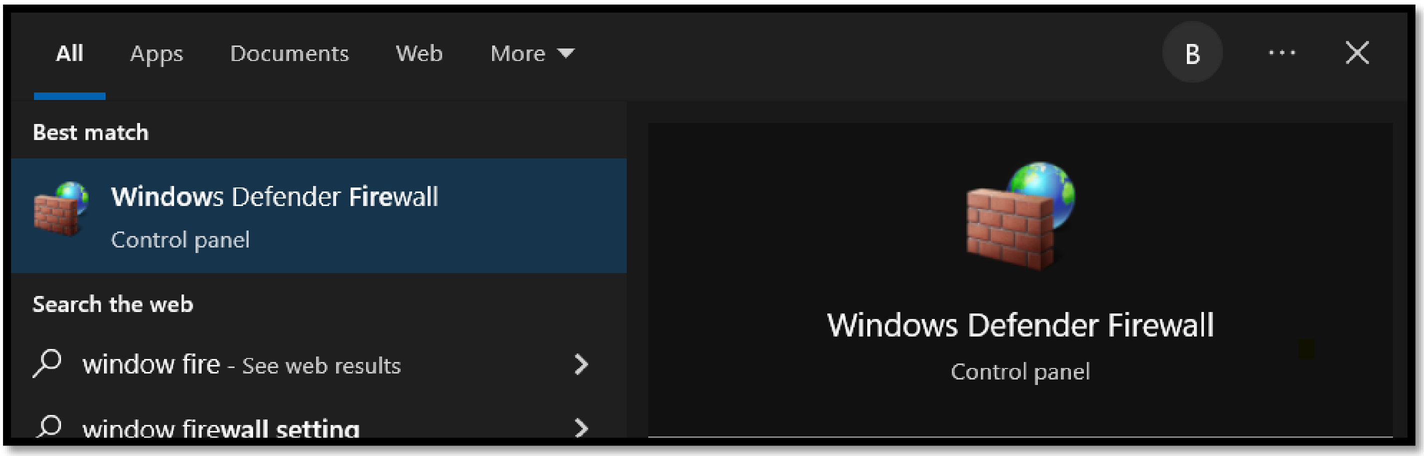
Practical No. 8

Aim: Firewall Configuration and Rule-based Filtering:

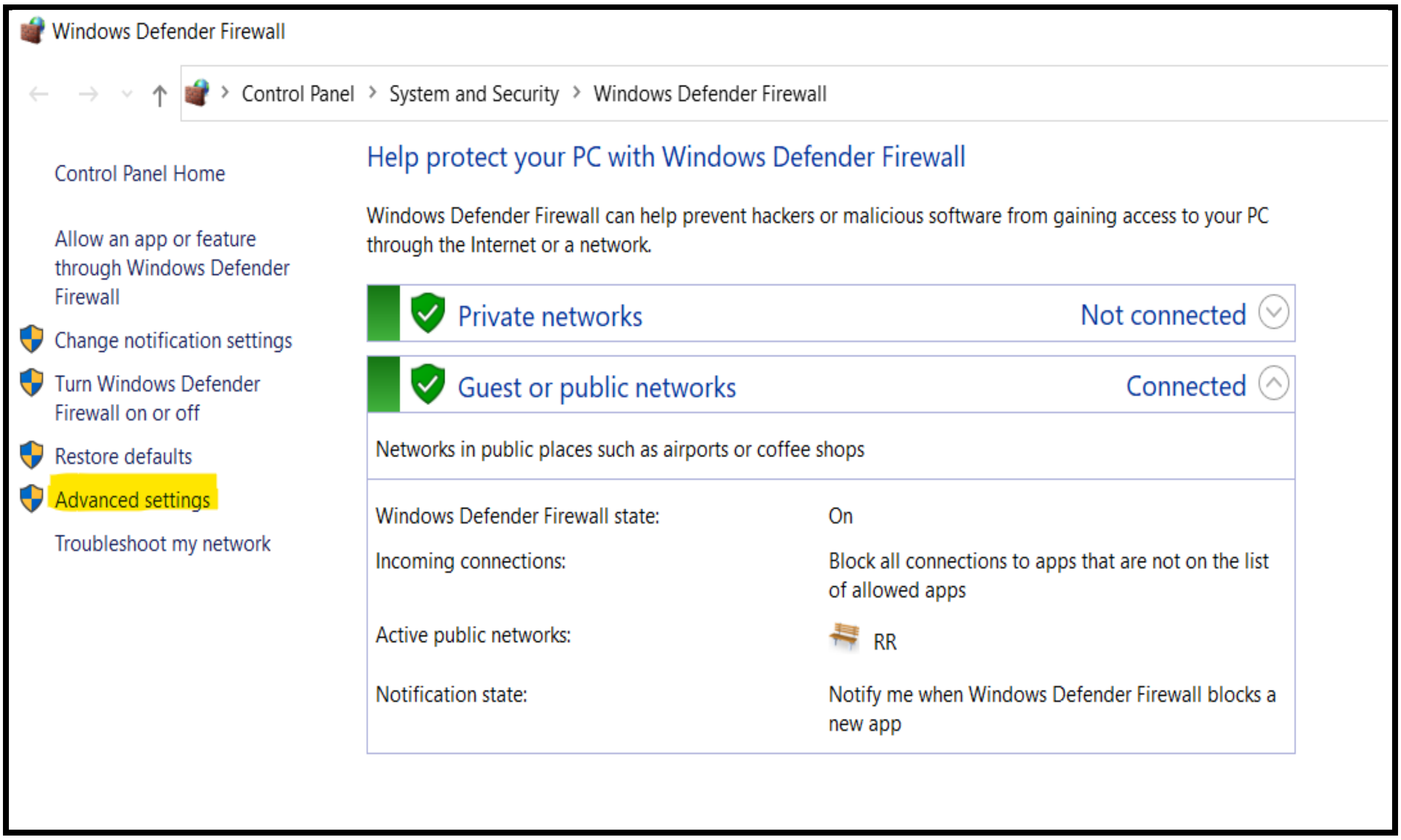
- **Configure and test firewall rules to control network traffic, filter packets based on specified criteria, and protect network resources from unauthorized access.**

A. Port

Step 1: Goto Control Panel>Windows Firewall.



Step 2: Click on Advanced Settings.


Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
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

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.

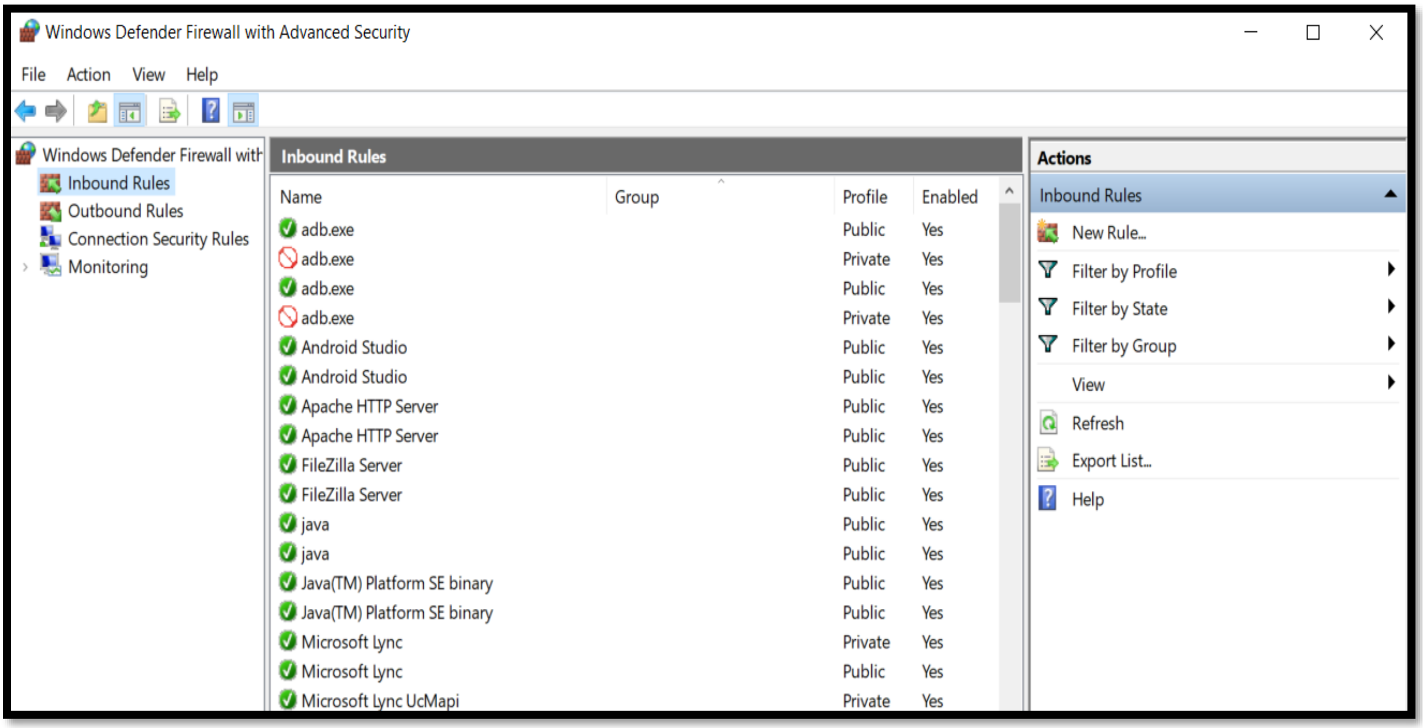
Private networks Not connected

Guest or public networks Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	RR
Notification state:	Notify me when Windows Defender Firewall blocks a new app

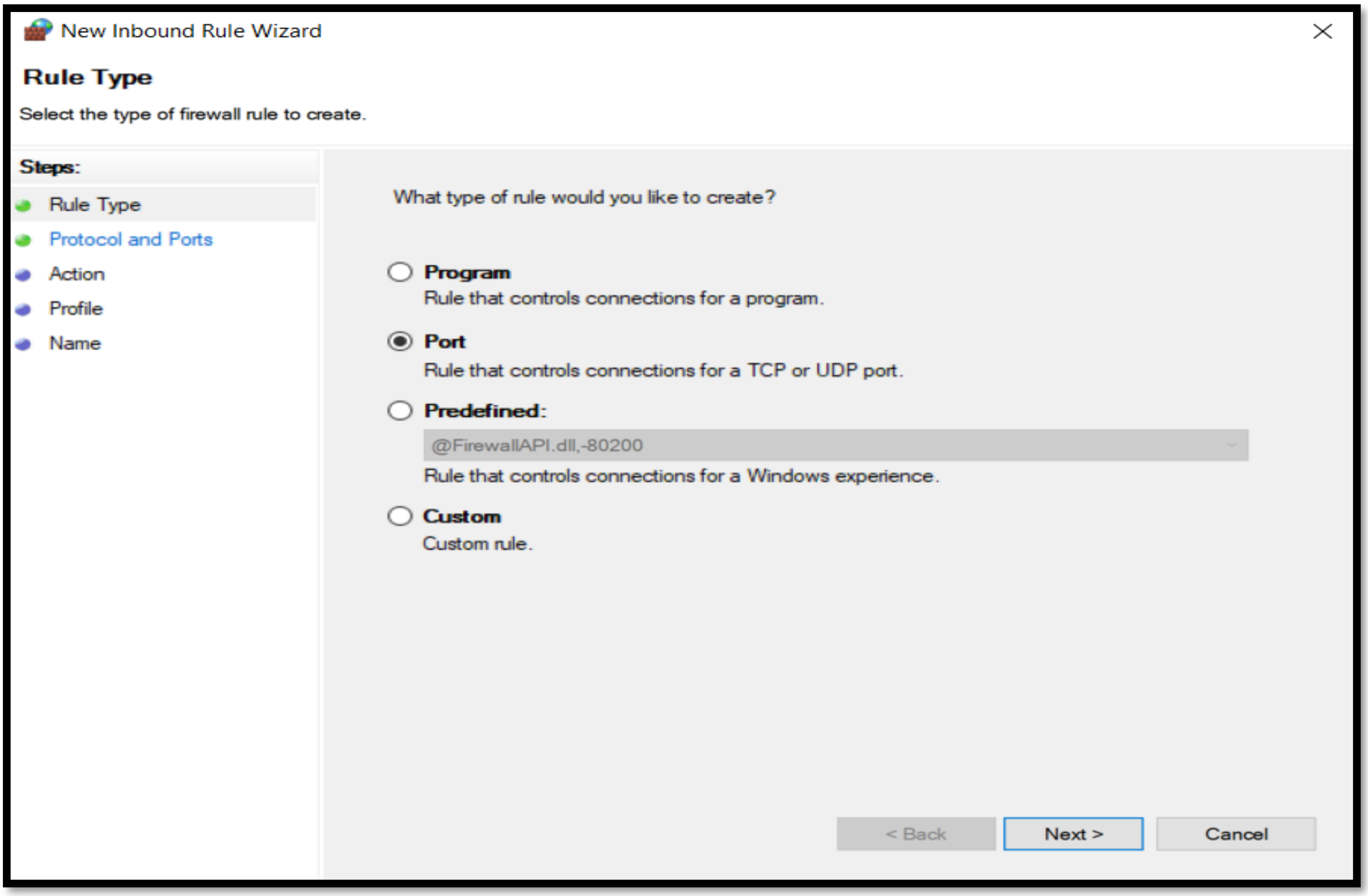
Step 3: Select INBOUND tab and click on NEW RULE from right window.



Inbound Rules

Name	Group	Profile	Enabled
✓ adb.exe		Public	Yes
⊘ adb.exe		Private	Yes
✓ adb.exe		Public	Yes
⊘ adb.exe		Private	Yes
✓ Android Studio		Public	Yes
✓ Android Studio		Public	Yes
✓ Apache HTTP Server		Public	Yes
✓ Apache HTTP Server		Public	Yes
✓ FileZilla Server		Public	Yes
✓ FileZilla Server		Public	Yes
✓ java		Public	Yes
✓ java		Public	Yes
✓ Java(TM) Platform SE binary		Public	Yes
✓ Java(TM) Platform SE binary		Public	Yes
✓ Microsoft Lync		Private	Yes
✓ Microsoft Lync		Public	Yes
✓ Microsoft Lync UcMapi		Private	Yes

Step 4: Select Port option and click on NEXT button.



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

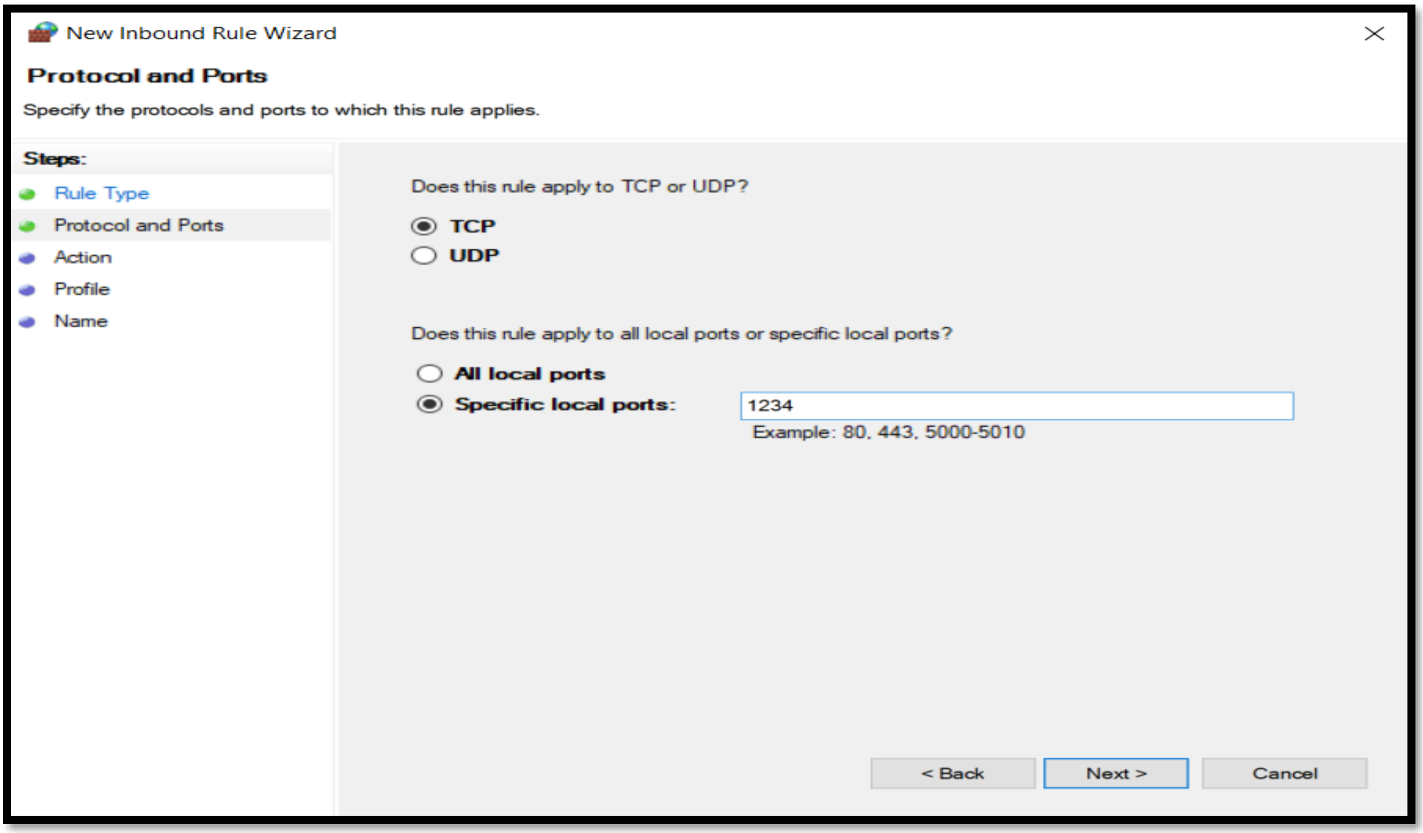
○ **Program**
Rule that controls connections for a program.

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

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

○ **Custom**
Custom rule.

Step 5: Type port number in specific local ports option and click on NEXT button.



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?

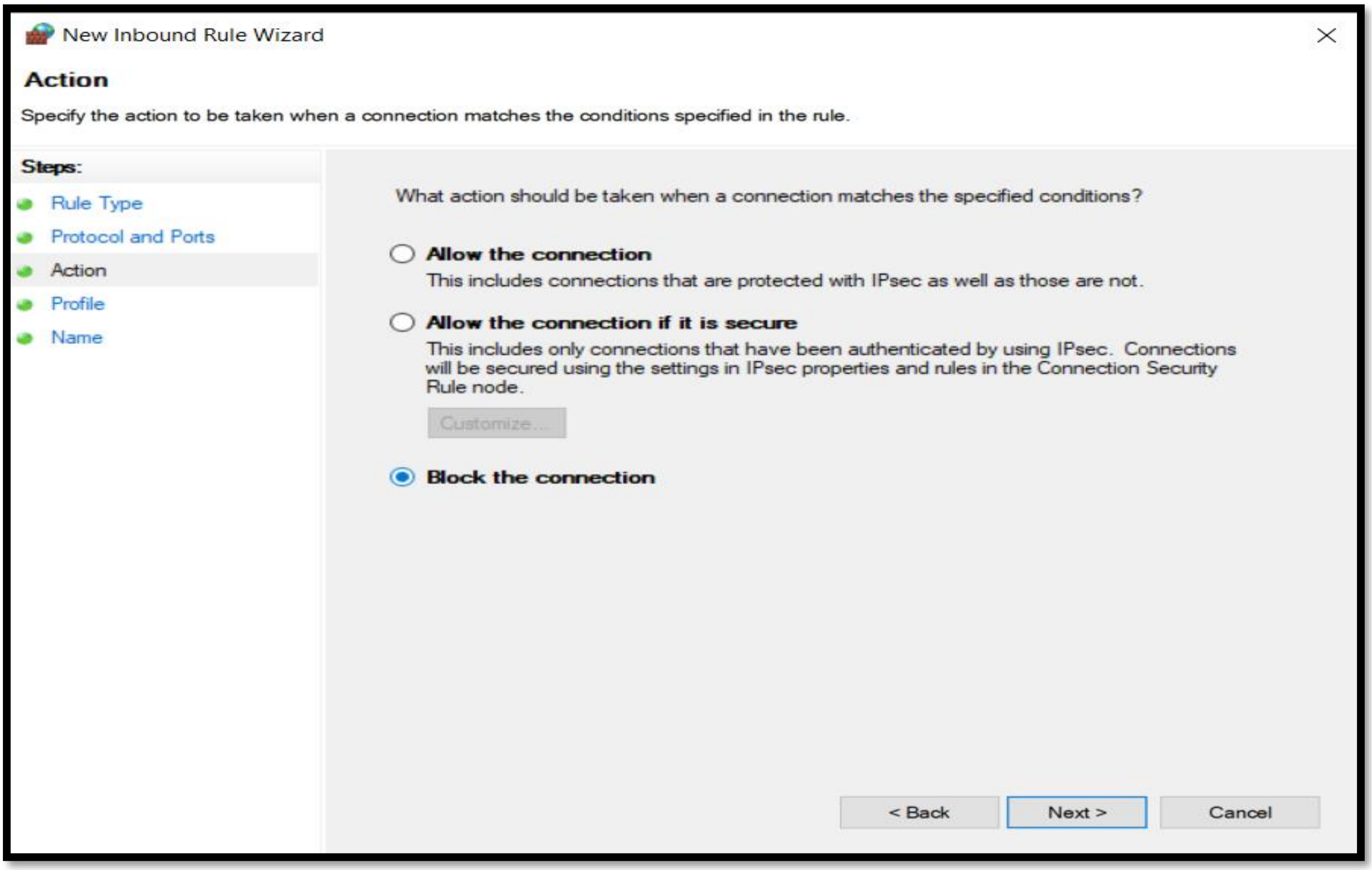
● TCP
○ UDP

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

○ All local ports
● Specific local ports: 1234

Example: 80, 443, 5000-5010

Step 6: Choose Block the Connection option in order to block port and click on NEXT button.



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

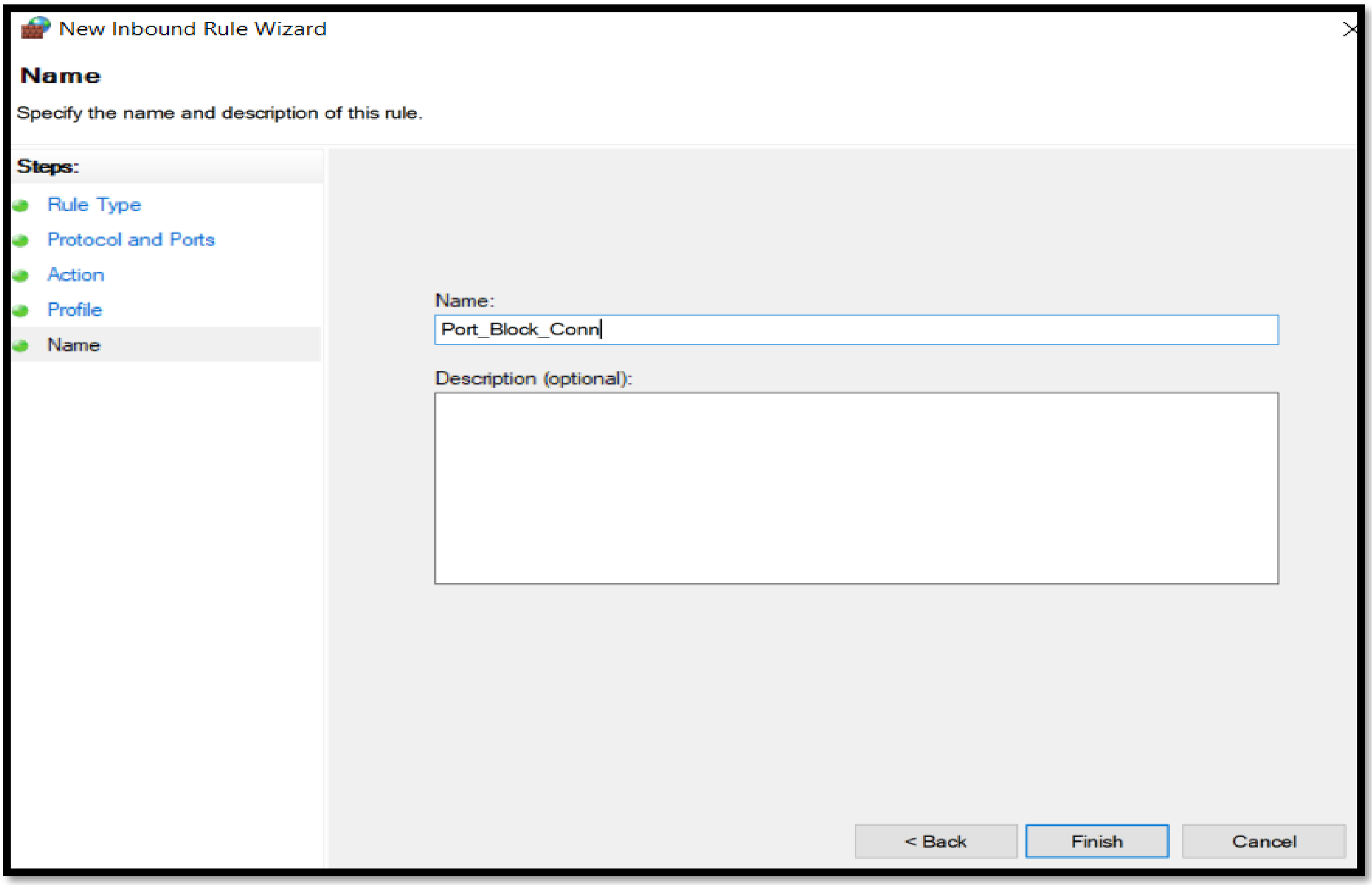
What action should be taken when a connection matches the specified conditions?

○ 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.

● Block the connection

Step 7: Click on Next and give any name for the rule and click on FINISH button.



New Inbound Rule Wizard

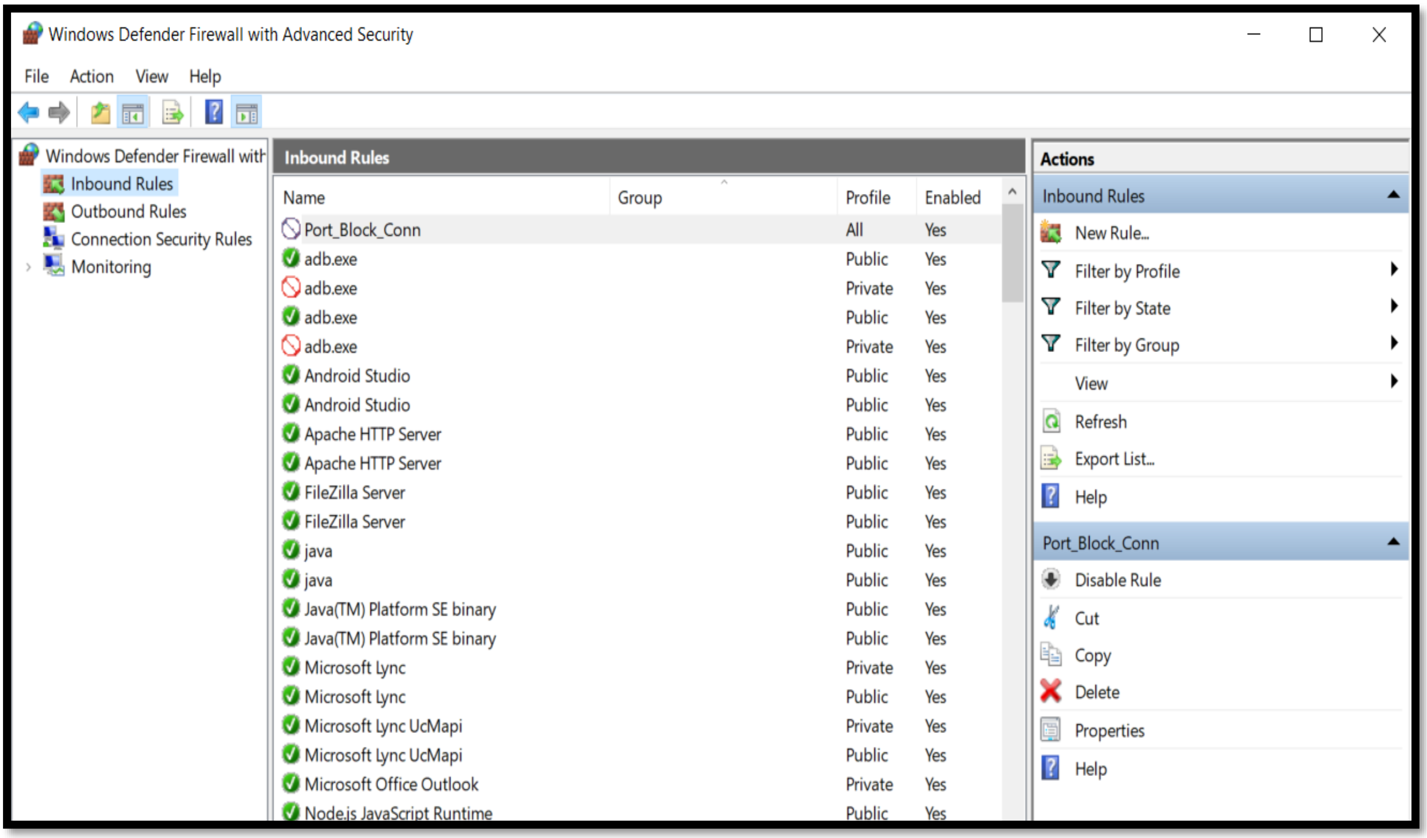
Name

Specify the name and description of this rule.

Name: Port_Block_Conn

Description (optional):

We can see that port1234 inbound rule is created which will block port number 1234.



Windows Defender Firewall with Advanced Security

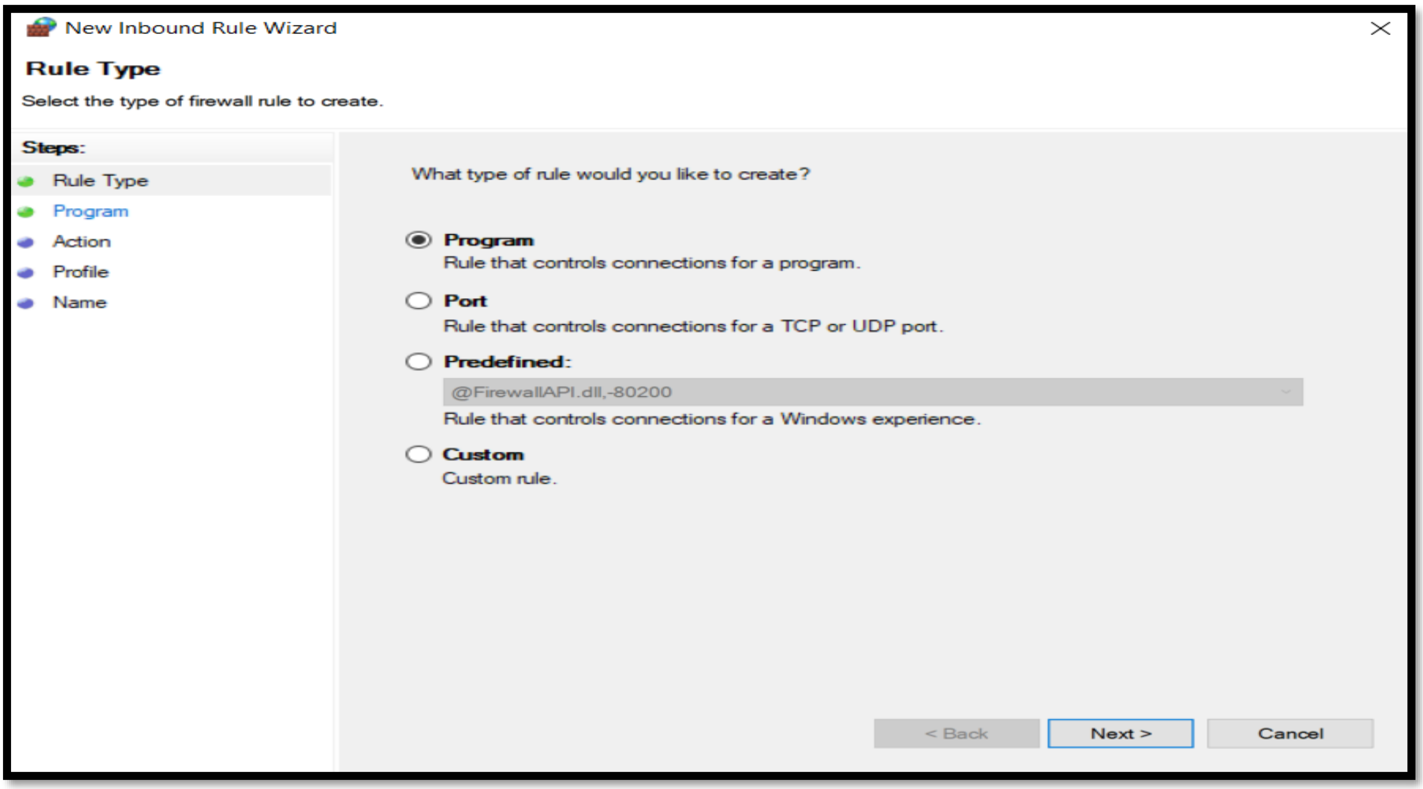
Inbound Rules

Name	Group	Profile	Enabled
Port_Block_Conn		All	Yes
adb.exe		Public	Yes
adb.exe		Private	Yes
adb.exe		Public	Yes
adb.exe		Private	Yes
Android Studio		Public	Yes
Android Studio		Public	Yes
Apache HTTP Server		Public	Yes
Apache HTTP Server		Public	Yes
FileZilla Server		Public	Yes
FileZilla Server		Public	Yes
java		Public	Yes
java		Public	Yes
Java(TM) Platform SE binary		Public	Yes
Java(TM) Platform SE binary		Public	Yes
Microsoft Lync		Private	Yes
Microsoft Lync		Public	Yes
Microsoft Lync UcMapi		Private	Yes
Microsoft Lync UcMapi		Public	Yes
Microsoft Office Outlook		Private	Yes
Node.js JavaScript Runtime		Public	Yes

B. Program

Step 1: Select INBOUND tab and click on NEW RULE from right window.

Step 2: Choose Program option and click on NEXT button.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

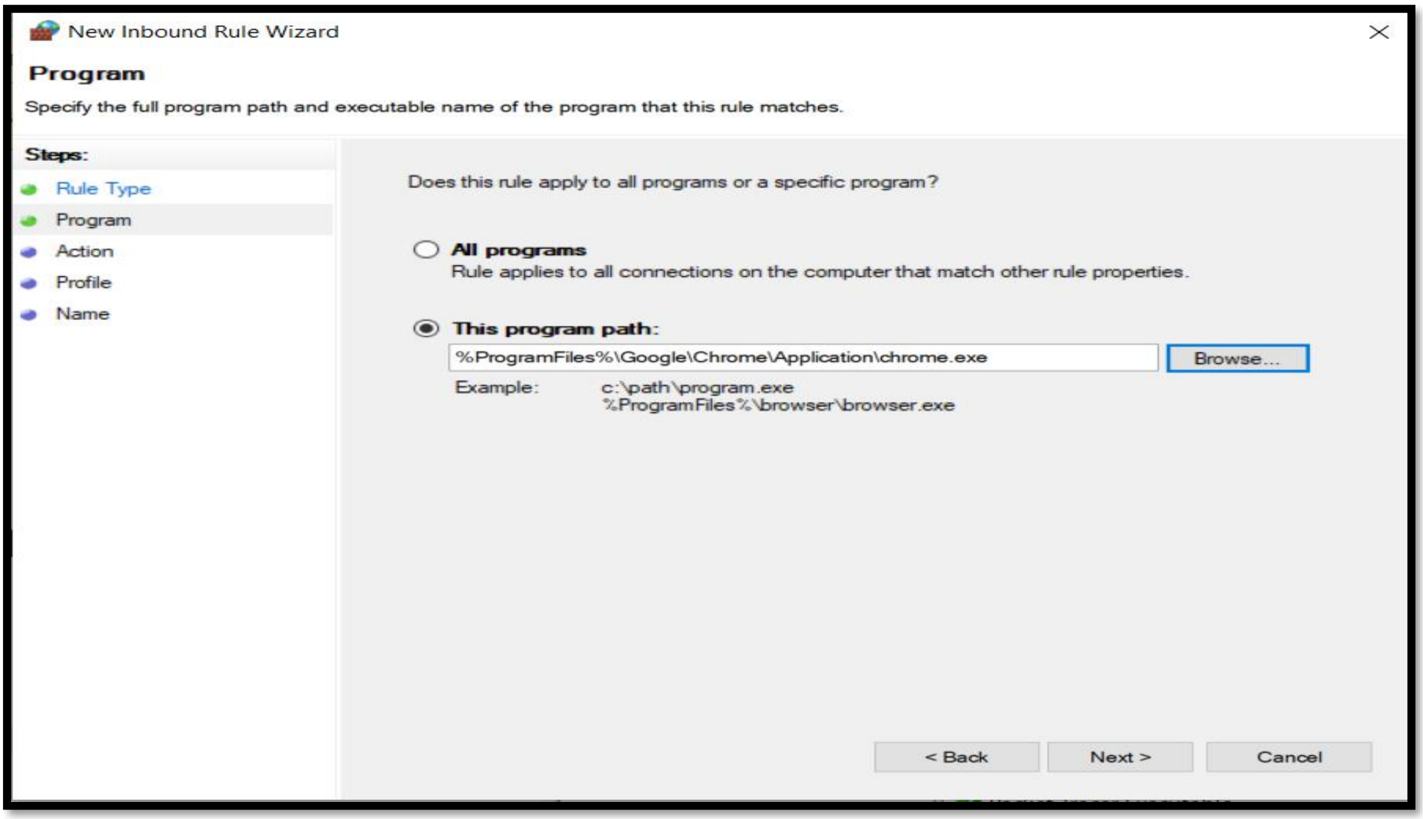
● **Program**
Rule that controls connections for a program.

○ **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.

Step 3: Click on Browse button and select the path of any application which you want to block.



New Inbound Rule Wizard

Program

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

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

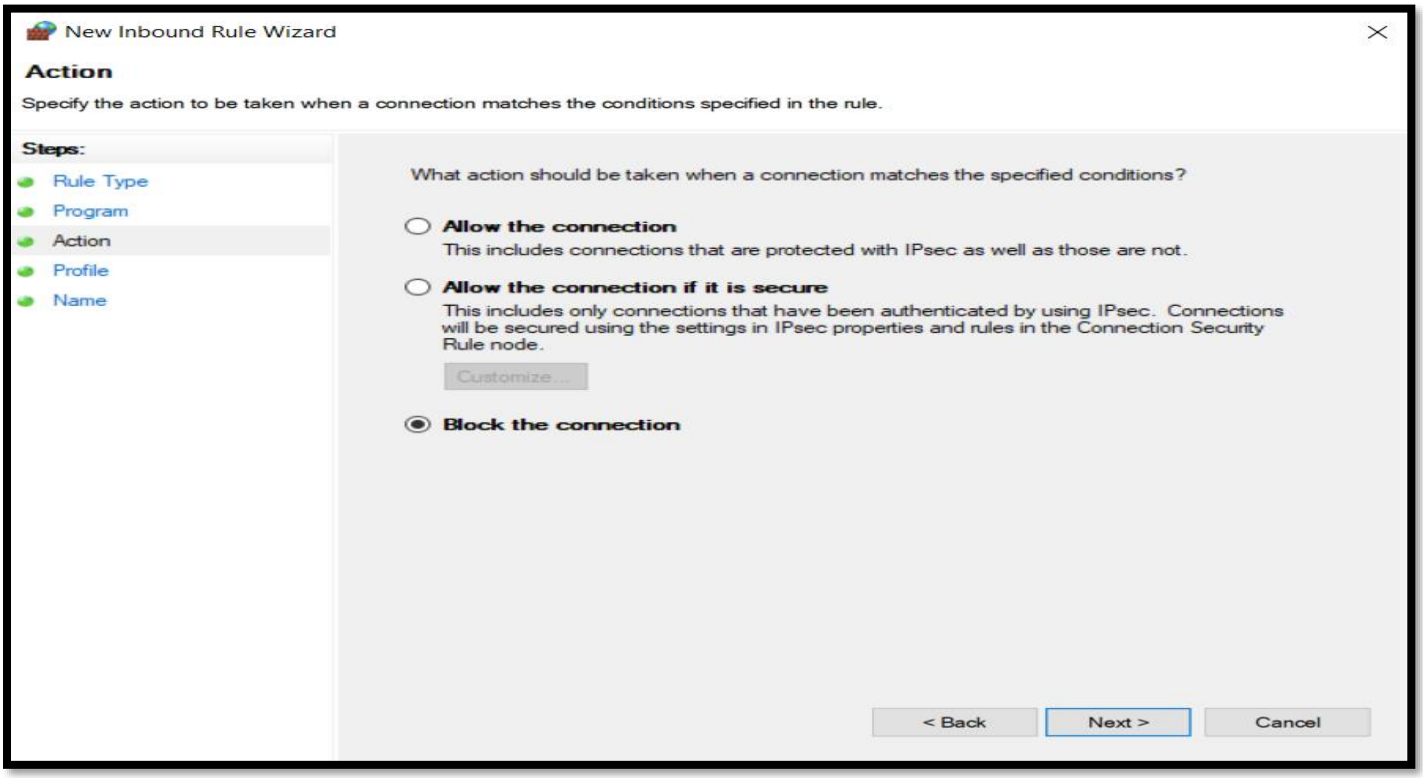
Does this rule apply to all programs or a specific program?

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

● **This program path:**
%ProgramFiles%\Google\Chrome\Application\chrome.exe

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

Step 4: Choose Block the Connection option in order to block port and click on NEXT button.



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
- Action
- Profile
- Name

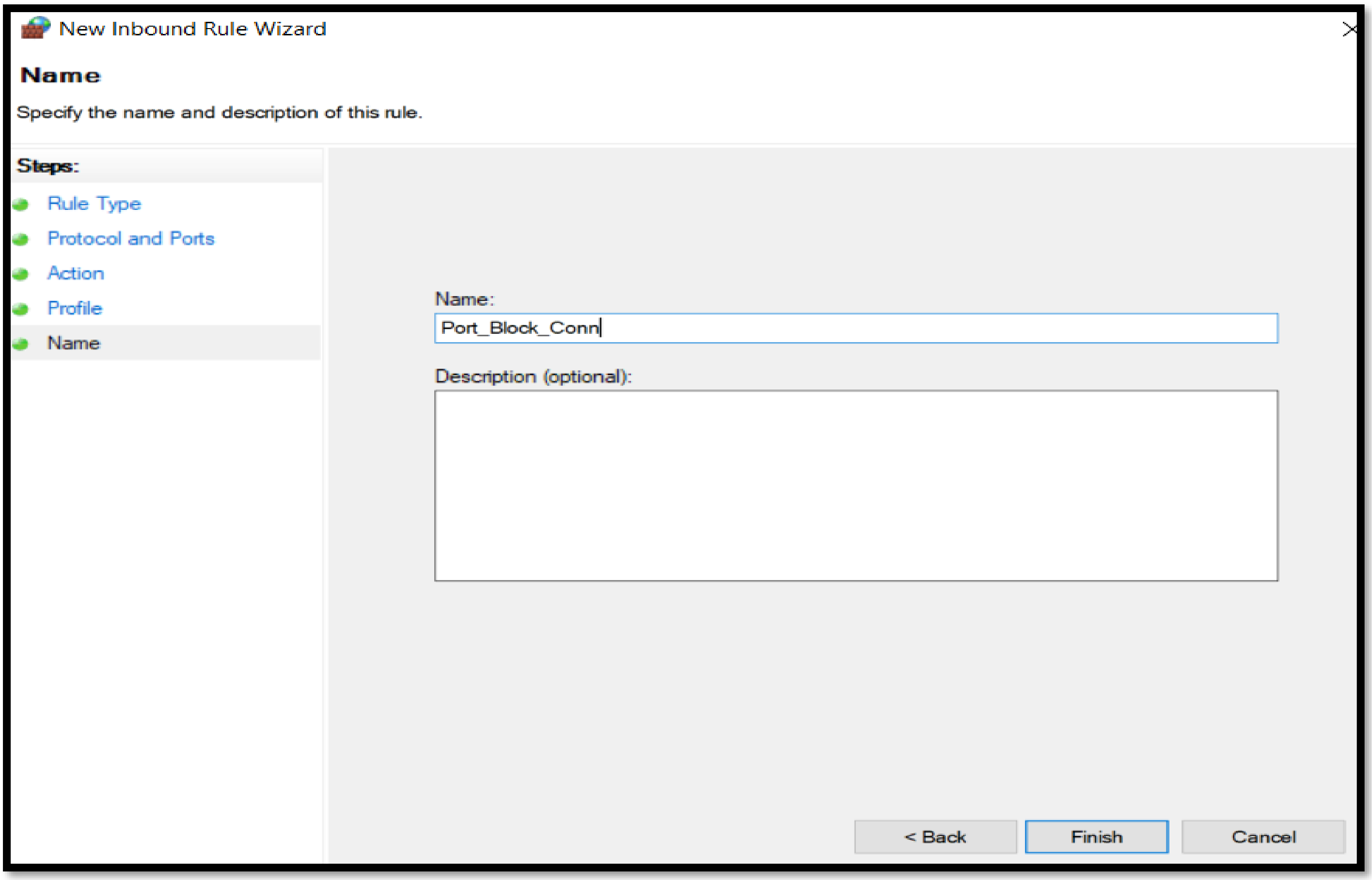
What action should be taken when a connection matches the specified conditions?

○ **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**

Step 5: Click on Next and give any name for the rule and click on FINISH button.



New Inbound Rule Wizard

Name

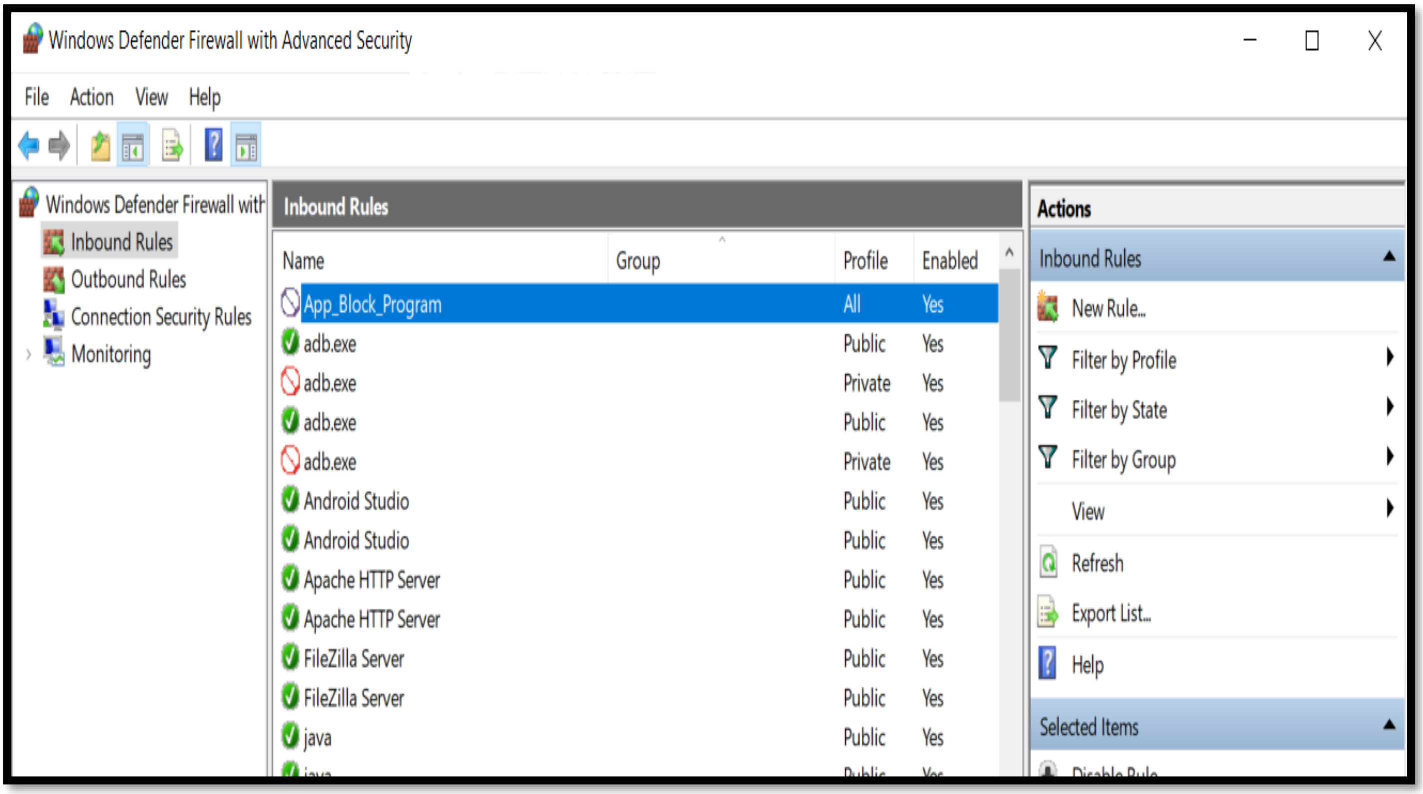
Specify the name and description of this rule.

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

Name: Port_Block_Conn

Description (optional):

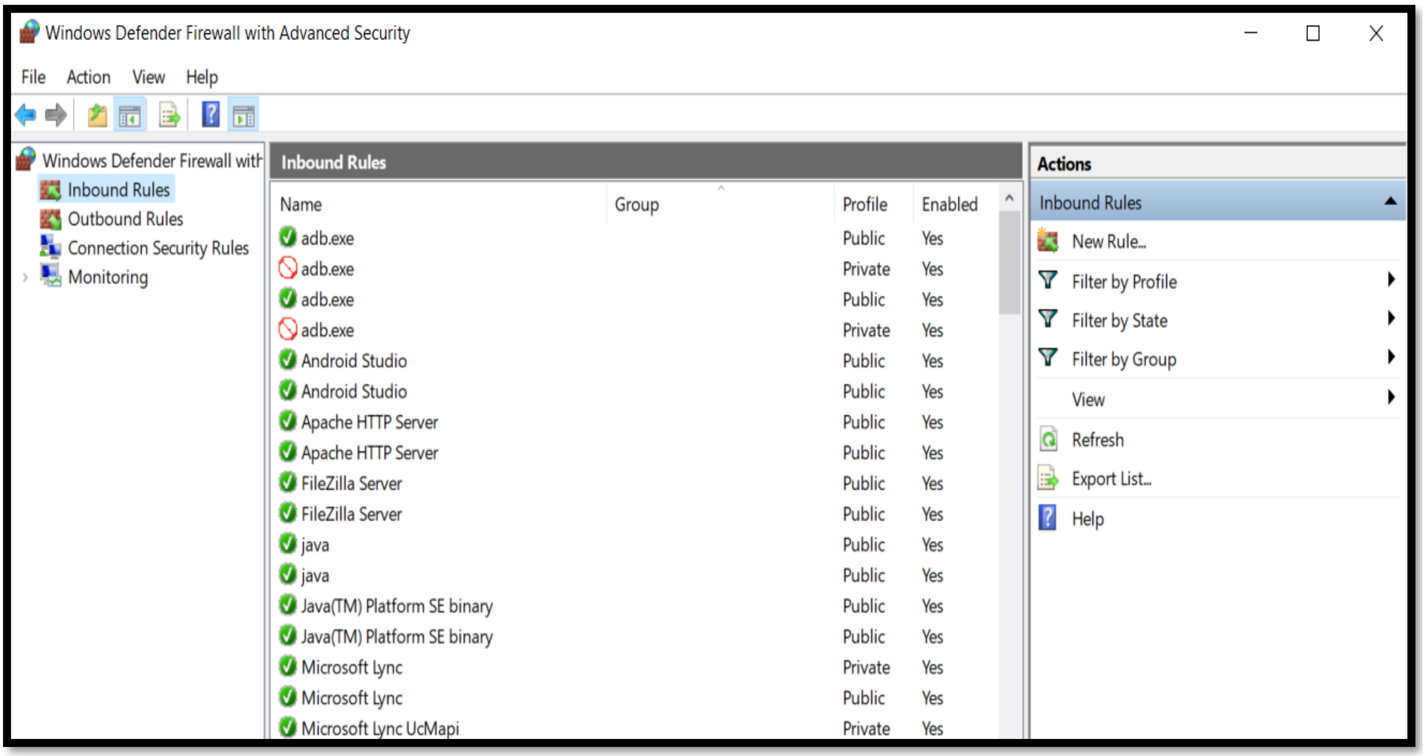
We can see that App_Block_Program inbound rule is created which will block Chrome application.



Name	Group	Profile	Enabled
App_Block_Program		All	Yes
adb.exe		Public	Yes
adb.exe		Private	Yes
adb.exe		Public	Yes
adb.exe		Private	Yes
Android Studio		Public	Yes
Android Studio		Public	Yes
Apache HTTP Server		Public	Yes
Apache HTTP Server		Public	Yes
FileZilla Server		Public	Yes
FileZilla Server		Public	Yes
java		Public	Yes
java		Public	Yes

C. Website

Step 1: Select INBOUND tab and click on NEW RULE from right window.

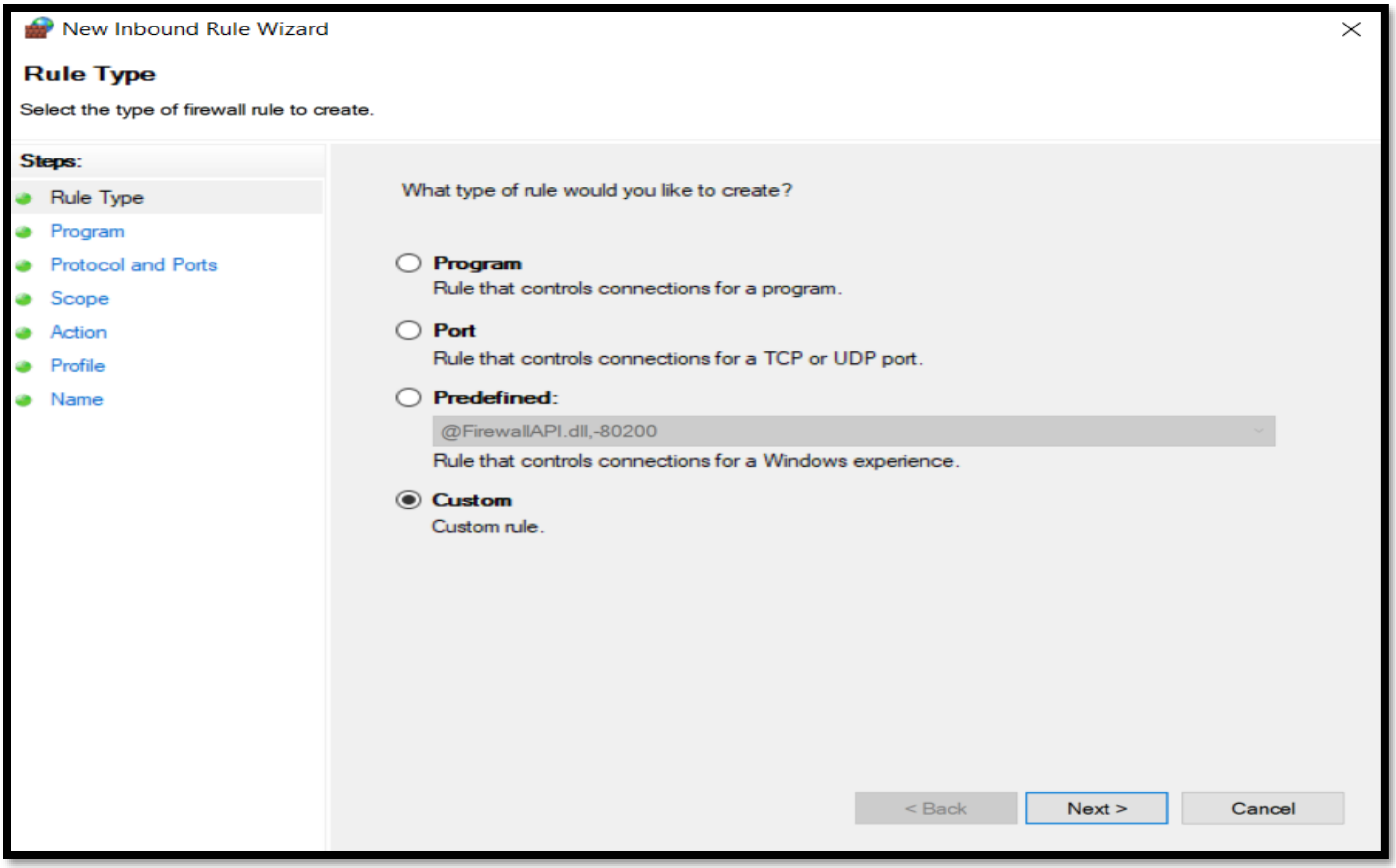


Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled
✓ adb.exe		Public	Yes
⊘ adb.exe		Private	Yes
✓ adb.exe		Public	Yes
⊘ adb.exe		Private	Yes
✓ Android Studio		Public	Yes
✓ Android Studio		Public	Yes
✓ Apache HTTP Server		Public	Yes
✓ Apache HTTP Server		Public	Yes
✓ FileZilla Server		Public	Yes
✓ FileZilla Server		Public	Yes
✓ java		Public	Yes
✓ java		Public	Yes
✓ Java(TM) Platform SE binary		Public	Yes
✓ Java(TM) Platform SE binary		Public	Yes
✓ Microsoft Lync		Private	Yes
✓ Microsoft Lync		Public	Yes
✓ Microsoft Lync UcMapi		Private	Yes

Step 2: Select Custom option and click on NEXT button.



New Inbound Rule Wizard

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.

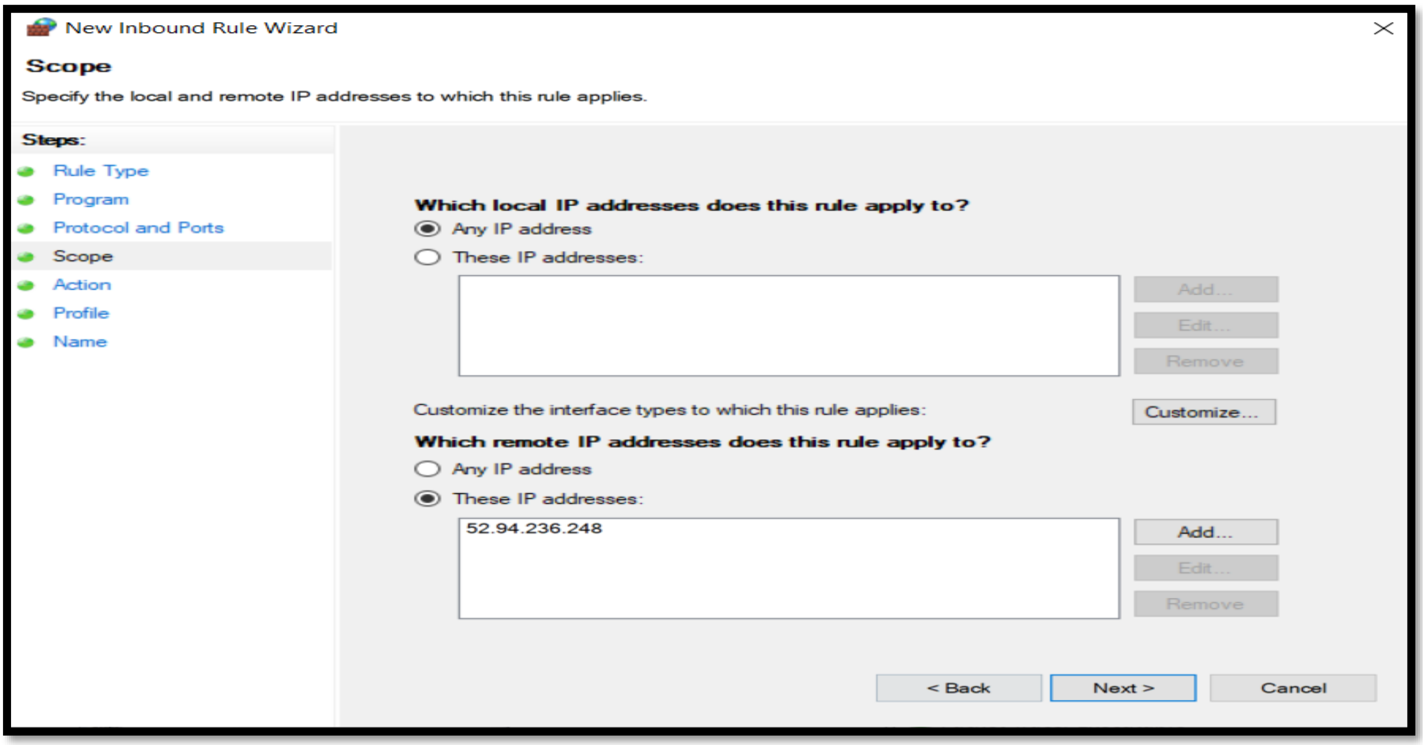
○ **Port**
Rule that controls connections for a TCP or UDP port.

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

● **Custom**
Custom rule.

Step 3: Click on NEXT button till you reach Scope.

Step 4: Choose 'These IP addresses' from remote IP addresses option and click on ADD button. Type IP address of a particular website [Amazon.com] which you want to block and click on OK button.



New Inbound Rule Wizard

Scope

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

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?

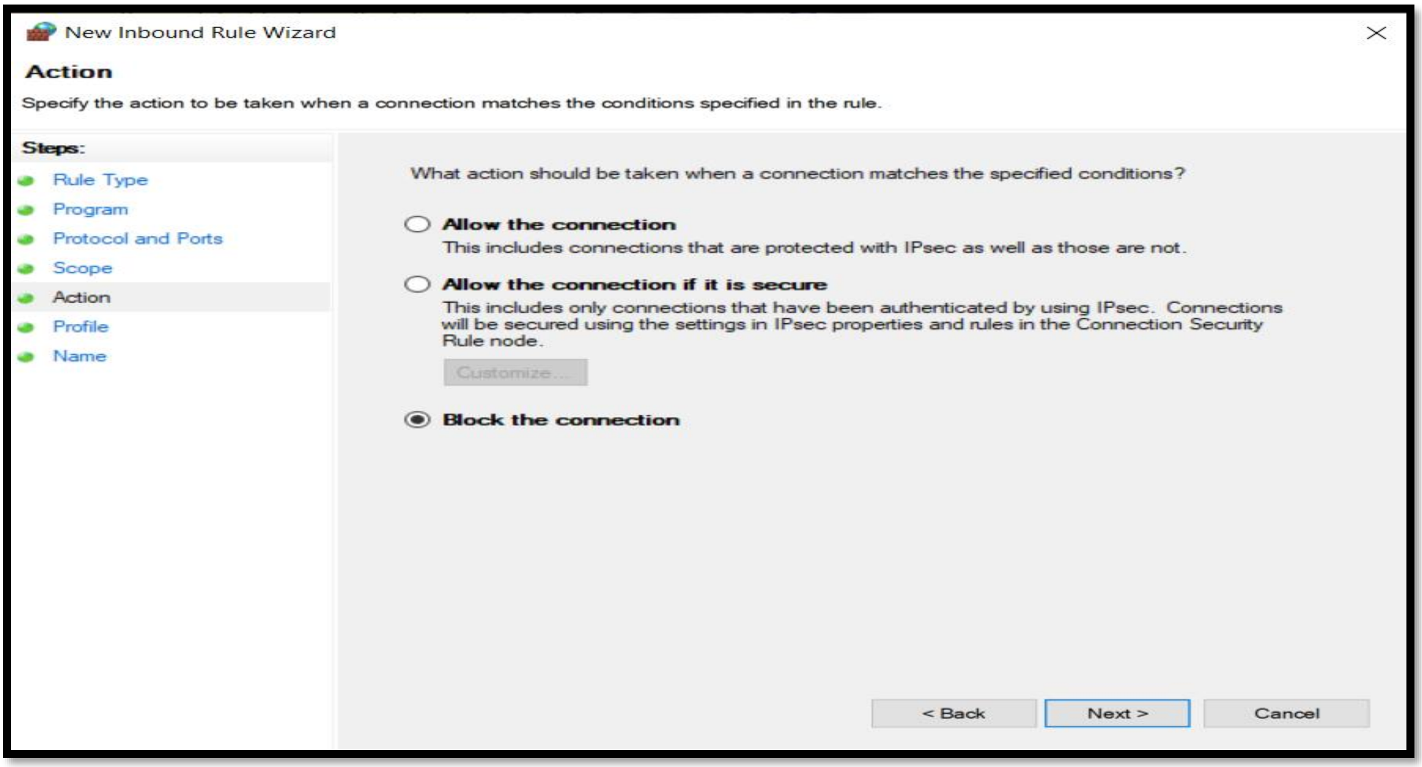
○ Any IP address

● These IP addresses:

52.94.236.248

Step 5: Click on NEXT button.

Step 6: Choose Block the Connection option in order to block IP address of particular website and click on NEXT button.



New Inbound Rule Wizard

Action

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

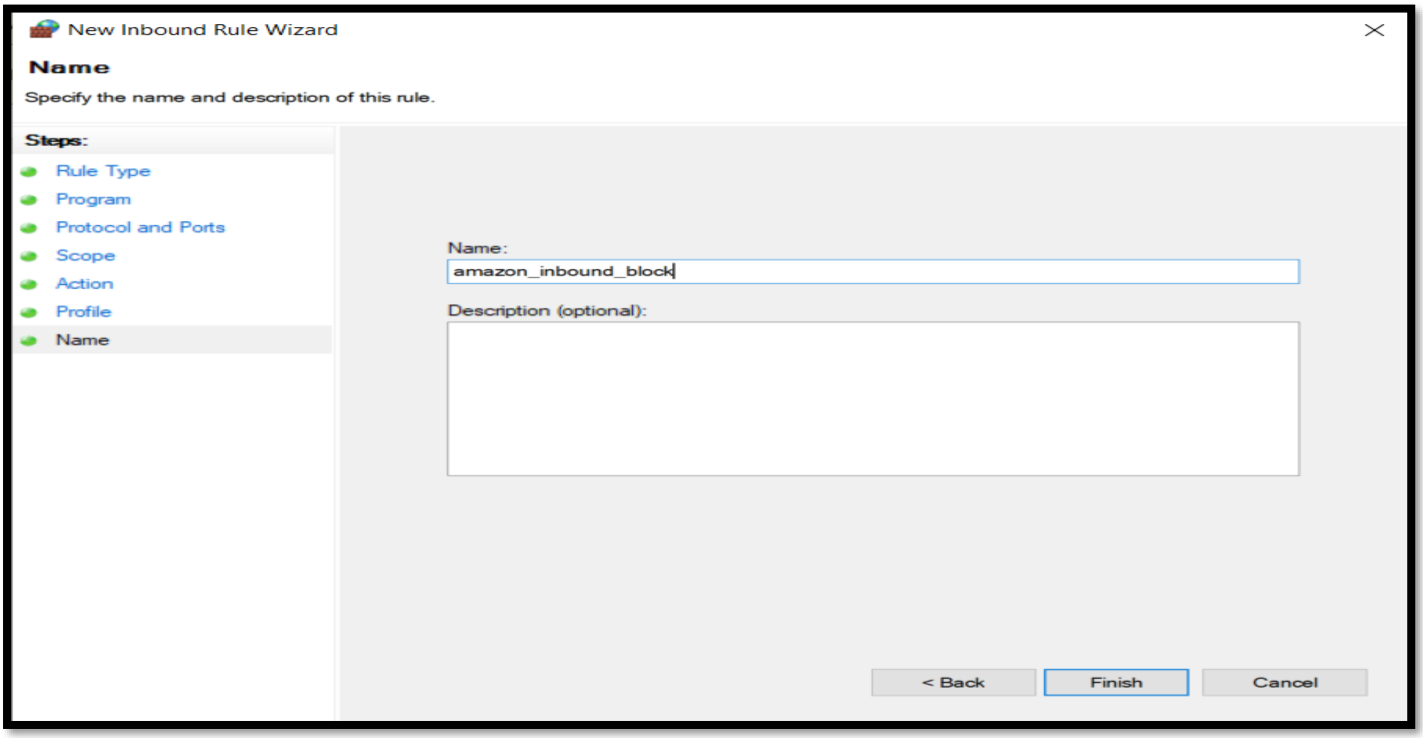
What action should be taken when a connection matches the specified conditions?

○ **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**

Step 7: Click on Next and give any name for the rule and click on FINISH button.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

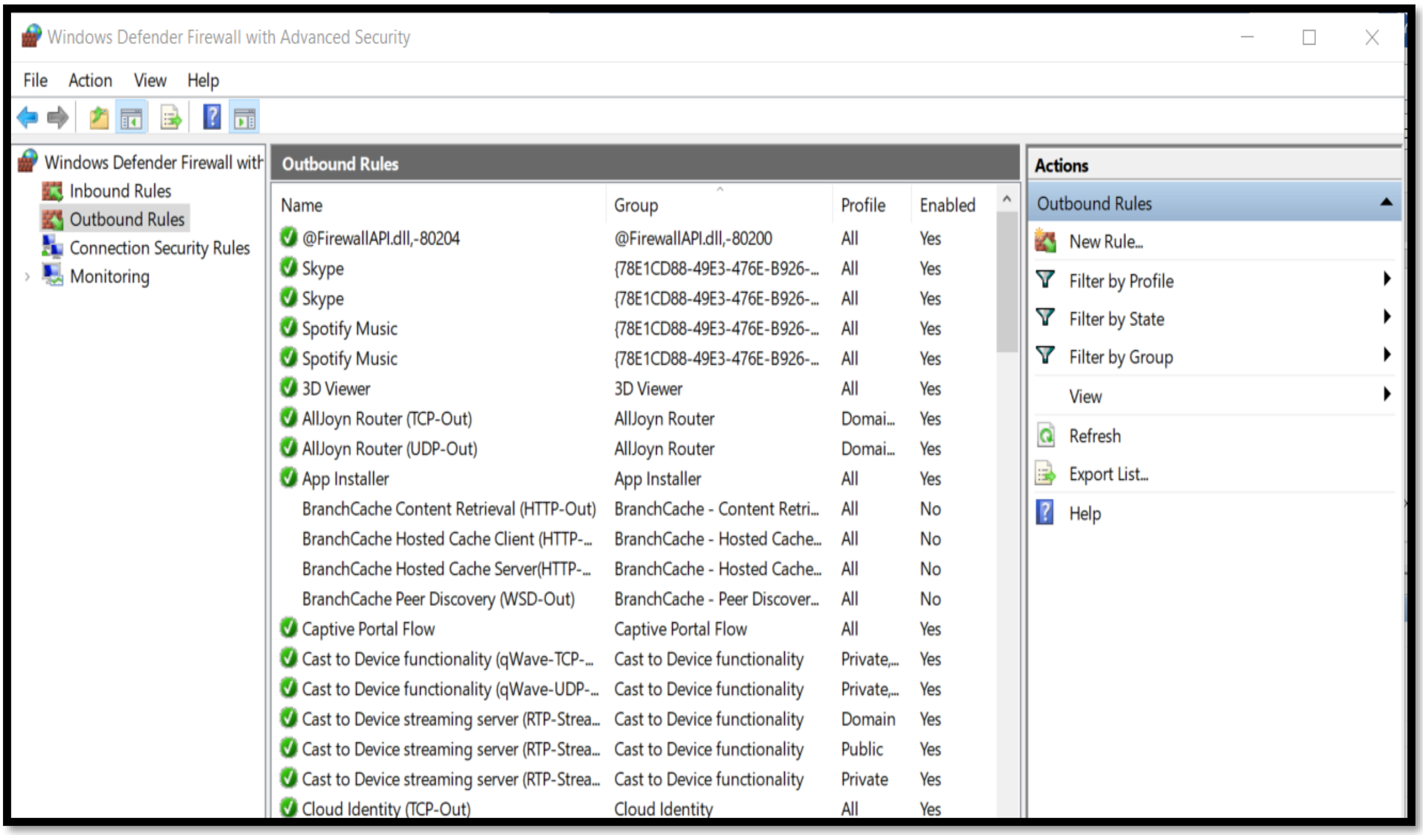
Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Name: amazon_inbound_block

Description (optional):

❖ **Same steps are to be followed for OUTBOUND Rule as well:**

Step 1: Select OUTBOUND tab and click on NEW RULE from right window.

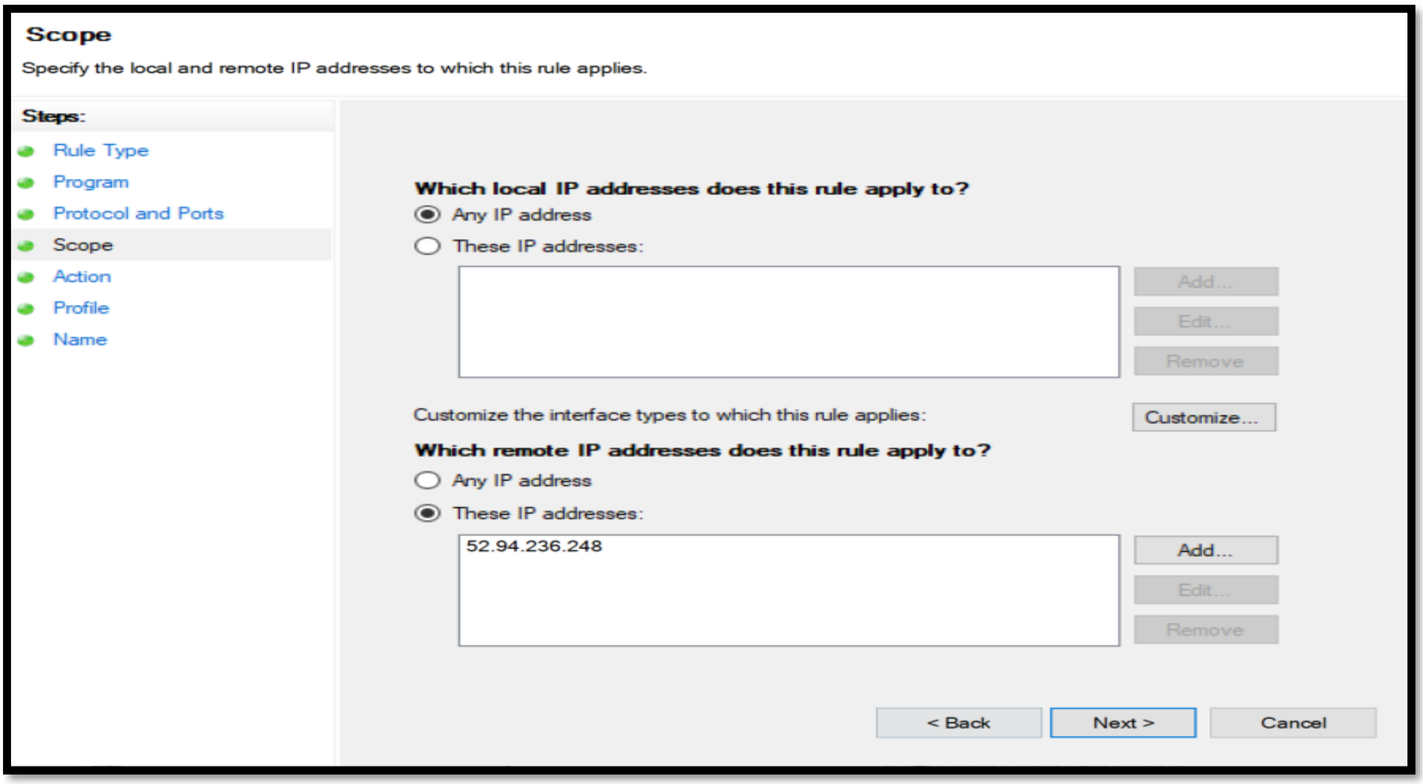


Outbound Rules

Name	Group	Profile	Enabled
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All	Yes
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
3D Viewer	3D Viewer	All	Yes
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes
App Installer	App Installer	All	Yes
BranchCache Content Retrieval (HTTP-Out)	BranchCache - Content Retri...	All	No
BranchCache Hosted Cache Client (HTTP-...	BranchCache - Hosted Cache...	All	No
BranchCache Hosted Cache Server(HTTP-...	BranchCache - Hosted Cache...	All	No
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discover...	All	No
Captive Portal Flow	Captive Portal Flow	All	Yes
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private,...	Yes
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes
Cloud Identity (TCP-Out)	Cloud Identity	All	Yes

Step 2: Click on NEXT button till you reach Scope.

Step 4: Choose 'These IP addresses' from remote IP addresses option and click on ADD button. Type IP address of a particular website [Amazon.com] which you want to block and click on OK button.



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?

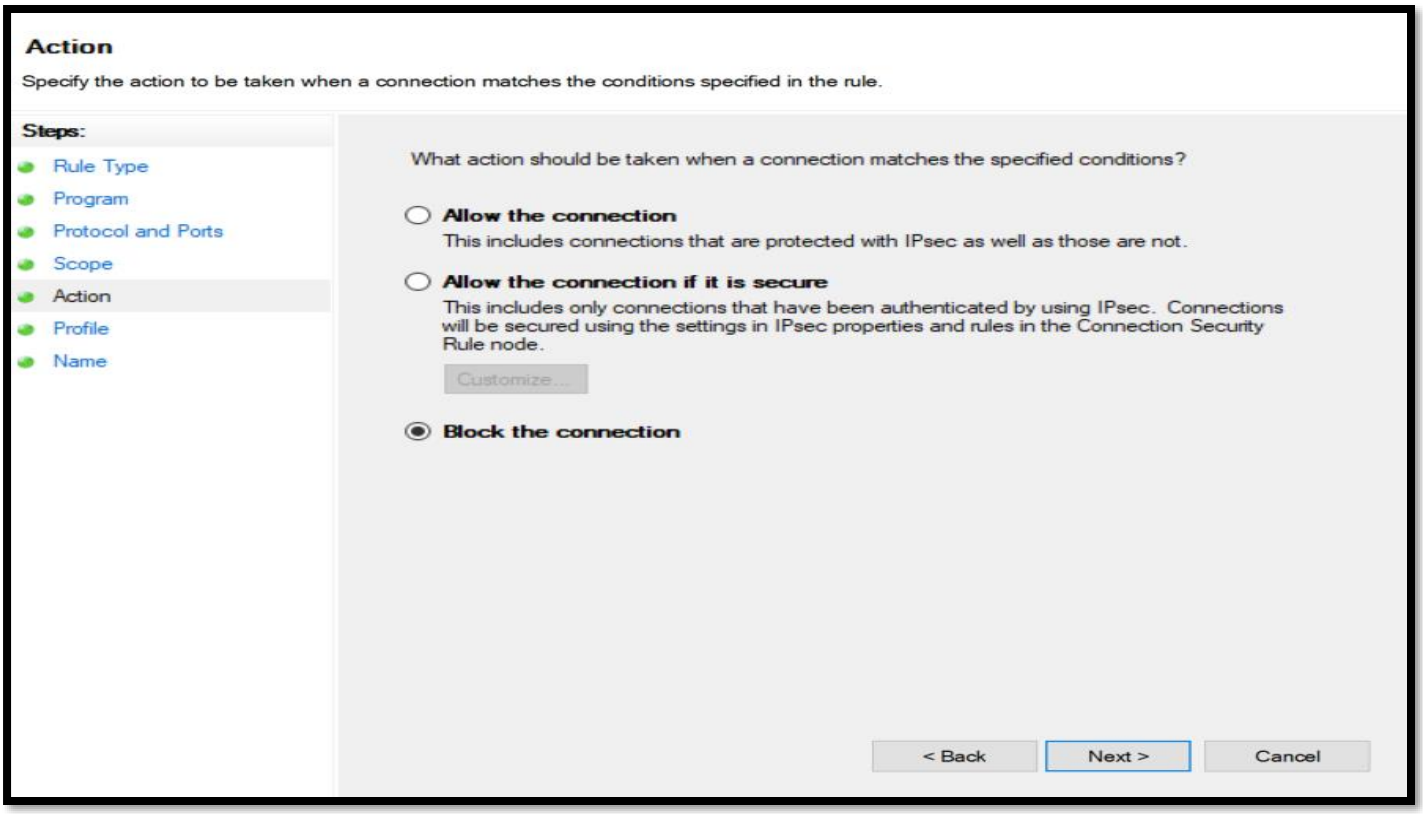
○ Any IP address

● These IP addresses:

52.94.236.248

Step 5: Click on NEXT button.

Step 6: Choose Block the Connection option in order to block IP address of particular website and click on NEXT button.



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**

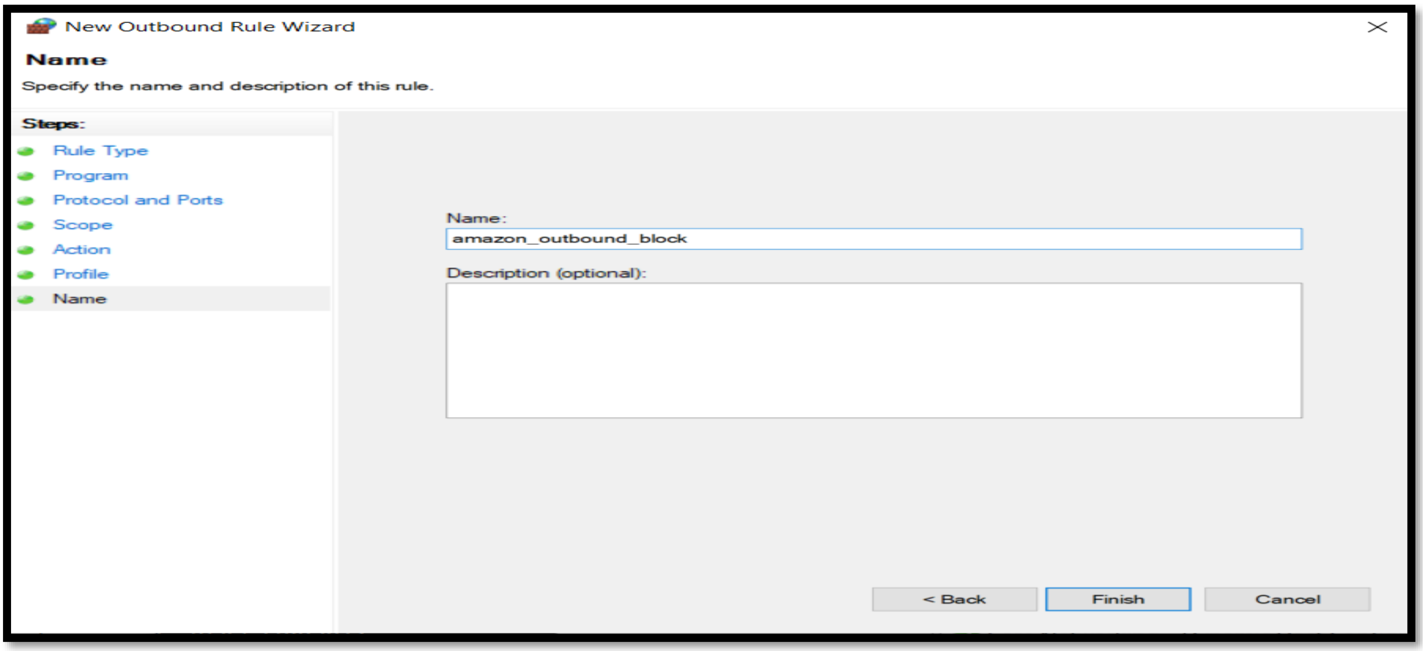
This includes connections that are protected with IPsec as well as those are not.

○ **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**

Step 7: Click on Next and give any name for the rule and click on FINISH button.



New Outbound Rule Wizard

Name

Specify the name and description of this rule.

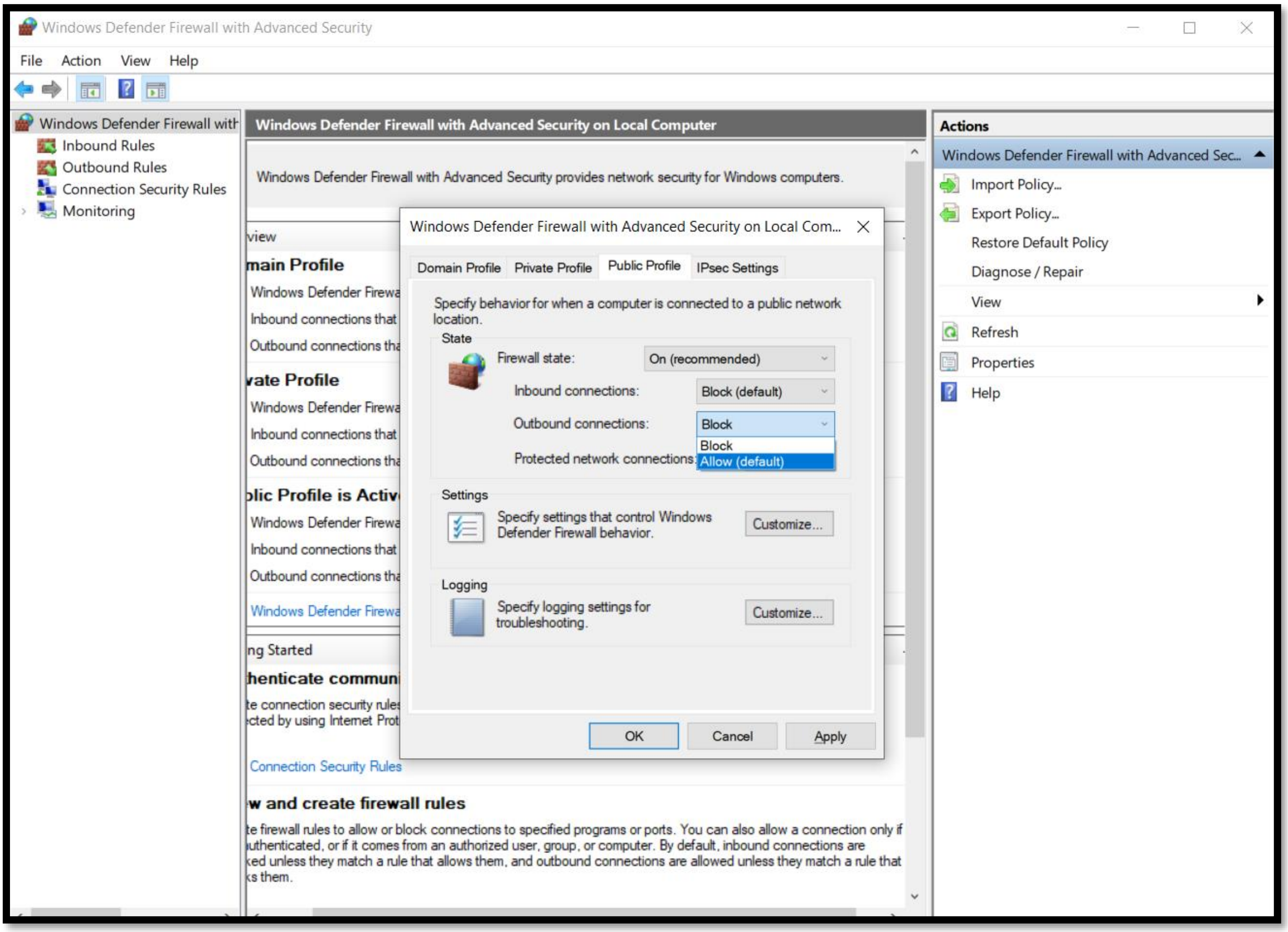
Steps:

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

Name: amazon_outbound_block

Description (optional):

- **Before Searching for Website**
- **Click on windows Defender Firewall with Advanced Setting on Local Computer and Block OUTBOUND on Domain, Private, Public.**



Windows Defender Firewall with Advanced Security on Local Computer

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

Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Block

Protected network connections: Block / Allow (default)

Settings

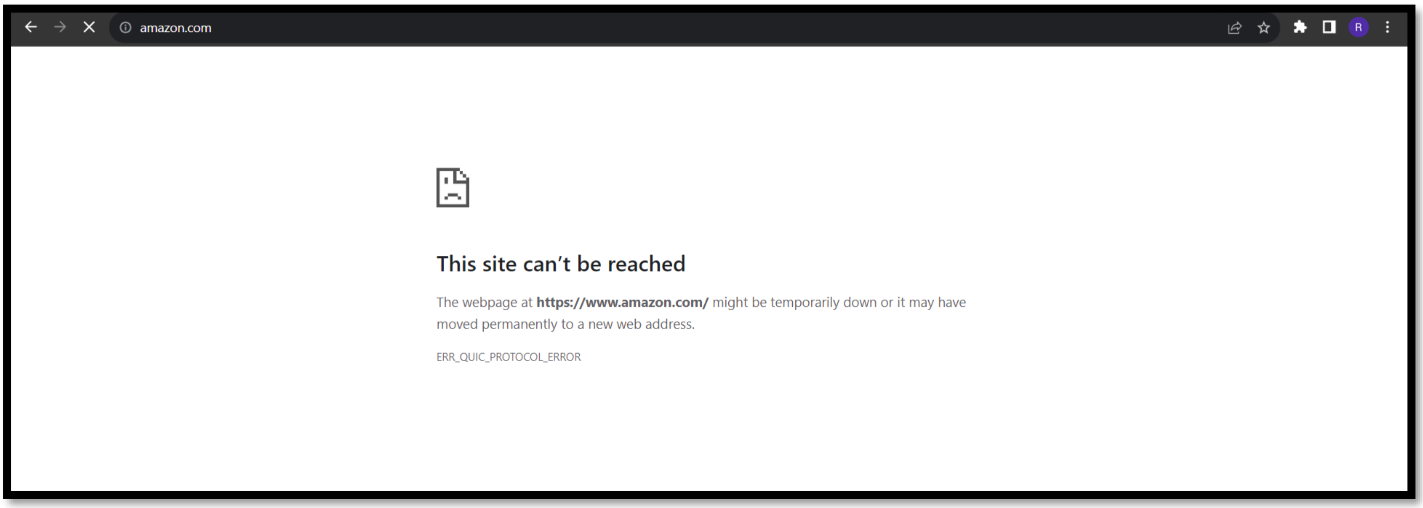
Specify settings that control Windows Defender Firewall behavior.

Logging

Specify logging settings for troubleshooting.

Output:

Amazon.com website gets blocked



This site can't be reached

The webpage at **https://www.amazon.com/** might be temporarily down or it may have moved permanently to a new web address.

ERR_QUIC_PROTOCOL_ERROR