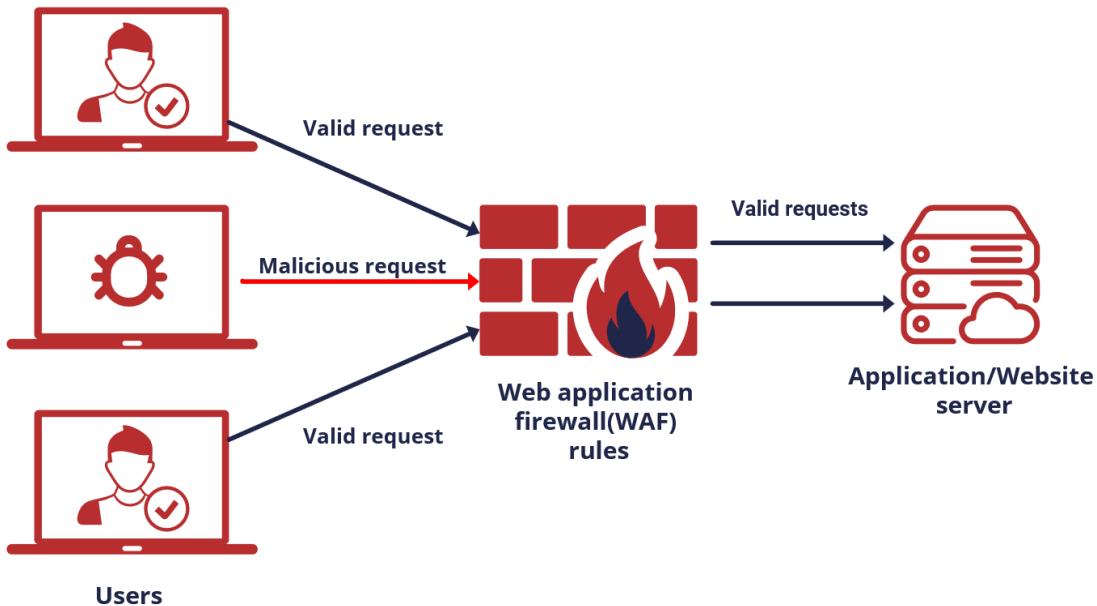


Securing a Web Application with AWS WAF



This document outlines a project to deploy a basic web server on an AWS EC2 instance and protect it using an Application Load Balancer (ALB) and AWS Web Application Firewall (WAF). The project demonstrates fundamental AWS networking concepts and security best practices by creating a custom Virtual Private Cloud (VPC), launching a web server, and configuring WAF to filter malicious traffic. The goal is to set up a robust, scalable, and secure web application infrastructure.

- **What is AWS WAF?** AWS Web Application Firewall (WAF) 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 which traffic to allow or block to your web applications by defining customizable web access control lists (web ACLs), rules, and rule groups.

Step-by-Step Guide to Deploying the Application

1. VPC and Networking Setup

First, you need to set up the network for your application. This involves creating a custom VPC, subnets, an Internet Gateway, and a route table.

- **Create VPC:** Navigate to the VPC dashboard and create a new VPC. Give it a name like WAF-project-4th sept and a CIDR block (e.g., 50.0.0.0/16).

The screenshot shows the 'Create VPC' page in the AWS VPC console. The 'VPC settings' section is active, with the 'Resources to create' dropdown set to 'VPC only'. Other options like 'VPC and more' and 'IPAM-managed VPC' are available. A 'Name tag - optional' field contains 'WAF-project-4th sept'. Under 'IPv4 CIDR block', the CIDR '50.0.0.0/16' is specified. Under 'IPv6 CIDR block', the option 'No IPv6 CIDR block' is selected. The 'Tenancy' dropdown is set to 'Default'. A success message at the top indicates the VPC was successfully created.

● Verify VPC

The screenshot shows the 'VPC dashboard' page. On the left, the 'Virtual private cloud' sidebar lists 'Your VPCs'. The main area displays the details of the newly created VPC: 'vpc-0fc1b920d008ef31b / WAF-project-4th sept'. The 'Details' section shows the VPC ID, state (Available), and other configurations. A green banner at the top confirms the creation.

- **Create Subnets:** Create two subnets within the VPC you just created. For example, WAF-subnet-2a with a CIDR block of 50.0.1.0/24 and WAF-Project-2b with a CIDR block of 50.0.2.0/24.

The screenshot shows the 'Create subnet' page. In the 'VPC' section, the VPC ID 'vpc-0fc1b920d008ef31b (WAF-project-4th sept)' is selected. The 'Associated VPC CIDRs' section shows a single entry: 'IPv4 CIDRs 50.0.0.0/16'.

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
WAF-subnet-2a
The name can be up to 256 characters long.

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (Ohio) / us-east-2a (us-east-2a)

IPv4 VPC CIDR block
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
50.0.0.0/16

IPv4 subnet CIDR block
50.0.1.0/24
256 IPs

Tags - optional
Key: Name Value - optional: WAF-subnet-2a
Add new tag

- Verify the subnet

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-0d25c37210724fcfd	Available	vpc-0bcedd90e4cd983c9	Off	172.31.0.0/20
-	subnet-0a0e598e8af231b73	Available	vpc-0bcedd90e4cd983c9	Off	172.31.32.0/2
-	subnet-0ccc04079ba5fa530	Available	vpc-0bcedd90e4cd983c9	Off	172.31.16.0/2
WAF-subnet-2a	subnet-036c02f22a6ee7b1b	Available	vpc-0fc1b920d008ef31b WAF-...	Off	50.0.1.0/24
WAP-Project-2b	subnet-0f932ff351d65b3da	Available	vpc-0fc1b920d008ef31b WAF-...	Off	50.0.2.0/24

- Create and Attach Internet Gateway: Create an Internet Gateway (IGW) and attach it to your VPC. This allows resources in your VPC to communicate with the internet.

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
WAF-IG

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key: Name Value - optional: WAF-IG
Add new tag
You can add 49 more tags.

Create internet gateway

- Attach VPC

Attach to VPC (igw-0fb59d08eef15f47e)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.
vpc-0fc1b920d008ef31b

AWS Command Line Interface command

Attach internet gateway

- Verify VPC

The screenshot shows the AWS VPC Internet Gateways page. A success message at the top states: "Internet gateway igw-0fb59d08eef15f47e successfully attached to vpc-0fc1b920d008ef31b". The main card displays the Internet gateway ID (igw-0fb59d08eef15f47e), state (Attached), VPC ID (vpc-0fc1b920d008ef31b | WAF-project-4th sept), and owner (648223607342). Below this, a "Tags" section shows a single tag named "Name" with the value "WAF-IG".

- **Create Route Table:** Create a new route table and associate it with your VPC.

The screenshot shows the AWS Route Tables page. A "Create route table" form is open. In the "Route table settings" section, the "Name - optional" field contains "WAF-Project-RT". The "VPC" dropdown is set to "vpc-0fc1b920d008ef31b (WAF-project-4th sept)". In the "Tags" section, a single tag "Name" with value "WAF-Project-RT" is added. At the bottom right, there are "Cancel" and "Create route table" buttons.

- **Add Route and Subnet Association:** Edit the route table to add a new route with a destination of 0.0.0.0/0 and a target of the Internet Gateway. Then, associate your subnets with this route table to enable them to access the internet.

The screenshot shows the AWS Route Tables page. A route table named "rtb-0dd4c89bed8b432eb / WAF-Project-RT" is selected. The "Subnet associations" tab is active. The "Explicit subnet associations" section is empty. The "Routes" tab shows a single route with a destination of 0.0.0.0/0 and a target of the Internet Gateway "igw-0fb59d08eef15f47e". The "Edge associations" section is also empty.

- Add that subnets

Available subnets (1/1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
WAF-subnet-2a	subnet-036c02f22a6ee7b1b	50.0.1.0/24	-	Main (rtb-0757e332d7b25bf98)

Selected subnets

subnet-036c02f22a6ee7b1b / WAF-subnet-2a	X
--	---

Buttons: Cancel, Save associations

- Verify subnet Association

Details Info

Route table ID rtb-0dd4c89bed8b432eb	Main No	Explicit subnet associations subnet-036c02f22a6ee7b1b / WAF-subnet-2a	Edge associations -
VPC vpc-0fc1b920d008ef31b WAF-project-4th-sept	Owner ID 648223607342		

Routes (1)

Destination	Target	Status	Propagated	Route Origin
50.0.0.0/16	local	Active	No	Create Route Table

- Add Route to IG

Edit routes

Destination	Target	Status	Propagated	Route Origin
50.0.0.0/16	local	Active	No	CreateRouteTable
0.0.0.0/0	Internet Gateway igw-0fb59d08eff15f47e	-	No	CreateRoute

Buttons: Add route, Cancel, Preview, Save changes

- Verify Route Table

Details Info

Route table ID rtb-0dd4c89bed8b432eb	Main No	Explicit subnet associations subnet-036c02f22a6ee7b1b / WAF-subnet-2a	Edge associations -
VPC vpc-0fc1b920d008ef31b WAF-project-4th-sept	Owner ID 648223607342		

Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0fb59d08eff15f47e	Active	No	Create Route
50.0.0.0/16	local	Active	No	Create Route Table

2. Launching an EC2 Instance

Next, you will launch an EC2 instance to serve as your web server.

- **Launch Instance:** Go to the EC2 dashboard and select "Launch instance". Name it WAF-App-Server, choose an appropriate AMI (e.g., Ubuntu Server), and an instance type (e.g., t3.micro).

The screenshot shows the AWS EC2 'Launch an instance' wizard. The process is divided into several steps:

- Name and tags:** The instance is named "WAF-App-Server".
- Application and OS Images (Amazon Machine Image):** The "Quick Start" tab is selected. A search bar shows "Search our full catalog including 1000s of application and OS images". Below are recent and quick start AMIs: Amazon Linux, macOS, Ubuntu (selected), Windows, Red Hat, SUSE Linux, and Debian. A "Browse more AMIs" link is available.
- Amazon Machine Image (AMI):** The selected AMI is "Ubuntu Server 24.04 LTS (HVM), SSD Volume Type". It is marked as "Free tier eligible".
- Description:** It states that the instance uses "Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>)."
- Instance type:** The selected instance type is "t3.micro". It lists specifications: Family: t3, 2 vCPU, 1 GiB Memory, Current generation: true, On-Demand RHEL base pricing: 0.0392 USD per Hour, On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour, On-Demand Windows base pricing: 0.0196 USD per Hour, On-Demand SUSE base pricing: 0.0104 USD per Hour, On-Demand Linux base pricing: 0.0104 USD per Hour. It also indicates "Free tier eligible".
- Additional costs apply for AMIs with pre-installed software**
- Key pair (login):** A key pair named "sidhu" is selected. There is a "Create new key pair" button.

- **Configure Networking:** Select the VPC and one of the subnets you created (WAF-subnet-2a is a good choice for this example). Enable

"Auto-assign public IP" to make the instance accessible from the internet.

- **Create Security Group:** Create a new security group named WAF-Project-SG. Add inbound rules to allow traffic on port 80 (HTTP) and port 22 (SSH) from anywhere (0.0.0.0/0).

▼ Network settings [Info](#)

VPC - required [Info](#)
vpc-0fc1b920d008ef31b (WAF-project-4th sept)
50.0.0.0/16

Subnet [Info](#)
subnet-036c02f22a6ee7b1b WAF-subnet-2a
VPC: vpc-0fc1b920d008ef31b Owner: 648223607342 Availability Zone: us-east-2a (use2-az1)
Zone type: Availability Zone IP addresses available: 251 CIDR: 50.0.1.0/24

Create new subnet [Create new subnet](#)

Auto-assign public IP [Info](#)
Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Security group name - required
WAP-Project-SG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _.-/[@!#\$%^&*(){}+=<>`~`]

Description - required [Info](#)
launch-wizard-1 created 2025-09-04T03:02:10.631Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type Info ssh	Protocol Info TCP	Port range Info 22
Source type Info Anywhere	Source Info <input type="text"/> Add CIDR, prefix list or security group	Description - optional Info e.g. SSH for admin desktop 0.0.0.0/X

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0) [Remove](#)

Type Info HTTP	Protocol Info TCP	Port range Info 80
Source type Info Anywhere	Source Info <input type="text"/> Add CIDR, prefix list or security group	Description - optional Info e.g. SSH for admin desktop 0.0.0.0/X

⚠ 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. [X](#)

[Add security group rule](#)

► Advanced network configuration

- Add User Data Script:** In the "User data" section, paste the following script. This script will automatically install Apache and host a simple static webpage when the instance launches.

User data - *optional* | [Info](#)

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

[Choose file](#)

```
#!/bin/bash
# User Data Script for EC2
# Installs Apache2 and hosts a static website
# Author: Sidhant Bote

# Update system
apt update -y

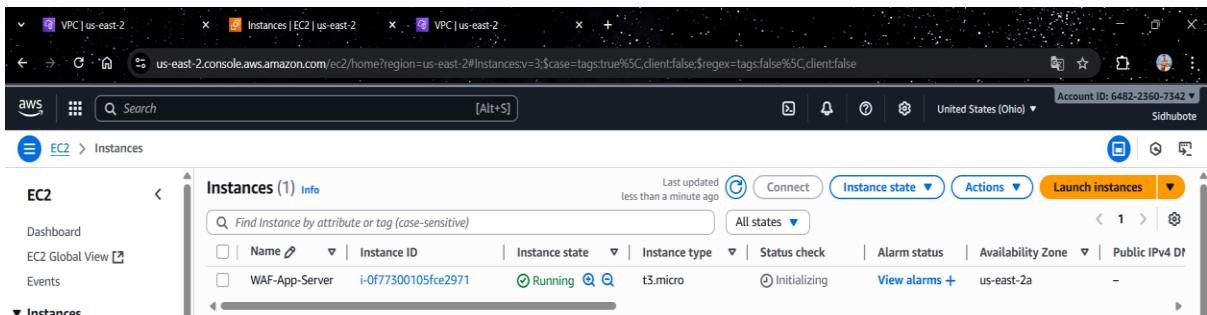
# Install Apache2
apt install apache2 -y

# Enable and start Apache service
systemctl enable apache2
systemctl start apache2

# Get Hostname and IP
HOSTNAME=$(hostname)
IPADDR=$(hostname -I | awk '{print $1}')

# Create a static index.html
cat > /var/www/html/index.html <<EOF
<!DOCTYPE html>
<html>
<head>
    <title>AWS Web Server</title>
    <style>
        body {
            background-color: #eef2f3;
            font-family: Arial, sans-serif;
            text-align: center;
            padding: 50px;
        }
        h1 { color: #34495e; }
    </style>
</head>
<body>
    <h1>Welcome to AWS Web Server!</h1>
    <p>This is a static webpage hosted by an Amazon EC2 instance.</p>
    <p>Hostname: $HOSTNAME</p>
    <p>Public IP: $IPADDR</p>
</body>
</html>
EOF
```

- Verify Instance:** After the instance is running, you can connect via SSH to verify the Apache installation and the webpage content using curl localhost. You can also access the website using the instance's public IP address in a web browser.



- Take ssh

```
PS C:\Users\botes\Downloads> ssh -i "sidhu.pem" ubuntu@3.137.215.107
The authenticity of host '3.137.215.107 (3.137.215.107)' can't be established.
ED25519 key fingerprint is SHA256:/TYVoBojJnPa6E0x3WZ984Y5lpdigM6bNjKGIupNPVQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.137.215.107' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1011-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Thu Sep  4 03:07:42 UTC 2025

System load:  0.3          Temperature:      -273.1 °C
Usage of /:   29.4% of 6.71GB  Processes:       120
Memory usage: 26%           Users logged in:  0
Swap usage:   0%            IPv4 address for ens5: 50.0.1.167

Expanded Security Maintenance for Applications is not enabled.

19 updates can be applied immediately.
17 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-50-0-1-167:~$ |
```

- Access application

```
ubuntu@ip-50-0-1-167:~$ curl localhost
<!DOCTYPE html>
<html>
<head>
    <title>AWS Web Server</title>
    <style>
        body {
            background-color: #eef2f3;
            font-family: Arial, sans-serif;
            text-align: center;
            padding: 50px;
        }
        h1 { color: #34495e; }
        p { font-size: 18px; }
        .card {
            background: #fff;
            padding: 20px;
            margin: 20px auto;
            width: 60%;
            border-radius: 12px;
            box-shadow: 0 4px 6px rgba(0,0,0,0.3);
        }
    </style>
</head>
<body>
    <h1>🚀 Apache2 Web Server on AWS 🚀</h1>
    <div class="card">
        <p><strong>Name:</strong> Sidhant Bote</p>
        <p><strong>Server Hostname:</strong> ip-50-0-1-167</p>
        <p><strong>Server IP:</strong> 50.0.1.167</p>
    </div>
    <p>This static website is hosted on an AWS EC2 instance using Apache2.</p>
    <p>🔒 Secured by AWS WAF, Security Groups & NACL 🔒</p>
</body>
</html>
```

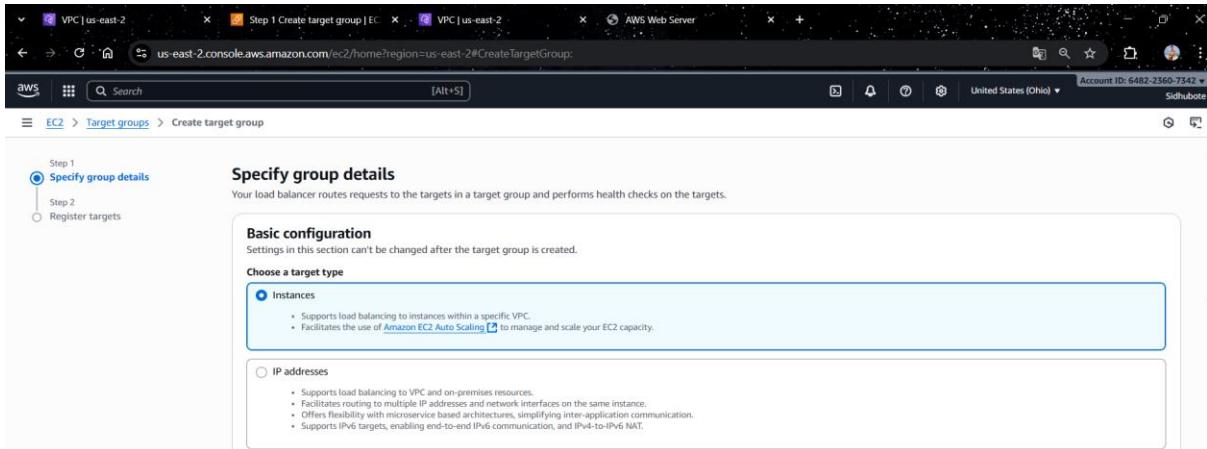
- Access on browser



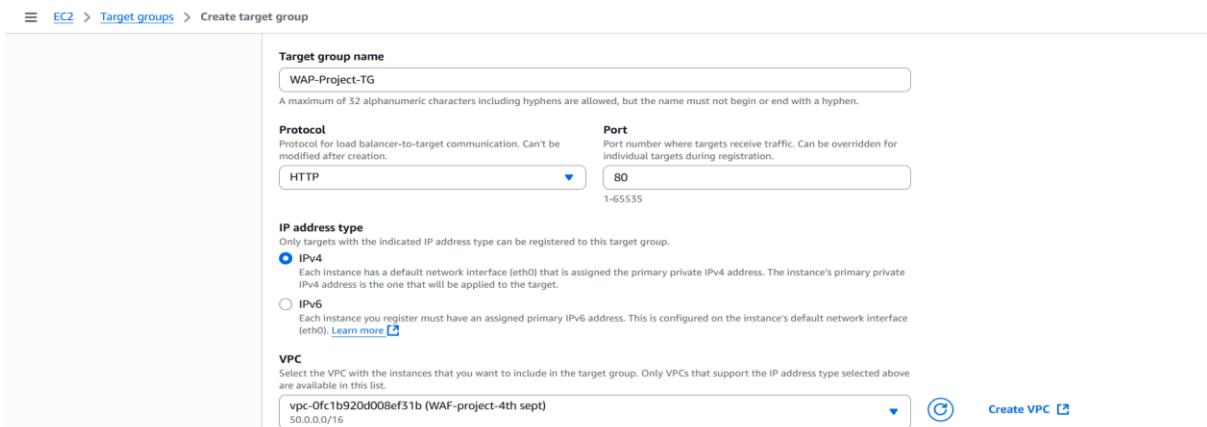
3. Configuring Application Load Balancer

An ALB will distribute traffic to your EC2 instance and will be the resource that WAF protects.

- **Create Target Group:** In the EC2 dashboard under "Load Balancing", create a new Target Group. Choose "Instances" as the target type and name it WAP-Project-TG. Specify the protocol as HTTP on port 80. Add your running WAF-App-Server instance to this target group.



- Configure the other things.



- Register targets & review target.

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 (1/1)

Instance ID	Name	State	Security groups	Zone
i-0f77300105fce2971	WAF-App-Server	Running	WAP-Project-SG	us-east-2a

1 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 (1)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID
i-0f77300105fce2971	WAF-App-Server	80	Running	WAP-Project-SG	us-east-2a	50.0.1.167	subnet-036c02f22a6ee7b

1 pending

[Remove all pending](#)

[Cancel](#) [Previous](#) [Create target group](#)

- Verify Target Group

WAP-Project-TG

Details

arn:aws:elasticloadbalancing:us-east-2:648225607342:targetgroup/WAP-Project-TG/90744c11d001b87f

Target type	Protocol : Port	Protocol version
Instance	HTTP: 80	HTTP1

IP address type

IPv4

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
1	0	0	1	0	0
0 Anomalous					

VPC

vpc-0fc1b920d008ef31b

- Create ALB: In the "Load Balancers" section, create a new Application Load Balancer.

Compare and 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

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

Network Load Balancer

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 application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latency.

Gateway Load Balancer

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](#)

- Name it WAP-Project-LB and make it "Internet-facing".

The screenshot shows the 'Basic configuration' step of the 'Create Application Load Balancer' wizard. It includes fields for the load balancer name (WAP-Project-LB), scheme (Internet-facing selected), and IP address type (IPv4 selected). A note indicates that IPv4 addresses have an additional cost.

- Select the VPC you created and both of your subnets.

The screenshot shows the 'Network mapping' step of the wizard. It lists two subnets: 'us-east-2a (use2-az1)' and 'us-east-2b (use2-az2)'. A warning message states that the selected subnet does not have a route to an internet gateway, so traffic will not receive internet traffic. The 'Create VPC' button is visible at the top right.

- Select the same security group as your EC2 instance or a new one that allows inbound traffic on port 80.

The screenshot shows the 'Security groups' step of the wizard. It lists a single security group 'WAP-Project-SG' selected for the load balancer.

- Configure the listener for HTTP on port 80 and forward requests to the WAP-Project-TG target group.

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Listener HTTP:80

Protocol	Port
HTTP	80 T-65535

Default action [Info](#)

Forward to	WAP-Project-TG Target type: Instance, IPv4
HTTP	Edit

[Create target group](#)

Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)
You can add up to 50 more tags.

[Add listener](#)
You can add up to 49 more listeners.

- **Verify ALB:** Once the ALB is active, you can access the website using the ALB's DNS name to verify it is working correctly.

Load balancers (1/1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	State	Type	Scheme	IP address type	VPC ID	Availability Zones
WAP-Project-LB	Active	application	Internet-facing	IPv4	vpc-0fc1b920d008ef31b	2 Availability Zones

- **Access using DNS in Browser**

Apache2 Web Server on AWS

Name: Sidhant Bote
Server Hostname: ip-50-0-1-167
Server IP: 50.0.1.167

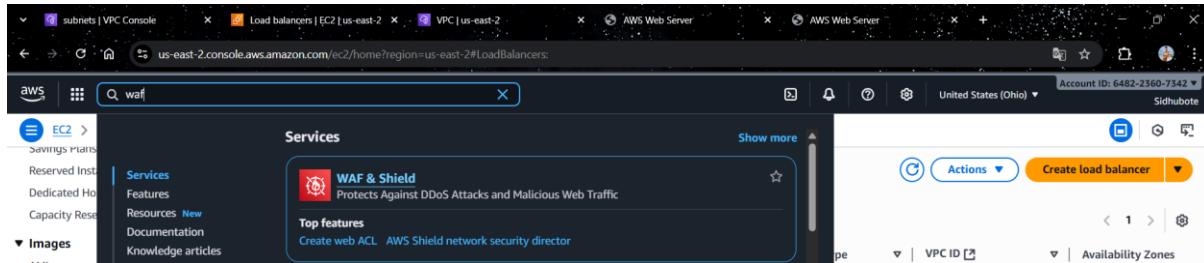
This static website is hosted on an AWS EC2 instance using Apache2.
Secured by AWS WAF, Security Groups & NACL

- **Access in the instance CLI**

```
ubuntu@ip-50-0-1-167:~$ curl http://wap-project-lb-64691563.us-east-2.elb.amazonaws.com/
<!DOCTYPE html>
<html>
<head>
    <title>AWS Web Server</title>
    <style>
        body {
            background-color: #eef2f3;
            font-family: Arial, sans-serif;
            text-align: center;
            padding: 50px;
        }
        h1 { color: #34495e; }
        p { font-size: 18px; }
        .card {
            background: #fff;
            padding: 20px;
            margin: 20px auto;
            width: 60%;
            border-radius: 12px;
            box-shadow: 0 4px 6px rgba(0,0,0,0.3);
        }
    </style>
</head>
<body>
    <h1>Apache2 Web Server on AWS</h1>
    <div class="card">
        <p><strong>Name:</strong> Sidhant Bote</p>
        <p><strong>Server Hostname:</strong> ip-50-0-1-167</p>
        <p><strong>Server IP:</strong> 50.0.1.167</p>
    </div>
    <p>This static website is hosted on an AWS EC2 instance using Apache2.</p>
    <p>Secured by AWS WAF, Security Groups & NACL</p>
</body>
</html>
```

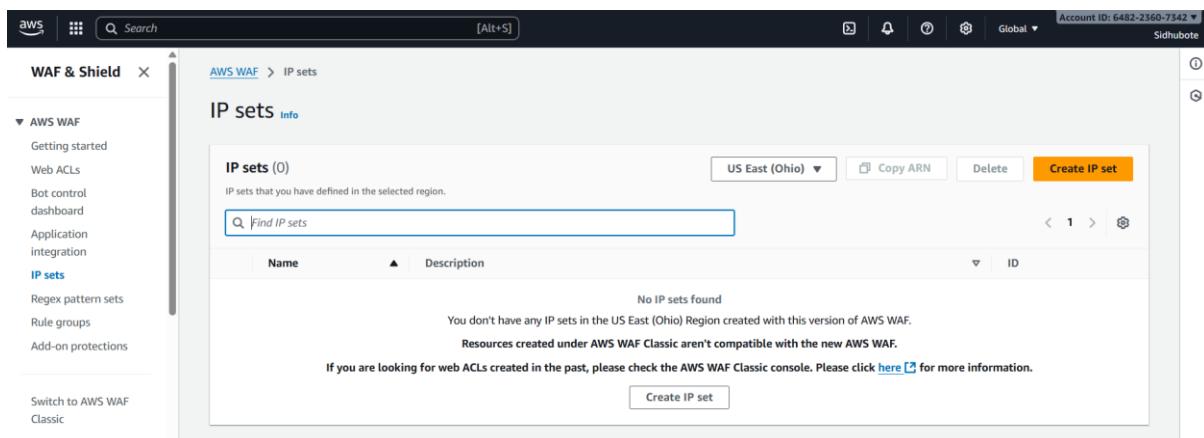
4. Configuring AWS WAF

Finally, you will create a Web ACL with a custom rule to protect your application.



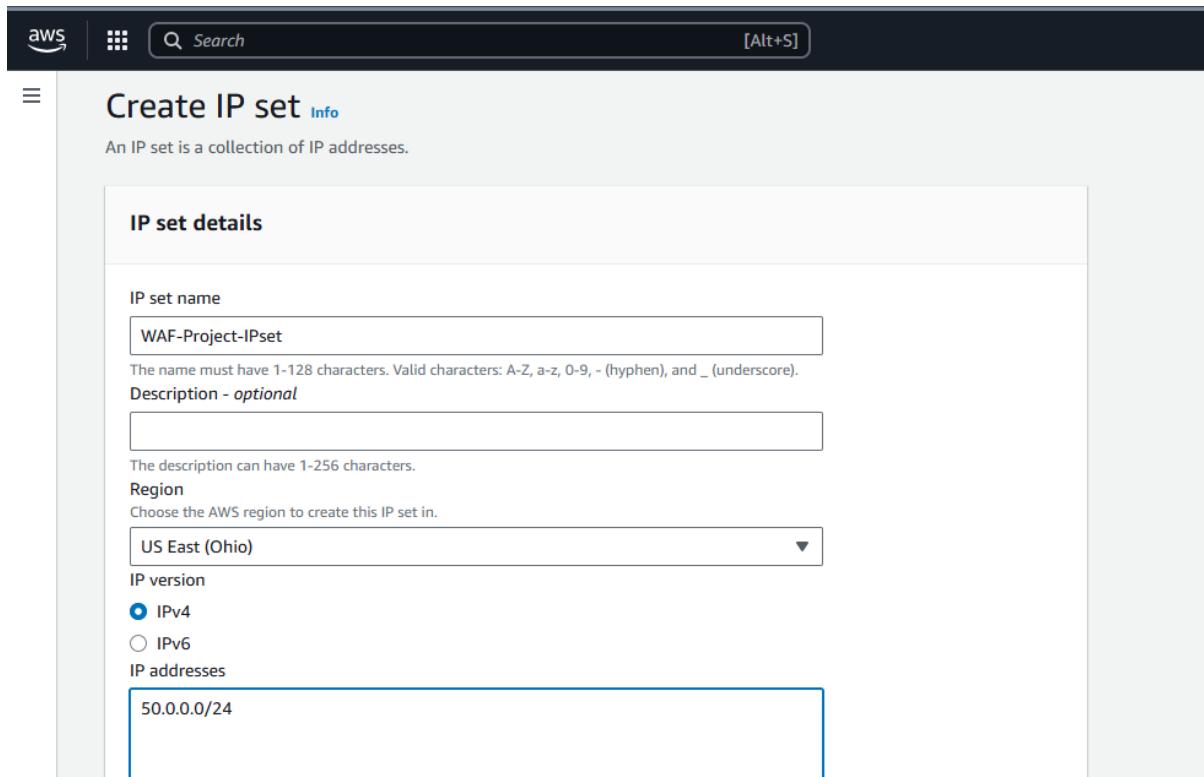
The screenshot shows the AWS WAF & Shield dashboard. In the center, there is a callout box for "Create web ACL". Below it, there is a section titled "Top features" with a link to "AWS Shield network security director". On the right side of the dashboard, there are buttons for "Actions", "Create load balancer", and dropdown menus for "VPC ID" and "Availability Zones". The top navigation bar includes tabs for "subnets", "Load balancers", "EC2", "VPC", "AWS Web Server", and "AWS Web Server". The search bar at the top has the term "waf" entered.

- **Create IP Set:** In the AWS WAF & Shield dashboard, navigate to "IP sets" and create a new IP set.



The screenshot shows the "IP sets" page under the "AWS WAF" section of the WAF & Shield dashboard. On the left, there is a sidebar with options like "Getting started", "Web ACLs", "Bot control dashboard", "Application integration", "IP sets" (which is selected), "Regex pattern sets", "Rule groups", and "Add-on protections". The main area shows a table with one row: "No IP sets found". Below the table, there is a message stating "You don't have any IP sets in the US East (Ohio) Region created with this version of AWS WAF." and "Resources created under AWS WAF Classic aren't compatible with the new AWS WAF." At the bottom, there is a "Create IP set" button. The top navigation bar includes tabs for "subnets", "Load balancers", "EC2", "VPC", "AWS Web Server", and "AWS Web Server". The search bar at the top has the term "Search" entered.

- **Name it WAF-Project-IPset and specify the IP addresses you want to block.**



The screenshot shows the "Create IP set" configuration page. The "IP set details" section contains the following fields:

- IP set name:** WAF-Project-IPset (highlighted with a blue border)
- Description - optional:** (empty field)
- Region:** US East (Ohio) (selected from a dropdown menu)
- IP version:** IPv4 (selected radio button)
- IP addresses:** 50.0.0.0/24 (entered into a text input field)

The top navigation bar includes tabs for "subnets", "Load balancers", "EC2", "VPC", "AWS Web Server", and "AWS Web Server". The search bar at the top has the term "Search" entered.

- **Create Web ACL:** Go to "Web ACLs" and create a new Web ACL. Name it WAF-Project-WEBAACL and choose "Regional resources".

Describe web ACL and associate it to AWS resources

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.
 US East (Ohio)

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

- **Associate the Web ACL with your WAP-Project-LB Application Load Balancer.**

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 Amazon App Runner service
 AWS AppSync API Amazon Cognito user pool AWS Verified Access

Resources (1)
Select the resource you want to associate with the web ACL.

Find AWS resources to associate

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	WAP-Project-LB

Cancel Add

Resource level DDoS protection - new
Protect critical resources from DDoS attacks using AWS managed threat list. This configuration currently only applies to Application Load Balancers.

Protection against low reputation sources

Active under DDos
Active under DDoS mode only blocks when very high request volumes are observed.

Always on
Always on mode actively blocks threats all the time.

Cancel Next

- Add Custom Rule:** In the "Add rules and rule groups" step, select "Add my own rules and rule groups".

The screenshot shows the AWS WAF 'Create web ACL' wizard at Step 2: 'Add rules and rule groups'. The left sidebar lists steps 1 through 4. The main area has a heading 'Add rules and rule groups' with a link to 'Info'. Below it is a table titled 'Rules (0)' with columns 'Name', 'Capacity', and 'Action'. There are buttons for 'Edit', 'Delete', and 'Add rules'. A dropdown menu shows 'Add managed rule groups' and 'Add my own rules and rule groups', with the latter being highlighted.

- Choose "IP set" as the rule type and name it WAF-Rule.**

The screenshot shows the 'Add my own rules and rule groups' step. The left sidebar lists steps 1 through 5. The main area has a heading 'Add my own rules and rule groups' with a link to 'Info'. Under 'Rule type', the 'IP set' option is selected. In the 'Rule' section, the 'Name' field contains 'WAF-Rule'.

- Select the WAF-Project-IPset you created and set the action to "Block".**

The screenshot shows the 'IP set' configuration page. The 'IP set' dropdown is set to 'WAF-Project-IPset'. Under 'Action', 'Source IP address' is selected, and 'Block' is selected as the action choice. Other options like 'Allow', 'Count', and 'Challenge' are also listed. At the bottom right are 'Cancel' and 'Add rule' buttons.

- Leave Other Configuration Default.

Add rules and rule groups

Rules (1)

Name	Capacity	Action
WAF-Rule	1	Block

Web ACL capacity units (WCUs) used by your 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

Token domain list - optional

Add token domain

Set rule priority

Rules (1/1)

Name	Capacity	Action
WAF-Rule	1	Block

Next

Configure metrics

Amazon CloudWatch metrics

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

Rules

WAF-Rule

CloudWatch metric name

WAF-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

Next

- **Review and Create:** Review the Web ACL settings and create it.

- **Verify WAF**

- **Verify WAF Functionality:** To verify the WAF is working, try to access your ALB's DNS name from an IP address that you have added to the IP set. You should be blocked from accessing the site.

```
ubuntu@ip-50-0-1-167:~$ curl http://wap-project-lb-64691563.us-east-2.elb.amazonaws.com/
```

- **Access Using Another IP.**

Apache2 Web Server on AWS

Name: Sidhant Bote
Server Hostname: ip-50-0-1-167
Server IP: 50.0.1.167

This static website is hosted on an AWS EC2 instance using Apache2.
Secured by AWS WAF, Security Groups & NACL