AWS WAF

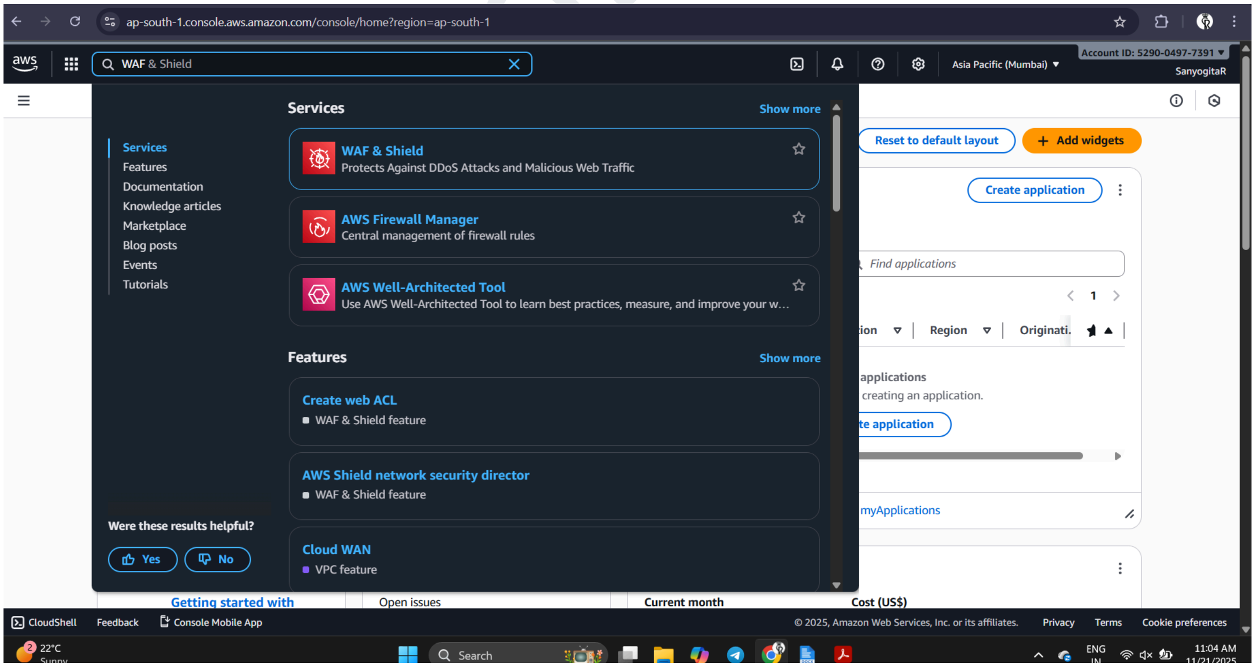
AWS WAF acts like a security shield in front of your websites and APIs.

1. Open AWS Console → Search “WAF”

You opened the AWS Management Console and typed **“WAF”** in the search bar.
This opened the **AWS WAF Dashboard**, which shows:

- Web ACLs
- Rule groups
- Sample protections
- Protection overview

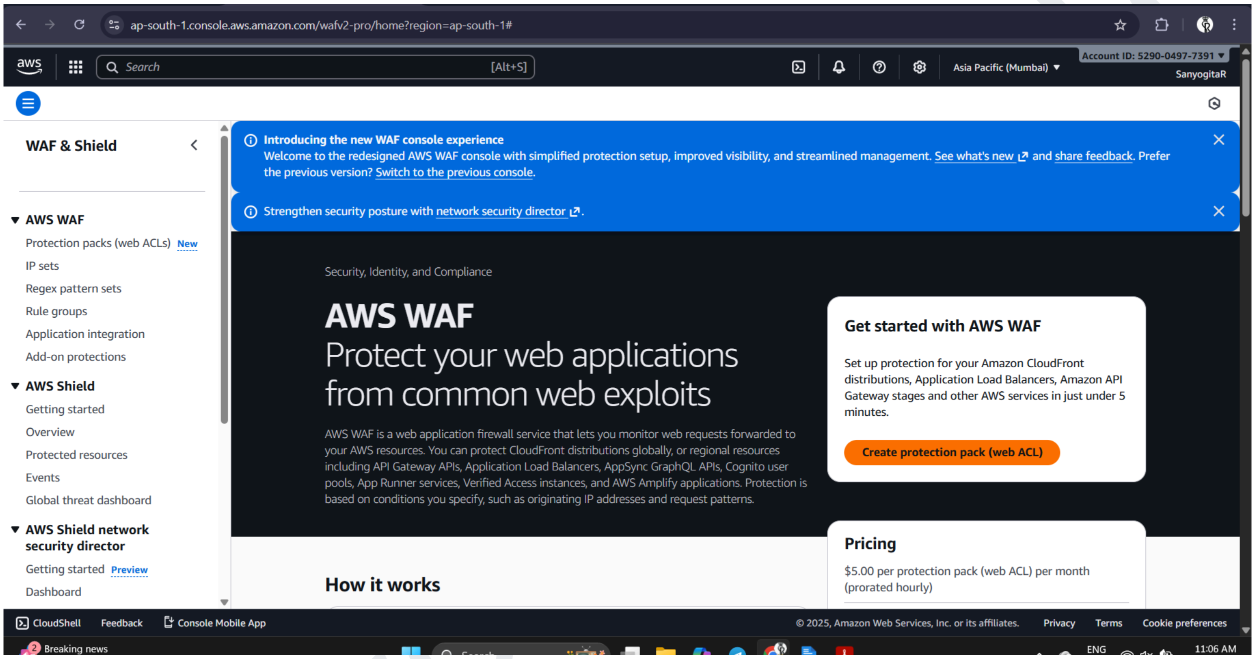
This is the central place where you configure your firewall.



2. Start Creating a Protection Pack (the new guided setup)

AWS has a feature called **Protection Pack**, which is a guided workflow that helps beginners quickly deploy security protections.

You clicked **Create Protection Pack**.



ap-south-1.console.aws.amazon.com/wafv2-pro/home?region=ap-south-1#

Account ID: 5290-0497-7391

Asia Pacific (Mumbai)

SanyogitaR

Introducing the new WAF console experience
Welcome to the redesigned AWS WAF console with simplified protection setup, improved visibility, and streamlined management. See what's new and share feedback. Prefer the previous version? Switch to the previous console.

Strengthen security posture with network security director.

Security, Identity, and Compliance

AWS WAF
Protect your web applications from common web exploits

AWS WAF is a web application firewall service that lets you monitor web requests forwarded to your AWS resources. You can protect CloudFront distributions globally, or regional resources including API Gateway APIs, Application Load Balancers, AppSync GraphQL APIs, Cognito user pools, App Runner services, Verified Access instances, and AWS Amplify applications. Protection is based on conditions you specify, such as originating IP addresses and request patterns.

Get started with AWS WAF
Set up protection for your Amazon CloudFront distributions, Application Load Balancers, Amazon API Gateway stages and other AWS services in just under 5 minutes.

Create protection pack (web ACL)

Pricing
$5.00 per protection pack (web ACL) per month (prorated hourly)

How it works

3. Choose Protection Type

On this page, AWS asks:
What kind of resource do you want to protect?

Options usually include:

- CloudFront Distribution
- Application Load Balancer
- API Gateway

- AppSync API
- Regional resources

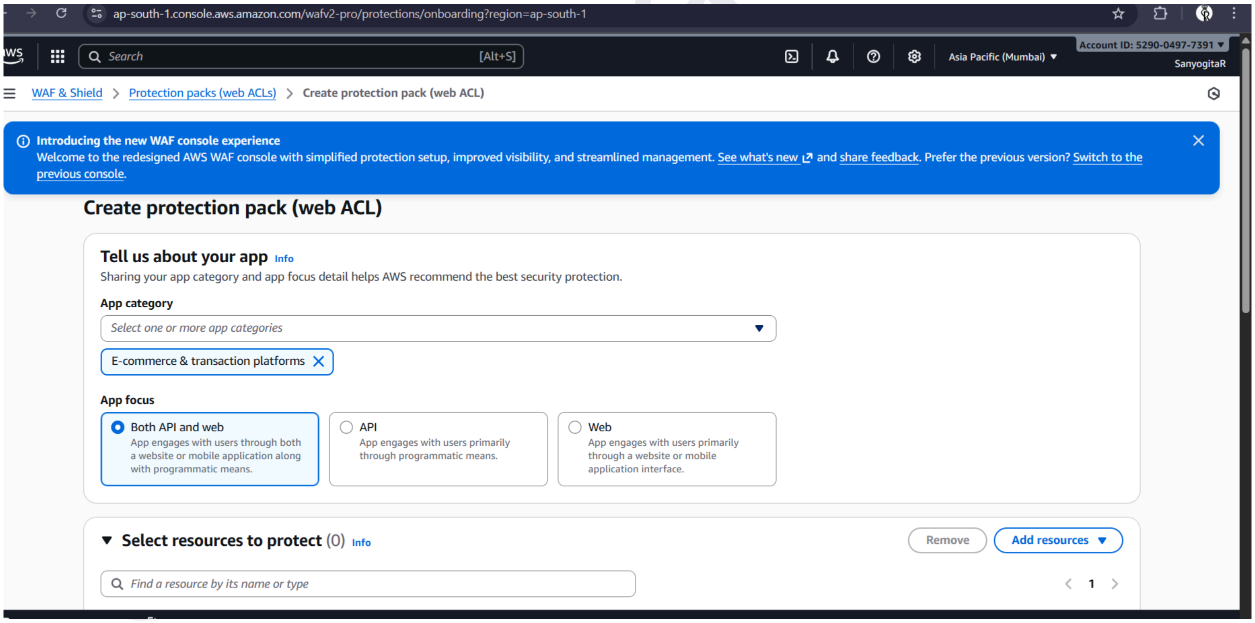
Since you created a **CloudFront distribution**, you selected:

👉 **CloudFront Distribution**
This means the Web ACL will be global (since CloudFront is a global service).

When to choose CloudFront?

- When you want global security
- When the site is static or served through CDN
- When performance matters

This was the correct choice for your experiment.



ap-south-1.console.aws.amazon.com/wafv2-pro/protections/onboarding?region=ap-south-1

Account ID: 5290-0497-7391
SanyogitaR

WAF & Shield > Protection packs (web ACLs) > Create protection pack (web ACL)

Introducing the new WAF console experience
Welcome to the redesigned AWS WAF console with simplified protection setup, improved visibility, and streamlined management. See what's new and share feedback. Prefer the previous version? Switch to the previous console.

Create protection pack (web ACL)

Tell us about your app Info
Sharing your app category and app focus detail helps AWS recommend the best security protection.

App category
Select one or more app categories
E-commerce & transaction platforms

App focus
● Both API and web — App engages with users through both a website or mobile application along with programmatic means.
○ API — App engages with users primarily through programmatic means.
○ Web — App engages with users primarily through a website or mobile application interface.

Select resources to protect (0) Info

4. Add Resource to Protect (Attach WAF to CloudFront)

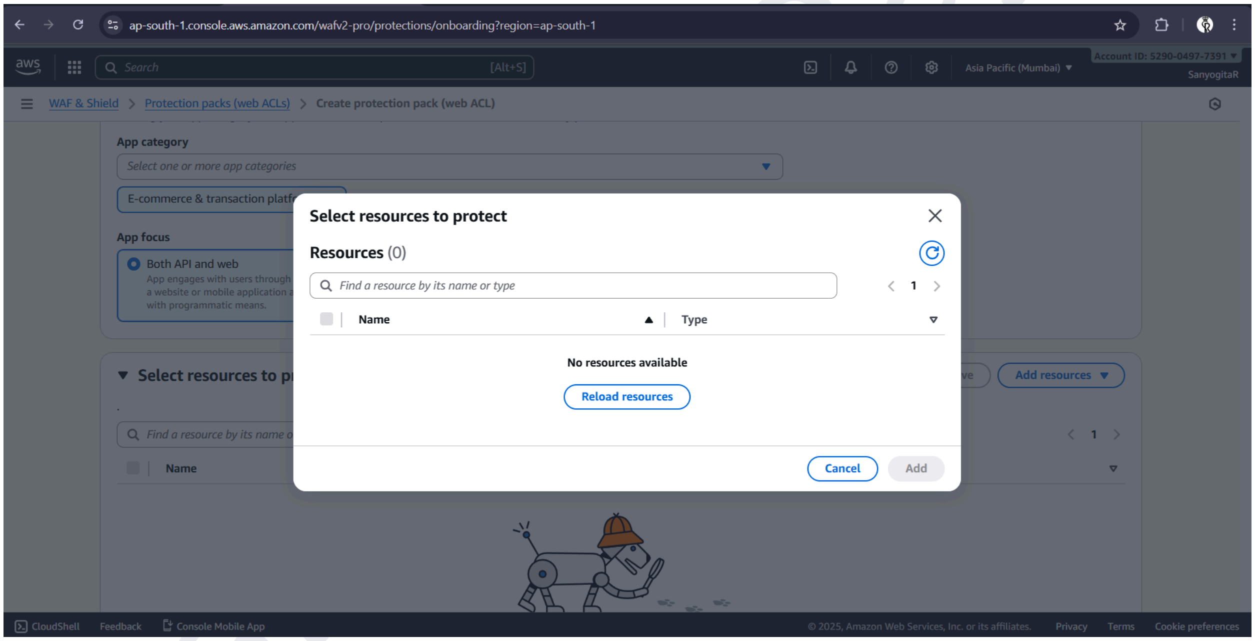
Here AWS asks you to choose **which CloudFront distribution** you want to attach the WAF to.

You selected your newly created CloudFront distribution.

This step tells AWS:
👉 “Apply all firewall rules to this distribution.”

When to add resources?

- Immediately if you already created CloudFront
- Later if you're planning rules first
- Multiple resources can be added to one Web ACL (except CloudFront Web ACLs, which are global)



ap-south-1.console.aws.amazon.com/wafv2-pro/protections/onboarding?region=ap-south-1

WAF & Shield > Protection packs (web ACLs) > Create protection pack (web ACL)

App category

Select one or more app categories

E-commerce & transaction platf

App focus

○ Both API and web
App engages with users through a website or mobile application with programmatic means.

Select resources to protect

Resources (0)

Find a resource by its name or type

☐	Name	Type

No resources available

Reload resources

Cancel Add

5. Configure Protection Options

This is where AWS shows multiple protection categories.

Common options include:

✔ AWS Managed Rule Groups

These are pre-built security rules designed by AWS.
Examples:

- Common Rule Set (CRS)
- SQL Injection Rule Group
- Amazon IP Reputation List
- Bad Bot Protection

When to choose?

- Always choose AWS Managed Rules for experiments
- Good for broad protection
- No need to write your own rules

✔ Custom Rules (Optional)

You can write your own conditions like:

- Block a specific IP
- Limit requests per minute
- Block certain strings or URLs

You could skip this if you only want managed protections.

6. Select Managed Rules (The Important Step)

AWS usually recommends enabling:

- Core Rule Set
- Bot Control (if available)

- SQL Injection
- Cross Site Scripting
- Known Bad Inputs

Enabling these gives strong basic protection.

When to enable what?

Rule Type	When to Choose
CRS (Common Rule Set)	Always – protects from most web attacks
SQLi & XSS rules	If you host APIs or dynamic websites
Bot Control	If you want to block scrapers or fake traffic
IP Reputation List	To block known malicious sources

For your experiment, enabling **CRS + SQLi/XSS** is perfect.

⭐ 7. Configure Rule Priorities

Rules are applied in order, so AWS lets you rearrange priority.

You typically keep:

1. IP whitelist rules first
2. Managed CRS
3. Bot rules
4. Rate limits
5. Last: Default Action (Allow or Block)

Since you're experimenting, the default order is fine.

⭐ 8. Set Default Web ACL Action

This decides what happens to a request if no rule matches.

Options:

- **Allow** (recommended)
- **Block**
- **Count**

When to choose what?

- Choose **Allow** if you want normal traffic to pass unless blocked by a rule.
- Choose **Block** only when testing or running a private API.
- Choose **Count** when experimenting without affecting traffic.

You likely used **Allow**.

⭐ 9. Review Everything

The review page shows:

- selected CloudFront resource
- managed rules
- custom rules (if added)
- priority
- default action

You checked the details and clicked **Create**.

⭐ 10. WAF Protection Activated

AWS WAF attaches itself to your CloudFront distribution.
Now every request going to CloudFront goes through your firewall rules.

You can see logs, blocked requests, and rule performance in the WAF dashboard.

📌 Important Note: Deleting WAF to Avoid Charges

WAF has charges based on:

- Number of rules
- Number of requests inspected

To avoid charges:

✔ Step 1: Remove the WAF Web ACL from CloudFront

Detach resource → so no requests hit it.

✔ Step 2: Delete the Web ACL

Open your Web ACL → click **Delete**.

✔ Step 3: Delete Rule Groups (if any)

Managed rules don’t cost extra, but custom rule groups might.

This ensures **zero cost**.