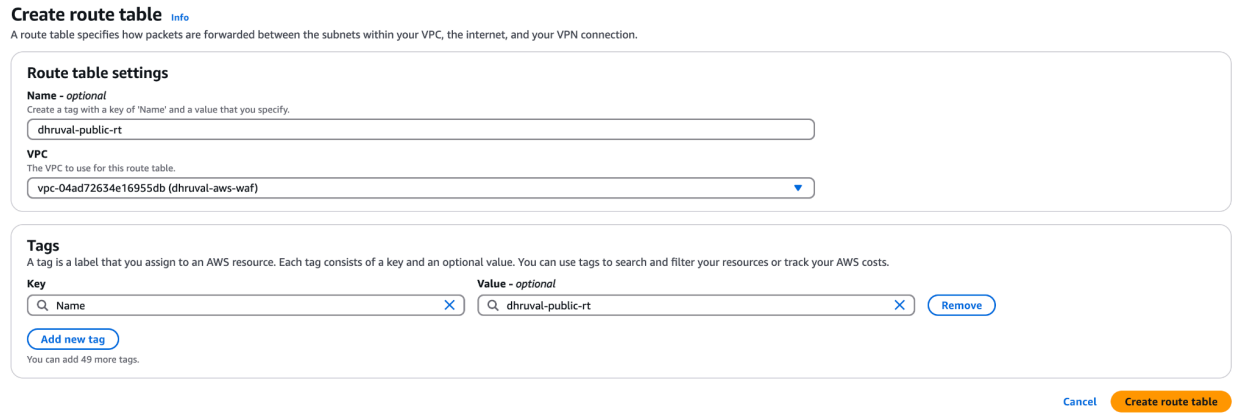
Note: two new subnets have been created.



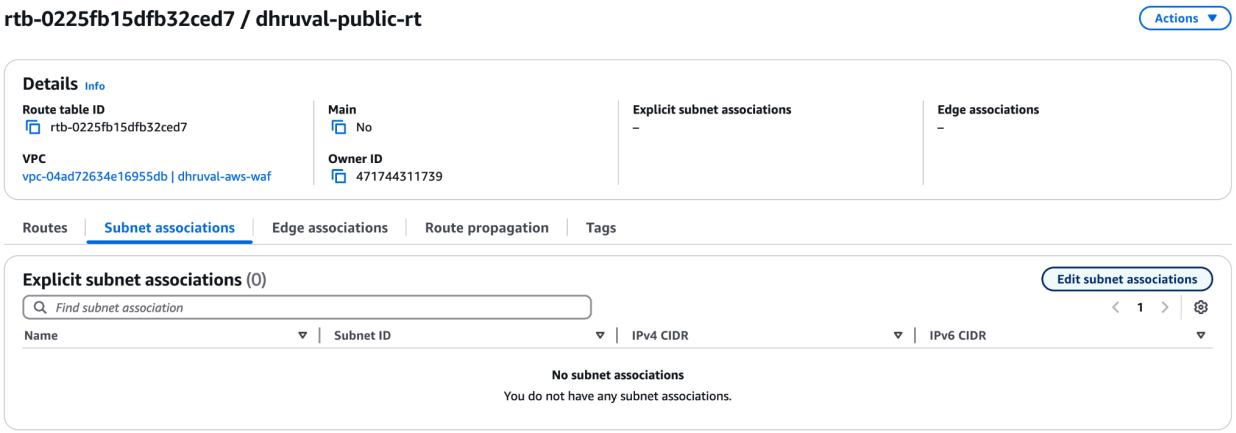
Create a Route table:

Note: Route table is needed so the internet gateway can be connected to the route table and the subnet can access the internet.

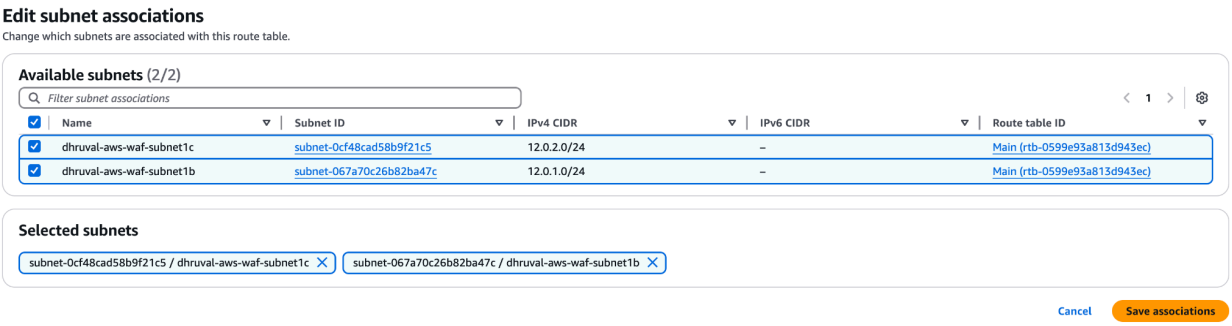
1. On the left side of the navigation bar in VPC, select Route table and then create route table.
2. Name the route table, select the created VPC, and create route table.



3. Then associate the subnets to the route table. On the created route table select the “Subnet associations” tab and then select edit subnet associations.

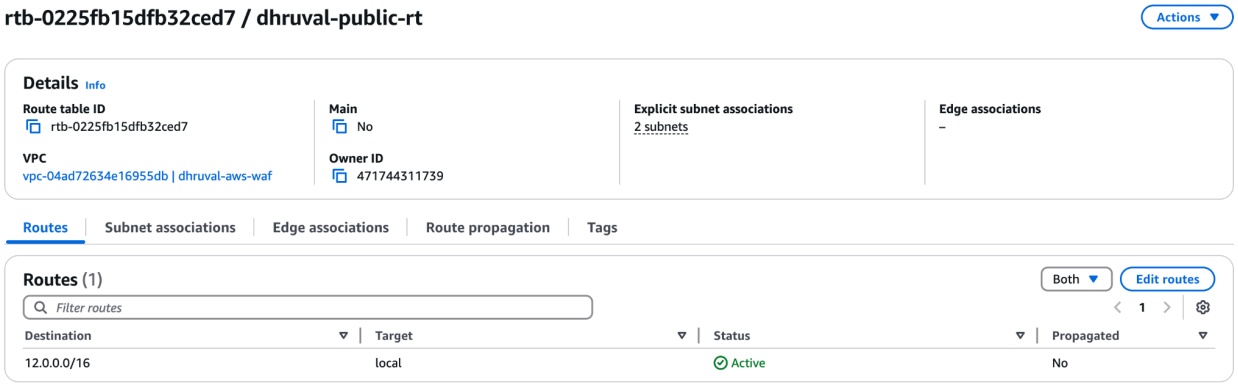


4. Select the created subnets and then save associations.

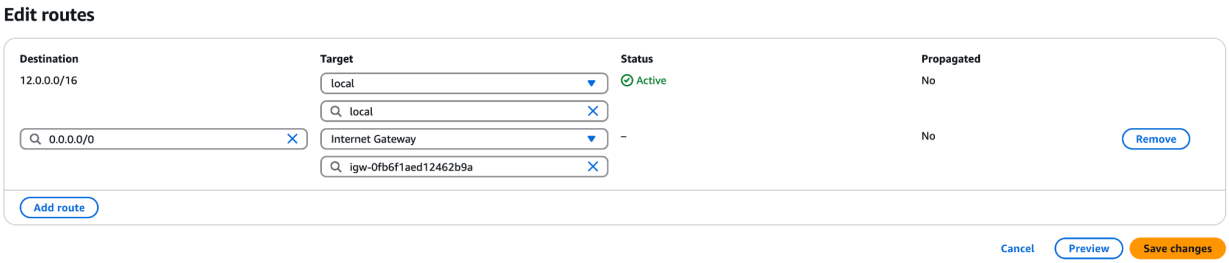


Note: the route table still does not have internet access so it's time to create routes.

5. Click on the routes tab in the created route table and edit routes.



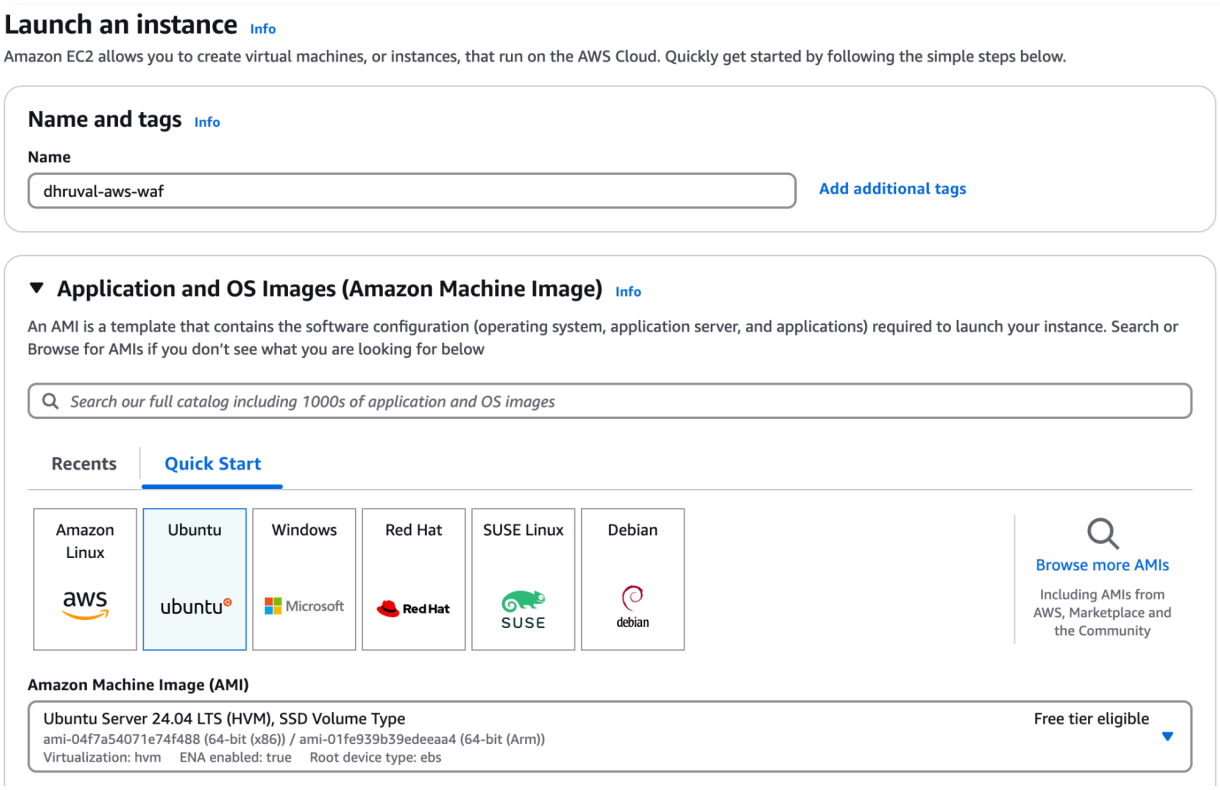
6. Add route, select 0.0.0.0/0 (anyone within and outside of the subnet can access the internet).
7. For target select Internet Gateway and then select the created internet gateway.



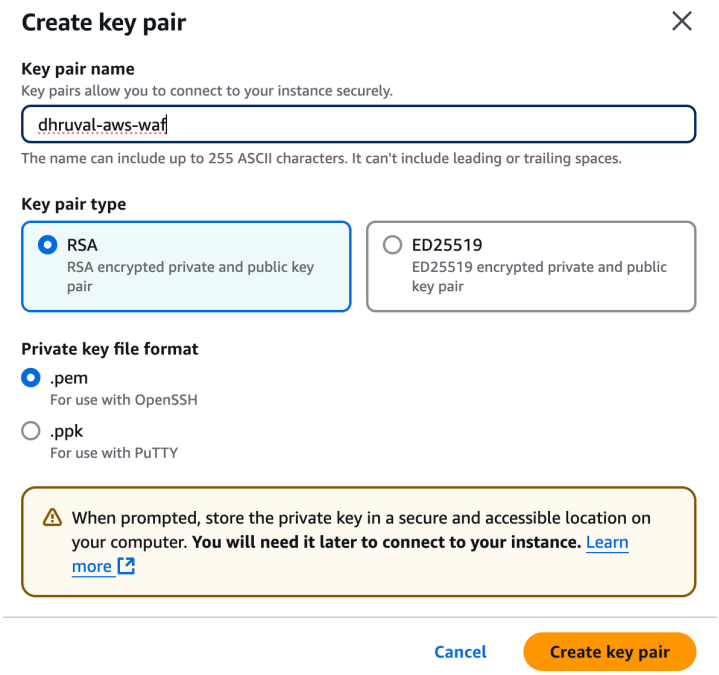
Create an EC2 instance:

Note: this will be the EC2 instance where a user either has access to it or not.

1. Search for EC2 and launch an instance.
2. Name the instance and select appropriate OS.

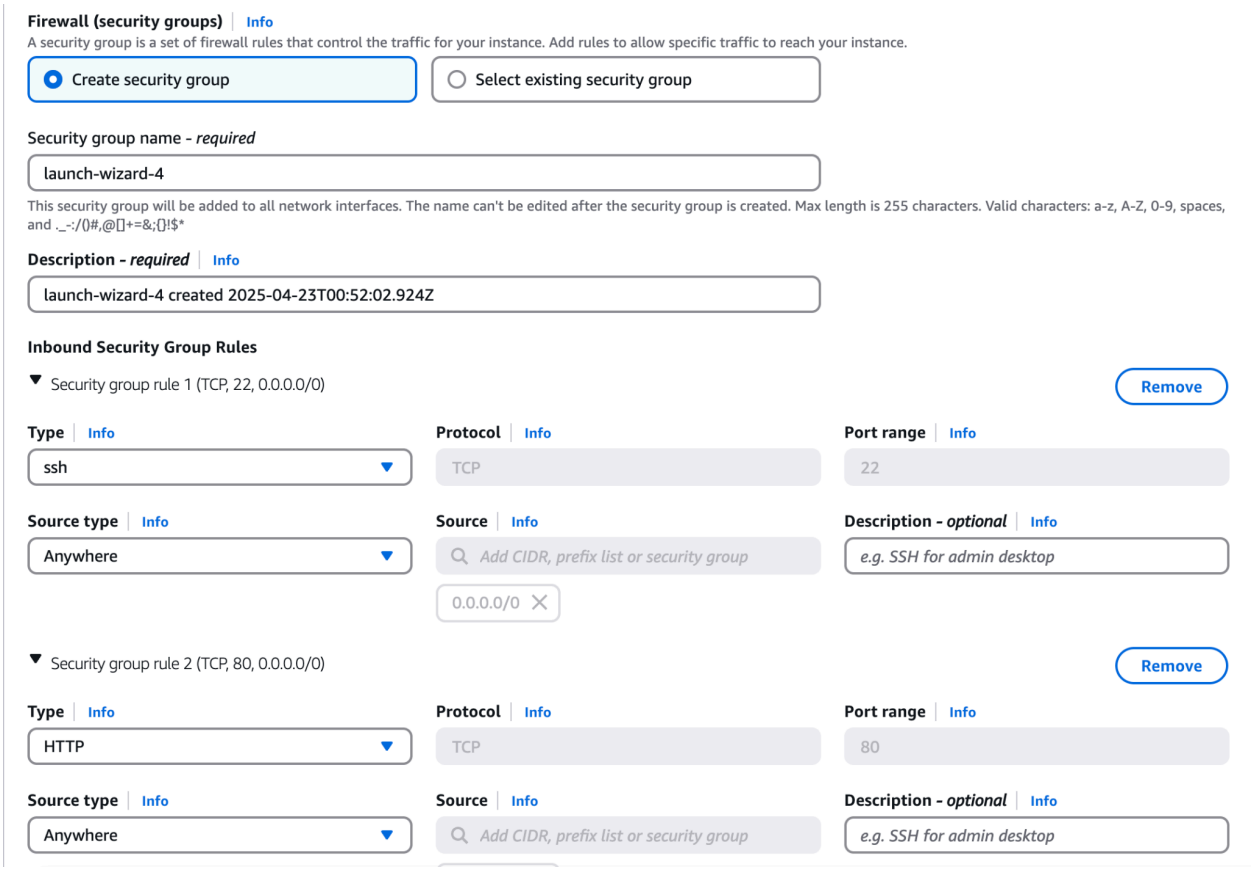


3. Create a key pair for SSH.

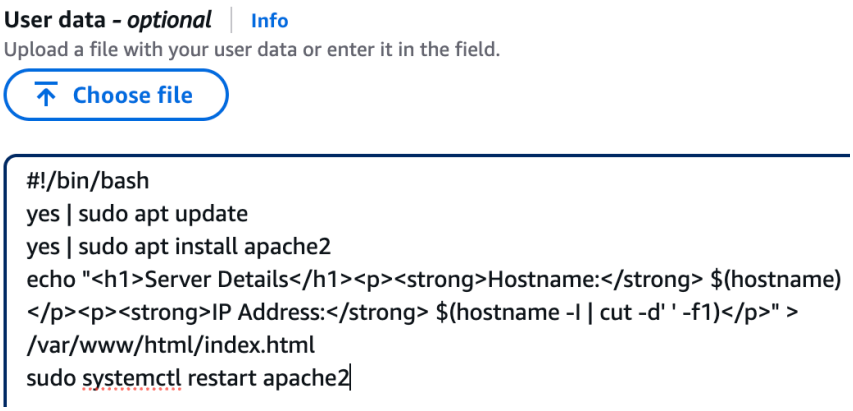


4. Edit the network settings to:
    a. Select the created VPC
    b. Select any subnet
    c. Enable auto-assign public IP

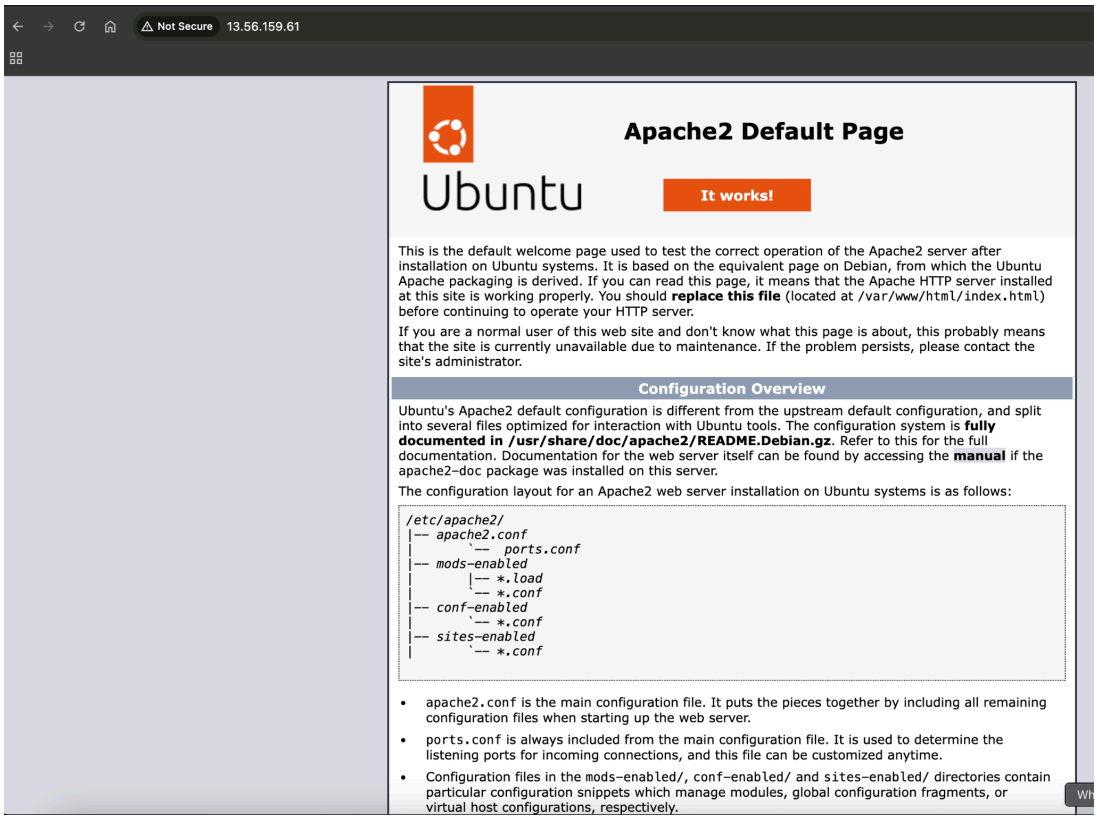
5. Add a new security group along with SSH.
    a. For type select HTTP
    b. Source type must be anywhere so anyone can access it



6. Click advanced details, head down to user data and add a script for the apache server for the EC2 instance. Then launch instance.



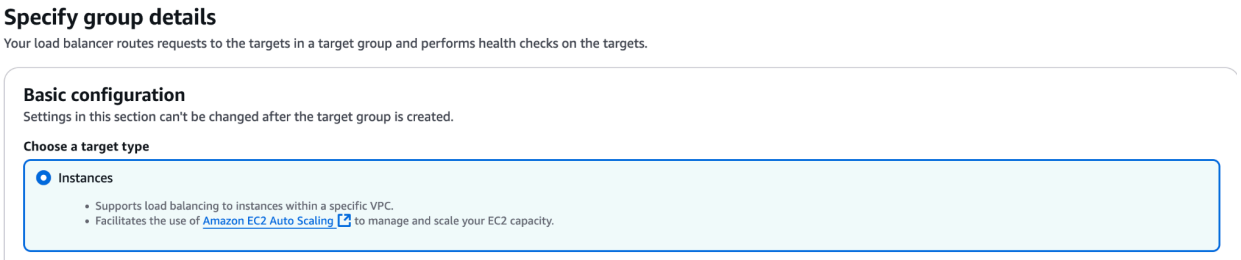
Note: Once the instance is created then copy its public IP, open in a new tab and it should load the apache.

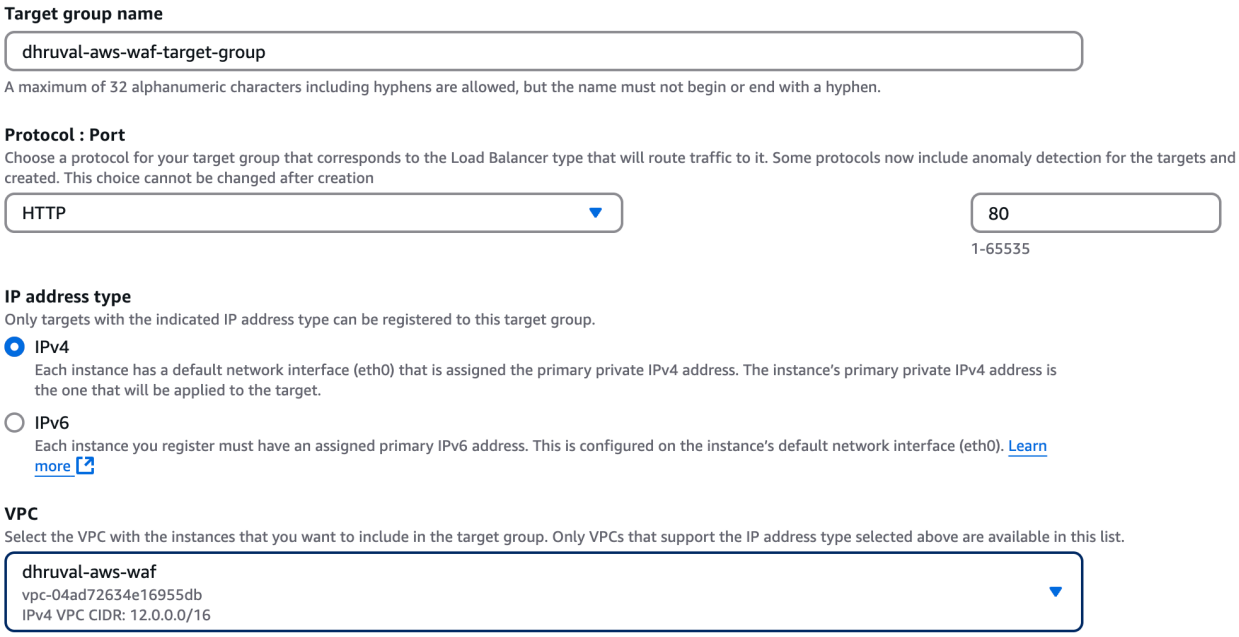


Create Application Load Balancer:

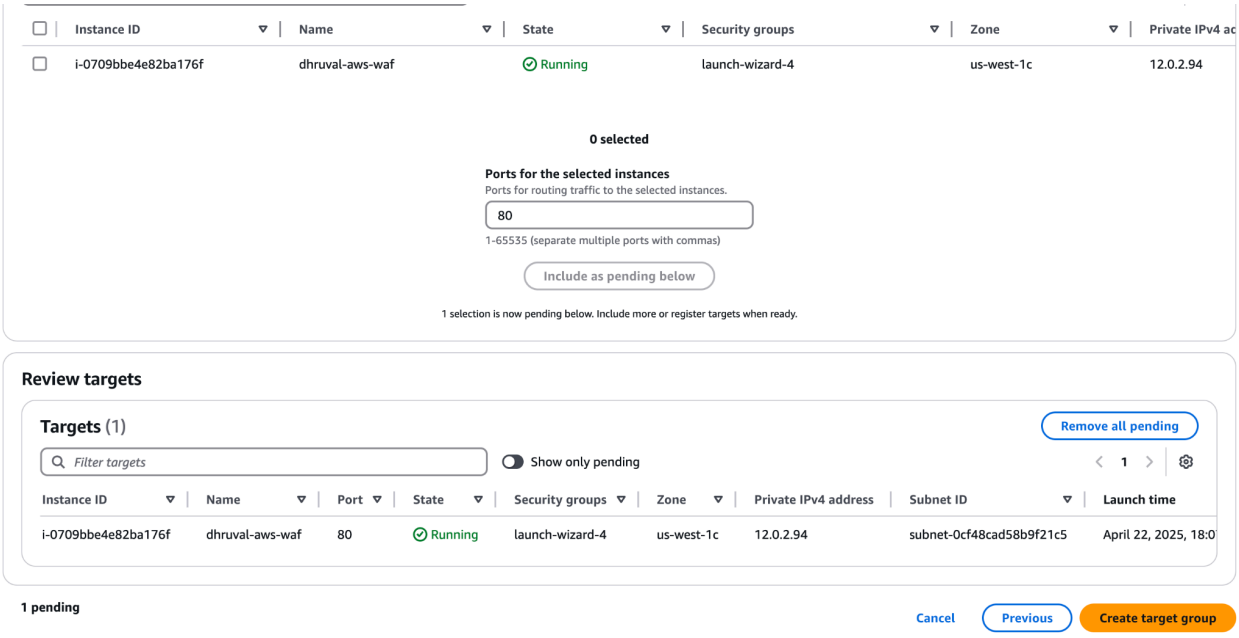
Note: a target group is needed first in order to create a load balancer.

1. On the left side of the navigation bar in EC2, select Target Groups and then create target group.
2. Choose instances as target type, name the target group, leave everything else default and then click next.

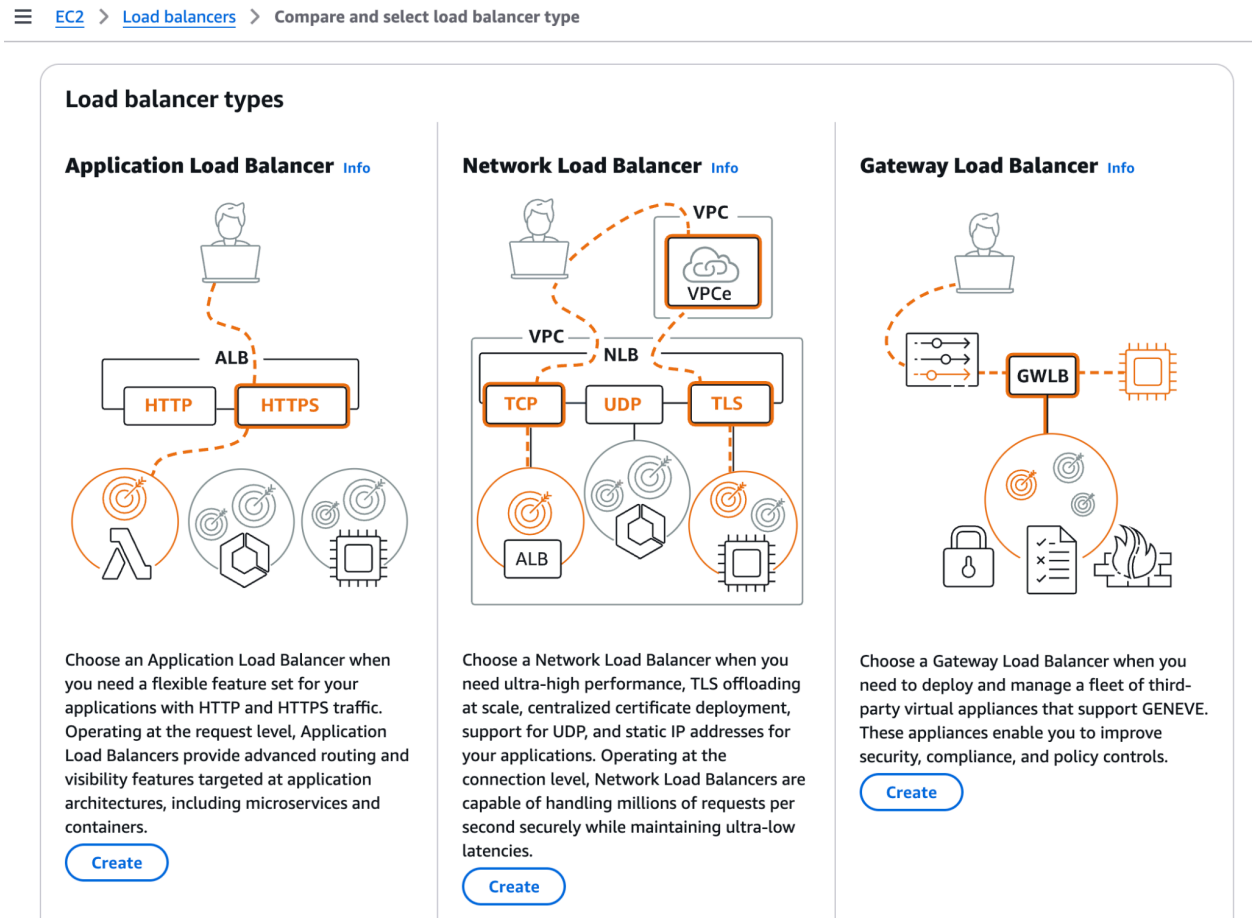




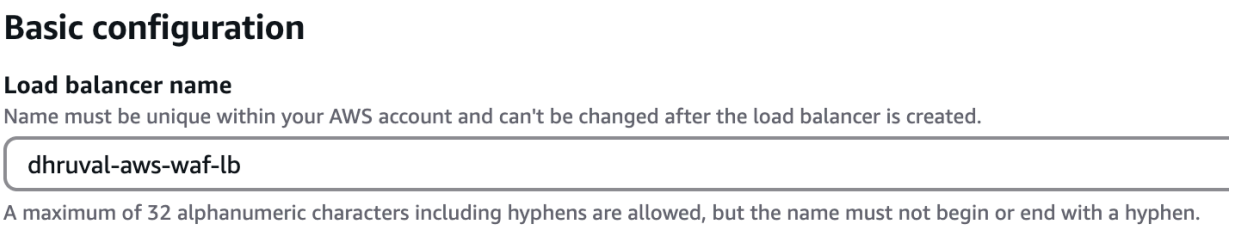
6. Select the EC2 instance, include as pending below, it will be part of the target group and then create target group.



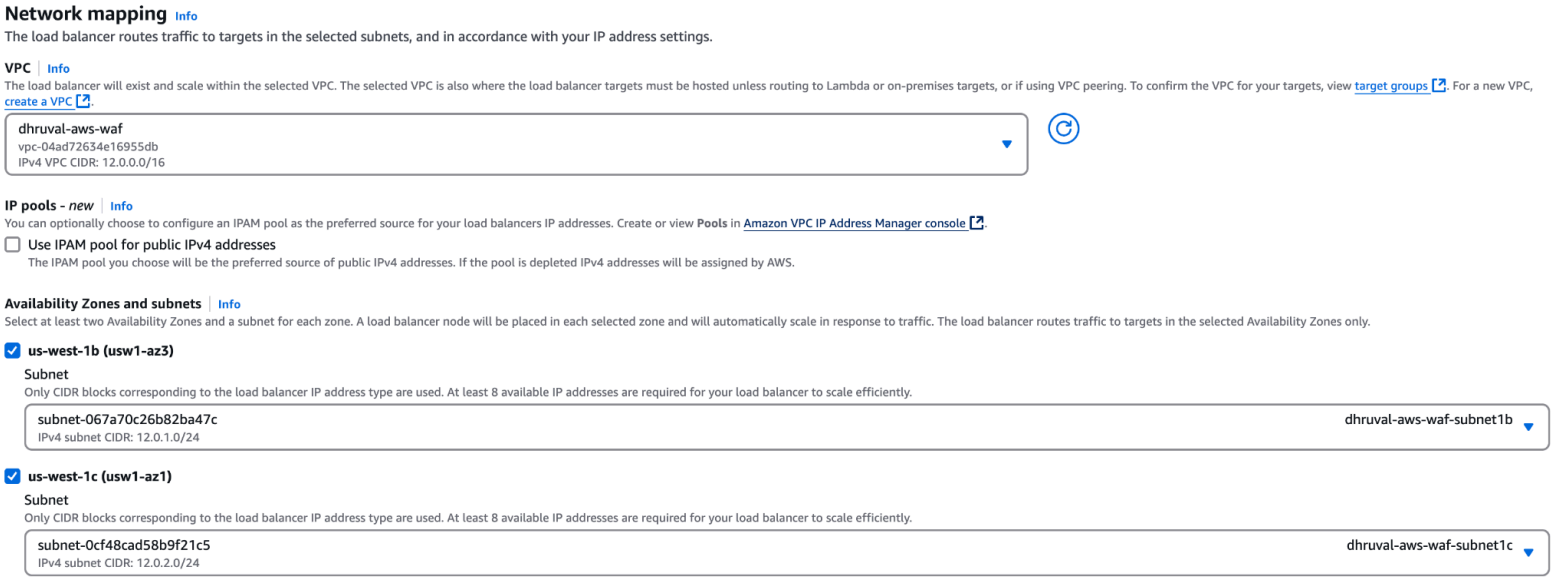
7. Now to create a load balancer again from the left side of the navigation bar in EC2, select Load balancers and create load balancer.
8. Choose the Application load balancer type out of the three and create.



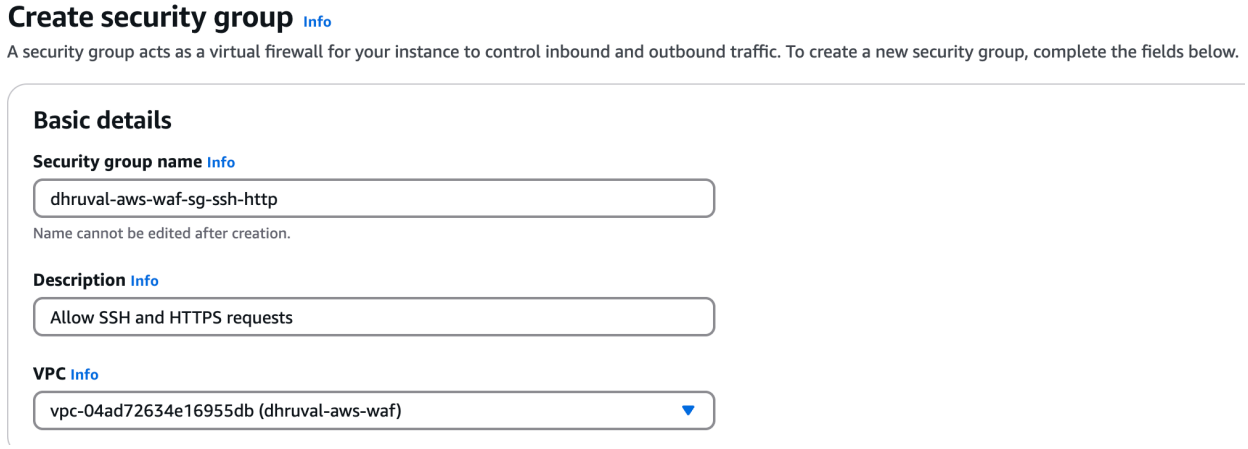
9. Name the load balancer.



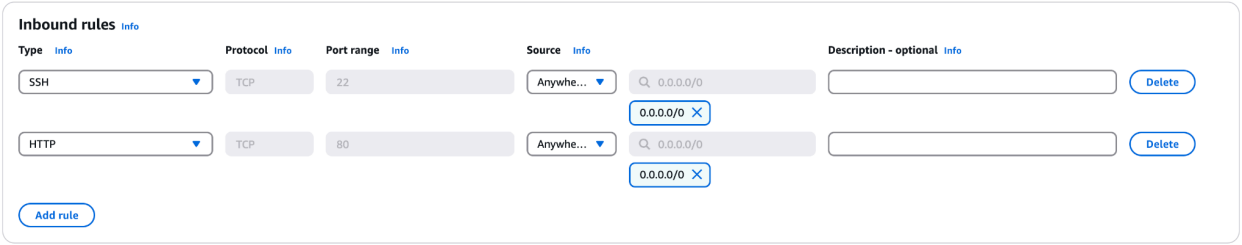
10. Select the created VPC, the two availability zones, and subnets.



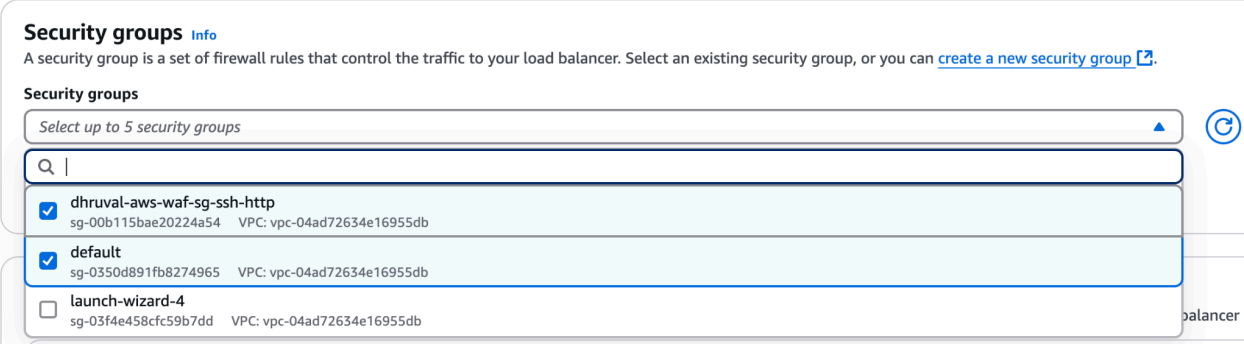
11. Create a new security group to allow SSH and HTTP requests on port 80 for the application load balancer.
12. Name the security group, add a description, and the created VPC.



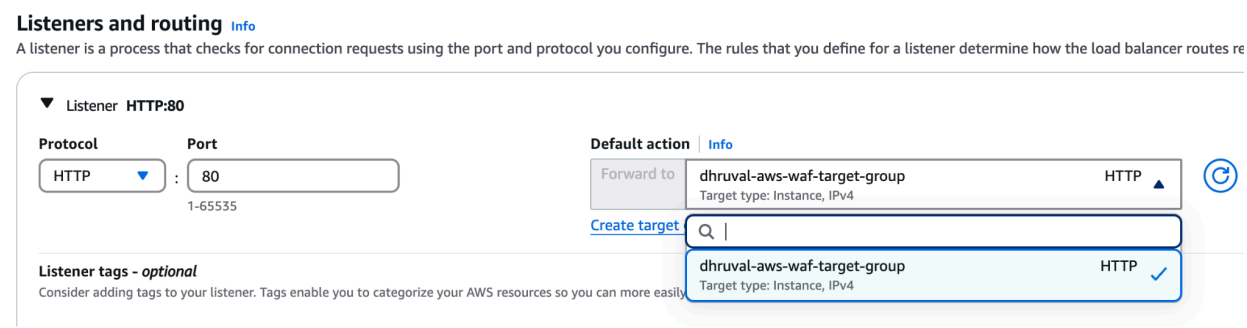
13. Create SSH and HTTP inbound rules with anywhere access (0.0.0.0/0). Then create security group.



14. Once the security group is created, then go back to create application load balancer tab and select the new security group created.

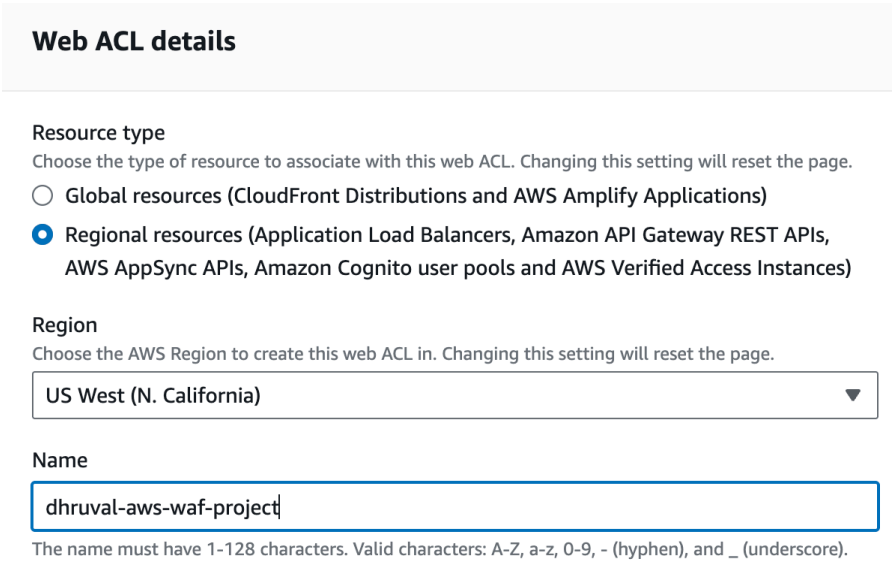


15. For listeners and routing select the target group created in default action. Then leave everything else and create load balancer. Check the DNS name of load balancer to see if it loads after creating it

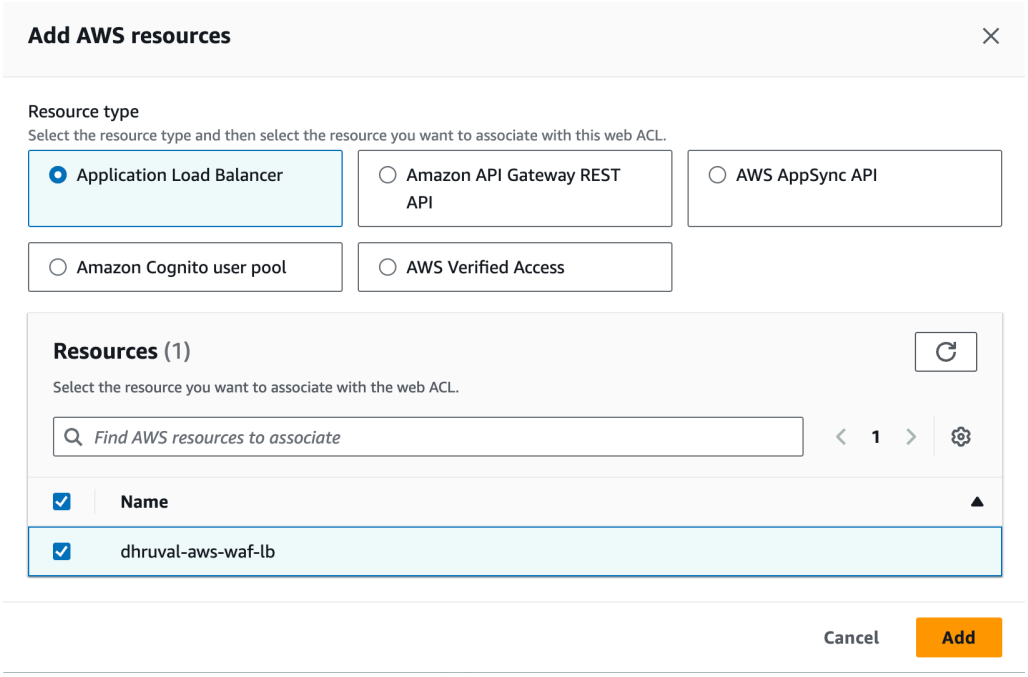


Create WAF (Web Application Firewall):

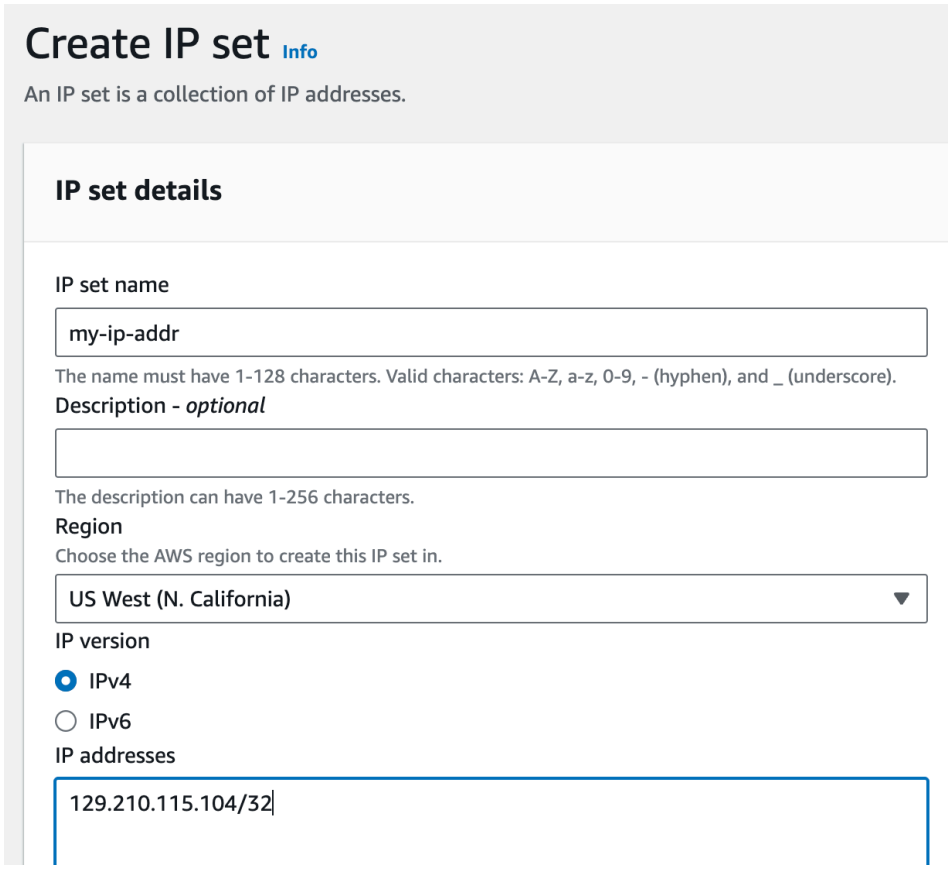
1. Search for WAF and Shield and from its dashboard select create Web ACL.
2. Name the Web ACL and check for the proper region.



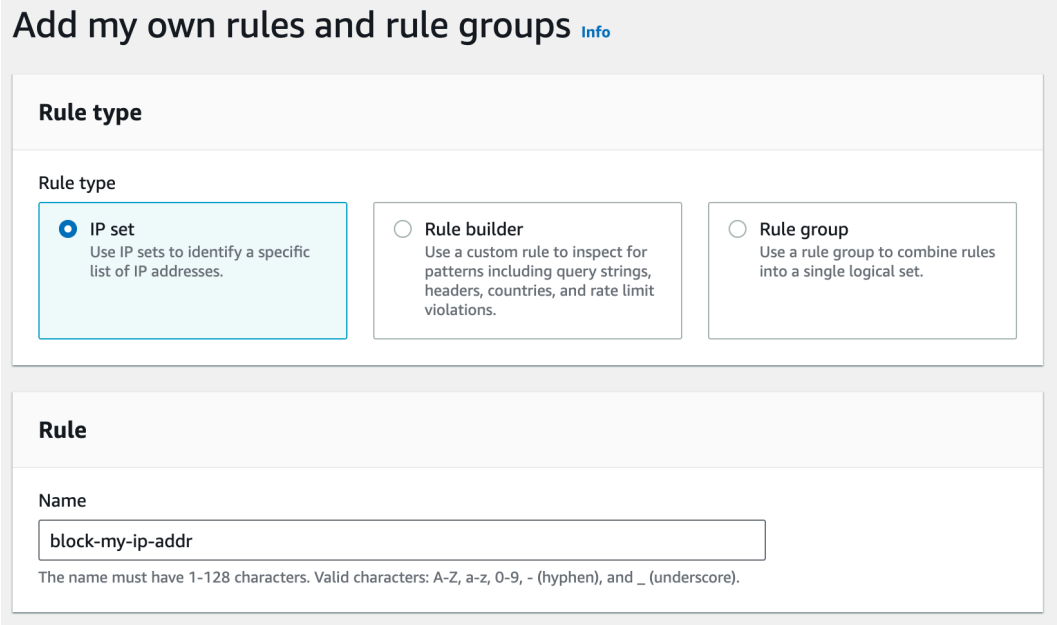
3. From add resources select application load balancer and choose the created load balancer. Add it and then click next.



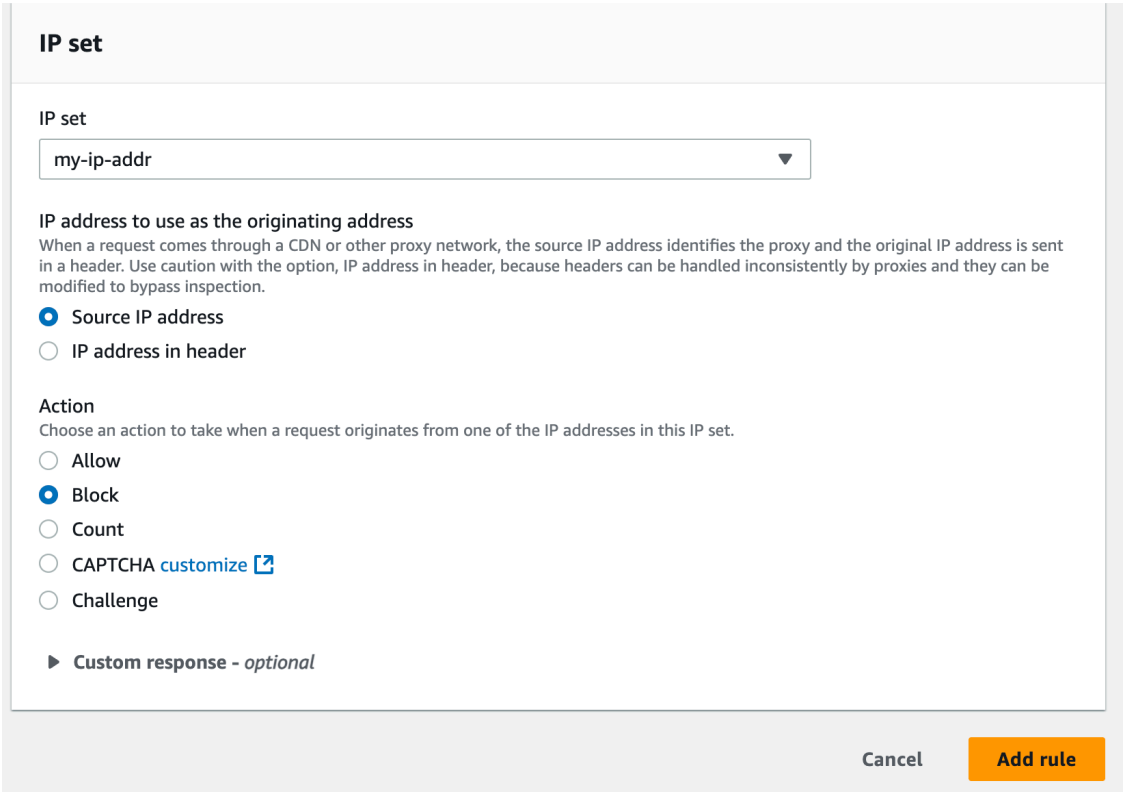
4. Then open the left navigation, select IP sets and create a new IP set to add an IP in order to allow or block it. Name the IP set and add the device IP address with a range.



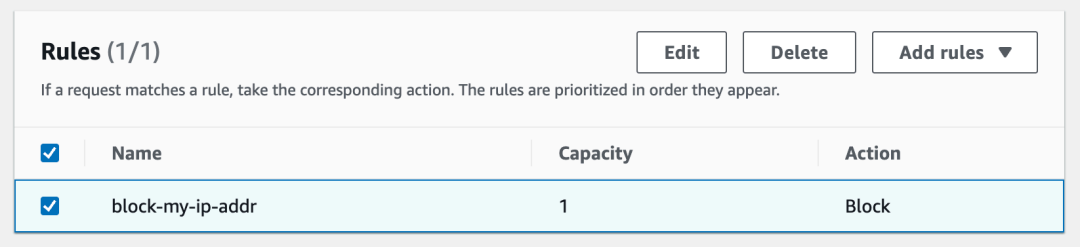
5. Then back to the Web ACL tab, select add rules, and add my own rules and rule groups.
6. Select IP set as rule type and name it.



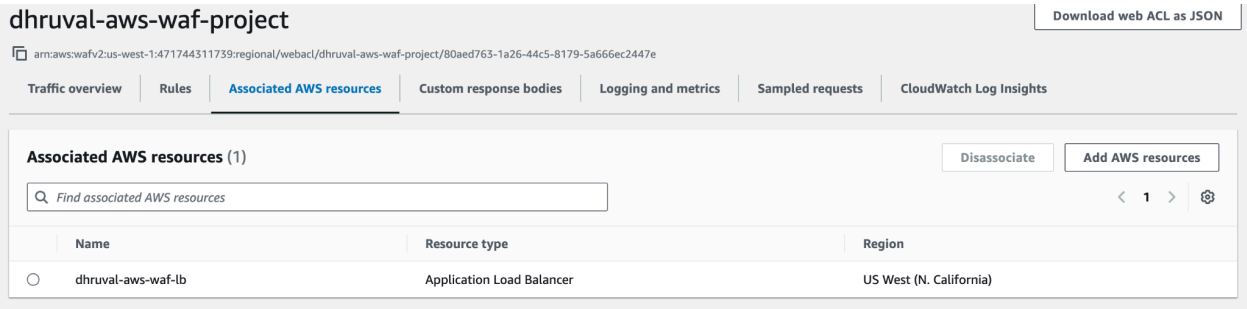
7. For IP set select the IP set created and for action select block. Then add rule.

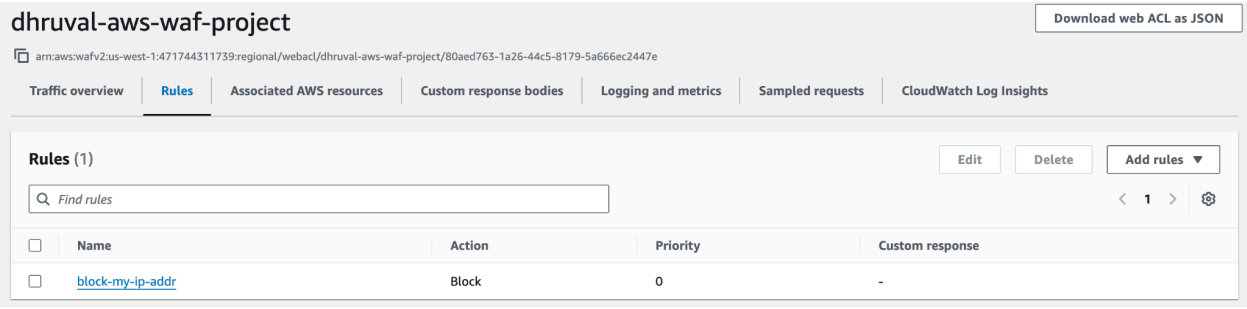


8. Then select the rule created.



9. Then select the rule again, keep everything else default and then create Web ACL.
10. Verify the associated AWS resources with the load balancer and rules in the created Web ACL.



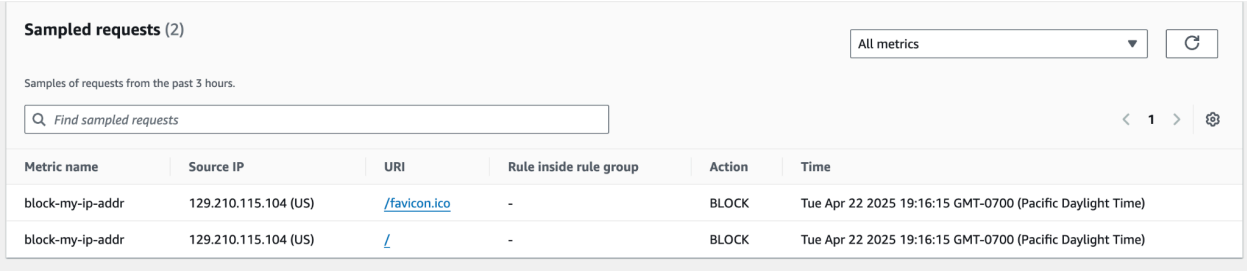


Test the WAF:

1. Go back to EC2, select load balancer, copy its url and open in a new tab and it should be blocked with a 403 forbidden message.

403 Forbidden

2. Check the created Web ACL sampled requests logs to check for blocked access.



Sampled requests (2)

All metrics

Samples of requests from the past 3 hours.

Find sampled requests

1

Metric name	Source IP	URI	Rule inside rule group	Action	Time
block-my-ip-addr	129.210.115.104 (US)	/favicon.ico	-	BLOCK	Tue Apr 22 2025 19:16:15 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/	-	BLOCK	Tue Apr 22 2025 19:16:15 GMT-0700 (Pacific Daylight Time)

Note: the rule can be edited to Allow or CAPTCHA as well for testing purposes. The logs below show allow and CAPTCHA traffic as well after editing the rule.

Sampled requests (11)

All metrics

Samples of requests from the past 3 hours.

Find sampled requests

1 2

Metric name	Source IP	URI	Rule inside rule group	Action	Time
dhruval-aws-waf-project	129.210.115.104 (US)	/	-	ALLOW	Tue Apr 22 2025 19:24:02 GMT-0700 (Pacific Daylight Time)
dhruval-aws-waf-project	129.210.115.104 (US)	/	-	ALLOW	Tue Apr 22 2025 19:24:05 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/	-	CAPTCHA	Tue Apr 22 2025 19:24:02 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/favicon.ico	-	ALLOW	Tue Apr 22 2025 19:23:49 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/	-	CAPTCHA	Tue Apr 22 2025 19:23:52 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/favicon.ico	-	BLOCK	Tue Apr 22 2025 19:16:15 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/	-	ALLOW	Tue Apr 22 2025 19:23:49 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/	-	ALLOW	Tue Apr 22 2025 19:21:54 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/favicon.ico	-	BLOCK	Tue Apr 22 2025 19:21:54 GMT-0700 (Pacific Daylight Time)
block-my-ip-addr	129.210.115.104 (US)	/	-	BLOCK	Tue Apr 22 2025 19:16:15 GMT-0700 (Pacific Daylight Time)

Successfully configured an AWS WAF with an Application Load Balancer to access an EC2 instance with allow, deny, or CAPTCHA actions.