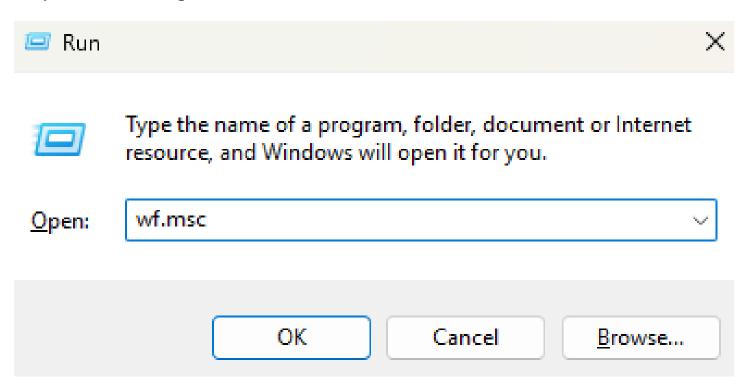
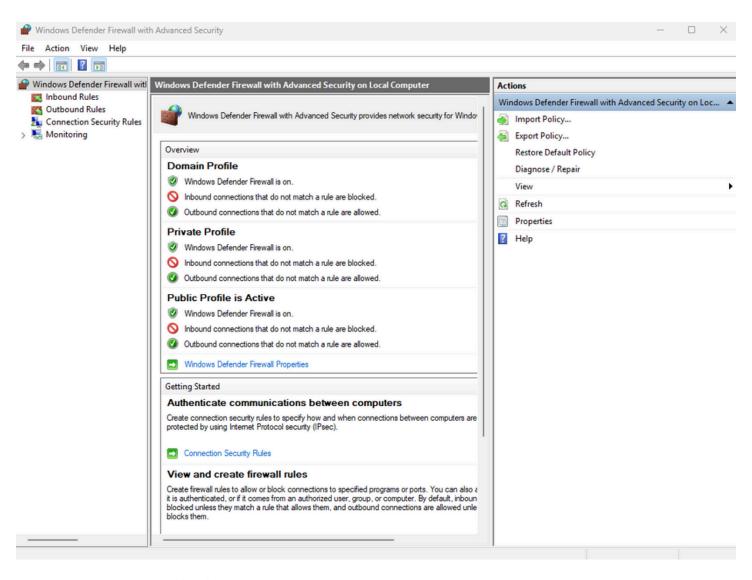
ELEVATE LABS CYBER SECURITY INTERNSHIP

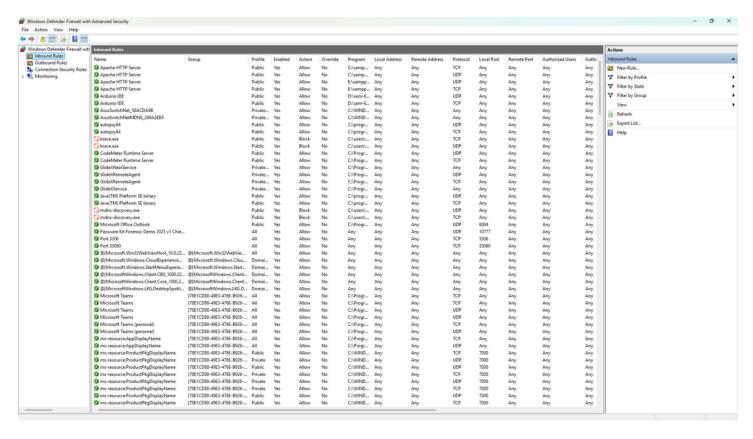
Task-4:

1. Open firewall configuration tool:





2.List current firewall rules.

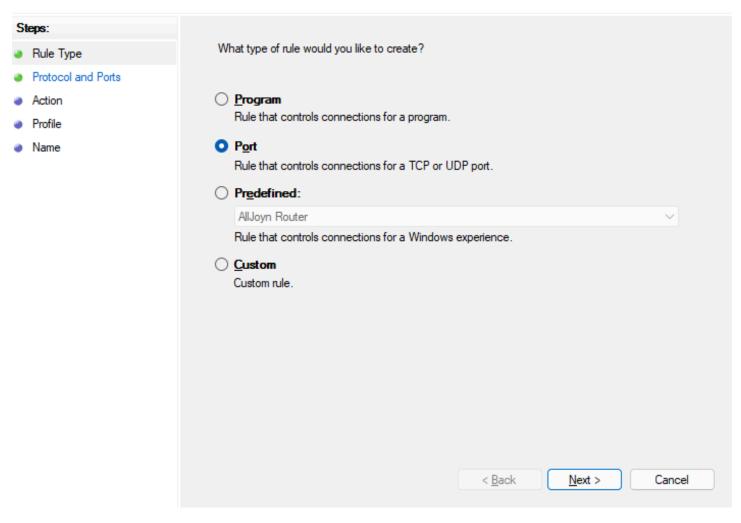


3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).



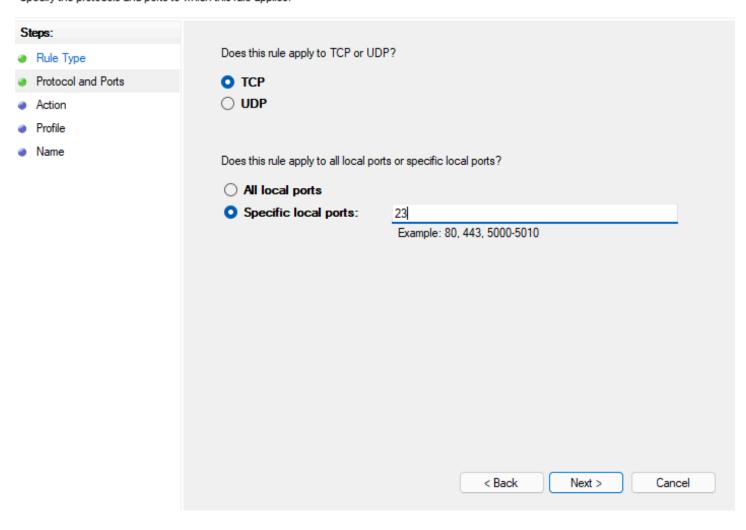
Rule Type

Select the type of firewall rule to create.



Protocol and Ports

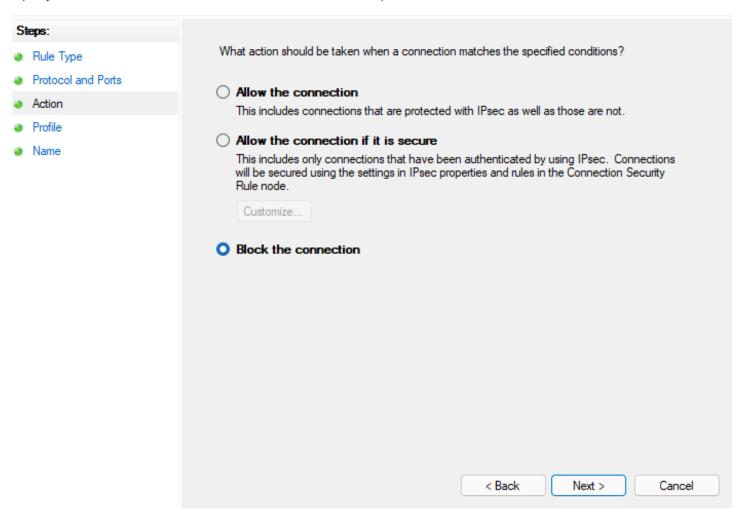
Specify the protocols and ports to which this rule applies.

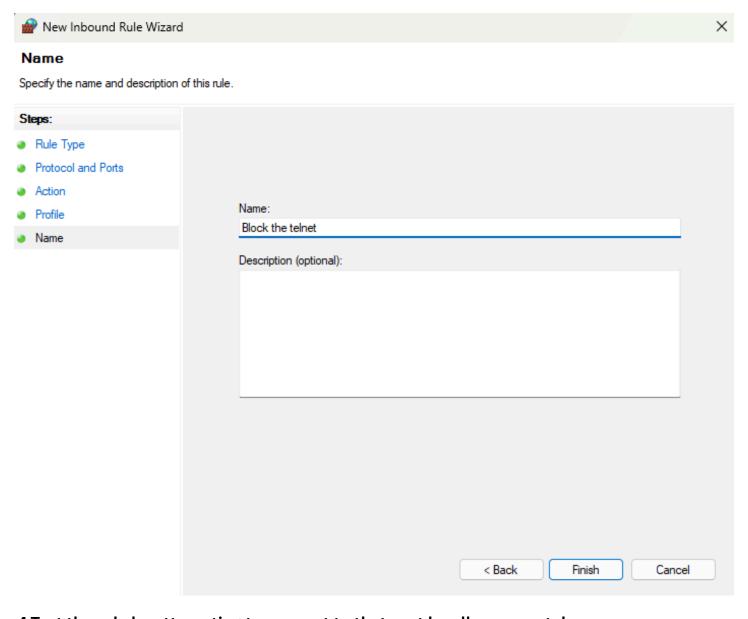




Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

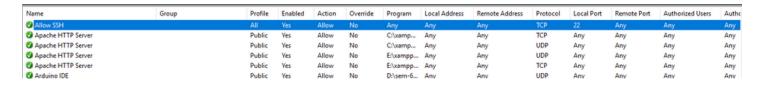




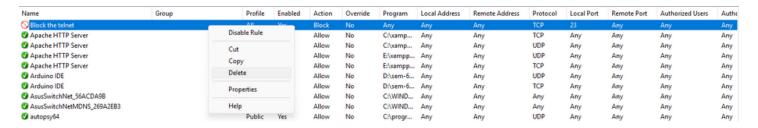
4. Test the rule by attempting to connect to that port locally or remotely.



5.Add rule to alow SSH (port 22).



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



7. Document Commands or GUI Steps Used

- Opened wf.msc
- Added inbound rule to block TCP port 23
- Verified using Telnet
- Allowed port 22 (SSH)
- Removed Telnet rule after testing

8. Summarize how firewall filters traffic.

Windows Firewall filters traffic by applying rules to incoming and outgoing connections. Each rule can allow or block traffic based on protocol, port, IP address, and profile (Domain, Private, Public). We tested this by blocking Telnet (port 23) and verifying it with a connection attempt, then allowed SSH (port 22). The firewall enforces these rules in real time to protect the system.