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

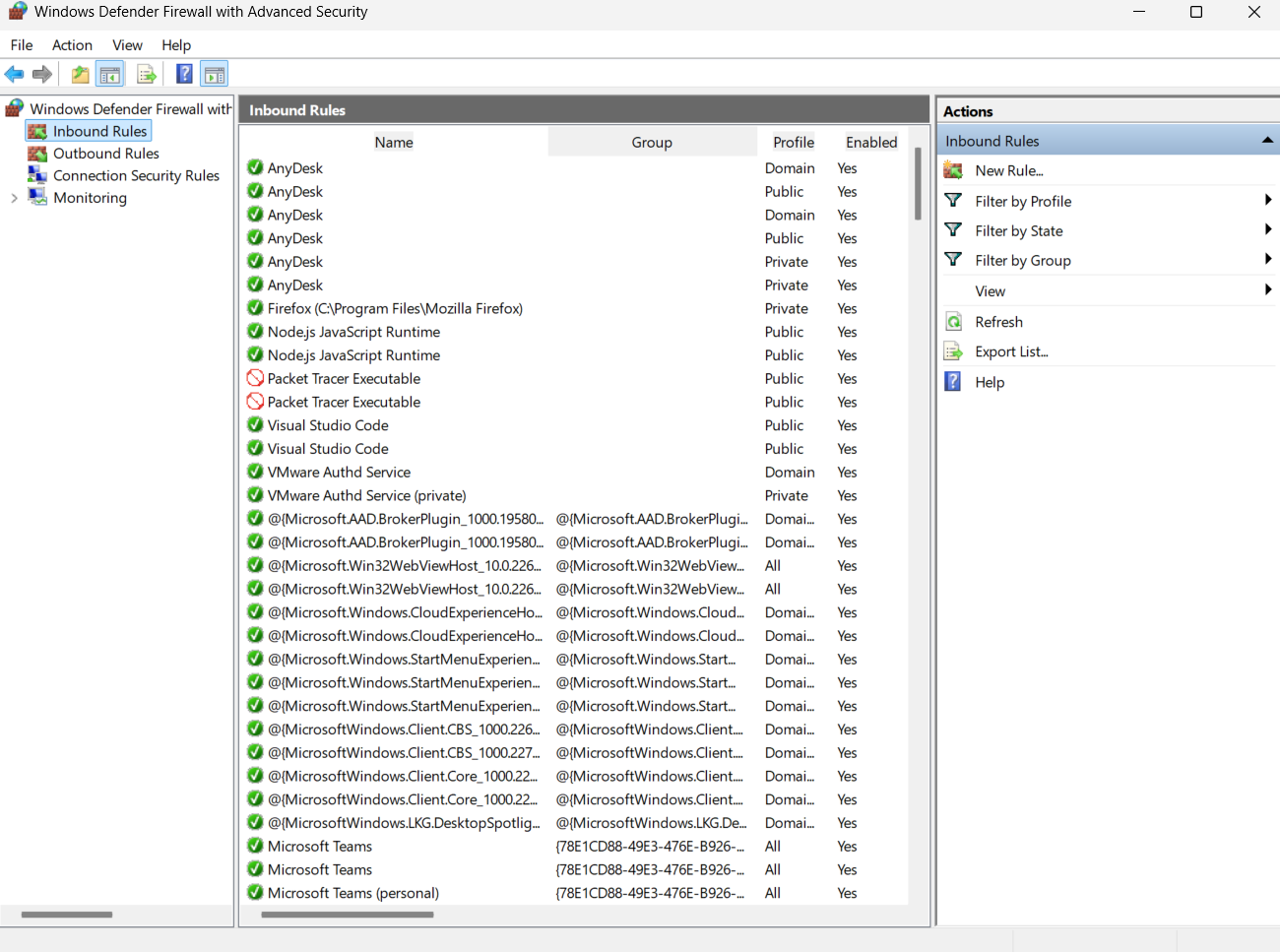
Objective: Configure and test basic firewall rules to allow or block traffic. Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux. Deliverables: Screenshot/configuration file showing firewall rules applied.

Here, Step by step guidance how to perform this task

First we can configure rule on windows machine:

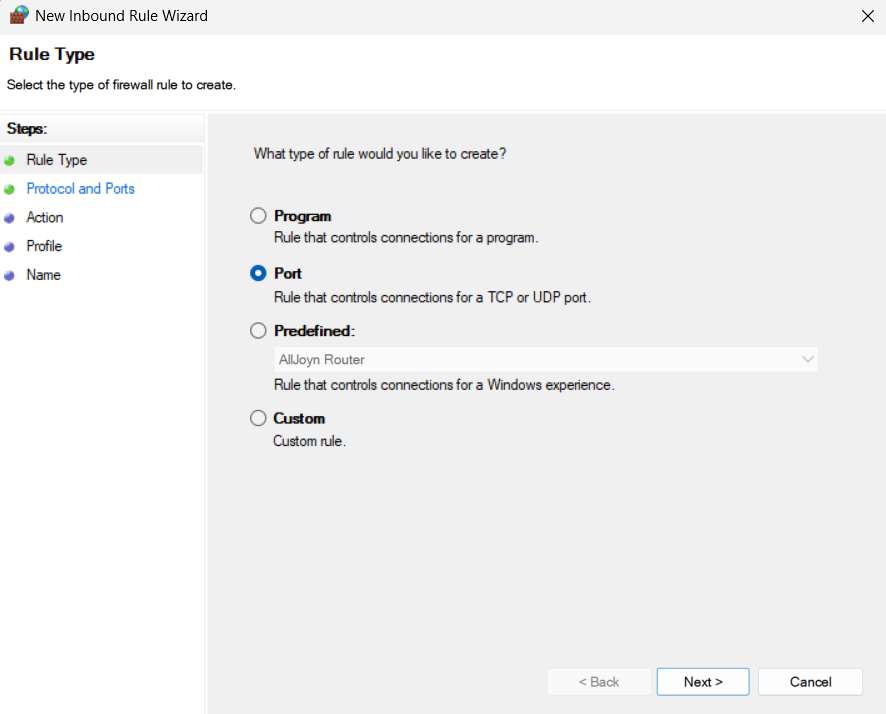
**A. Open the firewall tool**

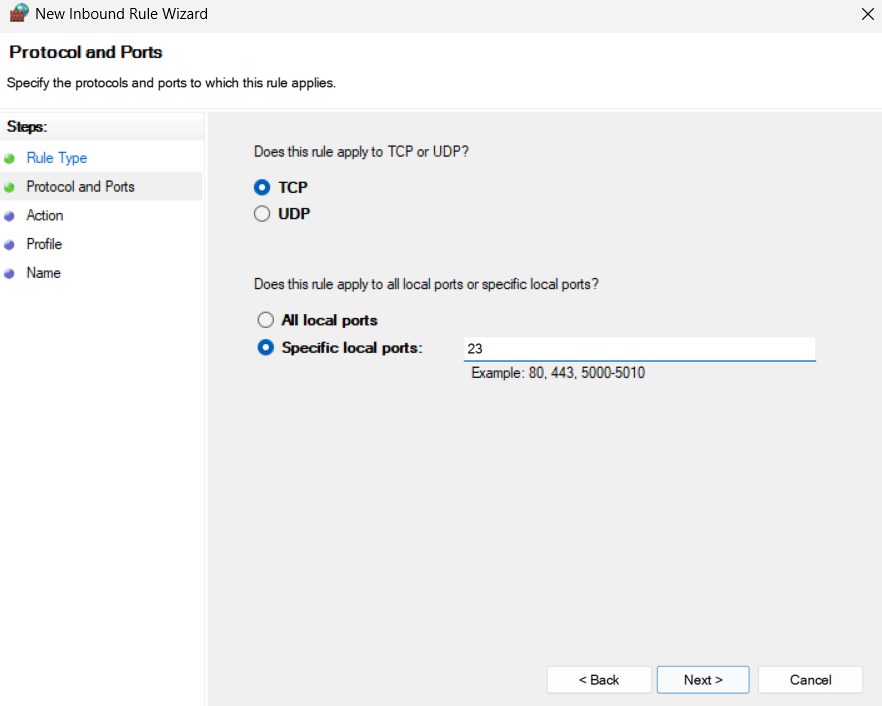
1. Press **Start**, type **Windows Defender Firewall with Advanced Security** and open it (or run wf.msc).
2. Click **Inbound Rules** (left pane) to view existing inbound rules.

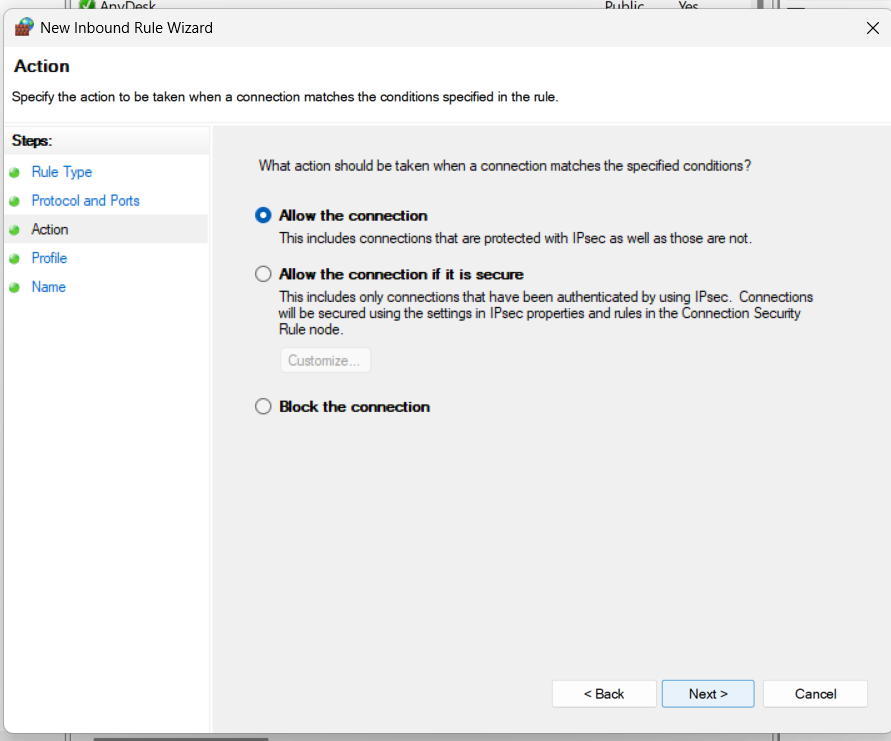


**B. Add a rule to block inbound TCP port 23 (Telnet) via GUI**

1. In **Inbound Rules** → on the right pane click **New Rule...**
2. Choose **Port** → Next.
3. Select **TCP**, **Specific local ports:** 23 → Next.
4. Action: **Block the connection** → Next.
5. Profile: check **Domain, Private, Public** (choose as needed) → Next.
6. Give it a name, e.g., **Block-Telnet-23** → Finish.







**C. Add a rule to allow a port (example: allow HTTP 80)**

* Same flow, but choose **Allow the connection** and set port 80. Name it **Allow-HTTP-80**.

Second we can add firewall Rule in linux, Here step by step command to run your linux machine to configure any kind of firewall service and block service.

Command :

**A. Install & enable UFW**

sudo apt update

sudo apt install ufw -y

# IMPORTANT: Allow SSH before enabling (if remote)

sudo ufw allow ssh # same as sudo ufw allow 22/tcp

# Then enable

sudo ufw enable

**B. Basic UFW commands (status, allow, deny, delete)**

* **Check status (verbose):**

sudo ufw status verbose

* **Block inbound TCP port 23 (Telnet):**

sudo ufw deny 23/tcp

# or: sudo ufw deny in proto tcp to any port 23

* **Allow SSH (if needed):**

sudo ufw allow 22/tcp

# or a named service:

sudo ufw allow OpenSSH

* **List numbered rules (to delete by number):**

sudo ufw status numbered

* **Delete rule by rule text or number:**

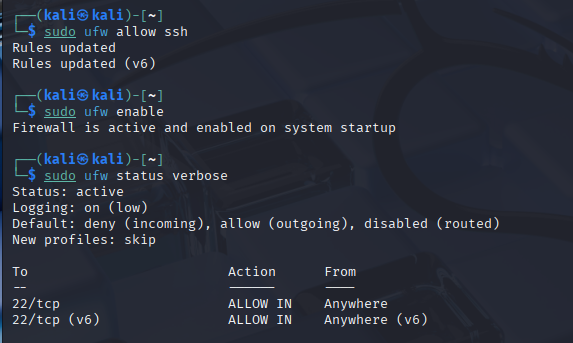
sudo ufw delete deny 23/tcp

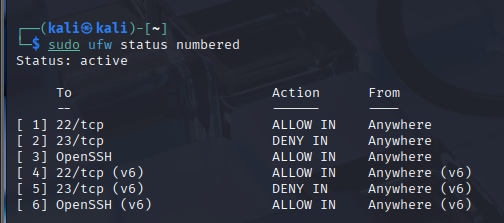
# or if numbered: sudo ufw delete 2

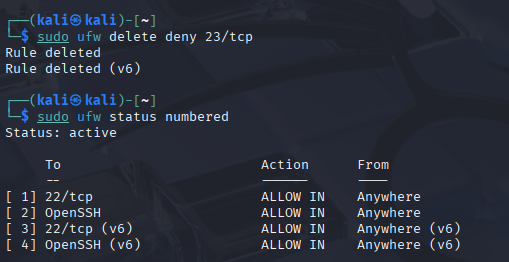
* **Disable / reload:**

sudo ufw disable

sudo ufw reload







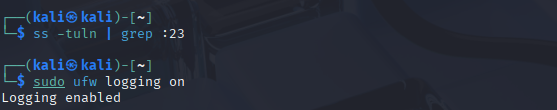
**C. Test UFW rules**

* **Check listening ports locally**:

ss -tuln | grep :23 # shows if something is listening on port 23

* **From the same machine** (local connect may bypass filtering if service bound to localhost) — better to test from another machine on same network:

nmap -p 23 <target-ip>



Output is nothing means not listing on port 23