

Task 4

- **Objective:** Configure and test basic firewall rules to allow or block traffic.
- **Tools:** Windows Firewall / UFW (Uncomplicated Firewall) on Linux.
- **Deliverables:** Screenshot/configuration file showing firewall rules applied.

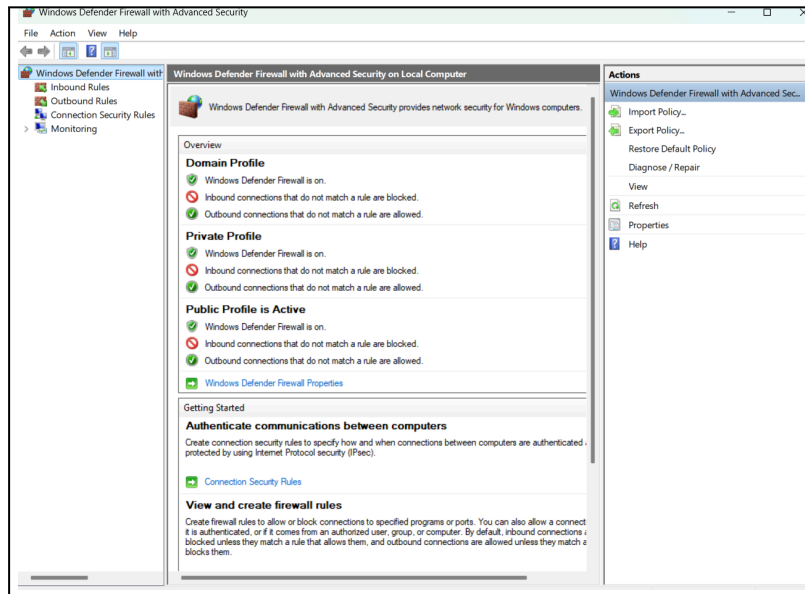
Environment

- **Operating System:** Windows 11 (for GUI) / Ubuntu 22.04 (for UFW commands)
 - **Firewall Tool:**
 - Windows → *Windows Defender Firewall with Advanced Security*
 - Linux → *UFW (Uncomplicated Firewall)*
-

1 Open Firewall Configuration Tool

Windows:

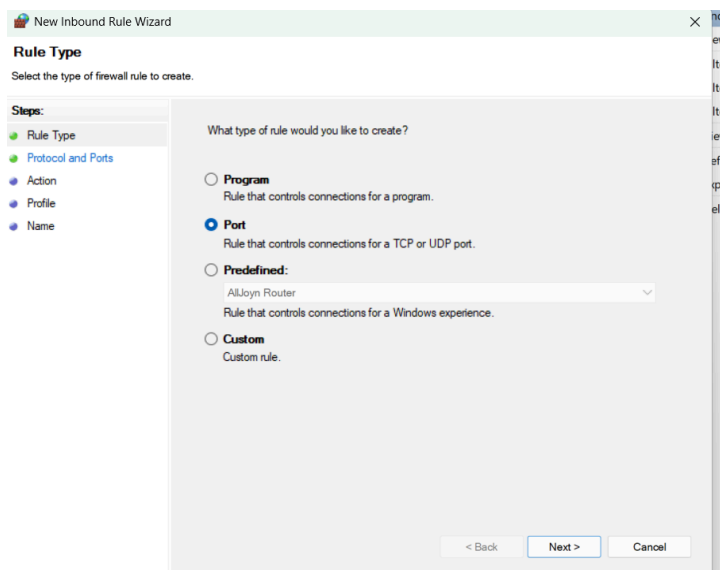
1. Press **Win + R** → type **wf.msc** → press Enter.
2. *Windows Defender Firewall with Advanced Security* window opens.



2 List Current Firewall Rules

Windows:

- **Navigate to Inbound Rules → check list of existing rules.**

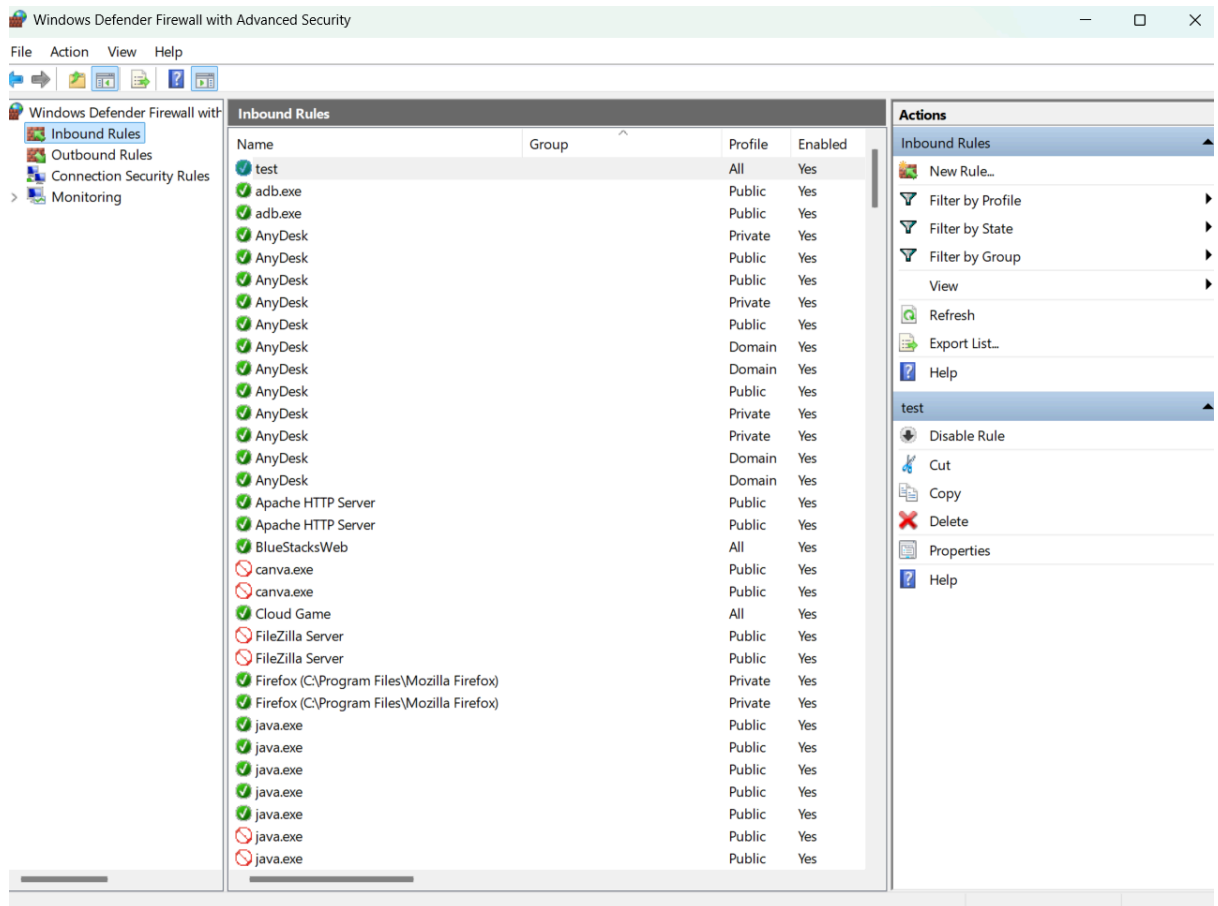


3 Add Rule to Block Inbound Traffic on Port 23 (Telnet)

Windows:

1. Go to Inbound Rules → Click New Rule → Choose Port.
2. Select TCP, enter 23.
3. Choose Block the connection, apply to all profiles, name it **Block Telnet**.

The screenshot shows the 'New Inbound Rule Wizard' window with the title bar 'New Inbound Rule Wizard' and a close button. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' sidebar lists 'Rule Type', 'Protocol and Ports' (highlighted), 'Action', 'Profile', and 'Name'. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with 'TCP' selected (radio button), and 'Does this rule apply to all local ports or specific local ports?' with 'Specific local ports:' selected (radio button). A text box next to 'Specific local ports:' contains the value '23', with an example 'Example: 80, 443, 5000-5010' below it. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.



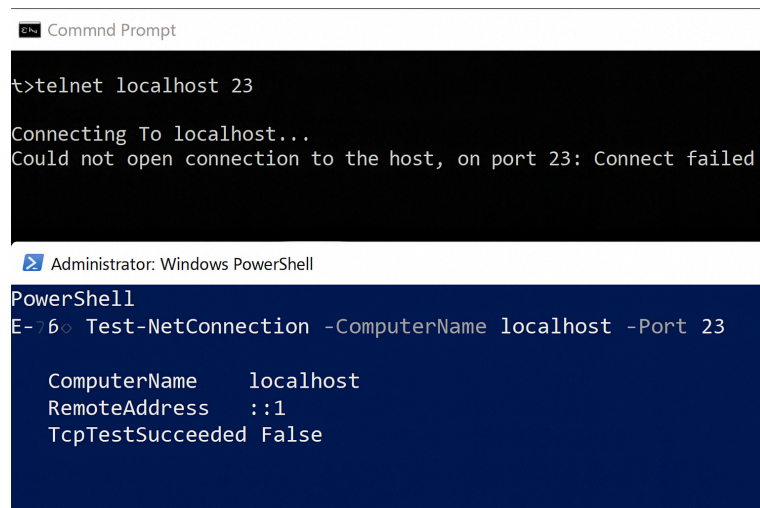
6 Remove the Test Block Rule

Windows:

- Right-click on **Block Telnet** → Select **Delete**.

Test Connection to the Port

Use telnet to try connecting to a port you blocked or allowed.

The image shows two terminal windows. The top window is a 'Command Prompt' with a black background and white text. It shows the command 'telnet localhost 23' being entered, followed by the output 'Connecting To localhost...' and 'Could not open connection to the host, on port 23: Connect failed'. The bottom window is an 'Administrator: Windows PowerShell' with a dark blue background and white text. It shows the command 'Test-NetConnection -ComputerName localhost -Port 23' being entered, followed by the output: 'ComputerName localhost', 'RemoteAddress ::1', and 'TcpTestSucceeded False'.

Summary

A firewall acts as a security guard between the system and network traffic.

It filters packets based on rules that define which ports/protocols/IPs are allowed or blocked.

- Inbound Rules: Control incoming traffic (e.g., allow SSH, block Telnet).
- Outbound Rules: Control outgoing traffic (e.g., prevent data exfiltration).
- Firewalls protect against unauthorized access, malicious scans, and network attacks by enforcing a security policy.