**Task 4 : Setup and Use a Firewall on Windows/Linux**

**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.

**1. Open Firewall Configuration Tool**

* Press Windows + R → type wf.msc → hit Enter  
  → This opens Windows Defender Firewall with Advanced Security (the GUI).  
  Or, open via Control Panel → System and Security → Windows Defender Firewall → Advanced Settings.

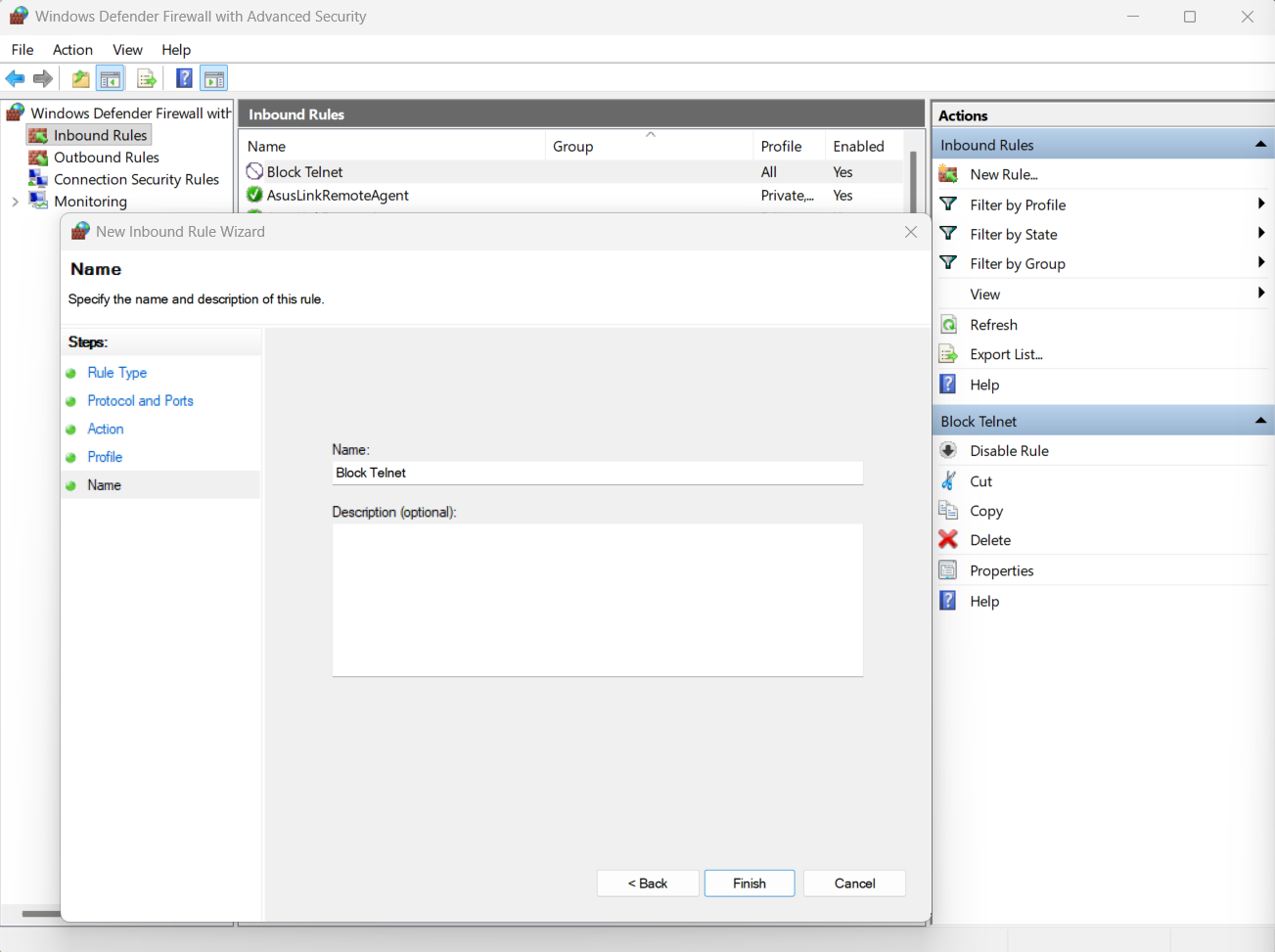
**2. List Current Firewall Rules**

* In the left pane → Click Inbound Rules or Outbound Rules
* You’ll see all the active firewall rules with names, ports, and protocols.

**3. Add a Rule to Block Inbound Traffic on a Specific Port (e.g., 23 for Telnet)**

GUI method:

1. In Inbound Rules, click New Rule → Port → TCP → Specific local ports: 23
2. Select Block the connection → Apply to all profiles → Give it a name, e.g., “Block Telnet”.



**4. Test the Rule**

With Nmap:

nmap -p 23 localhost

→ It showed the port as closed.

A screenshot of a computer

AI-generated content may be incorrect.

**6. Remove the Test Block Rule**

Using Command Prompt:

netsh advfirewall firewall delete rule name="Block Telnet"

A screenshot of a computer

AI-generated content may be incorrect.

**7. Document Commands or GUI Steps Used**

- Used wf.msc to open Firewall

- Added inbound rule to block TCP port 23

- Verified with Nmap that port 23 was closed

- Removed the test rule to restore firewall

**8. Summarize How Firewall Filters Traffic**

A firewall filters traffic by monitoring and controlling incoming and outgoing network packets based on predefined security rules. It allows or blocks connections according to IP addresses, ports, and protocols, acting as a barrier between trusted internal networks and untrusted external ones.