

DAY 4 - TASK 4

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.

Firewall Rule Creation, Testing & Removal Report

1) Objective

To configure a firewall rule that blocks inbound TCP connections on Telnet port (23), test its functionality, and restore the original firewall state.

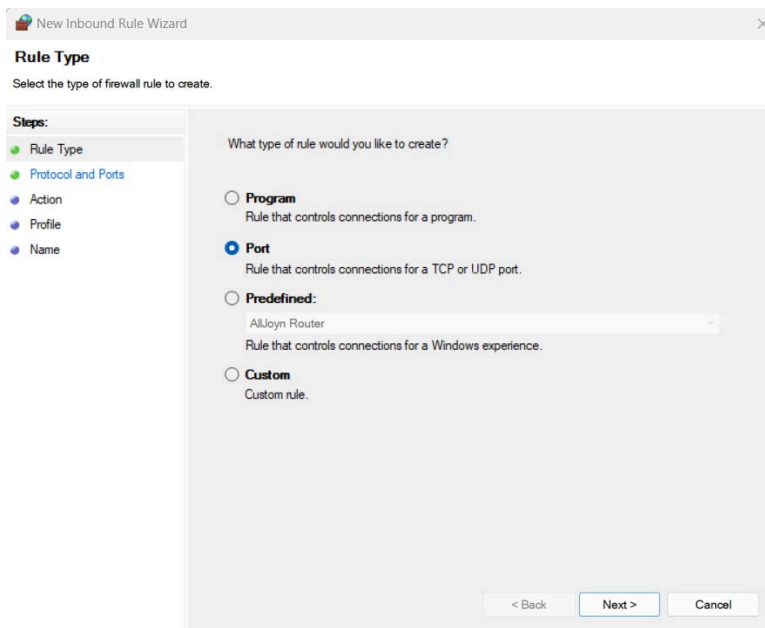
2) Steps -

1. Open Windows Firewall Configuration

- Press **Windows + R**, type **wf.msc**, and press **Enter** to open Windows Defender Firewall with Advanced Security.

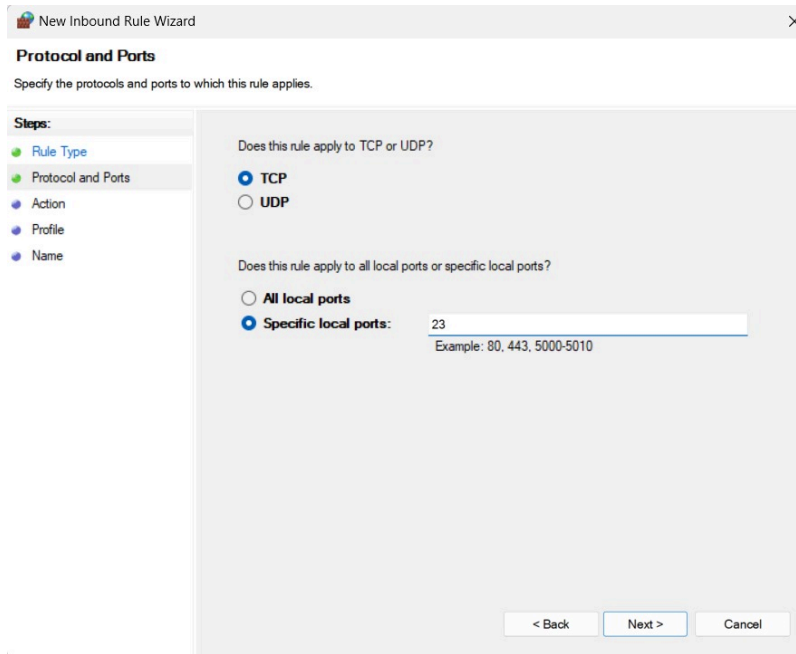
2. Create New Inbound Rule

1. Click **Inbound Rules** → **New Rule**
2. Select **Port** → Click **Next**.



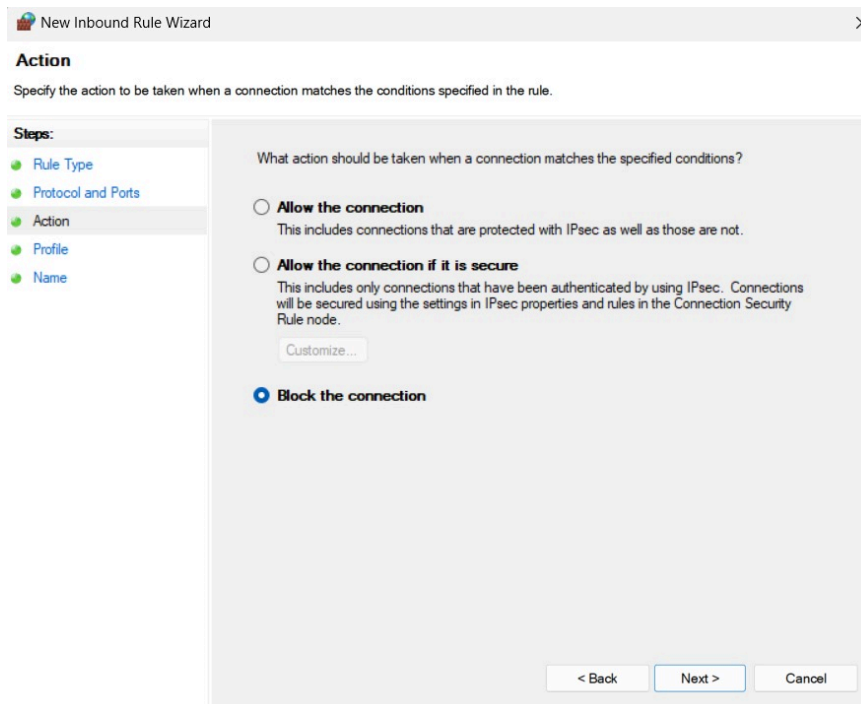
3.

4. Choose **TCP**, enter **23** in **Specific local ports** → Click **Next**.



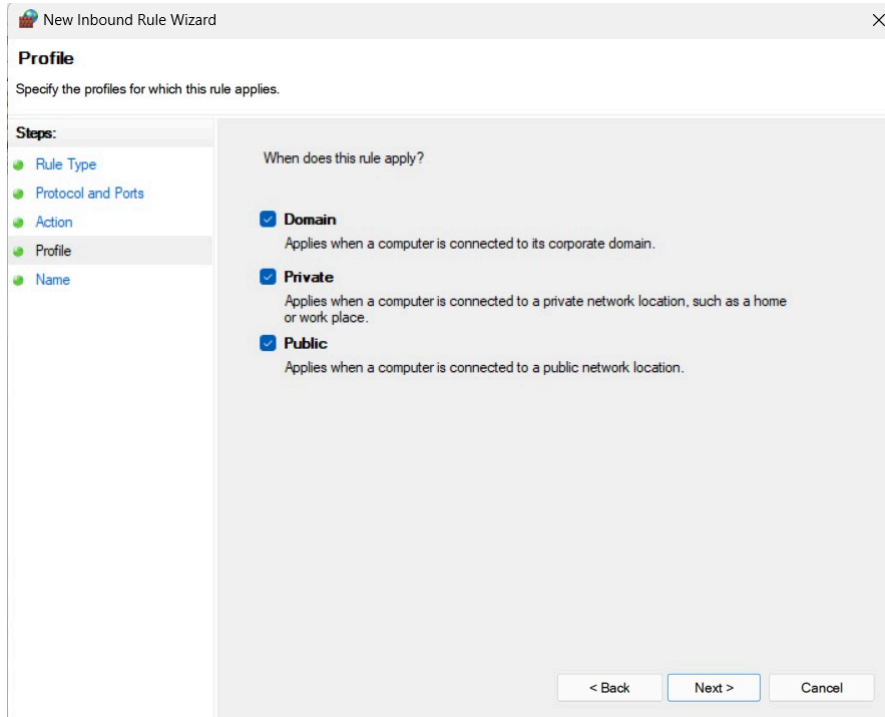
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two questions. The first question is 'Does this rule apply to TCP or UDP?' with radio buttons for TCP (selected) and UDP. The second question is 'Does this rule apply to all local ports or specific local ports?' with radio buttons for All local ports and Specific local ports (selected). A text box next to 'Specific local ports' contains the value '23' and has a hint 'Example: 80, 443, 5000-5010'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

5. Select **Block the connection** → Click **Next**.



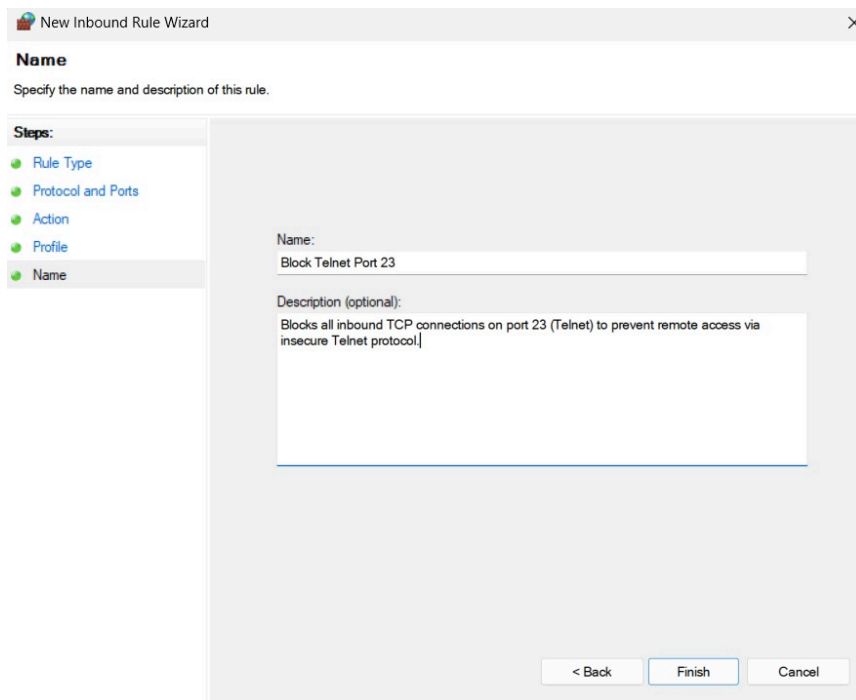
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area contains the question 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (with a sub-note 'This includes connections that are protected with IPsec as well as those are not.'), 'Allow the connection if it is secure' (with a sub-note 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' and a 'Customize...' button), and 'Block the connection' (selected). At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

6. Select all profiles (**Domain**, **Private**, **Public**) → Click **Next**.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Profile' step. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile' (highlighted), and 'Name'. The main area is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

7. Name the rule **Block Telnet Port 23** → Click **Finish**.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Name' step. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name' (highlighted). The main area has a 'Name:' label followed by a text box containing 'Block Telnet Port 23'. Below that is a 'Description (optional):' label followed by a text box containing 'Blocks all inbound TCP connections on port 23 (Telnet) to prevent remote access via insecure Telnet protocol.' At the bottom right are buttons for '< Back', 'Finish', and 'Cancel'.

3. Install Telnet Client for Testing

- Open **Command Prompt as Administrator** and run:

```
dism /online /Enable-Feature /FeatureName:TelnetClient
```

4. Test the Rule

In Command Prompt: `telnet localhost 23`

```
C:\Windows\System32>telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed
```

This confirms that inbound TCP traffic on port 23 is blocked.

5. Remove the Test Block Rule

- In Windows Defender Firewall with Advanced Security, click **Inbound Rules**.
 - Locate **Block Telnet Port 23**, right-click → **Delete**.
-

Firewall Filtering Summary

A firewall inspects network packets and decides whether to allow or block them based on rules-

- **Allow rules** let specified traffic through.
 - **Block/Deny rules** drop or reject packets.
 - Filtering can be based on **IP address**, **protocol** (TCP/UDP), and **port number**.
 - In this, TCP traffic on **port 23** was blocked to prevent Telnet connections, reducing potential security risks.
-

Conclusion

The firewall successfully blocked inbound Telnet traffic on port 23, as verified by testing. The rule was then removed to restore the original firewall configuration.

