Connecting Green Check to BioTrack

In order to set up automatic sales data ingestion between BioTrack and Green Check we'll need to make sure that the port 5432 is opened to the Green Check servers. Here are some steps that may be needed to ensure that these software can communicate with each other. Please be aware that in our "Windows Firewall" section, we are only allowing the Green Check Verified servers to connect to the computer that is running the BioTrack server. If you need to open the port to additional third parties, you will need to open the rule to specify their IP addresses alongside the Green Check ones.

Port Forwarding

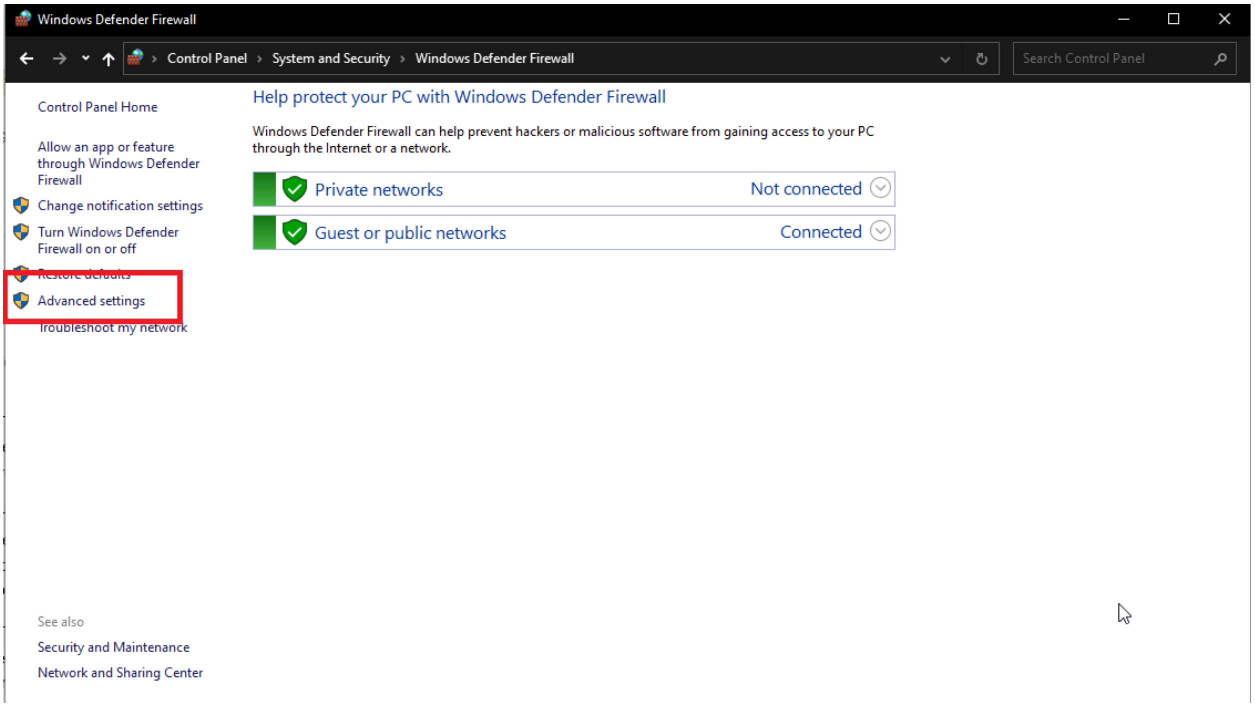
First, you'll need to tell the router where to route traffic requests made to port 5432 and which server should answer that request.

Steps may vary based on the manufacturer of the router you are using, but this guide should cover the basics: https://portforward.com/how-to-port-forward/

Windows Firewall

Then, you'll need to open the port 5432 to the Green Check IP Addresses. The following steps need to be followed on the computer where the BioTrack server is installed.

Open the Windows Defender Firewall settings and on the left side of the screen click **Advanced settings**.


Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

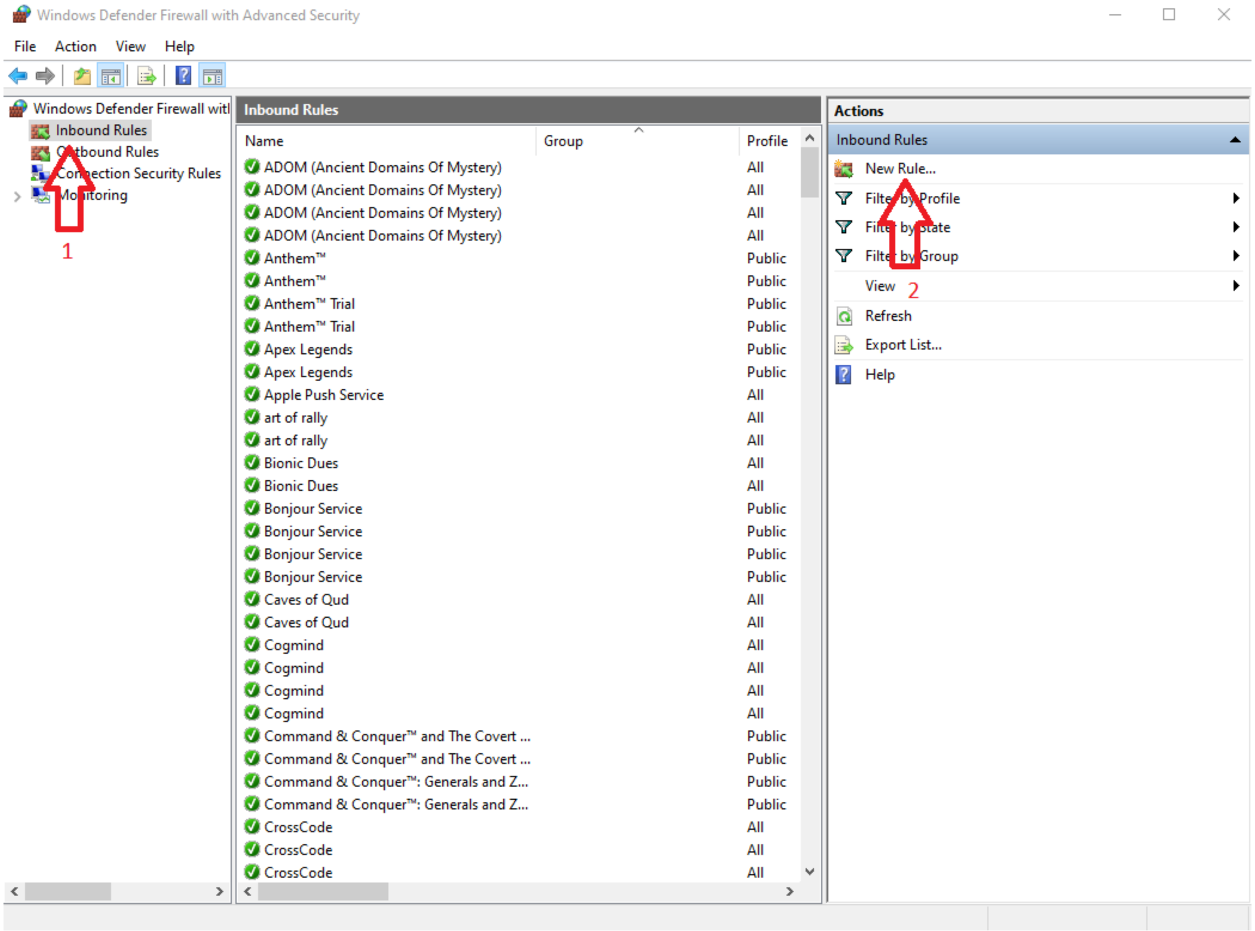
Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

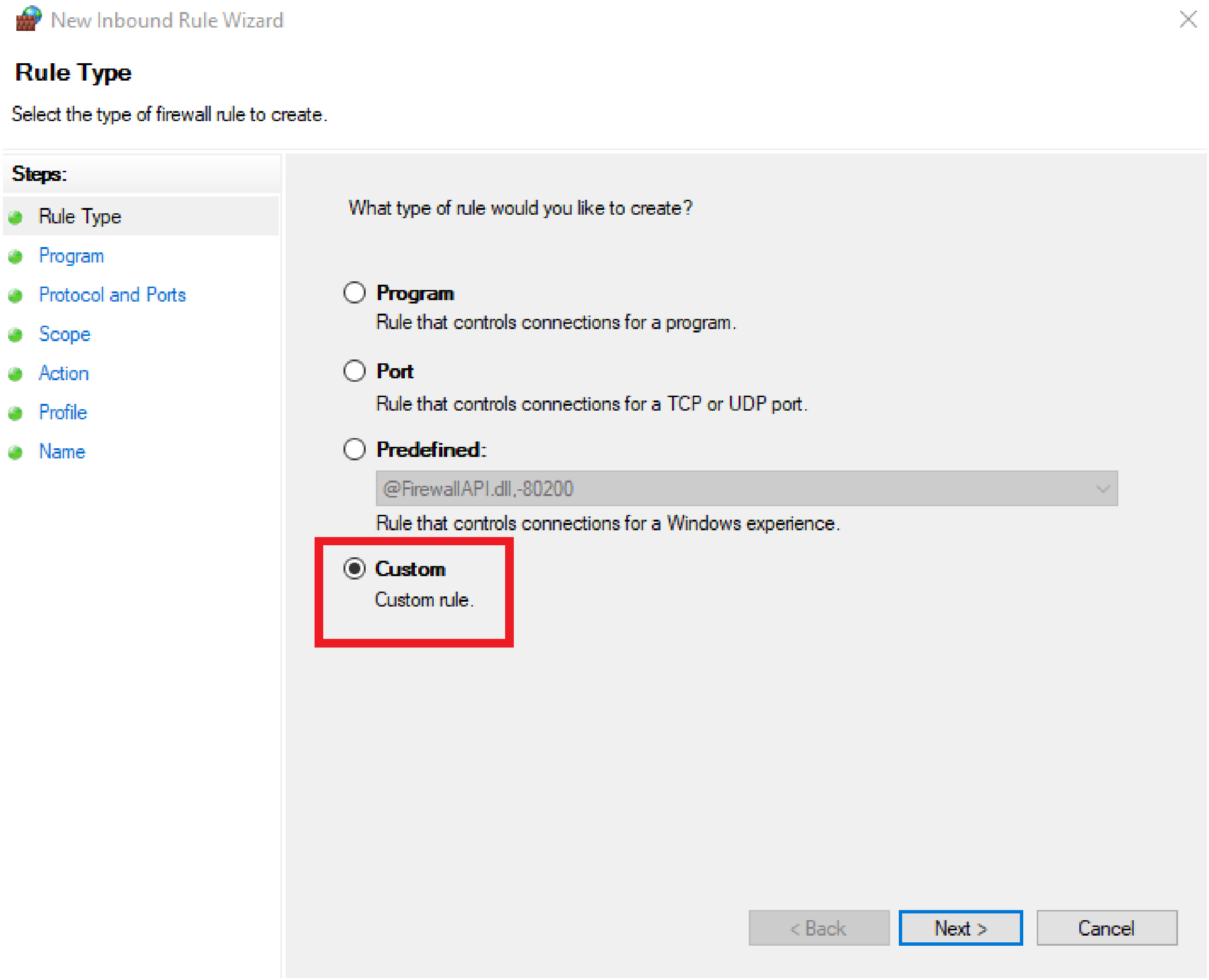
Guest or public networks — Connected

Select **Inbound Rules** on the left and then select **New Rule** on the right.



Name	Group	Profile
ADOM (Ancient Domains Of Mystery)		All
ADOM (Ancient Domains Of Mystery)		All
ADOM (Ancient Domains Of Mystery)		All
ADOM (Ancient Domains Of Mystery)		All
Anthem™		Public
Anthem™		Public
Anthem™ Trial		Public
Anthem™ Trial		Public
Apex Legends		Public
Apex Legends		Public
Apple Push Service		All
art of rally		All
art of rally		All
Bionic Dues		All
Bionic Dues		All
Bonjour Service		Public
Bonjour Service		Public
Bonjour Service		Public
Bonjour Service		Public
Caves of Qud		All
Caves of Qud		All
Cogmind		All
Cogmind		All
Cogmind		All
Cogmind		All
Command & Conquer™ and The Covert ...		Public
Command & Conquer™ and The Covert ...		Public
Command & Conquer™: Generals and Z...		Public
Command & Conquer™: Generals and Z...		Public
CrossCode		All
CrossCode		All
CrossCode		All

Select the **Custom rule** option 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?

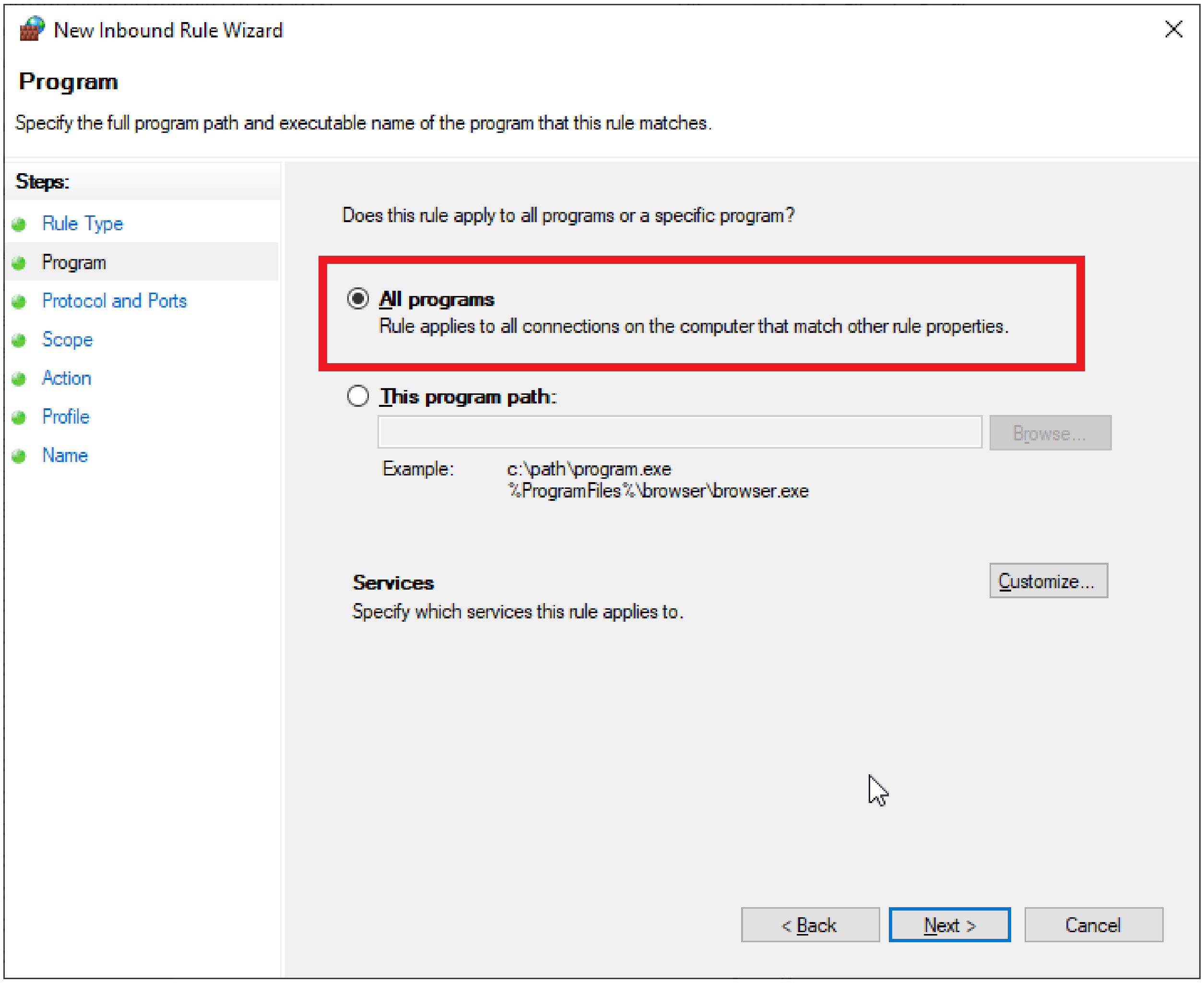
○ **Program**
Rule that controls connections for a program.

○ **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.

Select the **All programs** option and click **Next**.



New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Does this rule apply to all programs or a specific program?

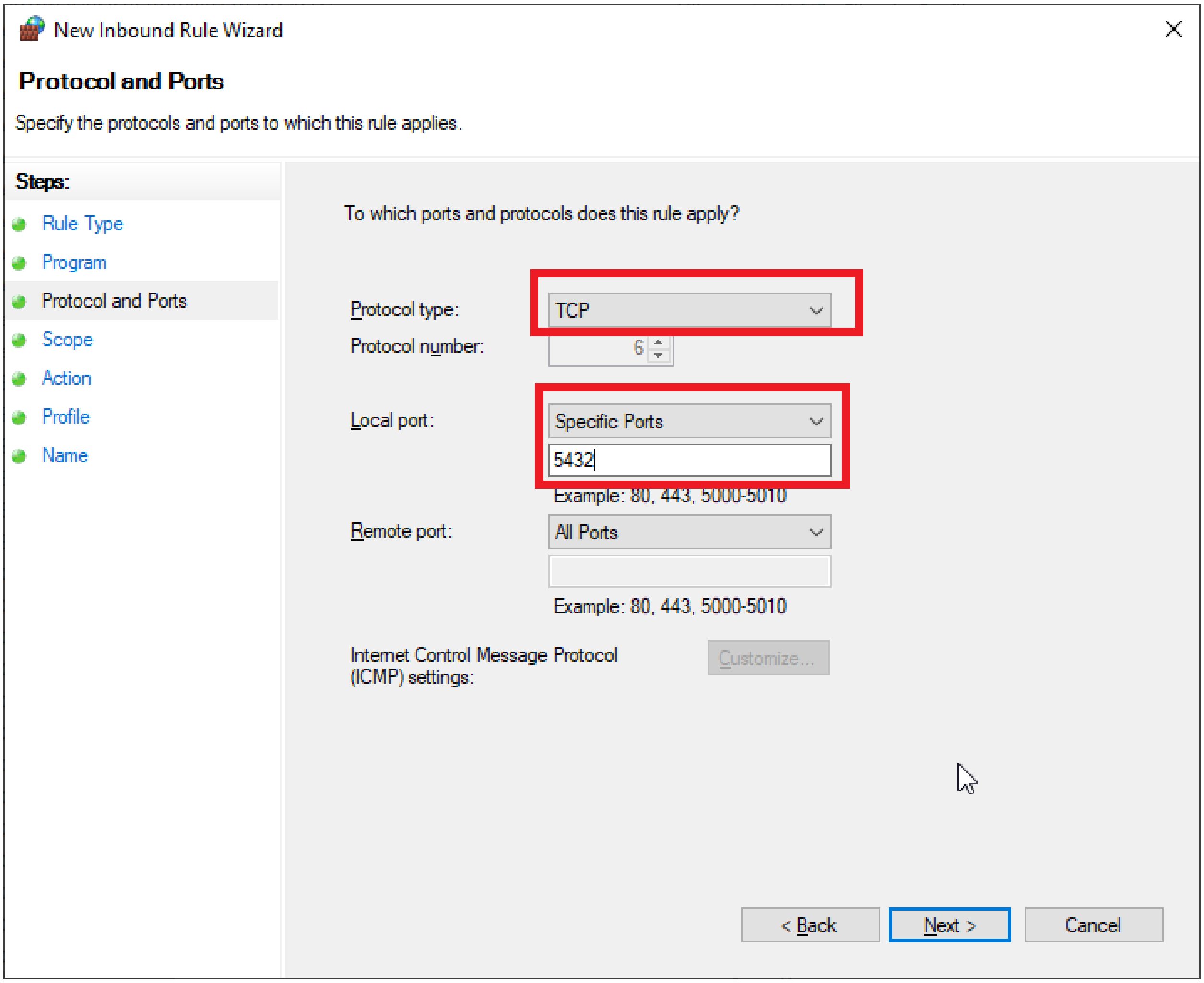
● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

Change the Protocol type to **TCP** and the Local Port to **Specific Ports** and enter **5432**.



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

5432

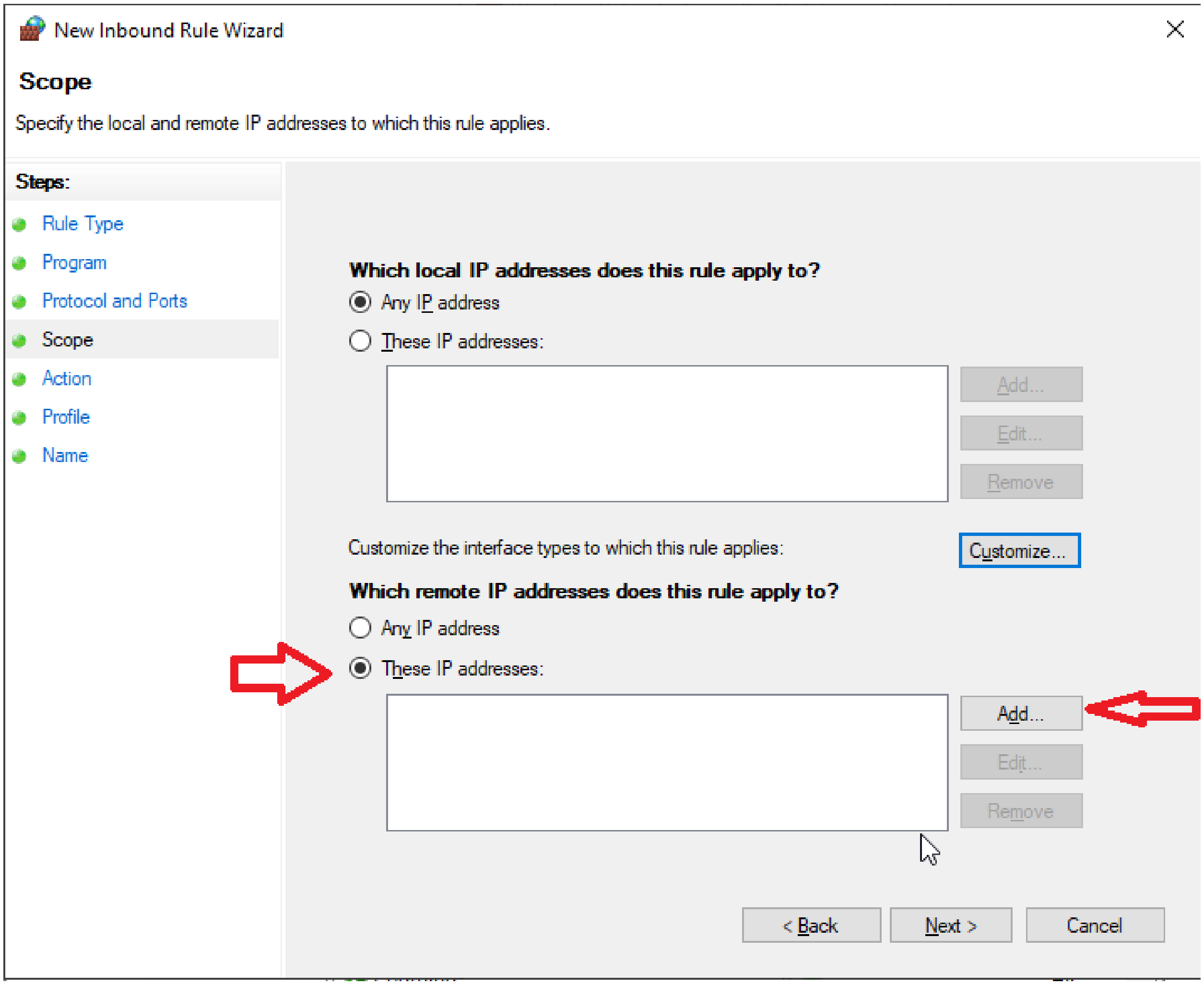
Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

Click **These IP addresses** under Which remote IP address and then click the **Add** button.



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:

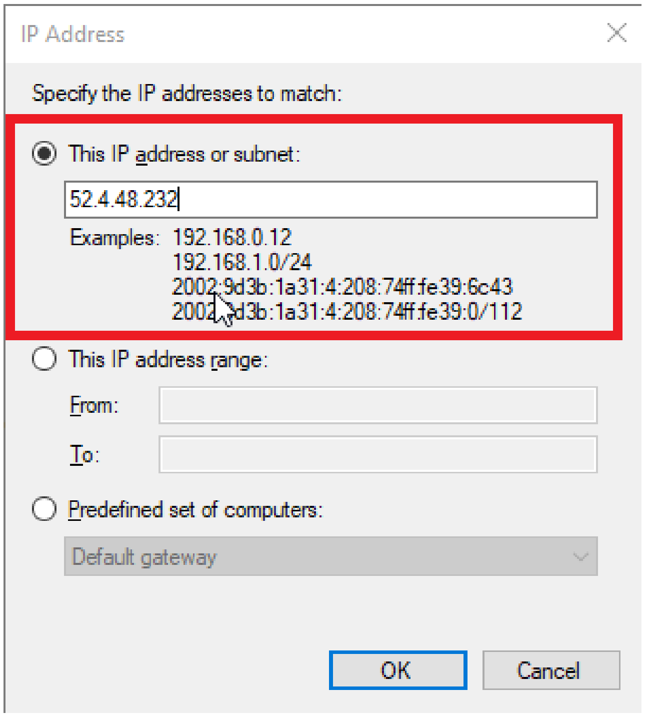
Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

We need to add both of the Green Check IP addresses separately: **52.4.48.232** and **35.169.209.100**.



IP Address

Specify the IP addresses to match:

● This IP address or subnet:

52.4.48.232

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

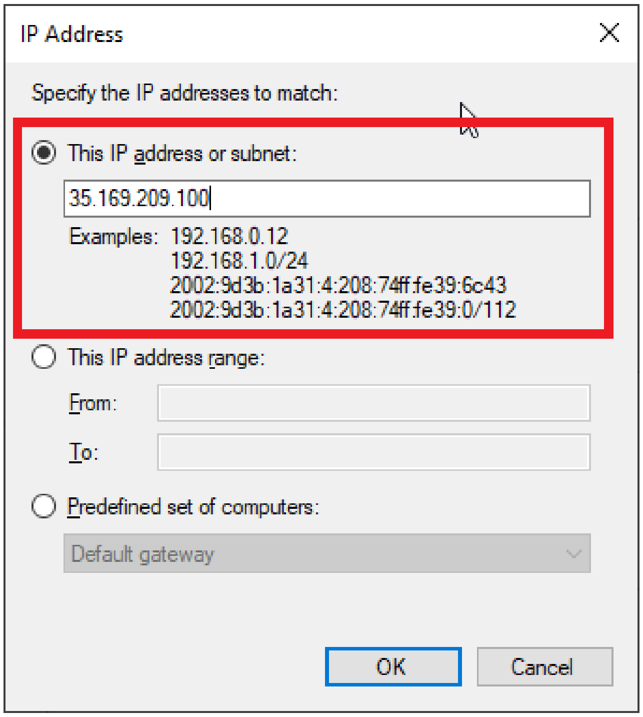
○ This IP address range:

From:

To:

○ Predefined set of computers:

Default gateway



IP Address

Specify the IP addresses to match:

● This IP address or subnet:

35.169.209.100

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:

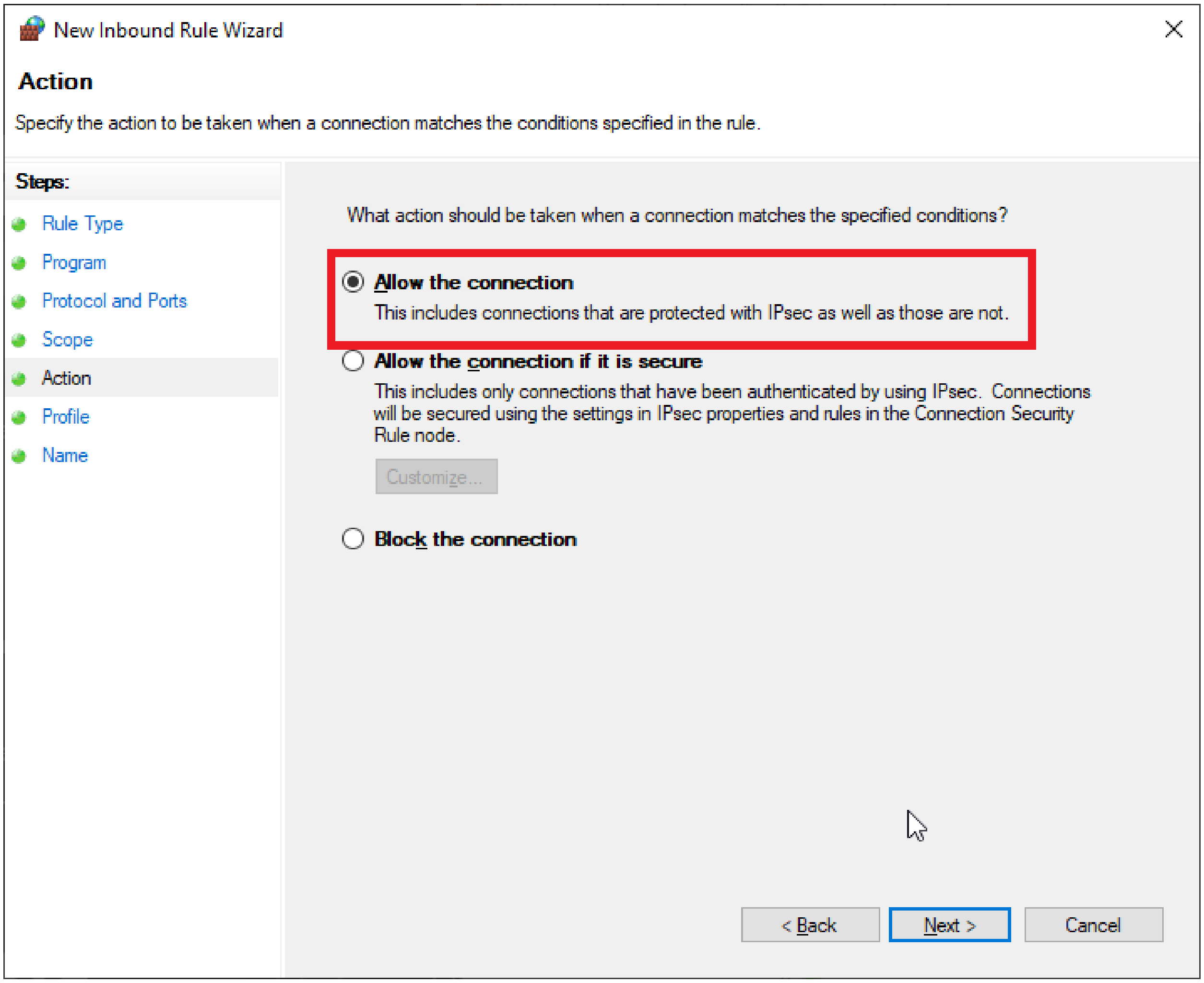
From:

To:

○ Predefined set of computers:

Default gateway

Select **Allow the connection**.



New Inbound Rule Wizard

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

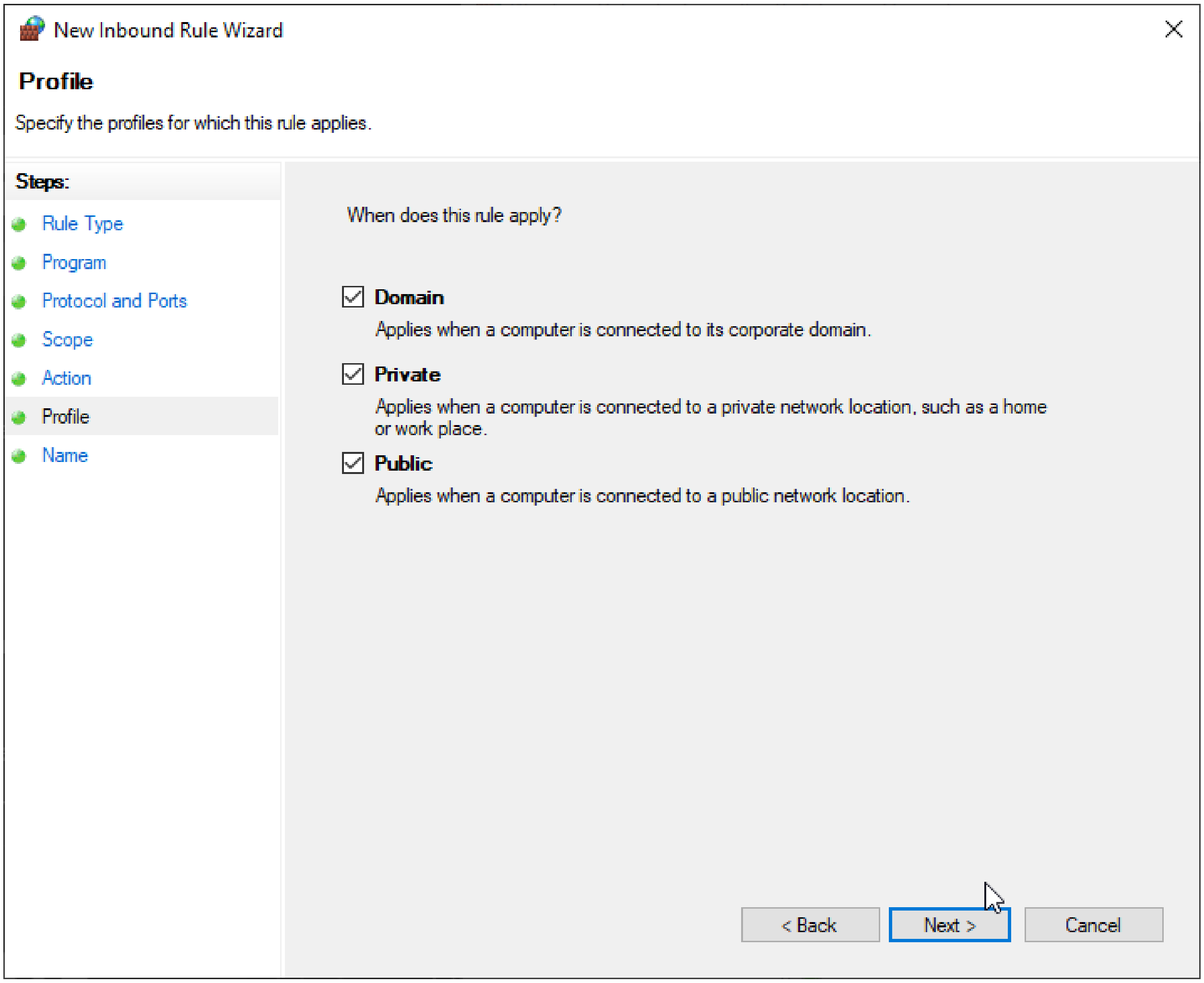
What action should be taken when a connection matches the specified conditions?

● 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.

○ Block the connection

Select **all three checkboxes**.



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.

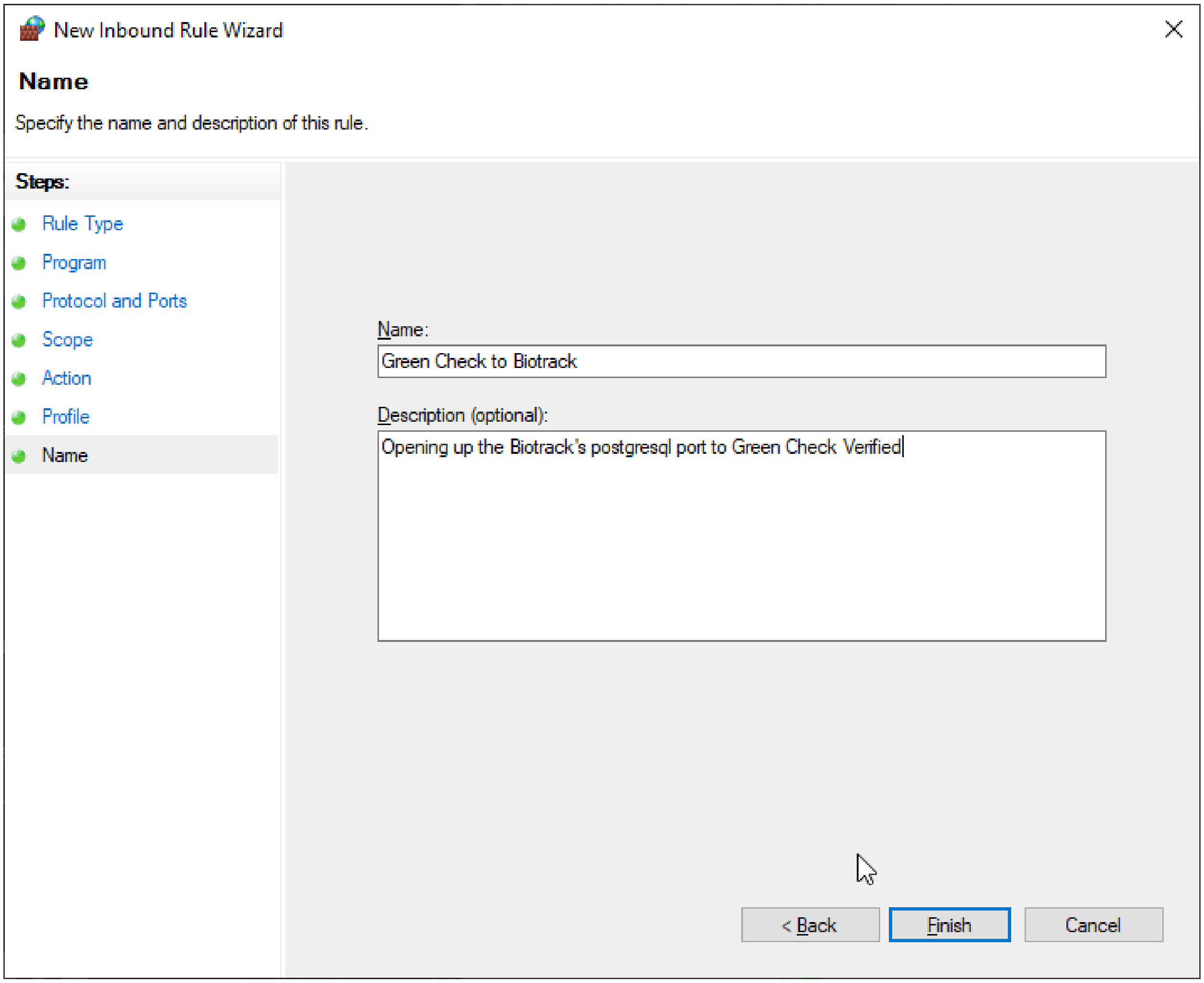
☑ **Private**

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.

Give the rule a **Name** and click **Finish**.



Name

Specify the name and description of this rule.

Name: Green Check to Biotrack

Description (optional): Opening up the Biotrack's postgresql port to Green Check Verified