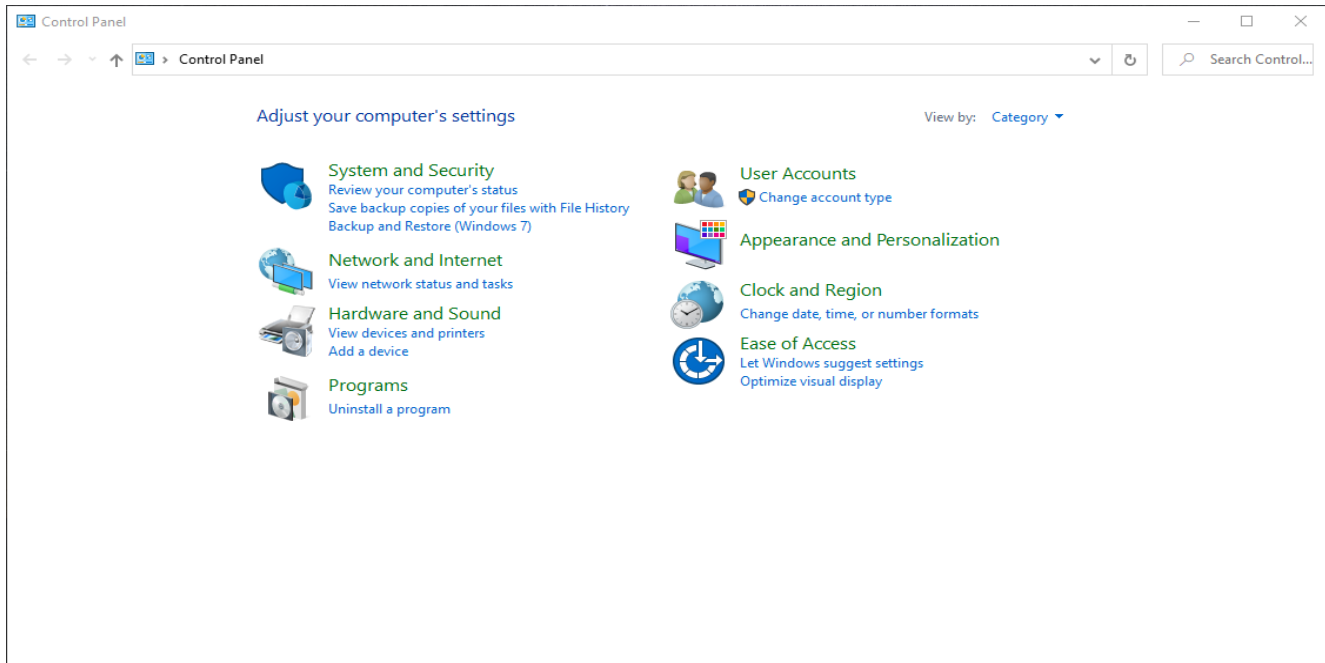
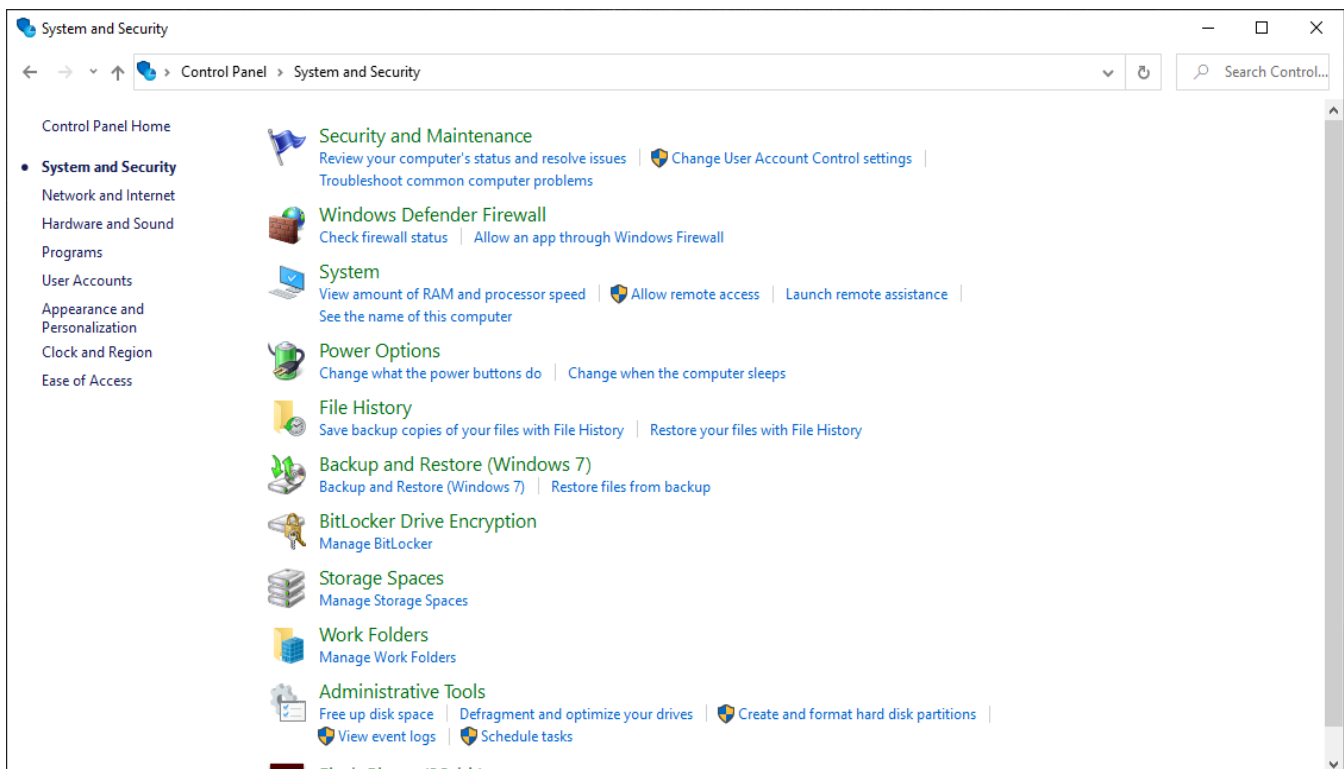


Date:07/11/2020

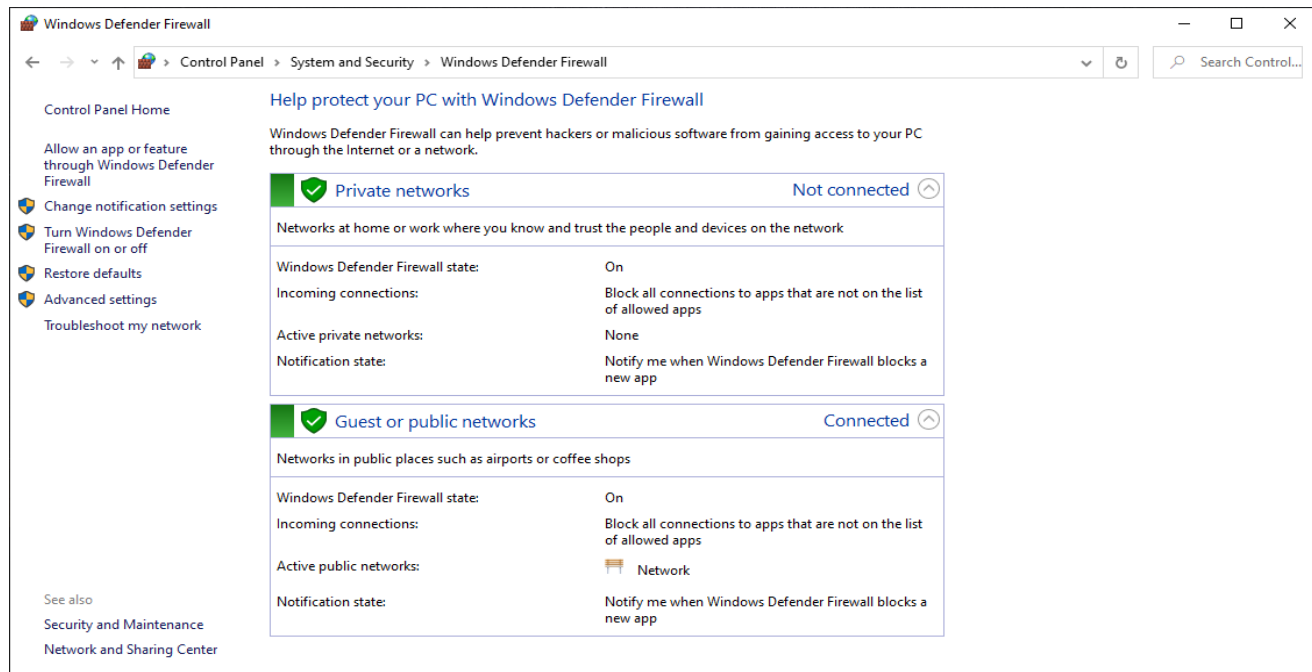
**Practical no 9****AIM:** Configure windows firewall to block

- 1) A port 2) An Program 3) A Website

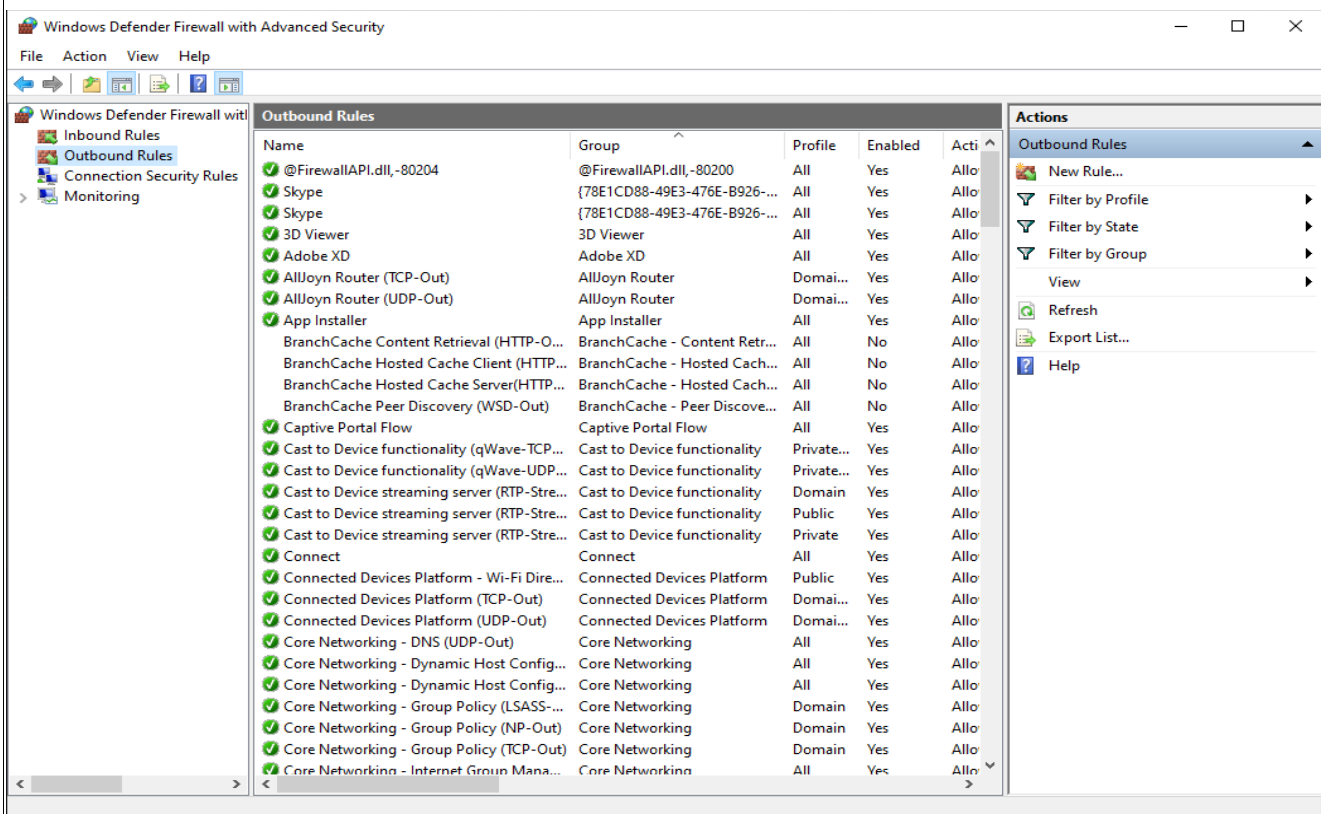
**Different Types of Profiles available/ When does this rule applies****Domain:** Applies when computer is connected to corporate domain**Private:** Applies when computer is connected to a private network location, such as a home or workplace.**Public:** Applies when computer is connected to public network connection.**Different types of actions available/What action should be taken when a connection matches the specified the 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.

**A) Blocking a port:****Step 1:** Open control panel and go to System Security**Step 2:** Now Select Windows Defender Firewall.

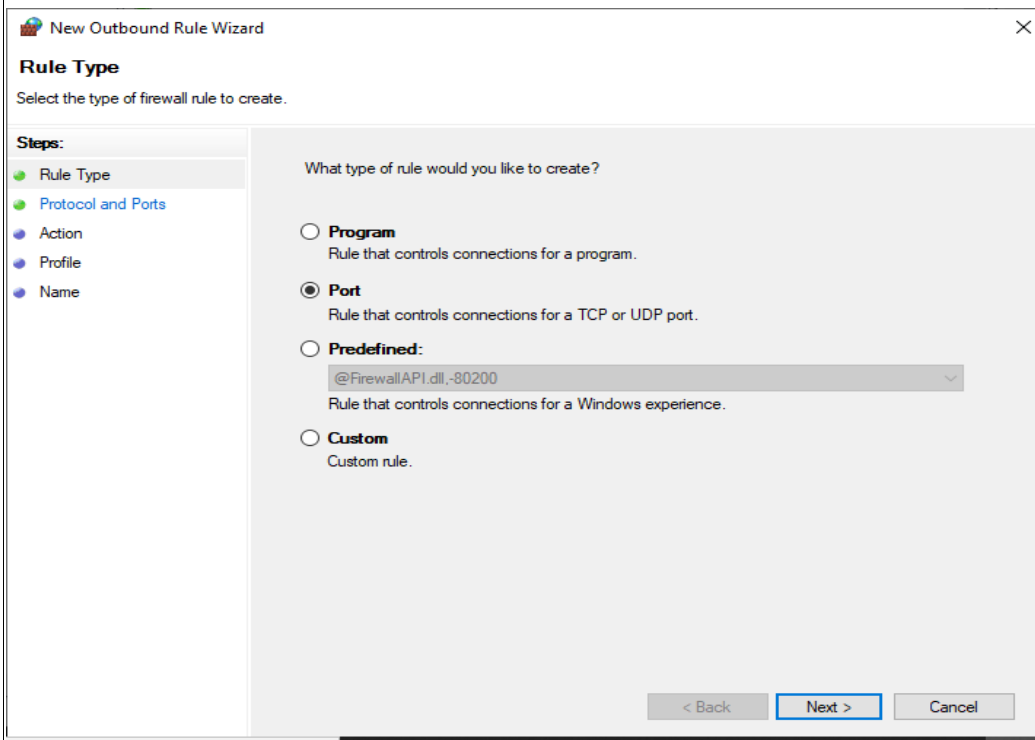
**Step 3:** Now you need to select Advanced setting.



**Step 4:** Now Select Outbound Rules.

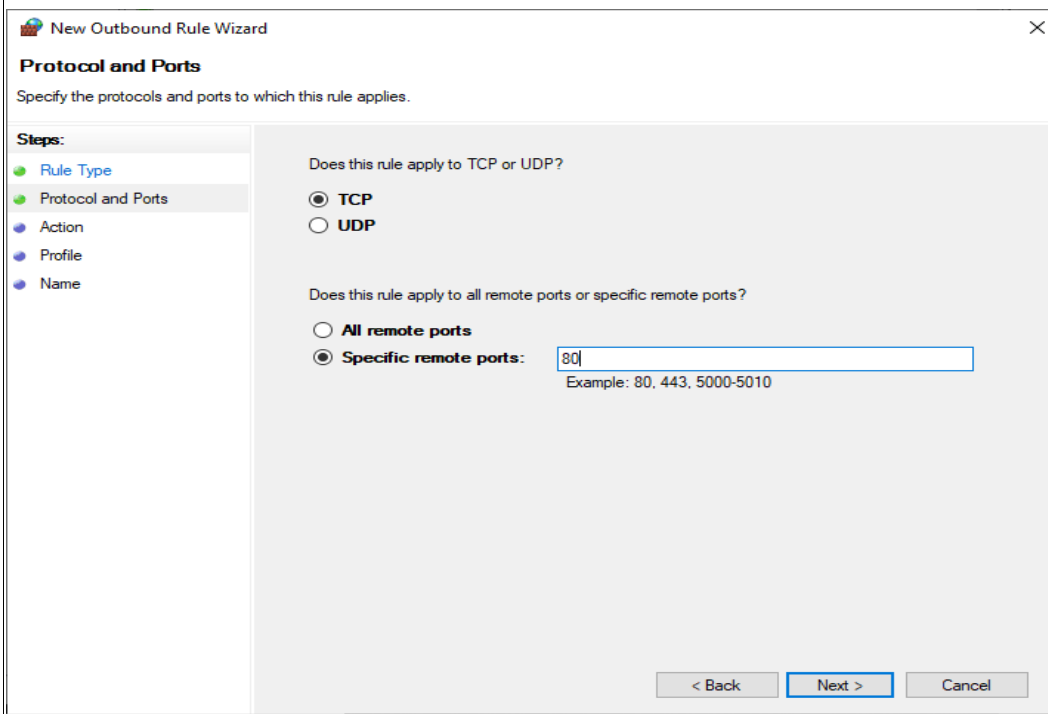


**Step 5:** Inside Outbound rules -> Select New Rules -> select Port and then click on next.

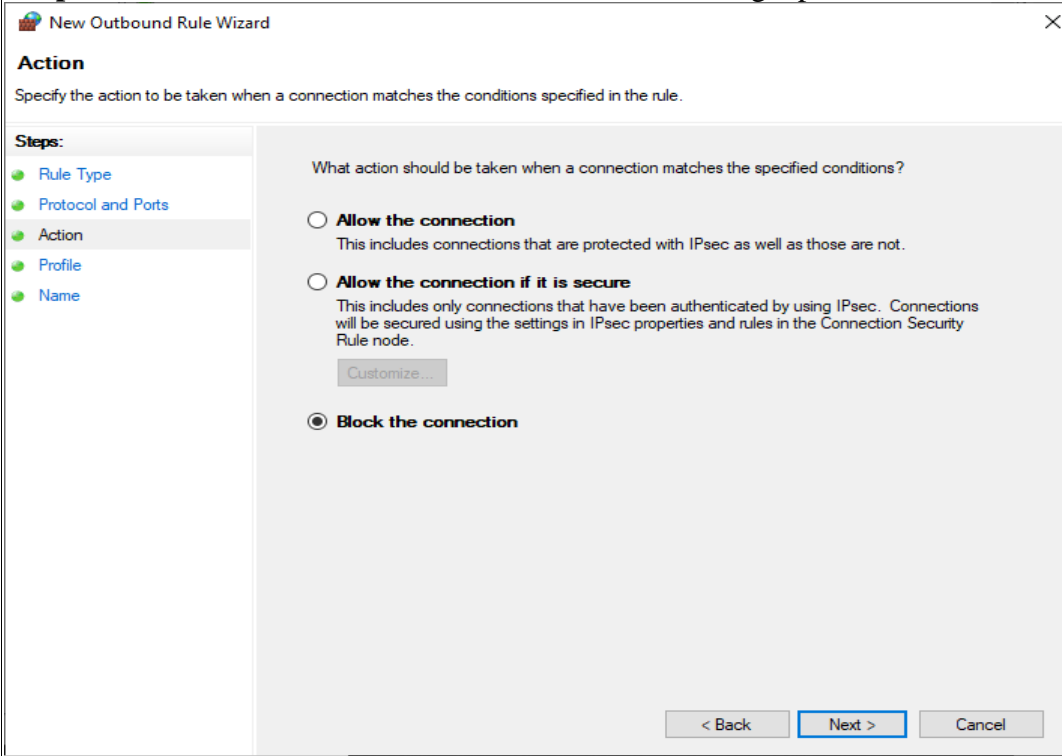


The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Rule Type' step. The title bar reads 'New Outbound Rule Wizard'. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps' pane lists: Rule Type (selected), Protocol and Ports, Action, Profile, and Name. The main area asks 'What type of rule would you like to create?' with four radio button options:   
- **Program**: Rule that controls connections for a program.   
- **Port** (selected): Rule that controls connections for a TCP or UDP port.   
- **Predefined:**: A dropdown menu shows '@FirewallAPI.dll,-80200'; the description is 'Rule that controls connections for a Windows experience.'   
- **Custom**: Custom rule.   
At the bottom right are buttons for '< Back', 'Next >' (highlighted), and 'Cancel'.

**Step 6:** Select the protocols and enter the port that you want to want to block



The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The title bar reads 'New Outbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' pane lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area has two questions:   
1. 'Does this rule apply to TCP or UDP?' with radio buttons for **TCP** (selected) and **UDP**.   
2. 'Does this rule apply to all remote ports or specific remote ports?' with radio buttons for **All remote ports** and **Specific remote ports:** (selected). The 'Specific remote ports' section has a text box containing '80' and an example text 'Example: 80, 443, 5000-5010' below it.   
At the bottom right are buttons for '< Back', 'Next >' (highlighted), and 'Cancel'.

**Step 7:** Select the action block the connection for blocking a port

New Outbound 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

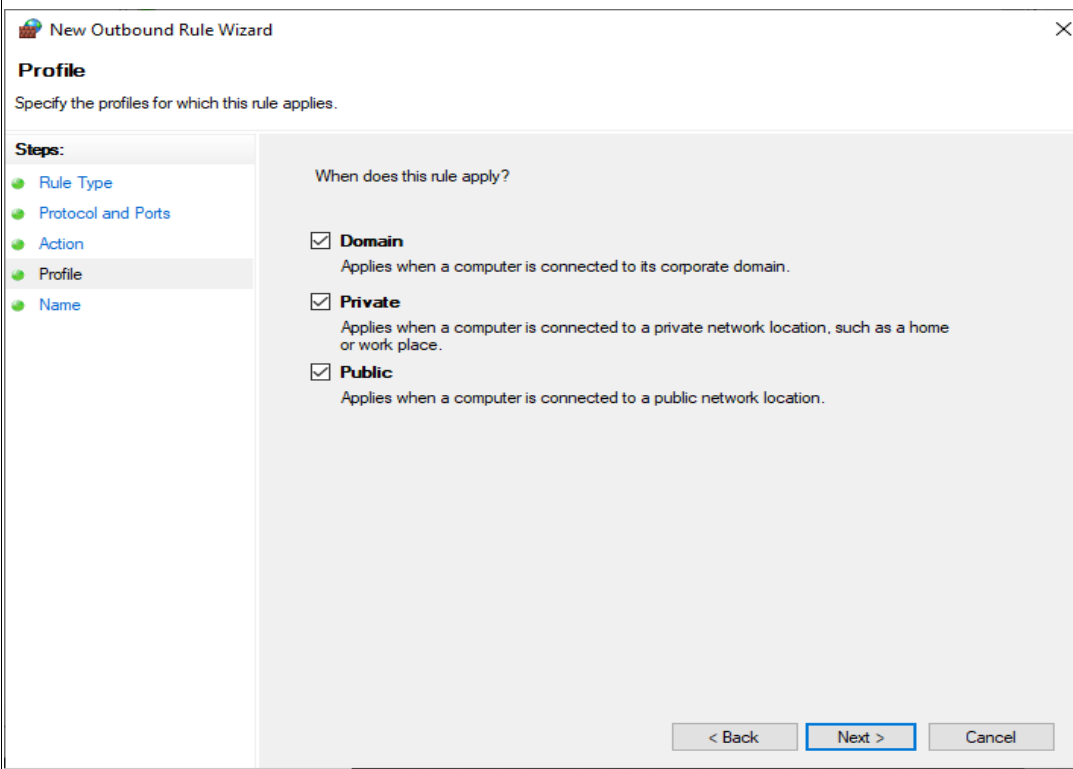
What action should be taken when a connection matches the specified conditions?

☐ **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

**Step 8:** Select the profiles domain private or public.

New Outbound 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?

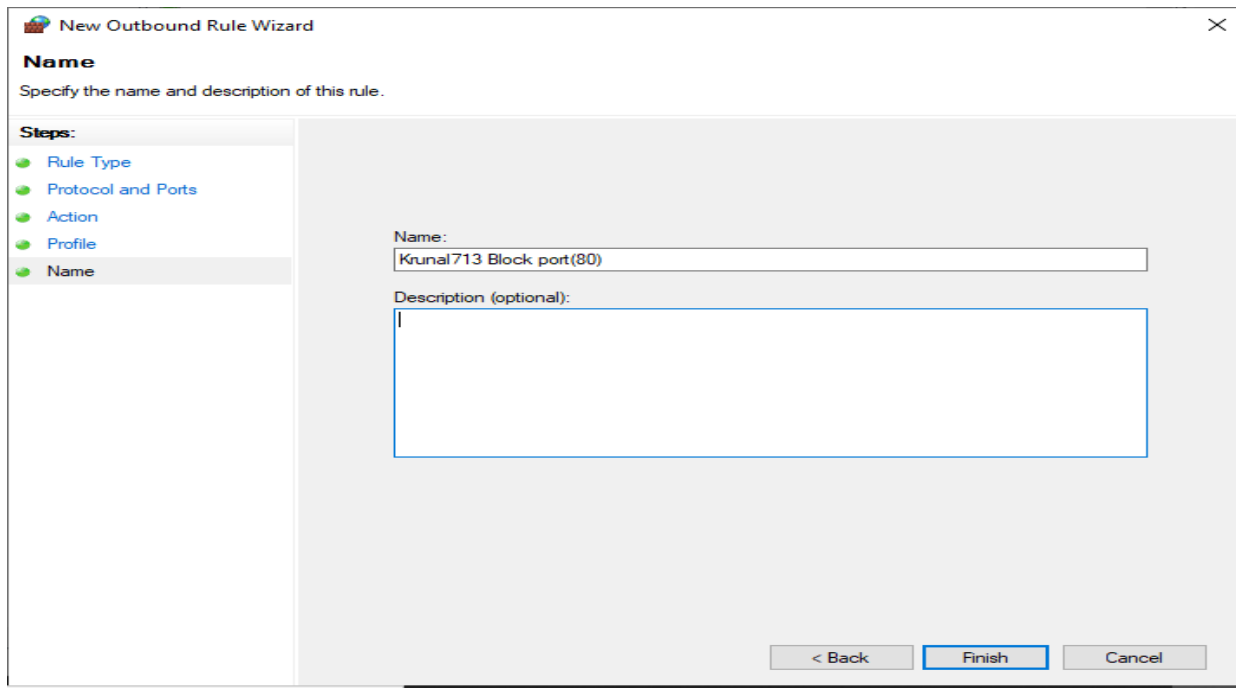
☒ **Domain**  
Applies when a computer is connected to its corporate domain.

☒ **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

**Step 9:** Give a name to our new set rule and click on finish.



**New Outbound Rule Wizard**

**Name**  
Specify the name and description of this rule.

**Steps:**

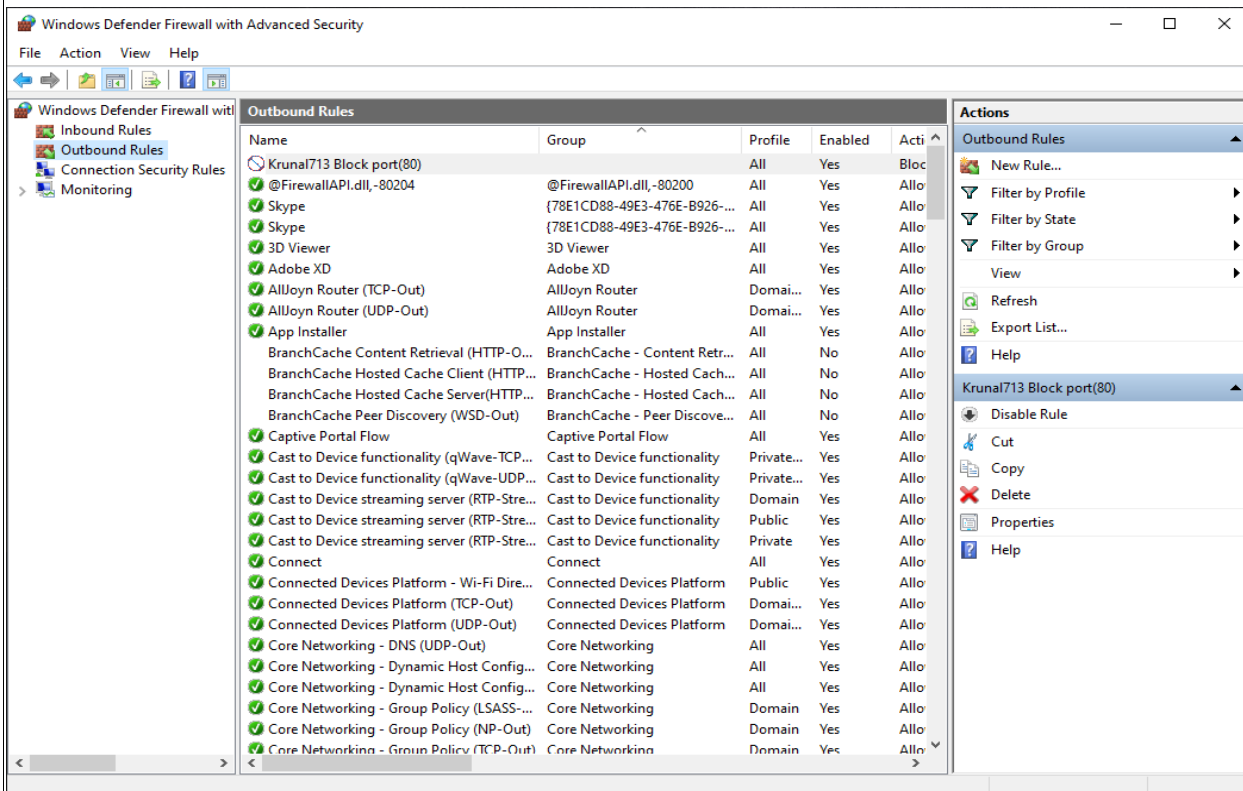
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name: Krunal713 Block port(80)

Description (optional):

< Back Finish Cancel

**Output:**



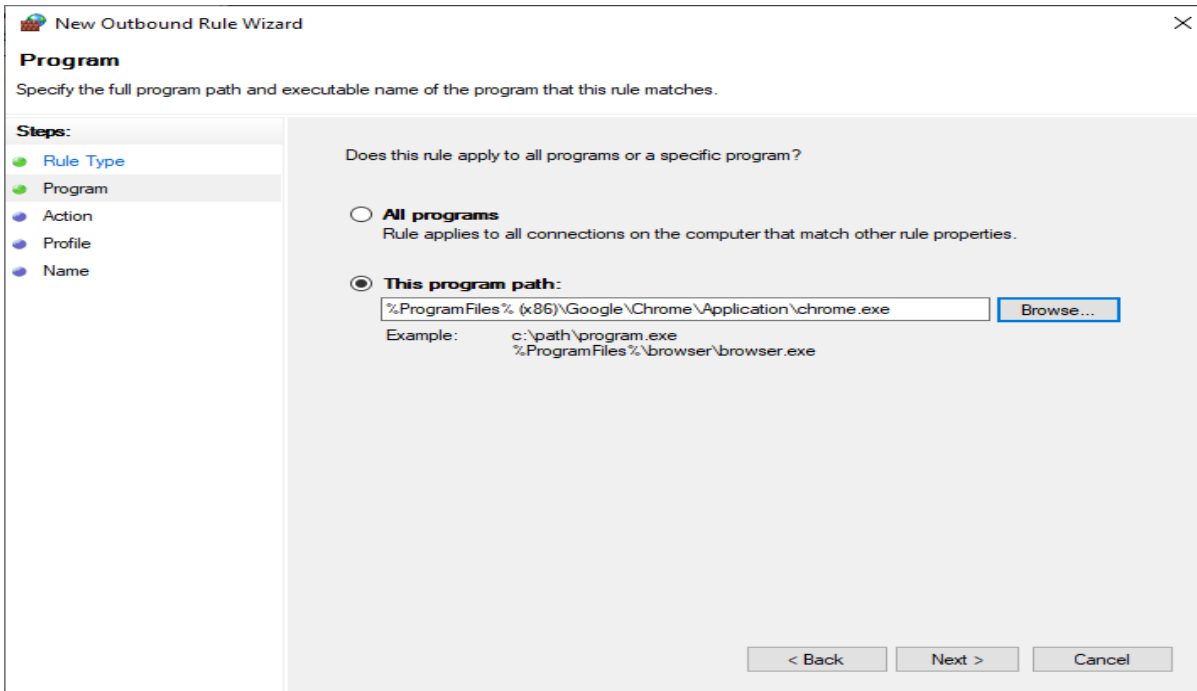
**B) Blocking a program:****Rule that controls the connection of a program**

**Step1: Repeat PartA Step1 to Step4.**

**Step 5:** Inside Outbound rules -> Select New Rules -> select a program and then click on next.

The screenshot shows the 'New Outbound Rule Wizard' window. The title bar says 'New Outbound Rule Wizard' with a close button. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps:' list shows 'Rule Type' as the current step, followed by 'Program', 'Action', 'Profile', and 'Name'. The main area asks 'What type of rule would you like to create?' and offers four options: 'Program' (selected), 'Port', 'Predefined:', and 'Custom'. The 'Program' option is described as 'Rule that controls connections for a program.' The 'Port' option is 'Rule that controls connections for a TCP or UDP port.' The 'Predefined:' option has a dropdown menu showing '@FirewallAPI.dll,-80200' and is described as 'Rule that controls connections for a Windows experience.' The 'Custom' option is 'Custom rule.' At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

**Step 6:** Choose the path of the program from the directory.



The screenshot shows the 'New Outbound Rule Wizard' window at the 'Program' step. The title bar reads 'New Outbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program (selected), Action, Profile, and Name. The main area asks 'Does this rule apply to all programs or a specific program?'. There are two radio button options: 'All programs' (unselected) and 'This program path:' (selected). Below the selected option is a text box containing '%ProgramFiles%\Google\Chrome\Application\chrome.exe' and a 'Browse...' button. An example shows 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

**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.

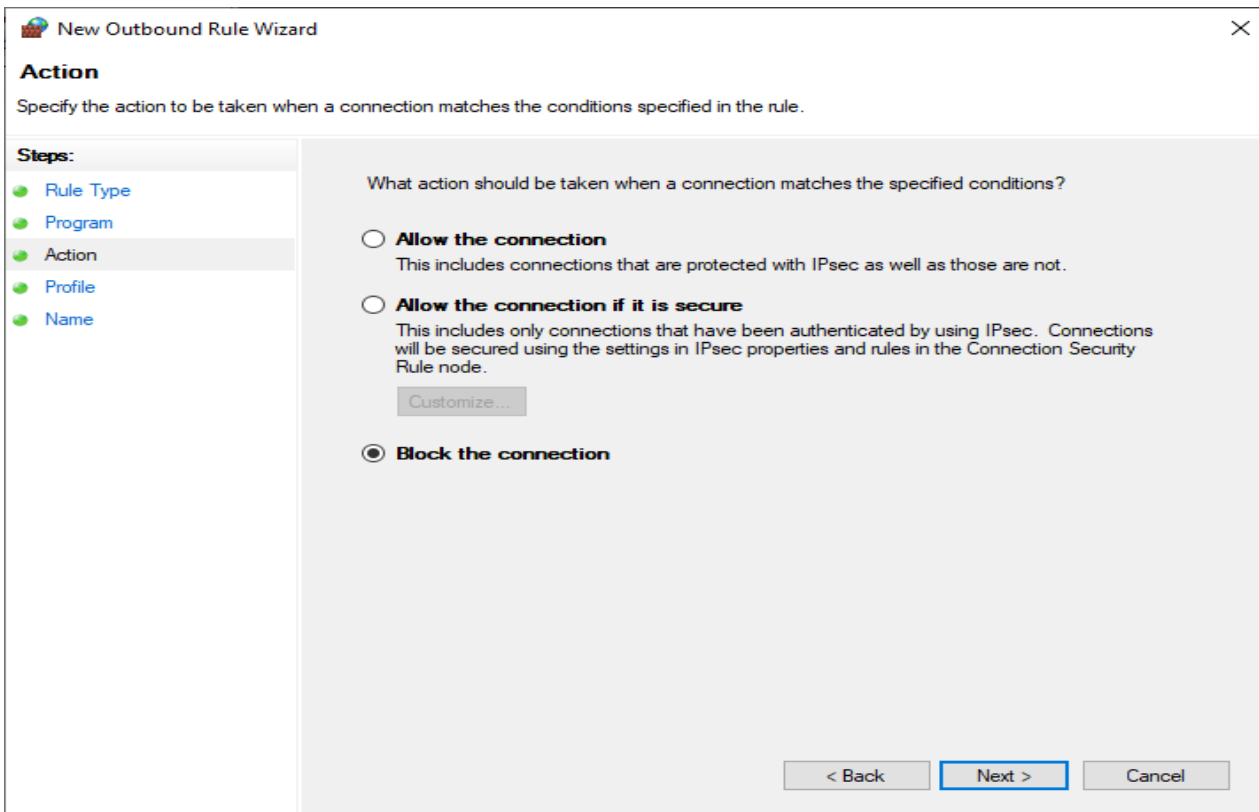
☒ **This program path:**

%ProgramFiles%\Google\Chrome\Application\chrome.exe **Browse...**

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

< Back   Next >   Cancel

**Step 7:** Click on Block the connection.



The screenshot shows the 'New Outbound Rule Wizard' window at the 'Action' step. The title bar reads 'New Outbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, Action (selected), Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (unselected), 'Allow the connection if it is secure' (unselected), and 'Block the connection' (selected). Below the first two options are descriptions. A 'Customize...' button is visible under the second option. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

**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.

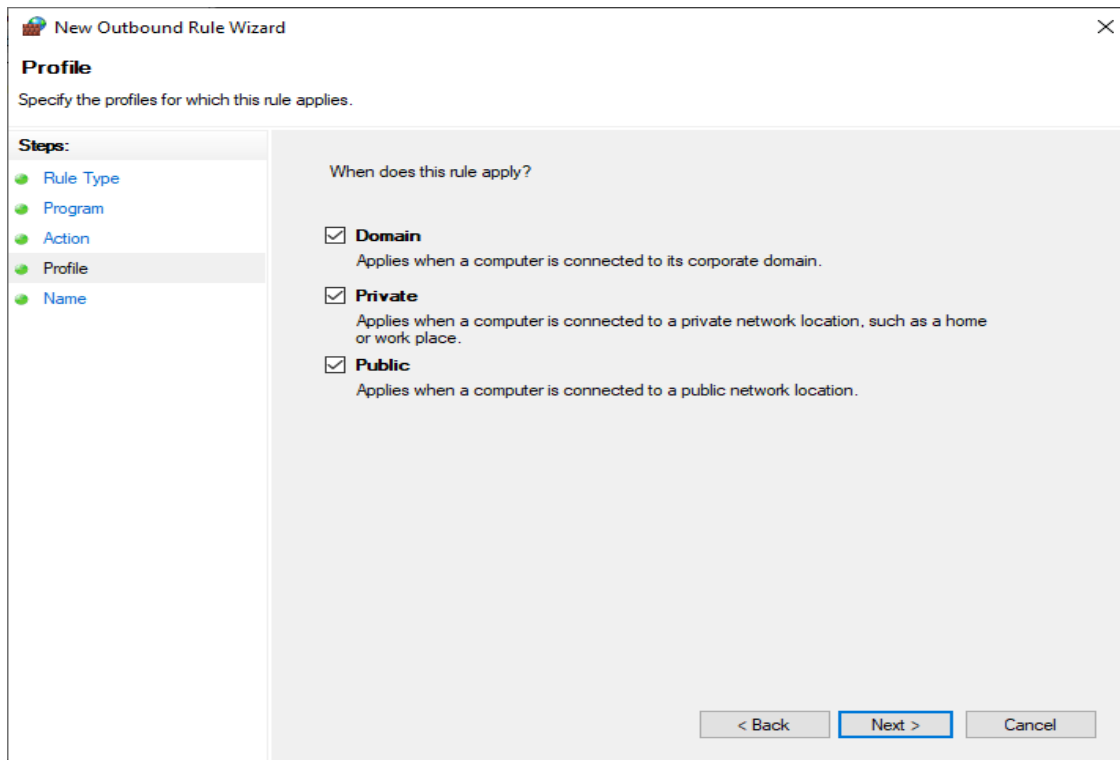
☐ **Allow the connection if it is secure**  
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.  
**Customize...**

☒ **Block the connection**

< Back   **Next >**   Cancel

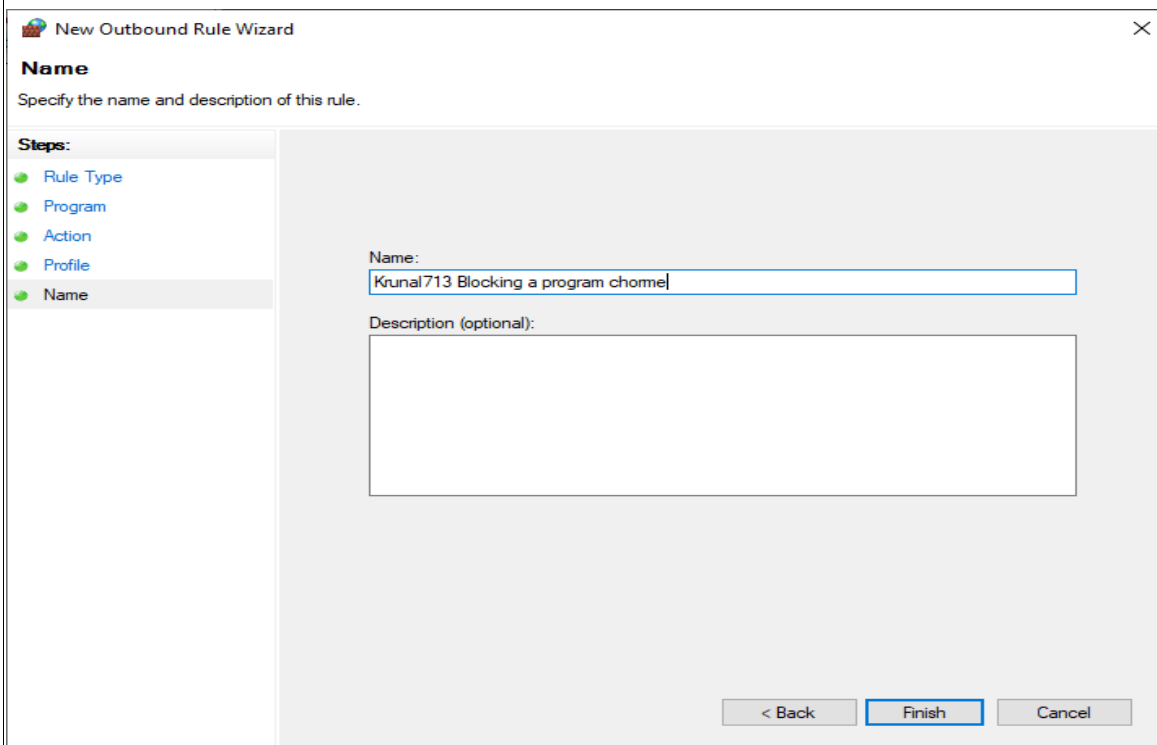


**Step 8:** Select the profiles domain private or public.

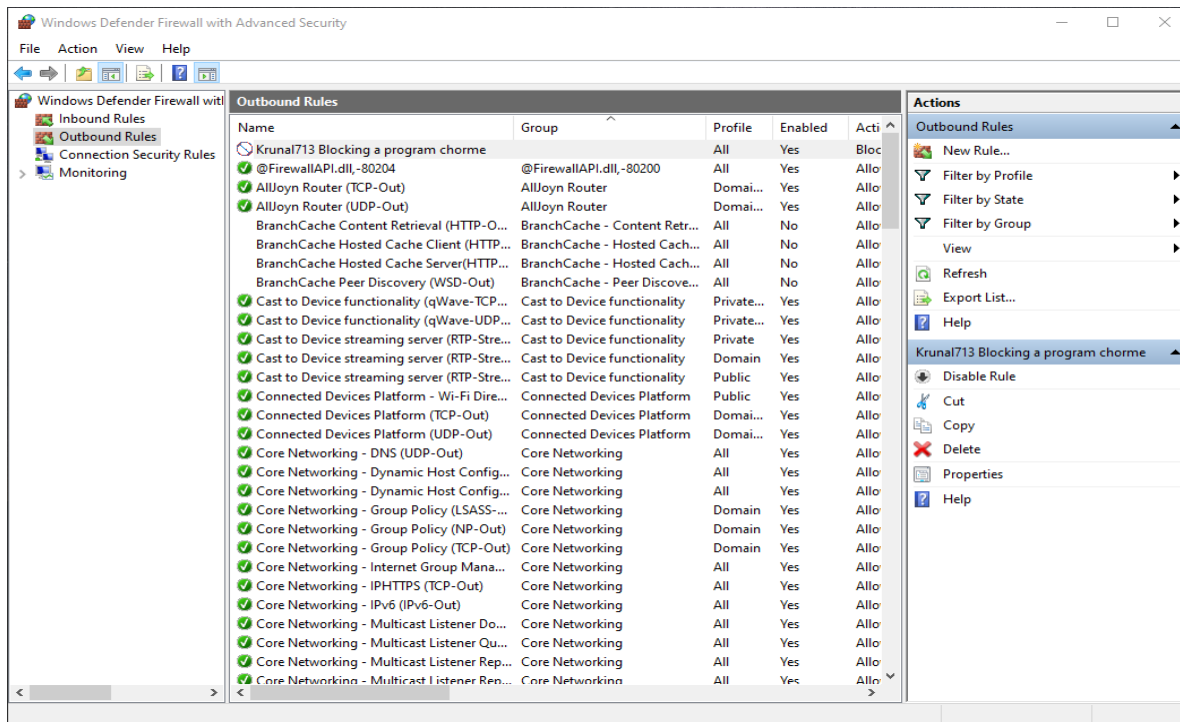
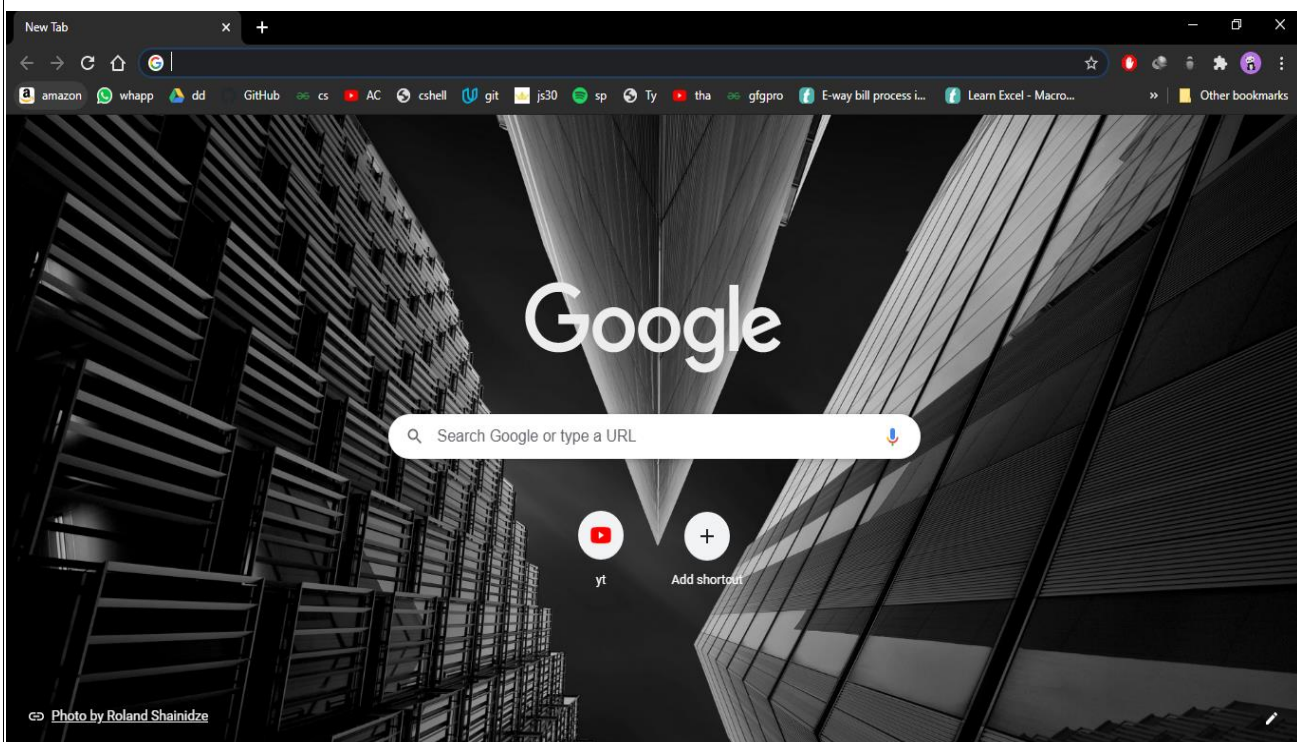


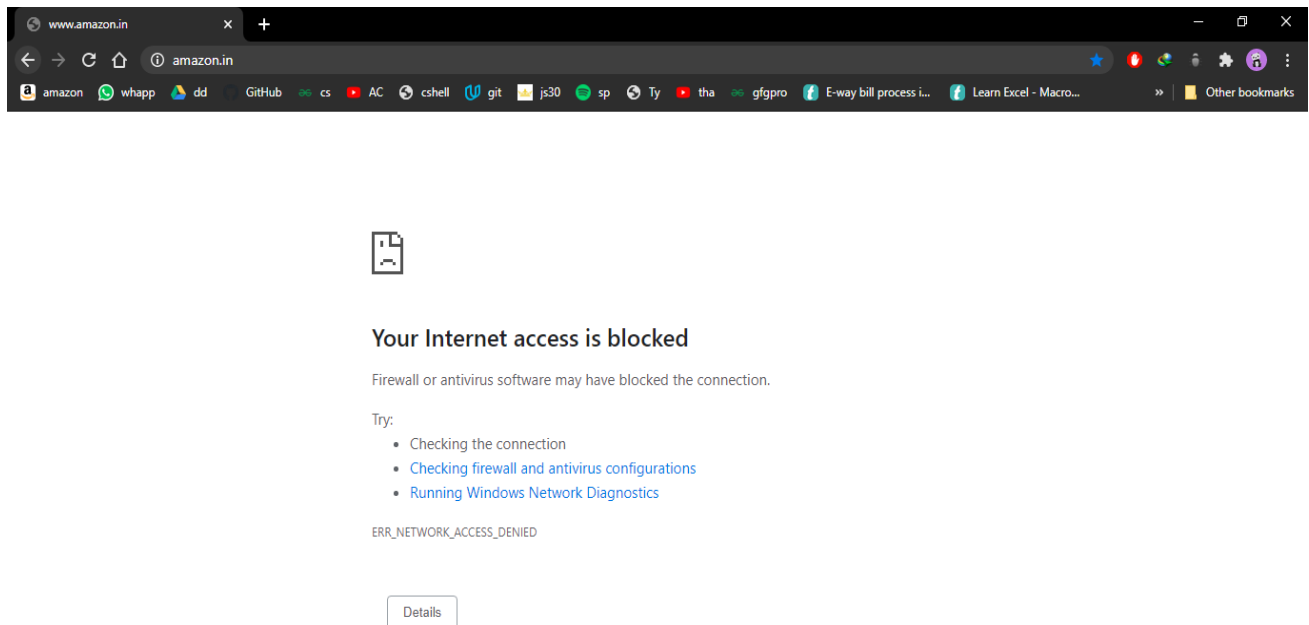
The screenshot shows the 'New Outbound Rule Wizard' window at the 'Profile' step. The title bar reads 'New Outbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Action', 'Profile' (highlighted), and 'Name'. The main area is titled 'When does this rule apply?' and 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 buttons for '< Back', 'Next >', and 'Cancel'.

**Step 9:** Give a name to your new set rule and click on finish.



The screenshot shows the 'New Outbound Rule Wizard' window at the 'Name' step. The title bar reads 'New Outbound Rule Wizard'. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Action', 'Profile', and 'Name' (highlighted). The main area has a 'Name:' label followed by a text box containing 'Krunal713 Blocking a program chrome|'. Below it is a 'Description (optional):' label followed by a large empty text box. At the bottom right are buttons for '< Back', 'Finish', and 'Cancel'.

**Output:****Before Applying the Rule:**

**After Applying the Rule:**

**C) Blocking a website:****Step1: Repeat PartA Step1 to Step4.****Step 5:** Inside Outbound rules -> Select New Rules -> select custom and then click on next.

**New Outbound 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.

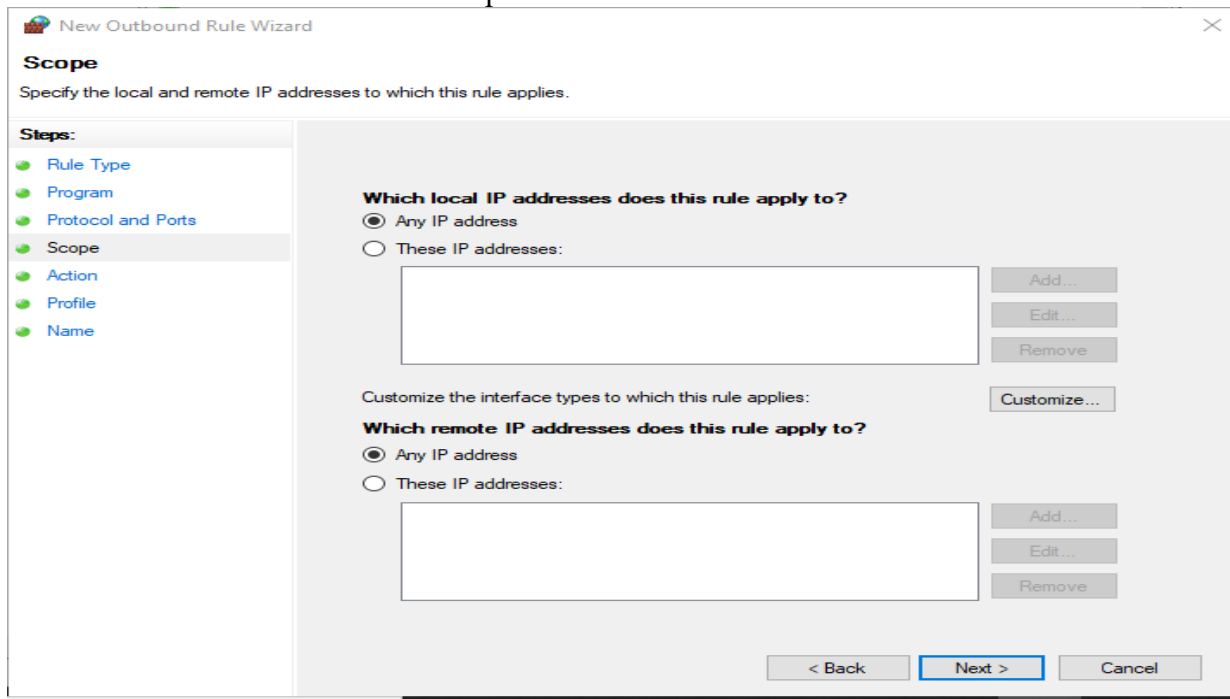
☐ **Port**  
Rule that controls connections for a TCP or UDP port.

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

☒ **Custom**  
Custom rule.

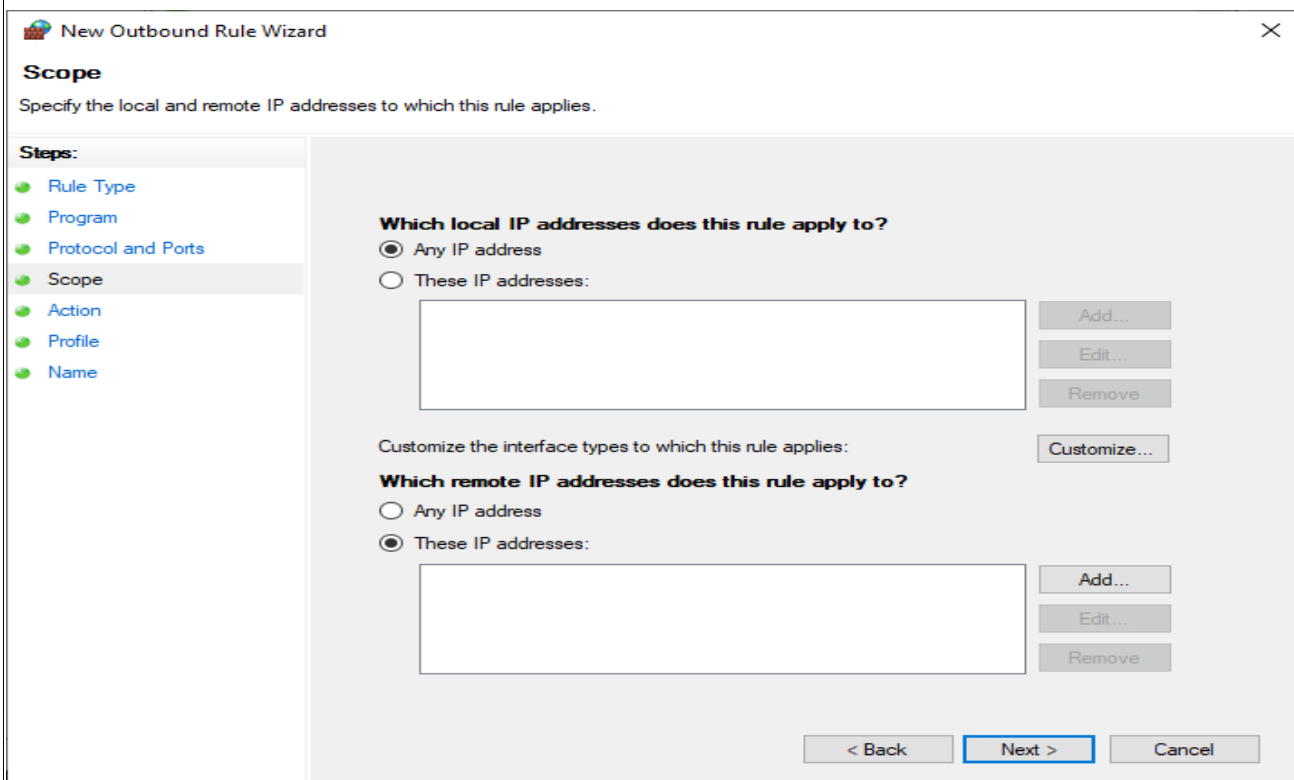
< Back   Next >   Cancel

**Step 6:** When you click next you would see a window where you will see “Steps:” on left hand side of the screen. From that select “Scope”.



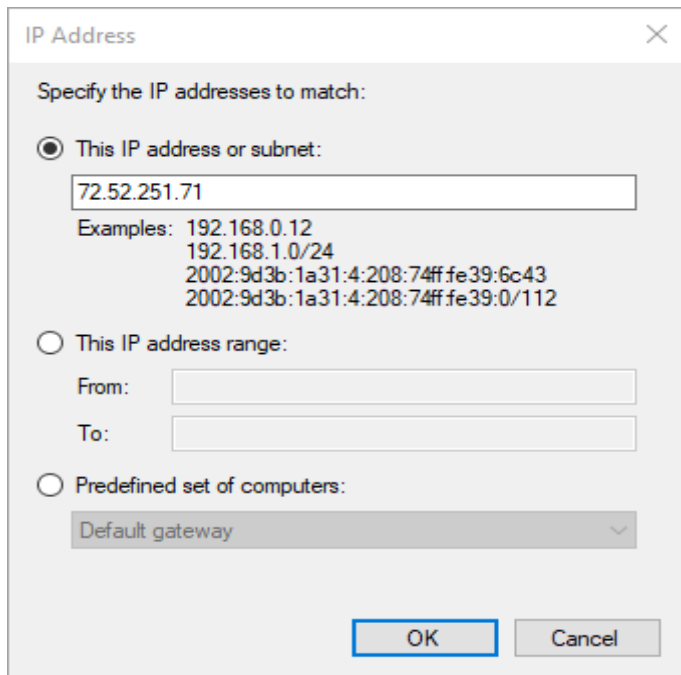
The screenshot shows the 'New Outbound Rule Wizard' window at the 'Scope' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope (selected), Action, Profile, and Name. The main area is titled 'Specify the local and remote IP addresses to which this rule applies.' It contains two sections: 'Which local IP addresses does this rule apply to?' and 'Which remote IP addresses does this rule apply to?'. Each section has two radio buttons: 'Any IP address' (selected) and 'These IP addresses:'. Below each 'These IP addresses:' option is a text box and three buttons: 'Add...', 'Edit...', and 'Remove...'. There is also a 'Customize...' button for interface types. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

**Step 7:** In scope click on These IP addresses in remote IP



This screenshot is similar to the previous one, but in the 'Which remote IP addresses does this rule apply to?' section, the 'These IP addresses:' radio button is selected instead of 'Any IP address'. The rest of the window, including the sidebar and other options, remains the same.

**Step 8:** Click on add and Add the IP address of the website that you want to block and click ok.



IP Address

Specify the IP addresses to match:

☒ This IP address or subnet:

72.52.251.71

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:

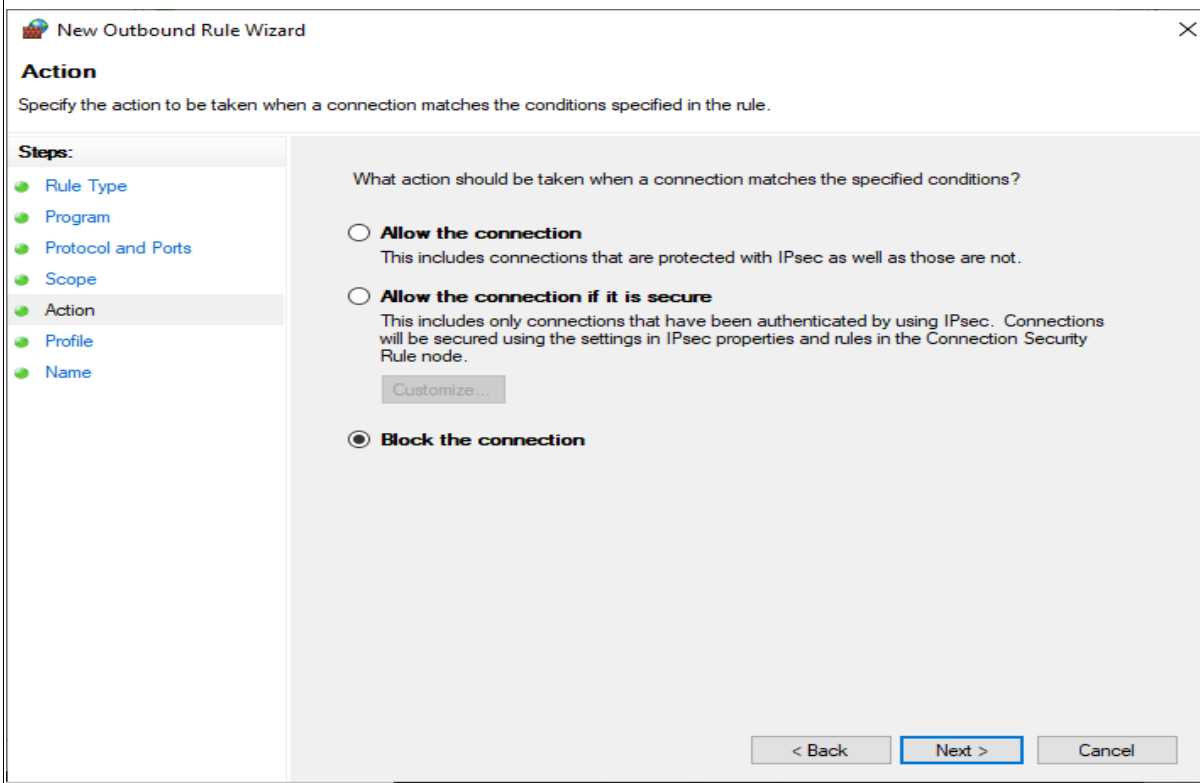
From:   
To:

☐ Predefined set of computers:

Default gateway

OK Cancel

**Step 9:** Click on Block the connection in action



New Outbound 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?

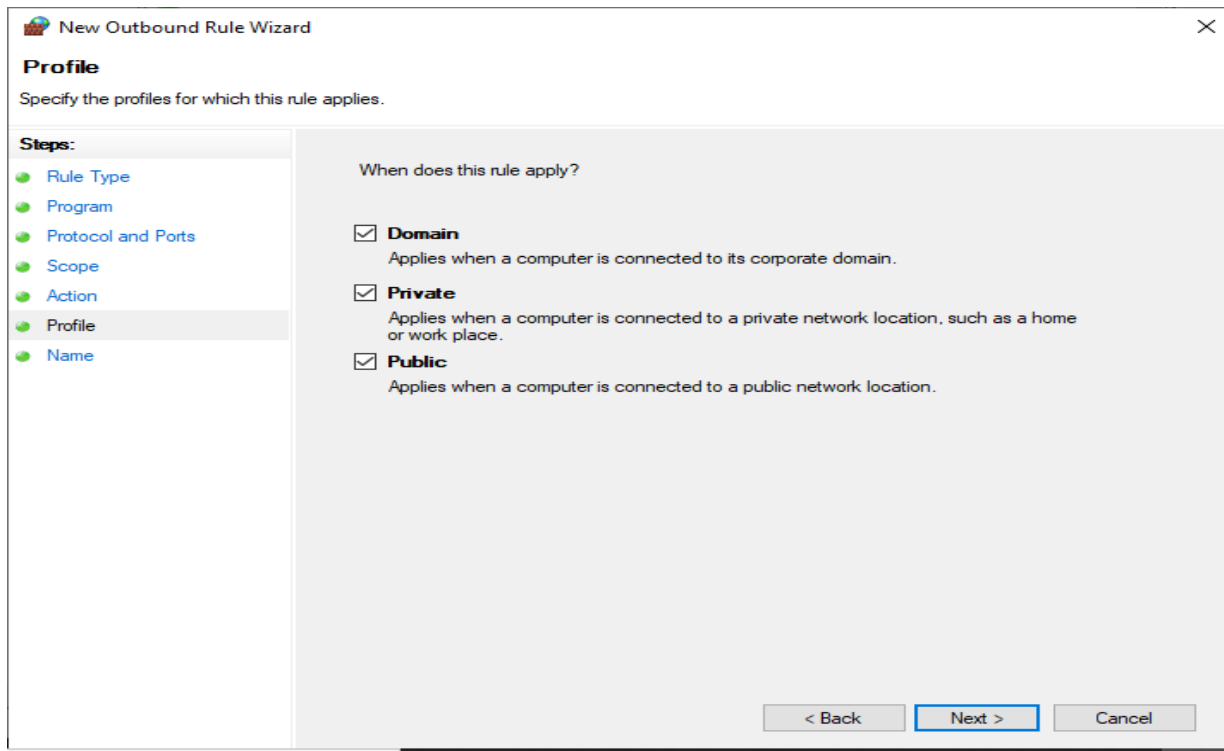
☐ **Allow the connection**  
This includes connections that are protected with IPsec as well as those are not.

☐ **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.  
Customize...

☒ **Block the connection**

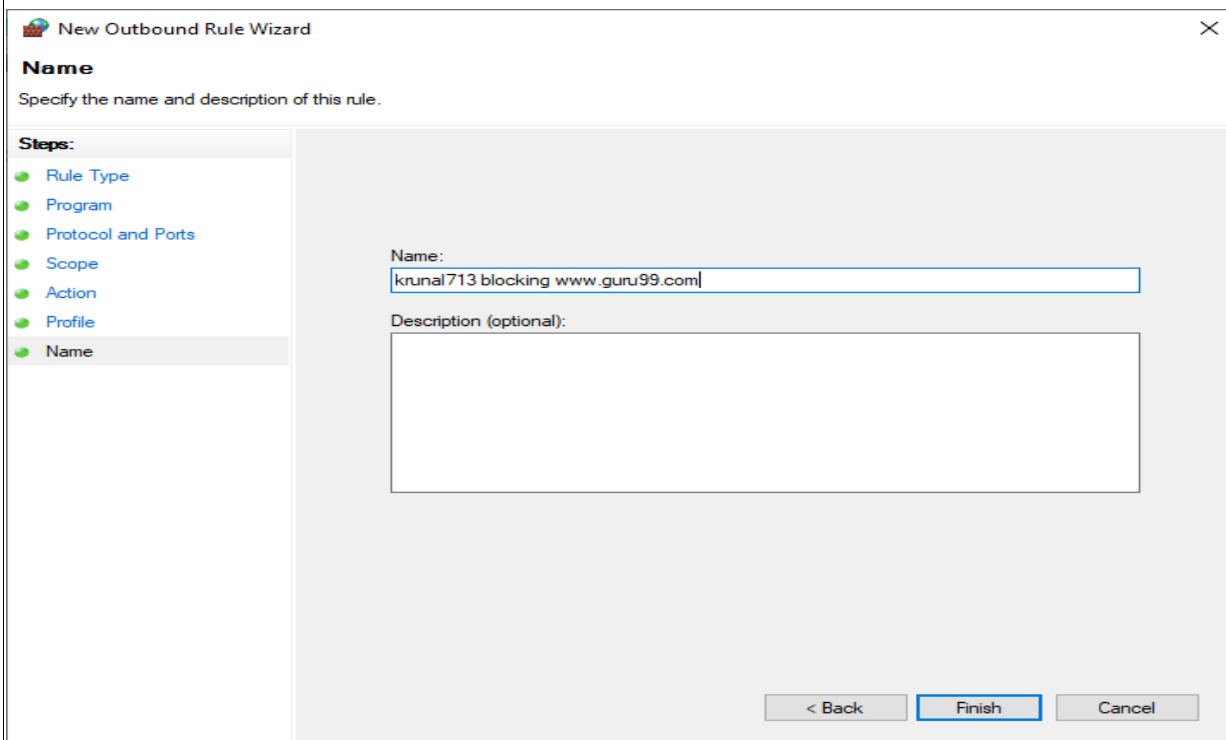
< Back Next > Cancel

**Step 10:** Select the profiles domain private or public.

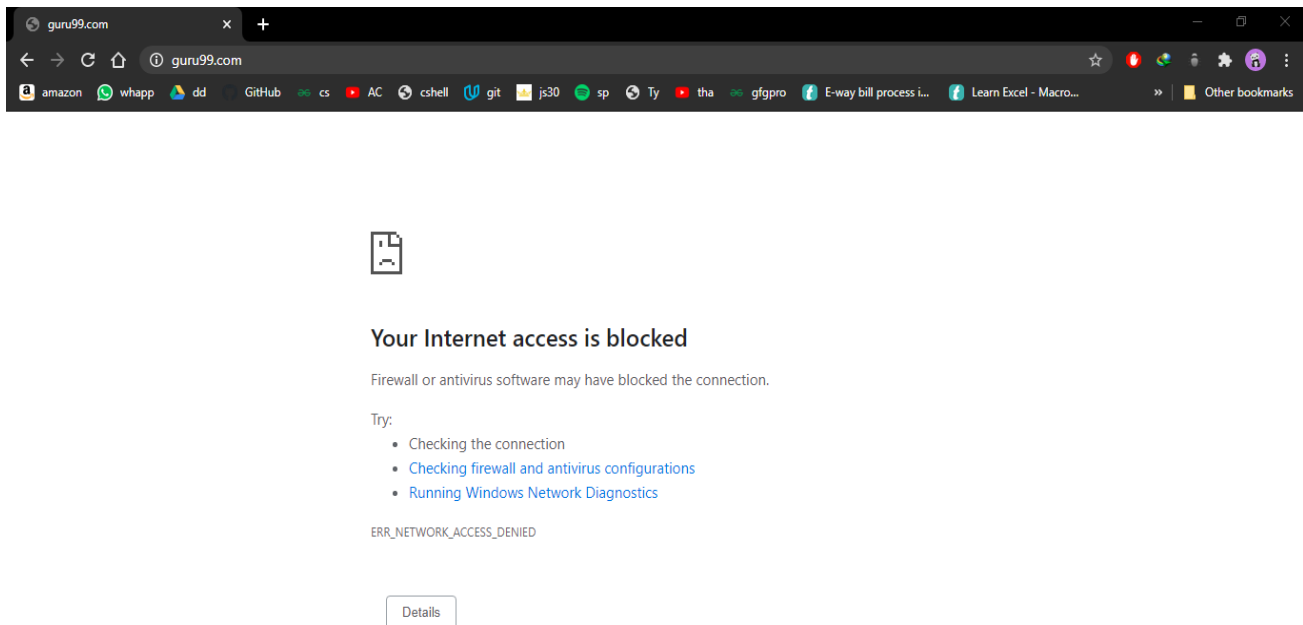


The screenshot shows the 'New Outbound Rule Wizard' window at the 'Profile' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action, Profile (selected), and Name. The main area is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies 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, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

**Step 11:** Give a name to your new set rule and click on finish.



The screenshot shows the 'New Outbound Rule Wizard' window at the 'Name' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action, Profile, and Name (selected). The main area is titled 'Specify the name and description of this rule.' and contains two input fields: 'Name:' with the text 'krunal713 blocking www.guru99.com' and 'Description (optional):' with an empty text area. At the bottom right, there are three buttons: '< Back', 'Finish' (highlighted with a blue border), and 'Cancel'.

**Output:**

```
Command Prompt

C:\Users\BlackBot>ping www.guru99.com

Pinging guru99.com [72.52.251.71] with 32 bytes of data:
General failure.
General failure.
General failure.
General failure.

Ping statistics for 72.52.251.71:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\BlackBot>
```