Task-4 Cybersecurity

Configure and test basic firewall rules to allow or block traffic

Report

1.Open firewall configuration tool (Windows Firewall or terminal for UFW)…….

2.List current firewall rules……

3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet)……

4.Test the rule by attempting to connect to that port locally or remotely……

5.Add rule to allow SSH (port 22) if on Linux……

6.Remove the test block rule to restore original state……

7.Document commands or GUI steps used……..

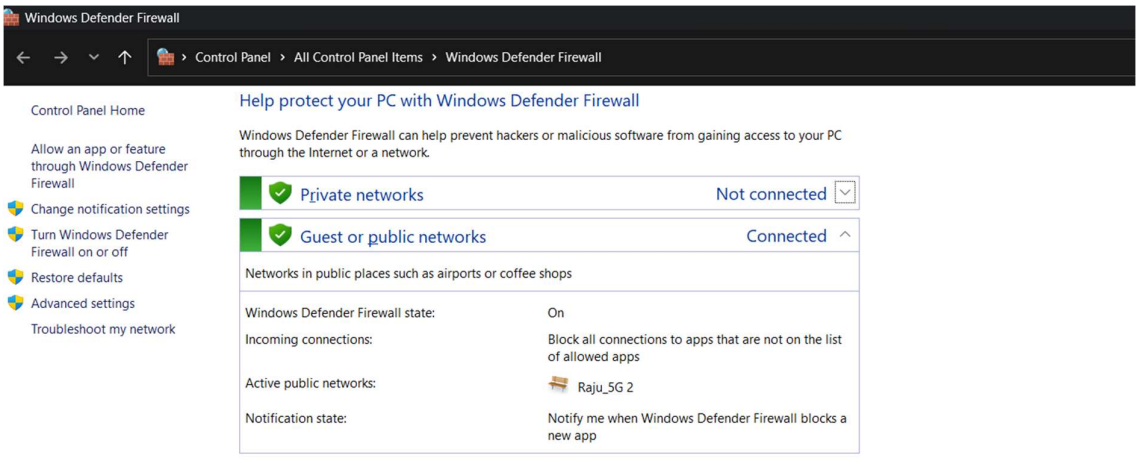
8.Summarize how firewall filters traffic……

1.Open firewall configuration tool (Windows Firewall or terminal for UFW)

Let’s check out the step’s to open the firewall setting

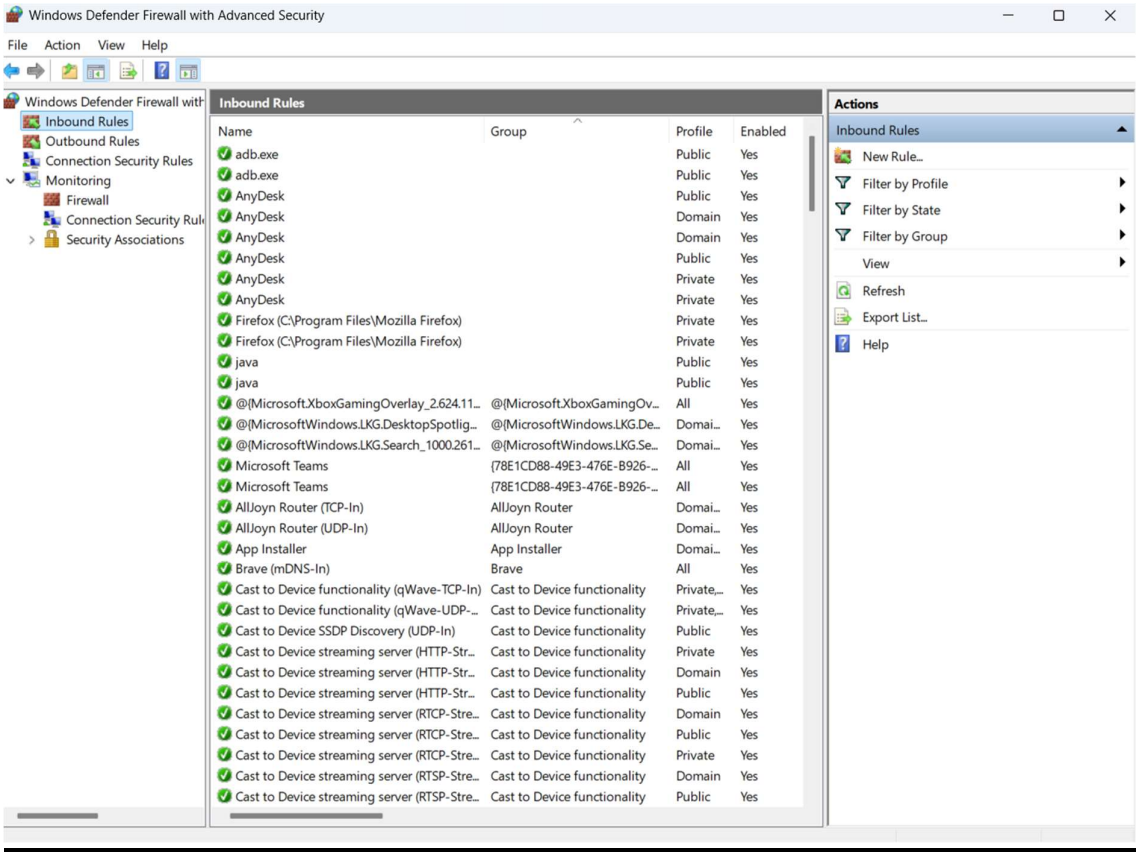
go to setting < search < windows defender firewall < open

Here is the screenshot for the windows firewall



2.List current firewall rules

Here is the screenshot of current firewall rule

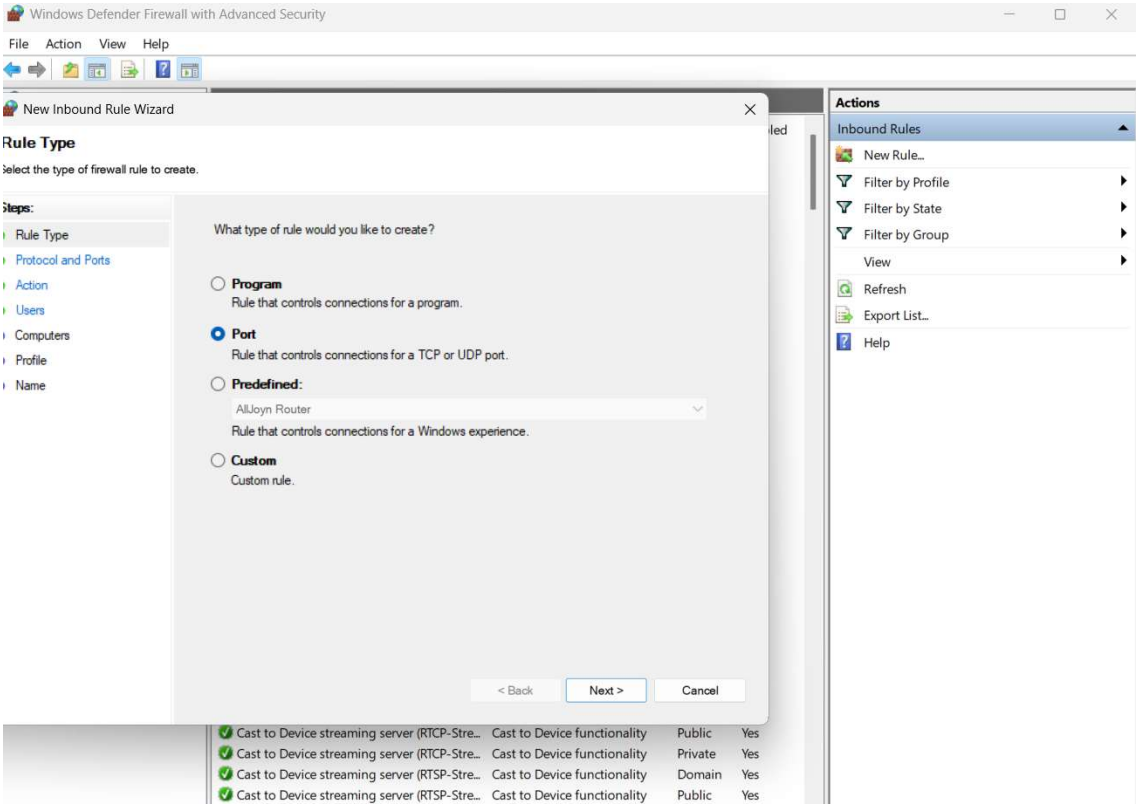


3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).

Steps to add inbound traffic in a specific port

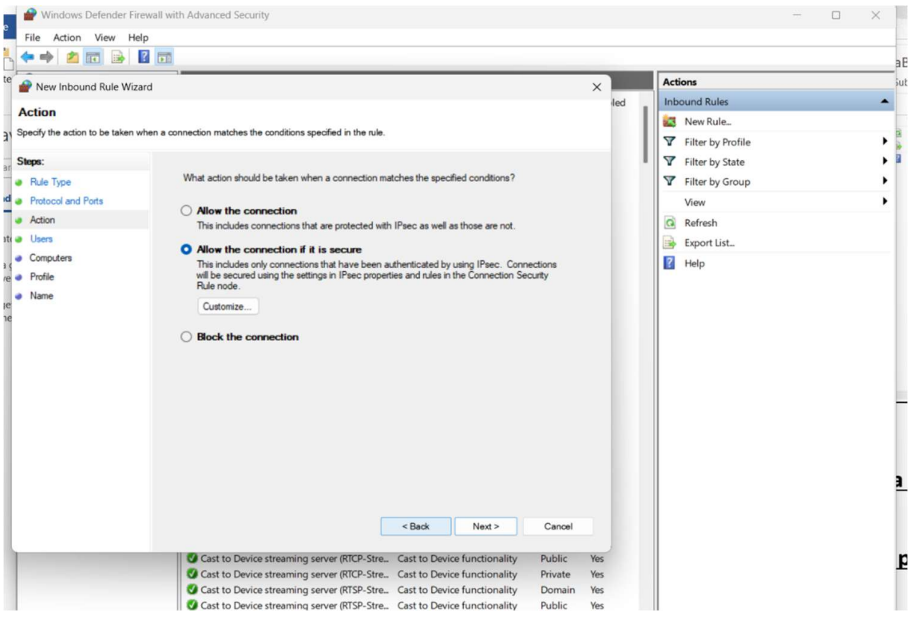
Step 1

So need to click on add Rules. Then we select “port” for rule type (as per the question)



Step 2

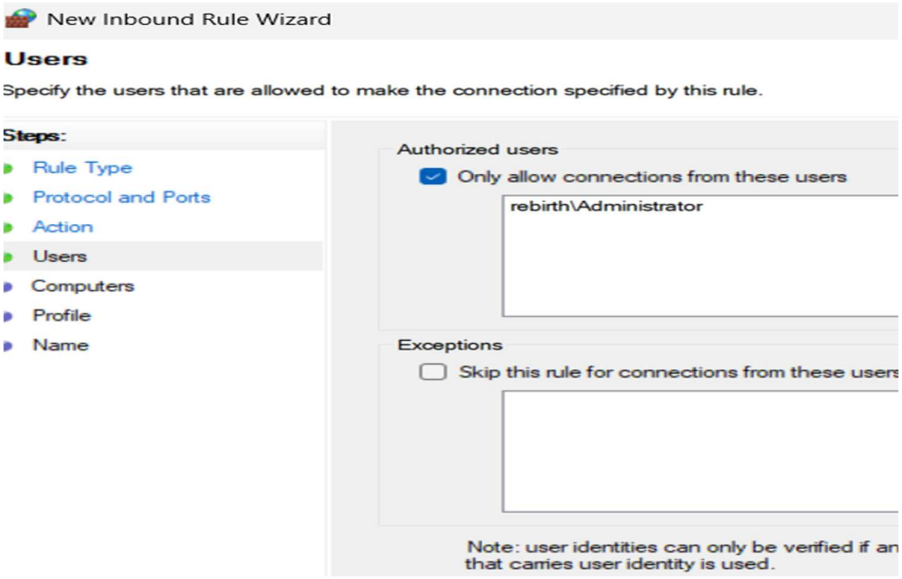
Then we need select action type what type of action we need to perform.



Step 3

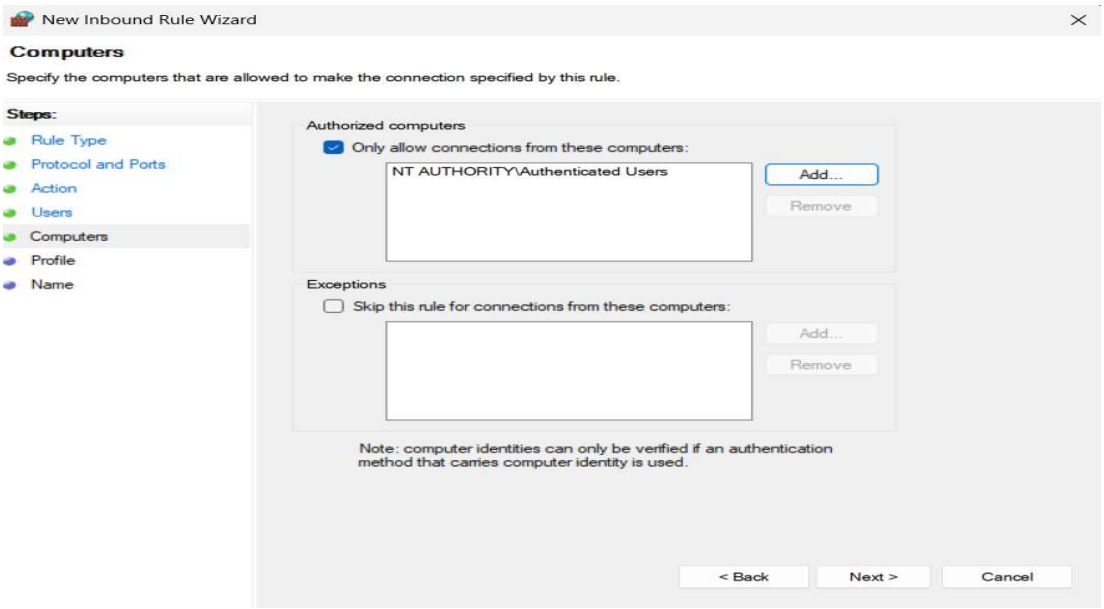
Select user type

It state that which user are to be allow according to the rule



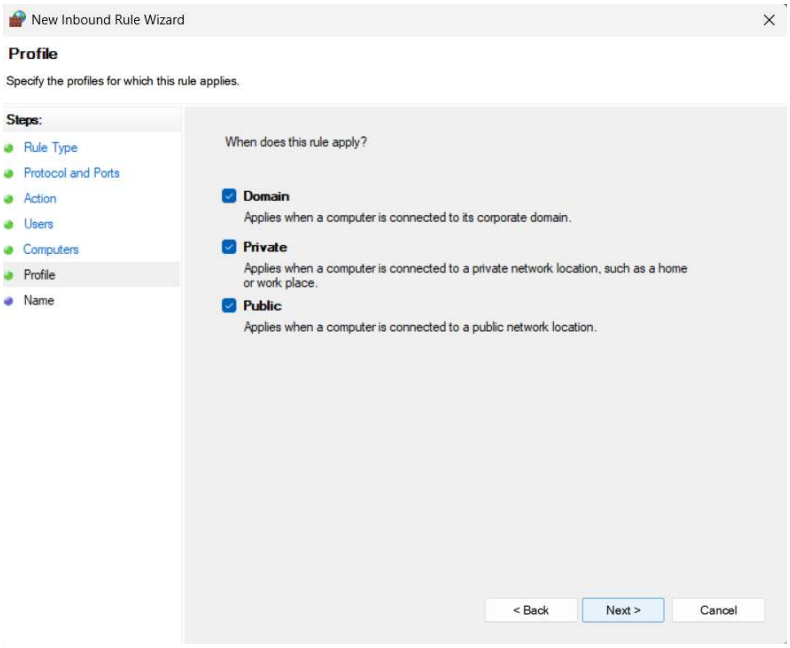
Step 4

Specify the computers that are allowed to make the connection by specified the rule.



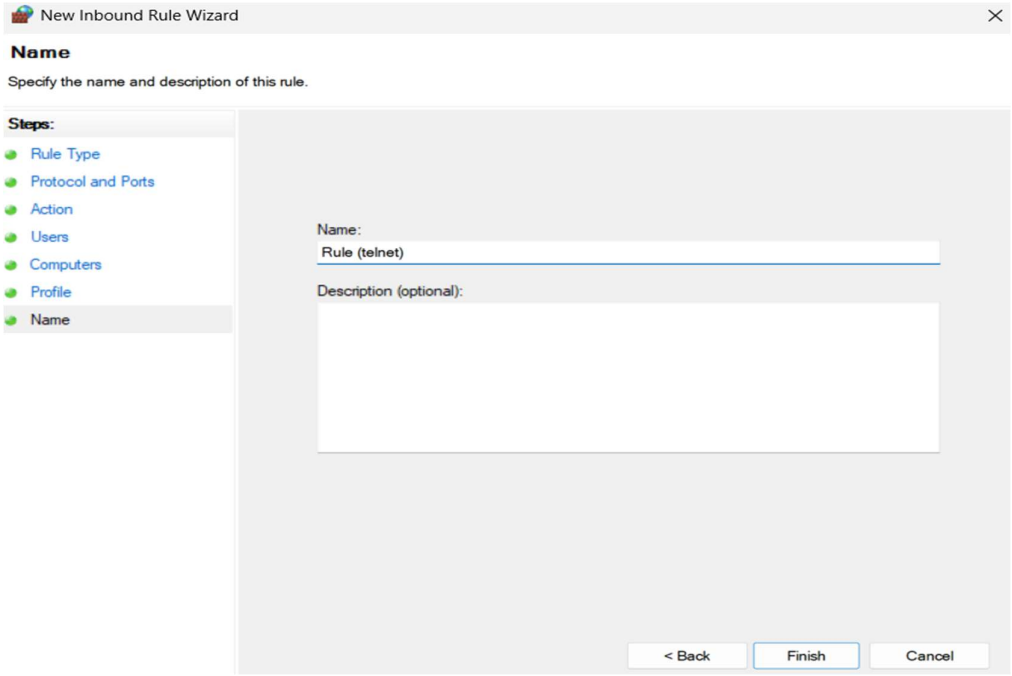
Step 5

In this step we need to specifie the profile for which the rules will apply.



Step 6

Specify the name and description of the rule

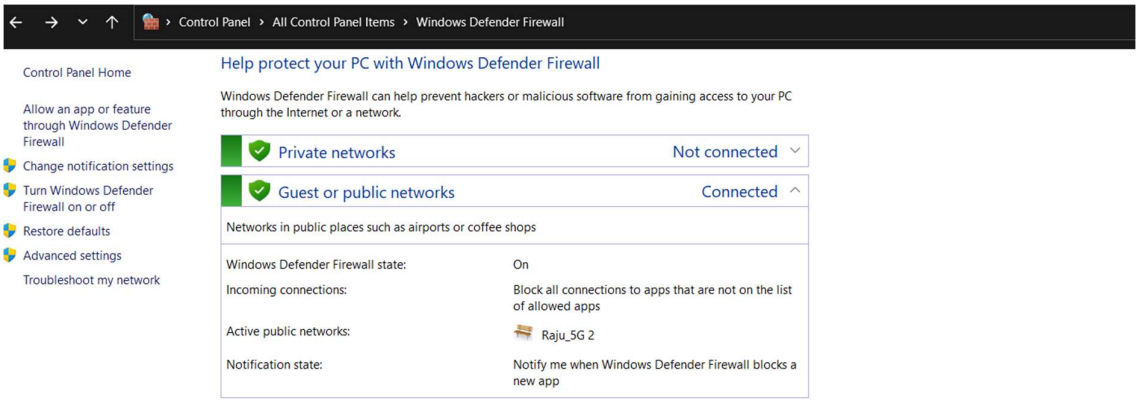


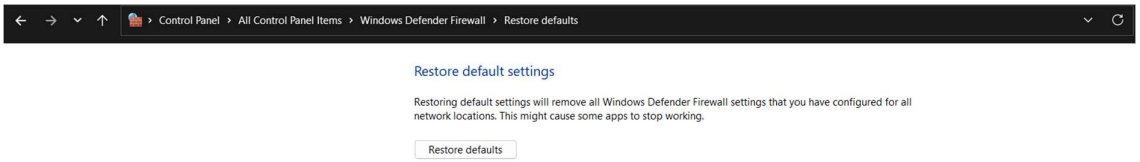
4.Test the rule by attempting to connect to that port locally or remotely.

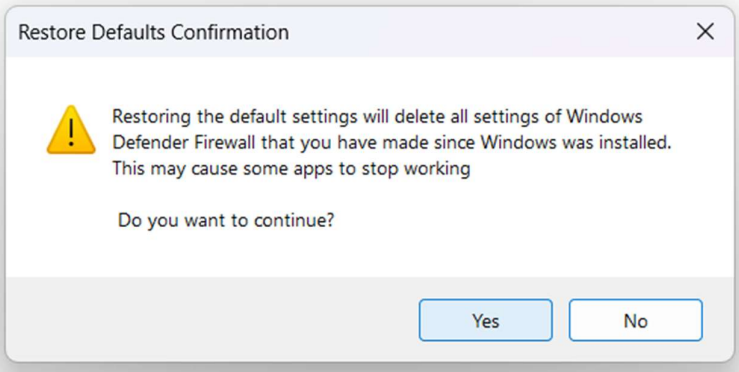
5.Add rule to alow SSH (port 22) if on Linux.

6.Remove the test block rule to restore original state.

Here is how we delete the rules from the firewall by restoring the changes







7.Document commands or GUI steps used.

The above are the steps that we will follow

8.Summarize how firewall filters traffic.

The firewall act as a security guard for our open ports when any services are trying to run in our system then it need to come throught the open ports so here the role of firewall take place it is a set of rule if the services which want to access the desired port for their work then they must satisfy the rules of the firewall or else the firewall will not allow the service to access the port.

It gives a extra layer of security our system.