CYBER SECURITY INTERNSHIP - TASK 4

Task Title: Set Up and Use a Firewall on Windows

Objective: Set up and test default firewall rules for allowing or blocking traffic by using Windows Defender Firewall.

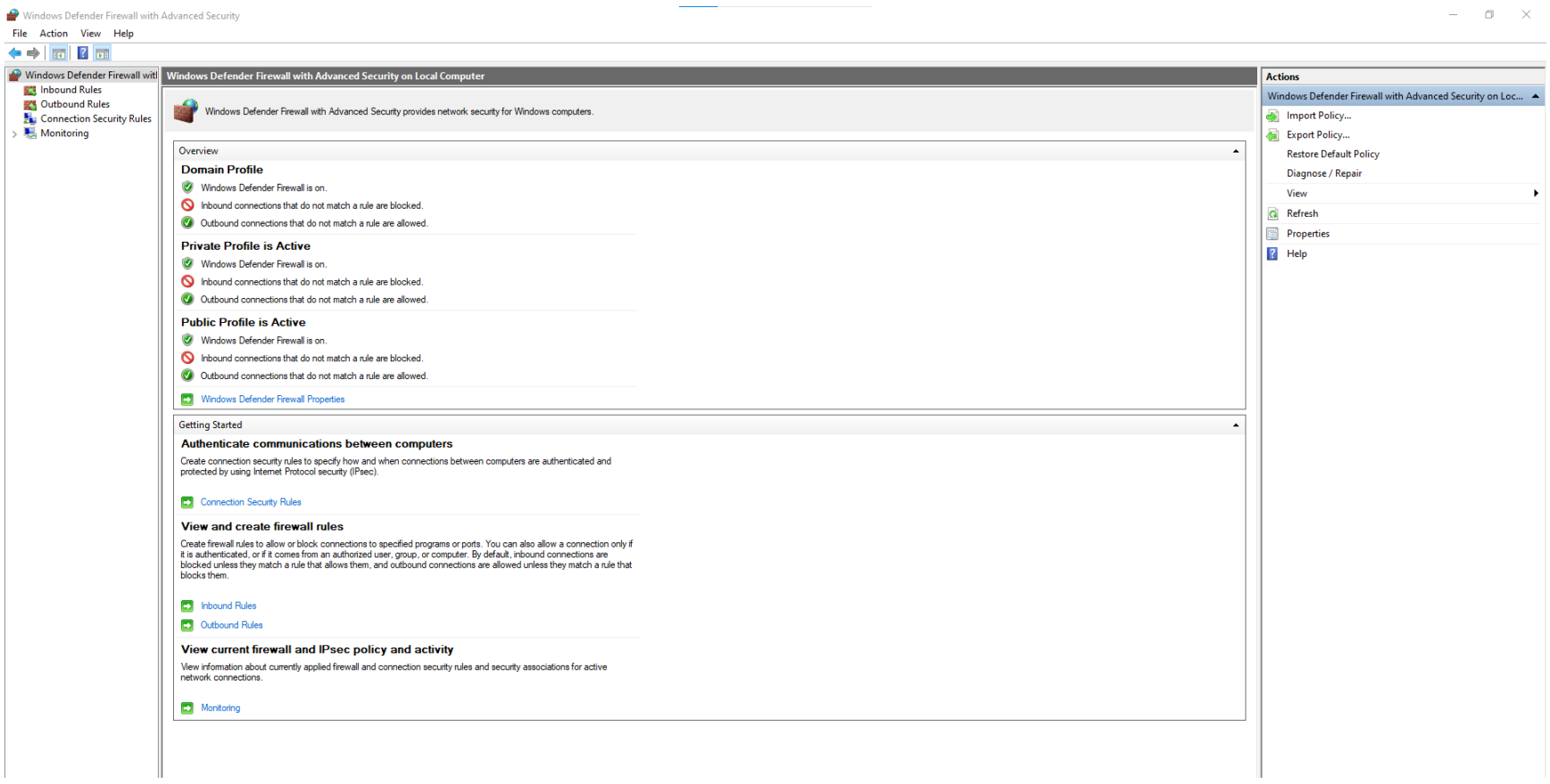
Tool Used: Windows Defender Firewall with Advanced Security

Here's what I did :

Step 1: Open Firewall Configuration Tool

Visited Windows Defender Firewall > Advanced Settings.

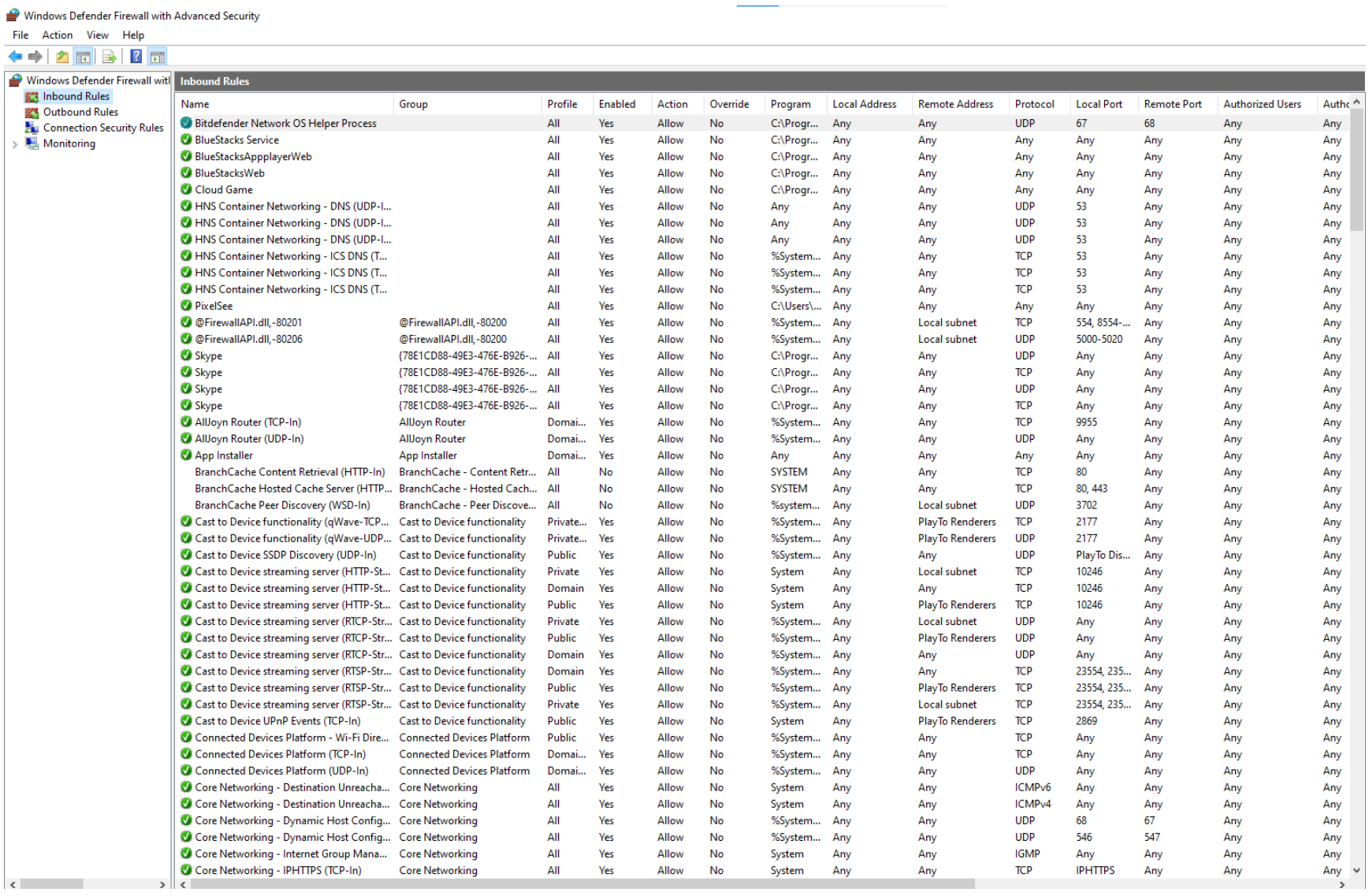
Opened "Inbound Rules" section to handle traffic.



Screenshot 1: Windows Firewall Advanced Settings main window.

Step 2: List Current Firewall Rules

Reviewed system default inbound rules already installed on the system.



Screenshot 2: Default inbound rules list.

Step 3: Block Inbound Traffic to Port 23 (Telnet)

Added a new inbound rule:

Type: Port

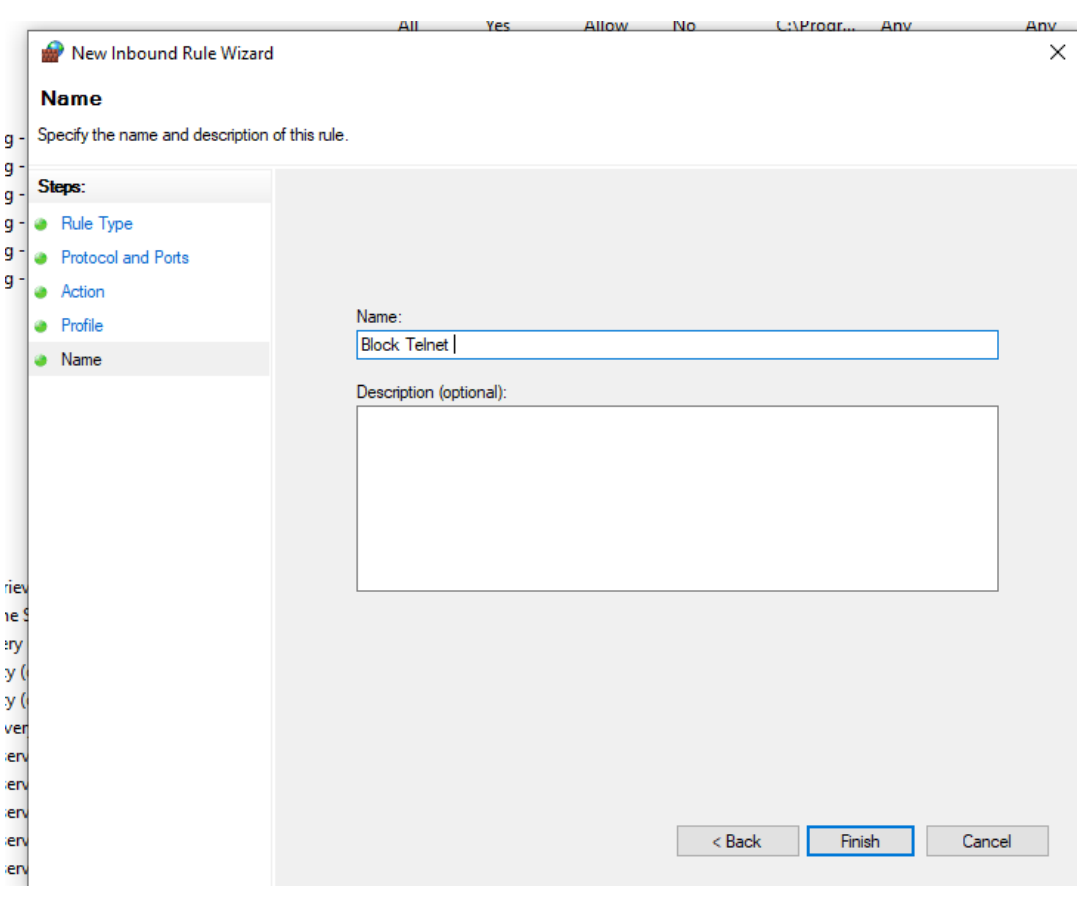
Protocol: TCP

Port: 23

Action: Block the connection

Profile: Domain, Private, Public

Name: "Block Telnet"



Screenshot 3: Port 23 blocking rule added.

Step 4: Add Rule to Allow SSH (Port 22)

Added another inbound rule:

Type: Port

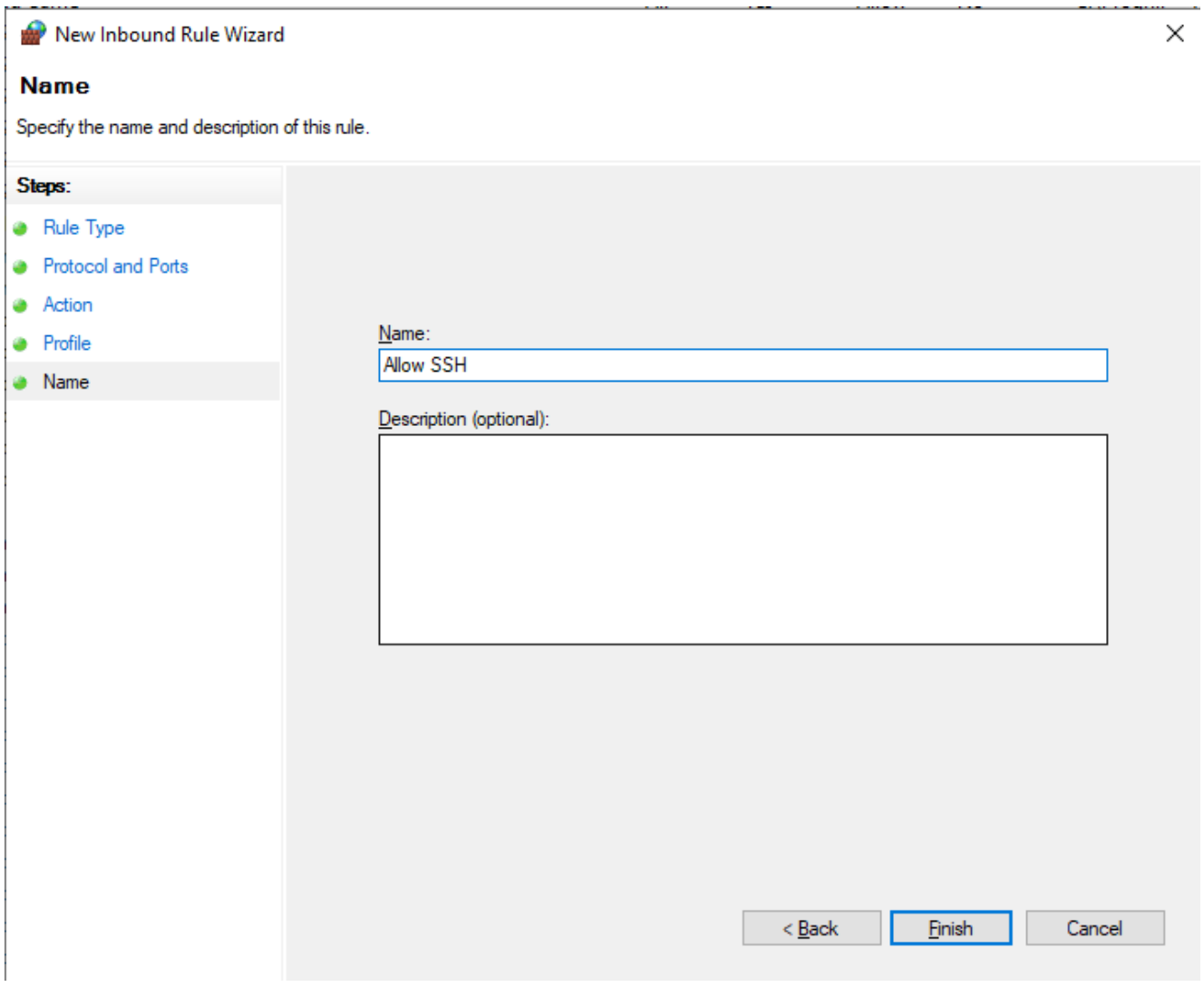
Protocol: TCP

Port: 22

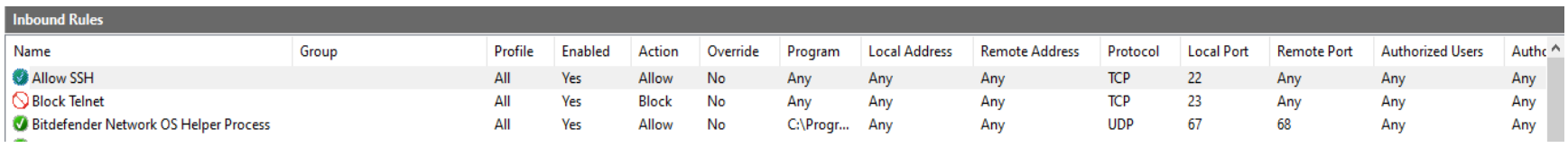
Action: Allow the connection

Profile: Domain, Private, Public

Name: "Allow SSH"



Screenshot 4: New rule for port 22 added.



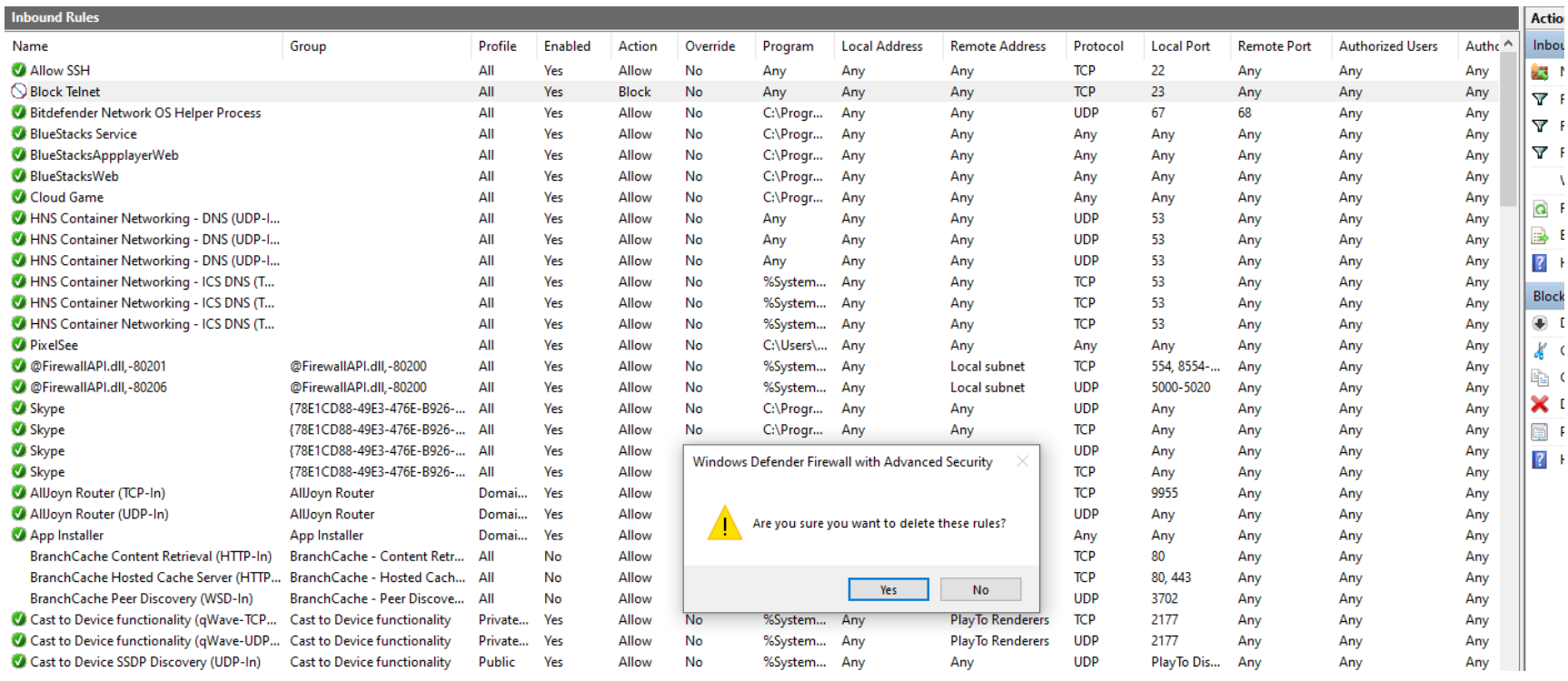
Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authc
Allow SSH		All	Yes	Allow	No	Any	Any	Any	TCP	22	Any	Any	Any
Block Telnet		All	Yes	Block	No	Any	Any	Any	TCP	23	Any	Any	Any
Bitdefender Network OS Helper Process		All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	67	68	Any	Any

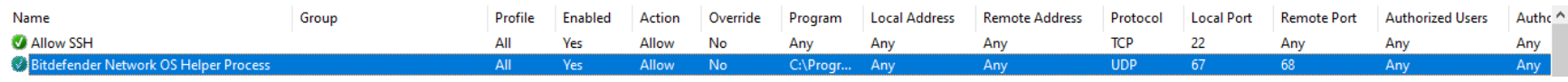
Screenshot 5: Rules list showing both Telnet block and SSH allow

Step 5: Delete the Telnet Rule

Deleted the previously made "Block Telnet" rule to return original state of firewall.



Screenshot 6: Confirmation of rule deletion.



Screenshot 7: after deletion of telnet rule.

Summary

This activity taught me how to set up inbound traffic rules in the Windows Firewall with GUI tools. I blocked Telnet, which is insecure and obsolete, and opened SSH, a secure remote access protocol. These rules were added successfully, confirmed, and then reset to the original system configuration.