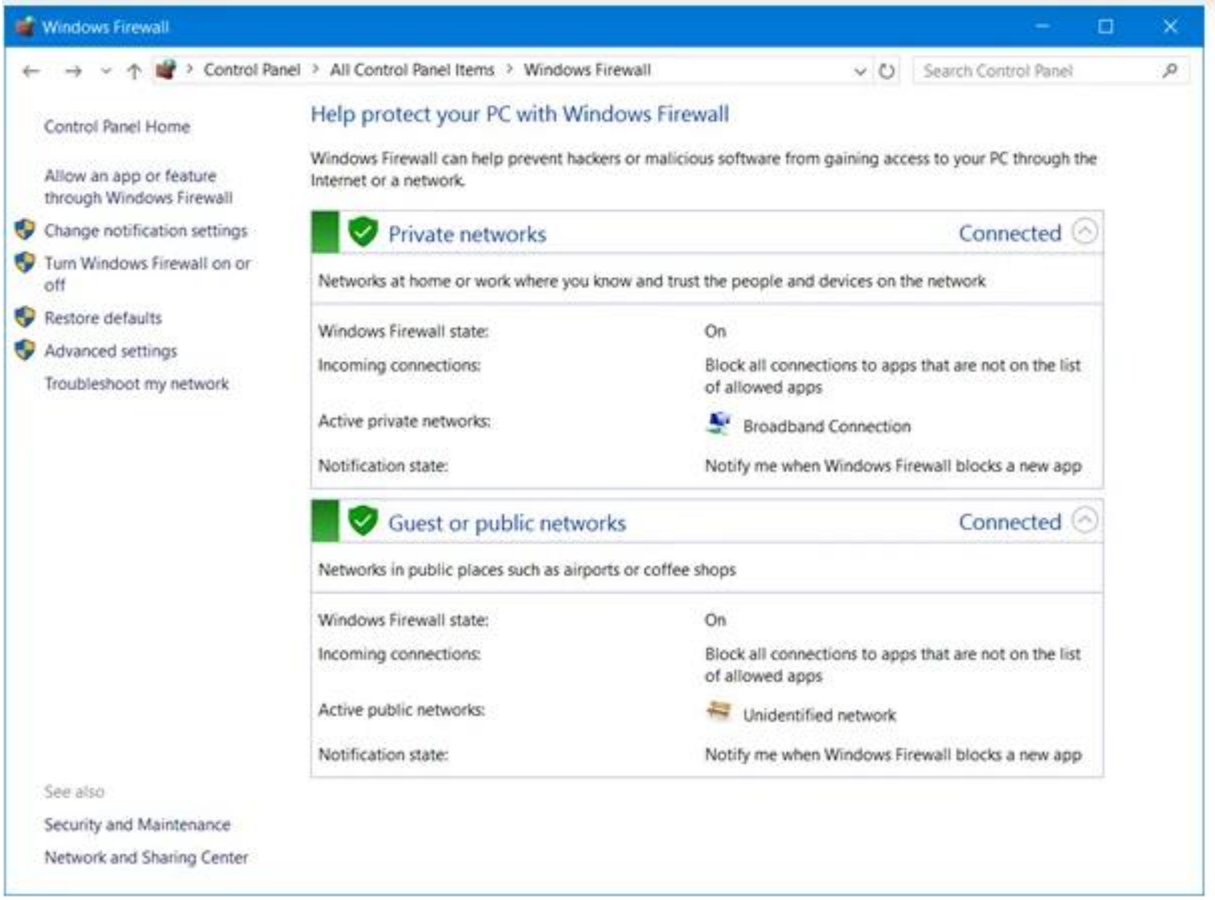
A firewall is a software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on your firewall settings. A firewall can help prevent hackers or malicious software from gaining access to your Windows computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.

Configure Windows Firewall

You can customize most settings of your Windows Firewall through the left pane of the Firewall applet in Control Panel.


Windows Firewall
Control Panel > All Control Panel Items > Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows 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 Firewall

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

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

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

1. Turn on Windows Firewall

This setting is selected by default. When Windows Firewall is On, most programs are blocked from communicating through the firewall. Clicking on the **Turn**

Firewall On or Off will let you enable or disable the Windows Firewall on your computer.

2. Block all incoming firewall connections, including those in the list of allowed programs

This setting blocks all unsolicited attempts to connect to your computer. Use this setting when you need maximum protection for your computer, such as when you connect to a public network in a hotel or airport, or when a computer worm is spreading over the Internet. With this setting, you are not notified when Windows Firewall blocks programs, and programs in the list of allowed programs are ignored. When you block all incoming connections, you can still view most web pages, send and receive an e-mail, and send and receive instant messages.

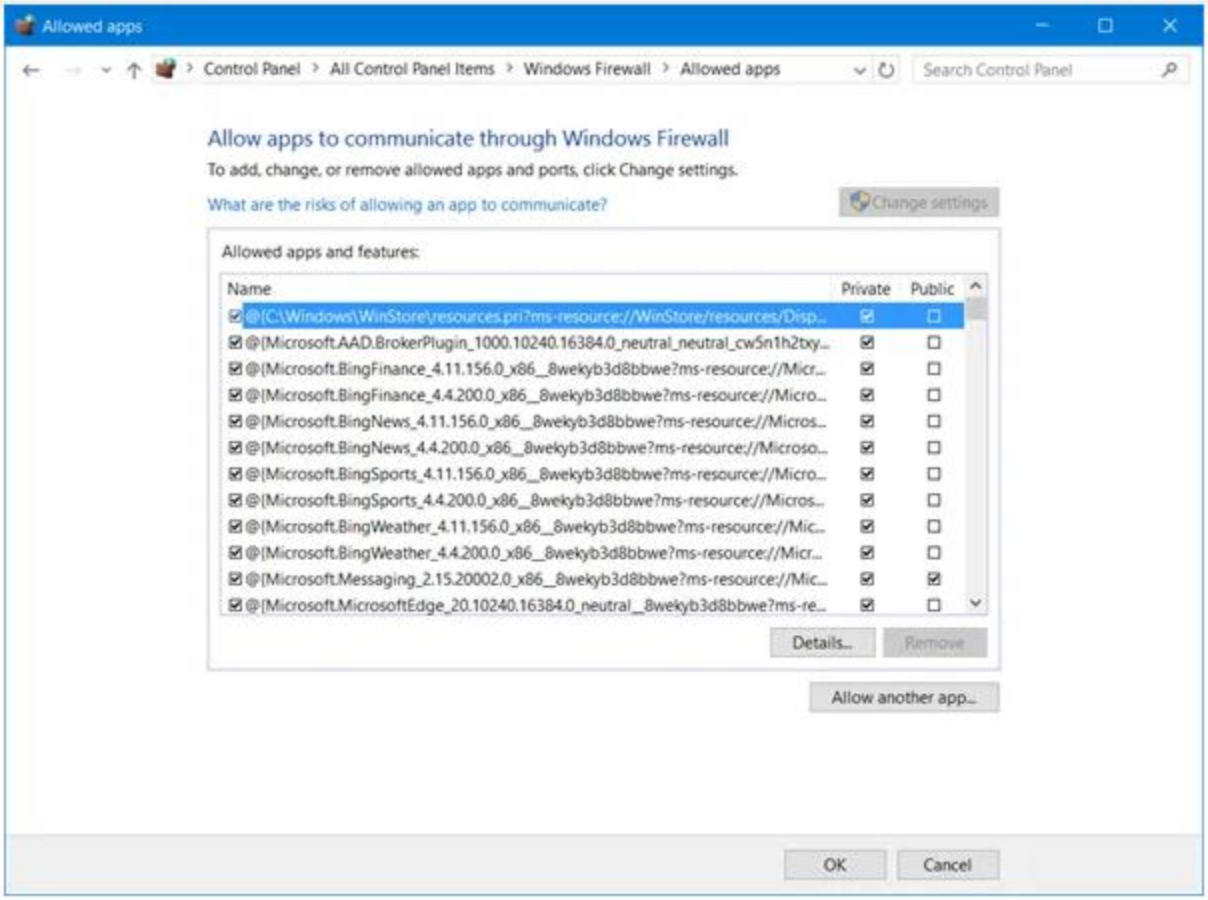
3. Turn off Windows Firewall

Avoid using this setting unless you have another firewall running on your computer. Turning off Windows Firewall might make your computer more vulnerable to damage from hackers and malicious software. Clicking on the **Turn Firewall On or Off** will let you enable or disable the Windows Firewall on your computer.

4. Block or Allow Programs through the Windows Firewall

By default, most programs are blocked by Windows Firewall to help make your computer more secure. To work properly, some programs might require you to allow them to communicate through the firewall. Here's how to do that:

Click **Allow an app or feature through Windows Firewall**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

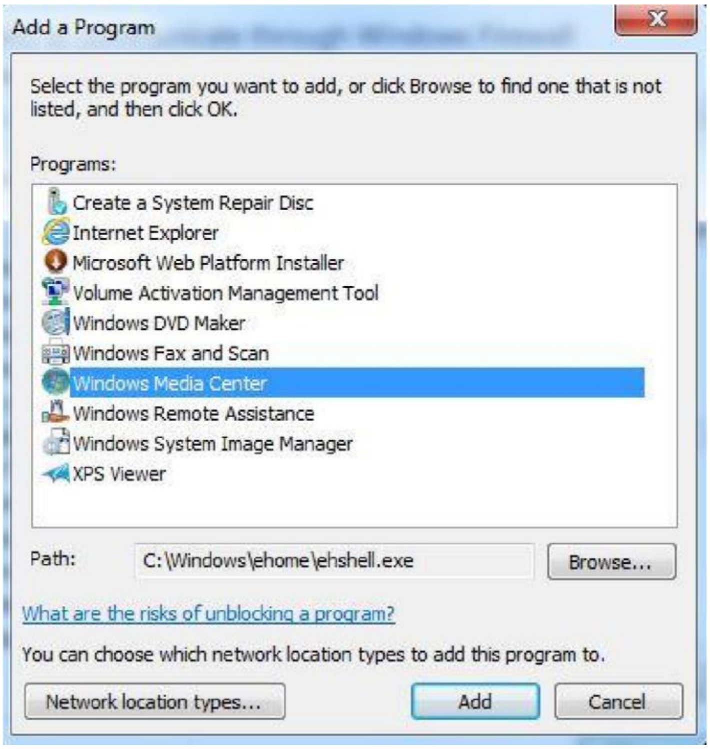
Allowed apps and features:

Name	Private	Public
☑ @{C:\Windows\WinStore\resources.pri?ms-resource://WinStore/resources/Disp...	☑	☐
☑ @{Microsoft.AAD.BrokerPlugin_1000.10240.16384.0_neutral_neutral_cw5n1h2txy...	☑	☐
☑ @{Microsoft.BingFinance_4.11.156.0_x86__8wekyb3d8bbwe?ms-resource://Micr...	☑	☐
☑ @{Microsoft.BingFinance_4.4.200.0_x86__8wekyb3d8bbwe?ms-resource://Micro...	☑	☐
☑ @{Microsoft.BingNews_4.11.156.0_x86__8wekyb3d8bbwe?ms-resource://Micros...	☑	☐
☑ @{Microsoft.BingNews_4.4.200.0_x86__8wekyb3d8bbwe?ms-resource://Microso...	☑	☐
☑ @{Microsoft.BingSports_4.11.156.0_x86__8wekyb3d8bbwe?ms-resource://Micro...	☑	☐
☑ @{Microsoft.BingSports_4.4.200.0_x86__8wekyb3d8bbwe?ms-resource://Micros...	☑	☐
☑ @{Microsoft.BingWeather_4.11.156.0_x86__8wekyb3d8bbwe?ms-resource://Mic...	☑	☐
☑ @{Microsoft.BingWeather_4.4.200.0_x86__8wekyb3d8bbwe?ms-resource://Micr...	☑	☐
☑ @{Microsoft.Messaging_2.15.20002.0_x86__8wekyb3d8bbwe?ms-resource://Mic...	☑	☑
☑ @{Microsoft.MicrosoftEdge_20.10240.16384.0_neutral__8wekyb3d8bbwe?ms-re...	☑	☐

Select the check box next to the program you want to allow, select the network location types you want to allow communication on, and then click OK.

If you want to allow a program to communicate through the firewall, you can add it to the list of allowed programs. For example, you might not be able to send photos in an instant message until you add the instant messaging program to the list of allowed programs. To add or remove a program to the list, click on the **Allow an app or feature through Windows Firewall** link to open the following panel, where you will be able to get more details about allowed programs and allow another app to communicate through the firewall.

We can also add program to this list by clicking **allow another app** button.



Add a Program

Select the program you want to add, or click Browse to find one that is not listed, and then click OK.

Programs:

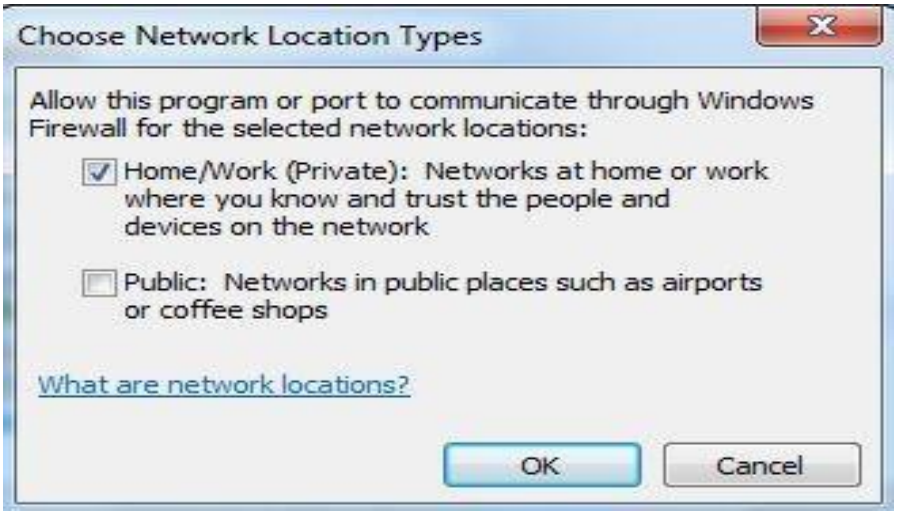
- Create a System Repair Disc
- Internet Explorer
- Microsoft Web Platform Installer
- Volume Activation Management Tool
- Windows DVD Maker
- Windows Fax and Scan
- Windows Media Center
- Windows Remote Assistance
- Windows System Image Manager
- XPS Viewer

Path: C:\Windows\ehome\ehshell.exe

What are the risks of unblocking a program?

You can choose which network location types to add this program to.

Here we have to browse to the executable of our program and then click the Add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button.



Choose Network Location Types

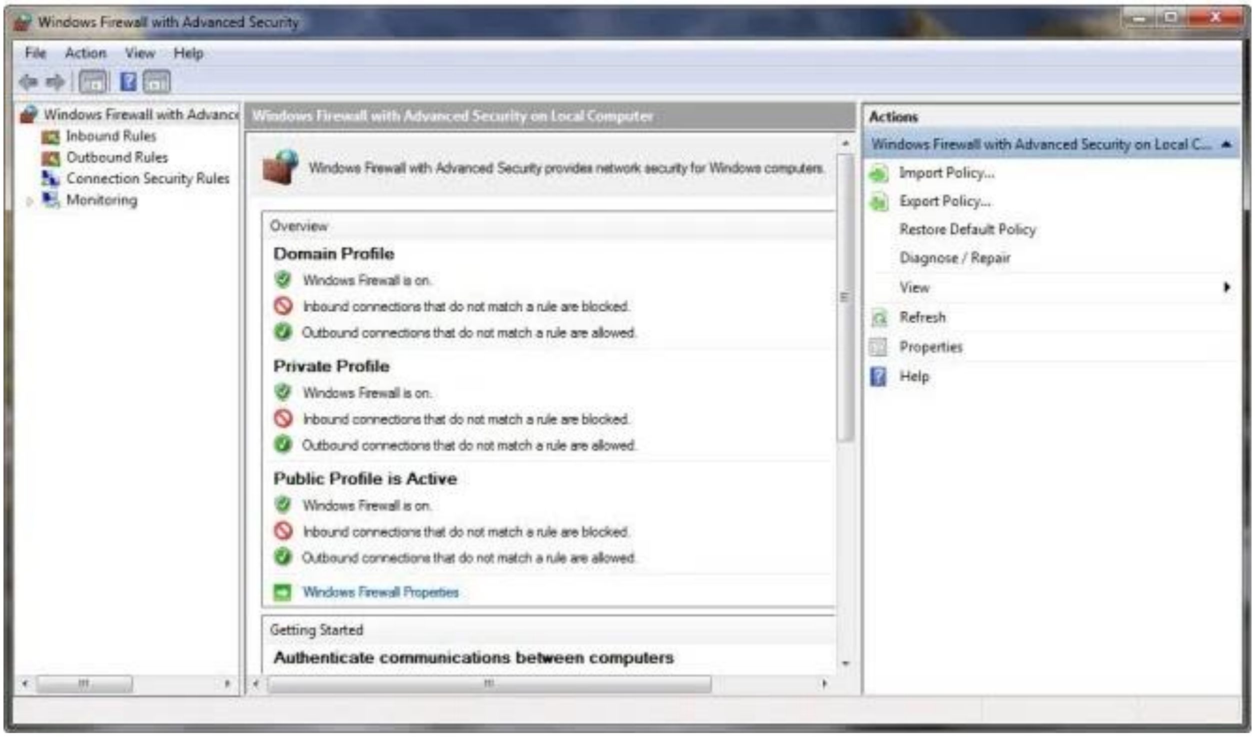
Allow this program or port to communicate through Windows Firewall for the selected network locations:

☑ Home/Work (Private): Networks at home or work where you know and trust the people and devices on the network

☐ Public: Networks in public places such as airports or coffee shops

What are network locations?

Click to open Windows Firewall. In the left pane, click **Advanced settings**.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Actions
Windows Firewall with Advanced Security on Local C...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

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

Overview

Domain Profile

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

Windows Firewall Properties

Getting Started

Authenticate communications between computers

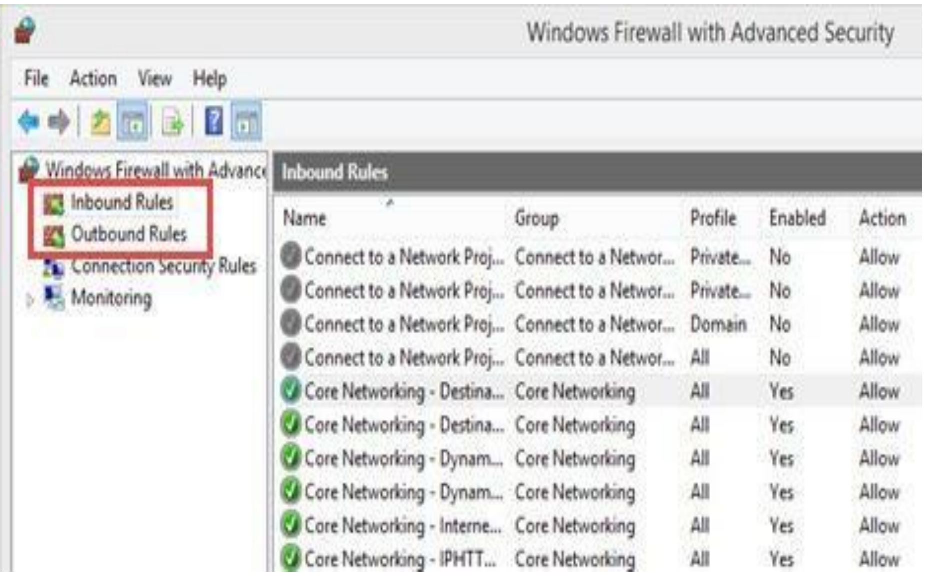
What Are The Inbound & Outbound Rules?

In order to provide the security you need, the Windows Firewall has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are connected to.

Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computer to the network or the Internet.

These rules can be configured so that they are specific to: computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to.

In the Windows Firewall with Advanced Security, you can access all rules and edit their properties. All you have to do is click or tap the appropriate unit in the left-side panel.

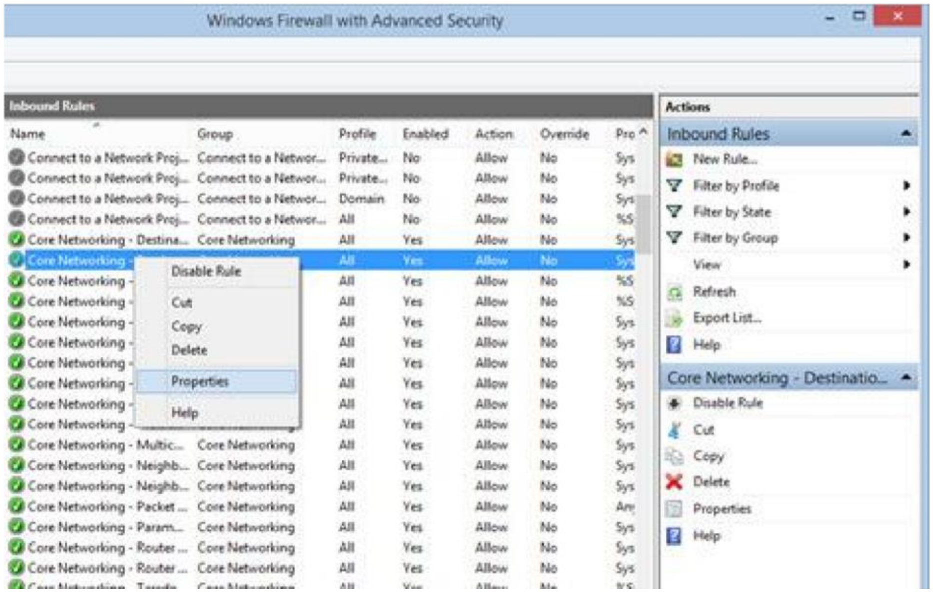


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Group	Profile	Enabled	Action
● Connect to a Network Proj...	Connect to a Networ...	Private...	No	Allow
● Connect to a Network Proj...	Connect to a Networ...	Private...	No	Allow
● Connect to a Network Proj...	Connect to a Networ...	Domain	No	Allow
● Connect to a Network Proj...	Connect to a Networ...	All	No	Allow
✓ Core Networking - Destina...	Core Networking	All	Yes	Allow
✓ Core Networking - Destina...	Core Networking	All	Yes	Allow
✓ Core Networking - Dynam...	Core Networking	All	Yes	Allow
✓ Core Networking - Dynam...	Core Networking	All	Yes	Allow
✓ Core Networking - Interne...	Core Networking	All	Yes	Allow
✓ Core Networking - IPHTT...	Core Networking	All	Yes	Allow

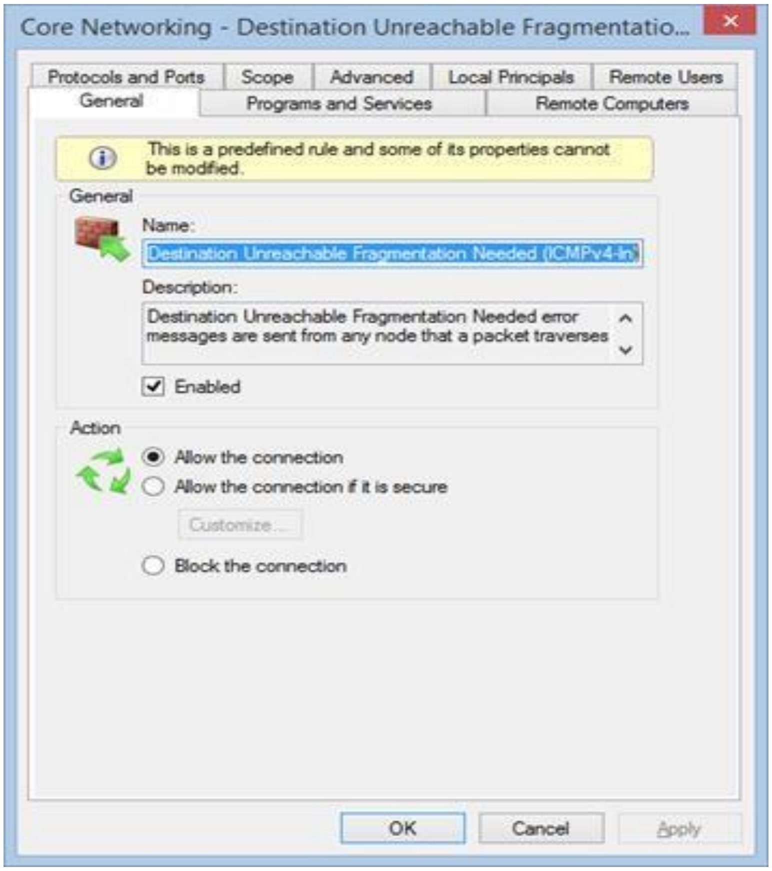
The rules used by the Windows Firewall can be enabled or disabled. The ones which are enabled or active are marked with a green check-box in the Name column. The ones that are disabled are marked with a gray check-box.

If you want to know more about a specific rule and learn its properties, right click on it and select Properties or select it and press Properties in the column on right, which lists the actions that are available for your selection.



Name	Group	Profile	Enabled	Action	Override	Pro
● Connect to a Network Proj...	Connect to a Networ...	Private...	No	Allow	No	Sys
● Connect to a Network Proj...	Connect to a Networ...	Private...	No	Allow	No	Sys
● Connect to a Network Proj...	Connect to a Networ...	Domain	No	Allow	No	Sys
● Connect to a Network Proj...	Connect to a Networ...	All	No	Allow	No	%S
✓ Core Networking - Destina...	Core Networking	All	Yes	Allow	No	Sys
✓ Core Networking -		All	Yes	Allow	No	Sys
✓ Core Networking -		All	Yes	Allow	No	%S
✓ Core Networking -		All	Yes	Allow	No	%S
✓ Core Networking -		All	Yes	Allow	No	Sys
✓ Core Networking -		All	Yes	Allow	No	Sys
✓ Core Networking -		All	Yes	Allow	No	Sys
✓ Core Networking -		All	Yes	Allow	No	Sys
✓ Core Networking -		All	Yes	Allow	No	Sys
✓ Core Networking -		All	Yes	Allow	No	Sys
✓ Core Networking - Multic...	Core Networking	All	Yes	Allow	No	Sys
✓ Core Networking - Neighb...	Core Networking	All	Yes	Allow	No	Sys
✓ Core Networking - Neighb...	Core Networking	All	Yes	Allow	No	Sys
✓ Core Networking - Packet ...	Core Networking	All	Yes	Allow	No	Any
✓ Core Networking - Param...	Core Networking	All	Yes	Allow	No	Sys
✓ Core Networking - Router ...	Core Networking	All	Yes	Allow	No	Sys
✓ Core Networking - Router ...	Core Networking	All	Yes	Allow	No	Sys

In the Properties window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.



Core Networking - Destination Unreachable Fragmentatio...

This is a predefined rule and some of its properties cannot be modified.

General

Name: Destination Unreachable Fragmentation Needed (ICMPv4-In)

Description: Destination Unreachable Fragmentation Needed error messages are sent from any node that a packet traverses

☑ Enabled

Action

● Allow the connection

○ Allow the connection if it is secure

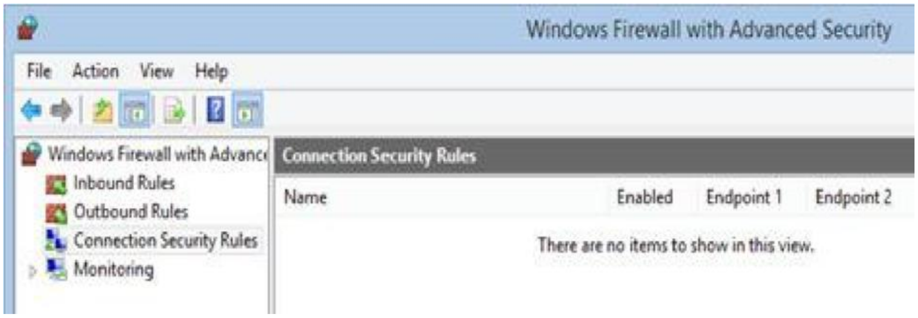
○ Block the connection

What Are The Connection Security Rules?

Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted.

Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.

If you want to see if there are any such rules on your computer, click or tap "Connection Security Rules" on the panel on the left. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator.

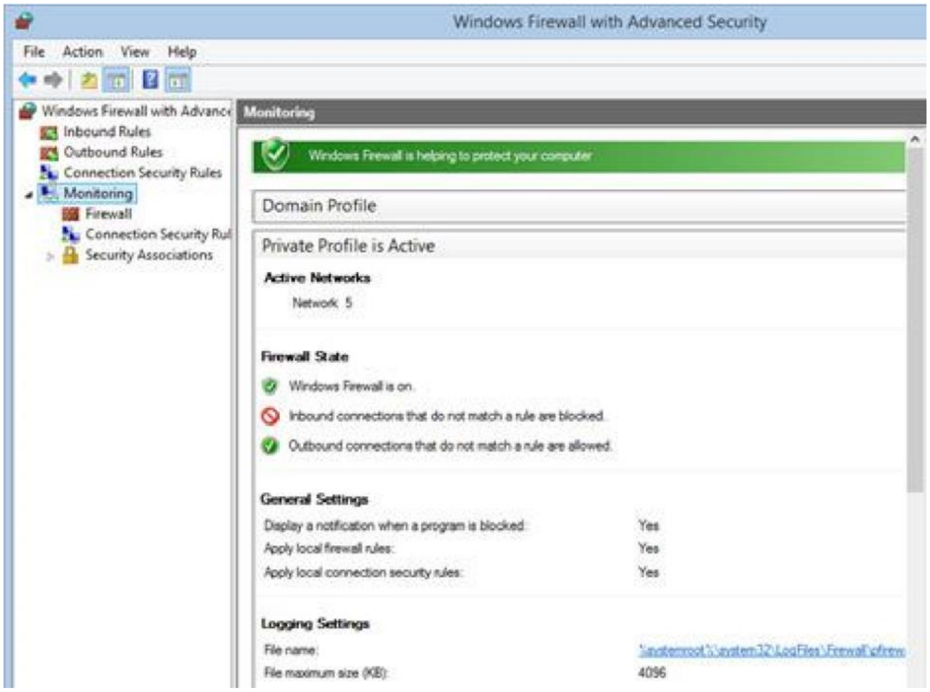

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Connection Security Rules

Name	Enabled	Endpoint 1	Endpoint 2

There are no items to show in this view.

2.1.3.4 What Does the Windows Firewall with Advanced Security Monitor?

The Windows Firewall with Advanced Security includes some monitoring features as well. In the Monitoring section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.



Windows Firewall is helping to protect your computer

Domain Profile

Private Profile is Active

Active Networks

Network 5

Firewall State

✓ Windows Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

General Settings

Display a notification when a program is blocked:	Yes
Apply local firewall rules:	Yes
Apply local connection security rules:	Yes

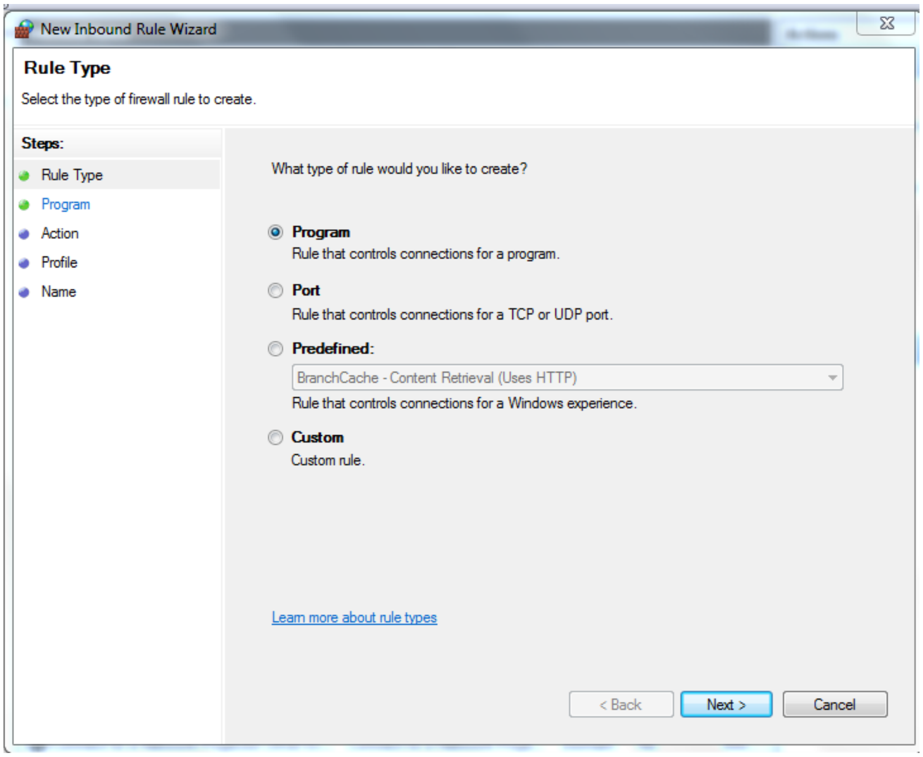
Logging Settings

File name:	%systemroot%\system32\LogFiles\Firewall\pfirew
File maximum size (KB):	4096

You should note that the Monitoring section shows only the active rules for the current network location.

Create inbound rule: rules for incoming traffic

1. Block ICMP – block ping command
   Create inbound rule in one system. Select program and click next.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

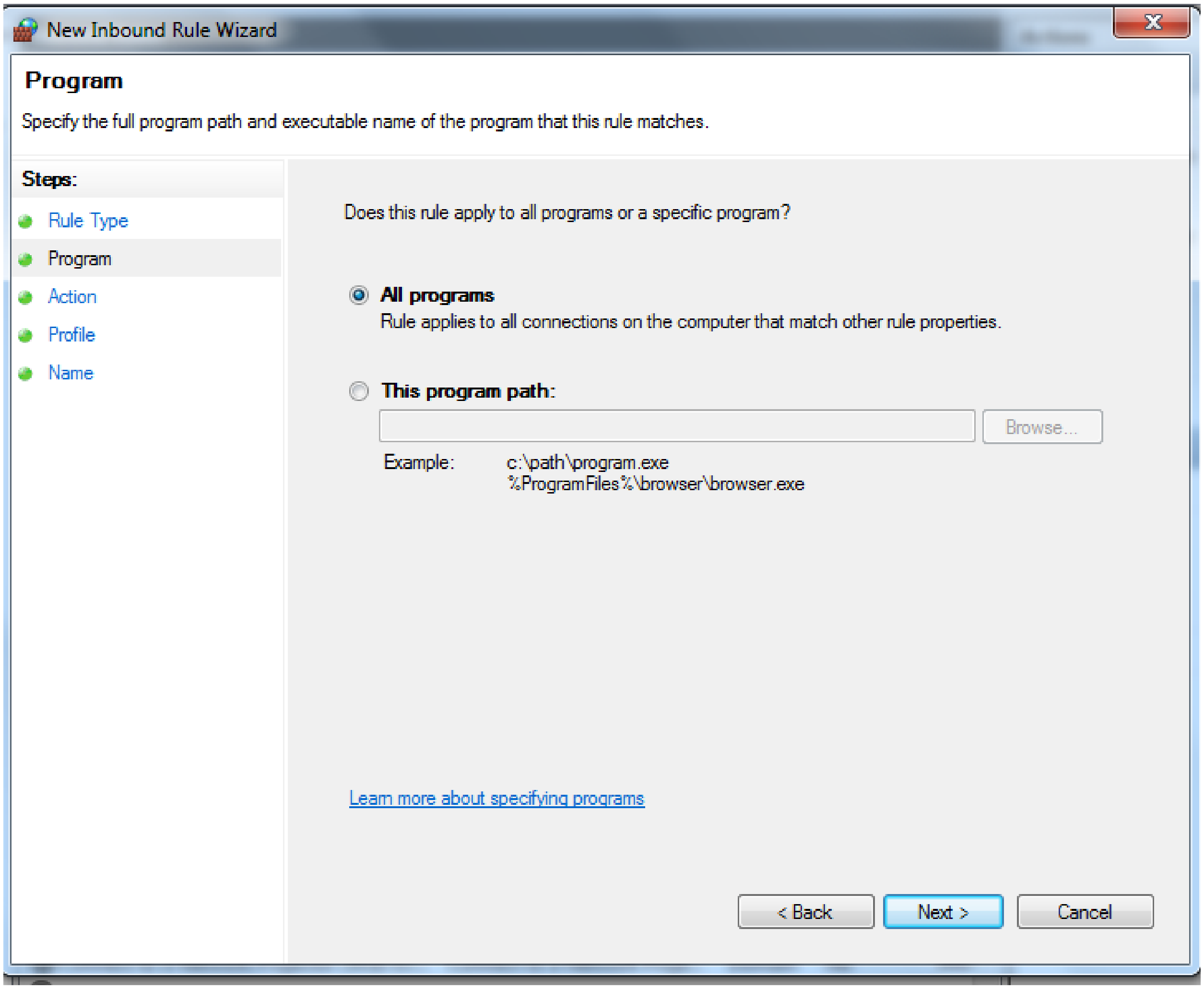
● **Program**
Rule that controls connections for a program.

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

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

2. Now select all program and click next



New Inbound Rule Wizard

Program

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

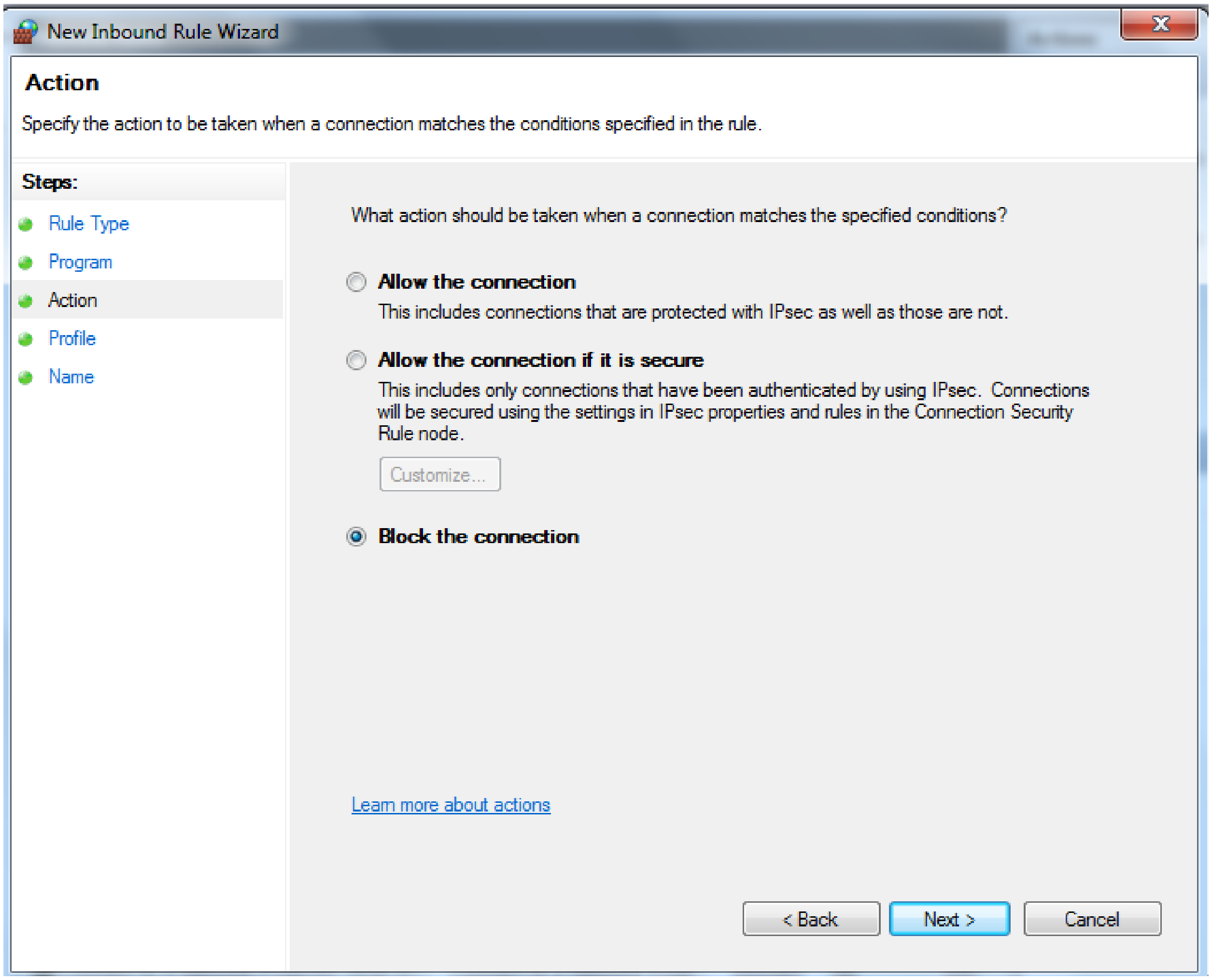
Does this rule apply to all programs or a specific program?

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

○ **This program path:**

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

3. Now select block connection and click next



New Inbound Rule Wizard

Action

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

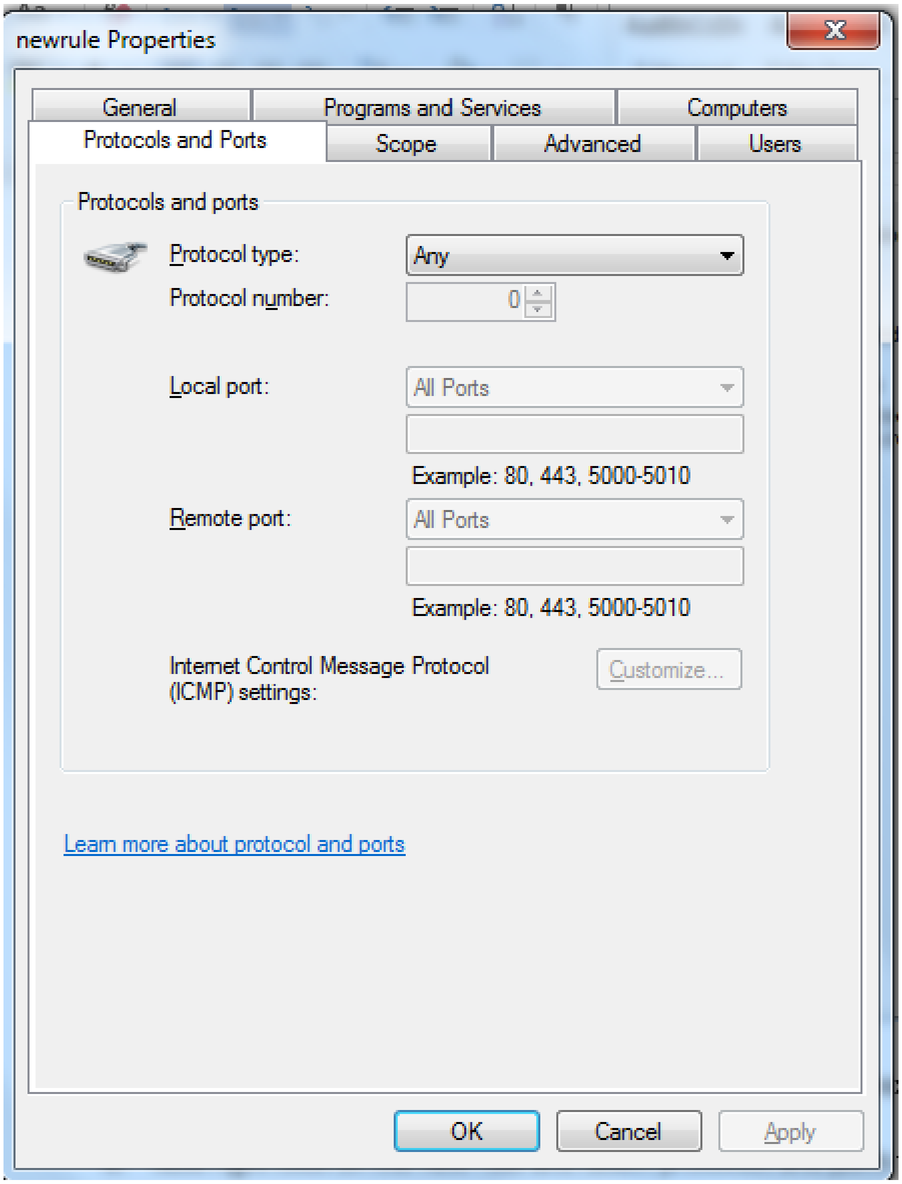
What action should be taken when a connection matches the specified conditions?

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

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

● **Block the connection**

4. Now select all domain, private and public network and click next.
5. Set the name of the rule and click finish.
6. Now right click on the new rule and select protocols and ports tab.


newrule Properties

Protocols and ports

Protocol type: Any

Protocol number: 0

Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: All Ports

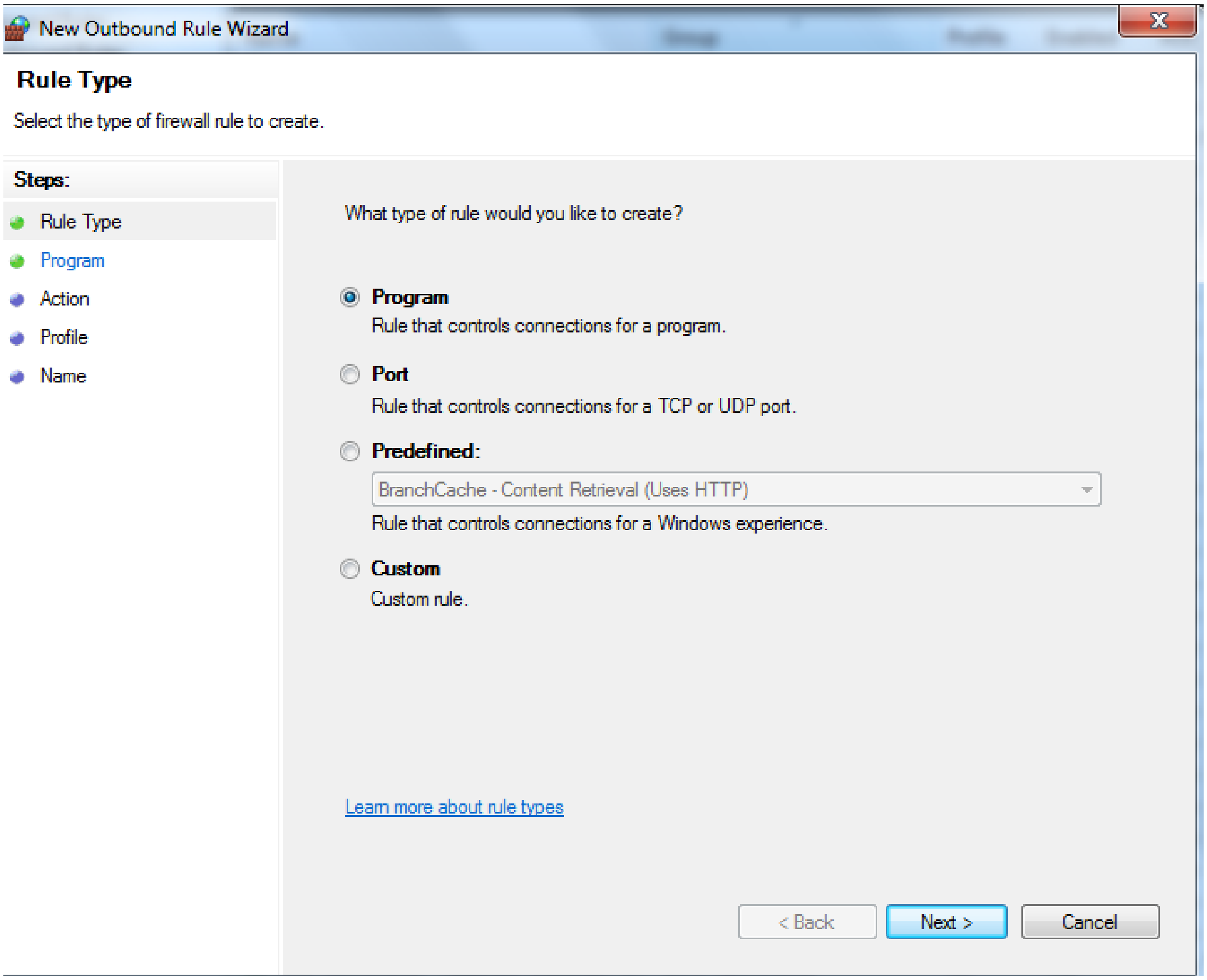
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

7. Select protocol type ICMP4, apply and click ok.
8. Now for checking send ping to this computer from another computer.
9. It will show request time out.

Create outbound rule: stop users from using internet

1. Create new outbound rule, select program and click next.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

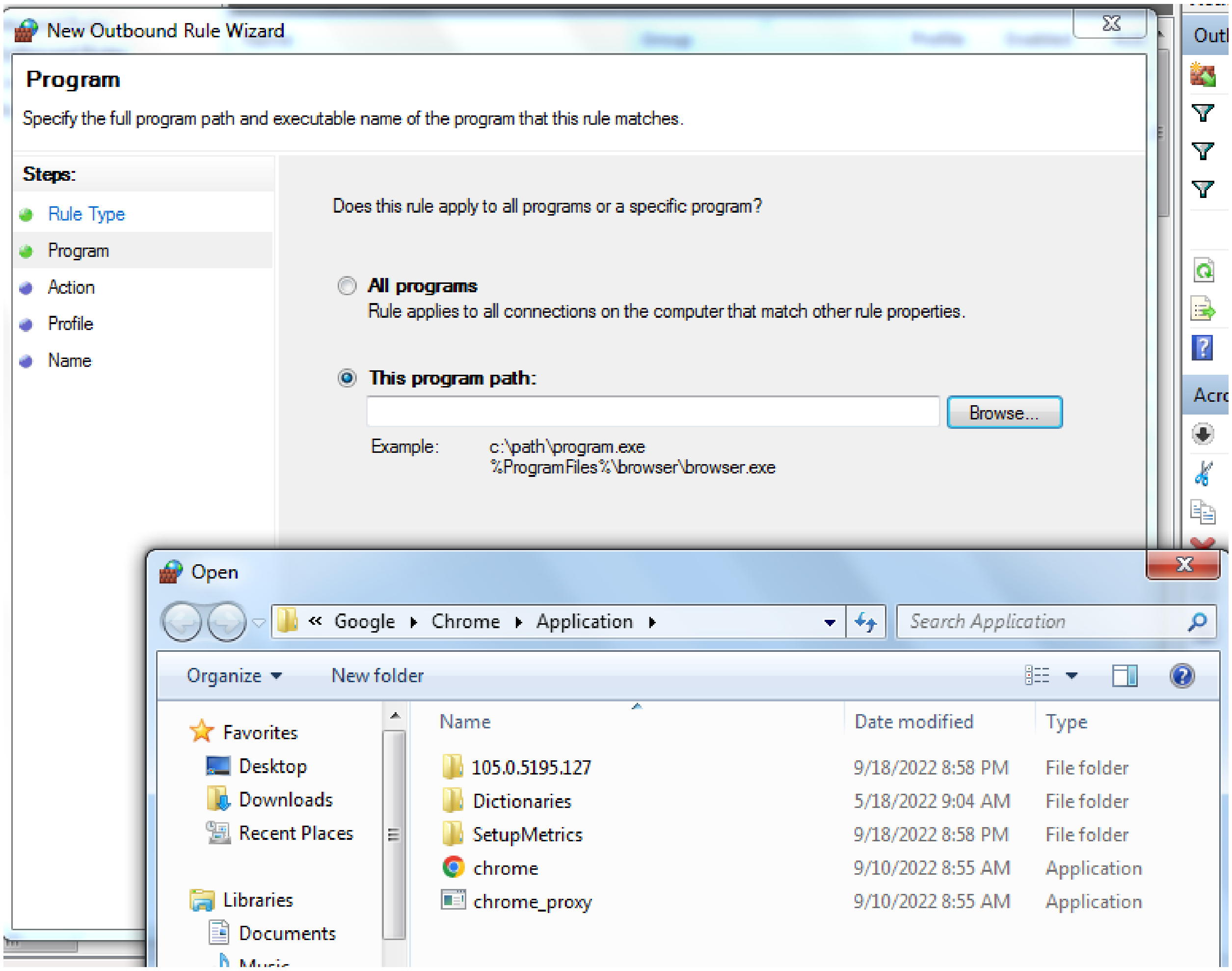
● **Program**
Rule that controls connections for a program.

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

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

2. Now here select program path and select .exe file of chrome and click next.



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:**

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

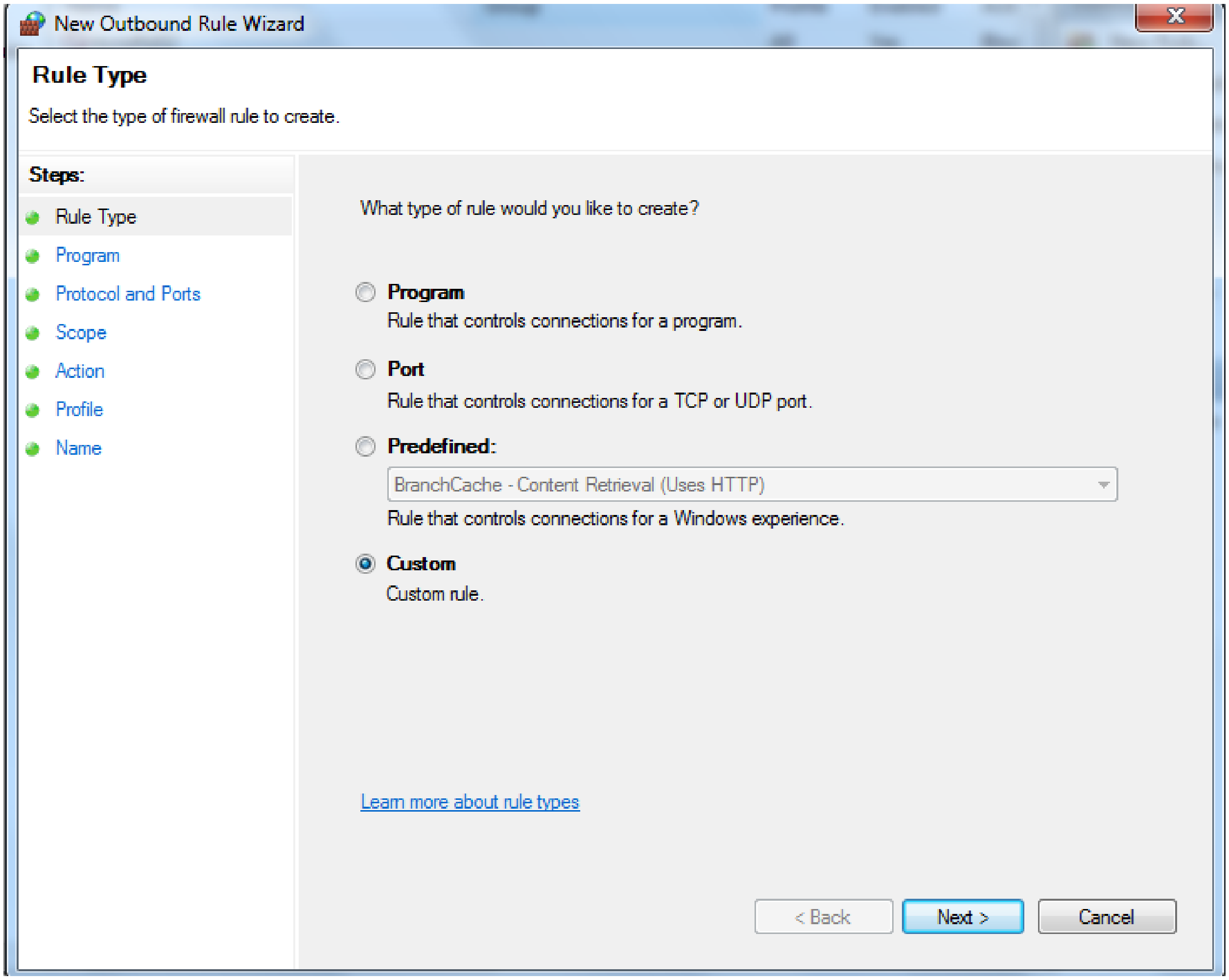
Name	Date modified	Type
105.0.5195.127	9/18/2022 8:58 PM	File folder
Dictionaries	5/18/2022 9:04 AM	File folder
SetupMetrics	9/18/2022 8:58 PM	File folder
chrome	9/10/2022 8:55 AM	Application
chrome_proxy	9/10/2022 8:55 AM	Application

3. Now in next screen select block connection.
4. Then in next screen select domain, private and public network.
5. Then set name of rule and click finish.
6. Now open chrome and search any website.
7. Internet will work due to this new outbound rule.

3. **Block particular domain or website**

1. Create new outbound rule

2. select custom rule, click next.



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:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

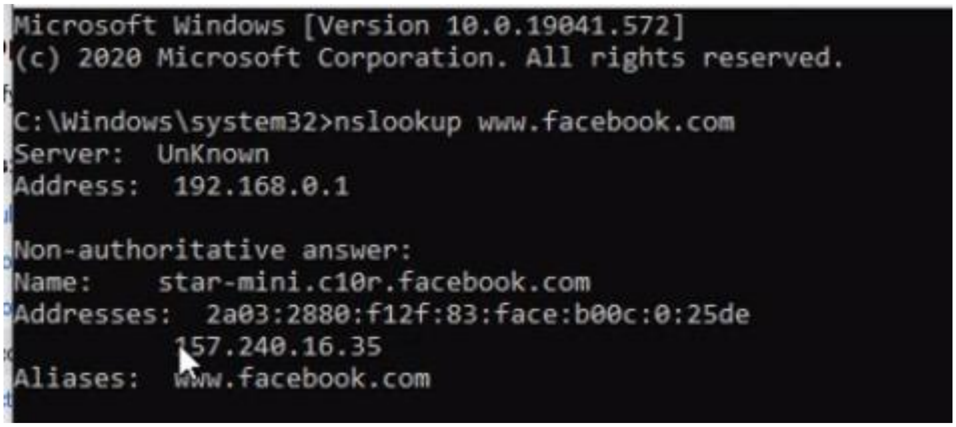
● **Custom**
Custom rule.

3. select all programs click next.

4. select protocol any click next.

5. enter remote ip address

For that open command prompt and type nslookup www.facebook.con



```
Microsoft Windows [Version 10.0.19041.572]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup www.facebook.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f12f:83:face:b00c:0:25de
          157.240.16.35
Aliases:  www.facebook.com
```

6. enter both addresses and click next

7. select all network and click next

8. enter rule name and click finish.

9. now try to open www.facebook.com into browser it will not opened.