

Task - 4 : Setup and Use a Firewall on Windows

1. Open Windows Firewall Configuration Tool

- Press **Win + R**, type **wf.msc**, and hit Enter.
- This opens Windows Defender Firewall with Advanced Security.

2. List of Current Firewall Rules

a. Inbound Rules :

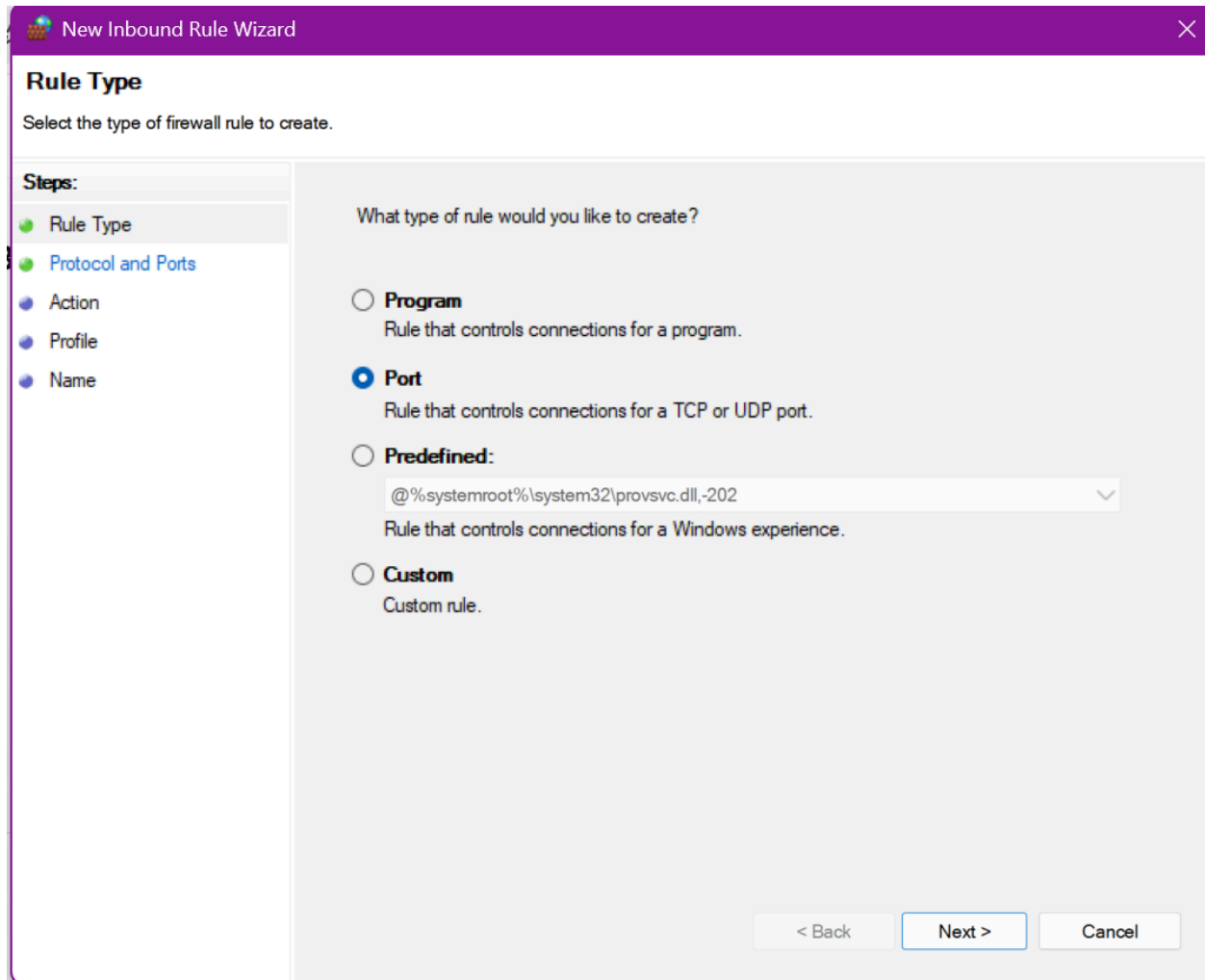
Inbound Rules							
Name	Group	Profile	Enabled	Action	Override	Program	Local Address
✓ Apache HTTP Server		Private	Yes	Allow	No	C:\xampp...	Any
✓ Apache HTTP Server		Private	Yes	Allow	No	C:\xampp...	Any
✓ Apache NetBeans IDE Launcher		Public	Yes	Allow	No	C:\progra...	Any
✓ Apache NetBeans IDE Launcher		Private	Yes	Allow	No	C:\progra...	Any
✓ Apache NetBeans IDE Launcher		Public	Yes	Allow	No	C:\progra...	Any
✓ Apache NetBeans IDE Launcher		Private	Yes	Allow	No	C:\progra...	Any
✓ Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progra...	Any
✓ Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progra...	Any
✓ Java(TM) Platform SE binary		Private	Yes	Allow	No	C:\progra...	Any
✓ Java(TM) Platform SE binary		Private	Yes	Allow	No	C:\progra...	Any
✓ Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progra...	Any
✓ mysqld		Private	Yes	Allow	No	C:\xampp...	Any
✓ mysqld		Private	Yes	Allow	No	C:\xampp...	Any
✓ @!Microsoft.AAD.BrokerPlugin_1000.19041...	@!Microsoft.AAD.BrokerPlugi...	Domai...	Yes	Allow	No	Any	Any
✓ @!Microsoft.Win32WebViewHost_10.0.190...	@!Microsoft.Win32WebView...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.CloudExperienceHo...	@!Microsoft.Windows.Cloud...	Domai...	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.Search_1.14.17.1904...	@!Microsoft.Windows.Search...	Domai...	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.SecHealthUI_10.0.19...	@!Microsoft.Windows.SecHe...	Domai...	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.StartMenuExperien...	@!Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any
✓ @!MicrosoftWindows.Client.CBS_1000.190...	@!MicrosoftWindows.Client...	Domai...	Yes	Allow	No	Any	Any
✓ @!MicrosoftWindows.LKG.DesktopSpotlig...	@!MicrosoftWindows.LKG.De...	Domai...	Yes	Allow	No	Any	Any
✓ Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
✓ App Installer	App Installer	Domai...	Yes	Allow	No	Any	Any
✓ App Installer	App Installer	Domai...	Yes	Allow	No	Any	Any

b. Outbound Rules :

Outbound Rules							
Name	Group	Profile	Enabled	Action	Override	Program	Local Address
✓ @!Microsoft.AAD.BrokerPlugin_1000.19041...	@!Microsoft.AAD.BrokerPlugi...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.AccountsControl_10.0.19041.4...	@!Microsoft.AccountsContro...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.LockApp_10.0.19041.4239_neu...	@!Microsoft.LockApp_10.0.19...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Win32WebViewHost_10.0.190...	@!Microsoft.Win32WebView...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.Apprep.ChxApp_10...	@!Microsoft.Windows.Appre...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.CloudExperienceHo...	@!Microsoft.Windows.Cloud...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.ContentDeliveryMa...	@!Microsoft.Windows.Conte...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.OOBENetworkCapti...	@!Microsoft.Windows.OOBE...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.ParentalControls_1...	@!Microsoft.Windows.Parent...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.PeopleExperienceH...	@!Microsoft.Windows.Peopl...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.Search_1.14.17.1904...	@!Microsoft.Windows.Search...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.SecHealthUI_10.0.19...	@!Microsoft.Windows.SecHe...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.SecureAssessmentB...	@!Microsoft.Windows.Secure...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.ShellExperienceHos...	@!Microsoft.Windows.Shelle...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.Windows.StartMenuExperien...	@!Microsoft.Windows.Start...	All	Yes	Allow	No	Any	Any
✓ @!Microsoft.XboxGameCallableUI_1000.19...	@!Microsoft.XboxGameCalla...	All	Yes	Allow	No	Any	Any
✓ @!MicrosoftWindows.Client.CBS_1000.190...	@!MicrosoftWindows.Client...	All	Yes	Allow	No	Any	Any
✓ @!MicrosoftWindows.LKG.AccountsService...	@!MicrosoftWindows.LKG.Ac...	All	Yes	Allow	No	Any	Any
✓ @!MicrosoftWindows.LKG.DesktopSpotlig...	@!MicrosoftWindows.LKG.De...	All	Yes	Allow	No	Any	Any
✓ @!MicrosoftWindows.LKG.IrisService_1000...	@!MicrosoftWindows.LKG.Iris...	All	Yes	Allow	No	Any	Any
✓ @!MicrosoftWindows.LKG.RulesEngine_10...	@!MicrosoftWindows.LKG.Ru...	All	Yes	Allow	No	Any	Any
✓ @!MicrosoftWindows.LKG.SpeechRuntime...	@!MicrosoftWindows.LKG.Sp...	All	Yes	Allow	No	Any	Any
✓ 3D Viewer	3D Viewer	All	Yes	Allow	No	Any	Any
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
✓ App Installer	App Installer	All	Yes	Allow	No	Any	Any
✓ App Installer	App Installer	All	Yes	Allow	No	Any	Any

3. Add a Rule to Block Inbound Traffic on Port 23 (Telnet)

- a. Go to Inbound Rules > New Rule (right panel).



The image shows the 'New Inbound Rule Wizard' window in Windows Firewall. The title bar is purple with the text 'New Inbound Rule Wizard' and a close button. The main area is titled 'Rule Type' and contains the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps:' pane lists five steps: 'Rule Type' (selected with a green dot), 'Protocol and Ports' (blue dot), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot). The main content area asks 'What type of rule would you like to create?' and lists four options: 'Program' (radio button), 'Port' (selected radio button), 'Predefined:' (radio button), and 'Custom' (radio button). The 'Predefined:' option has a dropdown menu showing '@%systemroot%\system32\provsvc.dll,-202'. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

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.

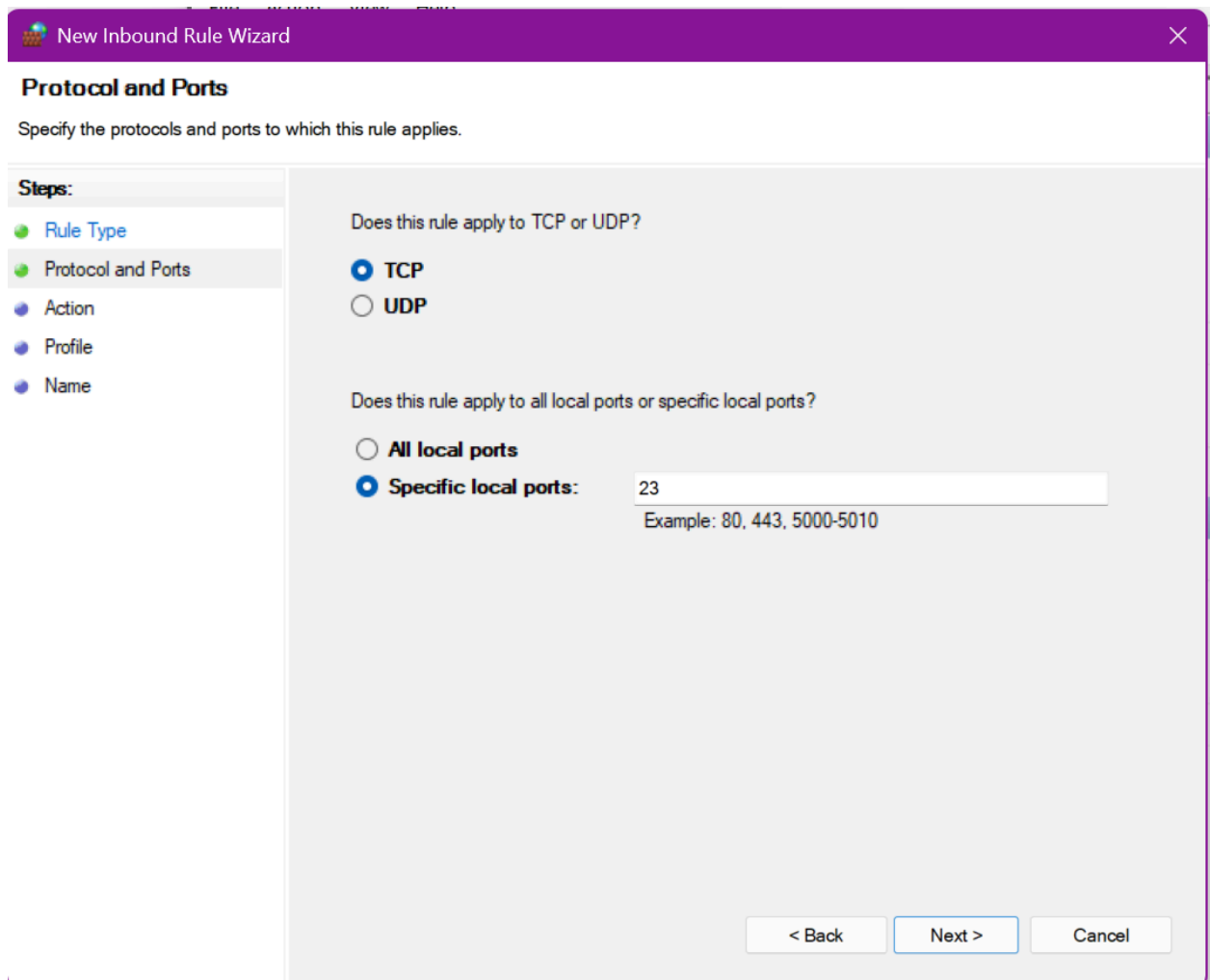
☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
@%systemroot%\system32\provsvc.dll,-202
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back Next > Cancel

b. Choose Port → Click Next.



The image shows a Windows Firewall 'New Inbound Rule Wizard' window. The title bar is purple and says 'New Inbound Rule Wizard' with a close button. The main area is titled 'Protocol and Ports' and has a subtitle 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' sidebar lists 'Rule Type', 'Protocol and Ports' (which is highlighted), 'Action', 'Profile', and 'Name'. The main content area has two questions. The first is 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'. The second is 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports:' (selected). Below the 'Specific local ports:' radio button is a text input field containing '23' and a hint text 'Example: 80, 443, 5000-5010'. At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

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?

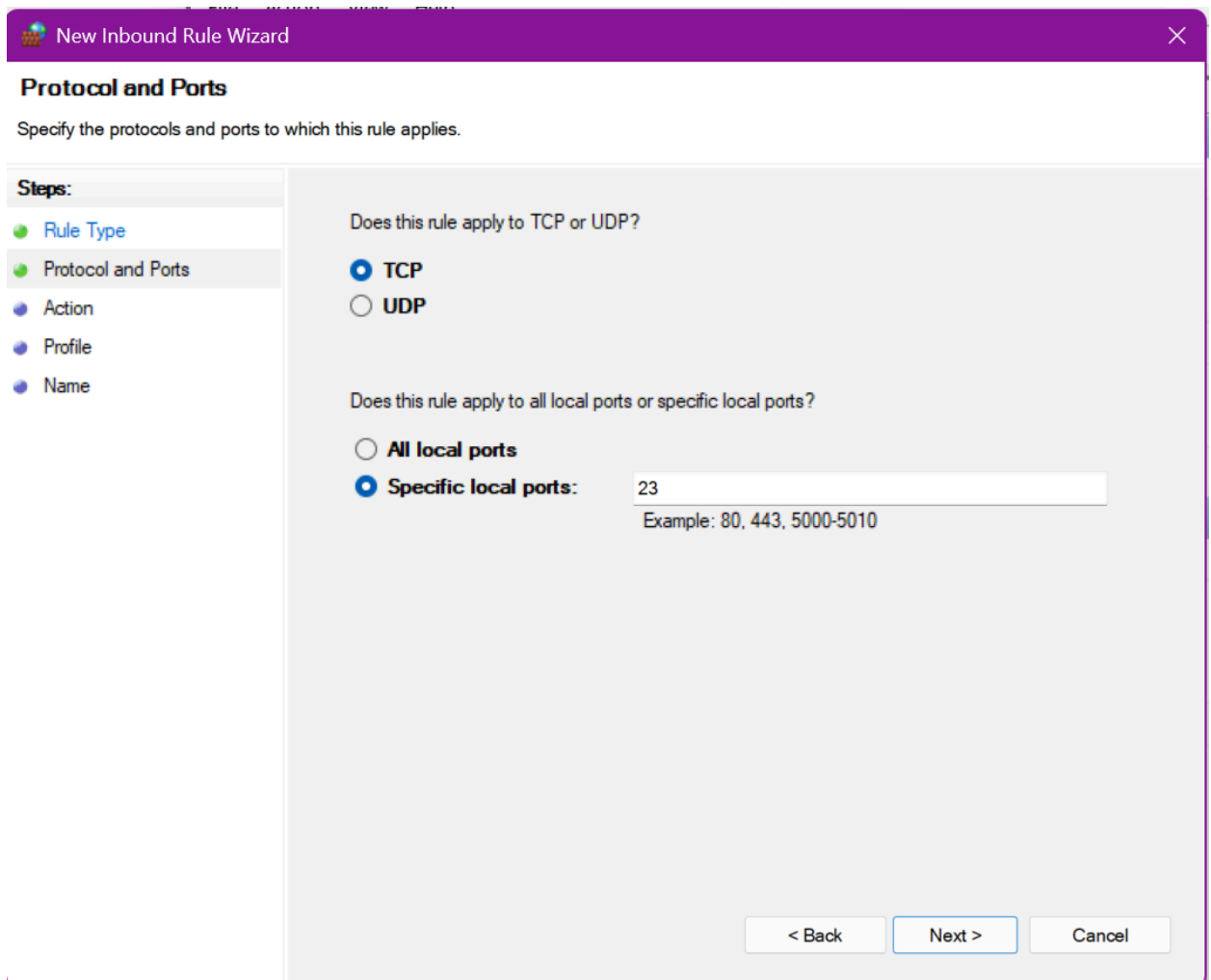
☐ All local ports

☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel

- c. Select TCP and enter 23 → Click Next.



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window has a purple title bar with the text 'New Inbound Rule Wizard' and a close button. Below the title bar, the section 'Protocol and Ports' is highlighted. The instruction 'Specify the protocols and ports to which this rule applies.' is displayed. On the left, a 'Steps:' sidebar lists 'Rule Type', 'Protocol and Ports' (selected), 'Action', 'Profile', and 'Name'. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports:' (selected). A text input field next to 'Specific local ports:' contains the value '23', with an example 'Example: 80, 443, 5000-5010' below it. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted), and 'Cancel'.

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

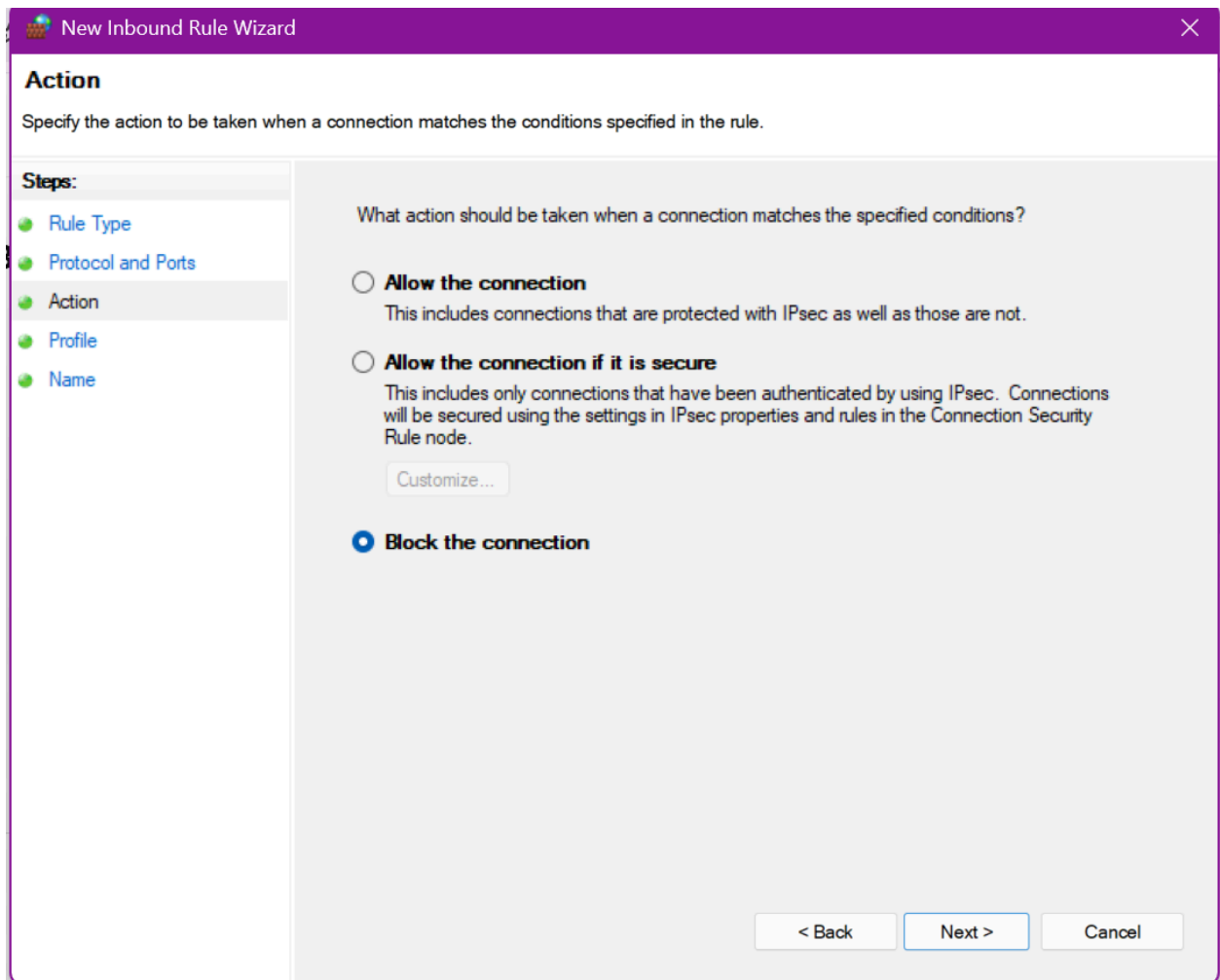
Does this rule apply to all local ports or specific local ports?

☐ All local ports
☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel

d. Select **Block the connection** → Click **Next**.



The image shows a Windows Firewall 'New Inbound Rule Wizard' window. The title bar is purple and contains the text 'New Inbound Rule Wizard' and a close button. The main window has a white background. On the left, there is a 'Steps:' pane with a list of steps: 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Action' step is currently selected and highlighted. The main area of the wizard is titled 'Action' and contains the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' Below this, there is a question: 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (with a description: 'This includes connections that are protected with IPsec as well as those are not.'), 'Allow the connection if it is secure' (with a description: '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.' and a 'Customize...' button), and 'Block the connection' (which is selected). At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

New Inbound Rule Wizard

Action

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

Steps:

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

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

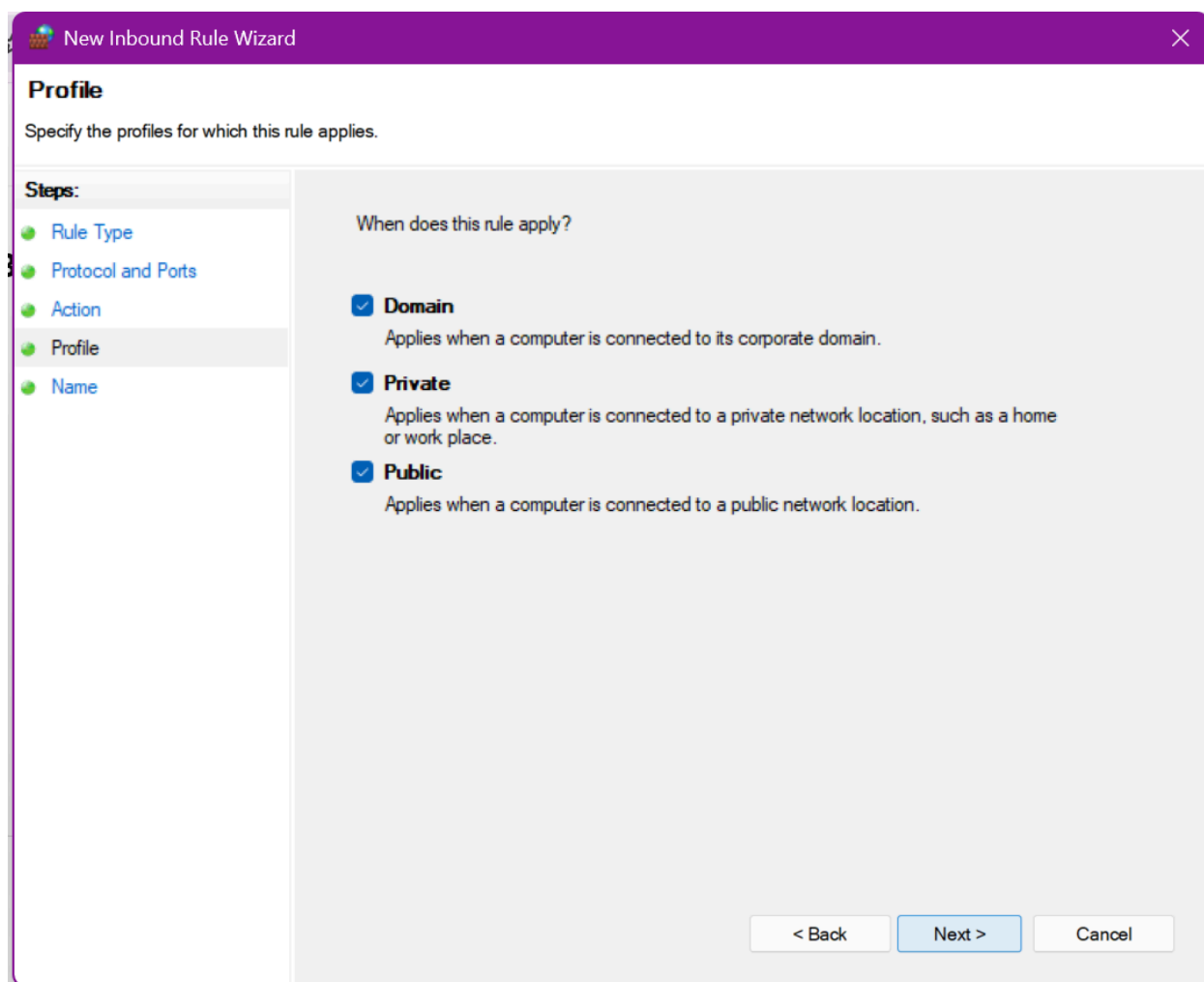
☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **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.
[Customize...](#)

☒ **Block the connection**

< Back Next > Cancel

e. Apply to all profiles (Domain, Private, Public) → Click Next.



The screenshot shows the 'New Inbound Rule Wizard' window with the 'Profile' step selected. The window has a purple title bar with the text 'New Inbound Rule Wizard' and a close button. The main area is titled 'Profile' and contains the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list shows 'Rule Type', 'Protocol and Ports', 'Action', 'Profile' (highlighted), and 'Name'. The main content area asks 'When does this rule apply?' and lists three options, all of which are checked: '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.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted), and 'Cancel'.

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

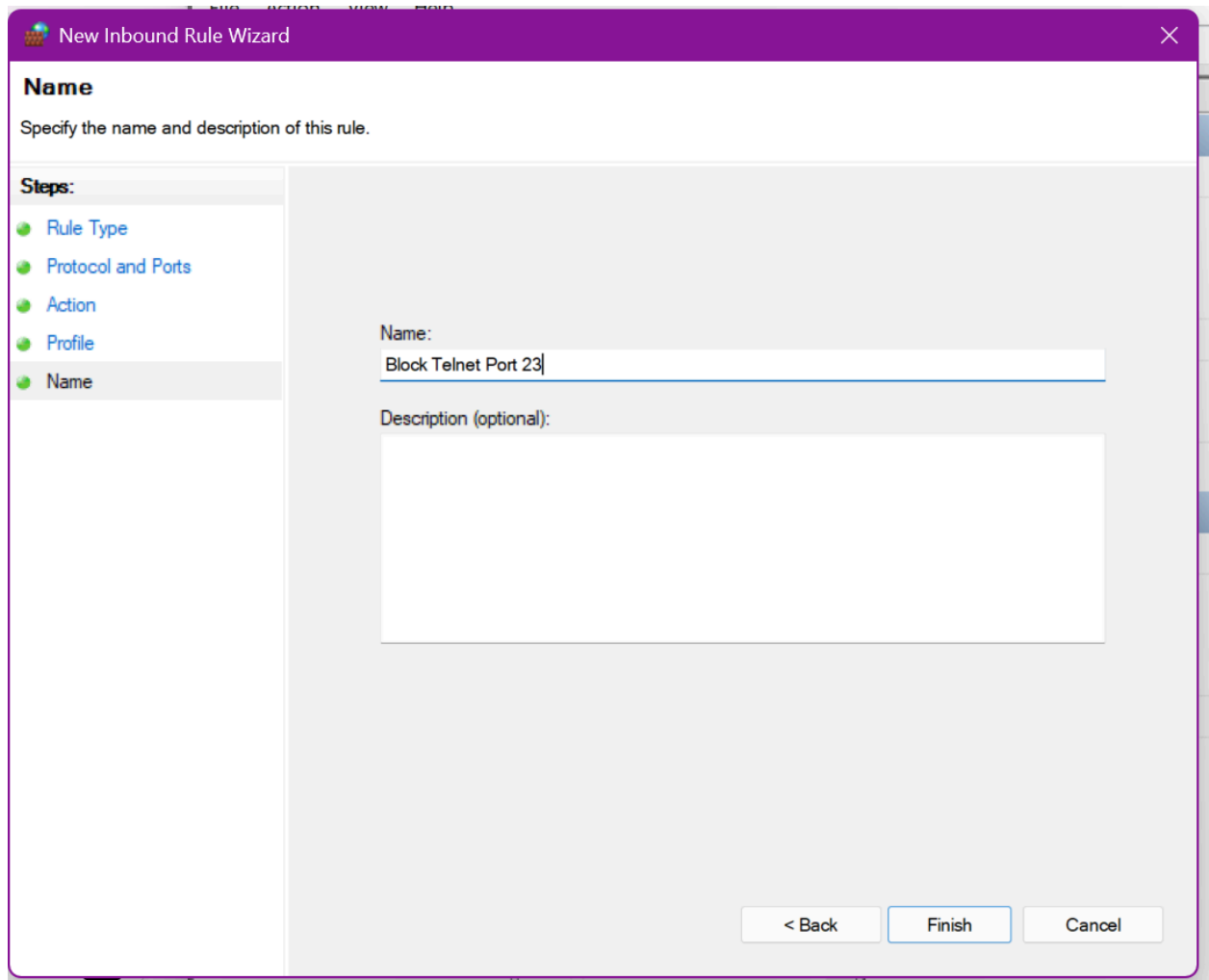
- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

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.

< Back Next > Cancel

f. Name it: **Block Telnet Port 23** → Click Finish.



The image shows the 'New Inbound Rule Wizard' dialog box in Windows Firewall. The 'Name' step is selected in the left-hand 'Steps' list. The main area contains a 'Name' field with the text 'Block Telnet Port 23' and an empty 'Description (optional)' text box. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'.

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

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

Name:
Block Telnet Port 23

Description (optional):

< Back Finish Cancel





4. Test the Rule

```
C:\Users\admin>telnet localhost 23
```












Connecting To localhost...Could not open connection to the host, on port 23: Connect failed

5. Remove the Test Rule

a. Go to Inbound Rules.

Inbound Rules								Acti
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Inbo
 Block Telnet Port 23		All	Yes	Block	No	Any	Any	
 Apache HTTP Server		Private	Yes	Allow	No	C:\xampp...	Any	
 Apache HTTP Server		Private	Yes	Allow	No	C:\xampp...	Any	
 Apache NetBeans IDE Launcher		Public	Yes	Allow	No	C:\progra...	Any	

b. Right-click on **Block Telnet Port 23** → Click Delete.

Inbound Rules							
Name	Group	Profile	Enabled	Action	Override	Program	Local Address
 Block Telnet Port 23		All	Yes	Block	No	Any	Any
 Apache HTTP Server		Private	Yes	Allow	No		
 Apache HTTP Server		Private	Yes	Allow	No		
 Apache NetBeans IDE Launcher		Public	Yes	Allow	No		
 Apache NetBeans IDE Launcher		Private	Yes	Allow	No		
 Apache NetBeans IDE Launcher		Public	Yes	Allow	No		
 Apache NetBeans IDE Launcher		Private	Yes	Allow	No		
 Java(TM) Platform SE binary		Public	Yes	Allow	No		
 Java(TM) Platform SE binary		Public	Yes	Allow	No		
 Java(TM) Platform SE binary		Private	Yes	Allow	No		
 Java(TM) Platform SE binary		Private	Yes	Allow	No		

- Disable Rule
- Cut
- Copy
- Delete
- Properties
- Help

c. Confirm.