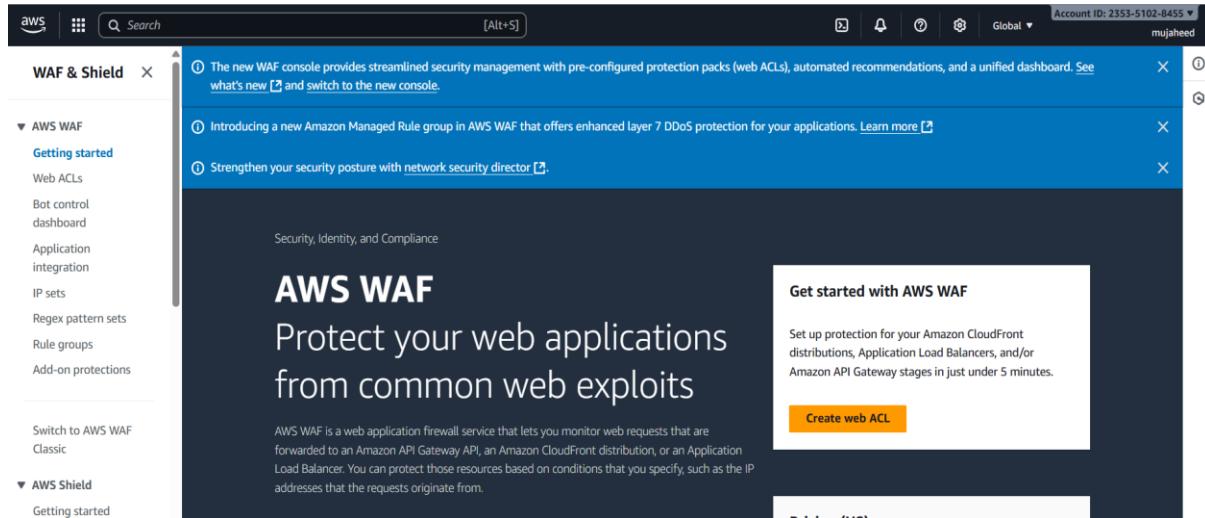
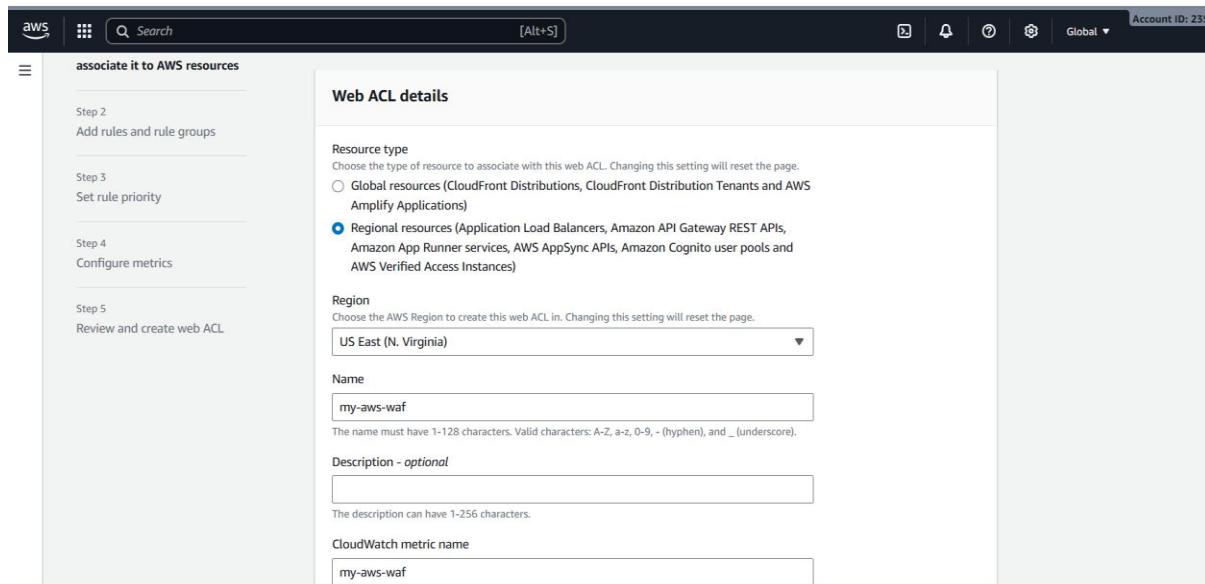


AWS WAF:

go to aws console and click on search bar as AWS WAF



Click on create web ACL and give name for that waf and click on next.



Click on add rules and select add my own rules and rule groups.

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

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.

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

Rules (0)

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

Edit Delete Add rules ▲ Add managed rule groups Add my own rules and rule groups

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](#)

In waf console click on create ip set. Give name and select ipv4 and give 1 ip address.

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
my-ip-set

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.

US East (N. Virginia)

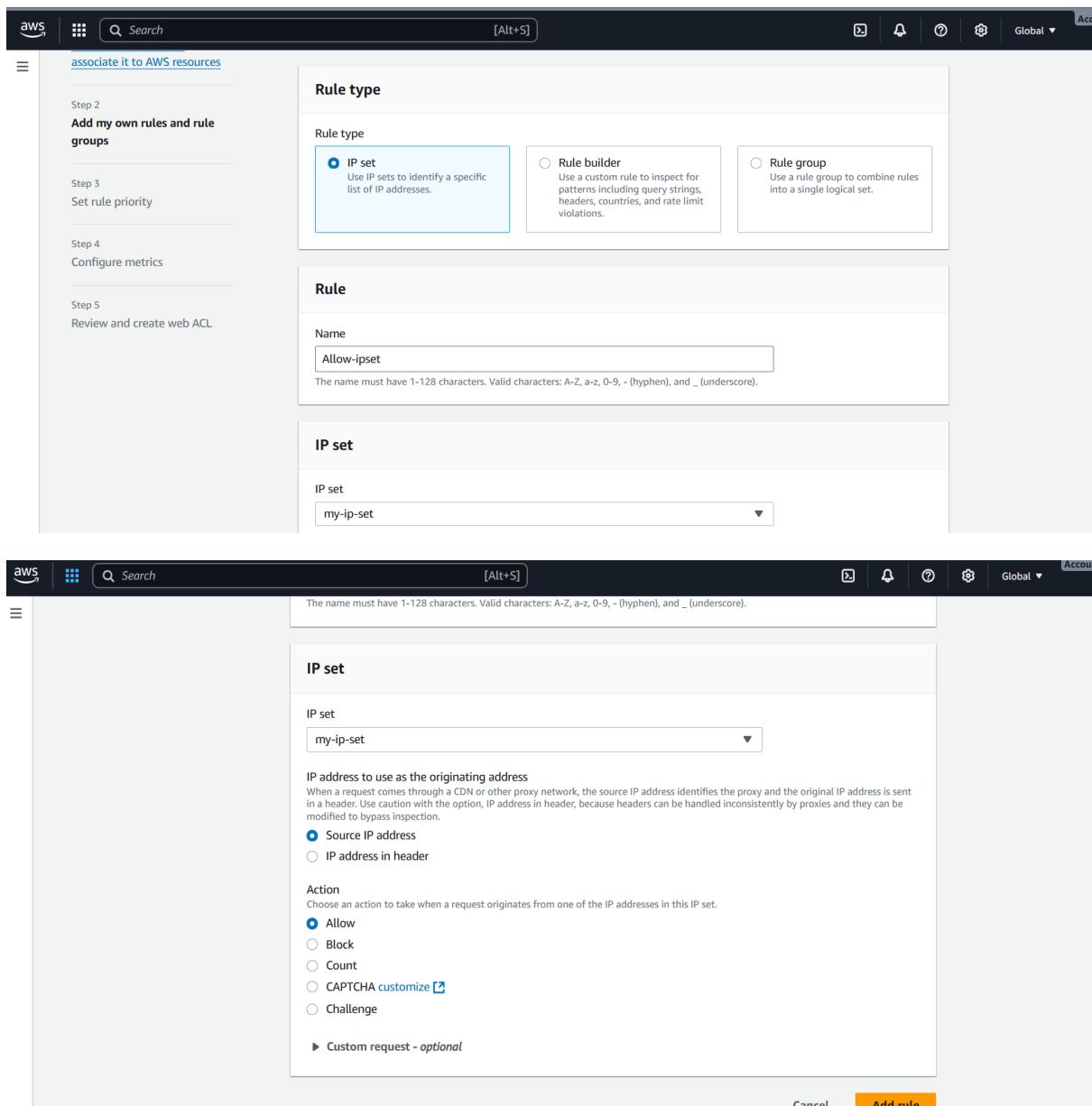
IP version

IPv4

IPv6

IP addresses
10.0.0.0/18

In creation of waf select ip set and give the name and select your created ipset and enable the action to allow or deny and click on add rule.



The image contains two screenshots of the AWS CloudFront console for creating an IP set.

Screenshot 1: Rule type selection

This screenshot shows the "Rule type" section of the configuration wizard. It includes:

- A sidebar with steps: Step 2 (Add my own rules and rule groups), Step 3 (Set rule priority), Step 4 (Configure metrics), and Step 5 (Review and create web ACL).
- A main panel titled "Rule type" with three options:
 - IP set** (selected): "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."

Screenshot 2: IP set configuration

This screenshot shows the "IP set" configuration screen. It includes:

- A header bar with the AWS logo, search bar, and account information.
- A message: "The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore)."
- A main panel titled "IP set" with an "IP set" input field containing "my-ip-set".
- Section "IP address to use as the originating address":
 - Description: "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."
 - Options:
 - Source IP address
 - IP address in header
- Section "Action":
 - Description: "Choose an action to take when a request originates from one of the IP addresses in this IP set."
 - Options:
 - Allow
 - Block
 - Count
 - CAPTCHA [customize](#)
 - Challenge
- Link: "▶ Custom request - optional"
- Buttons at the bottom: "Cancel" and "Add rule" (highlighted in orange).

Select your ip-set and choose the action and click on create.

Screenshot of the AWS WAF Web ACL creation wizard Step 4: Configure metrics.

Rules (1/1)

Name	Capacity	Action
Allow-ipset	1	Allow

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](#)

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

Default action: Allow

CloudShell Feedback

Screenshot of the AWS WAF Web ACL creation wizard Step 4: Configure metrics.

Configure metrics

Amazon CloudWatch metrics

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

Rules	CloudWatch metric name
Allow-ipset	Allow-ipset

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

Cancel Previous Next

The screenshot shows the AWS WAF & Shield console. On the left, a navigation sidebar for 'WAF & Shield' is visible, with 'AWS WAF' expanded to show 'Web ACLs' (which is selected), 'Bot control', 'dashboard', 'Application integration', 'IP sets', 'Regex pattern sets', 'Rule groups', and 'Add-on protections'. Below these are links to 'Switch to AWS WAF Classic' and 'AWS Shield' (with 'Getting started' under it). The main content area is titled 'Web ACLs' with an 'Info' link. It displays a table titled 'Web ACLs (1)' with one entry: 'my-aws-waf'. The table has columns for 'Name', 'Description', and 'ARN'. The ARN value is partially visible as 'arn:aws:wafv2:us-east-1:235351028455:regional/weba...'. A search bar at the top says 'Find web ACLs'. The top right of the main area shows 'US East (N. Virginia)' and 'Delete' buttons.

Name	Description	ARN
my-aws-waf	-	arn:aws:wafv2:us-east-1:235351028455:regional/weba...