* ***Documented Steps – windows firewall GUI***

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Action | Tool / Interface | Details |
| 1 | Open Firewall Settings | Control Panel → System and Security → Windows Defender Firewall | Or run firewall.cpl |
| 2 | View Current Rules | Advanced Settings (left pane) → Inbound Rules / Outbound Rules | You can sort or filter by port or name |
| 3 | Block Port 23 (Telnet) | Windows Defender Firewall with Advanced Security | - Click **Inbound Rules** → **New Rule** - Select **Port** - Choose **TCP**, specify port **23** - Action: **Block the connection** - Apply to all profiles (Domain, Private, Public) - Name the rule: *Block Telnet Port 23* |
| 4 | Test the Rule | CMD / PowerShell / Telnet / Nmap | telnet localhost 23 or nmap -p 23 localhost |
| 5 | Allow SSH (Port 22) | Advanced Settings → Inbound Rules → New Rule | - Same steps as above - Choose **Allow the connection** - Specify port **22 (SSH)** - Name the rule: *Allow SSH* |
| 6 | Remove Test Rule | Inbound Rules → Locate "Block Telnet Port 23" | - Right-click the rule - Click **Delete** to remove it |
| 7 | Confirm Rule Removal | Refresh rule list in Inbound Rules | Ensure the port 23 rule is deleted |