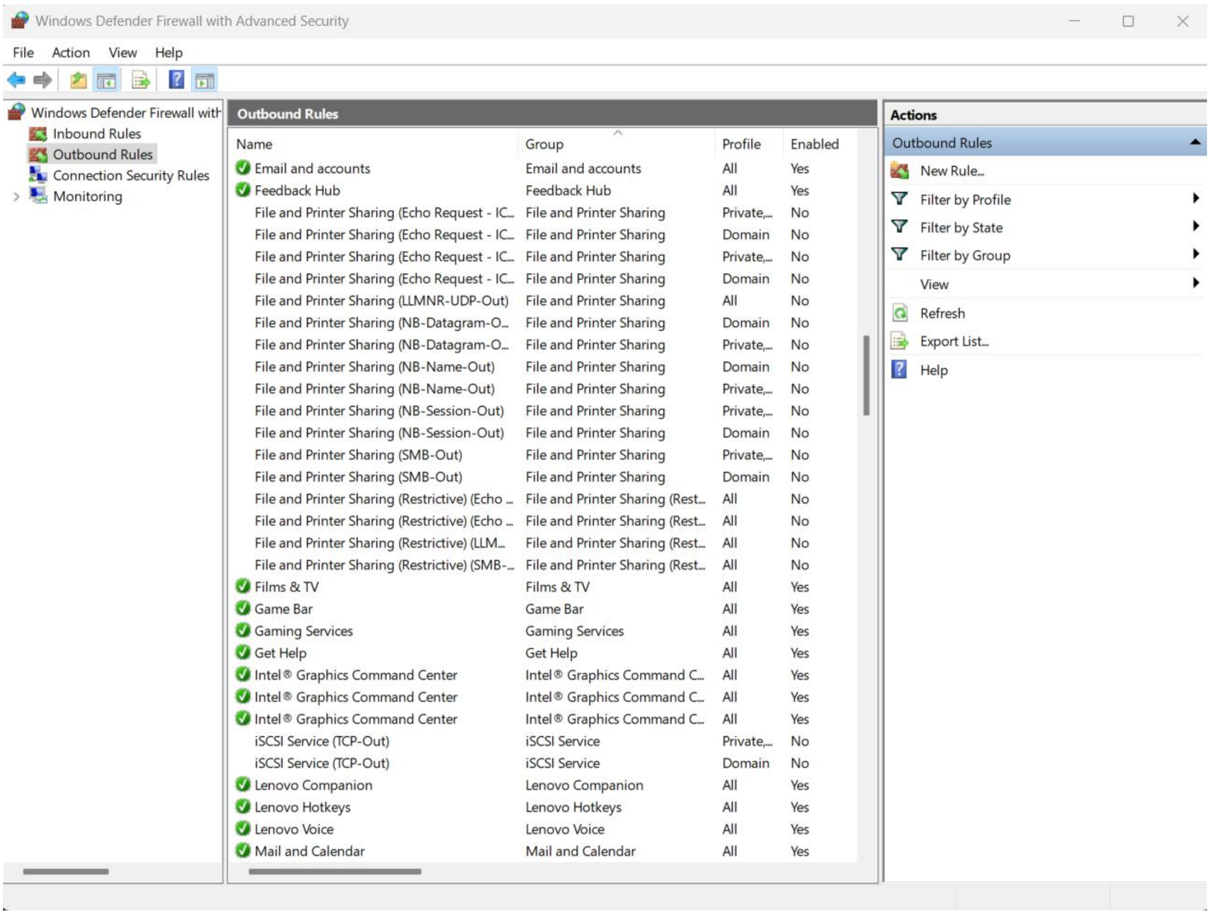
Windows Firewall Configuration and Testing
Task 4

Soumil Gupta

1. Open Windows Firewall with Advanced Security

   1. Press Win + R to open Run dialog
   2. Type wf.msc and press Enter
   3. Windows Firewall with Advanced Security console will open



Outbound Rules

Name	Group	Profile	Enabled
✓ Email and accounts	Email and accounts	All	Yes
✓ Feedback Hub	Feedback Hub	All	Yes
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	Private,...	No
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	Private,...	No
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	Domain	No
File and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Datagram-O...	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Datagram-O...	File and Printer Sharing	Private,...	No
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Private,...	No
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Private,...	No
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-Out)	File and Printer Sharing	Private,...	No
File and Printer Sharing (SMB-Out)	File and Printer Sharing	Domain	No
File and Printer Sharing (Restrictive) (Echo ...	File and Printer Sharing (Rest...	All	No
File and Printer Sharing (Restrictive) (Echo ...	File and Printer Sharing (Rest...	All	No
File and Printer Sharing (Restrictive) (LLM...	File and Printer Sharing (Rest...	All	No
File and Printer Sharing (Restrictive) (SMB-...	File and Printer Sharing (Rest...	All	No
✓ Films & TV	Films & TV	All	Yes
✓ Game Bar	Game Bar	All	Yes
✓ Gaming Services	Gaming Services	All	Yes
✓ Get Help	Get Help	All	Yes
✓ Intel® Graphics Command Center	Intel® Graphics Command C...	All	Yes
✓ Intel® Graphics Command Center	Intel® Graphics Command C...	All	Yes
✓ Intel® Graphics Command Center	Intel® Graphics Command C...	All	Yes
iSCSI Service (TCP-Out)	iSCSI Service	Private,...	No
iSCSI Service (TCP-Out)	iSCSI Service	Domain	No
✓ Lenovo Companion	Lenovo Companion	All	Yes
✓ Lenovo Hotkeys	Lenovo Hotkeys	All	Yes
✓ Lenovo Voice	Lenovo Voice	All	Yes
✓ Mail and Calendar	Mail and Calendar	All	Yes

Step 2: Alternative Access Methods

- Through Control Panel: Control Panel → System and Security → Windows Defender Firewall → Advanced settings
- Through Settings: Settings → Network & Internet → Windows Firewall → Advanced settings

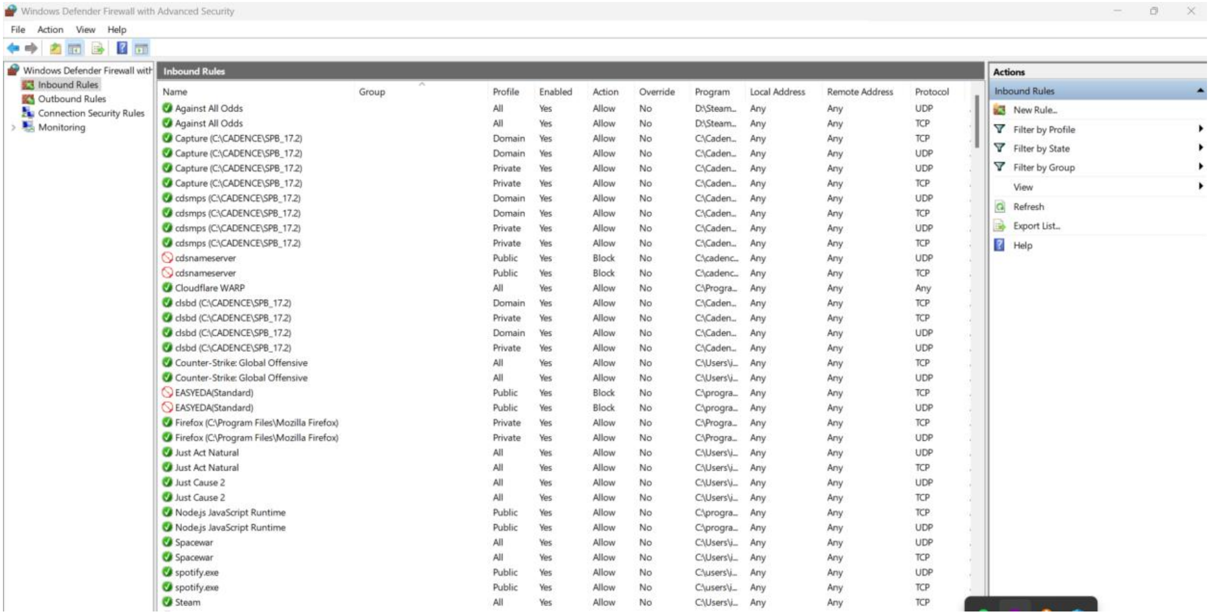
---

2. Listing Current Firewall Rules

GUI Method

Step 1: View Inbound Rules

1. In the left pane, click on "Inbound Rules"
2. Review the list of current inbound rules
3. Note the enabled/disabled status and actions (Allow/Block)

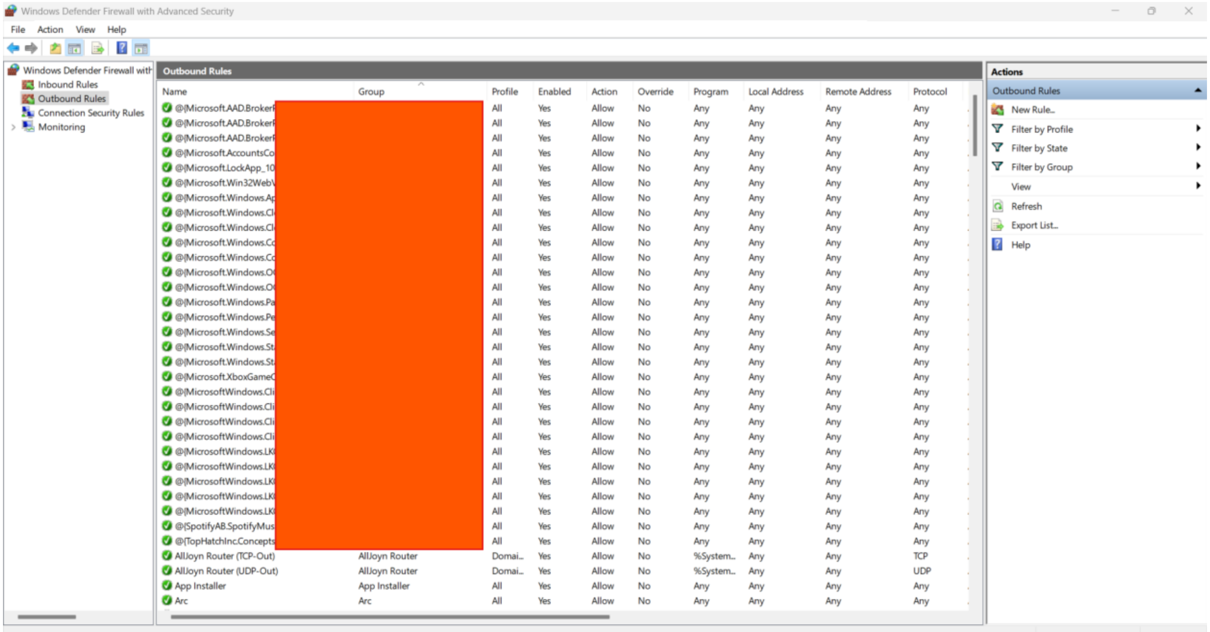


Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
✓ Against All Odds		All	Yes	Allow	No	D:\Steam…	Any	Any	UDP
✓ Against All Odds		All	Yes	Allow	No	D:\Steam…	Any	Any	TCP
✓ Capture (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden…	Any	Any	TCP
✓ Capture (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden…	Any	Any	UDP
✓ Capture (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden…	Any	Any	UDP
✓ Capture (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden…	Any	Any	TCP
✓ cdsmps (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden…	Any	Any	UDP
✓ cdsmps (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden…	Any	Any	TCP
✓ cdsmps (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden…	Any	Any	UDP
✓ cdsmps (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden…	Any	Any	TCP
⊘ cdsnameserver		Public	Yes	Block	No	C:\cadenc…	Any	Any	UDP
⊘ cdsnameserver		Public	Yes	Block	No	C:\cadenc…	Any	Any	TCP
✓ Cloudflare WARP		All	Yes	Allow	No	C:\Progra…	Any	Any	Any
✓ clsbd (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden…	Any	Any	TCP
✓ clsbd (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden…	Any	Any	TCP
✓ clsbd (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden…	Any	Any	UDP
✓ clsbd (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden…	Any	Any	UDP
✓ Counter-Strike: Global Offensive		All	Yes	Allow	No	C:\Users\i…	Any	Any	TCP
✓ Counter-Strike: Global Offensive		All	Yes	Allow	No	C:\Users\i…	Any	Any	UDP
⊘ EASYEDA(Standard)		Public	Yes	Block	No	C:\progra…	Any	Any	TCP
⊘ EASYEDA(Standard)		Public	Yes	Block	No	C:\progra…	Any	Any	UDP
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra…	Any	Any	TCP
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra…	Any	Any	UDP
✓ Just Act Natural		All	Yes	Allow	No	C:\Users\i…	Any	Any	UDP
✓ Just Act Natural		All	Yes	Allow	No	C:\Users\i…	Any	Any	TCP
✓ Just Cause 2		All	Yes	Allow	No	C:\Users\i…	Any	Any	UDP
✓ Just Cause 2		All	Yes	Allow	No	C:\Users\i…	Any	Any	TCP
✓ Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra…	Any	Any	TCP
✓ Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra…	Any	Any	UDP
✓ Spacewar		All	Yes	Allow	No	C:\Users\i…	Any	Any	UDP
✓ Spacewar		All	Yes	Allow	No	C:\Users\i…	Any	Any	TCP
✓ spotify.exe		Public	Yes	Allow	No	C:\users\i…	Any	Any	UDP
✓ spotify.exe		Public	Yes	Allow	No	C:\users\i…	Any	Any	TCP
✓ Steam		All	Yes	Allow	No	C:\Users\i…	Any	Any	TCP

Step 2: View Outbound Rules

1. In the left pane, click on "Outbound Rules"
2. Review the list of current outbound rules



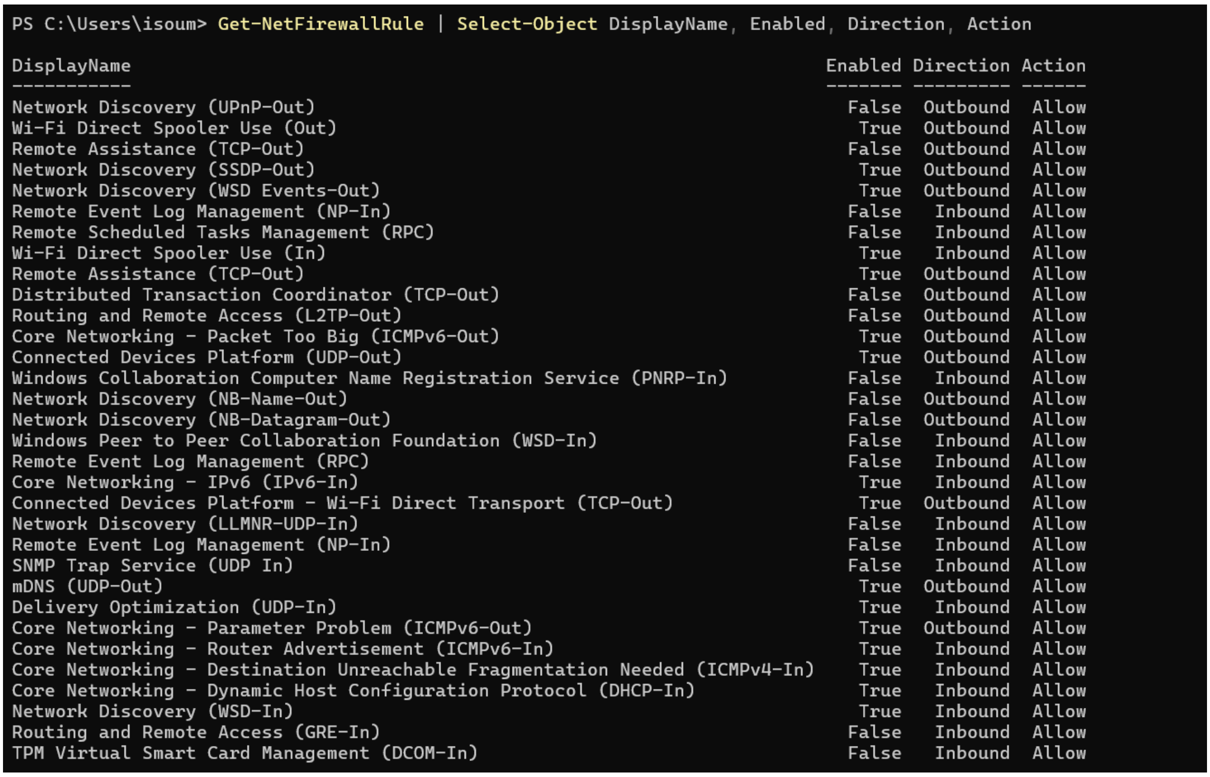
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
@{Microsoft.AAD.Broker [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.AAD.Broker [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.AAD.Broker [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.AccountsCo [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.LockApp_10 [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Win32Web [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.A [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.Cl [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.Cl [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.C [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.C [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.O [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.O [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.Pa [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.Pe [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.Se [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.St [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.St [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.XboxGame [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Cli [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Cli [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Cli [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Cli [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LK [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LK [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LK [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LK [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LK [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{SpotifyAB.SpotifyMus [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
@{TopHatchInc.Concepts [redacted]	[redacted]	All	Yes	Allow	No	Any	Any	Any	Any
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any
Arc	Arc	All	Yes	Allow	No	Any	Any	Any	Any

Command Line Method

PowerShell Commands:

List all firewall rules

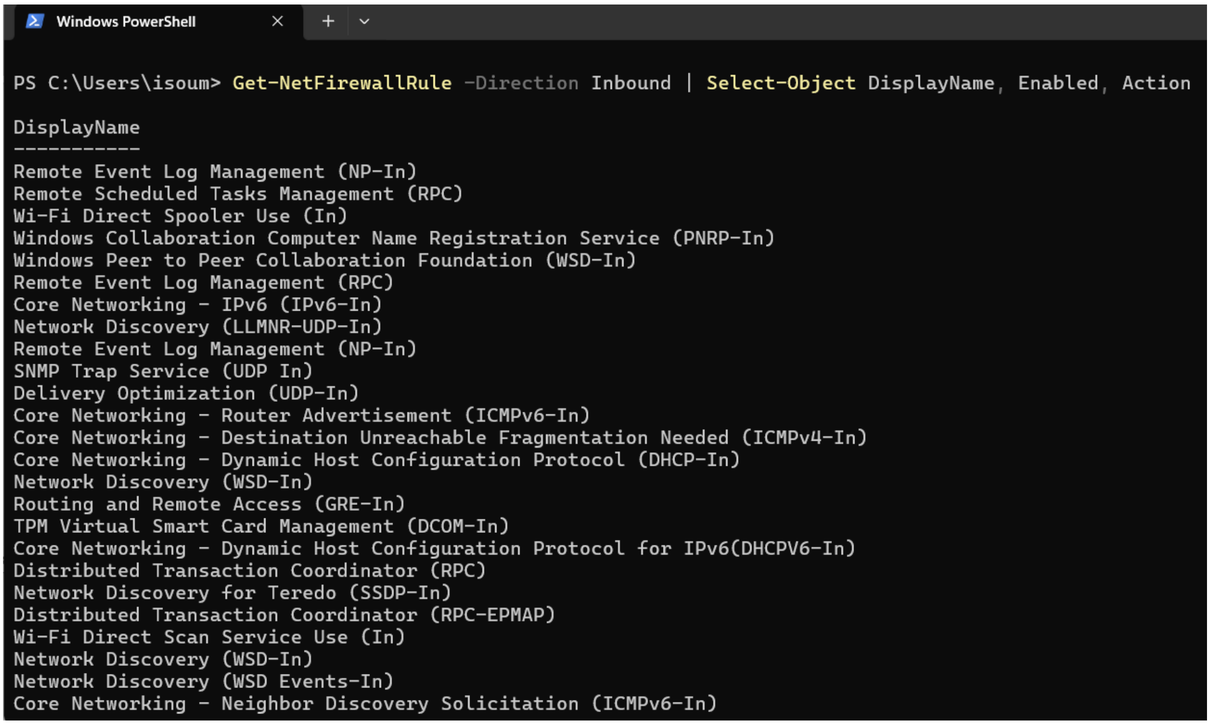
Get-NetFirewallRule | Select-Object DisplayName, Enabled, Direction, Action



```
PS C:\Users\isoum> Get-NetFirewallRule | Select-Object DisplayName, Enabled, Direction, Action

DisplayName                                                                Enabled Direction Action
-----------                                                                ------- --------- ------
Network Discovery (UPnP-Out)                                                 False  Outbound  Allow
Wi-Fi Direct Spooler Use (Out)                                                True  Outbound  Allow
Remote Assistance (TCP-Out)                                                  False  Outbound  Allow
Network Discovery (SSDP-Out)                                                  True  Outbound  Allow
Network Discovery (WSD Events-Out)                                            True  Outbound  Allow
Remote Event Log Management (NP-In)                                          False   Inbound  Allow
Remote Scheduled Tasks Management (RPC)                                      False   Inbound  Allow
Wi-Fi Direct Spooler Use (In)                                                 True   Inbound  Allow
Remote Assistance (TCP-Out)                                                   True  Outbound  Allow
Distributed Transaction Coordinator (TCP-Out)                                False  Outbound  Allow
Routing and Remote Access (L2TP-Out)                                         False  Outbound  Allow
Core Networking - Packet Too Big (ICMPv6-Out)                                 True  Outbound  Allow
Connected Devices Platform (UDP-Out)                                          True  Outbound  Allow
Windows Collaboration Computer Name Registration Service (PNRP-In)           False   Inbound  Allow
Network Discovery (NB-Name-Out)                                              False  Outbound  Allow
Network Discovery (NB-Datagram-Out)                                          False  Outbound  Allow
Windows Peer to Peer Collaboration Foundation (WSD-In)                       False   Inbound  Allow
Remote Event Log Management (RPC)                                            False   Inbound  Allow
Core Networking - IPv6 (IPv6-In)                                              True   Inbound  Allow
Connected Devices Platform - Wi-Fi Direct Transport (TCP-Out)                 True  Outbound  Allow
Network Discovery (LLMNR-UDP-In)                                             False   Inbound  Allow
Remote Event Log Management (NP-In)                                          False   Inbound  Allow
SNMP Trap Service (UDP In)                                                   False   Inbound  Allow
mDNS (UDP-Out)                                                                True  Outbound  Allow
Delivery Optimization (UDP-In)                                                True   Inbound  Allow
Core Networking - Parameter Problem (ICMPv6-Out)                              True  Outbound  Allow
Core Networking - Router Advertisement (ICMPv6-In)                            True   Inbound  Allow
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)    True   Inbound  Allow
Core Networking - Dynamic Host Configuration Protocol (DHCP-In)               True   Inbound  Allow
Network Discovery (WSD-In)                                                    True   Inbound  Allow
Routing and Remote Access (GRE-In)                                           False   Inbound  Allow
TPM Virtual Smart Card Management (DCOM-In)                                  False   Inbound  Allow
```

List inbound rules only

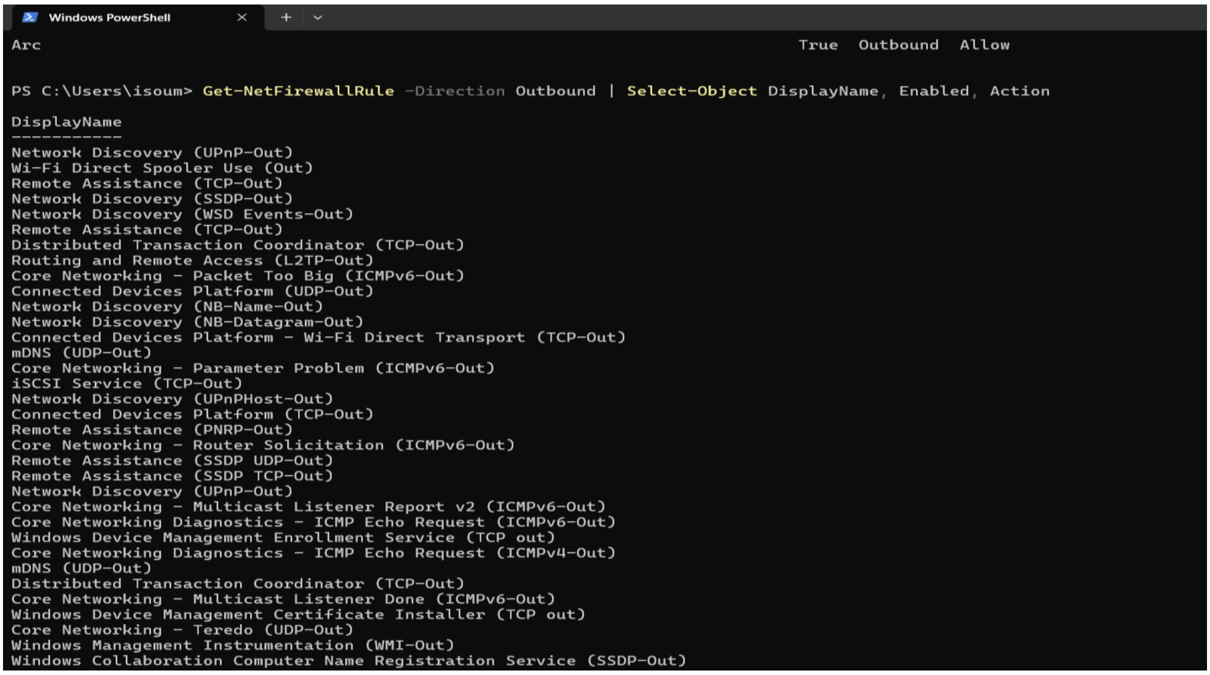
Get-NetFirewallRule -Direction Inbound | Select-Object DisplayName, Enabled, Action



```
PS C:\Users\isoum> Get-NetFirewallRule -Direction Inbound | Select-Object DisplayName, Enabled, Action

DisplayName
-----------
Remote Event Log Management (NP-In)
Remote Scheduled Tasks Management (RPC)
Wi-Fi Direct Spooler Use (In)
Windows Collaboration Computer Name Registration Service (PNRP-In)
Windows Peer to Peer Collaboration Foundation (WSD-In)
Remote Event Log Management (RPC)
Core Networking - IPv6 (IPv6-In)
Network Discovery (LLMNR-UDP-In)
Remote Event Log Management (NP-In)
SNMP Trap Service (UDP In)
Delivery Optimization (UDP-In)
Core Networking - Router Advertisement (ICMPv6-In)
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)
Core Networking - Dynamic Host Configuration Protocol (DHCP-In)
Network Discovery (WSD-In)
Routing and Remote Access (GRE-In)
TPM Virtual Smart Card Management (DCOM-In)
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
Distributed Transaction Coordinator (RPC)
Network Discovery for Teredo (SSDP-In)
Distributed Transaction Coordinator (RPC-EPMAP)
Wi-Fi Direct Scan Service Use (In)
Network Discovery (WSD-In)
Network Discovery (WSD Events-In)
Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)
```

List outbound rules only

Get-NetFirewallRule -Direction Outbound | Select-Object DisplayName, Enabled, Action



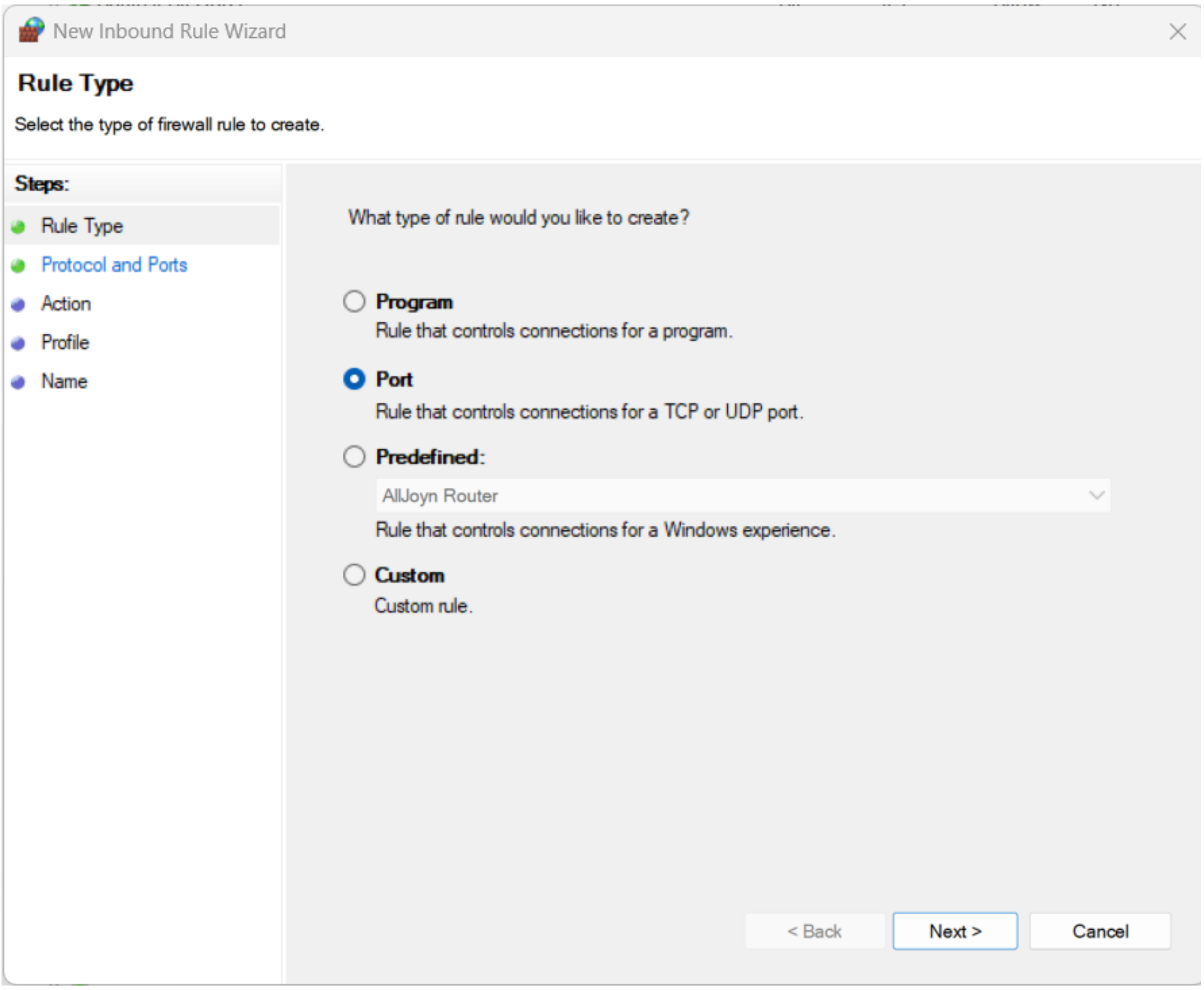
```
Arc                                                                  True  Outbound  Allow

PS C:\Users\isoum> Get-NetFirewallRule -Direction Outbound | Select-Object DisplayName, Enabled, Action

DisplayName
-----------
Network Discovery (UPnP-Out)
Wi-Fi Direct Spooler Use (Out)
Remote Assistance (TCP-Out)
Network Discovery (SSDP-Out)
Network Discovery (WSD Events-Out)
Remote Assistance (TCP-Out)
Distributed Transaction Coordinator (TCP-Out)
Routing and Remote Access (L2TP-Out)
Core Networking - Packet Too Big (ICMPv6-Out)
Connected Devices Platform (UDP-Out)
Network Discovery (NB-Name-Out)
Network Discovery (NB-Datagram-Out)
Connected Devices Platform - Wi-Fi Direct Transport (TCP-Out)
mDNS (UDP-Out)
Core Networking - Parameter Problem (ICMPv6-Out)
iSCSI Service (TCP-Out)
Network Discovery (UPnPHost-Out)
Connected Devices Platform (TCP-Out)
Remote Assistance (PNRP-Out)
Core Networking - Router Solicitation (ICMPv6-Out)
Remote Assistance (SSDP UDP-Out)
Remote Assistance (SSDP TCP-Out)
Network Discovery (UPnP-Out)
Core Networking - Multicast Listener Report v2 (ICMPv6-Out)
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-Out)
Windows Device Management Enrollment Service (TCP out)
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-Out)
mDNS (UDP-Out)
Distributed Transaction Coordinator (TCP-Out)
Core Networking - Multicast Listener Done (ICMPv6-Out)
Windows Device Management Certificate Installer (TCP out)
Core Networking - Teredo (UDP-Out)
Windows Management Instrumentation (WMI-Out)
Windows Collaboration Computer Name Registration Service (SSDP-Out)
```

3. Creating a Block Rule for Telnet (Port 23)

GUI Method

Step 1: Create New Inbound Rule

1. Right-click on "Inbound Rules" in the left pane
2. Select "New Rule..." from the context menu
3. New Inbound Rule Wizard will open



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.

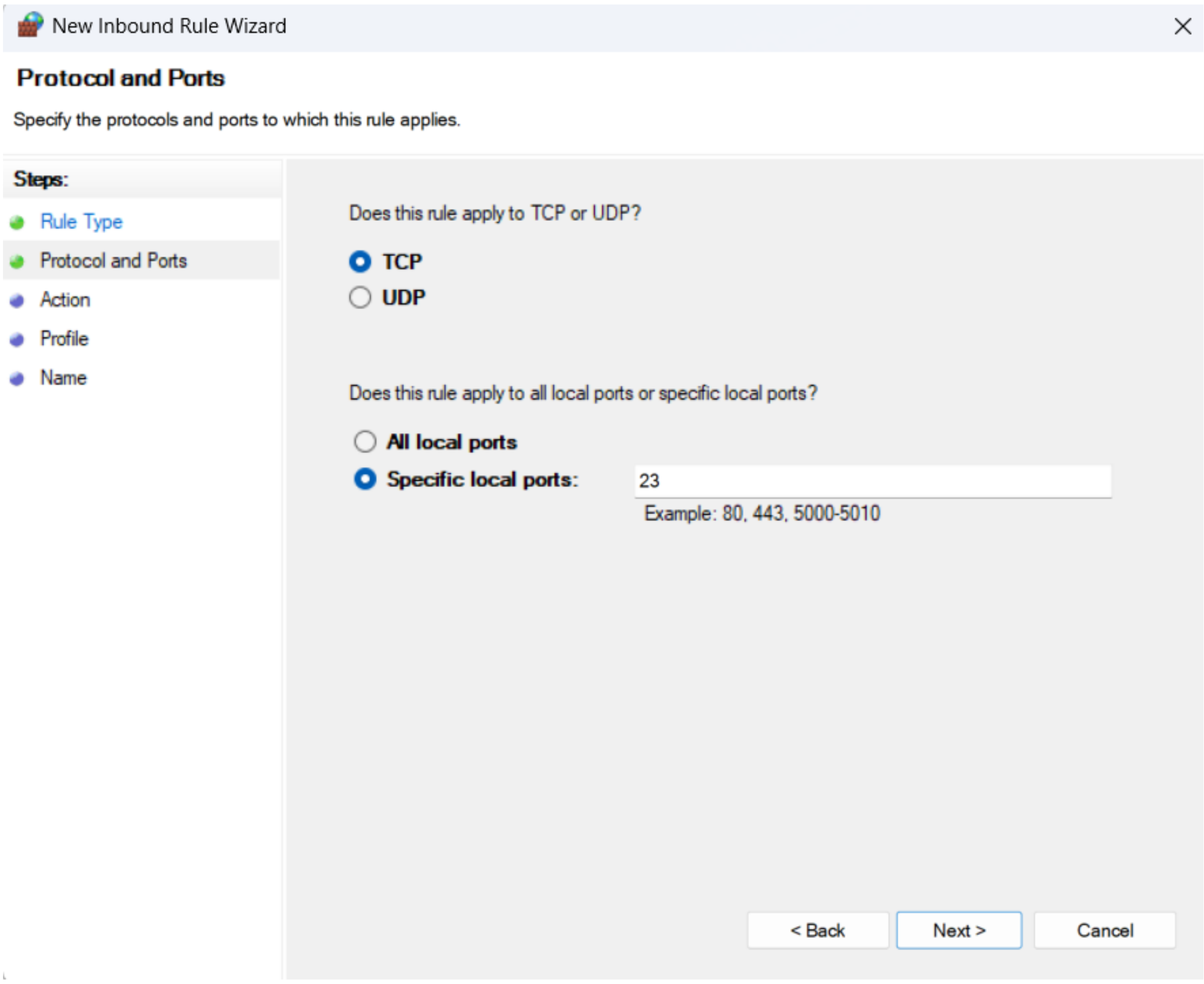
Step 2: Configure Rule Type

1. Select "Port" as the rule type
2. Click "Next"

Step 3: Configure Protocol and Ports

1. Select "TCP"
2. Select "Specific local ports"

3. Enter "23" in the text field
4. Click "Next"



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

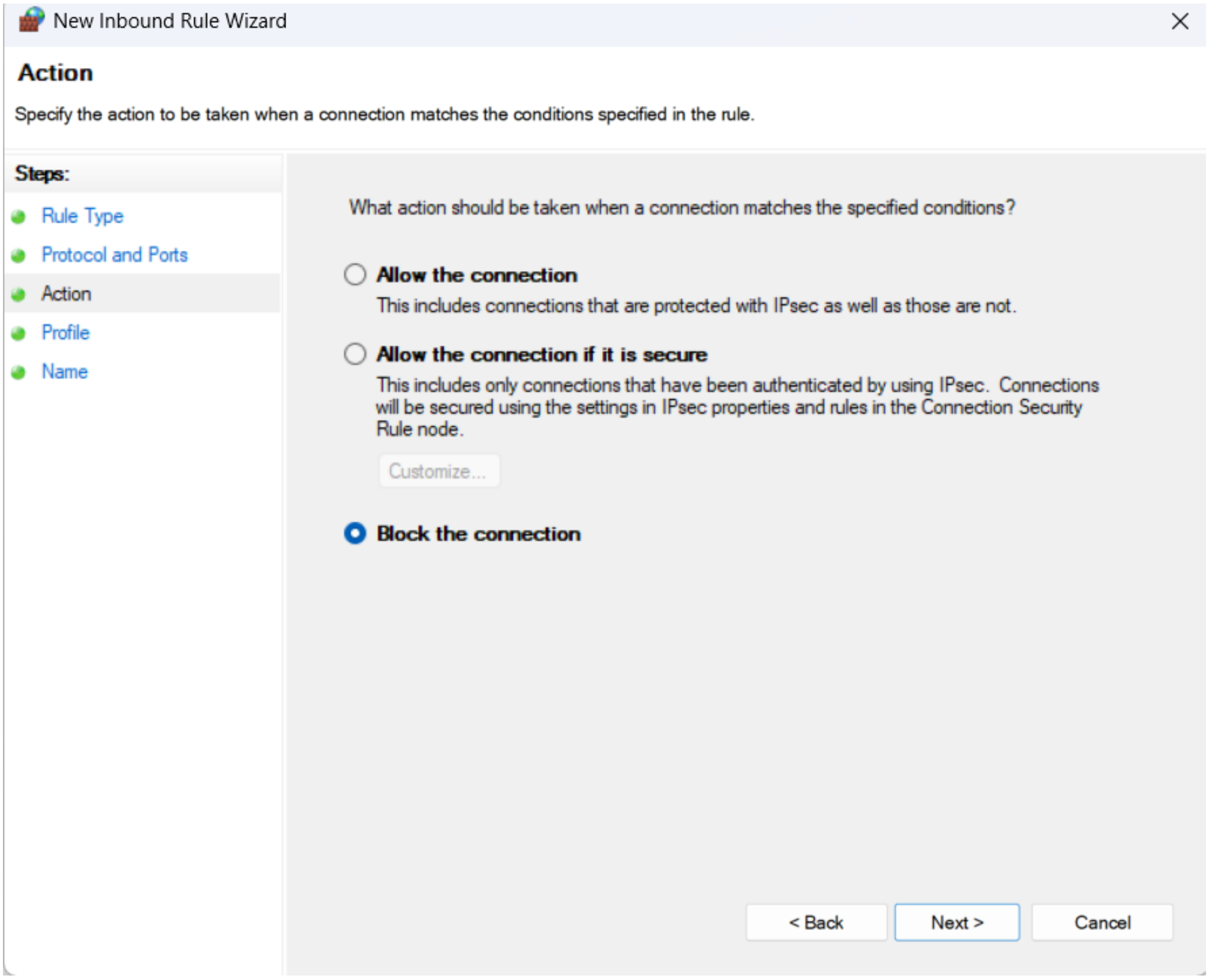
Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 23

Example: 80, 443, 5000-5010

Step 4: Configure Action

1. Select "Block the connection"
2. Click "Next"



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?

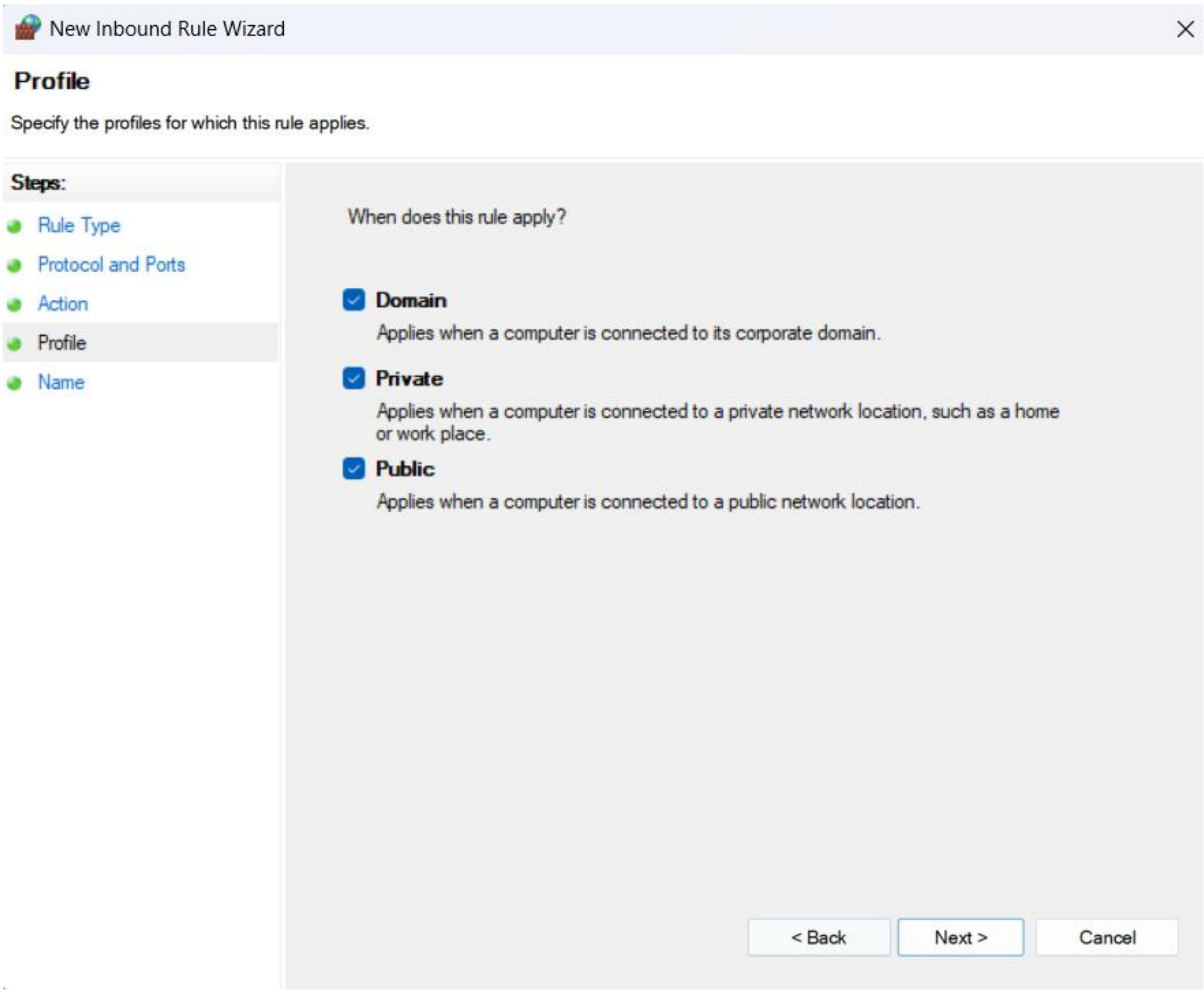
○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **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**

Step 5: Configure Profile

1. Keep all profiles selected (Domain, Private, Public)
2. Click "Next"



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

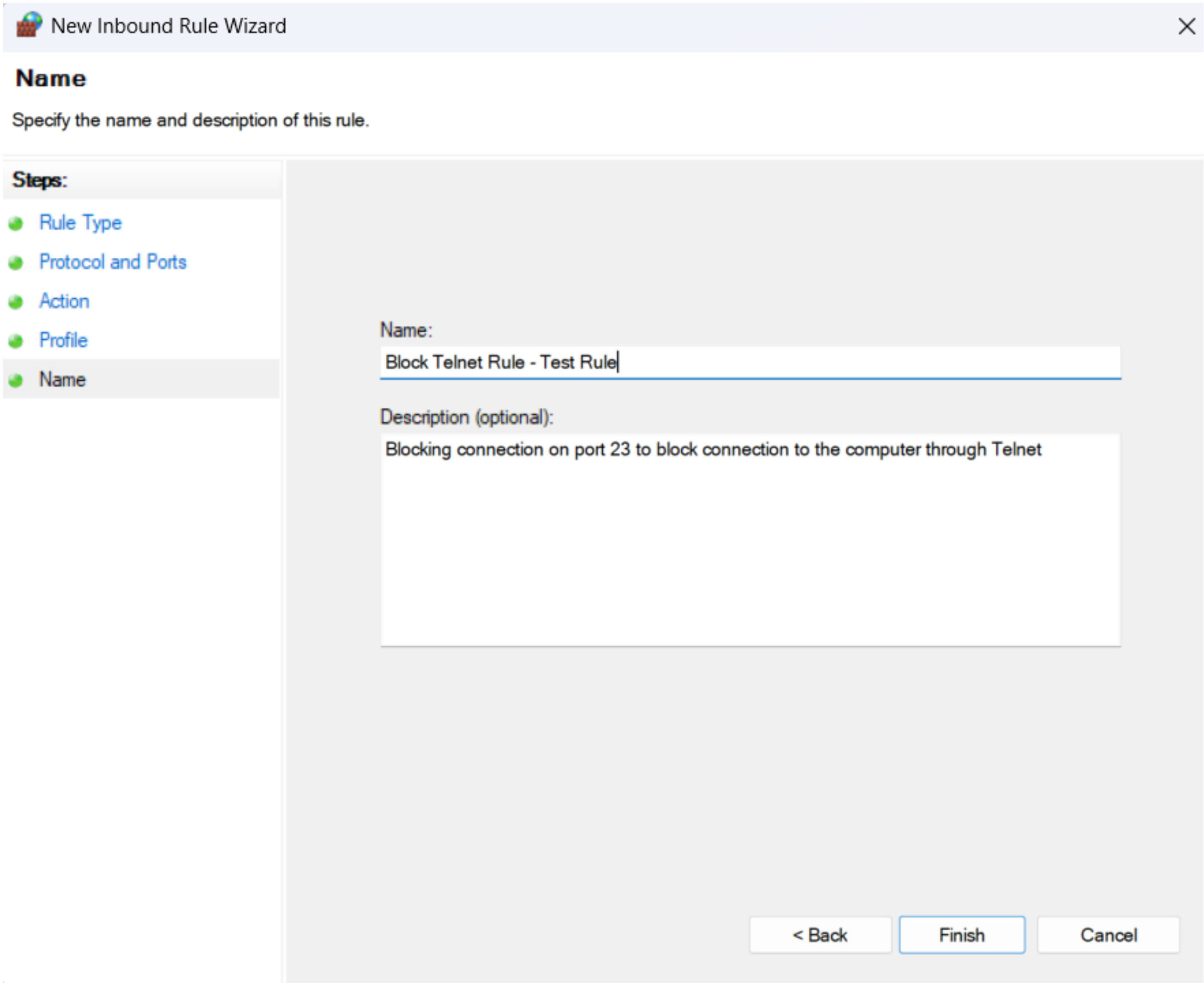
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **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.

Step 6: Name the Rule

1. Name: "Block Telnet Port 23 - Test Rule"
2. Description: "Test rule to block inbound Telnet traffic on port 23"
3. Click "Finish"



Name:
Block Telnet Rule - Test Rule

Description (optional):
Blocking connection on port 23 to block connection to the computer through Telnet

Command Line Method

PowerShell Command:

```
New-NetFirewallRule -DisplayName "Block Telnet Port 23 - Test Rule" -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block
```

Verification of Rule Creation:

```
Get-NetFirewallRule -DisplayName "Block Telnet Port 23 - Test Rule"
```

4. Testing the Firewall Rule

Test Method 1: Local Telnet Connection Attempt

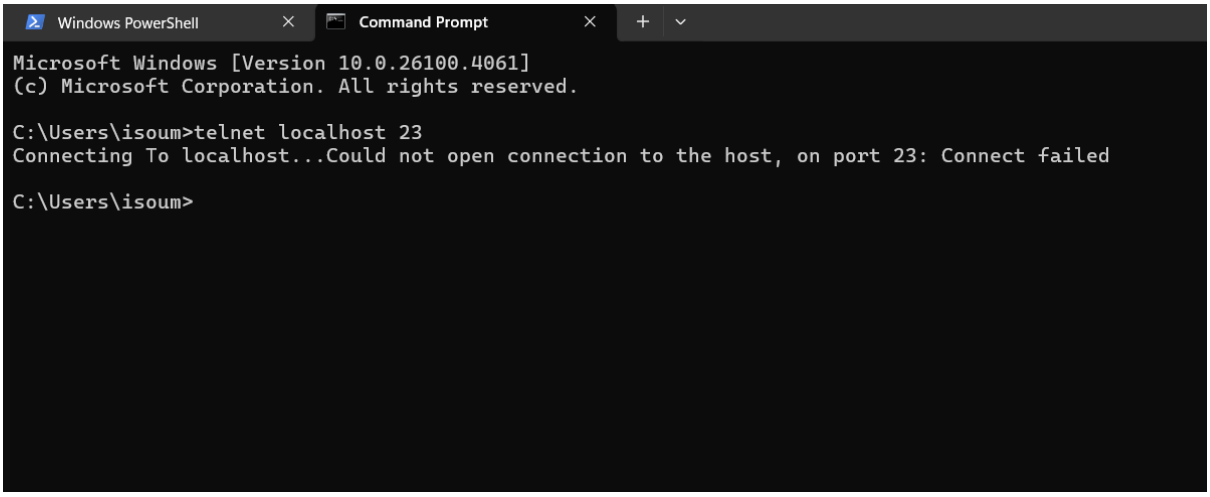
Step 1: Enable Telnet Client (if not already enabled)

1. Open "Turn Windows features on or off"
2. Check "Telnet Client"
3. Click OK and wait for installation

Step 2: Test Connection

telnet localhost 23

Expected Result: Connection should fail or timeout due to the firewall block rule.

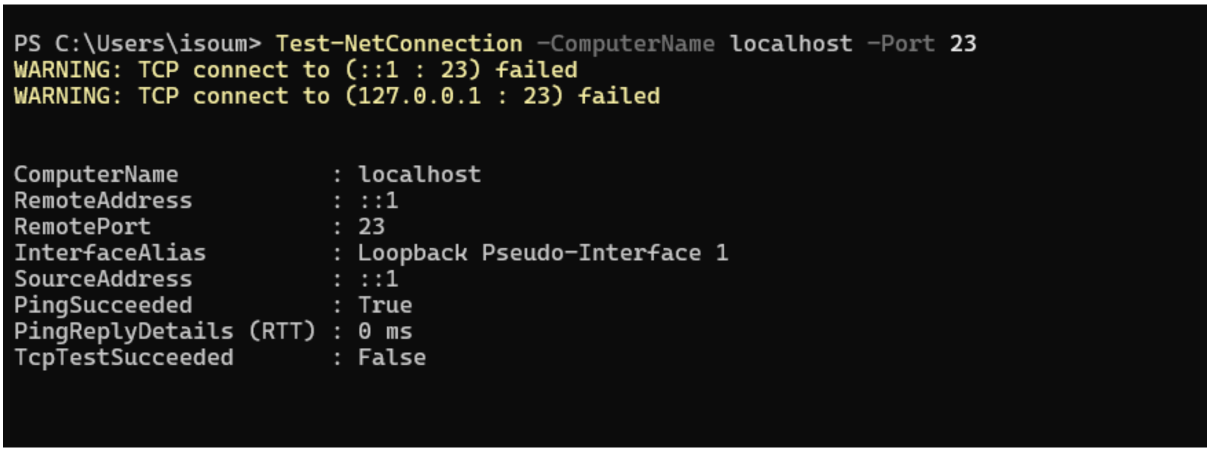


```
Microsoft Windows [Version 10.0.26100.4061]
(c) Microsoft Corporation. All rights reserved.

C:\Users\isoum>telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed

C:\Users\isoum>
```

Test Method 2: Using PowerShell Test-NetConnection

Test-NetConnection -ComputerName localhost -Port 23

Expected Result: TcpTestSucceeded should be False



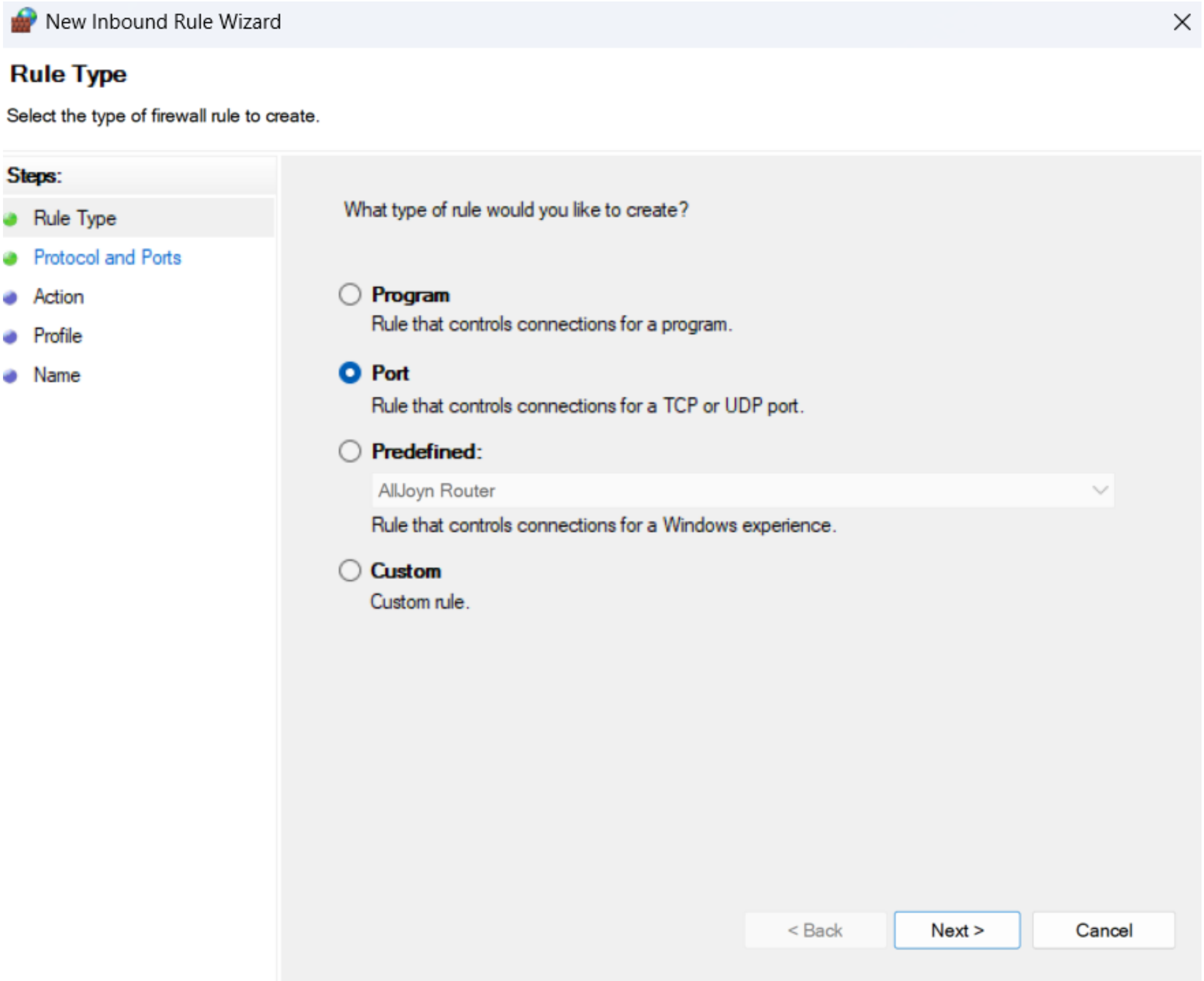
```
PS C:\Users\isoum> Test-NetConnection -ComputerName localhost -Port 23
WARNING: TCP connect to (::1 : 23) failed
WARNING: TCP connect to (127.0.0.1 : 23) failed


ComputerName           : localhost
RemoteAddress          : ::1
RemotePort             : 23
InterfaceAlias         : Loopback Pseudo-Interface 1
SourceAddress          : ::1
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False
```

5. Adding SSH Allow Rule (Port 22)

GUI Method

Step 1: Create New Inbound Rule for SSH

1. Right-click on "Inbound Rules"
2. Select "New Rule..."
3. Select "Port" → Next
4. Select "TCP" and enter "22" for specific local ports
5. Select "Allow the connection" → Next
6. Keep all profiles selected → Next
7. Name: "Allow SSH Port 22"
8. Description: "Allow inbound SSH connections on port 22"
9. Click "Finish"



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

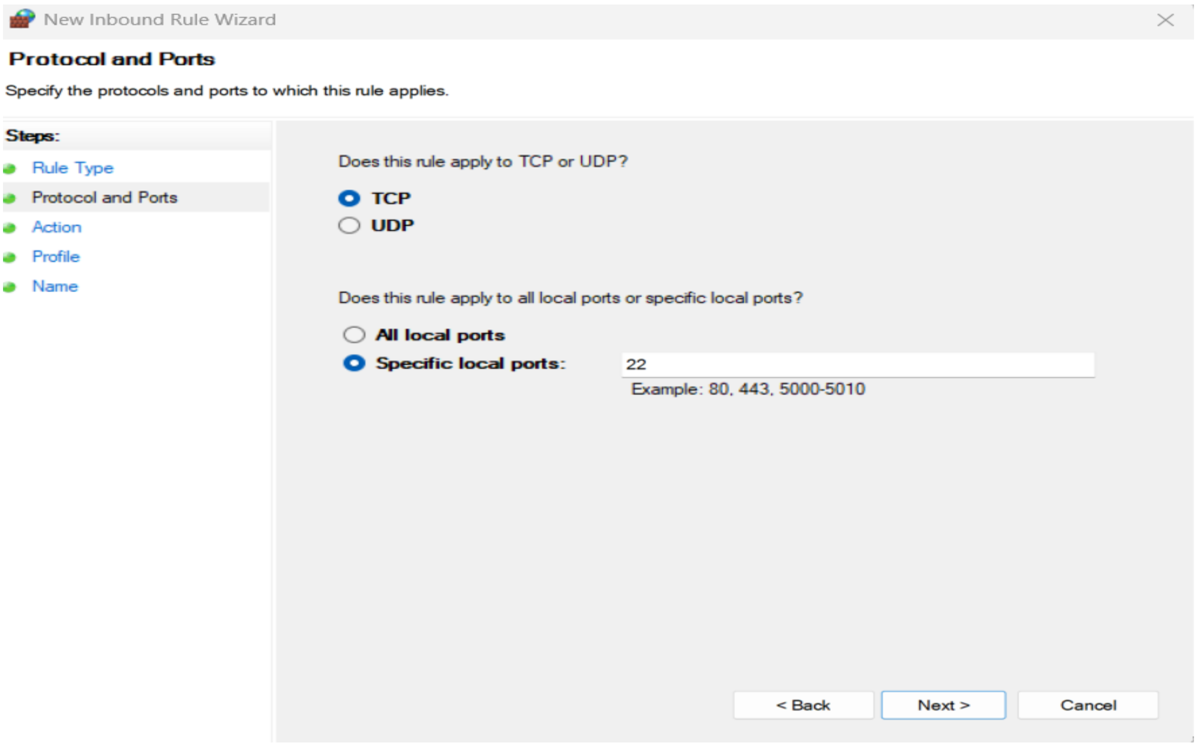
What type of rule would you like to create?

○ **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:

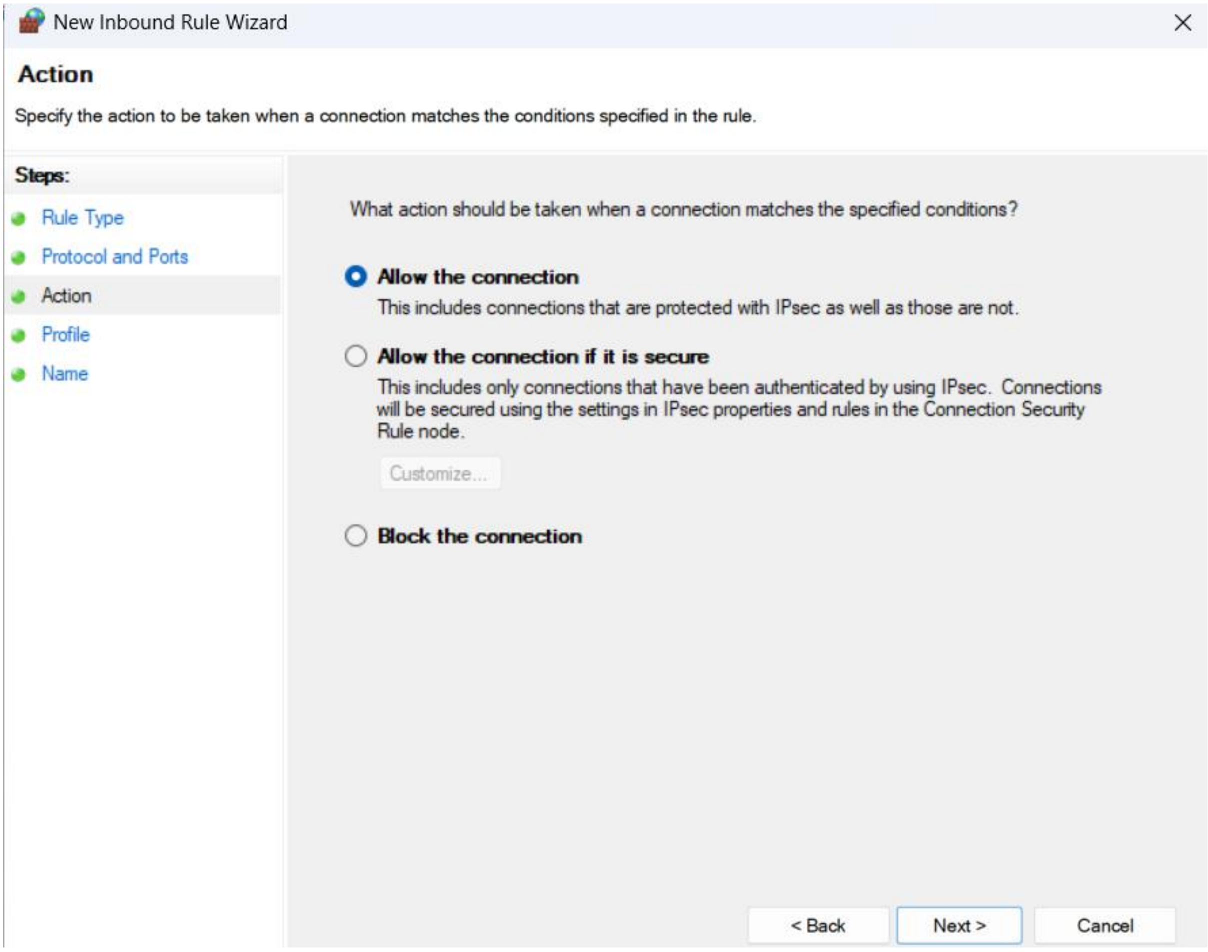
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

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:** 22
Example: 80, 443, 5000-5010



New Inbound Rule Wizard

Action

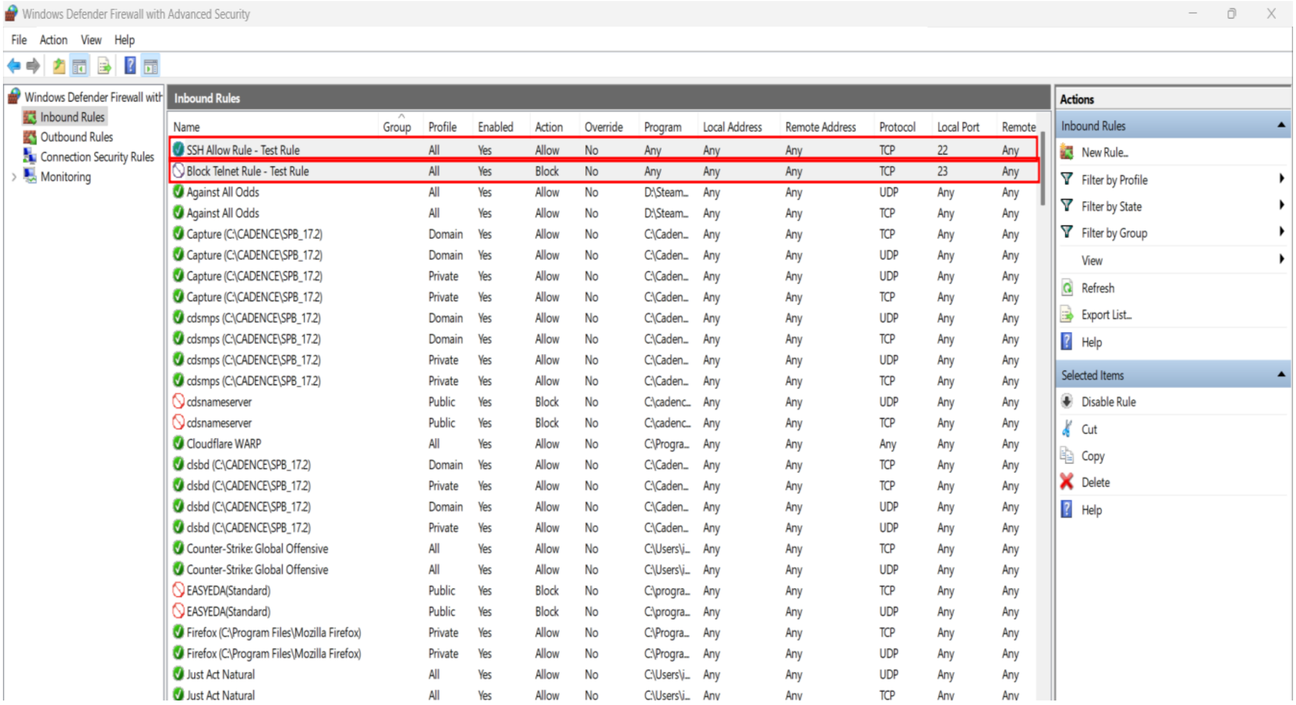
Specify the action to be taken when a connection matches the conditions specified in the rule.

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**



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote
SSH Allow Rule - Test Rule		All	Yes	Allow	No	Any	Any	Any	TCP	22	Any
Block Telnet Rule - Test Rule		All	Yes	Block	No	Any	Any	Any	TCP	23	Any
Against All Odds		All	Yes	Allow	No	D:\Steam...	Any	Any	UDP	Any	Any
Against All Odds		All	Yes	Allow	No	D:\Steam...	Any	Any	TCP	Any	Any
Capture (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
Capture (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
Capture (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
Capture (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
cdsmps (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
cdsmps (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
cdsmps (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
cdsmps (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
cdsnameserver		Public	Yes	Block	No	C:\cadenc...	Any	Any	UDP	Any	Any
cdsnameserver		Public	Yes	Block	No	C:\cadenc...	Any	Any	TCP	Any	Any
Cloudflare WARP		All	Yes	Allow	No	C:\Progra...	Any	Any	Any	Any	Any
clsbd (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
clsbd (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
clsbd (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
clsbd (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
Counter-Strike: Global Offensive		All	Yes	Allow	No	C:\Users\i...	Any	Any	TCP	Any	Any
Counter-Strike: Global Offensive		All	Yes	Allow	No	C:\Users\i...	Any	Any	UDP	Any	Any
EASYEDA(Standard)		Public	Yes	Block	No	C:\progra...	Any	Any	TCP	Any	Any
EASYEDA(Standard)		Public	Yes	Block	No	C:\progra...	Any	Any	UDP	Any	Any
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any	Any	TCP	Any	Any
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any	Any	UDP	Any	Any
Just Act Natural		All	Yes	Allow	No	C:\Users\i...	Any	Any	UDP	Any	Any
Just Act Natural		All	Yes	Allow	No	C:\Users\i...	Any	Any	TCP	Any	Any

Command Line Method

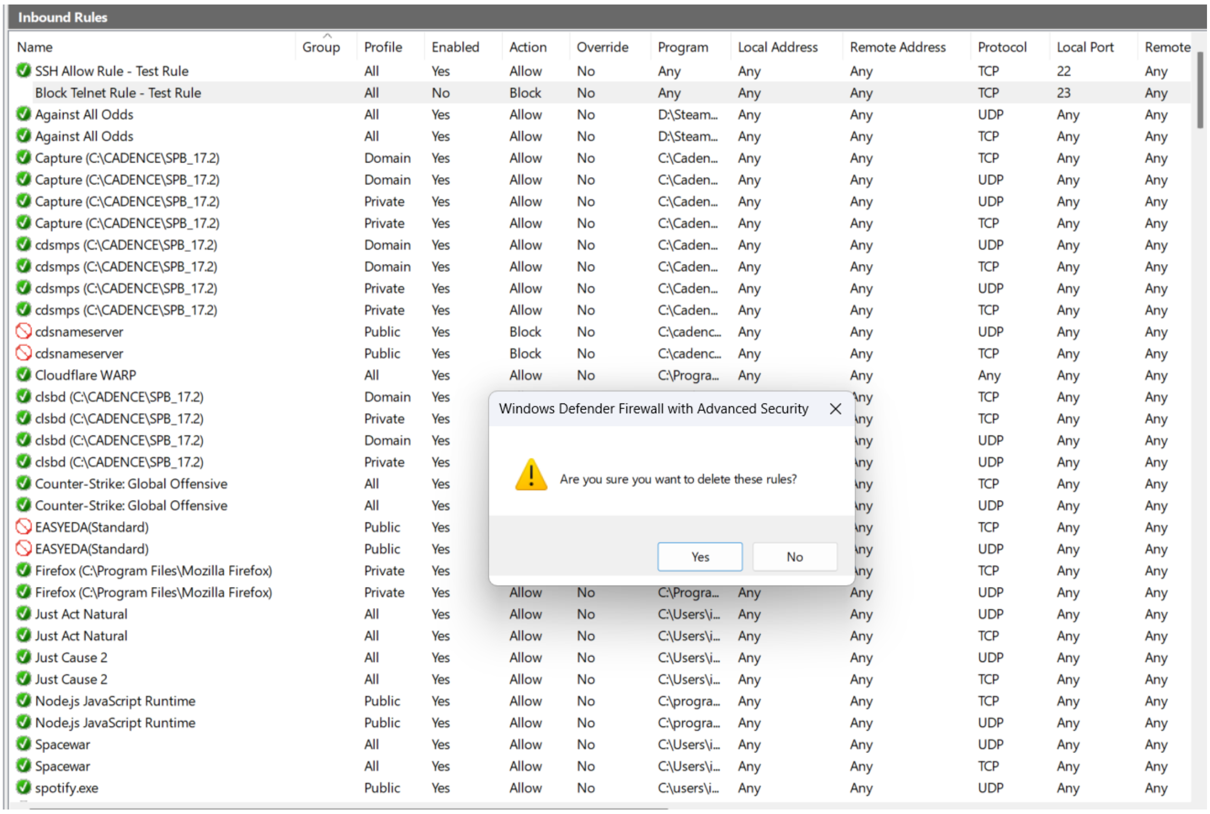
```
New-NetFirewallRule -DisplayName "Allow SSH Port 22" -Direction
Inbound -Protocol TCP -LocalPort 22 -Action Allow
```

Part 6: Removing the Test Block Rule

GUI Method

Step 1: Locate and Delete Rule

1. Navigate to "Inbound Rules"
2. Find "Block Telnet Port 23 - Test Rule"
3. Right-click on the rule
4. Select "Delete"
5. Confirm deletion



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote
✓ SSH Allow Rule - Test Rule		All	Yes	Allow	No	Any	Any	Any	TCP	22	Any
Block Telnet Rule - Test Rule		All	No	Block	No	Any	Any	Any	TCP	23	Any
✓ Against All Odds		All	Yes	Allow	No	D:\Steam...	Any	Any	UDP	Any	Any
✓ Against All Odds		All	Yes	Allow	No	D:\Steam...	Any	Any	TCP	Any	Any
✓ Capture (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
✓ Capture (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
✓ Capture (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
✓ Capture (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
✓ cdsmps (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
✓ cdsmps (C:\CADENCE\SPB_17.2)		Domain	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
✓ cdsmps (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	UDP	Any	Any
✓ cdsmps (C:\CADENCE\SPB_17.2)		Private	Yes	Allow	No	C:\Caden...	Any	Any	TCP	Any	Any
🛇 cdsnameserver		Public	Yes	Block	No	C:\cadenc...	Any	Any	UDP	Any	Any
🛇 cdsnameserver		Public	Yes	Block	No	C:\cadenc...	Any	Any	TCP	Any	Any
✓ Cloudflare WARP		All	Yes	Allow	No	C:\Progra...	Any	Any	Any	Any	Any
✓ clsbd (C:\CADENCE\SPB_17.2)		Domain	Yes					ny	TCP	Any	Any
✓ clsbd (C:\CADENCE\SPB_17.2)		Private	Yes					ny	TCP	Any	Any
✓ clsbd (C:\CADENCE\SPB_17.2)		Domain	Yes					ny	UDP	Any	Any
✓ clsbd (C:\CADENCE\SPB_17.2)		Private	Yes					ny	UDP	Any	Any
✓ Counter-Strike: Global Offensive		All	Yes					ny	TCP	Any	Any
✓ Counter-Strike: Global Offensive		All	Yes					ny	UDP	Any	Any
🛇 EASYEDA(Standard)		Public	Yes					ny	TCP	Any	Any
🛇 EASYEDA(Standard)		Public	Yes					ny	UDP	Any	Any
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes					ny	TCP	Any	Any
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any	Any	UDP	Any	Any
✓ Just Act Natural		All	Yes	Allow	No	C:\Users\i...	Any	Any	UDP	Any	Any
✓ Just Act Natural		All	Yes	Allow	No	C:\Users\i...	Any	Any	TCP	Any	Any
✓ Just Cause 2		All	Yes	Allow	No	C:\Users\i...	Any	Any	UDP	Any	Any
✓ Just Cause 2		All	Yes	Allow	No	C:\Users\i...	Any	Any	TCP	Any	Any
✓ Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP	Any	Any
✓ Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP	Any	Any
✓ Spacewar		All	Yes	Allow	No	C:\Users\i...	Any	Any	UDP	Any	Any
✓ Spacewar		All	Yes	Allow	No	C:\Users\i...	Any	Any	TCP	Any	Any
✓ spotify.exe		Public	Yes	Allow	No	C:\users\i...	Any	Any	UDP	Any	Any

Windows Defender Firewall with Advanced Security

Are you sure you want to delete these rules?

Command Line Method

```
Remove-NetFirewallRule -DisplayName "Block Telnet Port 23 - Test Rule"
```

Verification:

```
Get-NetFirewallRule -DisplayName "Block Telnet Port 23 - Test Rule"
```

7. Documentation of Commands Used

PowerShell Commands Summary

Command	Purpose
Get-NetFirewallRule	List existing firewall rules
New-NetFirewallRule	Create new firewall rule
Remove-NetFirewallRule	Delete firewall rule
Test-NetConnection	Test network connectivity

GUI Navigation Summary

1. Access Firewall: Win + R → wf.msc
2. Create Rule: Right-click Inbound/Outbound Rules → New Rule
3. Configure Rule: Port → Protocol/Port → Action → Profile → Name
4. Delete Rule: Right-click rule → Delete

Windows Firewall with Advanced Security acts as a network packet filter that examines incoming and outgoing network traffic based on predefined rules.

Traffic Filtering Process

1. Packet Inspection
    - Every network packet is examined against firewall rules
    - Rules are processed in order of precedence
    - First matching rule determines the action
2. Rule Types
    - Inbound Rules: Control traffic coming into the computer
    - Outbound Rules: Control traffic leaving the computer
3. Rule Criteria
    - Protocol: TCP, UDP, ICMP, etc.
    - Port Numbers: Specific ports or port ranges

    - IP Addresses: Source and destination addresses
    - Programs: Specific applications
    - Services: Windows services
4. Actions
    - Allow: Permit the traffic
    - Block: Deny the traffic
    - Allow if secure: Permit only authenticated/encrypted traffic
5. Profiles
    - Domain: When connected to domain network
    - Private: When connected to private network
    - Public: When connected to public network

Default Behaviour

- Inbound: Block by default, allow specific exceptions
- Outbound: Allow by default, can create block rules

Rule Precedence

1. Explicitly configured rules take precedence
2. Block rules generally override allow rules
3. More specific rules override general rules