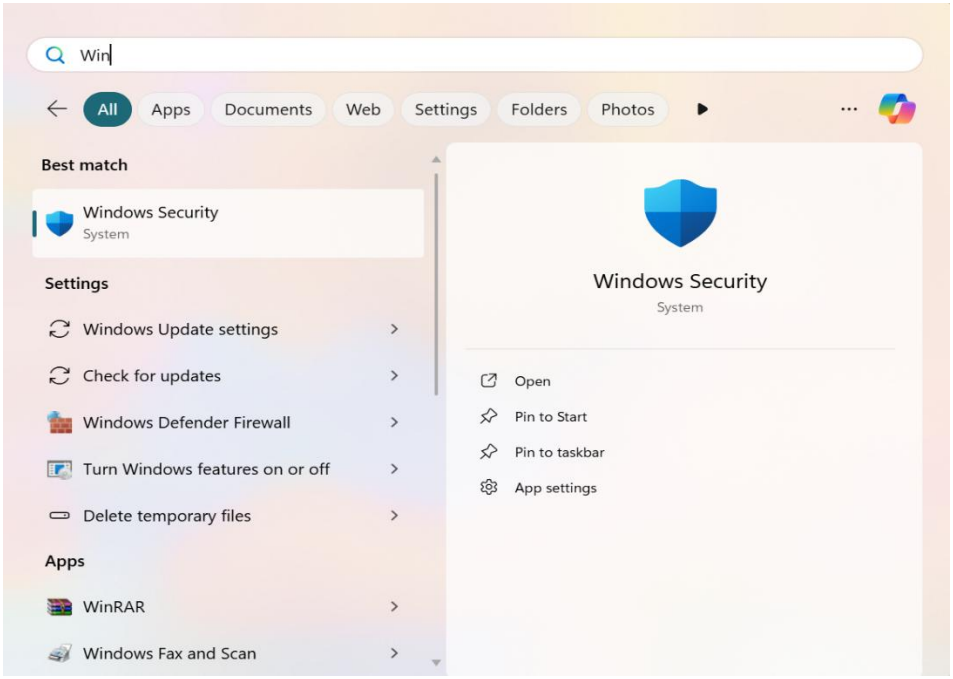
Cyber Security Internship

Task 4 – Setup and use a firewall on Windows/Linux

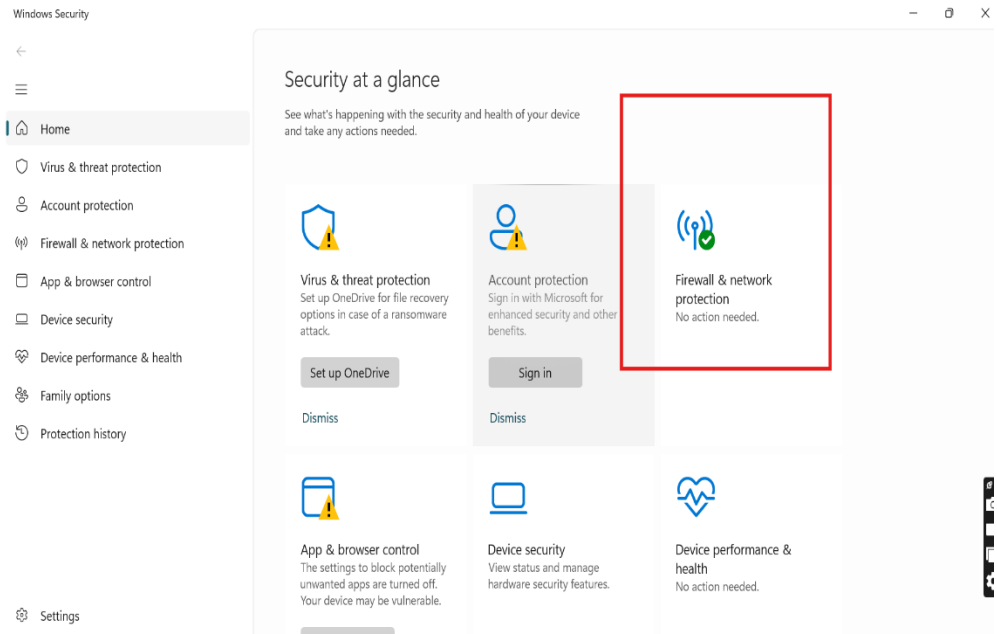
1. Opening firewall configuration tool in Windows PC

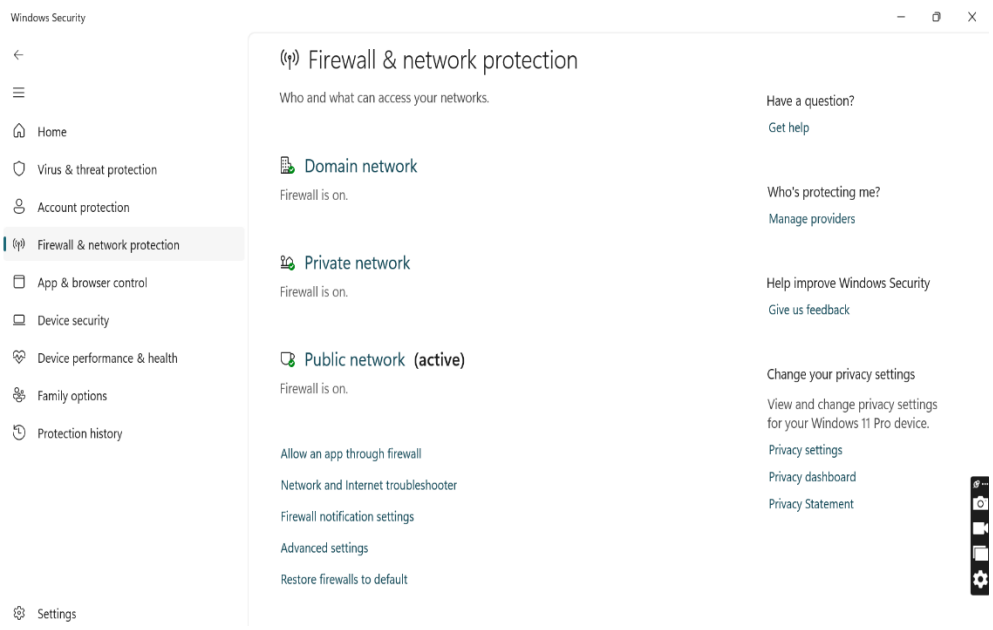
Method-1:

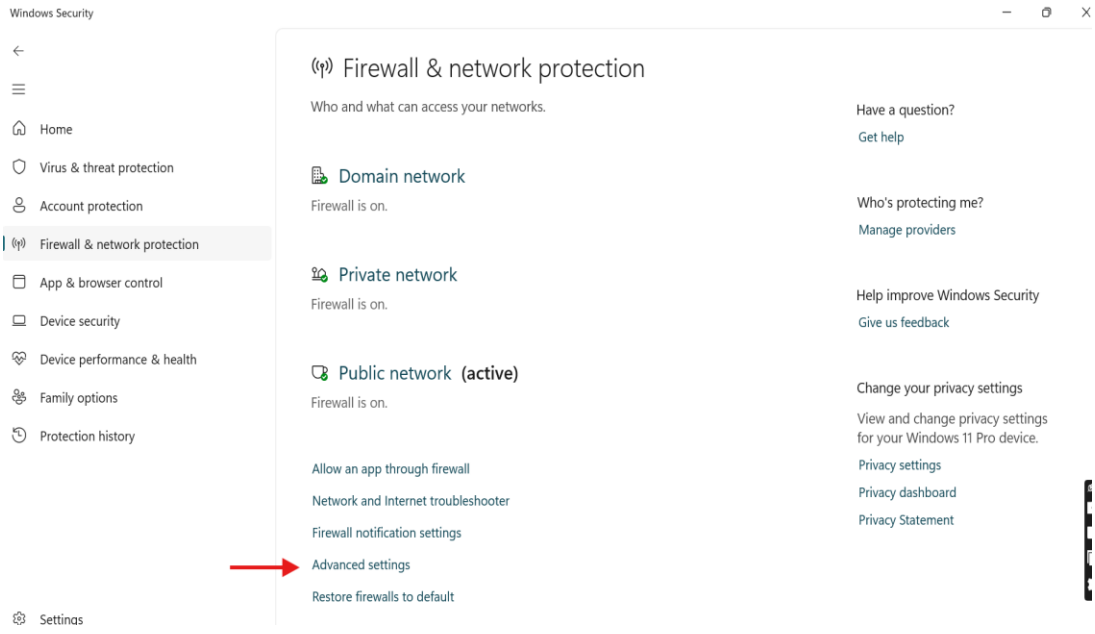
- Start → Windows security →Firewall & network protection → Advanced settings.
-

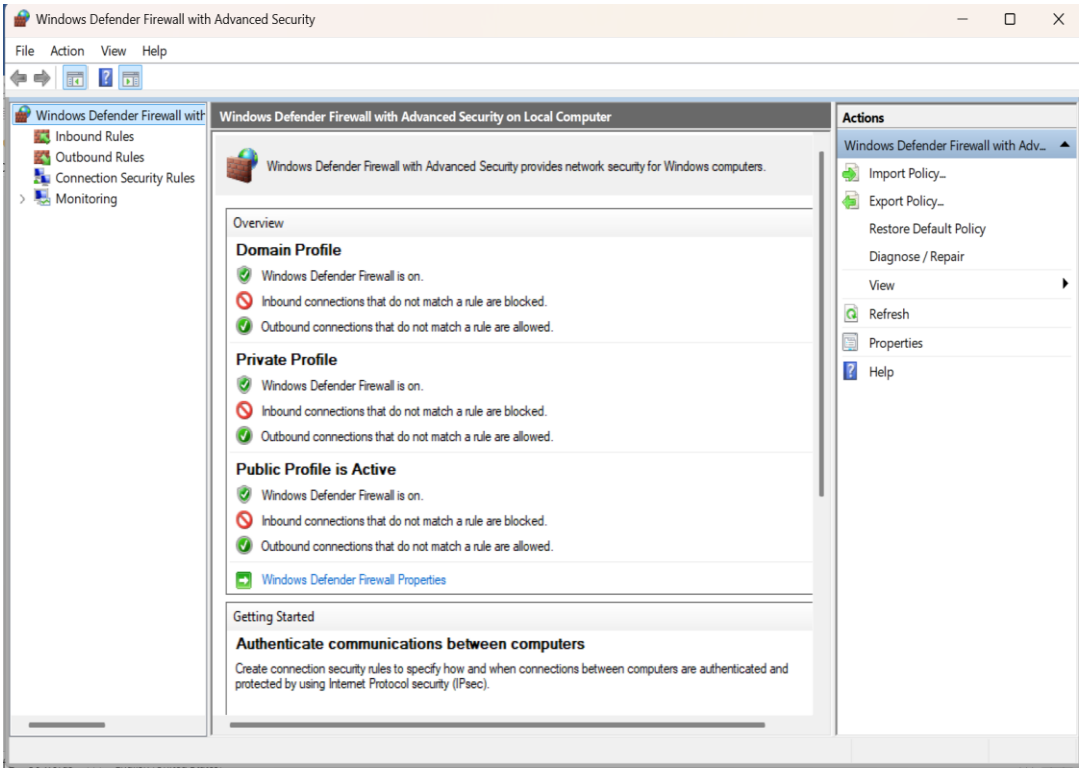


-

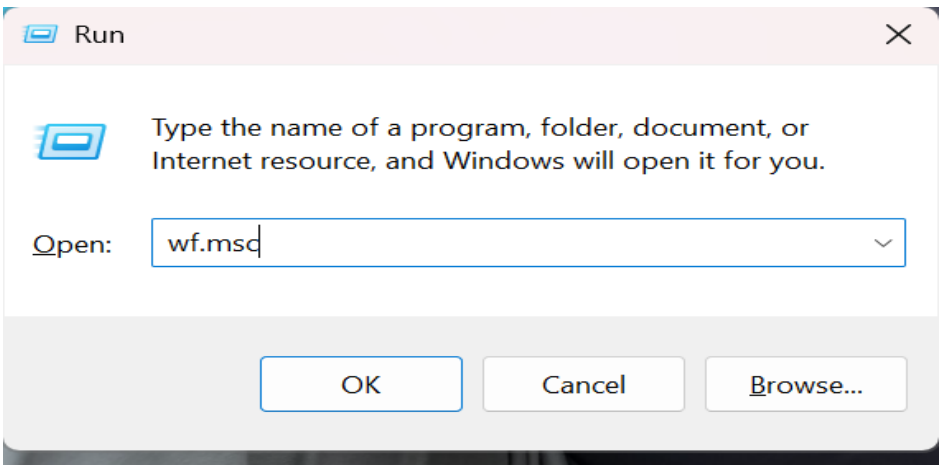


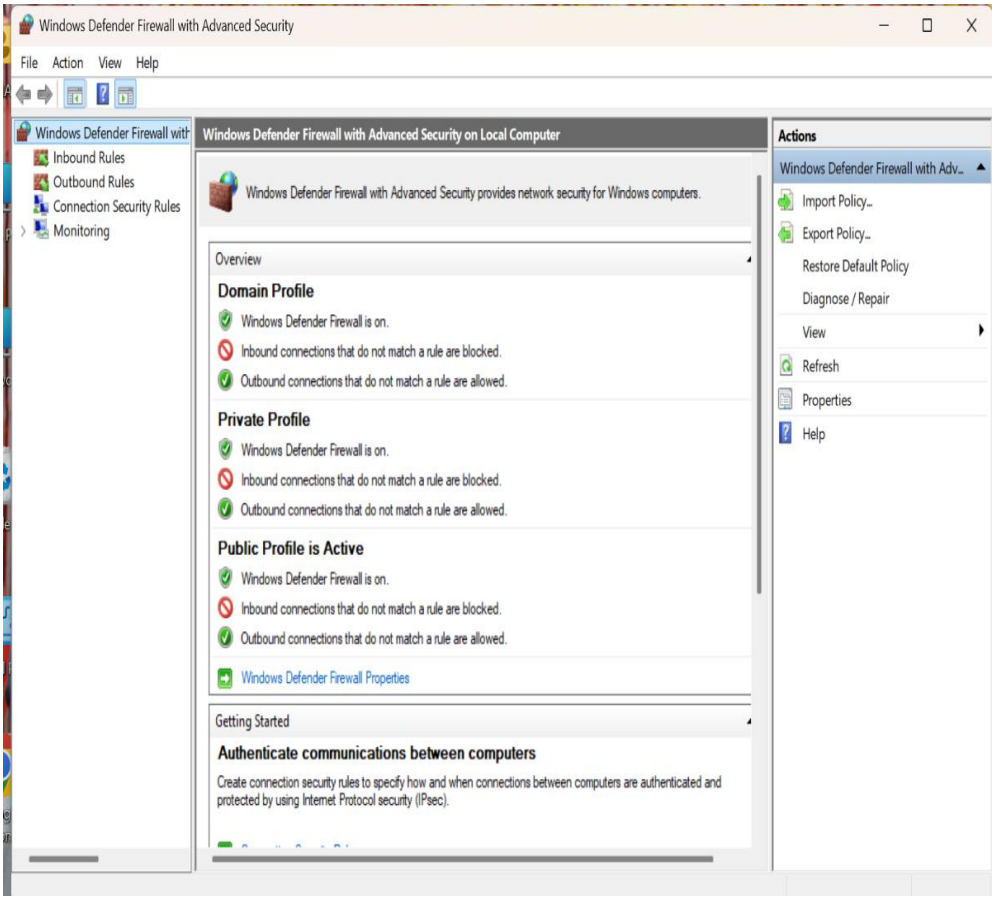

Windows Security
Firewall & network protection
Who and what can access your networks.
Domain network
Firewall is on.
Private network
Firewall is on.
Public network (active)
Firewall is on.
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 11 Pro device.
Privacy settings
Privacy dashboard
Privacy Statement
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Settings


Windows Security
Firewall & network protection
Who and what can access your networks.
Domain network
Firewall is on.
Private network
Firewall is on.
Public network (active)
Firewall is on.
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 11 Pro device.
Privacy settings
Privacy dashboard
Privacy Statement
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Settings



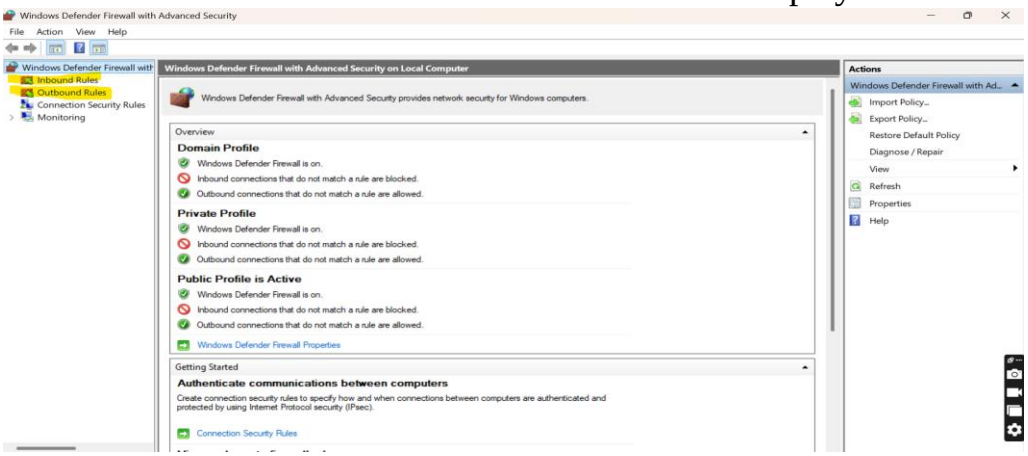
Method-2:

- Press **Win + R**
- Type: wf.msc
- Press Enter → this opens Windows Defender Firewall with Advanced Security
- 

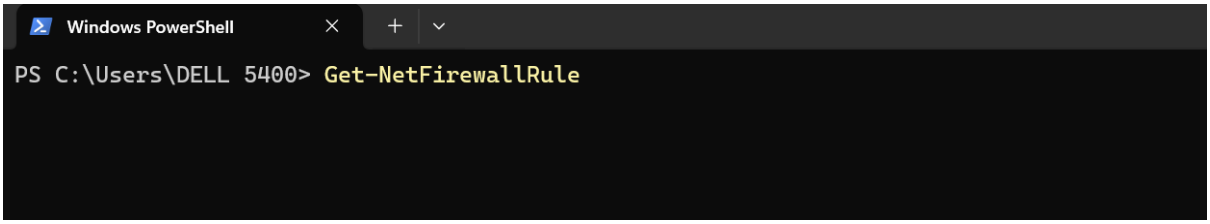
- 

2. Listing current firewall rules

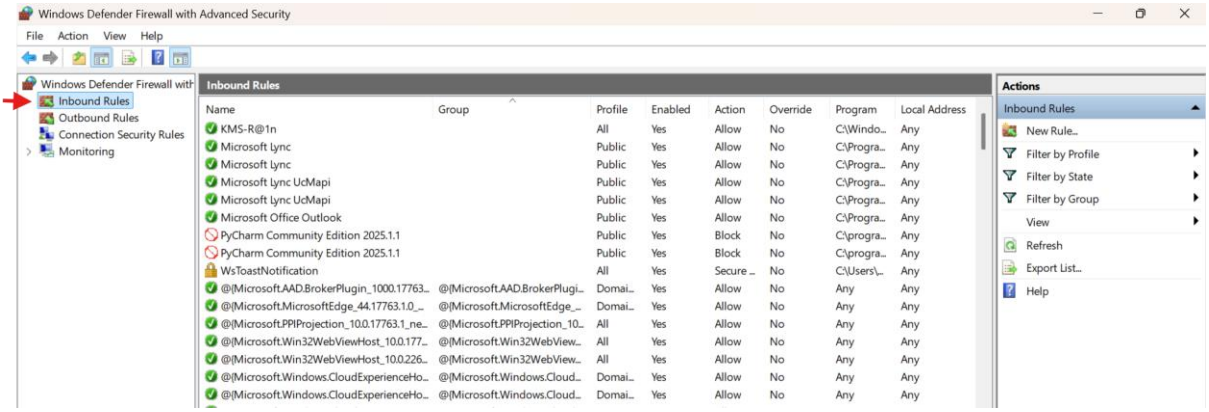
   In the left pane:

   - Click **Inbound rules** → All inbound rules are displayed
   - Click **Outbound rules** → All outbound rules are displayed
   - 

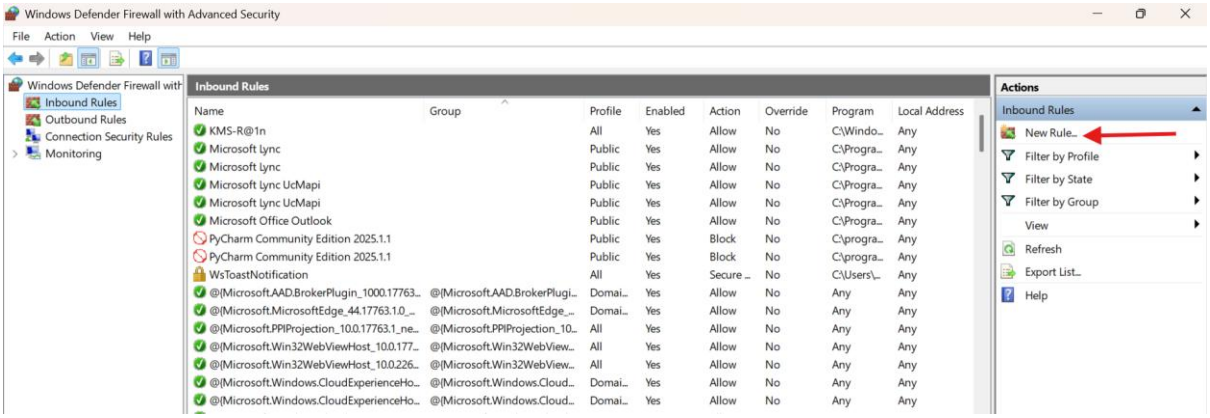
PowerShell Alternative:



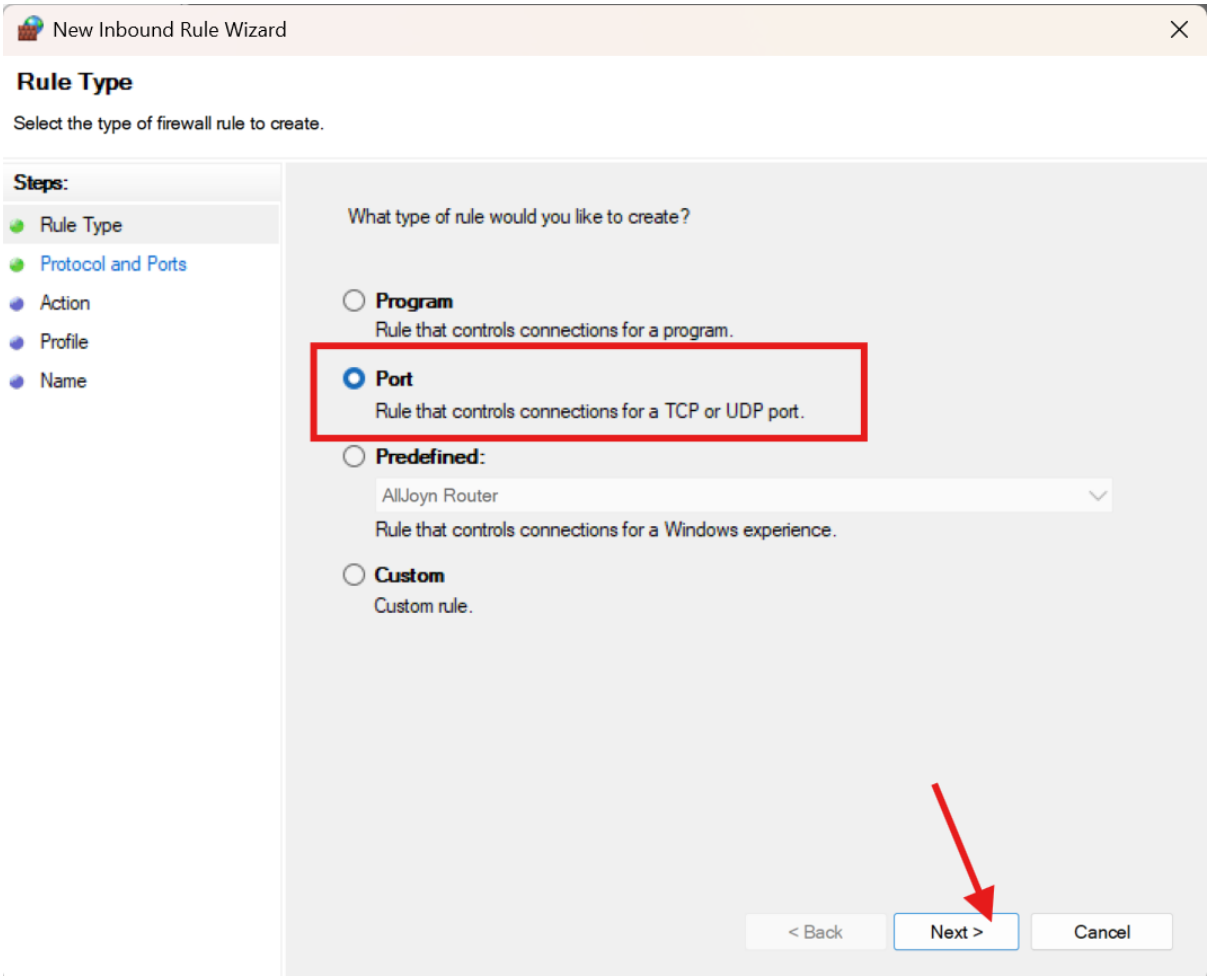
3. Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet)
    1) Open **Inbound Rules**



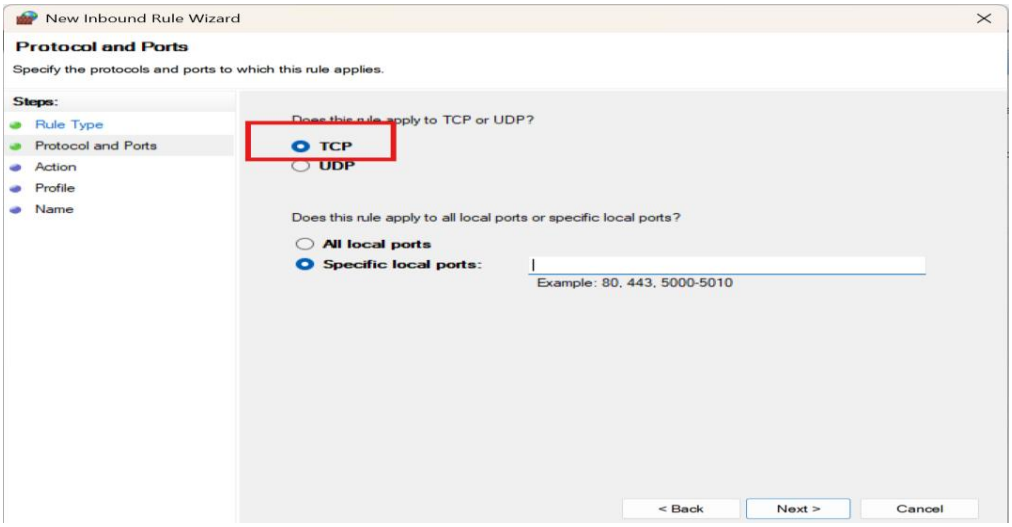
    2) Click **New Rule** (right side)



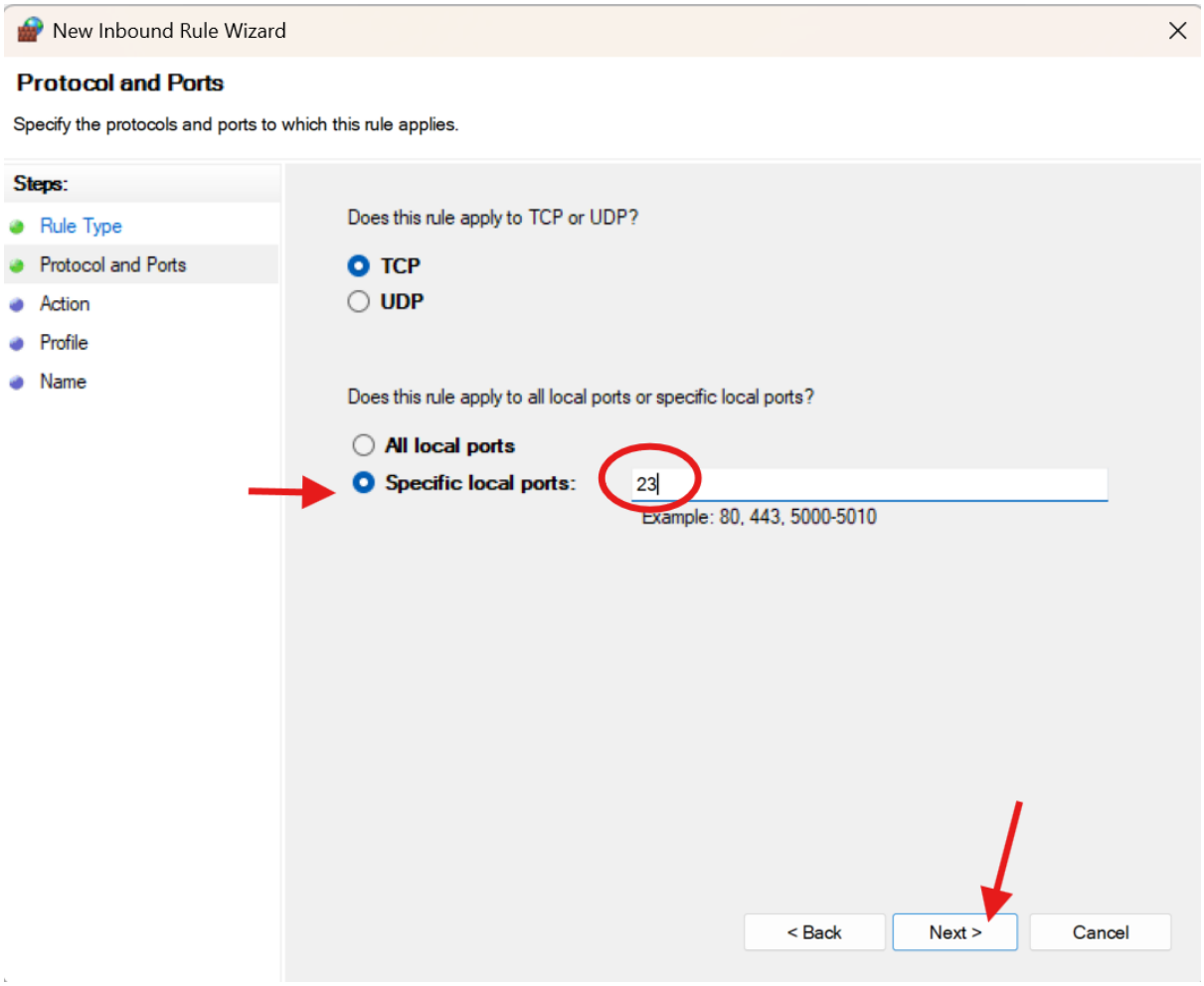
    3) Select **Port** → Next


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

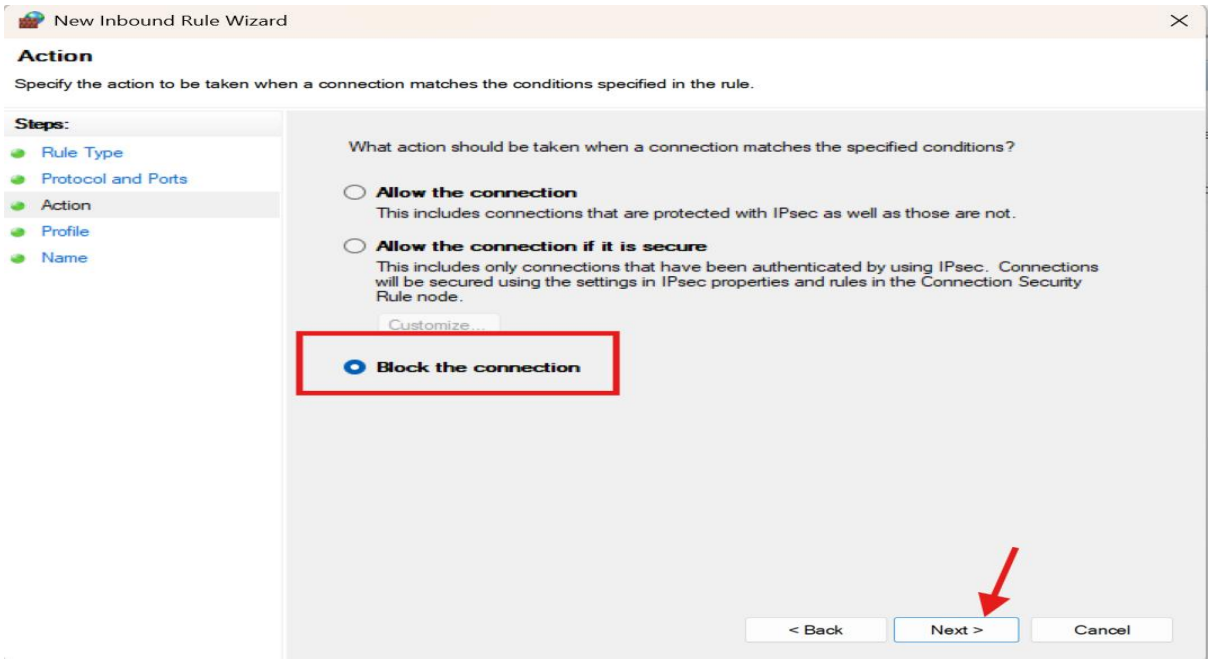
4) Select **TCP**


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
Example: 80, 443, 5000-5010
< Back
Next >
Cancel

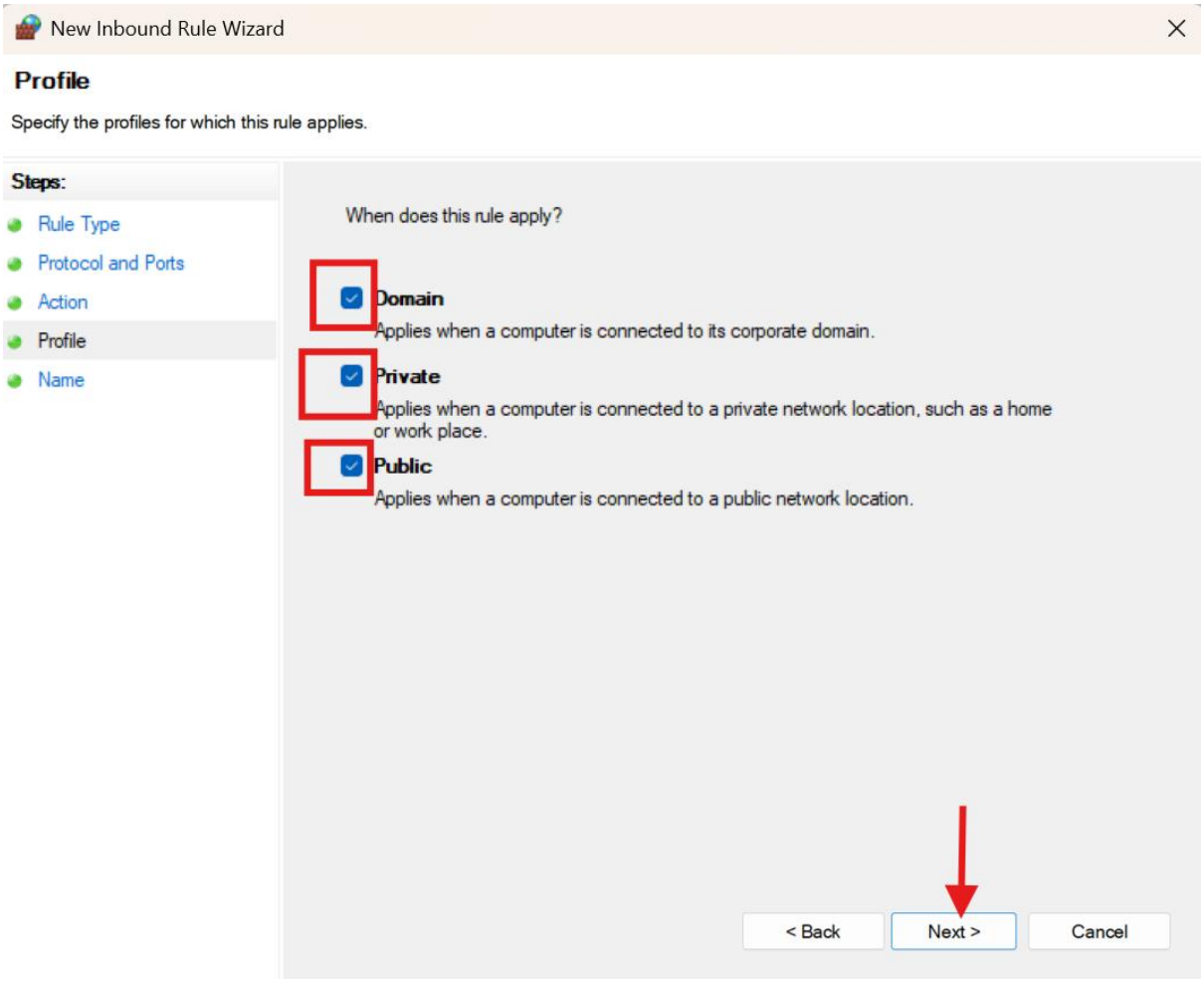
5) Enter specific port: **23**



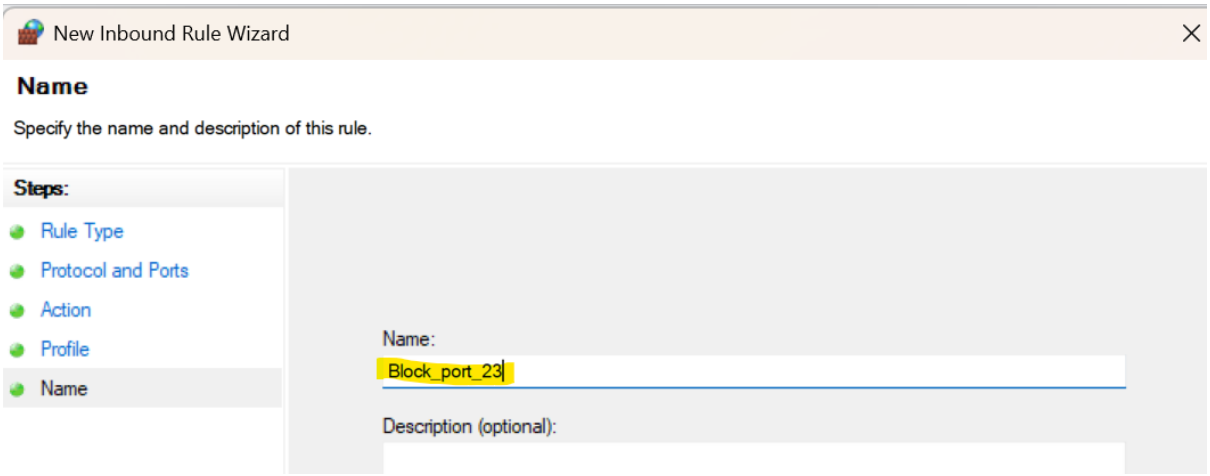
6) Choose **Block the connection**



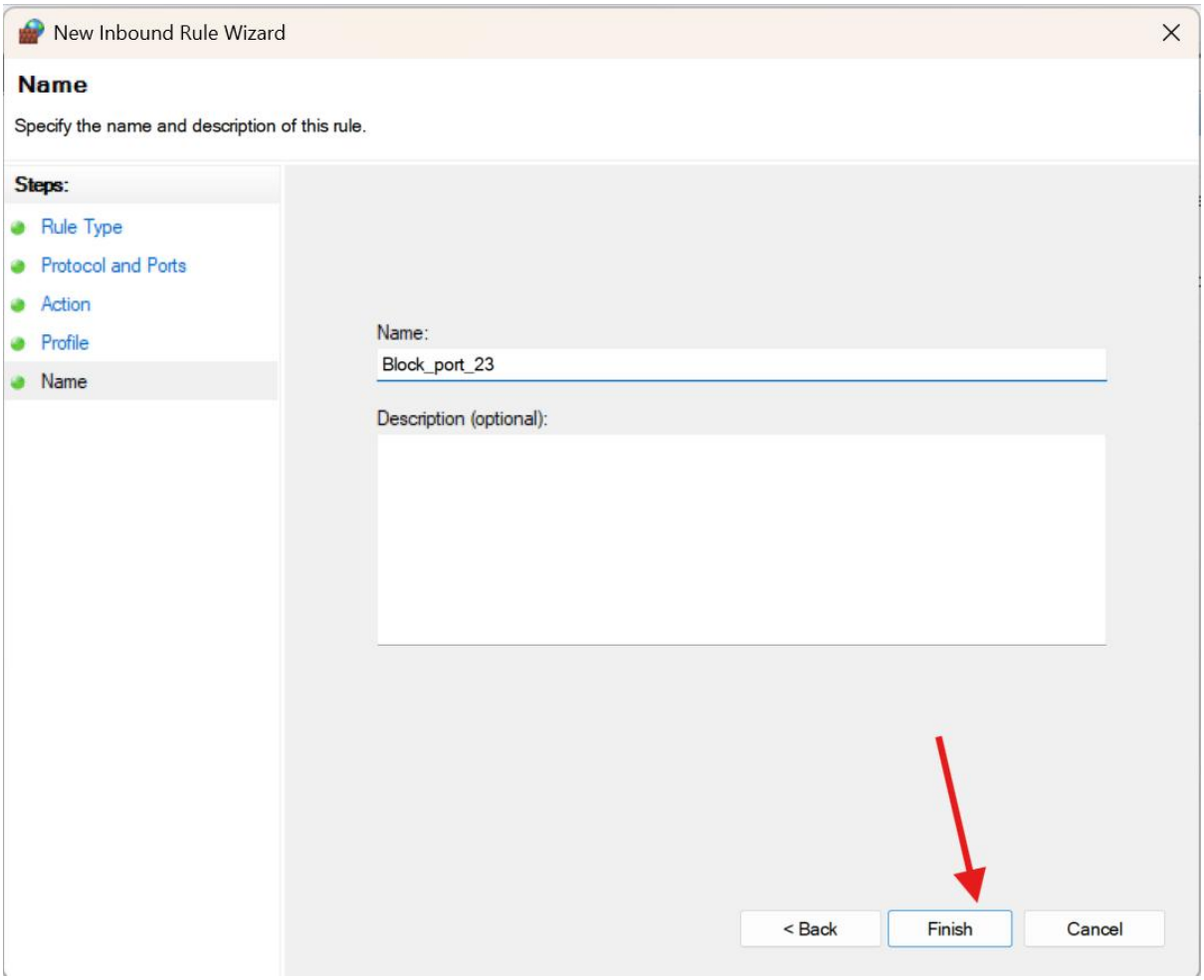
7) Apply to Domain / Private / Public



8) Name it: **Block_port_23**



9) Finish



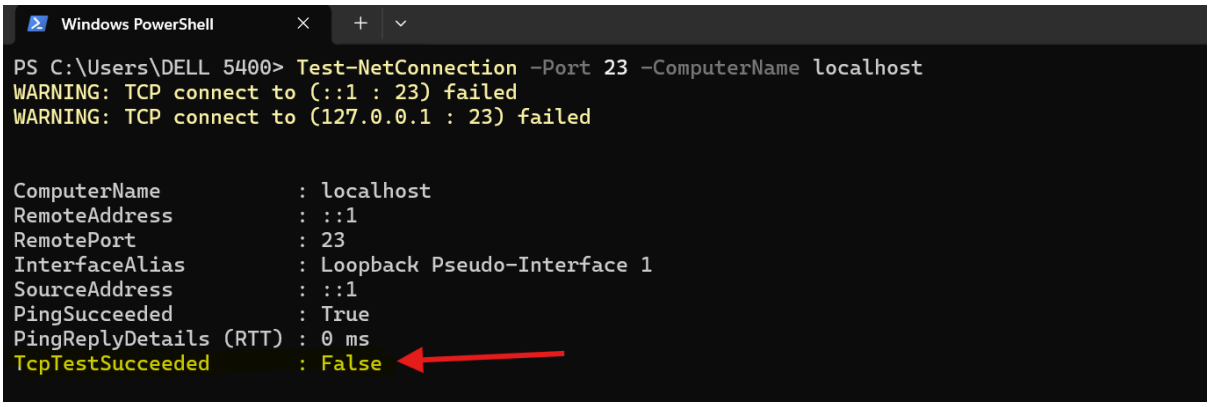
PowerShell Method:

“New-NetFirewallRule -DisplayName "Block_Telnet_23" -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block”

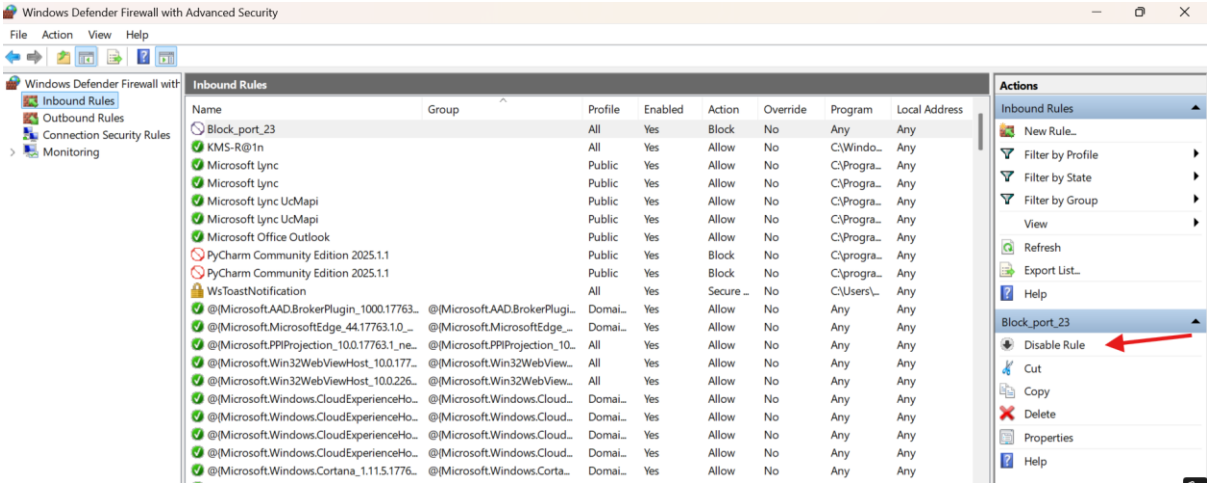
4. Test the Rule

For testing the rule, we can check by PowerShell using command: Test-**NetConnection -Port 23 -ComputerName localhost**

The test should **FAIL,** as we applied an **Inbound rule.**

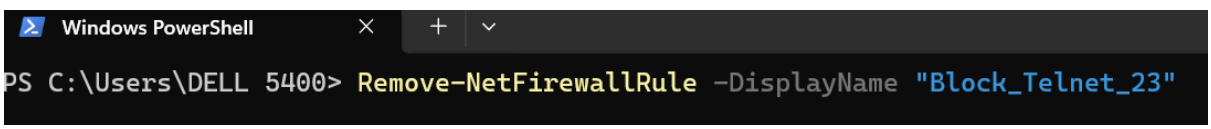


5. Remove / Disable the test rule (Restore original state)
   - Go to **Inbound rules**
   - Find **Block_port_23**
   - Right click → **Disable or Delete**

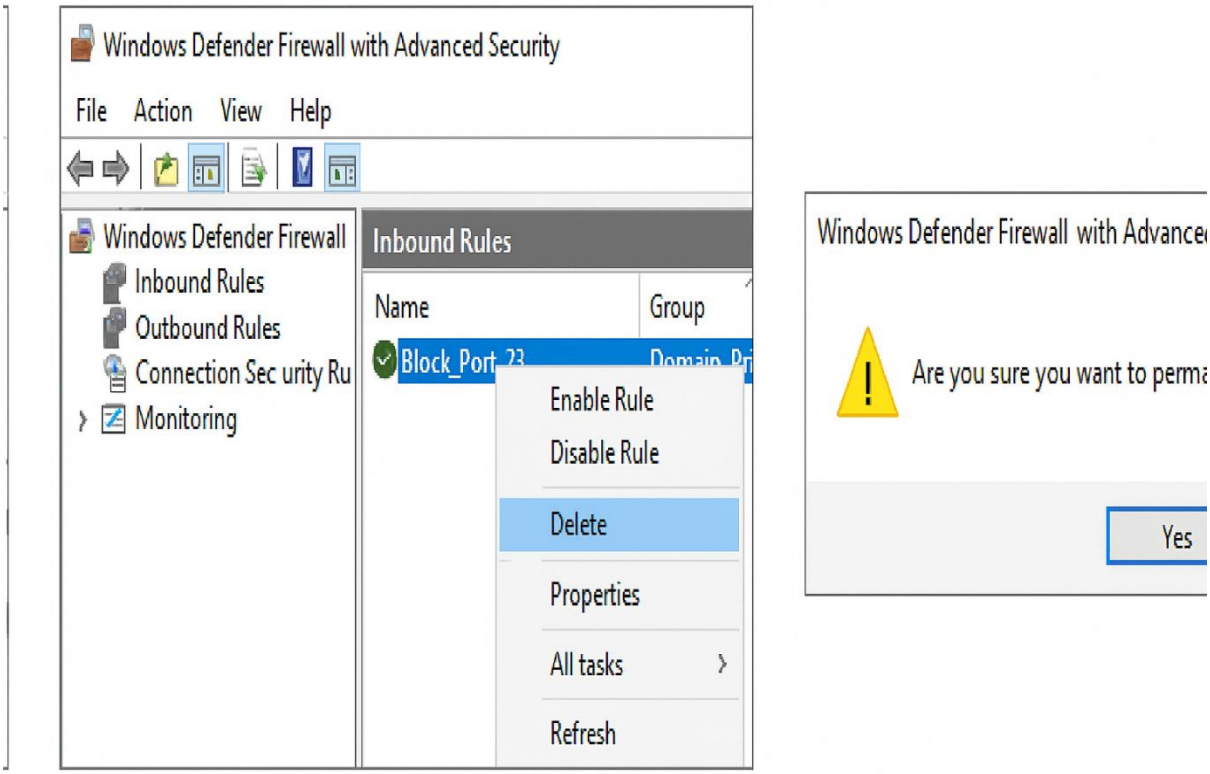


From PowerShell Command:

We can Disable/ Delete the rule by using command: **“Remove-NetFirewallRule -DisplayName "Block_Telnet_23"”**



6. Remove the test block rule



How Firewall filters traffic:

1. Each packet arriving or leaving the system is checked.
2. The firewall compares it against rule list **top to bottom**
3. When a rule match:
   - **Allow** → packet passes
   - **Deny / Block** → packet rejected
   - **Drop** → silently discarded
4. If no rule matches, the firewall uses the **default policy.**