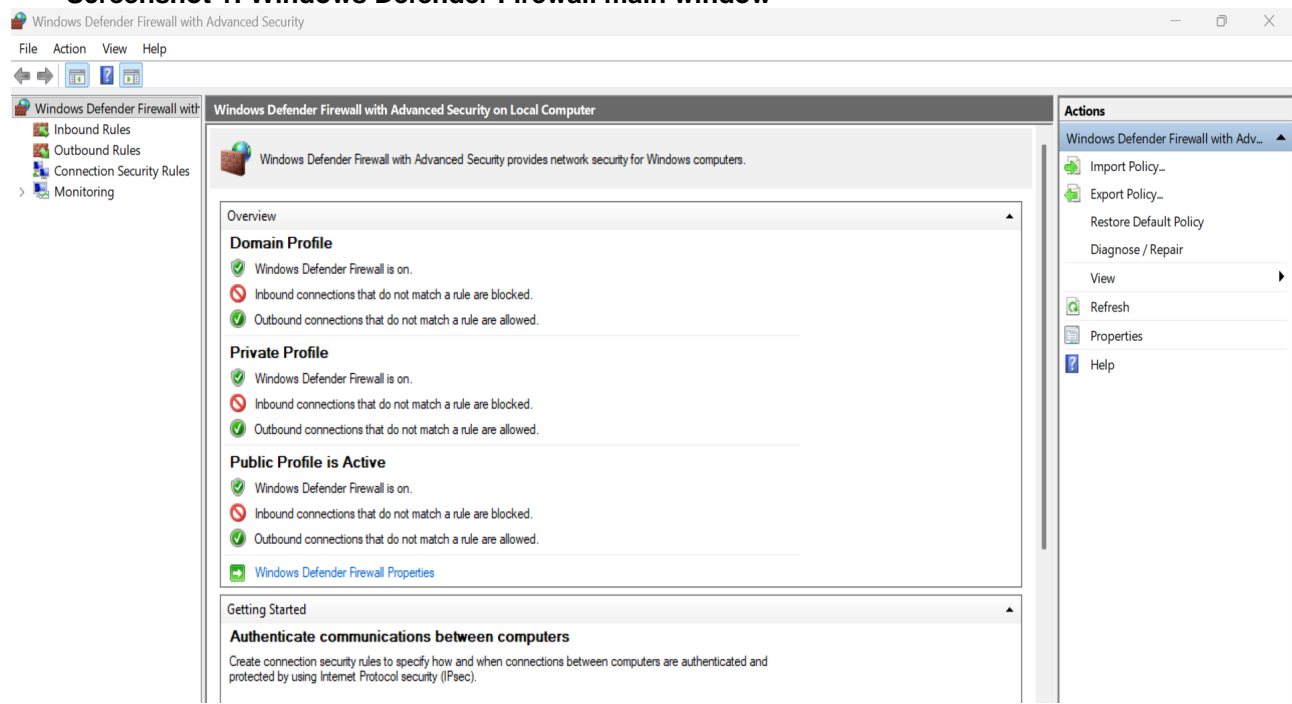


Task 4: Setup and Use a Firewall on Windows/Linux

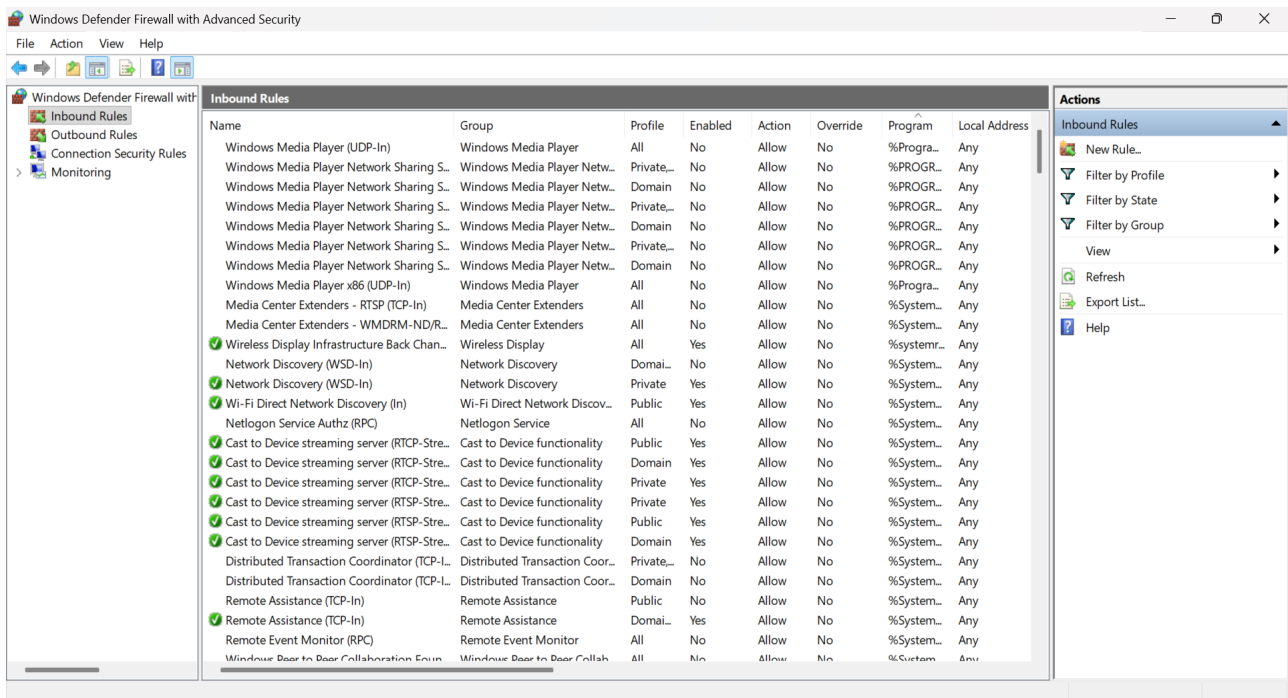
Objective: Configure and test basic firewall rules to allow or block traffic using Windows Firewall or UFW (Uncomplicated Firewall) on Linux.

Firewall Configuration Steps and Screenshots (Windows Example)

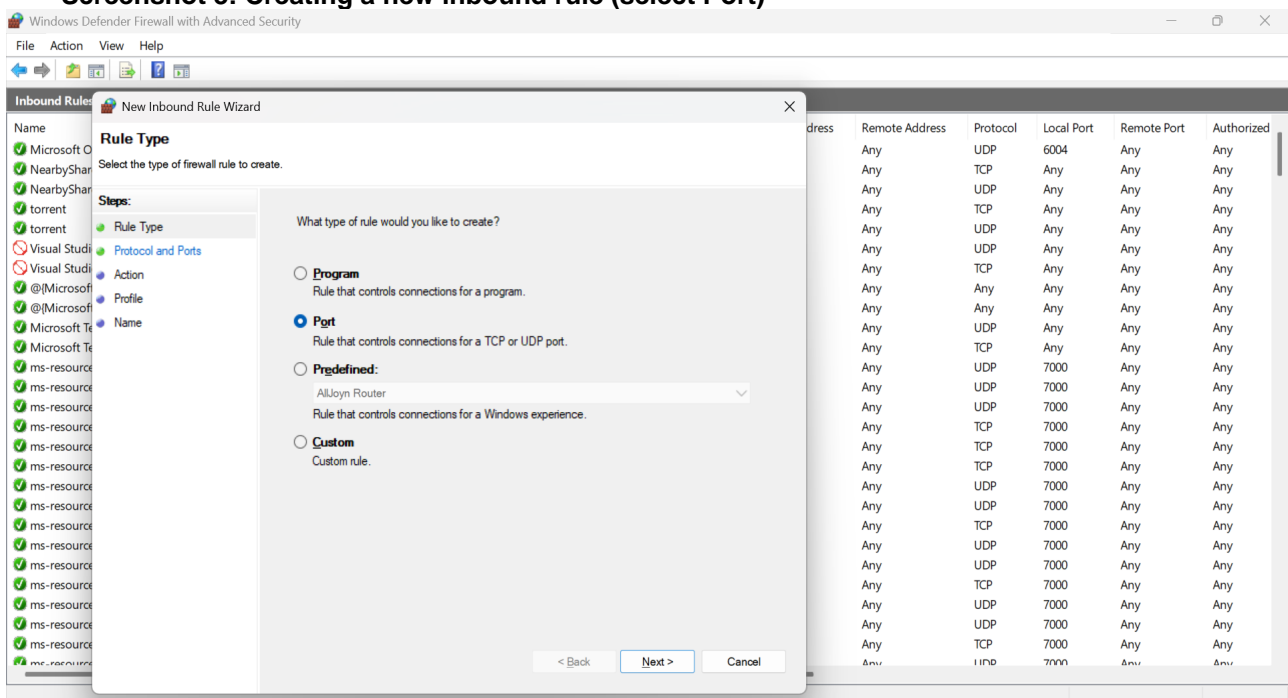
Screenshot 1: Windows Defender Firewall main window



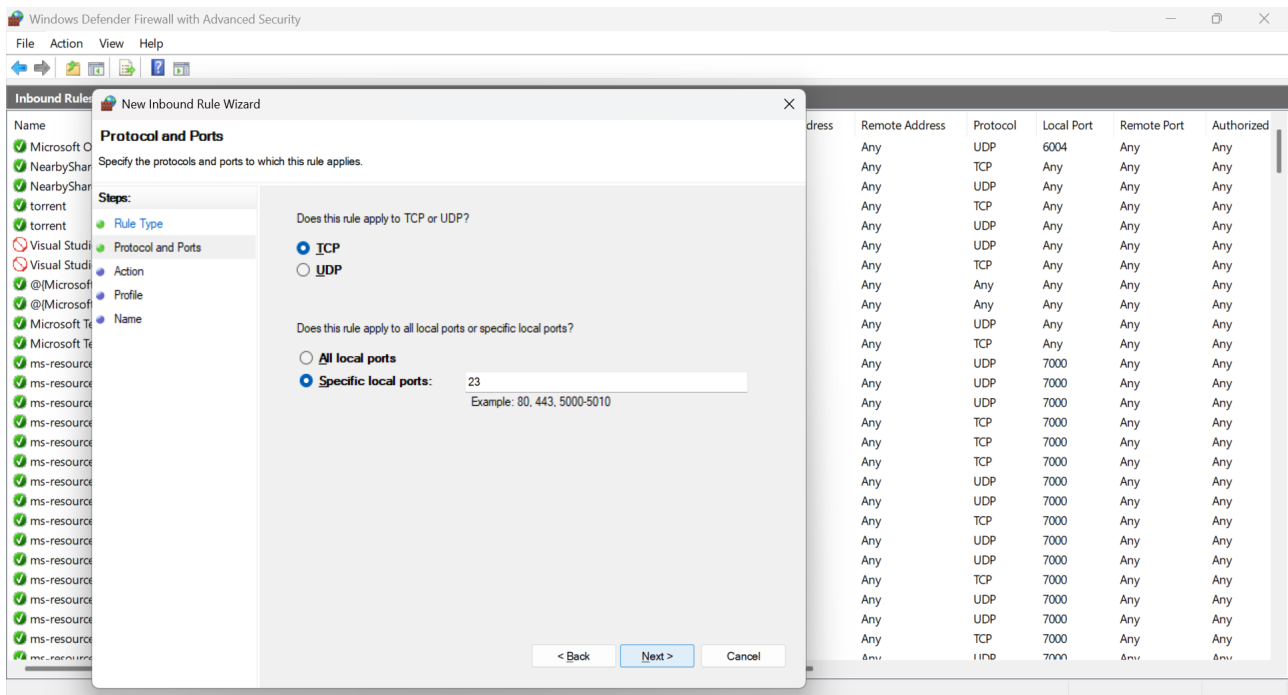
Screenshot 2: Inbound rules view



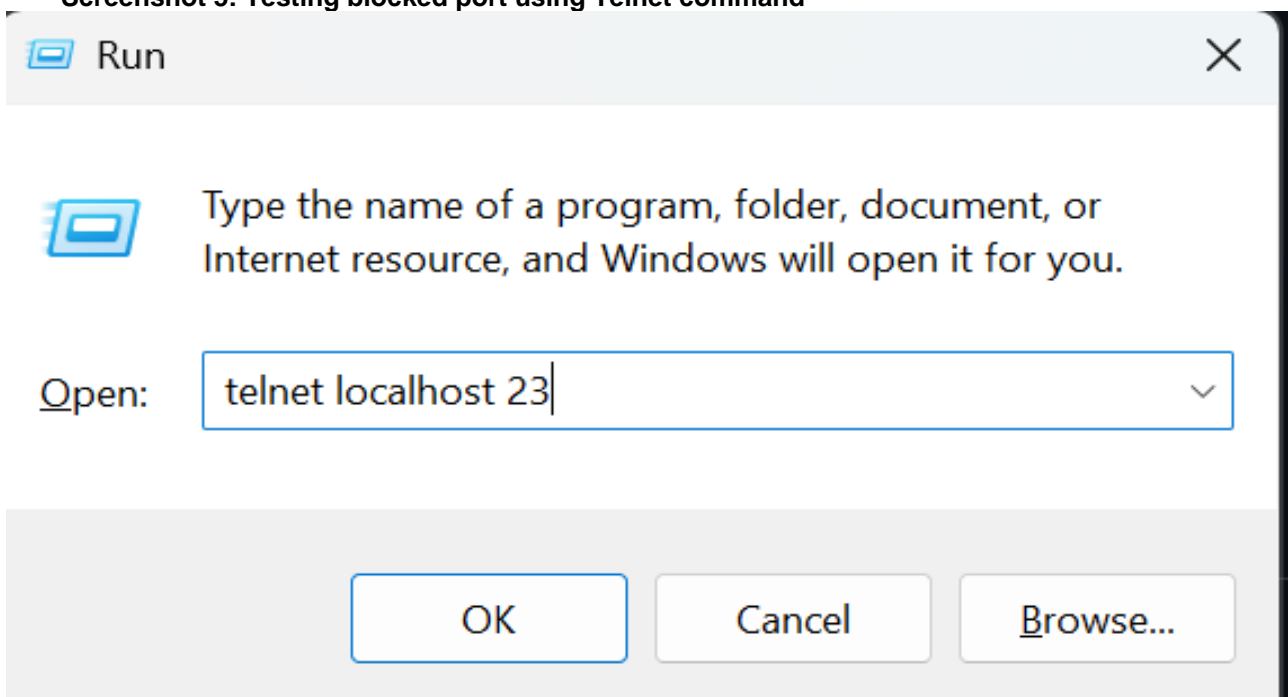
Screenshot 3: Creating a new inbound rule (select Port)



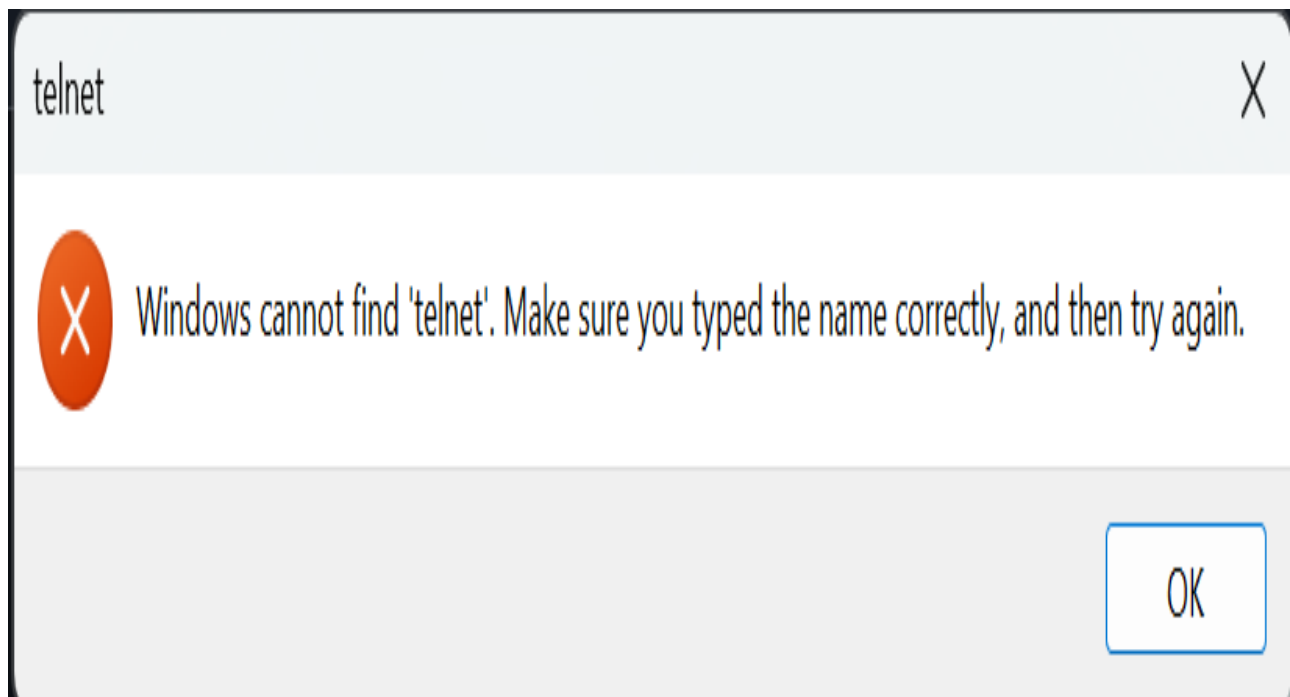
Screenshot 4: Blocking specific local port 23 (Telnet)



Screenshot 5: Testing blocked port using Telnet command



Screenshot 6: Telnet command blocked confirmation message



Summary:

In this task, the Windows Defender Firewall was configured to block incoming traffic on port 23 (Telnet). A test connection attempt confirmed that Telnet access was denied, demonstrating the firewall's effectiveness. After verification, the rule can be removed or disabled to restore normal connectivity.

Outcome:

- Successfully applied inbound firewall rules.
- Tested network port blocking (Telnet).
- Gained understanding of firewall-based traffic filtering in Windows.