

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

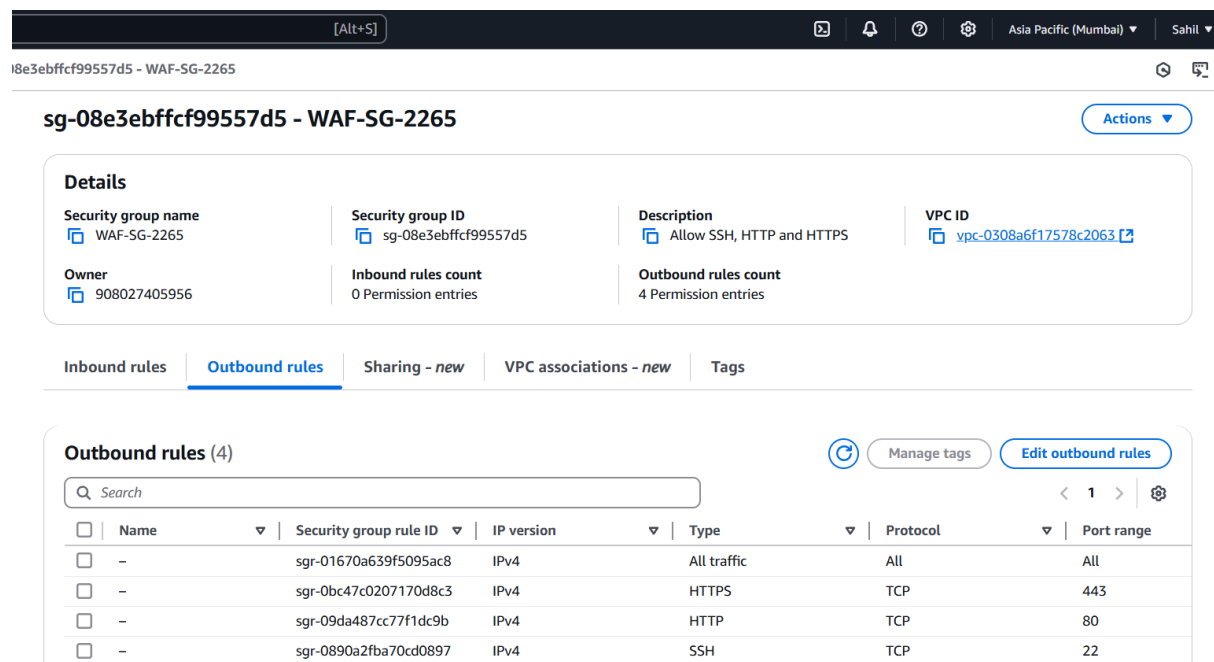
**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

**Step 1: Create Security Group & Launch 2 EC2 Instances.**

- Login to your AWS Console.
- Create a SG with name 'WAF-SG-2265' with rules: HTTP, SSH, HTTPS.



The screenshot shows the AWS Management Console interface for a Security Group. The top bar indicates the region is Asia Pacific (Mumbai) and the user is Sahil. The breadcrumb trail shows the path: I8e3ebffcf99557d5 - WAF-SG-2265. The main heading is 'sg-08e3ebffcf99557d5 - WAF-SG-2265' with an 'Actions' button. Below this, the 'Details' tab is active, showing the following information:

Details	
<b>Security group name</b> WAF-SG-2265	<b>Security group ID</b> sg-08e3ebffcf99557d5
<b>Description</b> Allow SSH, HTTP and HTTPS	<b>VPC ID</b> vpc-0308a6f17578c2063
<b>Owner</b> 908027405956	<b>Inbound rules count</b> 0 Permission entries
	<b>Outbound rules count</b> 4 Permission entries

Below the details, there are tabs for 'Inbound rules', 'Outbound rules' (which is selected), 'Sharing - new', 'VPC associations - new', and 'Tags'. The 'Outbound rules (4)' section shows a table with 4 rules:

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-01670a639f5095ac8	IPv4	All traffic	All	All
-	sgr-0bc47c0207170d8c3	IPv4	HTTPS	TCP	443
-	sgr-09da487cc77f1dc9b	IPv4	HTTP	TCP	80
-	sgr-0890a2fba70cd0897	IPv4	SSH	TCP	22

- Launch two instances with name "EC2-WAF-2265".
- Select AMI as "Amazon Linux 2".
- In Network setting select our created Security Group, i.e. 'WAF-SG-2265'.
- Add the below script in user data:

```
#!/bin/bash
```

```
sudo su
```

```
yum update -y
```

```
yum install httpd -y
```

## School of Computer Science, Engineering and Applications (SCSEA)

### B. Tech TY (CCSA)

### Subject: Cloud Architecture And Protocol

**Name of the Student:** Sahil S. Mandawgade

**PRN:** 20220802265

**Title of Practical:** 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.

systemctl start httpd

systemctl enable httpd

- After this, launch the instances.

[EC2](#) > [Instances](#) > Launch an instance

#### Name and tags [Info](#)

Name

EC2-WAF-2265

[Add additional tags](#)

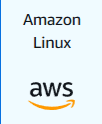


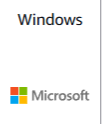



#### ▼ Application and OS Images (Amazon Machine Image) [Info](#)


An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents

[Quick Start](#)

 <p>Amazon Linux</p>	 <p>macOS</p>	 <p>Ubuntu</p>	 <p>Windows</p>	 <p>Red Hat</p>	 <p>SUSE Linux</p>	 <p>Debian</p>
---	--	---	--	--	---	---

  
[Browse more AMIs](#)  
Including AMIs from  
AWS, Marketplace and  
the Community

#### Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-01bd9d8f06d29d6a0 (64-bit (x86)) / ami-03ac4ac652b29b918 (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

#### 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

#### Common security groups [Info](#)

Select security groups ▼

WAF-SG-2265 sg-08e3ebffcf99557d5 ✕  
VPC: vpc-0308a6f17578c2063

 [Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

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

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

[Choose file](#)

```
#!/bin/bash
sudo su
yum update -y
yum install httpd -y
systemctl start httpd
systemctl enable httpd
```

### **Step 2: Host Website on Both EC2 Instances.**

- Connect Server A in the terminal → get to root user with command “sudo su”.
- Use command ‘wget {download url link of template}’ to install website template.
- Use command ‘unzip {downloaded zip file}’ → this will unzip your file.



### B. Tech TY (CCSA)

**Name of the Student: Sahil S. Mandawgade**

**Title of Practical:** 8. Enterprise-Grade Web Traffic Blocking: Configuring AWS WAF for Dynamic Threat Protection.

- Use “cd {unzip file}” to get into the file → use command mv \* /var/www/html → to push template to web server.

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

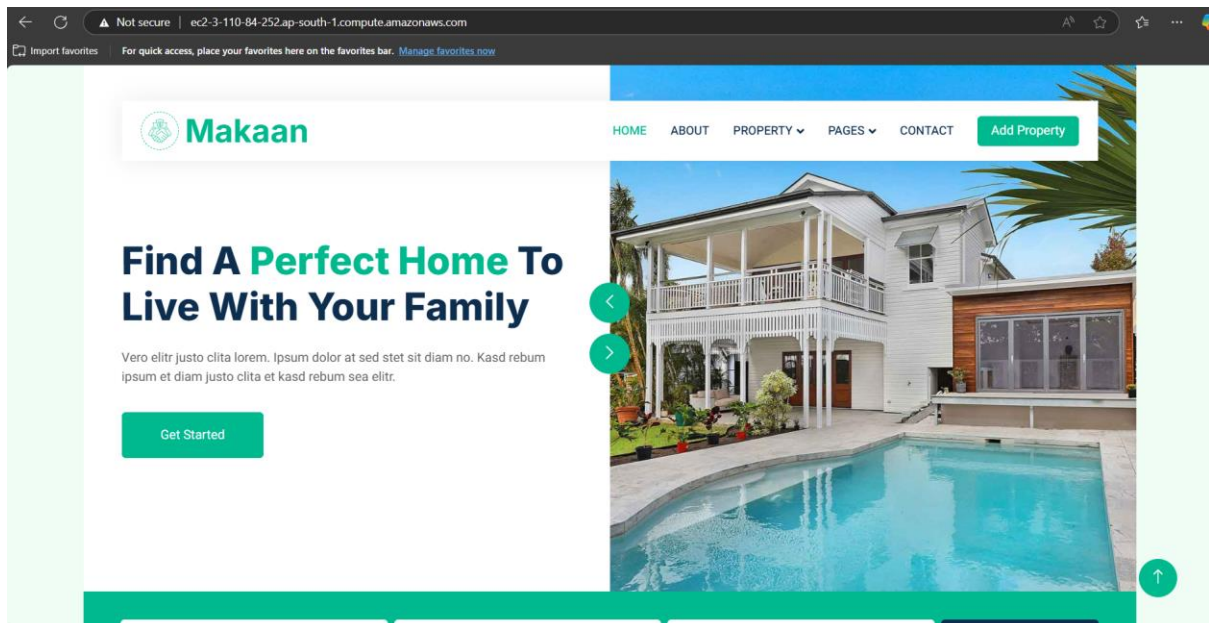
**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

```
[ec2-user@ip-172-31-10-122 ~]$ ls
makaan.zip  real-estate-html-template
[ec2-user@ip-172-31-10-122 ~]$ cd real-estate-html-template/
[ec2-user@ip-172-31-10-122 real-estate-html-template]$ sudo su
[root@ip-172-31-10-122 real-estate-html-template]# ls
404.html      css           js            property-agent.html  READ-ME.txt          testimonial.html
about.html    img          lib           property-list.html   real-estate-html-template.jpg
contact.html  index.html  LICENSE.txt   property-type.html   scss
[root@ip-172-31-10-122 real-estate-html-template]# mv * /var/www/html
mv: overwrite '/var/www/html/index.html'? yes
[root@ip-172-31-10-122 real-estate-html-template]# ls
[root@ip-172-31-10-122 real-estate-html-template]# cd /var/www/html
[root@ip-172-31-10-122 html]# ls
404.html      css           js            property-agent.html  READ-ME.txt          testimonial.html
about.html    img          lib           property-list.html   real-estate-html-template.jpg
contact.html  index.html  LICENSE.txt   property-type.html   scss
[root@ip-172-31-10-122 html]#
```

- Check Website Server IP to confirm hosting.



**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

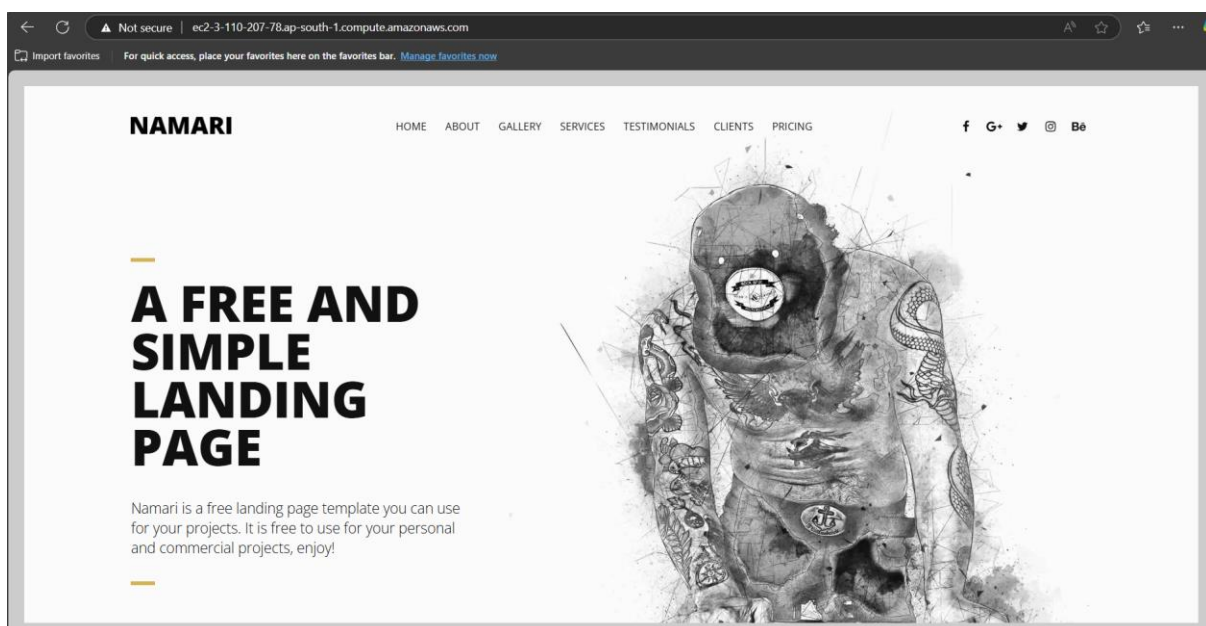
**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

- Do the same for web server B.



### **Step 3: Create a Target Group & Application Load Balancer.**

- Target type: Instances → Assign Name as 'WAF-TG-2265' → Health Check path: /index.html

#### **Health checks**

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

##### **Health check protocol**

HTTP

##### **Health check path**

Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

/index.html

Up to 1024 characters allowed.

► **Advanced health check settings**

## School of Computer Science, Engineering and Applications (SCSEA)

### B. Tech TY (CCSA)

### Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

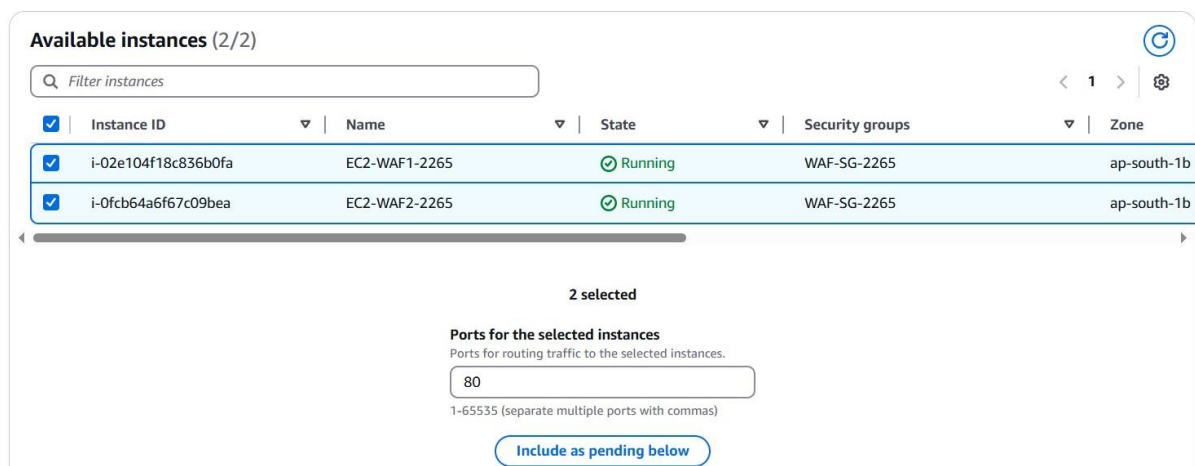
PRN: 20220802265

### Title of Practical: 8. Enterprise-Grade Web Traffic Blocking: Configuring AWS WAF for Dynamic Threat Protection.

- Add both Instances → Create Target Group.

#### 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 instances

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups	Zone
<input checked="" type="checkbox"/>	i-02e104f18c836b0fa	EC2-WAF1-2265	Running	WAF-SG-2265	ap-south-1b
<input checked="" type="checkbox"/>	i-0fcb64a6f67c09bea	EC2-WAF2-2265	Running	WAF-SG-2265	ap-south-1b

2 selected

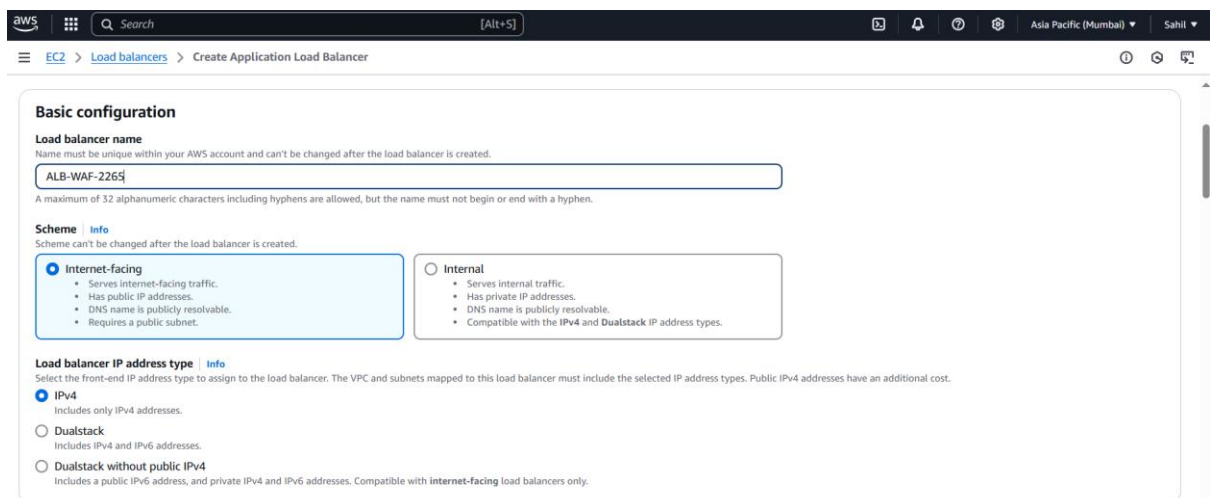
Ports for the selected instances  
Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below

- Go to Load Balancers → Create LB → Application load balancer → Assign Name as 'ALB-WAF-2265' → Scheme: Internet Facing.



aws Search [Alt+S]

EC2 > Load balancers > Create Application Load Balancer

#### Basic configuration

**Load balancer name**  
Name must be unique within your AWS account and can't be changed after the load balancer is created.

ALB-WAF-2265

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

**Scheme** [Info](#)  
Scheme can't be changed after the load balancer is created.

☒ **Internet-facing**

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

☐ **Internal**

- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.
- Compatible with the IPv4 and Dualstack IP address types.

**Load balancer IP address type** [Info](#)  
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

☒ **IPv4**  
Includes only IPv4 addresses.

☐ **Dualstack**  
Includes IPv4 and IPv6 addresses.

☐ **Dualstack without public IPv4**  
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with internet-facing load balancers only.



**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

- Allow all Availability Zones → Your Created Security Group & Target Group.

**Security groups** [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

**Security groups**

Select up to 5 security groups

WAF-SG-2265

sg-08e3ebffcf99557d5 VPC: vpc-0308a6f17578c2063

**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 is

▼ Listener HTTP:80

**Protocol**

HTTP

**Port**

80

1-65535

**Default action** [Info](#)

Forward to

WAF-TG-2265

Target type: Instance, IPv4

HTTP

[Create target group](#)

- Create Application load balancer.

**Step 4: Setup WAF & IP Set.**

- Go to WAF & Shield → IP sets → Create IP Sets.
- Search on chrome for your mobile IP.
- Add Your Mobile IP in the List with /32 → This will block the IPs trying to access your server if the IP matches the ones in your IP sets.



**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

[AWS WAF](#) > [IP sets](#) > Create IP set

## Create IP set [Info](#)

An IP set is a collection of IP addresses.

### IP set details

IP set name

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.

Region

Choose the AWS region to create this IP set in.

IP version

☒ IPv4

☐ IPv6

IP addresses

- Now to go Web ACL → Create Web ACL.
- Name as 'WEB-ACL-2625'. Add your LB in Associated AWS Resources.



**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

**Region**  
Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

Asia Pacific (Mumbai) ▼

**Name**

WEB-ACL-2265

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-ACL-2265

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

**Associated AWS resources - optional (1)** Remove Add AWS resources

🔍 Find associated AWS resources < 1 > ⚙️

	Name	Resource type	Region
<input type="radio"/>	ALB-WAF-2265	Application Load Balancer	Asia Pacific (Mumbai)

Cancel Next

- Add Rules → AWS managed rules

**School of Computer Science, Engineering and Applications (SCSEA)**

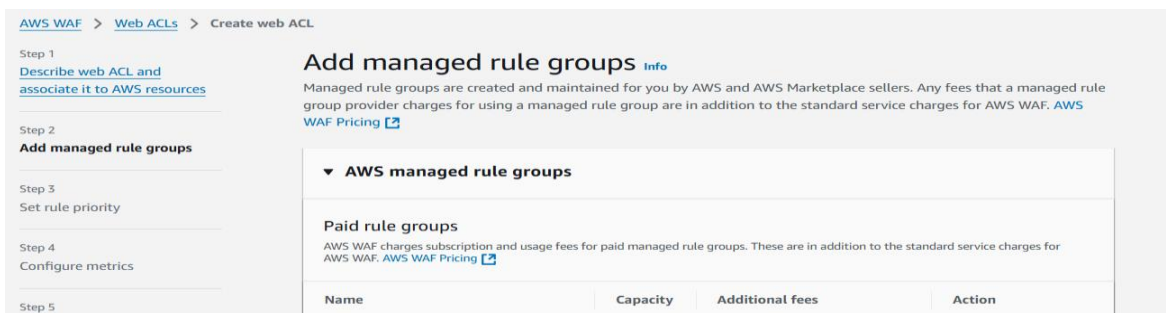
**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**



AWS WAF > Web ACLs > Create web ACL

Step 1  
[Describe web ACL and associate it to AWS resources](#)

Step 2  
**Add managed rule groups**

Step 3  
Set rule priority

Step 4  
Configure metrics

Step 5

### Add managed rule groups [info](#)

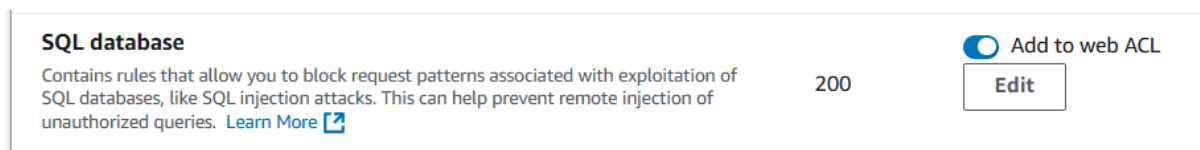
Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers. Any fees that a managed rule group provider charges for using a managed rule group are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

**▼ AWS managed rule groups**

**Paid rule groups**  
AWS WAF charges subscription and usage fees for paid managed rule groups. These are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

Name	Capacity	Additional fees	Action
------	----------	-----------------	--------

- AWS managed rules group → SQL Database → Add Rule



**SQL database**

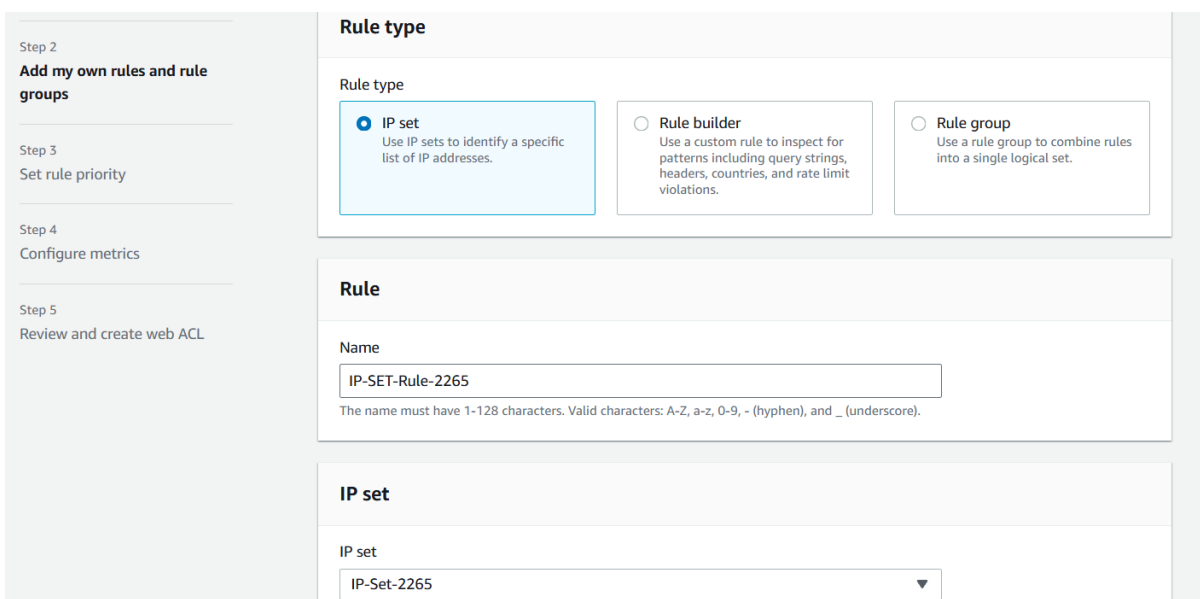
Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. [Learn More](#)

200

☒ Add to web ACL

[Edit](#)

- Add Rules → Add my own rules and own groups.
- Rule type: IP Set → Add Your IP Set → Action: Block → Add Rule



Step 2  
**Add my own rules and rule groups**

Step 3  
Set rule priority

Step 4  
Configure metrics

Step 5  
Review and create web ACL

### 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

IP-SET-Rule-2265

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

**IP set**

IP set

IP-Set-2265

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

- Again, your own rules → Rule builder → Assign name:  
'GeoLocationBlockRule2265' → Type: Regular Rule → Set : If a request – 'doesn't match the statement (NOT)'.

**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 builder**

[Rule visual editor](#)[Rule JSON editor](#)

You can use the JSON editor for complex statement nesting, for example to nest two OR statements inside an AND statement. The visual editor handles one level of nesting. For web ACLs and rule groups with complex nesting, the visual editor is disabled.

**Rule**

[Validate](#)

**Name**

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

**Type**

☒ **Regular rule**

☐ **Rate-based rule**  
Limits request rates for requests that match your criteria. Applies the action to matching requests when the limit is reached, and removes the action when the rate falls below the limit.

- Under Statement – Inspect – Select 'Originates from a country in' – Country codes – Select 'India IN'.
- This will block all geo-locations except India → Add rule

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

**If a request** doesn't match the statement (NOT) ▼

**Statement**

Inspect

Originates from a country in ▼

Country codes

Choose country codes ▼

India - IN ✕

IP address to use to determine the country of origin

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

- Add Another Rule - Rule builder → Rule name: QueryStringRule2265.
- Set : If a request – ‘matches the statement’.
- Under Statement – Inspect – Select ‘Query string’ – Match Type – Select ‘Contains string’ – Strings to match – Type ‘admin’. – Add Rule.



**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

**If a request** matches the statement ▼

**Statement**

Inspect

Query string ▼

Match type

Contains string ▼

String to match

admin

Text transformation

AWS WAF applies all transformations to the request before evaluating it. If multiple text transformations are added, then text transformations are applied in the order presented below with the top of the list being applied first.

None ▼

**Add text transformation**

You can add up to 10 text transformations.

- Block Access → next → next

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

Default action

☐ Allow

☒ Block

► Custom response - *optional*

- Next → Review and then Create Web ACL.

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

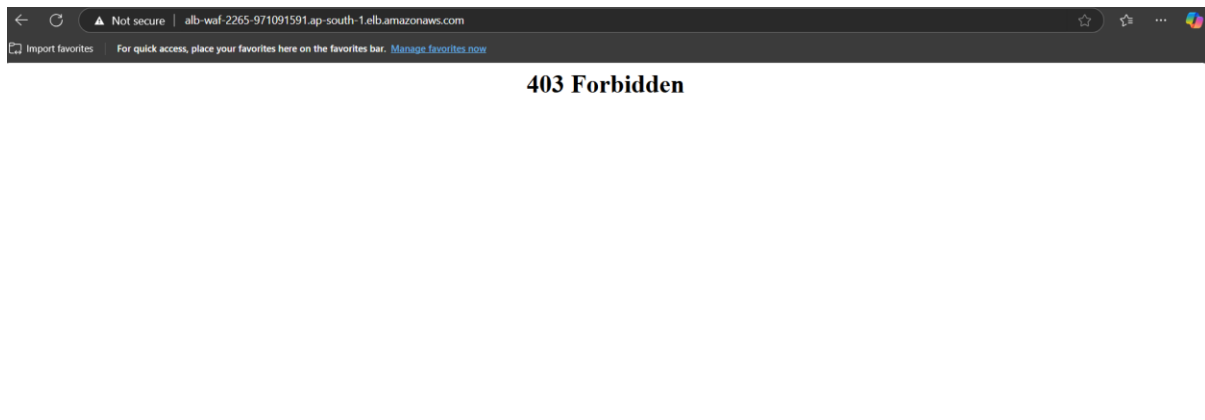
**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

**Step 5: Try to Access and validate your WAF.**

- Go to Load Balancer → Select your LB → Copy DNS
- Paste it in new tab.



- Now Access it Via your phone or laptop whose IP you have added in IP set → if 403 Forbidden comes → WAF Implementation Successful.
- Access which is blocked by IP-SET.



- Query String restriction → Add this extension with your DNS: **/?admin=123456**





**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

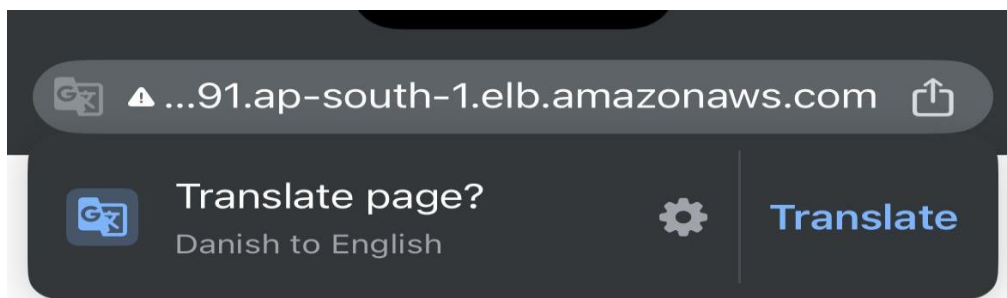
**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 8. Enterprise-Grade Web Traffic Blocking:  
Configuring AWS WAF for Dynamic Threat  
Protection.**

- VPN Access from outside India



- For SQL Injection use this extension after your DNS:  
**/product?item=securitynumber+OR+1- -**



**Now, start the deletion process:**

- Web ACL → Open → Dissociate LB → Delete rules.
- Delete WAF & IP-SET.
- Delete Load Balancer.
- Delete Target Group.
- Terminate EC2 Instances & Delete SG.