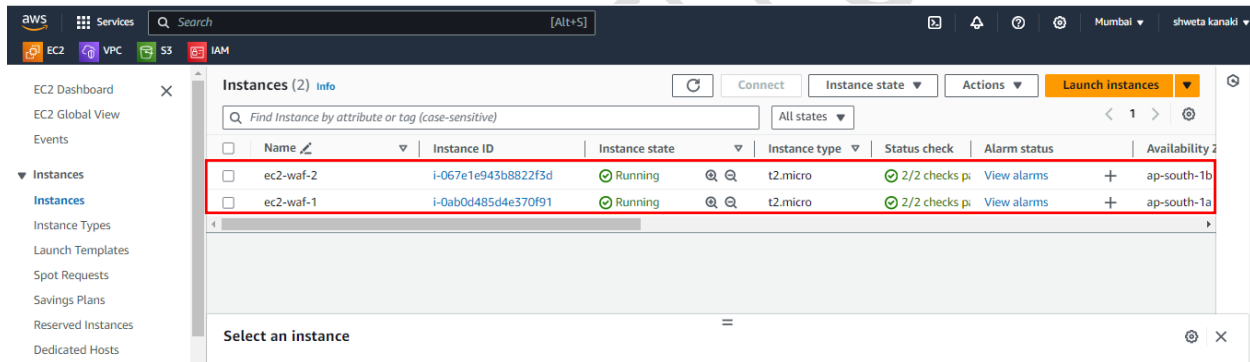


WEB APPLICATION FIREWALL (AWS WAF)

AWS WAF (Web Application Firewall) is a cloud-based firewall service provided by Amazon Web Services (AWS) that helps protect web applications from common web exploits and vulnerabilities. It offers several benefits and features that enhance the security of web applications.

SET UP AWS WAF (WEB APPLICATION FIREWALL) FOR AN EC2 INSTANCE

Step 1: Create two EC2 instances



Configure a simple index.html page in both the instances



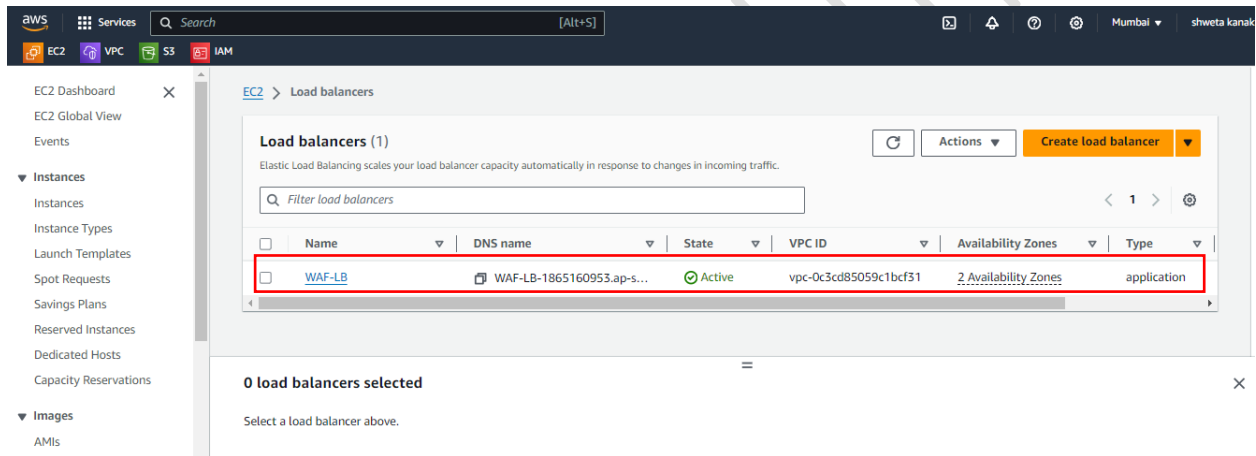
Instance "ec2-waf-1"



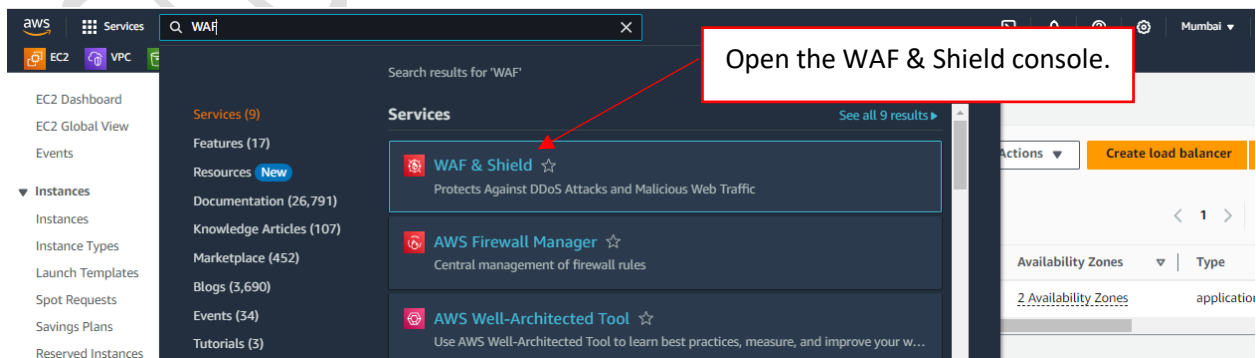
3.110.41.147 this is my ip address

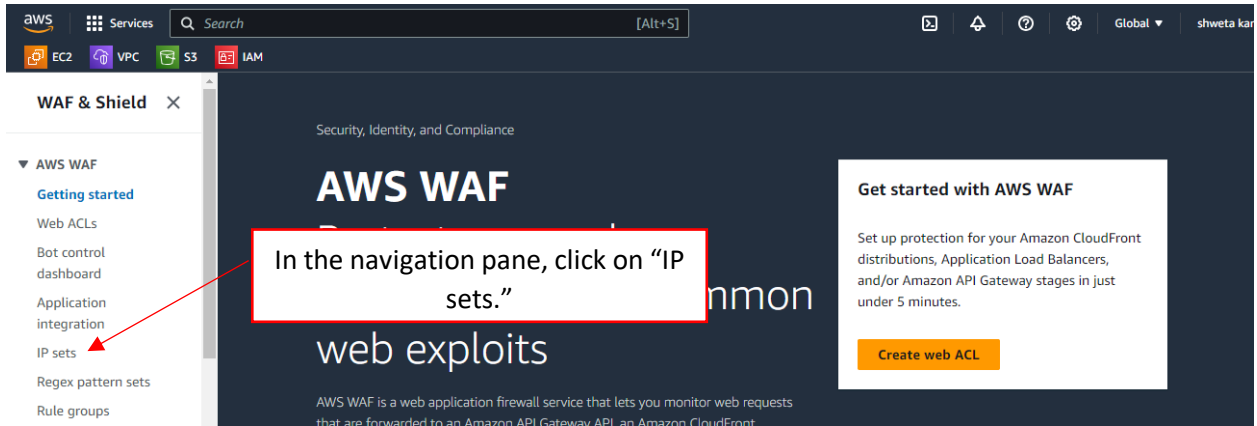
Instance "ec2-waf-2"

Step 2: Create an Application Load Balancer with the Target Group associated with it.



Step 3: Create an IP Set in AWS WAF





aws Services Search [Alt+S]

EC2 VPC S3 IAM

WAF & Shield

AWS WAF

- Getting started
- Web ACLs
- Bot control dashboard
- Application integration
- IP sets
- Regex pattern sets
- Rule groups

Security, Identity, and Compliance

AWS WAF

Common web exploits

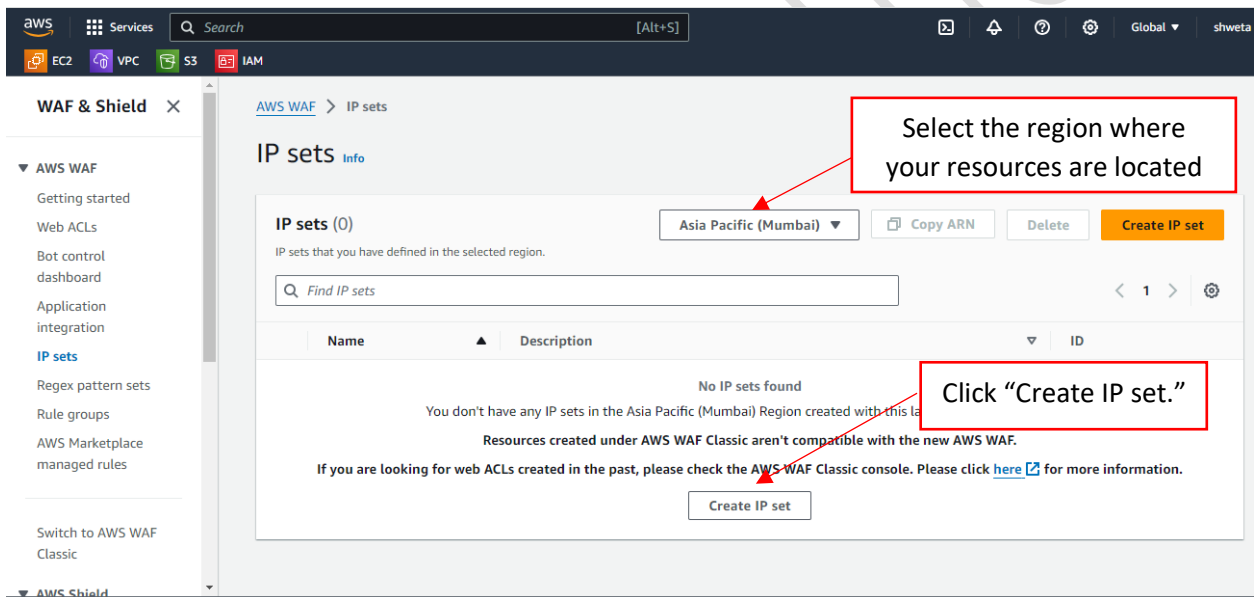
AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront

Get started with AWS WAF

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

Create web ACL

In the navigation pane, click on "IP sets."



aws Services Search [Alt+S]

EC2 VPC S3 IAM

WAF & Shield

AWS WAF

- Getting started
- Web ACLs
- Bot control dashboard
- Application integration
- IP sets
- Regex pattern sets
- Rule groups
- AWS Marketplace managed rules

Switch to AWS WAF Classic

AWS WAF > IP sets

IP sets Info

IP sets (0)

IP sets that you have defined in the selected region.

Find IP sets

Asia Pacific (Mumbai) Copy ARN Delete Create IP set

Name	Description	ID
No IP sets found		
You don't have any IP sets in the Asia Pacific (Mumbai) Region created with this IAM role.		
Resources created under AWS WAF Classic aren't compatible with the new AWS WAF.		
If you are looking for web ACLs created in the past, please check the AWS WAF Classic console. Please click here for more information.		
Create IP set		

Select the region where your resources are located

Click "Create IP set."

[AWS WAF](#) > [IP sets](#) > Create IP set

Create IP set Info

An IP set is a collection of IP addresses.

IP set details

IP set name

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.

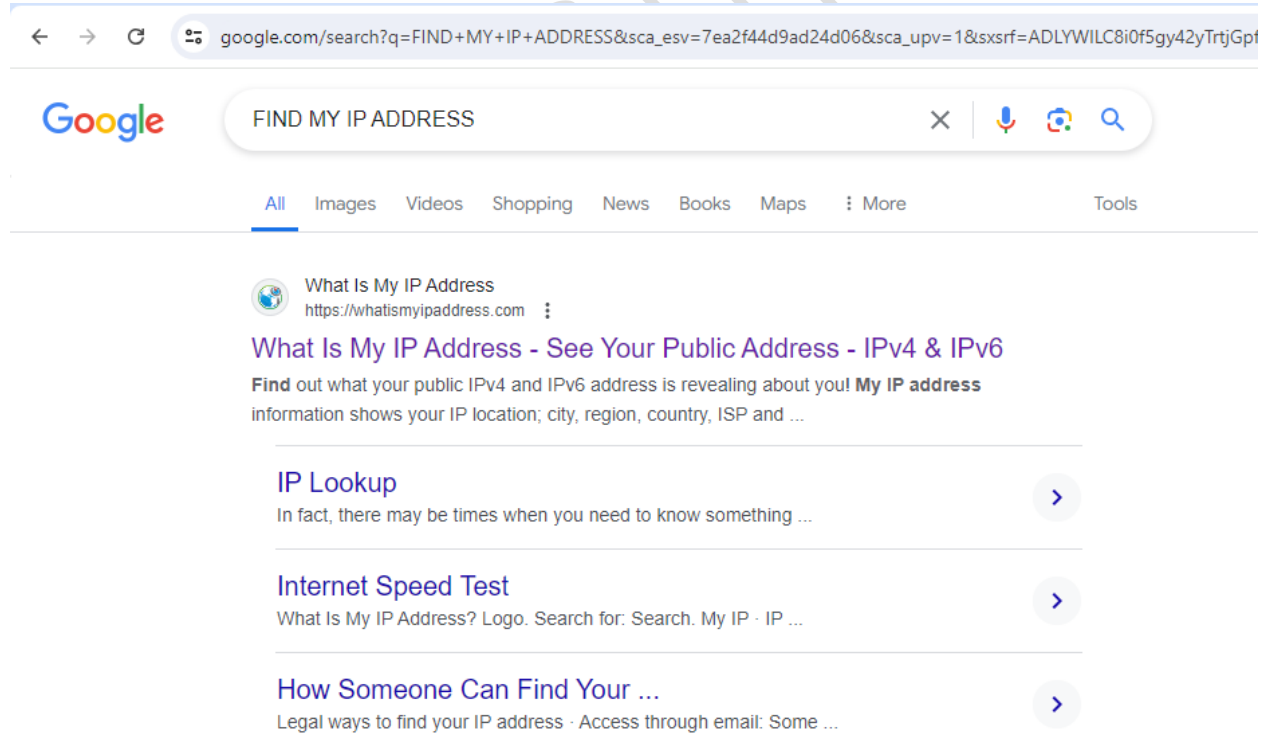
Region

Choose the AWS region to create this IP set in.

Asia Pacific (Mumbai)

Enter a name and for the IP set


Now go to your browser and check for your systems' IP address.



← → ↻ 🔍 google.com/search?q=FIND+MY+IP+ADDRESS&sca_esv=7ea2f44d9ad24d06&sca_upv=1&sxsrf=ADLYWILC8i0f5gy42yTrtjGpt

Google FIND MY IP ADDRESS × 🔊 🌐 🔍

[All](#) [Images](#) [Videos](#) [Shopping](#) [News](#) [Books](#) [Maps](#) [More](#) [Tools](#)

 What Is My IP Address
<https://whatismyipaddress.com>

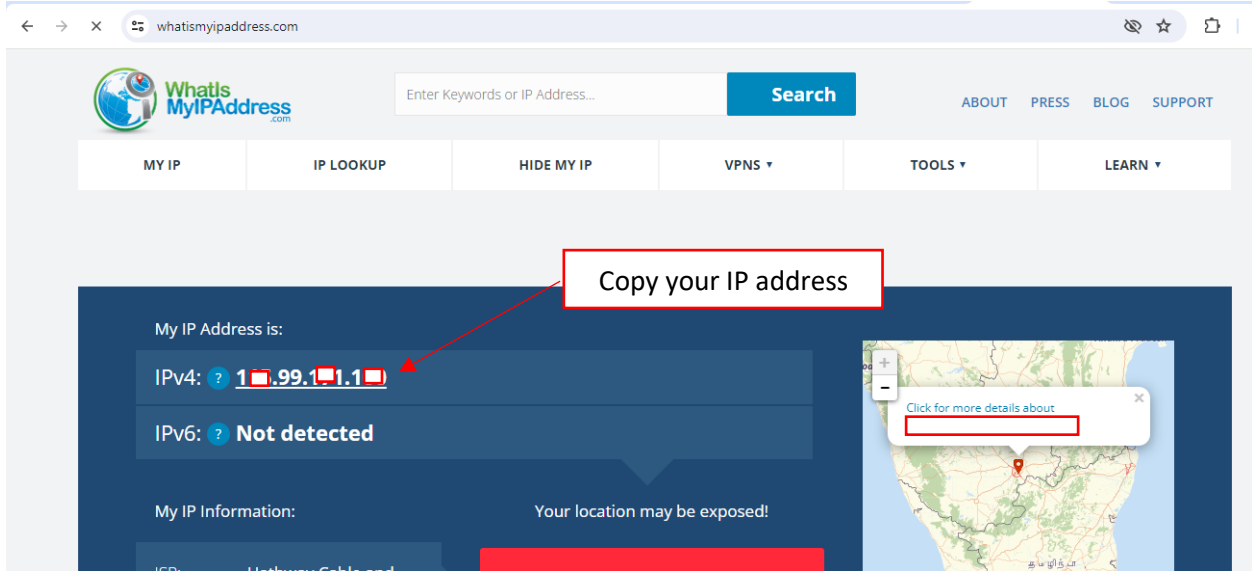
What Is My IP Address - See Your Public Address - IPv4 & IPv6

Find out what your public IPv4 and IPv6 address is revealing about you! **My IP address** information shows your IP location; city, region, country, ISP and ...

IP Lookup >
In fact, there may be times when you need to know something ...

Internet Speed Test >
What Is My IP Address? Logo. Search for: Search. My IP - IP ...

How Someone Can Find Your ... >
Legal ways to find your IP address · Access through email: Some ...



whatismyipaddress.com

Enter Keywords or IP Address... Search

ABOUT PRESS BLOG SUPPORT

MY IP IP LOOKUP HIDE MY IP VPNS TOOLS LEARN

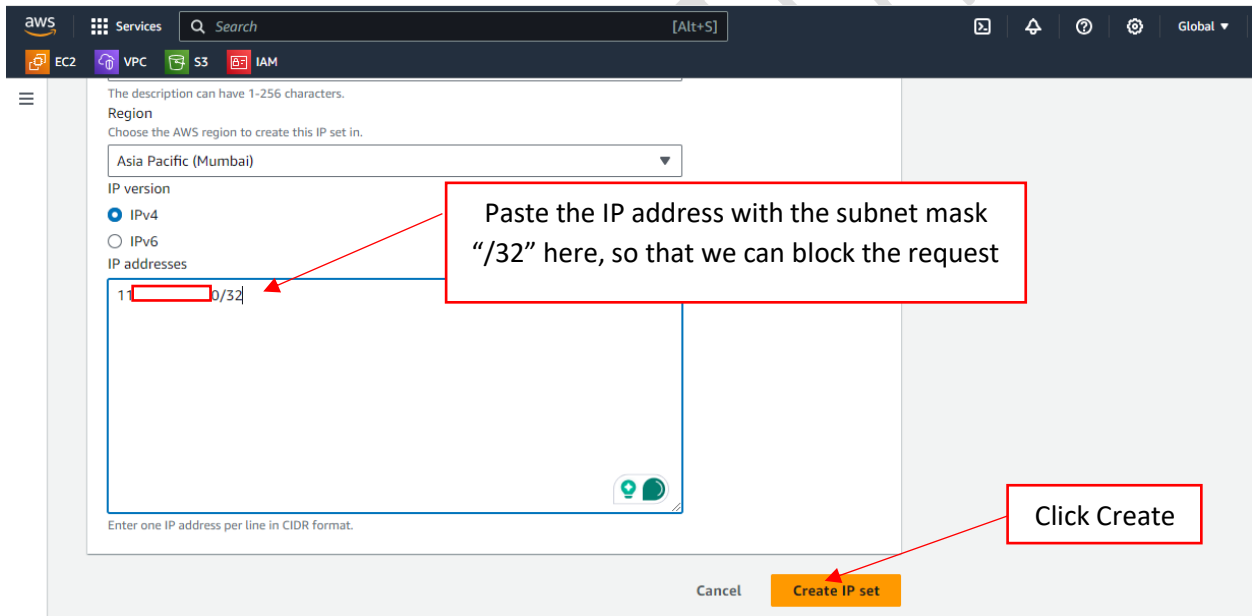
My IP Address is:

IPv4: ? 11.99.1.1

IPv6: ? Not detected

My IP Information: Your location may be exposed!

Copy your IP address



aws Services Search [Alt+S]

EC2 VPC S3 IAM

The description can have 1-256 characters.

Region

Choose the AWS region to create this IP set in.

Asia Pacific (Mumbai)

IP version

☒ IPv4

☐ IPv6

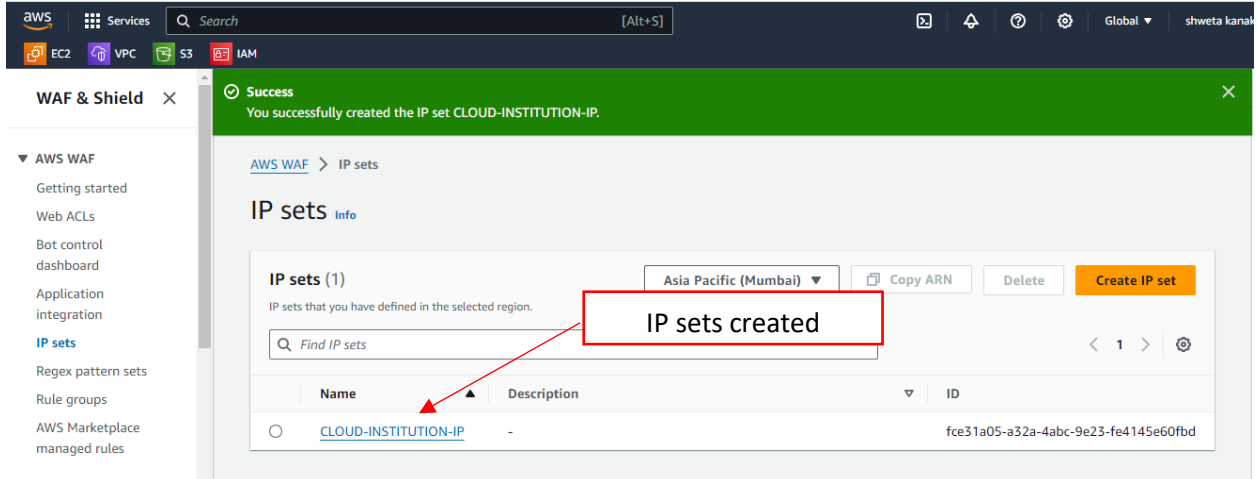
IP addresses

11.99.1.1/32

Paste the IP address with the subnet mask "/32" here, so that we can block the request

Click Create

Cancel Create IP set

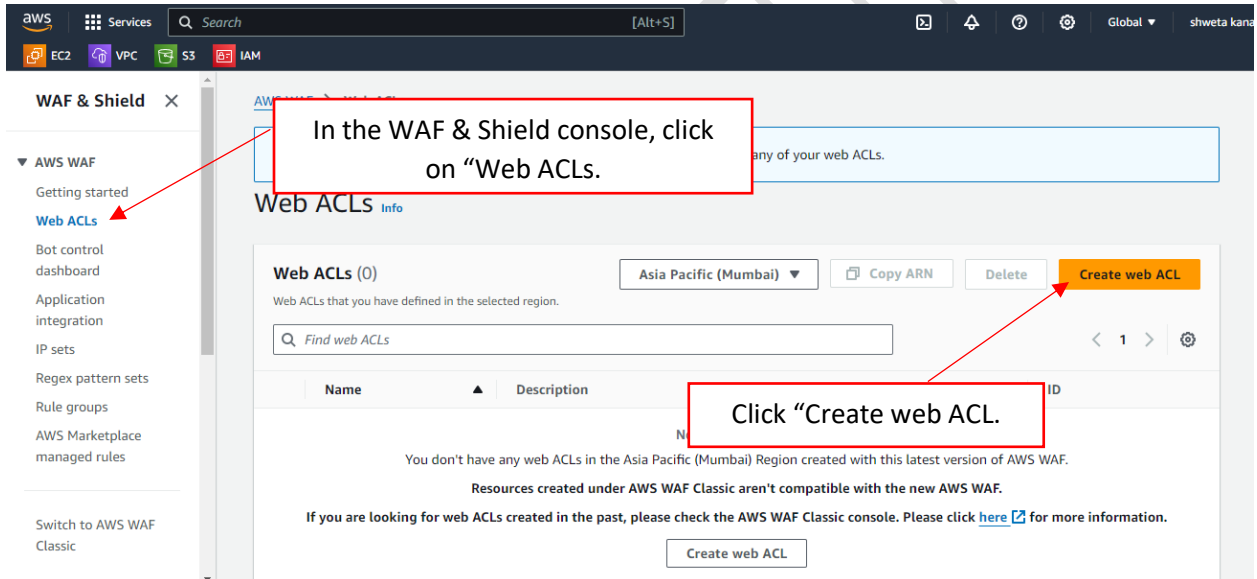


The screenshot shows the AWS WAF & Shield console. A green success banner at the top states: "Success You successfully created the IP set CLOUD-INSTITUTION-IP." The left sidebar shows the "WAF & Shield" menu with "IP sets" selected. The main content area displays "IP sets (1)" for the "Asia Pacific (Mumbai)" region. A table lists the created IP set:

Name	Description	ID
CLOUD-INSTITUTION-IP	-	fce31a05-a32a-4abc-9e23-fe4145e60fbd

Annotations: A red box labeled "IP sets created" points to the success banner. A red arrow points from the "Name" column header to the "CLOUD-INSTITUTION-IP" entry in the table.

Step 4: Create a Web ACL in AWS WAF.



The screenshot shows the AWS WAF & Shield console. The left sidebar shows the "WAF & Shield" menu with "Web ACLs" selected. The main content area displays "Web ACLs (0)" for the "Asia Pacific (Mumbai)" region. A message states: "You don't have any web ACLs in the Asia Pacific (Mumbai) Region created with this latest version of AWS WAF. Resources created under AWS WAF Classic aren't compatible with the new AWS WAF. If you are looking for web ACLs created in the past, please check the AWS WAF Classic console. Please click [here](#) for more information." A "Create web ACL" button is visible. Annotations: A red box labeled "In the WAF & Shield console, click on 'Web ACLs.'" points to the "Web ACLs" link in the left sidebar. A red box labeled "Click 'Create web ACL.'" points to the "Create web ACL" button.

aws Services Search [Alt+S]

EC2 VPC S3 IAM

AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

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.

Asia Pacific (Mumbai)

Name
MY-NEW-WAF

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

Select the Resource type

Enter a name for the Web ACL.

aws Services Search [Alt+S]

EC2 VPC S3 IAM

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
MY-NEW-WAF

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

Associated AWS resources - optional (0)

Remove Add AWS resources

Find associated AWS resources

Name	Resource type	Region
No items No items to display		

Cancel Next

Click on Add AWS Resource

Choose "Application Load Balancer."

Resource type

Select the resource type and then select the resource you want to associate with this web ACL.

☒ Application Load Balancer

☐ Amazon API Gateway REST API

☐ Amazon App Runner service

☐ AWS AppSync GraphQL API

☐ Amazon Cognito user pool

☐ AWS Verified Access

Select the resources you want to associate with the web ACL.

Find AWS resources to associate

< 1 >

☒ Name

☒ WAF-LB

Cancel

Add

Select the created LB and click ADD

aws Services Search [Alt+S]

EC2 VPC S3 IAM

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

MY-NEW-WAF

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

Associated AWS resources - optional (1)

Remove Add AWS resources

Find associated AWS resources

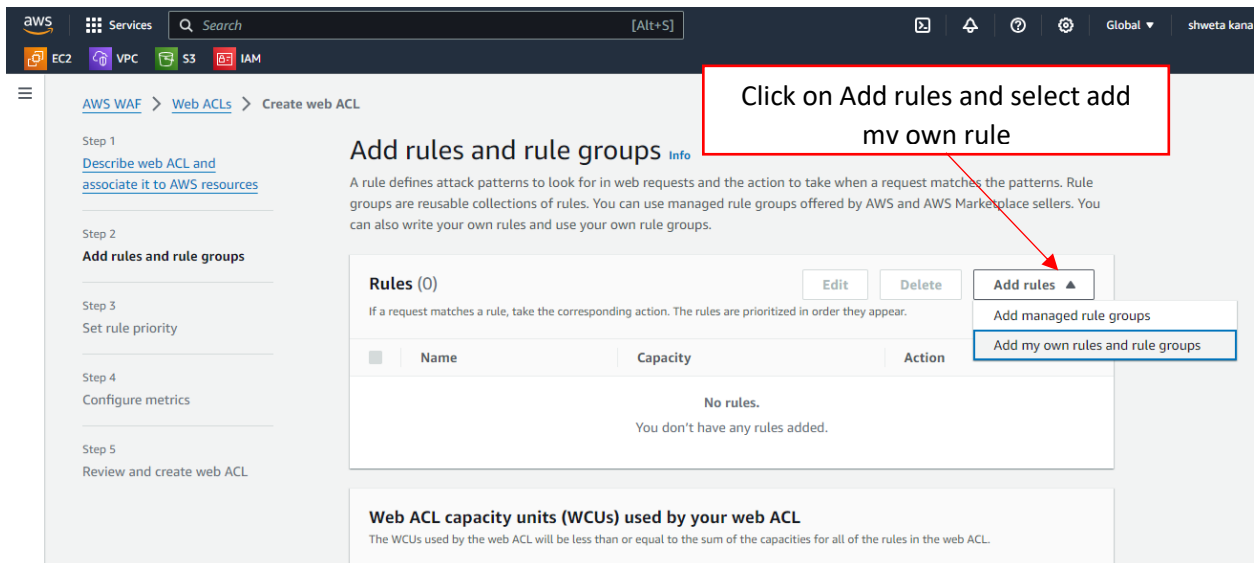
<input type="checkbox"/>	Name	Resource type	Region
<input type="checkbox"/>	WAF-LB	Application Load Balancer	Asia Pacific (Mumbai)

Resource added

Click Next

Cancel Next

Add Rules to the Web ACL



Click on Add rules and select add my own rule

Add rules and rule groups [Info](#)

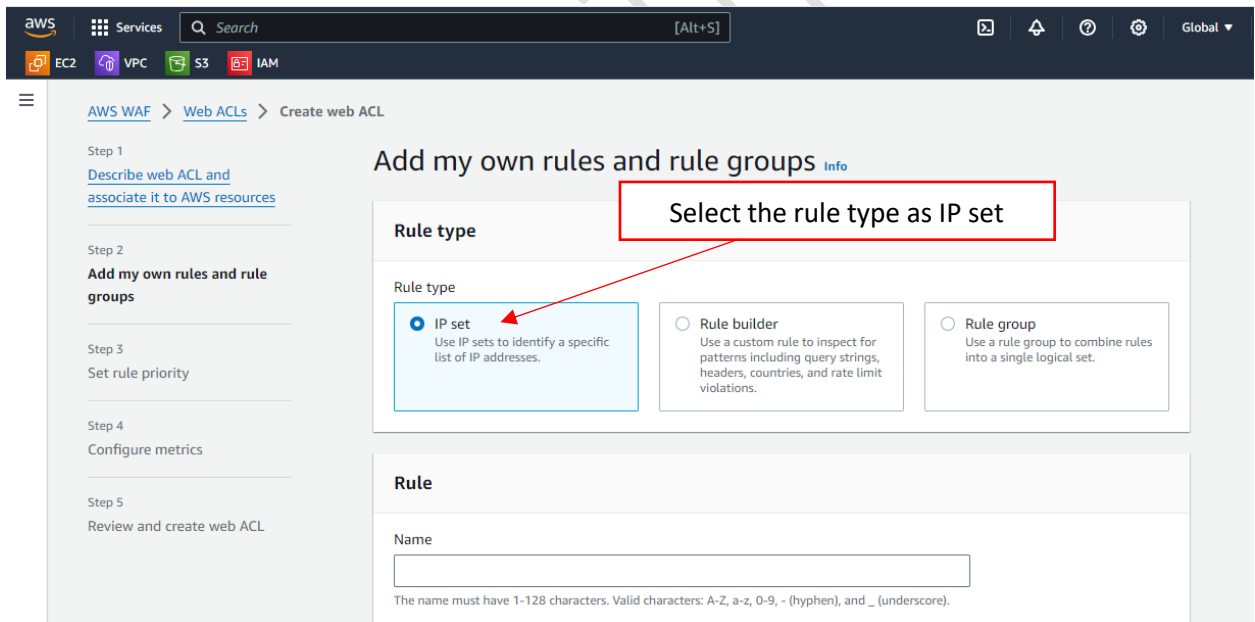
A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (0) [Edit](#) [Delete](#) [Add rules ▴](#)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

Name	Capacity	Action
No rules. You don't have any rules added.		

Web ACL capacity units (WCUs) used by your web ACL
The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.



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

Name

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

aws Services Search [Alt+S] Global

Click on Add AWS Resource

Step 5
Review and create web ACL

Rule

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

IP set

IP set
CLOUD-INSTITUTION-IP

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.

aws Services Search Global

EC2 VPC S3 IAM

Under IP set, select the created IP set from the dropdown menu.

IP set
CLOUD-INSTITUTION-IP

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

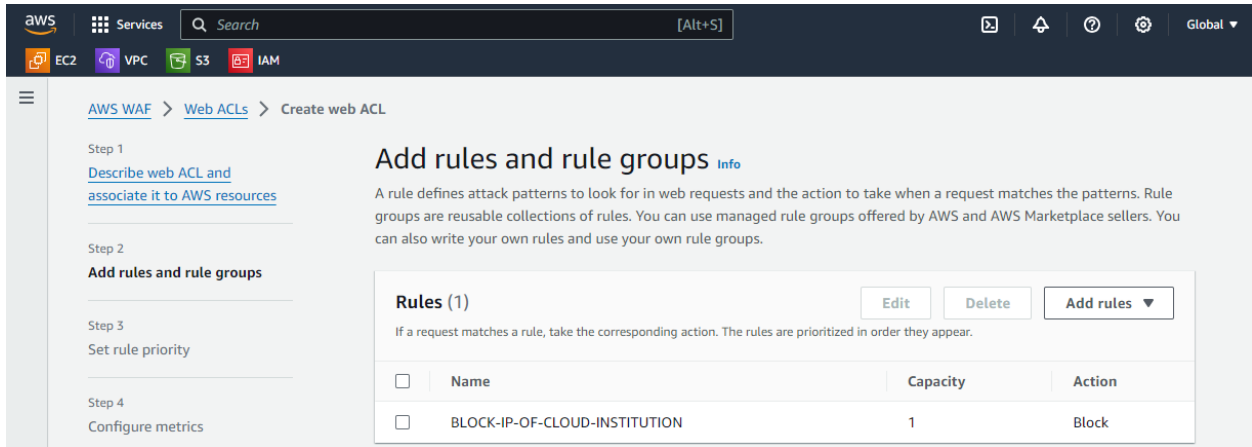
Action
Choose an action to take when a request originates from one of the IP addresses in this IP set.

☐ Allow
☒ Block
☐ Count
☐ CAPTCHA
☐ Challenge

► Custom response - optional

Specify the action to be taken (Allow, Block, or Count) for requests that match the IP set and click on ADD RULE.

Cancel Add rule



The screenshot shows the AWS WAF console with the 'Create web ACL' wizard. Step 2, 'Add rules and rule groups', is active. The 'Rules (1)' table lists one rule: 'BLOCK-IP-OF-CLOUD-INSTITUTION' with a capacity of 1 and an action of 'Block'. The left sidebar shows the progress of the wizard steps.

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

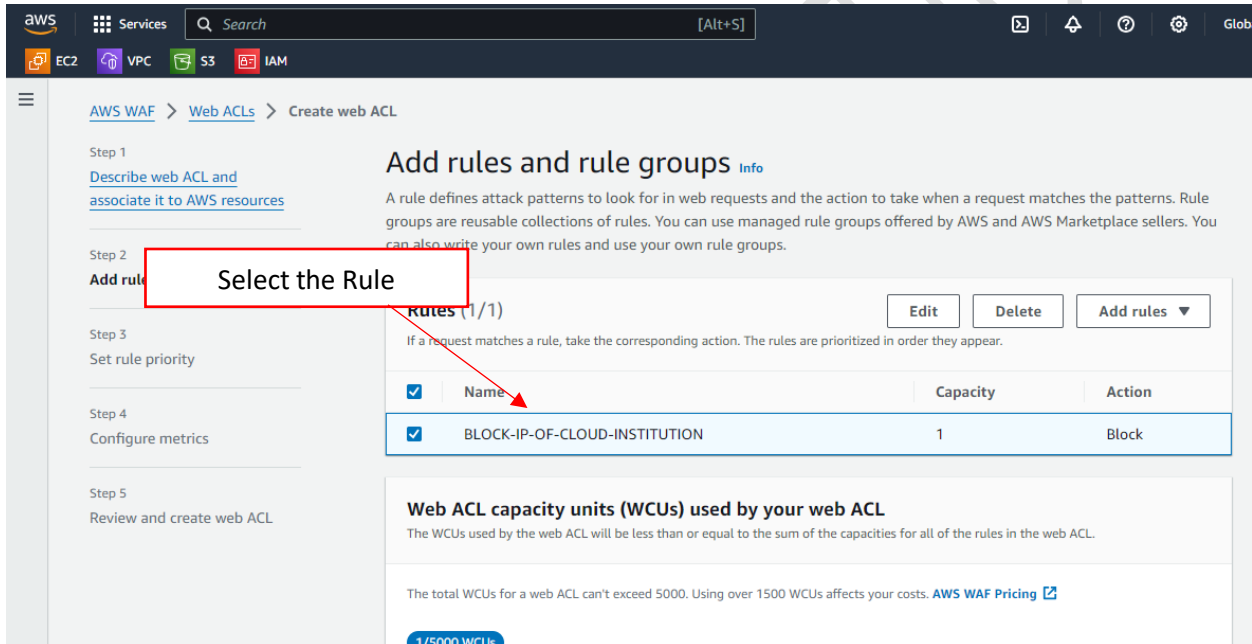
Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (1) [Edit](#) [Delete](#) [Add rules ▼](#)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	BLOCK-IP-OF-CLOUD-INSTITUTION	1	Block



The screenshot shows the AWS WAF console with the 'Create web ACL' wizard. Step 2, 'Add rules and rule groups', is active. A red box highlights the text 'Select the Rule' with an arrow pointing to the 'BLOCK-IP-OF-CLOUD-INSTITUTION' rule in the table. The 'Rules (1/1)' table lists one rule: 'BLOCK-IP-OF-CLOUD-INSTITUTION' with a capacity of 1 and an action of 'Block'. The left sidebar shows the progress of the wizard steps.

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (1/1) [Edit](#) [Delete](#) [Add rules ▼](#)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

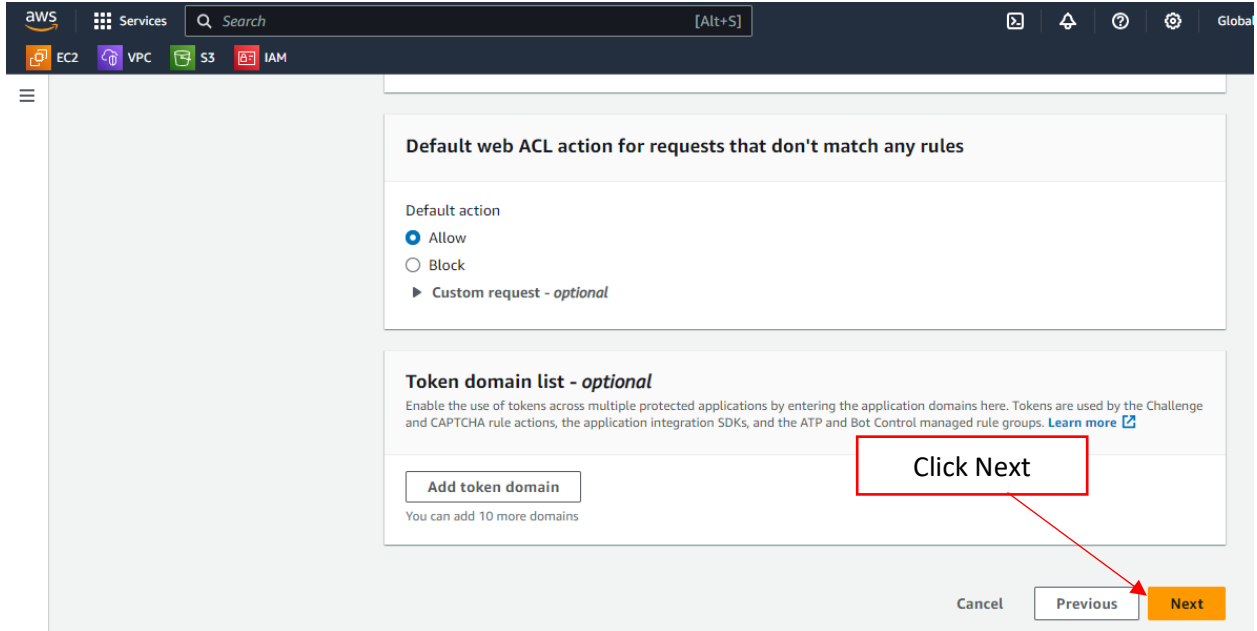
<input checked="" type="checkbox"/>	Name	Capacity	Action
<input checked="" type="checkbox"/>	BLOCK-IP-OF-CLOUD-INSTITUTION	1	Block

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. [AWS WAF Pricing](#)

1/5000 WCUs



Default web ACL action for requests that don't match any rules

Default action

☒ Allow

☐ Block

► Custom request - *optional*

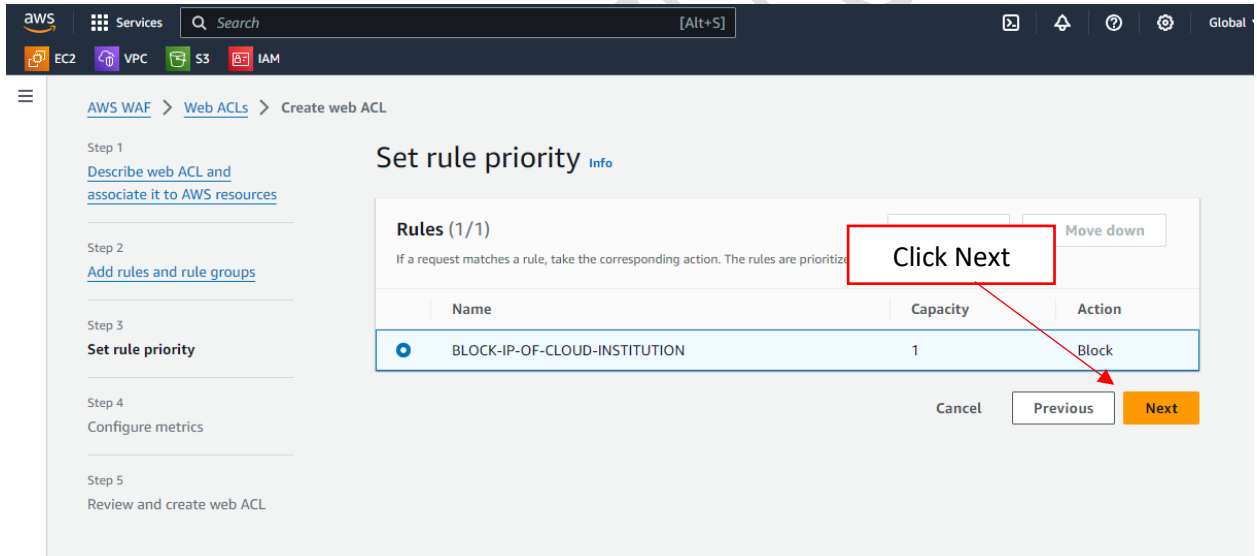
Token domain list - optional

Enable the use of tokens across multiple protected applications by entering the application domains here. Tokens are used by the Challenge and CAPTCHA rule actions, the application integration SDKs, and the ATP and Bot Control managed rule groups. [Learn more](#)

You can add 10 more domains

Click Next

Cancel Previous **Next**



AWS WAF > Web ACLs > Create web ACL

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
[Add rules and rule groups](#)

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Set rule priority Info

Rules (1/1)

If a request matches a rule, take the corresponding action. The rules are prioritized by the order in which they are listed.

Name	Capacity	Action
<input checked="" type="radio"/> BLOCK-IP-OF-CLOUD-INSTITUTION	1	Block

Click Next

Cancel Previous **Next**

aws Services Search [Alt+S]

EC2 VPC S3 IAM

AWS WAF > Web ACLs > Create web ACL

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
[Add rules and rule groups](#)

Step 3
[Set rule priority](#)

Step 4
Configure metrics

Step 5
[Review and create web ACL](#)

Configure metrics [Info](#)

Amazon CloudWatch metrics
CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.

Rules	CloudWatch metric name
<input checked="" type="checkbox"/> BLOCK-IP-OF-CLOUD-INSTITUTION	<input type="text" value="BLOCK-IP-OF-CLOUD-INSTITUTION"/>

Request sampling options
If you disable request sampling, you can't view requests that match your web ACL rules.

Options

- ☒ Enable sampled requests
- ☐ Disable sampled requests
- ☐ Enable sampled requests with exclusions

Click Next

Cancel Previous **Next**

aws Services Search [Alt+S]

EC2 VPC S3 IAM

AWS WAF > Web ACLs > Create web ACL

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
[Add rules and rule groups](#)

Step 3
[Set rule priority](#)

Step 4
[Configure metrics](#)

Step 5
Review and create web ACL

Review and create web ACL [Info](#)

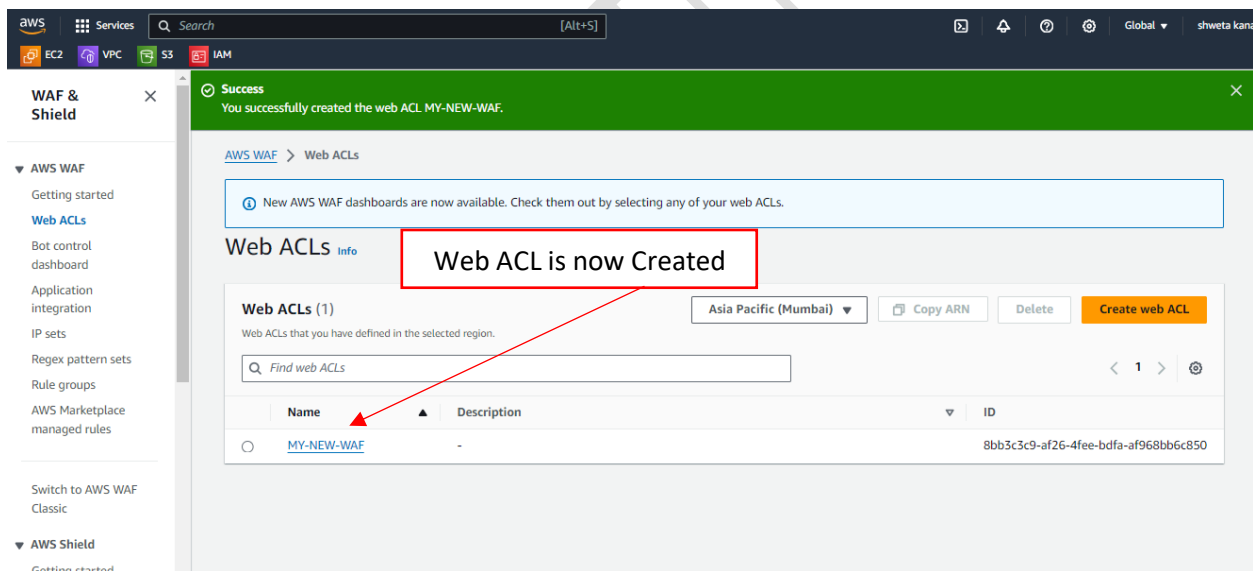
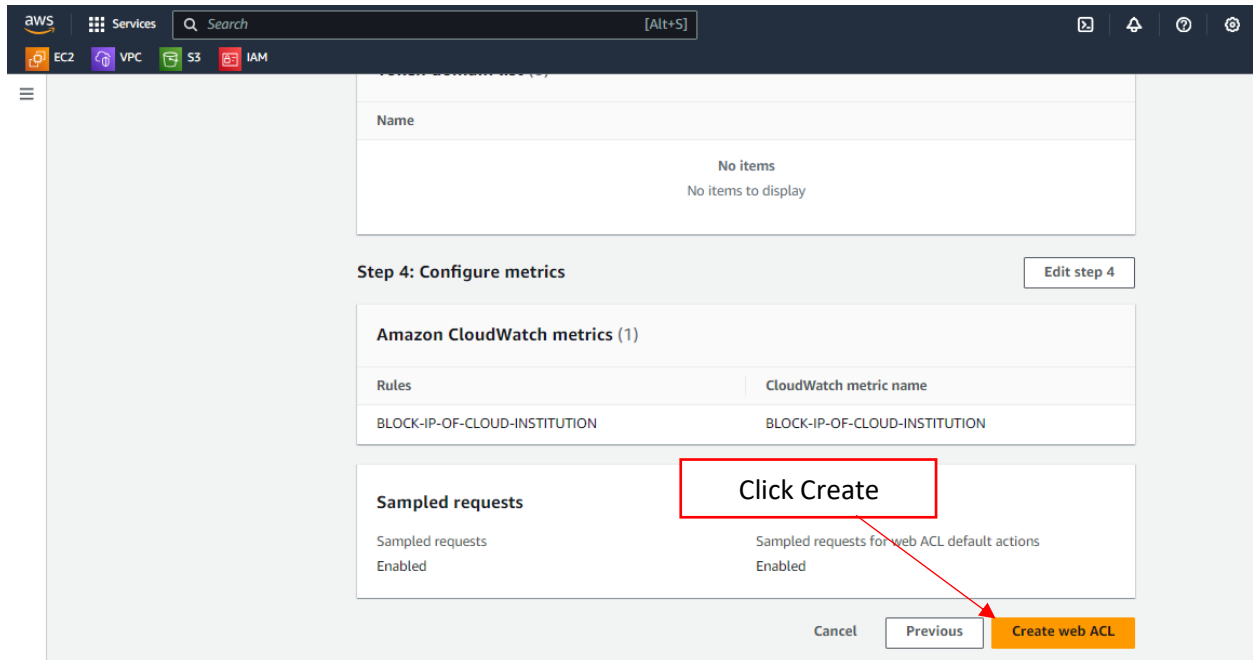
Step 1: Describe web ACL and associate it to AWS resources [Edit step 1](#)

Web ACL details

Name	MY-NEW-WAF	Scope	REGIONAL
Description		Region	ap-south-1
CloudWatch metric name	MY-NEW-WAF		

Steps 2 and 3: Add rules and set rule priority [Edit steps 2 and 3](#)

Rules (1)
If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.



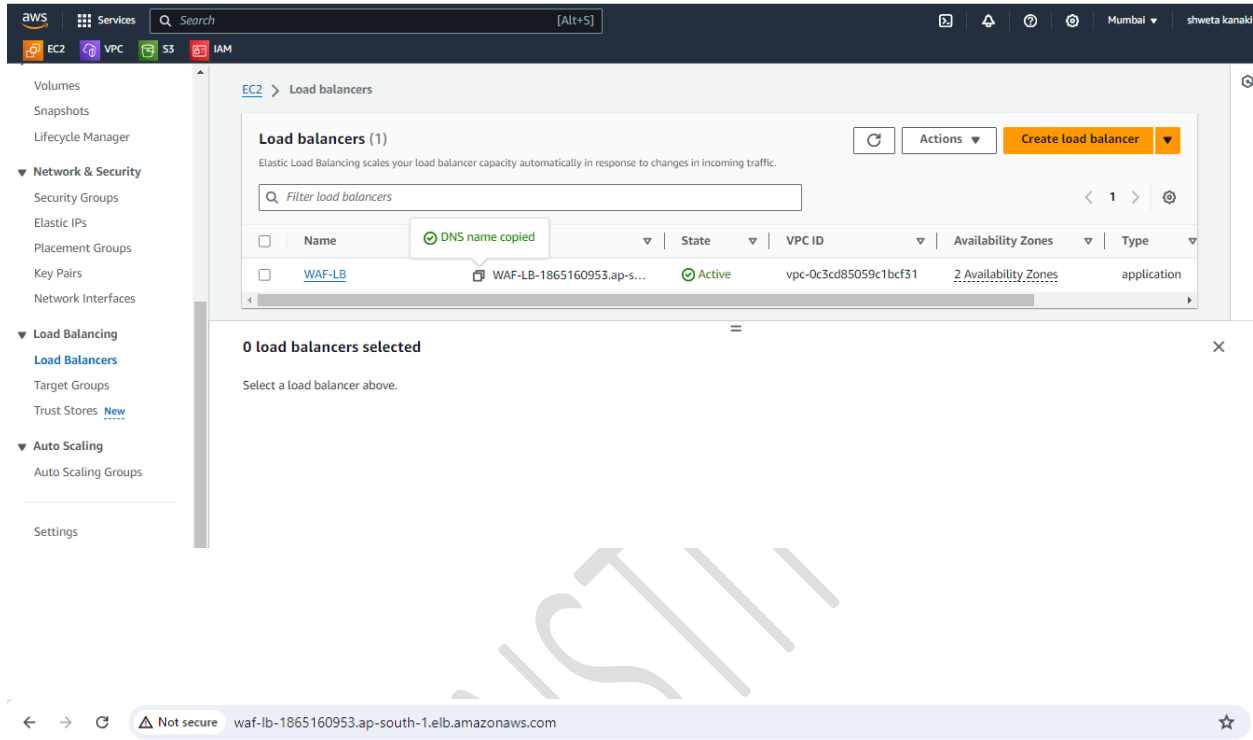
Step 5 : Verify the Configuration

Verify the Association:

- Navigate to the AWS WAF & Shield console.
- Select your Web ACL and check the "Associated AWS resources" tab.
- Ensure your Application Load Balancer is listed.

Step 6: Testing the AWS WAF.

Now go to the Load Balancer and copy the DNS Name and paste it in the browser.



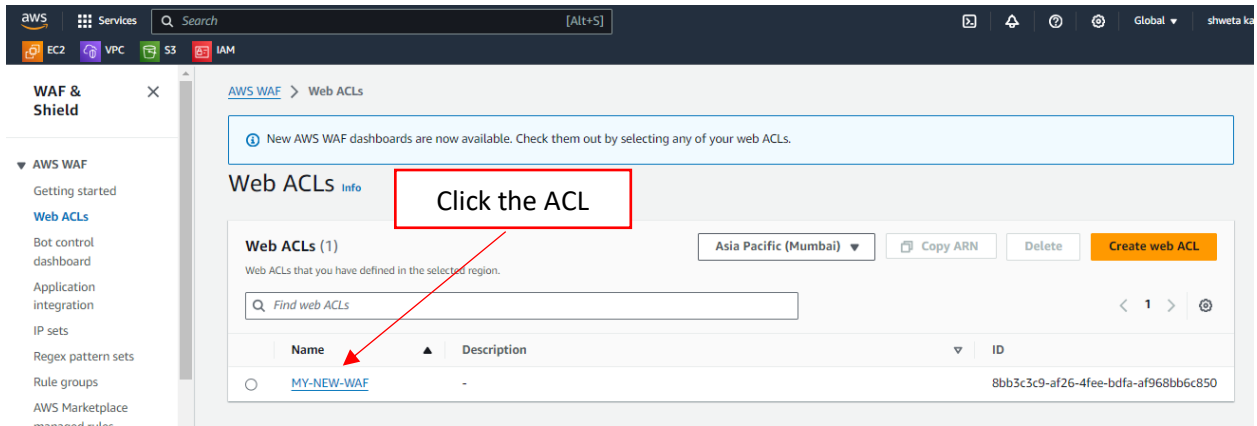
The screenshot shows the AWS Management Console interface. On the left, the navigation menu is visible with categories like Network & Security, Load Balancing, and Auto Scaling. The 'Load Balancers' page is selected, showing a table with one load balancer: 'WAF-LB-1865160953.ap-south-1.elb.amazonaws.com'. A tooltip indicates 'DNS name copied'. Below the table, it says '0 load balancers selected'. At the bottom, a browser window shows the URL 'waf-lb-1865160953.ap-south-1.elb.amazonaws.com' with a '403 Forbidden' error message.

Name	State	VPC ID	Availability Zones	Type
WAF-LB	Active	vpc-0c3cd85059c1b3f31	2 Availability Zones	application

403 Forbidden

It is giving a "403 forbidden" error because the access is blocked.

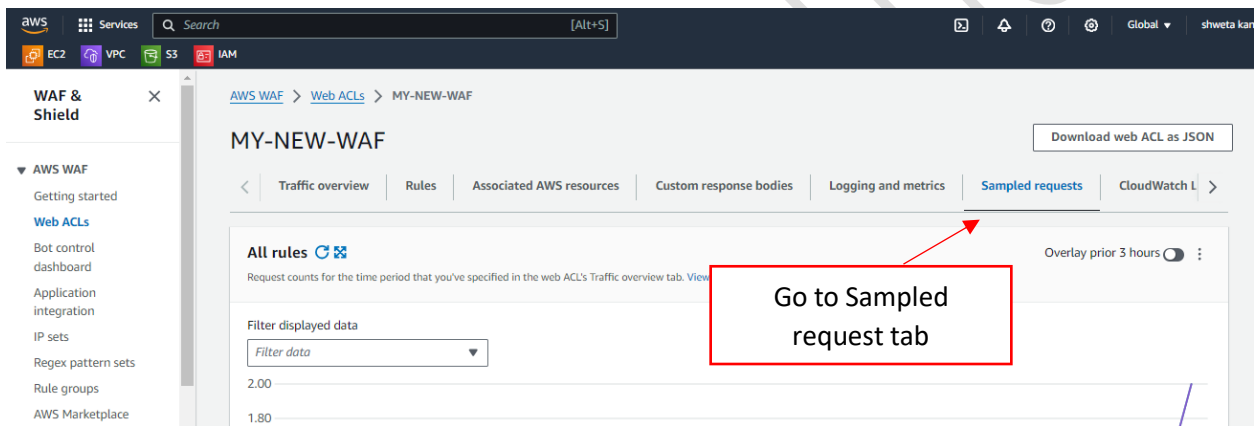
We can also see from where the requests are coming from.



Click the ACL

Web ACLs (1)

Name	Description	ID
MY-NEW-WAF	-	8bb3c3c9-af26-4fee-bdfa-af968bb6c850



Go to Sampled request tab

MY-NEW-WAF

Traffic overview | Rules | Associated AWS resources | Custom response bodies | Logging and metrics | **Sampled requests** | CloudWatch L

All rules

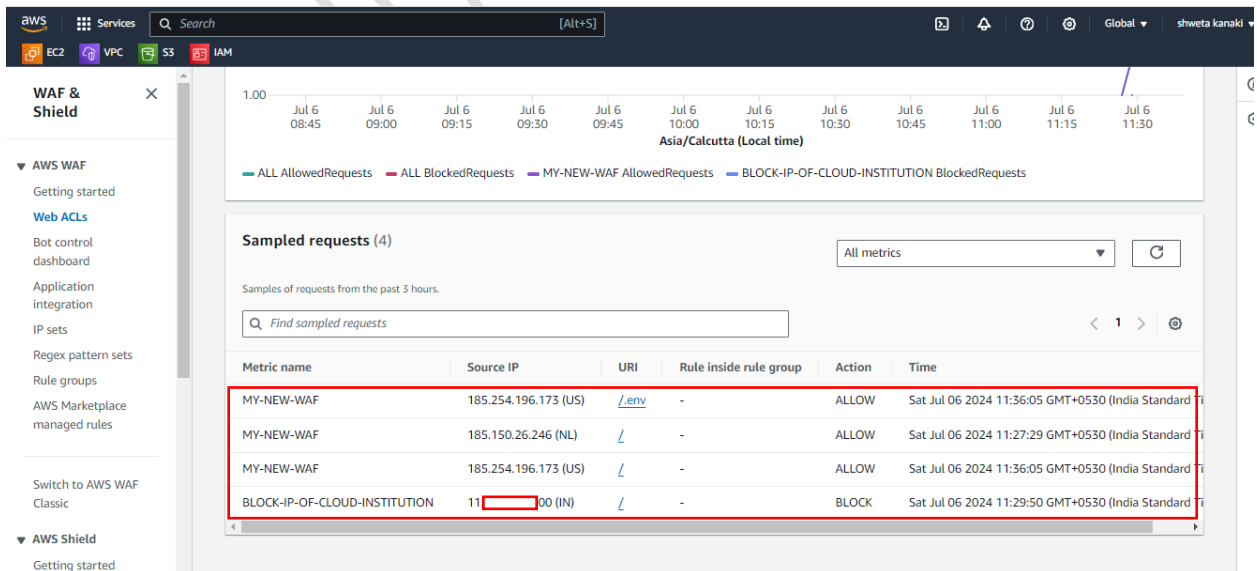
Request counts for the time period that you've specified in the web ACL's Traffic overview tab. View

Filter displayed data

Filter data

2.00

1.80



Go to Sampled request tab

Sampled requests (4)

Samples of requests from the past 3 hours.

Find sampled requests

Metric name	Source IP	URI	Rule inside rule group	Action	Time
MY-NEW-WAF	185.254.196.173 (US)	/env	-	ALLOW	Sat Jul 06 2024 11:36:05 GMT+0530 (India Standard Time)
MY-NEW-WAF	185.150.26.246 (NL)	/	-	ALLOW	Sat Jul 06 2024 11:27:29 GMT+0530 (India Standard Time)
MY-NEW-WAF	185.254.196.173 (US)	/	-	ALLOW	Sat Jul 06 2024 11:36:05 GMT+0530 (India Standard Time)
BLOCK-IP-OF-CLOUD-INSTITUTION	11.11.11.11 (IN)	/	-	BLOCK	Sat Jul 06 2024 11:29:50 GMT+0530 (India Standard Time)