Task 4 Report: Setup and Use a Firewall on Windows 10

Name: Srushti Uday Nikam

Date: 27/06/2025

Operating System: Windows 10

Firewall Tool Used: Windows Defender Firewall with Advanced Security

Objective :-

Configure and test basic firewall rules to allow or block traffic using Windows Firewall.

Tools Used:-

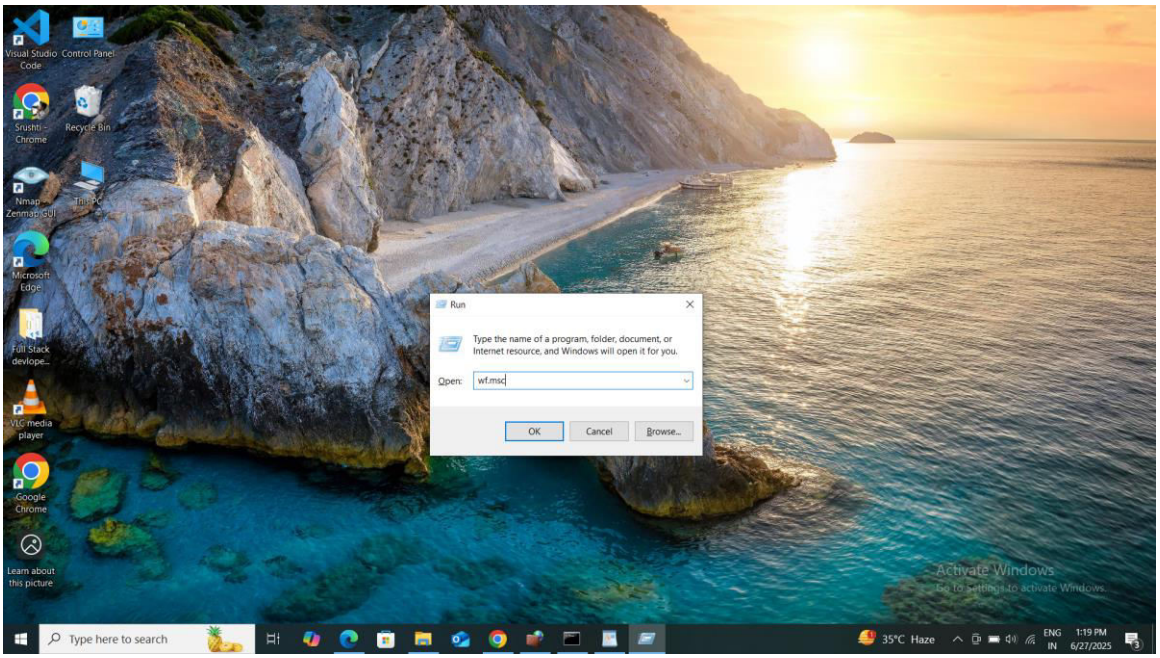
- Windows Defender Firewall
- Telnet Client (for testing)
- Command Prompt

Steps Performed:-

1. Open Windows Firewall Settings

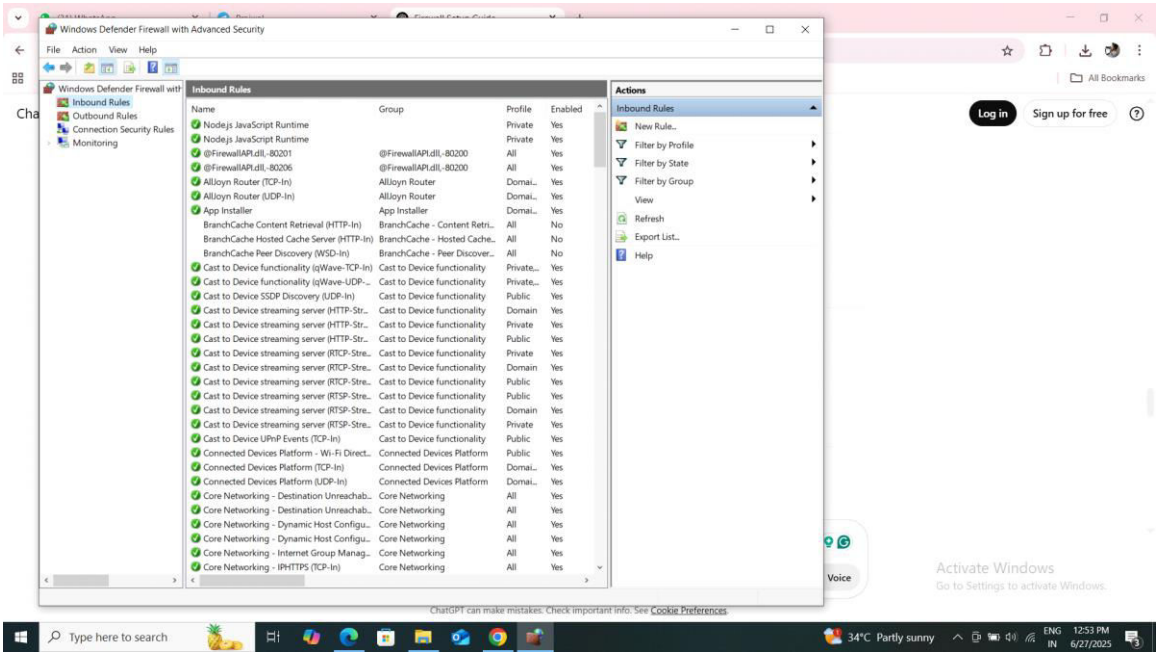
Press Win + R, type wf.msc, and hit Enter.

(This opens “Windows Defender Firewall with Advanced Security”)



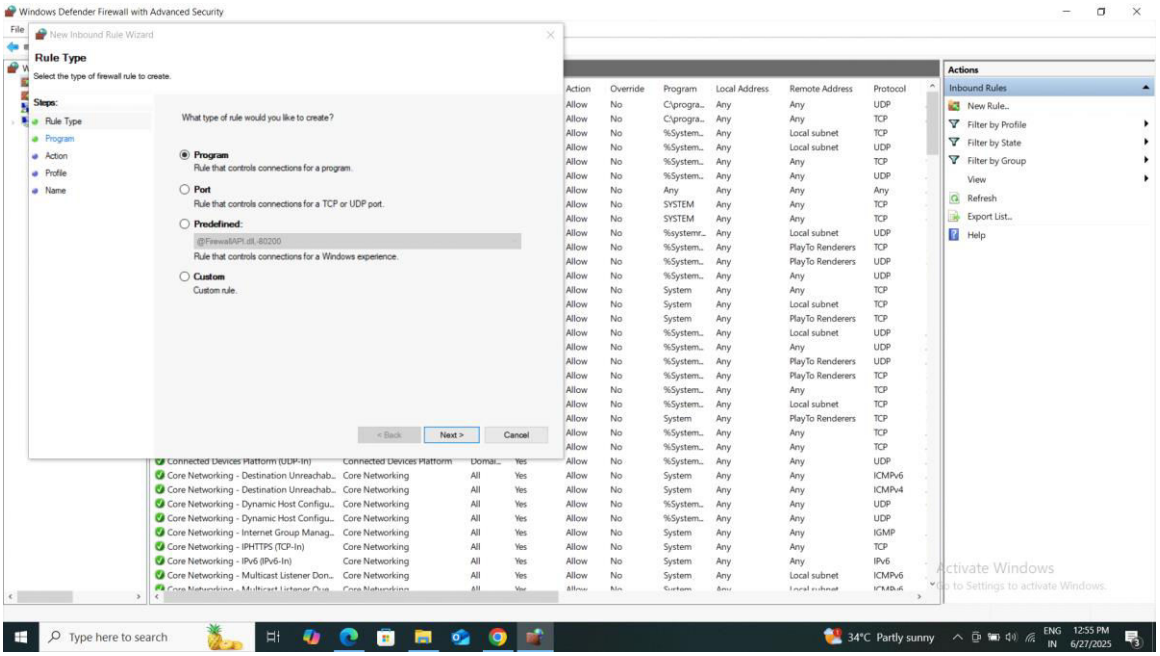
2. Listed Existing Rules

Viewed current Inbound Rules and Outbound Rules.



3. Created a Rule to Block Port 23 (Telnet)

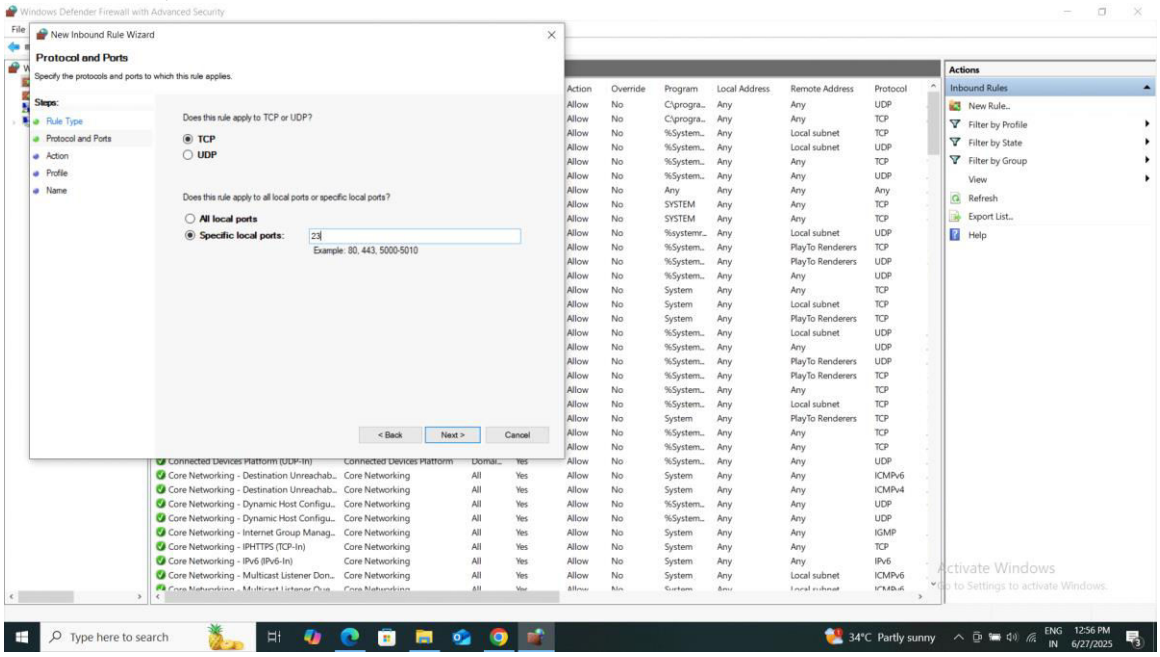
Opened New Inbound Rule Wizard



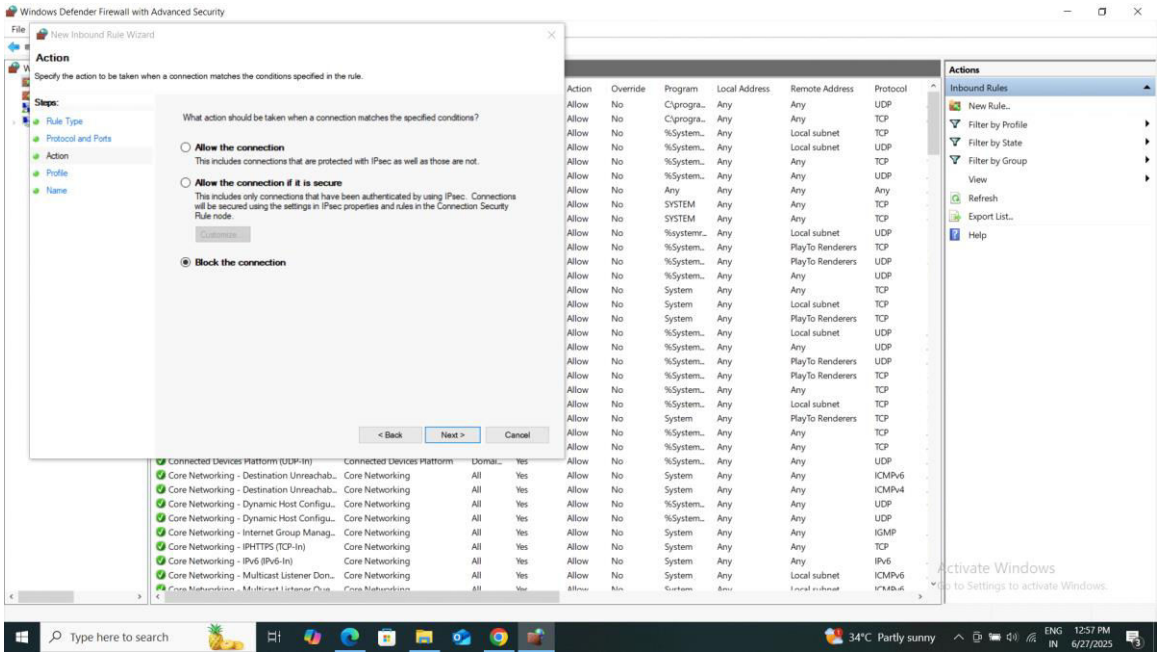
Selected:

i. Rule Type: Port

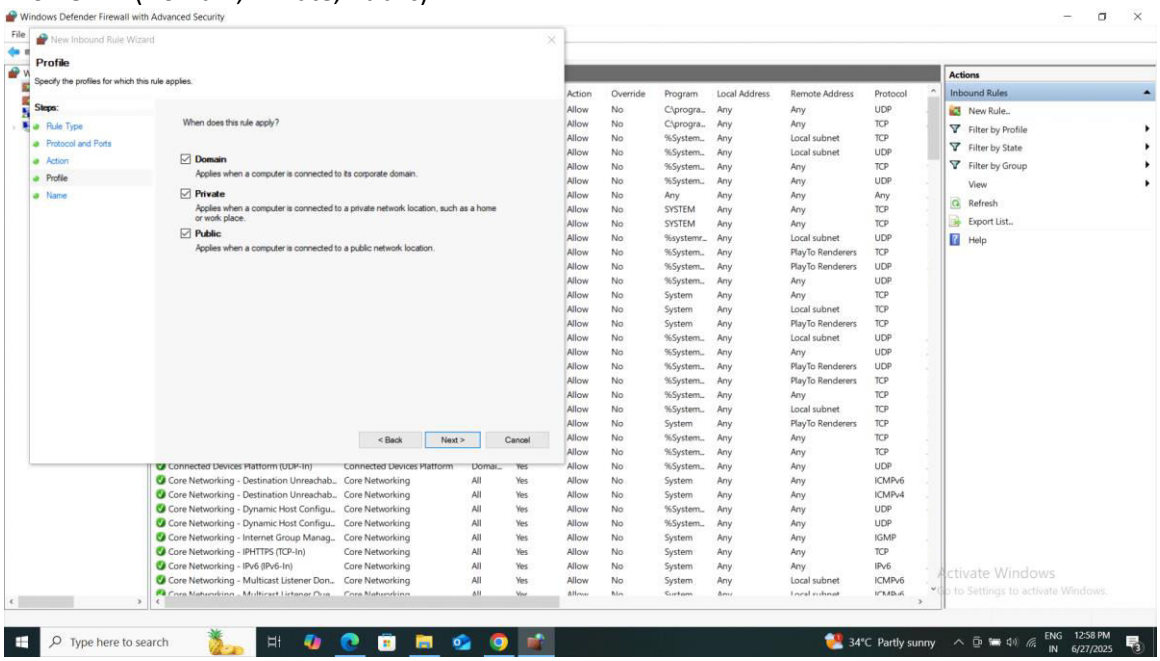
ii. Protocol: TCP, Port 23



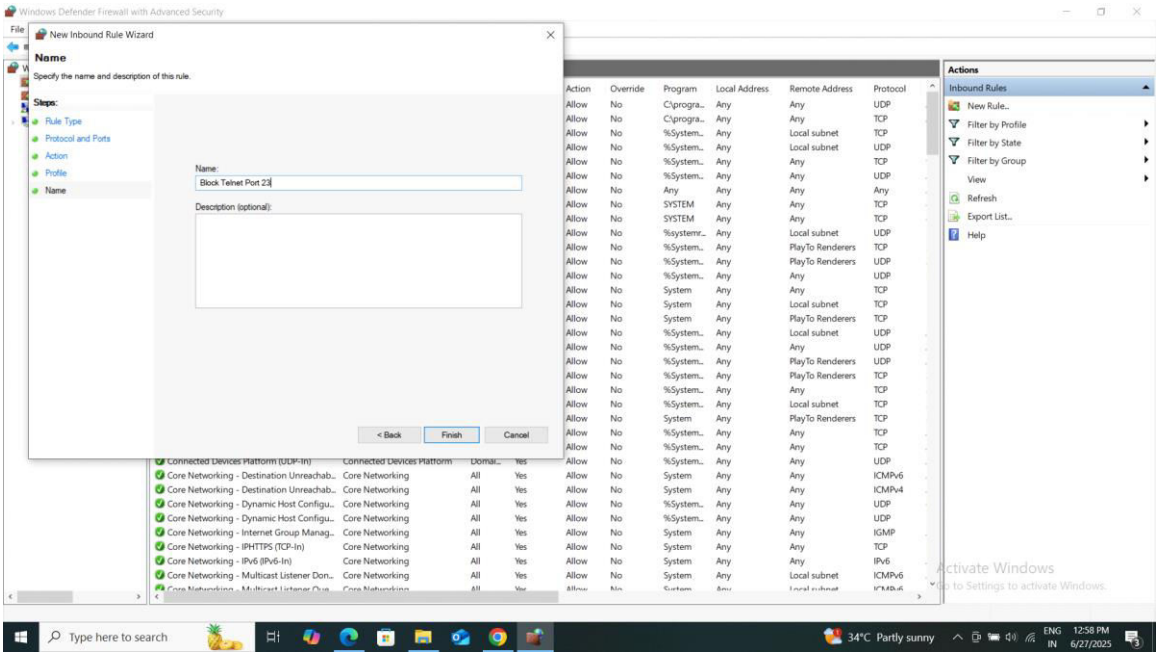
iii. Action: Block the connection



iv. Profile: All (Domain, Private, Public)

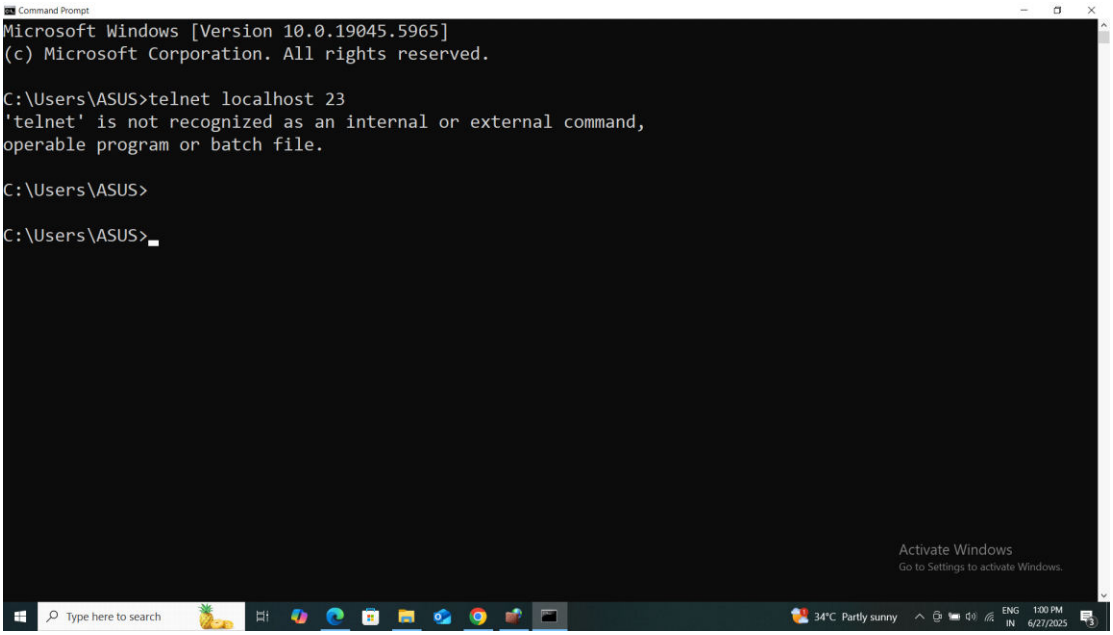


v. Name: Block Telnet Port 23



4. Tested the Block Rule:

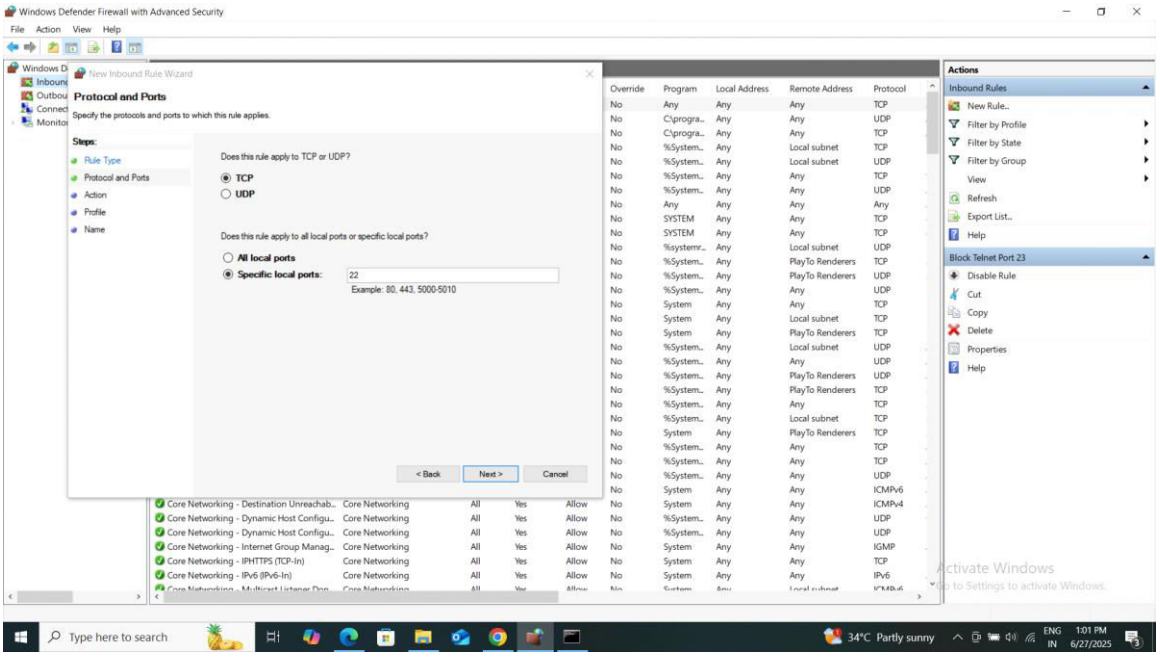
- Installed Telnet via Windows Features
- Ran: telnet localhost 23
- Result: Connection failed, as expected

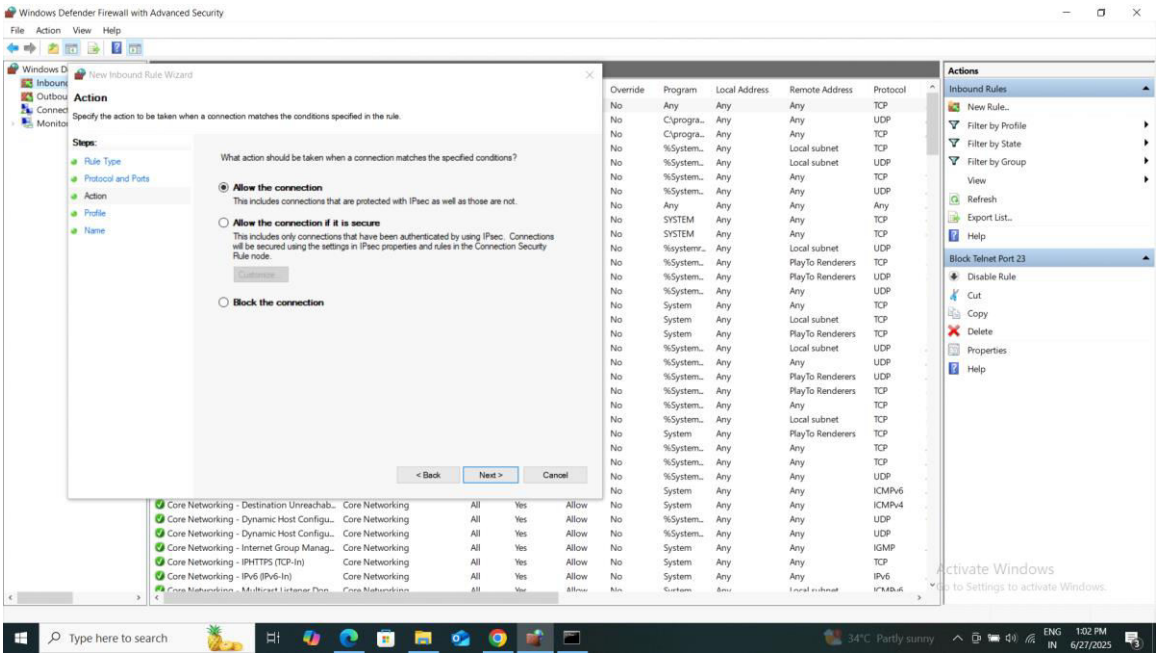


5. Created a Rule to Allow Port 22 (SSH)

Created new rule with:

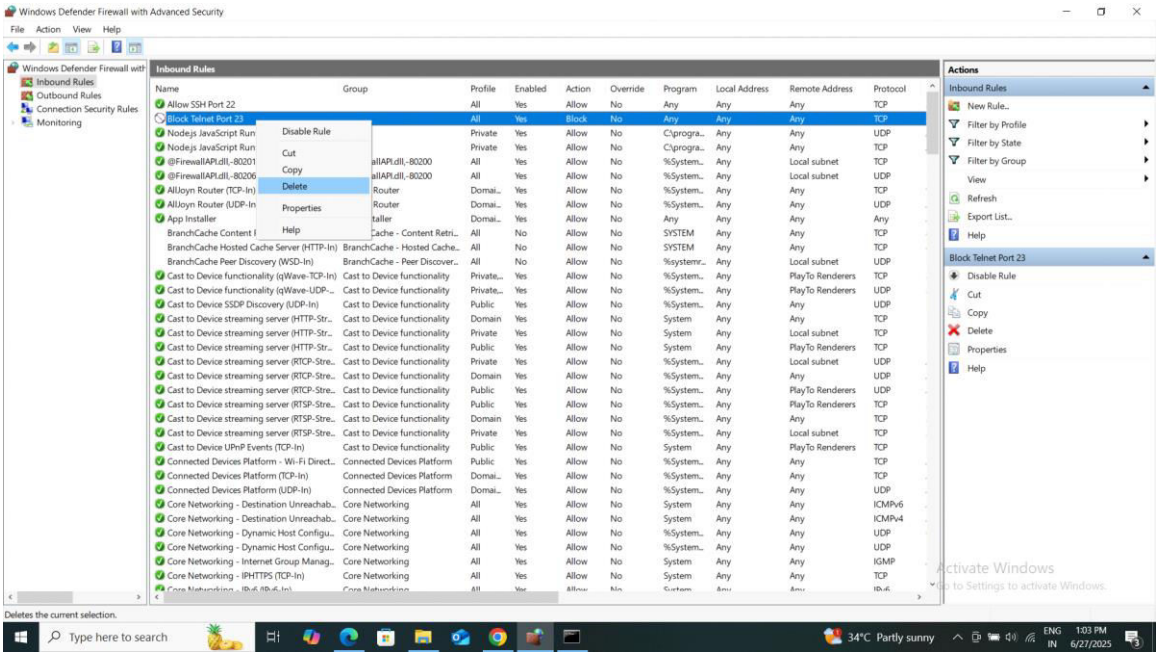
- Protocol: TCP, Port 22
- Action: Allow the connection
- Name: Allow SSH Port 22





6. Removed the Telnet Block Rule

Deleted Block Telnet Port 23 from Inbound Rules.



Summary: How Windows Firewall Filters Traffic

Windows Firewall filters network traffic using rules that allow or block connections based on:

- Port numbers
- Protocol (TCP/UDP)

Application

- Network profile (Domain, Private, Public)
- Inbound Rules control traffic entering the computer.
- Outbound Rules control traffic leaving the computer.

This helps secure the system against unauthorized access and restricts unnecessary exposure.