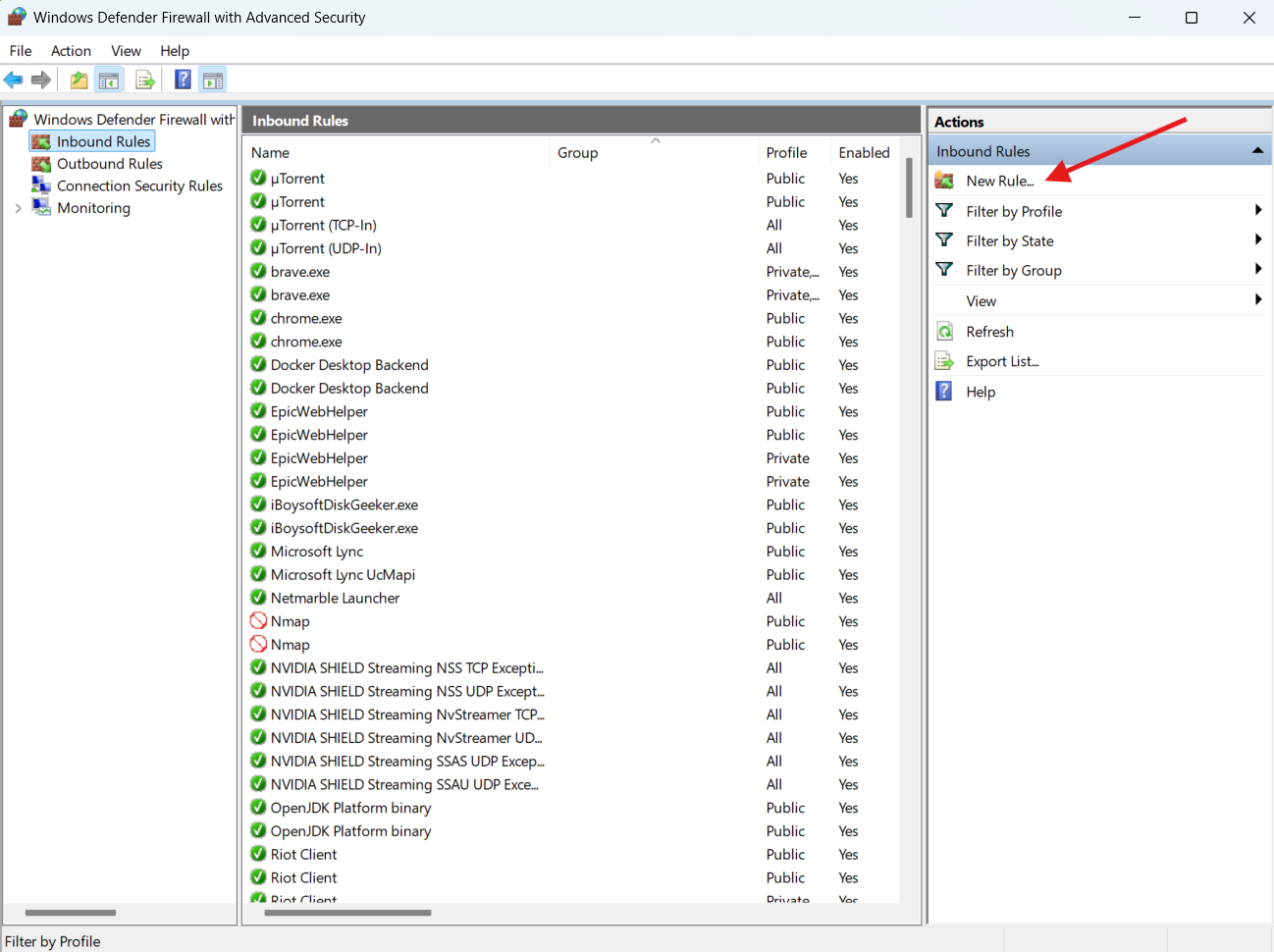
**Documentation Day – 3**

* **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.

**Procedure:**

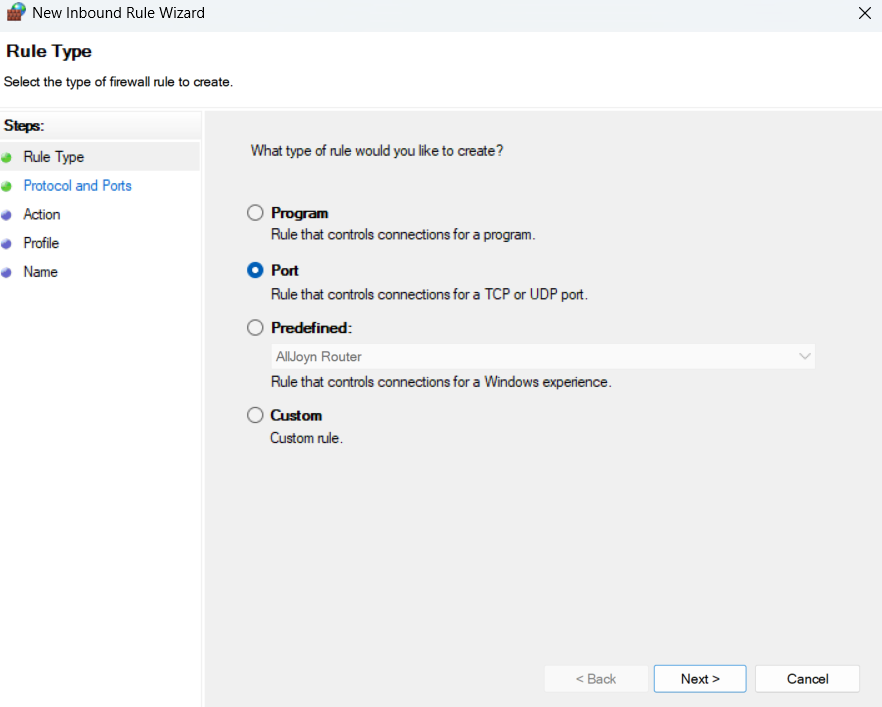
**On Windows:**

* Go to the start menu and search for **Windows Defender Firewall with Advanced Security.**
* To control incoming traffic to your computer. Click on the **Inbound rules.**
* To create a new rule, click on the **new rule.**

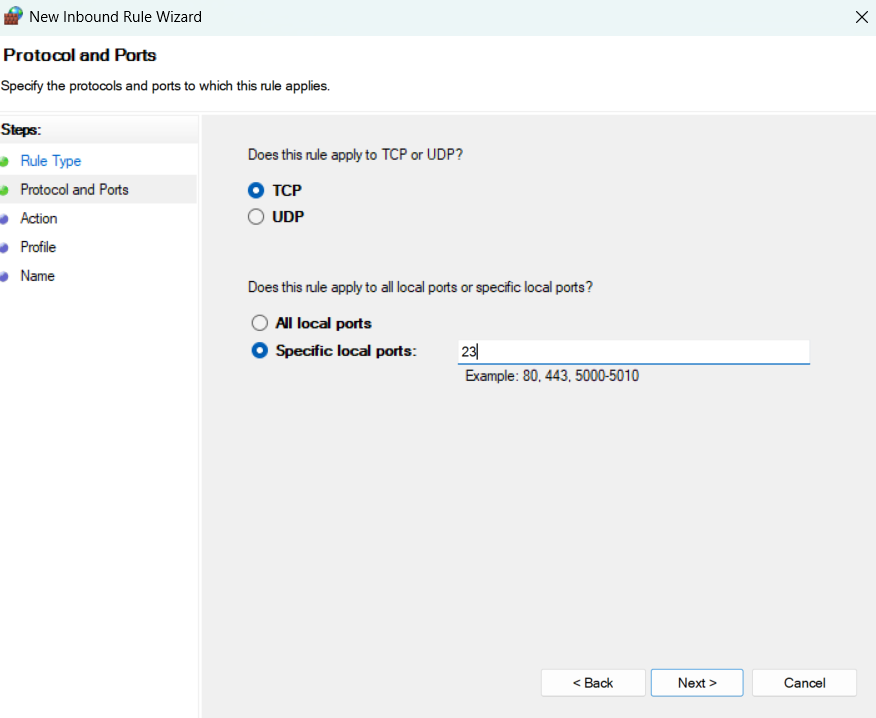


**You can see 4 types of rules:**

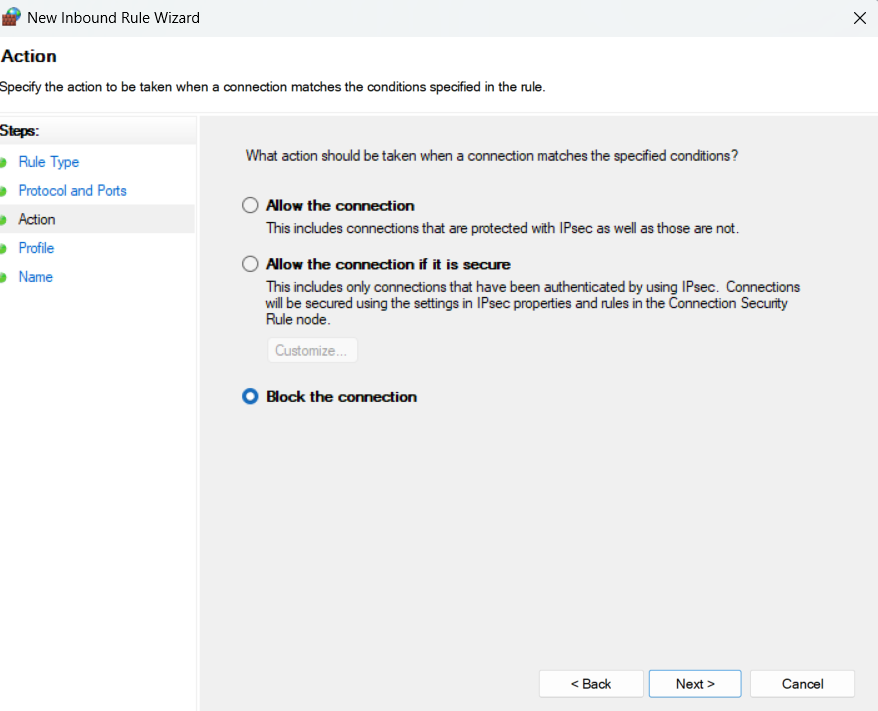
* Program: This rule controls one specific app (Like Chrome, Zoom, Game)
* Port: This rule controls one specific service (like telnet, ssh, http, dns, etc.)
* Predefined: This rule was readymade by Windows (like File and Printer Sharing, Remote Desktop, WMI, etc)
* Custom: An advanced rule, we can control everything here (like apps, ports, IP address, networks.



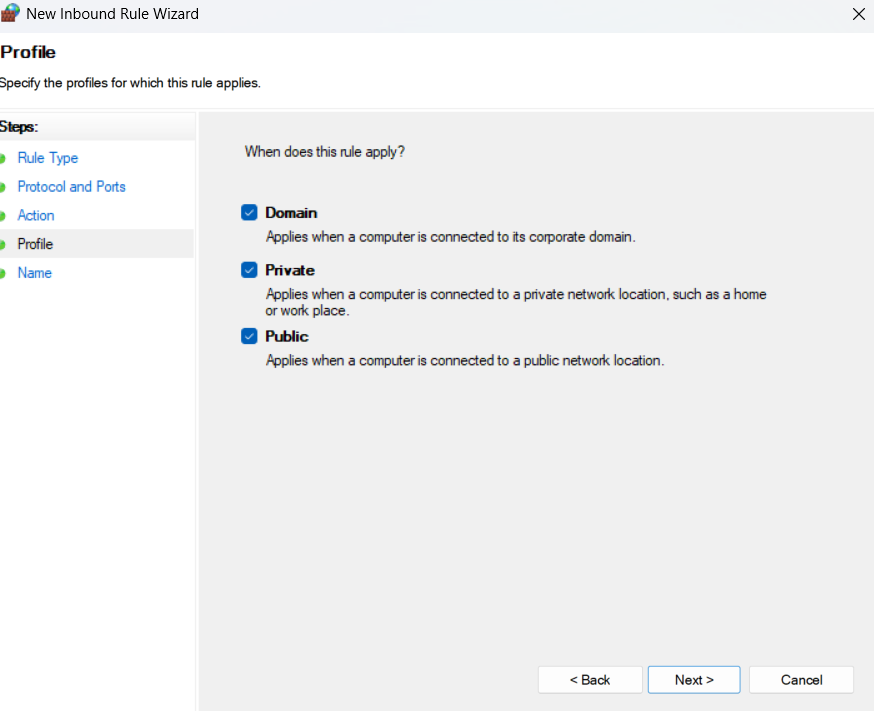
Here I want to block a port called telnet (i.e., port 23)



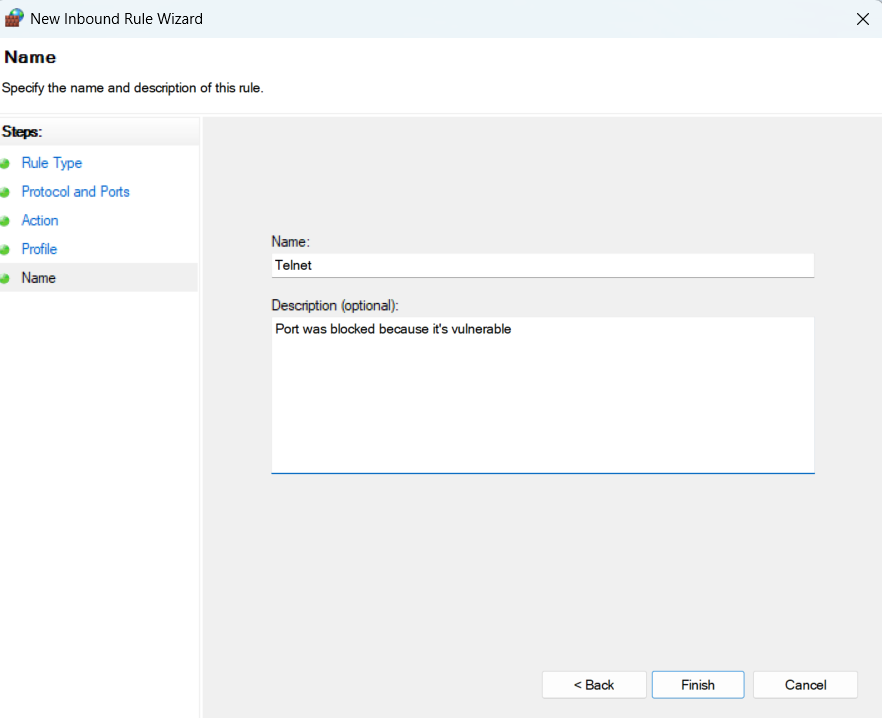
Block the connection with this port number.



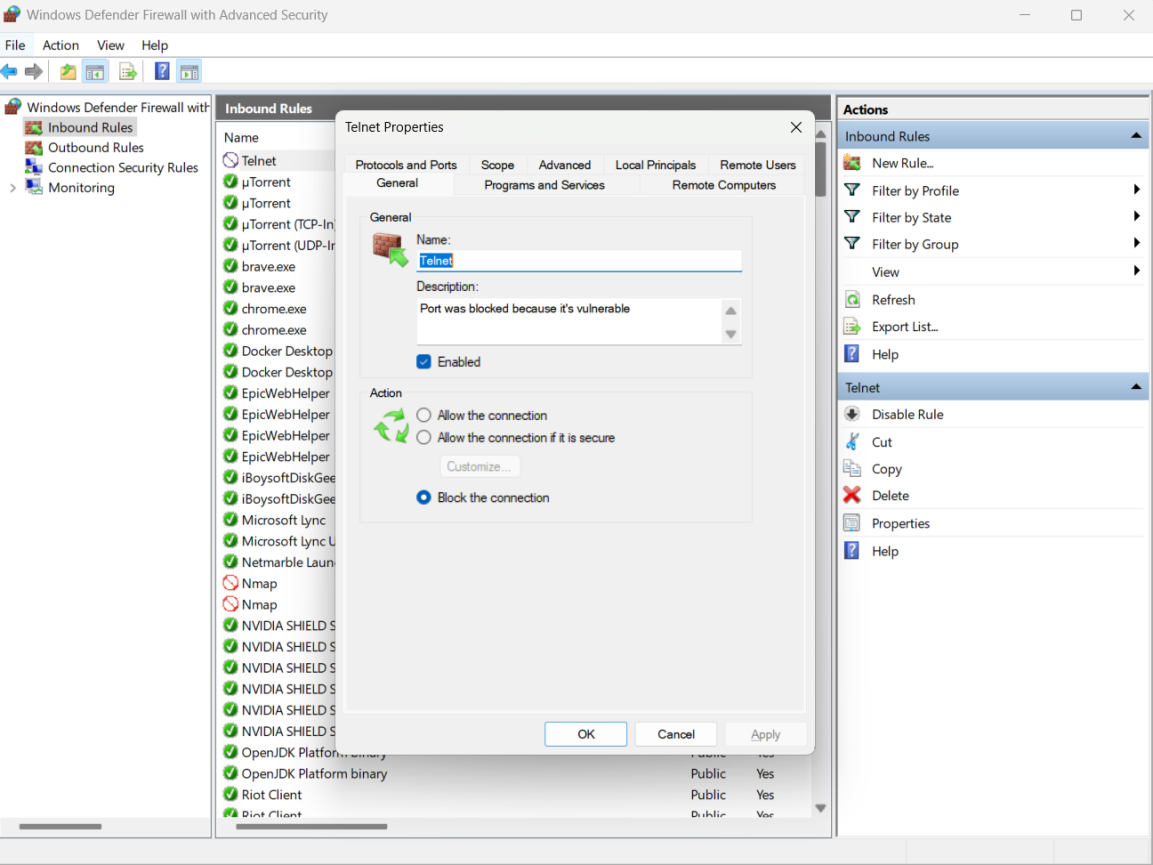
Based on your preferences, select the options.



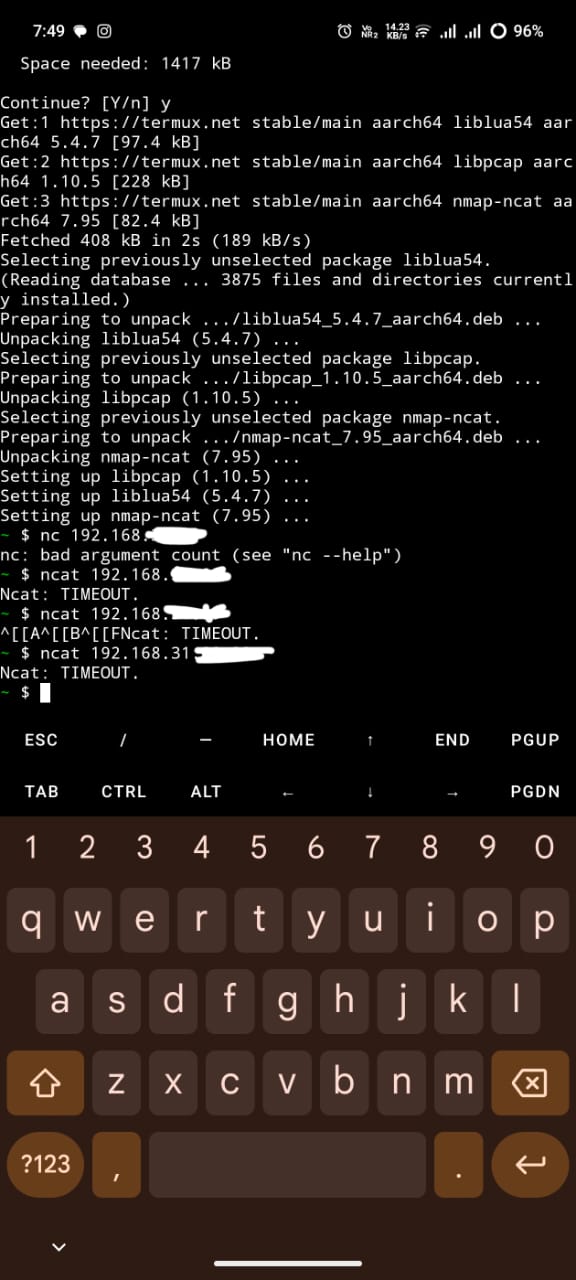
Provide a name to save the changes.



Blocking port number 23 was success. From now the communication with telnet is blocked. Until I allow the traffic for communication.



Let’s do a test either the port was blocked or not.



When I tried to connect to my computer on port 23 with my mobile, the result was **a timeout.**

This proves my firewall was blocking traffic on port 23.

**A firewall is a network security application that controls the traffic of a system. We can control the traffic by adding rules in the firewall.**

**How does it work?**

When a user intends to access a website, it requires port 443 and 53 to access a website. Here when you entered [www.g\*\*\*.c0m,](http://www.gvfuvb.com,) the traffic from your system need to check weather do we have access to that port or not, it goes to the firewall and checks the port 443 and 53 is set to allow or block, if it was allowed then in return from the server it need to confirms from the firewall do we have access to communicate from inbound rules, if allows we get communication uninterruptedly, else no.