Practical Malicious codes

Third class CY 2023

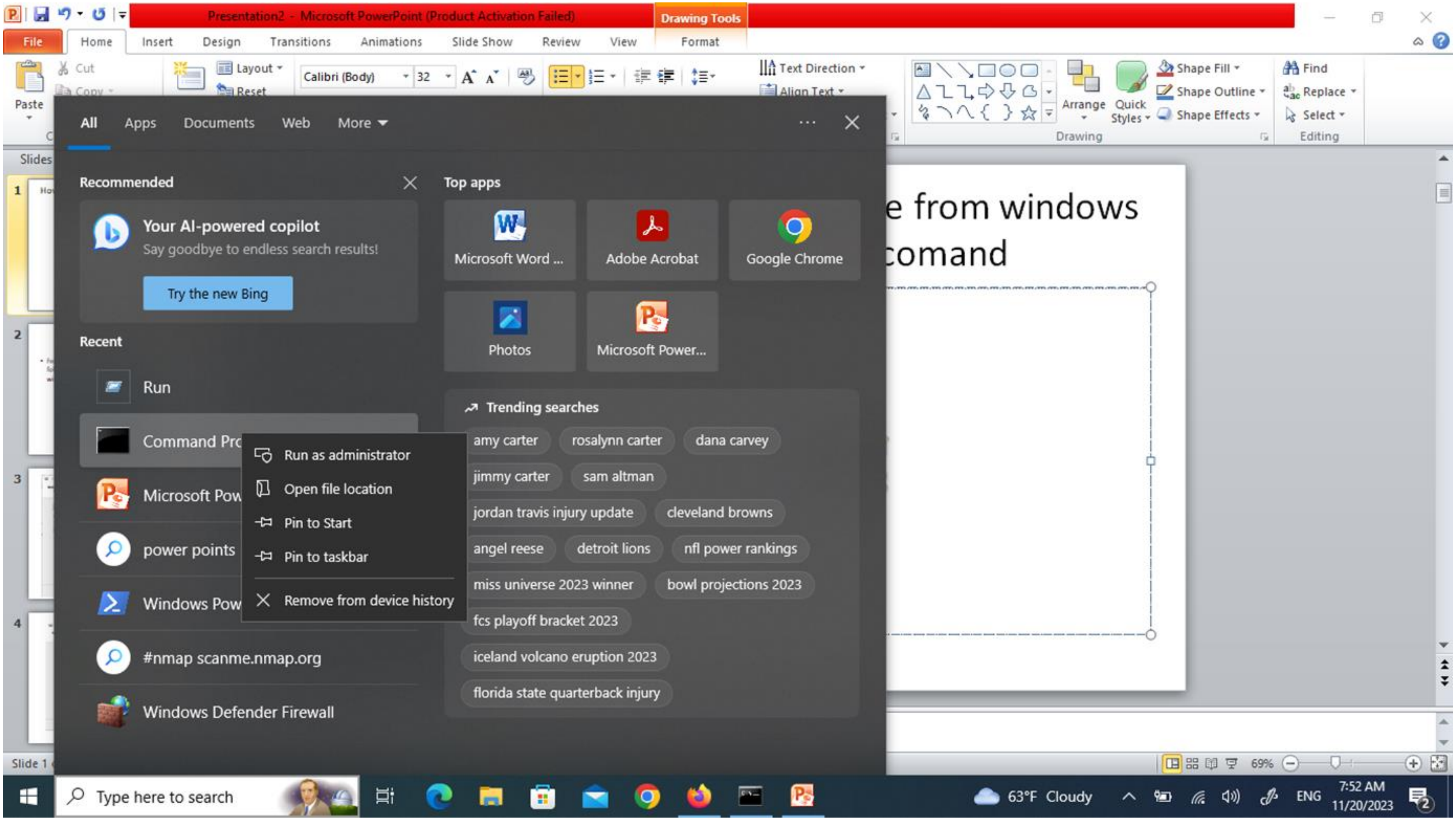
p2

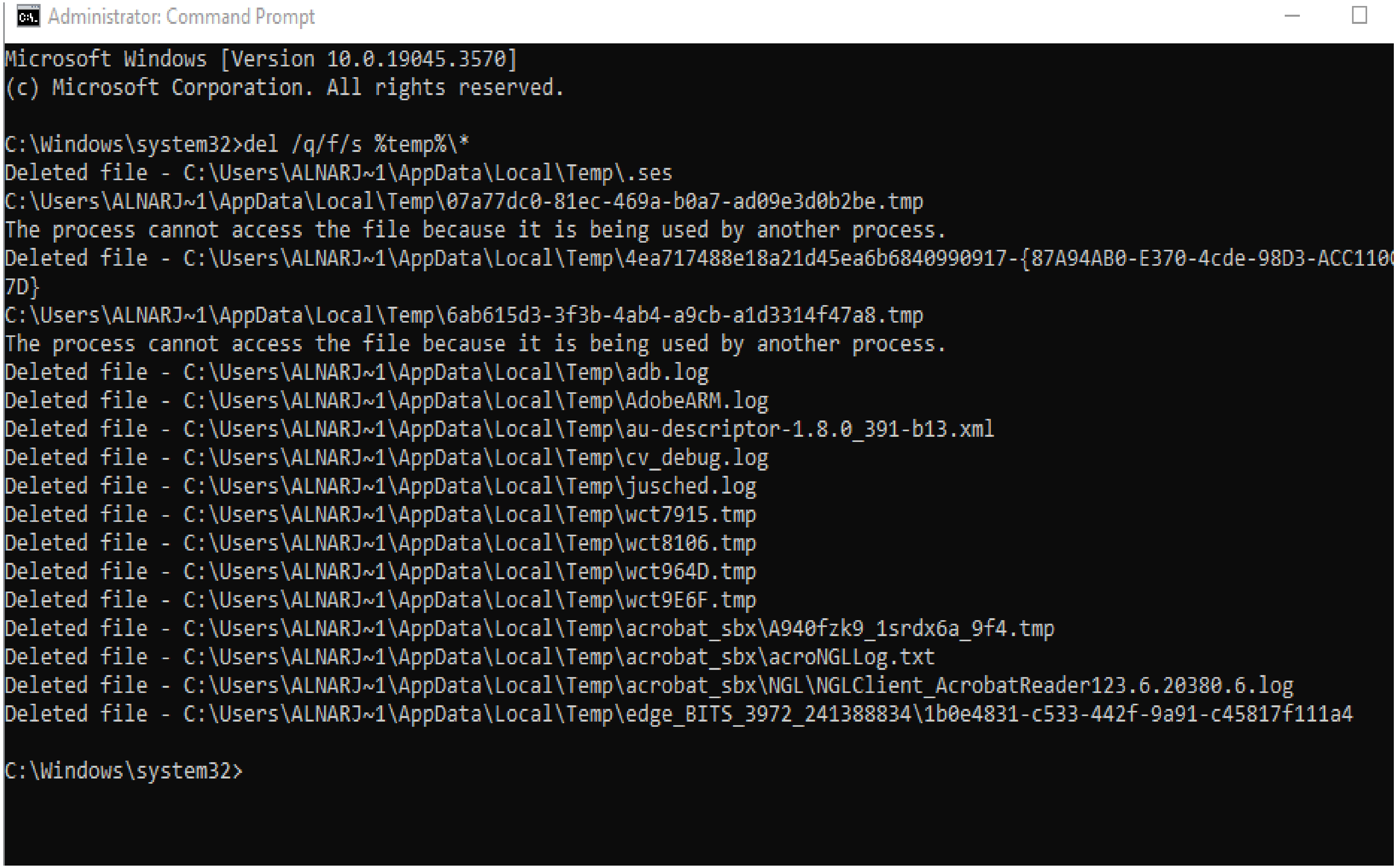
A.P

Mohanad Ali meteab

How to delete temp file from windows 10 using cmd comand

- Write in type here to search cmd
- Write click on it choose run as administration
- write this instruction
- delفراغ /q/f/sفراغ %temp%*
- Press inter
- You will see all the file of temp will be delete and any Malicious viurs


Presentation2 - Microsoft PowerPoint (Product Activation Failed)
Drawing Tools
File
Home
Insert
Design
Transitions
Animations
Slide Show
Review
View
Format
Paste
Cut
Copy
Layout
Reset
Calibri (Body)
32
Text Direction
Align Text
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
Slides
All
Apps
Documents
Web
More
Recommended
Your AI-powered copilot
Say goodbye to endless search results!
Try the new Bing
Recent
Run
Command Pro
Microsoft Pow
power points
Windows Pow
#nmap scanme.nmap.org
Windows Defender Firewall
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Remove from device history
Top apps
Microsoft Word ...
Adobe Acrobat
Google Chrome
Photos
Microsoft Power...
Trending searches
amy carter
rosalynn carter
dana carvey
jimmy carter
sam altman
jordan travis injury update
cleveland browns
angel reese
detroit lions
nfl power rankings
miss universe 2023 winner
bowl projections 2023
fcs playoff bracket 2023
iceland volcano eruption 2023
florida state quarterback injury
e from windows
comand
Slide 1
69%
Type here to search
63°F Cloudy
ENG
7:52 AM
11/20/2023



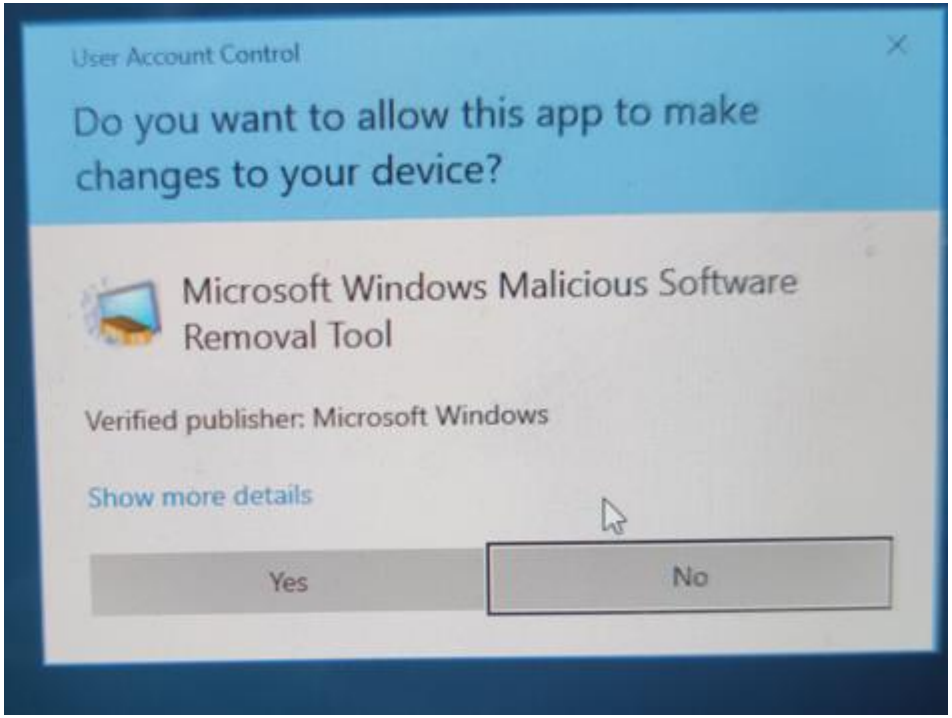
```
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>del /q/f/s %temp%\*
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\.ses
C:\Users\ALNARJ~1\AppData\Local\Temp\07a77dc0-81ec-469a-b0a7-ad09e3d0b2be.tmp
The process cannot access the file because it is being used by another process.
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\4ea717488e18a21d45ea6b6840990917-{87A94AB0-E370-4cde-98D3-ACC110
7D}
C:\Users\ALNARJ~1\AppData\Local\Temp\6ab615d3-3f3b-4ab4-a9cb-a1d3314f47a8.tmp
The process cannot access the file because it is being used by another process.
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\adb.log
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\AdobeARM.log
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\au-descriptor-1.8.0_391-b13.xml
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\cv_debug.log
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\jusched.log
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\wct7915.tmp
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\wct8106.tmp
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\wct964D.tmp
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\wct9E6F.tmp
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\acrobat_sbx\A940fzk9_1srdx6a_9f4.tmp
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\acrobat_sbx\acroNGLLog.txt
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\acrobat_sbx\NGL\NGLClient_AcrobatReader123.6.20380.6.log
Deleted file - C:\Users\ALNARJ~1\AppData\Local\Temp\edge_BITS_3972_241388834\1b0e4831-c533-442f-9a91-c45817f111a4

C:\Windows\system32>
```

Instruct MRT

- From the type here to search field, type the following instruction: MRT and wait then This window will appear

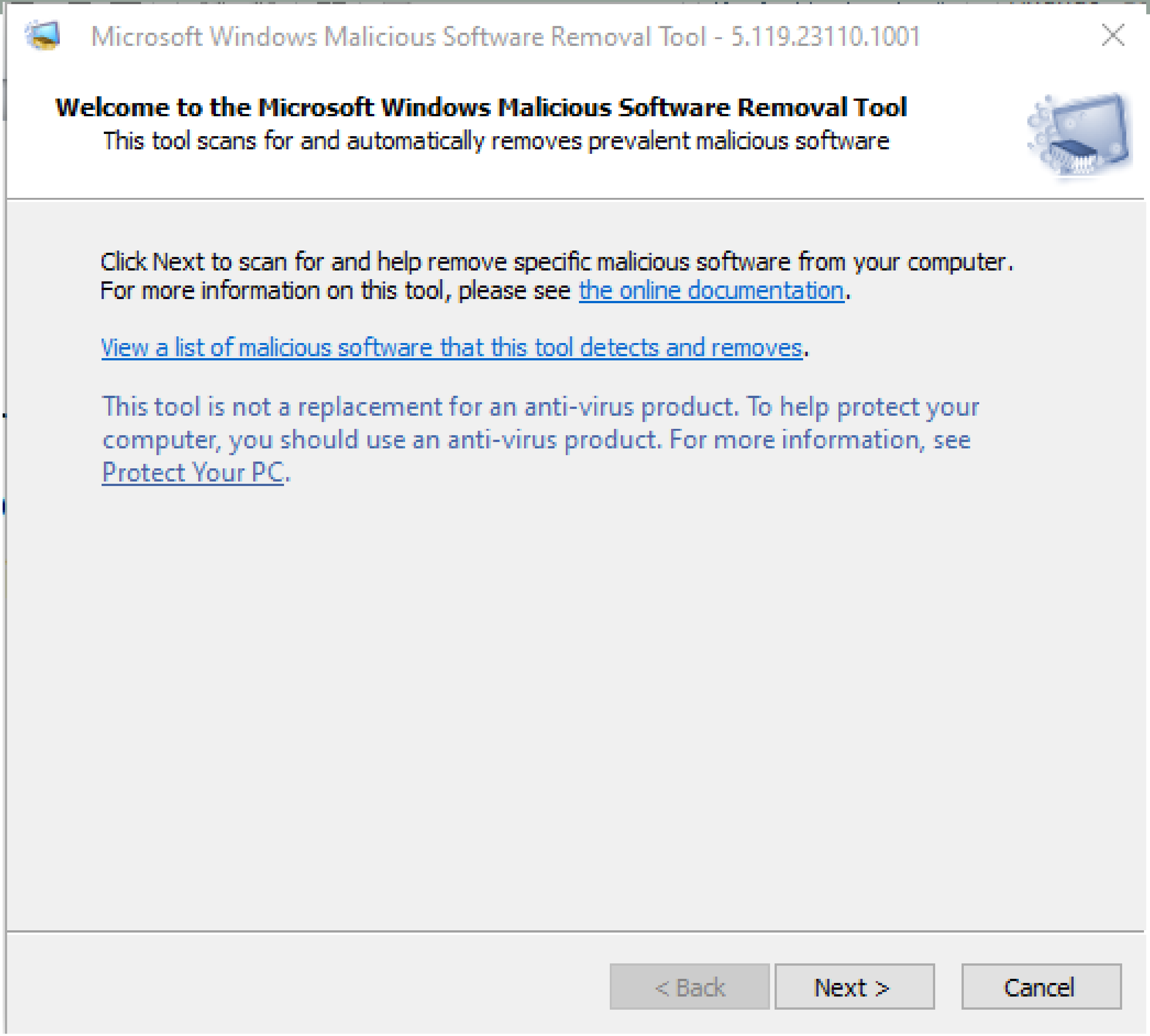


User Account Control

Do you want to allow this app to make changes to your device?

Microsoft Windows Malicious Software Removal Tool

Verified publisher: Microsoft Windows



Microsoft Windows Malicious Software Removal Tool - 5.119.23110.1001

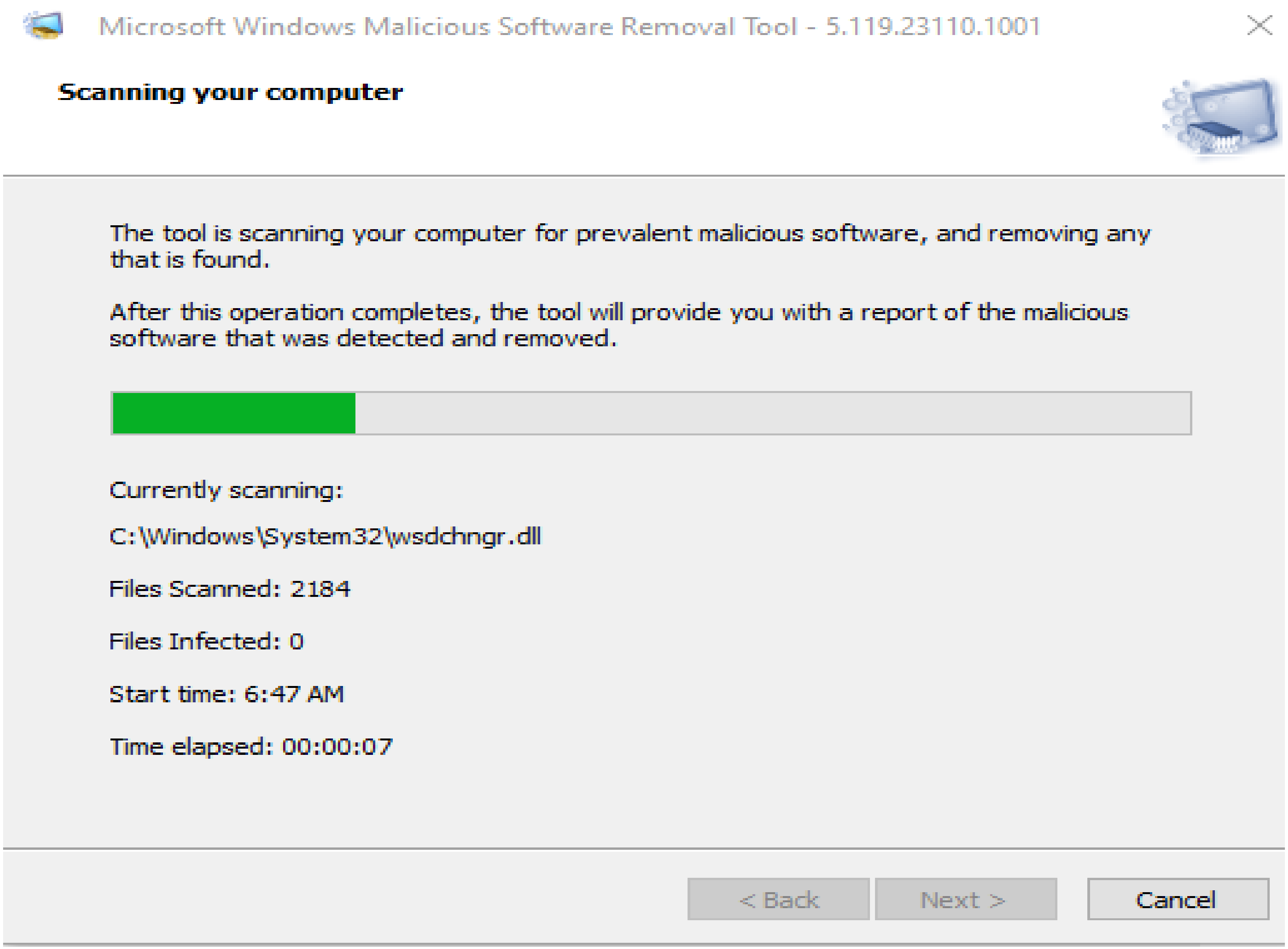
Welcome to the Microsoft Windows Malicious Software Removal Tool

This tool scans for and automatically removes prevalent malicious software

Click Next to scan for and help remove specific malicious software from your computer. For more information on this tool, please see the online documentation.

View a list of malicious software that this tool detects and removes.

This tool is not a replacement for an anti-virus product. To help protect your computer, you should use an anti-virus product. For more information, see Protect Your PC.



Microsoft Windows Malicious Software Removal Tool - 5.119.23110.1001

Scanning your computer

The tool is scanning your computer for prevalent malicious software, and removing any that is found.

After this operation completes, the tool will provide you with a report of the malicious software that was detected and removed.

Currently scanning:

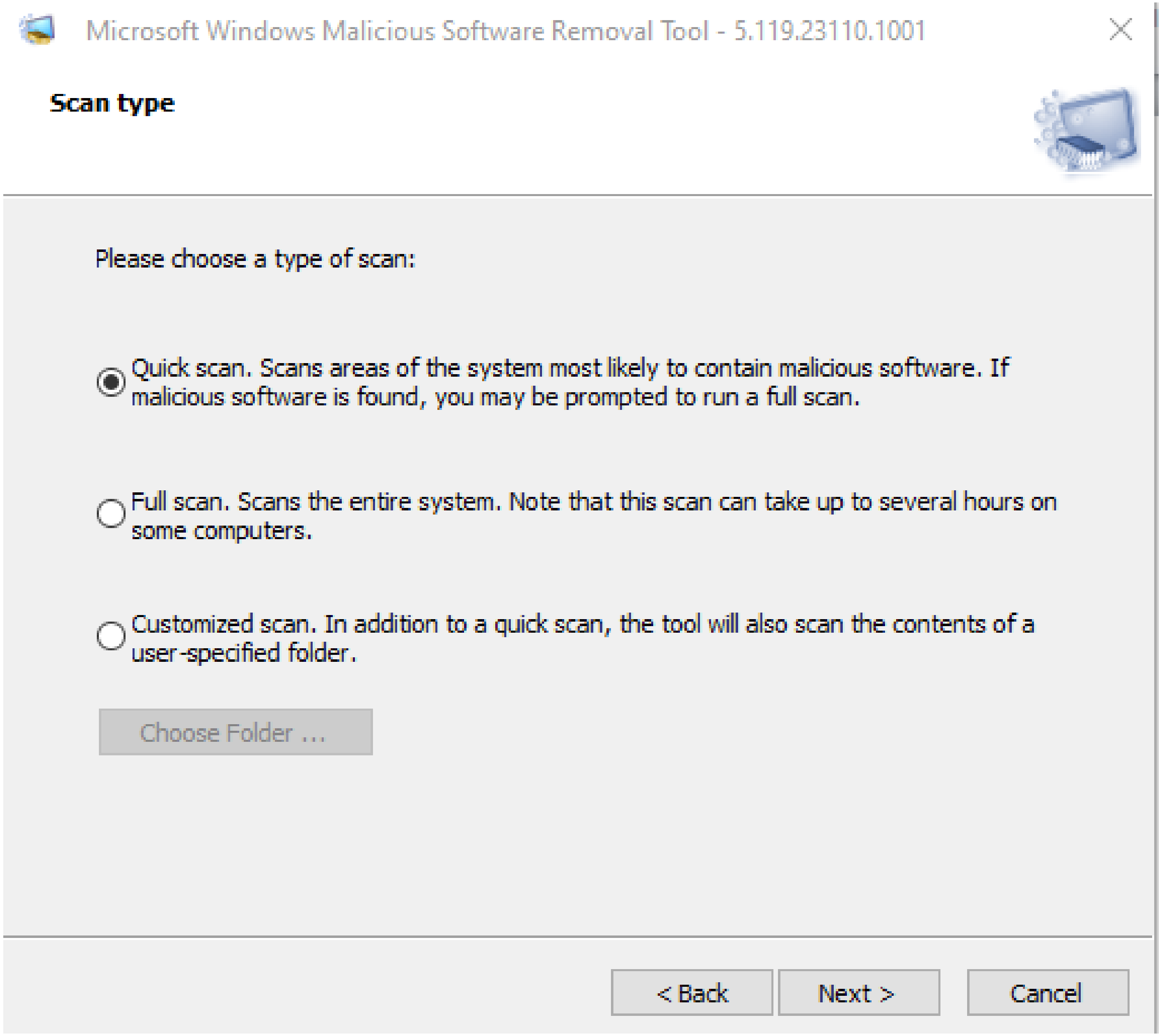
C:\Windows\System32\wsdchngr.dll

Files Scanned: 2184

Files Infected: 0

Start time: 6:47 AM

Time elapsed: 00:00:07



Microsoft Windows Malicious Software Removal Tool - 5.119.23110.1001

Scan type

Please choose a type of scan:

● Quick scan. Scans areas of the system most likely to contain malicious software. If malicious software is found, you may be prompted to run a full scan.

○ Full scan. Scans the entire system. Note that this scan can take up to several hours on some computers.

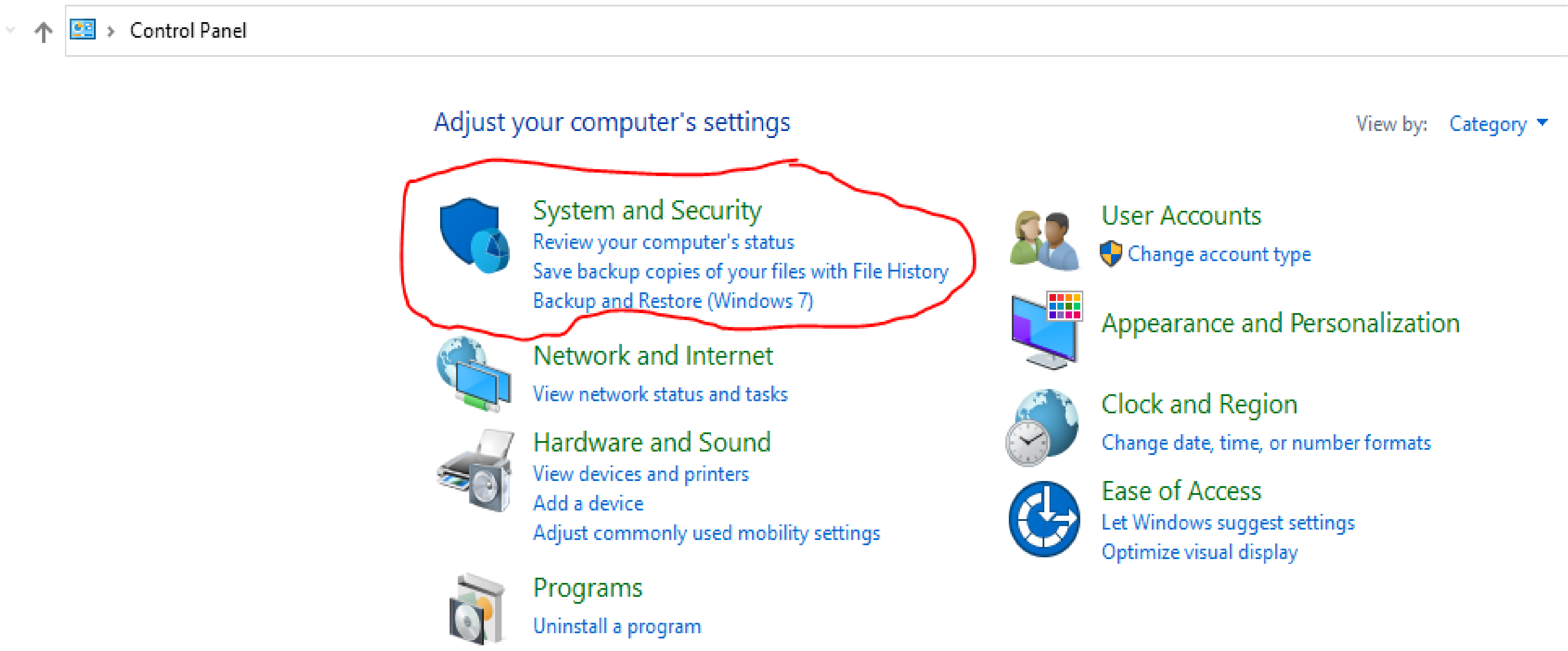
○ Customized scan. In addition to a quick scan, the tool will also scan the contents of a user-specified folder.

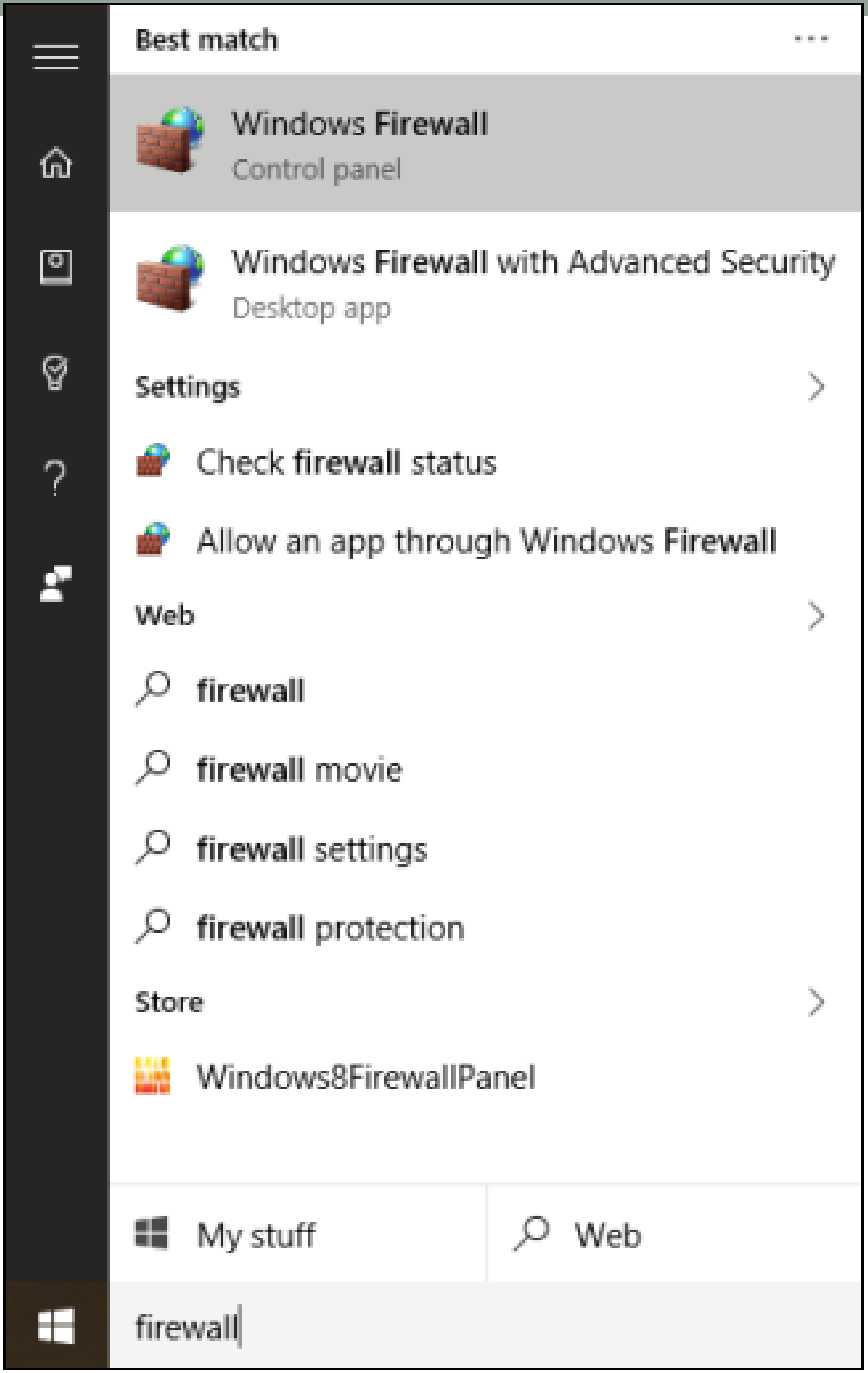
Windows Firewall

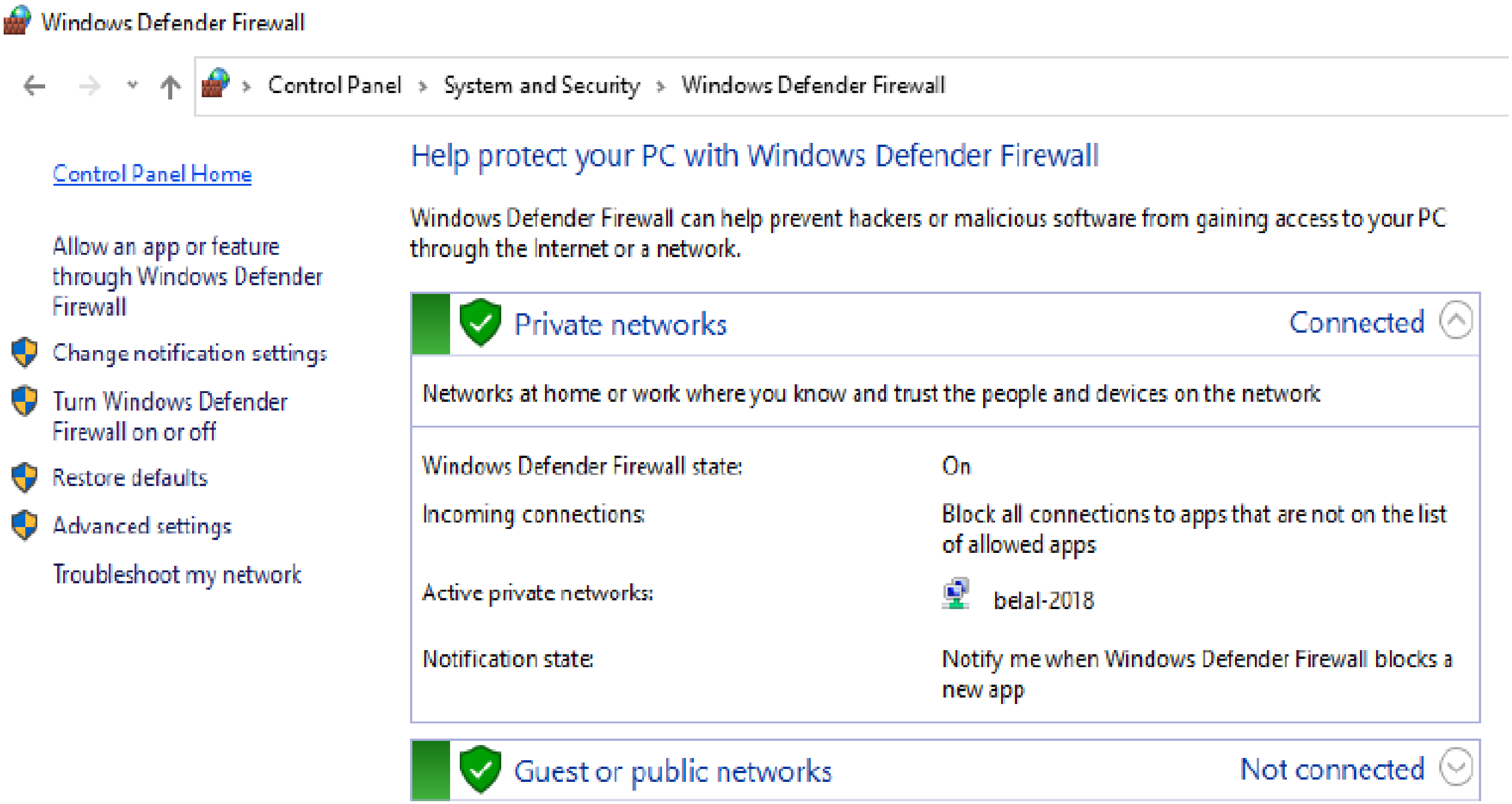
The firewall has not changed much since Windows 10 & Windows 11.

In general, connections to programs are blocked unless they are on the allowed list. Outgoing connections are not blocked if they do not match leaders. You also have a public and private network profile for the firewall and you can control exactly which program can connect to the private network instead of the Internet. Although outgoing connections are not blocked by default, you can configure firewall rules.

Although outgoing connections are not blocked by default, you can configure your own firewall rules in windows. You can either open the Control Panel and open the firewall from there or you can click Start and write firewall.


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
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

Best match
Windows Firewall
Control panel
Windows Firewall with Advanced Security
Desktop app
Settings
Check firewall status
Allow an app through Windows Firewall
Web
firewall
firewall movie
firewall settings
firewall protection
Store
Windows8FirewallPanel
My stuff
Web
firewall



Windows Defender Firewall

← → ˅ ↑ › Control Panel › System and Security › Windows Defender Firewall
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

Help protect your PC with Windows Defender Firewall

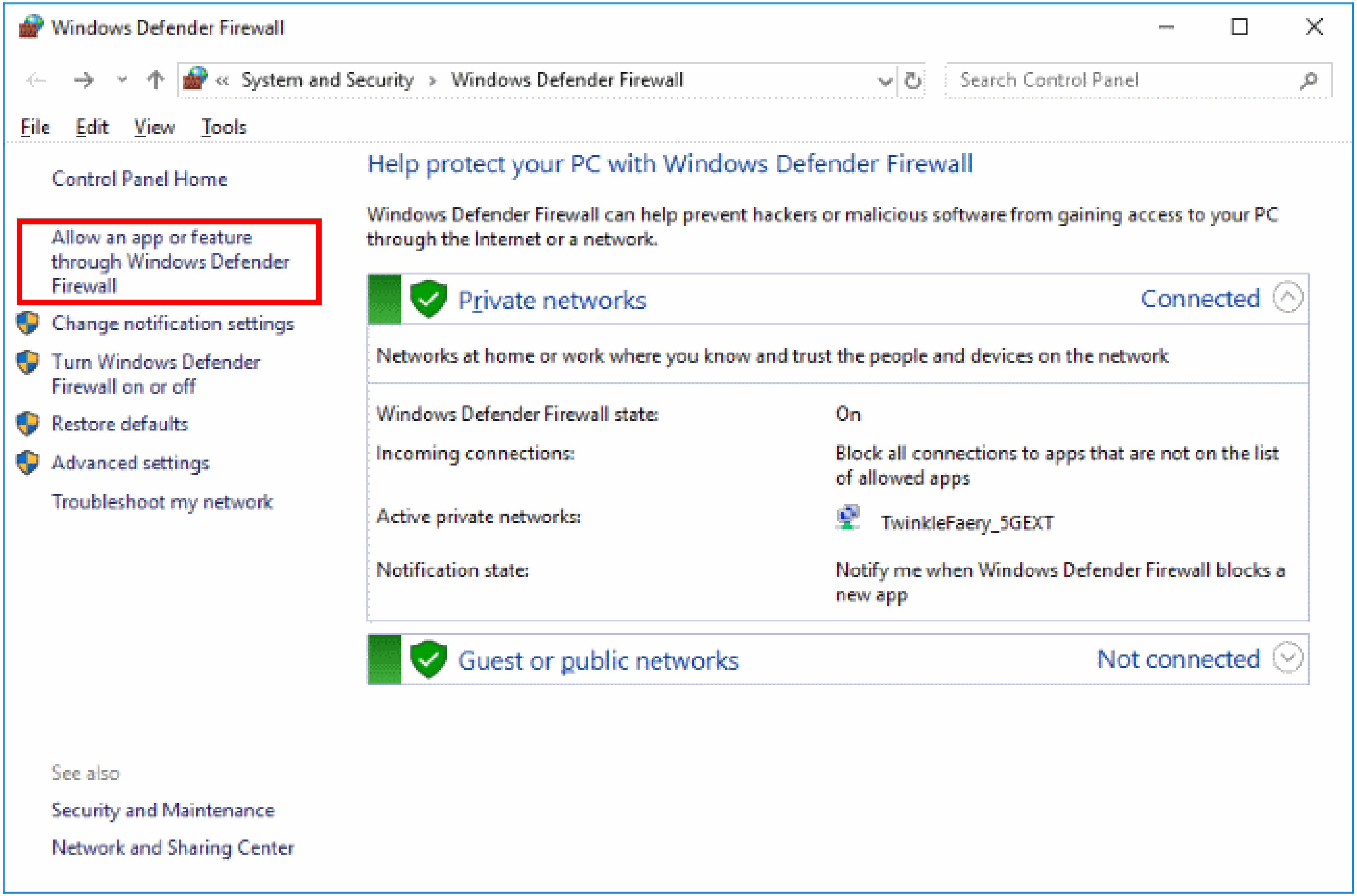
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

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:	belal-2018
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected



Windows Defender Firewall
« System and Security › Windows Defender Firewall
Search Control Panel
File Edit View Tools

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

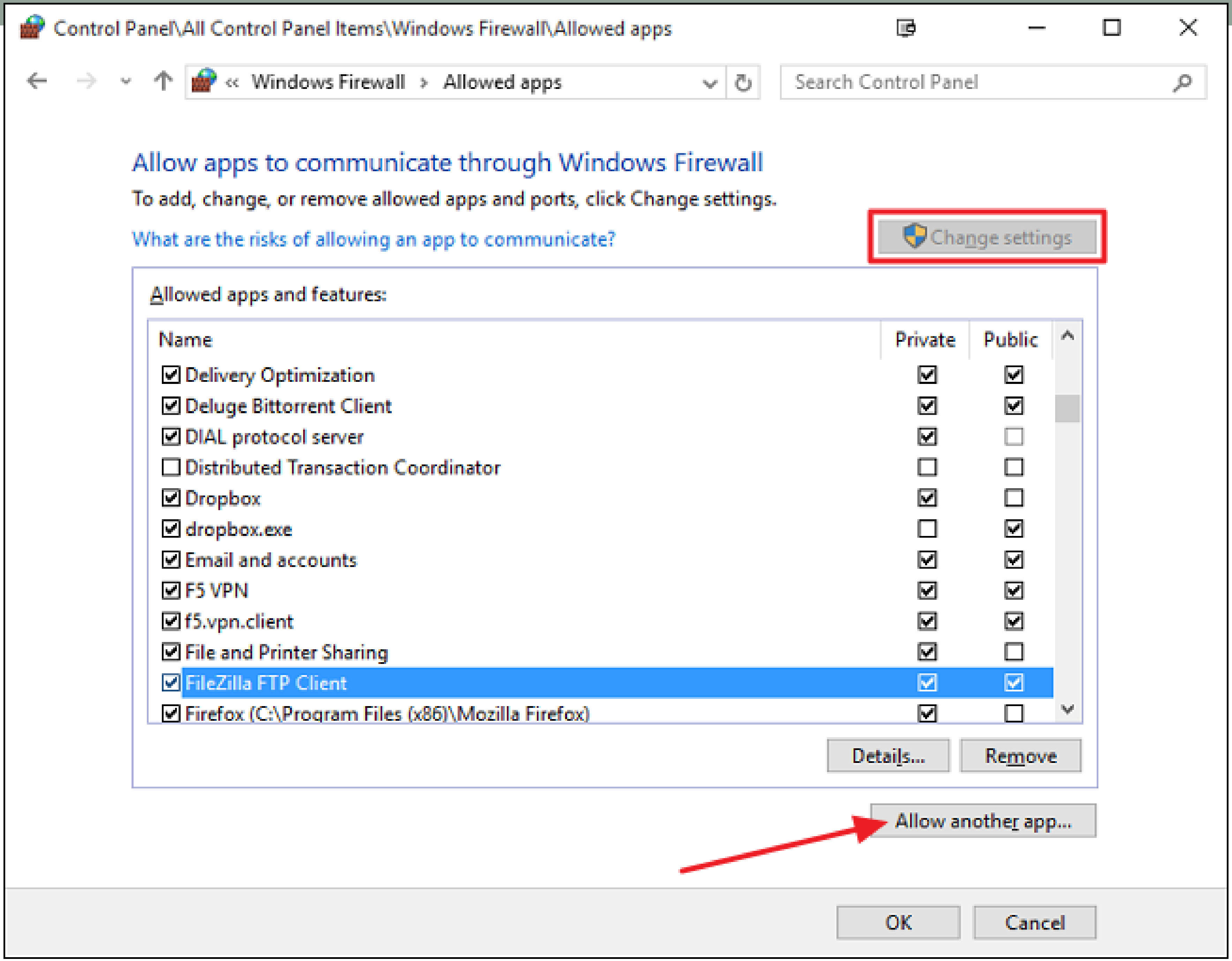
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

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:	TwinkleFaery_5GEXT
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected


Control Panel\All Control Panel Items\Windows Firewall\Allowed apps
« Windows Firewall › Allowed apps
Search Control Panel
Change settings
Details...
Remove
Allow another app...
OK
Cancel

Allow apps to communicate through Windows Firewall

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

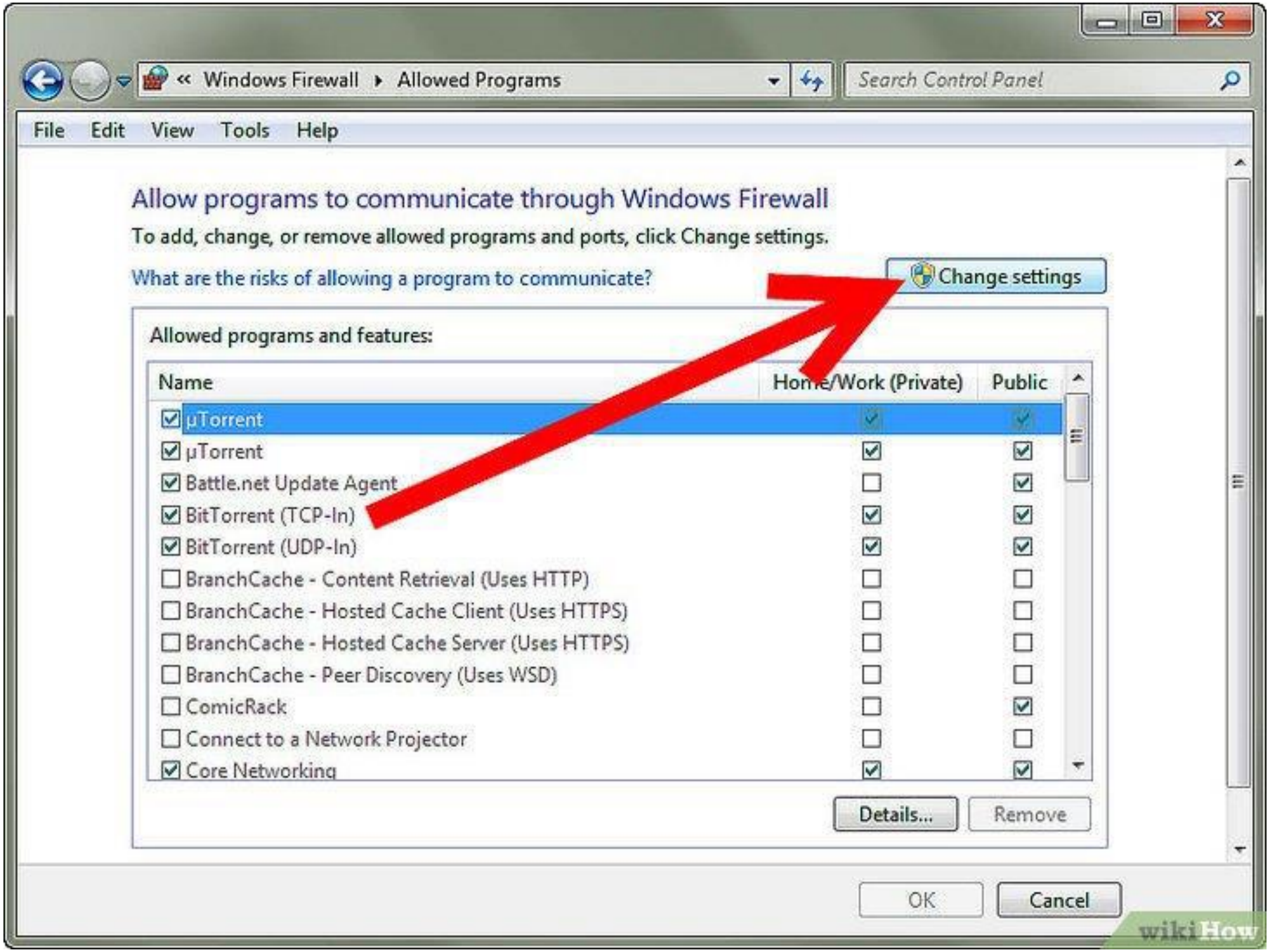
What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ Delivery Optimization	☑	☑
☑ Deluge Bittorrent Client	☑	☑
☑ DIAL protocol server	☑	□
□ Distributed Transaction Coordinator	□	□
☑ Dropbox	☑	□
☑ dropbox.exe	□	☑
☑ Email and accounts	☑	☑
☑ F5 VPN	☑	☑
☑ f5.vpn.client	☑	☑
☑ File and Printer Sharing	☑	□
☑ FileZilla FTP Client	☑	☑
☑ Firefox (C:\Program Files (x86)\Mozilla Firefox)	☑	□

Example: Block a specific program, such as comicRack

After opening the firewall, click on Change settings



Allow programs to communicate through Windows Firewall

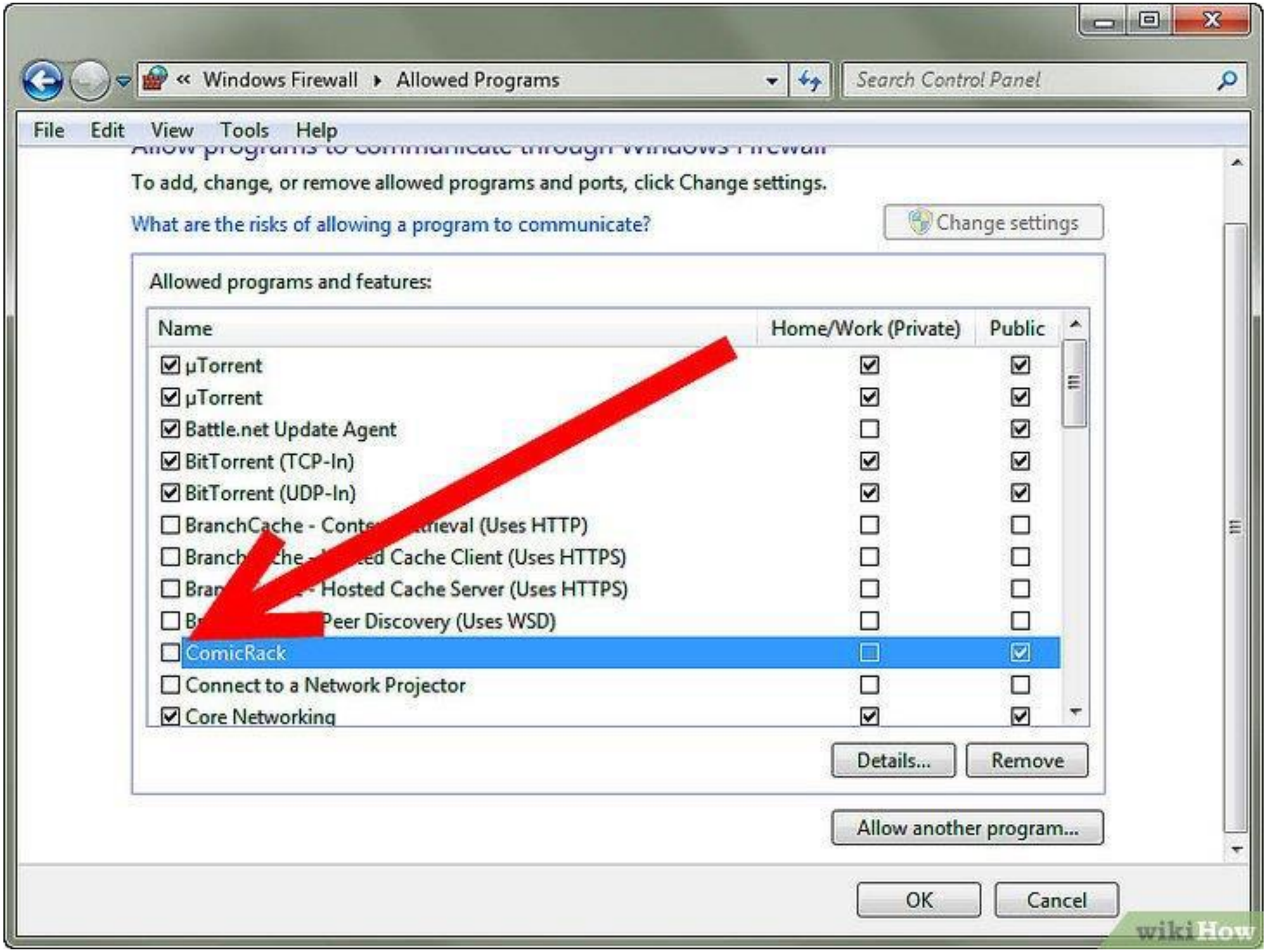
To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Home/Work (Private)	Public
☑ µTorrent	☑	☑
☑ µTorrent	☑	☑
☑ Battle.net Update Agent	□	☑
☑ BitTorrent (TCP-In)	☑	☑
☑ BitTorrent (UDP-In)	☑	☑
□ BranchCache - Content Retrieval (Uses HTTP)	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□
□ ComicRack	□	☑
□ Connect to a Network Projector	□	□
☑ Core Networking	☑	☑

Uncheck the box of the program you want to block. When you uncheck the box, the firewall will block this program from connecting to the Internet



« Windows Firewall ▸ Allowed Programs
Search Control Panel
File Edit View Tools Help

Allow programs to communicate through Windows Firewall

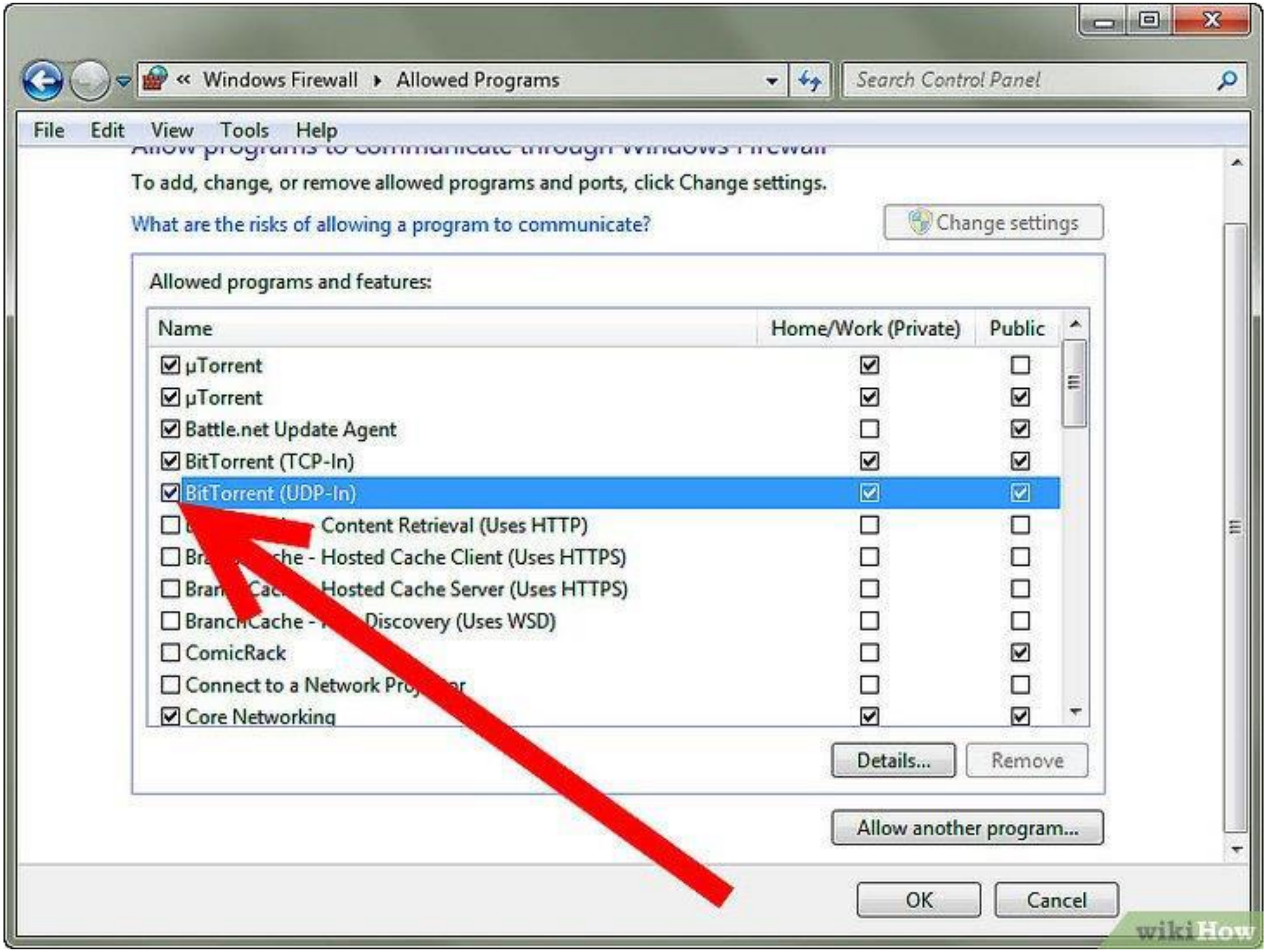
To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Home/Work (Private)	Public
☑ µTorrent	☑	☑
☑ µTorrent	☑	☑
☑ Battle.net Update Agent	□	☑
☑ BitTorrent (TCP-In)	☑	☑
☑ BitTorrent (UDP-In)	☑	☑
□ BranchCache - Conte trieval (Uses HTTP)	□	□
□ Branch che - ted Cache Client (Uses HTTPS)	□	□
□ Bran - Hosted Cache Server (Uses HTTPS)	□	□
□ Br Peer Discovery (Uses WSD)	□	□
□ ComicRack	□	☑
□ Connect to a Network Projector	□	□
☑ Core Networking	☑	☑

Checking the boxes will allow the program to connect to the Internet, so only programs you trust should be allowed.



« Windows Firewall ▸ Allowed Programs
Search Control Panel
File Edit View Tools Help

Allow programs to communicate through Windows Firewall

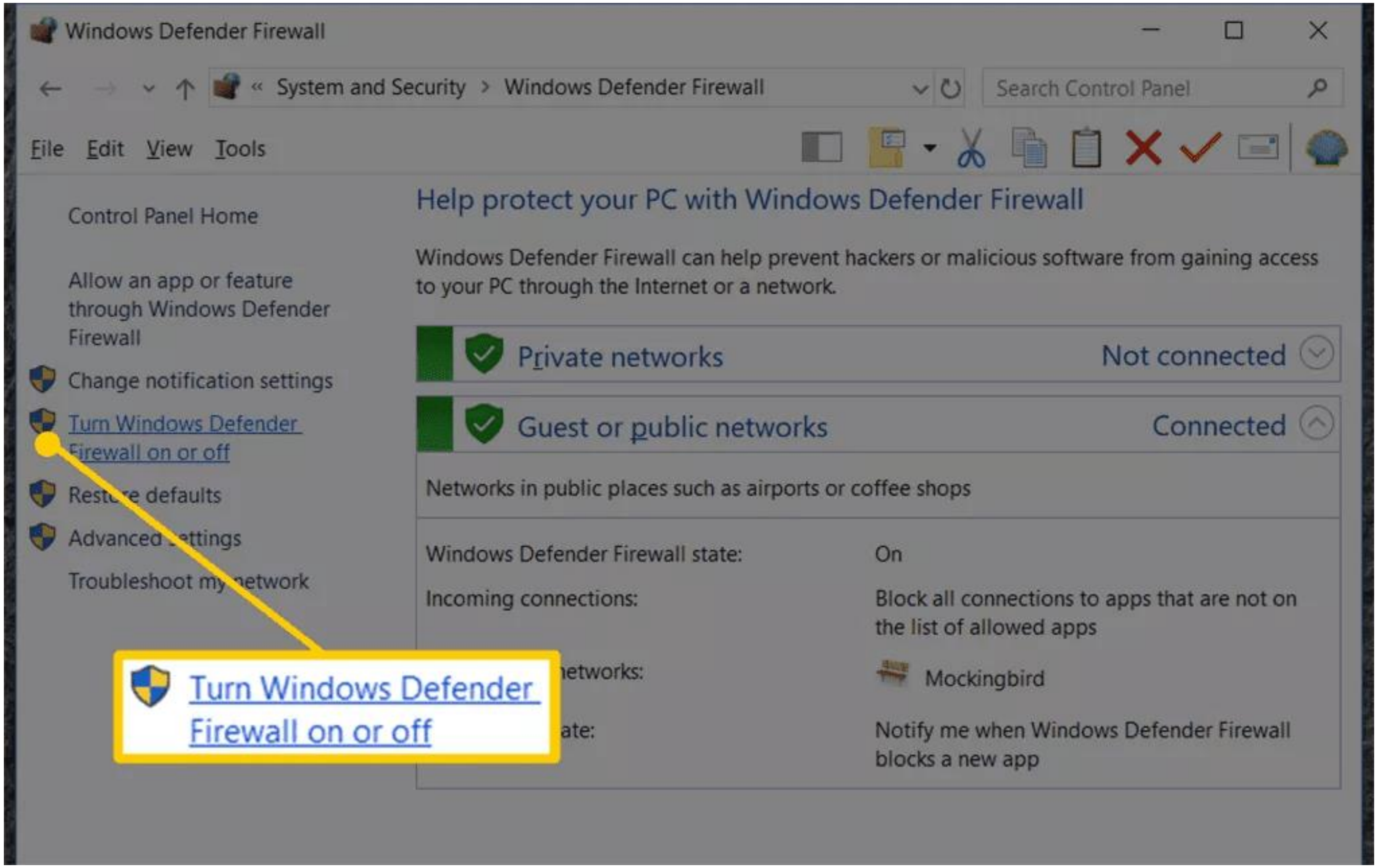
To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Home/Work (Private)	Public
☑ µTorrent	☑	☐
☑ µTorrent	☑	☑
☑ Battle.net Update Agent	☐	☑
☑ BitTorrent (TCP-In)	☑	☑
☑ BitTorrent (UDP-In)	☑	☑
☐ Content Retrieval (Uses HTTP)	☐	☐
☐ Br che - Hosted Cache Client (Uses HTTPS)	☐	☐
☐ Bran Cac Hosted Cache Server (Uses HTTPS)	☐	☐
☐ BranchCache - Discovery (Uses WSD)	☐	☐
☐ ComicRack	☐	☑
☐ Connect to a Network Pro r	☐	☐
☑ Core Networking	☑	☑

If you go back to the main firewall dialog, there is another link in the right pane called If you click on that, you will get the Turn windows firewall on or/off set of options as shown below:



Windows Defender Firewall
System and Security > Windows Defender Firewall
Search Control Panel
File Edit View Tools
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

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

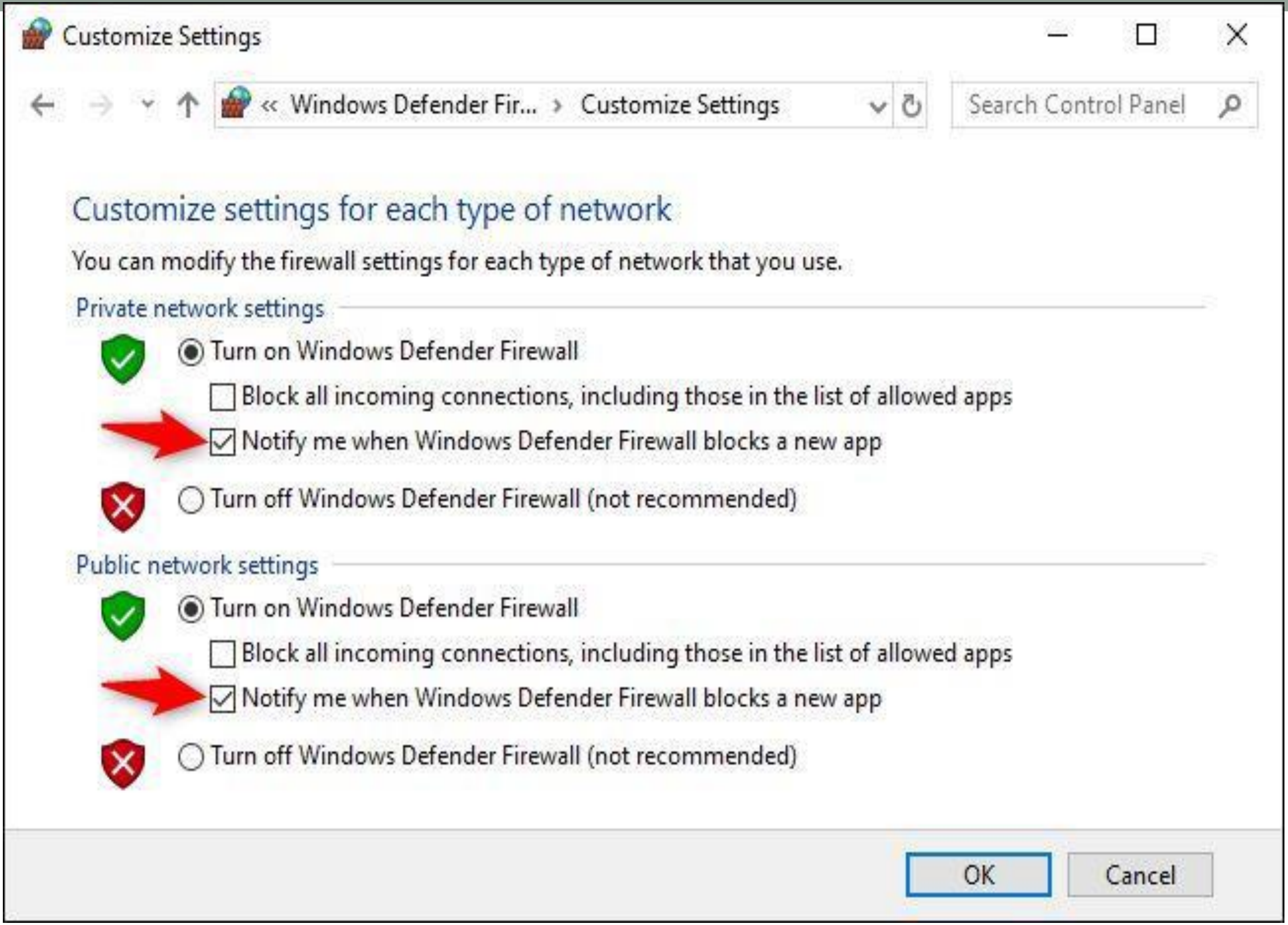
Networks in public places such as airports or coffee shops

Windows Defender Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

etworks: Mockingbird

ate: Notify me when Windows Defender Firewall blocks a new app



Customize Settings

« Windows Defender Fir... › Customize Settings

Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

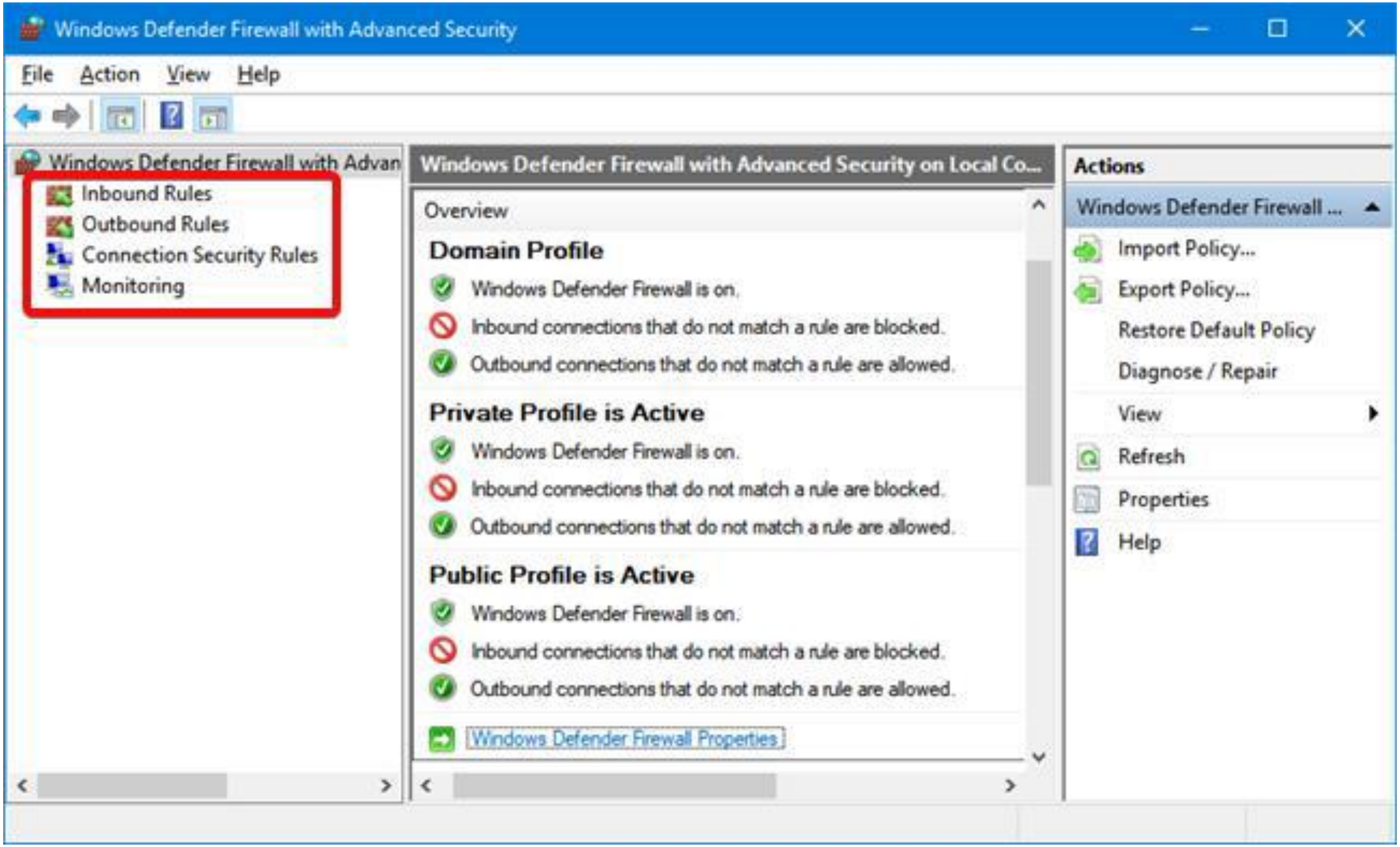
□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Advanced Settings

In the left pane of the main dialog box of the advanced settings firewall, click the link Windows firewall with advanced security protection, this will bring up a window



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

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 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.

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

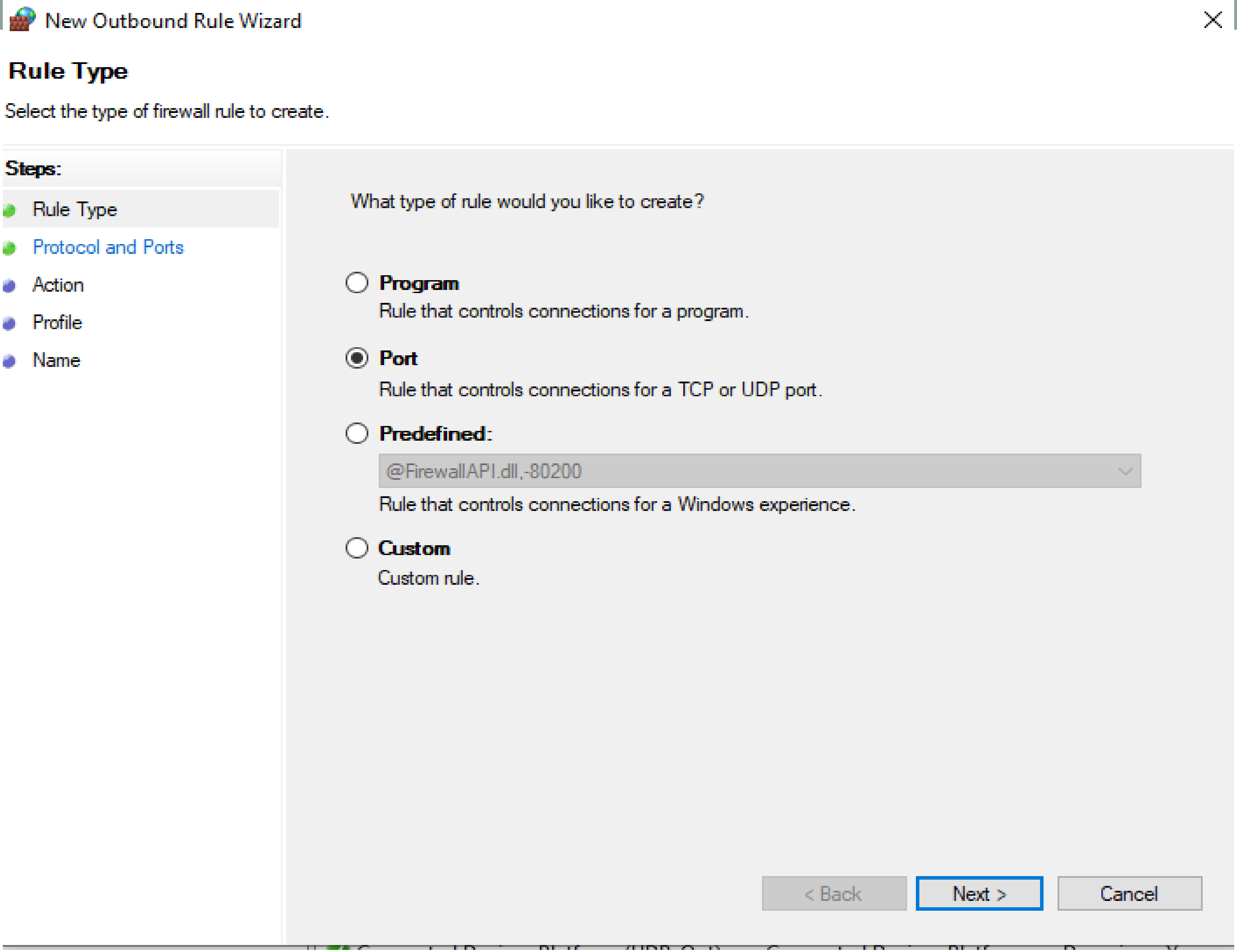
If you want to block an external connection, we do the following:

Click on Outbound Rules on the left side, then click on New Rule

A dialog box will appear asking about the type of rule

if we click on port, in order to block all outgoing connections on port 80, the HTTP port used by every web browser. In theory this should block Internet access and other browsers IE, Edge, Chrome in the browser

Click Next, select TCP and type the port number.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

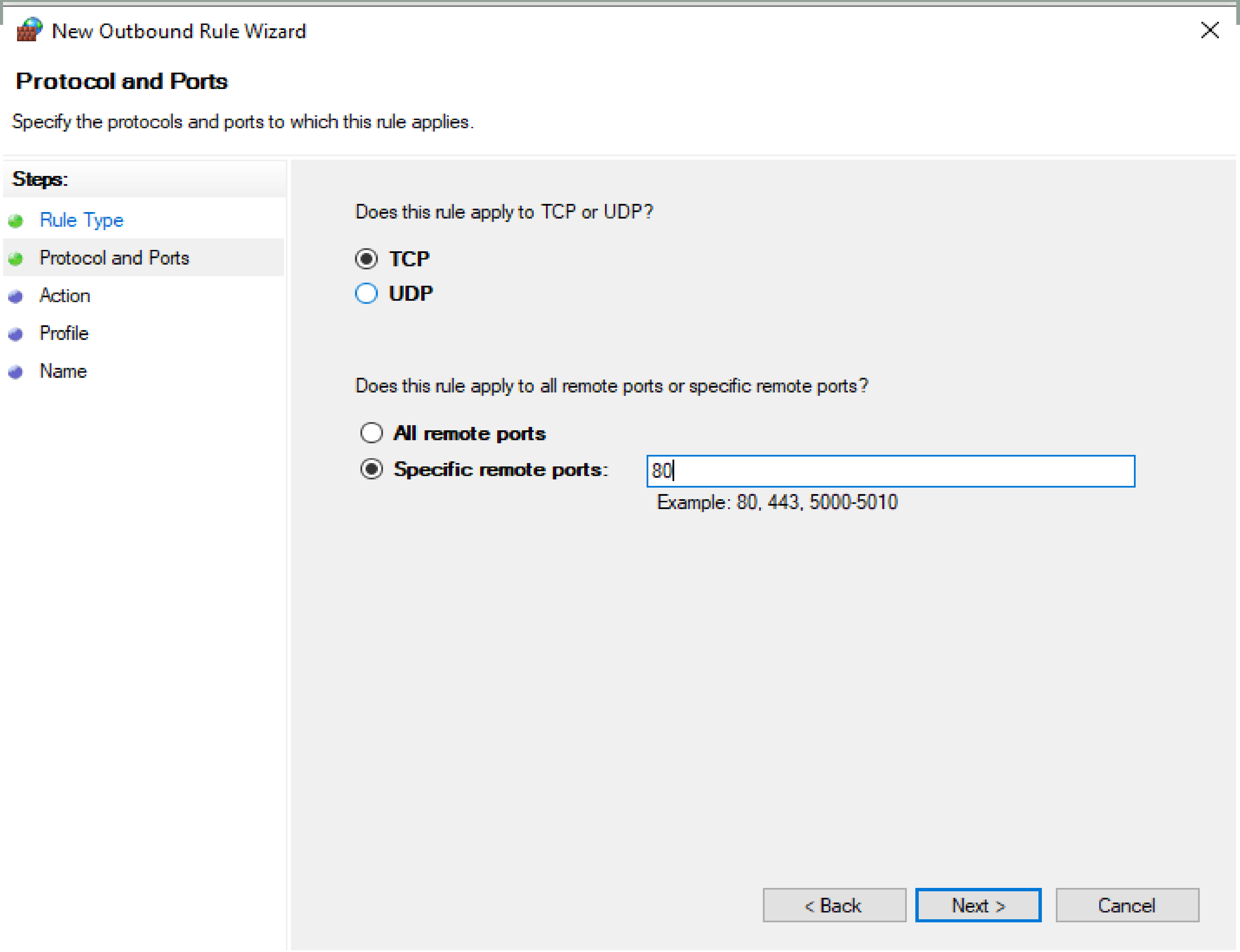
What type of rule would you like to create?

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

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

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

○ **Custom**
Custom rule.



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

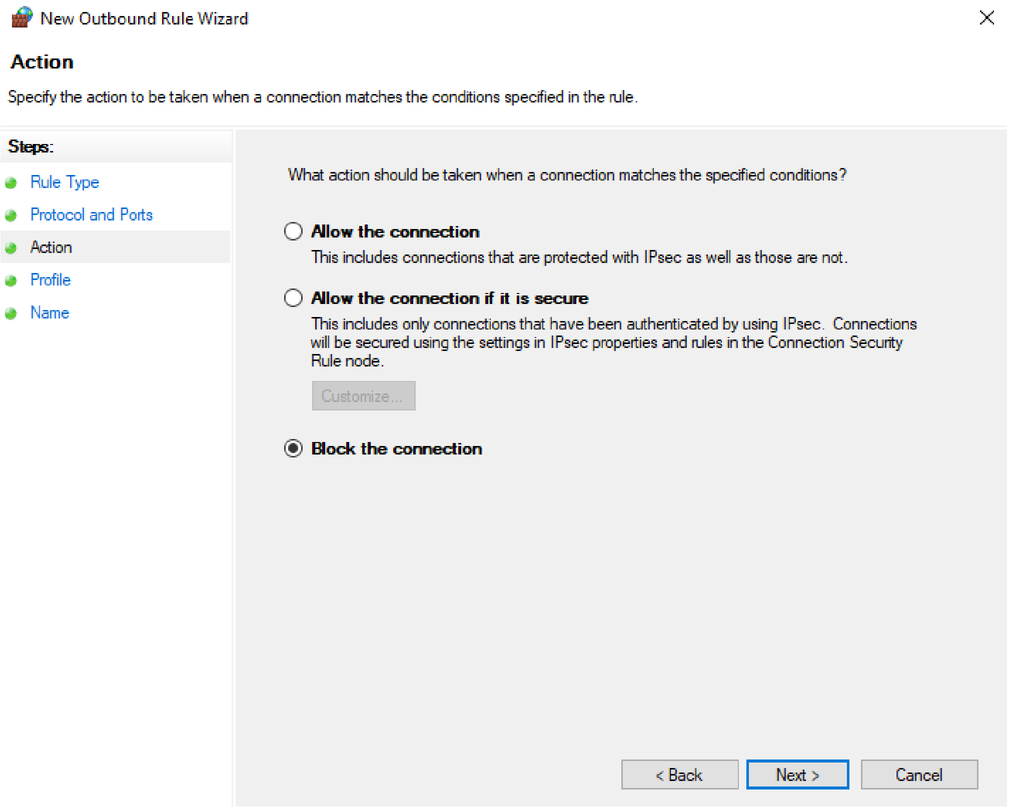
Does this rule apply to all remote ports or specific remote ports?

○ All remote ports

● Specific remote ports: 80

Example: 80, 443, 5000-5010

Then, after clicking on Next, we choose the action we want, and because we want to block the connection, we 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.

Steps:

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

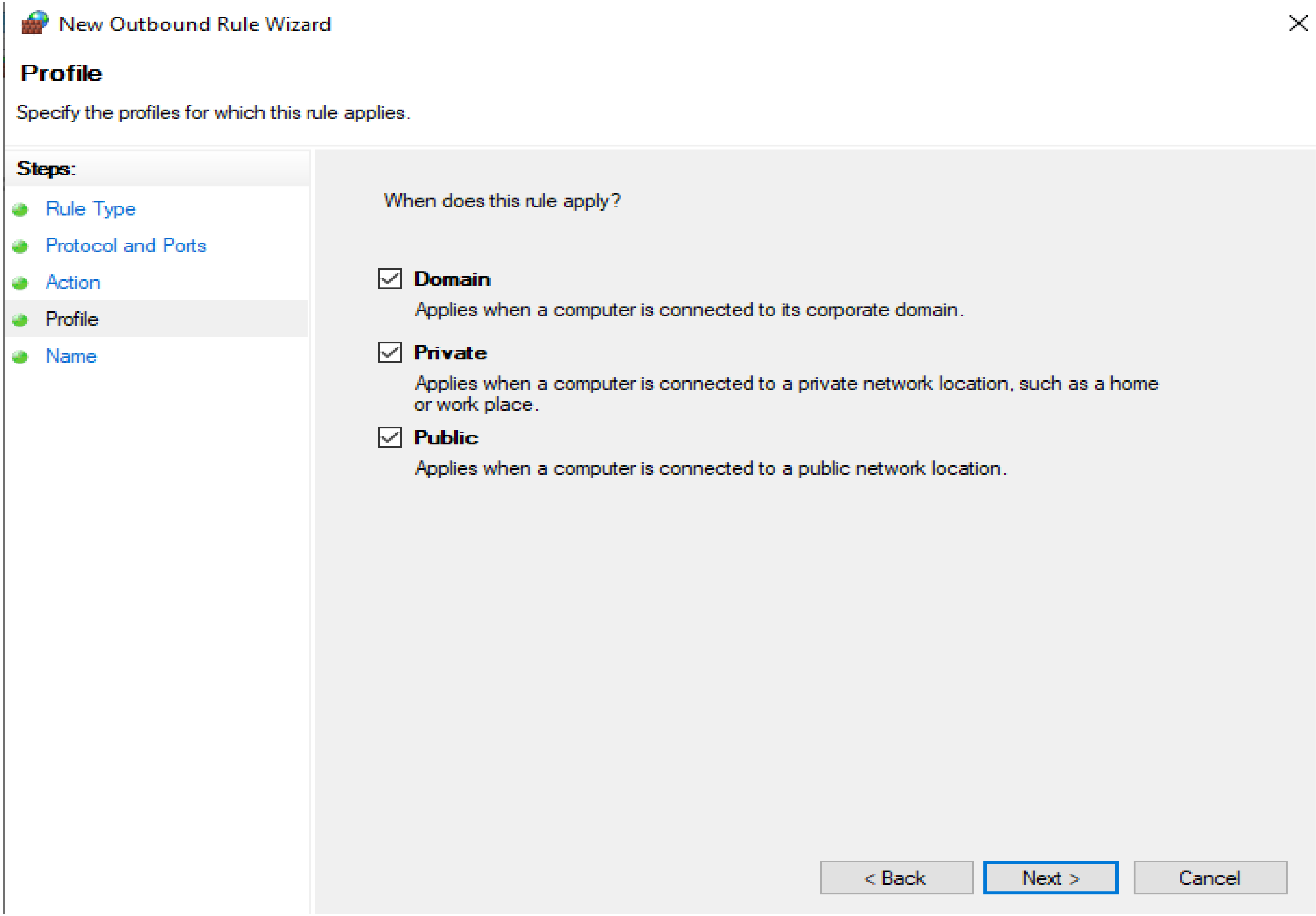
What action should be taken when a connection matches the specified conditions?

○ **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**

Then we choose which personal files we want to apply the rule to, so we choose, for example, everyone:



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.