[Task 4]

Title: Windows Firewall Configuration Guide

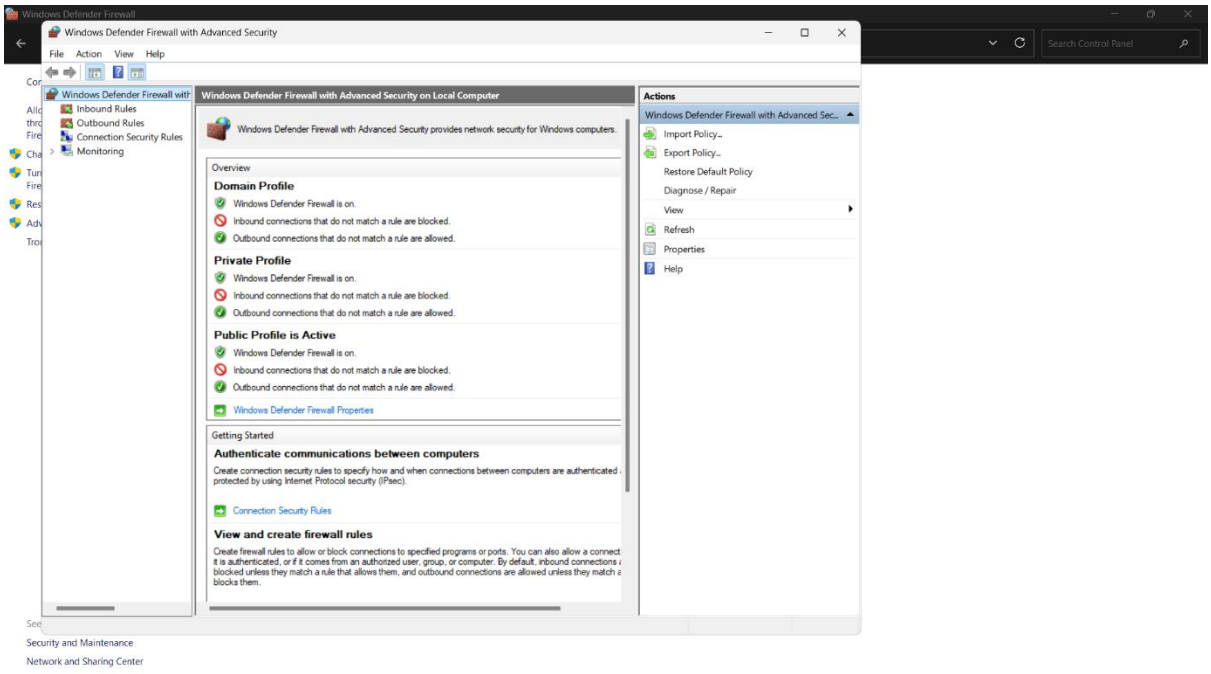
Objective: Block unwanted inbound traffic on specific ports to enhance system security.

Requirement: - Operating System: Windows 10/11 with administrative privileges,linux{optional}

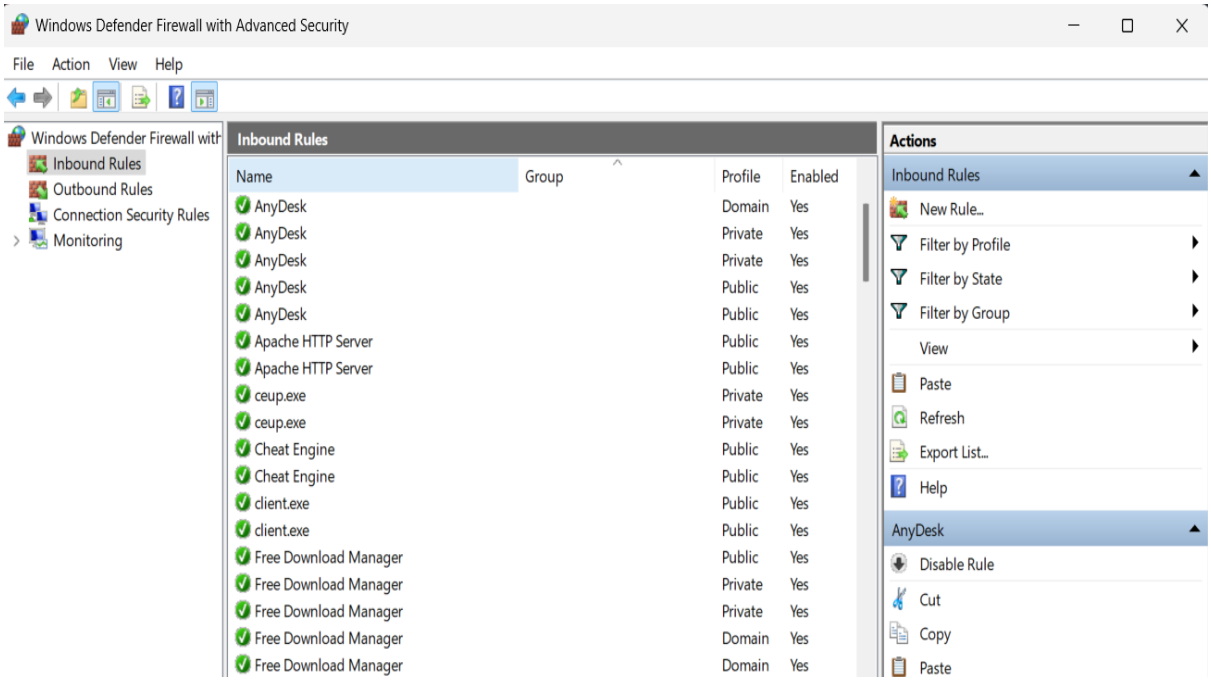
1. **Software:** Windows Defender Firewall (built-in).
2. **Tools:**
    - Access to **Windows Firewall with Advanced Security**.
    - Optional: Text editor (Notepad/Word) to export rules for documentation.
3. **Objective:** Block unwanted inbound traffic on specific ports to secure the system from potential threats.

Steps Performed:

1. **Open Windows Firewall**
    - Press Win + S, type **"Windows Defender Firewall"**, and press **Enter**.

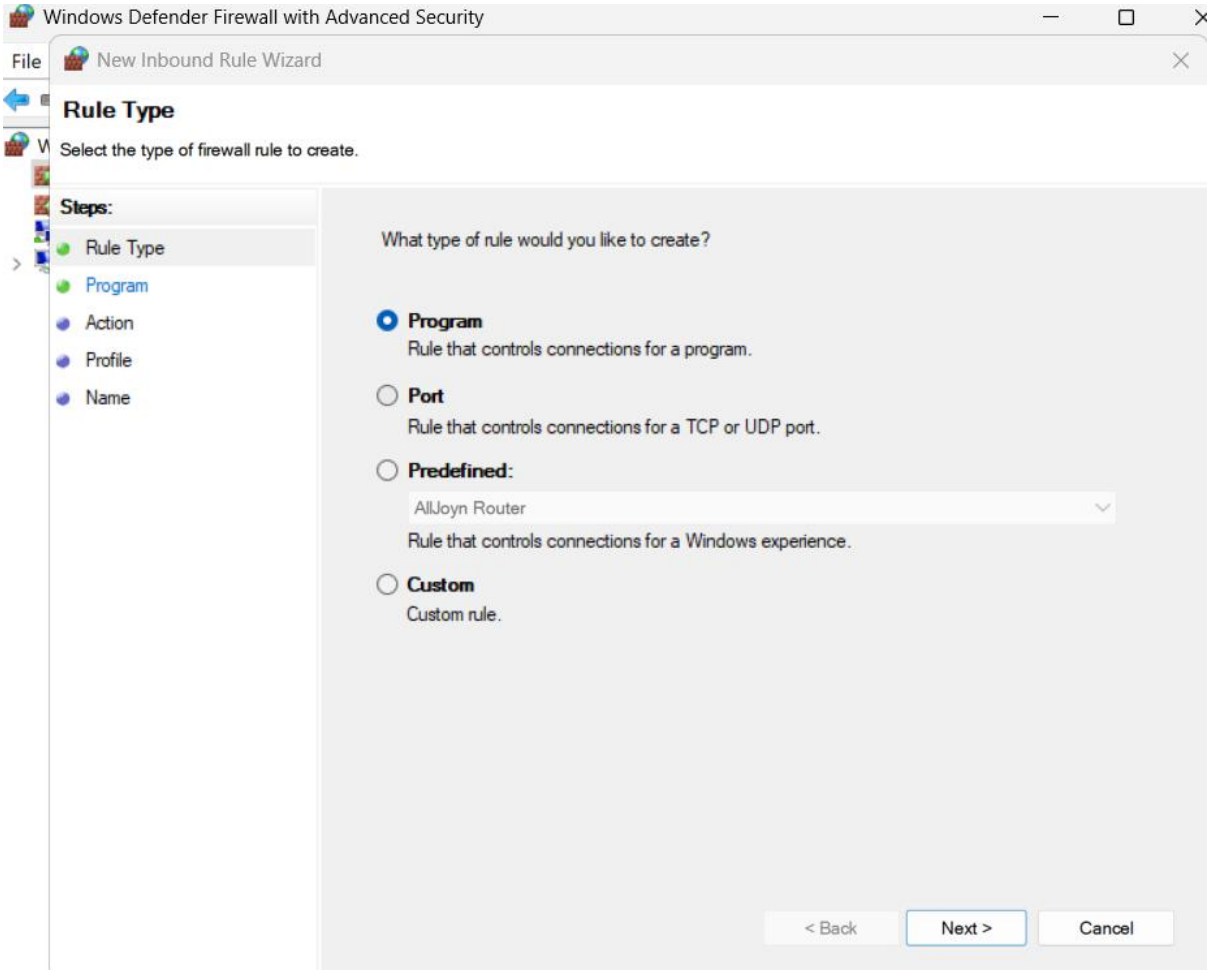


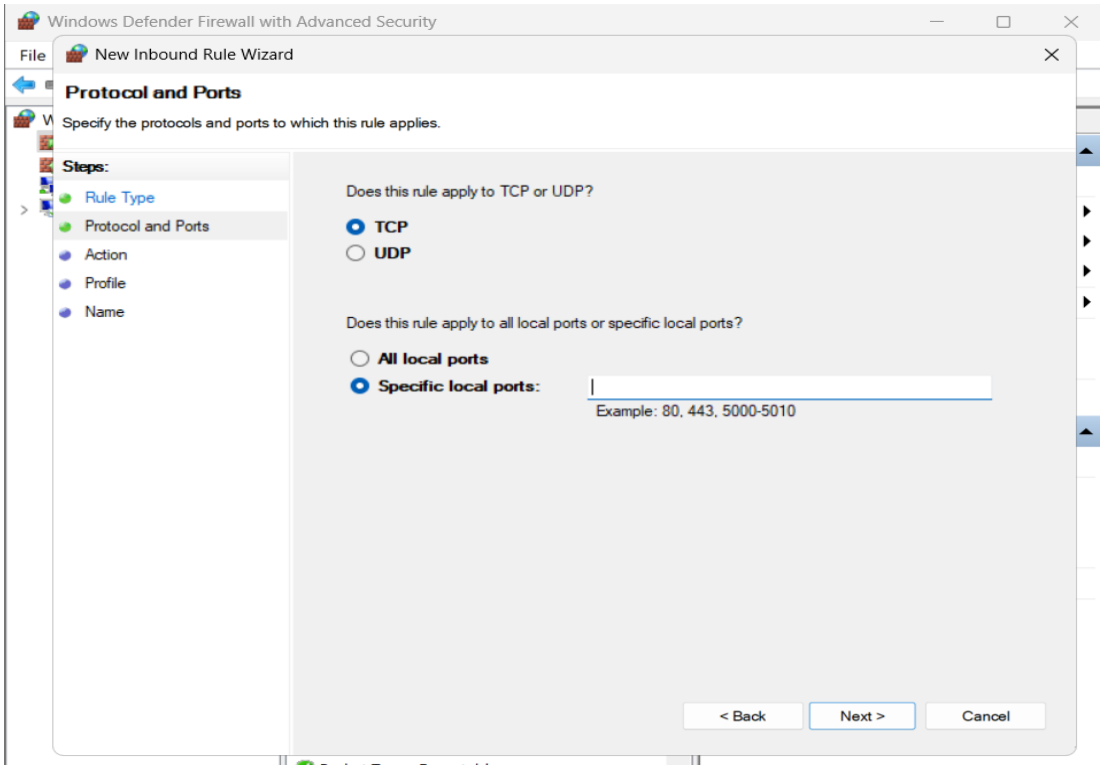
2. **Check Current Firewall Rules**
    - Click **“Advanced Settings”** on the left.
    - In the **Windows Defender Firewall with Advanced Security** window, view existing **Inbound Rules** and **Outbound Rules**.

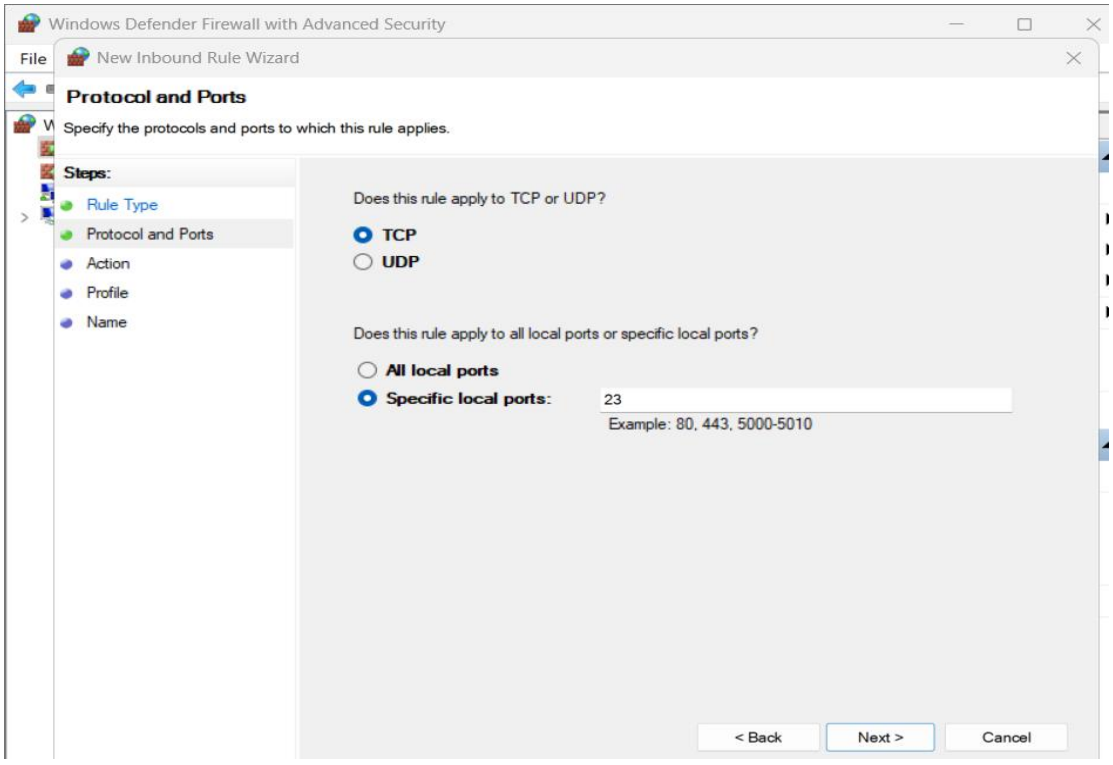


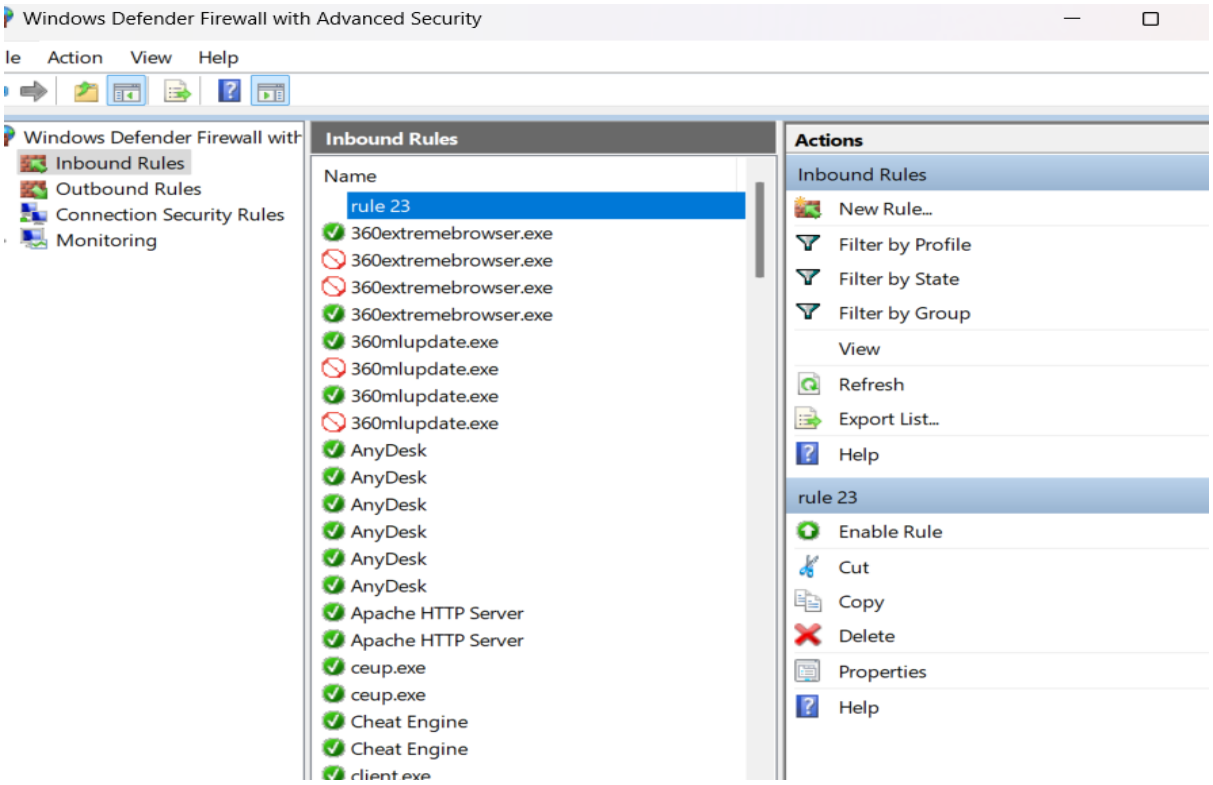

```
C:\Users\LENOVO>netsh advfirewall firewall show rule name=all

Rule Name:                            rule 23
----------------------------------------------------------------------
Enabled:                              No
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            23
RemotePort:                           Any
Edge traversal:                       No
Action:                               Block

Rule Name:                            Google Chrome (mDNS-In)
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:                             Google Chrome
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             UDP
LocalPort:                            5353
RemotePort:                           Any
```

3. **Add a New Rule to Block a Port**
    - In the left pane, select **Inbound Rules** → Click **New Rule…** on the right.
    - Select **Port** → Click **Next**.
    - Choose **TCP** or **UDP**, and enter the port number to block (e.g., 23 for Telnet) → Click **Next**.
    - Select **Block the connection** → Click **Next**.
    - Apply the rule to **Domain, Private, and Public** networks → Click **Next**.
    - Give the rule a **name** (e.g., "rule 23") → Click **Finish**

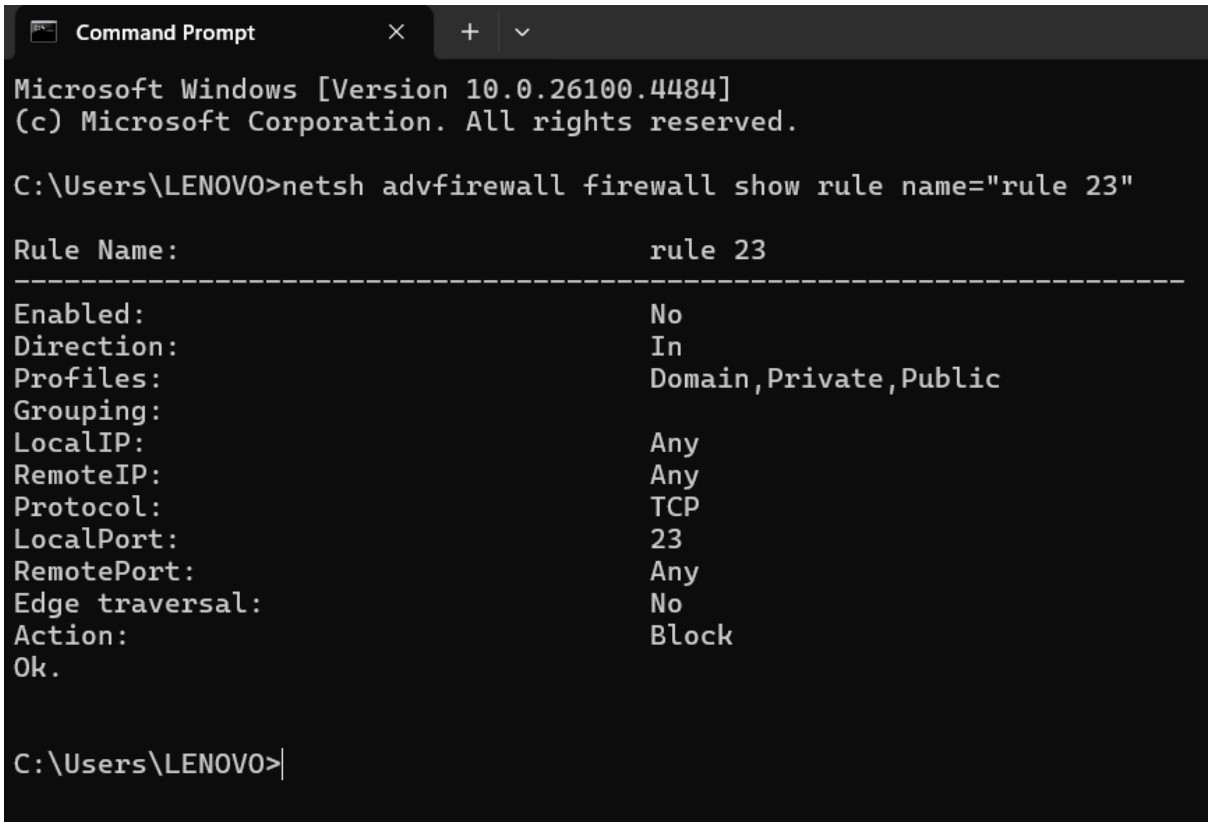



Windows Defender Firewall with Advanced Security
File
New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific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


Windows Defender Firewall with Advanced Security
File
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



4. **Verify the Rule**
    - Check the **Inbound Rules** list to ensure your new rule appears and is **enabled**.



Conclusion:-

By configuring the Windows Firewall, unwanted inbound traffic on specific ports was successfully blocked, enhancing the security of the system. This exercise demonstrated the importance of monitoring and controlling network access, using built-in Windows tools, and maintaining a secure computing environment. The steps performed are easy to replicate and provide a foundation for managing firewall rules effectively.