DATE: 28/09/2018

Practical no: 10

AIM: Configure windows firewall to block

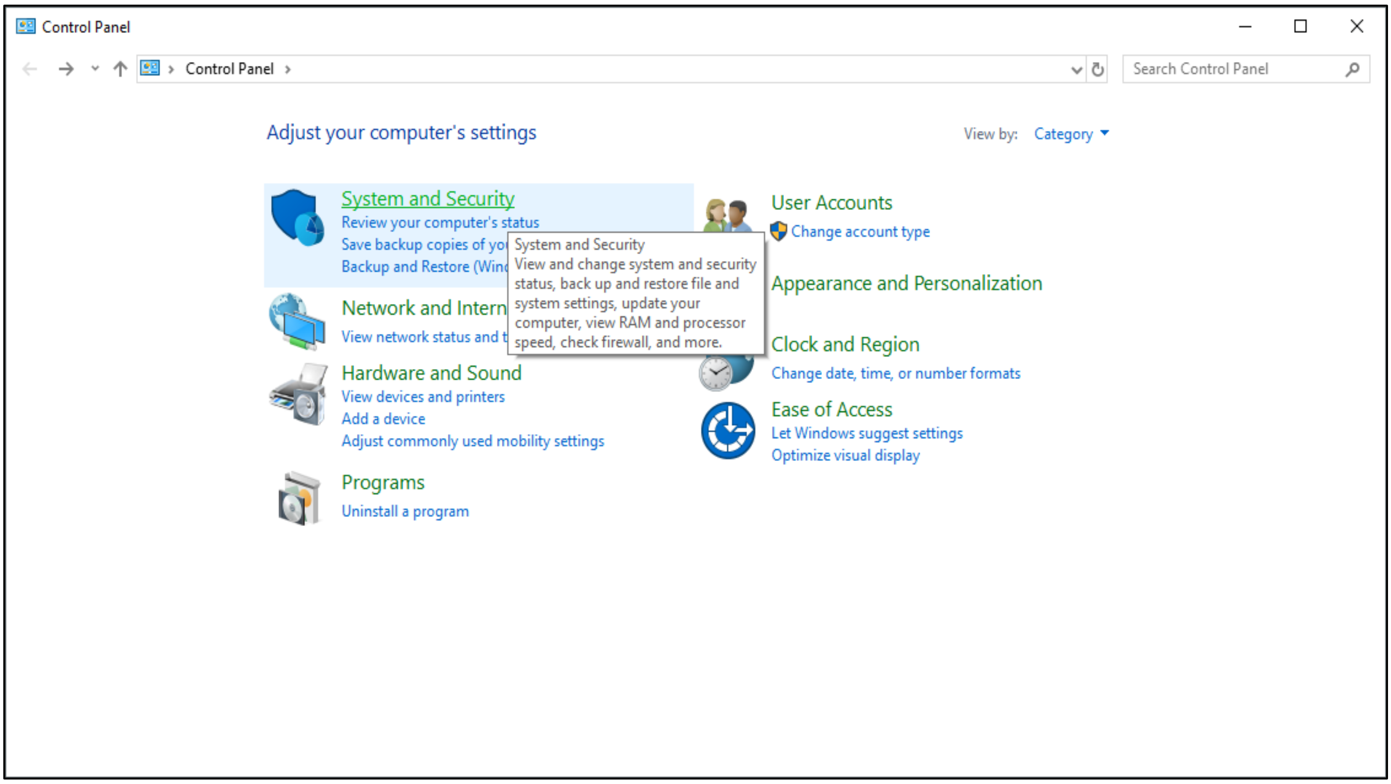
1) **A port**
2) **An Program**
3) **A Website**

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

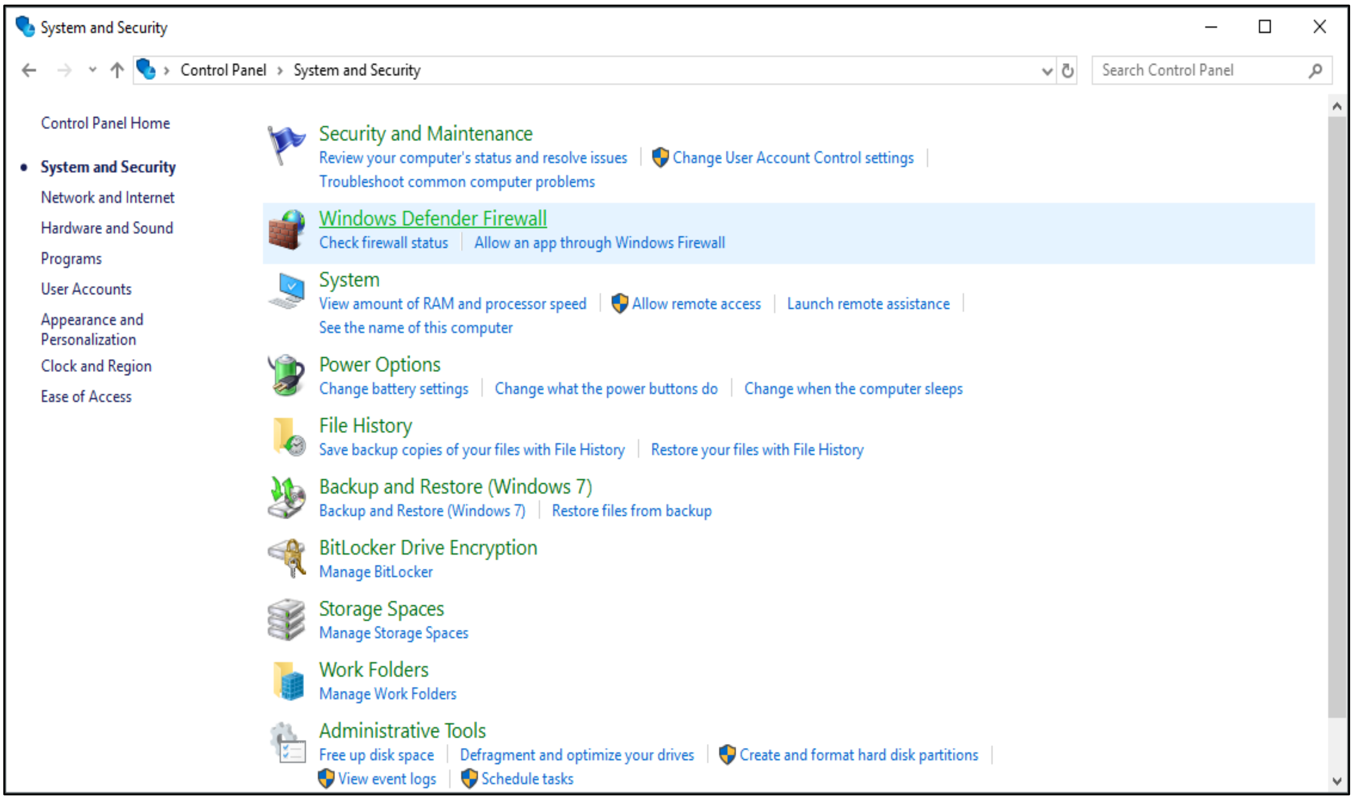
A) Blocking a port:

Step 1: Open control panel and go to System Security.

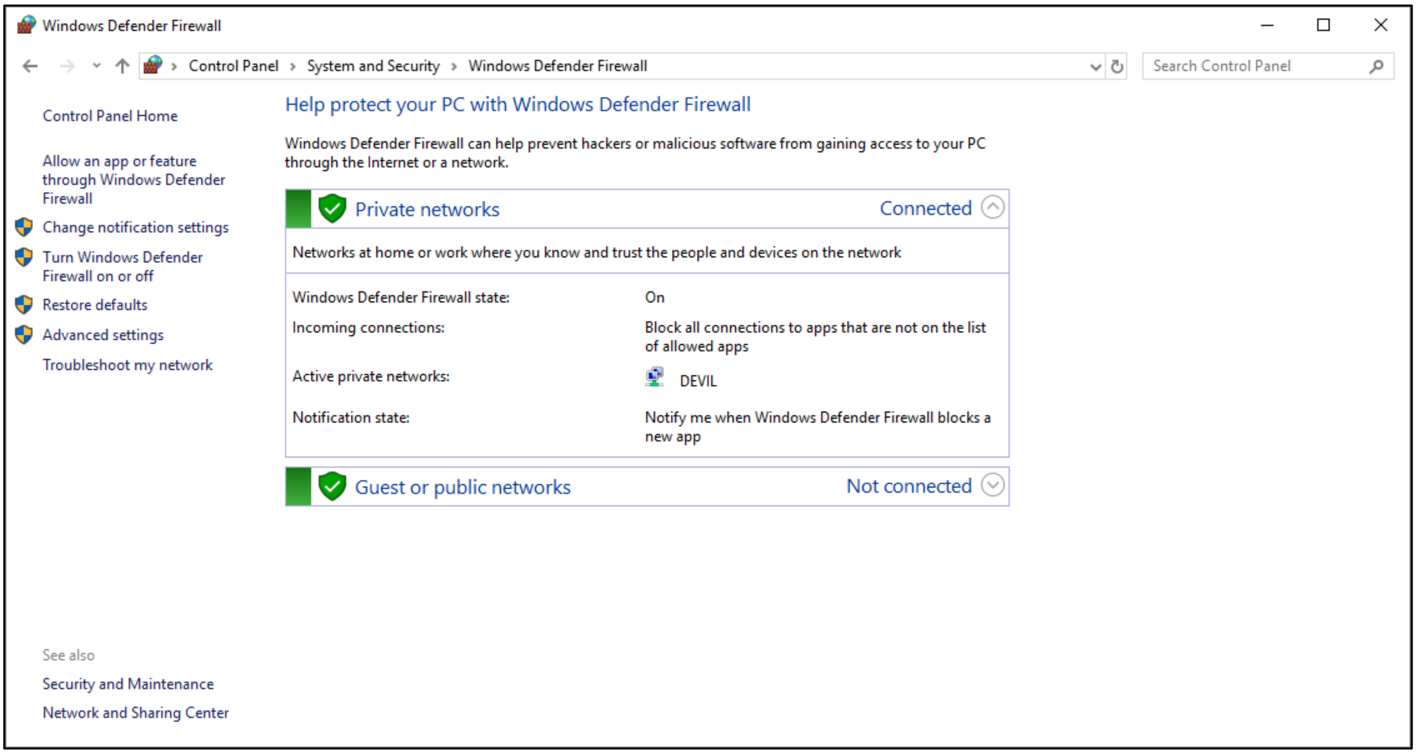


System and Security
View and change system and security status, back up and restore file and system settings, update your computer, view RAM and processor speed, check firewall, and more.

Step 2: Now Select Windows Defender Firewall.


System and Security
Control Panel › System and Security
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Power Options
Change battery settings
Change what the power buttons do
Change when the computer sleeps
File History
Save backup copies of your files with File History
Restore your files with File History
Backup and Restore (Windows 7)
Backup and Restore (Windows 7)
Restore files from backup
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Free up disk space
Defragment and optimize your drives
Create and format hard disk partitions
View event logs
Schedule tasks

Step 3: Now you need to select Advanced setting.



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.

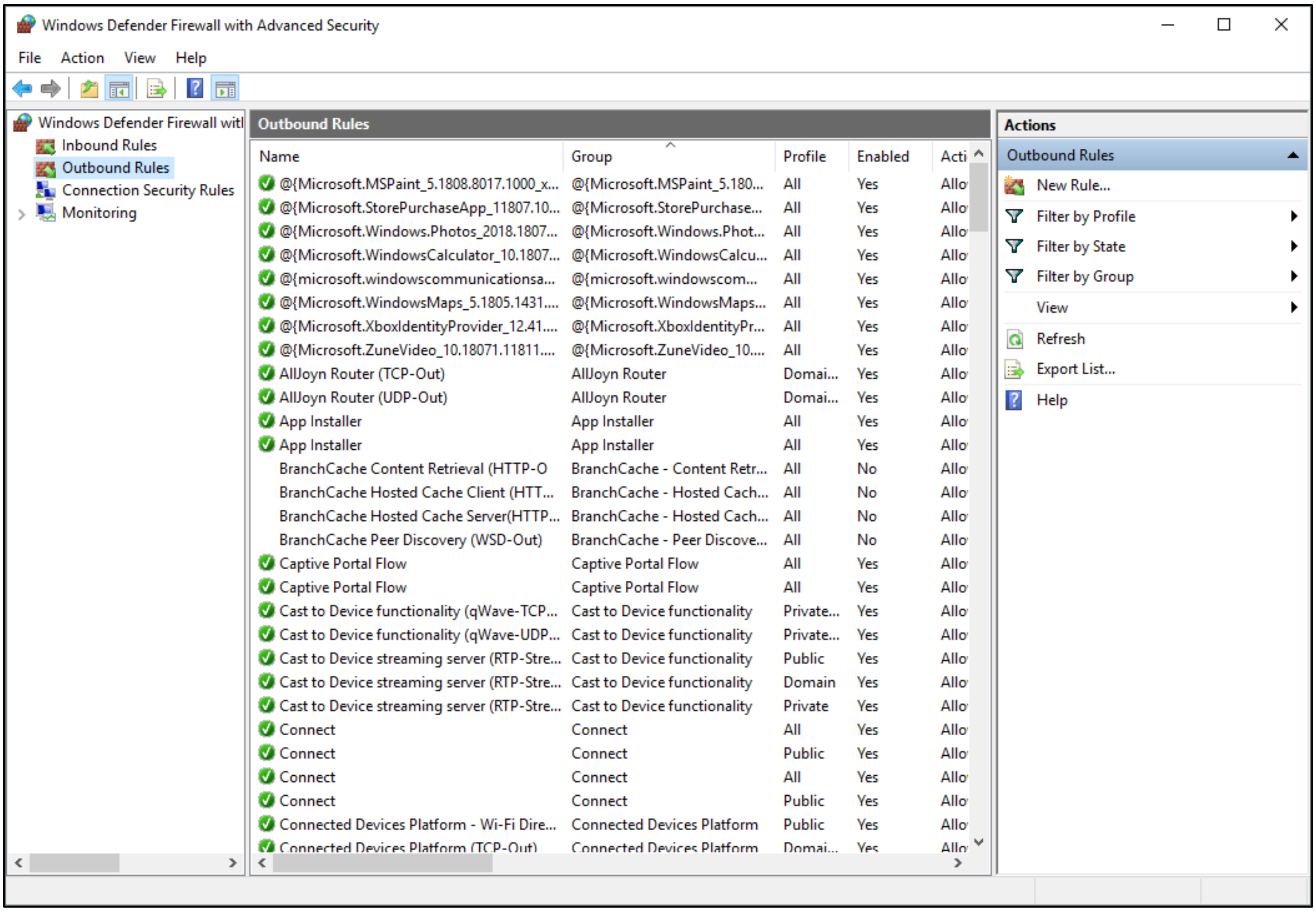
Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

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

Guest or public networks Not connected

Step 4: Now Select Outbound Rules.



Windows Defender Firewall wit
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

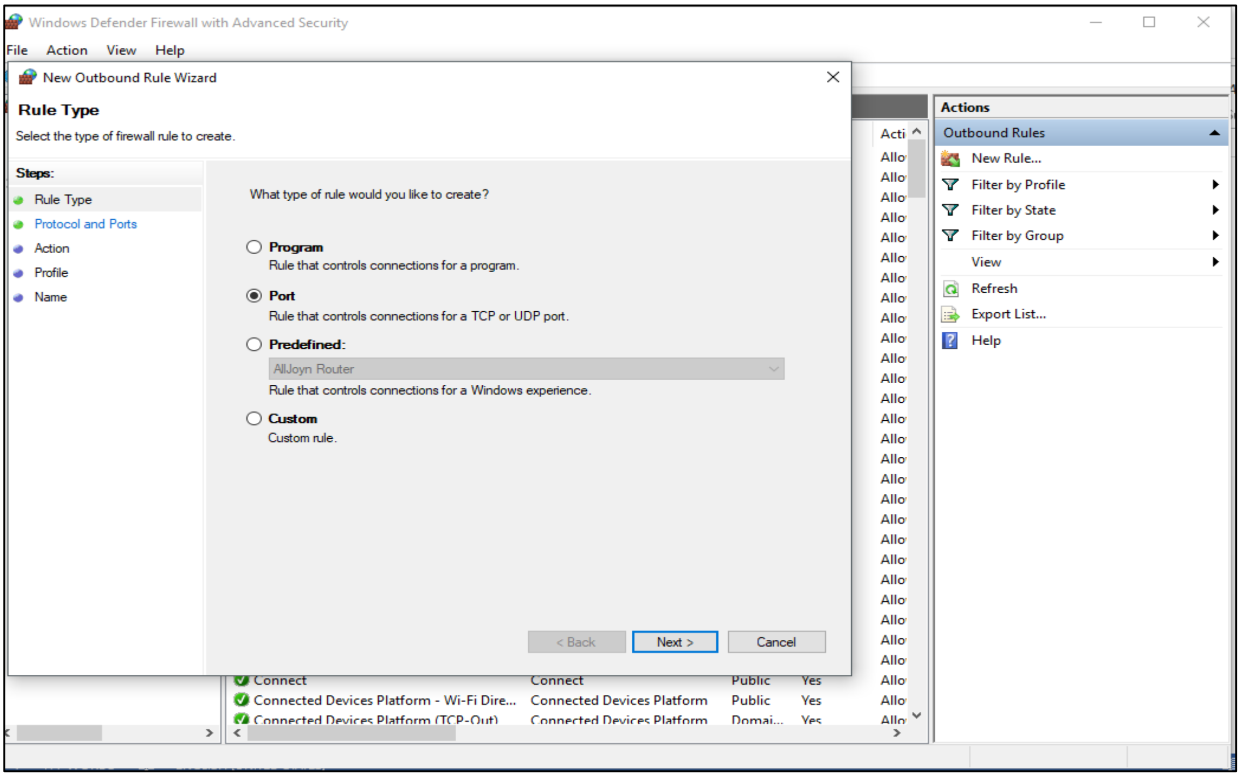
Outbound Rules

Name	Group	Profile	Enabled	Acti
@{Microsoft.MSPaint_5.1808.8017.1000_x...	@{Microsoft.MSPaint_5.180...	All	Yes	Allo
@{Microsoft.StorePurchaseApp_11807.10...	@{Microsoft.StorePurchase...	All	Yes	Allo
@{Microsoft.Windows.Photos_2018.1807...	@{Microsoft.Windows.Phot...	All	Yes	Allo
@{Microsoft.WindowsCalculator_10.1807...	@{Microsoft.WindowsCalcu...	All	Yes	Allo
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All	Yes	Allo
@{Microsoft.WindowsMaps_5.1805.1431....	@{Microsoft.WindowsMaps...	All	Yes	Allo
@{Microsoft.XboxIdentityProvider_12.41....	@{Microsoft.XboxIdentityPr...	All	Yes	Allo
@{Microsoft.ZuneVideo_10.18071.11811....	@{Microsoft.ZuneVideo_10....	All	Yes	Allo
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allo
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allo
App Installer	App Installer	All	Yes	Allo
App Installer	App Installer	All	Yes	Allo
BranchCache Content Retrieval (HTTP-O	BranchCache - Content Retr...	All	No	Allo
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allo
Captive Portal Flow	Captive Portal Flow	All	Yes	Allo
Captive Portal Flow	Captive Portal Flow	All	Yes	Allo
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allo
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allo
Connect	Connect	All	Yes	Allo
Connect	Connect	Public	Yes	Allo
Connect	Connect	All	Yes	Allo
Connect	Connect	Public	Yes	Allo
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allo
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allo

Actions

Outbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

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



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

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

What type of rule would you like to create?

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

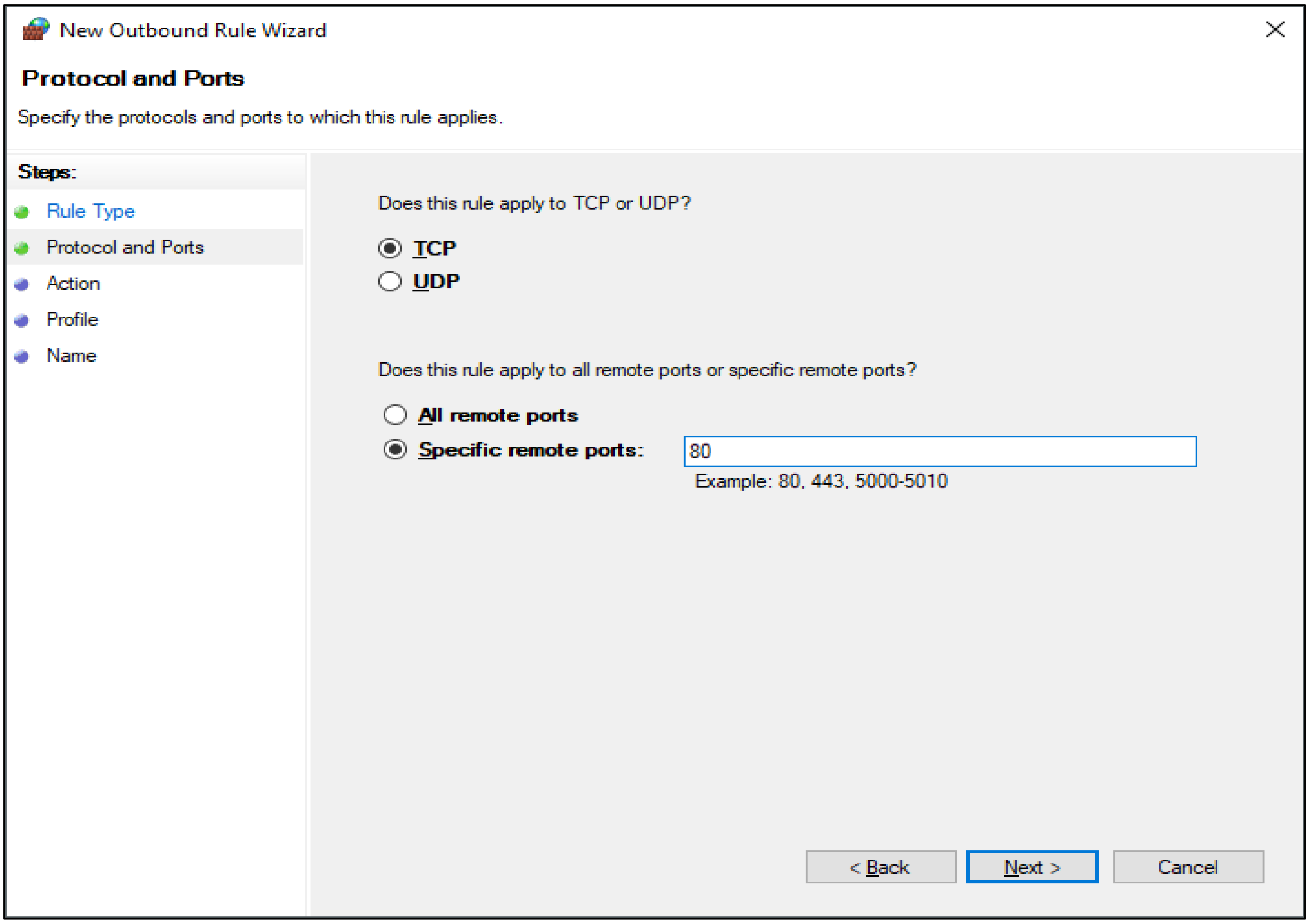
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Connect	Connect	Public	Yes	Allo
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allo
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allo

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



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

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

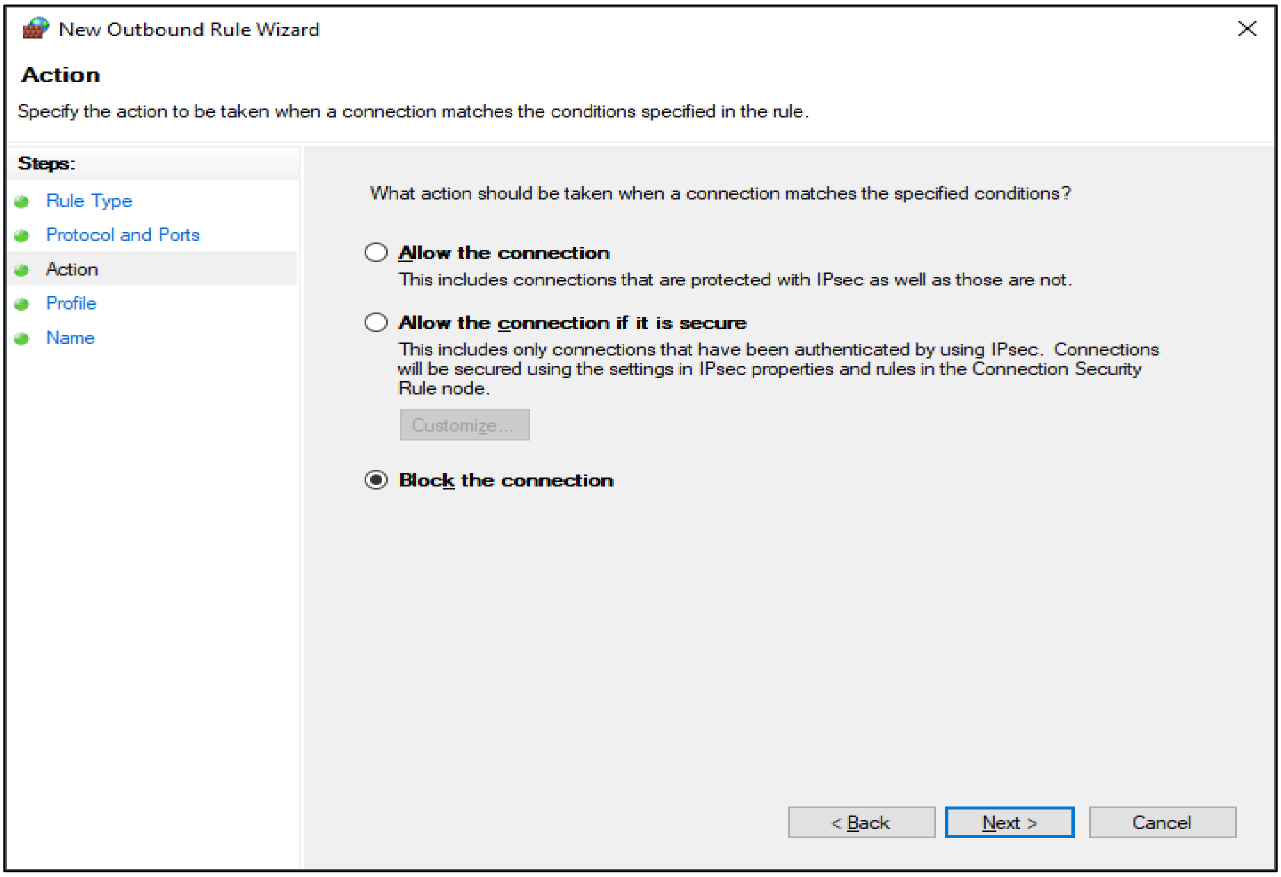
Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

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

○ **All remote ports**
● **Specific remote ports:** 80
Example: 80, 443, 5000-5010

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

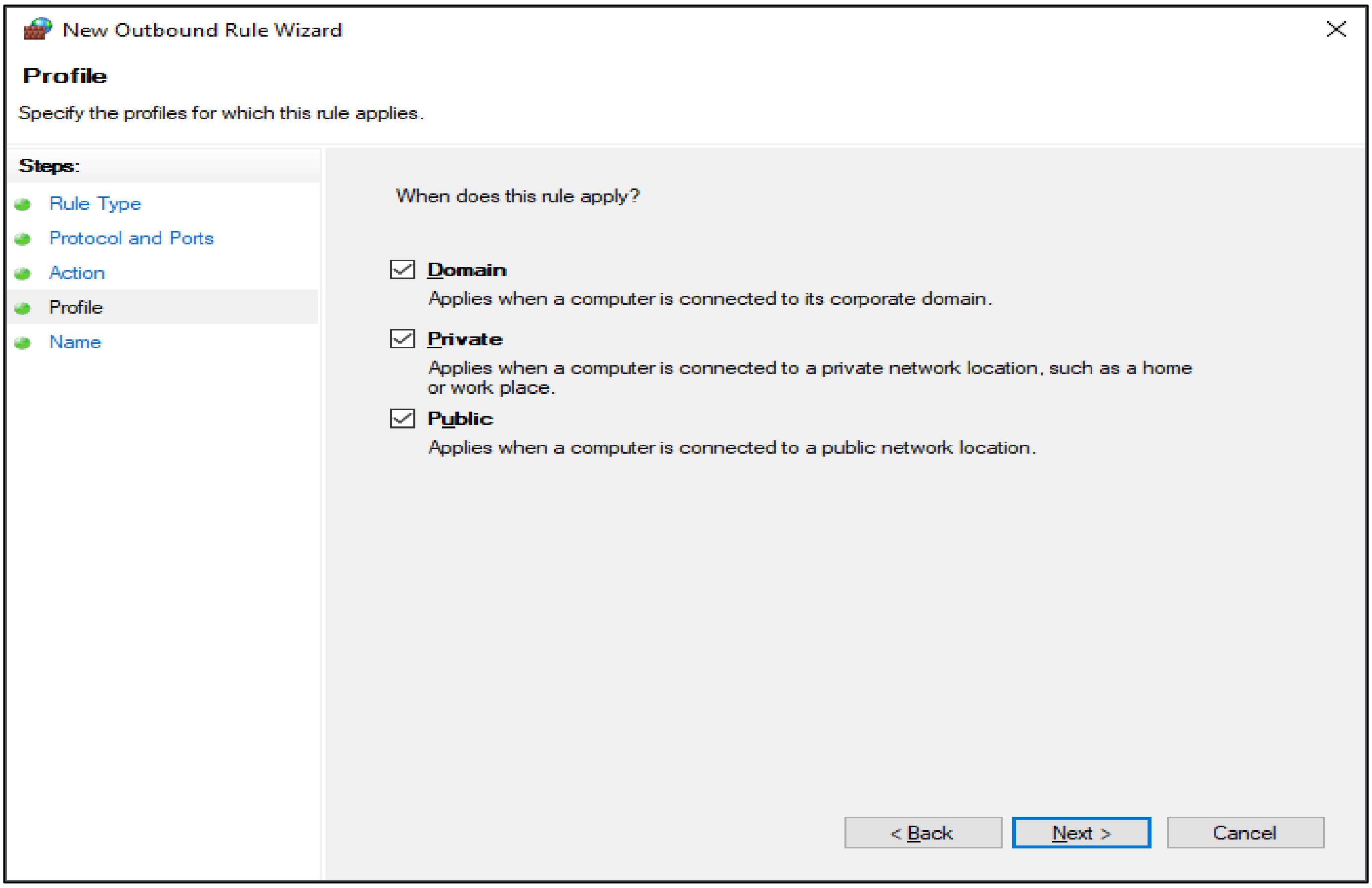
What action should be taken when a connection matches the specified conditions?

○ **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.

● **Block the connection**

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

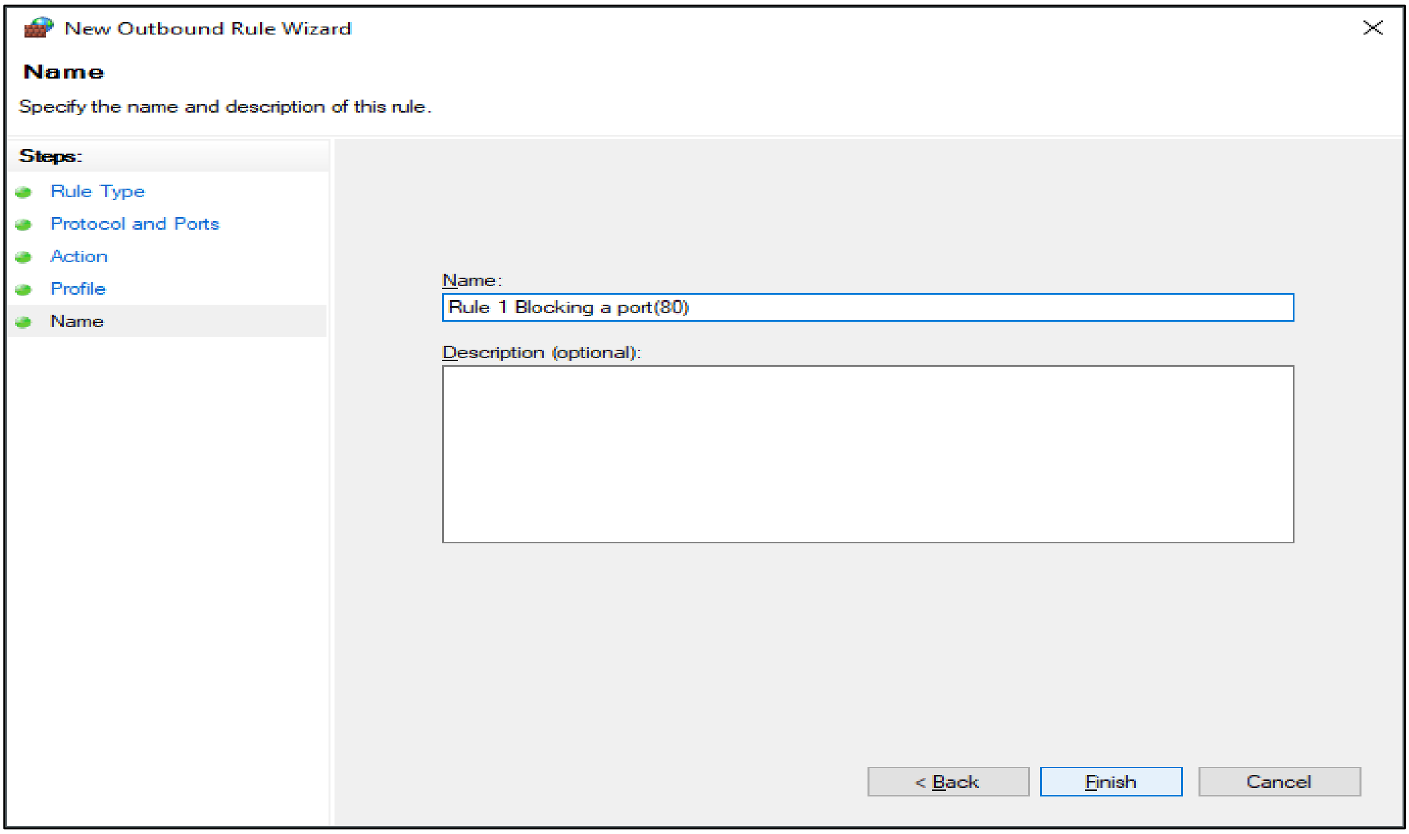
When does this rule apply?

☑ **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.

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



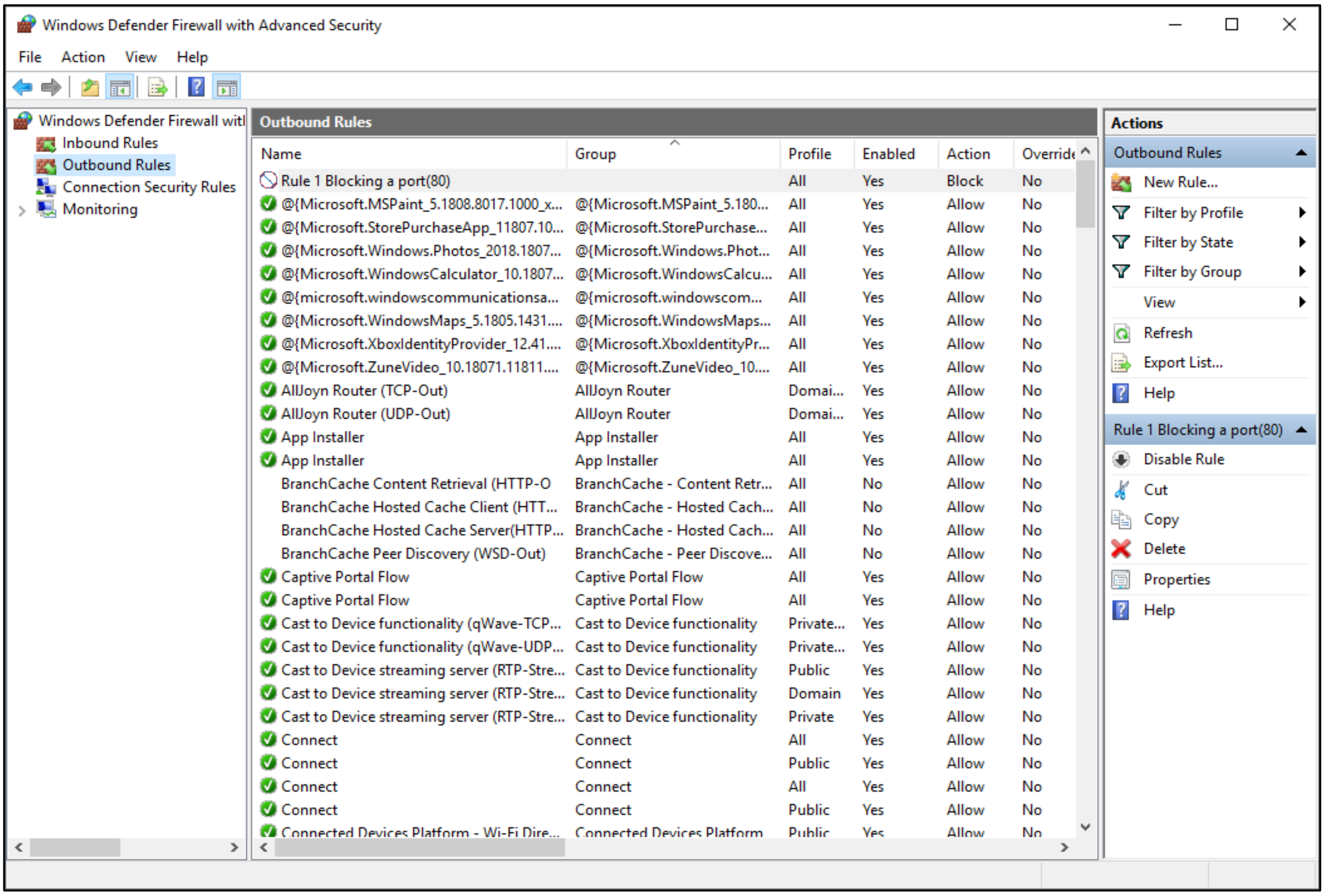
Name

Specify the name and description of this rule.

Name: Rule 1 Blocking a port(80)

Description (optional):

Output:

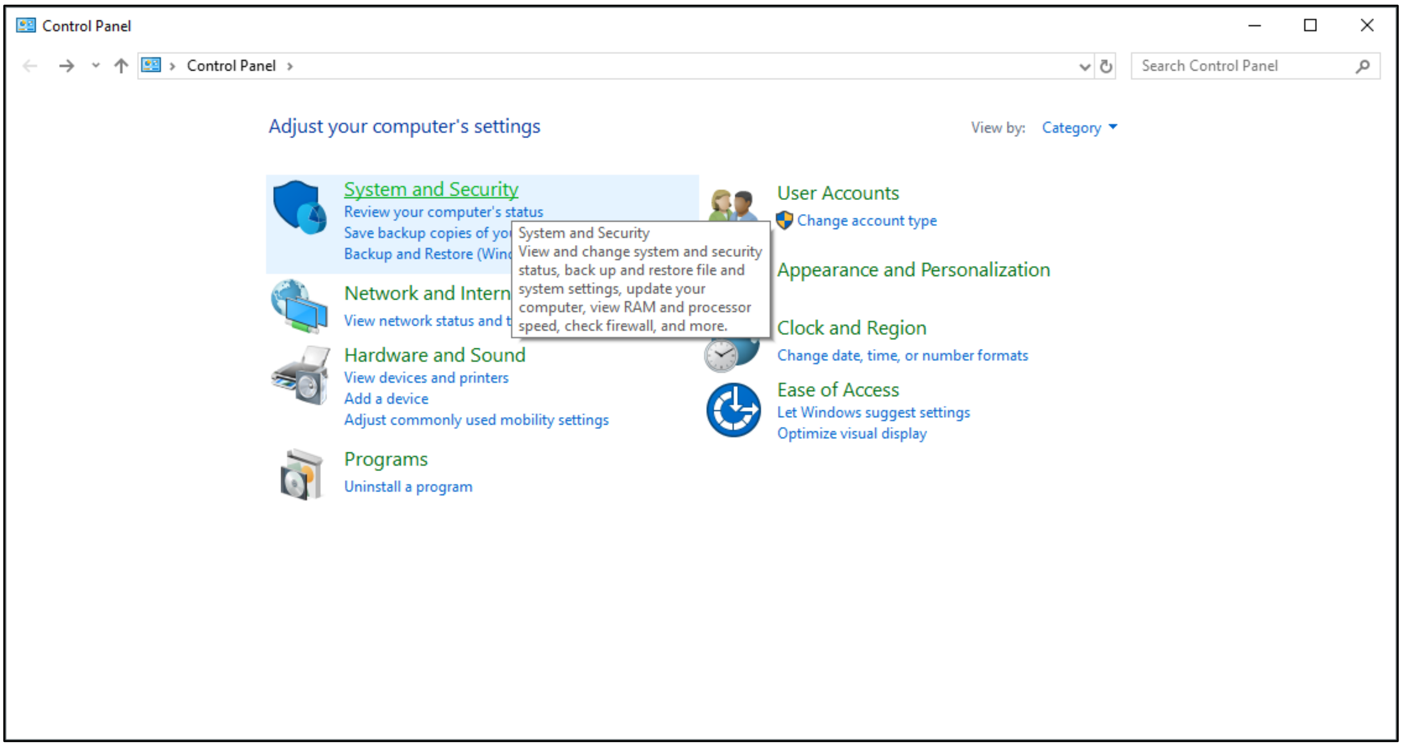


Outbound Rules

Name	Group	Profile	Enabled	Action	Override
Rule 1 Blocking a port(80)		All	Yes	Block	No
@{Microsoft.MSPaint_5.1808.8017.1000_x...	@{Microsoft.MSPaint_5.180...	All	Yes	Allow	No
@{Microsoft.StorePurchaseApp_11807.10...	@{Microsoft.StorePurchase...	All	Yes	Allow	No
@{Microsoft.Windows.Photos_2018.1807...	@{Microsoft.Windows.Phot...	All	Yes	Allow	No
@{Microsoft.WindowsCalculator_10.1807...	@{Microsoft.WindowsCalcu...	All	Yes	Allow	No
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All	Yes	Allow	No
@{Microsoft.WindowsMaps_5.1805.1431....	@{Microsoft.WindowsMaps...	All	Yes	Allow	No
@{Microsoft.XboxIdentityProvider_12.41....	@{Microsoft.XboxIdentityPr...	All	Yes	Allow	No
@{Microsoft.ZuneVideo_10.18071.11811....	@{Microsoft.ZuneVideo_10....	All	Yes	Allow	No
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No
App Installer	App Installer	All	Yes	Allow	No
App Installer	App Installer	All	Yes	Allow	No
BranchCache Content Retrieval (HTTP-O	BranchCache - Content Retr...	All	No	Allow	No
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	All	No	Allow	No
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow	No
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allow	No
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allow	No
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allow	No
Connect	Connect	All	Yes	Allow	No
Connect	Connect	Public	Yes	Allow	No
Connect	Connect	All	Yes	Allow	No
Connect	Connect	Public	Yes	Allow	No
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allow	No

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

Step 1: Open control panel and go to System Security.



Control Panel

Control Panel >

Search Control Panel

Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Save backup copies of yo
Backup and Restore (Winc

System and Security
View and change system and security status, back up and restore file and system settings, update your computer, view RAM and processor speed, check firewall, and more.

Network and Intern
View network status and t

Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Programs
Uninstall a program

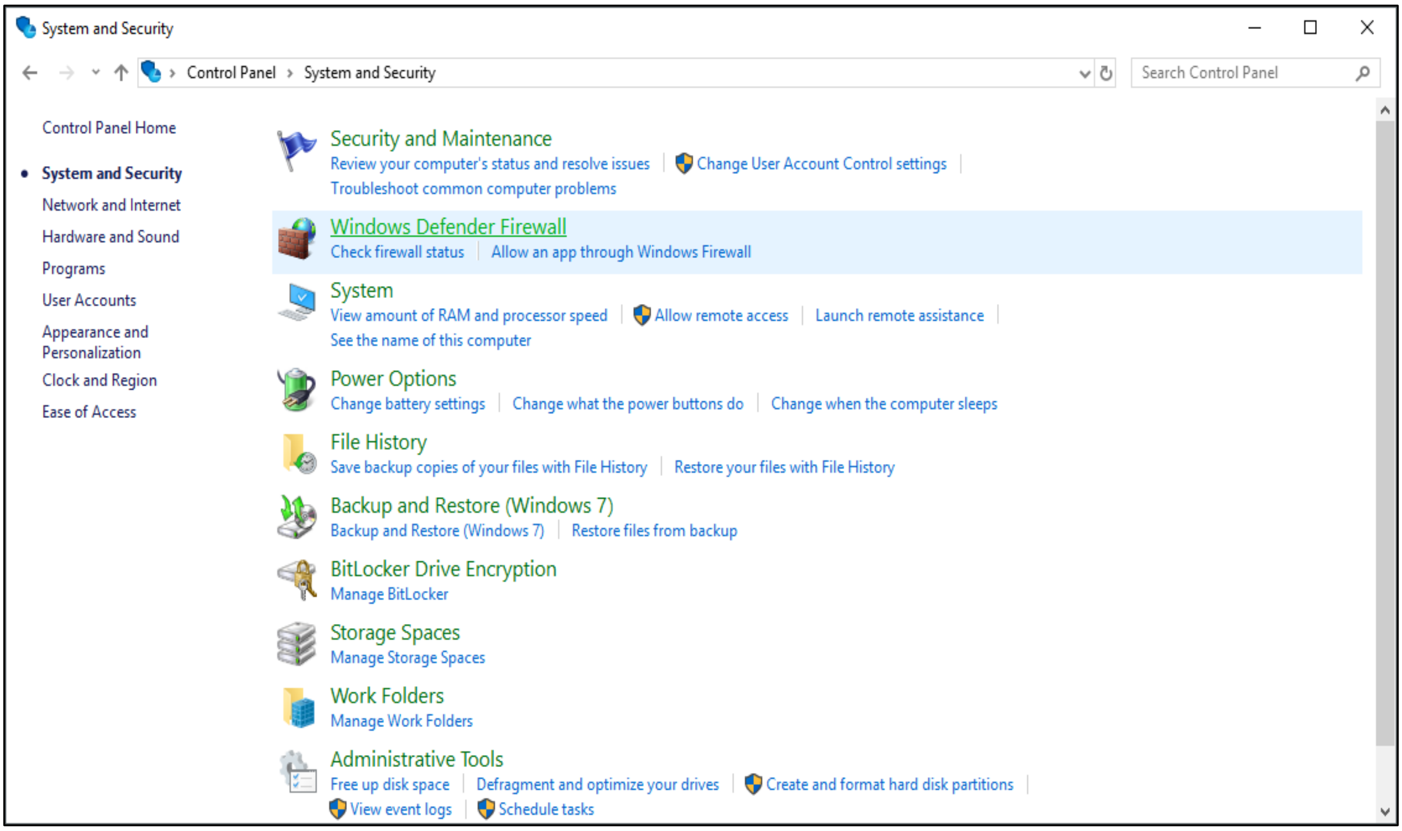
User Accounts
Change account type

Appearance and Personalization

Clock and Region
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

Step 2: Now Select Windows Defender Firewall.



System and Security

Control Panel > System and Security

Search Control Panel

Control Panel Home
- System and Security

Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access

Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall

System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer

Power Options
Change battery settings | Change what the power buttons do | Change when the computer sleeps

File History
Save backup copies of your files with File History | Restore your files with File History

Backup and Restore (Windows 7)
Backup and Restore (Windows 7) | Restore files from backup

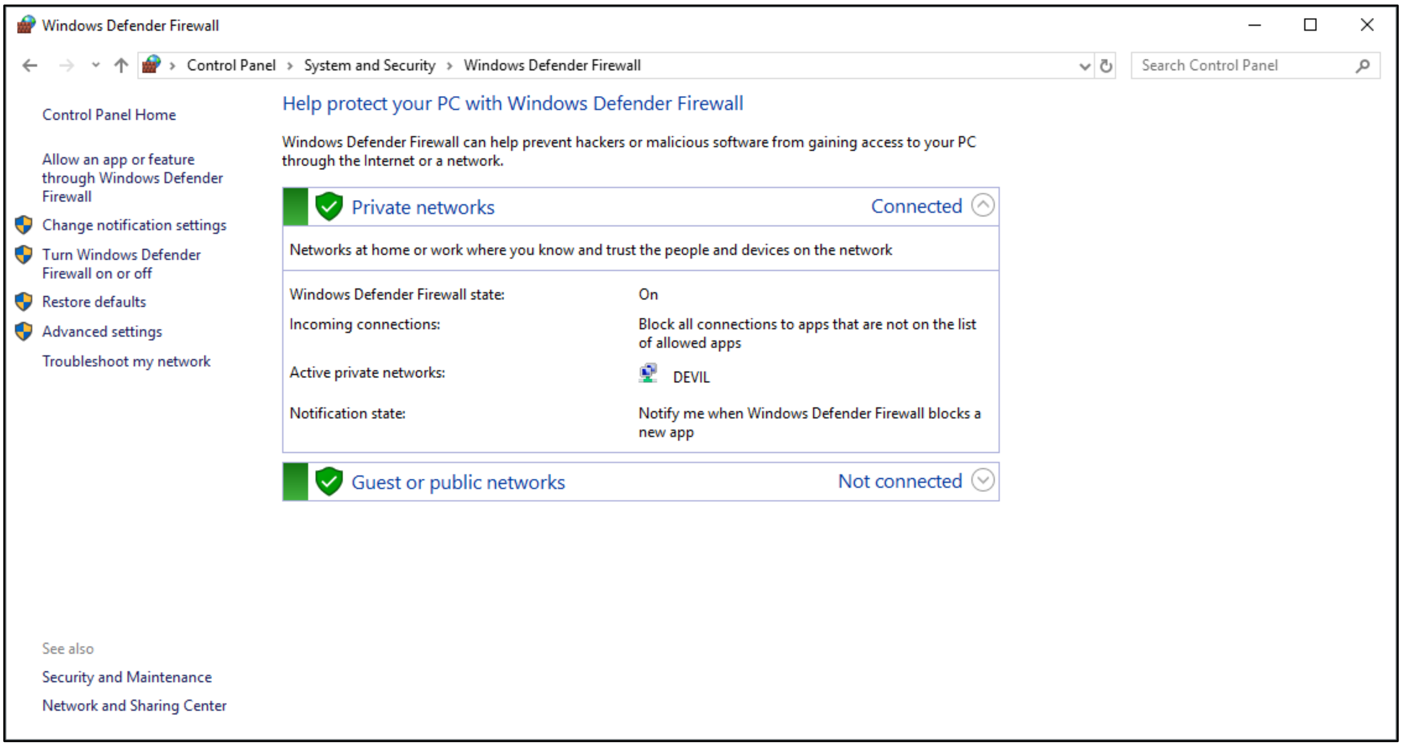
BitLocker Drive Encryption
Manage BitLocker

Storage Spaces
Manage Storage Spaces

Work Folders
Manage Work Folders

Administrative Tools
Free up disk space | Defragment and optimize your drives | Create and format hard disk partitions | View event logs | Schedule tasks

Step 3: Now you need to select Advanced setting.


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.

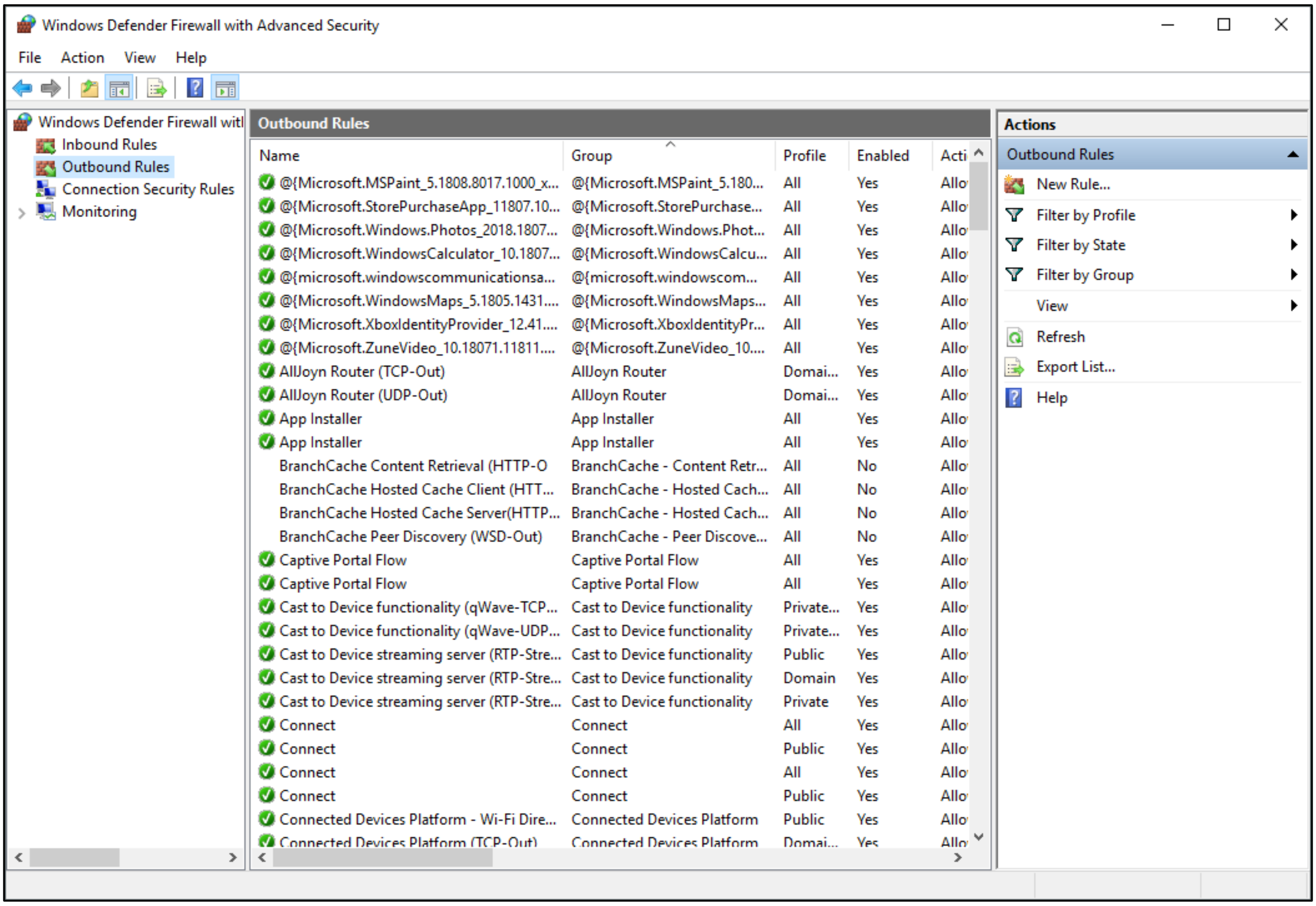
Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

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

Guest or public networks — Not connected

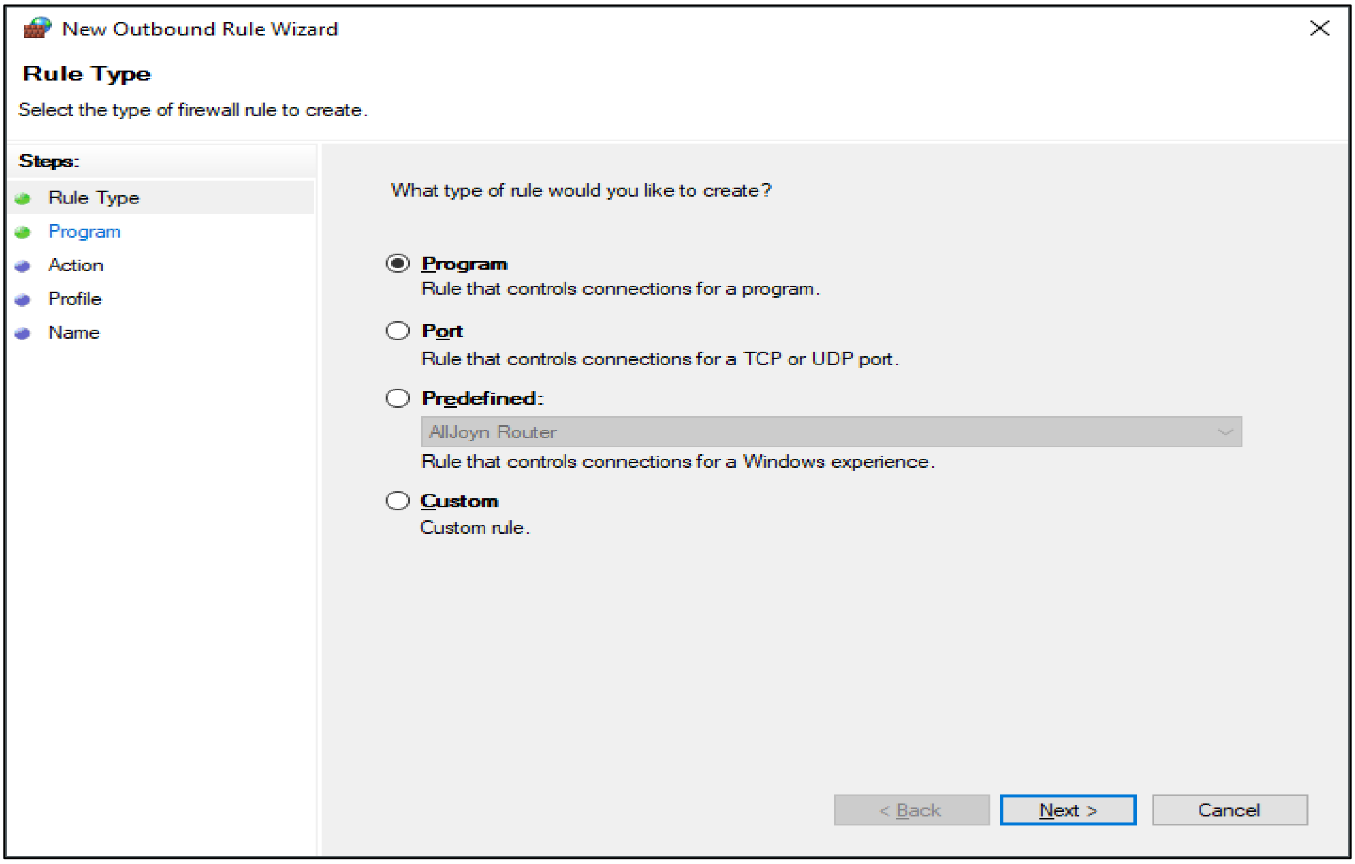
Step 4: Now Select Outbound Rules.



Outbound Rules

Name	Group	Profile	Enabled	Acti
✓ @{Microsoft.MSPaint_5.1808.8017.1000_x...	@{Microsoft.MSPaint_5.180...	All	Yes	Allo
✓ @{Microsoft.StorePurchaseApp_11807.10....	@{Microsoft.StorePurchase...	All	Yes	Allo
✓ @{Microsoft.Windows.Photos_2018.1807....	@{Microsoft.Windows.Phot...	All	Yes	Allo
✓ @{Microsoft.WindowsCalculator_10.1807....	@{Microsoft.WindowsCalcu...	All	Yes	Allo
✓ @{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All	Yes	Allo
✓ @{Microsoft.WindowsMaps_5.1805.1431....	@{Microsoft.WindowsMaps...	All	Yes	Allo
✓ @{Microsoft.XboxIdentityProvider_12.41....	@{Microsoft.XboxIdentityPr...	All	Yes	Allo
✓ @{Microsoft.ZuneVideo_10.18071.11811....	@{Microsoft.ZuneVideo_10....	All	Yes	Allo
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allo
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allo
✓ App Installer	App Installer	All	Yes	Allo
✓ App Installer	App Installer	All	Yes	Allo
BranchCache Content Retrieval (HTTP-O	BranchCache - Content Retr...	All	No	Allo
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allo
✓ Captive Portal Flow	Captive Portal Flow	All	Yes	Allo
✓ Captive Portal Flow	Captive Portal Flow	All	Yes	Allo
✓ Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allo
✓ Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allo
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allo
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allo
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allo
✓ Connect	Connect	All	Yes	Allo
✓ Connect	Connect	Public	Yes	Allo
✓ Connect	Connect	All	Yes	Allo
✓ Connect	Connect	Public	Yes	Allo
✓ Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allo
✓ Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allo

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



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

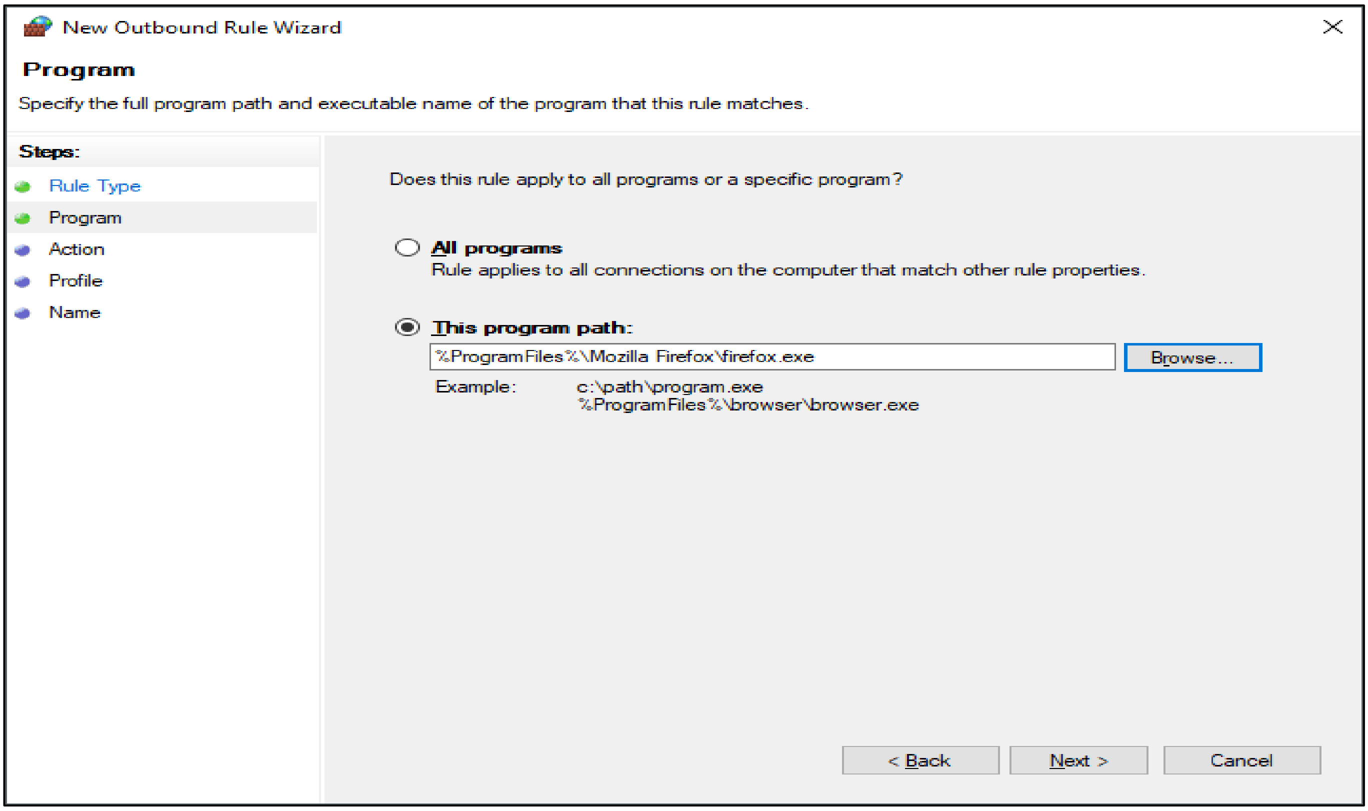
● **Program**
Rule that controls connections for a program.

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

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

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



New Outbound Rule Wizard

Program

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

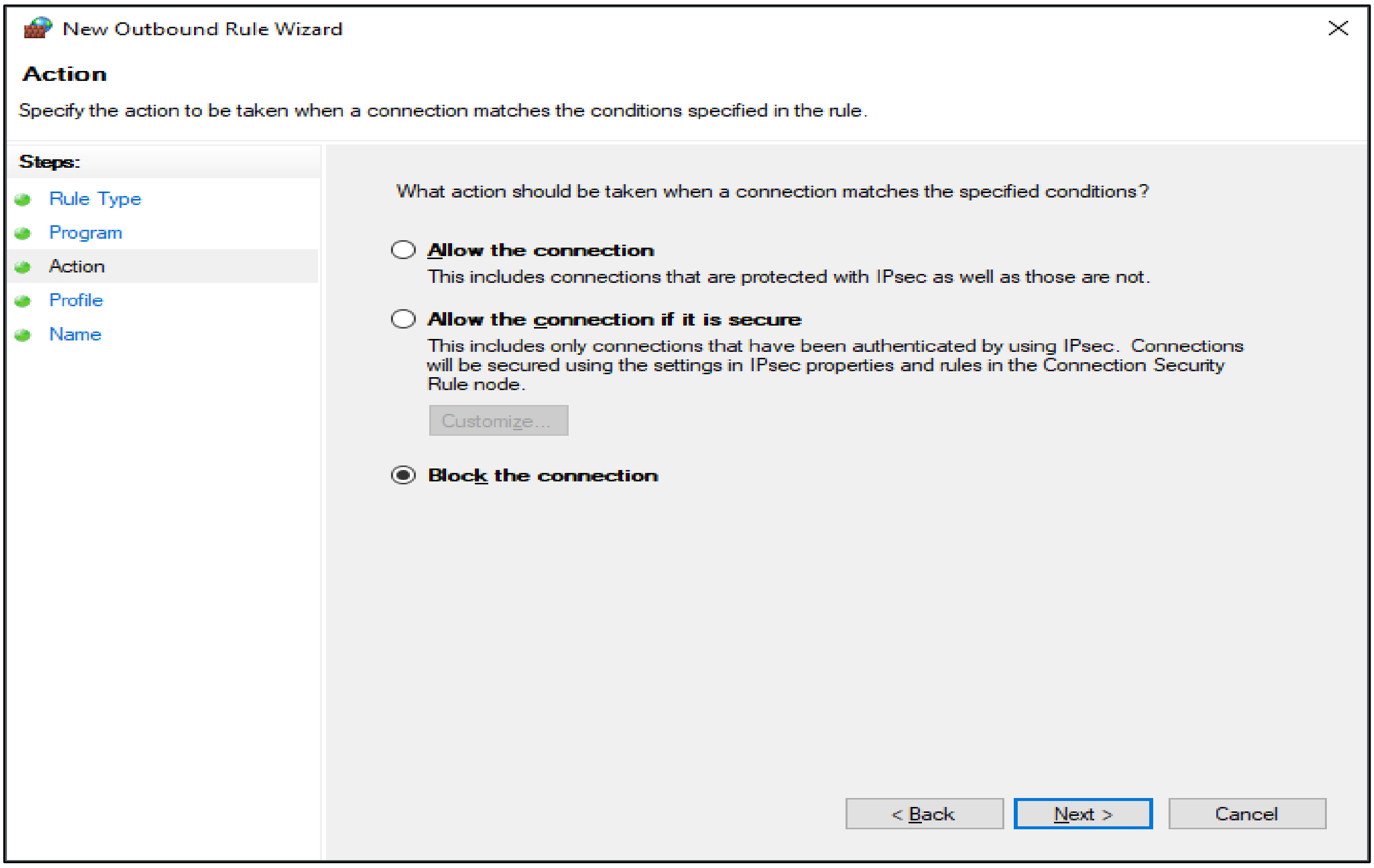
Does this rule apply to all programs or a specific program?

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

● **This program path:**
%ProgramFiles%\Mozilla Firefox\firefox.exe

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

Step 7: Click on Block the connection



New Outbound Rule Wizard

Action

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

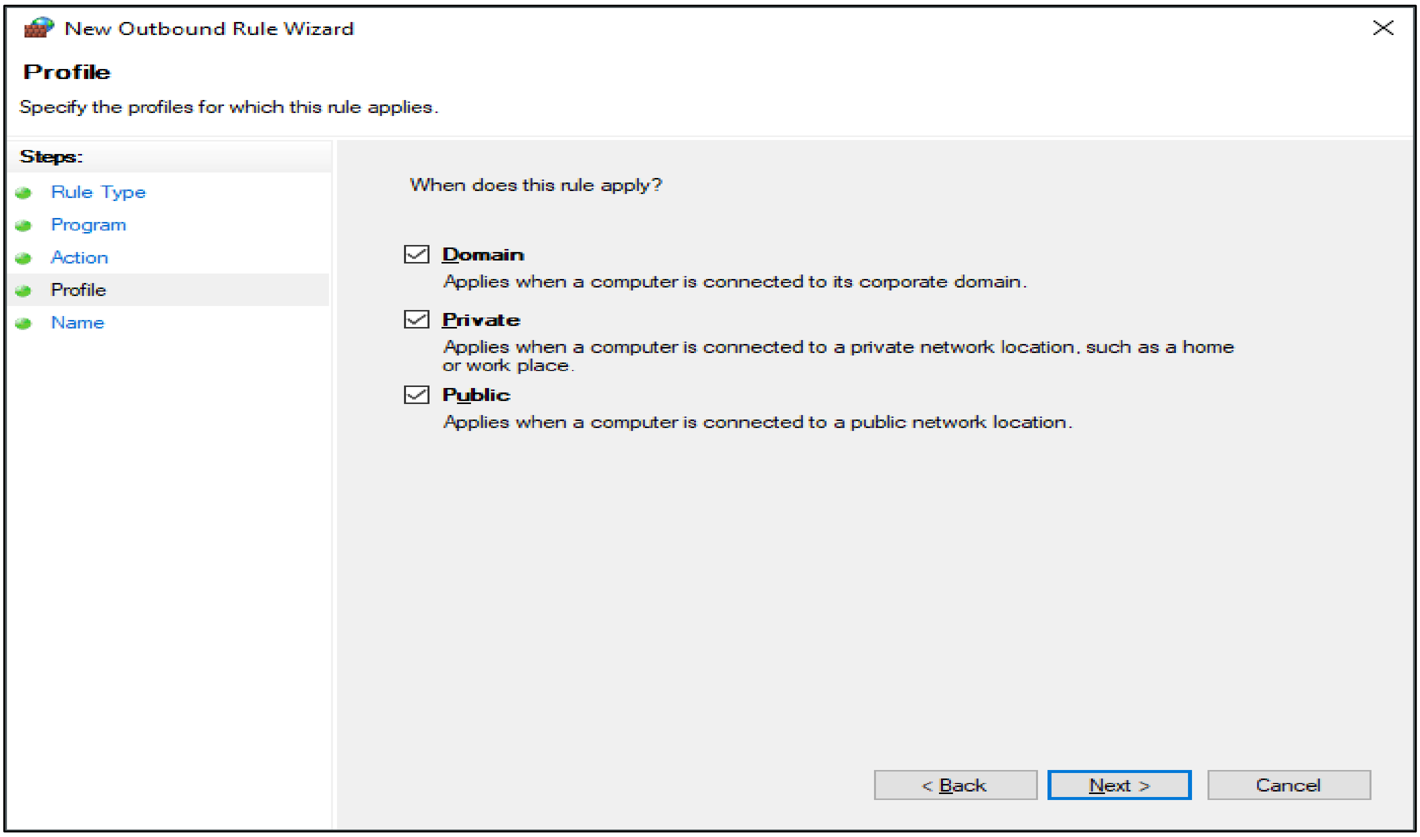
What action should be taken when a connection matches the specified conditions?

○ **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 8: Select the profiles domain private or public



New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

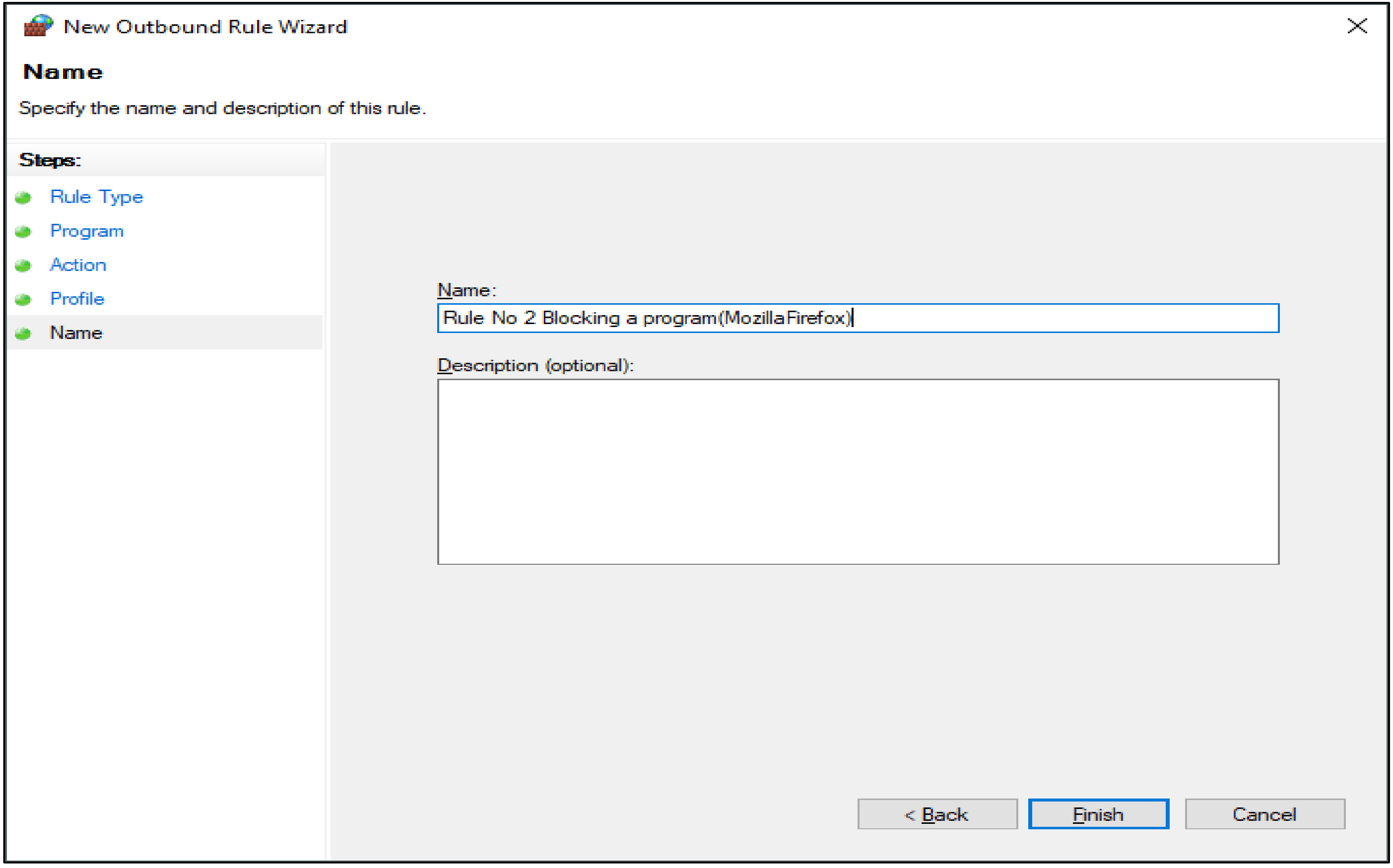
When does this rule apply?

☑ **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.

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



New Outbound Rule Wizard

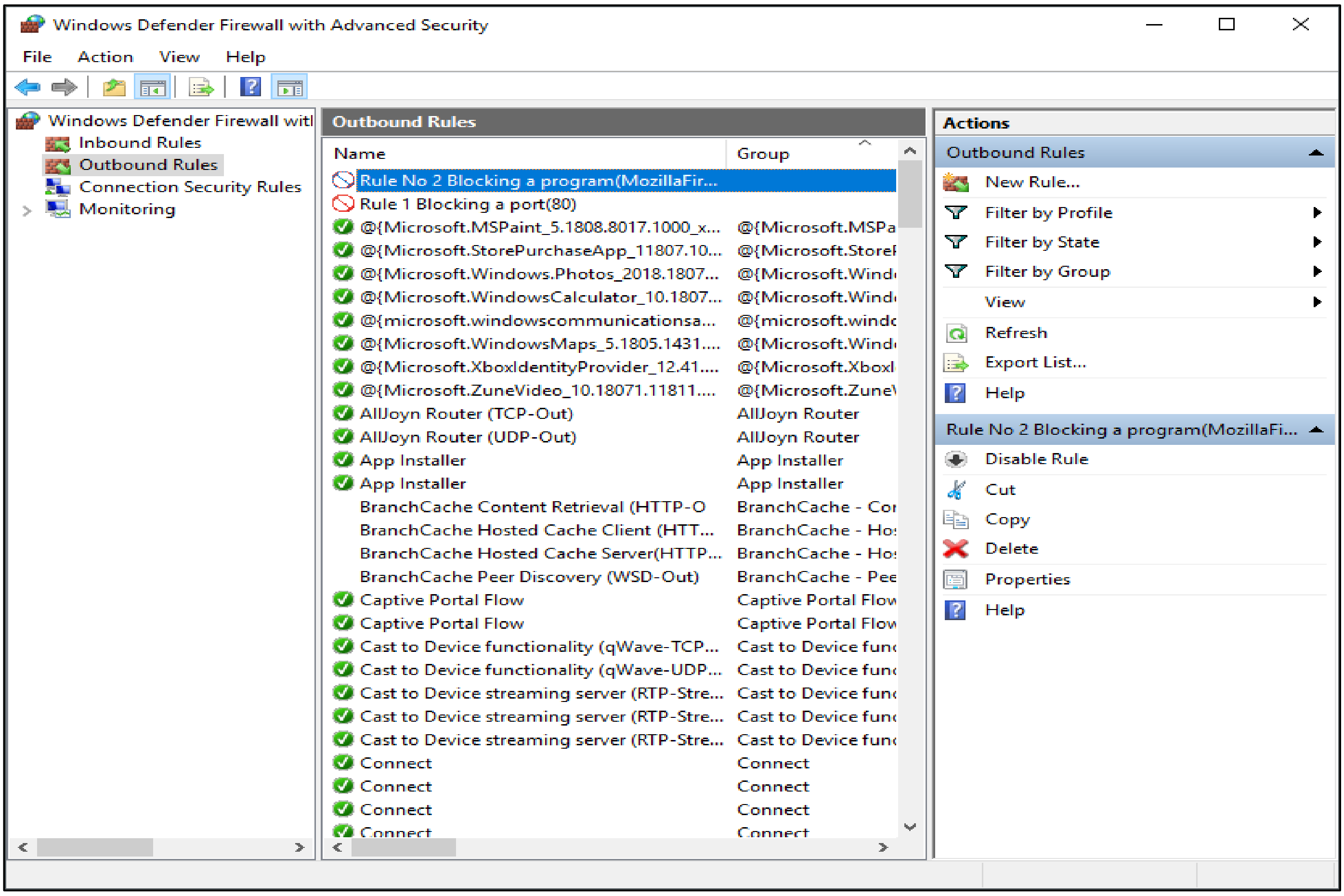
Name

Specify the name and description of this rule.

Name: Rule No 2 Blocking a program(MozillaFirefox)

Description (optional):

Output:

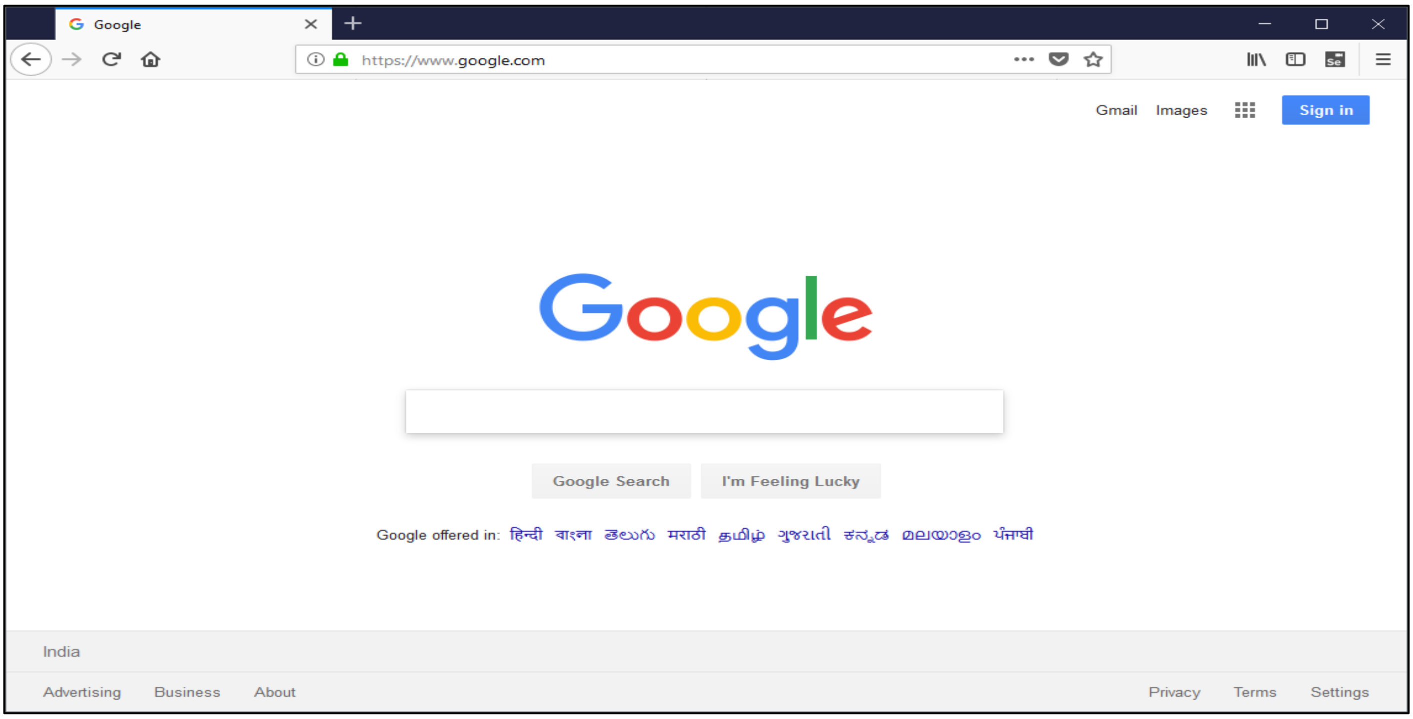


Windows Defender Firewall with Advanced Security

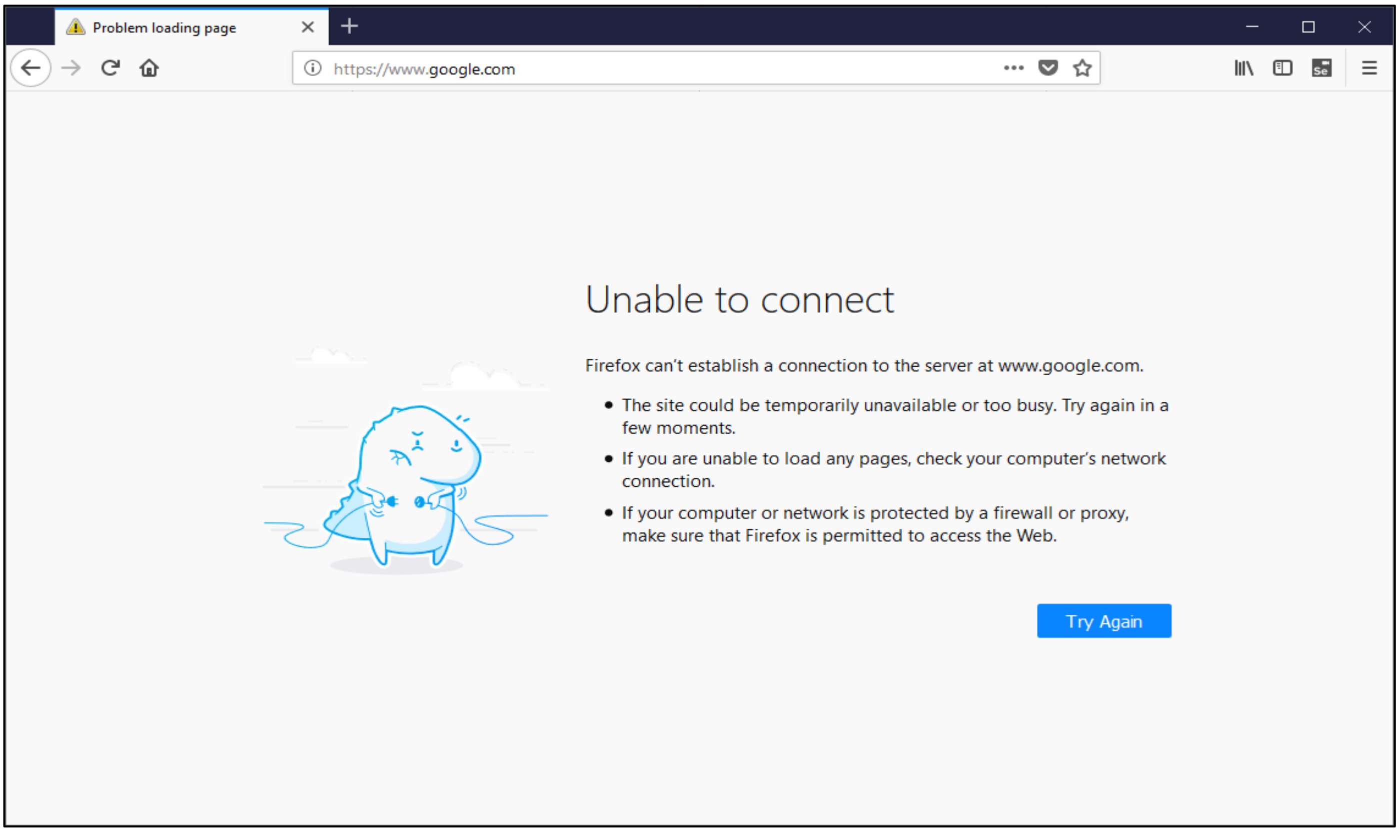
Outbound Rules

Name	Group
Rule No 2 Blocking a program(MozillaFir...	
Rule 1 Blocking a port(80)	
@{Microsoft.MSPaint_5.1808.8017.1000_x...	@{Microsoft.MSPa
@{Microsoft.StorePurchaseApp_11807.10...	@{Microsoft.StoreP
@{Microsoft.Windows.Photos_2018.1807...	@{Microsoft.Wind
@{Microsoft.WindowsCalculator_10.1807...	@{Microsoft.Wind
@{microsoft.windowscommunicationsa...	@{microsoft.windc
@{Microsoft.WindowsMaps_5.1805.1431....	@{Microsoft.Wind
@{Microsoft.XboxIdentityProvider_12.41....	@{Microsoft.XboxI
@{Microsoft.ZuneVideo_10.18071.11811....	@{Microsoft.Zune\
AllJoyn Router (TCP-Out)	AllJoyn Router
AllJoyn Router (UDP-Out)	AllJoyn Router
App Installer	App Installer
App Installer	App Installer
BranchCache Content Retrieval (HTTP-O	BranchCache - Cor
BranchCache Hosted Cache Client (HTT...	BranchCache - Ho:
BranchCache Hosted Cache Server(HTTP...	BranchCache - Ho:
BranchCache Peer Discovery (WSD-Out)	BranchCache - Pee
Captive Portal Flow	Captive Portal Flow
Captive Portal Flow	Captive Portal Flow
Cast to Device functionality (qWave-TCP...	Cast to Device func
Cast to Device functionality (qWave-UDP...	Cast to Device func
Cast to Device streaming server (RTP-Stre...	Cast to Device func
Cast to Device streaming server (RTP-Stre...	Cast to Device func
Cast to Device streaming server (RTP-Stre...	Cast to Device func
Connect	Connect
Connect	Connect
Connect	Connect
Connect	Connect

Before Applying the Rule:



After Applying the Rule:



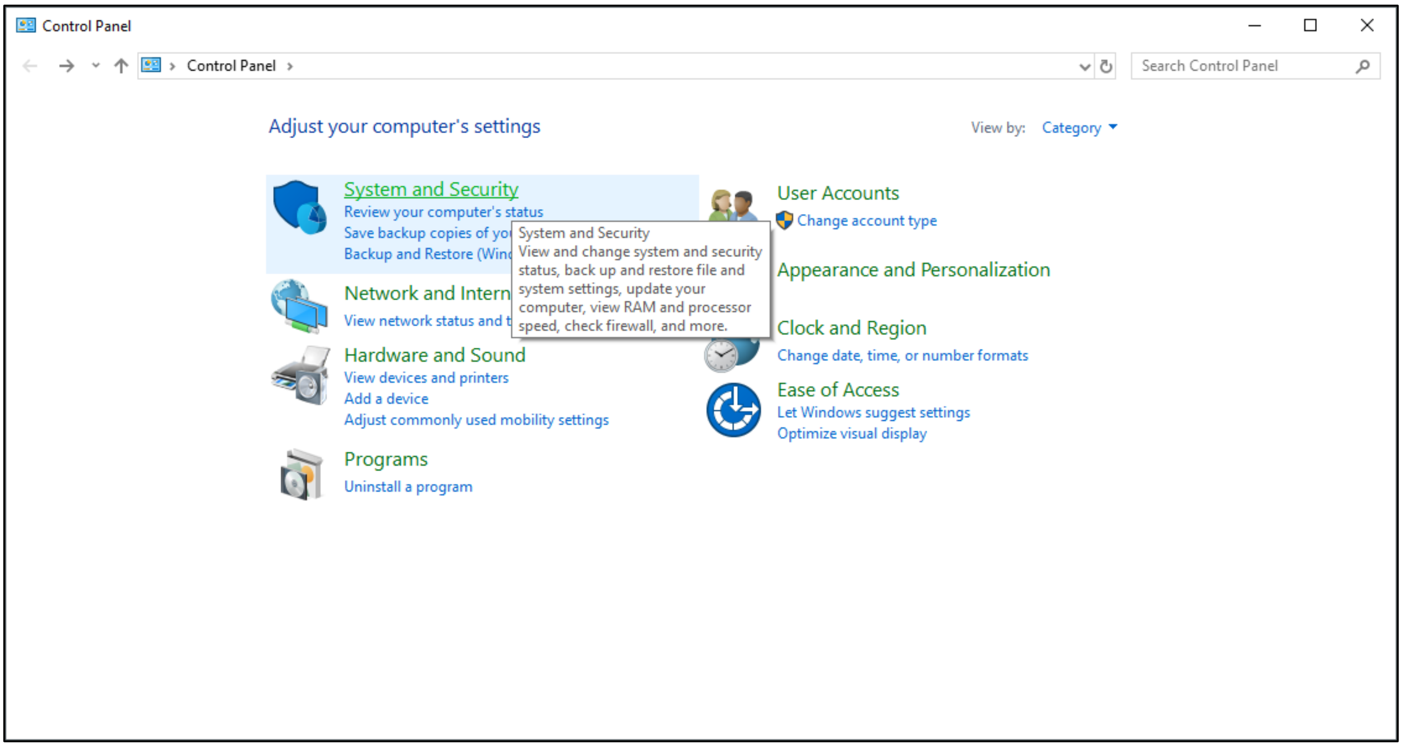
Unable to connect

Firefox can't establish a connection to the server at www.google.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

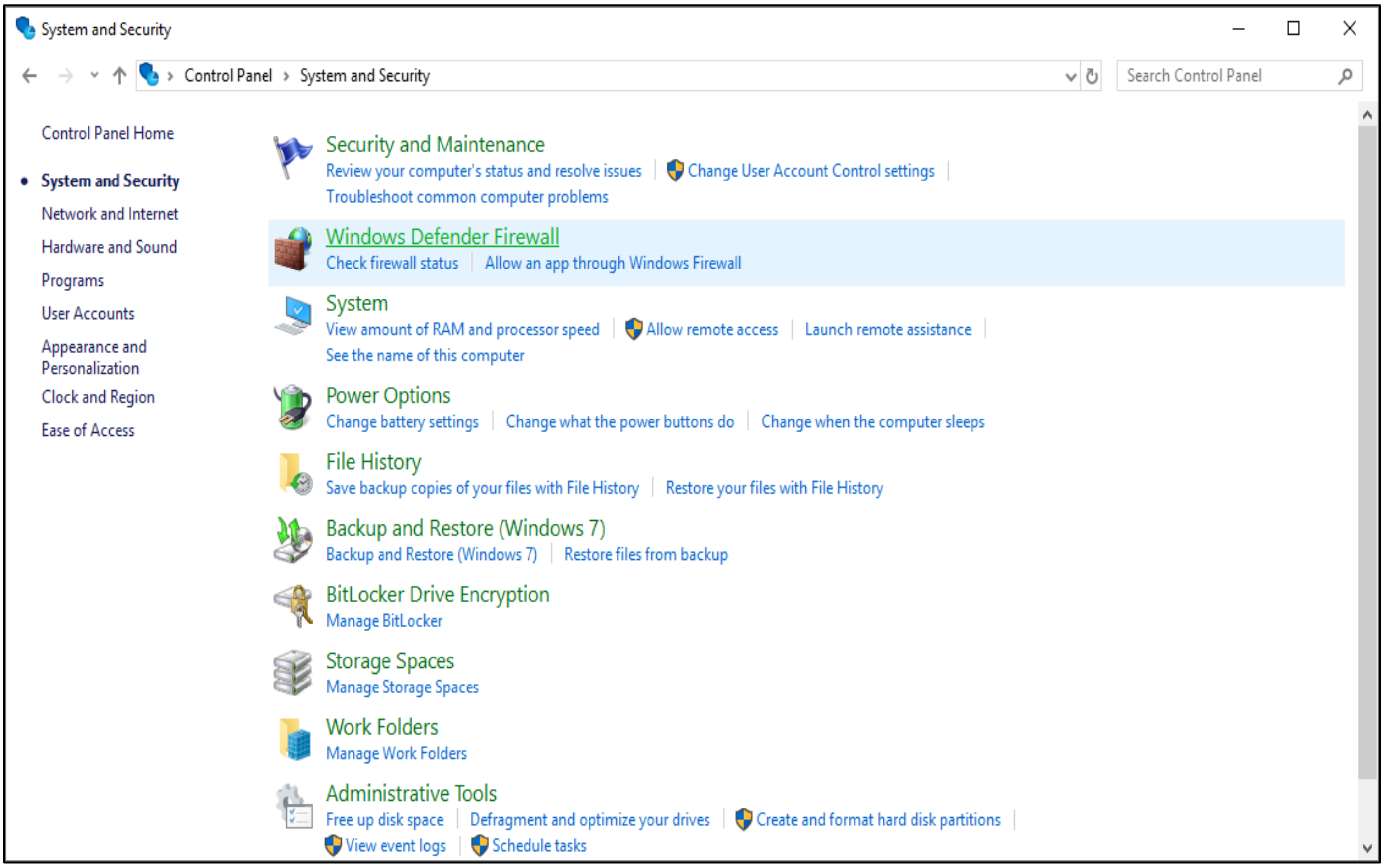
C) Blocking a website:

Step 1: Open control panel and go to System Security.

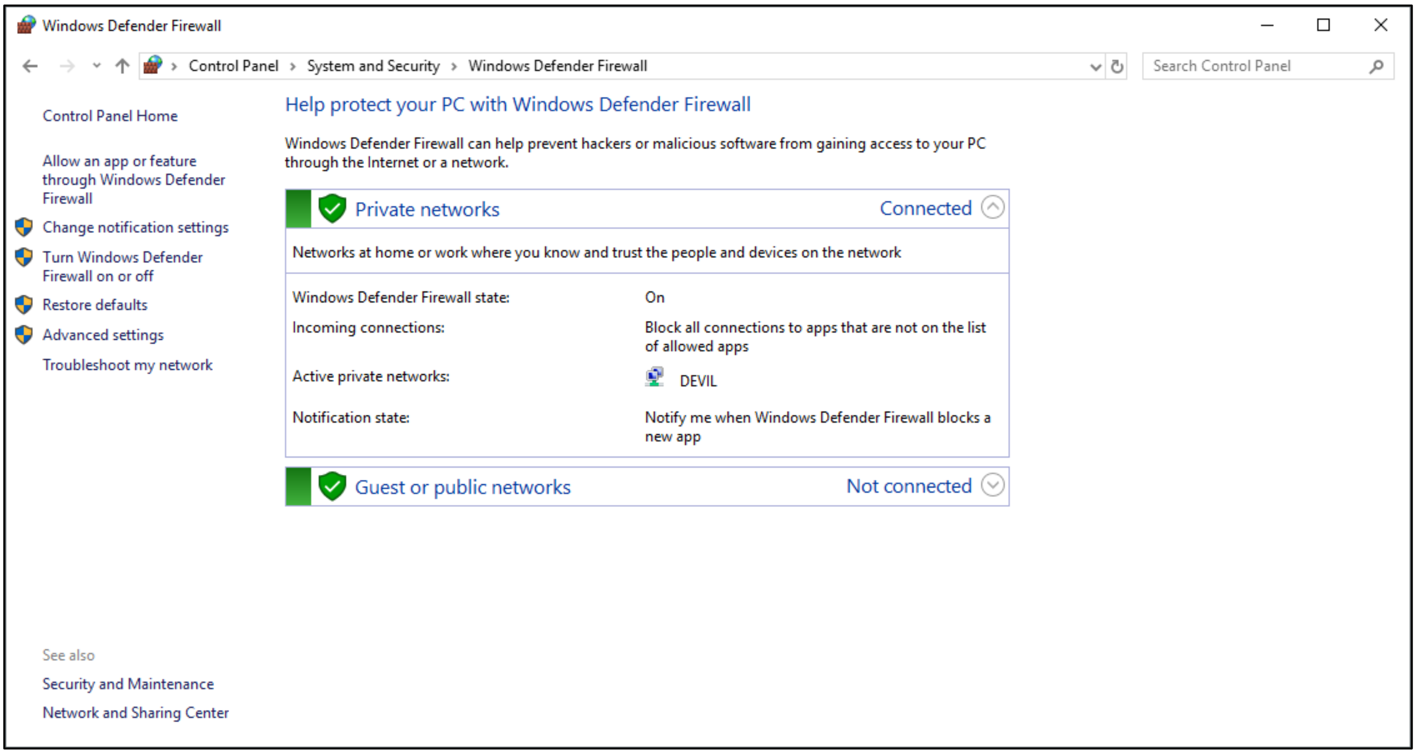


System and Security
View and change system and security status, back up and restore file and system settings, update your computer, view RAM and processor speed, check firewall, and more.

Step 2: Now Select Windows Defender Firewall.


System and Security
Control Panel › System and Security
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Power Options
Change battery settings
Change what the power buttons do
Change when the computer sleeps
File History
Save backup copies of your files with File History
Restore your files with File History
Backup and Restore (Windows 7)
Backup and Restore (Windows 7)
Restore files from backup
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Free up disk space
Defragment and optimize your drives
Create and format hard disk partitions
View event logs
Schedule tasks

Step 3: Now you need to select Advanced setting.



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.

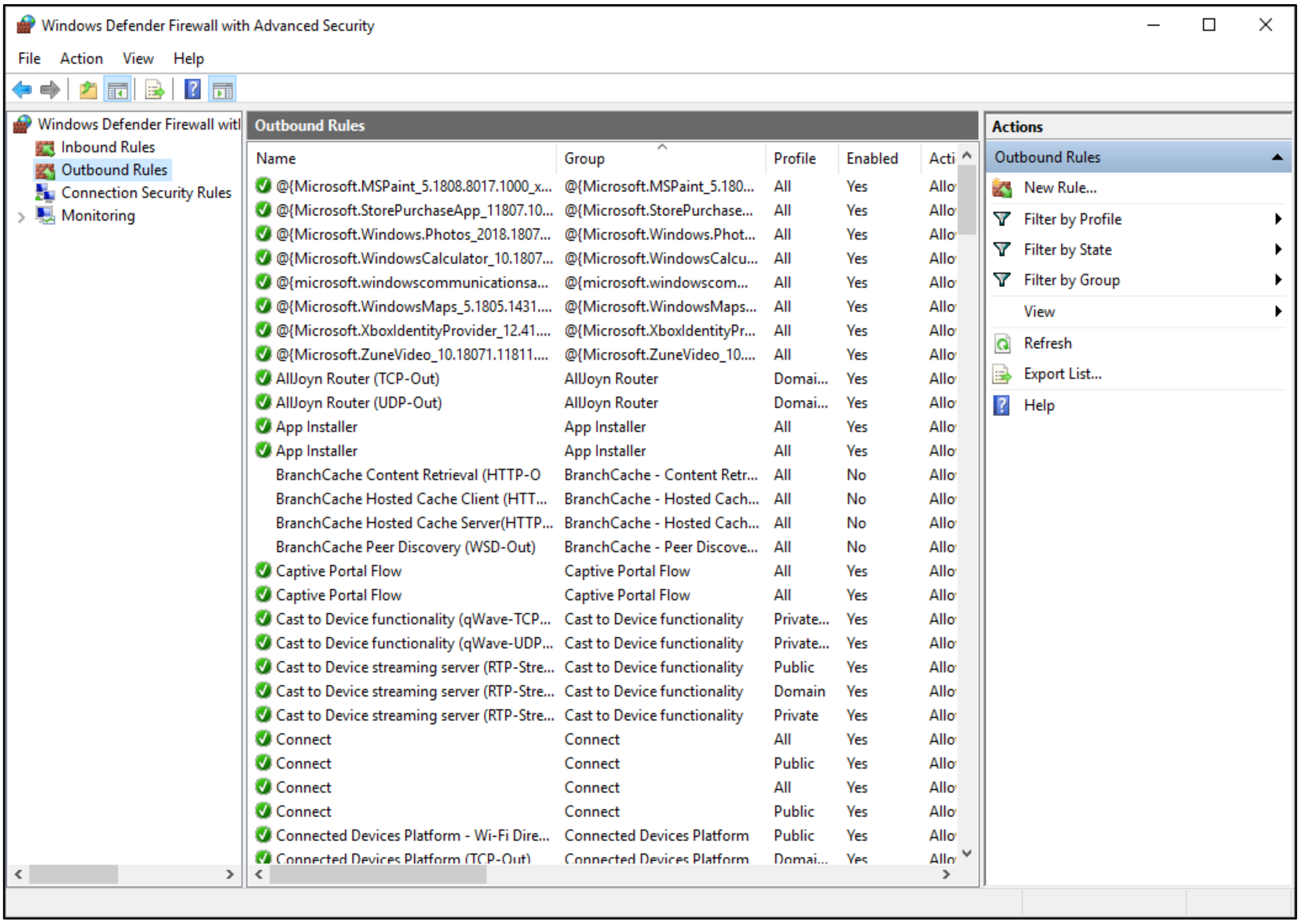
Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

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

Guest or public networks Not connected

Step 4: Now Select Outbound Rules.



Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall wit
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

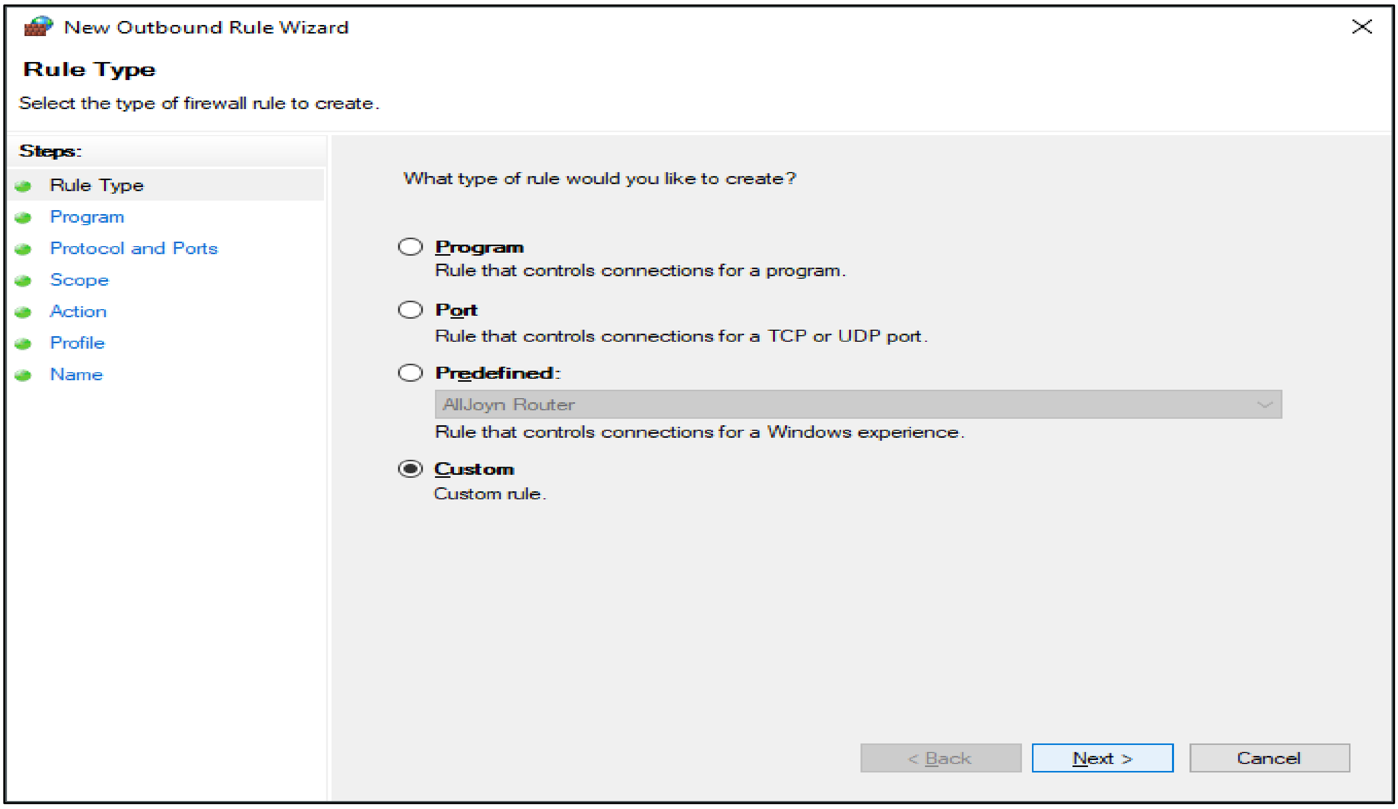
Outbound Rules

Name	Group	Profile	Enabled	Acti
@{Microsoft.MSPaint_5.1808.8017.1000_x...	@{Microsoft.MSPaint_5.180...	All	Yes	Allo
@{Microsoft.StorePurchaseApp_11807.10...	@{Microsoft.StorePurchase...	All	Yes	Allo
@{Microsoft.Windows.Photos_2018.1807....	@{Microsoft.Windows.Phot...	All	Yes	Allo
@{Microsoft.WindowsCalculator_10.1807....	@{Microsoft.WindowsCalcu...	All	Yes	Allo
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All	Yes	Allo
@{Microsoft.WindowsMaps_5.1805.1431....	@{Microsoft.WindowsMaps...	All	Yes	Allo
@{Microsoft.XboxIdentityProvider_12.41....	@{Microsoft.XboxIdentityPr...	All	Yes	Allo
@{Microsoft.ZuneVideo_10.18071.11811....	@{Microsoft.ZuneVideo_10....	All	Yes	Allo
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allo
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allo
App Installer	App Installer	All	Yes	Allo
App Installer	App Installer	All	Yes	Allo
BranchCache Content Retrieval (HTTP-O	BranchCache - Content Retr...	All	No	Allo
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allo
Captive Portal Flow	Captive Portal Flow	All	Yes	Allo
Captive Portal Flow	Captive Portal Flow	All	Yes	Allo
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allo
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allo
Connect	Connect	All	Yes	Allo
Connect	Connect	Public	Yes	Allo
Connect	Connect	All	Yes	Allo
Connect	Connect	Public	Yes	Allo
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allo
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allo

Actions

Outbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

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.

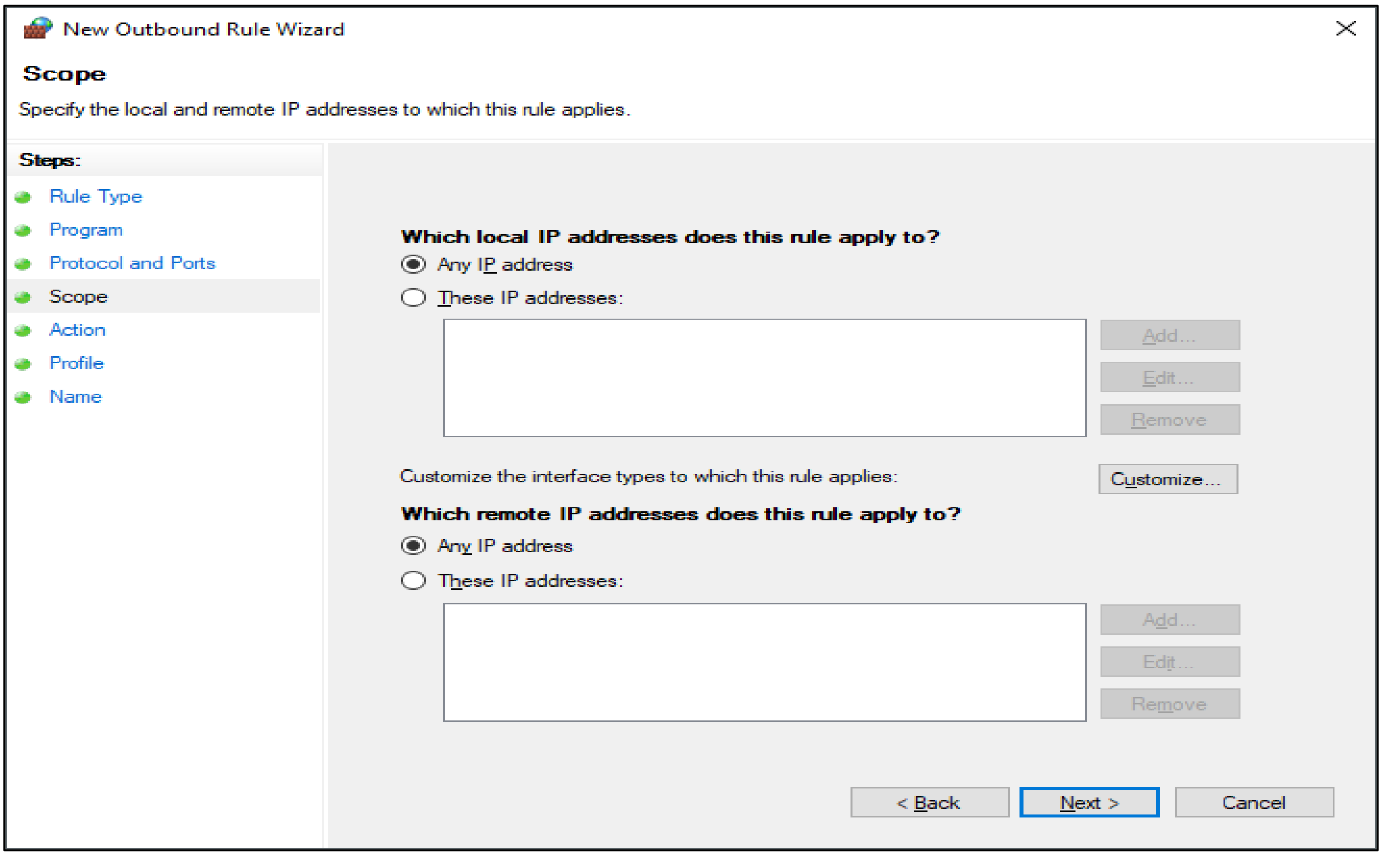
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
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".



New Outbound 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?

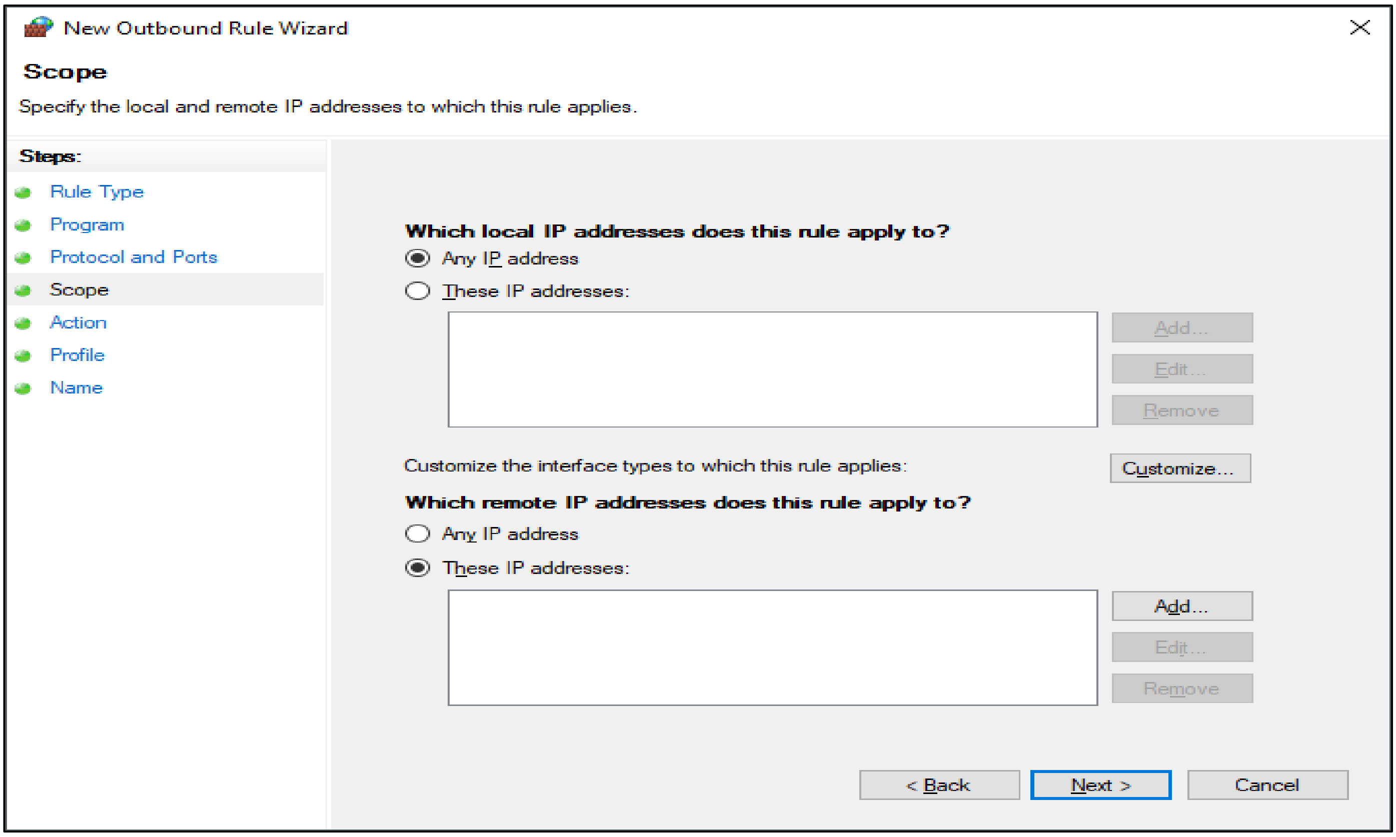
● Any IP address

○ These IP addresses:

Add... | Edit... | Remove

< Back | Next > | Cancel

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



New Outbound 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:

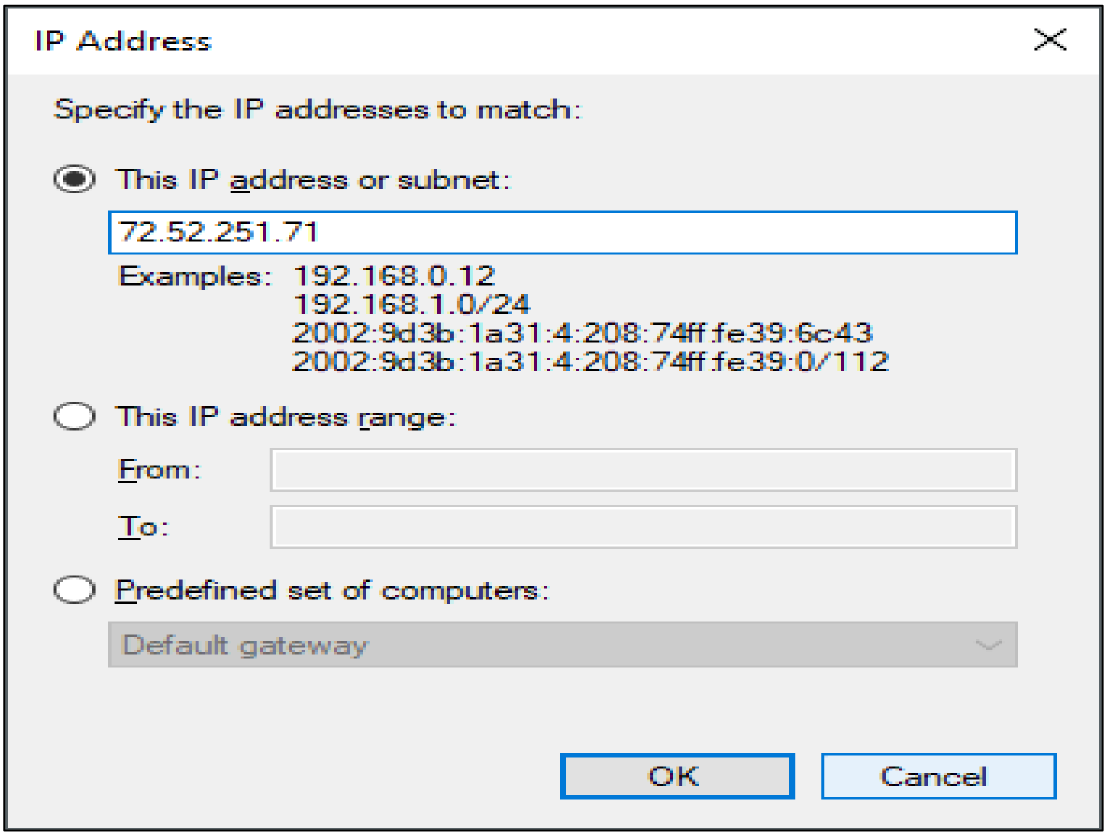
Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

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:

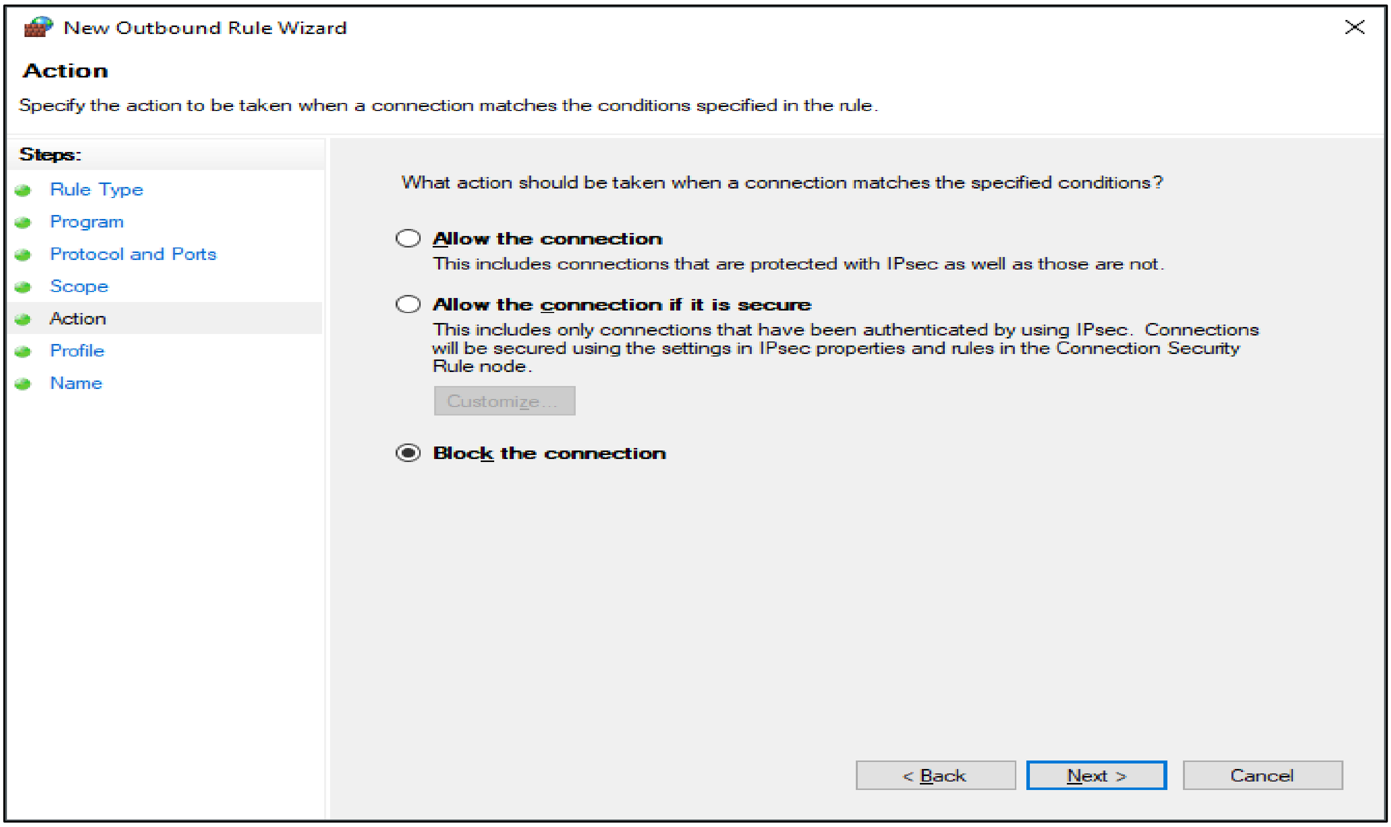
From:

To:

○ Predefined set of computers:

Default gateway

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

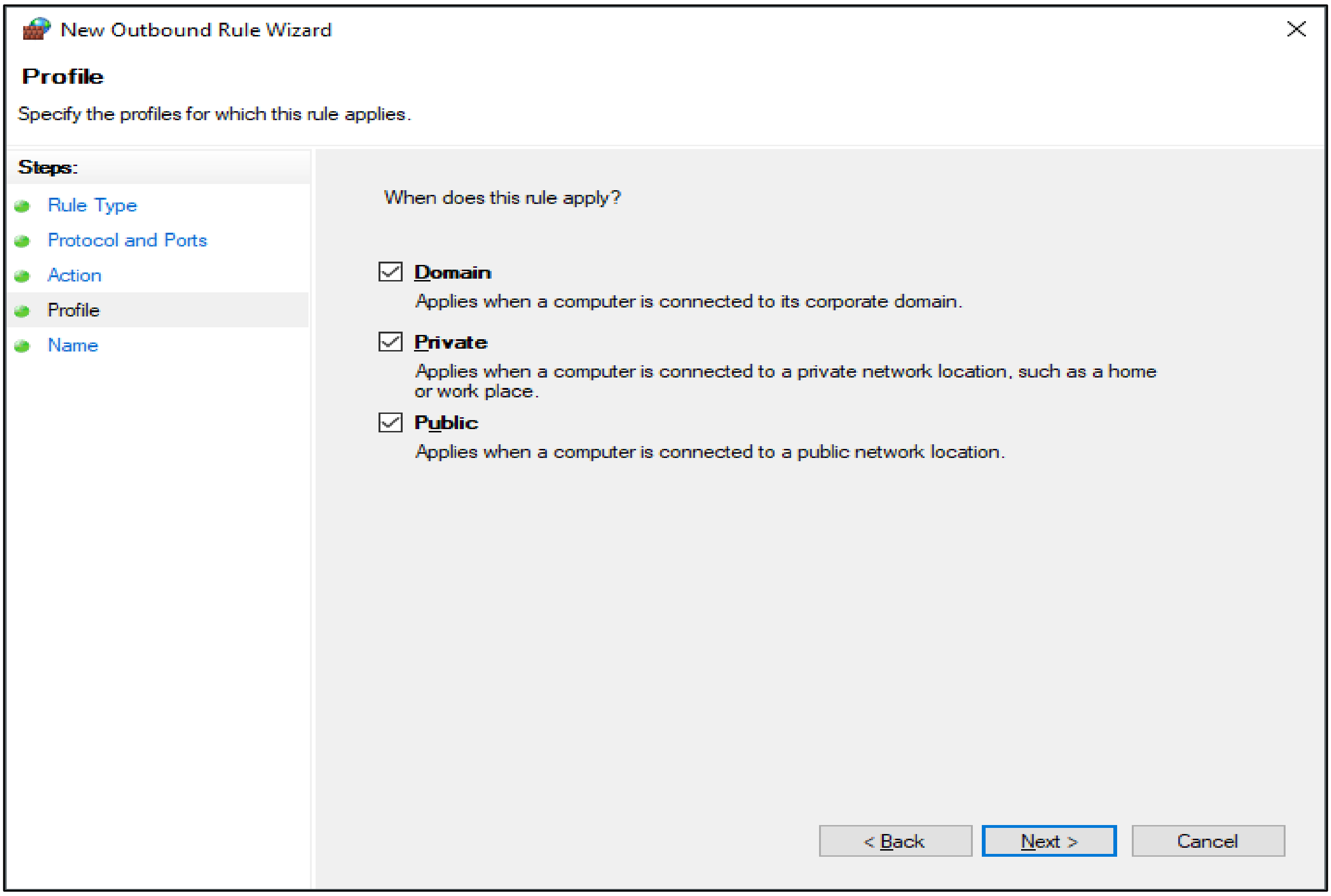
What action should be taken when a connection matches the specified conditions?

○ **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.

● **Block the connection**

Step 10: 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

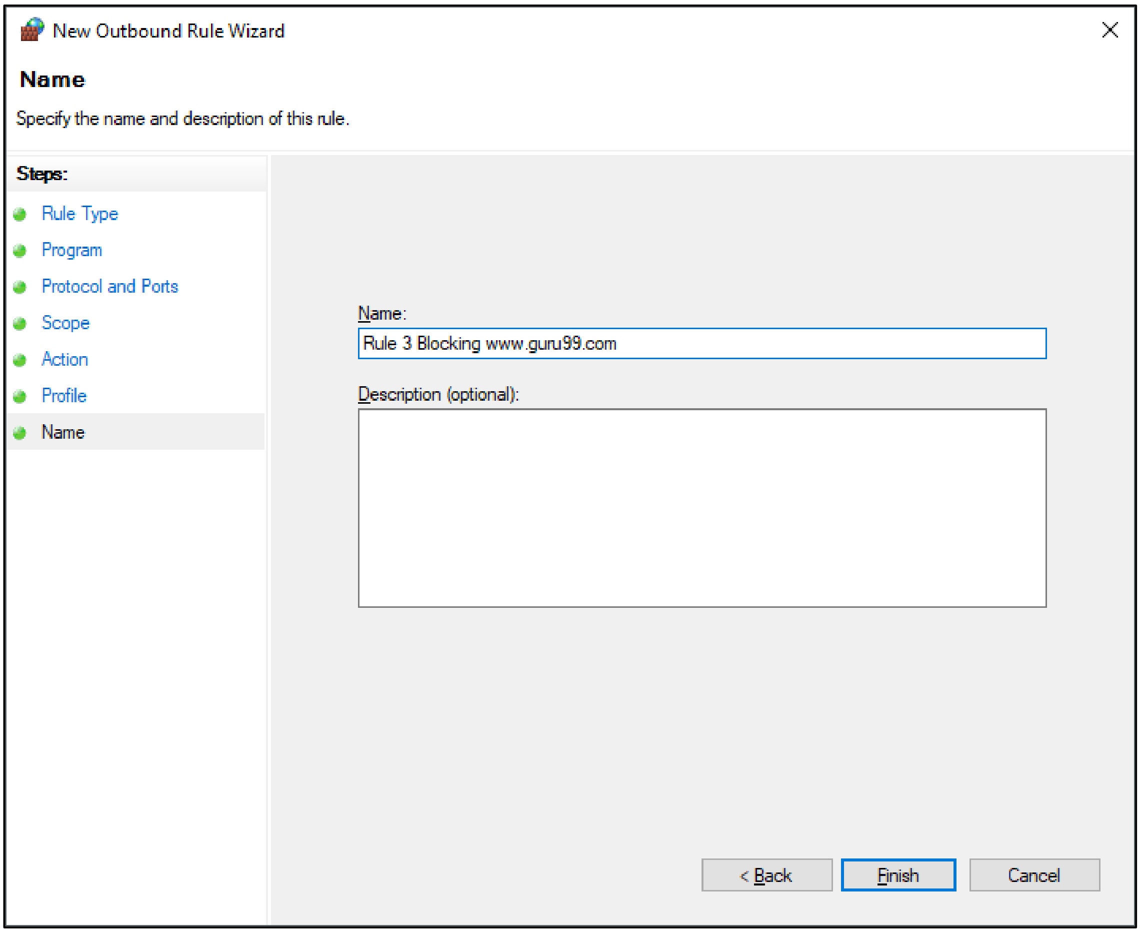
When does this rule apply?

☑ **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.

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



New Outbound Rule Wizard

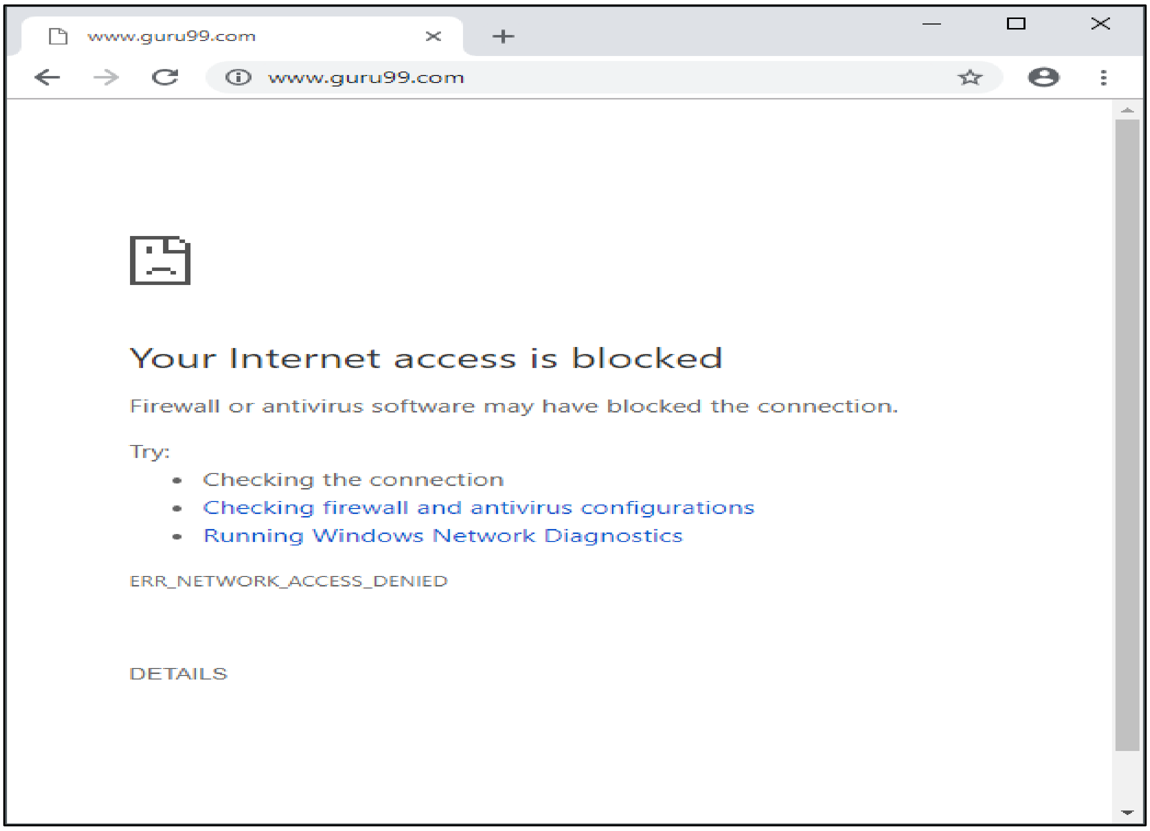
Name

Specify the name and description of this rule.

Name: Rule 3 Blocking www.guru99.com

Description (optional):

Output:



Your Internet access is blocked

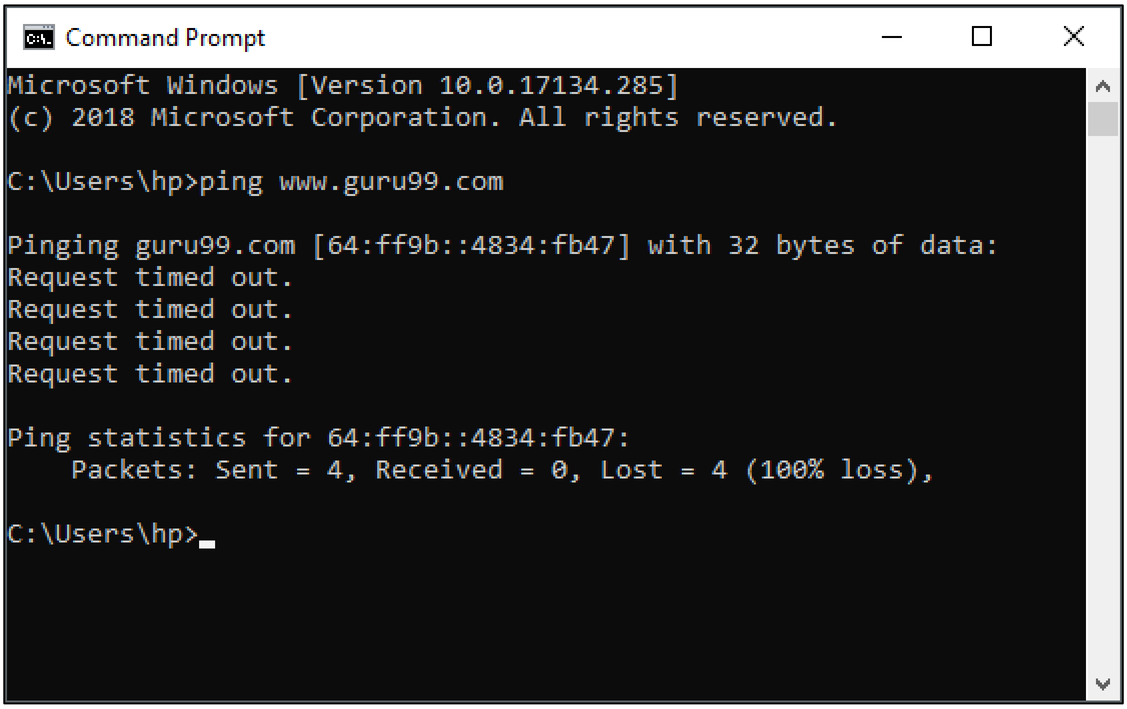
Firewall or antivirus software may have blocked the connection.

Try:

- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

ERR_NETWORK_ACCESS_DENIED

DETAILS



```
Microsoft Windows [Version 10.0.17134.285]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Pinging guru99.com [64:ff9b::4834:fb47] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 64:ff9b::4834:fb47:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\hp>_
```