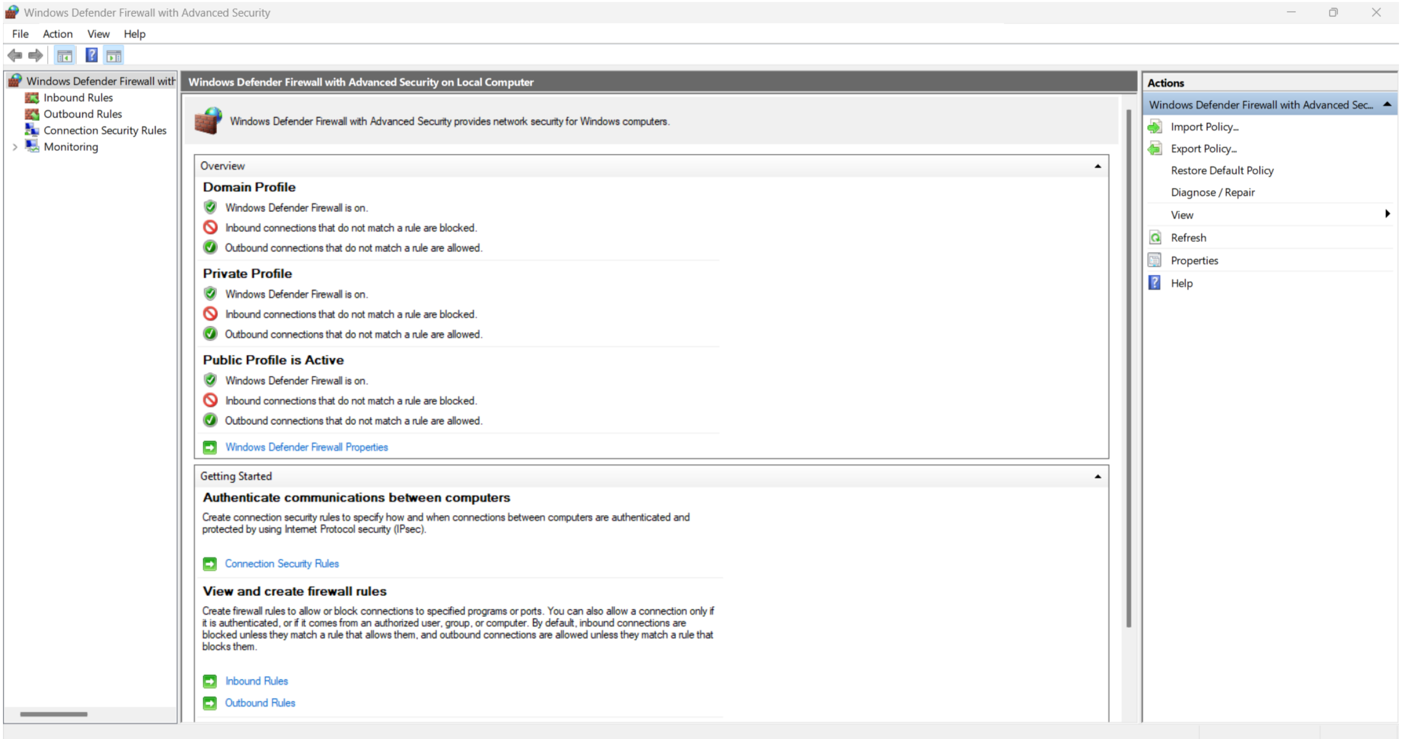
Task 4 : Setup and Use a Firewall on Windows/Linux

Objective: Configure and test basic firewall rules to allow or block traffic.

Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

Deliverables: Screenshot/configuration file showing firewall rules applied.

Windows firewall



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

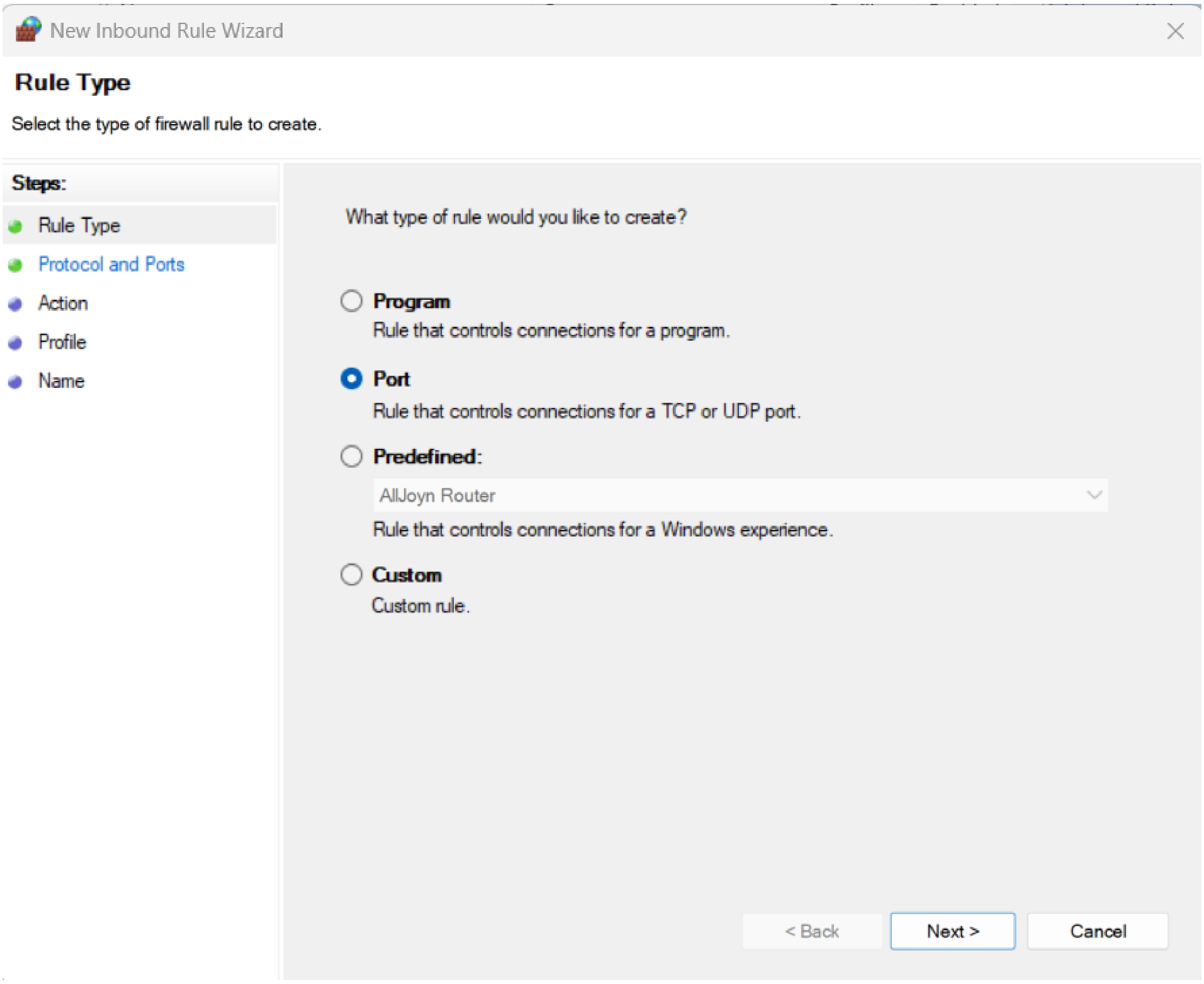
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

Outbound Rules

Steps to create a firewall rule (GUI Steps)



Rule Type

Select the type of firewall rule to create.

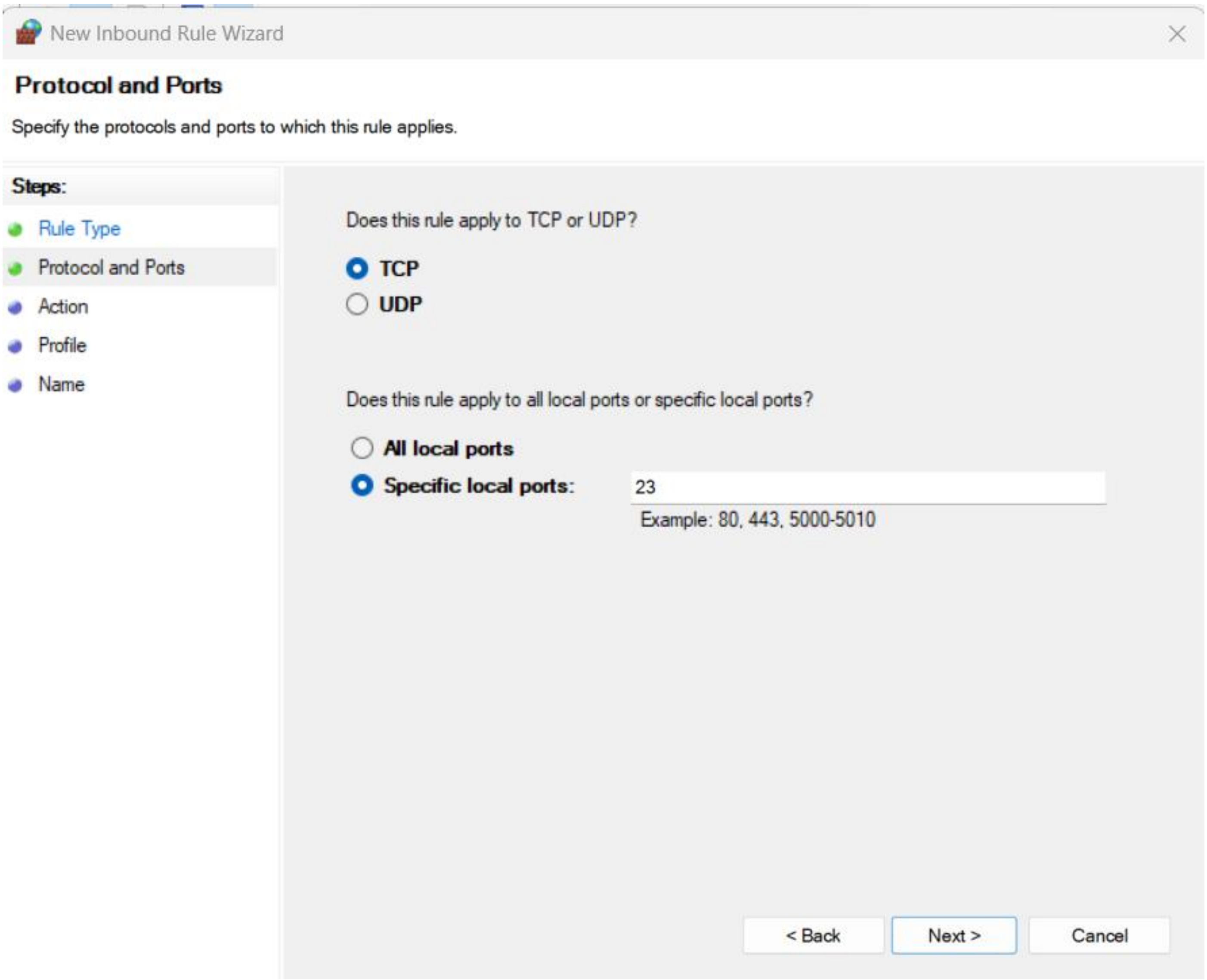
What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

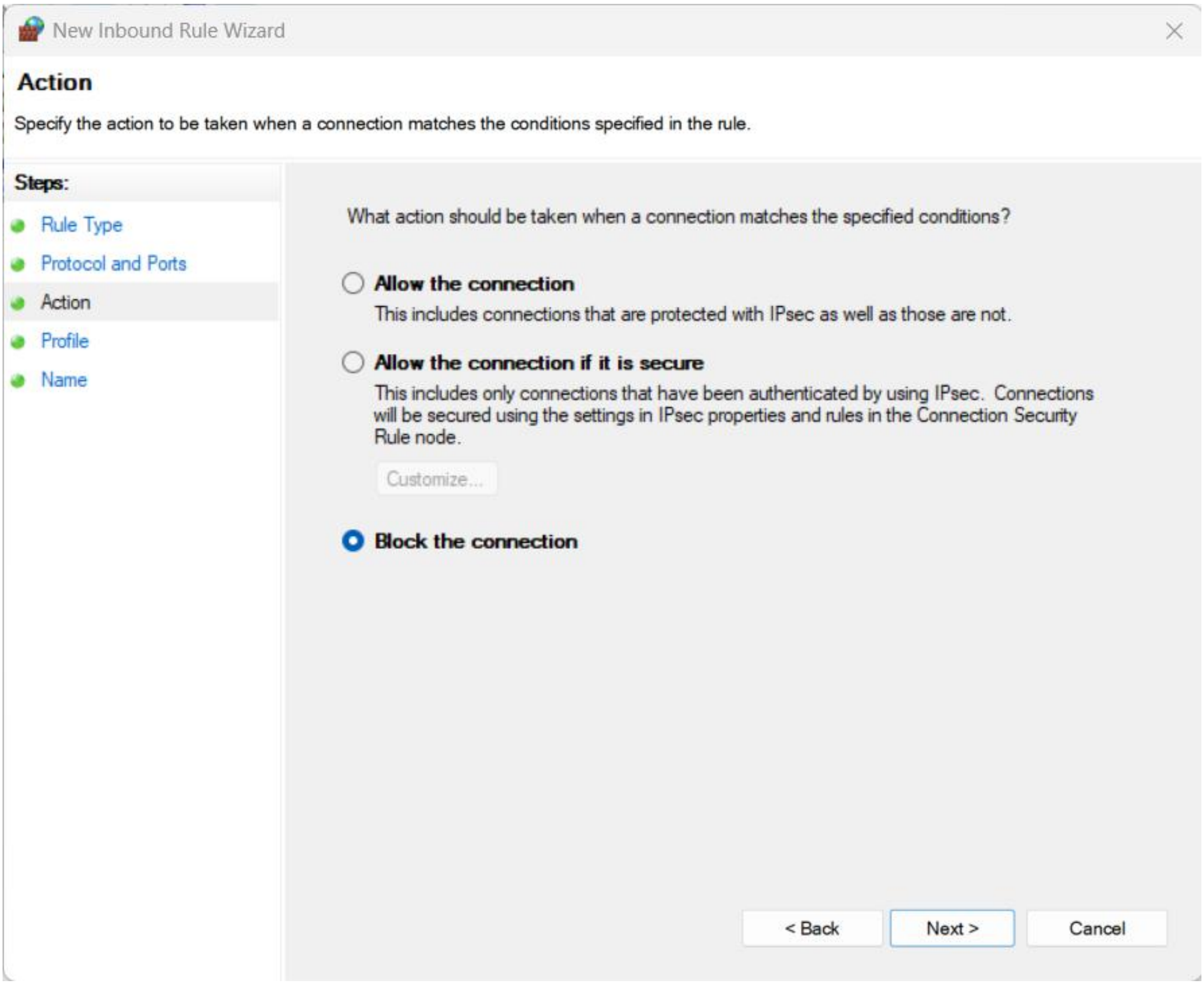
Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 23

Example: 80, 443, 5000-5010



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

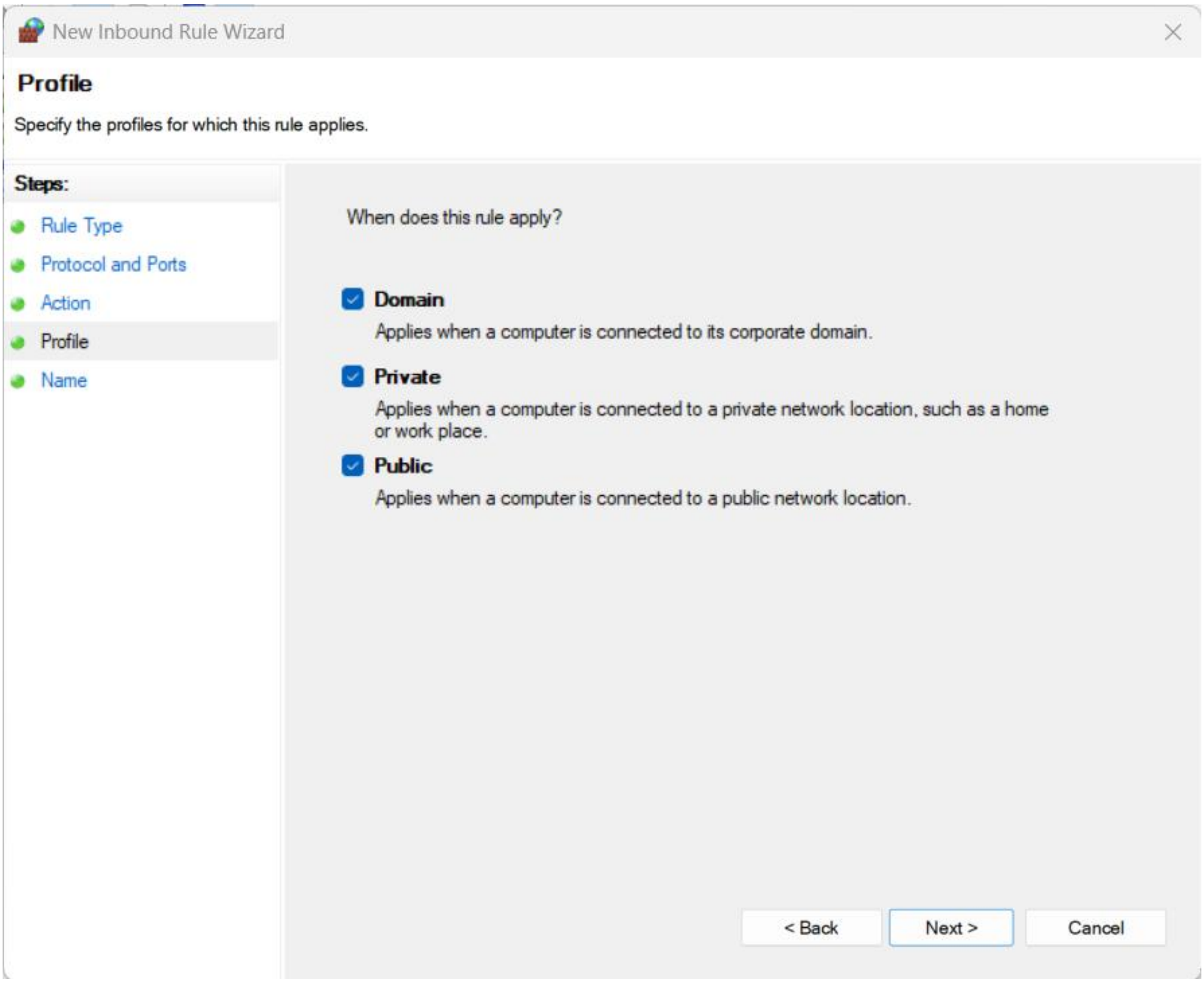
○ **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**



Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

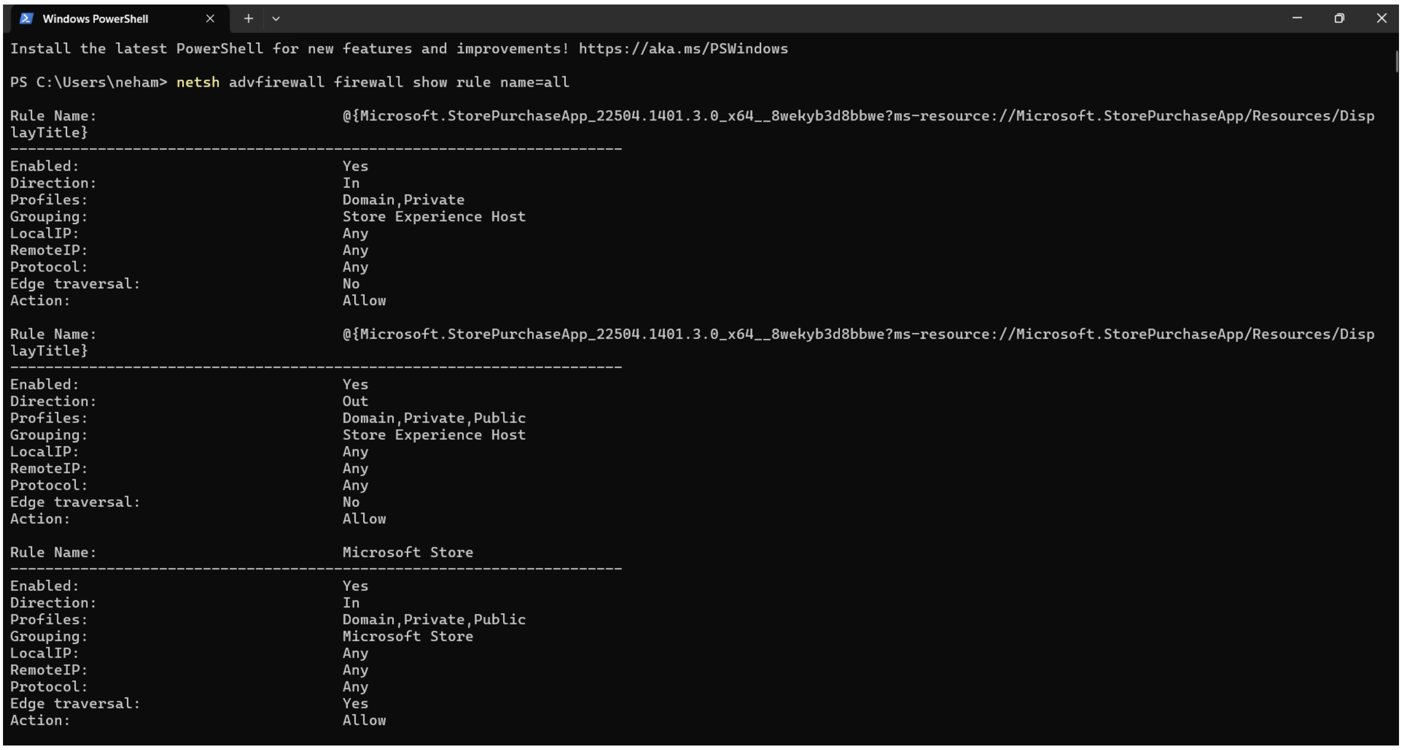
☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

Listing the firewall currently employed into my machine

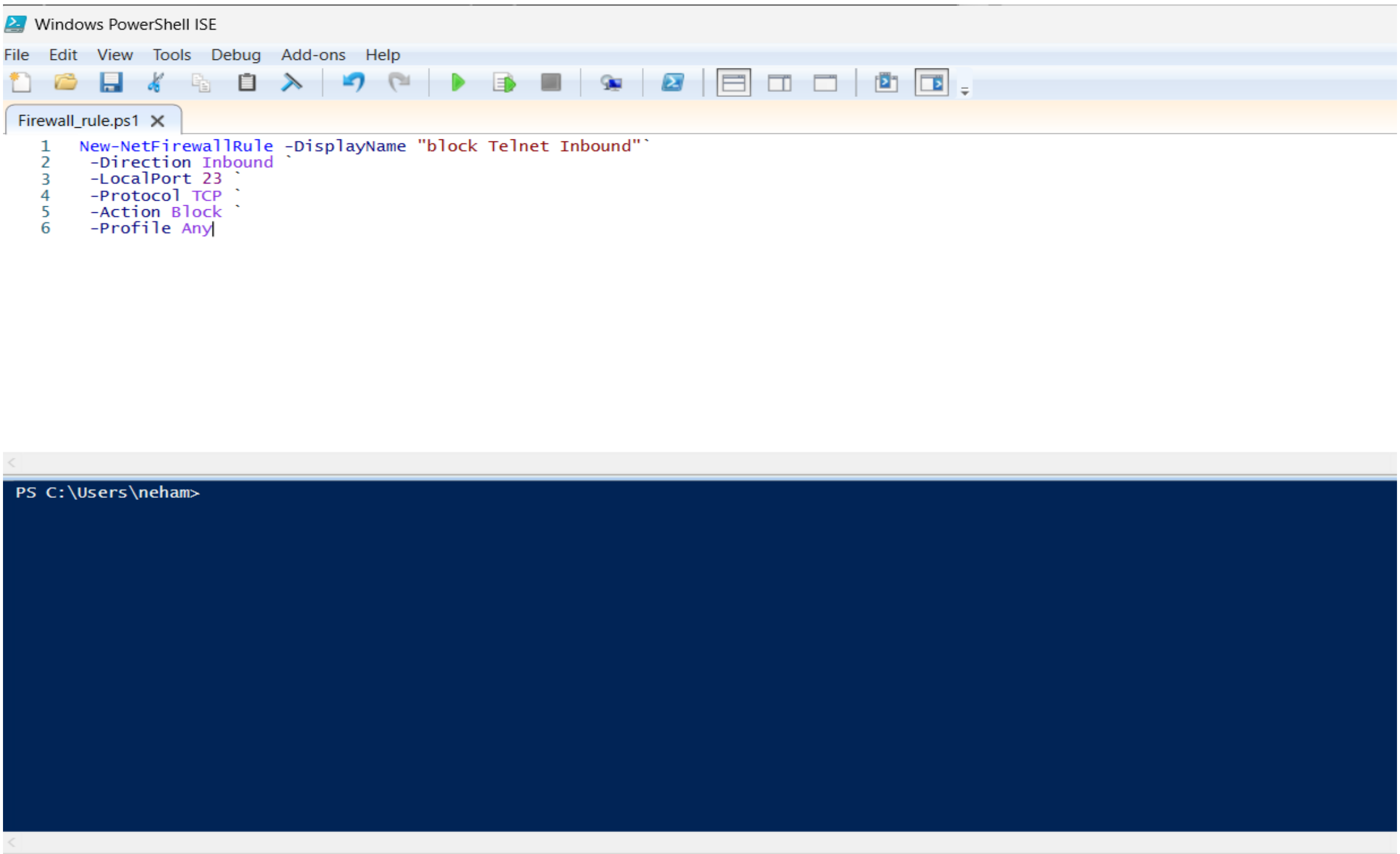
I am using PowerShell to list all the firewall rules.

The command I use is: **netsh advfirewall firewall show rule name=all**



```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\neham> netsh advfirewall firewall show rule name=all

Rule Name:                            @{Microsoft.StorePurchaseApp_22504.1401.3.0_x64__8wekyb3d8bbwe?ms-resource://Microsoft.StorePurchaseApp/Resources/Disp
layTitle}
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private
Grouping:                             Store Experience Host
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            @{Microsoft.StorePurchaseApp_22504.1401.3.0_x64__8wekyb3d8bbwe?ms-resource://Microsoft.StorePurchaseApp/Resources/Disp
layTitle}
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:                             Store Experience Host
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            Microsoft Store
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:                             Microsoft Store
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             Any
Edge traversal:                       Yes
Action:                               Allow
```

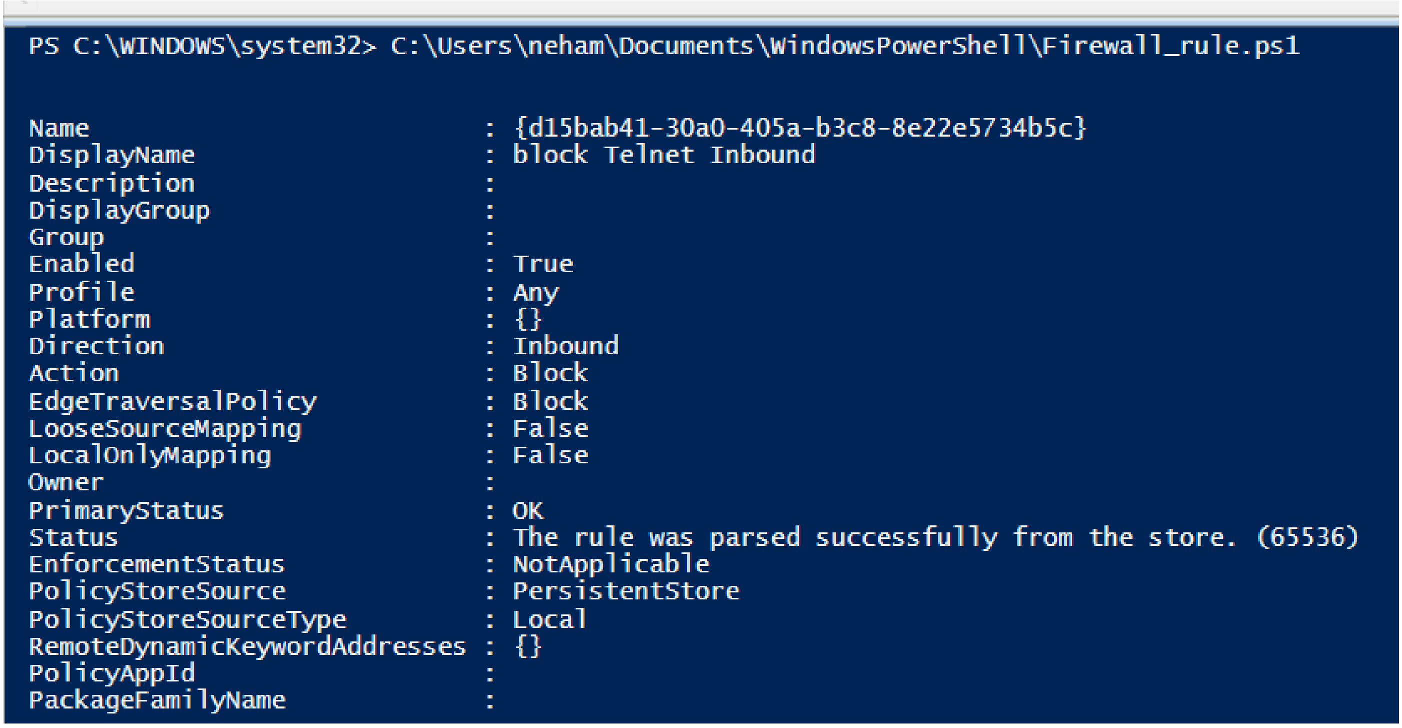
Here, I am writing a PowerShell script to automate setting firewall rules, specifically to block the Telnet port.



```
New-NetFirewallRule -DisplayName "block Telnet Inbound"`
 -Direction Inbound `
 -LocalPort 23 `
 -Protocol TCP `
 -Action Block `
 -Profile Any
```

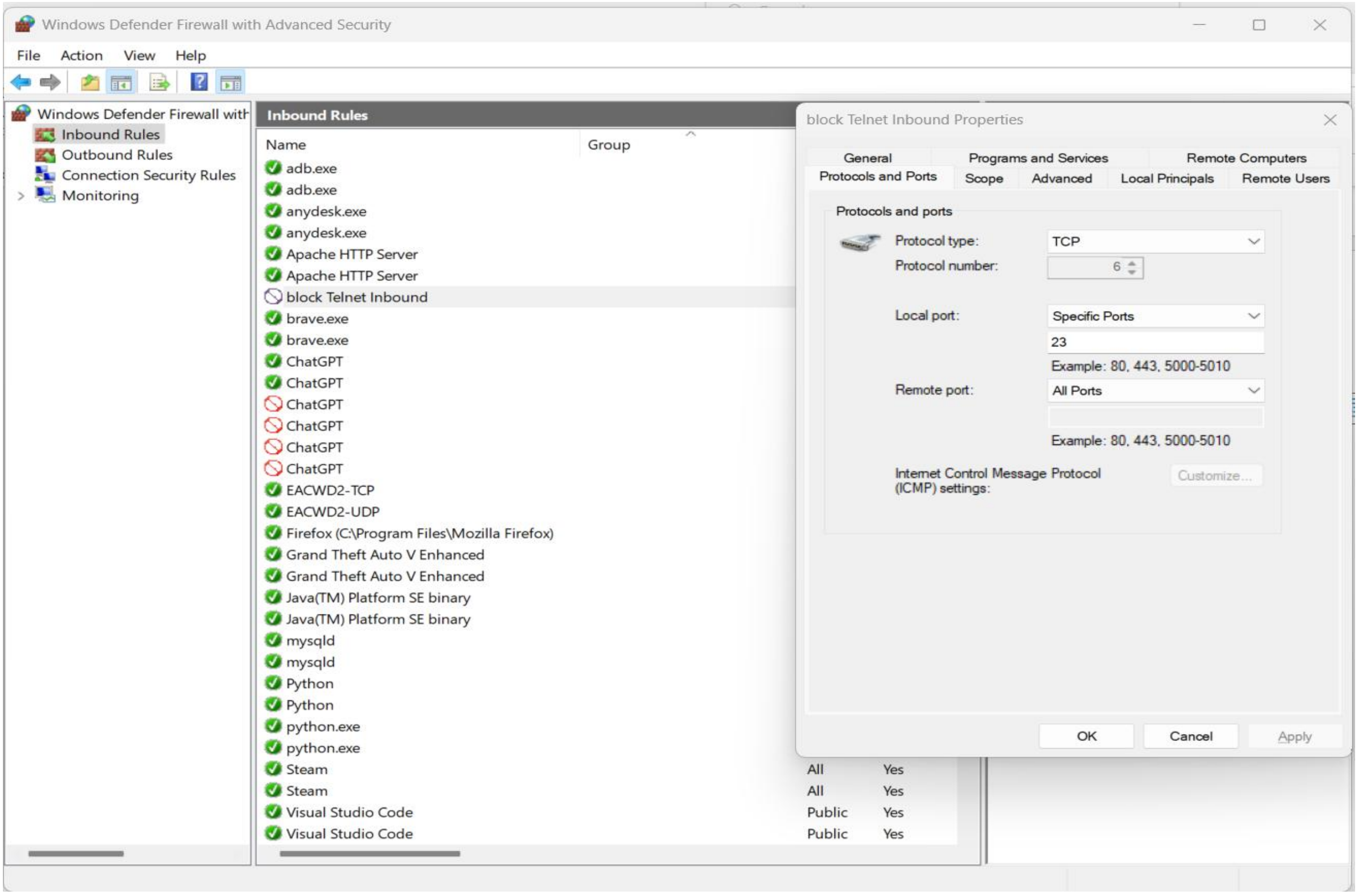
```
PS C:\Users\neham>
```

As shown, a firewall rule named 'Block Telnet Inbound' exists for all profiles on the Windows machine.



```
PS C:\WINDOWS\system32> C:\Users\neham\Documents\WindowsPowerShell\Firewall_rule.ps1


Name                          : {d15bab41-30a0-405a-b3c8-8e22e5734b5c}
DisplayName                   : block Telnet Inbound
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :
```

The rule is visible in the Windows Defender Firewall



Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Inbound Rules

Name	Group		
adb.exe			
adb.exe			
anydesk.exe			
anydesk.exe			
Apache HTTP Server			
Apache HTTP Server			
block Telnet Inbound			
brave.exe			
brave.exe			
ChatGPT			
ChatGPT			
ChatGPT			
ChatGPT			
ChatGPT			
ChatGPT			
EACWD2-TCP			
EACWD2-UDP			
Firefox (C:\Program Files\Mozilla Firefox)			
Grand Theft Auto V Enhanced			
Grand Theft Auto V Enhanced			
Java(TM) Platform SE binary			
Java(TM) Platform SE binary			
mysqld			
mysqld			
Python			
Python			
python.exe			
python.exe			
Steam		All	Yes
Steam		All	Yes
Visual Studio Code		Public	Yes
Visual Studio Code		Public	Yes

block Telnet Inbound Properties

Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: Specific Ports

23

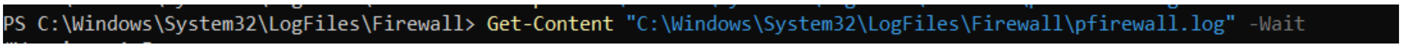
Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

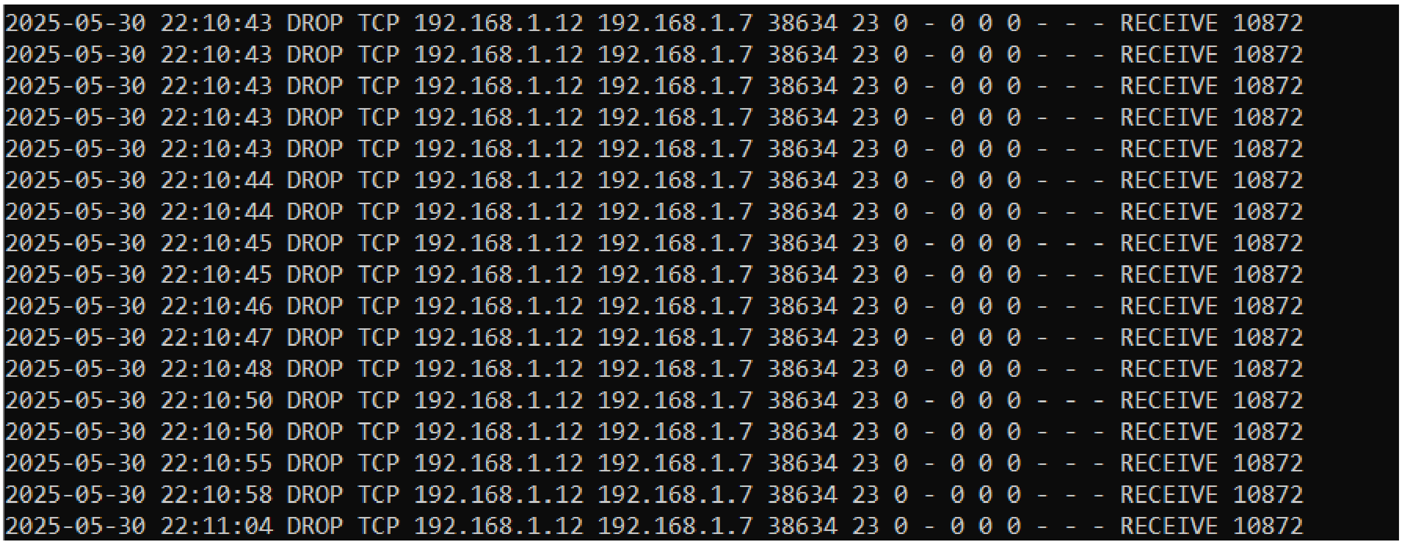
Internet Control Message Protocol (ICMP) settings:

Commands used to view the firewall logs in the Powershell



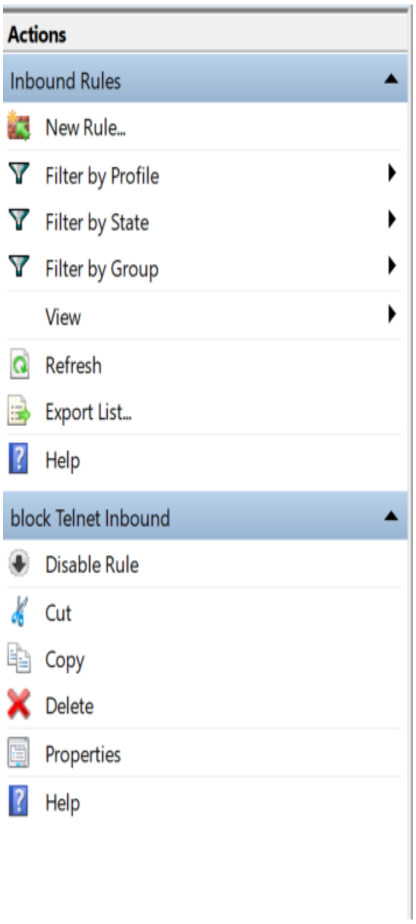
```
PS C:\Windows\System32\LogFiles\Firewall> Get-Content "C:\Windows\System32\LogFiles\Firewall\pfirewall.log" -Wait
```

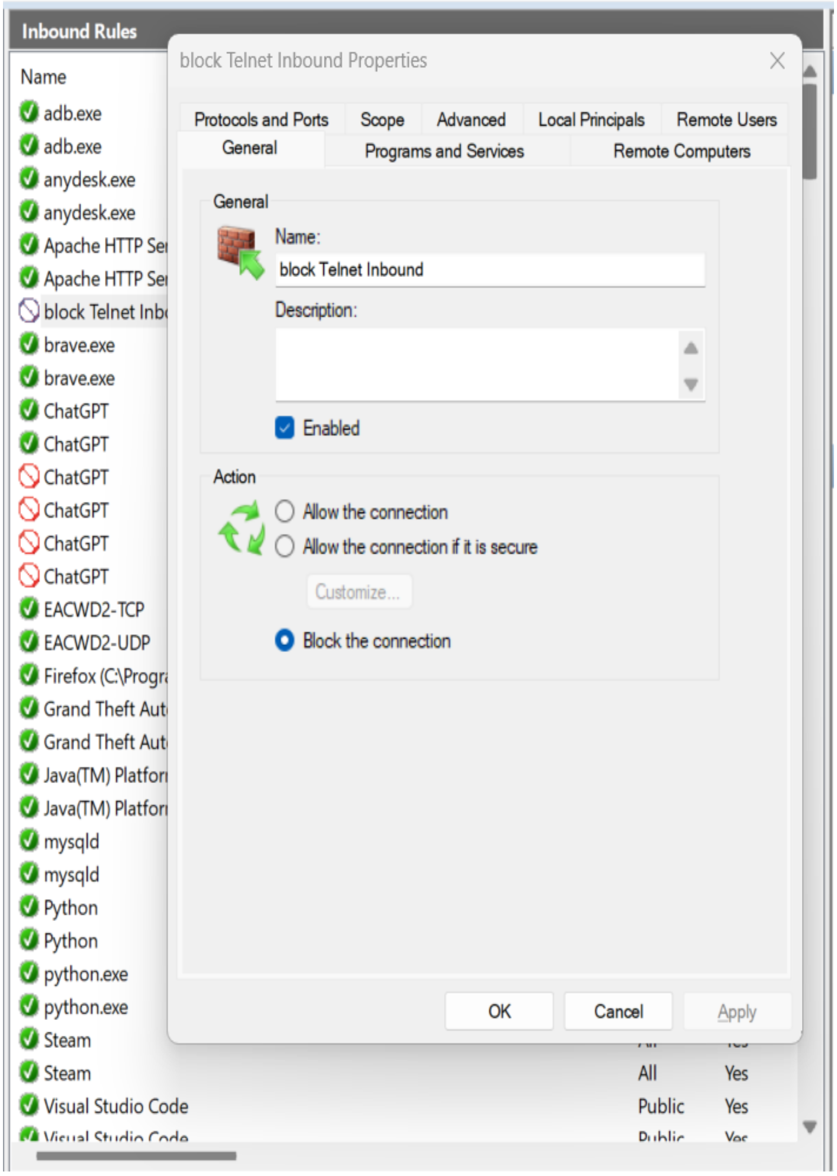
These logs show that attempts to connect to the Telnet service are being blocked by the firewall.



```
2025-05-30 22:10:43 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:43 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:43 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:43 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:43 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:44 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:44 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:45 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:45 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:46 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:47 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:48 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:50 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:50 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:55 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:10:58 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
2025-05-30 22:11:04 DROP TCP 192.168.1.12 192.168.1.7 38634 23 0 - 0 0 0 - - - RECEIVE 10872
```

To allow the connection, revert the firewall rule by opening its properties and enabling the connection.





Name: adb.exe, adb.exe, anydesk.exe, anydesk.exe, Apache HTTP Se, Apache HTTP Se, block Telnet Inb, brave.exe, brave.exe, ChatGPT, ChatGPT, ChatGPT, ChatGPT, ChatGPT, ChatGPT, EACWD2-TCP, EACWD2-UDP, Firefox (C:\Progr, Grand Theft Aut, Grand Theft Aut, Java(TM) Platfor, Java(TM) Platfor, mysqld, mysqld, Python, Python, python.exe, python.exe, Steam, Steam All Yes, Visual Studio Code Public Yes, Visual Studio Code Public Yes

block Telnet Inbound Properties

General

Name: block Telnet Inbound

Description:

☑ Enabled

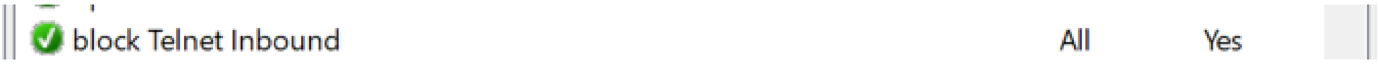
Action

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

The firewall is now allowing connections to the Telnet port.



block Telnet Inbound	All	Yes