
Documented Commands and GUI Steps Used

Windows Defender Firewall (GUI Steps)

1. Open **Control Panel**
2. Navigate to **Windows Defender Firewall**
3. Click **Advanced settings**
4. Select **Inbound Rules**
5. Click **New Rule**
6. Choose **Port** as rule type
7. Select **TCP** protocol
8. Enter **23** as the specific local port
9. Select **Block the connection**
10. Apply rule to **Domain, Private, and Public** profiles
11. Name the rule as **Block Telnet Port 23**
12. Click **Finish** to apply the rule

Command Prompt Commands Used

telnet localhost 23

Purpose:
Tests whether port 23 (Telnet) is blocked by the firewall.

Result:

Connecting To localhost...
Could not open connection to the host, on port 23: Connect failed

---

PowerShell Command (Alternative Testing Method)

Test-NetConnection localhost -Port 23

Purpose:
Verifies firewall rule functionality without requiring Telnet Client.

Expected Output:

TcpTestSucceeded : False

Optional Firewall Cleanup (GUI)

1. Go to **Inbound Rules**
2. Right-click **Block Telnet Port 23**
3. Select **Delete**

Conclusion

The documented GUI steps and commands confirm that the firewall successfully blocked inbound traffic on port 23, demonstrating effective network traffic filtering.
