

Windows Firewall Configuration Report

Task: Setup and Use a Firewall on Windows

Objective: Configure and test basic firewall rules to allow or block traffic.

1. Commands and GUI Steps Used

Step 1: Open Windows Firewall with Advanced Security

Method 1 (GUI): Press Win + S → Type 'Windows Defender Firewall' → Open 'Windows Defender Firewall with Advanced Security'.

Method 2 (Run Command): Press Win + R → Type *wf.msc* → Press Enter.

Step 2: List Current Firewall Rules

Open Command Prompt as Administrator and run:

```
netsh advfirewall firewall show rule name=all dir=in >
C:\FirewallRules_Inbound.txt
```

(This exports all inbound rules to C:\FirewallRules_Inbound.txt)

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

In Windows Defender Firewall with Advanced Security:

Click 'Inbound Rules' → 'New Rule...' → Port → TCP, Specific port: 23 → Block the connection → Apply to All Profiles → Name: 'Block_Telnet_Port23' → Finish.

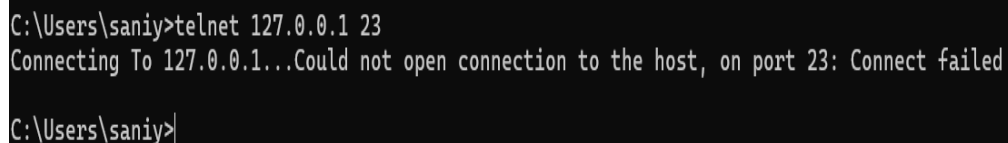
Step 4: Test the Block Rule

Command Used:

```
telnet 127.0.0.1 23
```

Result: 'Could not open connection to the host, on port 23: Connect failed' (Block successful).

Screenshot (Step 4 - Testing the Block Rule):



```
C:\Users\saniy>telnet 127.0.0.1 23
Connecting To 127.0.0.1...Could not open connection to the host, on port 23: Connect failed
C:\Users\saniy>
```

Step 5: Remove the Test Block Rule

In Inbound Rules, locate 'Block_Telnet_Port23', right-click → Delete → Confirm 'Yes'.

2. Summary: How Firewall Filters Traffic

A firewall acts as a security barrier between a trusted internal network (your PC) and untrusted external networks (the internet).

Rule-Based Filtering: Checks each incoming/outgoing connection against predefined rules (e.g., block port 23, allow port 80). Rules can be based on ports, protocols, IP addresses, or applications.

Actions: Allow (permits traffic) or Block (drops traffic).

Profiles: Domain (corporate networks), Private (home/work), Public (public Wi-Fi).

Default Behavior: Windows Firewall blocks unsolicited inbound traffic by default. Outbound is allowed unless explicitly blocked.

Key Takeaway: By creating a rule to block TCP port 23, we prevented Telnet traffic from entering the system, demonstrating how firewalls enforce security policies.