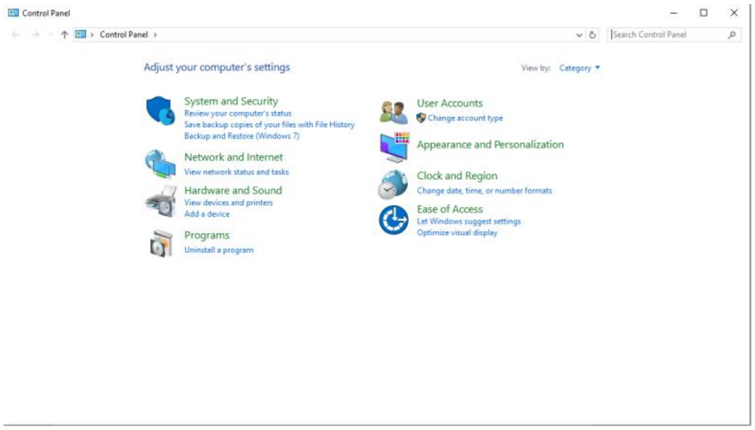
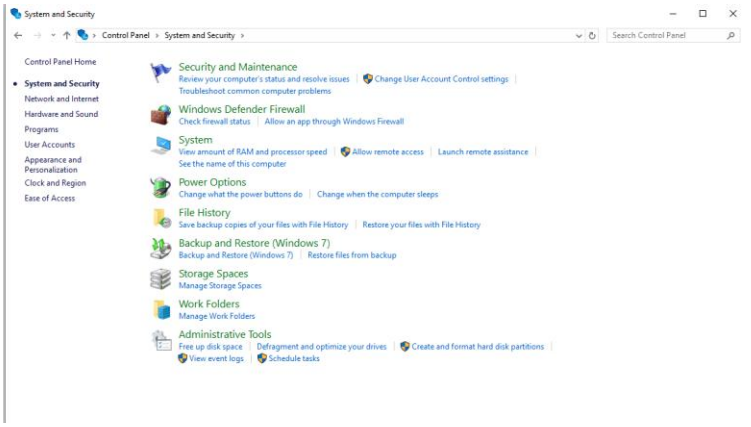
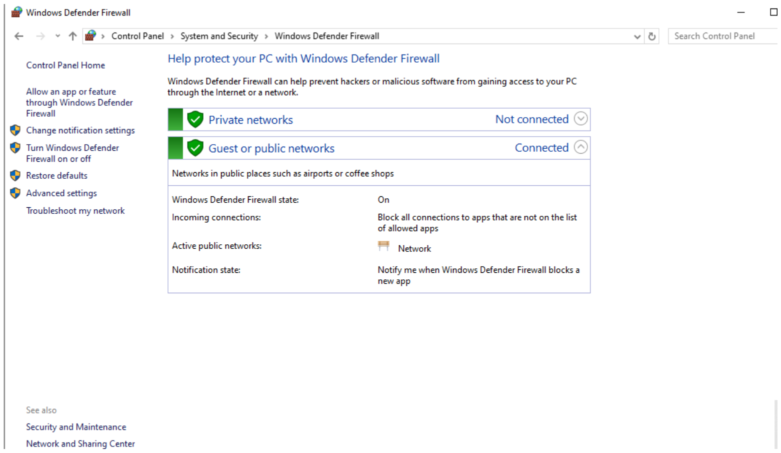
Practical 9

Aim: Firewall

To block a port


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 your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
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


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 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
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


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

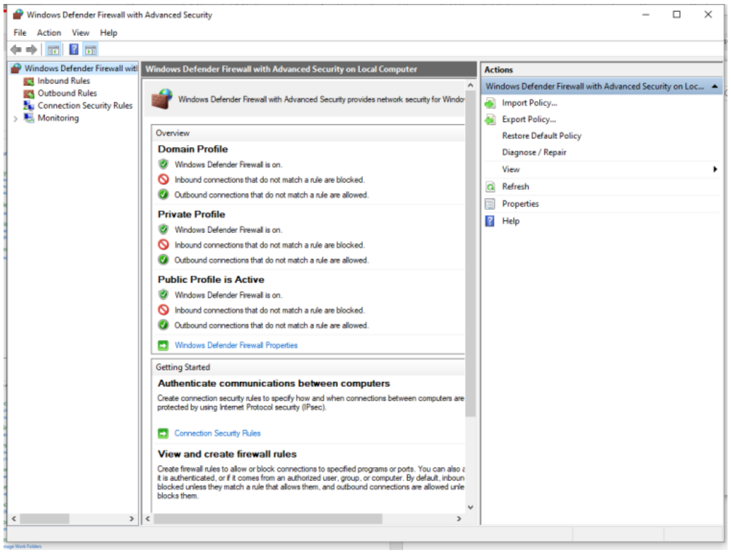
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

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:	Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windo

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

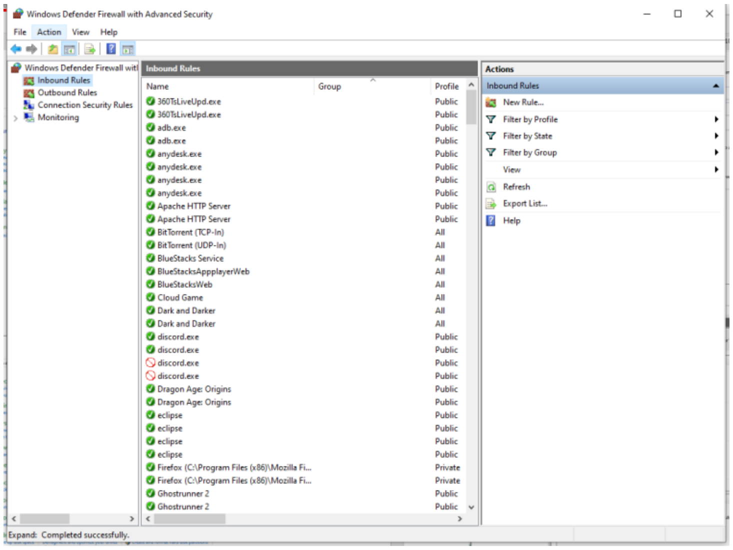
Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

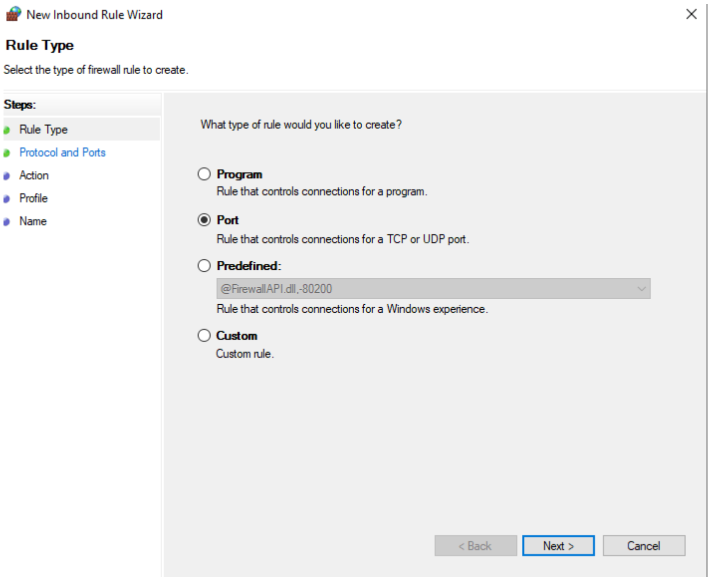
Create firewall rules to allow or block connections to specified programs or ports. You can also a it is authenticated, or if it comes from an authorized user, group, or computer. By default, inboun blocked unless they match a rule that allows them, and outbound connections are allowed unle blocks them.



Inbound Rules

Name	Group	Profile
✓ 360TsLiveUpd.exe		Public
✓ 360TsLiveUpd.exe		Public
✓ adb.exe		Public
✓ adb.exe		Public
✓ anydesk.exe		Public
✓ anydesk.exe		Public
✓ anydesk.exe		Public
✓ anydesk.exe		Public
✓ Apache HTTP Server		Public
✓ Apache HTTP Server		Public
✓ BitTorrent (TCP-In)		All
✓ BitTorrent (UDP-In)		All
✓ BlueStacks Service		All
✓ BlueStacksAppplayerWeb		All
✓ BlueStacksWeb		All
✓ Cloud Game		All
✓ Dark and Darker		All
✓ Dark and Darker		All
✓ discord.exe		Public
✓ discord.exe		Public
⃠ discord.exe		Public
⃠ discord.exe		Public
✓ Dragon Age: Origins		Public
✓ Dragon Age: Origins		Public
✓ eclipse		Public
✓ eclipse		Public
✓ eclipse		Public
✓ eclipse		Public
✓ Firefox (C:\Program Files (x86)\Mozilla Fi...		Private
✓ Firefox (C:\Program Files (x86)\Mozilla Fi...		Private
✓ Ghostrunner 2		Public
✓ Ghostrunner 2		Public

Expand: Completed successfully.



Rule Type

Select the type of firewall rule to create.

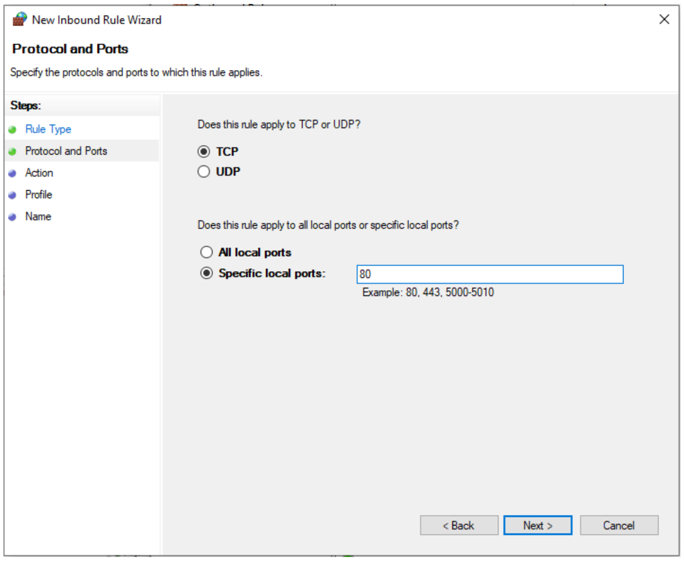
What type of rule would you like to create?

○ 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.


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

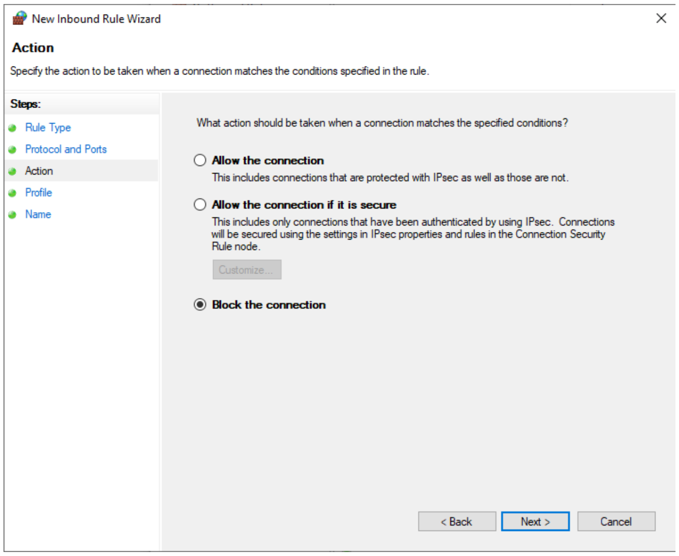
○ UDP

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

○ All local ports

● Specific local ports: 80

Example: 80, 443, 5000-5010


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?

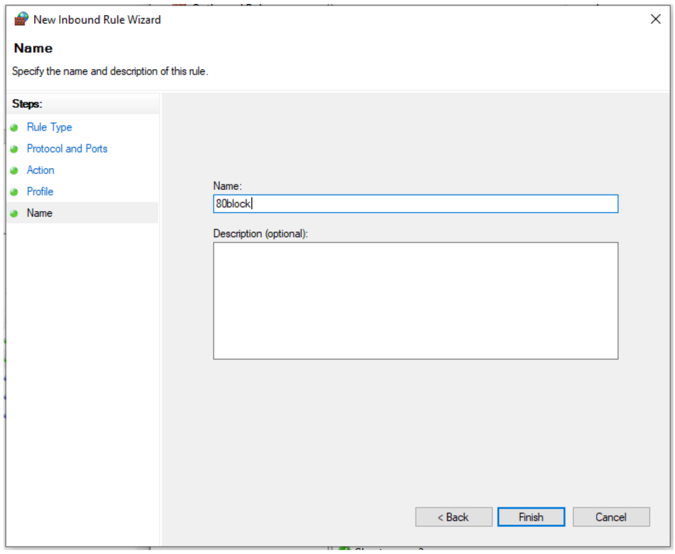
○ Allow the connection

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


New Inbound Rule Wizard

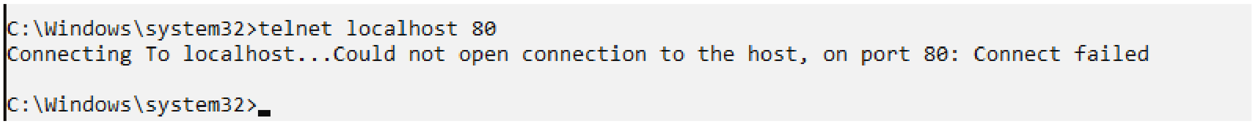
Name

Specify the name and description of this rule.

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

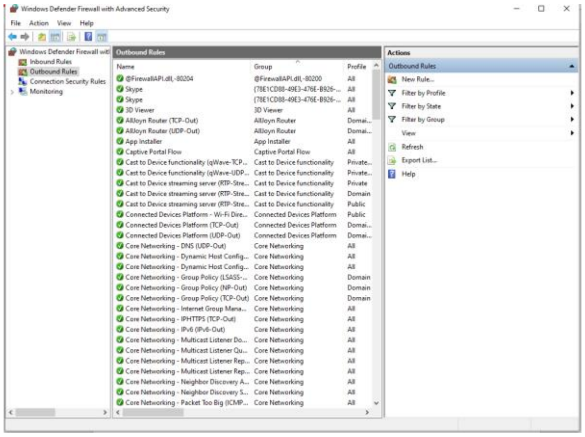
Name: 80block

Description (optional):



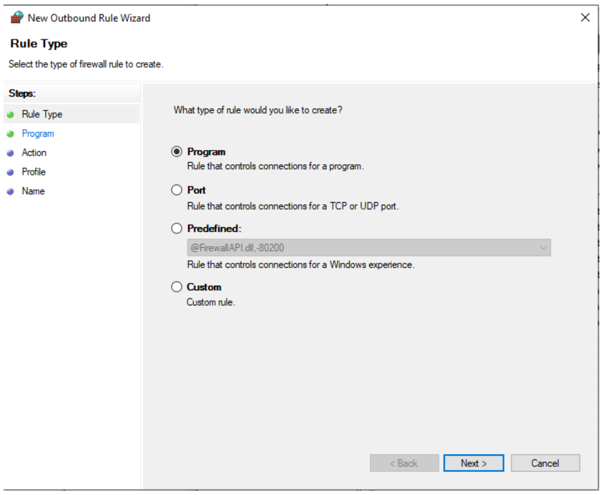
```
C:\Windows\system32>telnet localhost 80
Connecting To localhost...Could not open connection to the host, on port 80: Connect failed

C:\Windows\system32>_
```

To block a program



Outbound Rules

Name	Group	Profile
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All
Skype	{78E1CD88-49E3-476E-B926-...	All
Skype	{78E1CD88-49E3-476E-B926-...	All
3D Viewer	3D Viewer	All
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...
App Installer	App Installer	All
Captive Portal Flow	Captive Portal Flow	All
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...
Core Networking - DNS (UDP-Out)	Core Networking	All
Core Networking - Dynamic Host Config...	Core Networking	All
Core Networking - Dynamic Host Config...	Core Networking	All
Core Networking - Group Policy (LSASS-...	Core Networking	Domain
Core Networking - Group Policy (NP-Out)	Core Networking	Domain
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain
Core Networking - Internet Group Mana...	Core Networking	All
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All
Core Networking - IPv6 (IPv6-Out)	Core Networking	All
Core Networking - Multicast Listener Do...	Core Networking	All
Core Networking - Multicast Listener Qu...	Core Networking	All
Core Networking - Multicast Listener Rep...	Core Networking	All
Core Networking - Multicast Listener Rep...	Core Networking	All
Core Networking - Neighbor Discovery A...	Core Networking	All
Core Networking - Neighbor Discovery S...	Core Networking	All
Core Networking - Packet Too Big (ICMP...	Core Networking	All



Rule Type

Select the type of firewall rule to create.

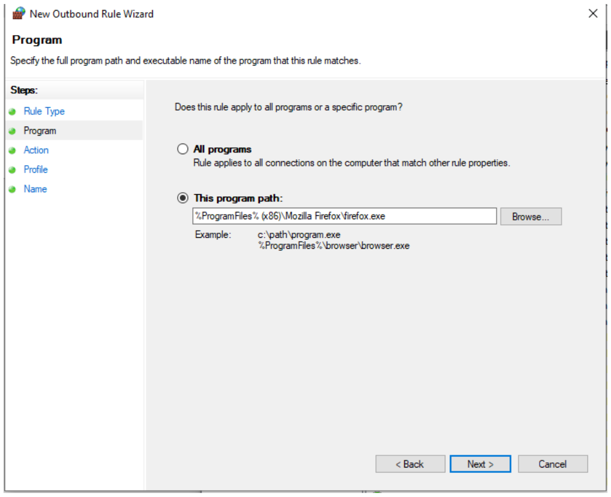
What type of rule would you like to create?

● **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.



Program

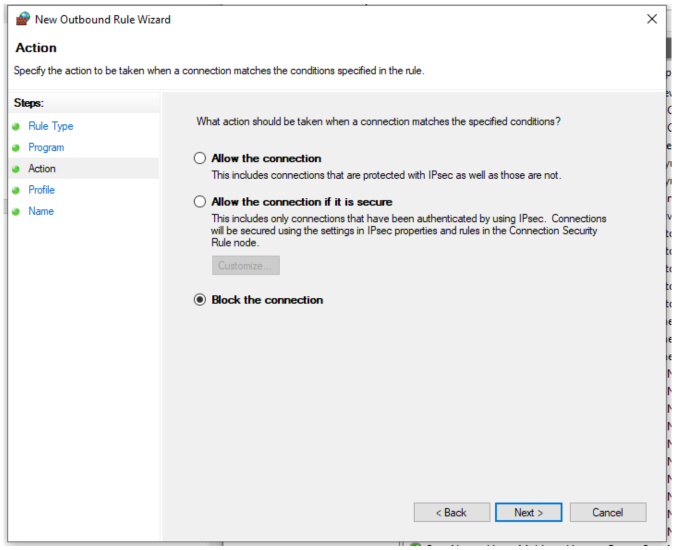
Specify the full program path and executable name of the program that this rule matches.

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% (x86)\Mozilla Firefox\firefox.exe

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



New Outbound Rule Wizard

Action

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

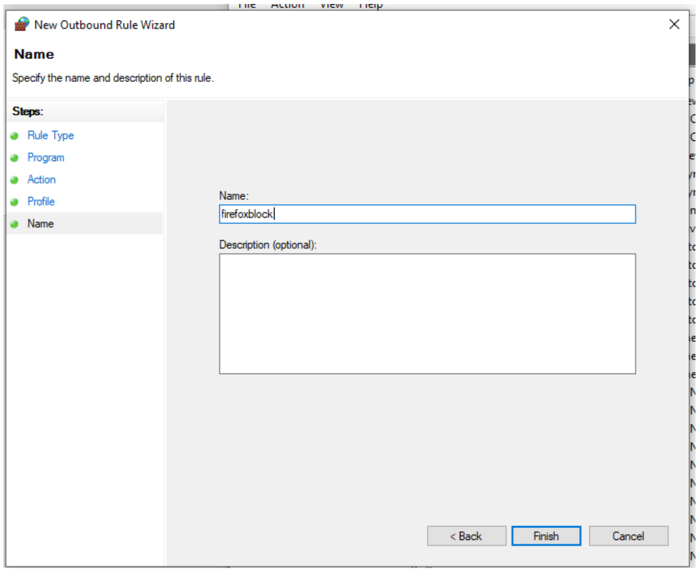
Steps:
- Rule Type
- Program
- Action
- Profile
- Name

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**



New Outbound Rule Wizard

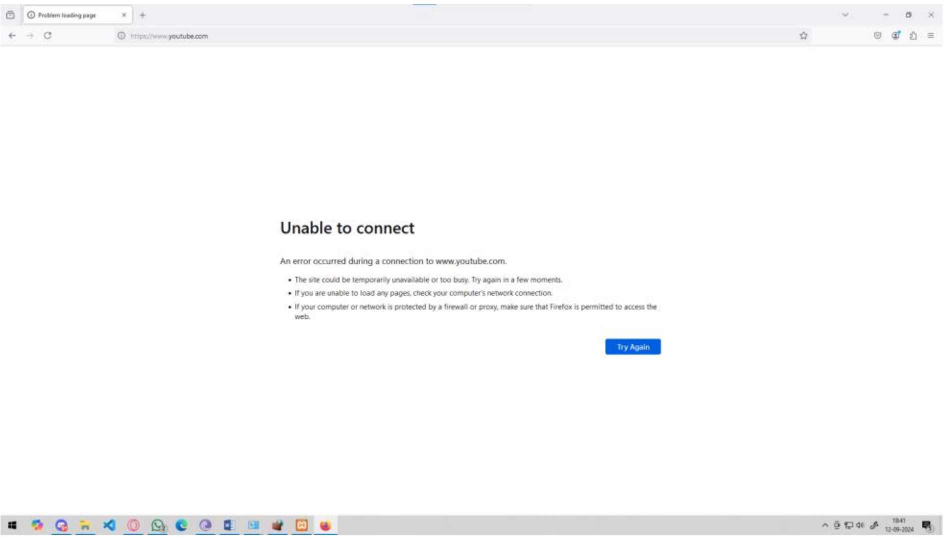
Name

Specify the name and description of this rule.

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

Name: firefoxblock

Description (optional):



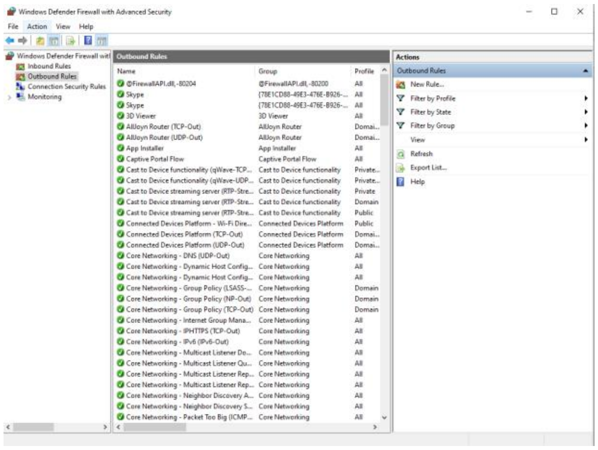
https://www.youtube.com

Unable to connect

An error occurred during a connection to www.youtube.com.

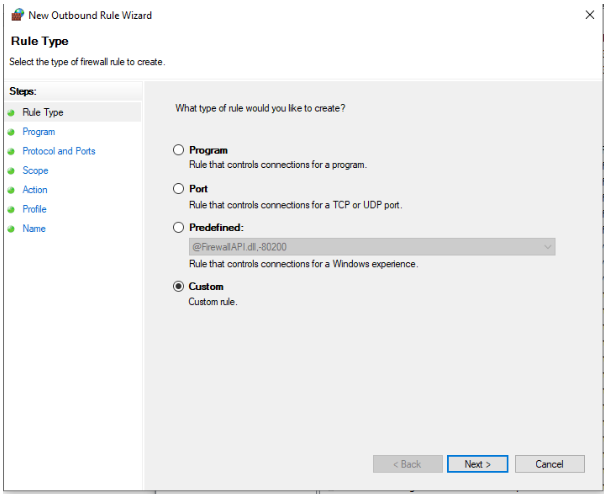
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

To block a site



Outbound Rules

Name	Group	Profile
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All
Skype	{78E1CD88-49E3-476E-B926-...	All
Skype	{78E1CD88-49E3-476E-B926-...	All
3D Viewer	3D Viewer	All
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...
App Installer	App Installer	All
Captive Portal Flow	Captive Portal Flow	All
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...
Core Networking - DNS (UDP-Out)	Core Networking	All
Core Networking - Dynamic Host Config...	Core Networking	All
Core Networking - Dynamic Host Config...	Core Networking	All
Core Networking - Group Policy (LSASS-...	Core Networking	Domain
Core Networking - Group Policy (NP-Out)	Core Networking	Domain
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain
Core Networking - Internet Group Mana...	Core Networking	All
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All
Core Networking - IPv6 (IPv6-Out)	Core Networking	All
Core Networking - Multicast Listener Do...	Core Networking	All
Core Networking - Multicast Listener Qu...	Core Networking	All
Core Networking - Multicast Listener Rep...	Core Networking	All
Core Networking - Multicast Listener Rep...	Core Networking	All
Core Networking - Neighbor Discovery A...	Core Networking	All
Core Networking - Neighbor Discovery S...	Core Networking	All
Core Networking - Packet Too Big (ICMP...	Core Networking	All



Rule Type

Select the type of firewall rule to create.

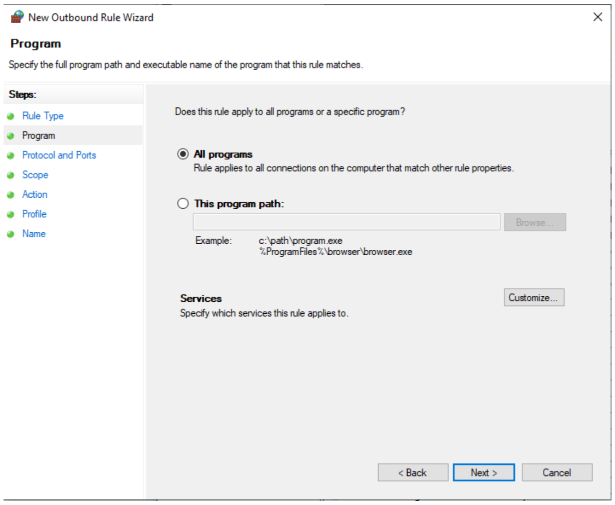
What type of rule would you like to create?

○ **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.



Program

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

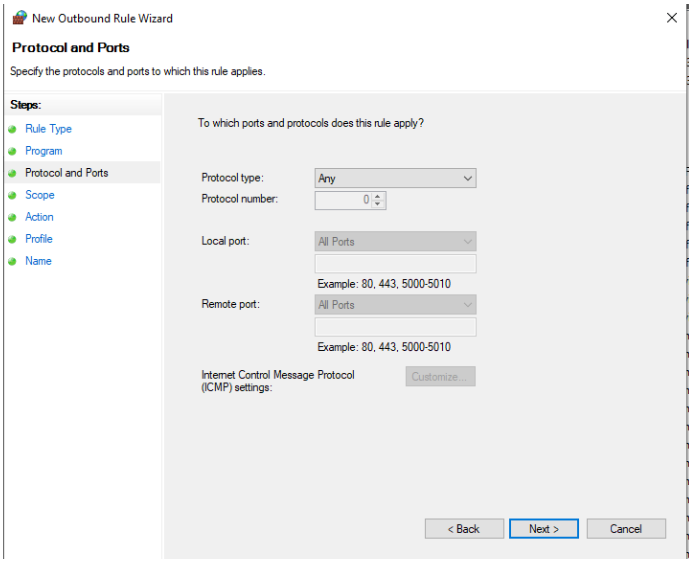
Does this rule apply to all programs or a specific program?

● **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.



New Outbound 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: Any

Protocol number: 0

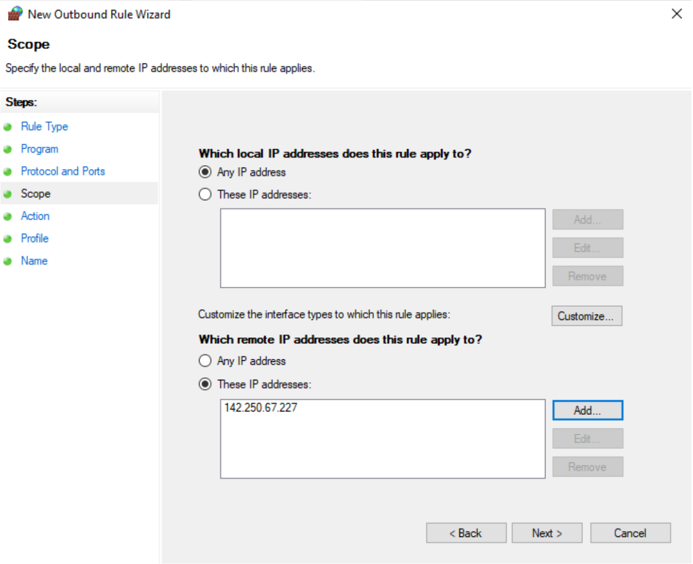
Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:



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:

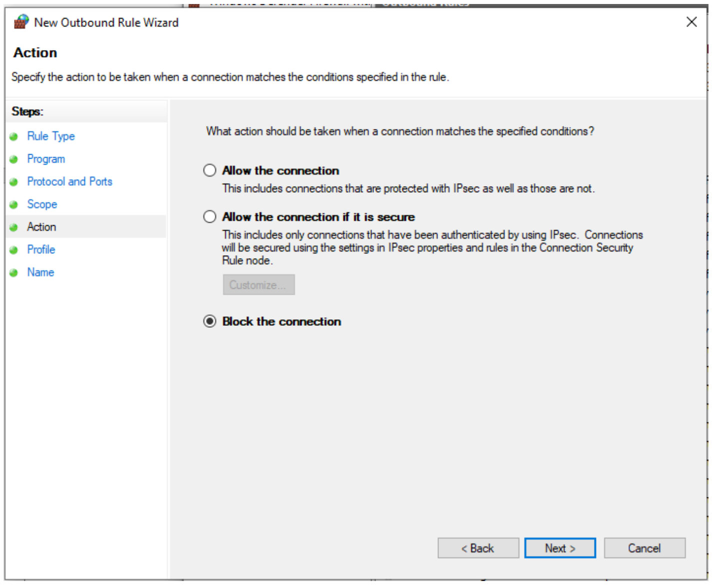
Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

142.250.67.227



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?

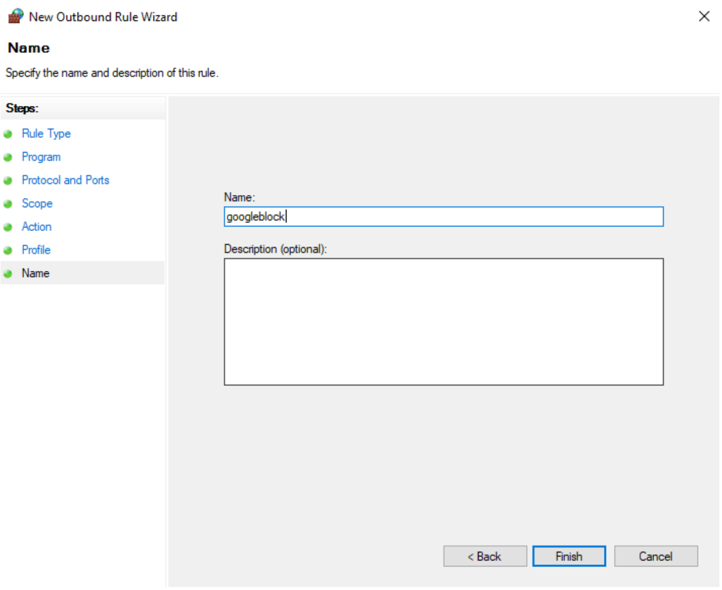
○ **Allow the connection**

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**



New Outbound Rule Wizard

Name

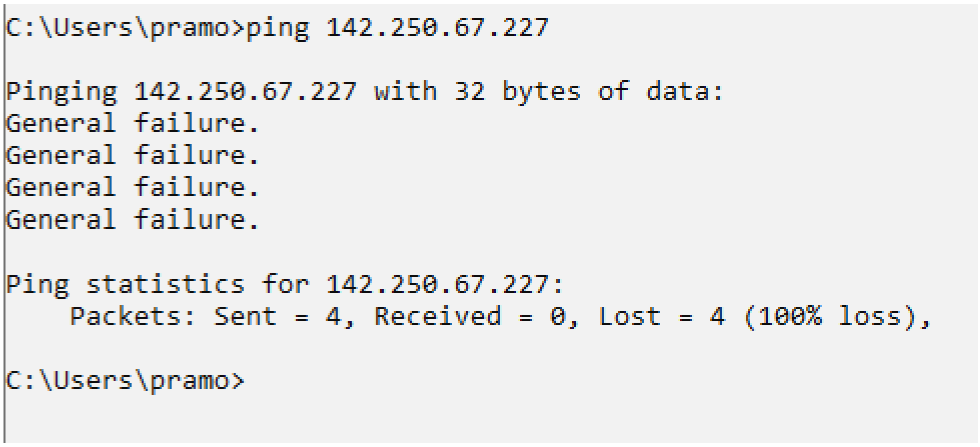
Specify the name and description of this rule.

Steps:

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

Name: googleblock

Description (optional):



```
C:\Users\pramo>ping 142.250.67.227

Pinging 142.250.67.227 with 32 bytes of data:
General failure.
General failure.
General failure.
General failure.

Ping statistics for 142.250.67.227:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\pramo>
```