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

Intern Name: Jainam Priteshkumar Shah

Date: 08/08/2025

Internship Provider: Elevate Labs

## 1. Objective

The objective of this task was to learn how to configure and test basic firewall rules on my Windows PC. This involved using the Windows Defender Firewall to create rules to explicitly block and allow traffic on specific ports, and understanding the process of testing those rules.

## 2. Tools Used

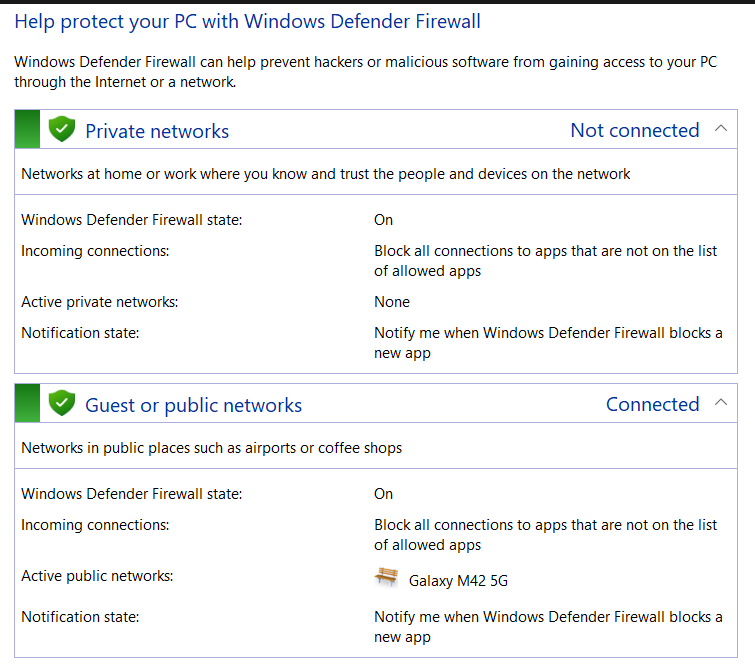
* **Windows Defender Firewall with Advanced Security:** The built-in host firewall for the Windows operating system.
* **PowerShell/Command Prompt:** Used to test the firewall rules.

## 3. Procedural Steps

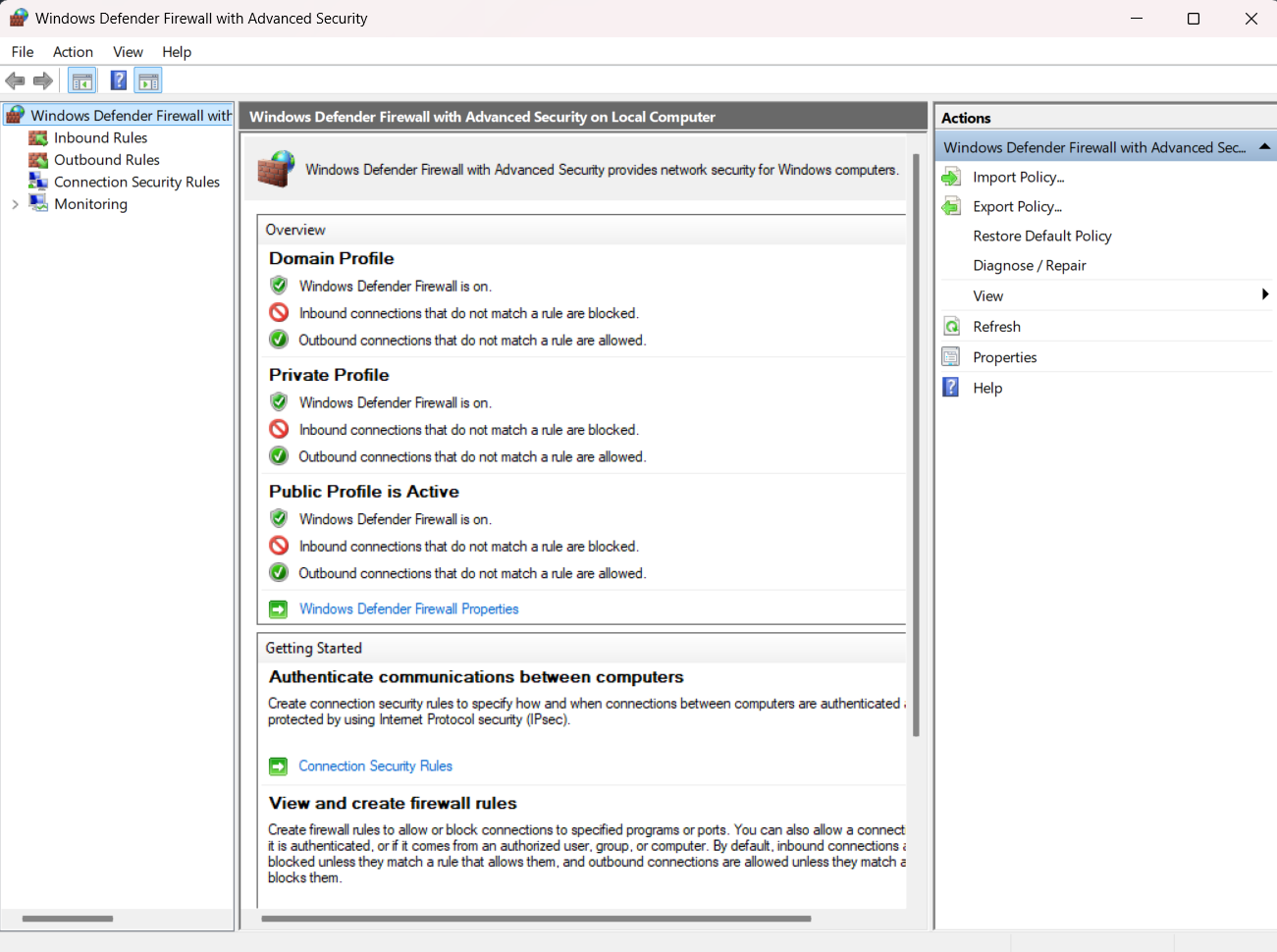
This section details the process I followed to configure and test the firewall rules.

### 3.1. Opening the Firewall Configuration Tool

First, I opened the "Windows Defender Firewall with Advanced Security" application. I did this by searching for it in the Windows Start Menu. This tool provides granular control over inbound and outbound network traffic.



4.1 Windows Defender Firewall

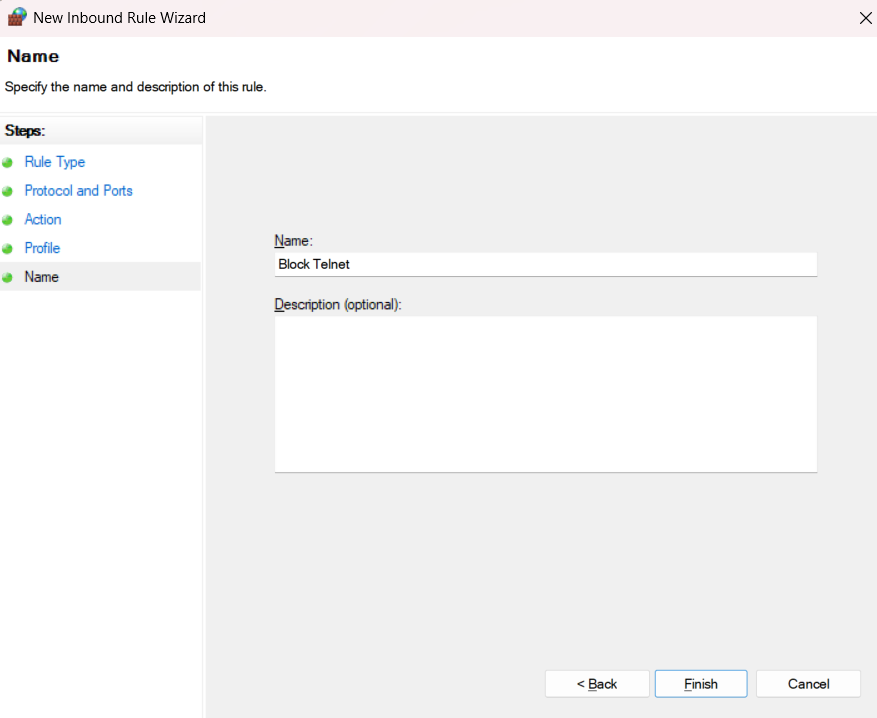


4.2 Advance Security

### 3.2. Creating a Rule to Block Inbound Traffic

My first action was to create a rule to block inbound traffic on a specific port, as per the task instructions. I chose to block **TCP port 23**, which is used by the insecure Telnet protocol.

1. In the firewall tool, I selected **Inbound Rules** and clicked **New Rule...**.
2. I chose the **Port** rule type.
3. I specified **TCP** and port **23**.
4. I selected the action **Block the connection**.
5. I applied the rule to all profiles (Domain, Private, Public).
6. I named the rule "Block Telnet".



4.3 Inbound Rule Creation

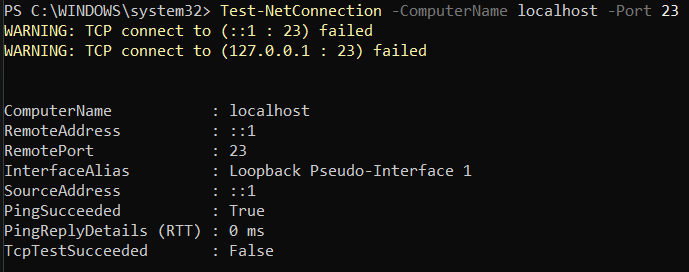


4.4 Created Rule

### 3.3. Testing the Block Rule

To verify the rule was working, I attempted to test the connection to port 23. While I don't have a Telnet server running, I used a PowerShell command to simulate a connection attempt:

**Test-NetConnection -ComputerName localhost -Port 23**

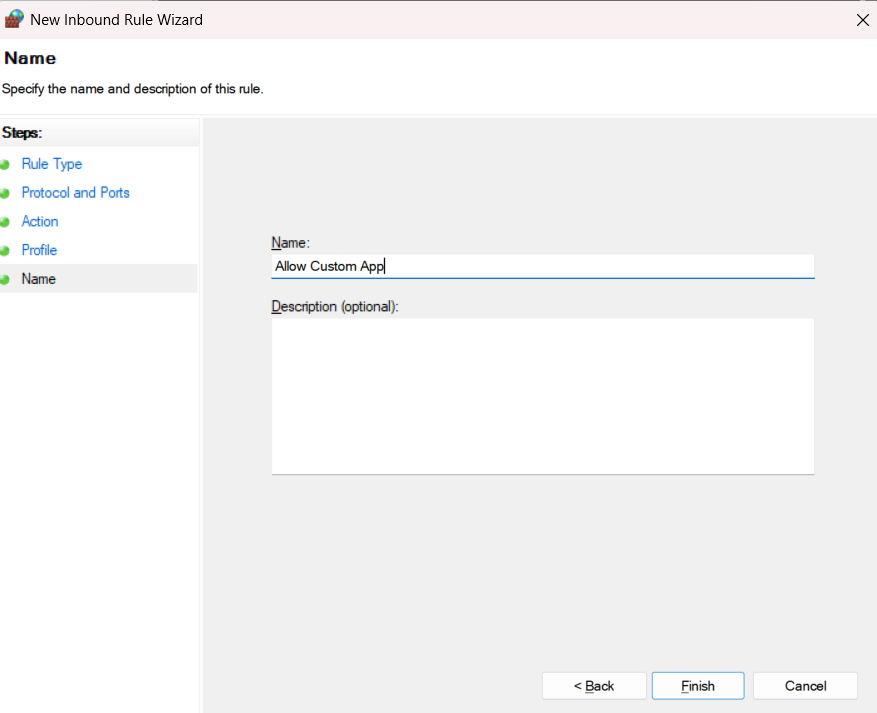


4.5 Command Output

### 3.4. Creating a Rule to Allow Inbound Traffic

Next, I created a rule to explicitly allow traffic. For this example, I created a rule to allow inbound traffic on a custom port, **TCP port 8088**.

1. I again selected **Inbound Rules** and clicked **New Rule...**.
2. I chose the **Port** rule type.
3. I specified **TCP** and port **8088**.
4. I selected the action **Allow the connection**.
5. I applied the rule to all profiles.
6. I named the rule "Allow Custom App".



4.6 Inbound Rule Creation

### 3.5. Removing the Test Block Rule

Finally, to restore my computer to its original state, I removed the temporary block rule. I located my "Block Telnet" rule in the list of Inbound Rules, right-clicked it, and selected **Delete**.

