

Hands-on-Lab: Windows Firewall with Advanced Security

Estimated time needed: **45** minutes

Objectives

By completing this lab, users will develop a comprehensive understanding of how to secure a Windows operating system using the real-time protection provided by Windows Firewall.

In this hands-on lab, you will review settings to enable firewall:

- Exercise 1: Configure Firewall Rules Using Windows Defender Firewall
- Exercise 2: Configure Firewall Rules Using Windows Defender Firewall with Advanced Security

Further in this hands-on lab, you will also explore few typical use cases:

The different scenarios in this lab will help you explore different aspects of security that can be controlled by Windows Firewall service.

- Scenario 1: Block Remote Desktop on the Public Network (Inbound Rules)
- Scenario 2: Block Outbound Traffic for Specified Applications (Outbound Rules)
- Scenario 3: Block Web Server (HTTP) Traffic on a Public Network (Inbound Rules)
- Scenario 4: Allow Key Management Service on the Domain and Private network, and deny the connection on the Public network (Inbound Rules)

Important Notices about This Lab

About Lab Sessions

Lab sessions are not persisted. This means that every time you connect to this lab, a new environment is created for you. Any data or files you saved in a previous session are no longer available. To avoid losing your data, plan to complete these tasks in a single session.

About the Lab Instructions and Solutions

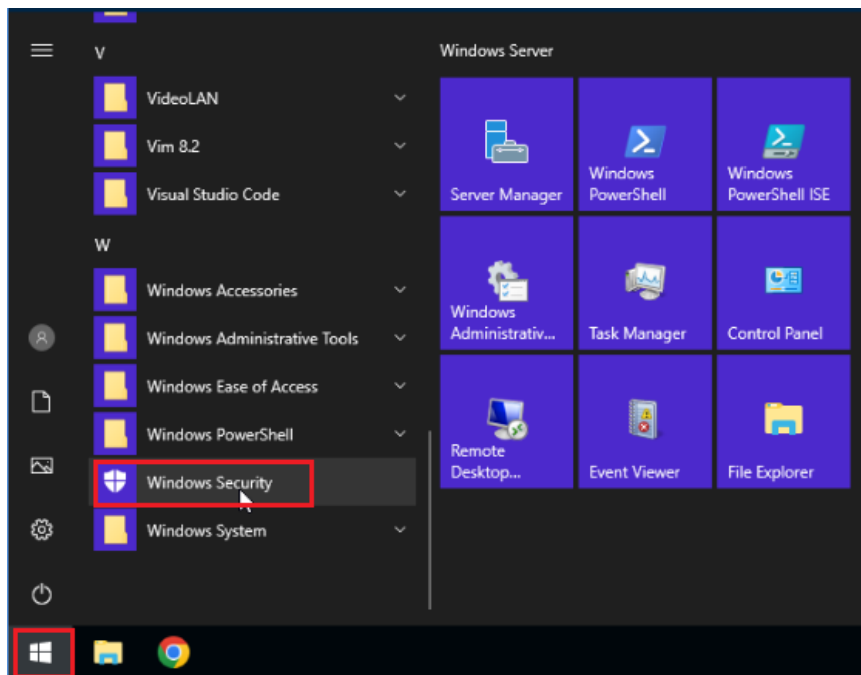
Microsoft Windows operating system features can vary based on the Windows edition. If completing these exercises on your machine, your navigation and solutions may differ from what's presented in this lab.

Enable firewall

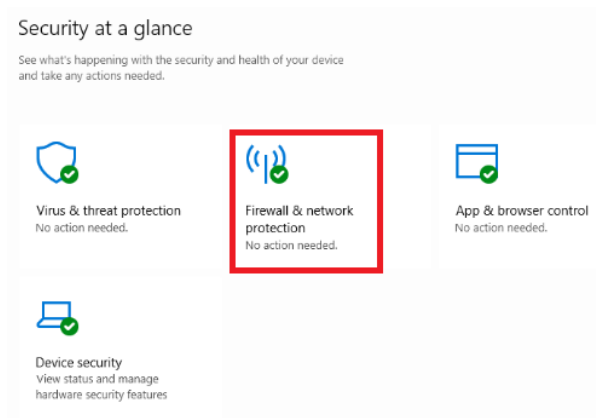
Exercise 1: Enable Firewall on different Network Profiles

In this exercise we will review Windows Defender Firewall configuration.

1. Click the Windows **Start** button. and then select **Windows Security**.

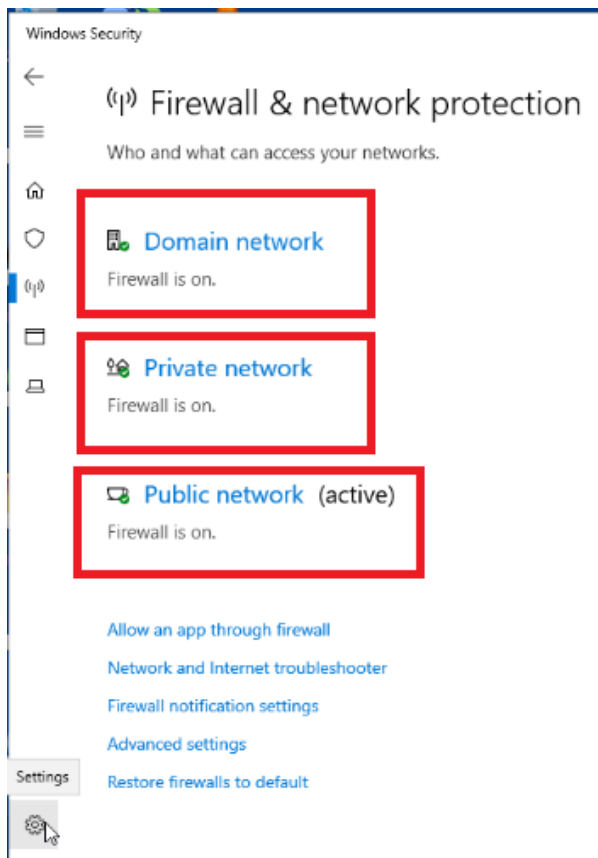


2. Click **Firewall & network protection**.

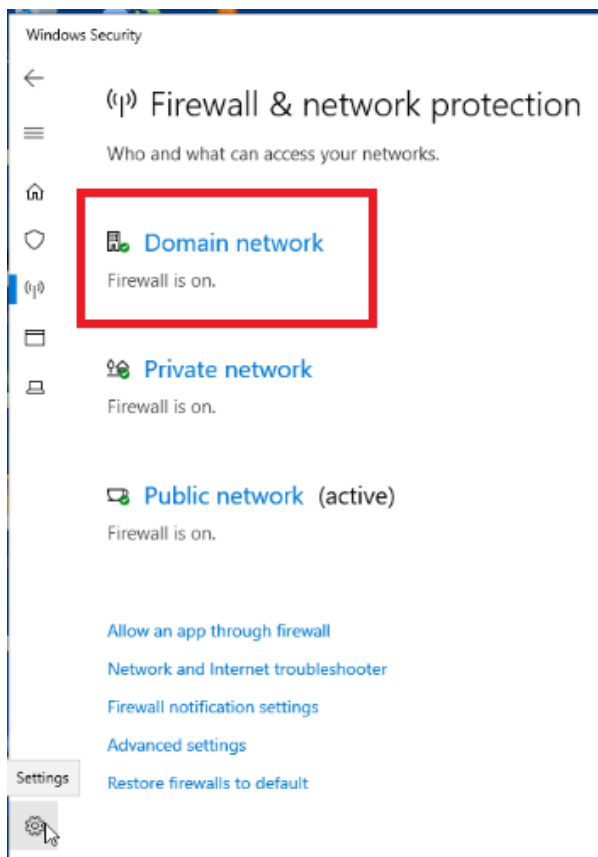


3. Here you will see the firewall status for the following:

- **Domain network:** Domain networks are workplace networks. A computer must be a part of the domain in order to communicate with other computers on that network.
- **Private network:** Private networks are discoverable networks, meaning that only devices on that network can see or discover other devices on that same network. Home networks are a good example of a private network.
- **Public network:** Public networks are non-discoverable networks. A non-discoverable network is a network where your device cannot be discovered by other devices on your network. A coffee shop or a library would be a good example of a public network. You do not want other individuals to be able to discover your device.



4. Click **Domain network**.



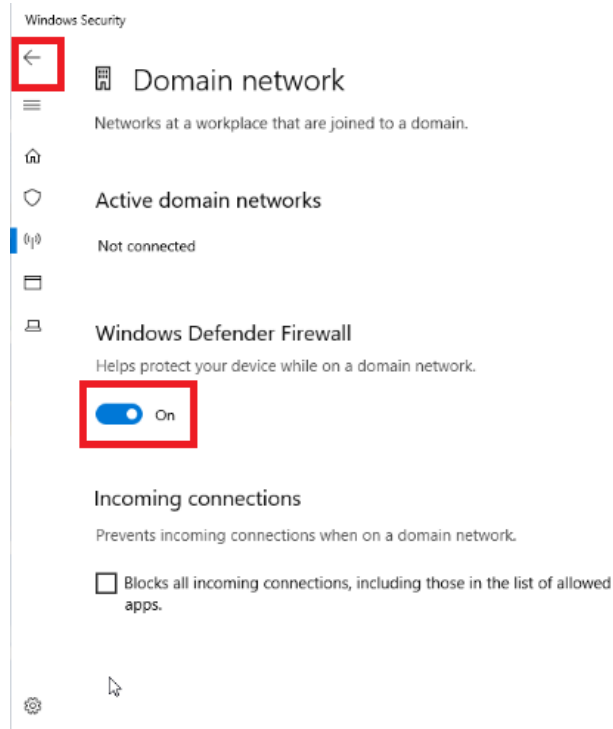
5. Verify that the Windows Defender Firewall is toggled to **On**.

Observe the option **Incoming connections**. If you need to block all incoming domain network traffic, including traffic that is typically allowed, then you only need to activate this option.

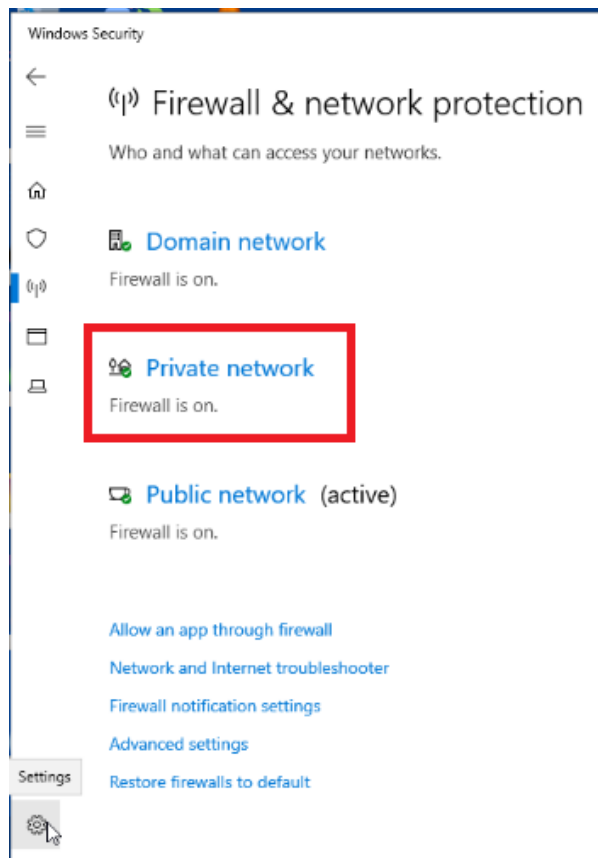
Note: You do not need to enable this option for this lab.

Note: If you have installed a 3rd Party anti-virus software, this option will be disabled. In this case, you can control the firewall settings only through the anti-virus software.

Select the back arrow button to return to the **Firewall and network protection** window.

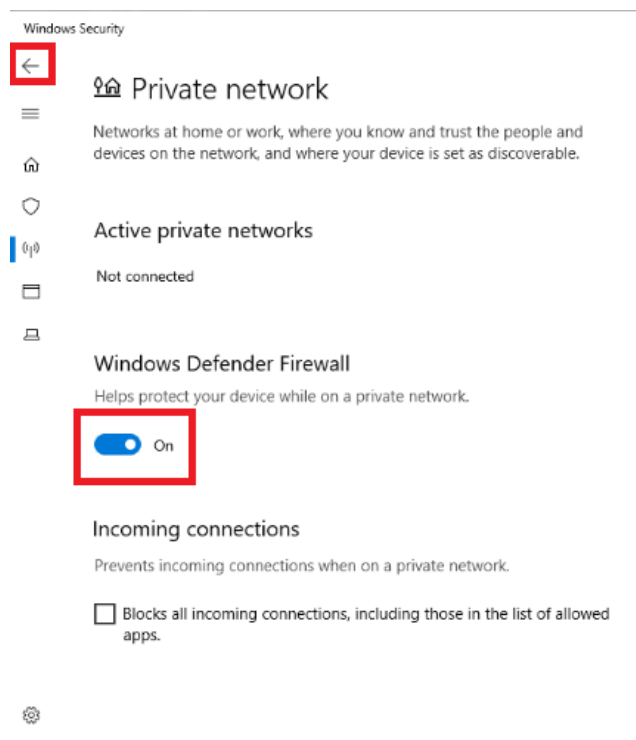


6. Click **Private network**.

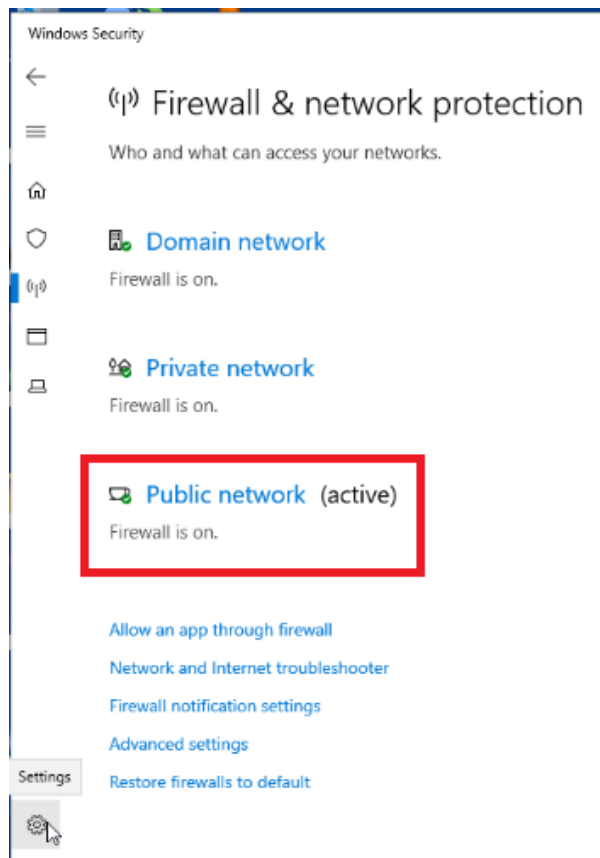


7. Verify that the Windows Defender Firewall is toggled to **On**.

Select the back arrow button to return to the **Firewall and network protection** window.

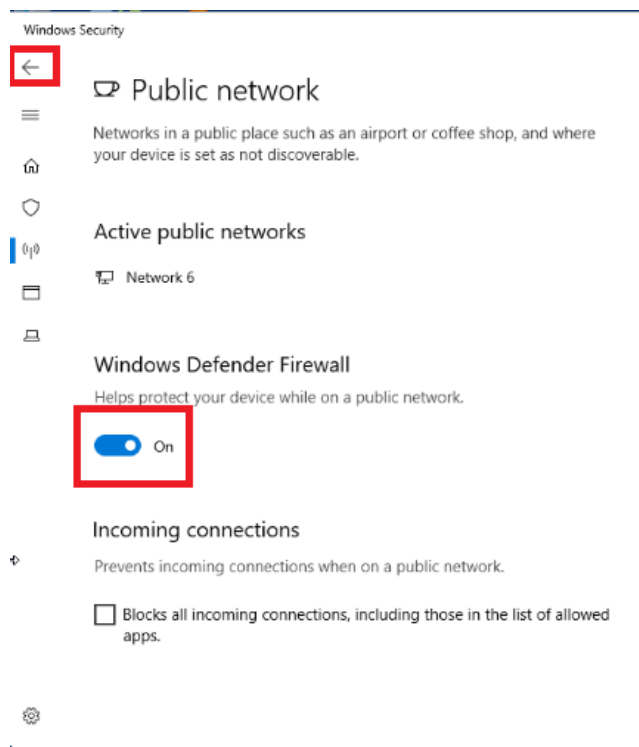


8. Click **Public network**.

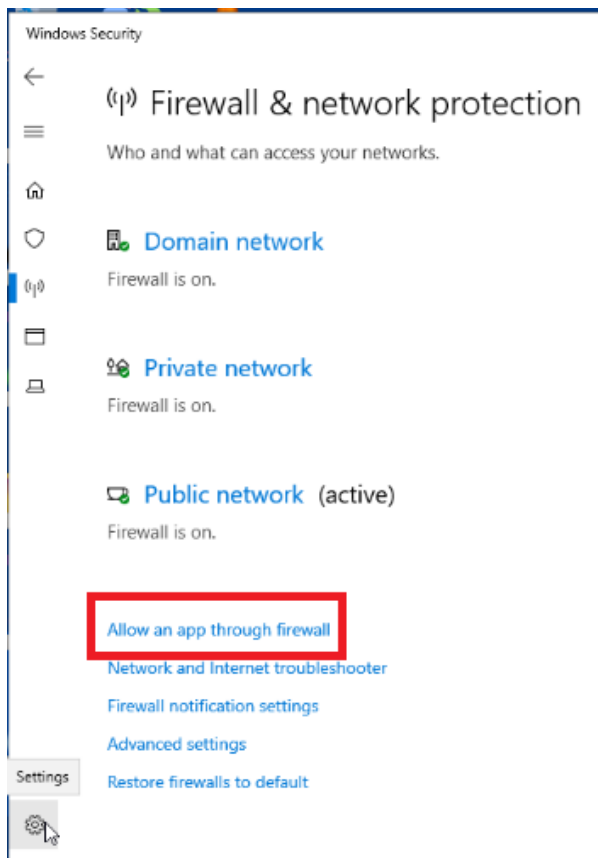


9. Verify that the Windows Defender Firewall is toggled to **On**.

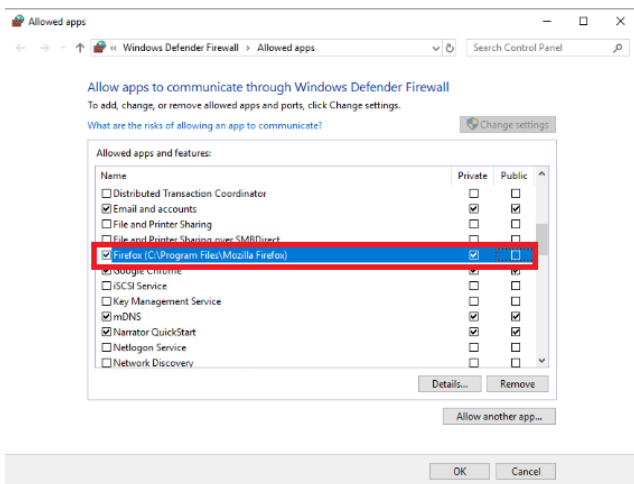
Select the back arrow button to return to the **Firewall and network protection** window.



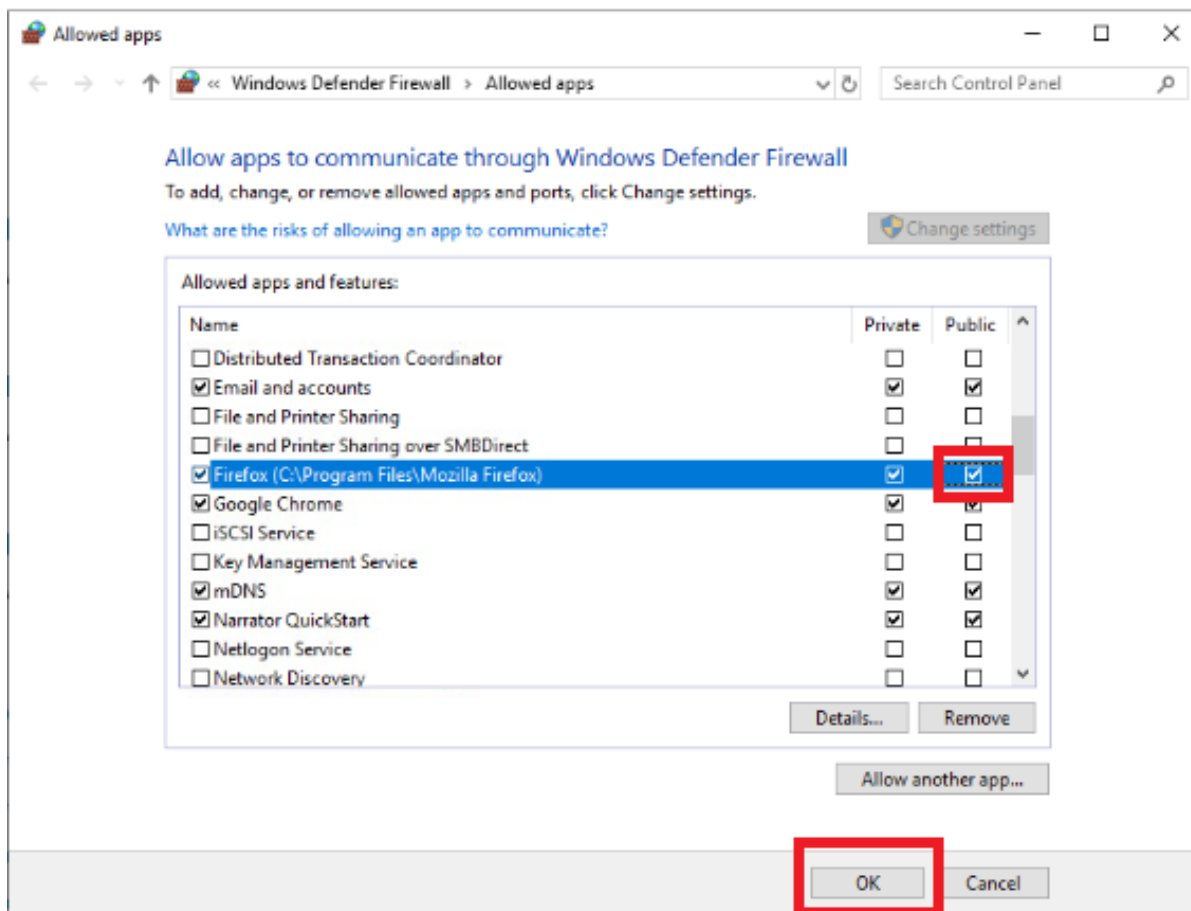
10. Click **Allow an app through firewall**.



11. Scroll to **Google Chrome** OR **Mozilla Firefox**. Observe in the screenshot below that the current configuration allows for Firefox to communicate on the Private network only but denies it from communicating on the Public network.



12. Click the **Public** box next to Firefox to allow Firefox to communicate through the Public network as well. A checkmark will appear. Click **OK** to return to the **Firewall & network protection** screen. Users will now be able to use Mozilla Firefox on the public network.



Typical use cases with Windows Firewall Advanced Security options

The first exercise is based in the consumer-friendly version of Windows Defender Firewall – a simplified interface ideal for a single device in a home setting. In this exercise, we will look at Windows Defender Firewall with Advanced Security. This advanced view provides more in-depth options for configuration. All Windows Firewall rules, and their details, are stored here, allowing you to edit configurations for each rule or exception.

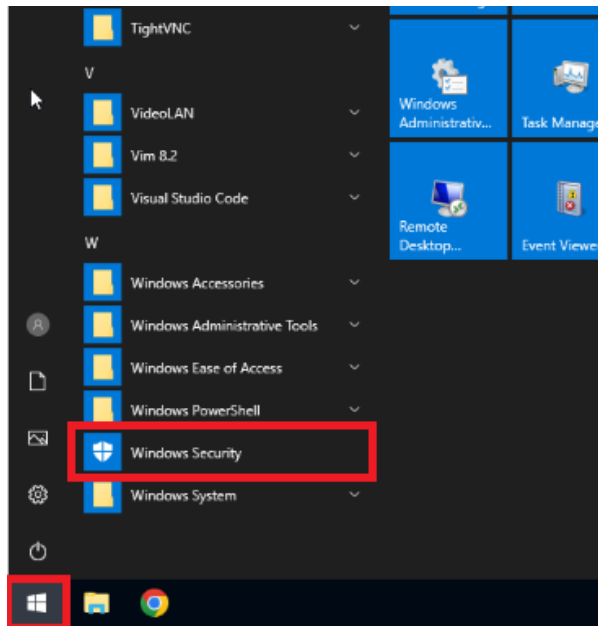
Scenario 1 - Block Remote Desktop on the Public Network Using Windows Firewall (Inbound Rules)

The Remote Desktop feature in Windows allows you to connect to and control a computer from a remote location. This can be particularly useful for accessing your work computer from home, assisting others with technical issues, or managing servers.

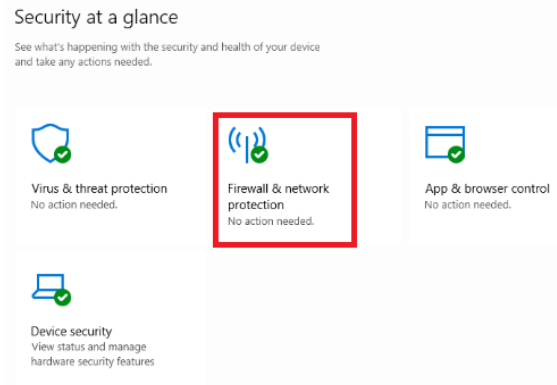
Blocking Remote Desktop on a public network using Windows Firewall can help enhance the security of your system by preventing unauthorized access. Here's how you can configure Windows Firewall to block Remote Desktop (RDP) on public networks.

1. Open the Windows Defender Firewall with Advanced Security options

- Click the Windows **Start** button. and then select **Windows Security**.

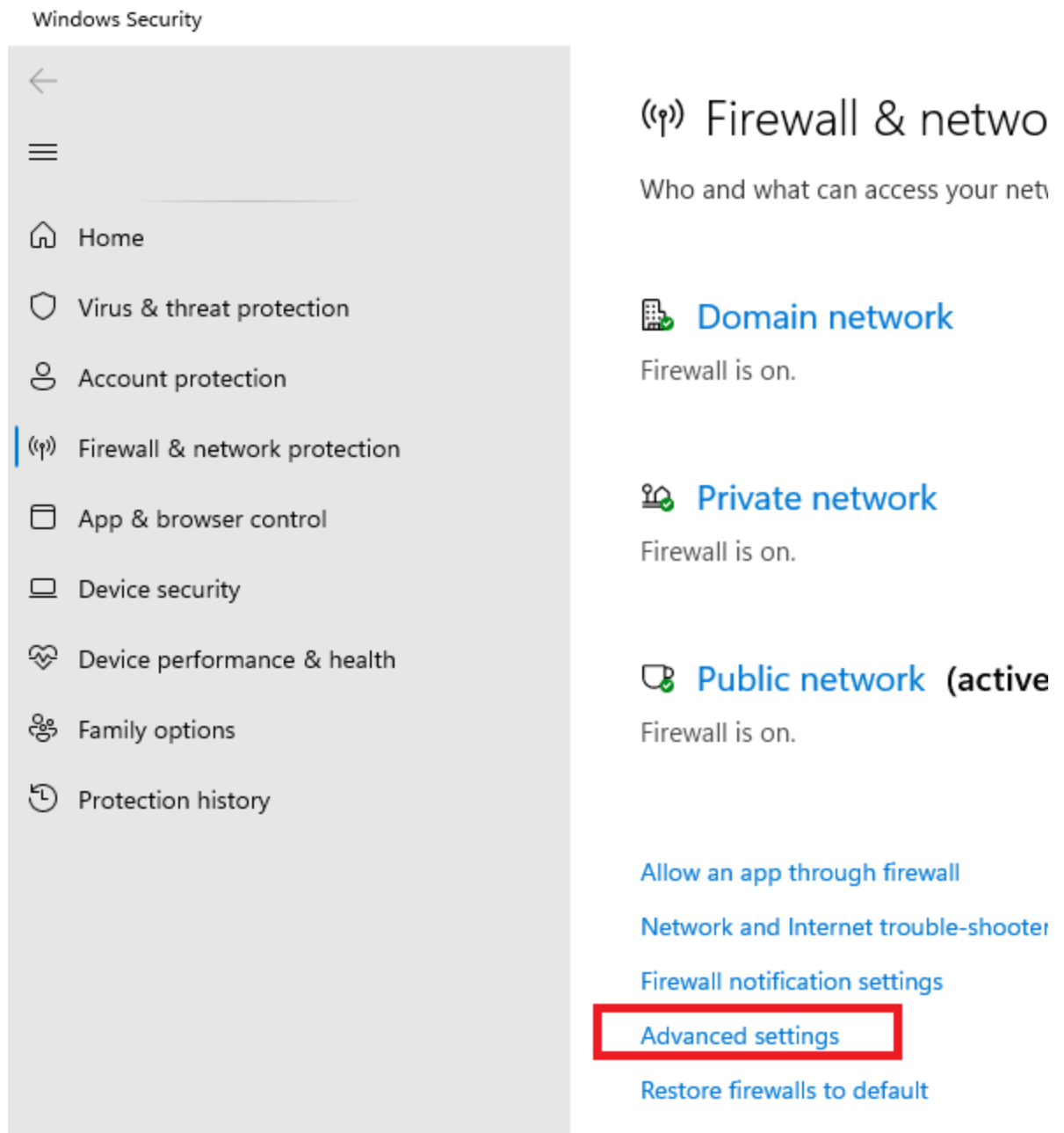


- Click **Firewall & network protection**.



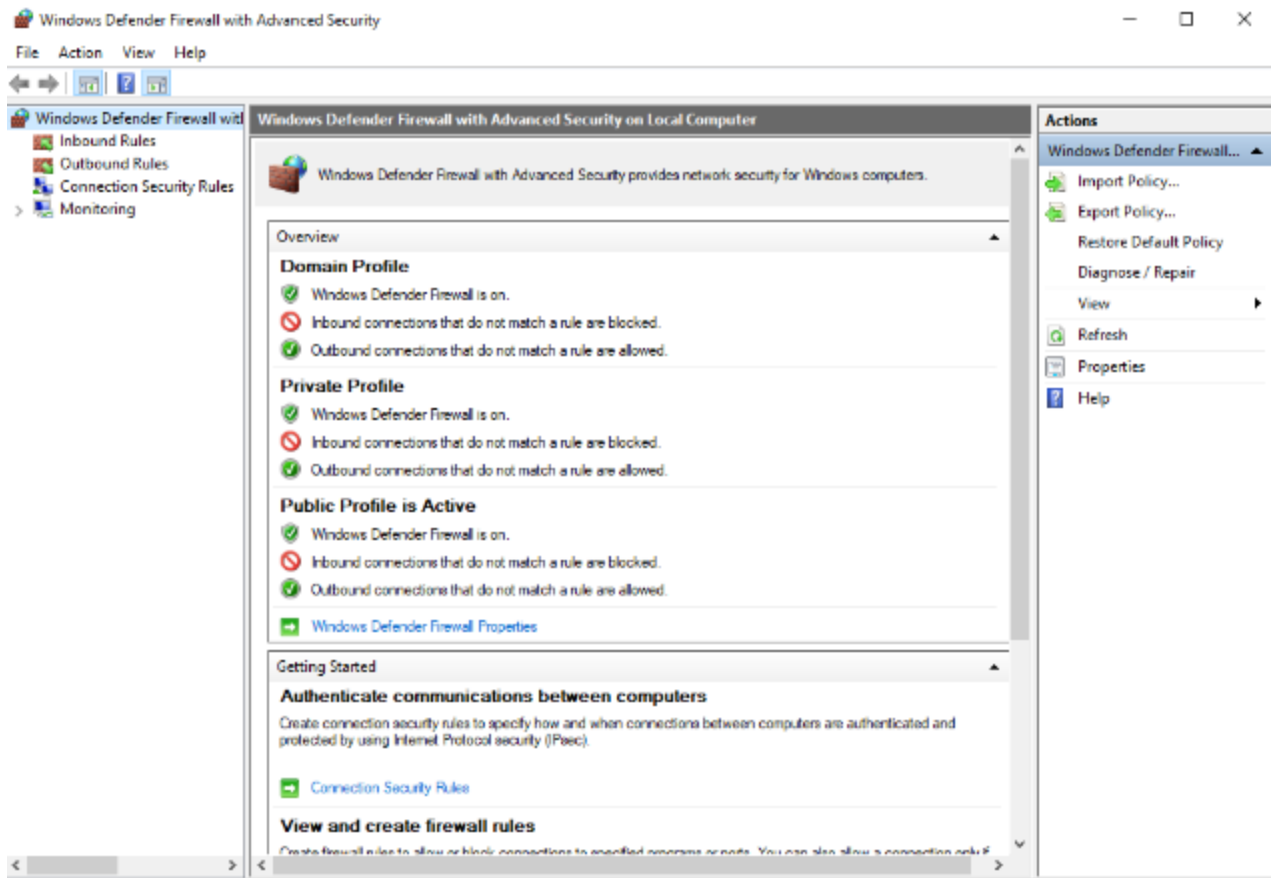
- Open Windows Firewall Advanced Settings

- In the Windows Defender Firewall window, click on **Advanced settings** in the left pane.



- This opens the Windows Defender Firewall with Advanced Security window. Here you will see an **Overview** in the center panel. Make special note of the rule types listed on the left panel:
 - Inbound rules:** Inbound rules determine what traffic is allowed to the computer.
 - Outbound rules:** Outbound rules determine what traffic is allowed to leave the computer.
 - Connection security rules:** Connection security rules define how and when computers should use IPsec (Internet Protocol Security) to secure traffic.
 - Monitoring:** Monitoring involves tracking and analyzing the traffic that is allowed or blocked by the firewall.

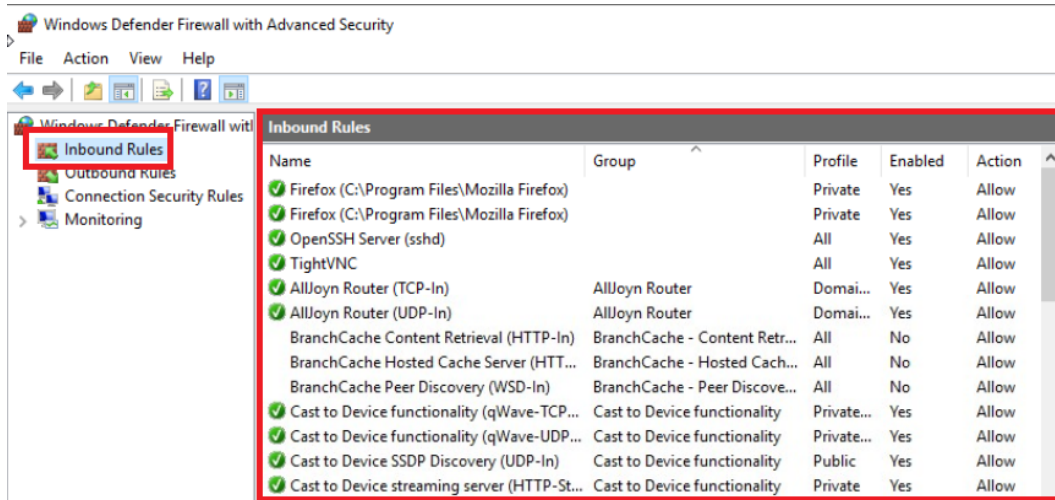
Each of these rules can be configured to filter traffic based on computers, users, applications, ports, protocols, and so on.



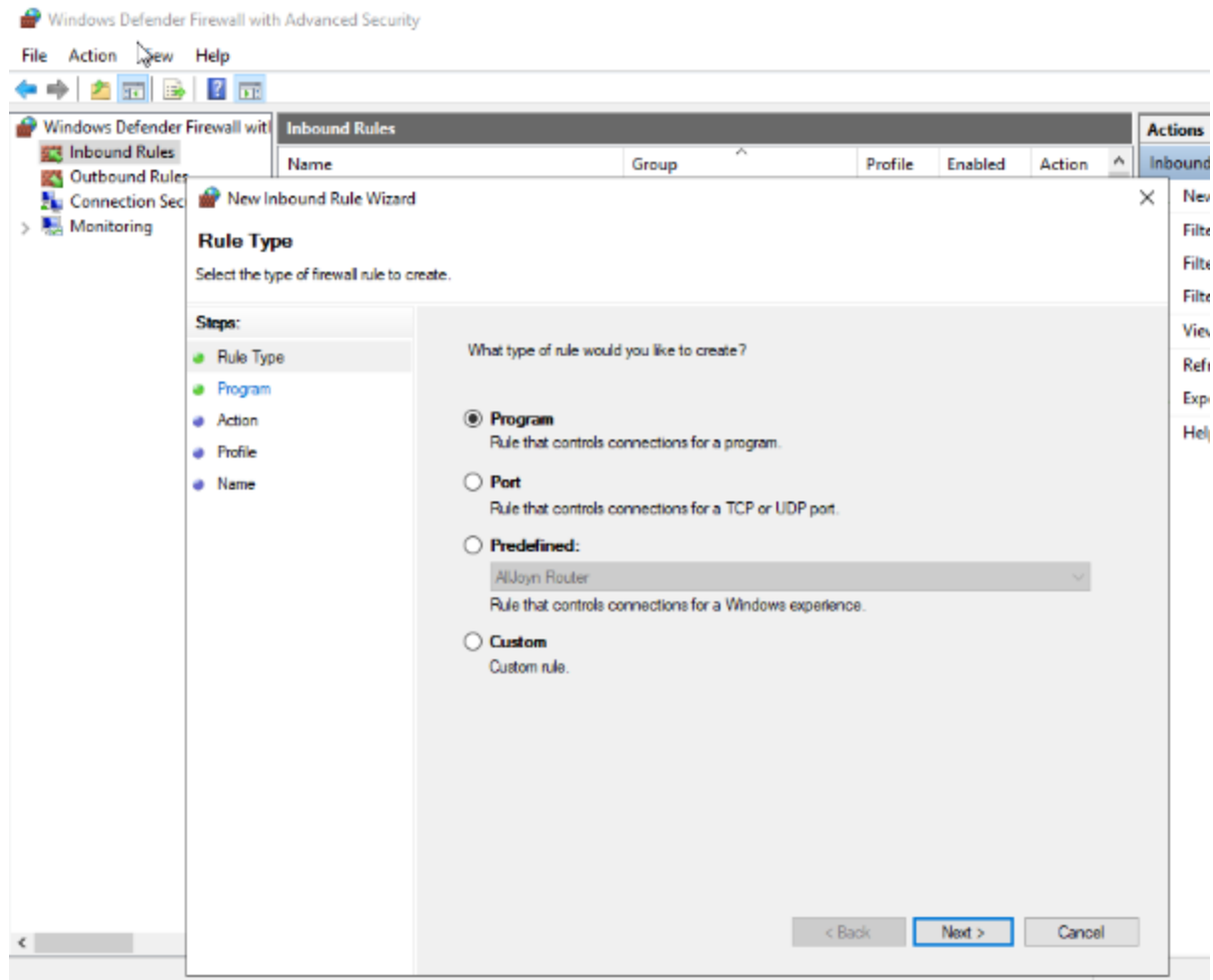
2. Disable Remote Desktop on the Public Network

- Create a New Inbound Rule
 - In the left pane, click on **Inbound Rules**.

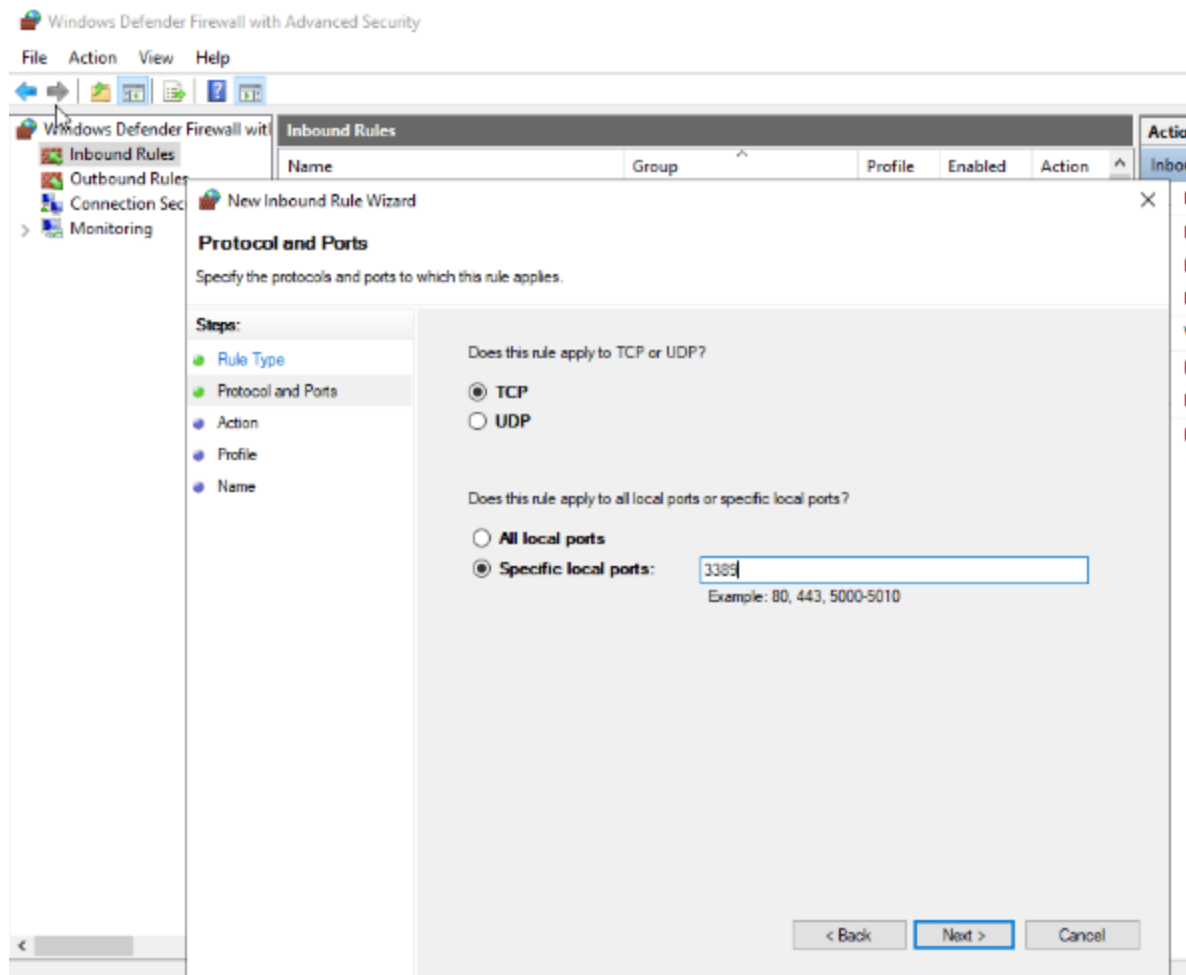
Here you will see a long list of inbound rules. Note that some of the rules have a green checkmark next to them. This indicates that the rule is enabled to allow inbound communication. The rules without a checkmark are available for use but are not enabled.



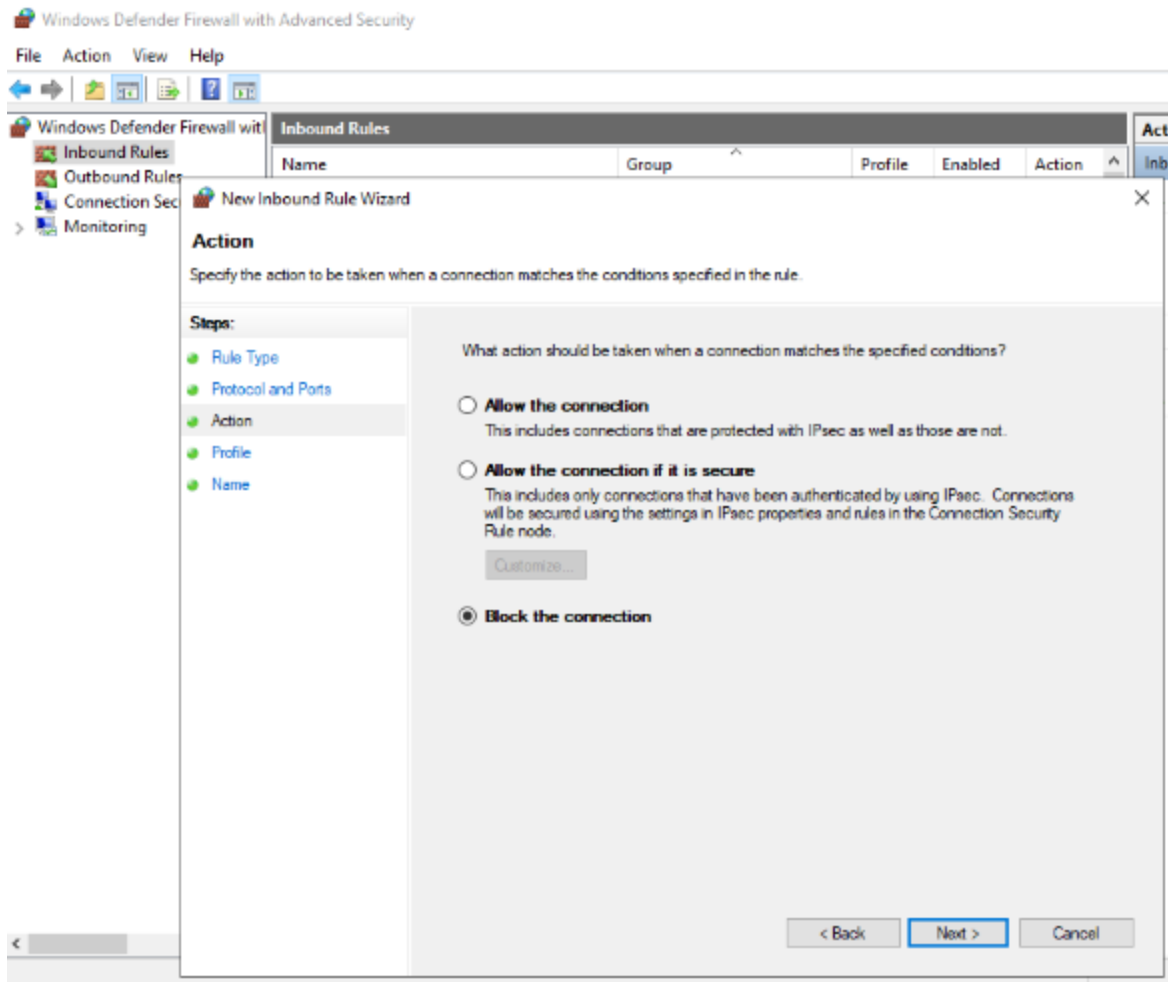
- In the right pane, click on **New Rule...**
- Select Rule Type- Select **Port** and click **Next**.



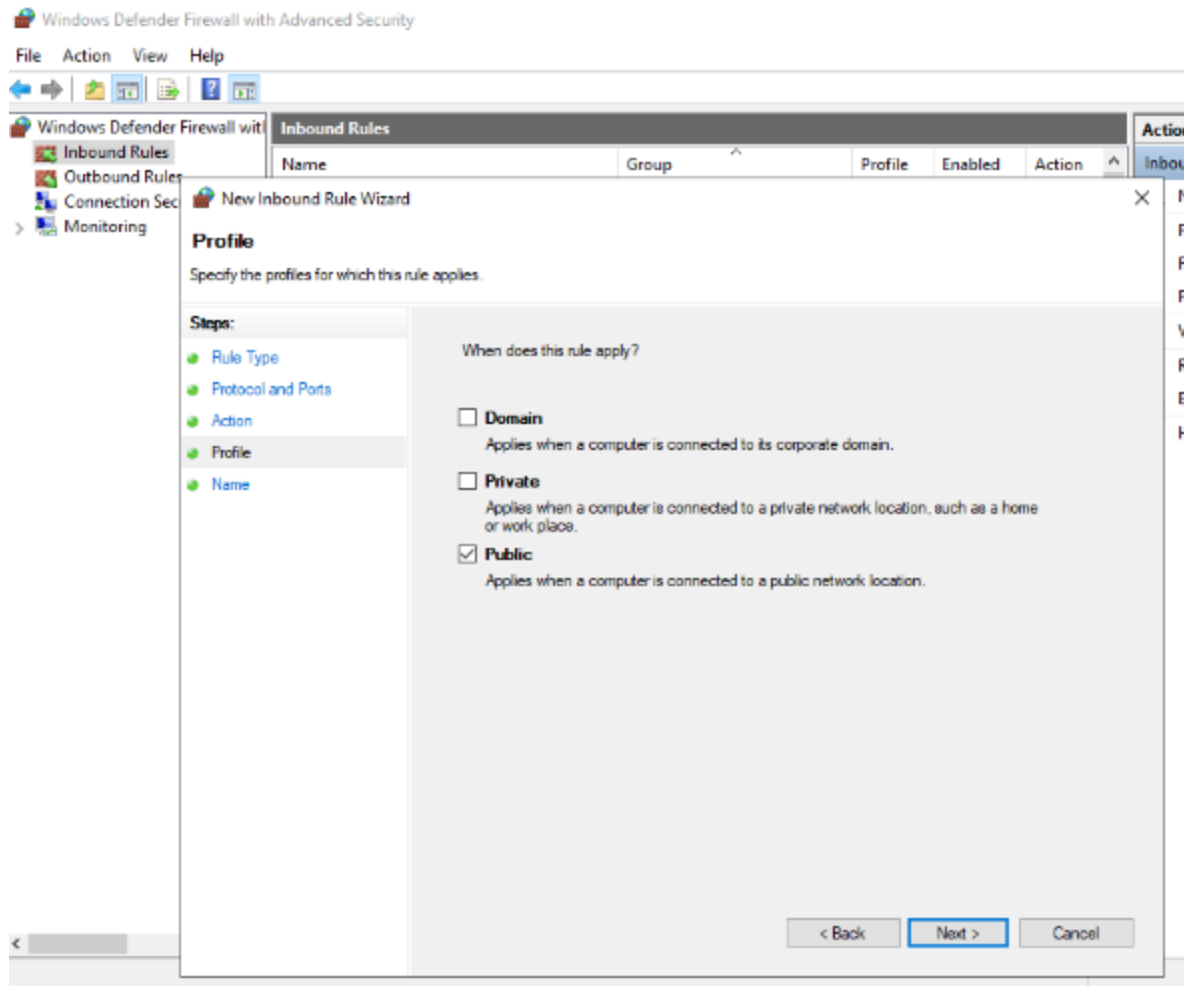
- Specify Port
 - Select TCP.
 - In **Specific local ports**, enter 3389 (the default port for Remote Desktop).
 - Click **Next**.



- Specify Action
 - Select **Block the connection**.
 - Click **Next**.

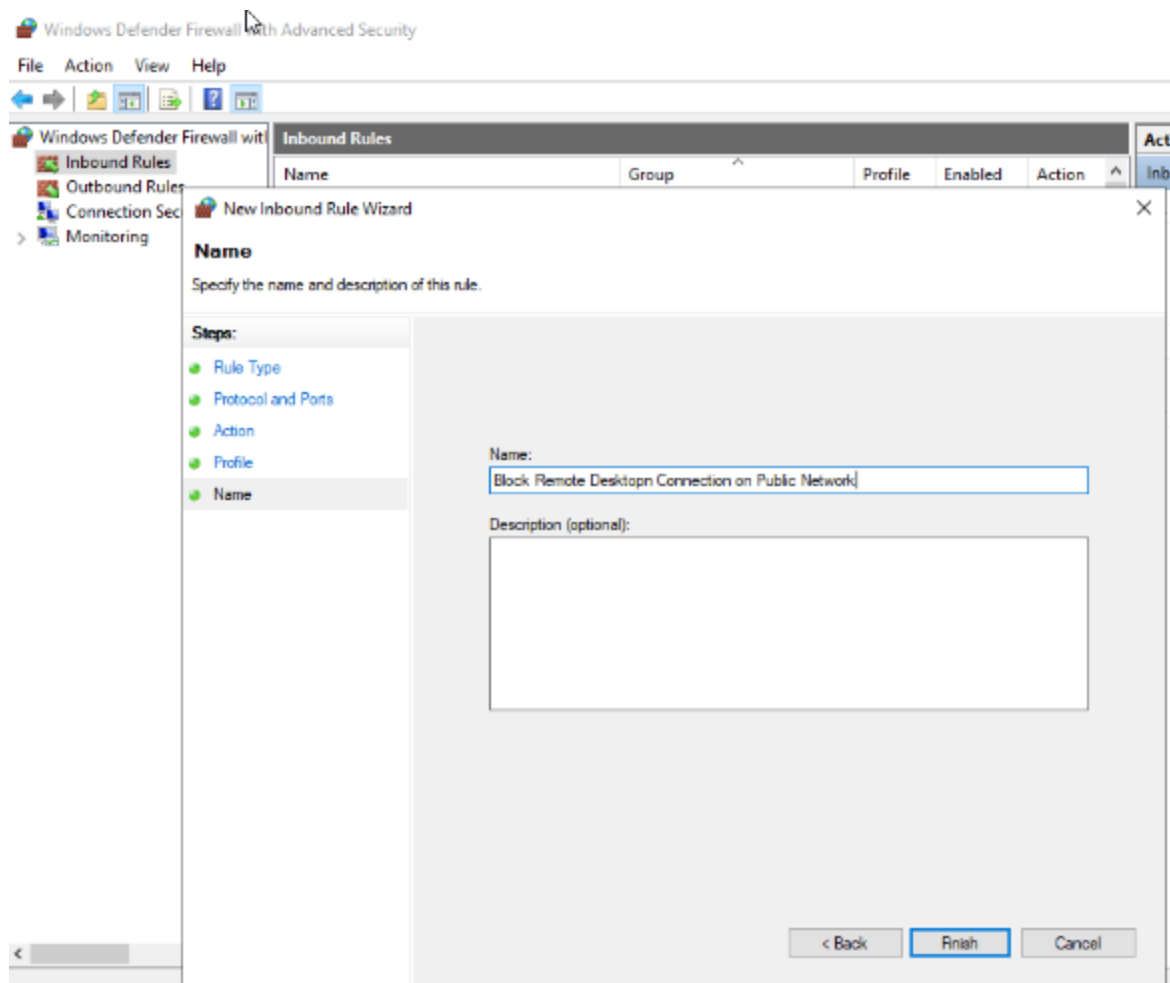


- Select Profile
 - Select only **Public**.
 - Deselect **Domain** and **Private**.
 - Click **Next**.

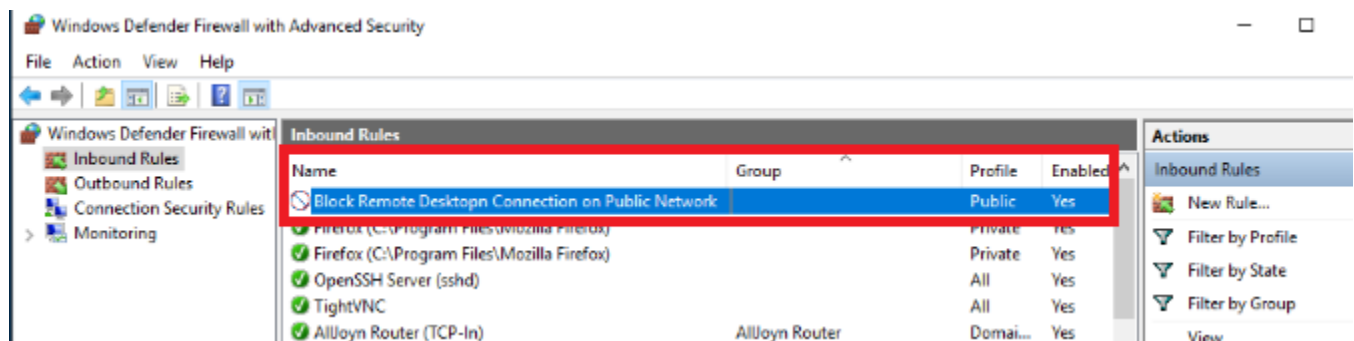


- Name the Rule

- Enter a name for the rule, such as '**Block Remote Desktop on Public Network**'.
- Optionally, provide a description.
- Click **Finish**.



- Verify the rule listed under Inbound Rules
 - Click **Inbound Rules** and verify the new rule **Enabled**. A red circle typically indicates that a rule is blocking traffic.

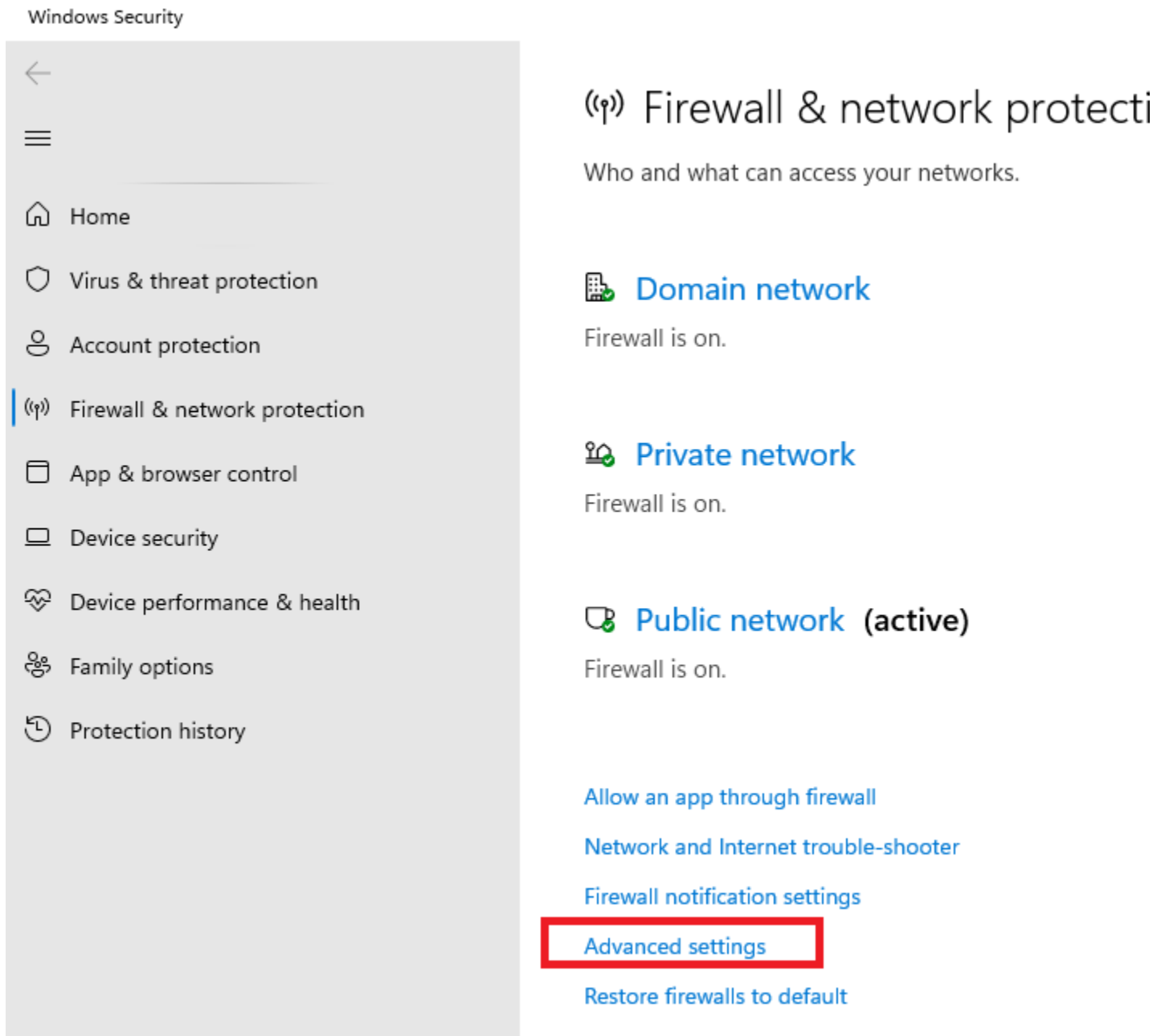


Scenario 2 - Block Outbound Traffic for Specified Applications (Outbound Rules)

Creating outbound rules to restrict applications from sending data over the internet can help enhance your system's security and control network traffic. Here are the steps to create such rules using Windows Defender Firewall with Advanced Security.

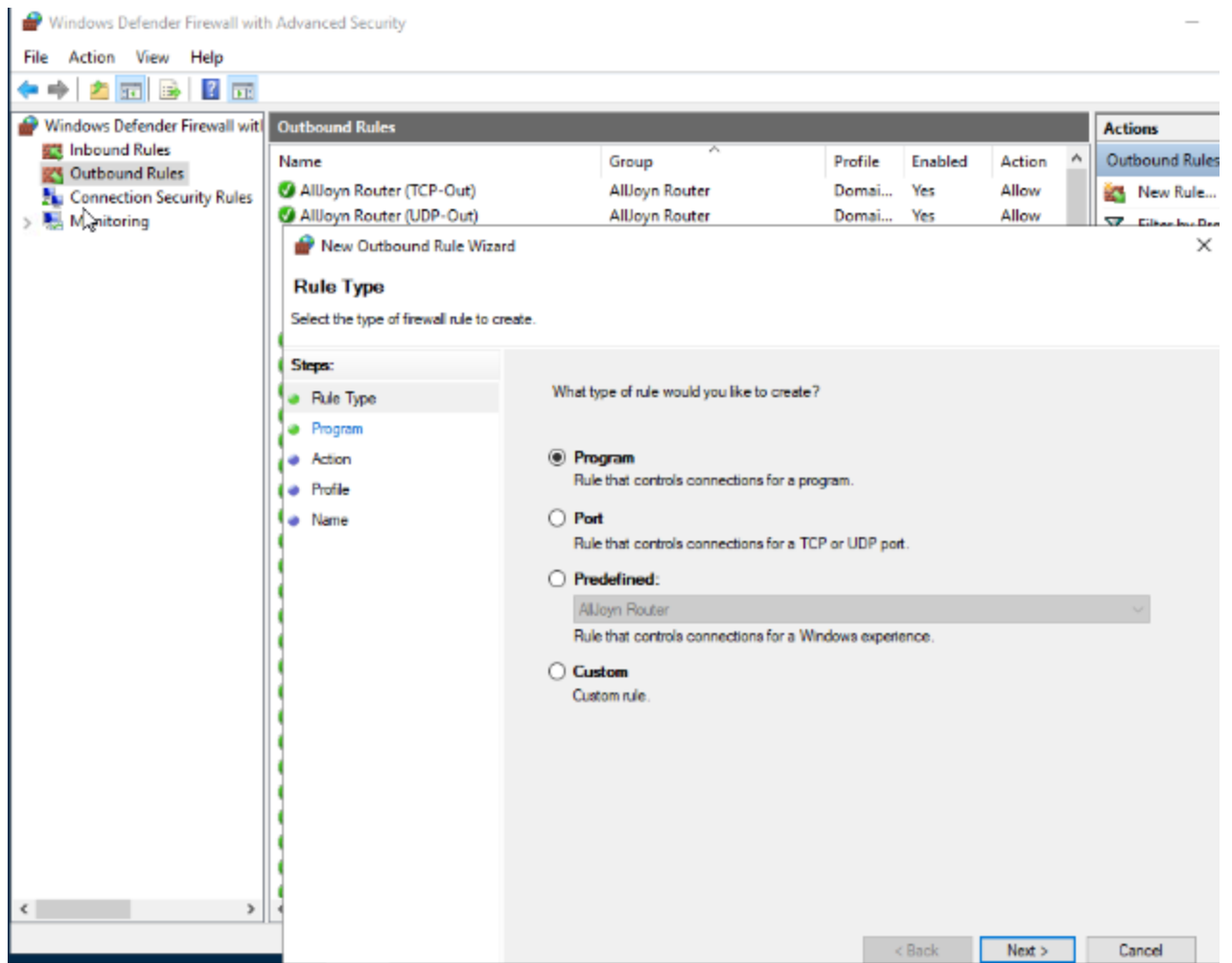
1. Open the Windows Defender Firewall with Advanced Security options

Follow steps in Scenario 1 to open the **Advanced Security** option window.

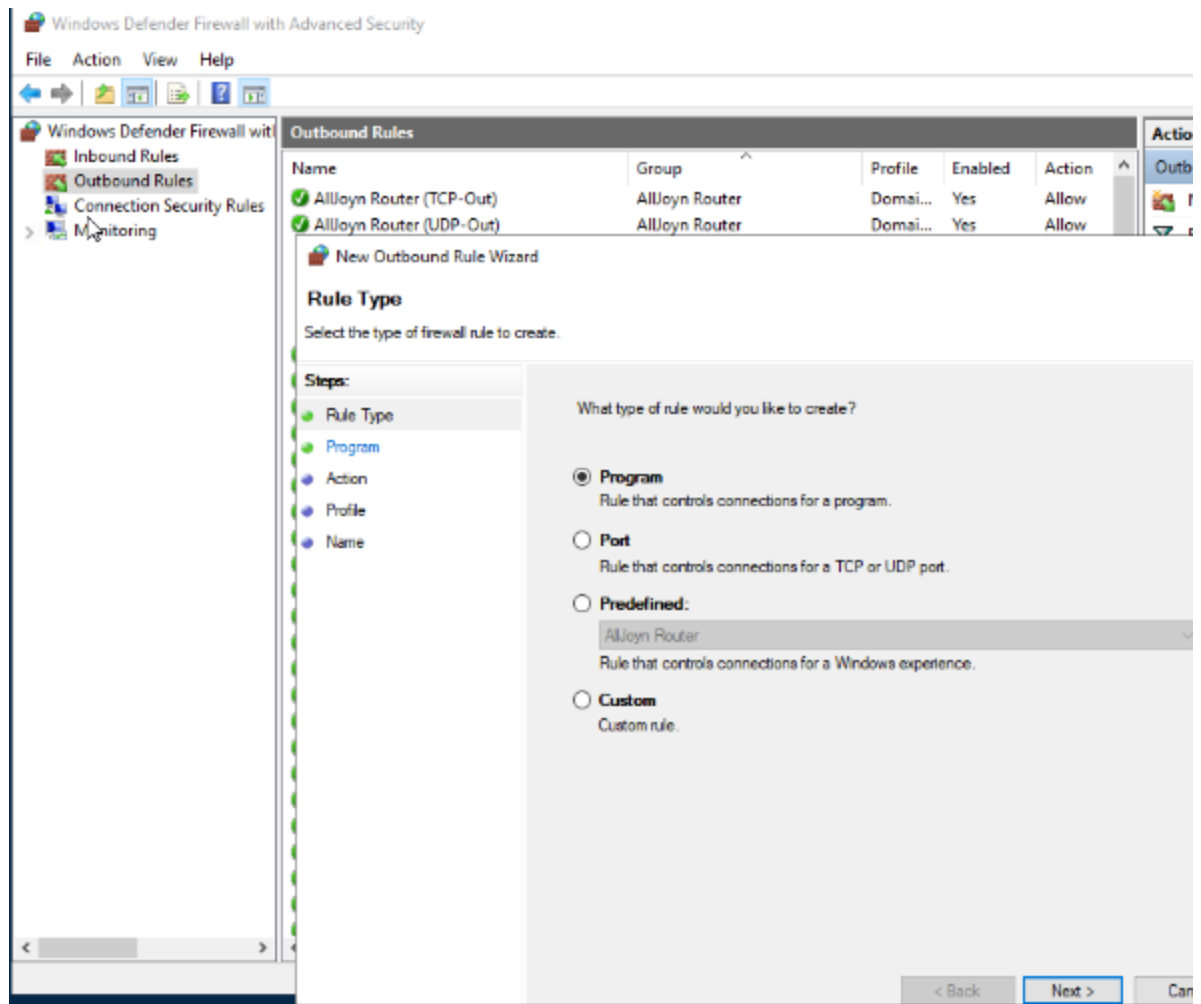


2. Select Outbound Rules and create a new Rule

- In the left pane, click on **Outbound Rules**.
- In the right pane, click on **New Rule....**

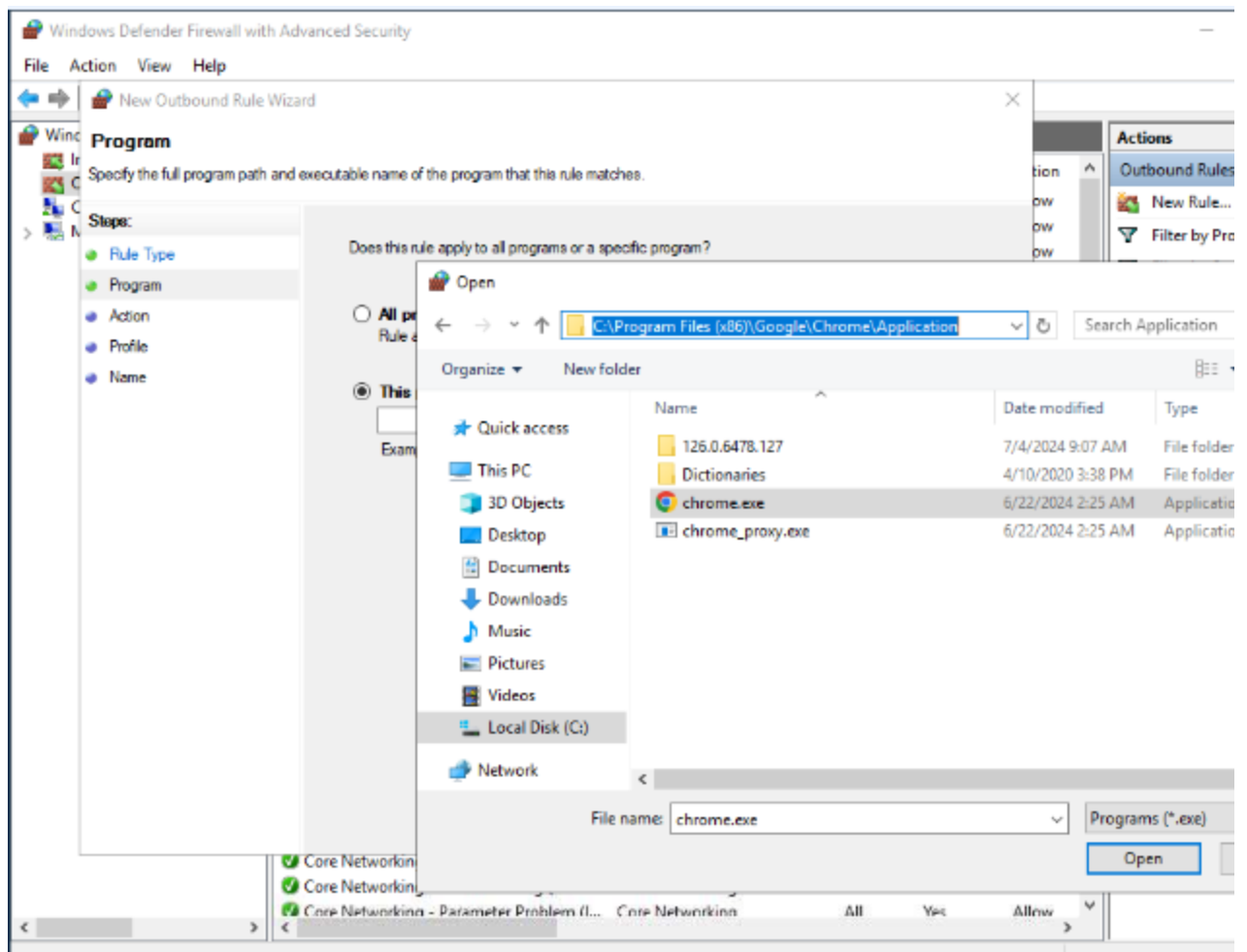


- Choose Rule Type
 - Select **Program** and click **Next**.

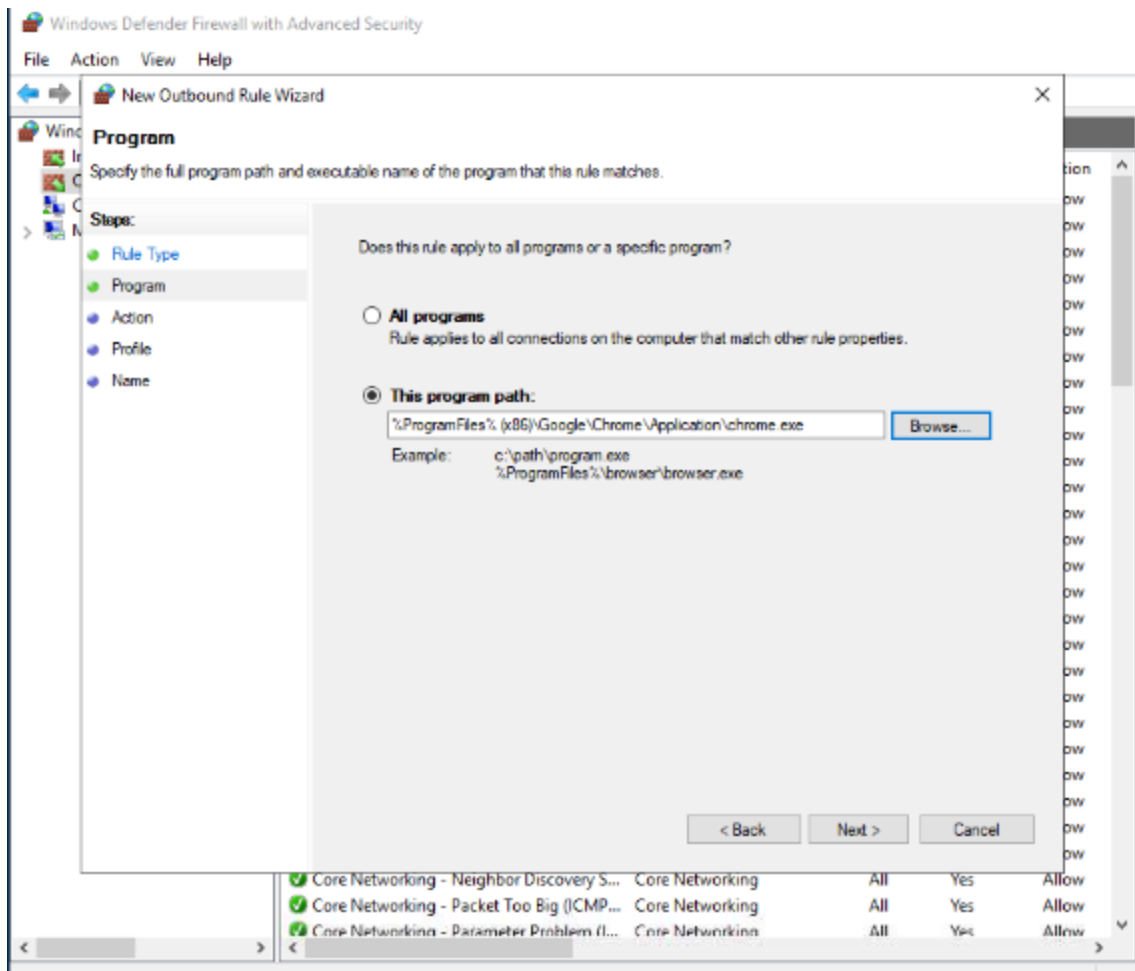


- Specify Program Path

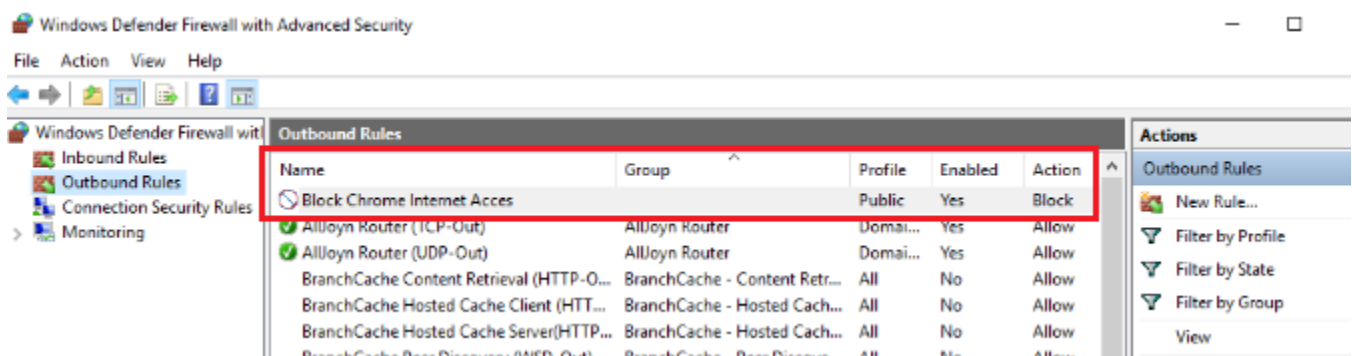
- Select **This program path:** and browse to the executable file of the application you want to block.
- For example, to block Google Chrome, you might navigate to C:\Program Files (x86)\Google\Chrome\Application\chrome.exe and click **Open**.



- Click Next.



- Select Action
 - Select **Block the connection** and click **Next**.
- Specify Profile
 - Choose when the rule applies: **Domain, Private, and Public**.
 - Check all profiles if you want the rule to apply in all scenarios.
 - Click **Next**.
- Name the Rule
 - Give the rule a name (e.g., “Block Chrome Internet Access”) and an optional description.
 - Click **Finish**.



- Verify the Rule
 - Open Chrome browser and try to browse internet. - You will not be able to access internet through the browser. This confirms that Rule is working.
 - If you go back to Outbound Rules setting and disable the Rule “Block Chrome Internet Access”, you will be able to browse internet on Chrome browser again.

Scenario 3 (Inbound Rules) - Block Web Server (HTTP) Traffic on a Public Network

Blocking HTTP traffic to your computer when connected to a public network ensures that no web server services are exposed to potential threats.

This rule will block all incoming HTTP traffic (port 80) when your computer is connected to a public network. This helps to secure your system by preventing potential web server attacks or unauthorized access through HTTP.

1. Open the Windows Defender Firewall with Advanced Security options

Follow steps in Scenario 1 to open the **Advanced Security** option window.

2. Disable File and Printer Sharing Rules

- In the left pane, click on **Inbound Rules**.
- In the right pane, click on **New Rule**
- Choose **Port** and click **Next**.
- Specify Ports:
 - Select **TCP**.
 - In Specific local ports, enter **80** (the default port for HTTP).
 - Click **Next**.
- Specify Action:
 - Select **Block the connection**.
 - Click **Next**.
- Specify Network Profile:
 - Check only the **Public** option.
 - Uncheck **Domain** and **Private**.
 - Click **Next**.
- Name the Rule:
 - Enter a name for the rule, such as “**Block HTTP on Public Network**”.
 - Add a description if desired.

- Click **Finish**.

Scenario 4 (Inbound Rules) - Allow Key Management Service on the Domain and Private network, and deny the connection on the Public network

A KMS is used to activate Microsoft products (such as Windows and Office) within an organization without requiring each machine to connect directly to Microsoft for activation.

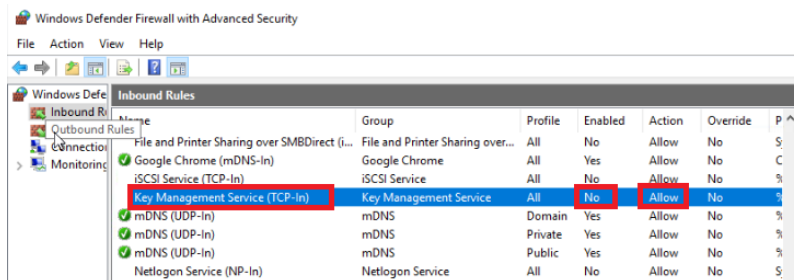
1. Open the Windows Defender Firewall with Advanced Security options

Follow steps in Scenario 1 to open the **Advanced Security** option window.

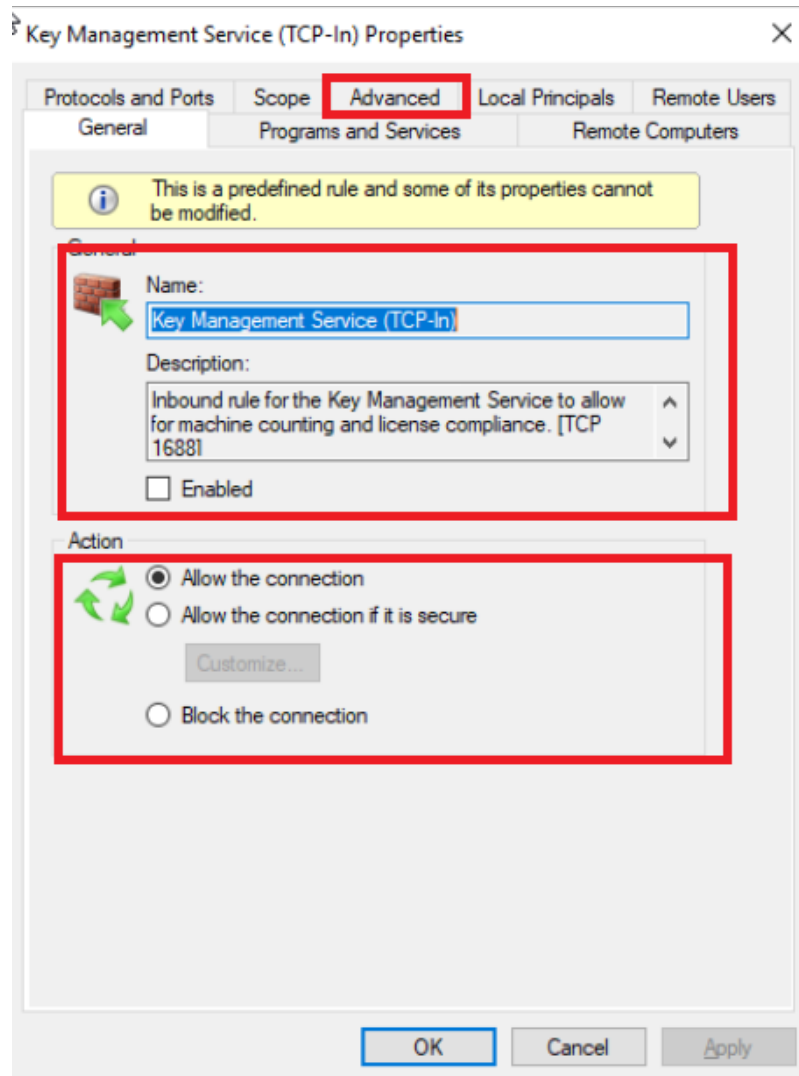
2. Scroll to the **Key Management Service** inbound rule in the Overview panel of **Windows Defender Firewall with Advanced Security**. Note the following:

- The policy is currently not enabled (the **Enabled** column says **No**.)
- If enabled, the rule would allow communication (the **Action** column says **Allow**.)

Double-click this rule.



3. Here you will see the details of this rule. You will note that the **General** tab includes the name of the rule, a description of the rule, and whether the rule has been allowed or blocked. In this case, the connection is allowed. Click the **Advanced** tab.



4. Here you will see which profiles the rule applies to. In this case, **Domain**, **Private** and **Public** are all selected.

Key Management Service (TCP-In) Properties



General Programs and Services Remote Computers
Protocols and Ports Scope **Advanced** Local Principals Remote Users

Profiles

Specify profiles to which this rule applies.

☒ Domain
☒ Private
☒ Public

Interface types

Specify the interface types to which this rule applies. [Customize...](#)

Edge traversal

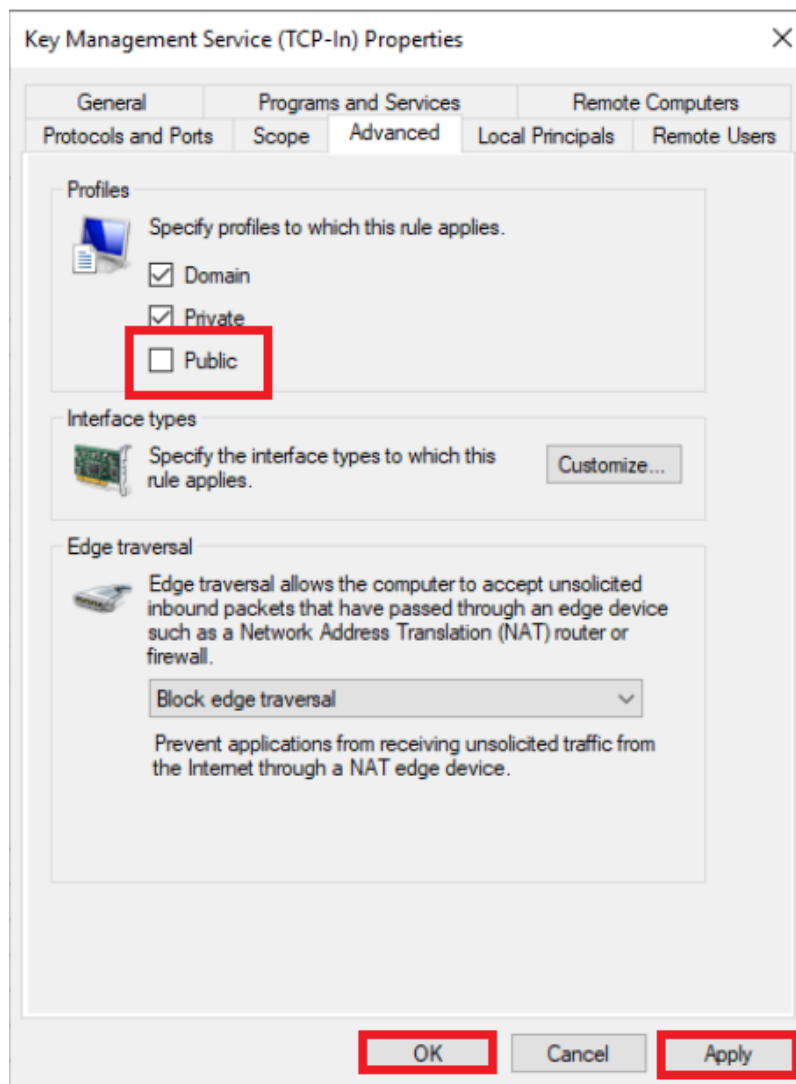
Edge traversal allows the computer to accept unsolicited inbound packets that have passed through an edge device such as a Network Address Translation (NAT) router or firewall.

Block edge traversal

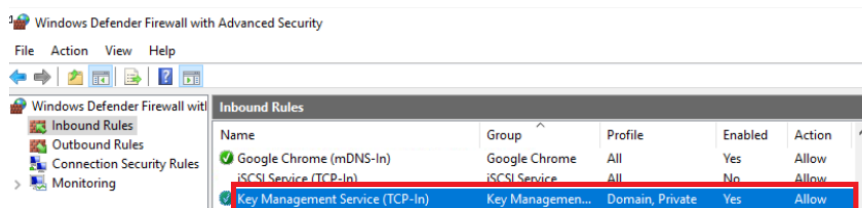
Prevent applications from receiving unsolicited traffic from the Internet through a NAT edge device.

[OK](#) [Cancel](#) [Apply](#)

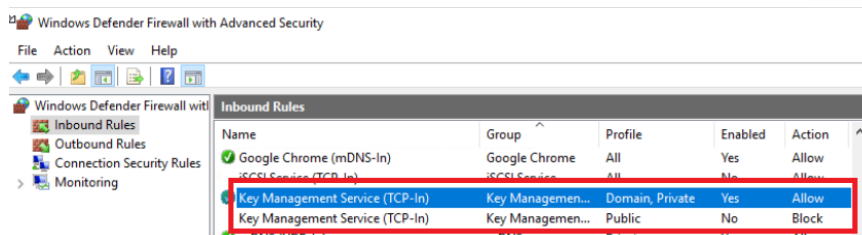
5. Because we want to allow communication only with the domain and private networks, For **Public** this box should not have a checkmark. Next, click **Apply**, then click **Ok**.



6. Now we will create an inbound rule that blocks communication with the public network. Since the new rule will be similar to the last, we will copy the existing rule. Right-click the **Key Management Service (TCP-In)** inbound rule and click **Copy**. Press **Ctrl+V** to paste.

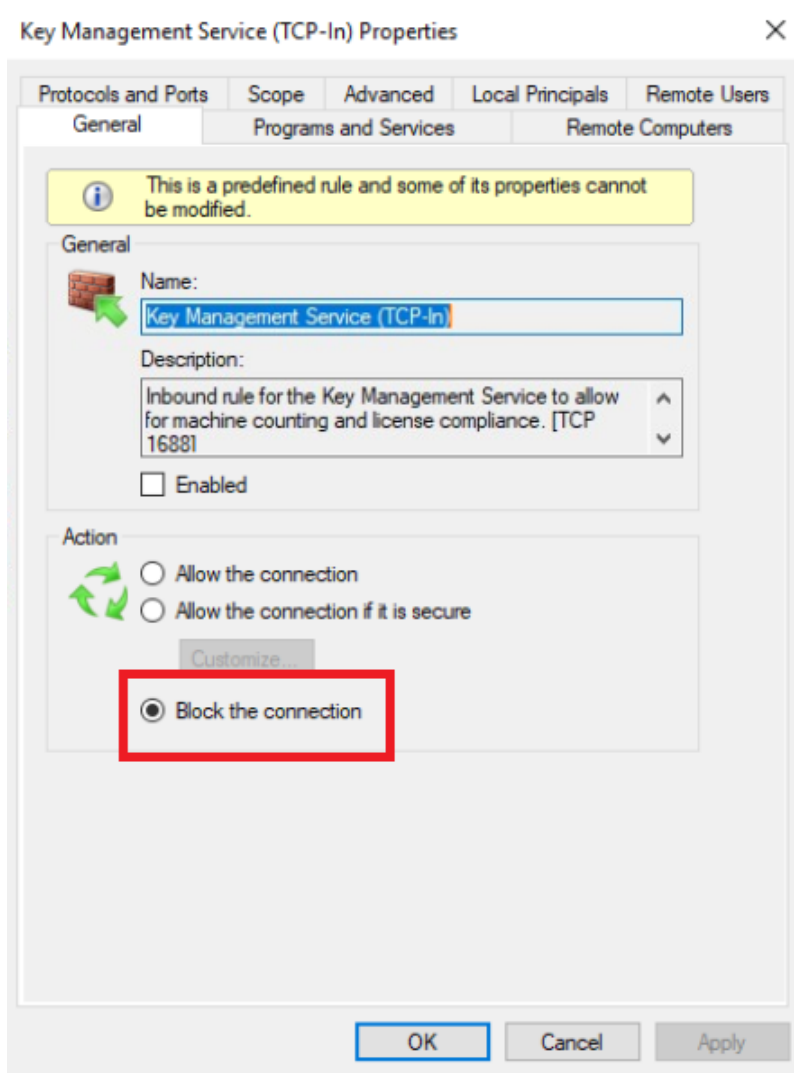


7. You will now see a second **Key Management Service (TCP-In)** inbound rule. Double-click the second rule to open the ****Key Management Service *TCP-IN) Properties**.

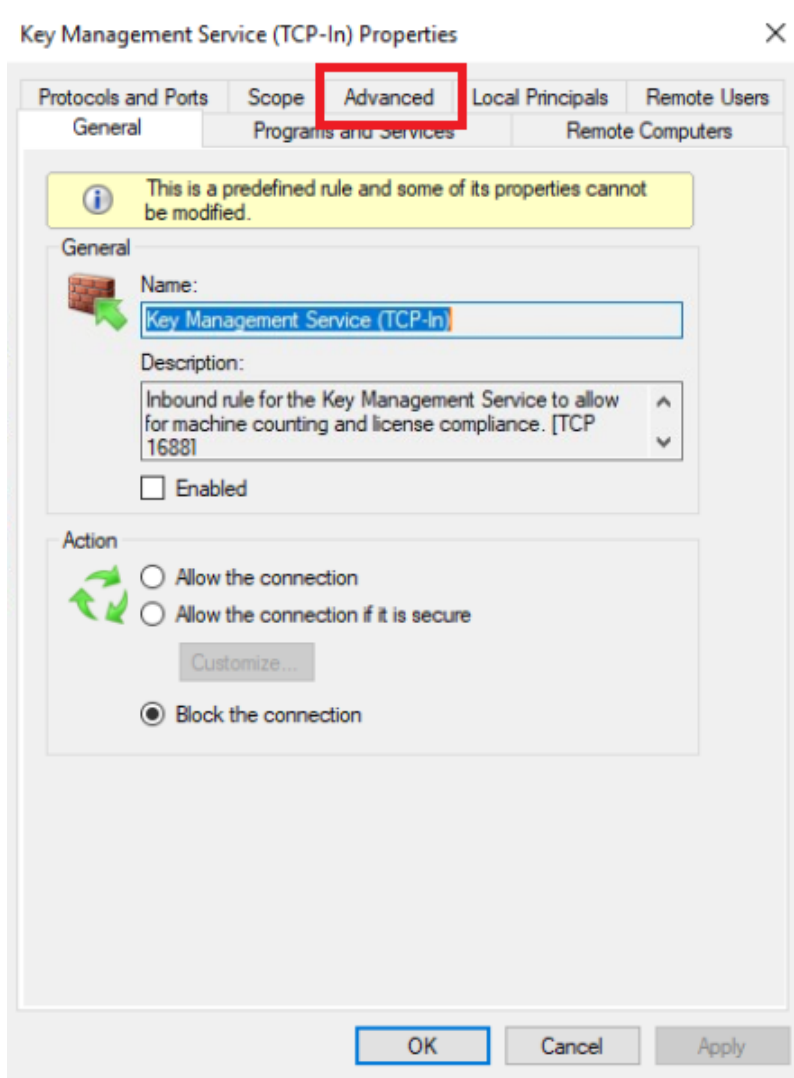


8. Since we want to block connection with the public network, select **Block the connection** on the

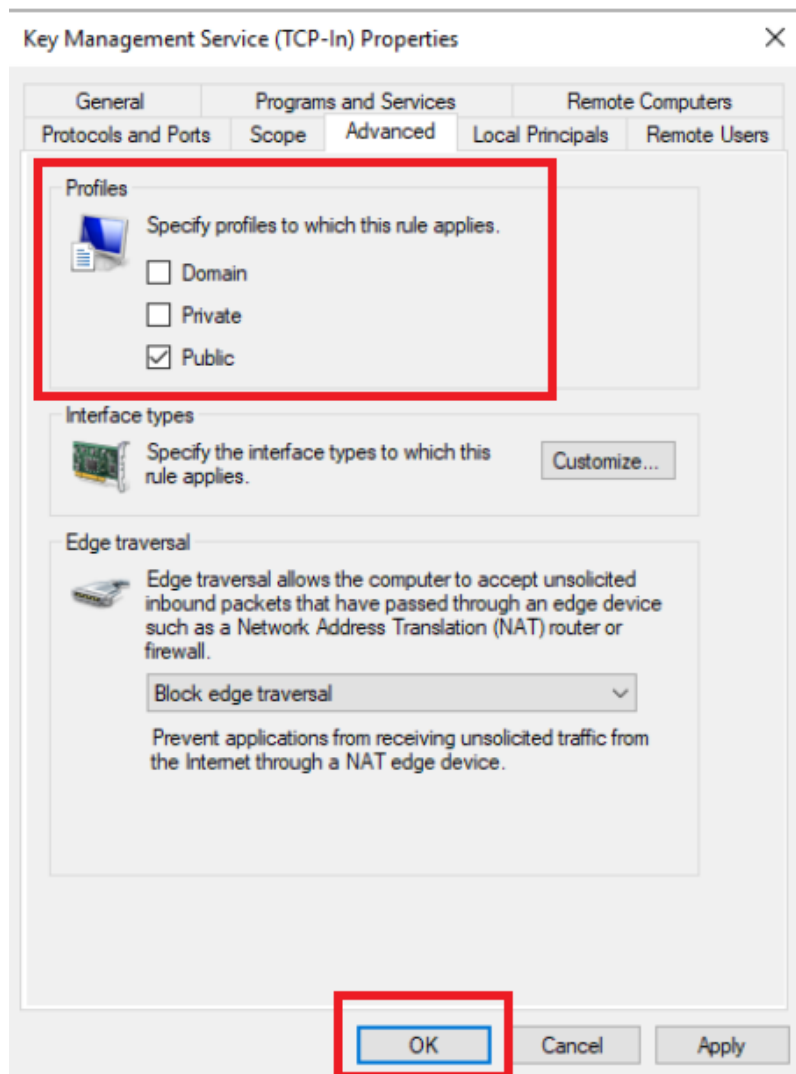
General tab. Click **Apply**.



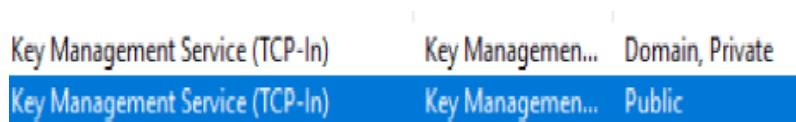
9. Click the **Advanced** tab.



10. Click the **Domain** and **Private** boxes to remove the checkmarks. Click the **Public** to add the checkmark. Click **Ok**.



11. The Overview panel will show your changes. Right-click each **Key Management Service (TCP-In)** rule and click **Enable rule**.



12. Now you will see that a green checkmark appears next to the first rule indicating that the rule allowing communication is enabled. A circle with a line through it appears next to the second rule indicating that the rule blocking communication is enabled.

| Inbound Rules | | | | |
|-----------------------------------|------------------|-----------------|---------|--------|
| Name | Group | Profile | Enabled | Action |
| ✓ Key Management Service (TCP-In) | Key Managemen... | Domain, Private | Yes | Allow |
| ⊗ Key Management Service (TCP-In) | Key Managemen... | Public | Yes | Block |

Congratulations! This concludes the different aspects of using Windows Firewall to enhance your network security.

Author(s)

Shilpa Giridhar



Skills Network