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

Name: Rahul Malatesh Sannapujar

Date: 26/09/2025

Objective

To configure and test basic firewall rules on Windows, specifically to block and test traffic on port 23 Telnet.

Tools Used

Windows Defender Firewall.

Telnet (built-in Windows client).

Command Prompt

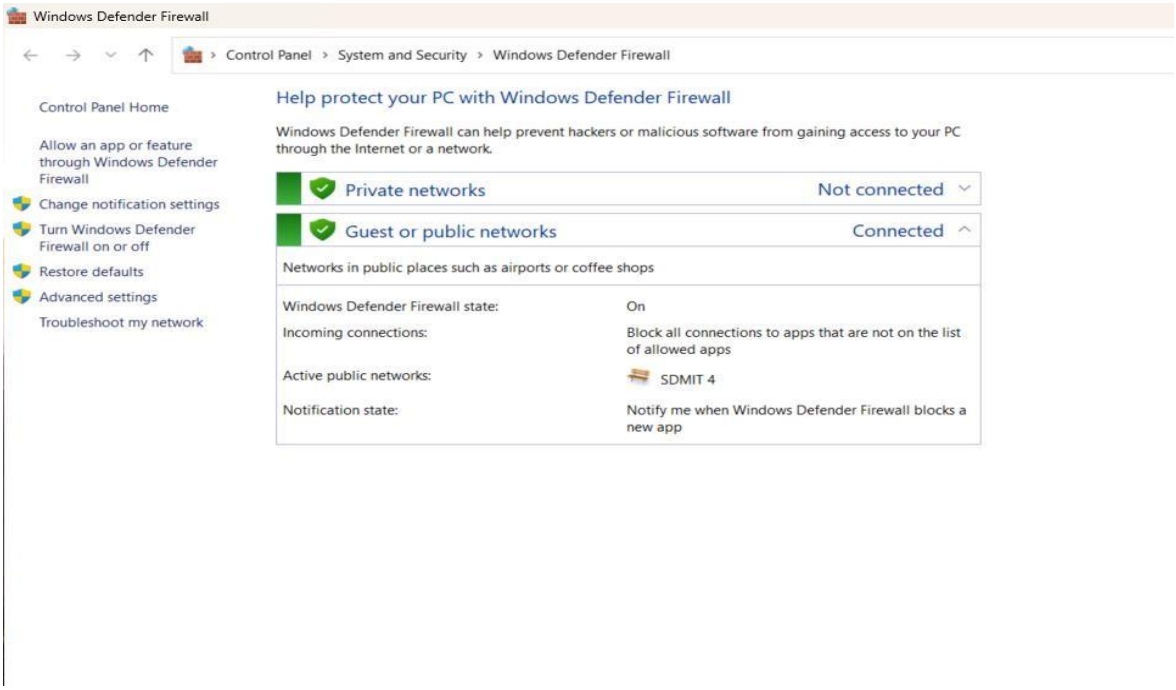
Screenshots for validation

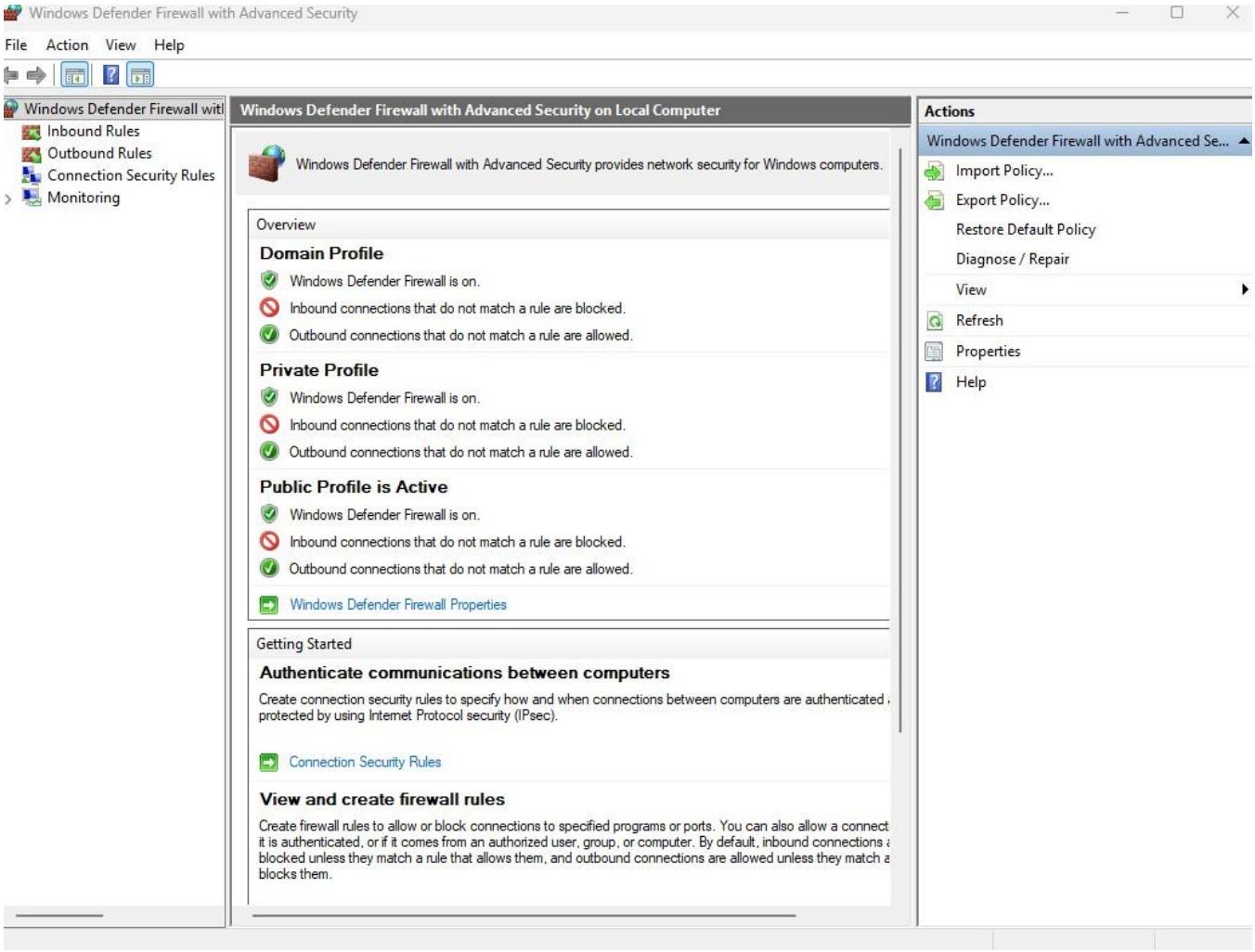
Step-by-Step Implementation

1. Open Windows Defender Firewall

Accessed via the Control Panel.

- Verified that firewall is enabled for private, public, and domainprofiles.





2. Create New Inbound Rule Block Port 23

Navigated to 'Advanced Settings' → 'Inbound Rules'.

Used 'New Rule Wizard' to configure rule: ○

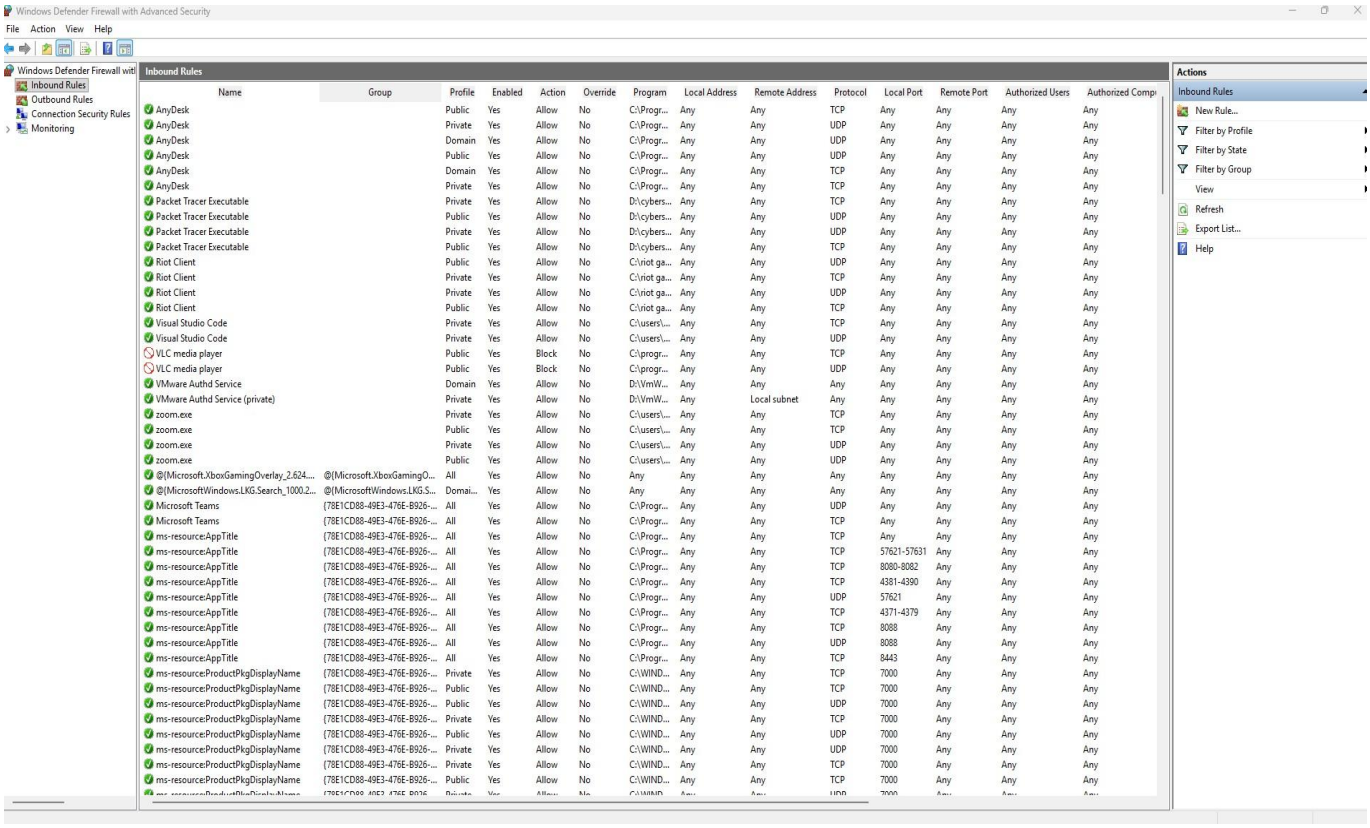
Rule Type: Port

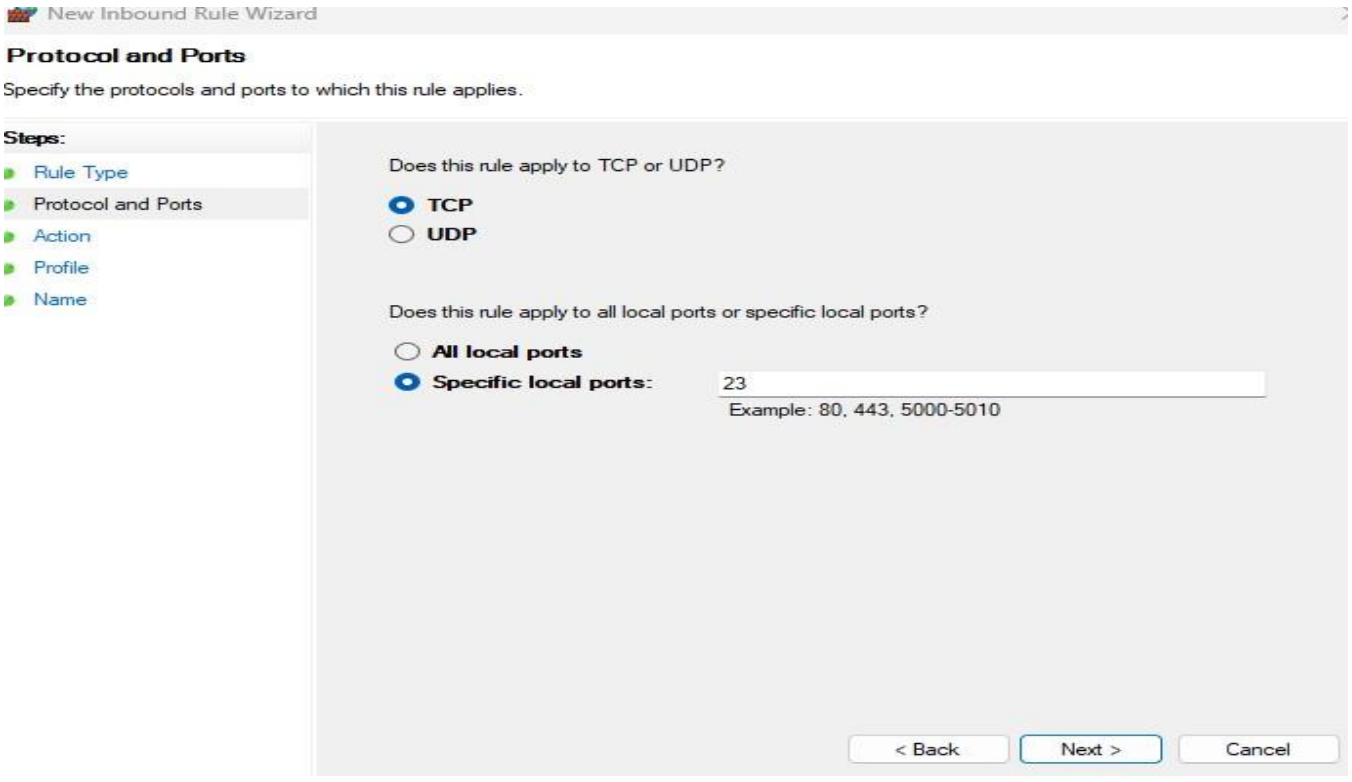
○ **Protocol**: TCP

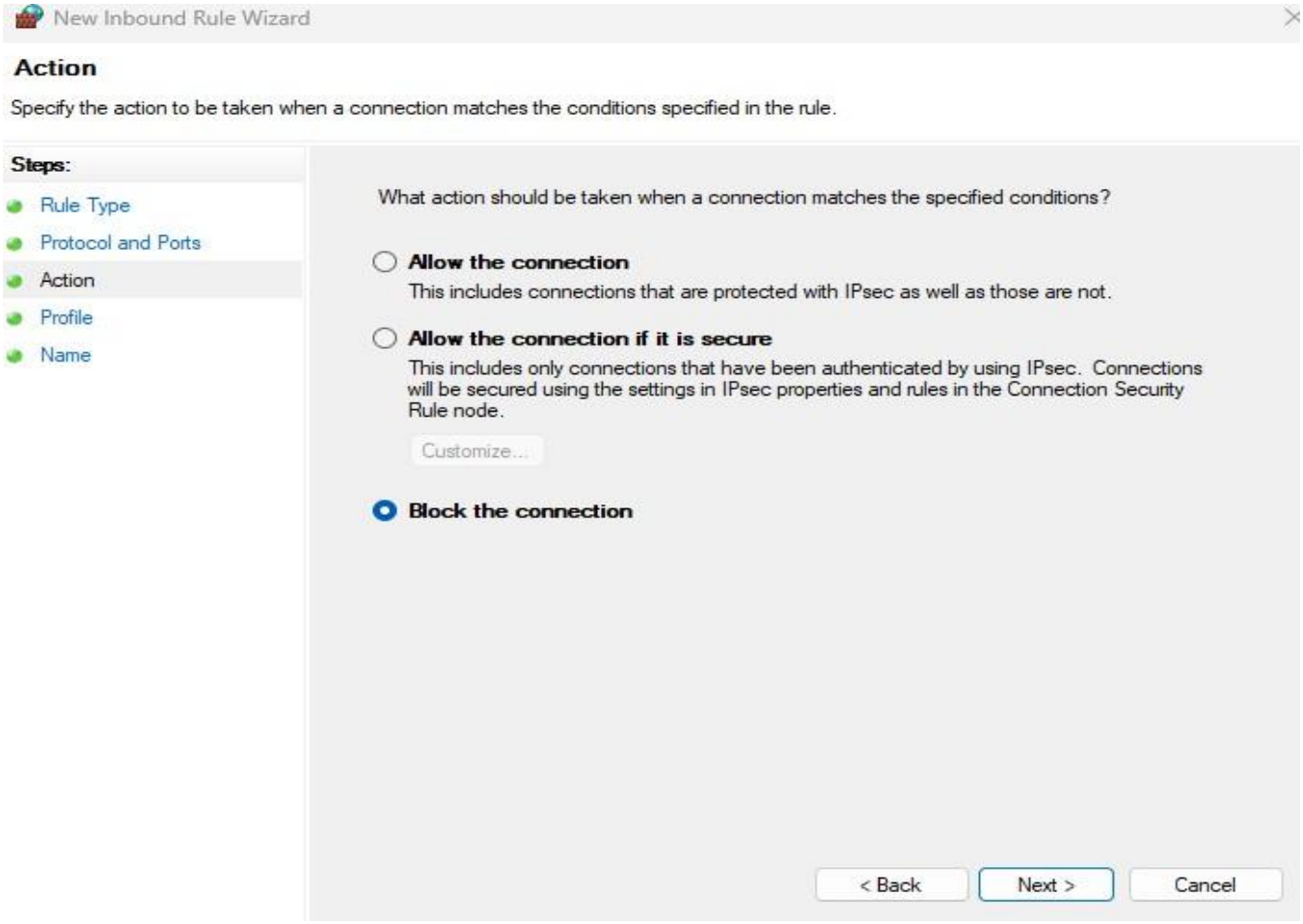
○ **Port**: 23

○ **Action**: Block the connection.

- Confirmed the rule named "Port 23" was created and active.


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with Advanced Security
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol Local Port Remote Port Authorized Users Authorized Compu
AnyDesk Public Yes Allow No C:\Progr... Any Any TCP Any Any Any Any
AnyDesk Private Yes Allow No C:\Progr... Any Any UDP Any Any Any Any
AnyDesk Domain Yes Allow No C:\Progr... Any Any UDP Any Any Any Any
AnyDesk Public Yes Allow No C:\Progr... Any Any UDP Any Any Any Any
AnyDesk Domain Yes Allow No C:\Progr... Any Any TCP Any Any Any Any
AnyDesk Private Yes Allow No C:\Progr... Any Any TCP Any Any Any Any
Packet Tracer Executable Private Yes Allow No D:\cybers... Any Any TCP Any Any Any Any
Packet Tracer Executable Public Yes Allow No D:\cybers... Any Any UDP Any Any Any Any
Packet Tracer Executable Private Yes Allow No D:\cybers... Any Any UDP Any Any Any Any
Packet Tracer Executable Public Yes Allow No D:\cybers... Any Any TCP Any Any Any Any
Riot Client Public Yes Allow No C:\riot ga... Any Any UDP Any Any Any Any
Riot Client Private Yes Allow No C:\riot ga... Any Any TCP Any Any Any Any
Riot Client Private Yes Allow No C:\riot ga... Any Any UDP Any Any Any Any
Riot Client Public Yes Allow No C:\riot ga... Any Any TCP Any Any Any Any
Visual Studio Code Private Yes Allow No C:\users\... Any Any TCP Any Any Any Any
Visual Studio Code Private Yes Allow No C:\users\... Any Any UDP Any Any Any Any
VLC media player Public Yes Block No C:\progr... Any Any TCP Any Any Any Any
VLC media player Public Yes Block No C:\progr... Any Any UDP Any Any Any Any
VMware Authd Service Domain Yes Allow No D:\VmW... Any Any Any Any Any Any Any
VMware Authd Service (private) Private Yes Allow No D:\VmW... Any Local subnet Any Any Any Any
zoom.exe Private Yes Allow No C:\users\... Any Any TCP Any Any Any Any
zoom.exe Public Yes Allow No C:\users\... Any Any TCP Any Any Any Any
zoom.exe Private Yes Allow No C:\users\... Any Any UDP Any Any Any Any
zoom.exe Public Yes Allow No C:\users\... Any Any UDP Any Any Any Any
@{Microsoft.XboxGamingOverlay_2.624.... @{Microsoft.XboxGamingO... All Yes Allow No Any Any Any Any Any Any Any Any
@{MicrosoftWindows.LKG.Search_1000.2... @{MicrosoftWindows.LKG.S... Domai... Yes Allow No Any Any Any Any Any Any Any Any
Microsoft Teams {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any UDP Any Any Any Any
Microsoft Teams {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any TCP Any Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any TCP Any Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any TCP 57621-57631 Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any TCP 8080-8082 Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any TCP 4381-4390 Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any UDP 57621 Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any TCP 4371-4379 Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any TCP 8088 Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any UDP 8088 Any Any Any
ms-resource:AppTitle {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progr... Any Any TCP 8443 Any Any Any
ms-resource:ProductPkgDisplayName {78E1CD88-49E3-476E-B926-... Private Yes Allow No C:\WIND... Any Any TCP 7000 Any Any Any
ms-resource:ProductPkgDisplayName {78E1CD88-49E3-476E-B926-... Public Yes Allow No C:\WIND... Any Any TCP 7000 Any Any Any
ms-resource:ProductPkgDisplayName {78E1CD88-49E3-476E-B926-... Public Yes Allow No C:\WIND... Any Any UDP 7000 Any Any Any
ms-resource:ProductPkgDisplayName {78E1CD88-49E3-476E-B926-... Private Yes Allow No C:\WIND... Any Any TCP 7000 Any Any Any
ms-resource:ProductPkgDisplayName {78E1CD88-49E3-476E-B926-... Public Yes Allow No C:\WIND... Any Any UDP 7000 Any Any Any
ms-resource:ProductPkgDisplayName {78E1CD88-49E3-476E-B926-... Private Yes Allow No C:\WIND... Any Any UDP 7000 Any Any Any
ms-resource:ProductPkgDisplayName {78E1CD88-49E3-476E-B926-... Private Yes Allow No C:\WIND... Any Any TCP 7000 Any Any Any
ms-resource:ProductPkgDisplayName {78E1CD88-49E3-476E-B926-... Public Yes Allow No C:\WIND... Any Any TCP 7000 Any Any Any
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

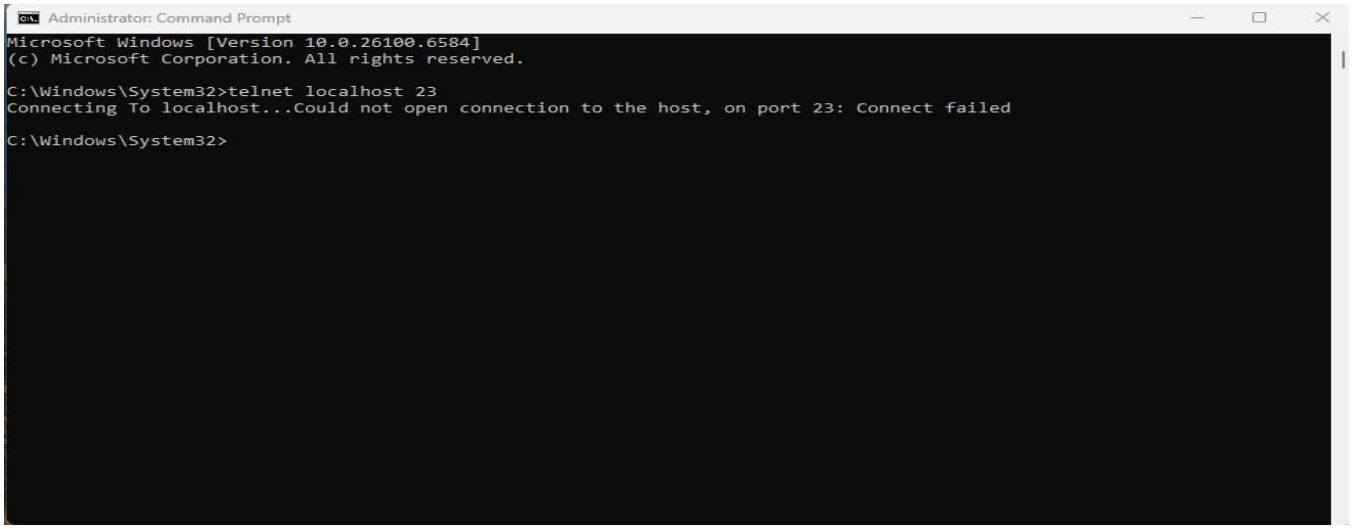

New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
23
Example: 80, 443, 5000-5010
< Back
Next >
Cancel



3. Test Port Blocking with Telnet

Ran `telnet localhost 23` in Command Prompt.

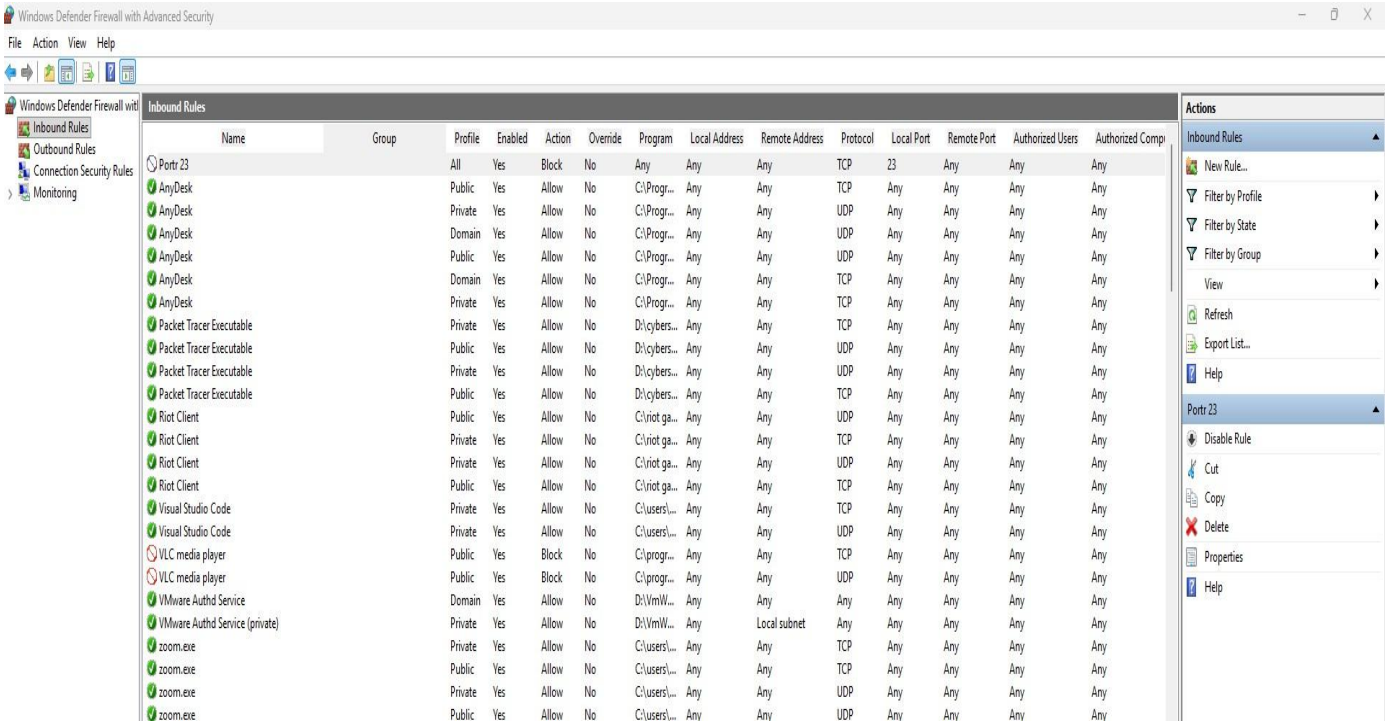
Observed message: "Could not open connection to the host, on port 23 Connect failed." Also tested port 22 to confirm no service was running and rule effectiveness.



4. Remove Inbound Rule for Port 23

Located "Portr 23" rule in Inbound Rules list.

- Deleted rule to restore system to original state after testing.



5. Final Firewall Status Check

Verified restored settings in Windows Defender Firewall.

6. Commands and Steps Used

- Accessed firewall via Control Panel and `wf.msc`.
- Created inbound blocking rule for port 23 using Advanced Settings.

Used Telnet via `telnet localhost 23` for verification.

Removed rule and checked firewall status.

7. Explanation: How Firewall Filters Traffic

A firewall filters network packets according to specified rules. In this task, blocking port 23 ensures that Telnet connections cannot be established, improving system security by preventing remote access via an insecure protocol. When a rule is active, incoming traffic matching the rule TCP on port 23) is rejected; once removed, traffic can pass if a service is present.

Conclusion

This task successfully demonstrated the configuration and testing of firewall rules on Windows Defender Firewall to block inbound traffic on port 23 (Telnet). By creating a rule to specifically block this port, the system effectively prevented Telnet connections, as verified through Telnet client tests resulting in connection failures. Removing the rule restored normal traffic flow. This process illustrated fundamental firewall management skills, including creating, verifying, and deleting firewall rules, which are essential for enhancing system network security. Proper firewall configuration helps protect against unauthorized access and potential network threats by filtering incoming and outgoing traffic based on defined rules.