Objective Configure and test basic firewall rules to allow or block traffic using Windows Firewall. System Used OS: Windows 10

Tool: Windows Defender Firewall with Advanced Security

Testing Tool: Telnet (Enabled via Windows Features)

# Step-by-Step Implementation

# Step 1: Open Firewall Tool Opened “Windows Defender Firewall with Advanced Security” via Start menu.

#Step 2: Listed Current Inbound Rules Clicked “Inbound Rules” to view existing firewall rules

#Step 3: Created Block Rule for Port 23 (Telnet)Created a new inbound rule:

Rule Type: Port

Protocol: TCP

Port: 23

Action: Block the connection

Applied to: Domain, Private, Public

Name: Block Telnet Port 23

#Step 4: Tested Telnet on Port 23Enabled Telnet client (via Windows Features)

Ran:

telnet localhost 23Output:

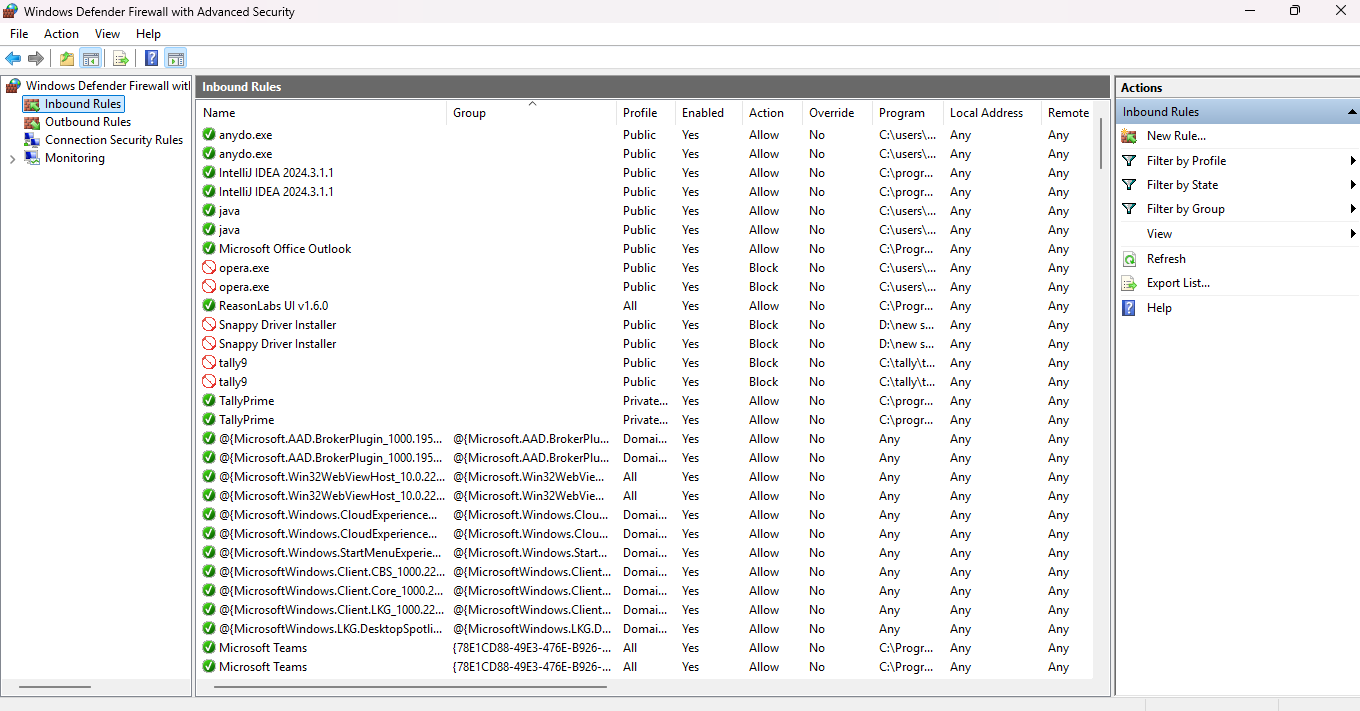
Could not open connection to the host, on port 23: Connect failed (connection failed)

# Step 5: (Optional) Allowed SSH (Port 22) Added a new inbound rule to allow TCP traffic on port 22

#Step 6: Removed Telnet Block Rule Deleted the “Block Telnet Port 23” rule to restore original firewall state.

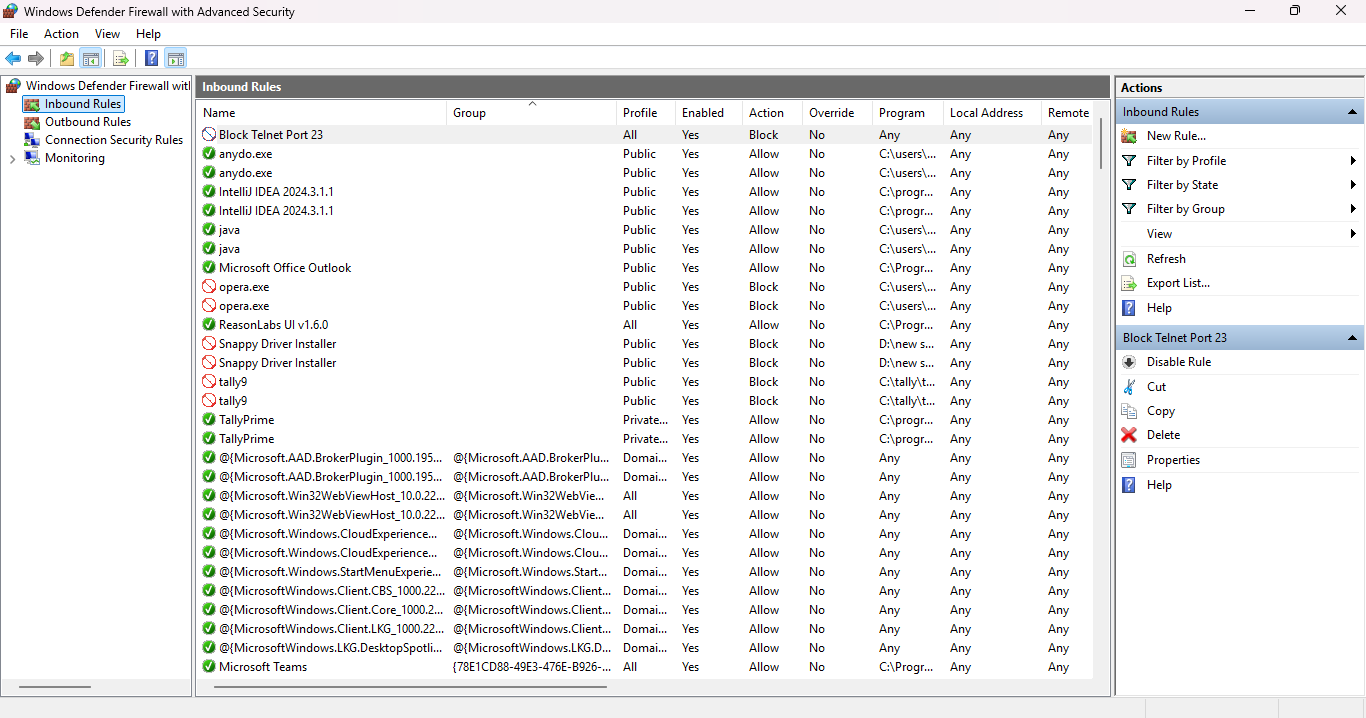
Firewall Summary Windows Firewall filters inbound and outbound network traffic using defined rules. These rules can be based on port number, application, IP address, or protocol. Blocking port 23 prevents Telnet connections, which enhances security by stopping remote access through that port.

Commands & Tools Used Tool Task Windows Defender Firewall Rule creation/deletion Telnet (CMD)Port test Windows Features Telnet installation.



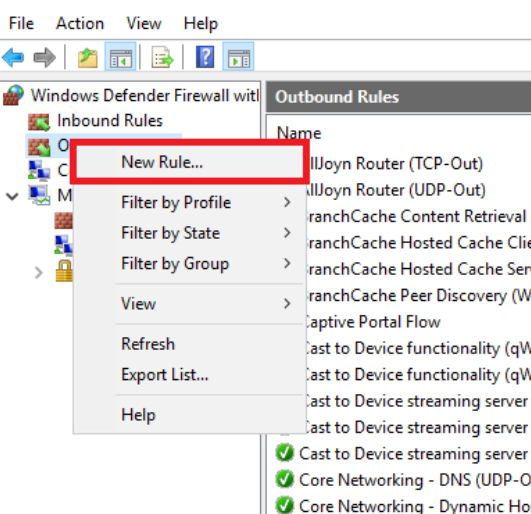
Screenshot of firewall\_open.png.

→ Opened Windows Defender Firewall with Advanced Security



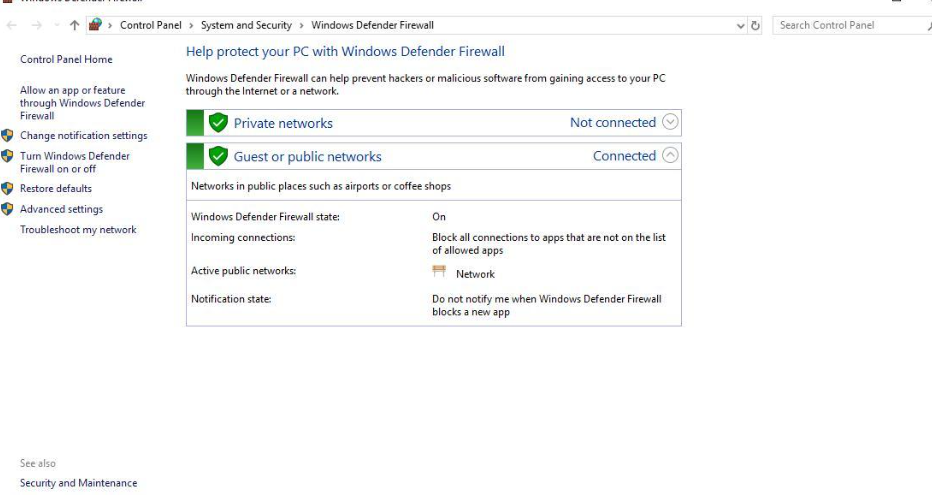
Screenshot of inbound\_rules.png

→ Displayed list of existing inbound rules.



Screenshot of block\_port23.png

→ Created a new rule to block TCP traffic on port 23 (Telnet)



Screenshot of rule\_deleted.png

→ Deleted the Telnet block rule to restore default state