Windows Firewall with Advanced Security

Objectives

By completing this project, 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 practical guide, 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 guide, you will also explore few typical use cases:

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

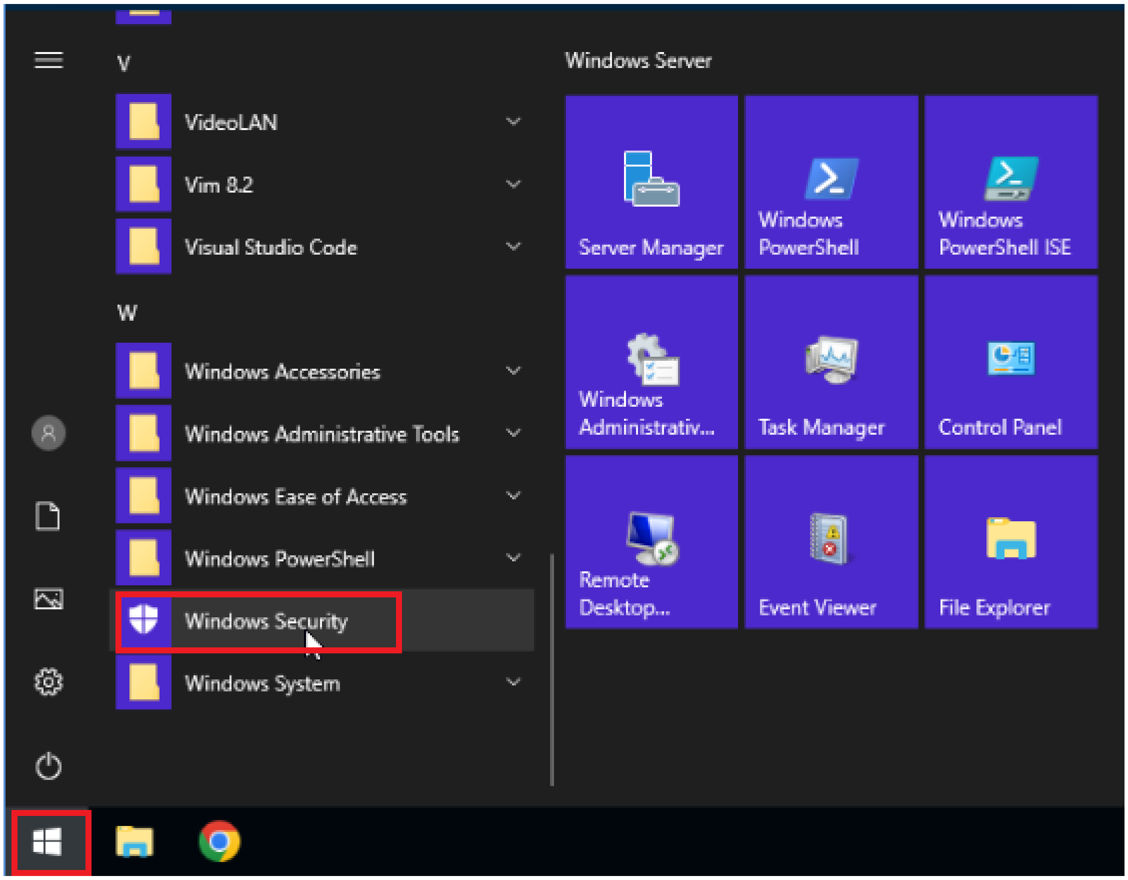
- Scenario 1: Blocking Remote Desktop on the Public Network (Inbound Rules)
- Scenario 2: Blocking Outbound Traffic for Specified Applications (Outbound Rules)
- Scenario 3: Block Web Server (HTTP) Traffic on a Public Network (Inbound Rules)
- Scenario 4: Allow Key Management Service on the Domain and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

Enable firewall

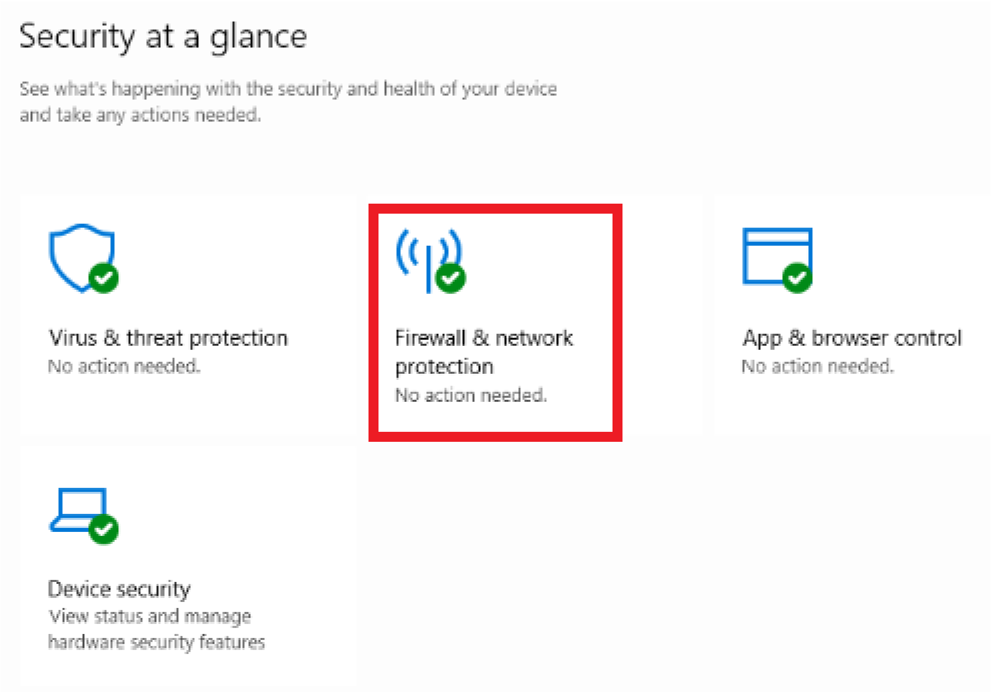
Exercise 1: Enable Firewall on different Network Profiles

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**.



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

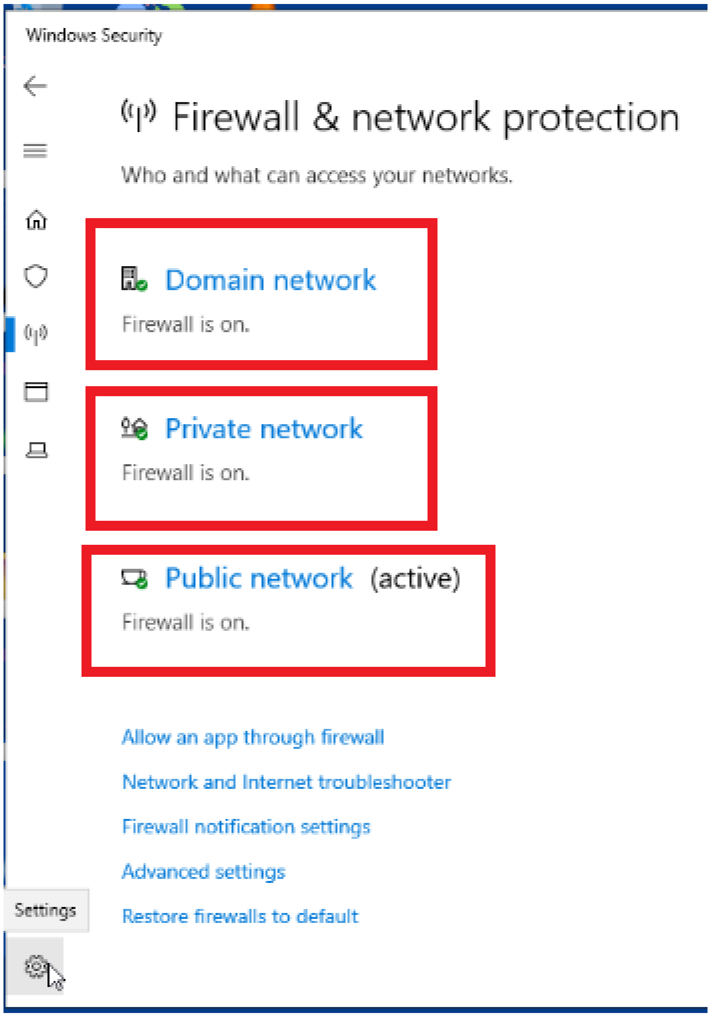
Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features

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.



Windows Security
Settings

Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

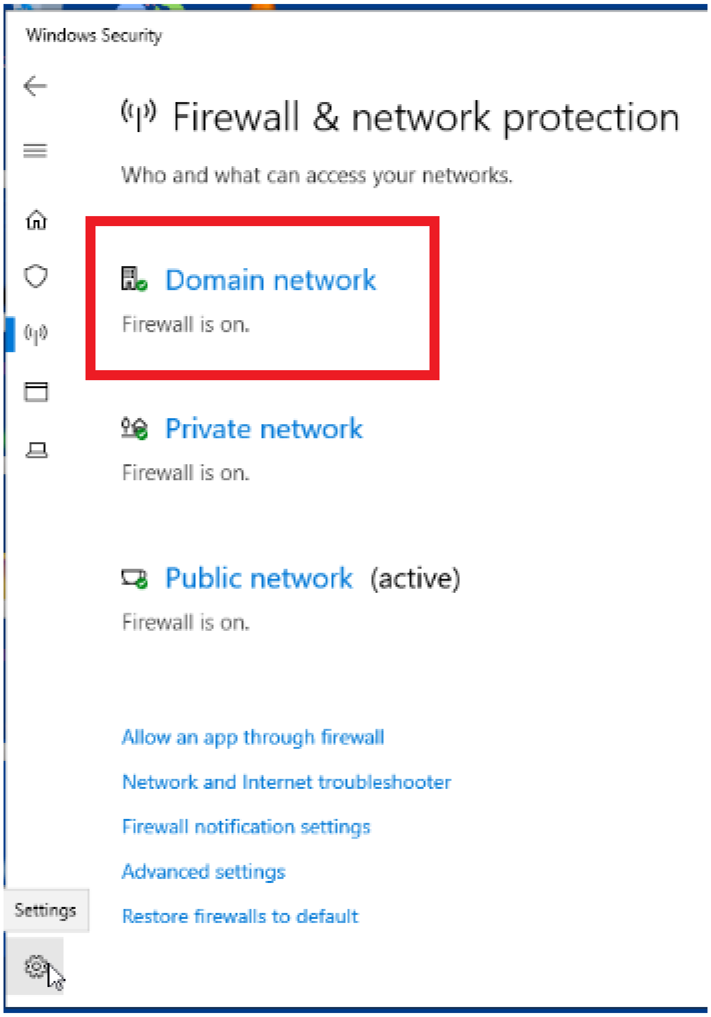
Firewall is on.

Public network (active)

Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

4. Click **Domain network**.



Windows Security

Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

Firewall is on.

Public network (active)

Firewall is on.

Allow an app through firewall

Network and Internet troubleshooter

Firewall notification settings

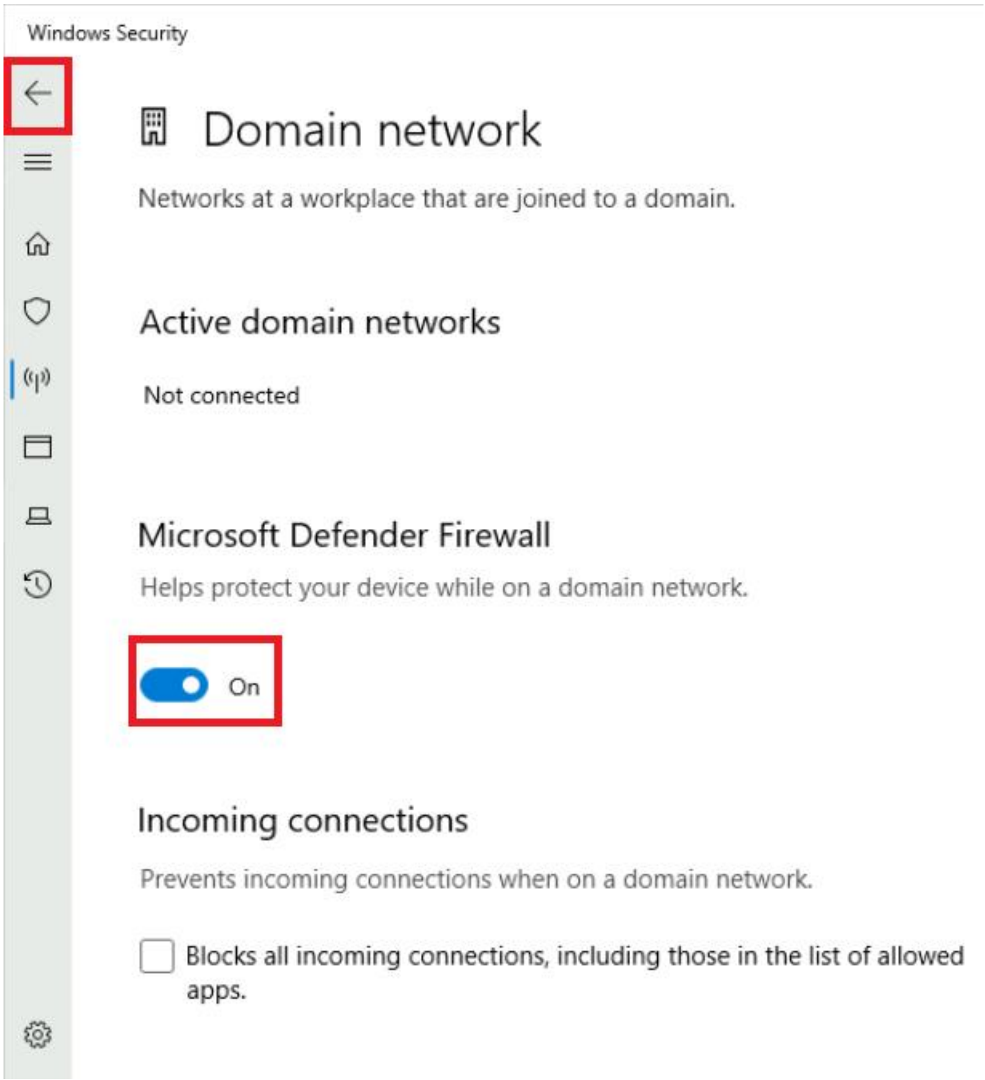
Advanced settings

Restore firewalls to default

5. Verify that the Microsoft 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.

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



Windows Security

Domain network

Networks at a workplace that are joined to a domain.

Active domain networks

Not connected

Microsoft Defender Firewall

Helps protect your device while on a domain network.

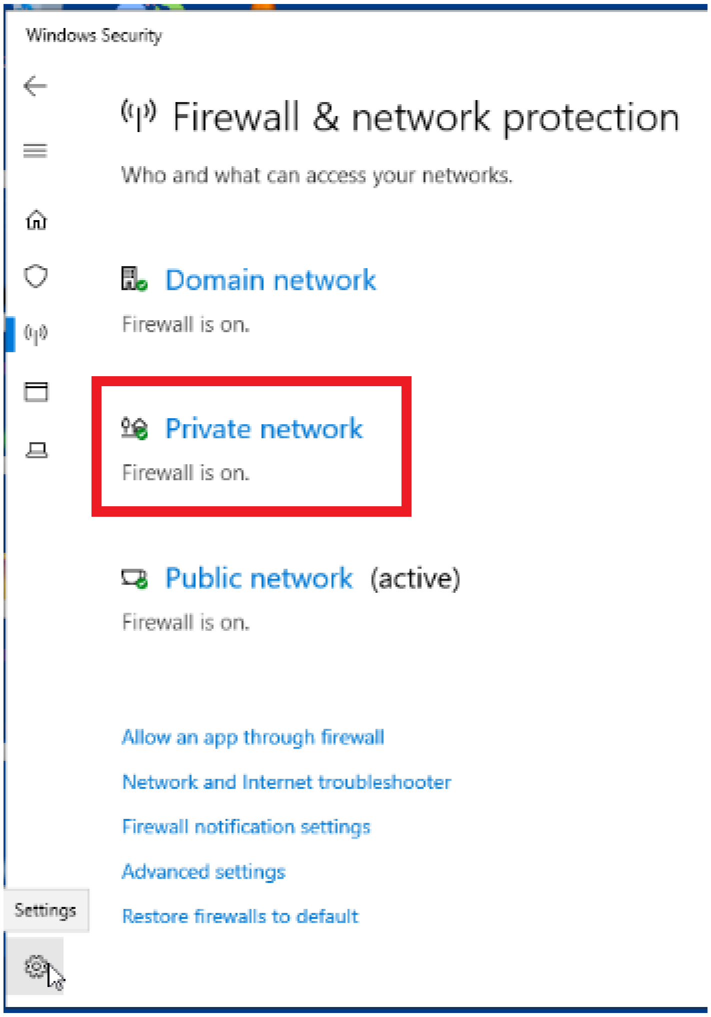
● On

Incoming connections

Prevents incoming connections when on a domain network.

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

6. Click **Private network**.



Windows Security
Settings
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

Firewall & network protection

Who and what can access your networks.

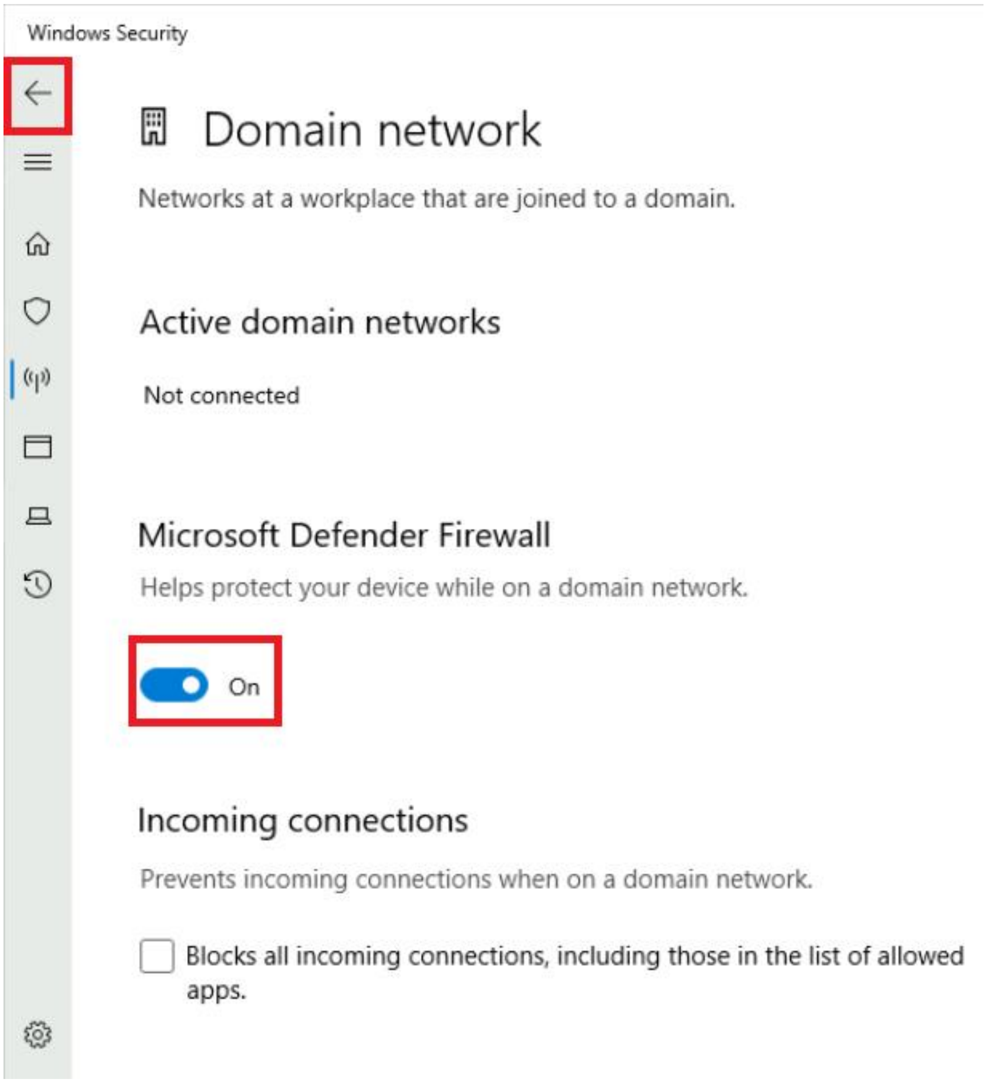
Domain network
Firewall is on.

Private network
Firewall is on.

Public network (active)
Firewall is on.

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

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



Windows Security

Domain network

Networks at a workplace that are joined to a domain.

Active domain networks

Not connected

Microsoft Defender Firewall

Helps protect your device while on a domain network.

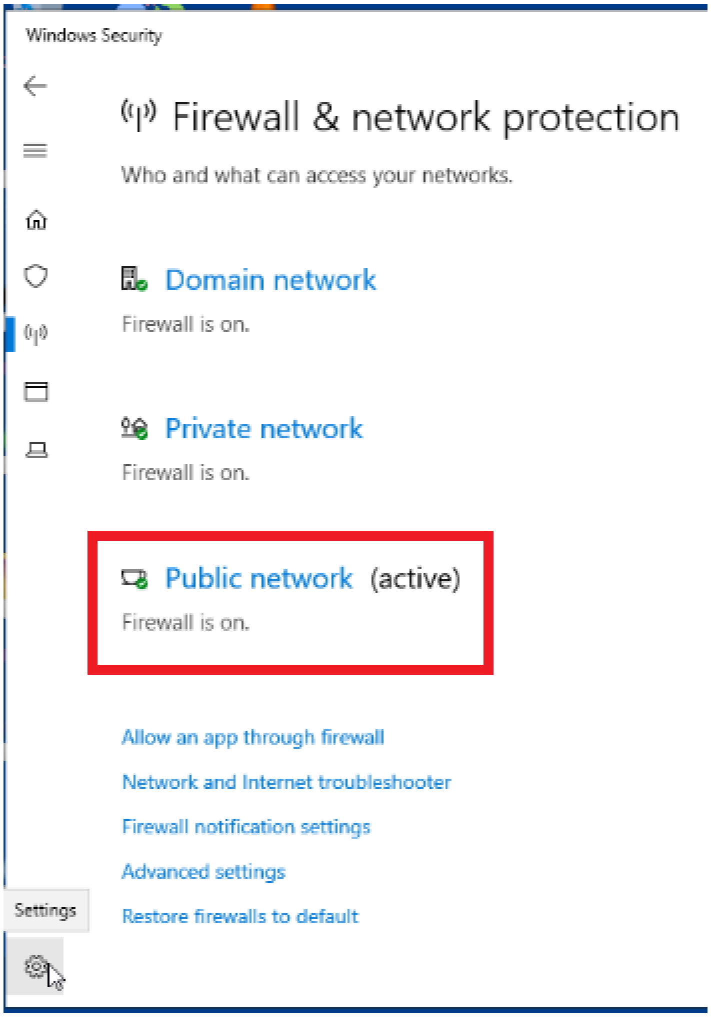
On

Incoming connections

Prevents incoming connections when on a domain network.

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

8. Click **Public network**.



Windows Security

Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

Firewall is on.

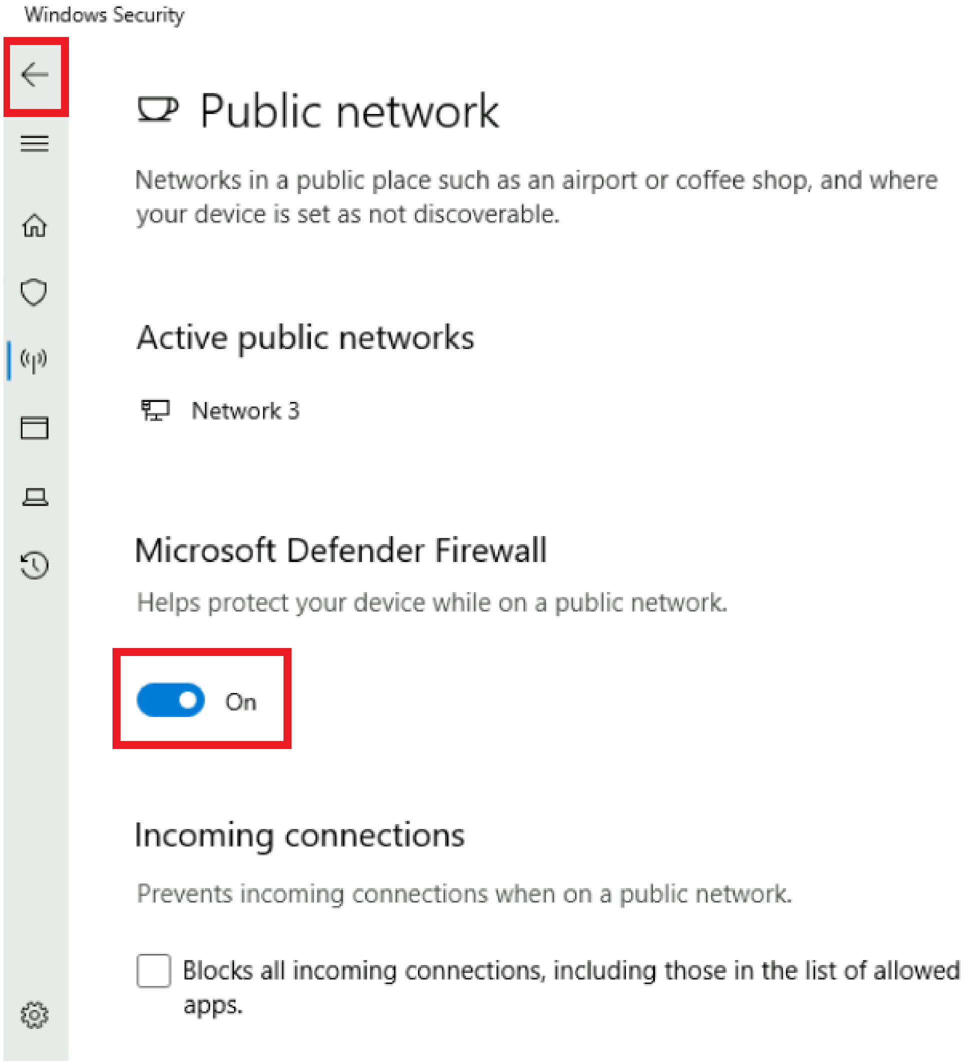
Public network (active)

Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default
Settings

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

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



Windows Security

Public network

Networks in a public place such as an airport or coffee shop, and where your device is set as not discoverable.

Active public networks

Network 3

Microsoft Defender Firewall

Helps protect your device while on a public network.

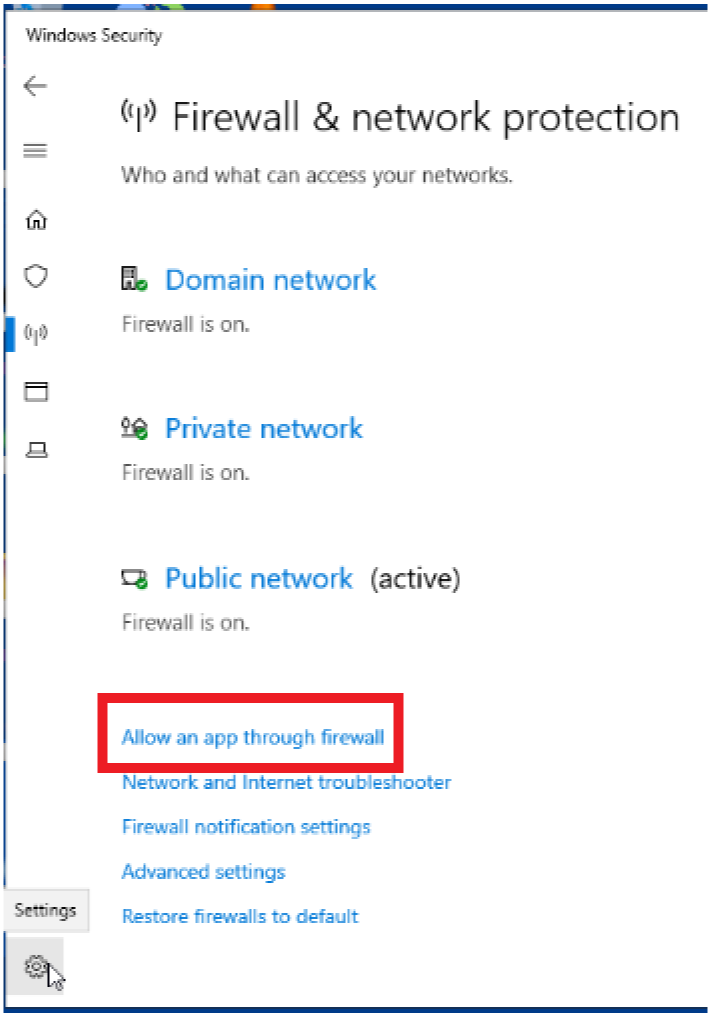
On

Incoming connections

Prevents incoming connections when on a public network.

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

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



Windows Security

Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

Firewall is on.

Public network (active)

Firewall is on.

Allow an app through firewall

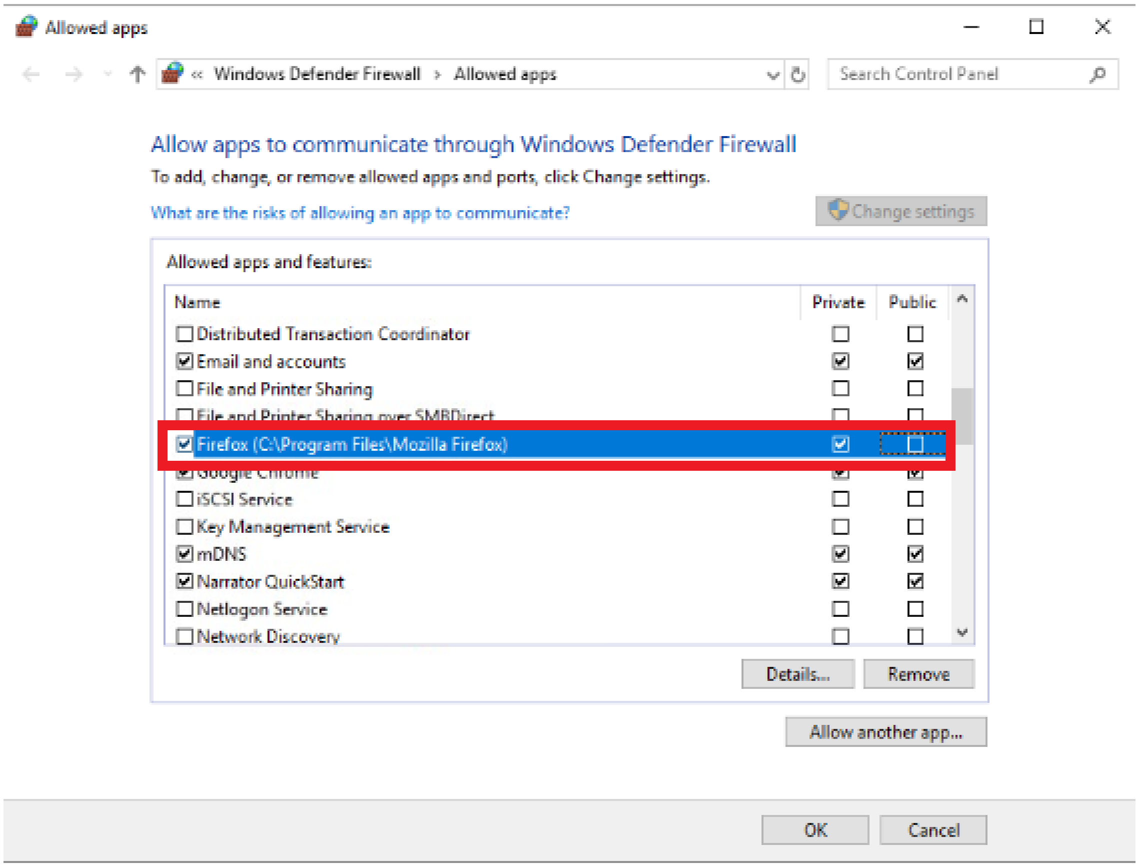
Network and Internet troubleshooter

Firewall notification settings

Advanced settings

Restore firewalls to default

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.



Allow apps to communicate through Windows Defender Firewall

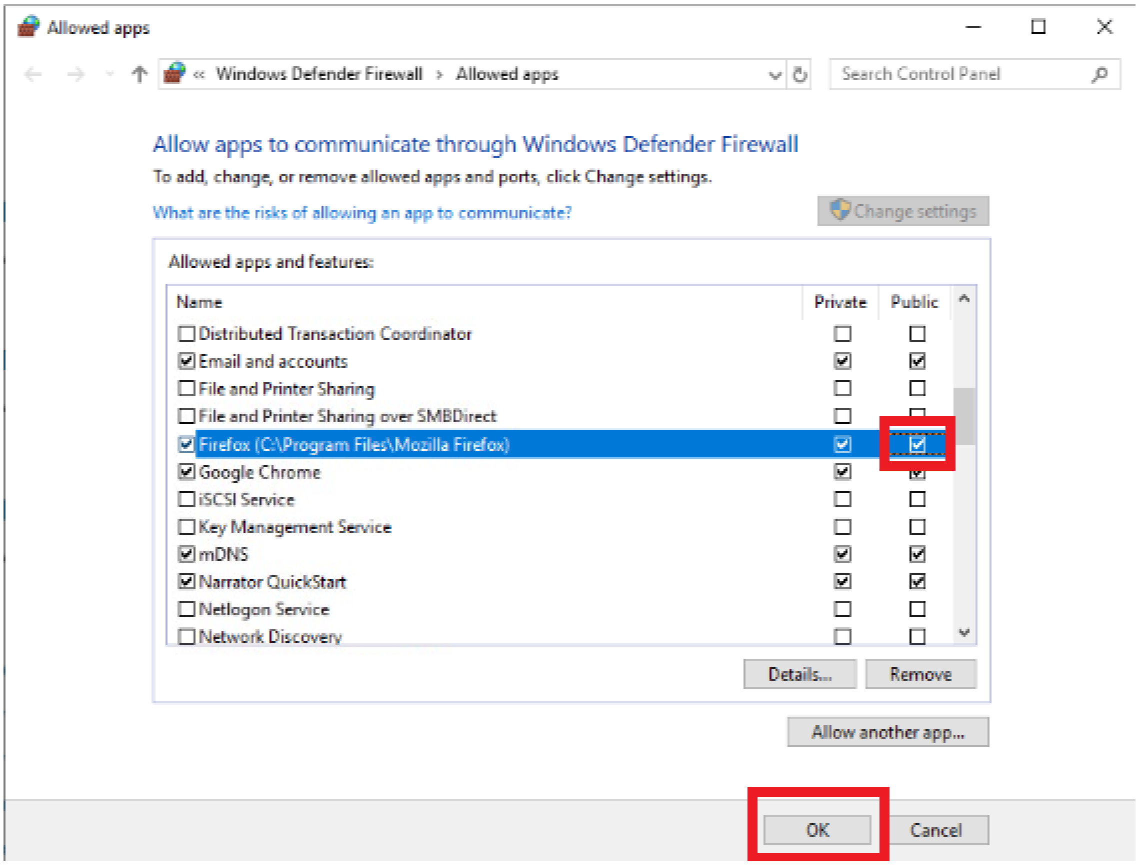
To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☐ Distributed Transaction Coordinator	☐	☐
☑ Email and accounts	☑	☑
☐ File and Printer Sharing	☐	☐
☐ File and Printer Sharing over SMBDirect	☐	☐
☑ Firefox (C:\Program Files\Mozilla Firefox)	☑	☐
☑ Google Chrome	☑	☑
☐ iSCSI Service	☐	☐
☐ Key Management Service	☐	☐
☑ mDNS	☑	☑
☑ Narrator QuickStart	☑	☑
☐ Netlogon Service	☐	☐
☐ Network Discovery	☐	☐

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.



Allow apps to communicate through Windows Defender 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
☐ Distributed Transaction Coordinator	☐	☐
☑ Email and accounts	☑	☑
☐ File and Printer Sharing	☐	☐
☐ File and Printer Sharing over SMBDirect	☐	☐
☑ Firefox (C:\Program Files\Mozilla Firefox)	☑	☑
☑ Google Chrome	☑	☑
☐ iSCSI Service	☐	☐
☐ Key Management Service	☐	☐
☑ mDNS	☑	☑
☑ Narrator QuickStart	☑	☑
☐ Netlogon Service	☐	☐
☐ Network Discovery	☐	☐

Typical use cases with Windows Firewall Advanced Security options

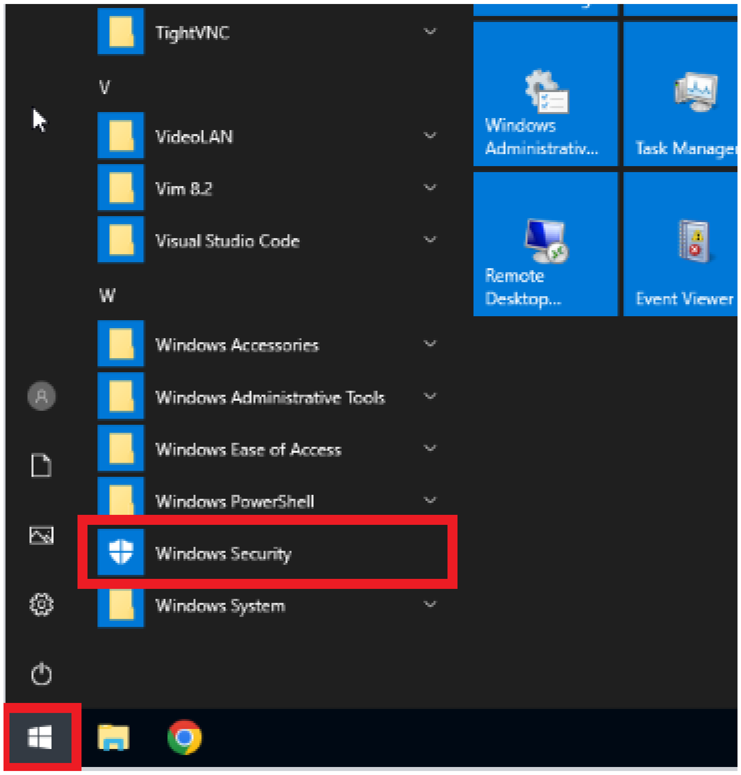
The first part is based in the consumer-friendly version of Windows Defender Firewall – a simplified interface ideal for a single device in a home setting. In this exercise, we will look at Windows Defender Firewall with Advanced Security. This advanced view provides more in-depth options for configuration.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

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

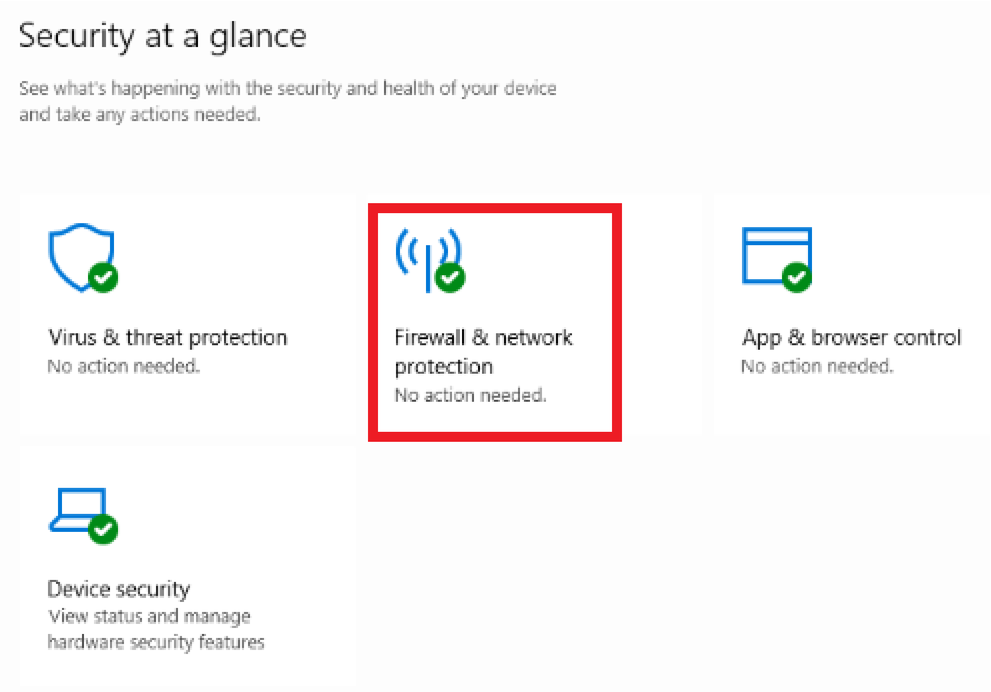
The Remote Desktop feature in Windows allows you to connect to and control a computer from a remote location. This can be particularly useful for accessing your work computer from home, assisting others with technical issues, or managing servers.

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



b. Click **Firewall & network protection**.



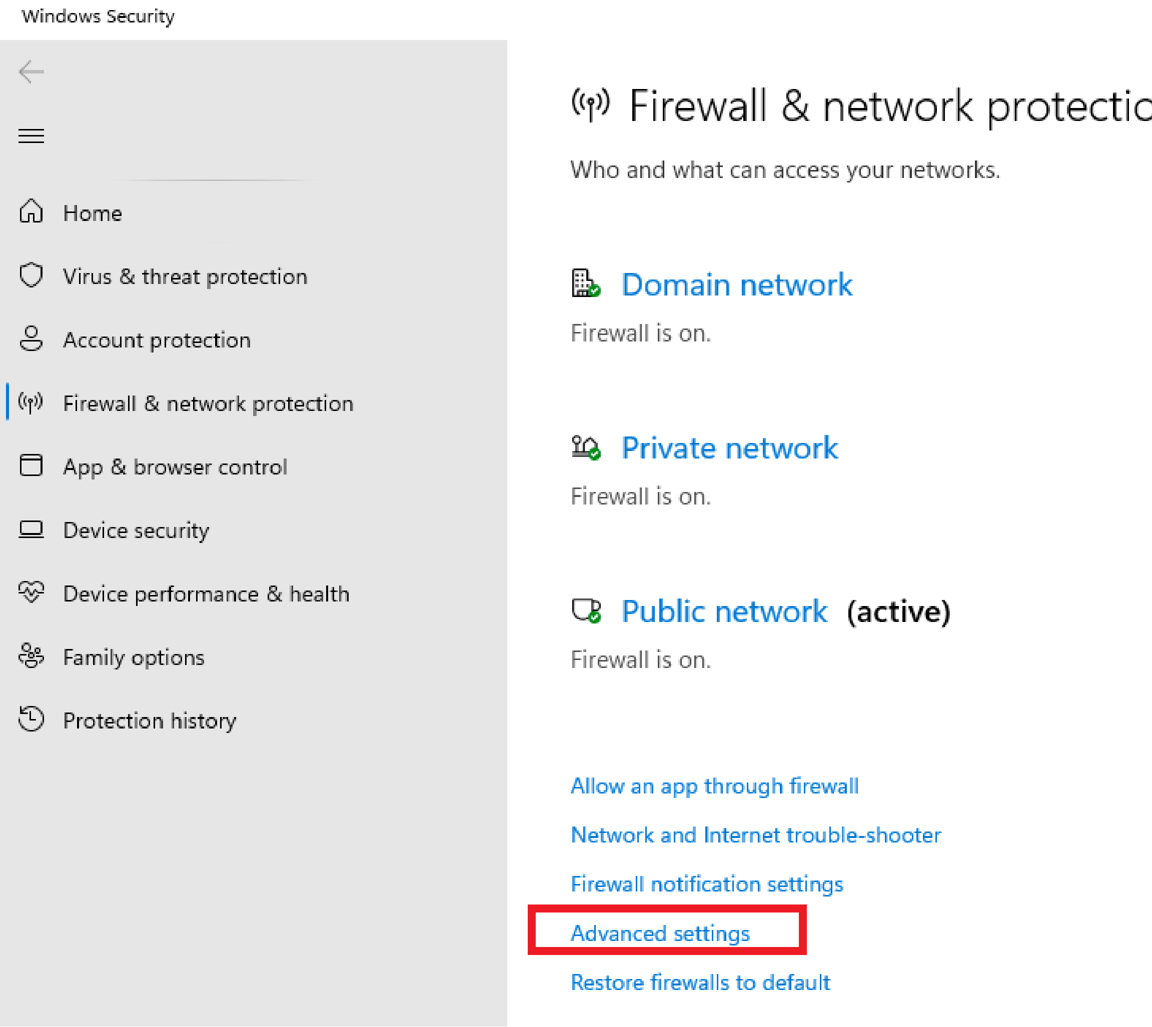
Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.
Firewall & network protection
No action needed.
App & browser control
No action needed.
Device security
View status and manage hardware security features

c. Open Windows Firewall Advanced Settings

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


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Firewall & network protectic
Domain network
Private network
Public network (active)
Allow an app through firewall
Network and Internet trouble-shooter
Firewall notification settings
Advanced settings
Restore firewalls to default

Who and what can access your networks.

Firewall is on.

Firewall is on.

Firewall is on.

ii. 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:

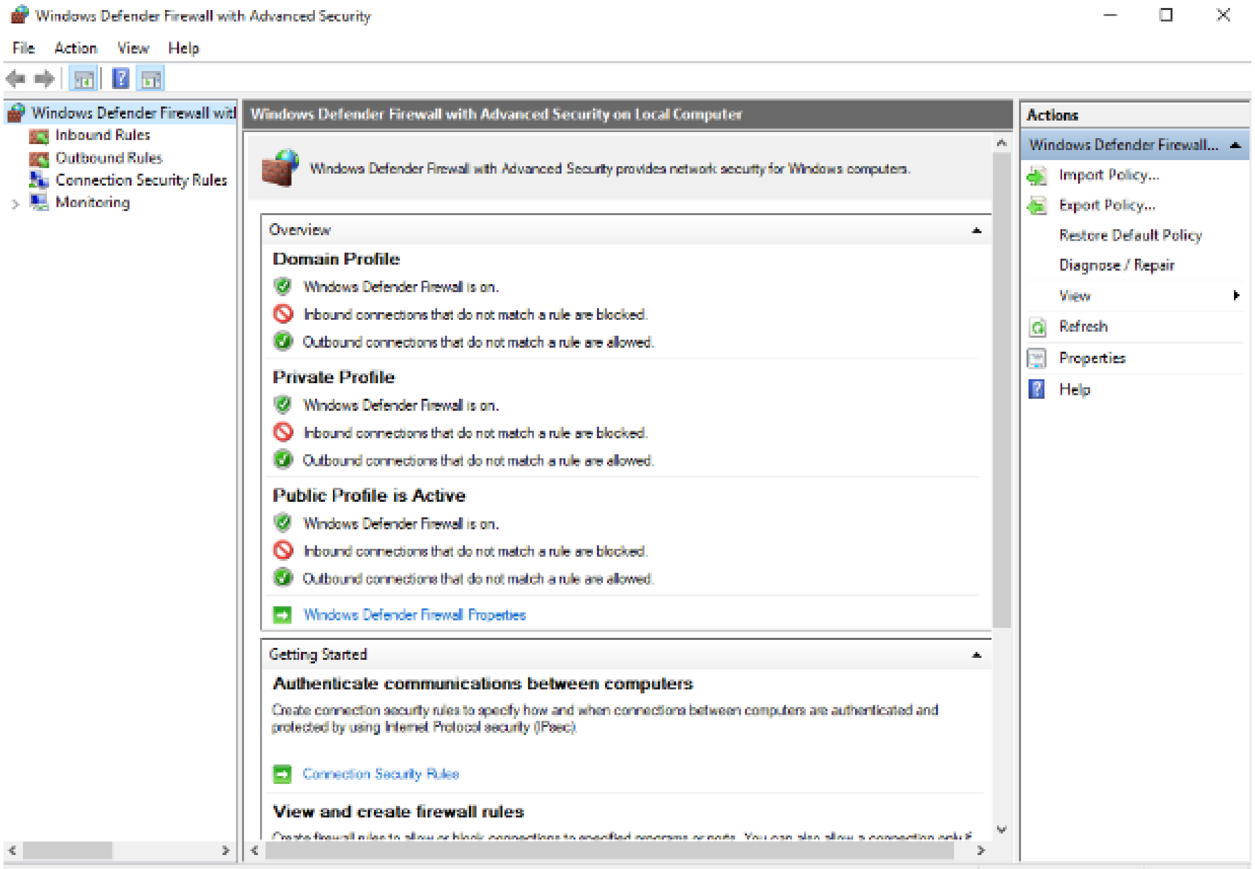
Inbound rules: Inbound rules determine what traffic is allowed to the computer.

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.


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

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

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 authenticated and protected by using Internet Protocol security (IPsec).

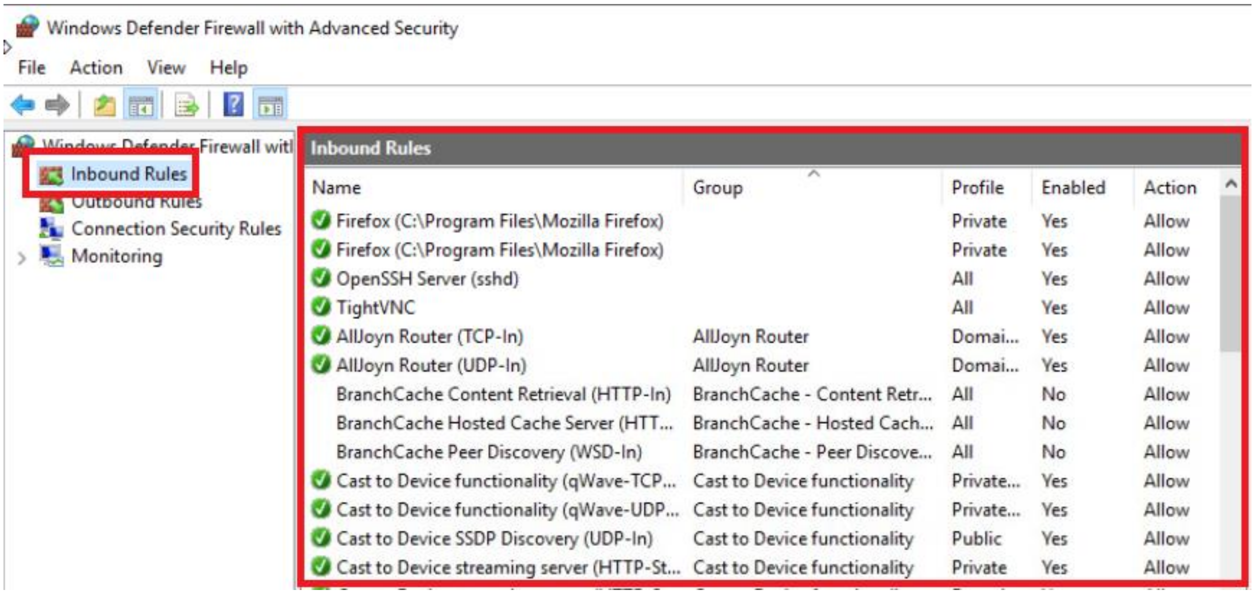
Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if

2. Disable Remote Desktop on the Public Network
    a. Create a New Inbound Rule
        i. In the left pane, click on **Inbound Rules**.

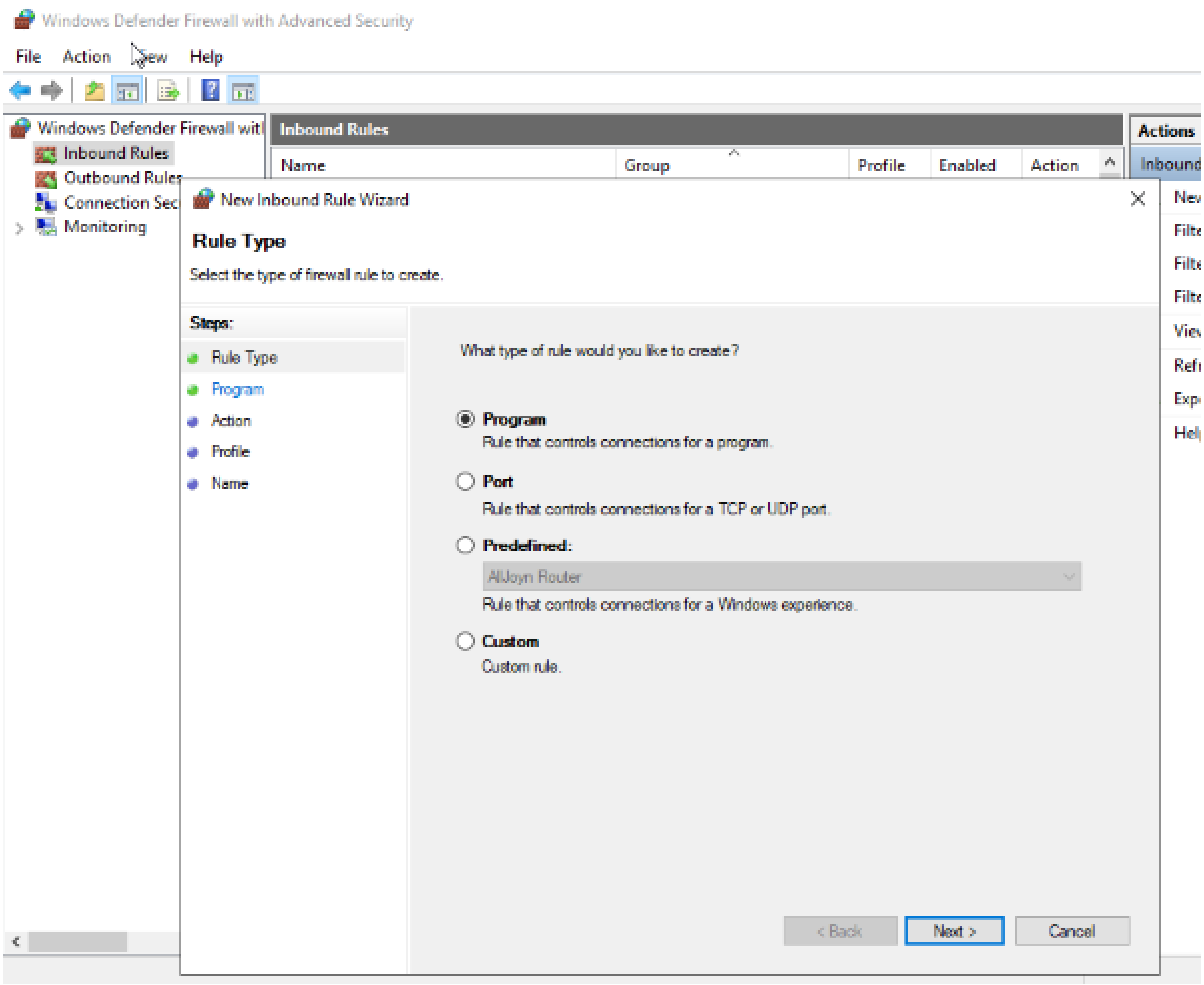
Here you will see a long list of inbound rules. Note that some of the rules have a green checkmark next to them. This indicates that the rule is enabled to allow inbound communication. The rules without a checkmark are available for use but are not enabled.


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

Name	Group	Profile	Enabled	Action
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
✓ OpenSSH Server (sshd)		All	Yes	Allow
✓ TightVNC		All	Yes	Allow
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
✓ Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow
✓ Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow
✓ Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow

ii. In the right pane, click on **New Rule…**.

iii. Select Rule Type- Select **Port** and click **Next**.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- 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.

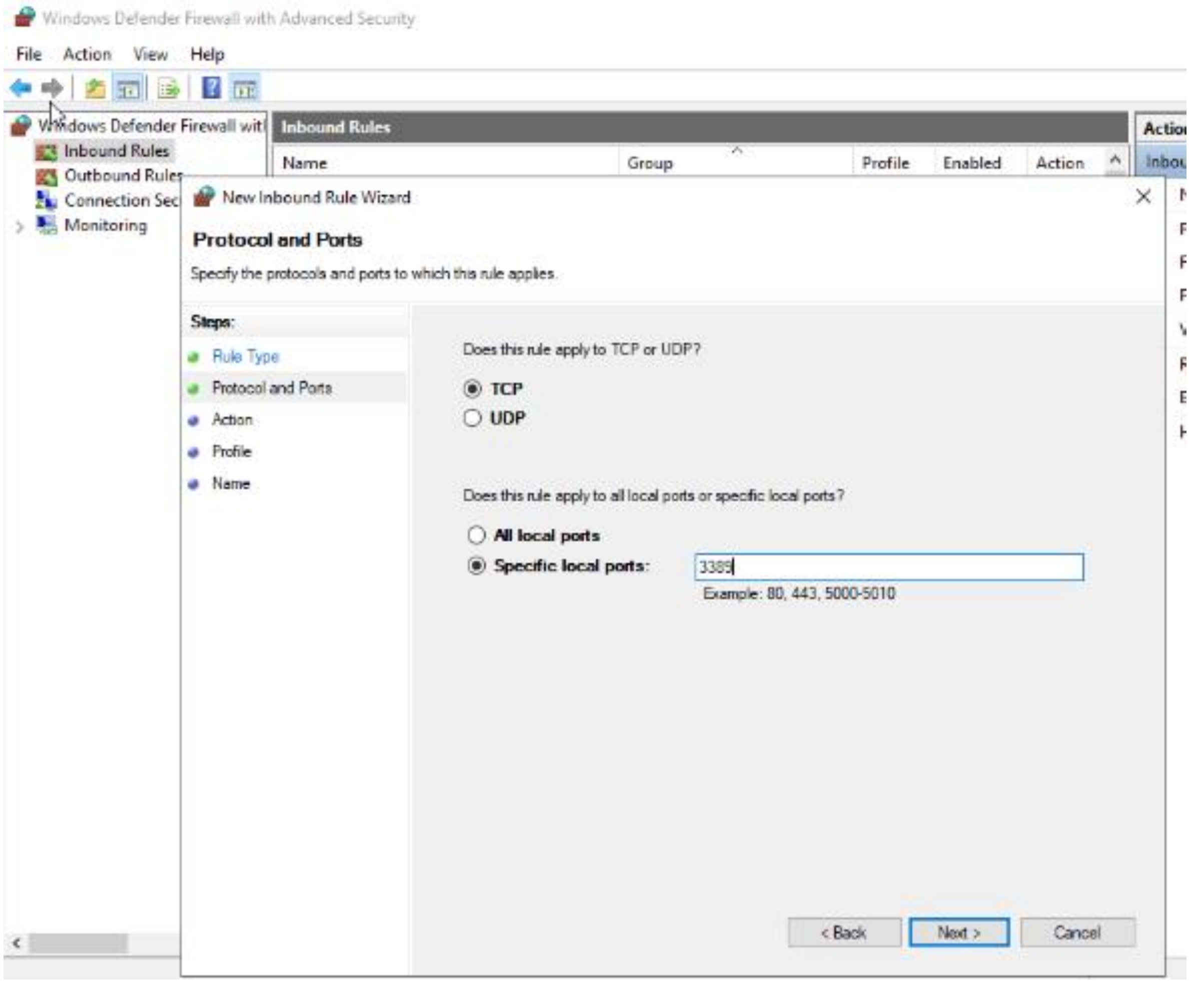
○ **Custom**
Custom rule.

b. Specify Port

   i. Select **TCP**.

   ii. In **Specific local ports**, enter 3389 (the default port for Remote Desktop).

   iii. Click **Next**.



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

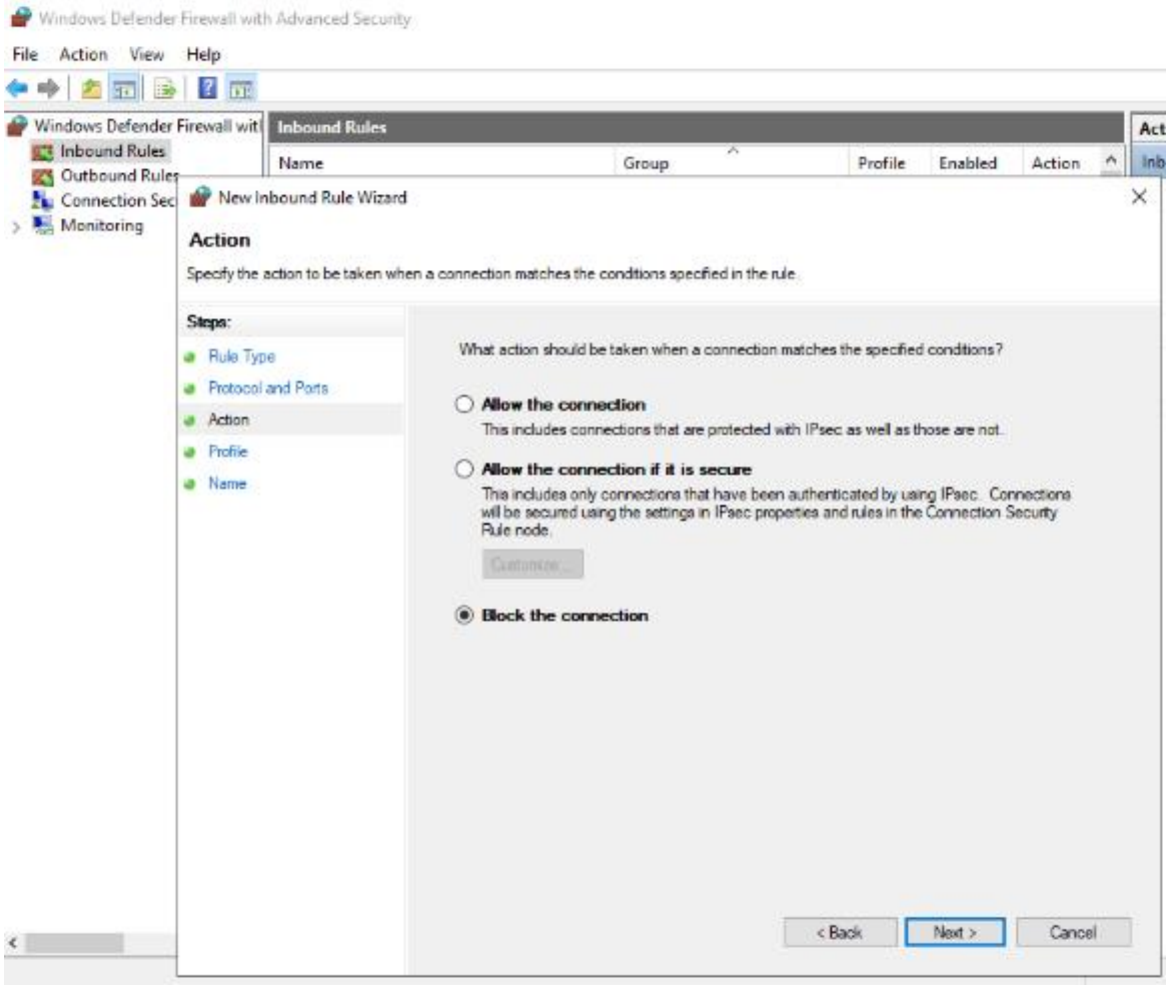
● Specific local ports: 3389

Example: 80, 443, 5000-5010

c. Specify Action

   i. Select **Block the connection**.

   ii. Click **Next**.



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.

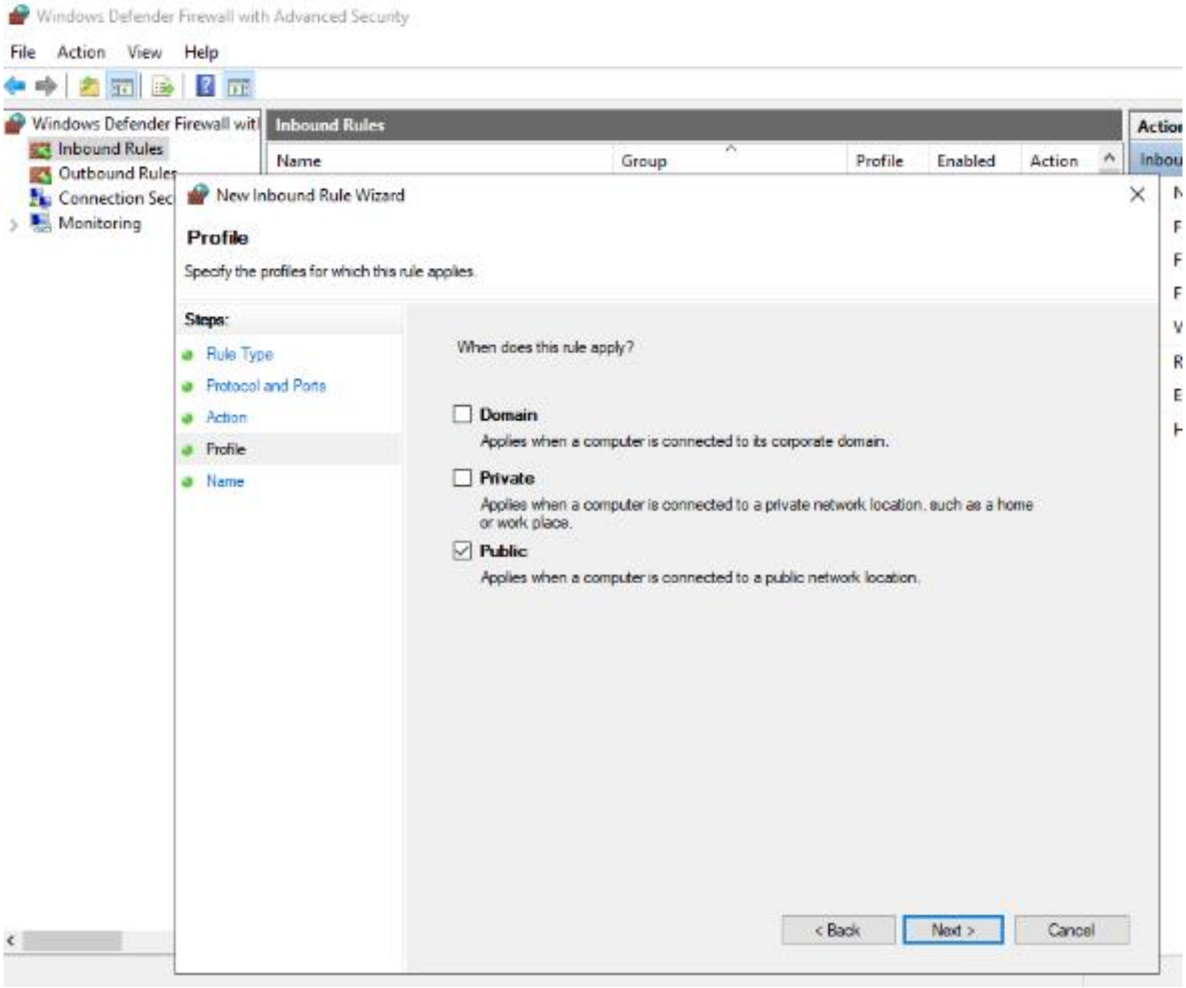
● **Block the connection**

d. Select Profile

   i. Select only **Public**.

   ii. Deselect **Domain** and **Private**.

   iii. Click **Next**.



New Inbound 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.

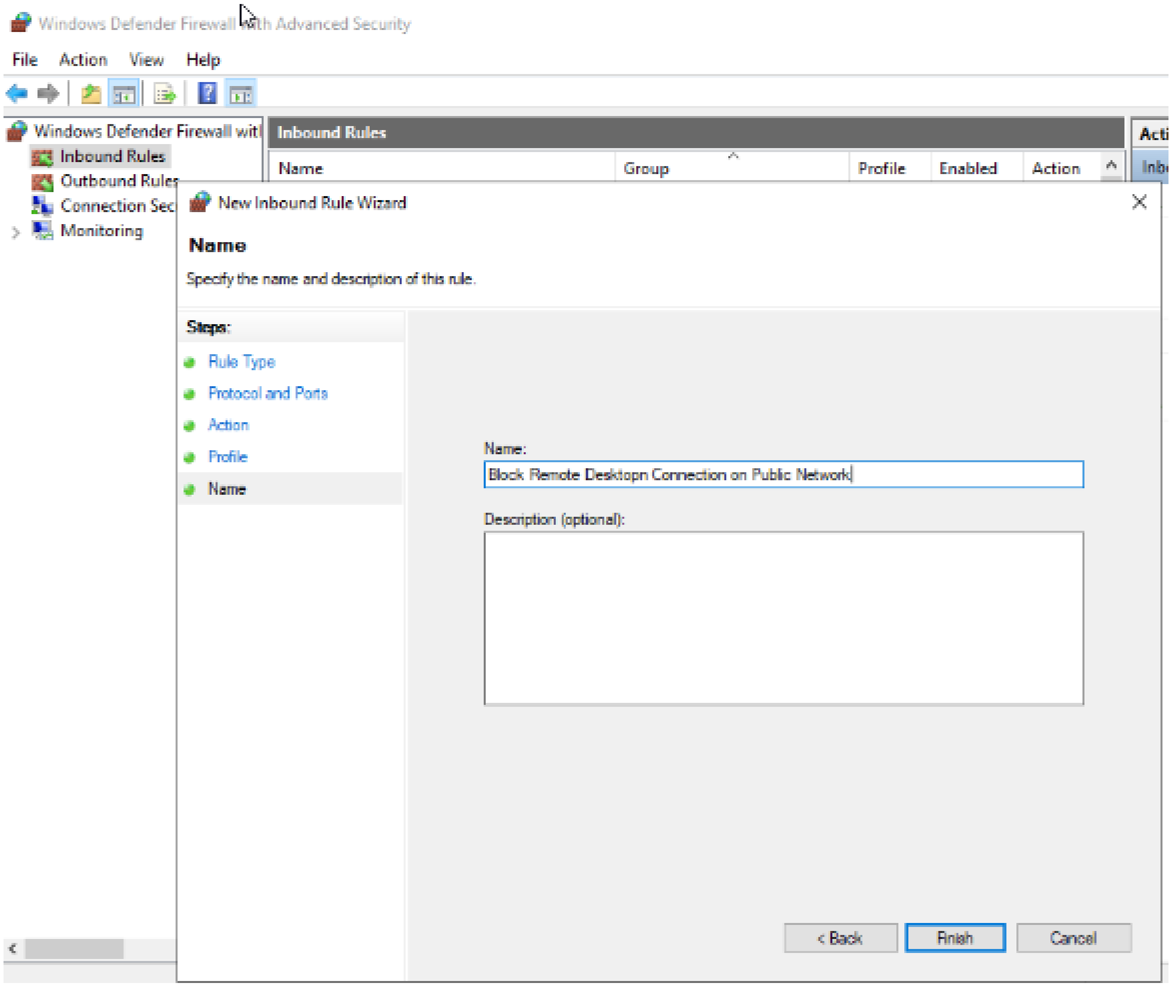
☑ **Public**
Applies when a computer is connected to a public network location.

e. Name the Rule

   i. Enter a name for the rule, such as '**Block Remote Desktop on Public Network**'.

   ii. Optionally, provide a description.

   iii. Click **Finish**.



Name

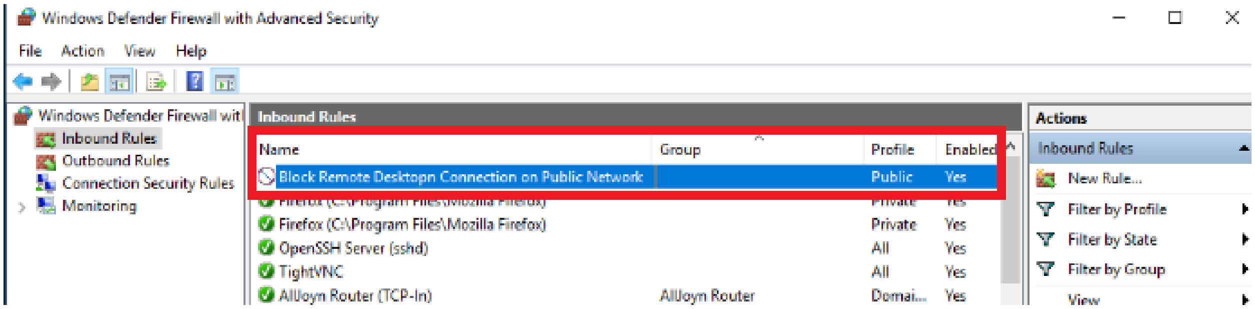
Specify the name and description of this rule.

Name: Block Remote Desktopn Connection on Public Network

Description (optional):

f. Verify the rule listed under Inbound Rules

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



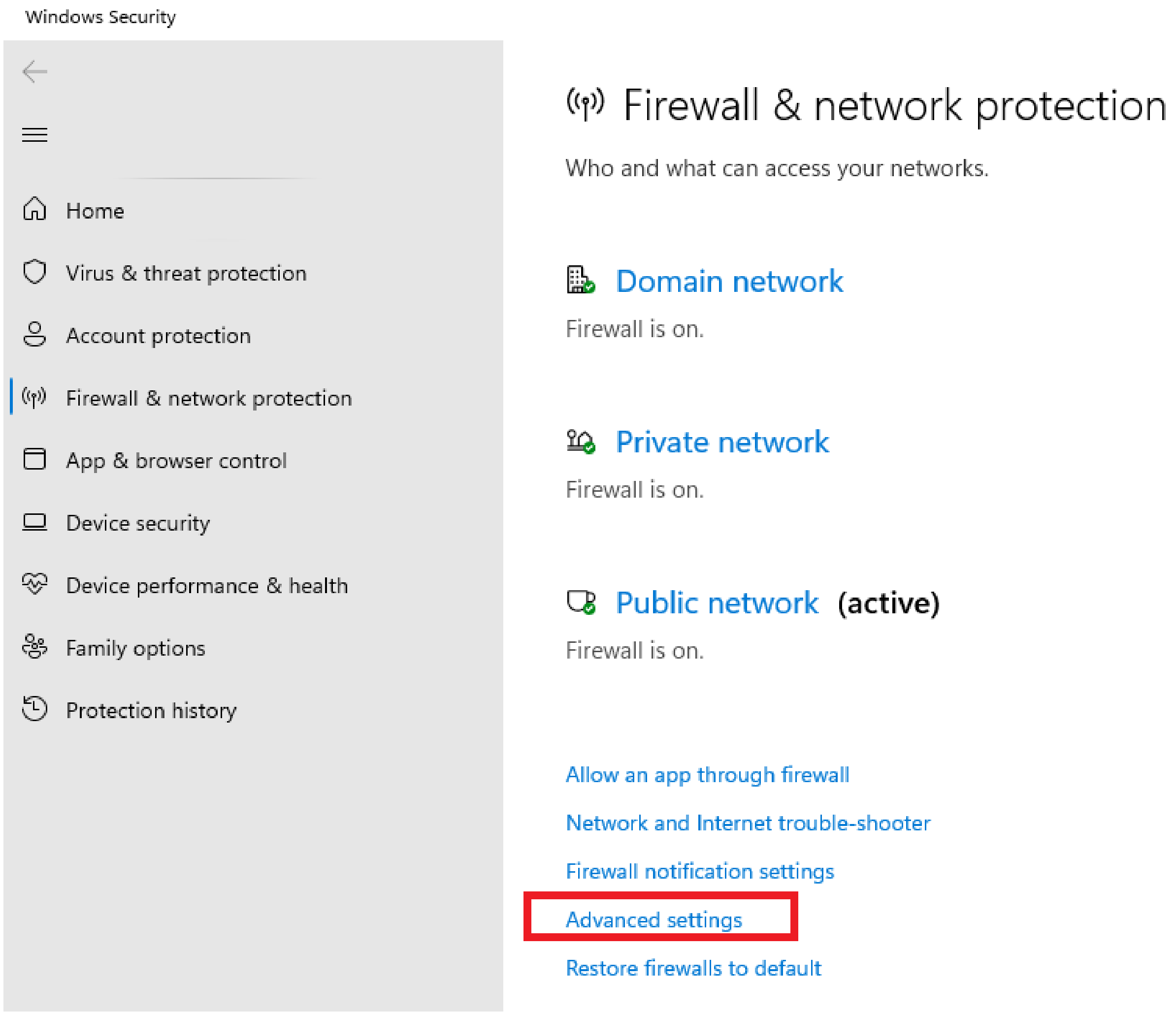
Name	Group	Profile	Enabled
Block Remote Desktopn Connection on Public Network		Public	Yes
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes
OpenSSH Server (sshd)		All	Yes
TightVNC		All	Yes
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes

Scenario 2 - Blocking 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.



Windows Security

Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

Firewall is on.

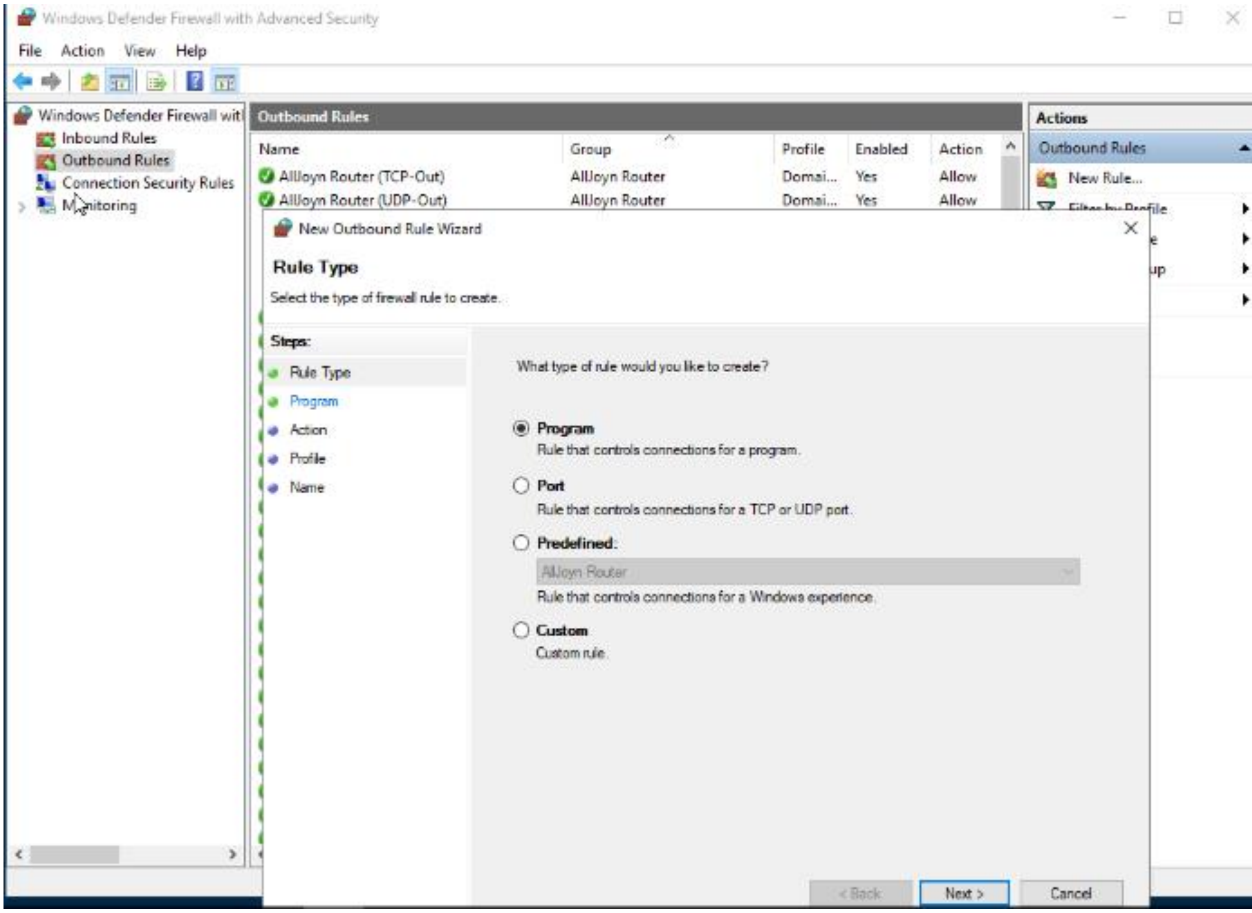
Public network (active)

Firewall is on.

Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Allow an app through firewall
Network and Internet trouble-shooter
Firewall notification settings
Advanced settings
Restore firewalls to default

2. Select Outbound Rules and create a new Rule
   a. In the left pane, click on **Outbound Rules**.

b. In the right pane, click on **New Rule…**.



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.

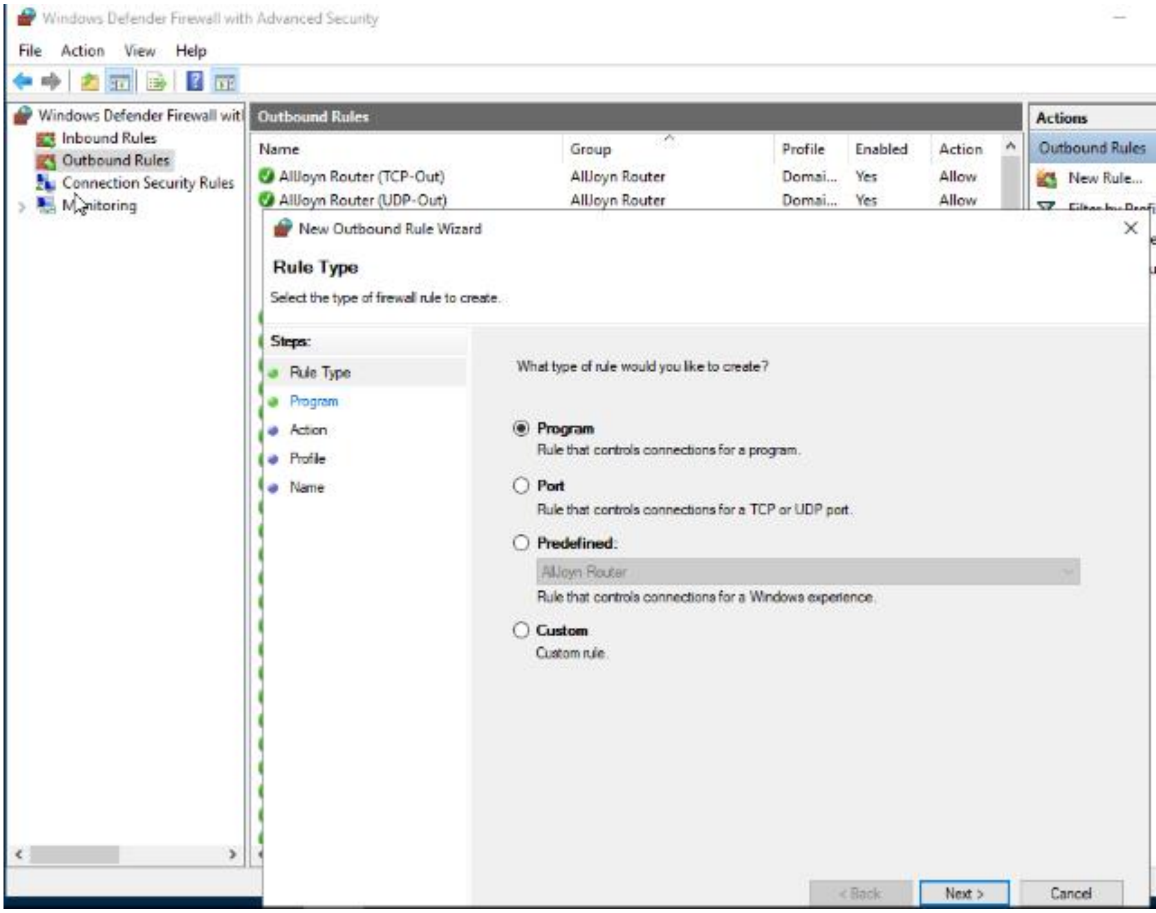
○ **Port**
Rule that controls connections for a TCP or UDP port.

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

○ **Custom**
Custom rule.

c. Choose Rule Type

i. 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:
AllJoyn Router
Rule that controls connections for a Windows experience.

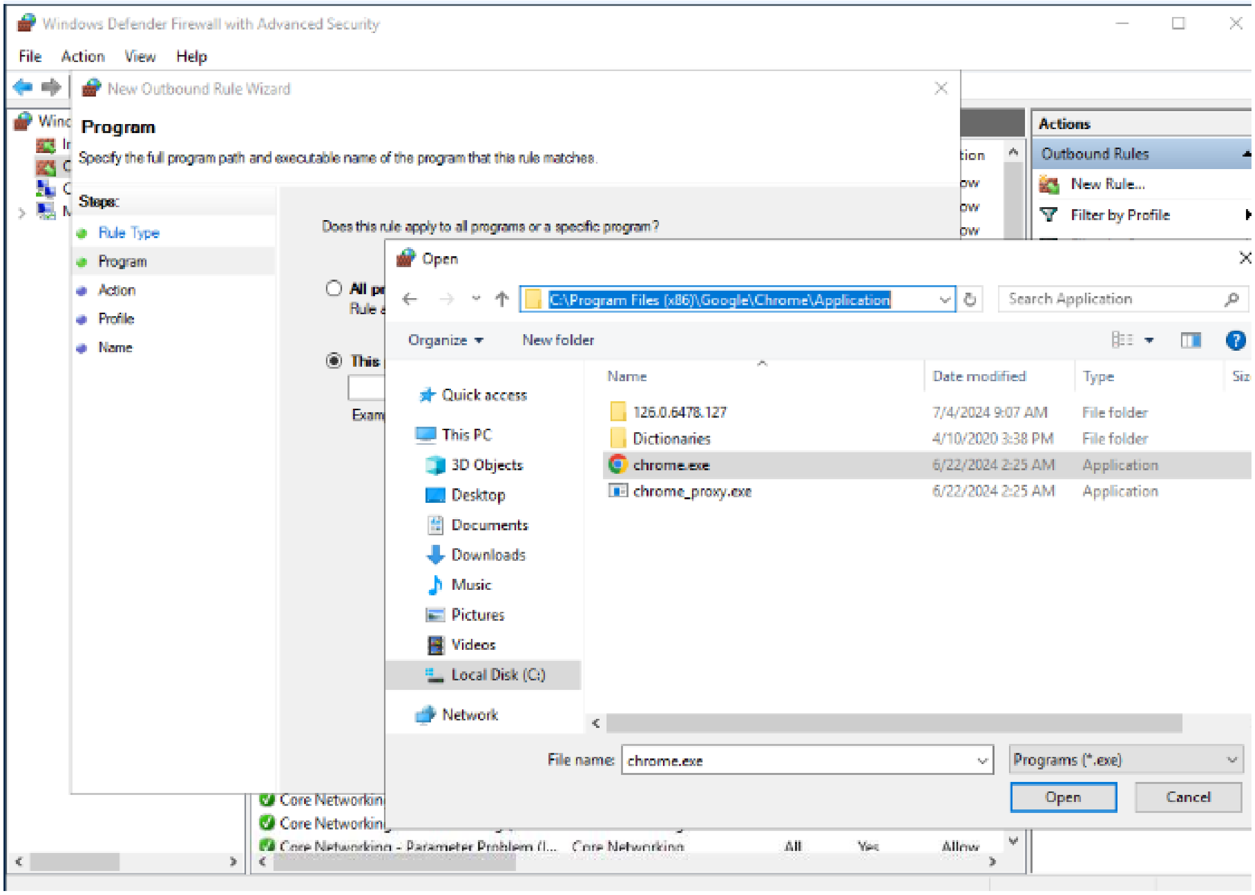
○ Custom
Custom rule.

Name	Group	Profile	Enabled	Action
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow

d. Specify Program Path

i. Select **This program path:** and browse to the executable file of the application you want to block.

ii. For example, to block Google Chrome, you might navigate to `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe` and click **Open**.



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 pr
Rule a

● This

Exam

C:\Program Files (x86)\Google\Chrome\Application

Search Application

Name	Date modified	Type
126.0.6478.127	7/4/2024 9:07 AM	File folder
Dictionaries	4/10/2020 3:38 PM	File folder
chrome.exe	6/22/2024 2:25 AM	Application
chrome_proxy.exe	6/22/2024 2:25 AM	Application

File name: chrome.exe

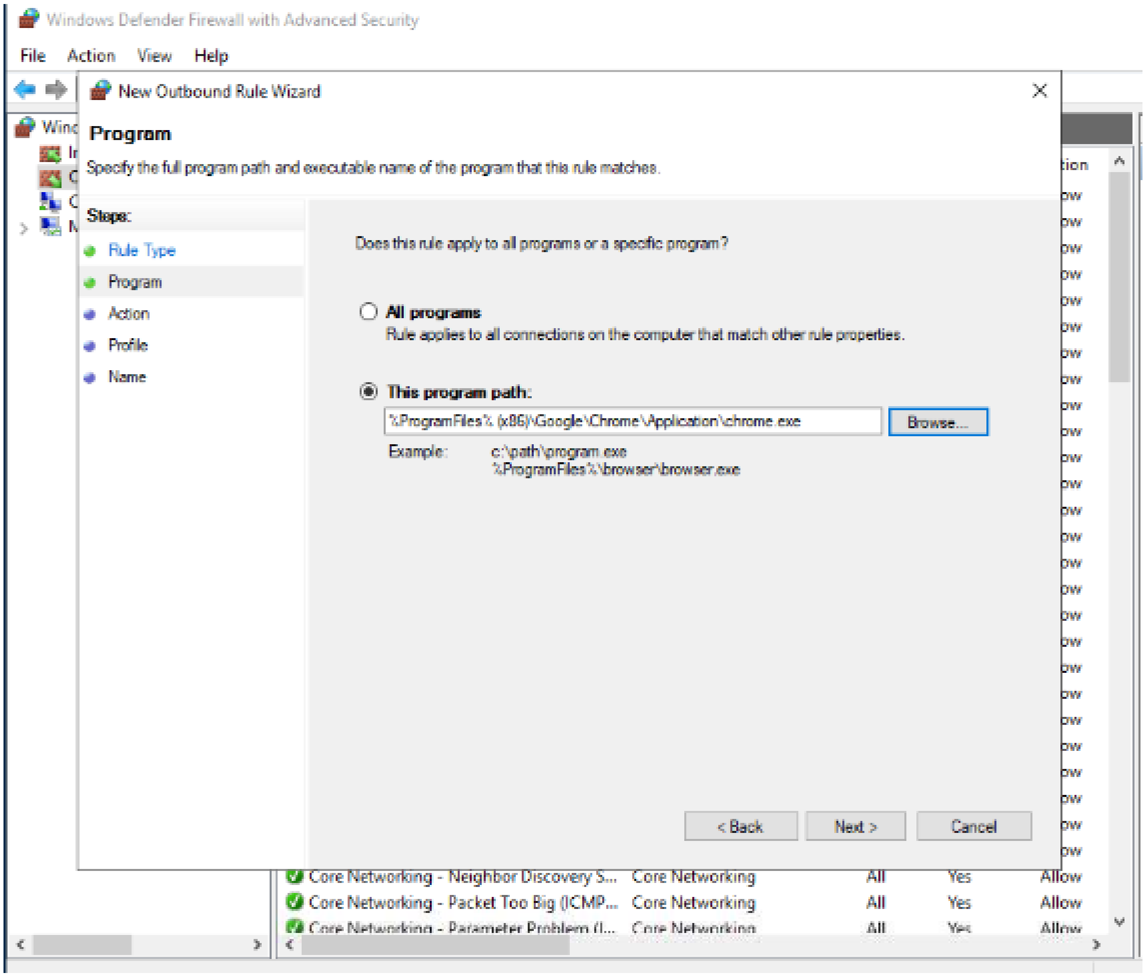
Programs (*.exe)

Core Networkin

Core Networkin

Core Networking - Parameter Problem (I... Core Networking All Yes Allow

iii. Click **Next**.



Windows Defender Firewall with Advanced Security

File Action View Help

New Outbound Rule Wizard

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:**

%ProgramFiles% (x86)\Google\Chrome\Application\chrome.exe Browse...

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

< Back Next > Cancel

Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow

e. Select Action

   i. Select **Block the connection** and click **Next**.

f. Specify Profile

   i. Choose when the rule applies: **Domain**, **Private**, and **Public**.

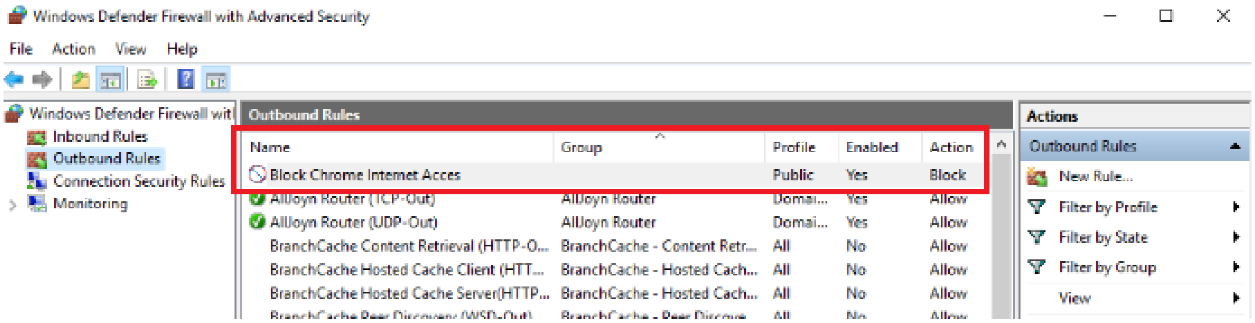
   ii. Check all profiles if you want the rule to apply in all scenarios.

   iii. Click **Next**.

g. Name the Rule

   i. Give the rule a name (e.g., “Block Chrome Internet Access”) and an optional description.

   ii. Click **Finish**.



Name	Group	Profile	Enabled	Action
Block Chrome Internet Acces		Public	Yes	Block
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove	All	No	Allow

h. Verify the Rule

i. 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.

ii. If you go back to Outbound Rules setting and disable the Rule "Block Chrome Internet Access" , you will be able to browser 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

a. In the left pane, click on **Inbound Rules**.

b. In the right pane, click on **New Rule**

c. Choose **Port** and click **Next**.
d. Specify Ports:
   i. Select **TCP**.
   ii. In Specific local ports, enter **80** (the default port for HTTP).
   iii. Click **Next**.
e. Specify Action:
   i. Select **Block the connection**.
   ii. Click **Next**.
f. Specify Network Profile:
   i. Check only the **Public** option.
   ii. Uncheck **Domain** and **Private**.
   iii. Click **Next**.
g. Name the Rule:
   i. Enter a name for the rule, such as "**Block HTTP on Public Network** ".
   ii. Add a description if desired.
   iii. 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

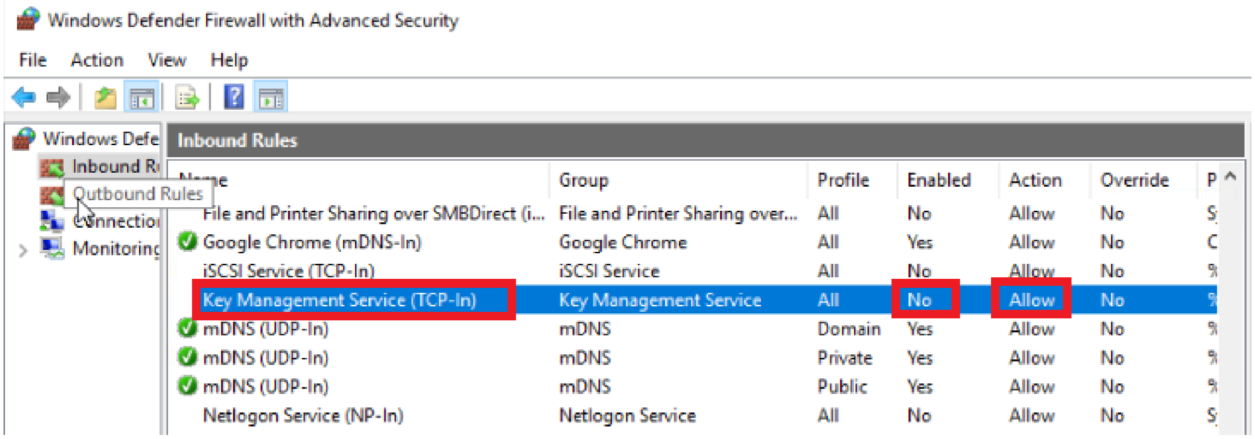
Follow steps in Scenario 1 to open the **Advanced Security** option window.

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**.)

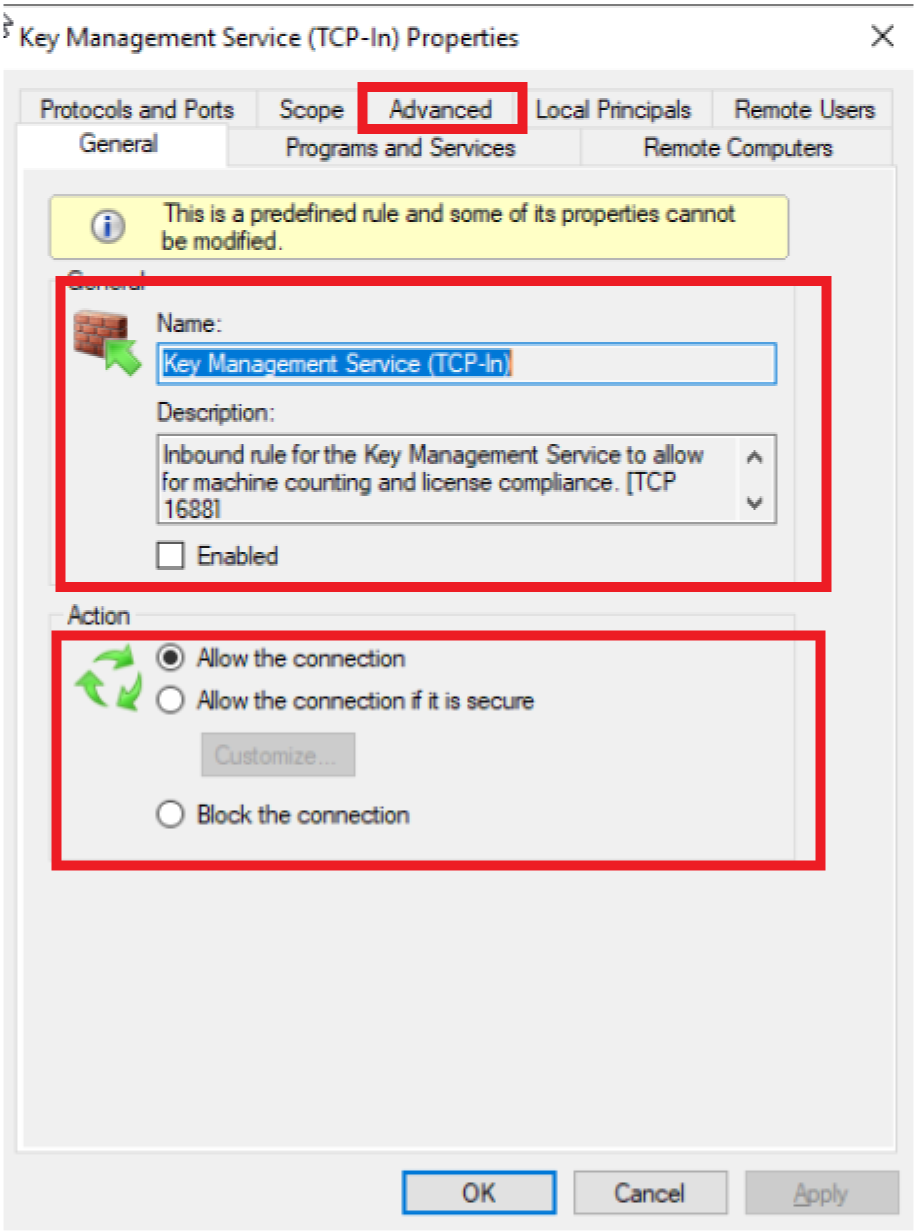
- If enabled, the rule would allow communication (the **Action** column says **Allow**.)

  Double-click this rule.



Name	Group	Profile	Enabled	Action	Override	P
File and Printer Sharing over SMBDirect (i...	File and Printer Sharing over...	All	No	Allow	No	S
✓ Google Chrome (mDNS-In)	Google Chrome	All	Yes	Allow	No	C
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow	No	%
Key Management Service (TCP-In)	Key Management Service	All	No	Allow	No	%
✓ mDNS (UDP-In)	mDNS	Domain	Yes	Allow	No	%
✓ mDNS (UDP-In)	mDNS	Private	Yes	Allow	No	%
✓ mDNS (UDP-In)	mDNS	Public	Yes	Allow	No	%
Netlogon Service (NP-In)	Netlogon Service	All	No	Allow	No	S

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.



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

General

Name:

Key Management Service (TCP-In)

Description:

Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 1688]

□ Enabled

Action

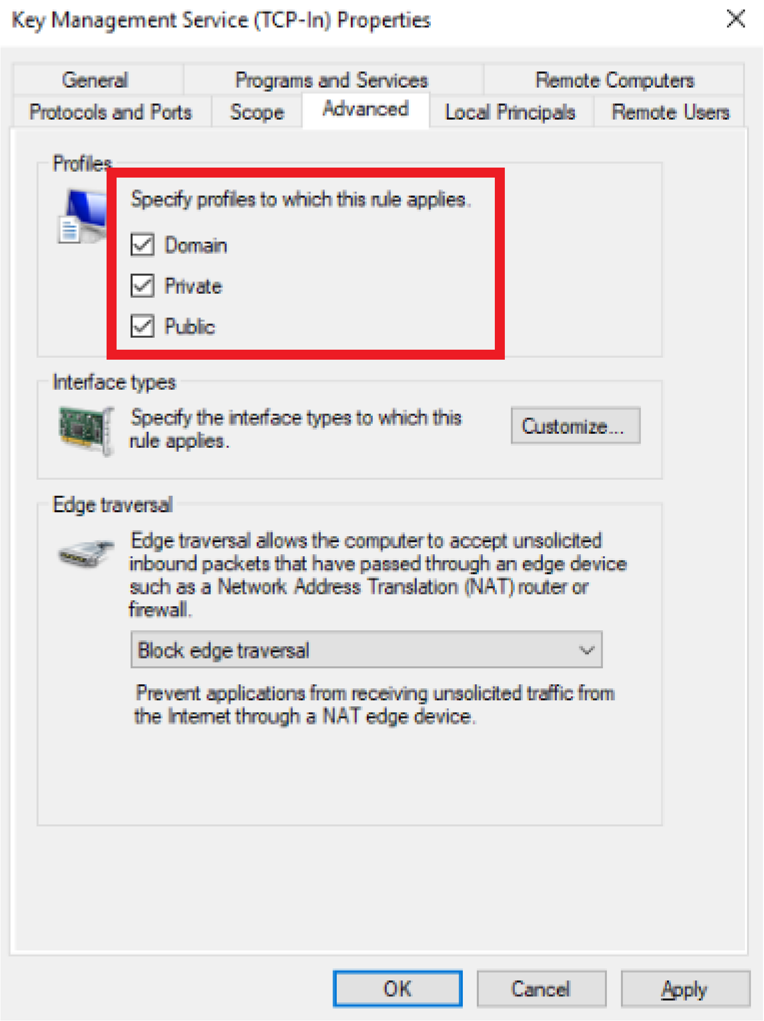
● Allow the connection

○ Allow the connection if it is secure

Customize...

○ Block the connection

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

Profiles

Specify profiles to which this rule applies.

☑ Domain

☑ Private

☑ Public

Interface types

Specify the interface types to which this rule applies.

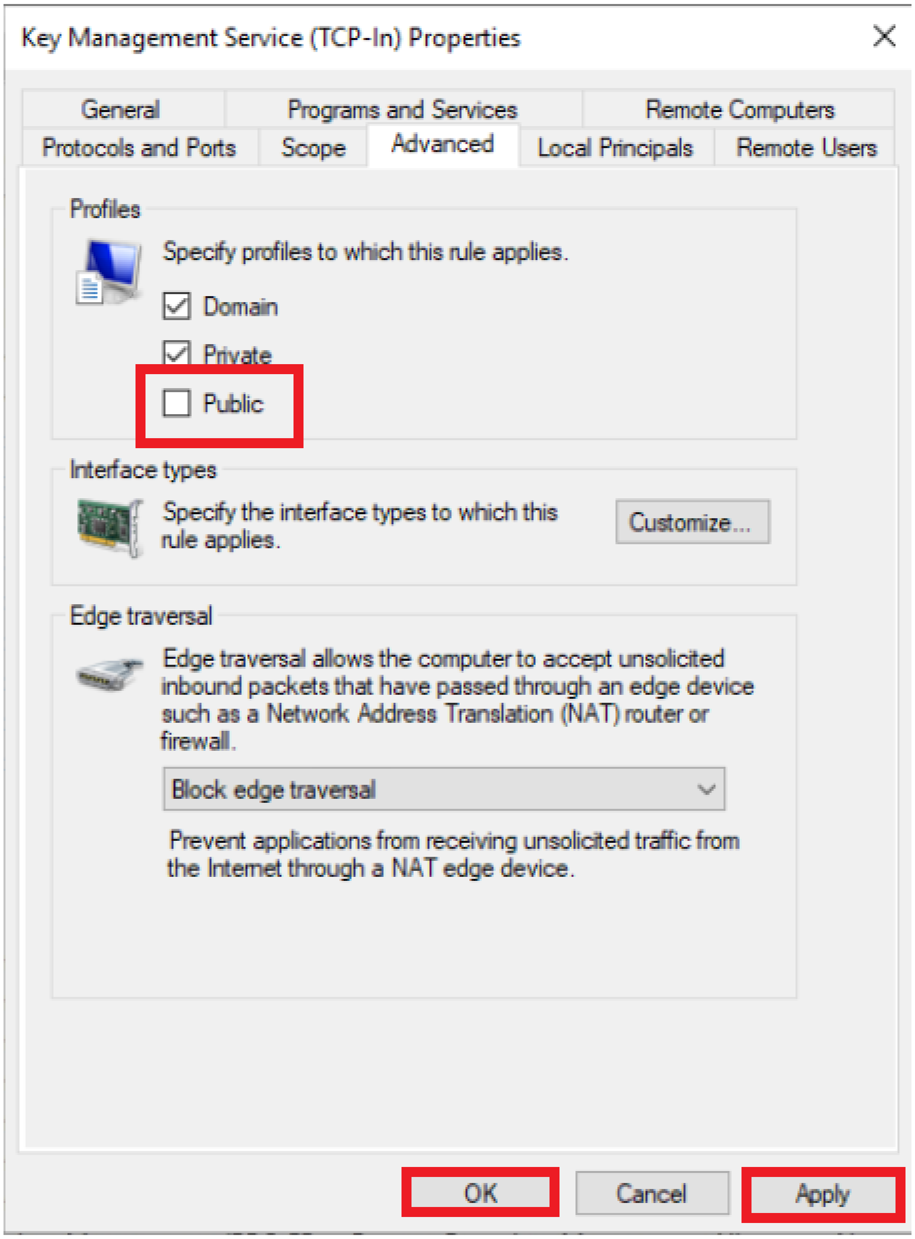
Edge traversal

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.

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**.



Key Management Service (TCP-In) Properties

Profiles

Specify profiles to which this rule applies.

☑ Domain

☑ Private

☐ Public

Interface types

Specify the interface types to which this rule applies.

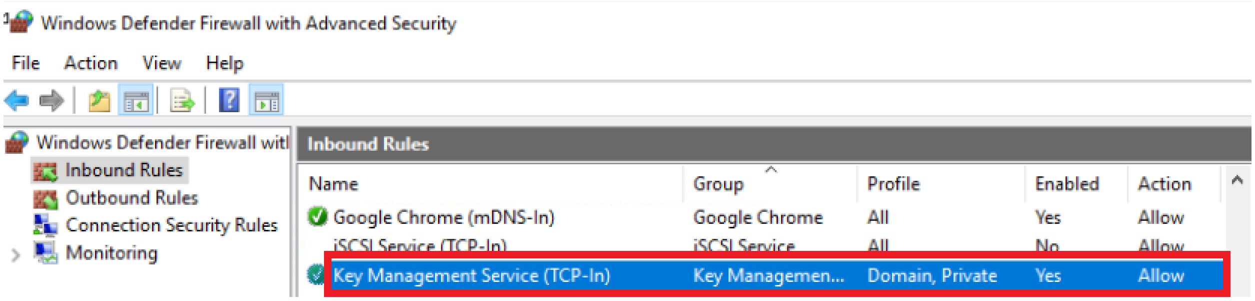
Edge traversal

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.

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.

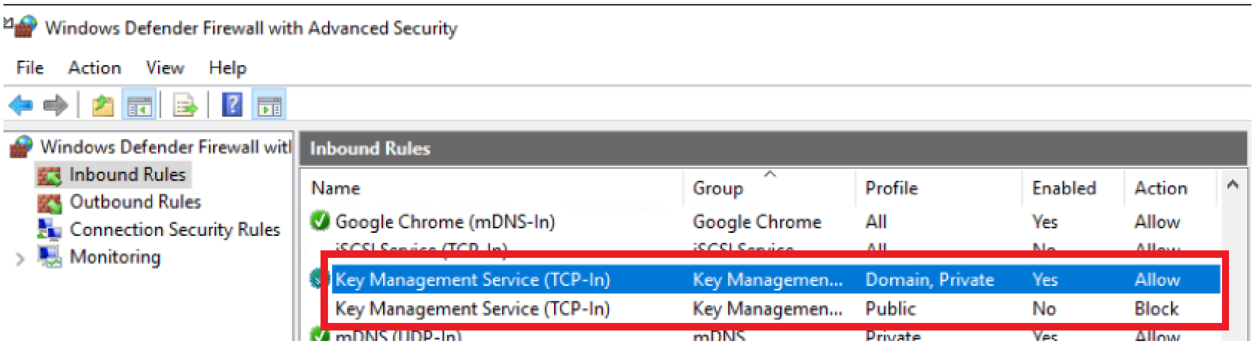


Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action
✓ Google Chrome (mDNS-In)	Google Chrome	All	Yes	Allow
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
✓ Key Management Service (TCP-In)	Key Managemen...	Domain, Private	Yes	Allow

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.

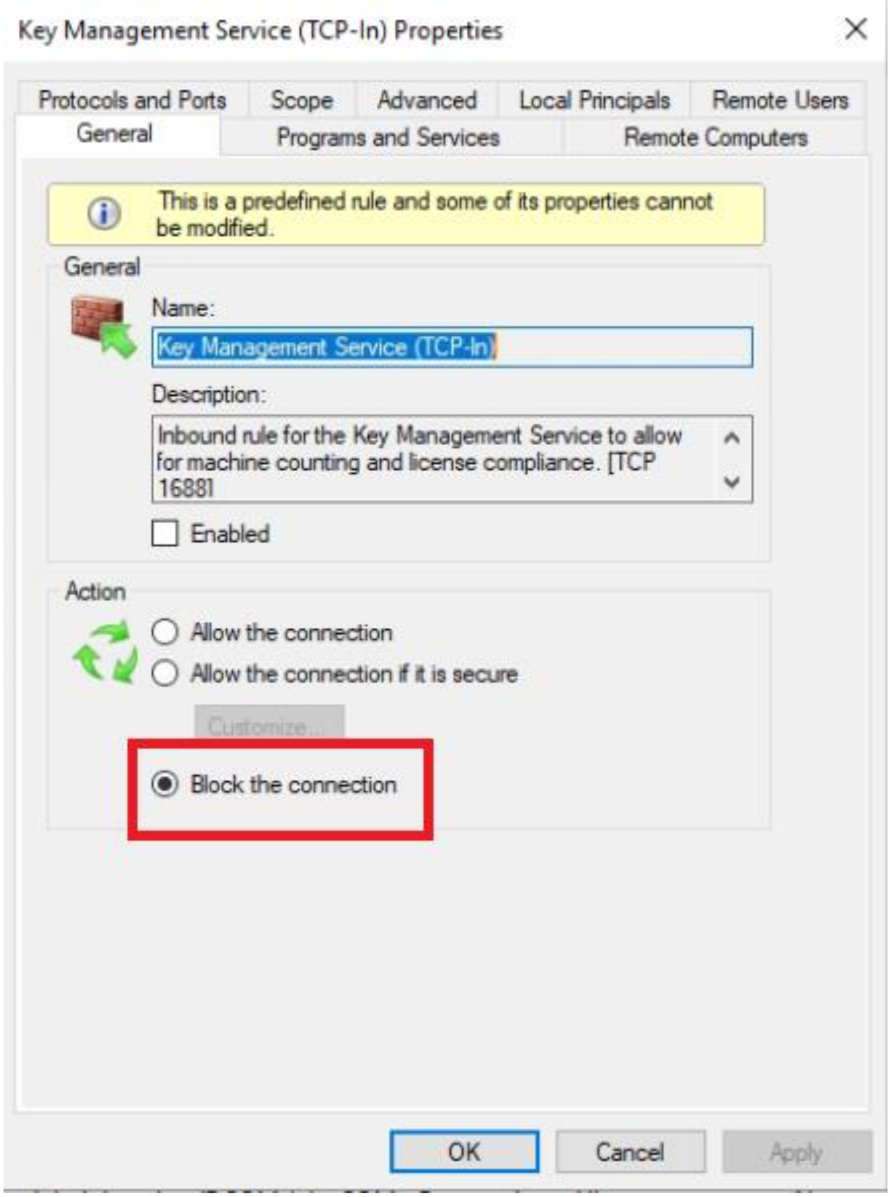


Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action
✓ Google Chrome (mDNS-In)	Google Chrome	All	Yes	Allow
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
✓ Key Management Service (TCP-In)	Key Managemen...	Domain, Private	Yes	Allow
Key Management Service (TCP-In)	Key Managemen...	Public	No	Block
✓ mDNS (UDP-In)	mDNS	Private	Yes	Allow

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



Key Management Service (TCP-In) Properties

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

General

Name:
Key Management Service (TCP-In)

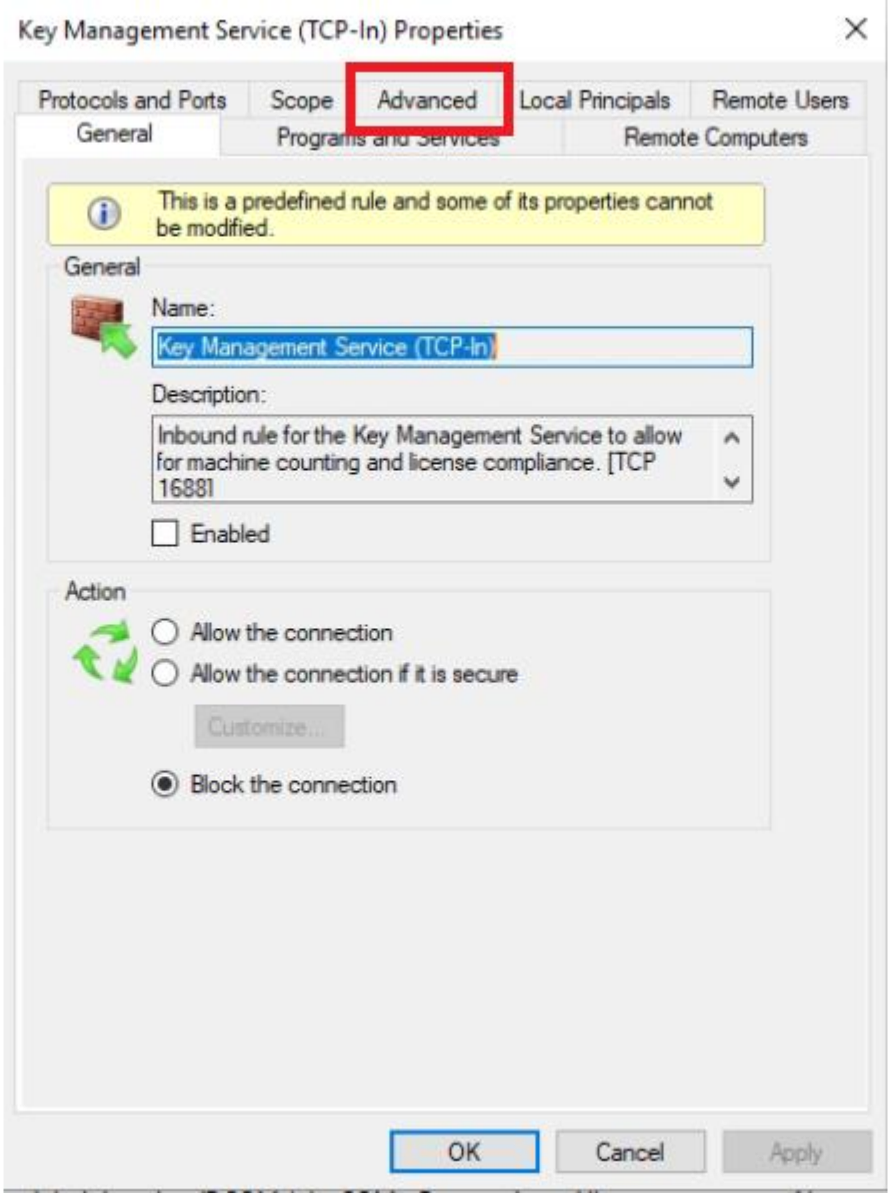
Description:
Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 1688]

□ Enabled

Action

○ Allow the connection
○ Allow the connection if it is secure
● Block the connection

9. Click the **Advanced** tab.



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

Name: Key Management Service (TCP-In)

Description: Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 1688]

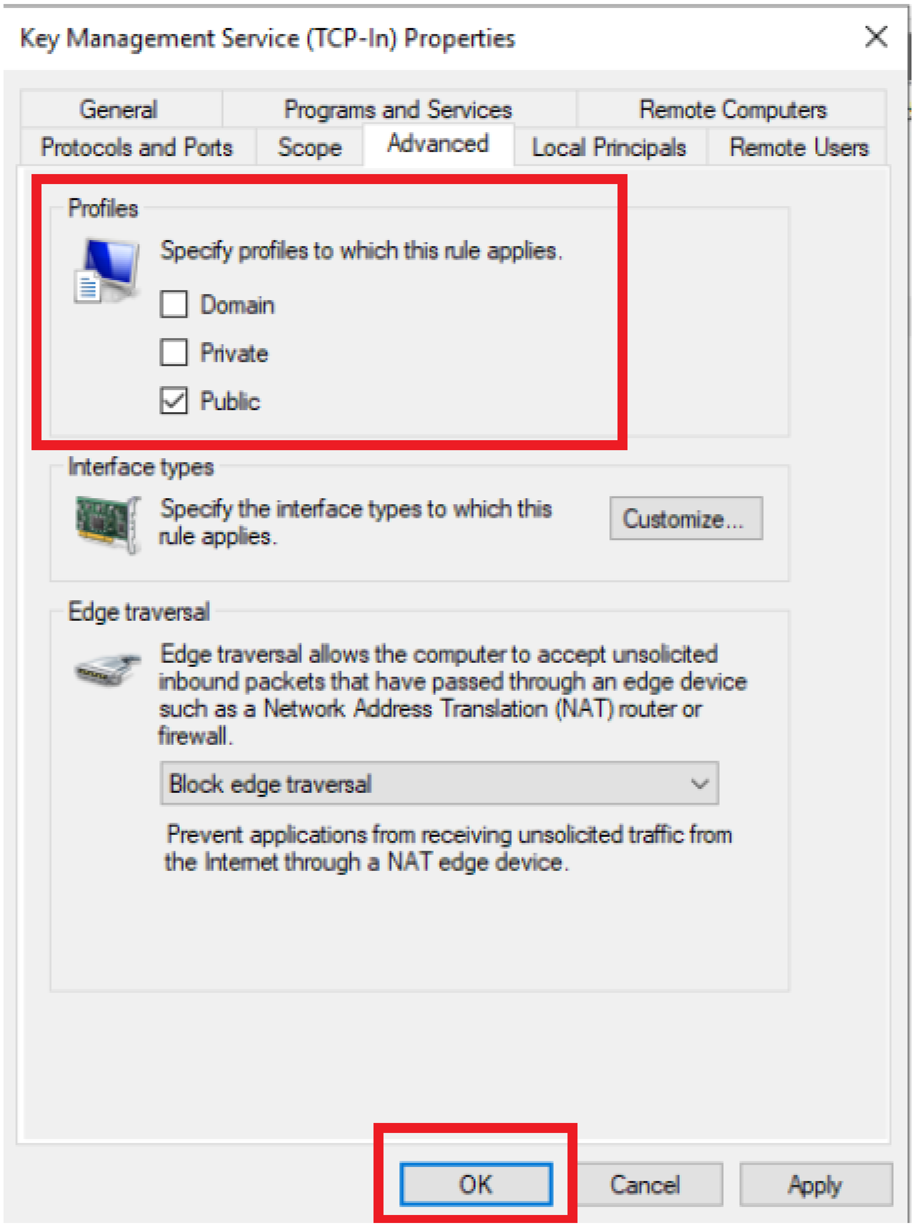
□ Enabled

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

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



Key Management Service (TCP-In) Properties

Profiles

Specify profiles to which this rule applies.

□ Domain

□ Private

☑ Public

Interface types

Specify the interface types to which this rule applies.

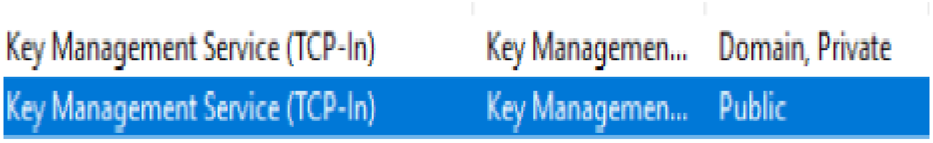
Edge traversal

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

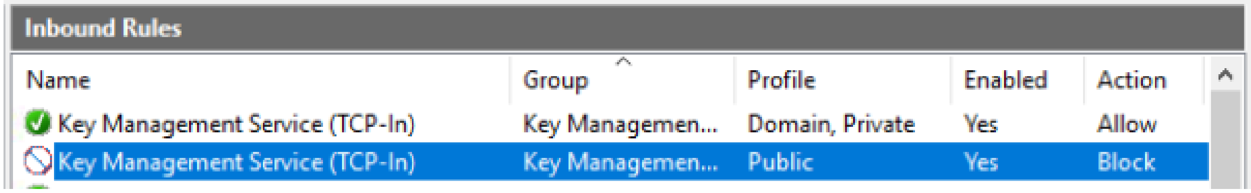
Prevent applications from receiving unsolicited traffic from the Internet through a NAT edge device.

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



Key Management Service (TCP-In)	Key Managemen...	Domain, Private
Key Management Service (TCP-In)	Key Managemen...	Public

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

Conclusion

This whole project provided a comprehensive understanding of the configuration and management of Windows Firewall using both the standard and advanced options of Windows Defender Firewall. Through the guide and scenarios, the following key skills were developed:

1. **Enabling and Verifying Firewall Settings:**
    a. Understanding the roles of Domain, Private, and Public network profiles and their impact on system security.
    b. Verifying and adjusting settings for allowed applications through the firewall.
2. **Configuring Basic and Advanced Rules:**
    a. Blocking and allowing specific inbound and outbound traffic using port and application-specific rules.
    b. Restricting Remote Desktop and HTTP traffic on Public networks to enhance security.
    c. Managing application-level traffic restrictions to control outbound network behavior.
3. **Scenario-Specific Rules for Enhanced Security:**
    a. Customizing rules for unique organizational needs, such as blocking or allowing specific services (e.g., Remote Desktop and KMS) under defined profiles.
    b. Demonstrating how advanced firewall rules can be tailored for specific network conditions, increasing security without sacrificing necessary functionality.

Key Takeaways:

- **Flexibility and Control:** Windows Firewall with Advanced Security provides granular control over inbound and outbound traffic, allowing administrators to implement strict security policies without hindering necessary communication.
- **Scenario-Specific Rule Application:** Tailoring rules to match network profiles ensures that different network conditions (e.g., Public vs. Private) are managed with appropriate security policies.
- **Efficient Troubleshooting:** The project illustrated how to enable and disable rules as needed, demonstrating efficient ways to verify configurations and resolve network access issues.

By following this guide, users can gainpractical knowledge and hands-on experience in managing network traffic and securing Windows systems through Windows Defender Firewall. This foundational skill set is critical for IT professionals tasked with ensuring organizational and endpoint security.