8/8/2025

# Configure Firewall and Test Rules

(LINUX, WINDOWS)

Sejal Rathwa

## Task 4: Setup and Use a Firewall on Windows/Linux

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

**Tools:** Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

**Deliverables**: Screenshot/configuration file showing firewall rules applied.

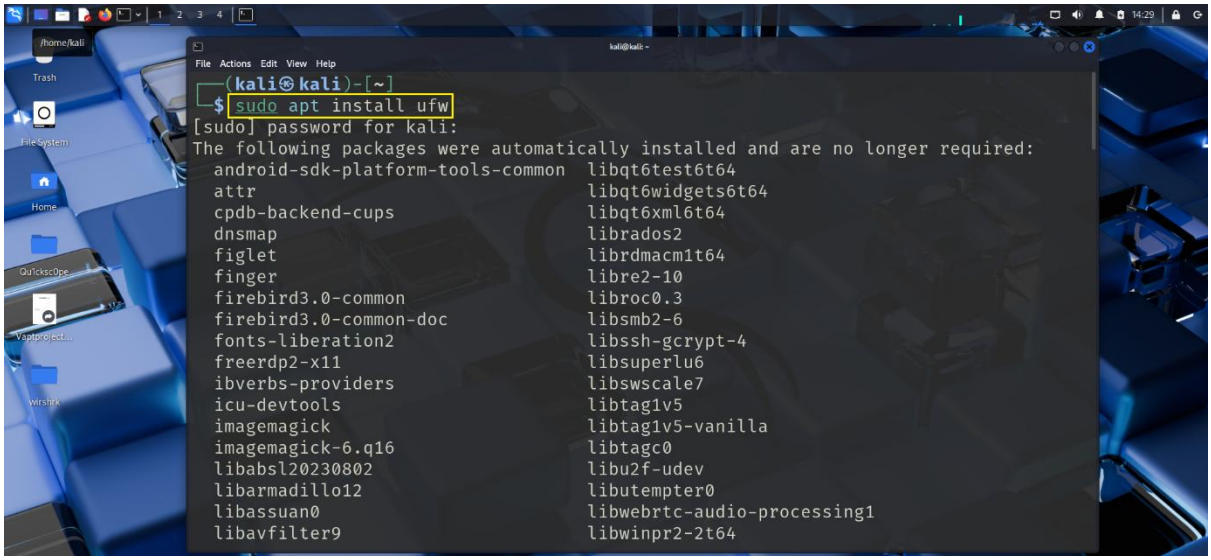
Here's a step-by-step guide to configure and test firewall rules on both Windows and Linux (UFW), depending on your system. Choose the section that matches your OS.

**FOR LINUX (UFW - Uncomplicated Firewall)**

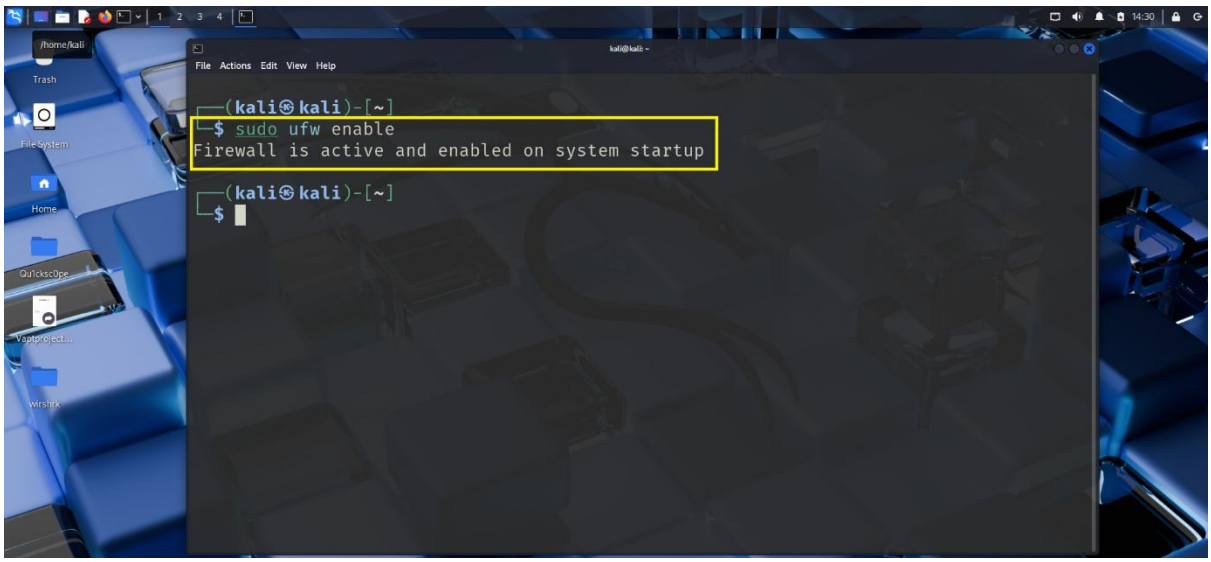
Make sure UFW is installed and enabled:

Run cmd

sudo apt install ufw



sudo ufw enable



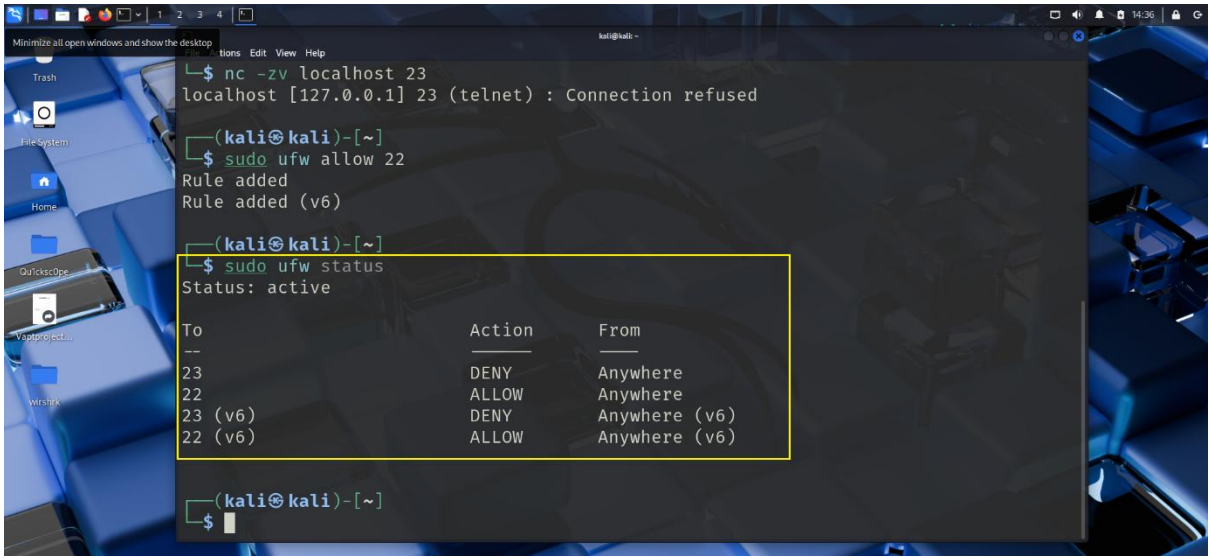

**1. Open Firewall Configuration Tool**

UFW is used via the terminal. No GUI needed.

**2. List Current Firewall Rules**

Rum cmd

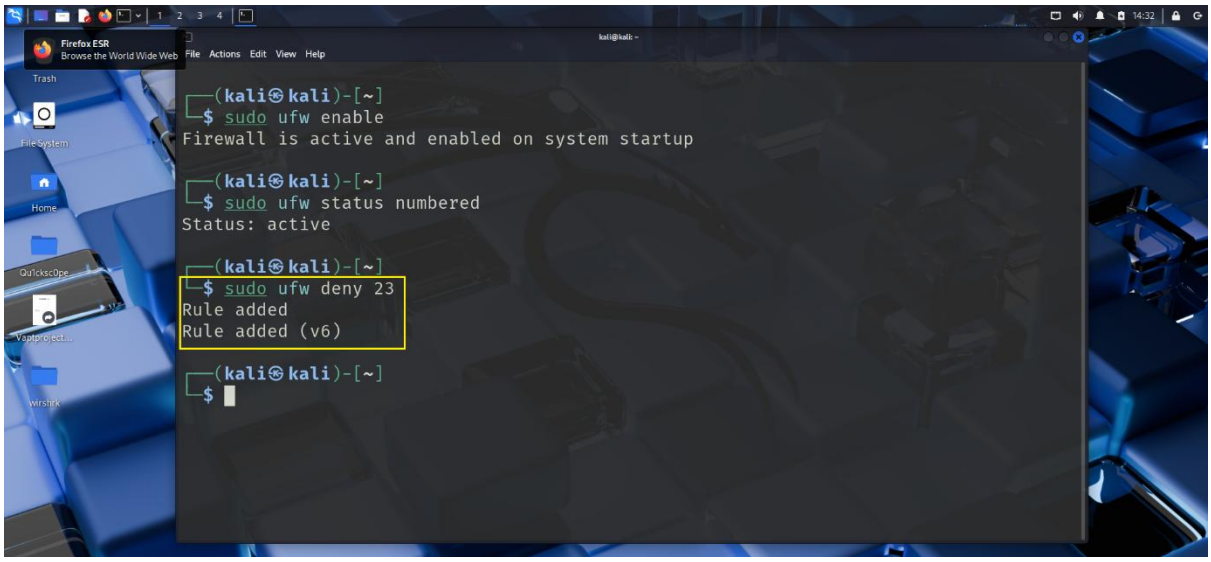
sudo ufw status numbered




**3. Add Rule to Block Inbound Traffic on Port 23 (Telnet)**

Run cmd

sudo ufw deny 23



**4. Test the Rule**

You can test with:

- Telnet client:

Run cmd

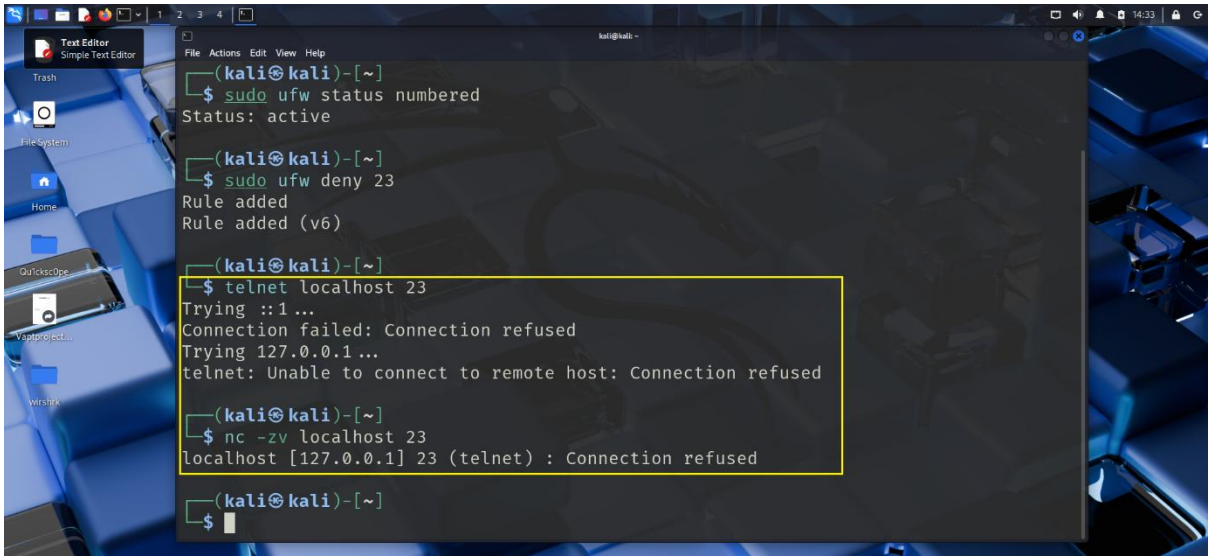
telnet localhost 23

Or use nc (netcat):

Run cmd

nc -zv localhost 23

Can see a connection refused or timeout.

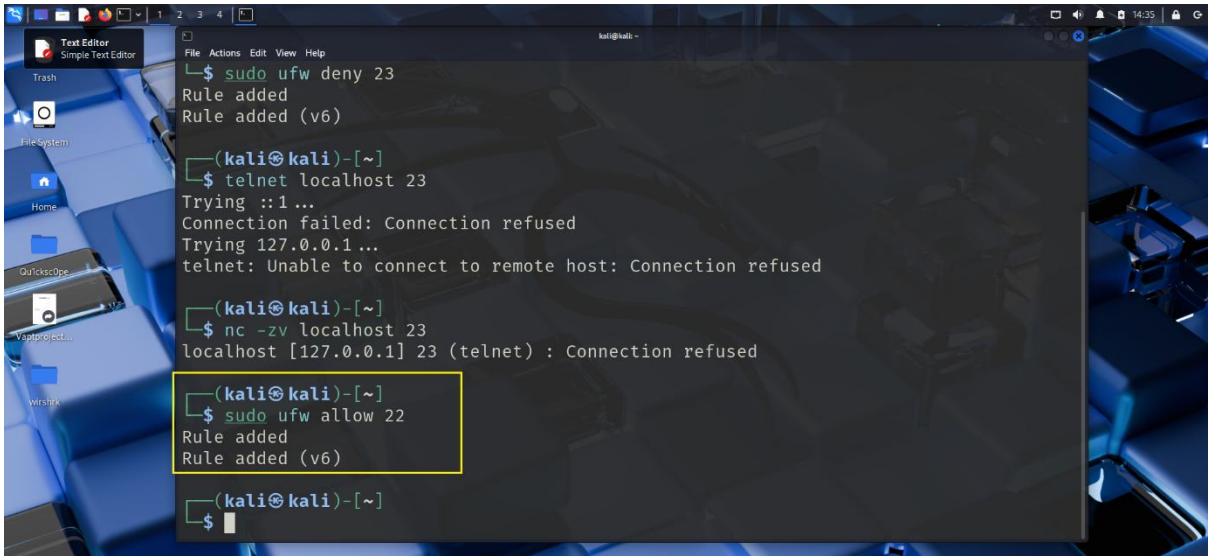


**5. Add Rule to Allow SSH (Port 22)**

Run cmd

sudo ufw allow 22

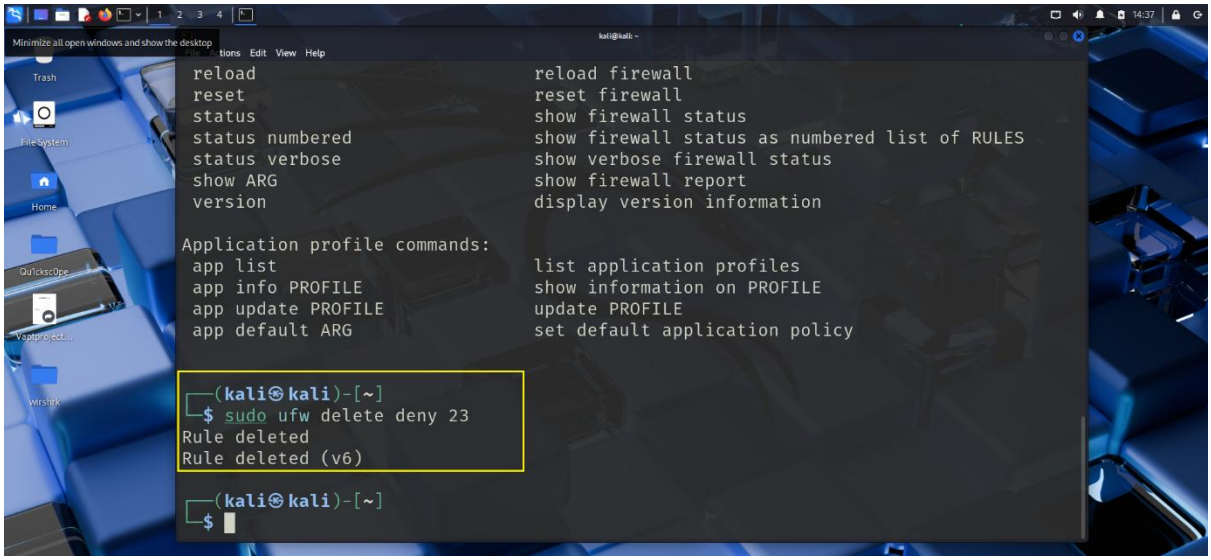
This is important if you're using SSH to manage the system remotely.



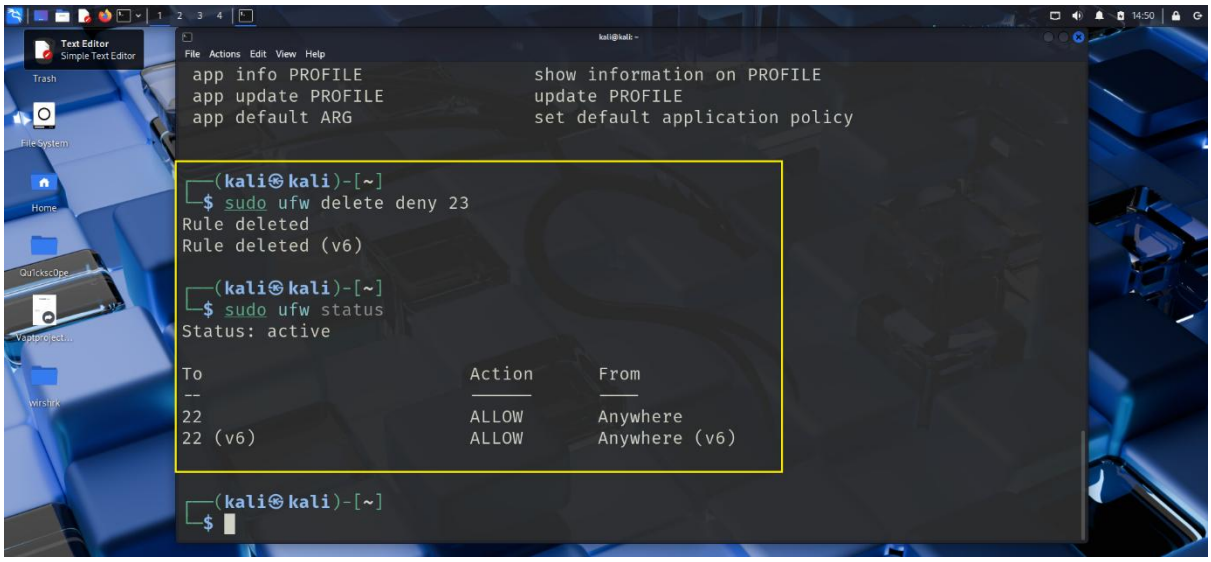
**6. Remove the Block Rule (Restore Original State)**

Rum cmd

sudo ufw delete deny 23



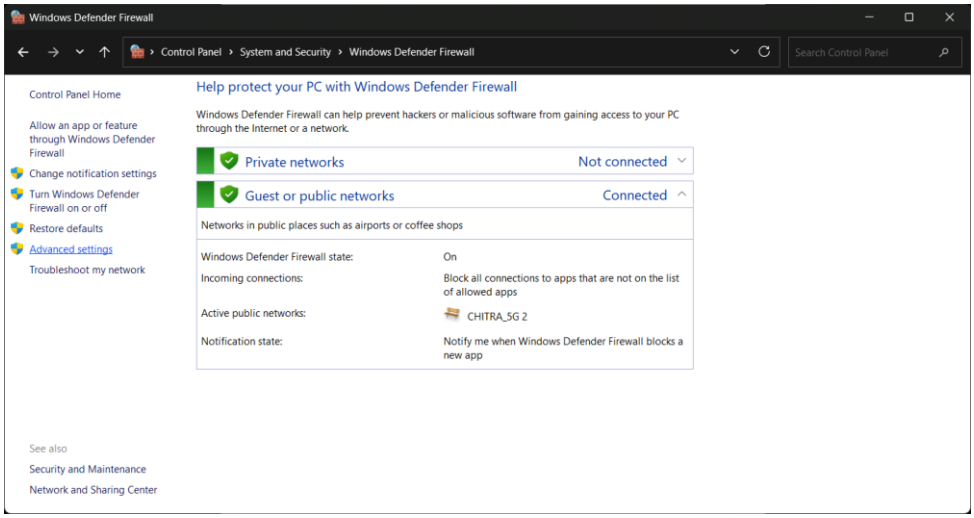

Use sudo ufw status numbered to find the rule number if needed.



**FOR WINDOWS (Windows Defender Firewall)**

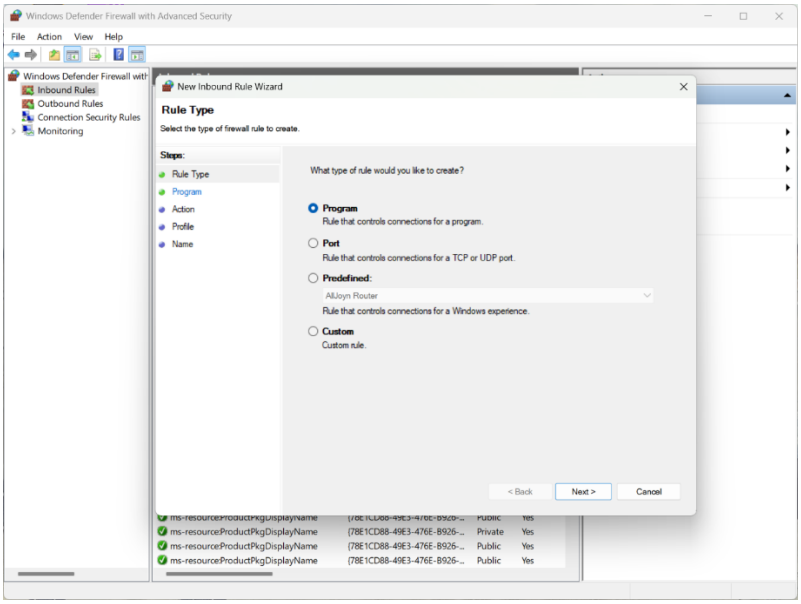
1. Open Firewall Configuration Tool

- Go to Control Panel > System and Security > Windows Defender Firewall.
- Or search: "Windows Defender Firewall with Advanced Security".



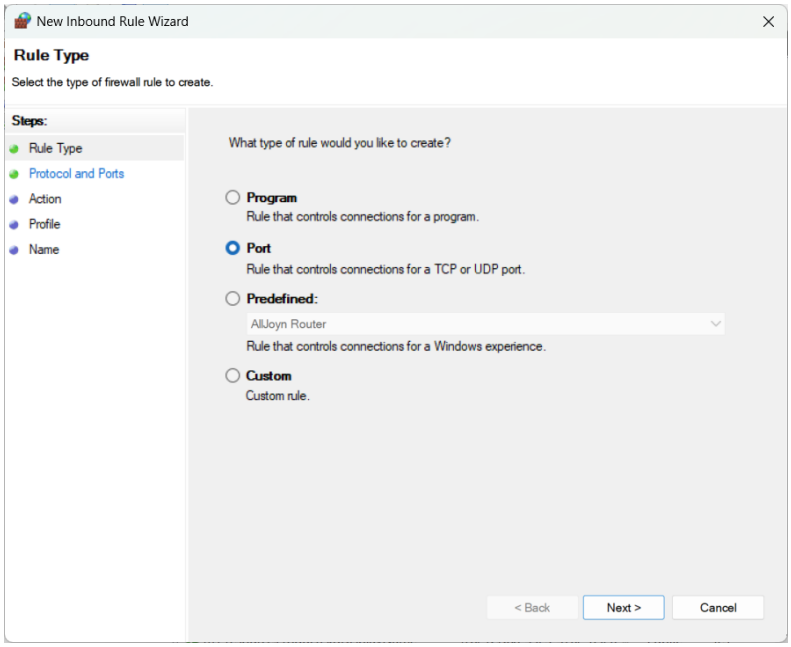

2. List Current Firewall Rules

- In the **Advanced Settings** panel, check:
  - Inbound Rules
  - Outbound Rules

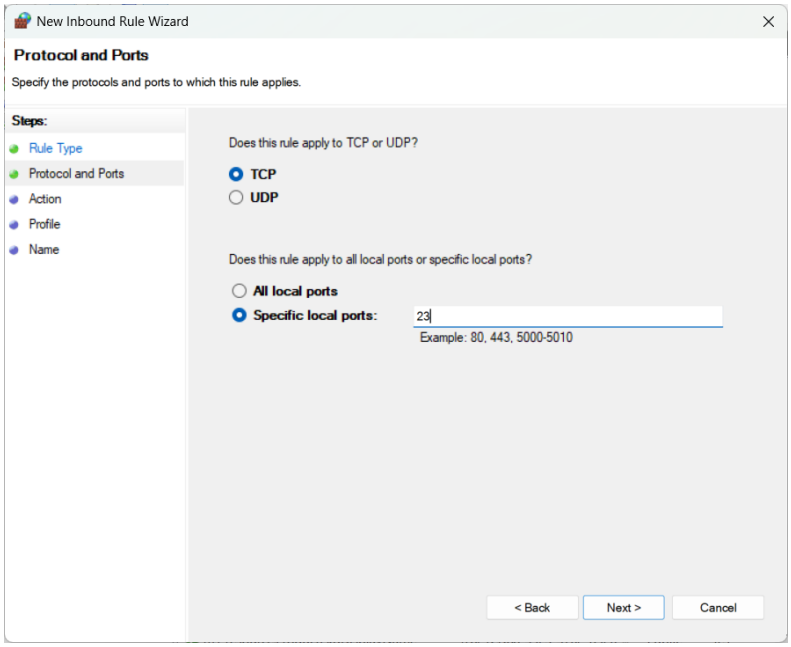


3. Block Inbound Traffic on Port 23

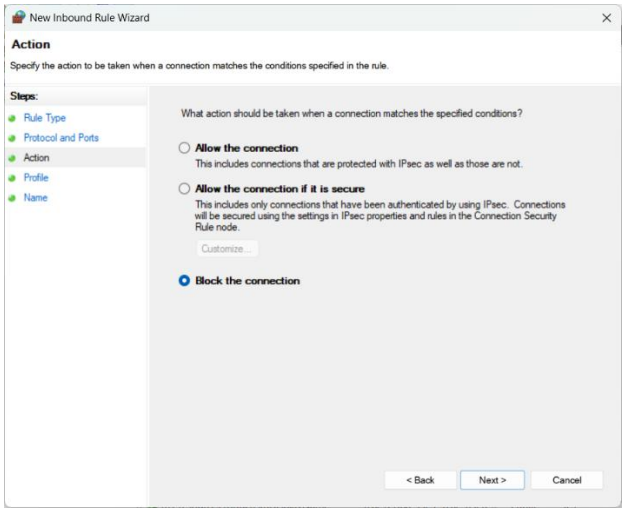
- In **Inbound Rules**, click **New Rule...**
- Select **Port** > Click **Next**



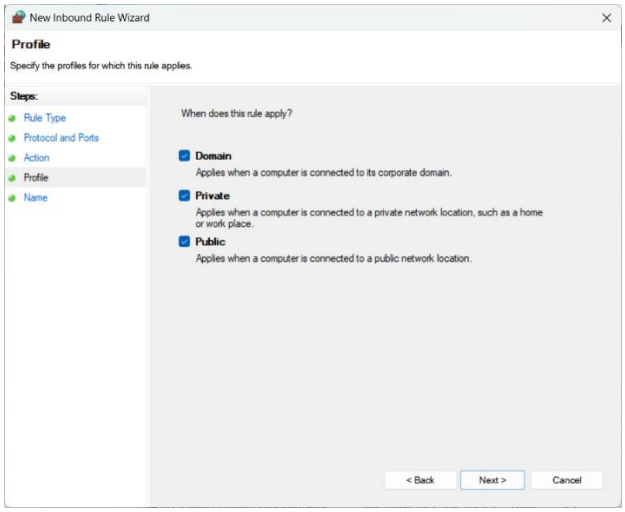

- Choose **TCP** > Specific local ports: 23



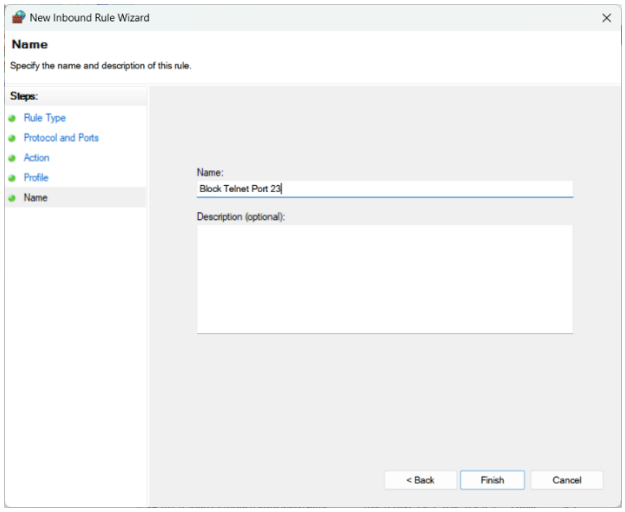
- Action: **Block the connection**




- Apply to all profiles (Domain, Private, Public)




- Name it: Block Telnet Port 23

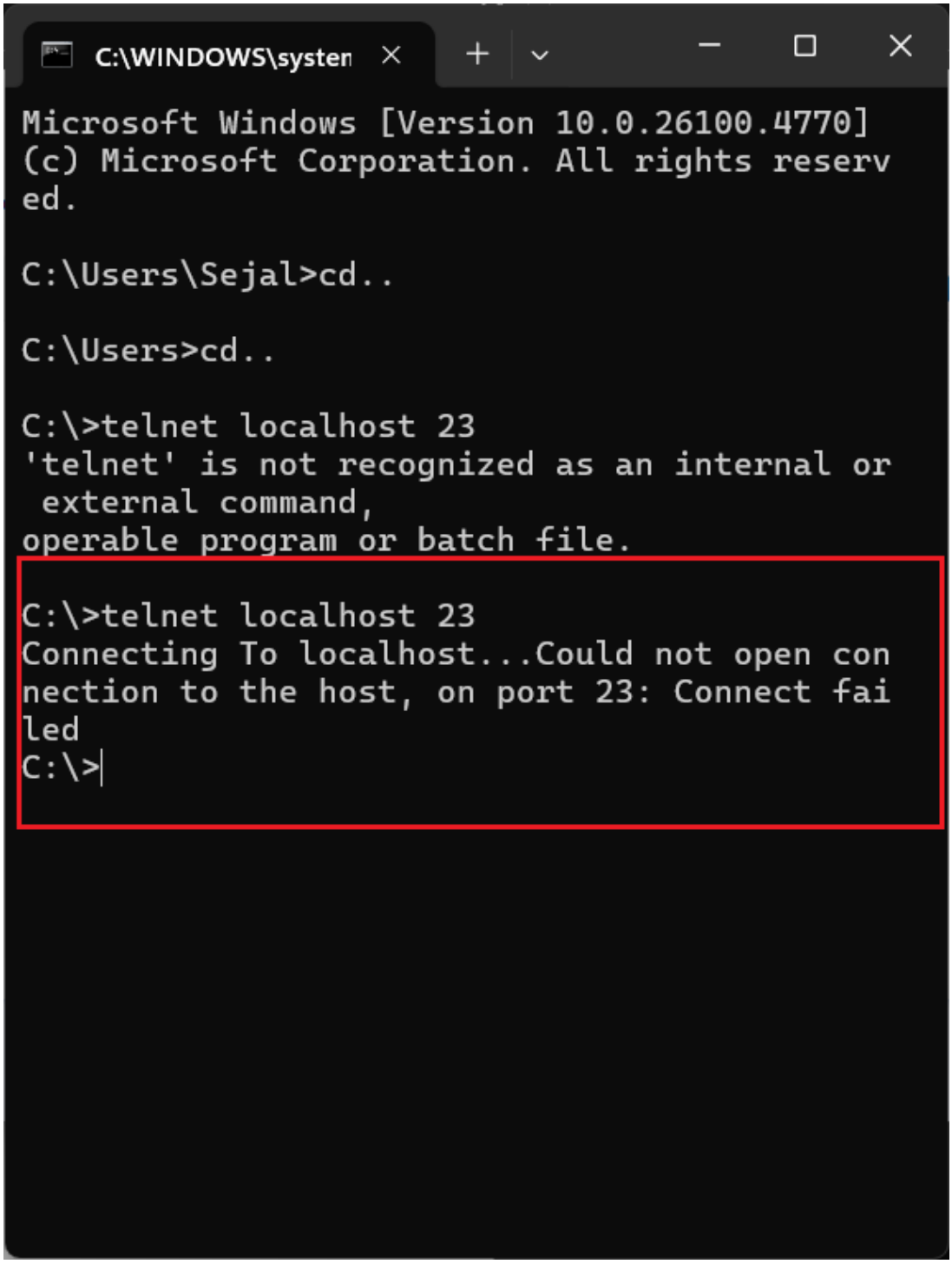


**4. Test the Rule**

Use Telnet client:

1. Install from Optional Features if not present.
2. Run cmd

   telnet localhost 23

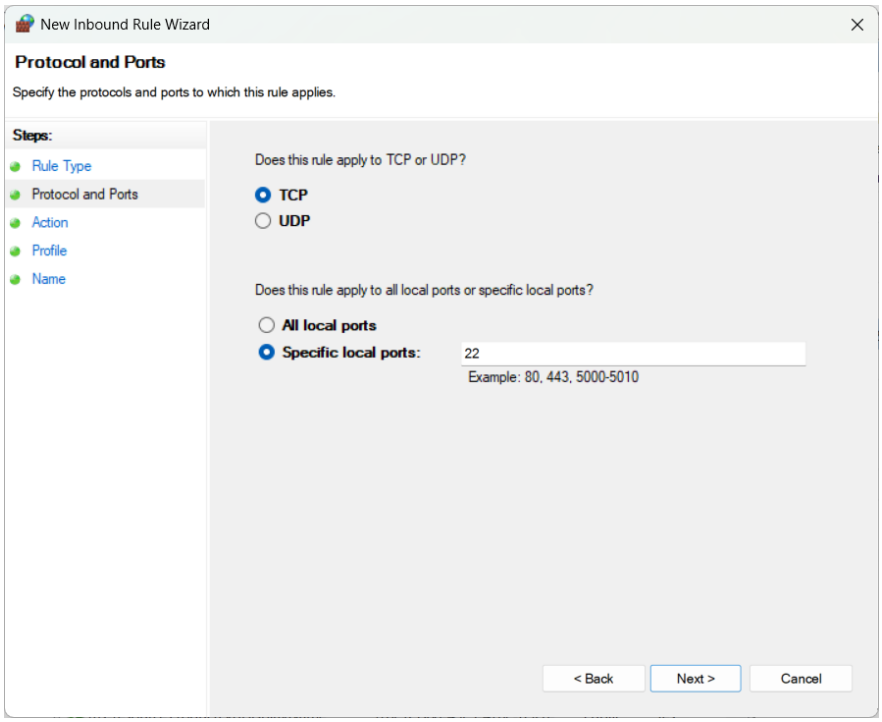



Get a failure to connect.

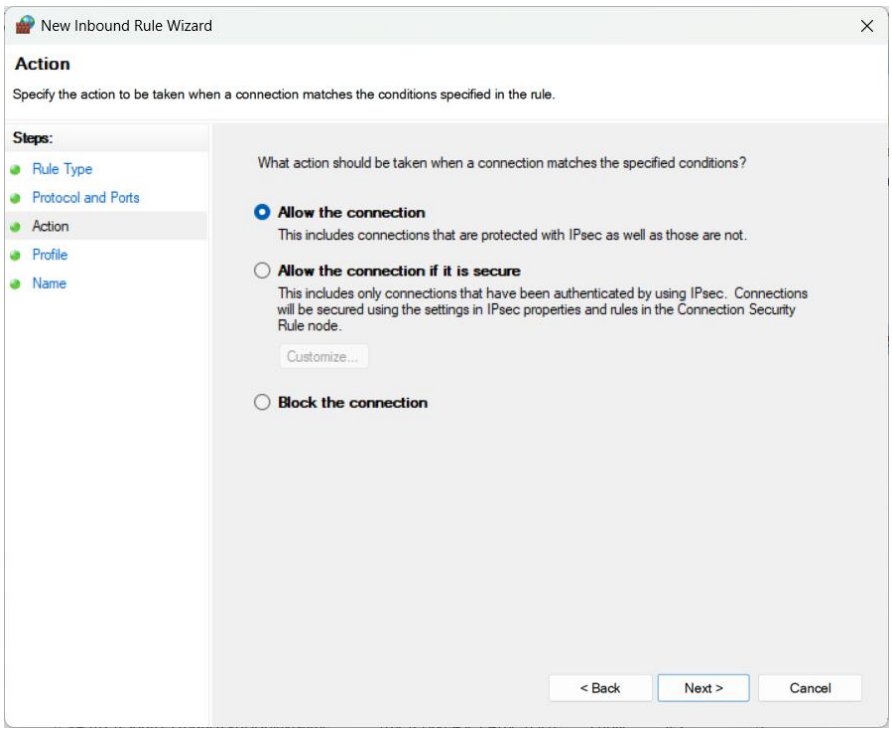
## 5. Allow SSH (Port 22) *(Optional for Windows)*

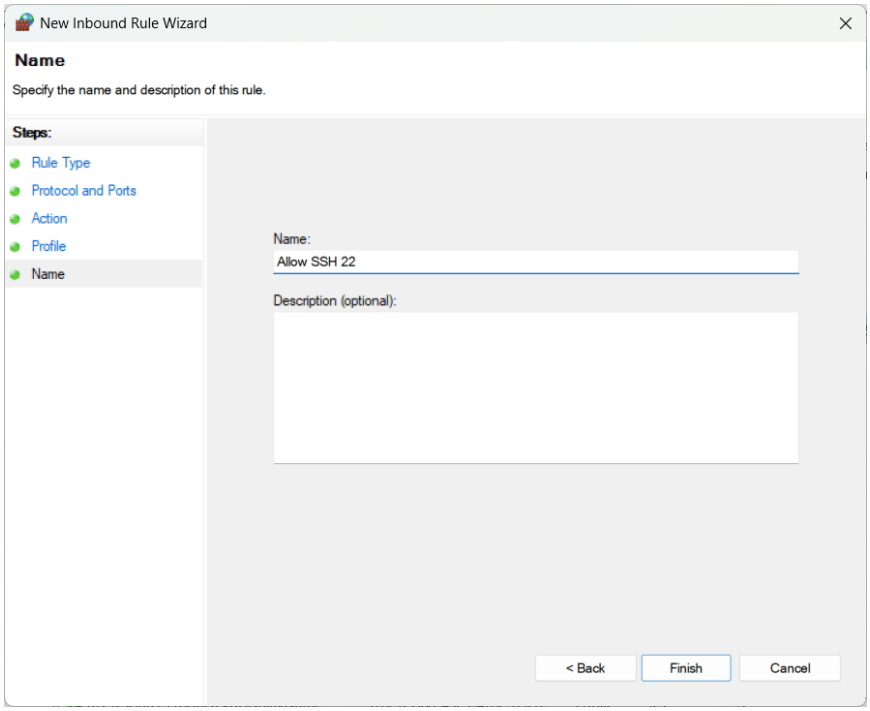
Not typically used unless you're running OpenSSH server. If so:

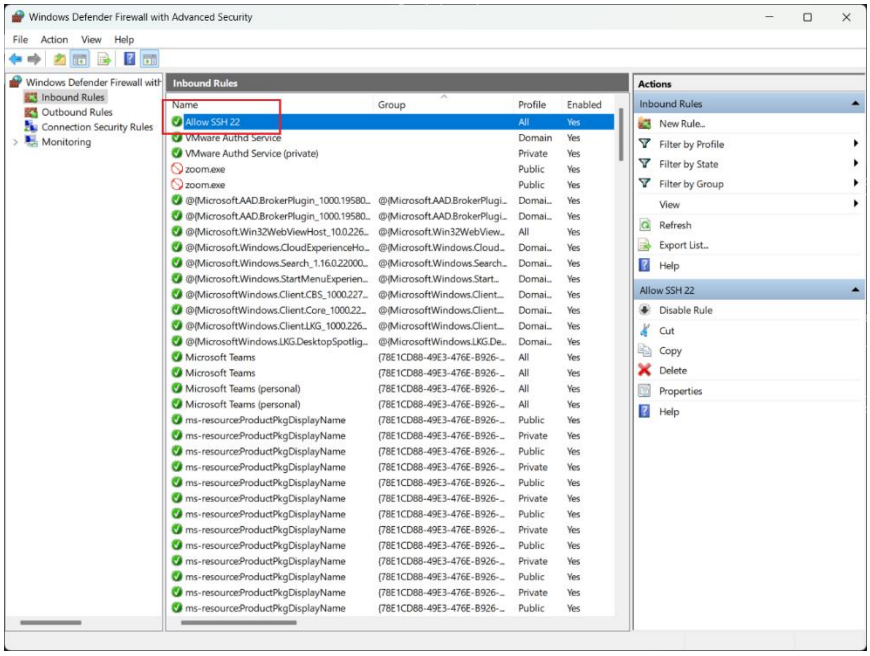
- Go to Inbound Rules > New Rule...




- Port: 22 > Allow the connection

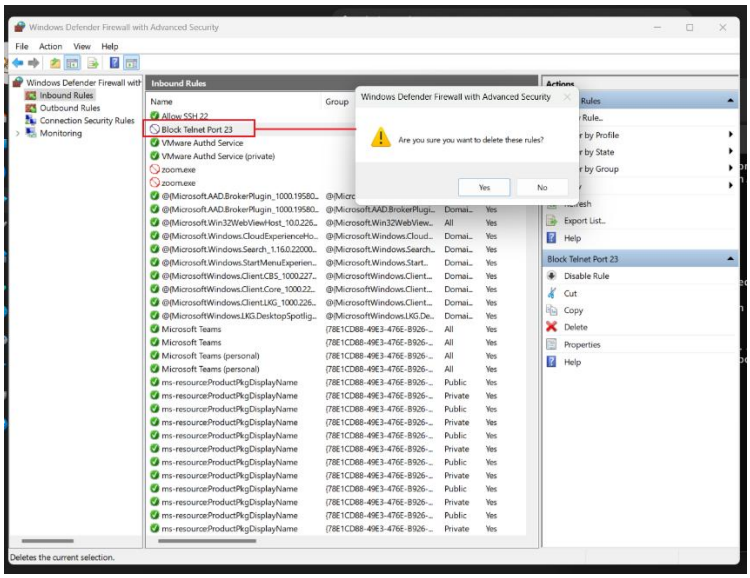



New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Allow SSH 22
Description (optional):
< Back
Finish
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Allow SSH 22
All
Yes
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Allow SSH 22
Disable Rule
Cut
Copy
Delete
Properties
Help

**6. Remove the Test Rule**

- Go to Inbound Rules
- Find Block Telnet Port 23, right-click > Delete




**Summary: How Firewall Filters Traffic**

**Firewall in Linux**

Firewalls monitor and control incoming and outgoing network traffic based on predefined rules. They:

- Allow or deny packets based on IP address, port, or protocol.
- Protect systems from unauthorized access.
- Act as a barrier between trusted and untrusted networks.

**Firewall in Windows**

Windows Firewall filters traffic using rules based on:

- Port numbers
- Application names
- Network profiles

It ensures that only authorized traffic can reach or leave your device, improving security.

**THANK YOU**

**END**