**Firewall Setup Report: Blocking Telnet (Port 23) on Windows**

**1. Objective**

The goal of this task was to configure and verify firewall rules to block inbound traffic on TCP port 23 (commonly used for Telnet) using Windows Firewall, and to demonstrate basic firewall management and network traffic filtering skills.

**2. Tools Used**

Windows Defender Firewall with Advanced Security (wf.msc)

**3. Steps Performed**

Step 1: Open Firewall Configuration Tool

* Opened the Run dialog with Win + R
* Entered wf.msc and pressed Enter
* This launched the Windows Defender Firewall with Advanced Security GUI

Step 2: List Current Firewall Rules

* Navigated to Inbound Rules section in the left pane
* Reviewed existing rules to understand current traffic policies

Step 3: Add Rule to Block Inbound Traffic on Port 23 (Telnet)

* Clicked New Rule… in the right Actions pane
* Selected Port as rule type, clicked Next
* Chose TCP and entered 23 in Specific local ports, clicked Next
* Selected Block the connection, clicked Next
* Applied the rule to all profiles: Domain, Private, Public, clicked Next
* Named the rule "block telnet port 23" and finished the wizard
* The rule appeared enabled in Inbound Rules list with status Enabled

Step 4: Testing the Rule (Documented Approach)

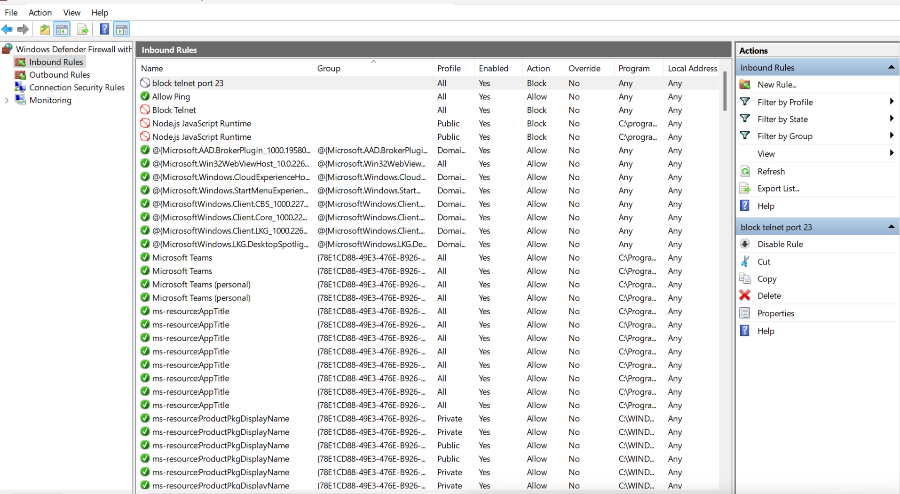
* Ideally, tested from another device on the same network by attempting:
* telnet <target\_machine\_ip> 23
* Expected result: Connection refused or timeout, indicating the port is blocked
* Because no second device was available, this test was documented as a theoretical verification step

Step 5: Remove Test Block Rule

After testing, plan to delete or disable the "block telnet port 23" rule to restore the environment to original state

**4. Screenshot Evidence**

* Included in the report is a screenshot of the Windows Firewall Inbound Rules interface showing the "block telnet port 23" rule:
* Rule is enabled
* Action is set to Block
* Applies to All profiles
* This confirms the creation of the firewall rule per the assignment requirements.



**5. Summary of How Firewall Filters Traffic**

* A firewall monitors and controls network traffic according to security policies. It evaluates incoming and outgoing packets and allows or denies them based on criteria such as IP addresses, port numbers, and protocols.
* In this case, the rule blocks inbound TCP traffic on port 23 to prevent Telnet connections.
* Blocking unused or insecure ports reduces attack surface and improves system security.
* Firewalls can be stateful, tracking connection state to permit only legitimate traffic.

**7. Notes on Linux Firewall (UFW)**

The original assignment also mentions UFW on Linux. This report covers the Windows firewall part. If Linux setup is required, similar steps apply to configure rules via terminal, including allowing SSH on port 22.

**8. Final Remarks**

This report, along with the screenshot and documented steps, fulfills the task requirements for firewall management skills and shows understanding of network traffic filtering by firewalls.