



JJ Tech

AWS WAF – Web Application Firewall

(Note: Use this automation script for whole web and agent installation as a userdata:
<https://github.com/JJTechInc/ecommerce-web-app/blob/main/userdata1.sh>)

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting. You can also customise rules that filter out specific traffic patterns. You can get started quickly using Managed Rules for AWS WAF, a pre-configured set of rules managed by AWS or AWS Marketplace Sellers to address issues like the OWASP Top 10 security risks and automated bots that consume excess resources, skew metrics, or can cause downtime. These rules are regularly updated as new issues emerge. AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of security rules.

AWS WAF Overview

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.

Common Web Attacks



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Before protecting your applications, you need to know the most common web attacks mention below.



JJ Tech

DDoS(Denial-Of-Service) attacks: This is probably the most common attack. Attackers overload an application by sending bulk requests to the web servers. Thousands of hosts infected with malware are used in this attack, which utilizes more than one unique IP address or machine. This slows down the application and significantly hurt the value of a brand.

SQL injections: SQL injection is a code injection procedure that might destroy your SQL database. Attackers can run malicious SQL queries on your web applications.

Cross-Site Scripting: If your application is vulnerable to cross-site scripting, then the attacker can run or inject malicious scripts, generally in the form of a browser side script. These scripts can even rewrite the content of the HTML pages.

AWS WAF Features

Amazon Web Application Firewall offer lots of features to its users mentioned below.

- **Protection Against Web Attacks:** With minimum latency impact on incoming traffic, AWS WAF offers many rules to inspect any element of a web request. AWS WAF protects web applications against threats by filtering traffic according to the rules created.
- **Establish Rules Accordingly:** AWS WAF is a versatile and valuable tool for protecting the infrastructures of applications. And this is because it allows users to establish rules according to their needs and vulnerabilities that they wish to stop. We can consider it as a great solution to protect any web applications environment at the enterprise level.
- **Web traffic filtering:** WAF allows users to create rules to filter web traffic. It filters IP addresses, HTTP headers, HTTP body, or URI strings from a web request.
- **Flexible Integration With AWS Services:** AWS Web Application Firewall offers easy integration with other AWS services like Amazon EC2, CloudFront, Load balancer etc.
- **Monitor Rules:** AWS Web Application Firewall allows us to create rules and review and customize them to prevent unknown attracts.



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





JJ Tech

Benefits

Agile protection against web attacks

AWS WAF rule propagation and updates take under a minute, enabling you to quickly update security across your environment when issues arise. WAF supports hundreds of rules that can inspect any part of the web request with minimal latency impact to incoming traffic. AWS WAF protects web applications from attacks by filtering traffic based on rules that you create. For example, you can filter any part of the web request, such as IP addresses, HTTP headers, HTTP body, or URI strings. This allows you to block common attack patterns, such as SQL injection or cross-site scripting.

Save time with managed rules

With Managed Rules for AWS WAF, you can quickly get started and protect your web application or APIs against common threats. You can select from many rule types, such as ones that address issues like the Open Web Application Security Project (OWASP) Top 10 security risks, threats specific to Content Management Systems (CMS), or emerging Common Vulnerabilities and Exposures (CVE). Managed rules are automatically updated as new issues emerge, so that you can spend more time building applications.

Improved web traffic visibility

AWS WAF gives near real-time visibility into your web traffic, which you can use to create new rules or alerts in Amazon CloudWatch. You have granular control over how the metrics are emitted, allowing you to monitor from the rule level to the entire inbound traffic. In addition, AWS WAF offers comprehensive logging by capturing each inspected web request's full header data for use in security automation, analytics, or auditing purposes.

Ease of deployment & maintenance

AWS WAF is easy to deploy and protect applications deployed on either Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts all your origin servers, Amazon API Gateway for your REST APIs, or AWS AppSync for your GraphQL APIs. There is no additional software to deploy, DNS configuration,



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





JJ Tech

SSL/TLS certificate to manage, or need for a reverse proxy setup. With AWS Firewall Manager integration, you can centrally define and manage your rules, and reuse them across all the web applications that you need to protect.

Easily monitor, block, or rate-limit bots

With AWS WAF Bot Control, you get visibility and control over common and pervasive bot traffic to your applications. Within the AWS WAF console, you can monitor common bots, such as status monitors and search engines, and get detailed, real-time visibility into the category, identity, and other details of bot traffic. You can also block, or rate-limit, traffic from pervasive bots, such as scrapers, scanners, and crawlers. Using AWS Firewall Manager, you can deploy the Bot Control managed rule group across multiple accounts in your AWS Organization.

Security integrated with how you develop applications

Every feature in AWS WAF can be configured using either the AWS WAF API or the AWS Management Console. This allows your DevOps team to define application-specific rules that increase web security as they develop applications. This lets you put web security at multiple points in the development process chain, from the hands of the developer initially writing code, to the DevOps engineer deploying software, to the security administrators enforcing a set of rules across the organization.

How It Works

AWS Web Application Firewall protect the applications from malicious attacks. Working of WAF mentioned below.

- **AWS Firewall Manage:** It Manages multiple AWS Web Application Firewall Deployments
- **AWS WAF:** Protect deployed application from common web exploits.
- **Create a Policy:** Now you can build your own rules using the visual rule builder.
- **Block Filter:** Block filter protect against exploits and vulnerabilities attacks.



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

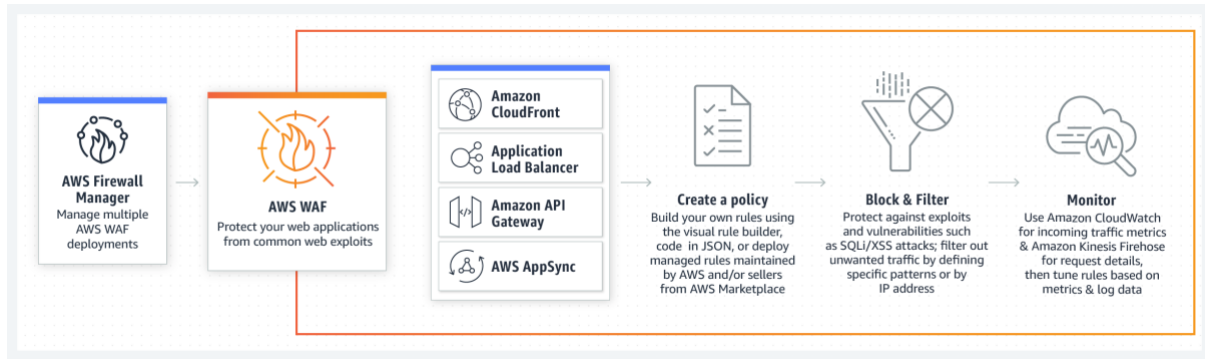
14103 Hammermil Field Dr Bowie MD 20720





JJ Tech

Monitor: Use Amazon CloudWatch for incoming traffic metrics & Amazon Kinesis Firehose for request details, then tune rules based on metrics and log data.



JJ Tech



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





Demo : Control Web Traffic using Web Application Firewall (WAF)

JJ Tech

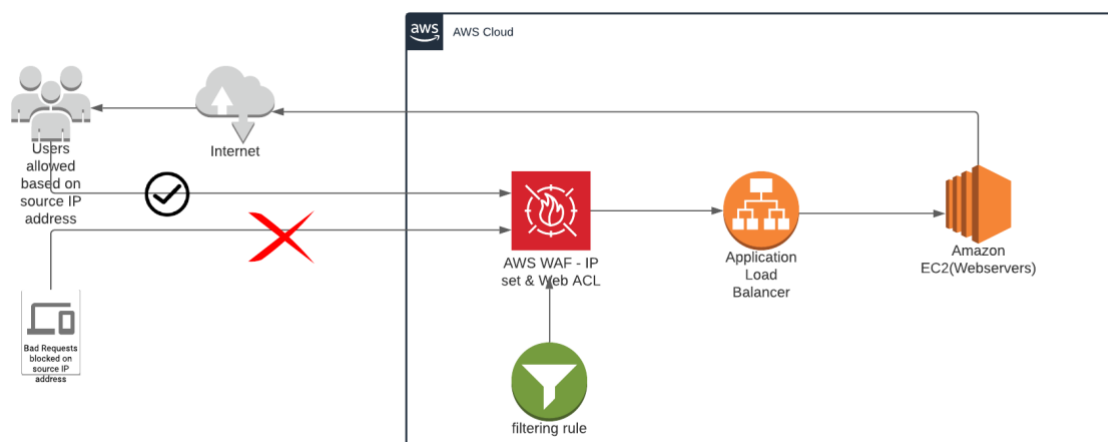
Step 1 : Launch 2 webserver in 2 different Az's

Step 2 : Create Application Load Balancer

Step 3 : Create IP set in WAF

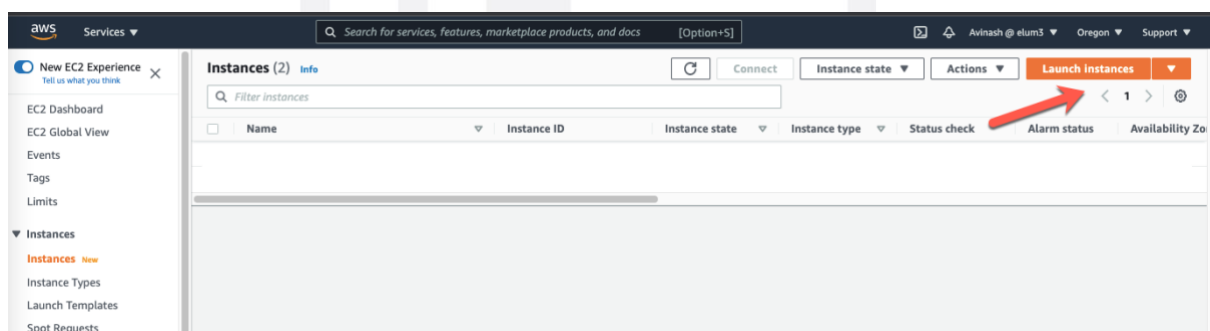
Step 4 : Create Web ACL in WAF

Step 5 : Test the working on WAF



Step 1 : Launch 2 webserver in 2 different Az's

- Navigate to AWS EC2 console



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



EC2 > Instances > Launch an Instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or Instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

[Add additional tags](#)

Summary

Number of instances Info

Software Image (AMI)

Amazon Linux 2023 AMI 2023.5.2...[read more](#)
ami-0a69ba12b3333ea951

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Instance type Info | Get advice

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand RHEL base pricing: 0.0272 USD per Hour

On-Demand Windows base pricing: 0.0174 USD per Hour

On-Demand SUSE base pricing: 0.0128 USD per Hour

On-Demand Linux base pricing: 0.0128 USD per Hour

☐ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

[Create new key pair](#)

Storage

Number of volumes

Software image

Amazon Linux 2023 AMI 2023.5.2...[read more](#)
ami-0a69ba12b3333ea951

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

☒ Create security group ☐ Select existing security group

We'll create a new security group called 'launch-wizard-9' with the following rules:

☒ Allow SSH traffic from
Helps you connect to your instance
0.0.0.0/0

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.



+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



JJ Tech

User data - optional | Info

Upload a file with your user data or enter it in the field.

Choose file

```
# Update the system
sudo yum update -y
# Install Apache HTTP Server (httpd)
sudo yum install httpd -y
# Install Git
sudo yum install git -y
# Clone the repository
git clone https://github.com/JJTechInc/ecommerce-web-app.git
# Copy the files inside the cloned folder to the desired location
sudo cp -r ecommerce-web-app/server1/* /var/www/html/
# To get the current hostname address
echo "<center><p>Running the website from instance host: $(hostname -f)</p>
</center>" >> /var/www/html/index.html
# Start and enable the HTTP server
sudo systemctl start httpd
sudo systemctl enable httpd
```

☐ User data has already been base64 encoded

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the

Cancel Launch instance Review commands

- Please create the second EC2 instance with same configuration and userdata in another AZ

<input type="checkbox"/>	JJTech-EC2-1	i-013f9ed1c9e35cc41	Running	t2.micro	Initializing	No alarms	+	us-west-2a
<input type="checkbox"/>	JJTech-EC2-2	i-0487a0a18c90c4aad	Running	t2.micro	Initializing	No alarms	+	us-west-2b

Step 2 : Create Application Load Balancer

- Navigate to EC2 console > TargetGroup



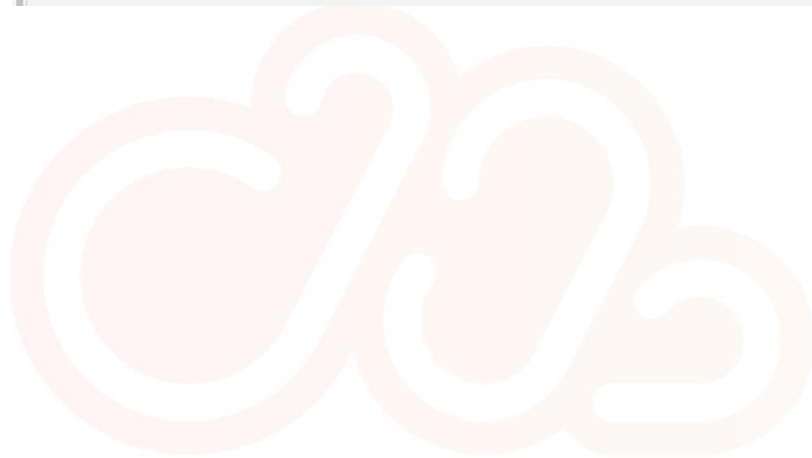
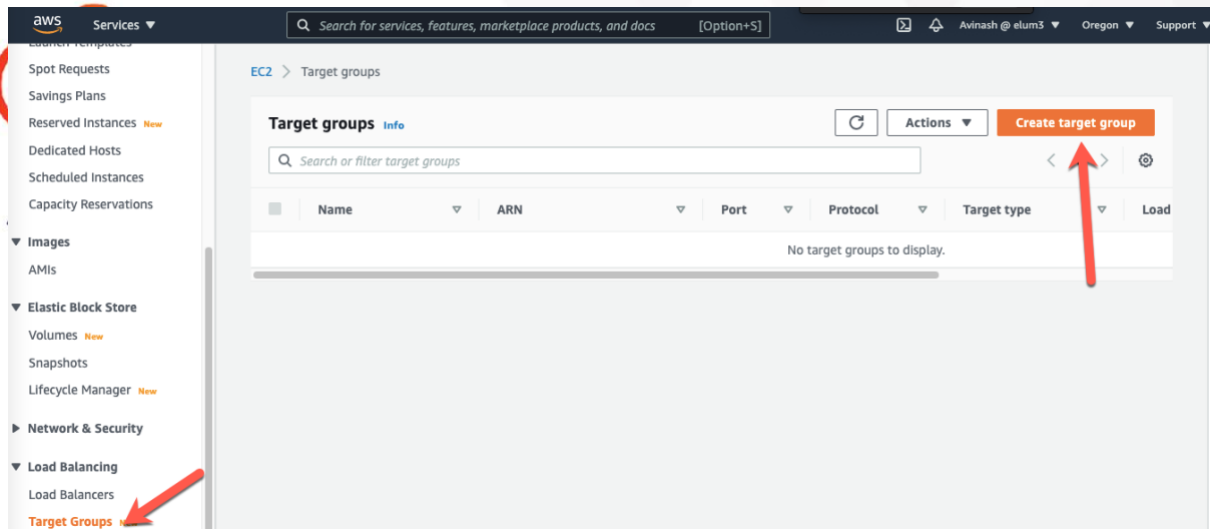
+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





JJ Tech



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Step 1
Specify group detailsStep 2
Register targets

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section cannot be changed after the target group is created.

Choose a target type

☒ Instances

- Supports load balancing to instances within a specific VPC.

☐ IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.

☐ Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

☐ Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol

Port

VPC

Select the VPC with the instances that you want to include in the target group.

vpc-0b1a467e85796eabc
IPv4: 10.0.0.0/20

Protocol version

☒ HTTP1

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

☐ HTTP2

Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

☐ gRPC

Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

Health check path

Use the default path of "/" or specify a custom path if preferred.

Up to 1024 characters allowed.

► Advanced health check settings

► Tags - optional

Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Cancel](#)[Next](#)

aws Services Search for services, features, marketplace products, and docs [Option+S] Avinash @ elum3 Oregon Support

EC2 > Target groups > Create target group

Step 1 Specify group details

Step 2 Register targets

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2/2)

Filter resources by property or value

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups	Zone	Subnet ID
<input checked="" type="checkbox"/>	i-0487a0a18c90c4aad	JJTech-EC2-2	running	Open	us-west-2b	subnet-0075e31df72419f9c
<input checked="" type="checkbox"/>	i-013f9ed1c9e35cc41	JJTech-EC2-1	running	launch-wizard-8	us-west-2a	subnet-05f3a4202f1e7127f

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below

Review targets

Targets (2)

All Filter resources by property or value

Remove all pending

Remove	Health status	Instance ID	Name	Port	State	Security groups	Zone	Subnet ID
×	Pending	i-013f9ed1c9e35cc41	JJTech-EC2-1	80	running	launch-wizard-8	us-west-2a	subnet-05f3a4202f1e7127f
×	Pending	i-0487a0a18c90c4aad	JJTech-EC2-2	80	running	Open	us-west-2b	subnet-0075e31df72419f9c

2 pending

Cancel Previous **Create target group**

EC2 > Target groups

Target groups (1) Info

Search or filter target groups

1

<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load
<input type="checkbox"/>	JJTech-TG	arn:aws:elasticloadbalancin...	80	HTTP	Instance	-

- Navigate to EC2 console > Load balancer
- Create ALB, with above Target group



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720

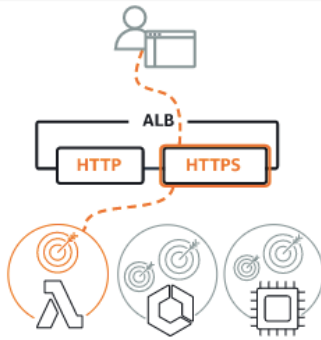


Select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

Load balancer types

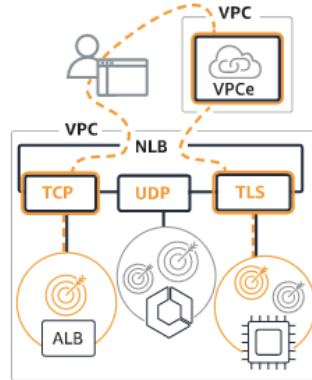
Application Load Balancer [Info](#)



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

Network Load Balancer [Info](#)



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

Gateway Load Balancer [Info](#)



Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

JJ Tech



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



aws

Services

Search for services, features, marketplace products, and docs

[Option+S]

🔍🔔👤 Avinash @ elu

EC2 > Load balancers > Create Application Load Balancer

Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▶ How Application Load Balancers work

Basic configuration

Load balancer name

Name must be unique within your AWS account and cannot be changed after the load balancer is created.

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme Info

Scheme cannot be changed after the load balancer is created.

☒ Internet-facing

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☐ Internal

An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type Info

Select the type of IP addresses that your subnets use.

☒ IPv4

Recommended for internal load balancers.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC Info

Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

vpc-0b1a467e85796eabc
IPv4: 10.0.0.0/20

↻

Mappings Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection. Subnets cannot be removed after the load balancer is created, but additional subnets can be added.

☒ us-west-2a

Subnet

JJTech-Pub-A

IPv4 settings

Assigned by AWS

☒ us-west-2b

Subnet

JJTech-Pub-B

IPv4 settings

Assigned by AWS

☒ us-west-2c

Subnet

JJTech-Pub-C

IPv4 settings

Assigned by AWS

87049

inc.co

inc.co

14103 Hammermil Field Dr Bowie MD 20720

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups

Select security groups

[Create new security group](#)

Open sg-0b8359f2179d6836b X
VPC: vpc-0b1a467e85796eabc

Listeners and routing [Info](#)

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification. You can specify multiple rules and multiple certificates per listener after the load balancer is created.

▼ Listener HTTP:80

Remove

Protocol

HTTP

Port

80

1-65535

Default action [Info](#)

Forward to

JJTech-TG

Target type: Instance, IPv4

HTTP

[Create target group](#)

Add listener

► Tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Summary

Review and confirm your configurations. [Estimate cost](#)

Basic configuration [Edit](#)

JJTech-ALB

- Internet-facing
- IPv4

Security groups [Edit](#)

- Open [sg-0b8359f2179d6836b](#)

Network mapping [Edit](#)

VPC [vpc-0b1a467e85796eabc](#)
JJTech-VPC

- us-west-2a
[subnet-05f3a4202f1e7127f](#)
JJTech-Pub-A
- us-west-2b
[subnet-0075e31df72419f9c](#)
JJTech-Pub-B
- us-west-2c
[subnet-06308f70ab7b52003](#)
JJTech-Pub-C

Listeners and routing [Edit](#)

- HTTP:80 defaults to [JJTech-TG](#)

Tags [Edit](#)

None

Attributes

ⓘ Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Cancel

Create load balancer



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Search for services, features, marketplace products, and docs [Option+S] Avinash @ elum3 Oregon Support

Create Load Balancer Actions

search : JJTech-ALB Add filter

Name	DNS name	State	VPC ID
JJTech-ALB	JJTech-ALB-629571939.us-...	Active	vpc-0b1a467e85796eabc

Load balancer: JJTech-ALB

Description Listeners Monitoring Integrated services Tags

Basic Configuration

Name JJTech-ALB

ARN arn:aws:elasticloadbalancing:us-west-2:464599248654:loadbalancer/app/JJTech-ALB/71f43214c5ec47ed

DNS name JJTech-ALB-629571939.us-west-2.elb.amazonaws.com (A Record)

State Active

Not Secure | jjtech-alb-629571939.us-west-2.elb.amazonaws.com

Hello AZ1

- Refresh the browser traffic will be loaded to another EC2 Instance
- Now, you are able to access the app from load balancer
- Let's restrict the access through WAF

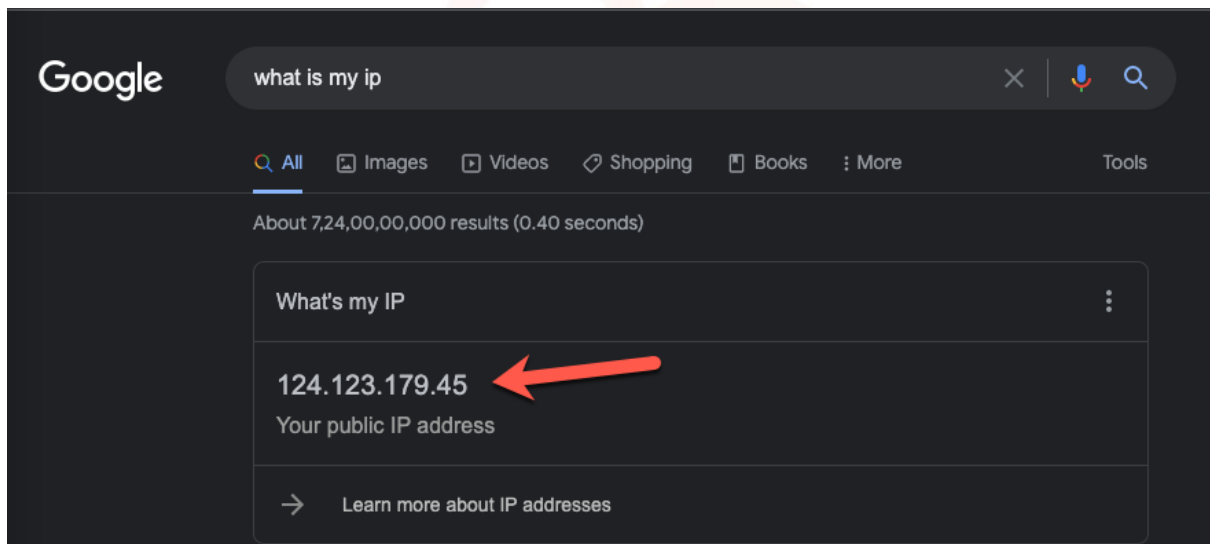
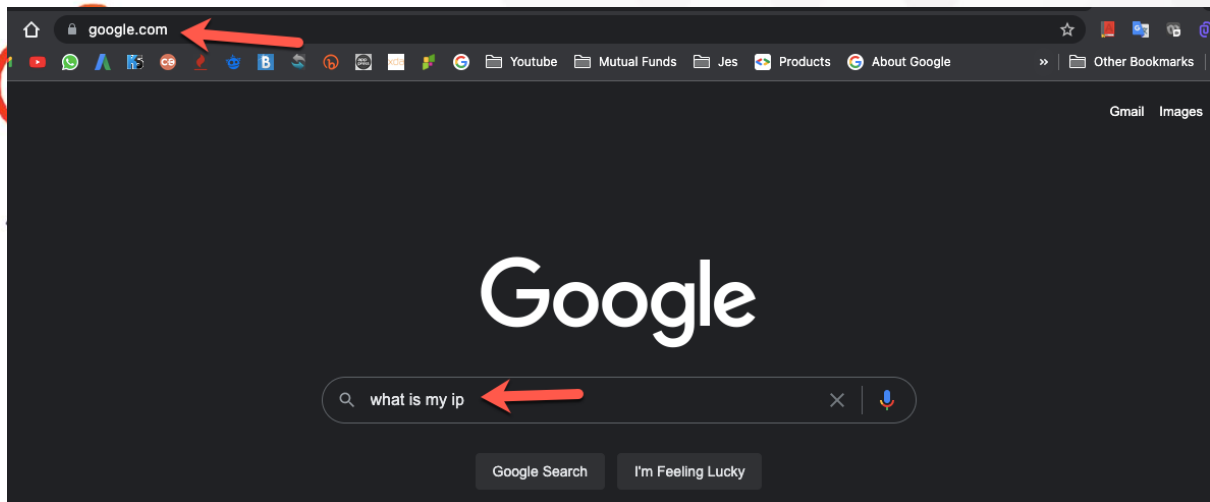
Step 3 : Create IP set in WAF

- Before we setup IP set, let's get your ip by typing "what is my ip" in Google search

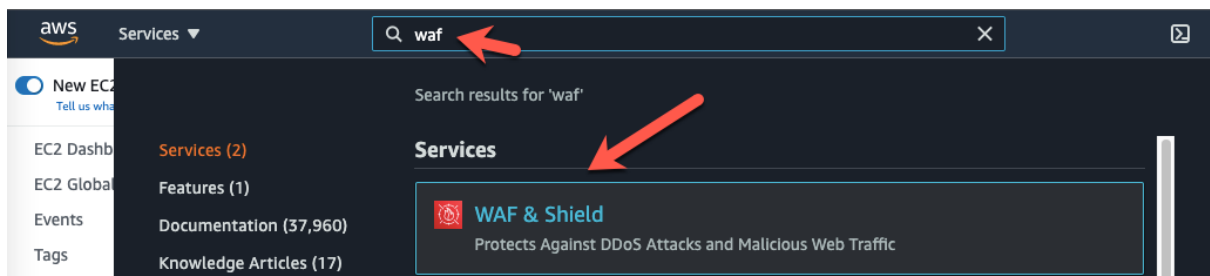
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





- Navigate to WAF AWS Console and create an IP set



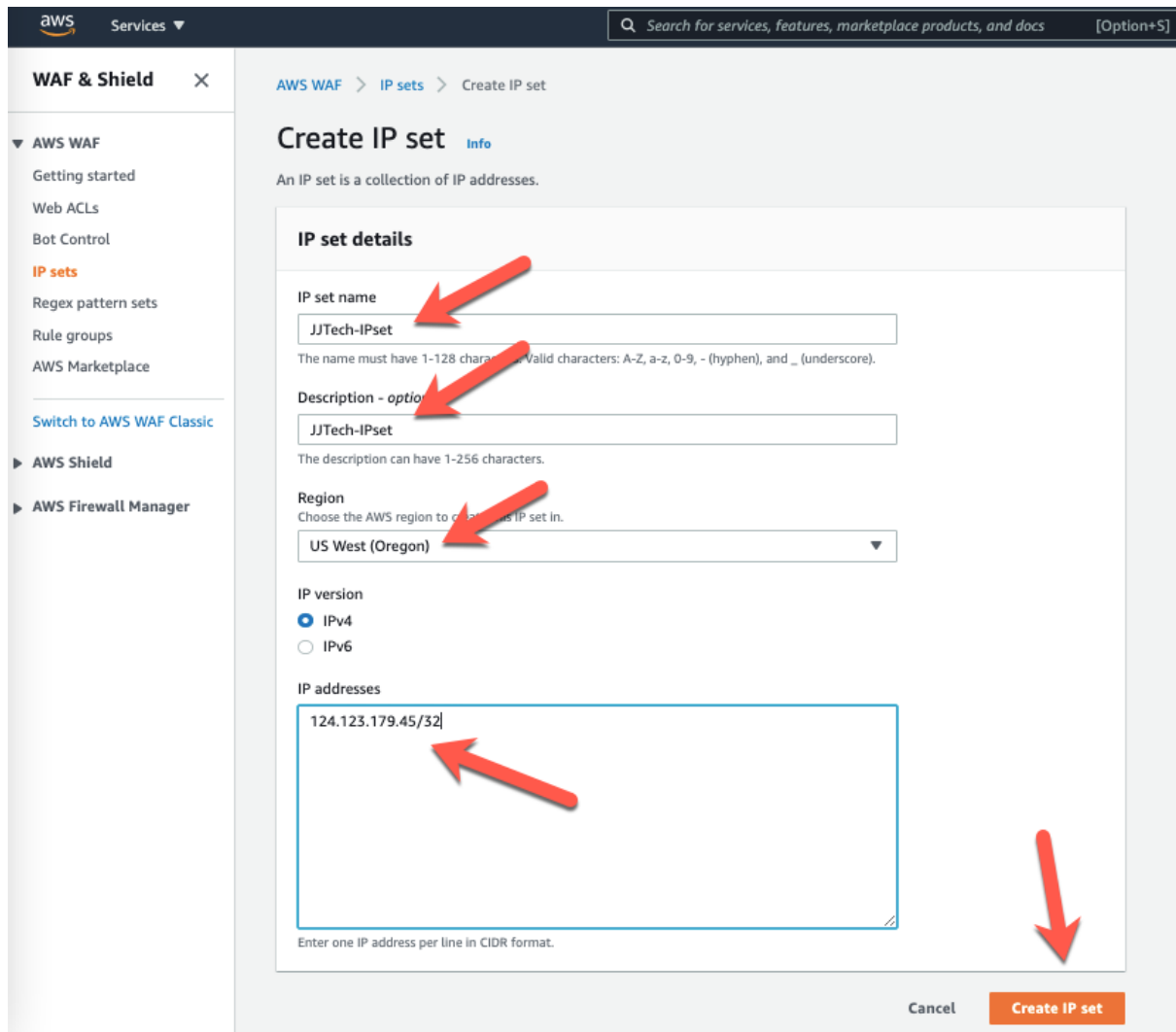
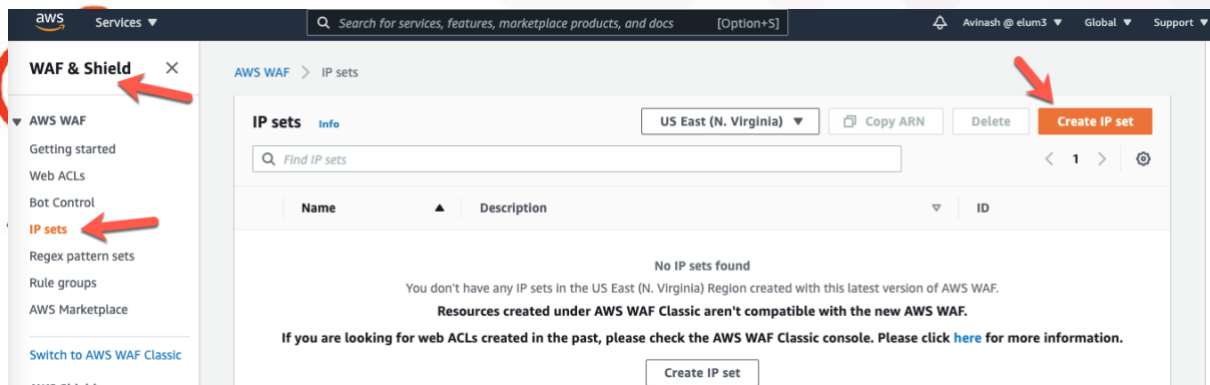
+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





- Add the IP address you got from “what is my ip” with /32



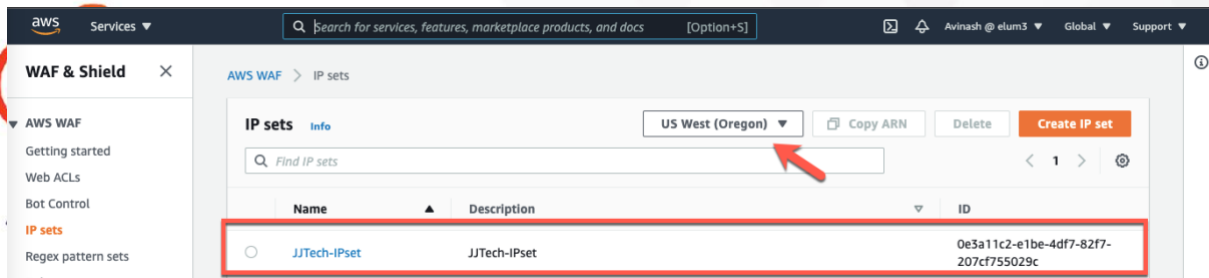
+1 (410) 8887049

contact@jjtechinc.co

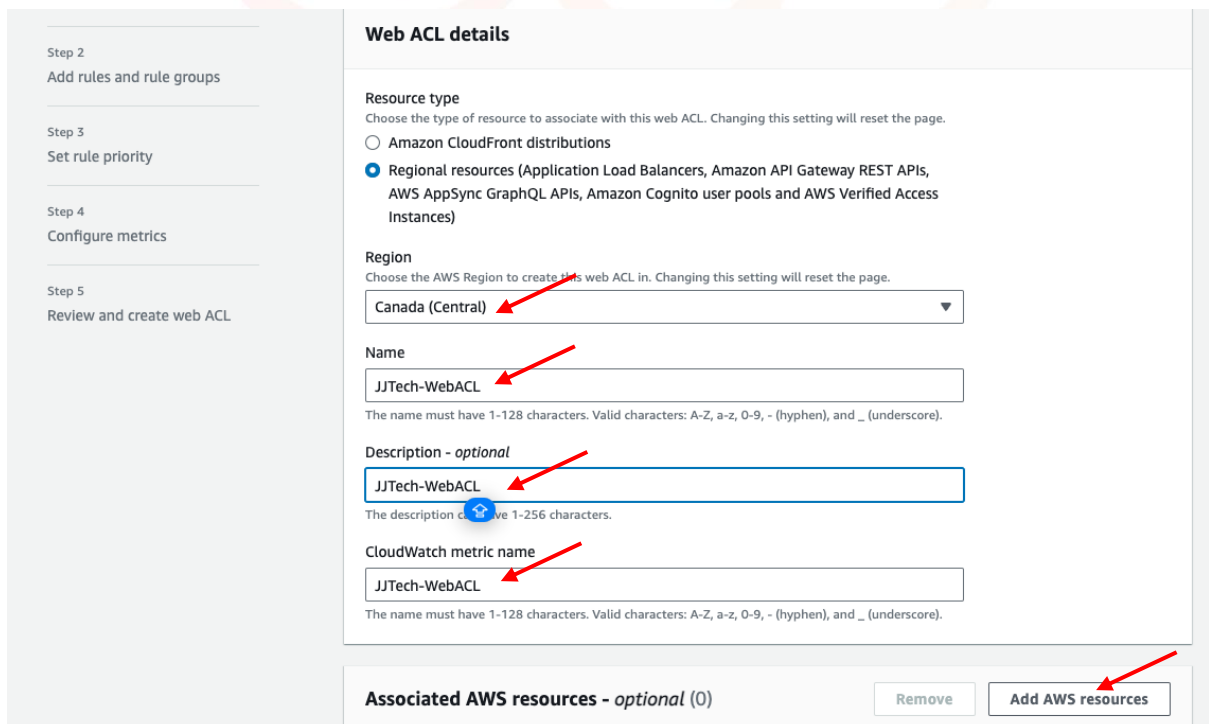
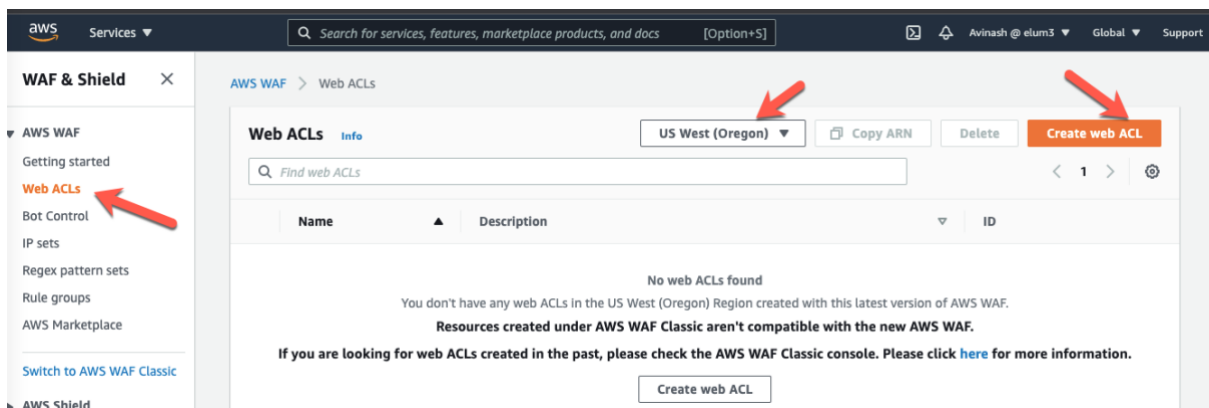
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





- Navigate to AWS WAF Web ACL's console



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





JJ Tech

Add AWS resources

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 ☐ 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

☒ Name

☒ JJTech-ALB

Cancel Add

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.

Rules
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

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

Web ACL rule capacity units used

- In this test we are going to block our own IP and allowing remaining all Ips



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Services Search for services, features, marketplace products, and docs [Option+S] Avinash @ elum3 Global Sup

WAF & Shield

- AWS WAF
 - Getting started
 - Web ACLs**
 - Bot Control
 - IP sets
 - Regex pattern sets
 - Rule groups
 - AWS Marketplace
- Switch to AWS WAF Classic
- AWS Shield
- AWS Firewall Manager

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: Add my own**

Step 3 Set rule priority

Step 4 Configure metrics

Step 5 Review and create web ACL

Add my own rules and rule groups

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

JJTech-IPset-Rule

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

IP set

IP set

JJTech-IPset

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**

Services Search for services, features, marketplace products, and docs [Option+S] Avinash @ elum3 G

WAF & Shield

- AWS WAF
 - Getting started
 - Web ACLs**
 - Bot Control
 - IP sets
 - Regex pattern sets
 - Rule groups
 - AWS Marketplace
- Switch to AWS WAF Classic
- AWS Shield
- AWS Firewall Manager

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

Rules

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

▲ Move up ▼ Move down

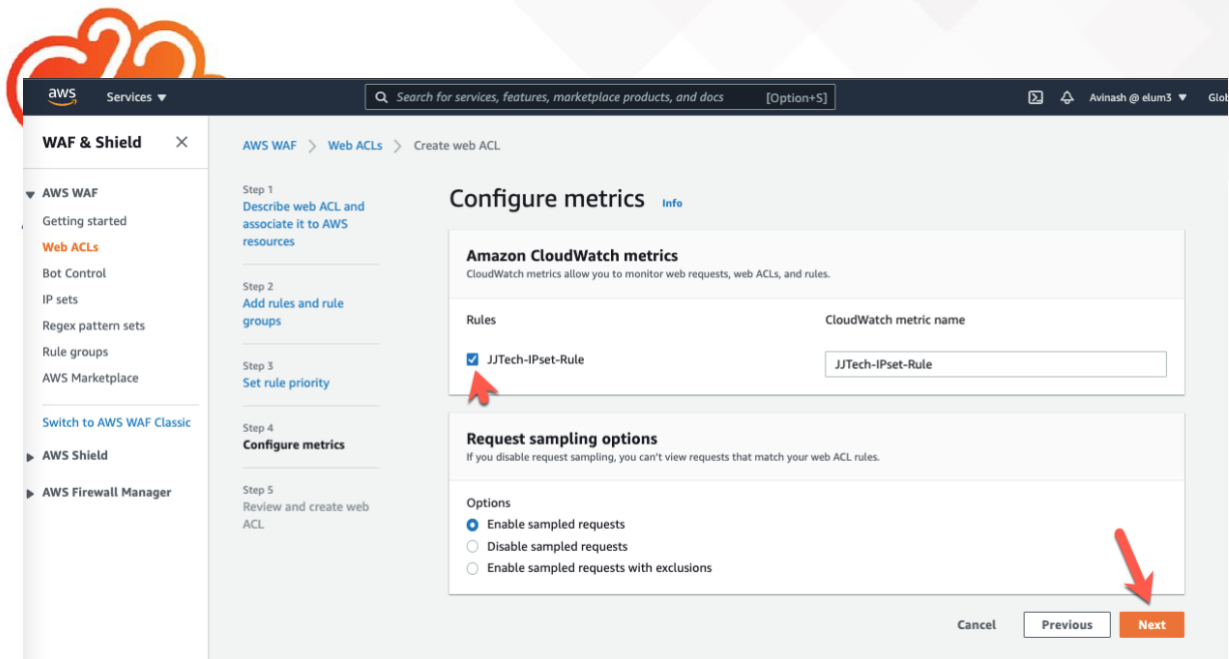
	Name	Capacity	Action
<input type="radio"/>	JJTech-IPset-Rule	1	Block

Cancel Previous **Next**



+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



WAF & Shield ×

AWS WAF

- Getting started
- Web ACLs**
- Bot Control
- IP sets
- Regex pattern sets
- Rule groups
- AWS Marketplace

Switch to AWS WAF Classic

AWS Shield

AWS Firewall Manager

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.

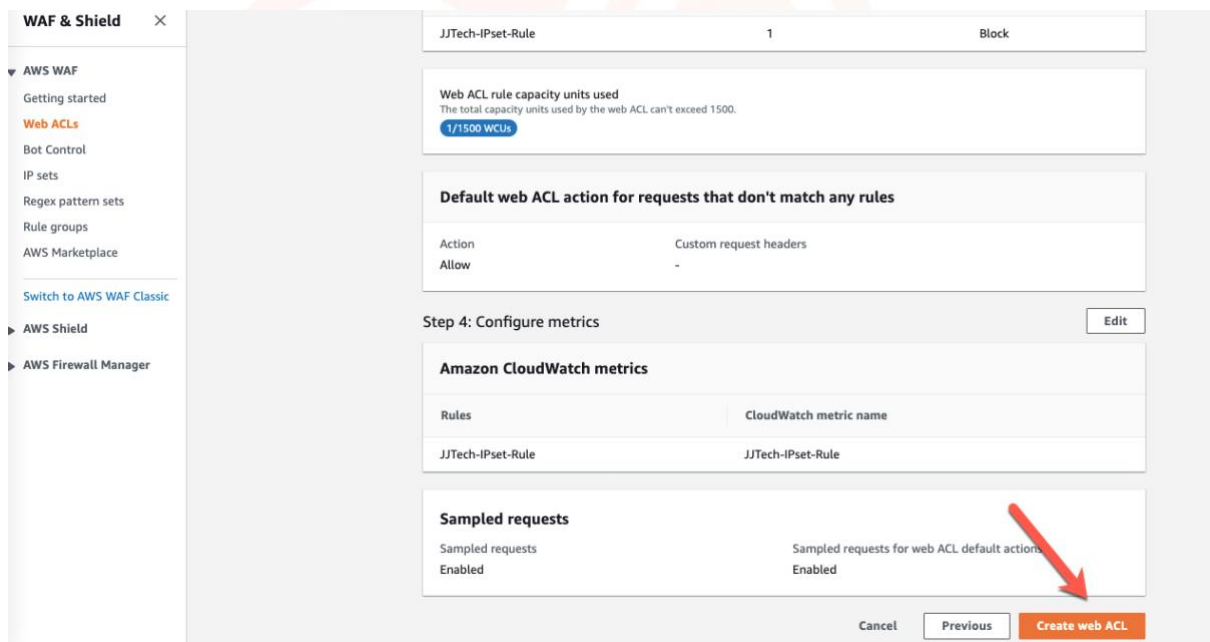
Rules	CloudWatch metric name
<input checked="" type="checkbox"/> JJTech-IPSet-Rule	JJTech-IPSet-Rule

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**



WAF & Shield ×

AWS WAF

- Getting started
- Web ACLs**
- Bot Control
- IP sets
- Regex pattern sets
- Rule groups
- AWS Marketplace

Switch to AWS WAF Classic

AWS Shield

AWS Firewall Manager

JJTech-IPSet-Rule 1 Block

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

Action	Custom request headers
Allow	-

Step 4: Configure metrics Edit

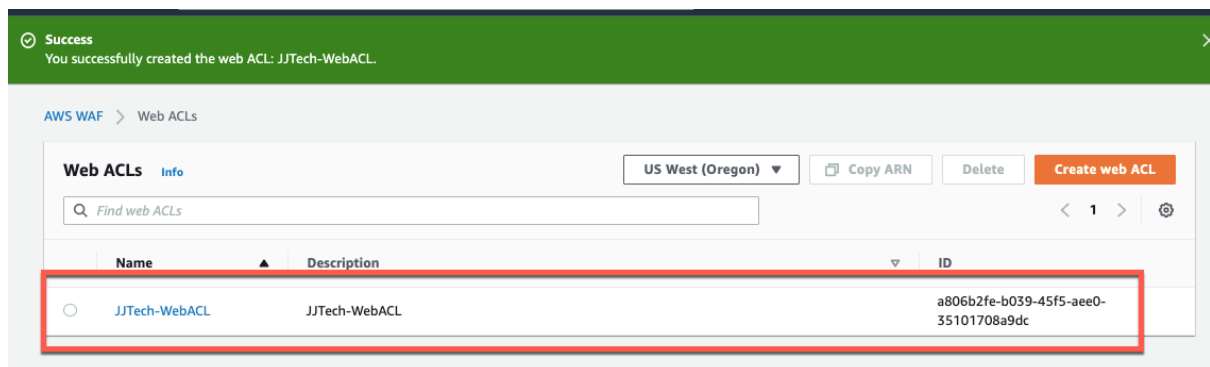
Amazon CloudWatch metrics

Rules	CloudWatch metric name
JJTech-IPSet-Rule	JJTech-IPSet-Rule

Sampled requests

Sampled requests	Sampled requests for web ACL default actions
Enabled	Enabled

Cancel Previous **Create web ACL**



Success
You successfully created the web ACL: JJTech-WebACL.

AWS WAF > Web ACLs

Web ACLs Info

US West (Oregon) Copy ARN Delete **Create web ACL**

Find web ACLs

Name	Description	ID
<input type="radio"/> JJTech-WebACL	JJTech-WebACL	a806b2fe-b039-45f5-aae0-35101708a9dc



Since we blocked our own IP, we cannot access the app from ALB DNS

Copy the DNS and search in google

403 Forbidden

- It's not working
- Our test is successful
- This is how we can block any Ips or/and allow any IPs

JJ Tech



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720

