CYBER SECURITY INTERNSHIP - TASK 4

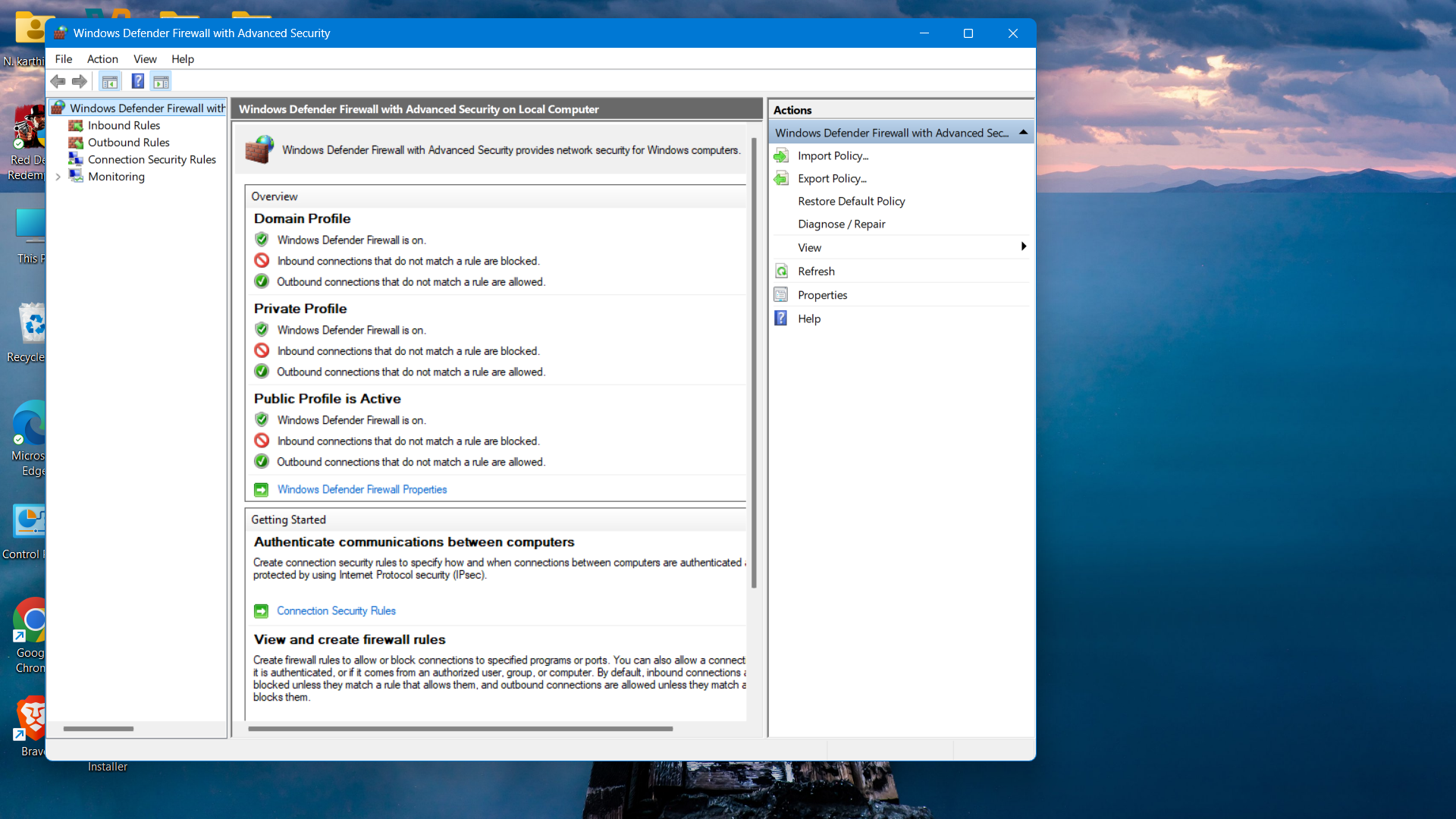
# 🔐 Summary

In this task, I configured the Windows Defender Firewall to block inbound traffic on Telnet port 23. This involved creating a custom inbound rule, testing the rule by attempting a connection, and then removing the rule to restore the original state. This hands-on firewall setup demonstrated the ability to filter traffic and secure a system from unwanted or insecure access.

## Open Windows Firewall Settings

To begin configuring the firewall, press Win + R to open the Run dialog box.  
Type wf.msc and press Enter to launch the Windows Defender Firewall with Advanced Security console.  
This interface allows you to view, create, and manage inbound and outbound firewall rules.

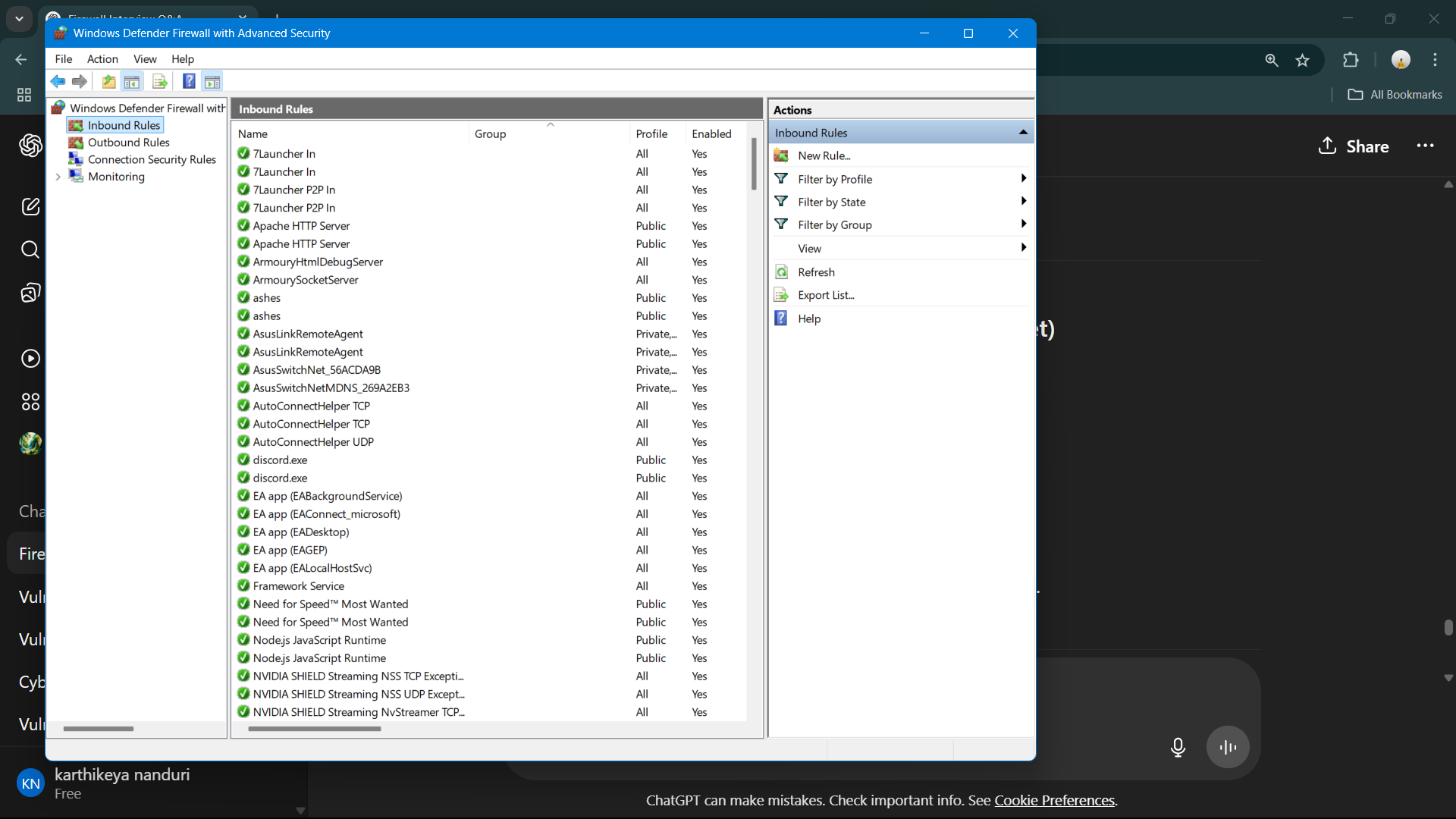
Screenshot:



## 2. View Current Firewall Rules

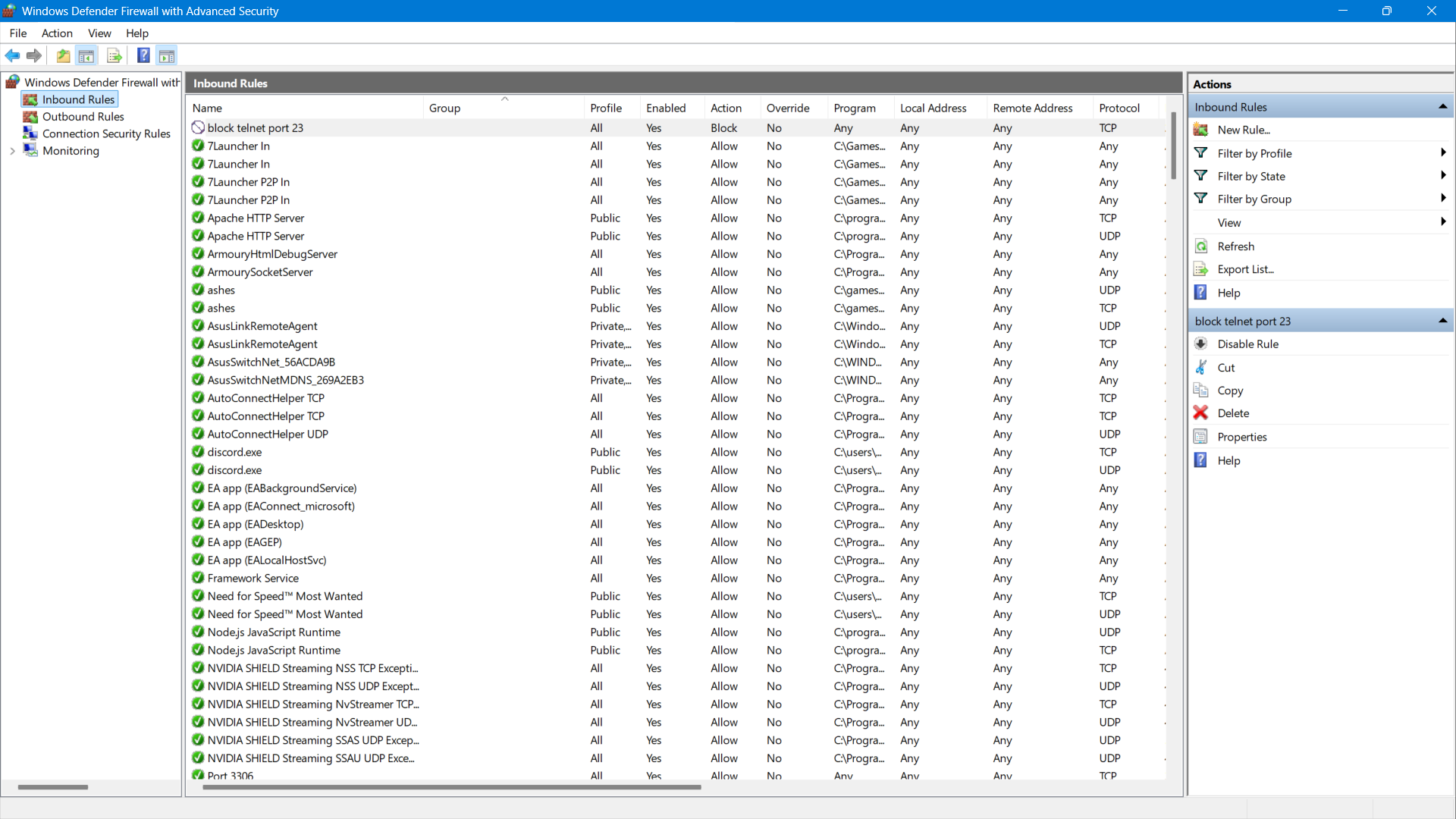
In the Windows Firewall console, navigate to **Inbound Rules** and **Outbound Rules** in the left panel.  
These sections display all the active rules controlling network traffic on your system.  
You can inspect rule details such as port numbers, protocols, actions (allow/block), and profiles.

Screenshot:



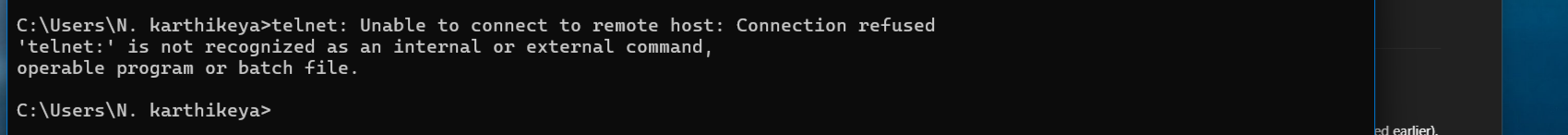
## Create Rule to Block Inbound Traffic on Port 23 (Telnet)

**Create Rule to Block Inbound Traffic on Port 23 (Telnet)**  
Click on **New Rule** under the Inbound Rules section and select **Port** as the rule type.  
Choose **TCP**, enter **23** as the specific port, and select **Block the Connection**.  
Apply the rule to all profiles and name it appropriately, such as *Block Telnet Port 23*.

Screenshot:

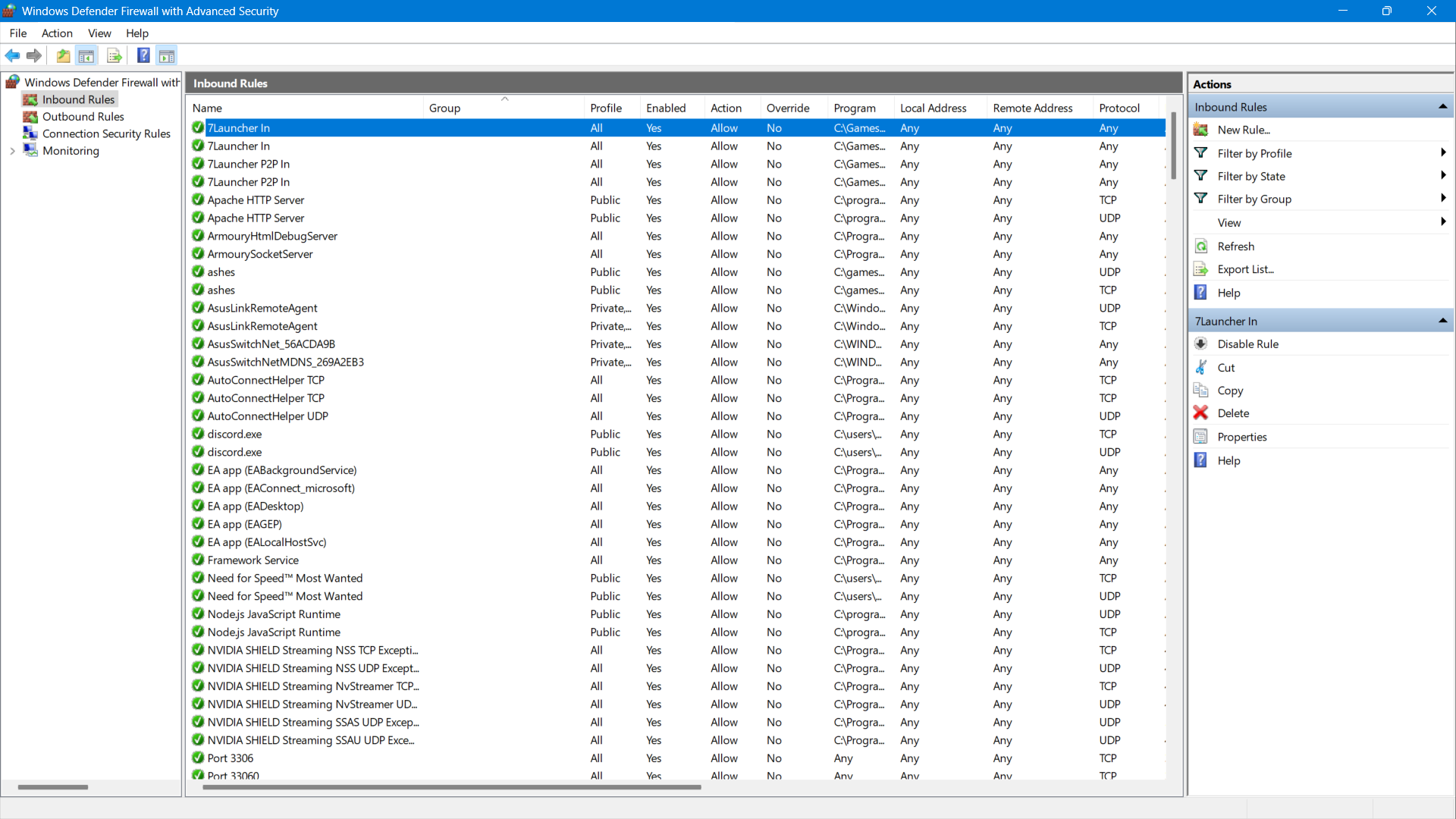
## 4. Test the Rule using Telnet or Port Query Tool

**Test the Rule using Telnet or Port Query Tool**  
Open **Command Prompt** on another device and run: telnet <your-IP> 23 to test the connection.  
If the firewall rule is working, the connection attempt will fail, confirming that port 23 is blocked.  
Alternatively, use the **PortQry** tool to query port status and verify it's inaccessible.

Screenshot:

## 5. Remove the Block Rule to Restore Original State

**Remove the Block Rule to Restore Original State**  
Open **Windows Defender Firewall with Advanced Security** and go to the **Inbound Rules** section.  
Locate the rule created to block port 23, right-click on it, and select **Delete**.  
This removes the restriction and restores the default firewall behaviour for Telnet traffic.

Screenshot:

# Firewall Filtering Understanding

A firewall acts as a barrier between trusted and untrusted networks. It filters network traffic based on configured rules, improving system and network security. By blocking insecure ports such as Telnet (port 23), systems can prevent unauthorized or unsafe remote access.