

Aim: Configure Windows Firewall to Block

A) A Port

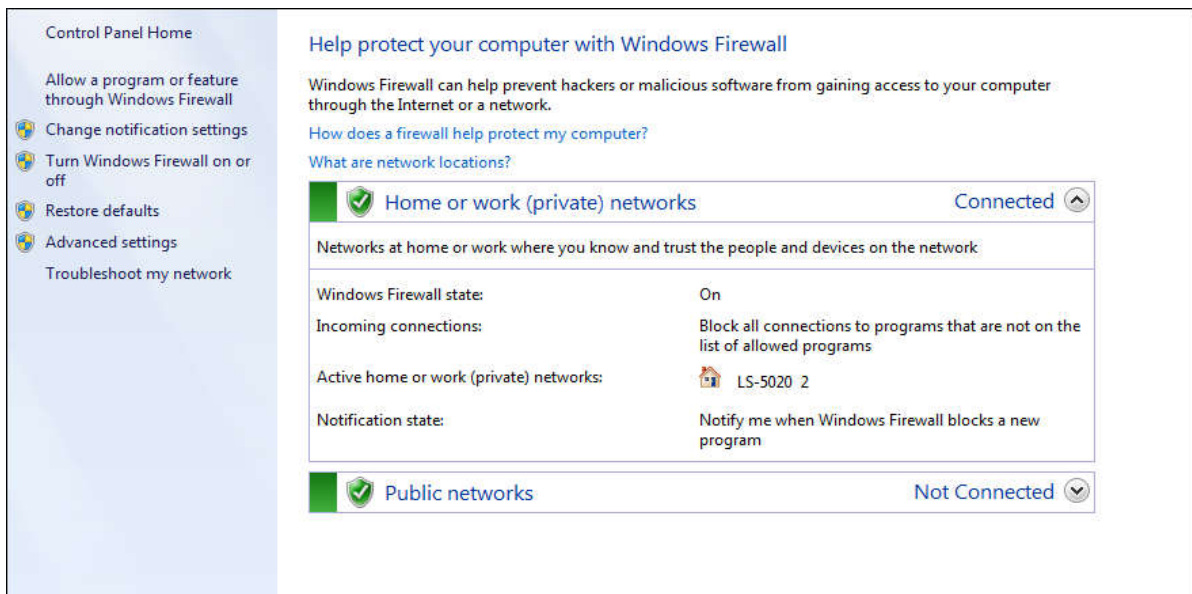
B) A Program

C) A Website

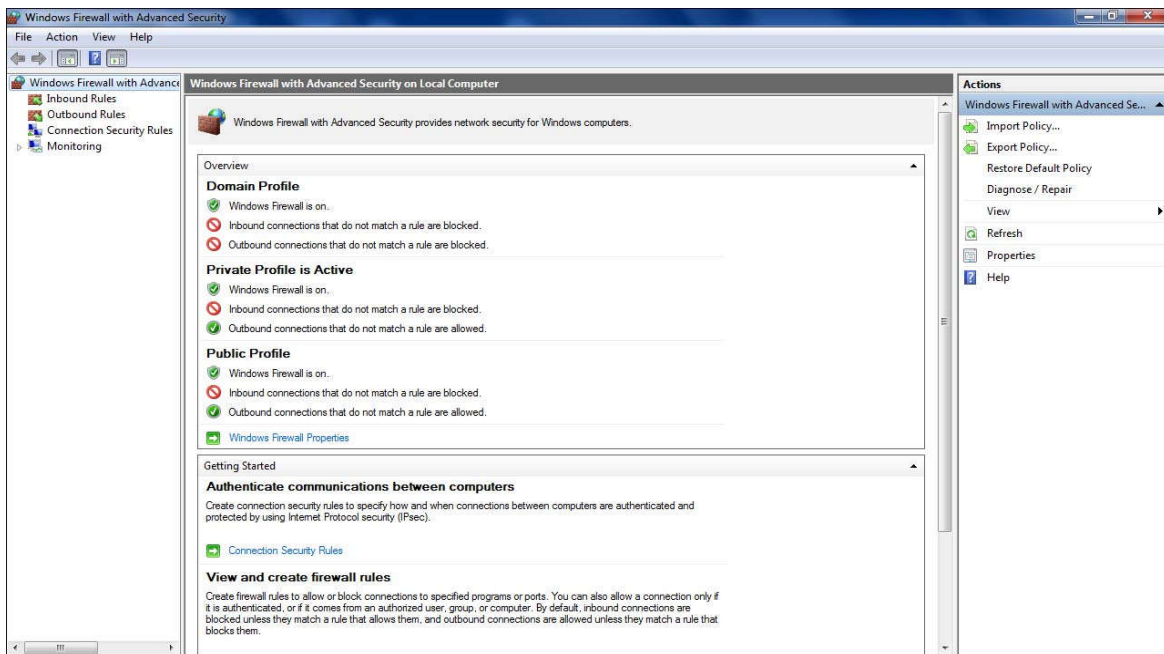
Steps:

A) A Port

1. Click on the Control Panel > System Security > Windows Firewall. The below screen will appear.



2. Click on Advanced Settings and below screen will appear.

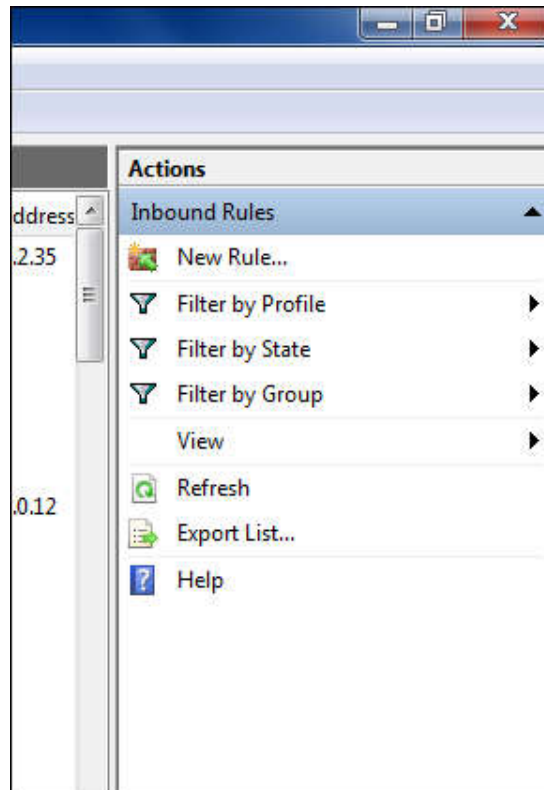


3. Click on Inbound Rules in the left side to display the inbound rules action .

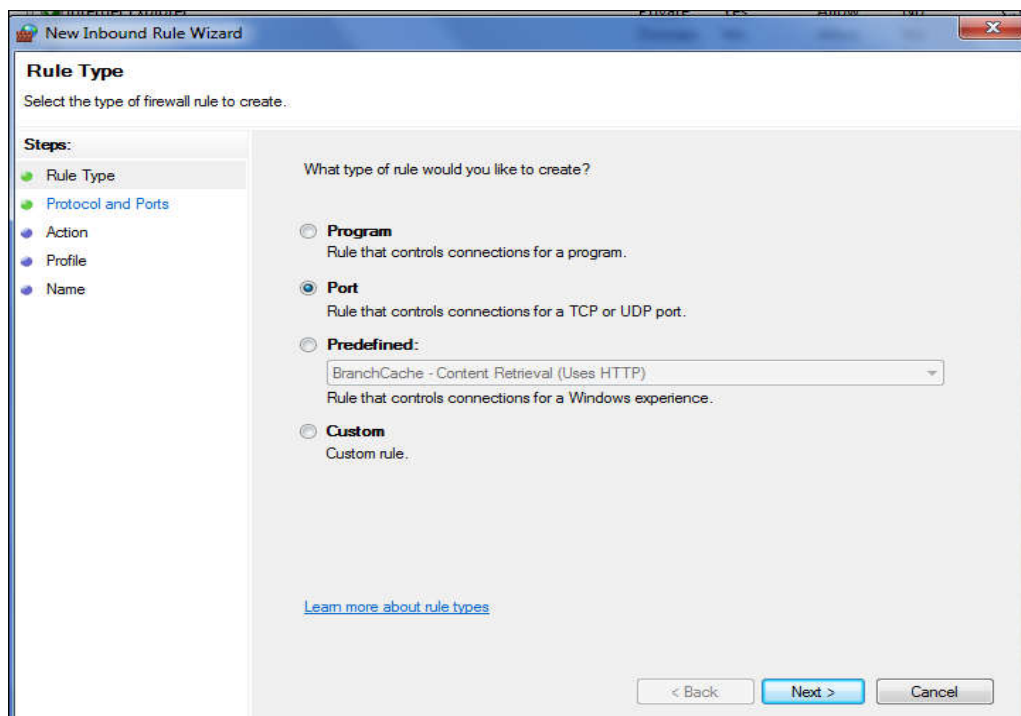
The screenshot shows the 'Inbound Rules' tab selected in the left-hand tree view. The main pane displays a list of inbound rules. Each rule is represented by a row in a table with columns for Name, Group, Profile, Enabled, Action, Override, Program, and Local Address.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
facebook		All	Yes	Block	No	Any	157.240.2.35
Internet Explorer		Private	Yes	Allow	No	C:\Progr...	Any
Internet Explorer		Private	Yes	Allow	No	C:\Progr...	Any
Internet Explorer		Domain	No	Allow	No	C:\Progr...	Any
Internet Explorer		Domain	No	Allow	No	C:\Progr...	Any
Internet Explorer		Domain	No	Allow	No	C:\Progr...	Any
Internet Explorer		Domain	No	Allow	No	C:\Progr...	Any
ip		All	No	Block	No	Any	192.168.0.12
Java(TM) Platform SE binary		Private	Yes	Allow	No	C:\progr...	Any
Java(TM) Platform SE binary		Public	Yes	Block	No	C:\progr...	Any
Java(TM) Platform SE binary		Public	Yes	Block	No	C:\progr...	Any
Java(TM) Platform SE binary		Private	Yes	Allow	No	C:\progr...	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any
Microsoft Office Outlook		Private	No	Allow	No	C:\Progr...	Any
NetBeans IDE		Private	Yes	Allow	No	C:\progr...	Any
NetBeans IDE		Private	Yes	Allow	No	C:\progr...	Any

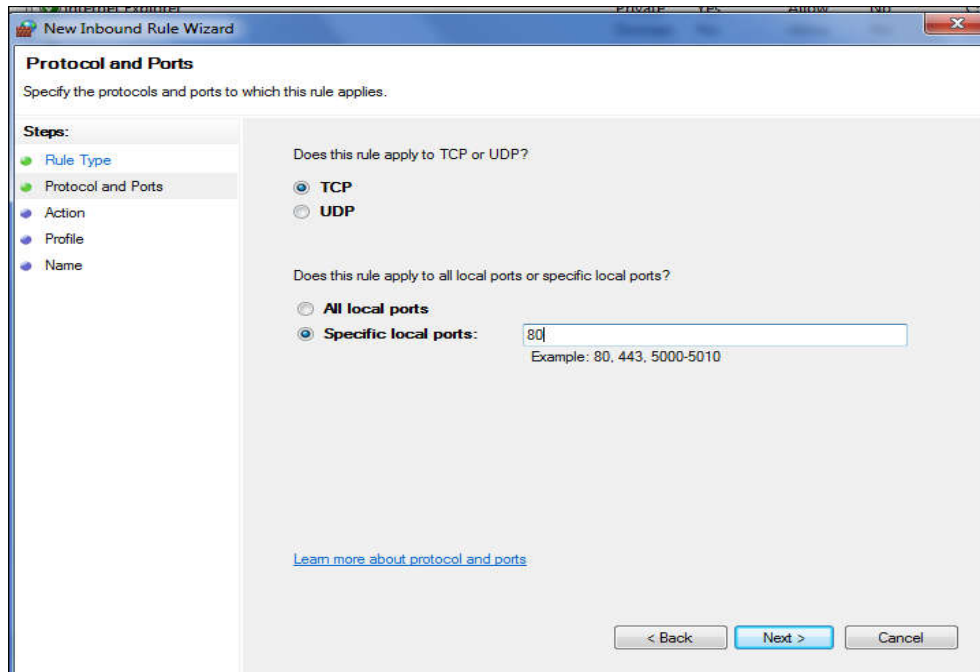
4. Click on the new rule on the right side .



5. After clicking on new rule the new inbound rule wizard will open . Select on port and click next .



6. Enter the port number i.e 80 and click next .

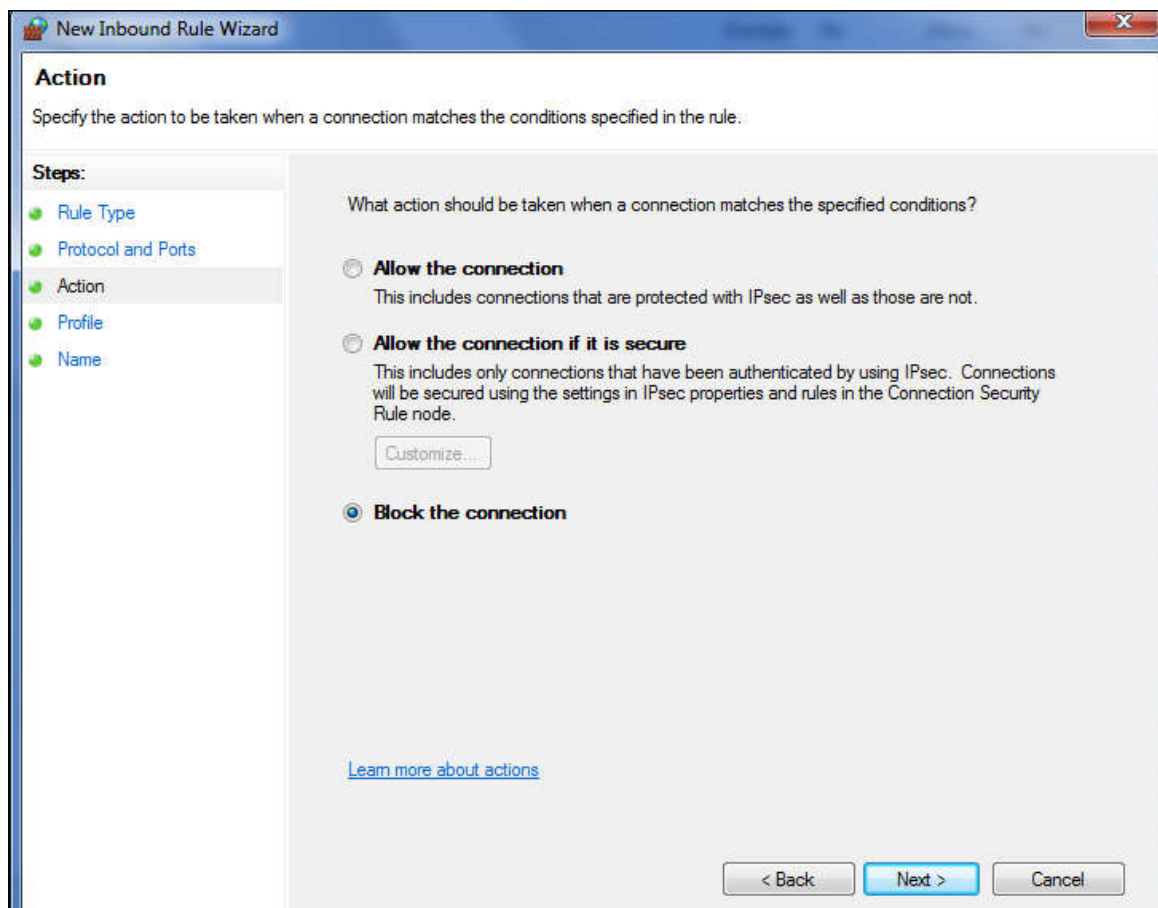


The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area contains the following options:

- 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

At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. A link 'Learn more about protocol and ports' is also present.

7. Now Select block the connection and click next .

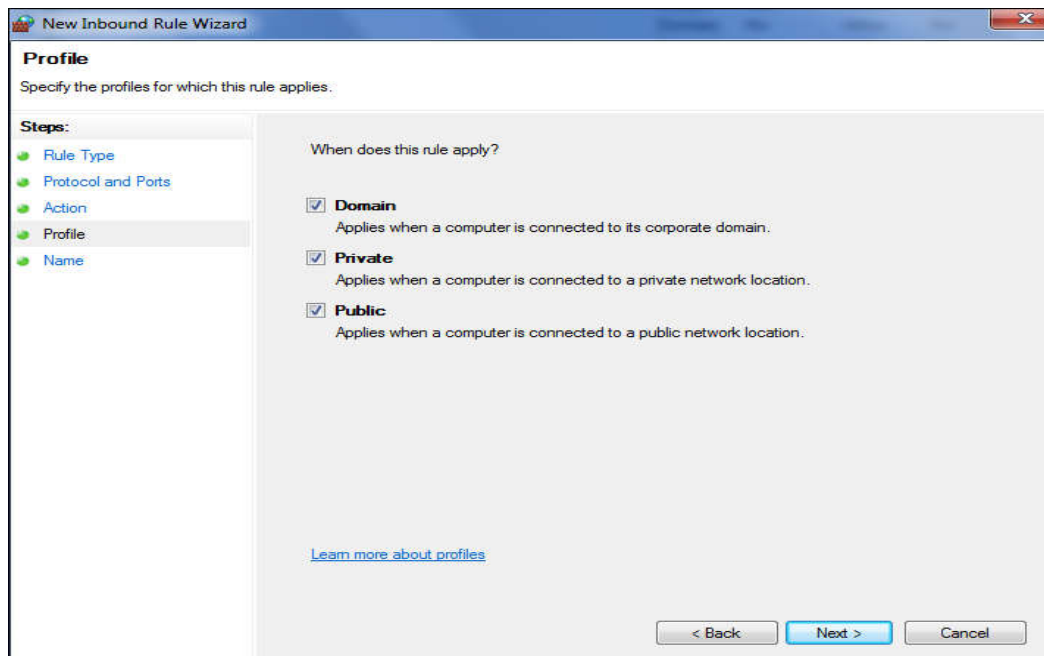


The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area contains the following options:

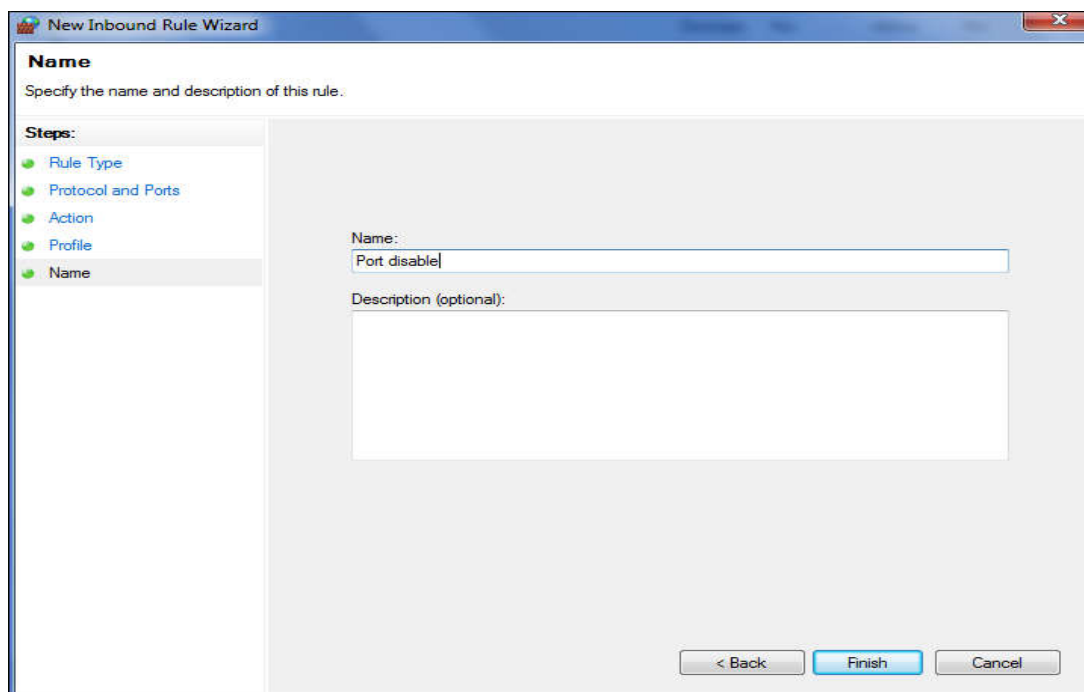
- What action should be taken when a connection matches the specified conditions?**
 - ☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.
 - ☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
 - ☒ **Block the connection**

At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. A link 'Learn more about actions' is also present.

8. Select all the profiles available on different types of connection (Domain, Private and Public) and Click next .



9. Give a specific name to the new rule and click on finish to apply the new changes.



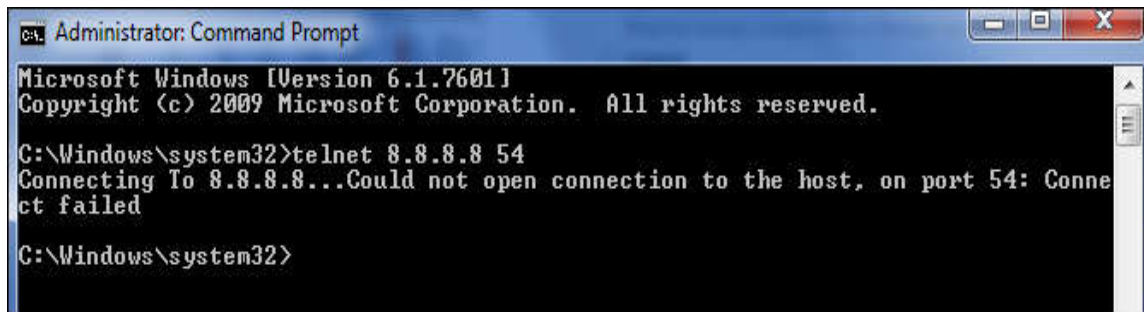
Note: Repeat all the steps for Outbound Rules

Output:

To check if the port is blocked or not:

Open command Prompt >navigate to C:>Type telnet 8.8.8.8 54

If the port is open the command will execute otherwise it will show connecting failed.



```
Administrator: Command Prompt

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

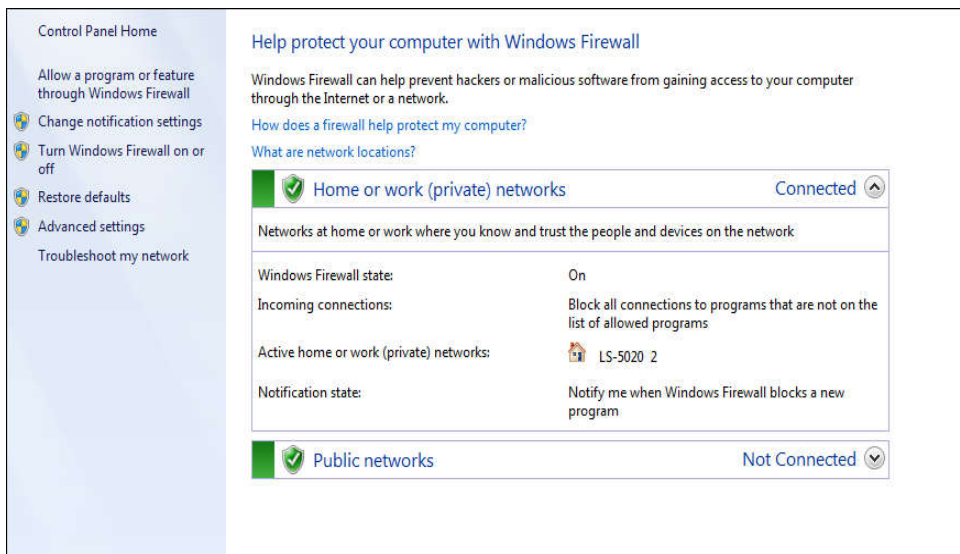
C:\Windows\system32>telnet 8.8.8.8 54
Connecting To 8.8.8.8...Could not open connection to the host, on port 54: Connection failed

C:\Windows\system32>
```

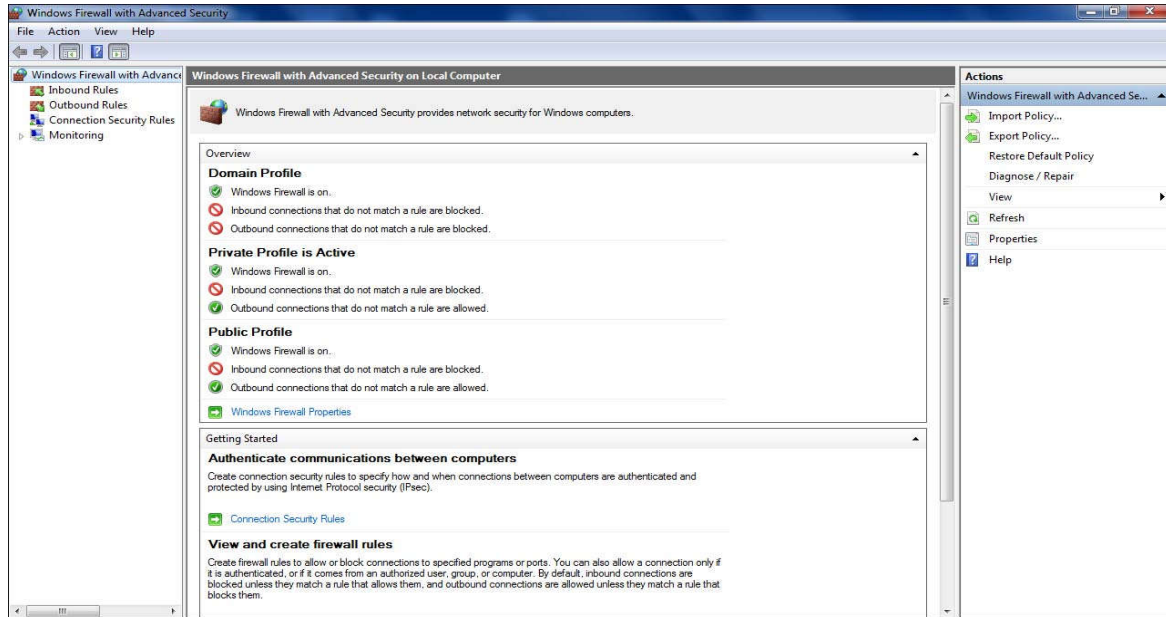
B) A Program

Steps:

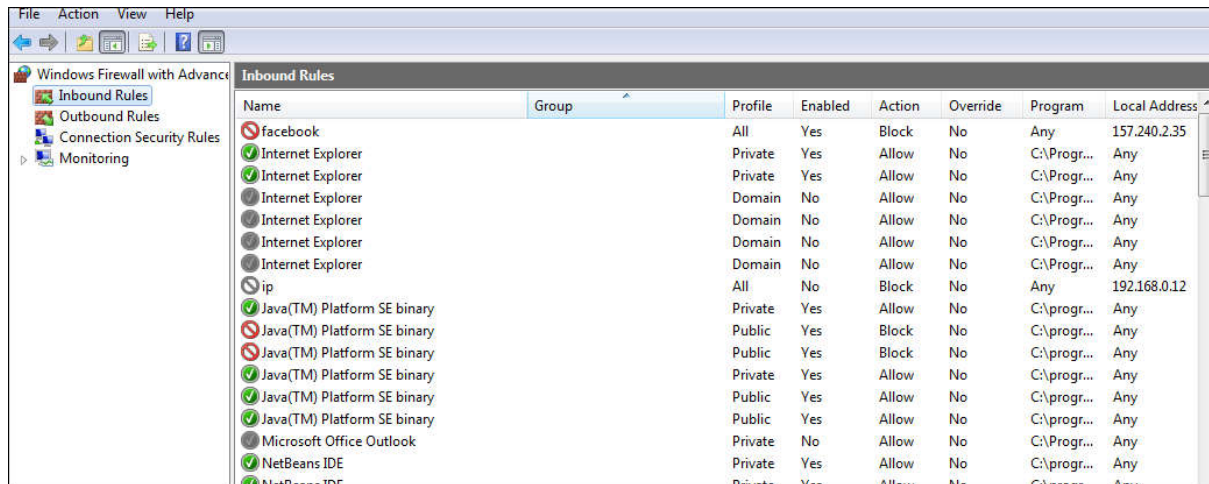
1.Click on the Control Panel> System Security> Windows Firewall. The below screen will appear.



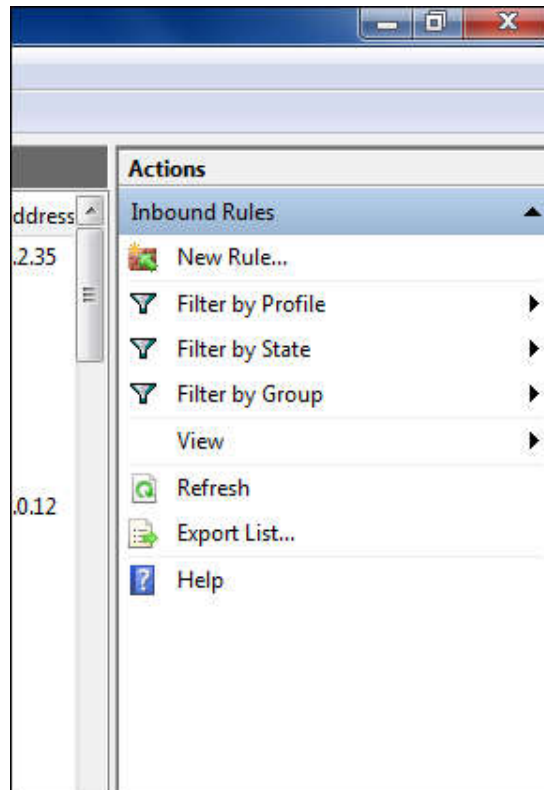
2. Click on Advanced Settings and below screen will appear.



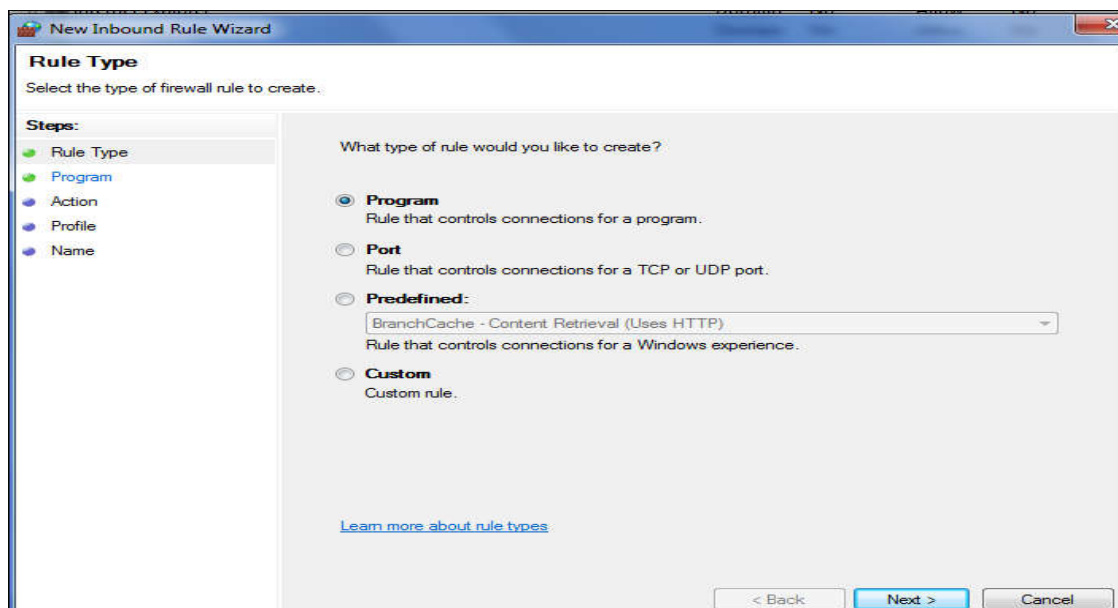
3. Click on Inbound Rules in the left side to display the inbound rules action.



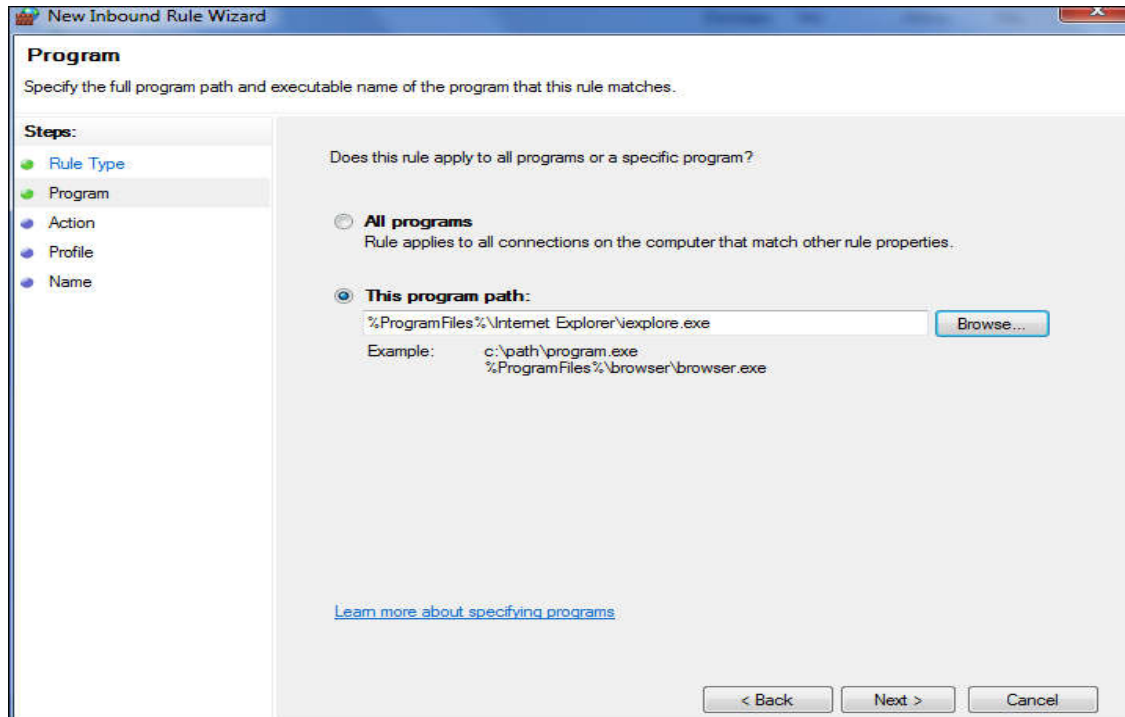
4. Click on the new rule on the right side .



5. After clicking on new rule the new inbound rule wizard will open. Select on program and click next .



6. Enter the path of the program and click next .



The screenshot shows the 'Program' step of the 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, 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' and 'This program path:'. The 'This program path:' option is selected, and a text box contains the path '%ProgramFiles%\Internet Explorer\explore.exe'. A 'Browse...' button is next to the text box. Below the text box, an 'Example:' shows two paths: 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. A link 'Learn more about specifying programs' is also present.

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.

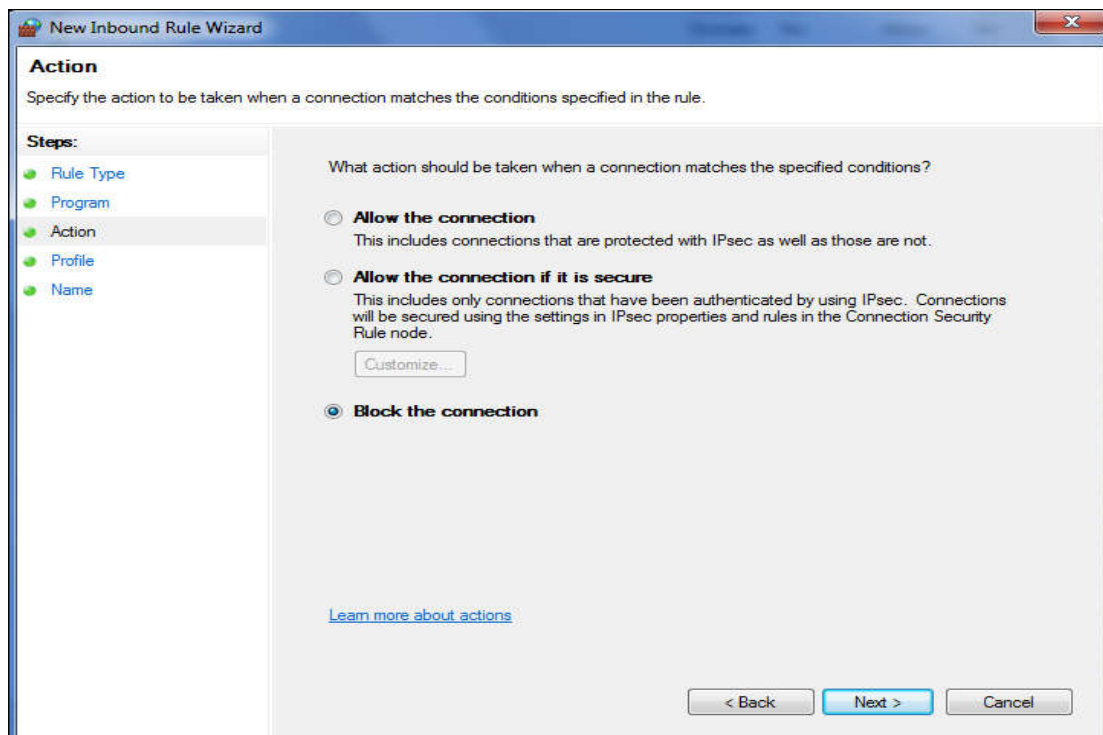
☒ **This program path:**
%ProgramFiles%\Internet Explorer\explore.exe Browse...

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

[Learn more about specifying programs](#)

< Back Next > Cancel

7. Now Select block the connection and click next



The screenshot shows the 'Action' step of the 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, Action, 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', 'Allow the connection if it is secure', and 'Block the connection'. The 'Block the connection' option is selected. Below the 'Allow the connection if it is secure' option, there is a 'Customize...' button. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. A link 'Learn more about actions' is also present.

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.

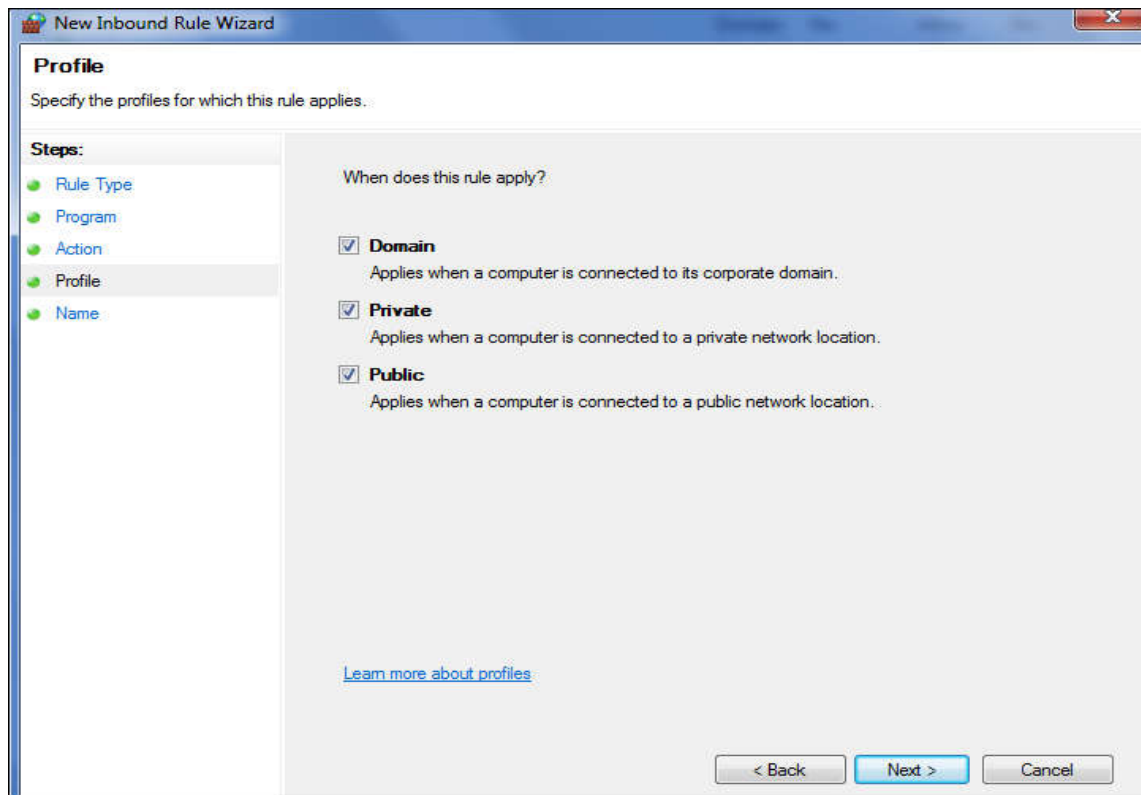
☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...

☒ **Block the connection**

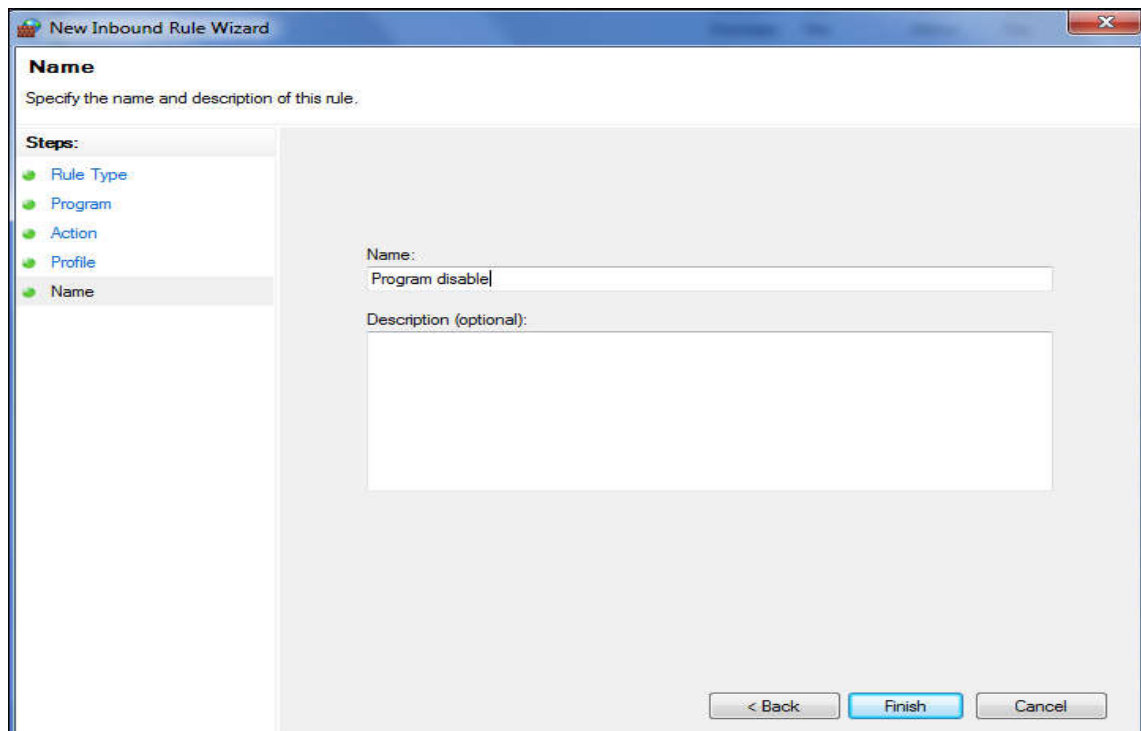
[Learn more about actions](#)

< Back Next > Cancel

8. Select all the profiles available on different types of connection (Domain, Private and Public) and Click next .

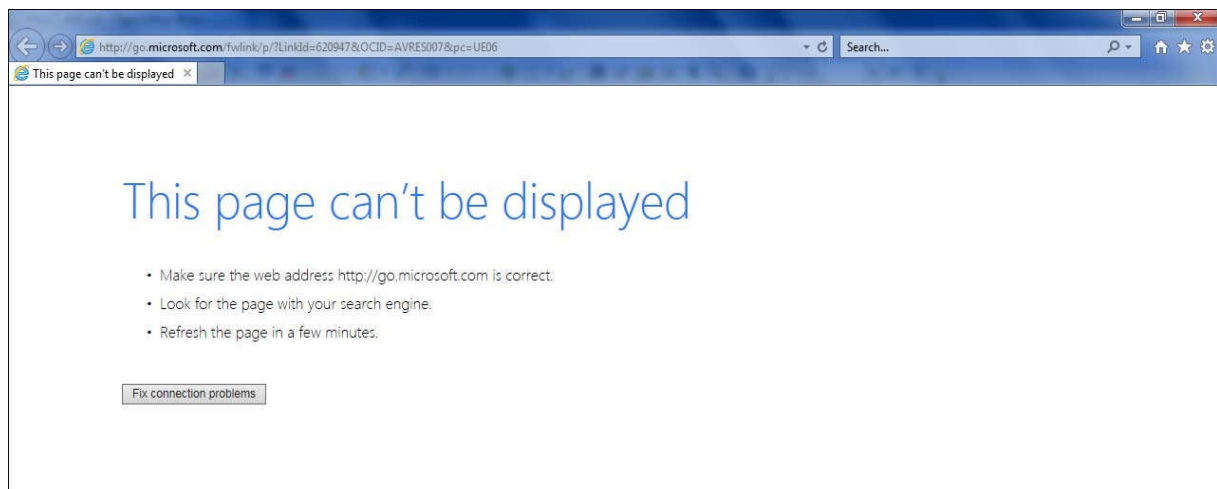


9. Give a specific name to the new rule and click on finish to apply the new changes.



Note: Repeat all the steps for Outbound Rules.

Output:



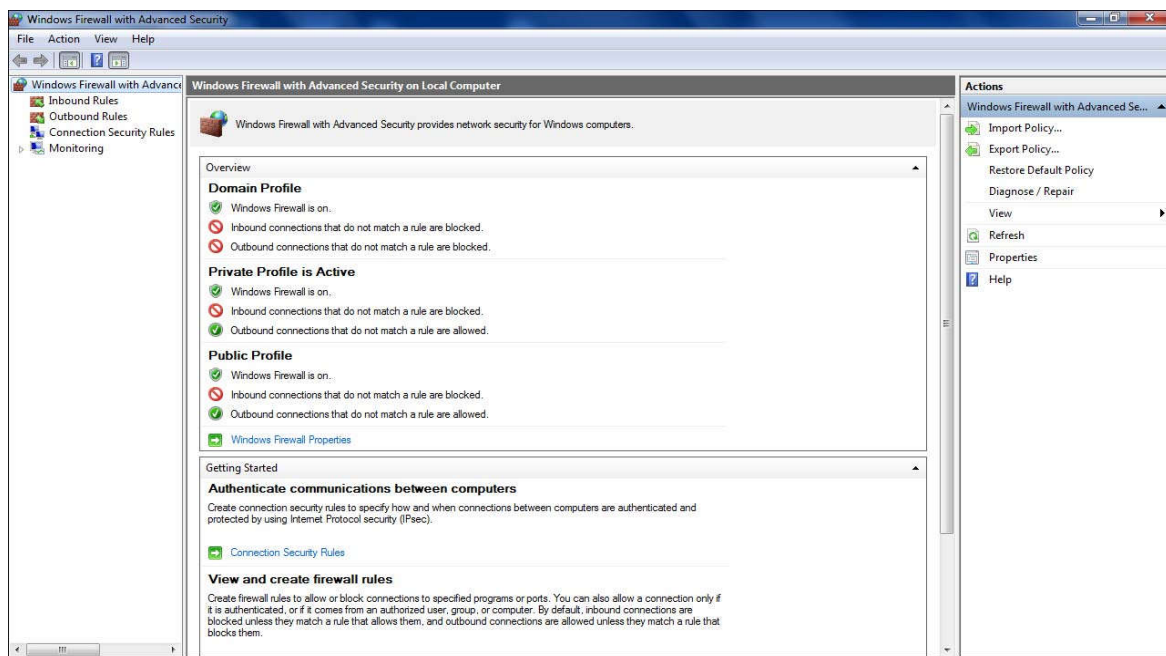
CJA Website

Steps:

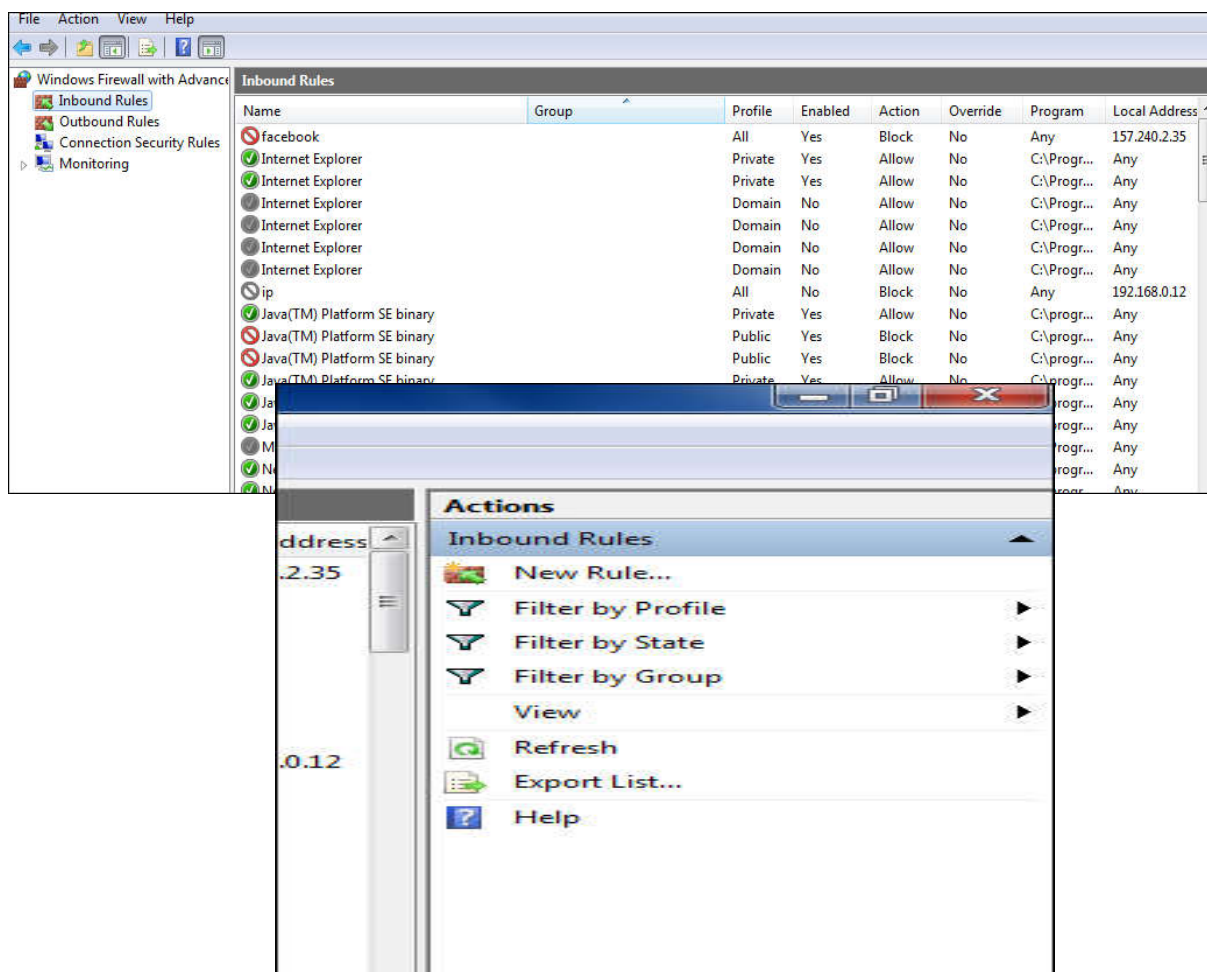
1. Click on the Control Panel > System Security > Windows Firewall. The below screen will appear.



2. Click on Advanced Settings and below screen will appear.

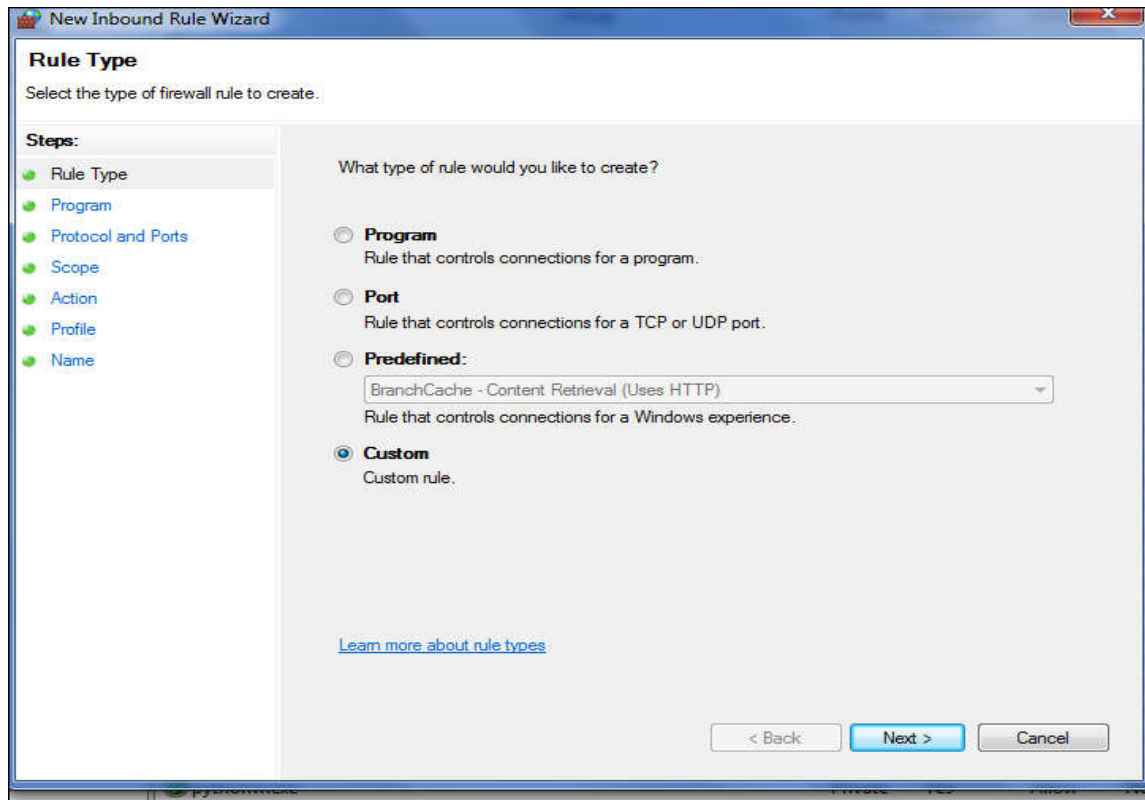


3. Click on Inbound Rules in the left side to display the inbound rules action .



4. Click on the new rule on the right side.

5. After clicking on new rule the new inbound rule wizard will open. Select on custom and click next.



6. Don't change anything just click next.

New Inbound Rule Wizard

Program

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

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- 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:**

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

Services
Specify which services this rule applies to.

[Learn more about specifying programs](#)

< Back Next > Cancel

7. Don't change anything just 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:

Protocol number:

Local port:

Example: 80, 443, 5000-5010

Remote port:

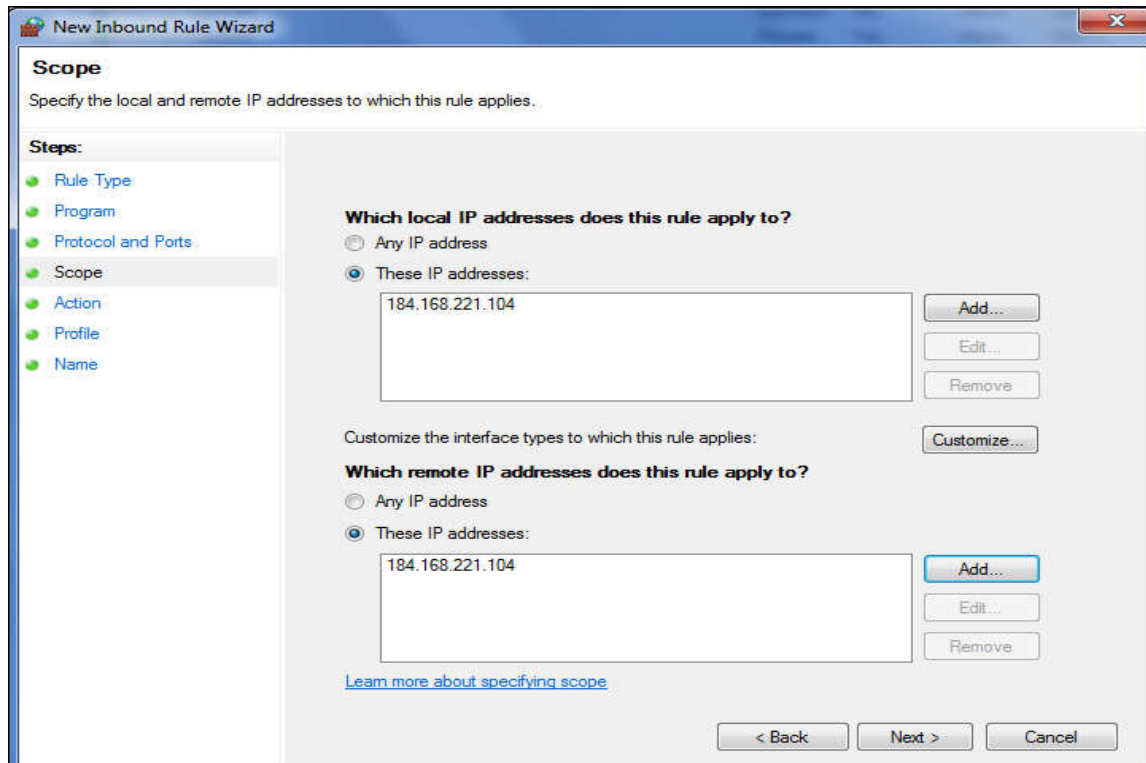
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

[Learn more about protocol and ports](#)

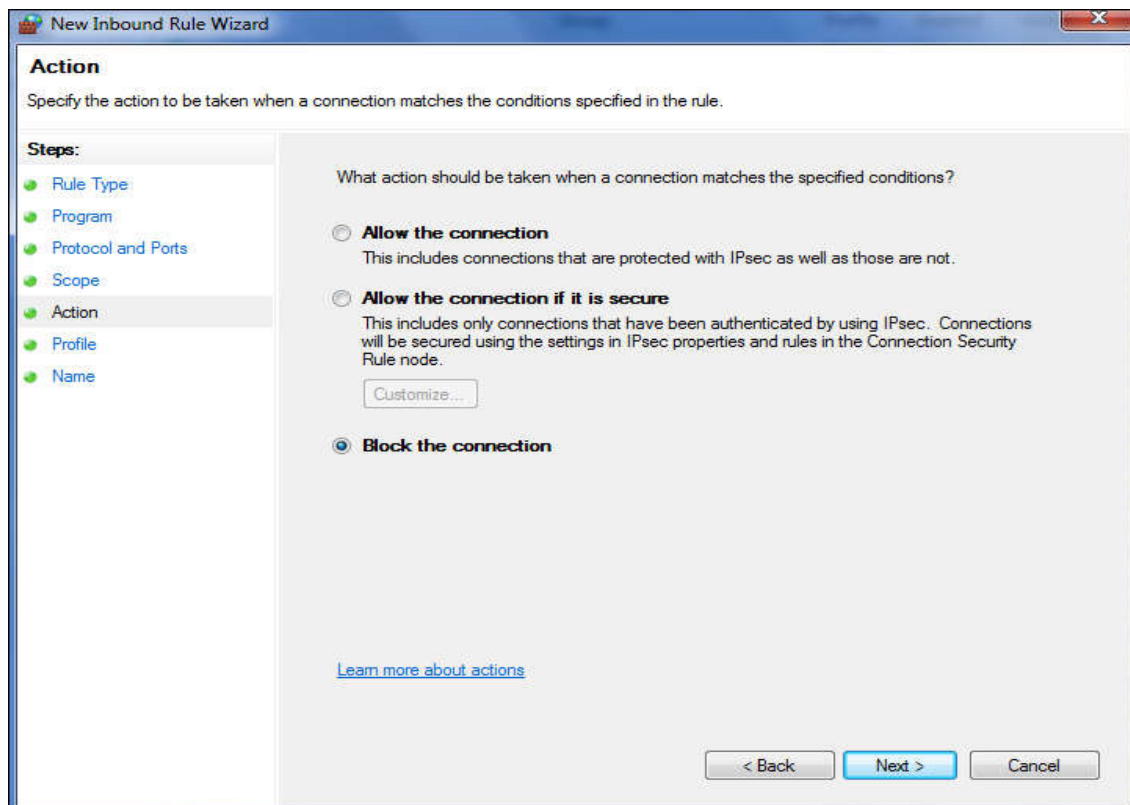
< Back Next > Cancel

8. Click on These IP address > Add > Enter the IP address of the website > Then Click on next



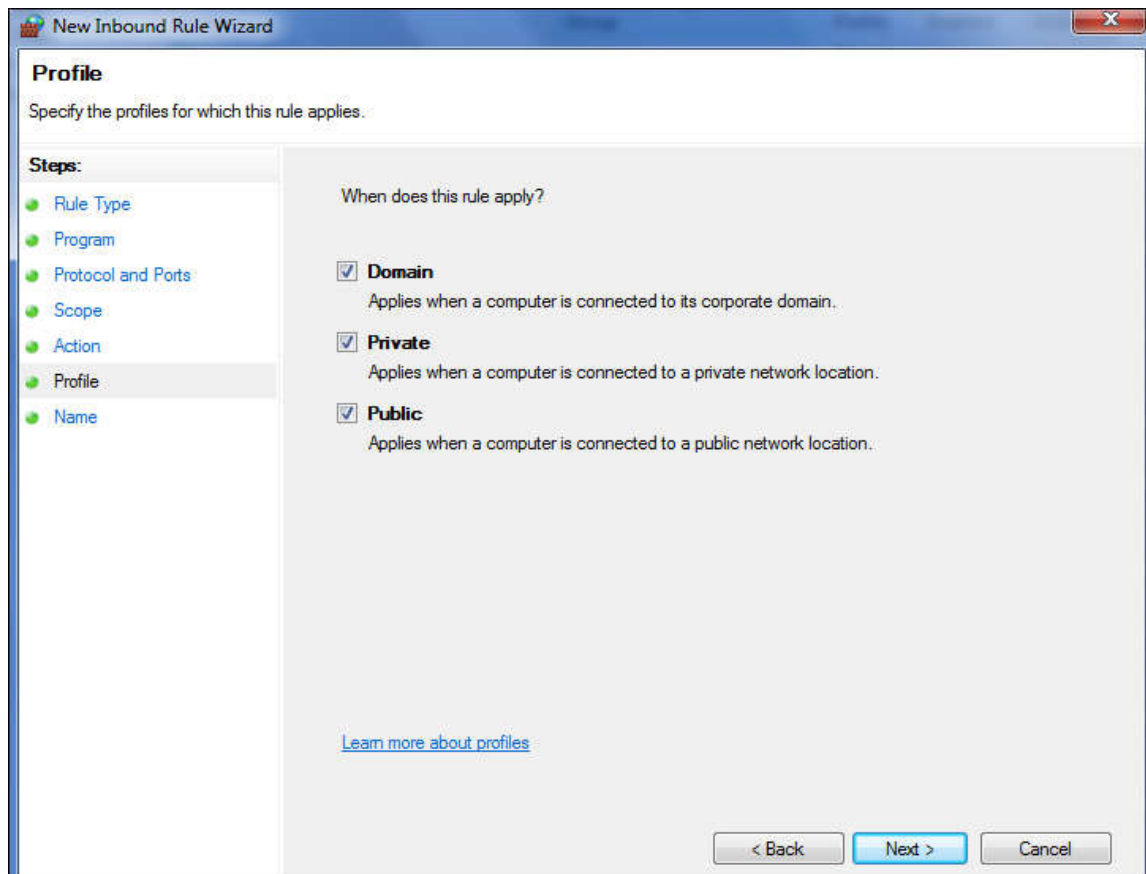
The 'New Inbound Rule Wizard' window is shown at the 'Scope' step. The left sidebar lists steps: Rule Type, Program, Protocol and Ports, Scope (selected), Action, Profile, and Name. The main area is titled 'Specify the local and remote IP addresses to which this rule applies.' It contains two sections: 'Which local IP addresses does this rule apply to?' and 'Which remote IP addresses does this rule apply to?'. Both sections have radio buttons for 'Any IP address' and 'These IP addresses:'. In both, 'These IP addresses:' is selected, and a text box contains '184.168.221.104'. To the right of each text box are buttons for 'Add...', 'Edit...', and 'Remove'. Below the remote section is a 'Customize...' button. At the bottom are '< Back', 'Next >', and 'Cancel' buttons. A link 'Learn more about specifying scope' is at the bottom left.

9. Now Select block the connection and click next .



The 'New Inbound Rule Wizard' window is shown at the 'Action' step. The left sidebar lists steps: Rule Type, Program, Protocol and Ports, Scope, Action (selected), Profile, and Name. The main area is titled 'Specify the action to be taken when a connection matches the conditions specified in the rule.' It contains the question 'What action should be taken when a connection matches the specified conditions?' and three radio button options: 'Allow the connection', 'Allow the connection if it is secure', and 'Block the connection'. The first two options have descriptive text below them. The 'Block the connection' option is selected. A 'Customize...' button is below the first two options. At the bottom are '< Back', 'Next >', and 'Cancel' buttons. A link 'Learn more about actions' is at the bottom left.

10. Select all the profiles available on different types of connection (Domain, Private and Public) and Click next .



11. Give a specific name to the new rule and click on finish to apply the new changes.

Note: Repeat all the steps for Outbound Rules

Output:

