Firewall Procedure

WINDOWS FIREWALL STEPS

1. Open Firewall Configuration Tool

Go to Control Panel → System and Security → Windows Defender Firewall

Click on Advanced Settings for Inbound/Outbound Rules

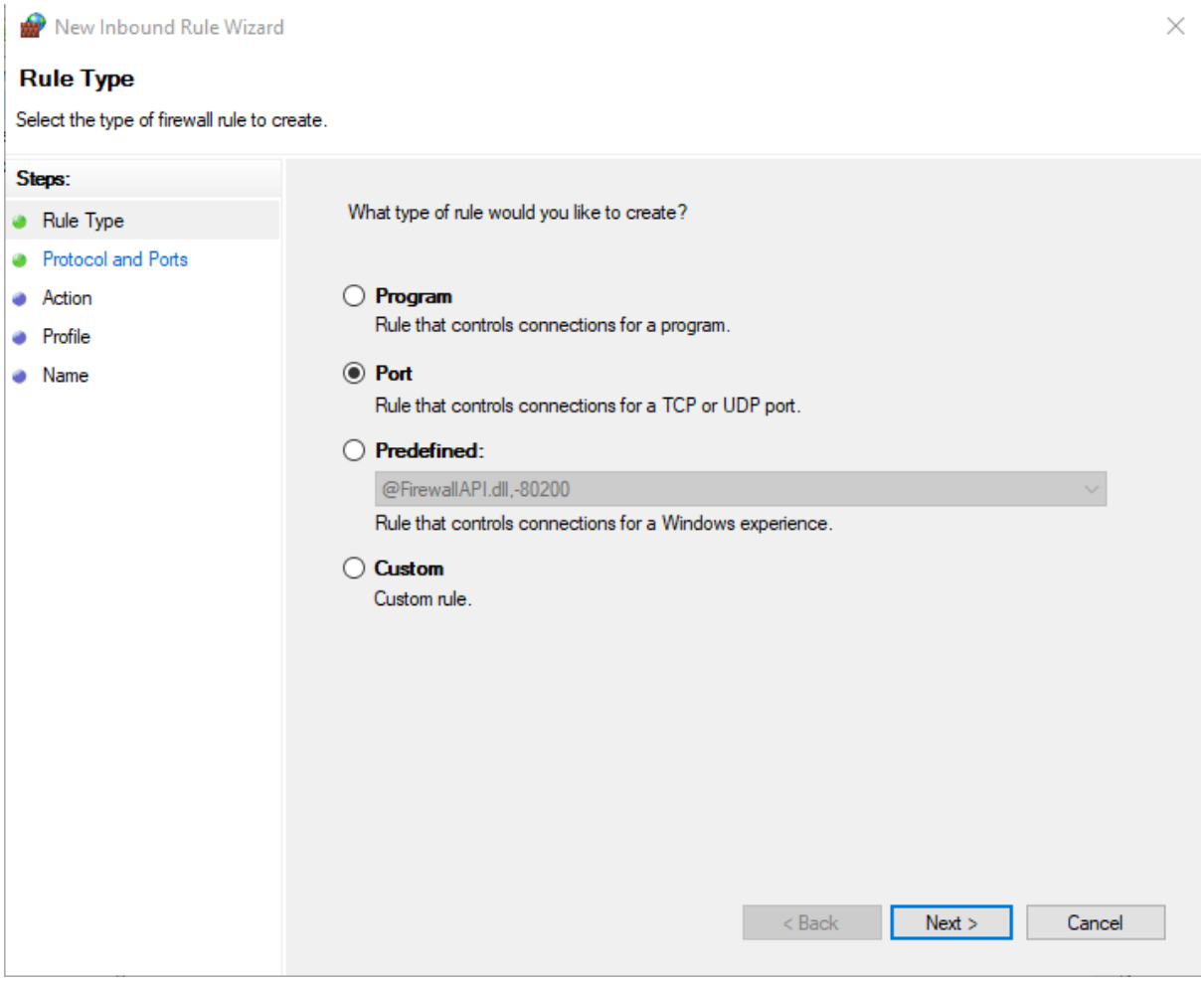
2. List Current Firewall Rules

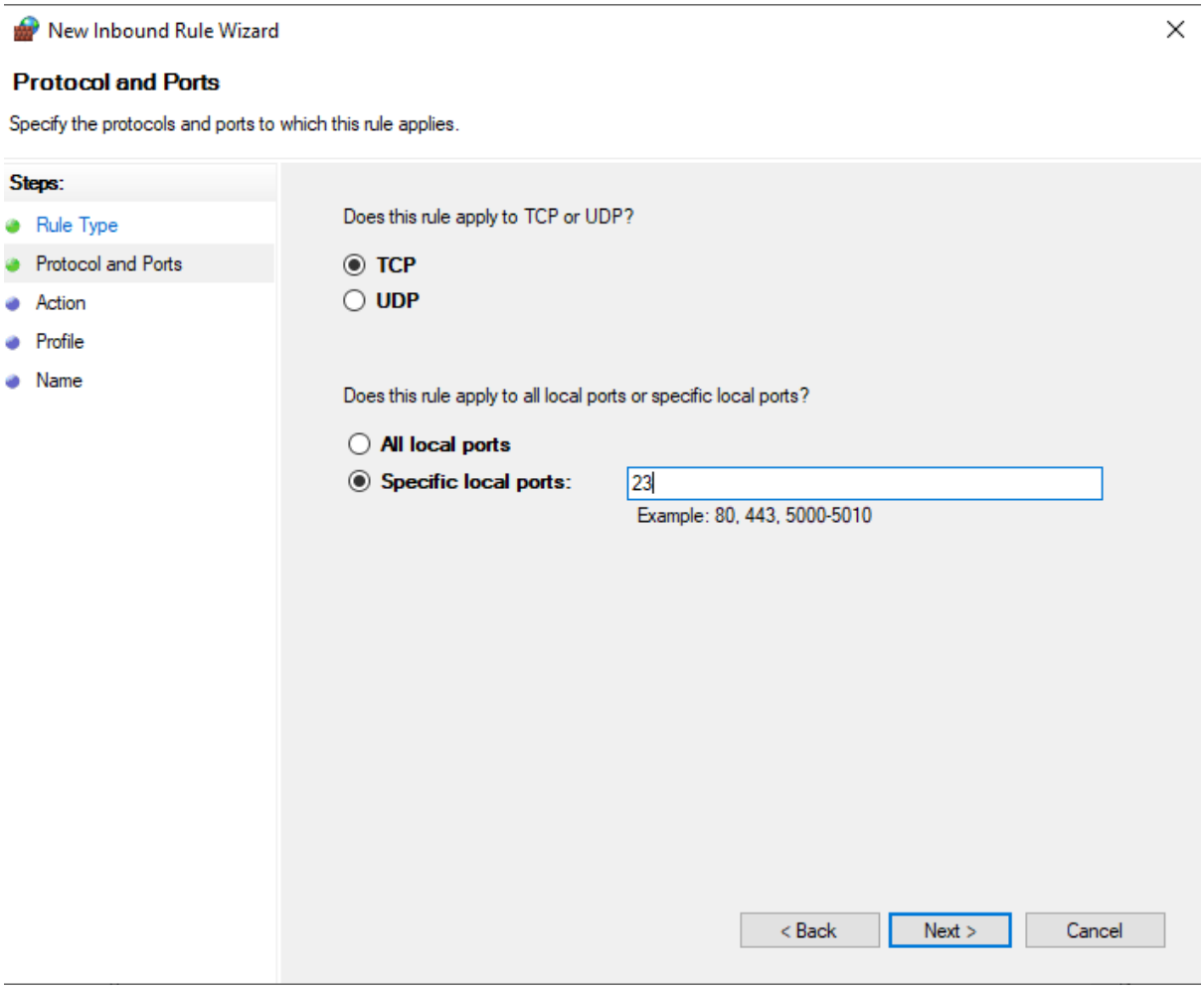
Open Windows Defender Firewall with Advanced Security

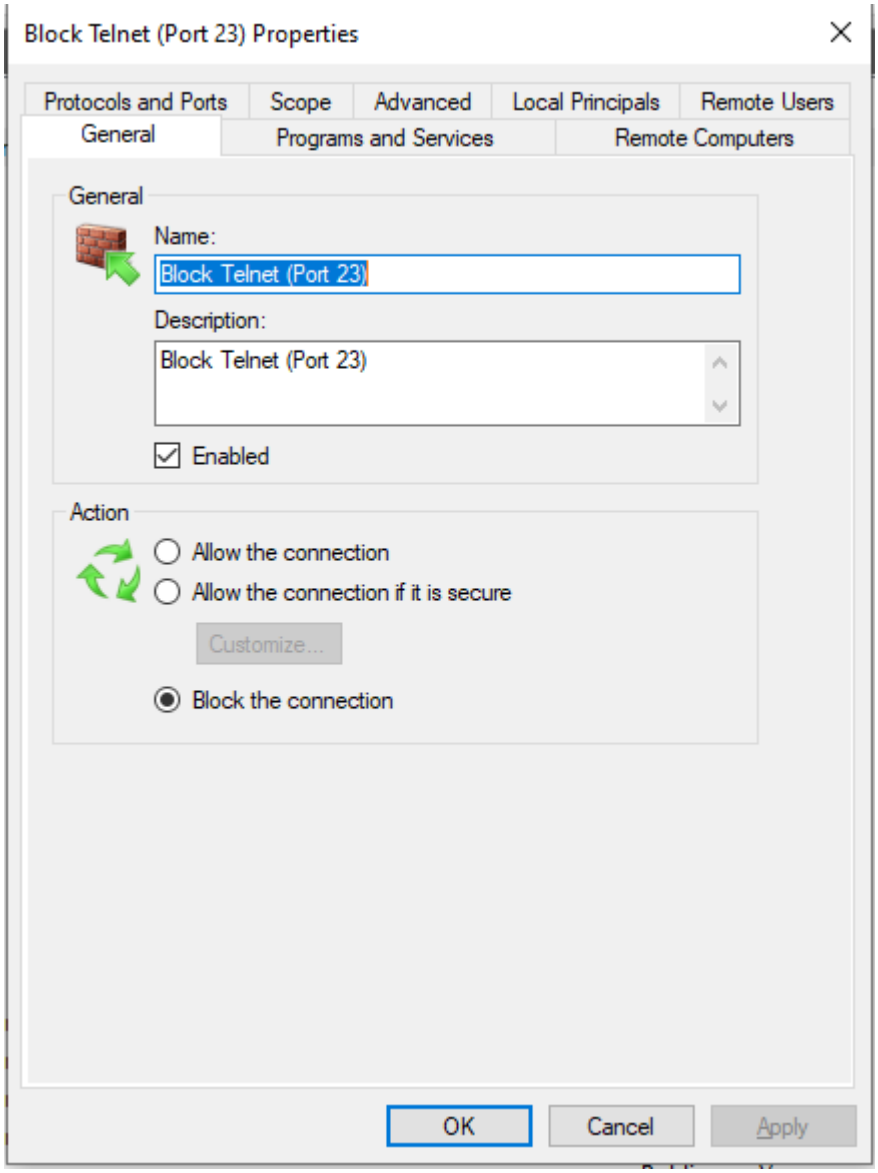
Click Inbound Rules / Outbound Rules to see the list

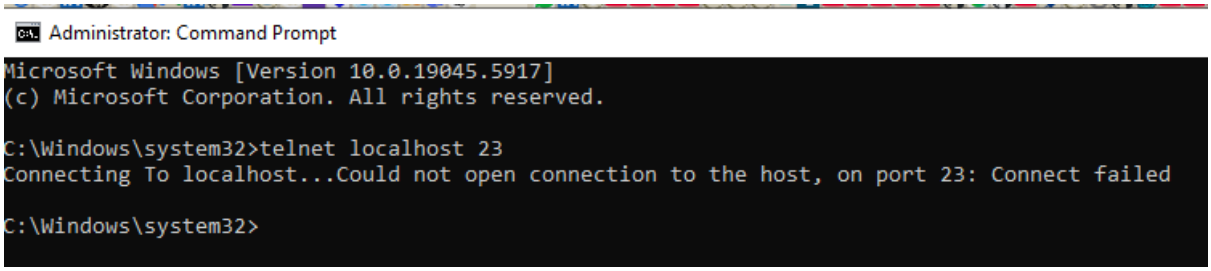
3. Add a Rule to Block Port 23 (Telnet)

Go to Inbound Rules > New Rule




New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
23
Example: 80, 443, 5000-5010
< Back
Next >
Cancel





Select Port → TCP → Specific port: 23

Choose Block the connection

Name it: Block Telnet (Port 23)

4. Test the Rule

Run

telnet localhost 23

Should fail with connection error

5. Remove the Rule

Find rule Block Telnet (Port 23) in Inbound Rules

Right-click > Delete

LINUX (UFW - Uncomplicated Firewall) STEPS

1. Open Terminal and Enable UFW

sudo ufw enable

2. List Current Rules

sudo ufw status numbered

3. Block Inbound Traffic on Port 23 (Telnet)

sudo ufw deny 23

4. Test Rule

From same machine or remote, run:

telnet localhost 23

It should time out or get denied.

5. Allow SSH (Port 22)

sudo ufw allow 22

6. Remove the Block Rule (Restore State)

sudo ufw delete deny 23

7. Disable UFW (optional)

sudo ufw disable