# 🛡️ Task 4 Report: Setup and Use a Firewall on Windows

## Objective:

To configure and test basic firewall rules to allow or block specific network traffic using the built-in Windows Defender Firewall with Advanced Security.

## Platform Used:

Windows 11  
Firewall Tool: Windows Defender Firewall (GUI-based interface)

## 📝 Step-by-Step Procedure:

### 1. Open Windows Firewall Settings:

Navigated to:  
Control Panel → System and Security → Windows Defender Firewall  
Clicked on 'Advanced Settings' from the left panel to access advanced rule configuration.

### 2. View Current Firewall Rules:

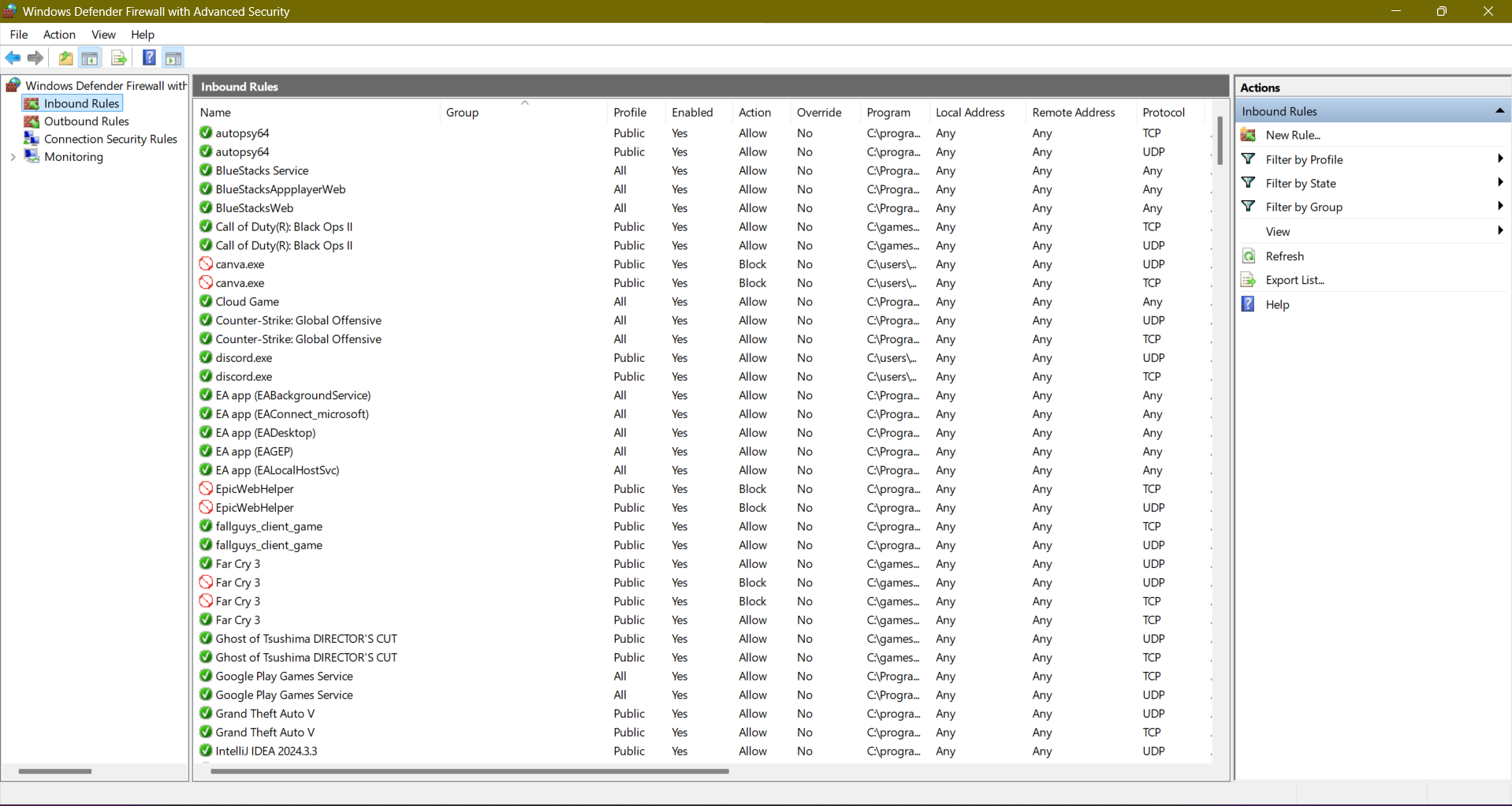
Selected 'Inbound Rules' to view existing traffic rules.  
Observed default rules for applications and system services.

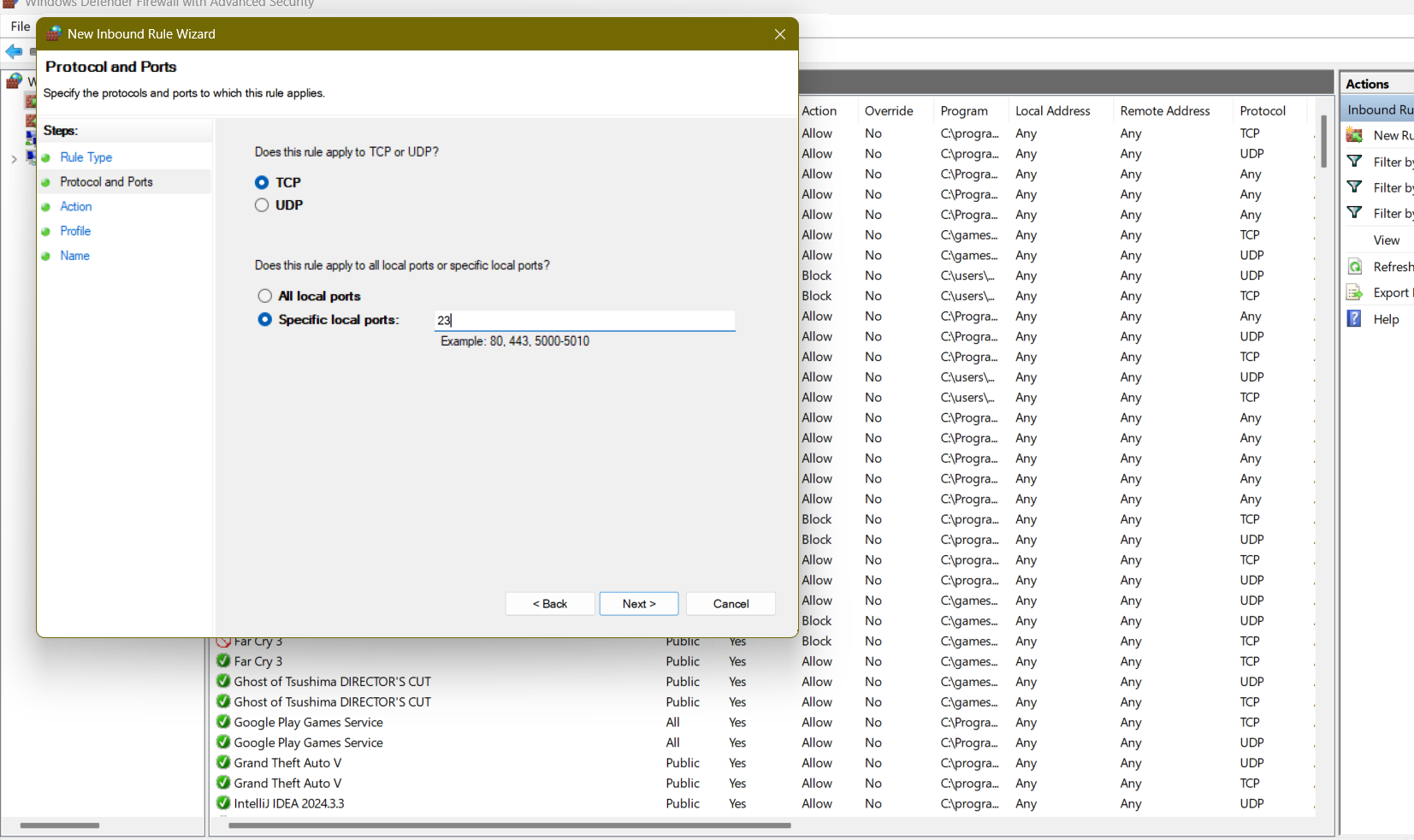
### 3. Create Rule to Block Inbound Traffic on Port 23 (Telnet):

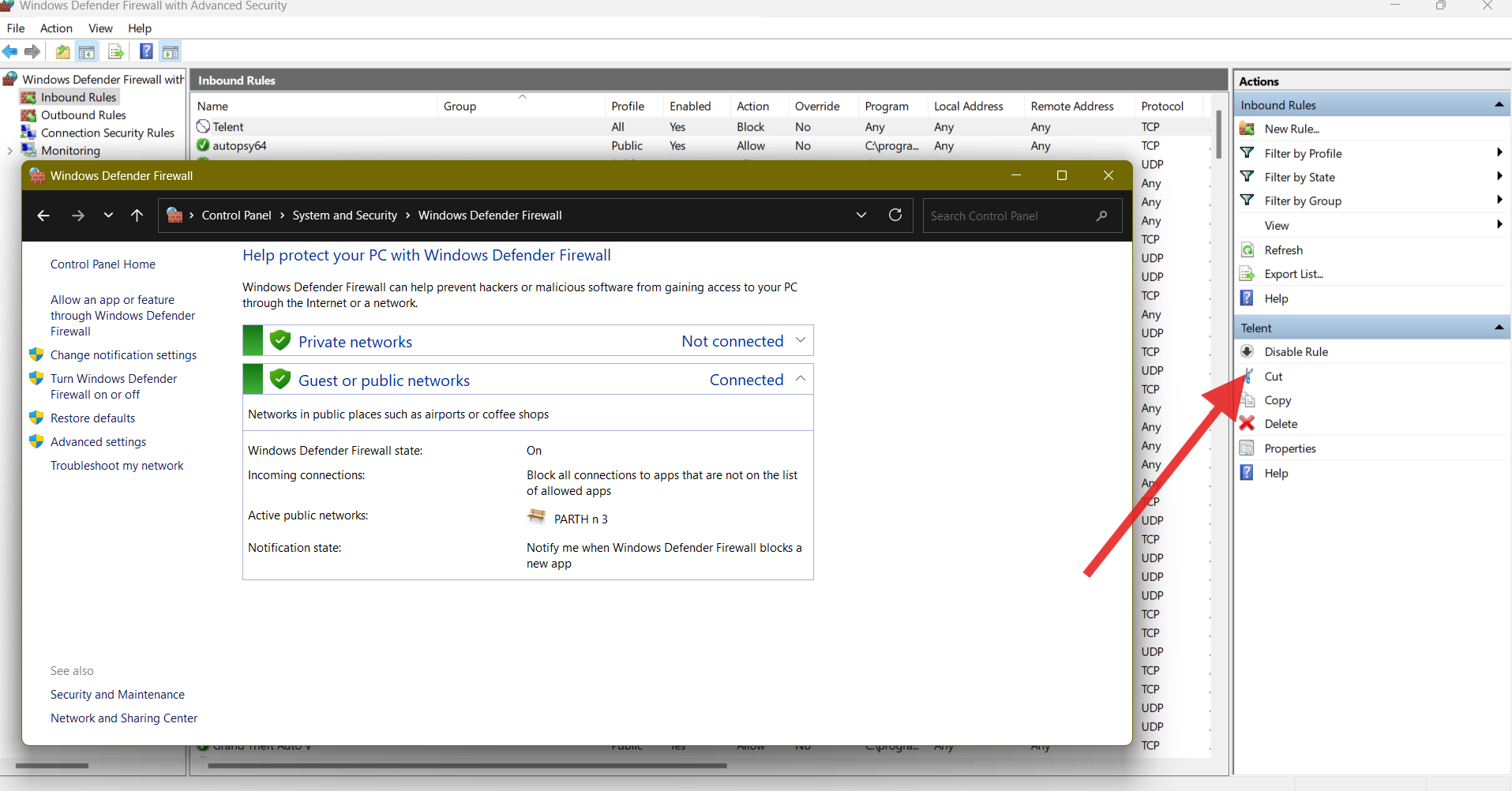
• Clicked 'New Rule' in Inbound Rules.  
• Selected 'Port' as the rule type.  
• Chose 'TCP', specified port 23.  
• Action: Block the connection.  
• Applied rule to: Domain, Private, Public.  
• Gave it a name: Telnet.  
  
📝 Purpose:  
Port 23 is used by the insecure Telnet protocol. Blocking it prevents potential unauthorized access.

### 4. Test the Block Rule:

Opened Command Prompt and attempted to connect using:  
telnet localhost 23  
  
🧪 Result:  
Connection failed as expected, confirming the rule is active and working.







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

Returned to 'Inbound Rules'.  
Located the rule named 'Block Telnet'.  
Right-clicked → Delete.

## Outcome:

Successfully demonstrated:  
- Creating custom rules to block and allow traffic.  
- Testing and verifying firewall behavior.  
- Restoring firewall to its original state after testing.