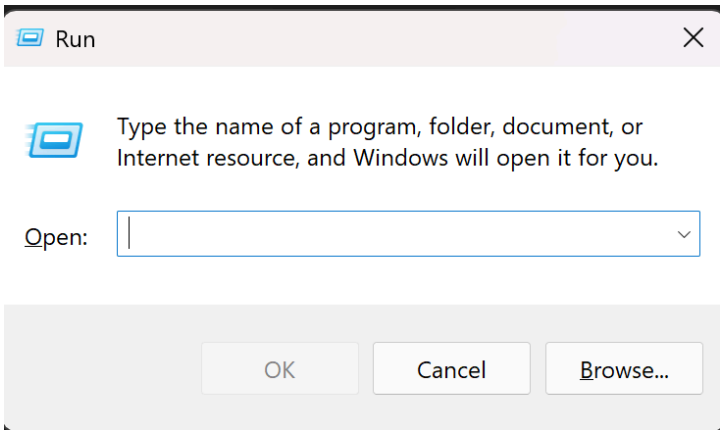
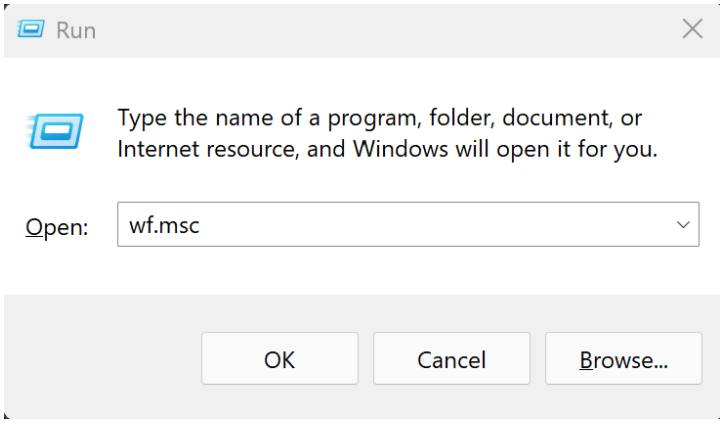
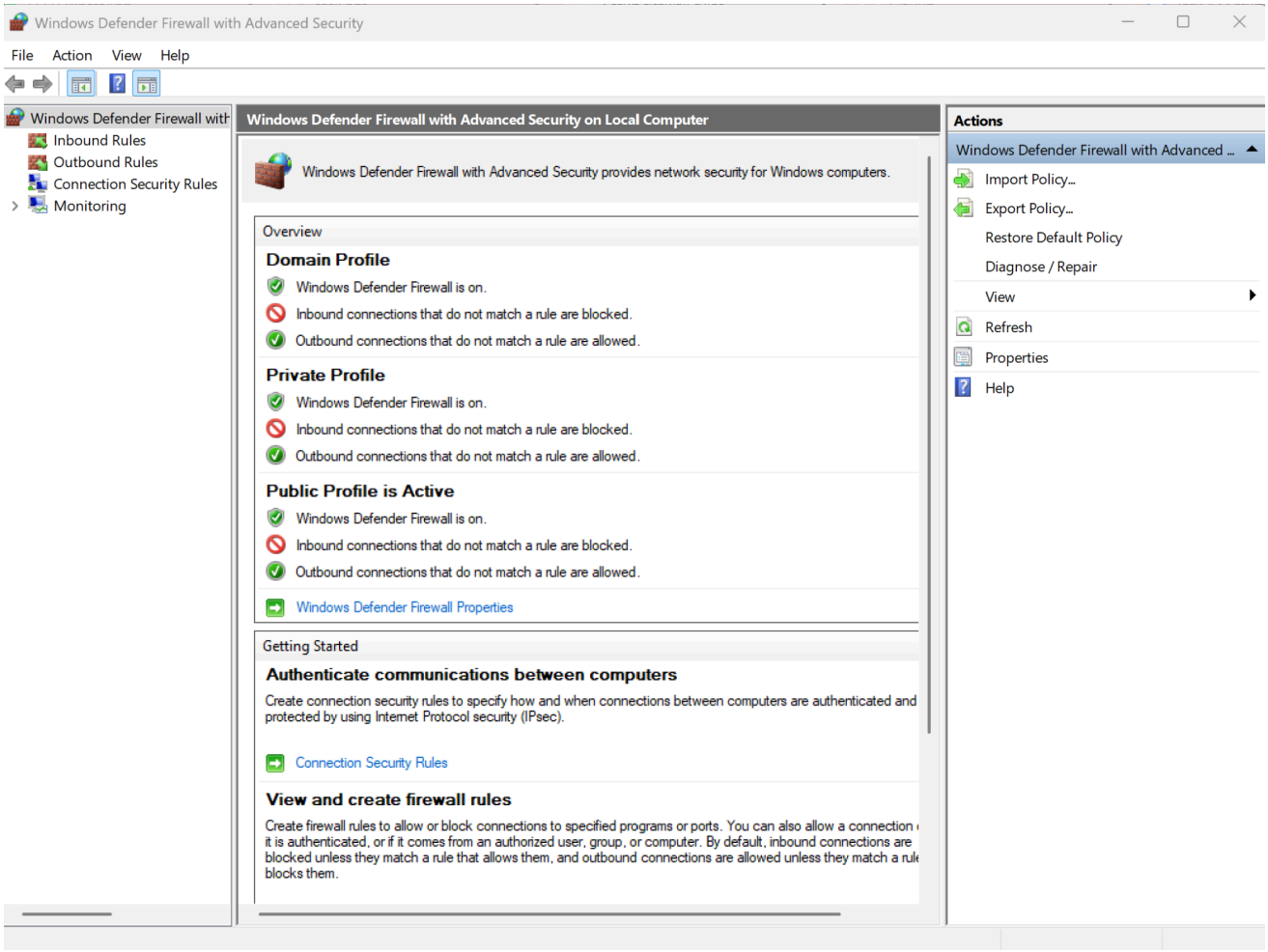
Task 4 : Setup and Use a Firewall on Windows/Linux

1.Open firewall configuration tool (Windows Firewall or terminal for UFW).



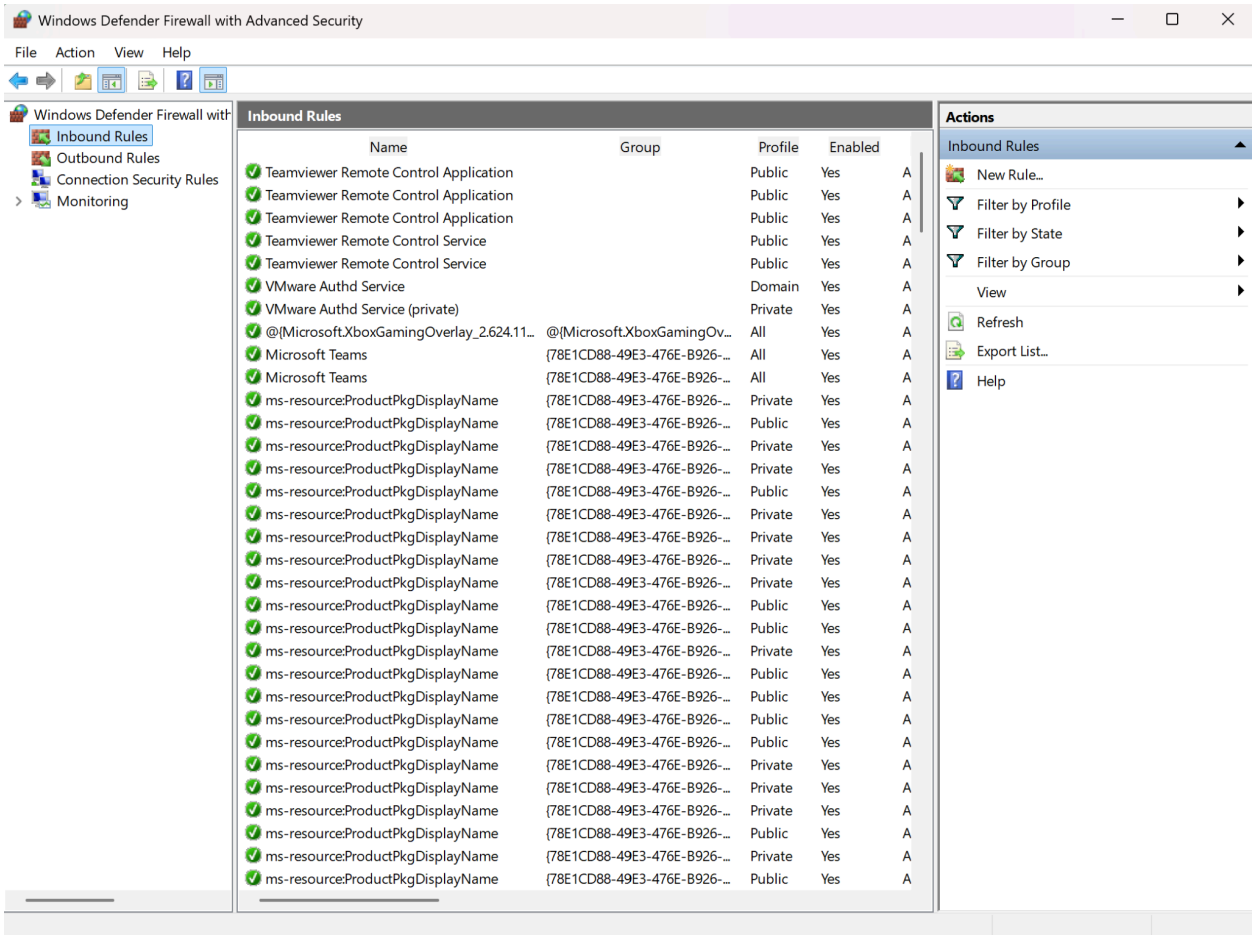


I run the command wf.msc which will open the windows defender firewall with advanced security

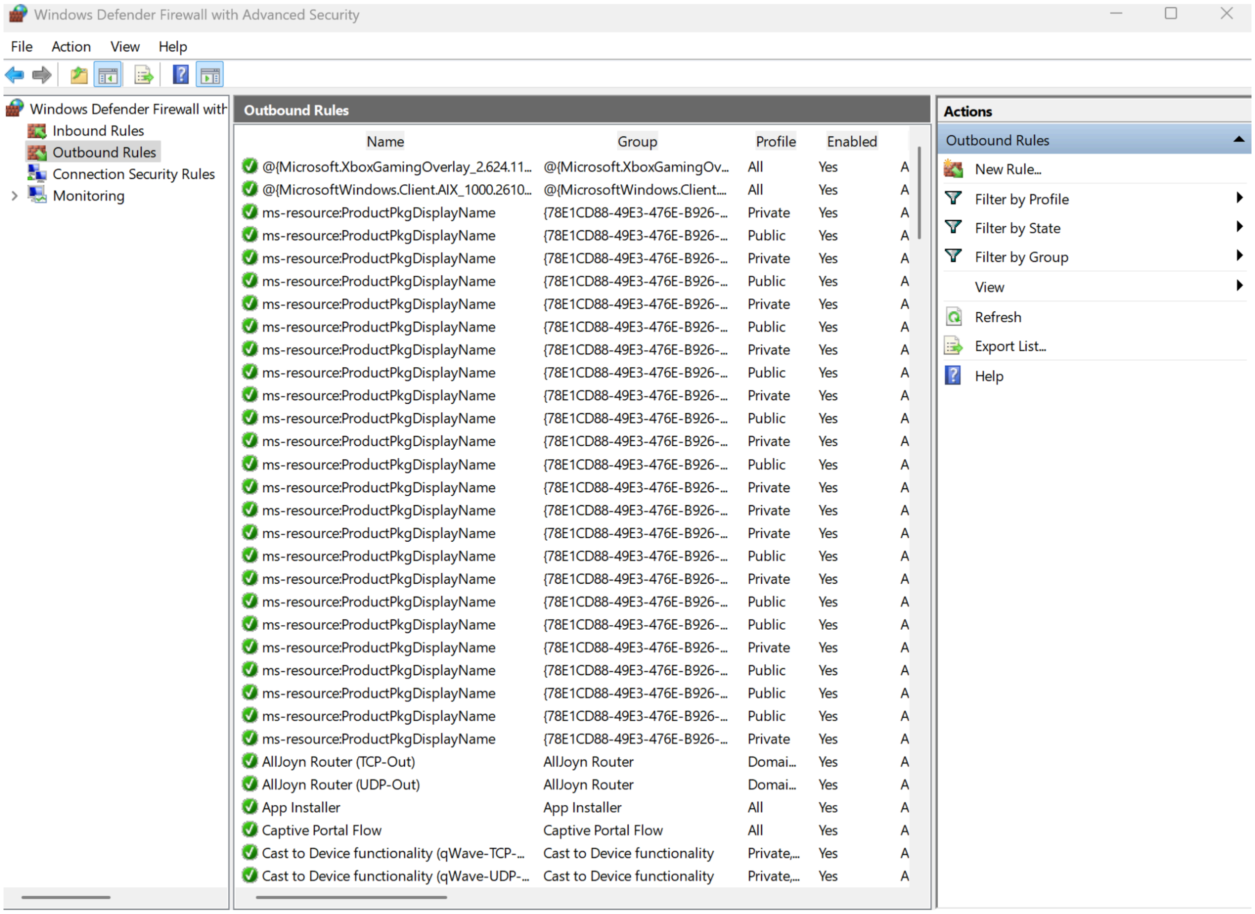


Opened the firewall configuration tool to manage network access settings. On Windows, accessed **Windows Defender Firewall with Advanced Security** using **wf.msc.** This interface allows viewing, creating, and modifying inbound and outbound traffic rules.

2.List current firewall rules.

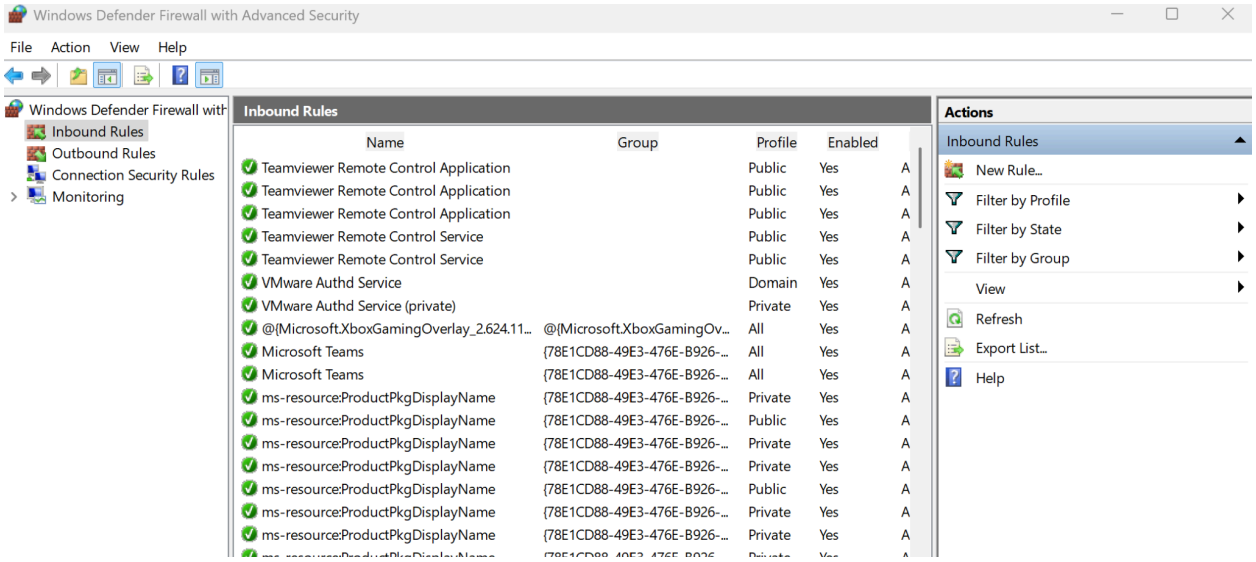


Inbound Rule - Viewed the list of inbound rules to see which applications and ports are allowed or blocked for incoming network traffic on the system.

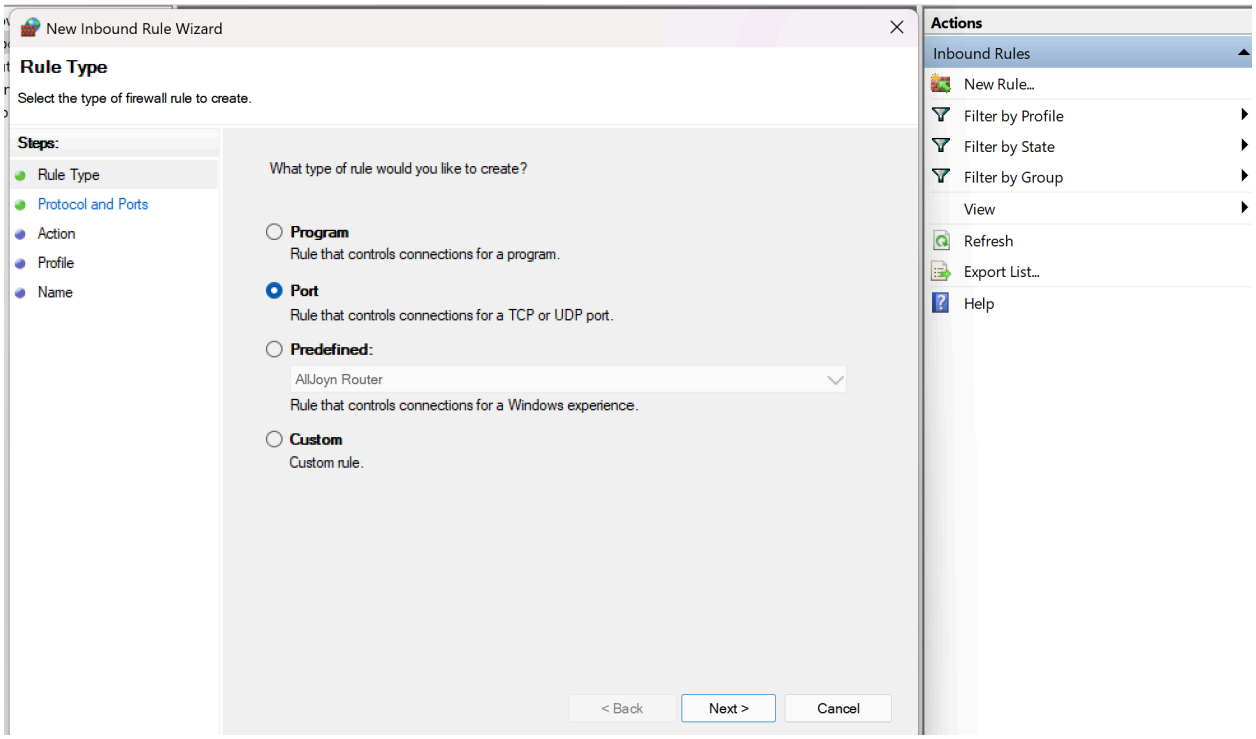


Outbound Rule - Viewed the list of outbound rules to check which applications and ports are allowed or blocked for outgoing network traffic from the system.

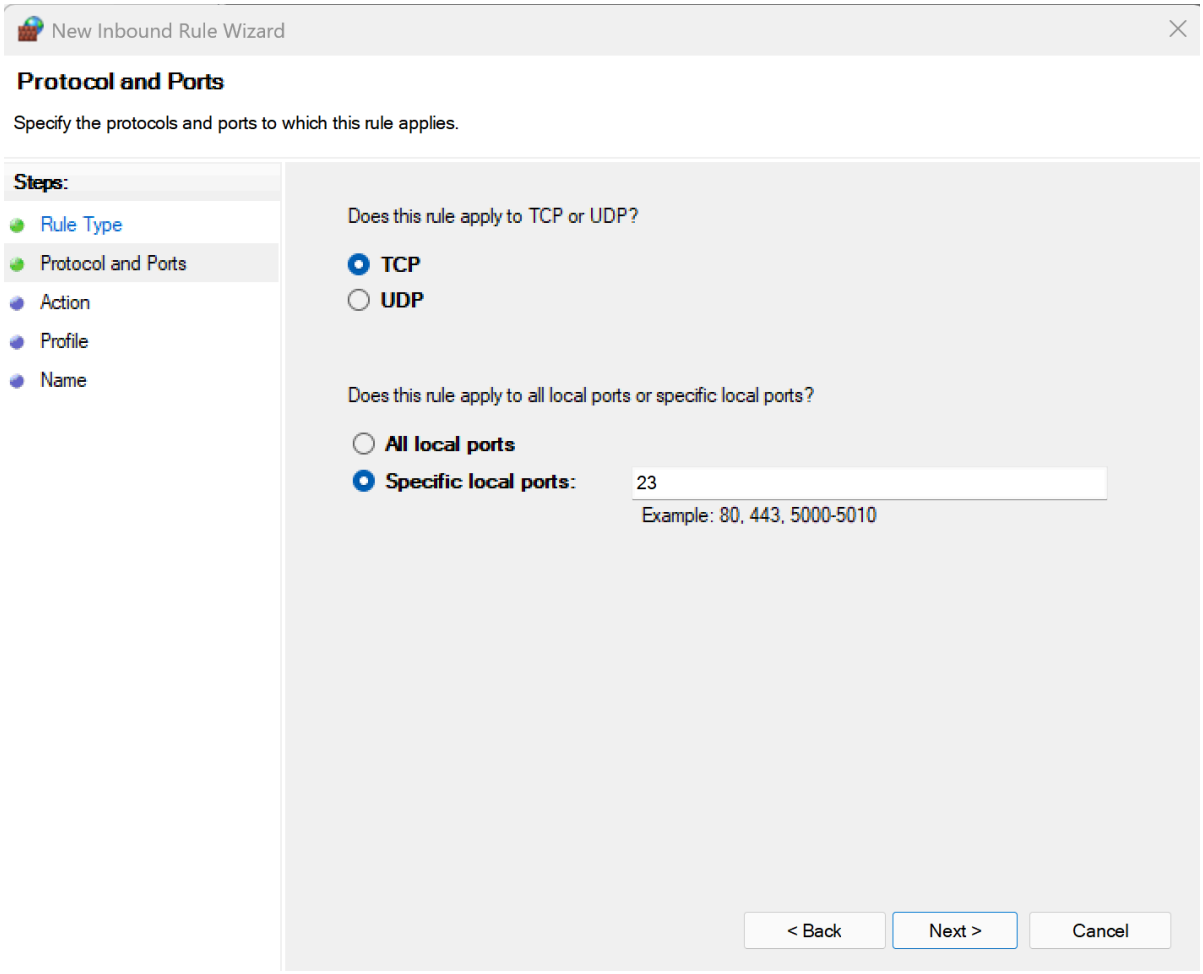
3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).



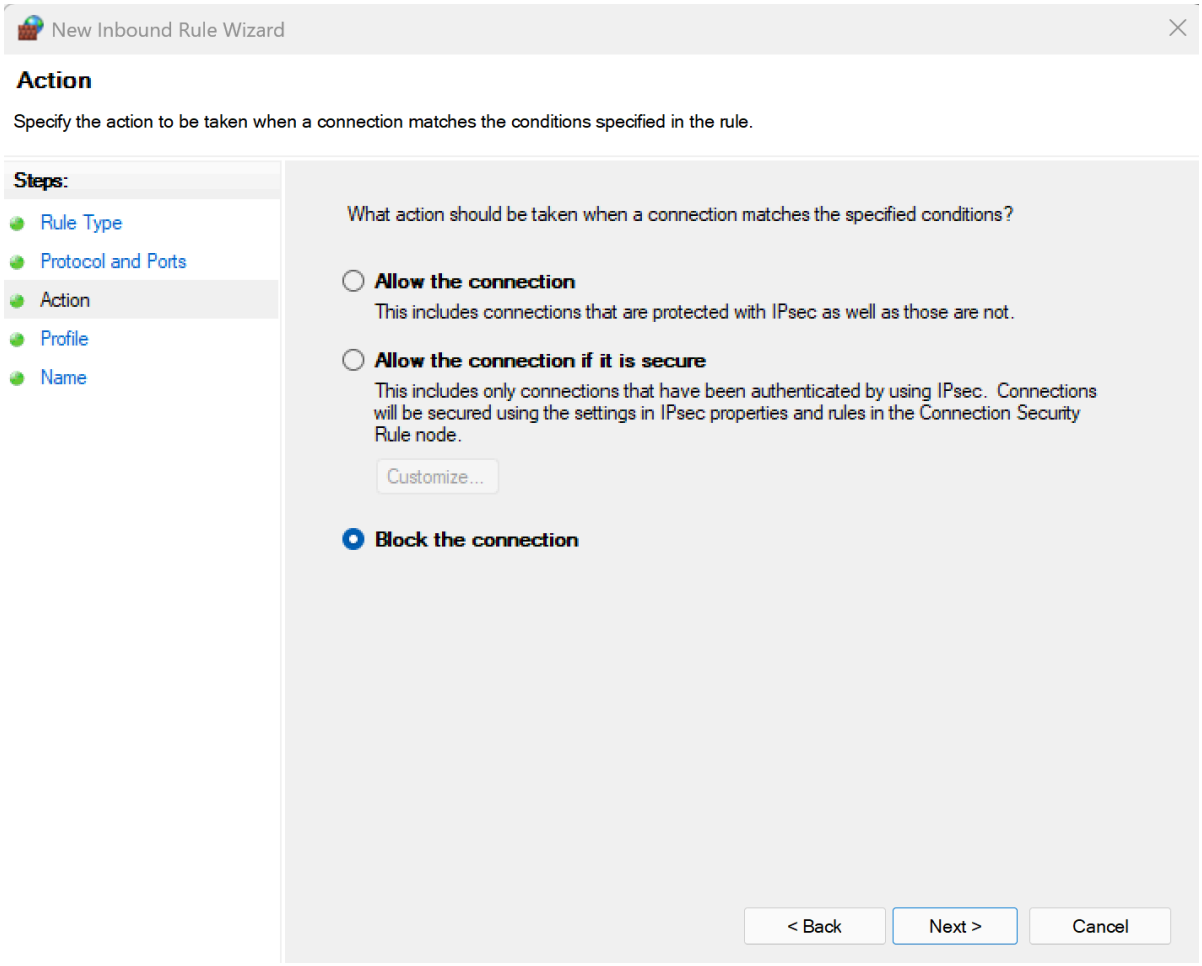
I Opened the Windows Defender Firewall with Advanced Security tool to manage network traffic rules.



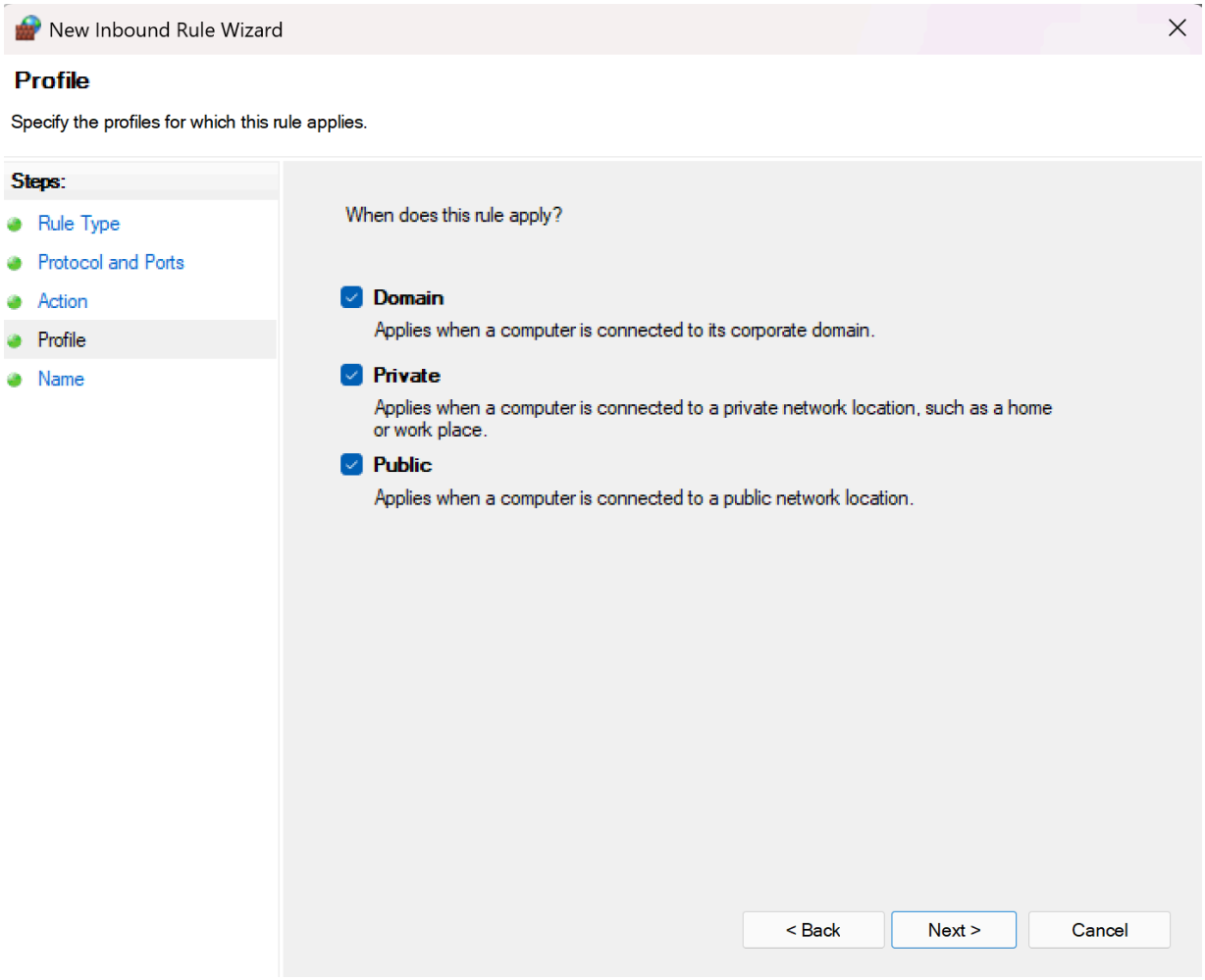
Selected 'Inbound Rules' from the left panel to create a rule for incoming traffic and licked 'New Rule' in the right panel to start creating a new inbound rule.Chose the 'Port' option in the wizard to block a specific port number.



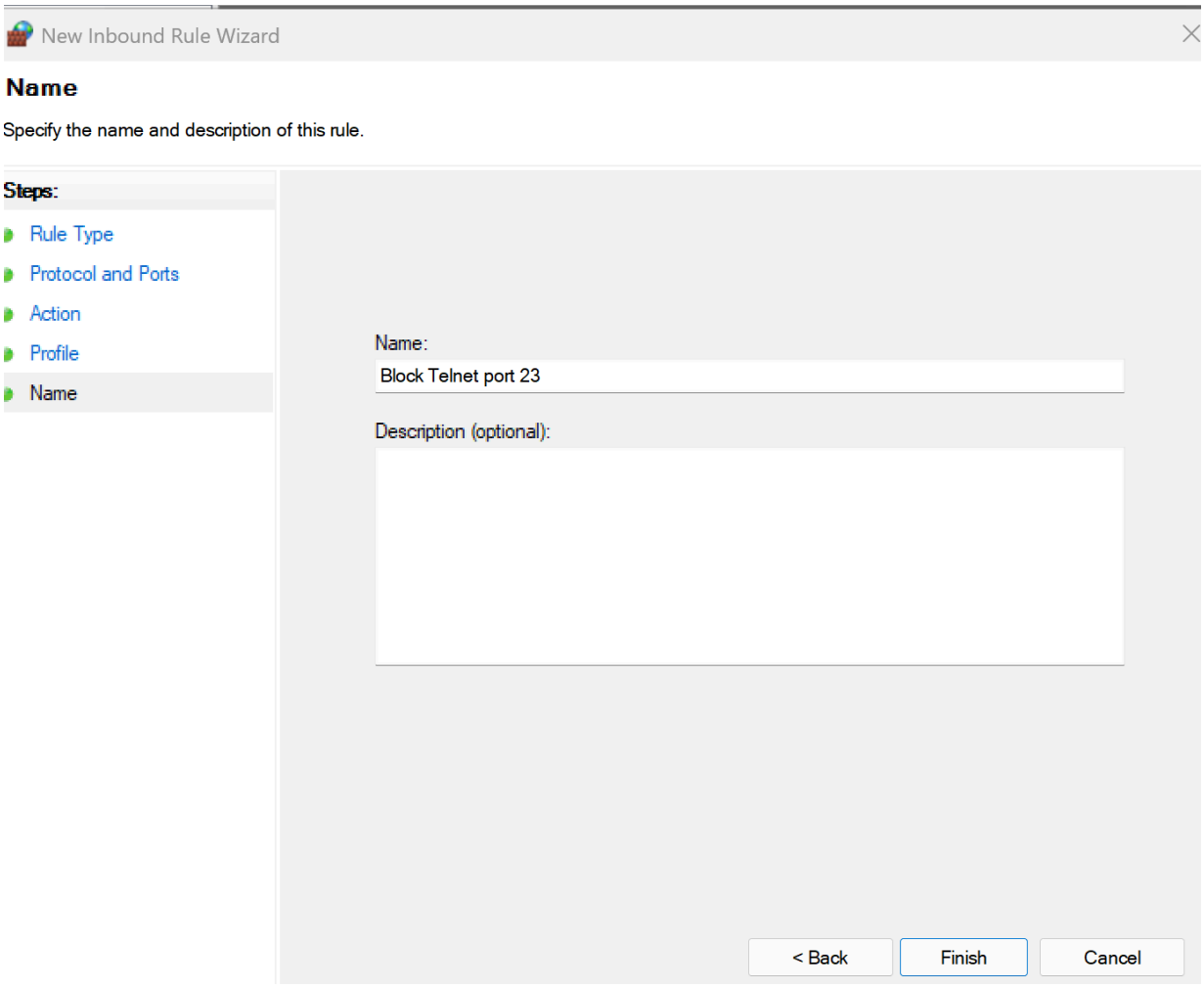
I Selected TCP protocol and entered port number 23 to target Telnet traffic.



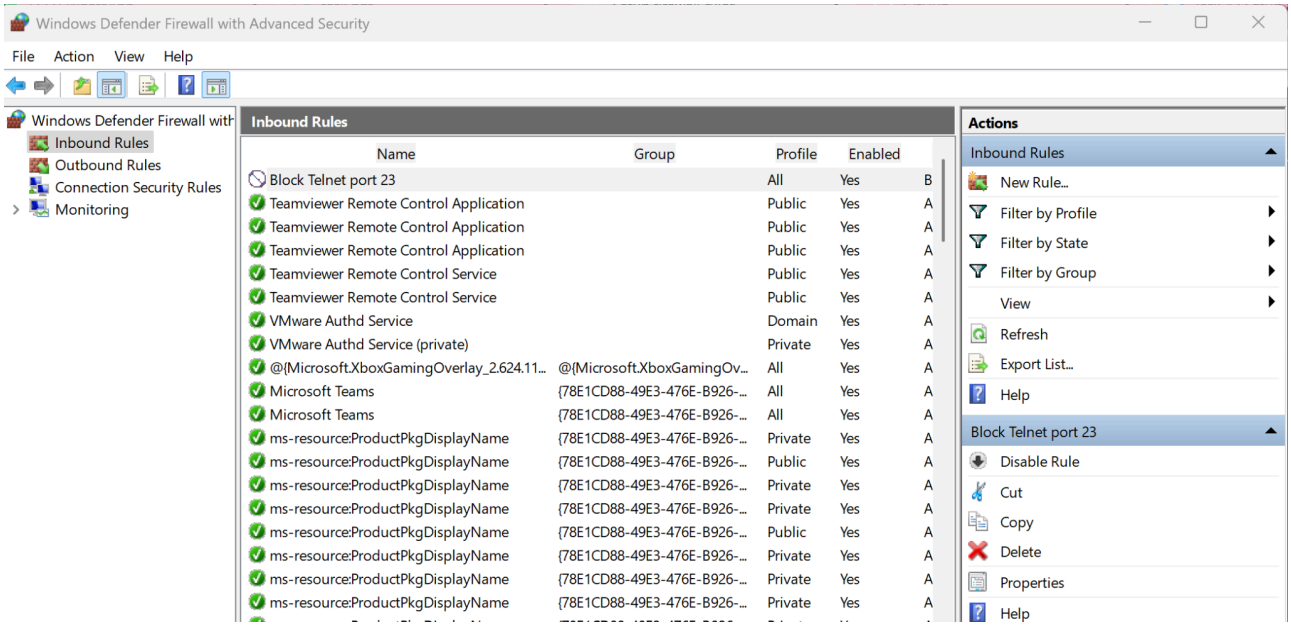
Picked 'Block the connection' so any traffic on port 23 will be denied.



I chosen when the rule applies - Domain, Private, and Public networks.

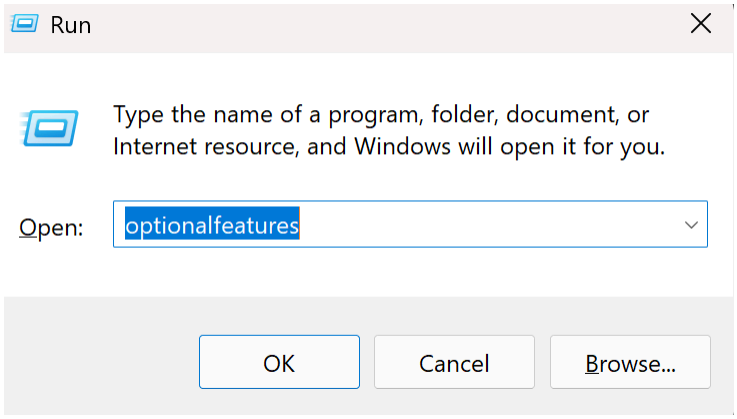


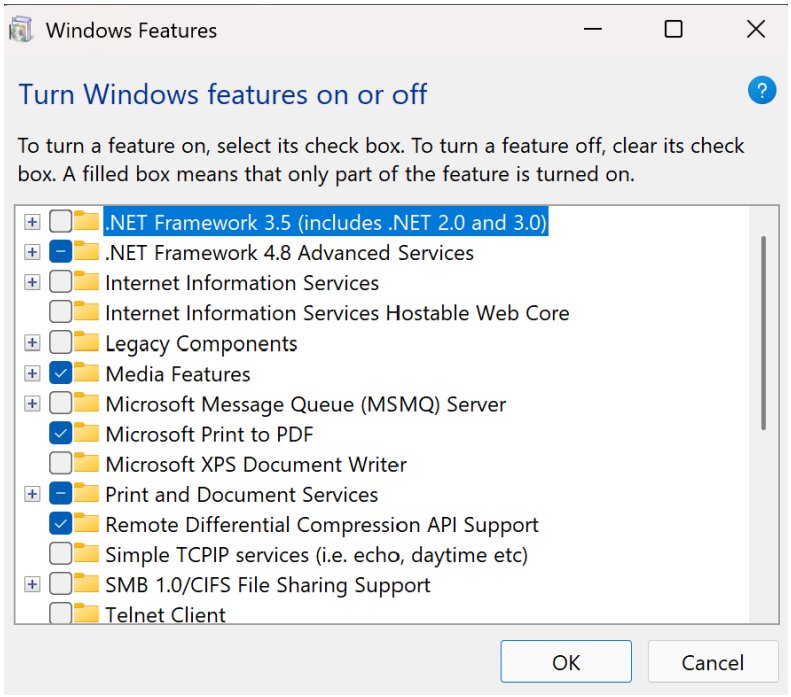
I Named the rule 'Block Telnet Port 23' and clicked Finish to save it.



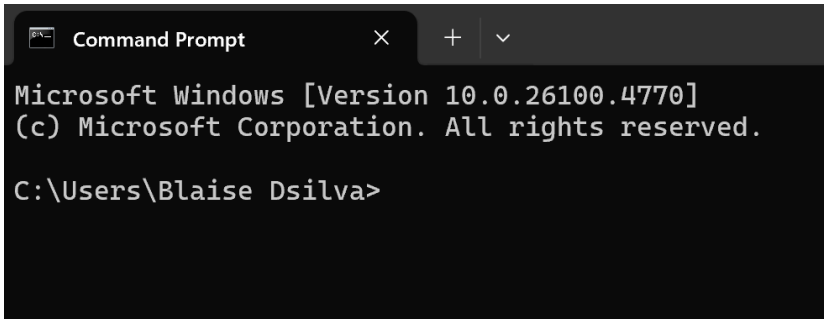
Inbound rule 'Block Telnet port 23' is active. It blocks all incoming traffic on port 23 (Telnet).

4.Test the rule by attempting to connect to that port locally or remotely.



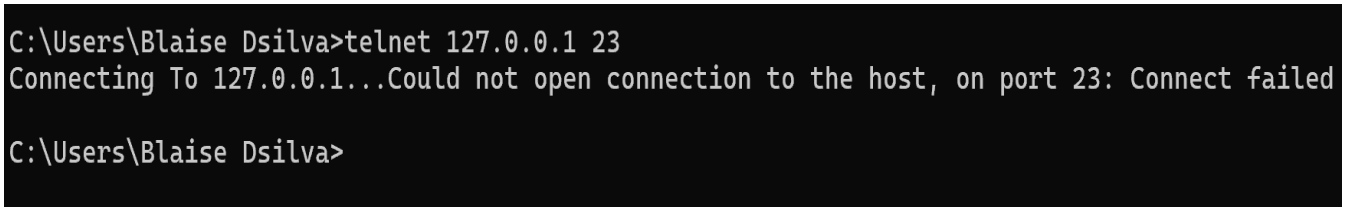


I ticked telnet client to enable it.



I opened cmd.

Run the following command telnet 127.0.0.1 23.

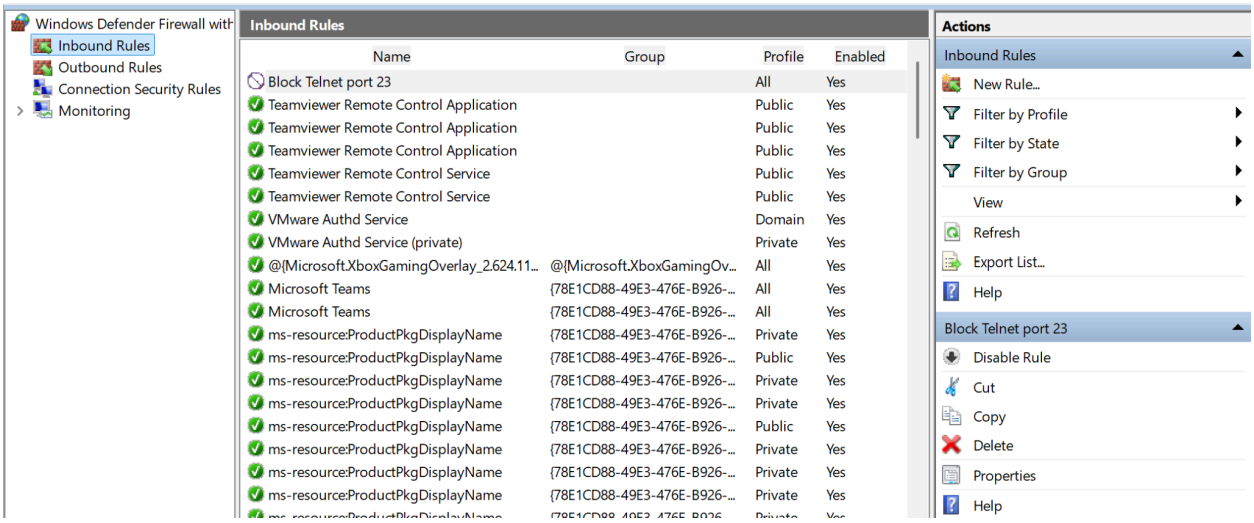


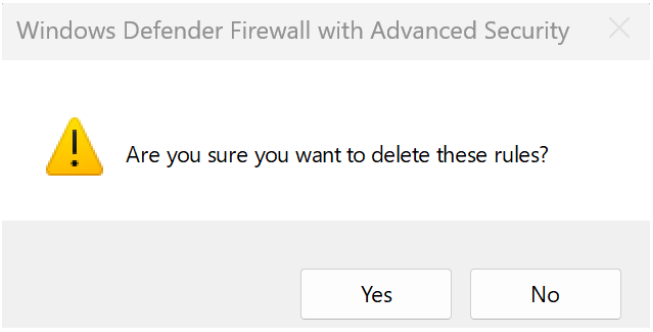
Tried connecting to localhost on port 23 using Telnet. The connection failed, confirming that the firewall rule is successfully blocking Telnet traffic.

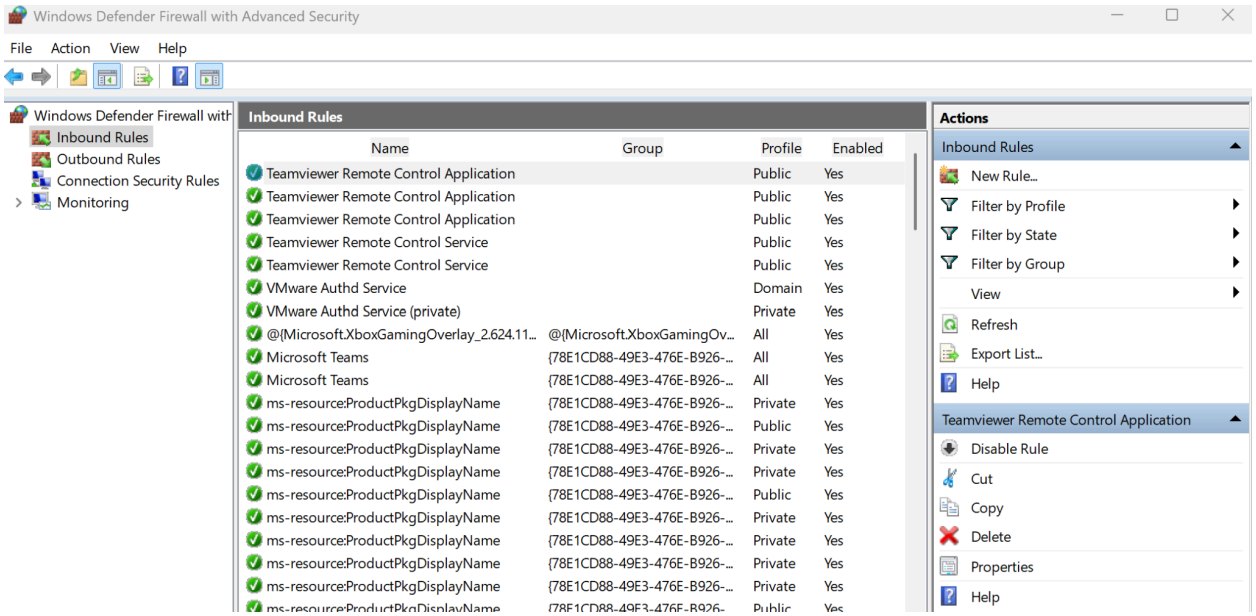
5.Add rule to allow SSH (port 22) if on Linux.

As im using windows.

6.Remove the test block rule to restore original state.







I opened the **Windows Firewall with Advanced Security**, navigated to the **Inbound Rules** section, and located the rule that was blocking port 23. I right-clicked on the rule and selected **Delete** to remove it.

7.Document commands or GUI steps used.

In this task, I documented the steps and commands used for configuring and testing the firewall on Windows.

1. Opening the Firewall Configuration Tool:
   On Windows, I opened Windows Defender Firewall with Advanced Security by typing the command wf.msc in the Run dialog box. This gave me access to manage both inbound and outbound firewall rules.

2. Listing Current Firewall Rules:
   I navigated to the Inbound Rules and Outbound Rules sections in the Windows Firewall to review the current rules in place. These rules show which applications and ports are allowed or blocked for incoming and outgoing traffic.

3. Adding a Rule to Block Inbound Traffic on Port 23 (Telnet):
   In the Inbound Rules section, I clicked on New Rule to create a new rule that blocks inbound traffic on port 23 (Telnet).
   I selected the Port option, chose TCP, and specified port 23. Then I selected Block the connection and applied the rule to Domain, Private, and Public networks.

4. Testing the Rule:
   I enabled Telnet Client in Windows Features, opened Command Prompt (cmd), and tested the rule by typing the command:
   bash
   CopyEdit
   telnet 127.0.0.1 23 The connection failed, confirming that the firewall rule was successfully blocking Telnet traffic.

5. Removing the Block Rule:
   To restore the original firewall settings, I navigated to the Inbound Rules section, located the block rule for port 23, right-clicked on it, and selected Delete to remove the rule.

8.Summarize how firewall filters traffic.

Through completing the tasks related to setting up and managing a firewall, I've gained a deeper understanding of how firewalls work to secure networks and manage traffic. Here's what I've learned step-by-step:

1. Opening and Configuring Firewalls (Windows)
   I learned how to access the firewall configuration tools, such as Windows Defender Firewall with Advanced Security using wf.msc, which allowed me to manage inbound and outbound rules effectively.
   I understood the importance of setting firewall rules to control which applications and services are allowed to communicate over the network, essentially controlling the flow of network traffic.

2. Listing Current Firewall Rules
   I learned how to view the current firewall rules using both GUI and command-line methods.
   By listing the inbound and outbound rules, I was able to see which services were permitted or blocked, and how different ports were being used by applications. This helped me understand how firewalls manage access at both the application and network levels.

3. Blocking Inbound Traffic on Specific Ports
   I understood how to block specific traffic by creating inbound rules. For example, by blocking port 23 (Telnet), I saw how certain types of network communication can be prevented.
   I realized the importance of such rules in preventing unauthorized access to services or potential exploitation of open ports in the system.

4. Testing Firewall Rules
   I learned how to test firewall rules by attempting to connect to a blocked port, like port 23, using Telnet. By seeing the connection failure, I confirmed that the firewall rule was working as intended.
   This practical testing gave me a clear understanding of how firewalls actively monitor and control traffic.

5. Removing a Rule to Restore the Original State
   I learned how to easily remove a firewall rule once testing is done, ensuring that the system returns to its original configuration. This also taught me the importance of

cleaning up and restoring settings after modifications to maintain system integrity.

6. Documenting Commands and GUI Steps
   I learned how to document every step I performed, including the commands used and GUI steps followed. This documentation helped me build a clear record of the process and will be useful for future reference or audits.

7. General Understanding of Firewall Traffic Filtering
   Finally, I gained a better understanding of how firewalls filter traffic by checking incoming and outgoing connections based on IP addresses, port numbers, protocols, and connection states. I now see how firewalls play a crucial role in protecting systems by allowing only authorized traffic and blocking malicious or unwanted access.

A firewall filters traffic by analyzing incoming and outgoing data packets based on predefined rules. It checks factors like **IP addresses**, **ports**, and **protocols** to decide whether to allow or block the traffic. This helps protect systems from unauthorized access, malicious activity, and network attacks.