

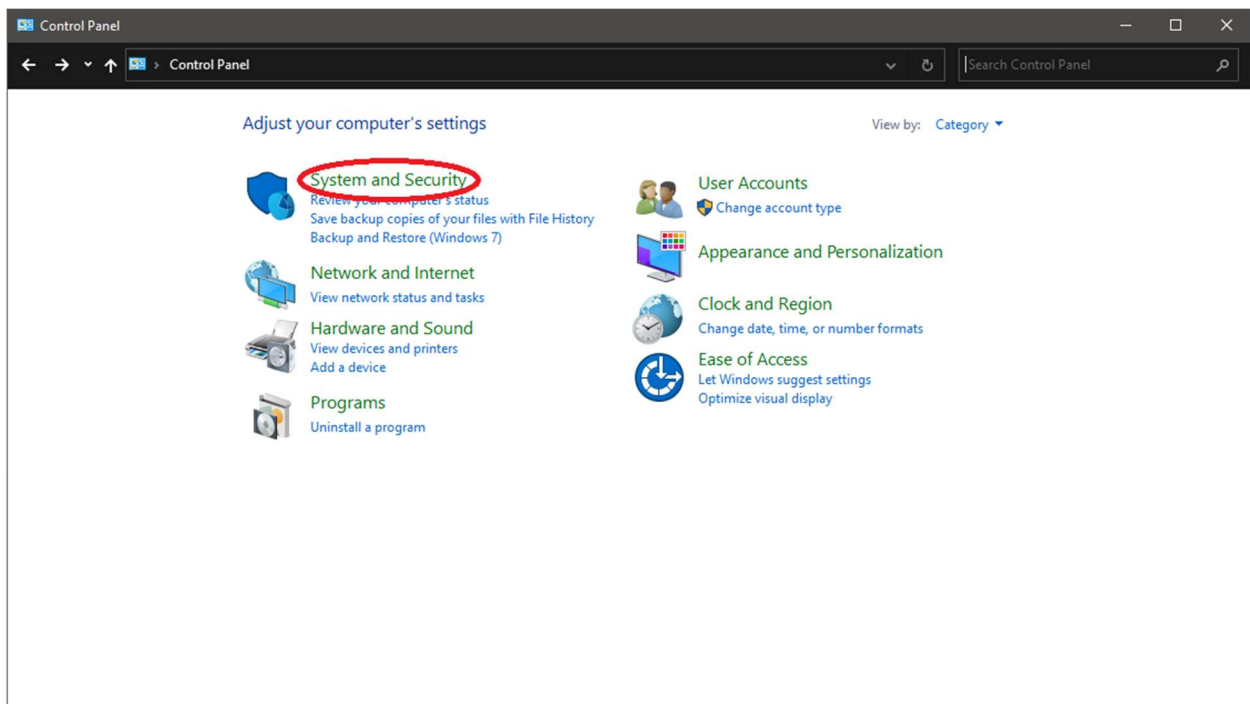
Opening XNS API Sample Subscriber Ports

When using the XNS API samples, your firewall may block results being sent from the XNS server to the subscribers in the sample. The subscribers sample uses port 8555 while the monitor for result sample uses port 8556. In the case that your firewall is blocking the results, you will have to open these ports on your computer so the server can send results to the XNS API samples program.

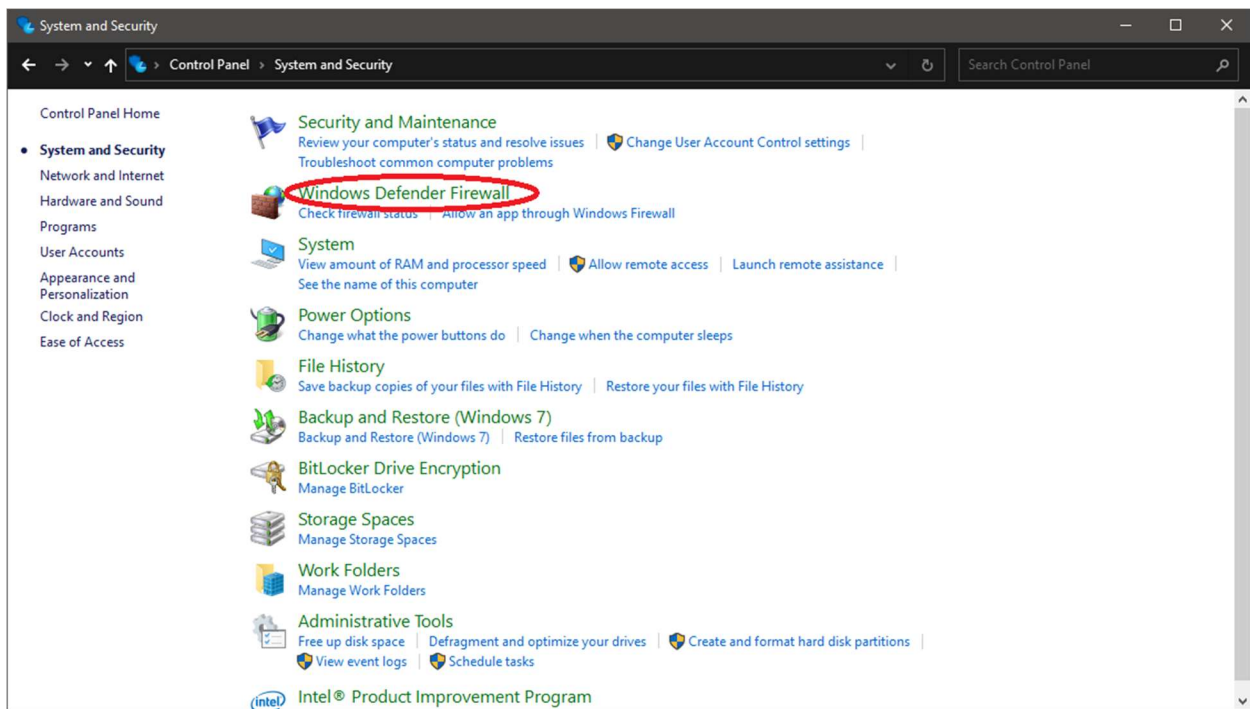
The following instructions show how to add a rule in the Windows Defender Firewall allowing the server to communicate with the XNS API Samples application. If you are using another firewall, you will similarly have to permit the server to communicate over ports 8555 and 8556 to your computer.

1. Go to the Windows Defender Firewall in the Control Panel.

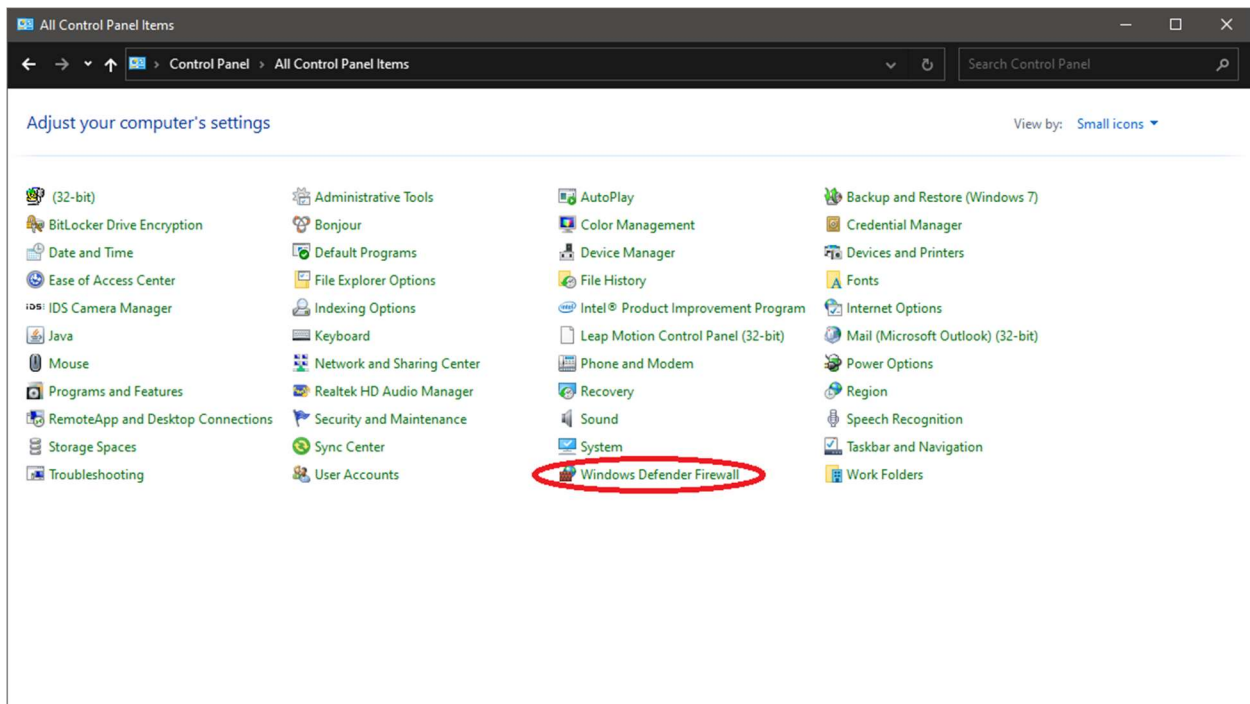
This can be done by opening the control panel and selecting “System and Security” > “Windows Defender Firewall” or just selecting “Windows Defender Firewall” depending on your control panel layout.



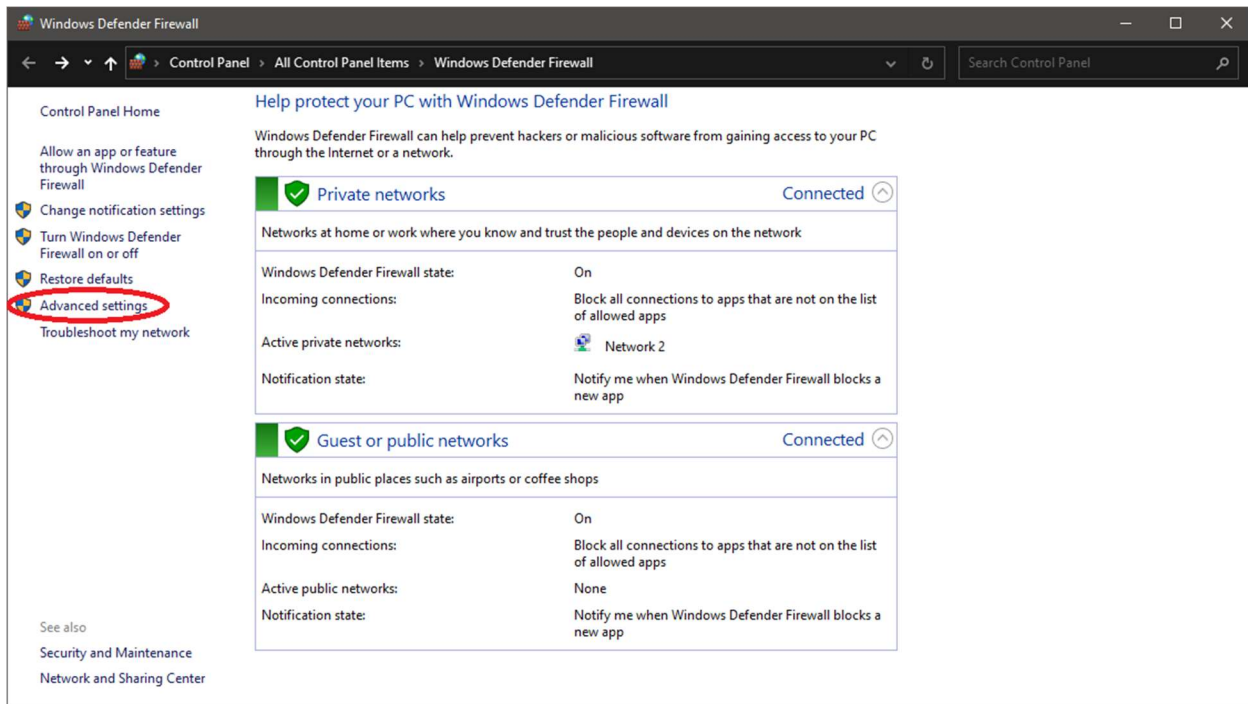
>



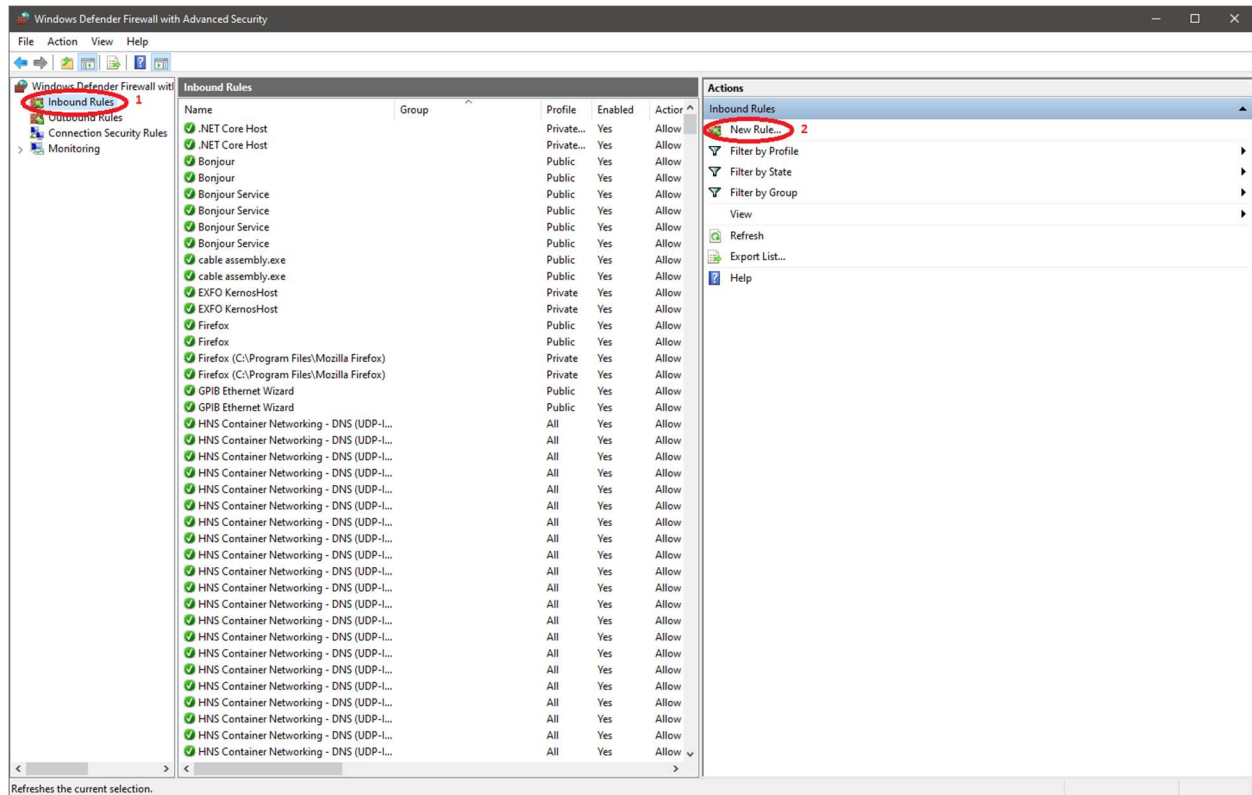
Or



2. In the Windows Defender Firewall, select “Advanced Settings”



3. In the Advanced Settings, select “Inbound Rules” and click “New Rule...”



4. In the Rule Type step, select “Custom” rule and click “Next”.

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

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

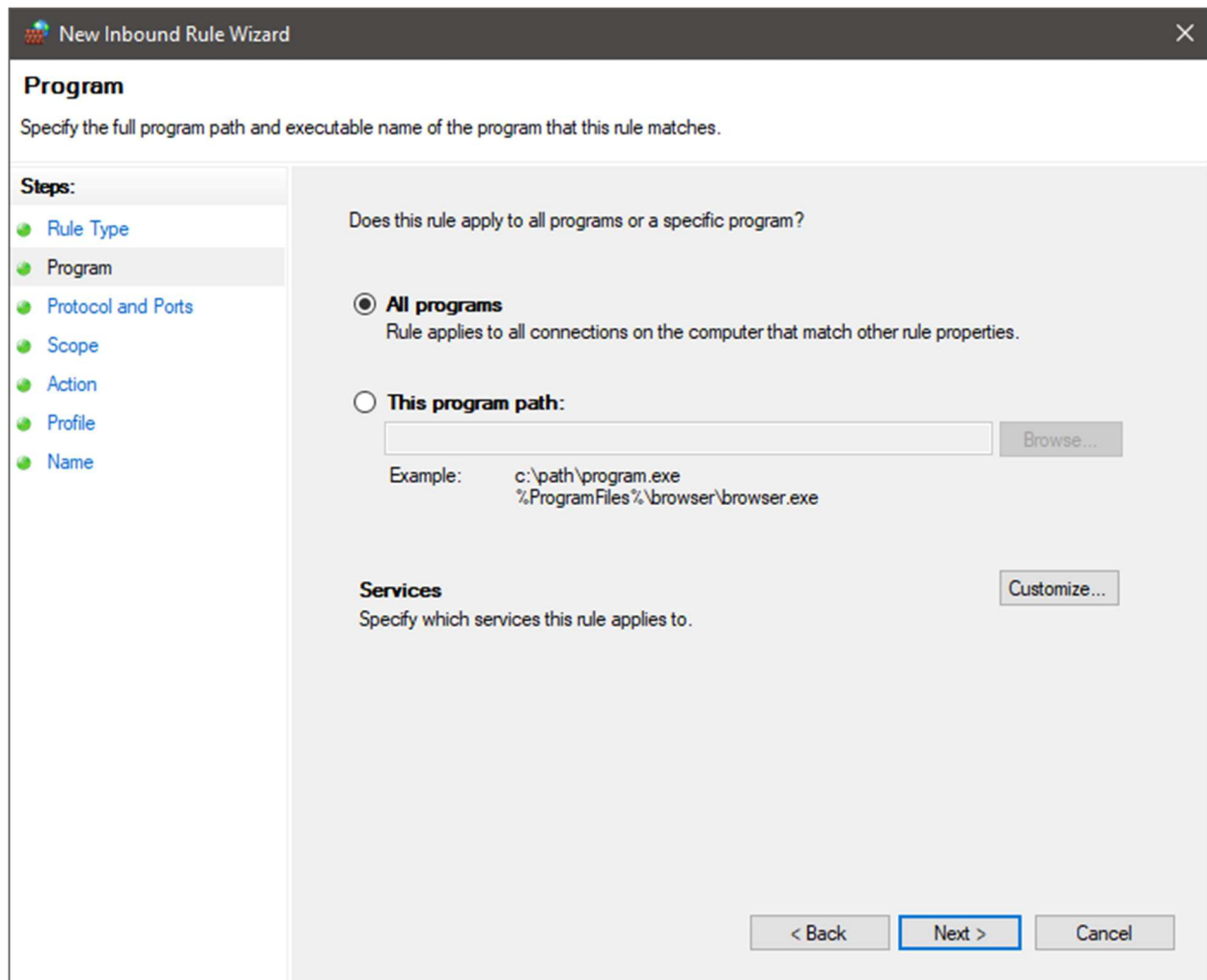
☐ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

☒ **Custom**
Custom rule.

< Back **Next >** Cancel

5. In the Program step, leave the Program selection as “All programs”. Alternatively, you could select just the XNS API Samples executable under “This program path”. Click “Next”.



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Program' step. The window has a title bar with the text 'New Inbound Rule Wizard' and a close button. The main content area is titled 'Program' and contains the instruction: 'Specify the full program path and executable name of the program that this rule matches.'

On the left side, there is a 'Steps:' pane with a list of steps: 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action', 'Profile', and 'Name'. The 'Program' step is currently selected and highlighted.

The main area of the wizard contains the following options:

- Does this rule apply to all programs or a specific program?**
 - ☒ **All programs**
Rule applies to all connections on the computer that match other rule properties.
 - ☐ **This program path:**
Below this option is a text input field and a 'Browse...' button. Below the input field, there are example paths:
Example: c:\path\program.exe
 %ProgramFiles%\browser\browser.exe
- Services**
Specify which services this rule applies to.
To the right of this section is a 'Customize...' button.

At the bottom of the wizard, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

6. In the Protocol and Ports step, select “TCP” for the “Protocol type”. Select “Specific Ports” for the “Local Port” and enter “8555,8556” for the ports. Click “Next”.

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

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

To which ports and protocols does this rule apply?

Protocol type: TCP

Protocol number: 6

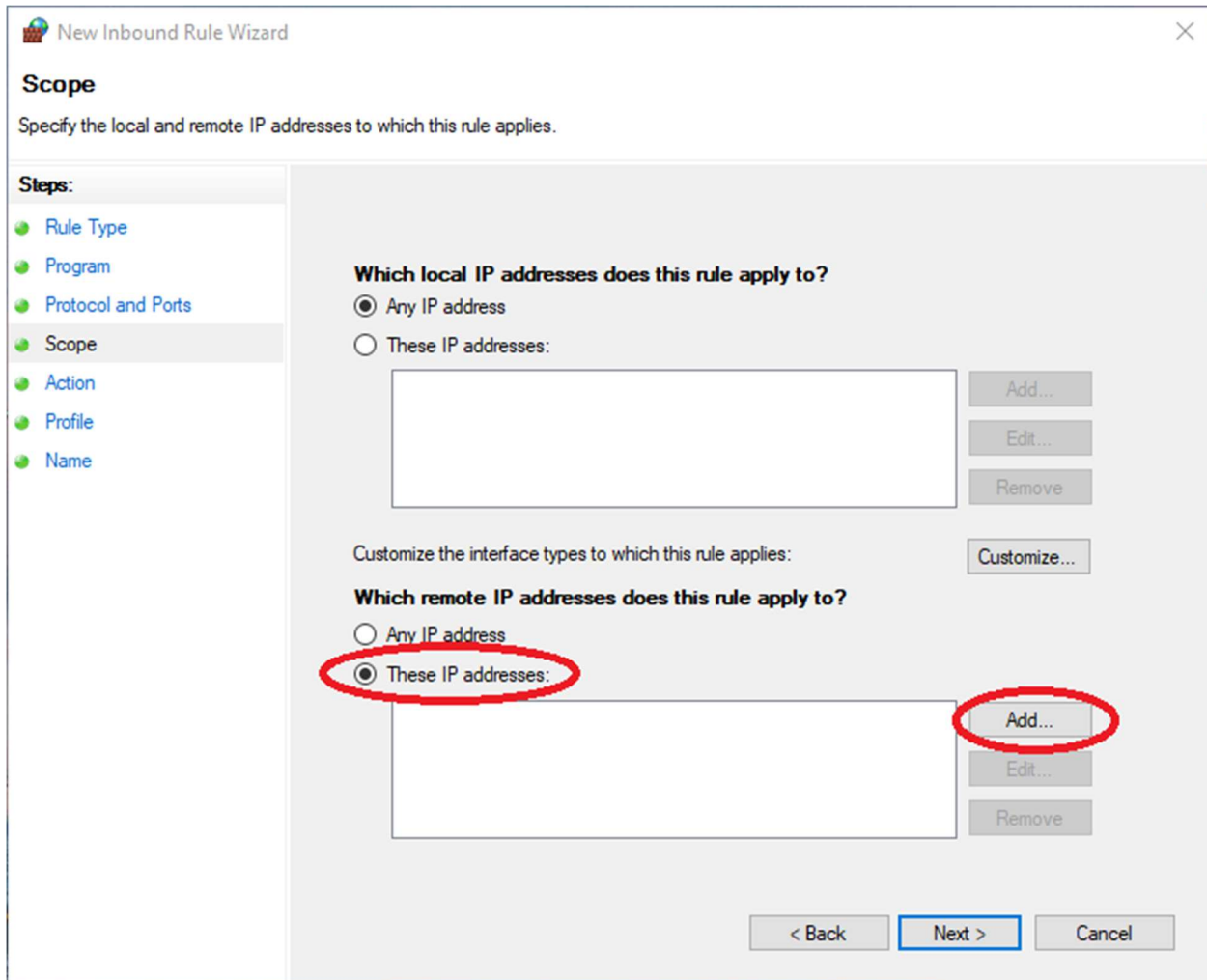
Local port: Specific Ports
8555,8556
Example: 80, 443, 5000-5010

Remote port: All Ports
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

< Back Next > Cancel

7. In the Scope step, select "These IP addresses:" for "Which remote IP address does this rule apply to?" and click "Add..."



The image shows the 'New Inbound Rule Wizard' window, specifically the 'Scope' step. The window title is 'New Inbound Rule Wizard'. The main heading is 'Scope', and the instruction is 'Specify the local and remote IP addresses to which this rule applies.' On the left, a 'Steps:' sidebar lists: Rule Type, Program, Protocol and Ports, Scope (highlighted), Action, Profile, and Name. The main area contains two sections. The first section, 'Which local IP addresses does this rule apply to?', has two radio buttons: 'Any IP address' (selected) and 'These IP addresses:'. Below the second radio button is an empty text box and three buttons: 'Add...', 'Edit...', and 'Remove'. The second section, 'Which remote IP addresses does this rule apply to?', also has two radio buttons: 'Any IP address' and 'These IP addresses:'. The 'These IP addresses:' radio button is circled in red. Below it is another empty text box and three buttons: 'Add...', 'Edit...', and 'Remove'. The 'Add...' button in this section is also circled in red. Between the two sections is a line of text: 'Customize the interface types to which this rule applies:' followed by a 'Customize...' button. At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

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

Which local IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

Which remote IP addresses does this rule apply to?

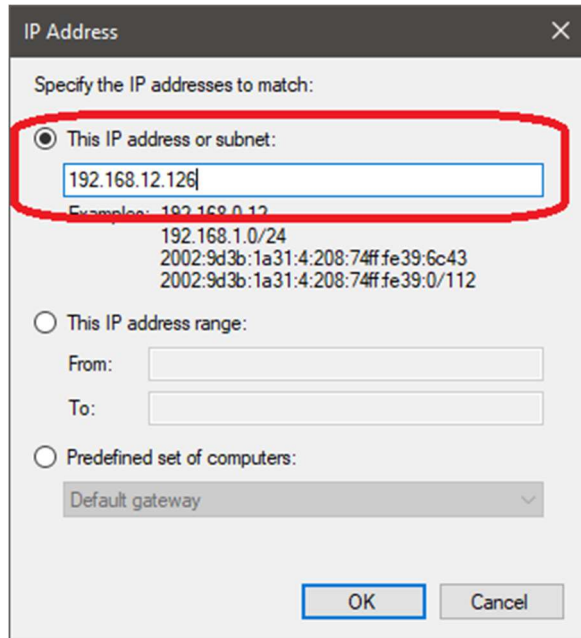
☐ Any IP address

☒ These IP addresses:

Add... Edit... Remove

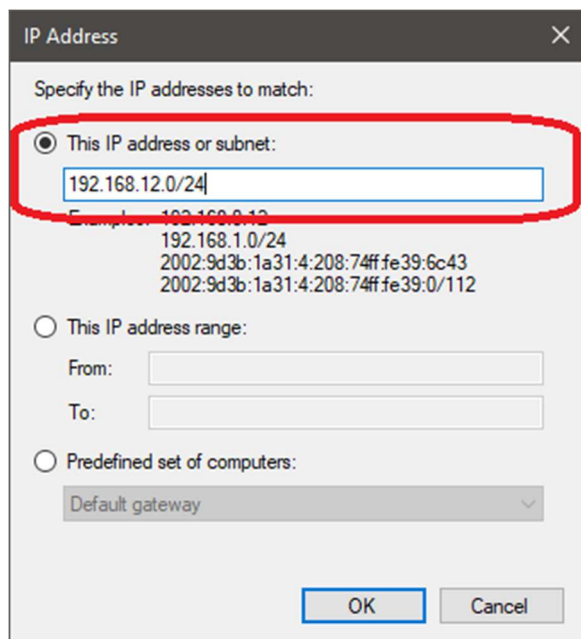
< Back Next > Cancel

8. In the IP Address dialog, select “This IP address or subnet”. You can either enter the exact IP address of your XNS server or just specify the subnet of the XNS server (useful if you want to use the XNS API samples with multiple servers on the same subnet). In the example, our XNS has an IP address of 192.168.12.126. However, we have multiple XNS servers all on the 192.168.12.0/24 subnet so we choose to specify the subnet. Click “OK”.



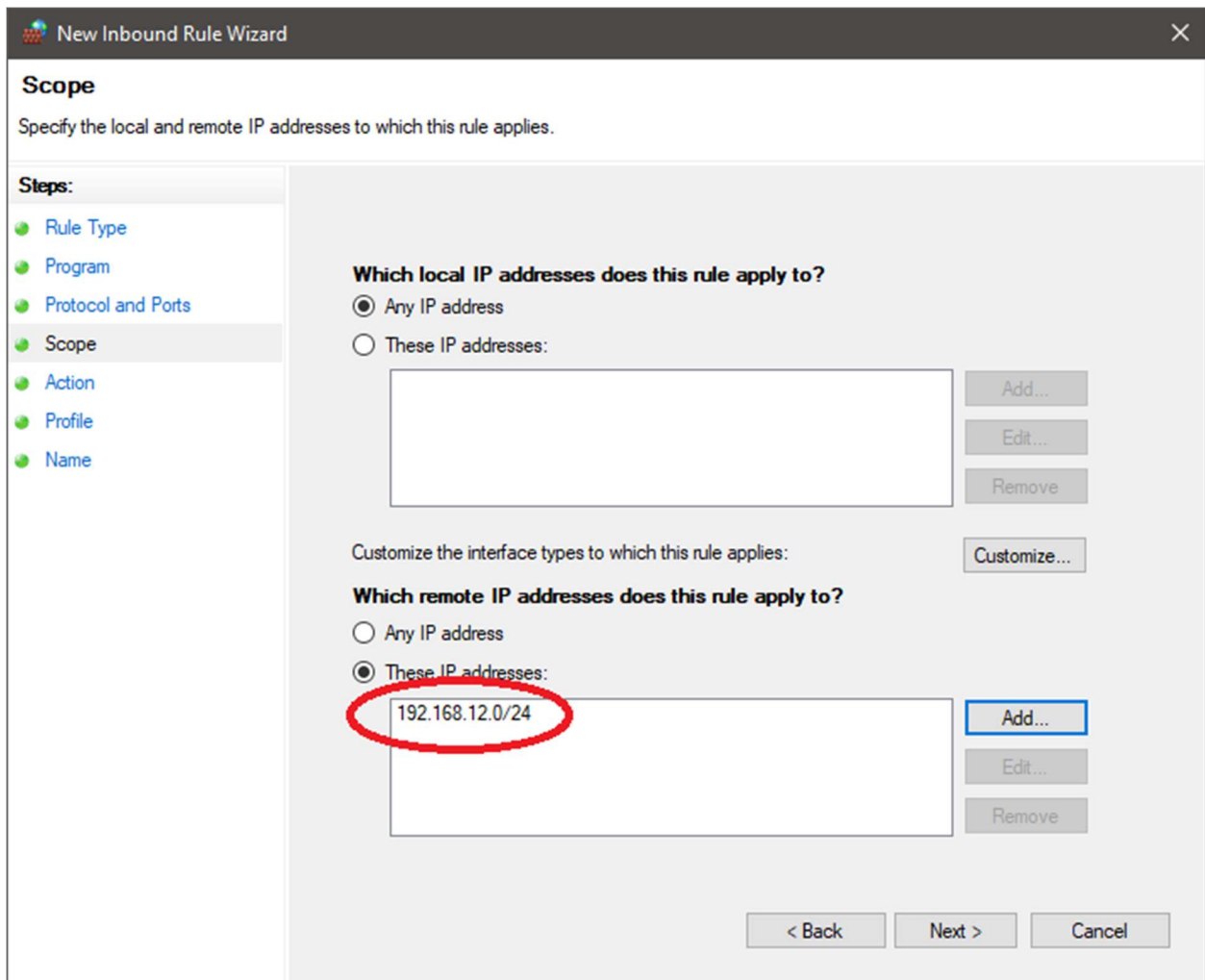
The IP Address dialog box is shown with the title bar 'IP Address' and a close button. The instruction 'Specify the IP addresses to match:' is at the top. The first radio button, 'This IP address or subnet:', is selected and circled in red. Below it, the text '192.168.12.126' is entered in the text field. Underneath the text field, the text 'Examples: 192.168.0.12' is followed by three lines of example addresses: '192.168.1.0/24', '2002:9d3b:1a31:4:208:74ff:fe39:6c43', and '2002:9d3b:1a31:4:208:74ff:fe39:0/112'. The second radio button, 'This IP address range:', is unselected and has two empty text fields labeled 'From:' and 'To:'. The third radio button, 'Predefined set of computers:', is unselected and has a dropdown menu showing 'Default gateway'. At the bottom are 'OK' and 'Cancel' buttons.

Or



The IP Address dialog box is shown with the title bar 'IP Address' and a close button. The instruction 'Specify the IP addresses to match:' is at the top. The first radio button, 'This IP address or subnet:', is selected and circled in red. Below it, the text '192.168.12.0/24' is entered in the text field. Underneath the text field, the text 'Examples: 192.168.0.12' is followed by three lines of example addresses: '192.168.1.0/24', '2002:9d3b:1a31:4:208:74ff:fe39:6c43', and '2002:9d3b:1a31:4:208:74ff:fe39:0/112'. The second radio button, 'This IP address range:', is unselected and has two empty text fields labeled 'From:' and 'To:'. The third radio button, 'Predefined set of computers:', is unselected and has a dropdown menu showing 'Default gateway'. At the bottom are 'OK' and 'Cancel' buttons.

9. The IP address or subnet you entered should now be listed. Click “Next”.



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Scope' step. The window has a dark title bar with the text 'New Inbound Rule Wizard' and a close button. Below the title bar, the word 'Scope' is displayed in bold. A subtitle reads 'Specify the local and remote IP addresses to which this rule applies.' On the left side, there is a 'Steps:' panel with a list of steps: 'Rule Type', 'Program', 'Protocol and Ports', 'Scope' (which is highlighted), 'Action', 'Profile', and 'Name'. The main area of the wizard is divided into two sections. The first section is titled 'Which local IP addresses does this rule apply to?' and contains two radio buttons: 'Any IP address' (selected) and 'These IP addresses:'. Below the 'These IP addresses:' radio button is a large empty text box. To the right of this box are three buttons: 'Add...', 'Edit...', and 'Remove'. Below this section is a line of text: 'Customize the interface types to which this rule applies:' followed by a 'Customize...' button. The second section is titled 'Which remote IP addresses does this rule apply to?' and contains two radio buttons: 'Any IP address' and 'These IP addresses:'. The 'These IP addresses:' radio button is selected. Below it is a text box containing the IP address '192.168.12.0/24', which is circled in red. To the right of this box are three buttons: 'Add...' (highlighted with a blue border), 'Edit...', and 'Remove'. At the bottom right of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

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

Which local IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

Which remote IP addresses does this rule apply to?

☐ Any IP address

☒ These IP addresses:

192.168.12.0/24

Add... Edit... Remove

< Back Next > Cancel

10. In the Action step, leave the action selection as “Allow the connection”. Click “Next”.

The screenshot shows the 'New Inbound Rule Wizard' window. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Action'. Below it, a subtitle says 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' sidebar lists: Rule Type, Program, Protocol and Ports, Scope, Action (highlighted), Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?'. It has three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those are not.' The 'Allow the connection if it is secure' option has 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.' Below this is a 'Customize...' button. At the bottom right are '< Back', 'Next >' (highlighted with a blue border), and 'Cancel' buttons.

Action

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

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- 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.

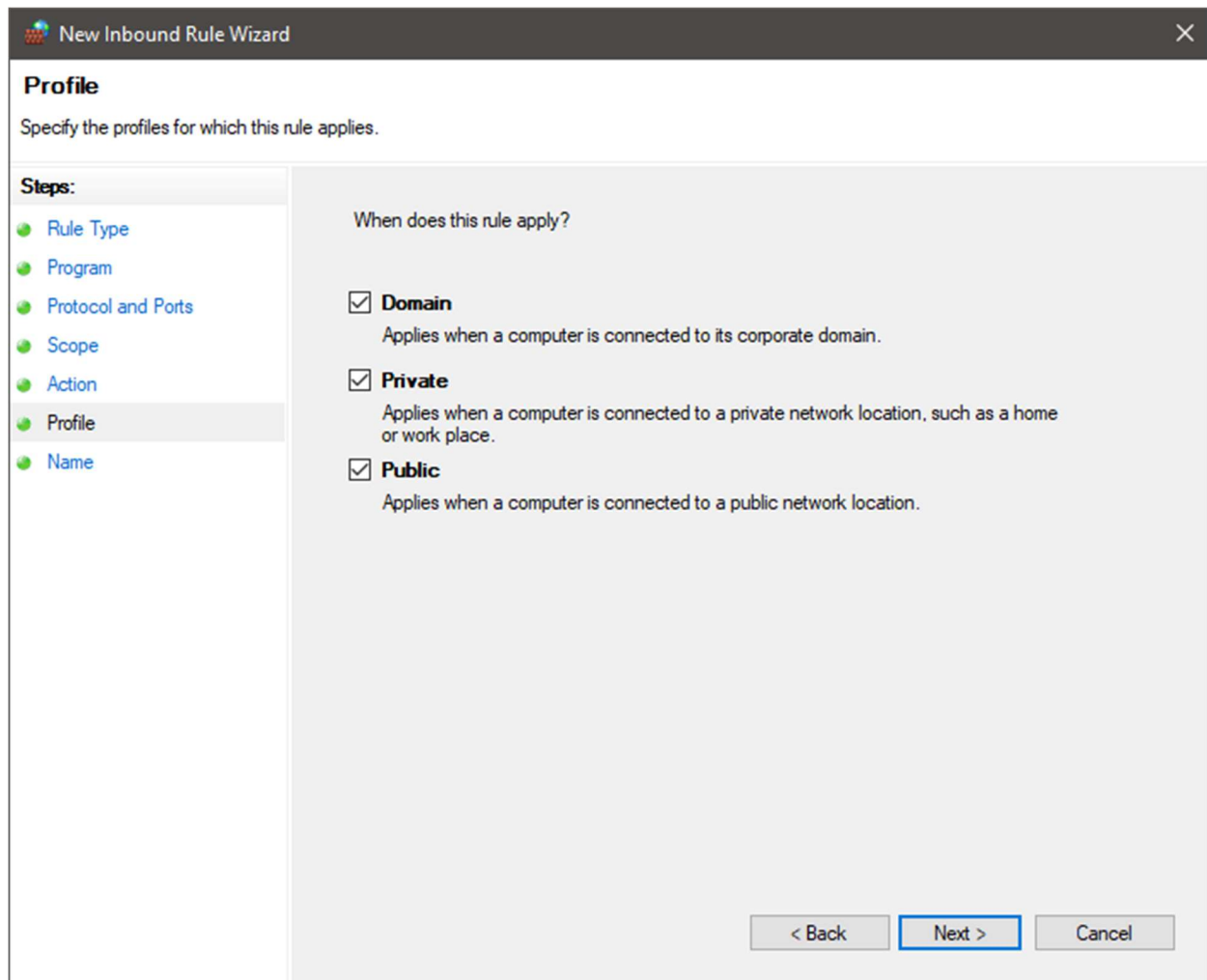
☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Customize...

☐ **Block the connection**

< Back **Next >** Cancel

11. In the Profile selection, leave “Domain”, “Private”, and “Public” selected. Alternatively, select only the type of network profile you are on. Click “Next”.



The image shows a Windows Firewall 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The window title is 'New Inbound Rule Wizard' with a close button (X) in the top right corner. Below the title bar, the section is labeled 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list contains: Rule Type, Program, Protocol and Ports, Scope, Action, Profile (highlighted), and Name. The main area, titled 'When does this rule apply?', contains three checked options: '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 are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

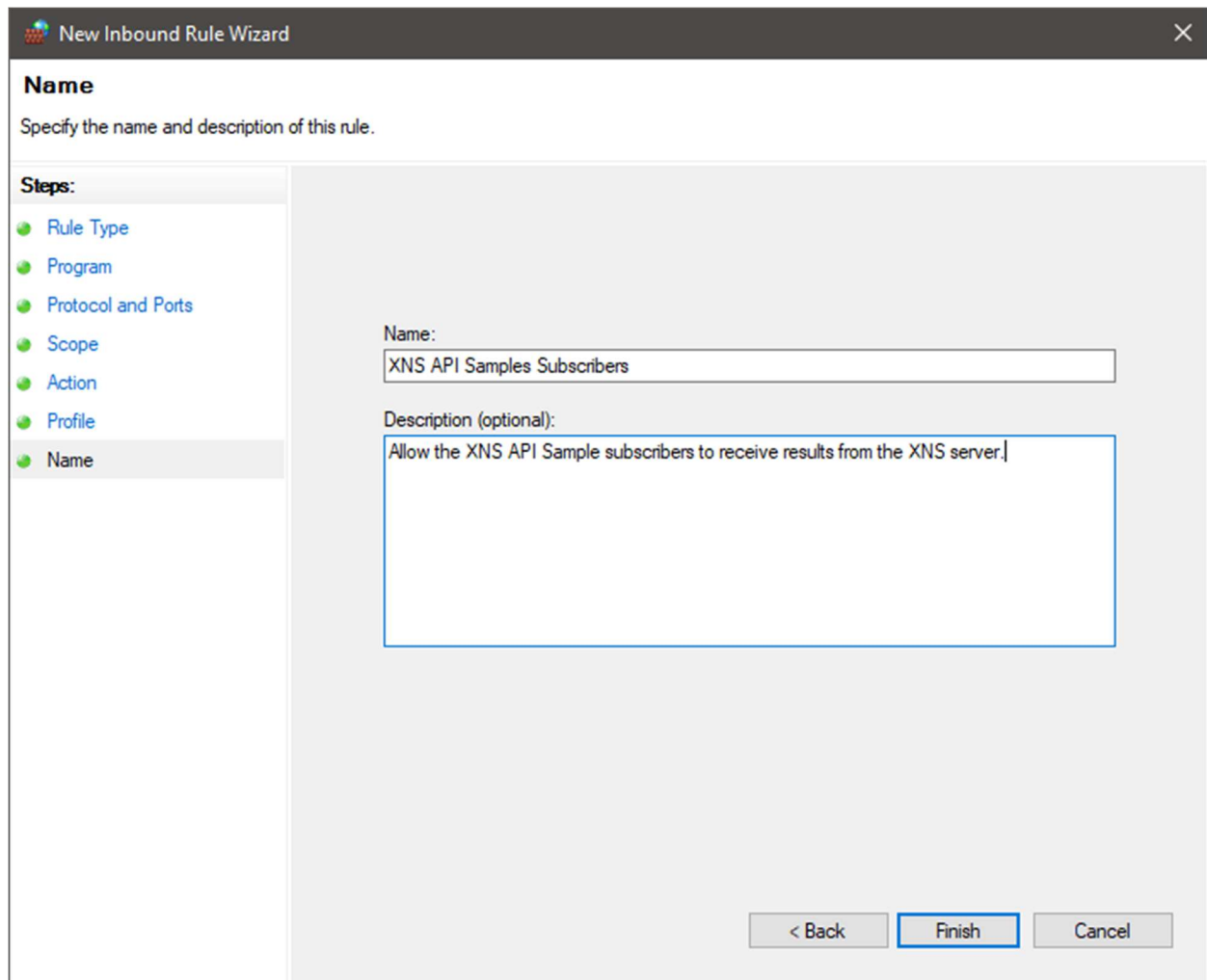
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile**
- Name

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

12. Add a name and optional description for the rule. Click “Finish”.



The image shows a 'New Inbound Rule Wizard' dialog box. The title bar reads 'New Inbound Rule Wizard' with a close button. The main area is titled 'Name' and contains the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action', 'Profile', and 'Name', with 'Name' selected. The main content area has a 'Name:' label above a text box containing 'XNS API Samples Subscribers'. Below this is a 'Description (optional):' label above a larger text box containing 'Allow the XNS API Sample subscribers to receive results from the XNS server.' At the bottom right are three buttons: '< Back', 'Finish' (highlighted with a blue border), and 'Cancel'.

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

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

Name:

XNS API Samples Subscribers

Description (optional):

Allow the XNS API Sample subscribers to receive results from the XNS server.

< Back **Finish** Cancel