**TASK – 4 ELEVATE LABS : Setup and Use a Firewall on**

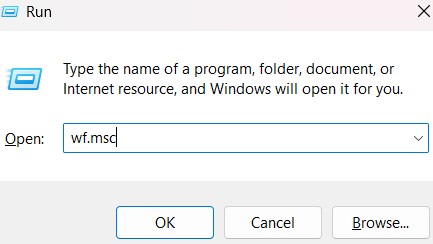
**Windows/Linux**

**OBJECTIVE : Configure and test basic firewall rules to allow or block traffic.**

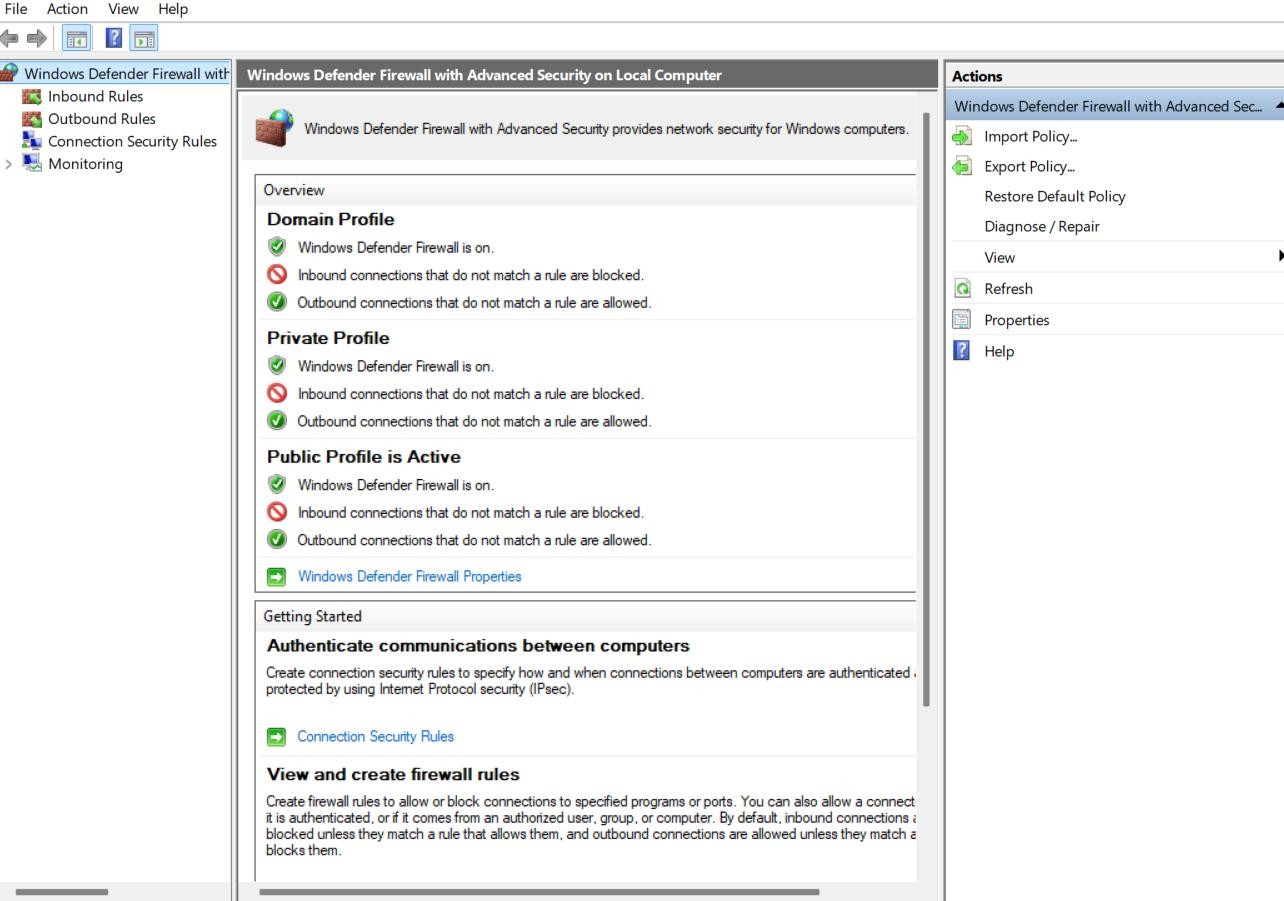
**NAME : rithubaran**

# Step 1: Open Firewall Configuration Tool

* • Press Windows + R, type 'wf.msc' and press Enter.

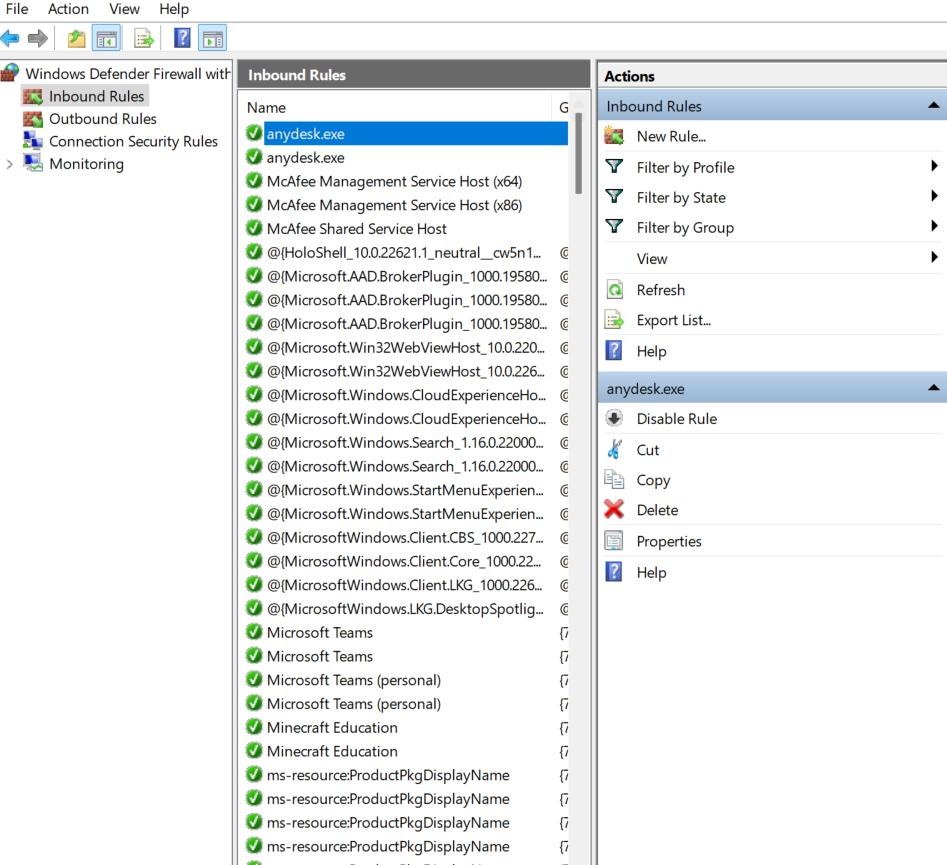


* • This opens 'Windows Defender Firewall with Advanced Security'.

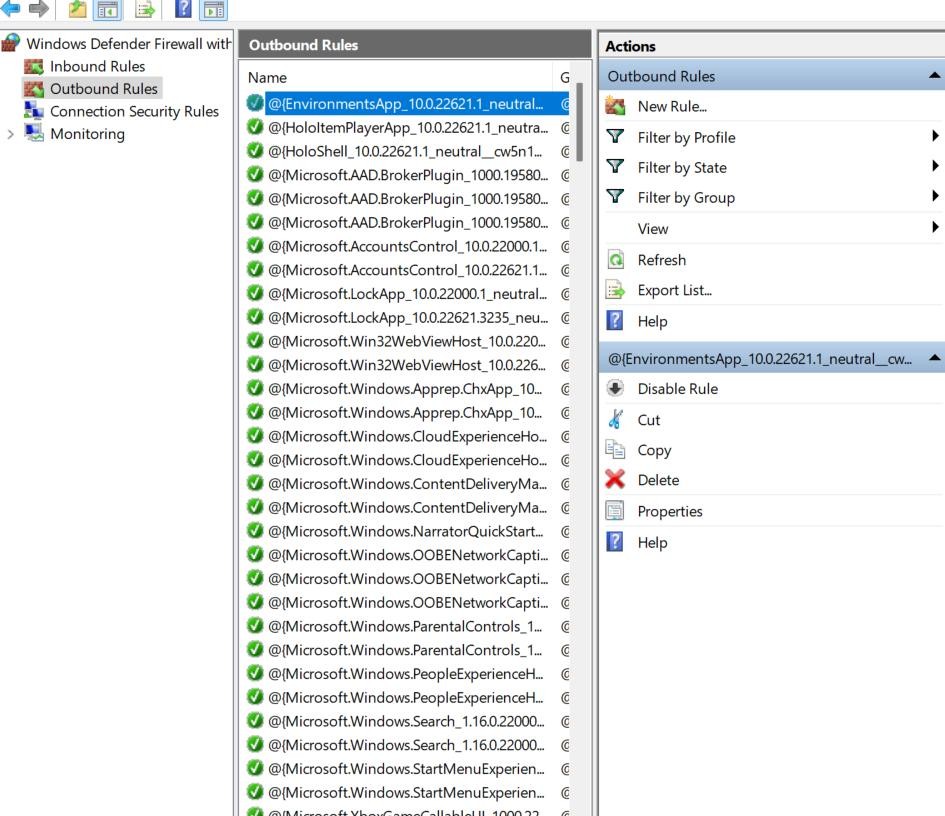


# Step 2: List Current Firewall Rules

* • In the left panel, click 'Inbound Rules' to view existing rules.



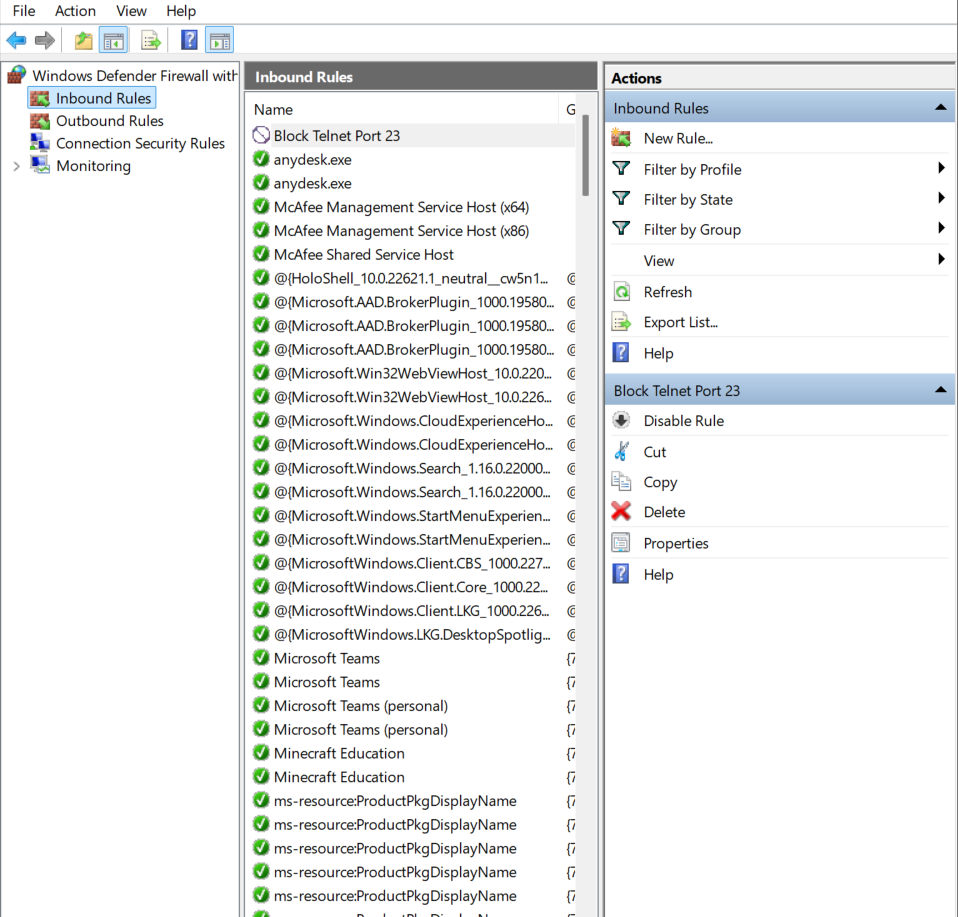
* Similarly, click 'Outbound Rules' to view outbound rules.

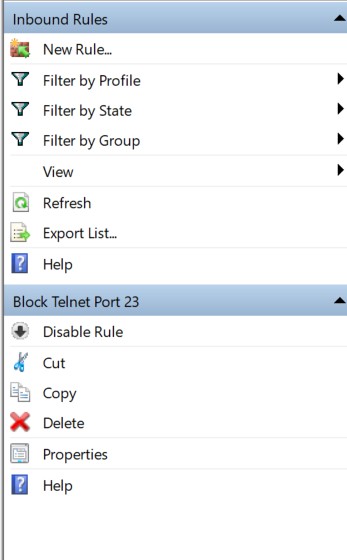


# Step 3: Add Rule to Block Inbound Traffic on Port 23 (Telnet)

* • In 'Inbound Rules', click 'New Rule...'.
* • Select 'Port' > Next > Choose 'TCP' and enter '23' > Next.
* • Select 'Block the connection' > Next.
* • Apply to all profiles > Next.
* • Name the rule 'Block Telnet Port 23' > Finish

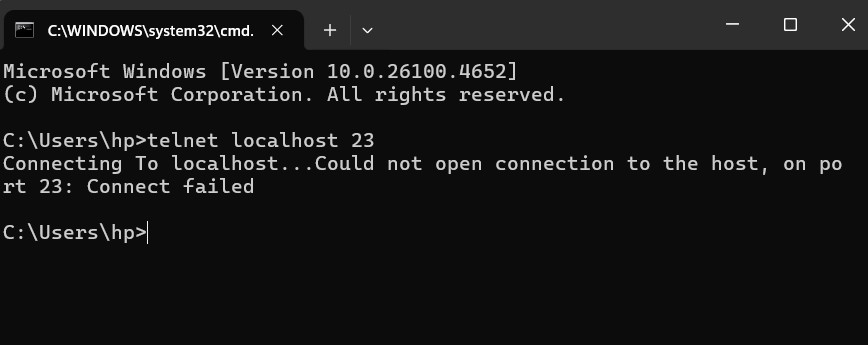
.

* 



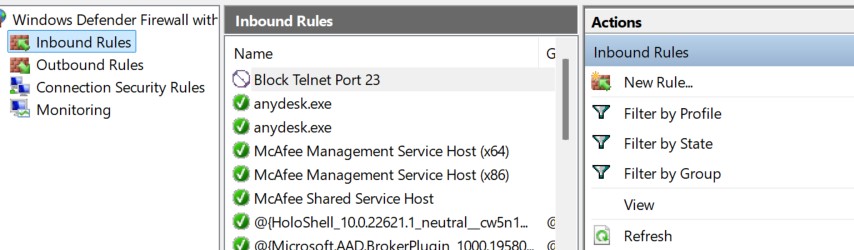
# Step 4: Test the Rule by Attempting to Connect to Port 23

* • Ensure 'Telnet Client' is enabled via Control Panel > Programs > Turn Windows features on or off.
* • Open Command Prompt and run: telnet localhost 23
* • You should see: 'Could not open connection to the host... Connect failed'.
* • This confirms the port is blocked by the firewall rule.



# Step 5: Remove the Test Block Rule

* • Go to 'Inbound Rules'.
* • Locate 'Block Telnet Port 23', right-click and select 'Delete'.



***Step 6: Document Commands or GUI Steps Used***

* • Documented all steps above with actions taken via the Windows Firewall GUI.