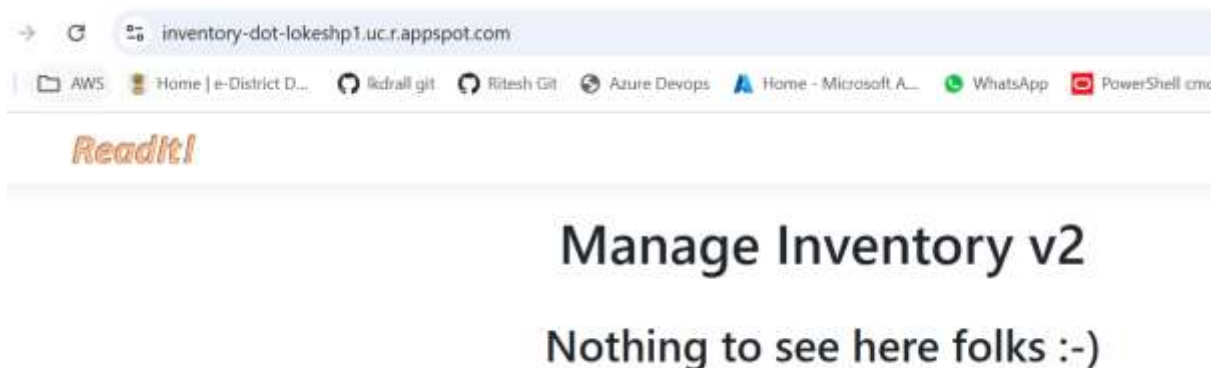
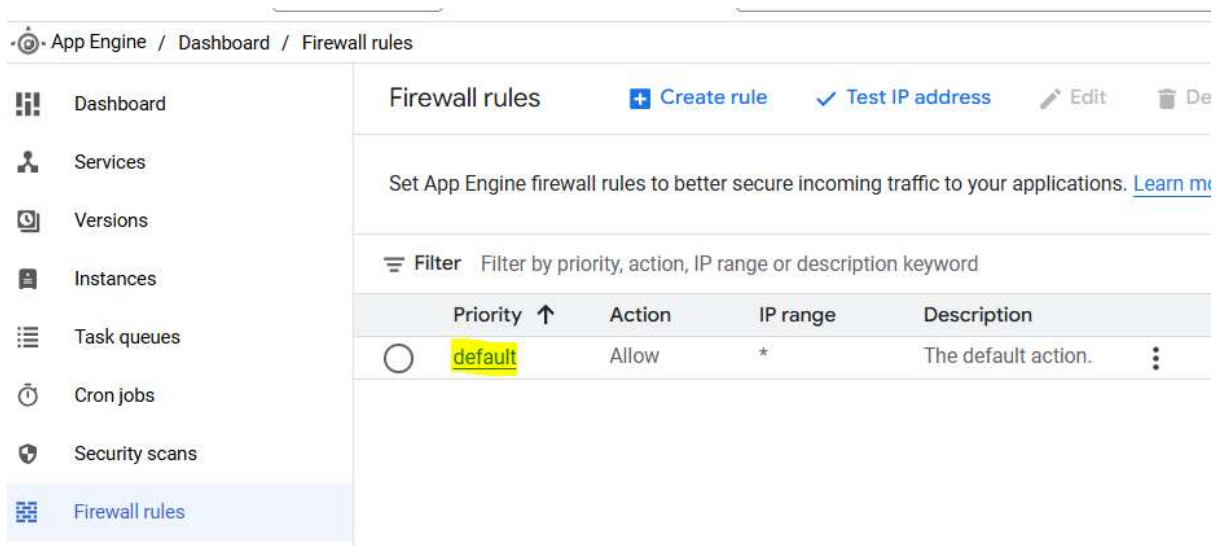


In this Lab, we will work on App Engine firewall configuration. We will see how we can block access from the whole internet to the App Engine service and how we can allow access to a specific IP address.

1. Go to App Engine on the GCP console, go to services, and try opening any of the services we created previously, like Inventory2 (it should open the webpage)



2. As of now, this service is accessible from the whole Internet
3. Now go to the Firewall rules page, where it will show a default rule already exists, which allows all traffic



4. Open the default rule, click Edit, and change it to Deny

←

Edit rule default

Priority

2147483647

?

Priority values are permanent.

[Check priority of existing firewall rules](#)

Action on match

☐ Allow

☒ Deny

IP range

*

?

Description

The default action.

19 / 100

Save

Cancel

5. Now, again, try to access the inventory service, it will give an error

←

→

↺

🔍

inventory-dot-lokeshp1.uc.r.appspot.com

🗑️

|

📁 AWS

🏠 Home | e-District D...

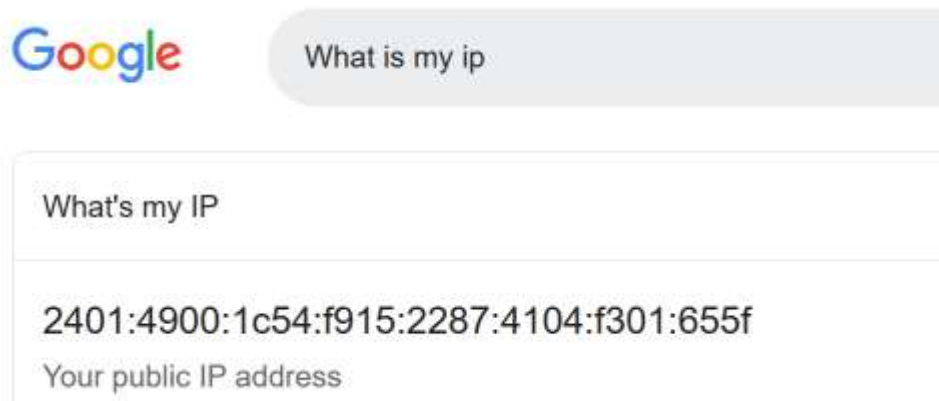
👤 lkdrall git

👤 Ritesh C

Error: Forbidden

Access is forbidden.

- Now go to Google and search What is my IP, and copy your public IP address (it may be IPv4 or IPv6)



Google

What is my ip

What's my IP

2401:4900:1c54:f915:2287:4104:f301:655f

Your public IP address

- Go to Firewall rules, click Test IP address, and paste your public IP, click Test
- It should show as denied

wall rules / Test IP address

← Test IP address

Test IP address *

2401:4900:1c54:f915:2287:4104:f301:655f

Enter an IP address to find the highest priority rule that matches.

Test Clear

⚠ IP denied

Matching rule (highest priority)

Priority ↑	Action	IP range	Description
default	Deny	*	The default action.

- Now create a new rule for allowing your public IP address (make sure to give priority number shorter than the default rule as the shorter the number higher the priority)

← Create a firewall rule

Priority *
100



Priority values are permanent. [Check priority of existing firewall rules](#)

Action on match

☒ Allow

☐ Deny

IP range *

2401:4900:1c54:f915:2287:4104:f301:655f



Description



0 / 100

Save

Cancel

10. Then again, test your IP address, and this time it should show as allow. Note that, Default rule denies all traffic, but as the priority number of your IP address rule is shorter so means it has higher priority, so it will show as allow

← Test IP address

Test IP address *

2401:4900:1c54:f915:2287:4104:f301:655f

Enter an IP address to find the highest priority rule that matches.

Test

Clear



IP allowed

Matching rule (highest priority)

Priority ↑	Action	IP range	Desc
100	Allow	2401:4900:1c54:f915:2287:4104:f301:655f	

11. Now again try to access the inventory service and this will again work for you.
12. But if you will try accessing this service from some other pc or once your IP address is changed then it will not work as we have allowed it for that specific IP address
13. This is why we always prefer to use range or fixed IP addresses for the firewall rules.

