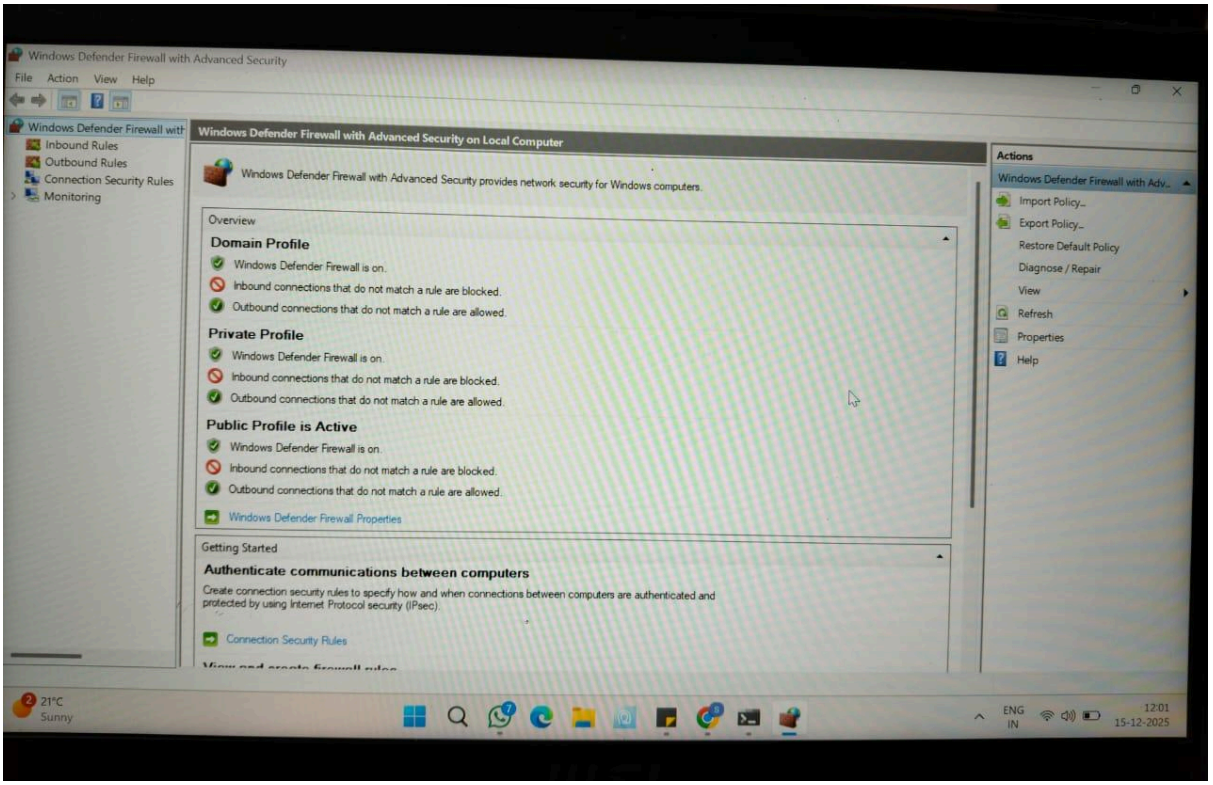
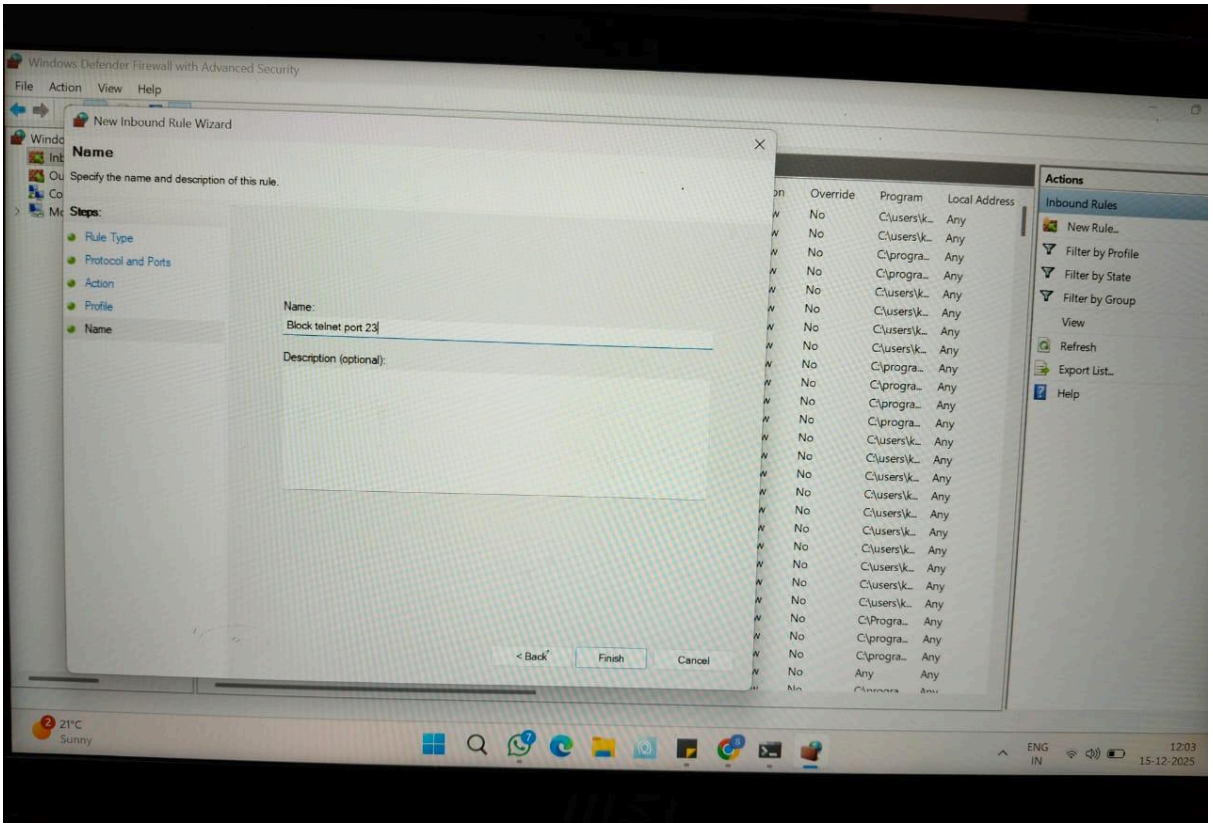
Task 4 : Setup and Use a Firewall on Windows/Linux

- **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.

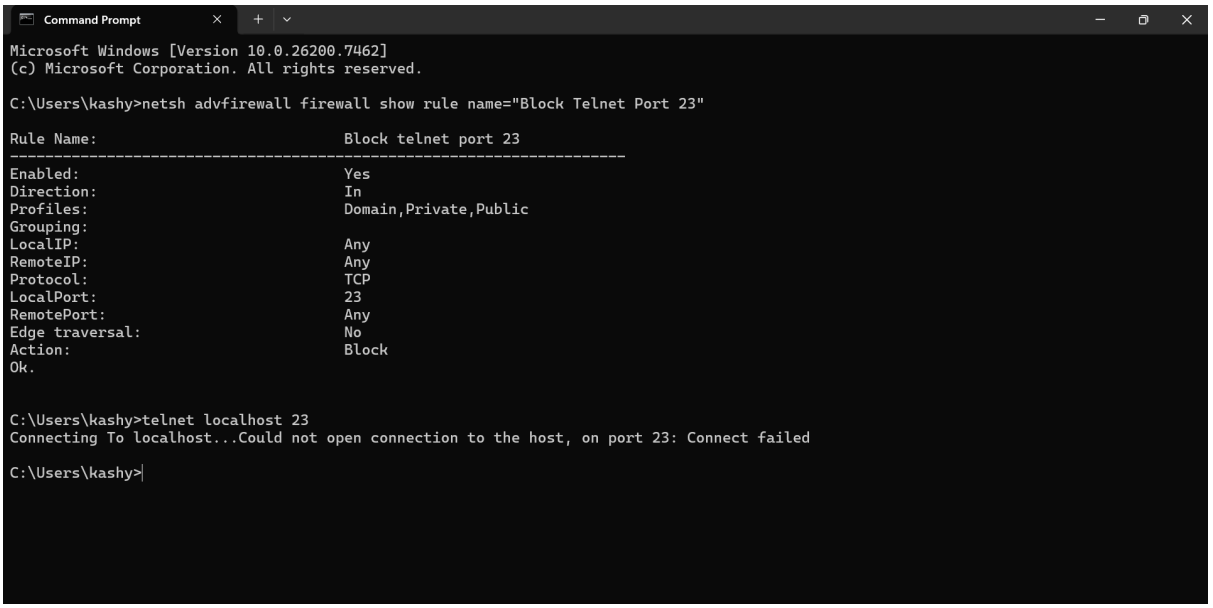
Since Windows Firewall doesn't allow screenshots , I captured the events through different devices. Here's a list of rules in firewall.



Further steps were taken to add the rule:



Now to test the rule on command line it can be showed whether the rule is enabled and further working or not.



Even though port 22 for SSH is for Linux , I applied in Windows to practice adding or removing Firewall rules.

```
C:\Users\kashy>netsh advfirewall firewall show rule name="Allow SSH Port 22"

No rules match the specified criteria.


C:\Users\kashy>netsh advfirewall firewall show rule name="Allow SSH 22 port"

Rule Name:                            Allow SSH 22 port
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            22
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow
Ok.


C:\Users\kashy>
```

Now after deleting the rules from the firewall and then testing again…

```
C:\Users\kashy>netsh advfirewall firewall show rule name="Allow SSH 22 port"

Rule Name:                            Allow SSH 22 port
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            22
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow
Ok.


C:\Users\kashy>netsh advfirewall firewall show rule name="Block Telnet Port 23"

No rules match the specified criteria.
```

This is how the original state was achieved for Windows.

Commands Used ➖

- wf.msc
- telnet localhost 23
- Netsh advfirewall show rule name=”Block telnet Port 22”

GUI Steps Used ➖

- Windows Defender Firewall with Advanced Security
- Inbound Rules → New Rule → Port-based filtering
- Block and Allow actions tested

Summary

Windows Defender Firewall filters network traffic by evaluating inbound and outbound packets against predefined rules. These rules are based on ports, protocols, IP addresses, and connection profiles. When traffic matches a blocking rule, it is denied access; when it matches an allowed rule, it is permitted. This ensures controlled access and protects the system from unauthorized network communication.