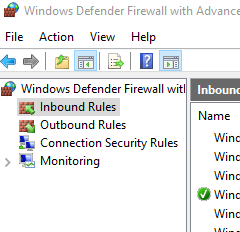
Firewall Configuration & Traffic Filtering

Windows Defender Firewall

Open Windows Firewall Tool

Press Windows Key → type “Windows Defender Firewall with Advanced Security”

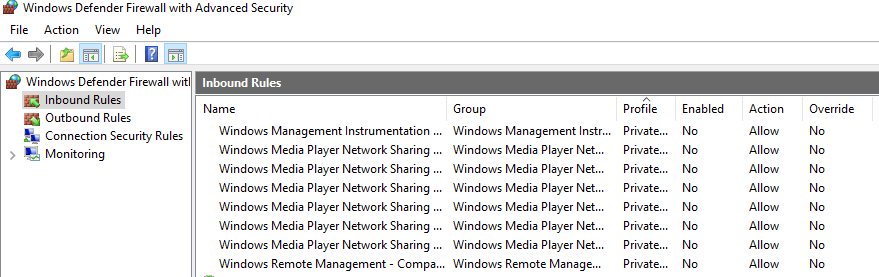
Or run: wf.msc



List Current Firewall Rules

Open Inbound Rules (left panel) to see all rules.

Use the right-side "Filter by Profile" or "Action" (Allow/Deny).



Add Rule to Block Port 23 (Telnet)

Click Inbound Rules > New Rule

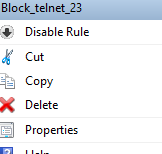
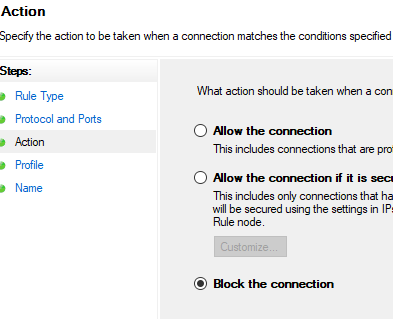
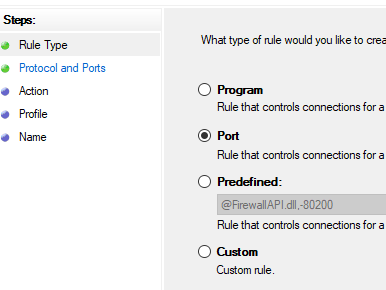
Choose Port → Next

Select TCP → Port 23 → Next

Choose Block the connection → Next

Apply to all profiles (Domain, Private, Public)

Name it: Block\_Telnet\_23

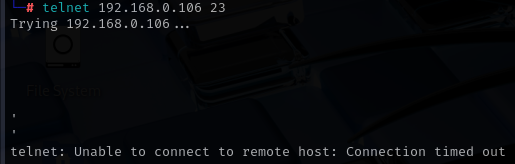


Test the Rule

On another device or using telnet:

telnet <your-IP> 23

It should fail to connect if the rule is working.



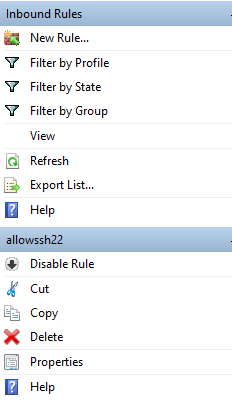
Allow Port 22 (If using SSH server on Windows)

Inbound Rules > New Rule > Port

TCP → Port 22 → Next

Allow the connection → Apply to all profiles

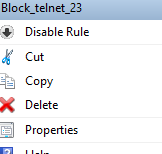
Name: Allow\_SSH\_22



Remove the Block Rule

Go back to Inbound Rules

Find Block\_Telnet\_23 → Right-click → Delete



Document GUI Steps

Used: wf.msc

Action: Created block rule for Port 23 via Inbound > New Rule > Port > Block

Verified with telnet

Removed test rule afterward

Firewall Filtering Summary (Windows)

Rules are processed top to bottom

Can filter by:

Port

Program

IP address

Protocol (TCP/UDP)

Blocked rules override allow if conflicts exist