

AWS Web Application Firewall

AWS Web Application Firewall (WAF) is a security tool that helps you to protect the application against web attacks. WAF monitors and controls unusual bot traffic, blocks common attack patterns, such as SQL Injection or Cross-site scripting, etc. It also lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer.

- Amazon WAF allows you to control your content by using an IP address from where the request originates.
- Three things make Amazon WAF work – Access control lists (ACL), Rules and Rule Group.
- Amazon WAF manages Web ACL capacity units (WCU) for rules, rule groups and web ACLs.
- Amazon WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of security rules.

Step by step Hands-on WAF:

Step 1 : Create Load balancer and attach it to the Working Ec2 instances.

- Launch the Ec2 instances which contains httpd running application with static webpage.
- Create load balancer and target group attach above two instances to that Target group.
- When the health checks are health then take DNS name and run in browser it will work.

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services' link, a search bar, and user information. Below this is a yellow banner about a new launch experience. The main content area shows the 'Step 1: Choose an Amazon Machine Image (AMI)' wizard. On the left, there's a sidebar with 'Quick Start' and 'My AMIs'. The main list shows two Amazon Linux 2 AMIs. The first one is 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type' with AMI ID 'ami-026b57f3c383c2eec'. The second one is 'Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type' with AMI ID 'ami-0464d49b8794eba32'. Both are marked as 'Free tier eligible'. Below this, there's a table showing two EC2 instances. The first instance is 'WAF_server1' with Instance ID 'i-00f08ff16e2b9c9bc', Instance state 'Running', Instance type 't2.micro', Status check '2/2 checks passed', Alarm status 'No alarms', and Availability Zone 'us-east-1c'. The second instance is 'WAF server2' with Instance ID 'i-041ce121a41952ceb', Instance state 'Running', Instance type 't2.micro', Status check '2/2 checks passed', Alarm status 'No alarms', and Availability Zone 'us-east-1c'. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. There are also buttons for 'Connect', 'Instance state', 'Actions', and 'Launch instances'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
WAF_server1	i-00f08ff16e2b9c9bc	Running	t2.micro	2/2 checks passed	No alarms	us-east-1c
WAF server2	i-041ce121a41952ceb	Running	t2.micro	2/2 checks passed	No alarms	us-east-1c

← → ↻ ⚠ Not secure | 54.144.246.202

welcome to waf server1 ip-172-31-24-213.ec2.internal

← → ↻ ⚠ Not secure | 3.83.236.9

welcome to server ip-172-31-18-6.ec2.internal

aws Services waf

EC2 > Target groups

Target groups (1/1) Info

Search or filter target groups

<input checked="" type="checkbox"/>	Name	ARN	Port	Protocol	Target type
<input checked="" type="checkbox"/>	WAFTG	arn:aws:elasticloadbalancing...	80	HTTP	Instance

Target group: WAFTG

Details Targets Monitoring Health checks Attributes Tags

Registered targets (2)

Filter resources by property or value

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details
<input type="checkbox"/>	i-00f08ff16e2b9cbc	WAF_server1	80	us-east-1c	healthy	
<input type="checkbox"/>	i-041ce121a41952ceb	WAF server2	80	us-east-1c	healthy	

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022 Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

aws Services waf

Create Load Balancer Actions

Filter by tags and attributes or search by keyword

<input checked="" type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type
<input checked="" type="checkbox"/>	WAFLB	WAFLB-829277897.us-east-...	Active	vpc-0a080ec13036dead2	us-east-1c, us-east-1a, ...	application

Name WAFLB

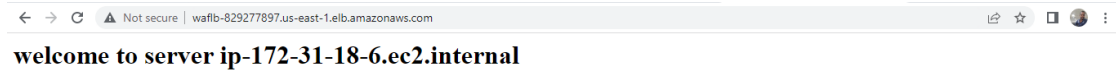
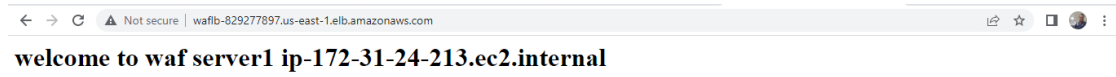
ARN arn:aws:elasticloadbalancing:us-east-1:881832161071:loadbalancer/app/WAFLB/422f450d89631ab

DNS name WAFLB-829277897.us-east-1.elb.amazonaws.com (A Record) Copied

State Active

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022 Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences



Step 2: Now create Web application firewall.

- Goto the AWS WAF dashboard, click create web ACL.
- WEB ACL details – >name - WAFACL, Region select the where the load balancer and TG are available. And make evarything default and create it.
- After creating web ACL in overview there will data available regarding hits of loadbalancer url.

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

WAF & Shield

AWS WAF

Getting started

Web ACLs

Bot Control

Application integration SDKs

IP sets

Regex pattern sets

Rule groups

AWS Marketplace

Switch to AWS WAF Classic

AWS Shield

AWS Firewall Manager

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 that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.

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

Pricing (US)

\$5.00 per web ACL per month (prorated hourly)

\$1.00 per rule per month (prorated hourly)

\$0.60 per million requests processed

What's new

Feature

New AWS WAF

AWS WAF Classic

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

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

Name

WAFACL

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

Description - optional

WAFACL

The description can have 1-256 characters.

CloudWatch metric name

WAFACL

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

Resource type

Choose the type of resource to associate with this web ACL.

☐ CloudFront distributions

☒ Regional resources (Application Load Balancer, API Gateway, AWS AppSync, Amazon Cognito User Pools)

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

ACL

Resource type

Choose the type of resource to associate with this web ACL.

☐ CloudFront distributions

☒ Regional resources (Application Load Balancer, API Gateway, AWS AppSync, Amazon Cognito User Pools)

Region

Choose the AWS region to create this web ACL in.

US East (N. Virginia)

Associated AWS resources - optional

Remove

Add AWS resources

Find associated AWS resources

< 1 >

Name	Resource type	Region
No results		
There are no results to display		

Cancel

Next

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

ACL

Resource type

Add AWS resources

Resource type

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

☐ Amazon API Gateway

☒ Application Load Balancer

☐ AWS AppSync

☐ Amazon Cognito User Pools

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

< 1 >

☒ Name

☒ WAFLB

Cancel

Add

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

Step 5
Review and create web ACL

CloudWatch metric name

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

Resource type

Choose the type of resource to associate with this web ACL.

☐ CloudFront distributions

☒ Regional resources (Application Load Balancer, API Gateway, AWS AppSync, Amazon Cognito User Pools)

Region

Choose the AWS region to create this web ACL in.

Associated AWS resources - optional

Remove

Add AWS resources

< 1 >

☐ Name

Resource type

Region

☐ WAFLB

Application Load Balancer

US East (N. Virginia)

Cancel

Next

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

Step 5
Review and create web ACL

Set rule priority

Name

Capacity

Action

No rules.
You don't have any rules added.

Web ACL rule capacity units used

The total capacity units used by the web ACL can't exceed 1500.

0/1500 WCU

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

Default action

☒ Allow

☐ Block

Custom request - optional

Cancel

Previous

Next

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

Action

Allow

Custom request headers

-

Step 4: Configure metrics

Edit

Amazon CloudWatch metrics

Rules

CloudWatch metric name

No results

There are no results to display

Sampled requests

Sampled requests

Disabled

Sampled requests for web ACL default actions

Enabled

Cancel

Previous

Create web ACL

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

WAF & Shield

Success

You successfully created the web ACL: WAFACL.

AWS WAF

Getting started

Web ACLs

Bot Control

Application integration SDKs

IP sets

Regex pattern sets

Rule groups

AWS Marketplace

AWS WAF

Web ACLs

Web ACLs

Info

US East (N. Virginia)

Copy ARN

Delete

Create web ACL

Find web ACLs

1

	Name	Description	ID
	WAFACL	WAFACL	85b3d160-7823-47ef-bd1d-2ccd23214fc2

The screenshot displays the AWS WAF console interface. The left sidebar shows the navigation menu with options like 'AWS WAF', 'Web ACLs', 'Bot Control', 'Application integration SDKs', 'IP sets', 'Regex pattern sets', 'Rule groups', and 'AWS Marketplace'. The main content area is titled 'WAFACL' and includes a 'Download web ACL as JSON' button. Below this, there's a section for 'Requests per 5 minute period' with a chart and a table of sampled requests.

Metric name	Source IP	URI	Rule inside rule group	Action	Time
WAFACL	106.51.122.2 (IN)	/	-	ALLOW	Tue Oct 04 2022 14:23:56 GMT+0530 (India Standard Time)
WAFACL	106.51.122.2 (IN)	/	-	ALLOW	Tue Oct 04 2022 14:24:12 GMT+0530 (India Standard Time)
WAFACL	52.114.14.71 (SG)	/	-	ALLOW	Tue Oct 04 2022 14:23:24 GMT+0530 (India Standard Time)
WAFACL	106.51.122.2 (IN)	/favicon.ico	-	ALLOW	Tue Oct 04 2022 14:23:45 GMT+0530 (India Standard Time)
WAFACL	52.114.14.71 (SG)	/favicon.ico	-	ALLOW	Tue Oct 04 2022 14:23:25 GMT+0530 (India Standard Time)
WAFACL	106.51.122.2 (IN)	/	-	ALLOW	Tue Oct 04 2022 14:22:04 GMT+0530 (India Standard Time)
WAFACL	106.51.122.2 (IN)	/	-	ALLOW	Tue Oct 04 2022 14:24:06 GMT+0530 (India Standard Time)
WAFACL	106.51.122.2 (IN)	/	-	ALLOW	Tue Oct 04 2022 14:22:01 GMT+0530 (India Standard Time)

Step 3 : Amazon WAF allows you to control your content by using an IP address from where the request originates. By using the IP sets.

- Goto the AWS WAF dashboard click create IP set.
- IP setname and region select it , IP adress im giving my present IP adress with 32 mask bit.
- And create it.
- Now goto the web acl rules, add a rule.
- Rule type – IP sets , IP set – give the IP set which are previously created.
- In actions select Block option and add rule and save it.
- Now take the load balancers DNS name and hit it in this related IP adress then the website will not work.

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

WAF & Shield

AWS WAF

Getting started

Web ACLs

Bot Control

Application integration SDKs

IP sets

Regex pattern sets

Rule groups

AWS Marketplace

Switch to AWS WAF Classic

AWS Shield

AWS Firewall Manager

AWS WAF

IP sets

US East (N. Virginia)

Copy ARN

Delete

Create IP set

Find IP sets

<

>

⚙

Name	Description	ID
No IP sets found		
You don't have any IP sets in the US East (N. Virginia) 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.		
Create IP set		

Google

my ip address

Tools

About 1,19,00,00,00,000 results (0.46 seconds)

What's my IP

106.51.122.2

Your public IP address

Learn more about IP addresses

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

Create IP set

Info

An IP set is a collection of IP addresses.

IP set details

IP set name

WAFIPSETS

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

Description - optional

WAFIPSETS

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

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

WAFIPSETS

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

106.51.122.2/32

Enter one IP address per line in CIDR format.

Cancel

Create IP set

Feedback

Looking for language editions? Find it in the new Unified Settings

© 2022 Amazon Internet Services Private Ltd. or its affiliates

Privacy

Terms

Cookie preferences

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

WAF & Shield

AWS WAF

Getting started

Web ACLs

Bot Control

Application integration SDKs

IP sets

Regex pattern sets

Rule groups

AWS WAF > IP sets

US East (N. Virginia)

Copy ARN

Delete

Create IP set

Find IP sets

< 1 >

Name	Description	ID
WAFIPSETS	WAFIPSETS	a1acfd2b-292e-4eda-a966-ebdc1cd9236f

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

WAF & Shield

AWS WAF

Getting started

Web ACLs

Bot Control

Application integration SDKs

IP sets

Regex pattern sets

Rule groups

AWS Marketplace

Switch to AWS WAF Classic

AWS Shield

AWS Firewall Manager

AWS WAF > Web ACLs > WAFACL

Download web ACL as JSON

Overview

Rules

Bot Control

Associated AWS resources

Custom response bodies

Logging and metrics

CloudWatch Log Insights

New AWS managed rule group available: Account takeover prevention

Protect your sign-in page against brute force and credential stuffing attacks. Account takeover prevention detects and mitigates against login attempts by malicious actors using stolen credentials.

Add to web ACL

Rules (0)

Edit

Delete

Add rules

Find rules

Add managed rule groups

Add my own rules and rule groups

	Name	Action	Priority	Custom response
No results				

There are no results to display

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Veeresh

AWS WAF > Web ACLs > WAFACL > Add rule

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

myofficeIP

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

IP set

IP set

WAFIPSETS

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.

☒ Block

☐ Allow

☐ Count

☐ CAPTCHA

Custom response - optional

Cancel

Add rule

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022 Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

The top screenshot shows the 'Set rule priority' dialog in the AWS WAF console. It displays a table with one rule: 'myofficelP' with a capacity of 1 and an action of 'Block'. The 'Save' button is highlighted.

The bottom screenshot shows the 'Rules' tab in the AWS WAF console. A notification banner at the top reads: 'New AWS managed rule group available: Account takeover prevention. Protect your sign-in page against brute force and credential stuffing attacks. Account takeover prevention detects and mitigates against login attempts by malicious actors using stolen credentials.' Below this, a table lists the rules. The 'myofficelP' rule is circled in red, showing its 'Block' action.

Name	Action	Priority	Custom response
myofficelP	Block	0	-

Web ACL rule capacity units used
The total capacity units used by the web ACL can't exceed 1500.

403 Forbidden

Step 4 : Again allow and check the rule of web acl is it working or not.

WAF & Shield

Success
You successfully updated the web ACL WAFACL.

CloudWatch Log Insights [New](#)

New AWS managed rule group available: Account takeover prevention
Protect your sign-in page against brute force and credential stuffing attacks. Account takeover prevention detects and mitigates against login attempts by malicious actors using stolen credentials. [Add to web ACL](#)

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

<input checked="" type="checkbox"/>	Name	Action	Priority	Custom response
<input checked="" type="checkbox"/>	myofficelP	Block	0	-

Web ACL rule capacity units used
The total capacity units used by the web ACL can't exceed 1500.
1/1500 WCUs

Then

Action

Action
Choose an action to take when a request matches the statements above.

☒ Allow
☐ Block
☐ Count
☐ CAPTCHA

Custom request - optional

Add label - optional
Add labels to requests that match this rule. Rules that are evaluated later in the same web ACL can reference the labels that this rule adds.

[Cancel](#) [Save rule](#)

Success
You successfully updated the web ACL WAFACL.

New AWS managed rule group available: Account takeover prevention
Protect your sign-in page against brute force and credential stuffing attacks. Account takeover prevention detects and mitigates against login attempts by malicious actors using stolen credentials. [Add to web ACL](#)

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

<input type="checkbox"/>	Name	Action	Priority	Custom response
<input type="checkbox"/>	myofficelP	Allow	0	-

Web ACL rule capacity units used
The total capacity units used by the web ACL can't exceed 1500.
1/1500 WCUs

Default web ACL action for requests that don't match any rules [Edit](#)

welcome to waf server1 ip-172-31-24-213.ec2.internal