

Week 6: Web Application Firewall (WAF) Setup

Name- Saish Dhiwar

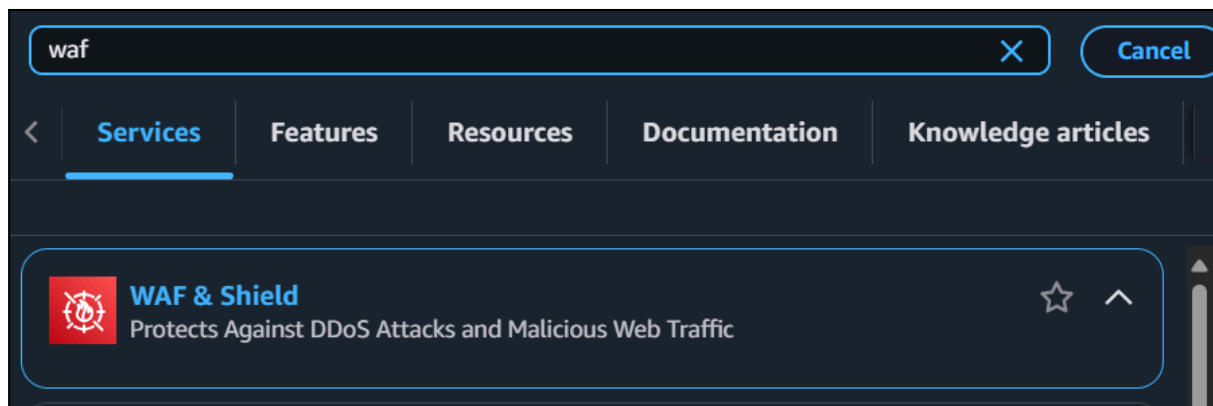
PRN- 2124UCSM2011

Email- saish.dhiwar_24ucs@sanjivani.edu.in

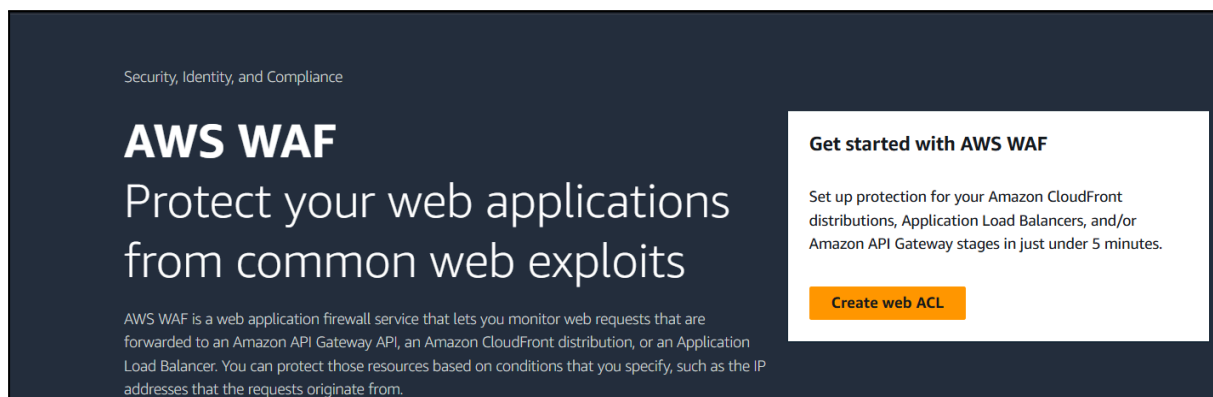
- Task-**
- 1) Configure Cloudflare or AWS WAF.
 - 2) Protect against OWASP Top 10 attacks.
 - 3) Upload configuration screenshots.

Task 1- Configure AWS WAF.

- 1) Log in to AWS Console. Go to <https://aws.amazon.com>, sign in to the AWS Management Console.
- 2) In the Search bar, type **WAF** and open the **AWS WAF & Shield** service.



- 3) Click on **Create Web ACL**.



- 4) Enter the **Web ACL Name** (e.g., **web-app-firewall**) and choose the **Scope**: **CloudFront** (Global) OR **Regional** (for ALB/API Gateway).

Web ACL details

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

☐ Global resources (CloudFront Distributions, CloudFront Distribution Tenants and AWS Amplify Applications)

☒ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync 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

web-app-firewall

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-app-firewall

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

5) Add **Managed Rule Groups** for OWASP Top 10 protection:

- **AWSManagedRulesCommonRuleSet** (SQL Injection, XSS, etc.)
- **AWSManagedRulesSQLiRuleSet**
- **AWSManagedRulesAnonymousIpList** (Blocks VPN/Tor IPs)

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 (3) 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"/>	AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions

6) Associate the Web ACL with the **CloudFront Distribution** or **ALB** hosting your application.

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](#)

950/5000 WCUs

7) Save and deploy the Web ACL.

Success

You successfully created the web ACL web-app-firewall.

[AWS WAF](#) > Web ACLs

Web ACLs

Web ACLs (1)

Web ACLs that you have defined in the selected region.

Find web ACLs

Asia Pacific (Mumbai)

Delete

Create web ACL

< 1 >

Name	Description	ARN	ID
web-app-firewall	-	arn:aws:wafv2:ap-south-1:240110921708:regional/webacl/web-app-fire...	7176c13a-6630-47b7-82a3-9ed194b96dcc

Task 2 – Protect Against OWASP Top 10 Attacks

1. Enabled AWS Managed Rules covering:

Rules (3/3)

Find rules

Edit

Delete

Add rules

< 1 >

<input checked="" type="checkbox"/>	Name	Action	Priority	Custom response
<input checked="" type="checkbox"/>	AWS-AWSManagedRulesSQLiRuleSet	Use rule actions	0	-
<input checked="" type="checkbox"/>	AWS-AWSManagedRulesAnonymousIpList	Use rule actions	1	-
<input checked="" type="checkbox"/>	AWS-AWSManagedRulesCommonRuleSet	Use rule actions	2	-