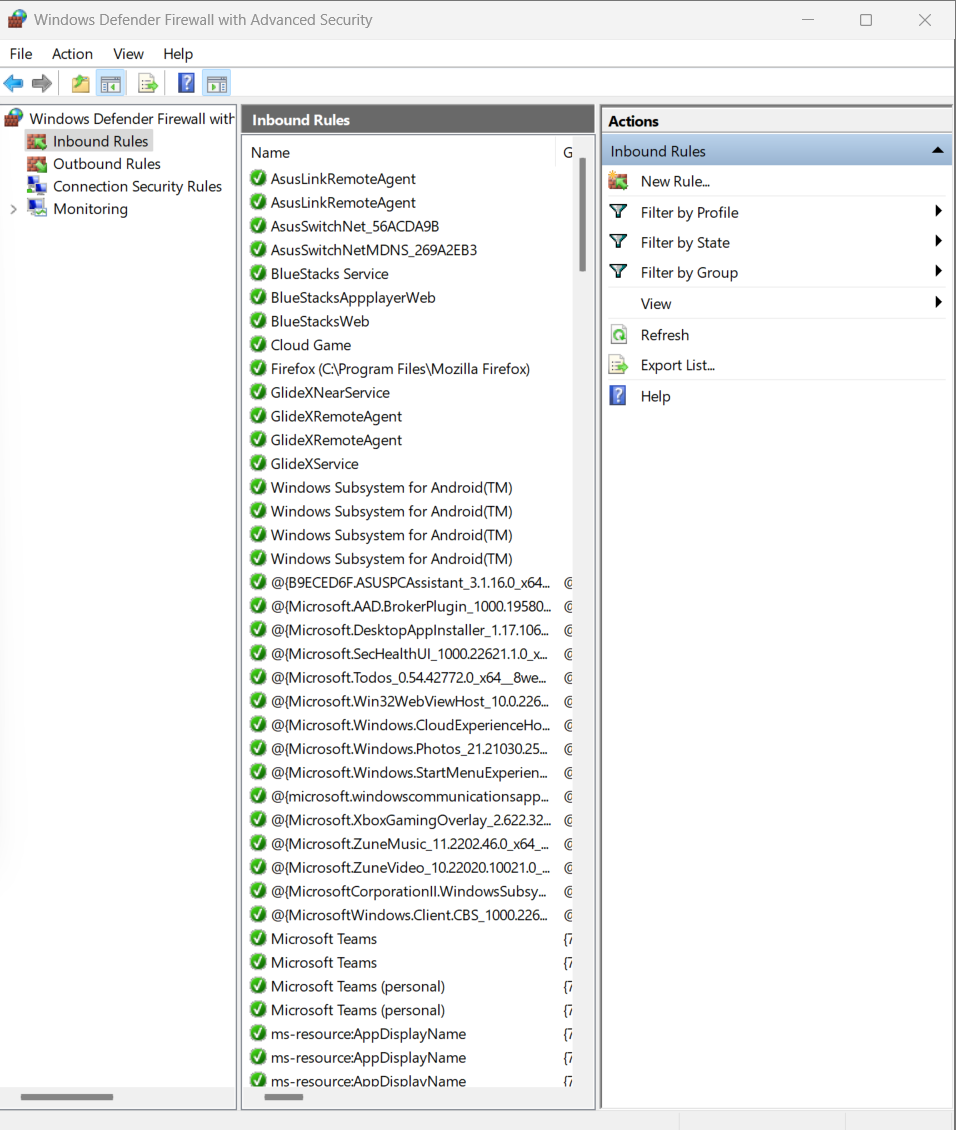
TASK 4

AIM:- Setup and Use a Firewall on Windows/Linux



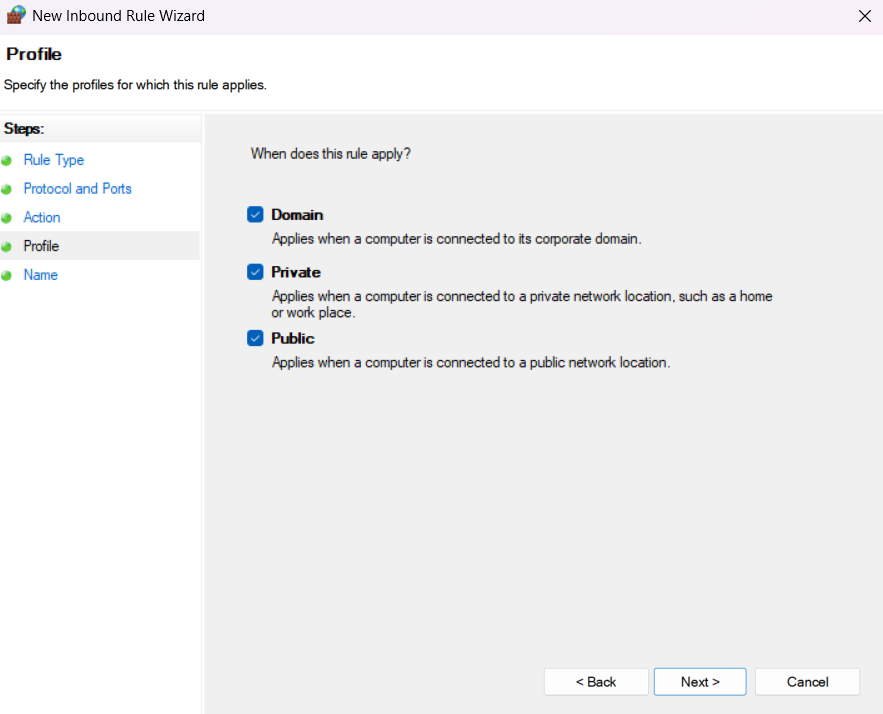
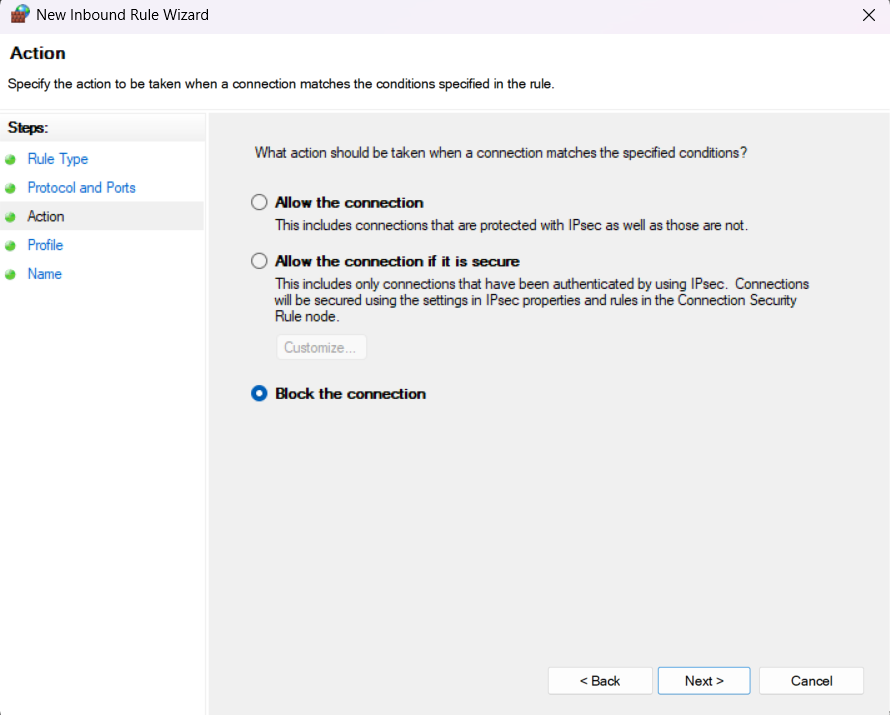
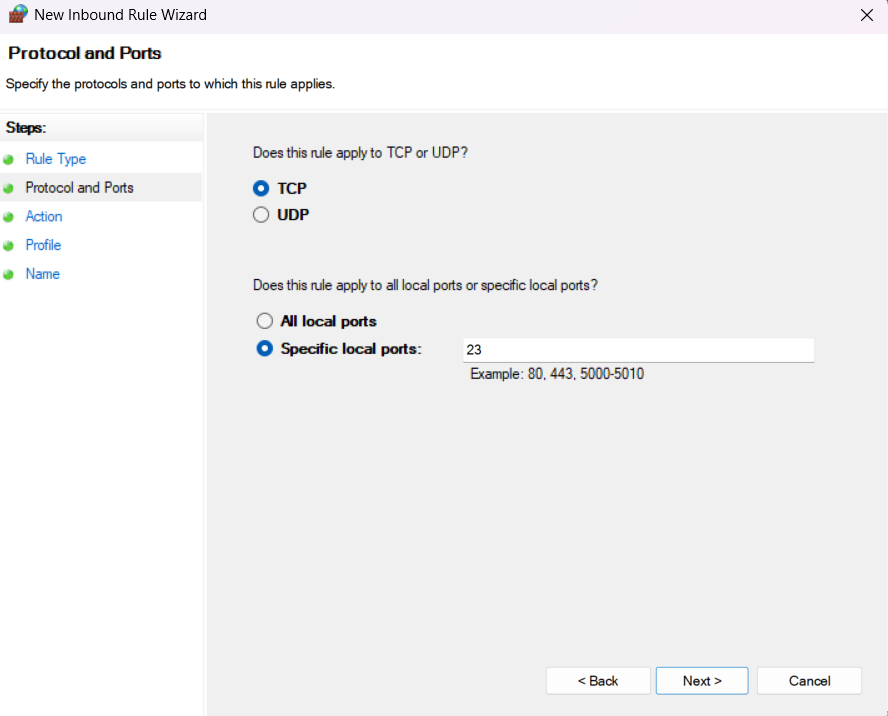
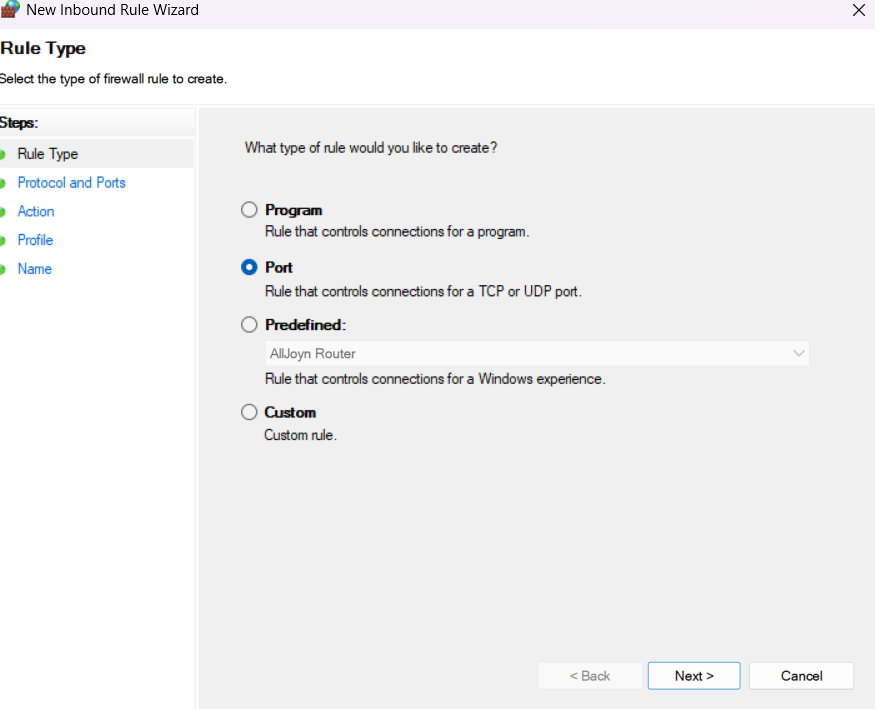
List current firewall rules.

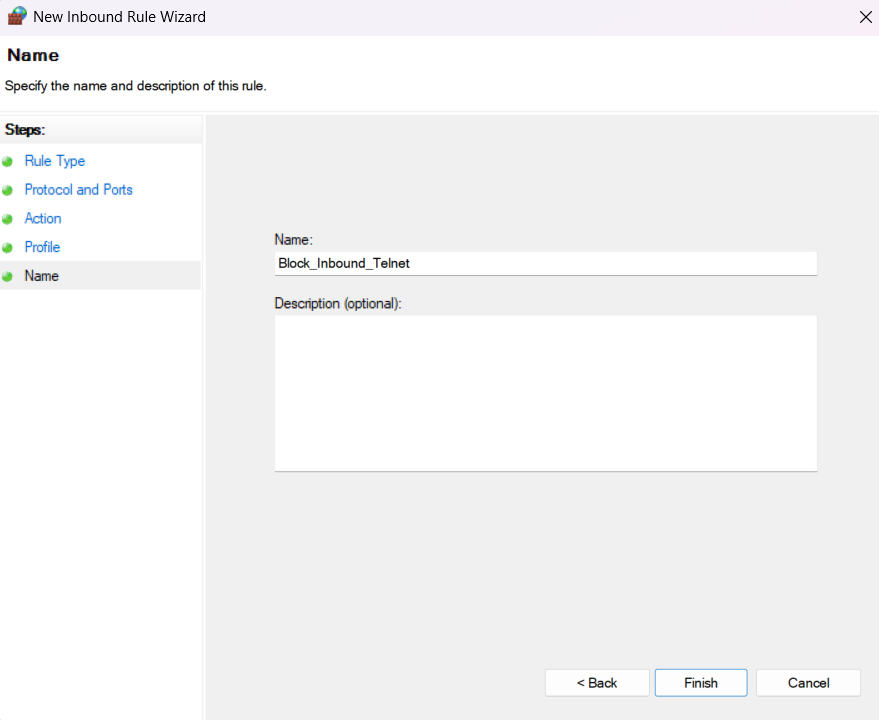
 Press Win+R, press **Enter**.

 In the left pane, select **Inbound Rules** or **Outbound Rules**.

 You'll see a list of all rules, including:

* Rule name
* Enabled/Disabled
* Action (Allow/Block)
* Profile (Domain, Private, Public)





HERE IS THE GUI STEPS USED TO BLOCK INBOUND RULE

Attempting to connect to that port locally .



COMMAND USED:-Test-NetConnection -ComputerName localhost -Port 23

IT LOOK Like blocked by **Windows Firewall**, or nothing is listening on that port

how firewall filters traffic.

A **firewall** filters traffic based on a set of rules that **allow or block network connections**. It acts as a **security gate** between your device/network and external sources.

**Traffic Direction**

* **Inbound traffic**: From the network → into your computer
* **Outbound traffic**: From your computer → out to the network

**Filtering Criteria**

Firewalls filter traffic based on:

| **Filter Type** | **Example** |
| --- | --- |
| IP Address | Block traffic from 192.168.1.5 |
| Port Number | Block TCP port 23 (Telnet) |
| Protocol | Allow only HTTP (TCP), block ICMP |
| Application | Block access for example.exe |
| Domain/Profiles | Rules apply on Private, Public, Domain networks |
| A firewall filters traffic by evaluating network packets against defined rules, determining whether to allow or block the traffic based on direction, port, IP, protocol, or application. |  |