

**Cloud Computing Architecture Lab**

**Name:** Pratham Kandari

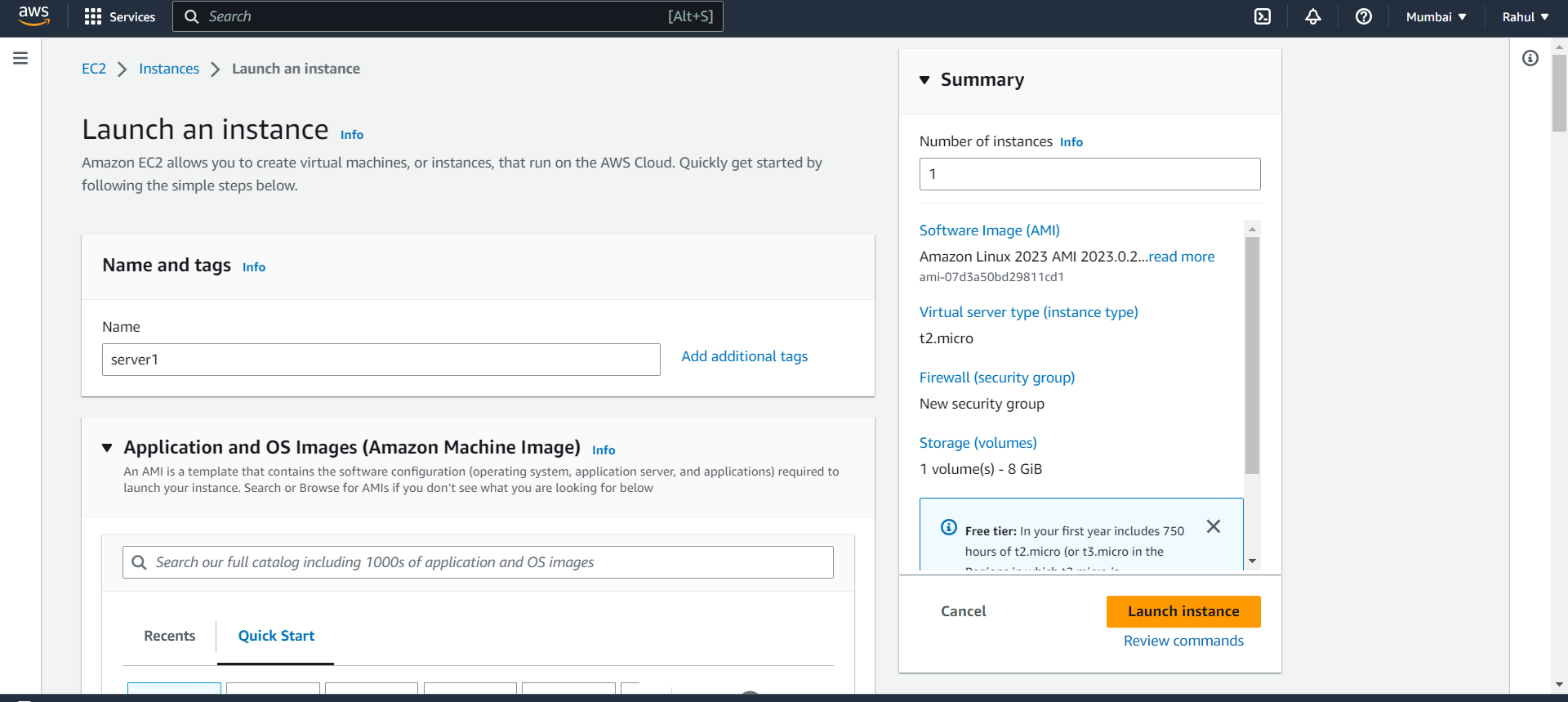
**Sap Id:** 500097663

**Batch:** 7

**Experiment -13**

# AWS Web Application Firewall (WAF)

Step 1) First we have to create two instances.



Step 2) Select Linux OS.



Step 3) And paste this script under advanced -> user data.

#!/bin/bash

sudo su

yum update -y

yum install -y httpd

systemctl start httpd.service

systemctl enable httpd.service

echo "<h1> At $(hostname -f) </h1>" > /var/www/html/index.html

Graphical user interface, application

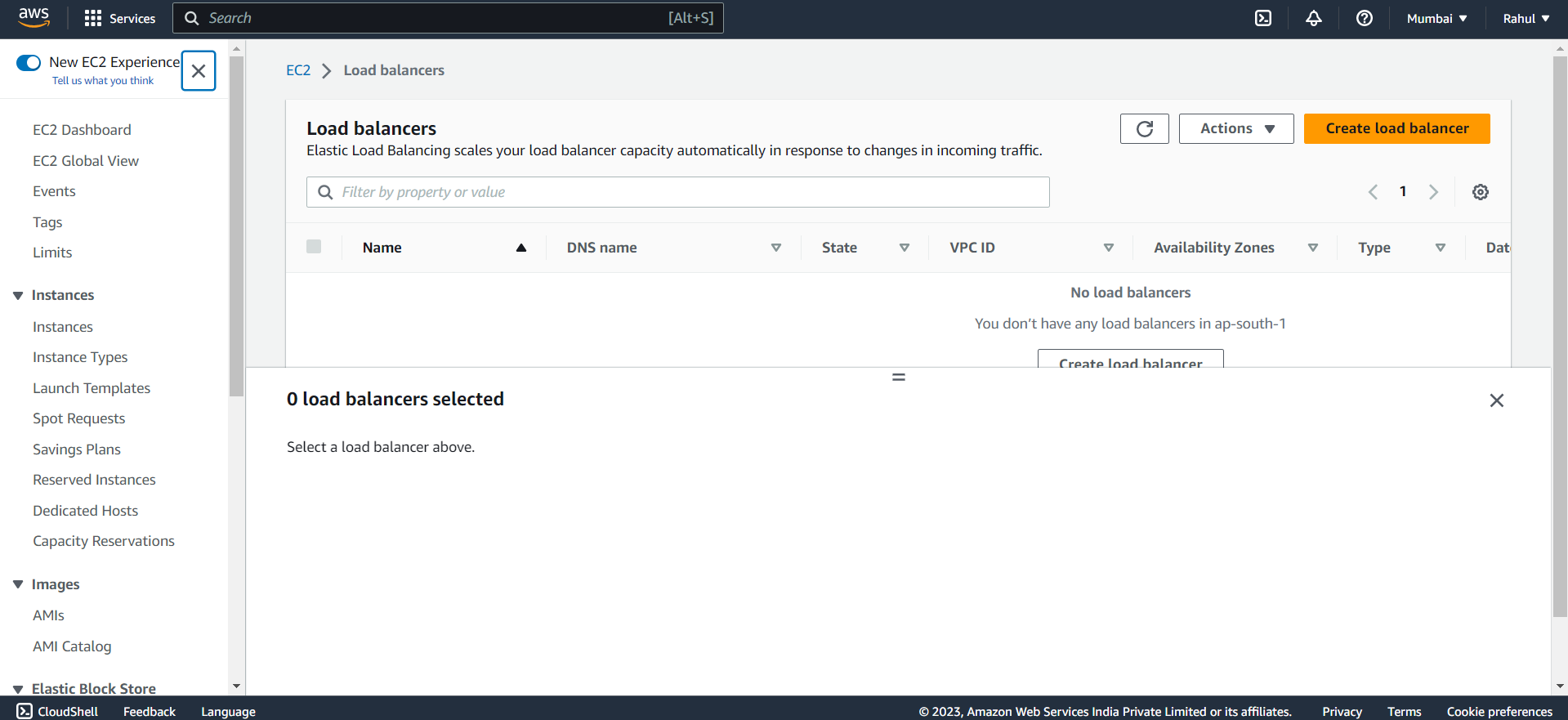
Description automatically generated

Step 4) Your two instances are ready.

Graphical user interface, application, Word

Description automatically generated

Step 5) Go to Load Balancers and create Load Balancer.



Step 6) Select Application Load Balancer.

A picture containing graphical user interface

Description automatically generated

Step 7) Give it a name, Scheme -> Internet facing , Ip address type -> IPv4.

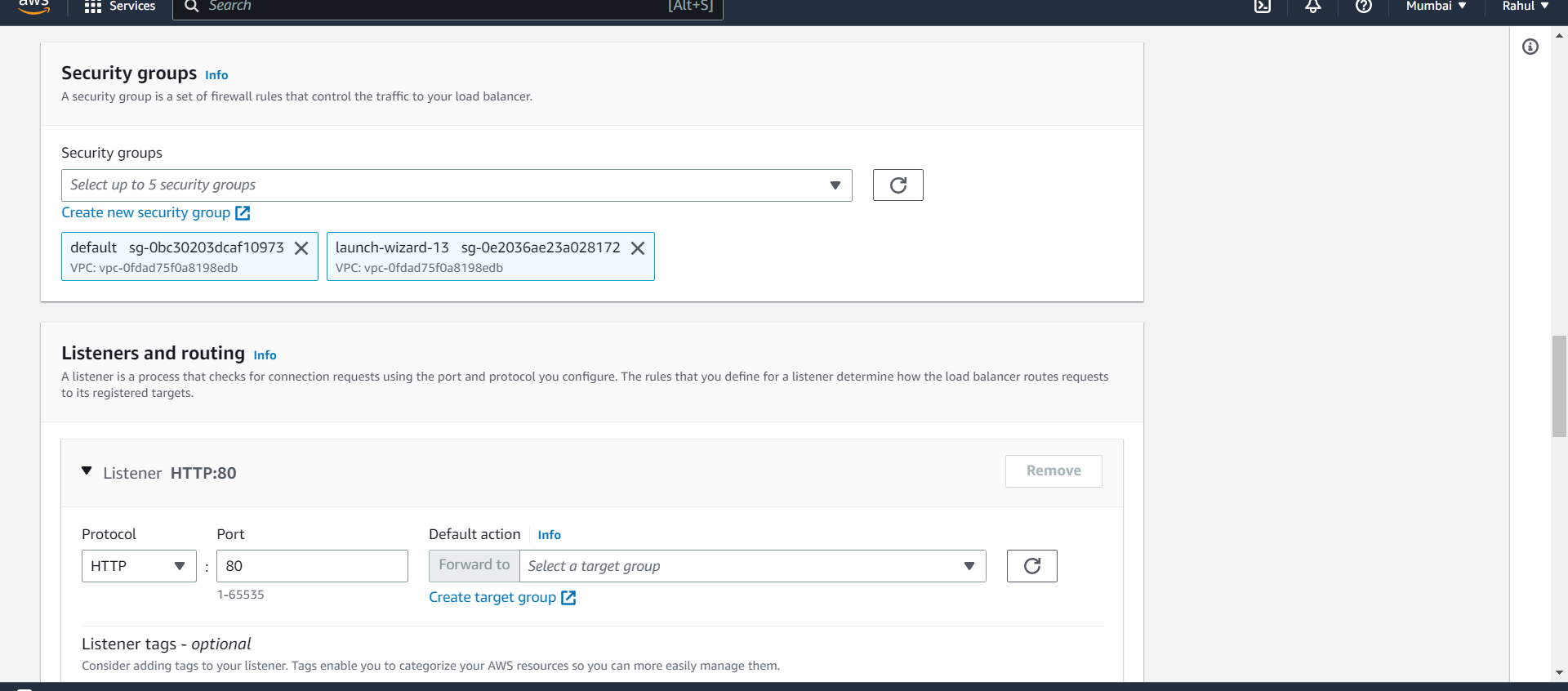
Graphical user interface, application

Description automatically generated

Step 8) Under Network Mapping let VPC be default, and select all three Availability zones and subnets.Graphical user interface, text, application

Description automatically generated

Step 9) Under security groups add the security group used in your instance.



Step 10) Now go to Create target groups and select instances.Graphical user interface, text, application

Description automatically generated

Step 11) Protocol as HTTP and give it a name.

Graphical user interface, application, Teams

Description automatically generated

Step 12) Select both instances and click on include as pending below. Graphical user interface, text, application

Description automatically generated

Step 13) Now target group is created.

A screenshot of a computer

Description automatically generated

Step 14) Come back to Load balancer and under Listeners and routing add your target groups.Graphical user interface, application

Description automatically generated

Step 15) And then create your Load Balancer.

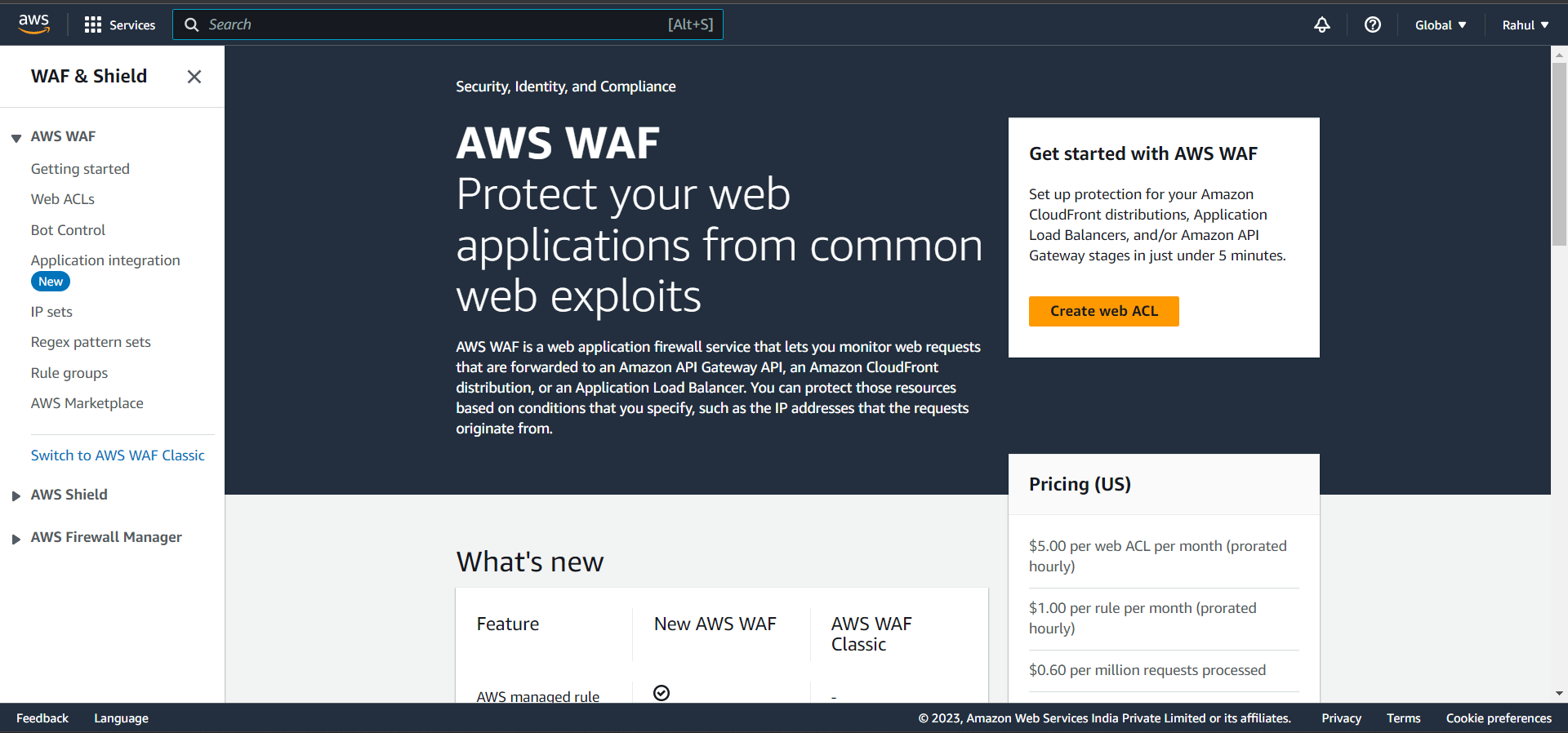
Graphical user interface, text, application

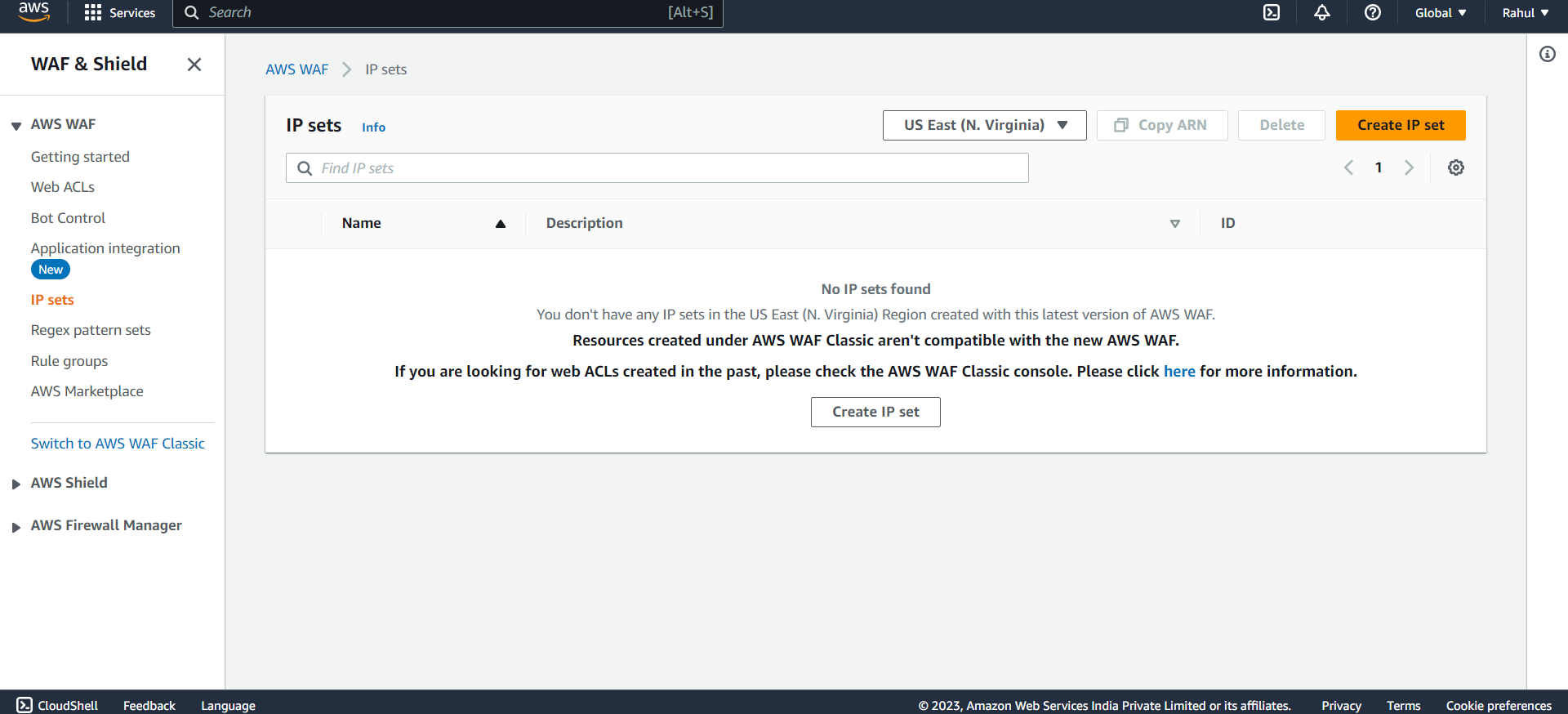
Description automatically generated

Step 16) Load balancer created.Graphical user interface, text, application, email

Description automatically generated

Step 17) Now go to WAF and click on IP sets.

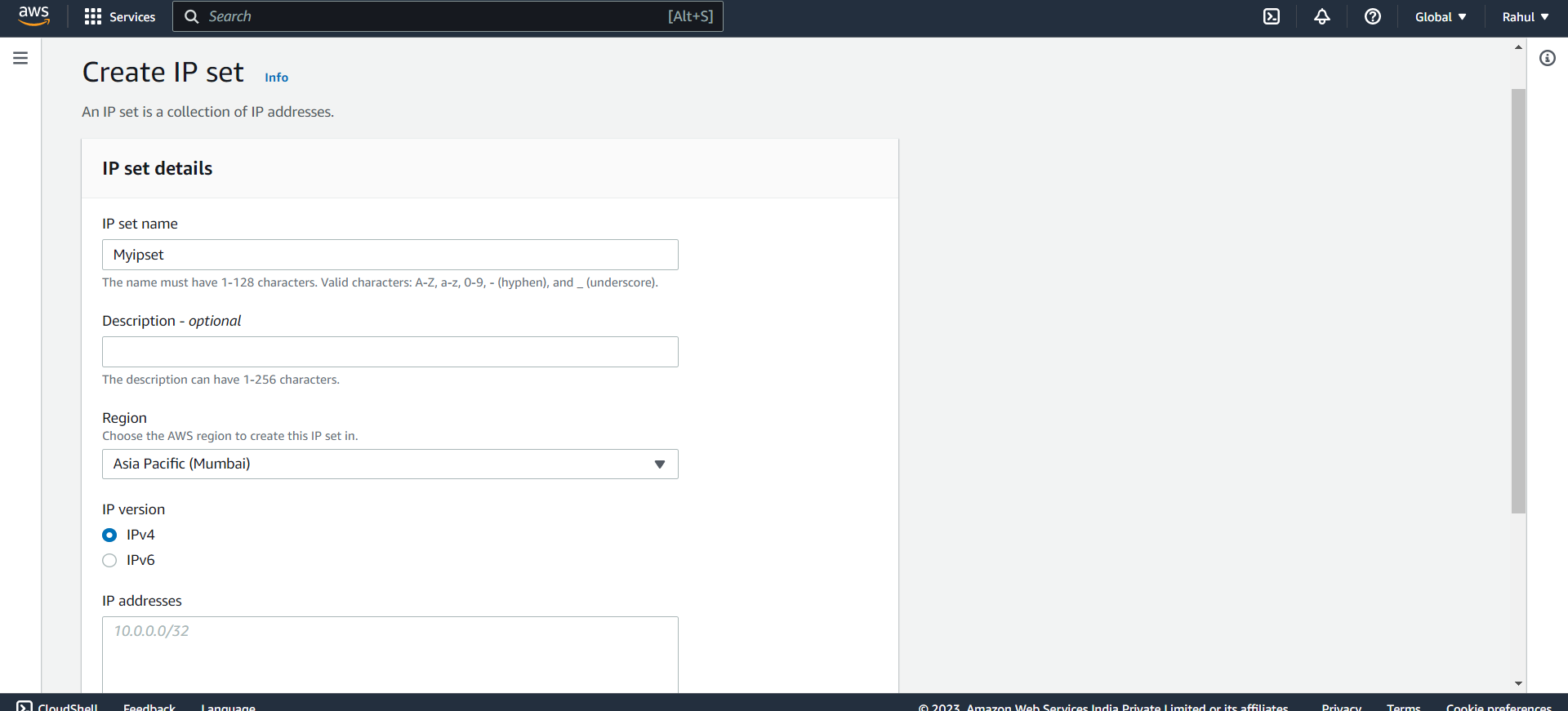


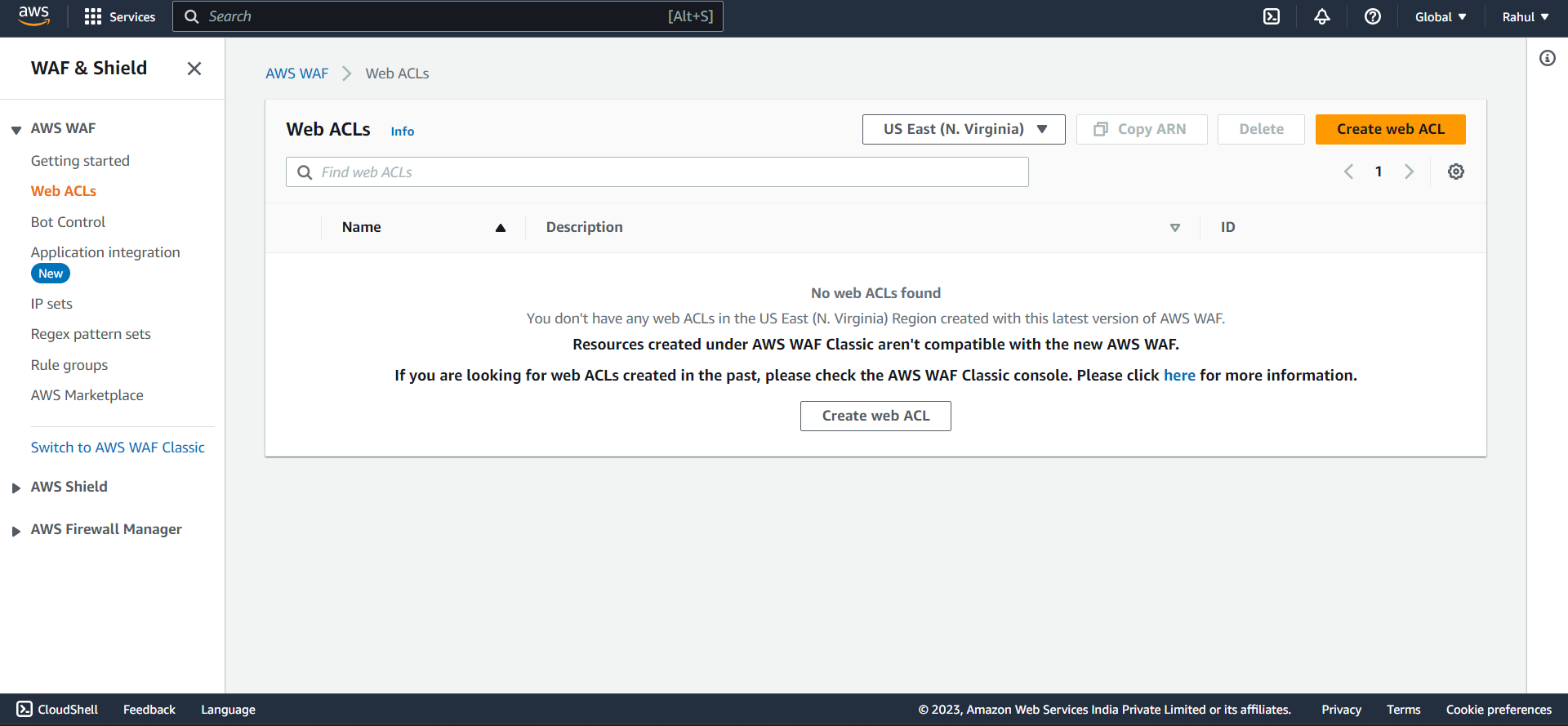
Step 18) Create IP set.

Step 19) Give it a name and paste your Ip address.

(your IP can be found by going to this website

https://whatismyipaddress.com/ )

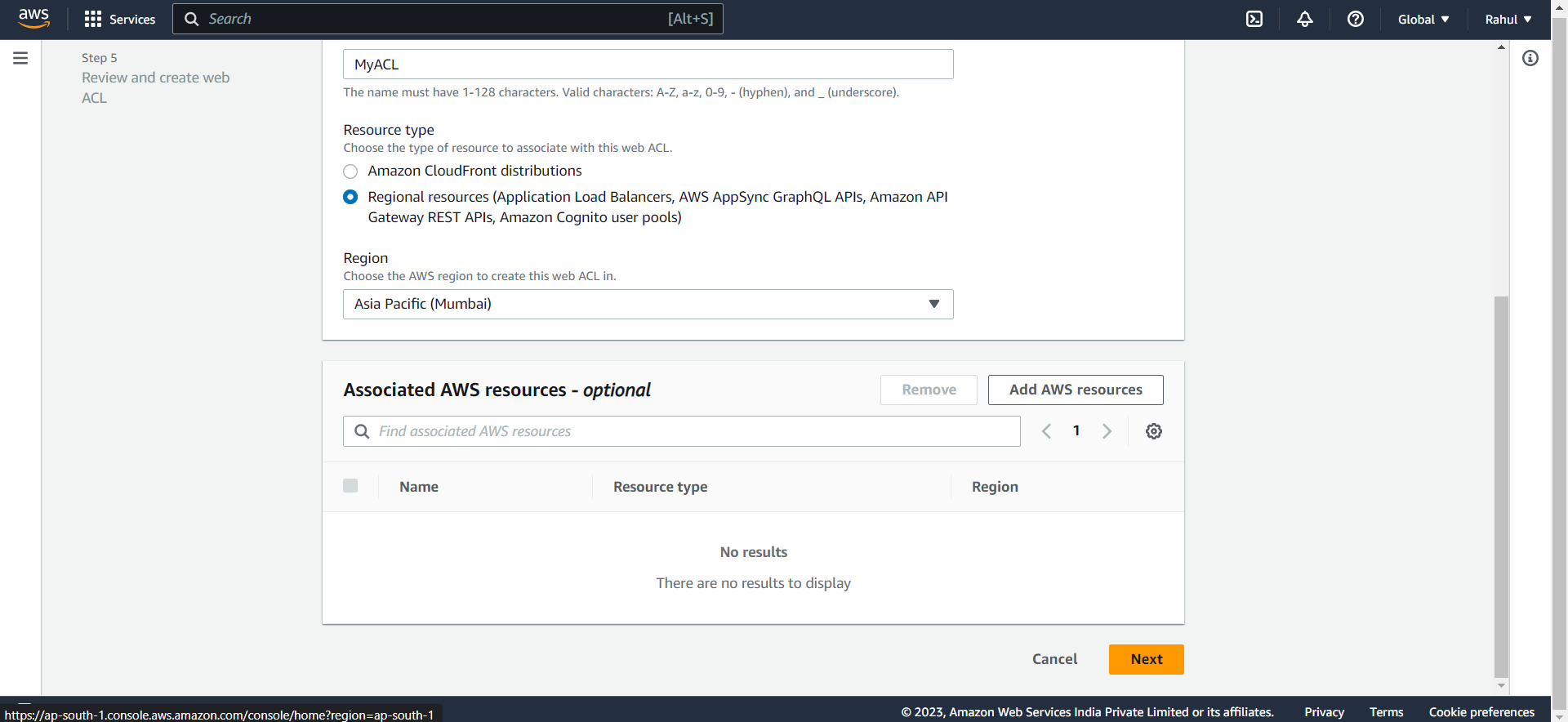


Step 20) Now go to Web ACLs and click on create web ACL.

Step 21) Give it a name, select resource type -> Regional resource and Region -> Asia pacific Mumbai.

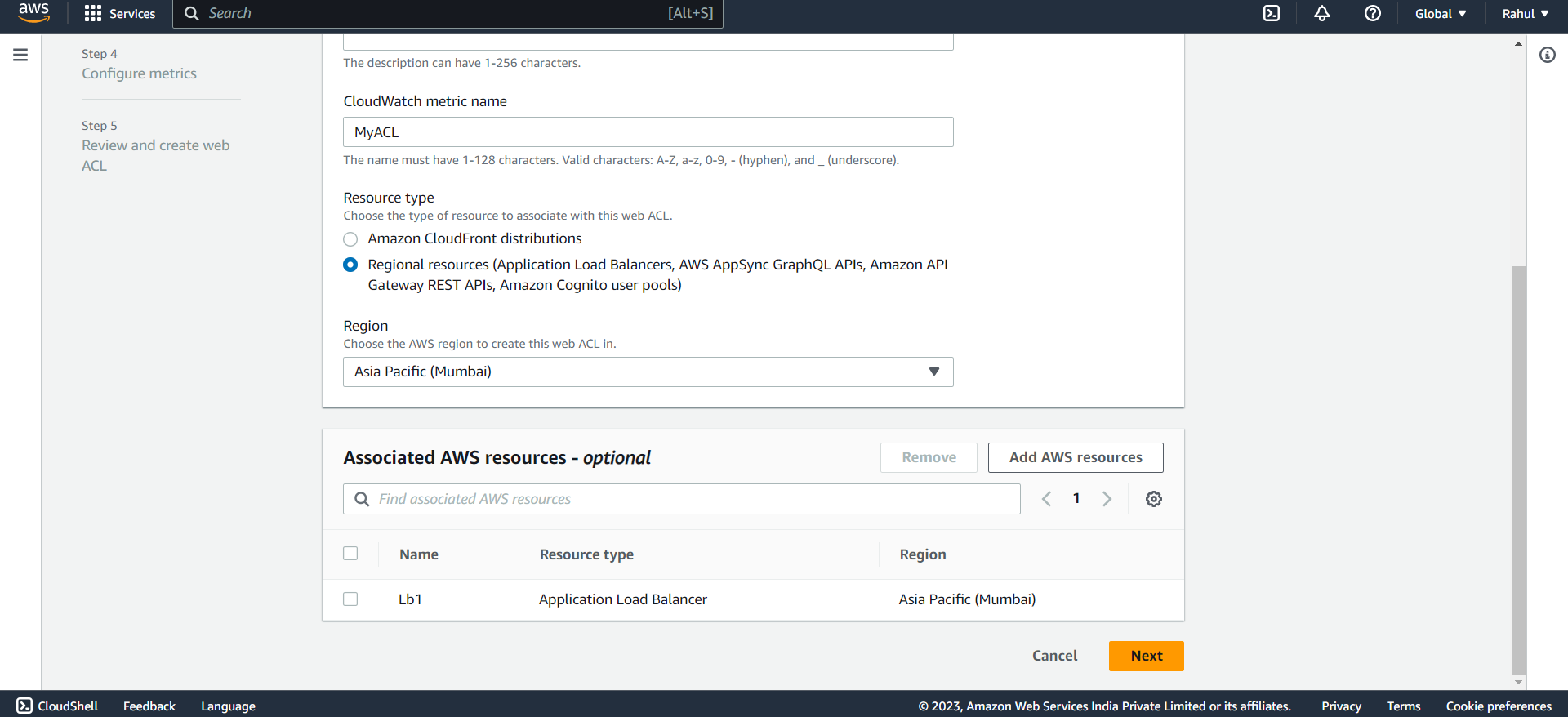
A screenshot of a computer

Description automatically generated

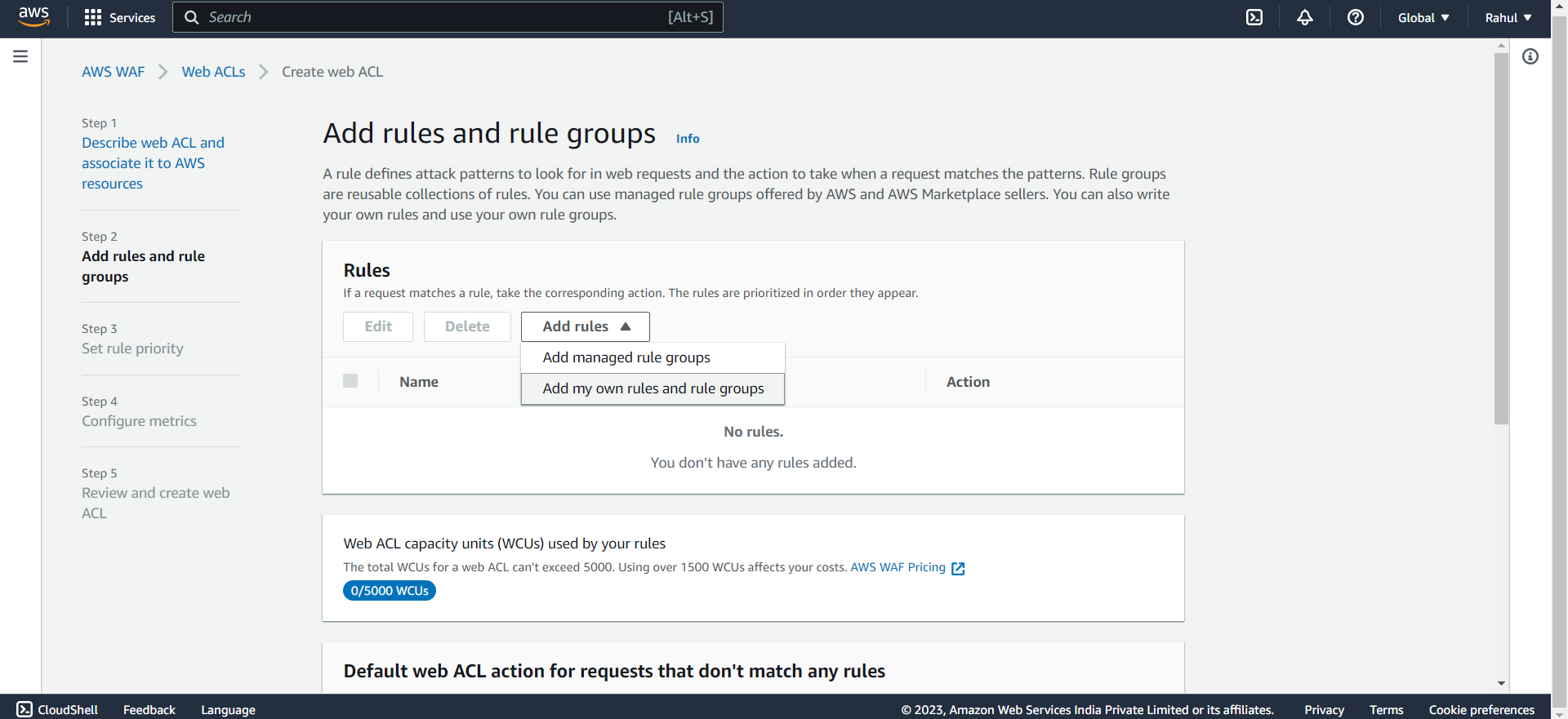
Step 22) Now click on Add resources.

Step 23) Select Application Load Balancer and select your Load balancer created before.Graphical user interface, application

Description automatically generated

Step 24) After adding click on nect.

Step 25) Under rules click on Add rules -> Add my own rules and rule groups.



Step 26) Select rule type -> IP set.A screenshot of a computer

Description automatically generated

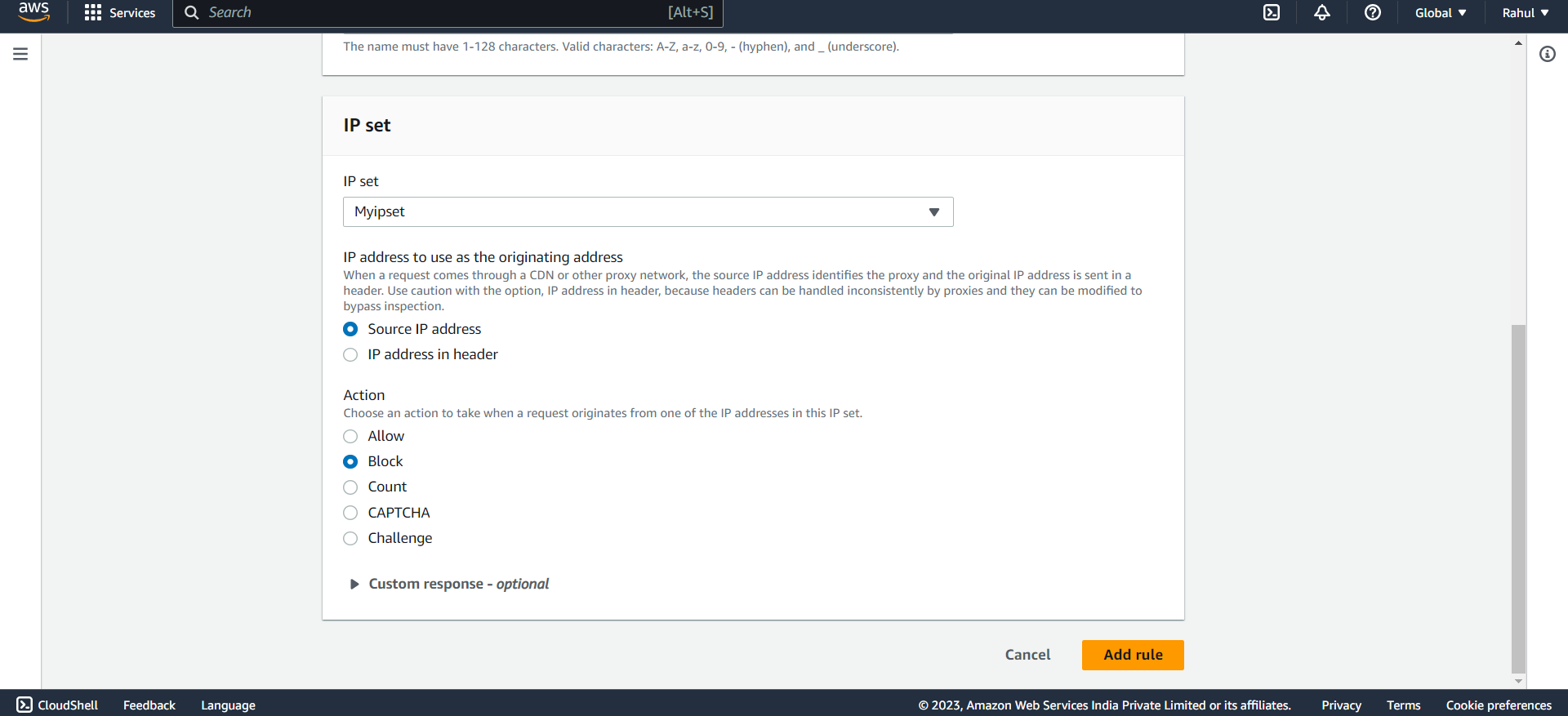
Step 27) Give it a name and select your Ip set created before.

Select

IP address to use as the originating address -> Source IP address.

Action -> Block

And click on Add Rule.



Step 28) Rule will be added.A screenshot of a computer

Description automatically generated

Step 29) Under Default web ACL action for requests that don't match any rules

Select Allow.

Graphical user interface, text, application, email

Description automatically generated

Select 30) Under Set Rule priority click on next.Graphical user interface, application

Description automatically generated

Step 31) Under Configure metrics let everything be default and click on next.

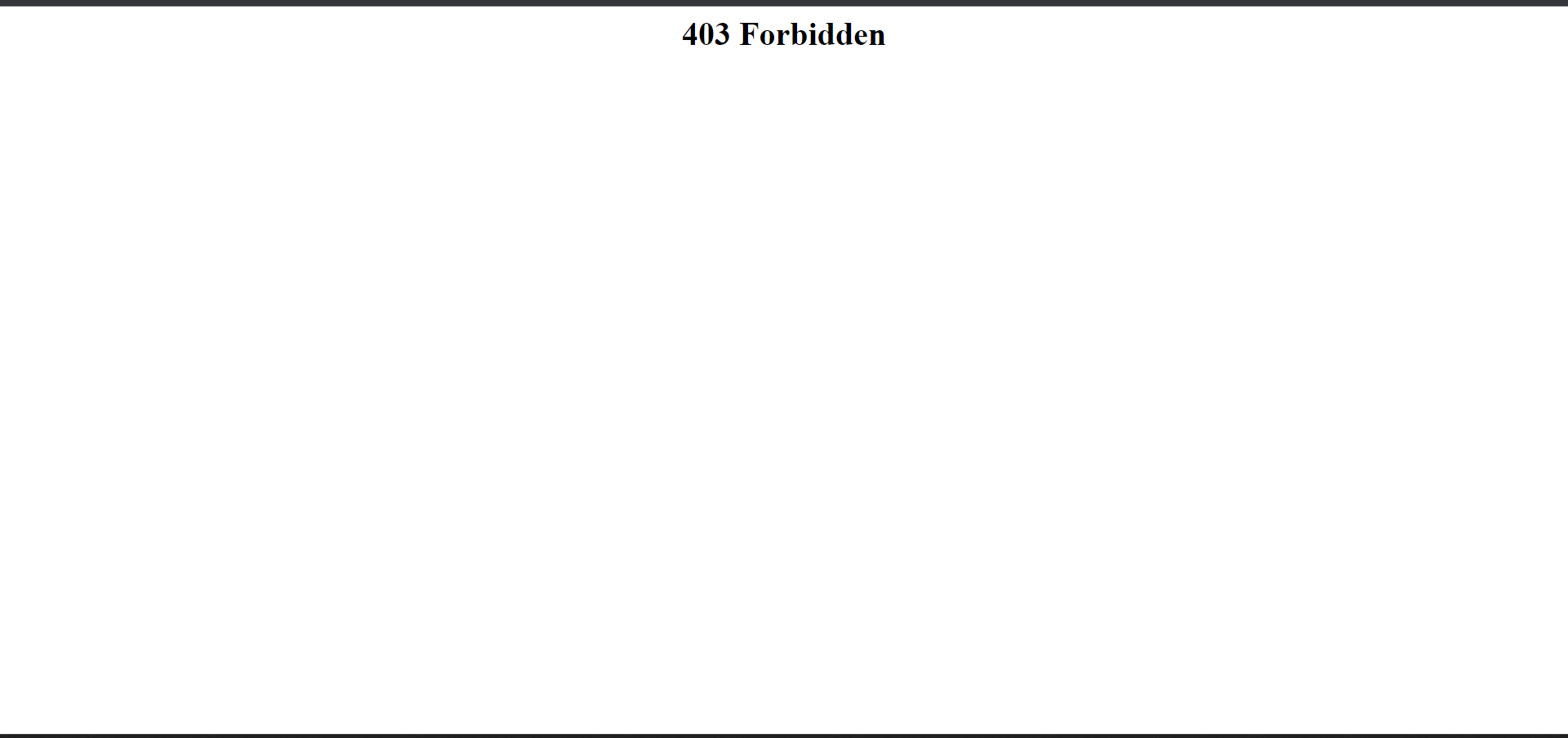
A screenshot of a computer

Description automatically generated

Step 32) Review and create web ACL.Graphical user interface, text, application

Description automatically generated

Step 33) After pasting the DNS of the load Balancer on the browser and we can see that our IP is banned.



Step 34) Now go back to the WebACL created and Add one more rule.

Graphical user interface, text, application, email

Description automatically generated

Step 35) Select IP set.Graphical user interface, text, application

Description automatically generated

Step 36)

Select

IP address to use as the originating address -> Source IP address.

Action -> Allow

And click on Add Rule.

Graphical user interface, text, application

Description automatically generated

Step 37) Now under rule priority set the priority of the new rule above than previous rule and save it.Graphical user interface, application

Description automatically generated

Step 38) Now again refresh the page and you can see that our IP is now unblocked and we are able to access the page.

A picture containing text

Description automatically generated