Hands-on Lab: Create a Firewall Rule in Microsoft Windows Defender

Estimated time needed: **30** minutes

About This Lab

This exercise 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.

Objectives

In this hands-on lab, you will:

- Use Windows Defender Firewall with Advanced Security to edit an existing firewall rule.
- Enforce the following rules:
- Allow the connection for Key Management Service on the Domain and Private network.
- Deny the connection for Key Management Service on the Public network.

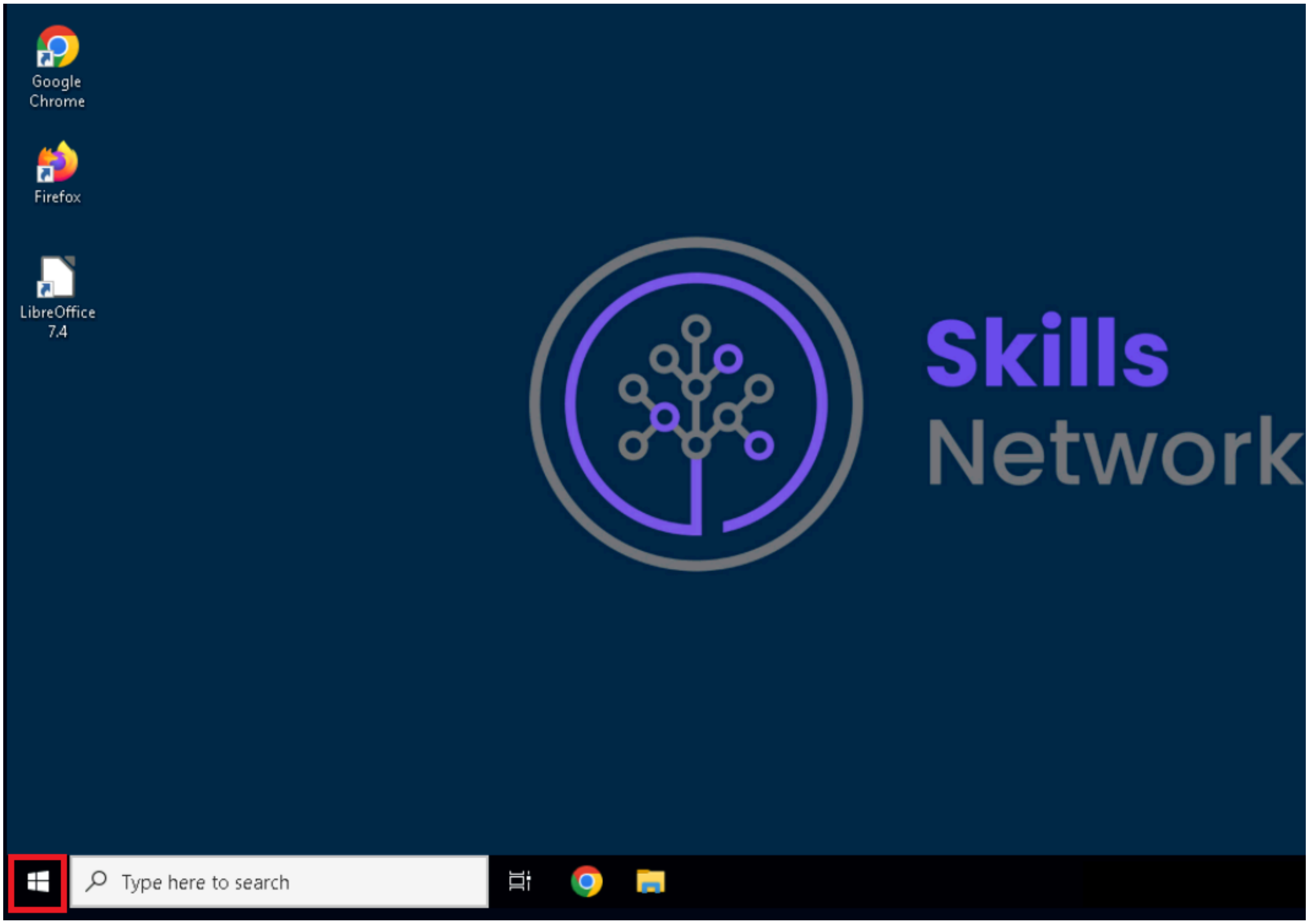
Important Information About Lab Instructions and Solutions

In case you try to use your physical keyboard in the lab environment, it might not produce any visible results. To avoid this issue, please use the On-Screen Keyboard (you can find it by searching for `On-Screen Keyboard` in the search bar at the bottom of your screen). If search functionality doesn't work, you can also click on the `Windows icon`, scroll down to find `Windows Ease of Access`, click on it, and then select `On-Screen Keyboard`.

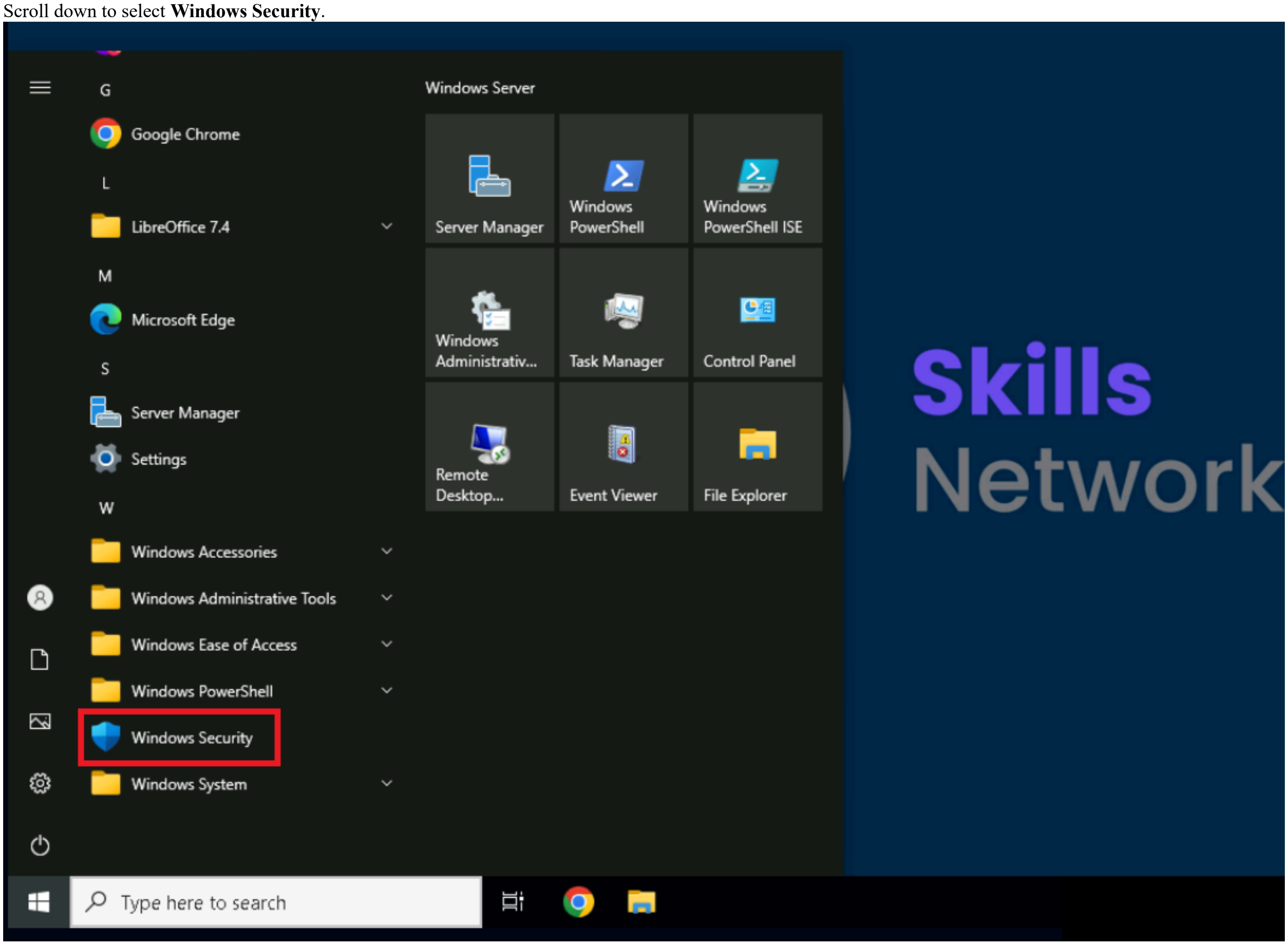
Microsoft Windows operating system features can vary based on the Windows edition. If completing these exercises on your machine, your navigation and solutions may differ from what's presented in this lab.

Exercise 1: Allow an app through a firewall

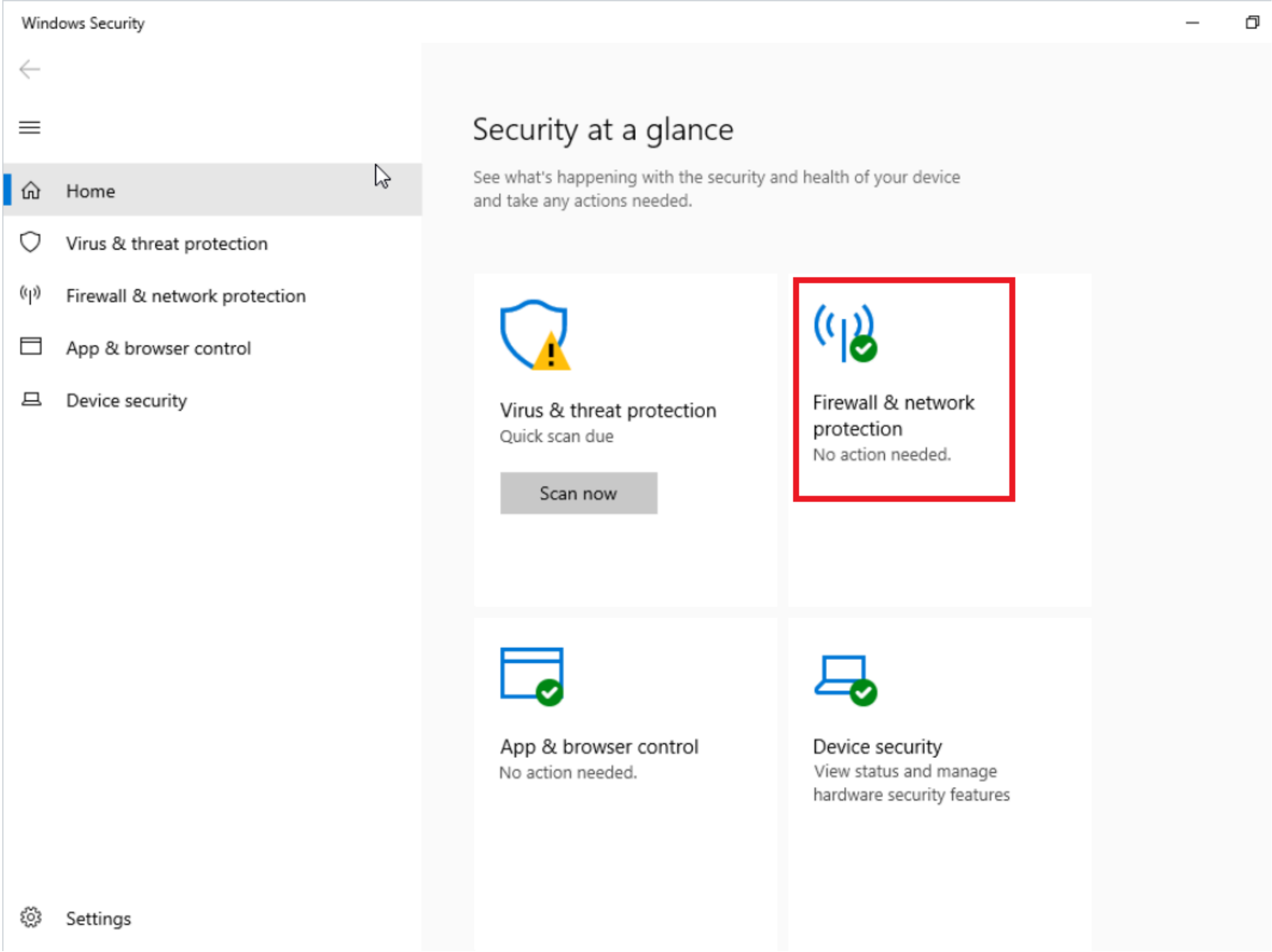
1. Select the Windows **Start** button.



2. Scroll down to select **Windows Security**.



3. Select **Firewall & network protection**.



Security at a glance

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

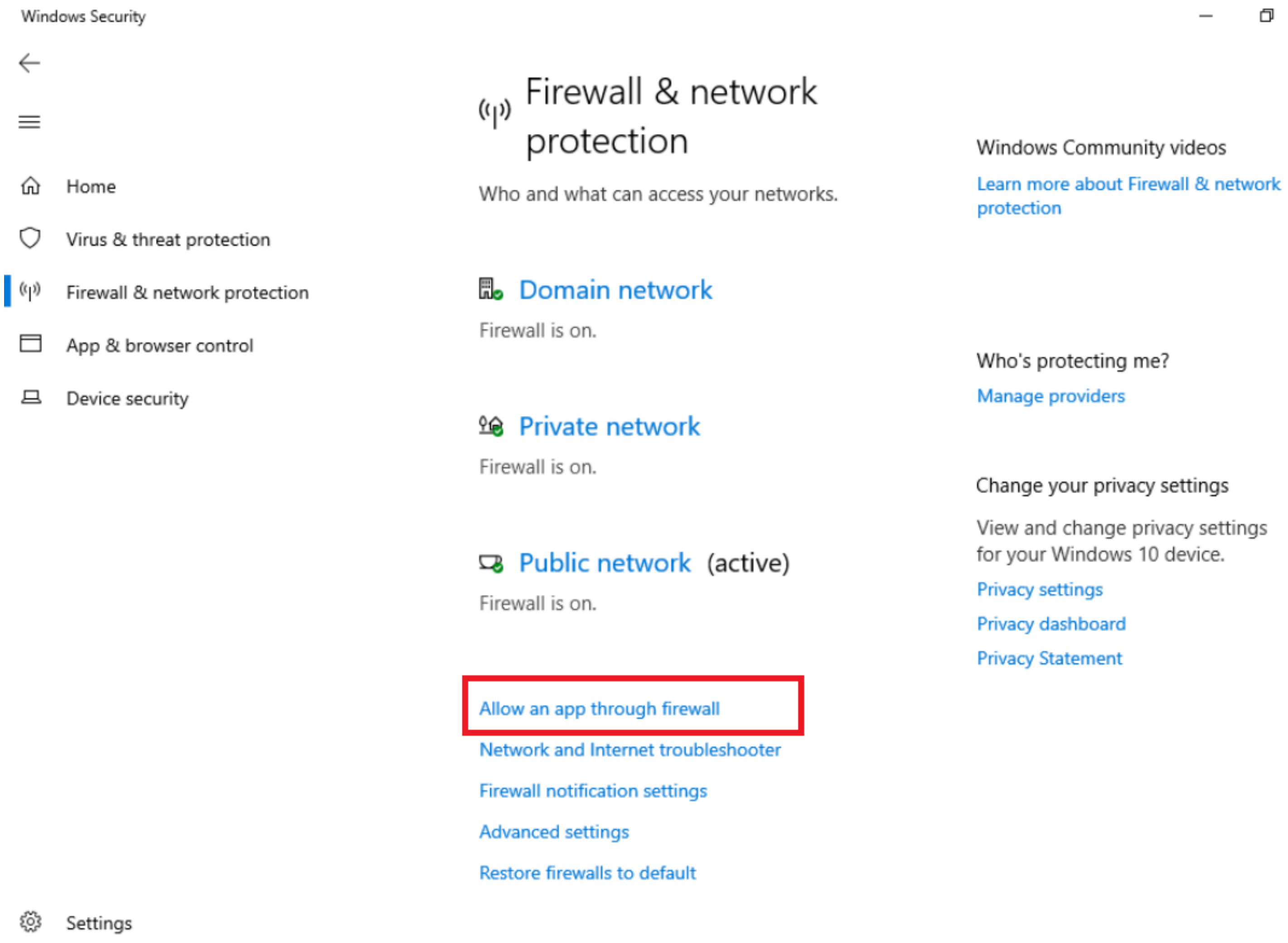
Virus & threat protection
Quick scan due

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features

4. Select **Allow an app through firewall**.



Windows Security

Firewall & network protection

Who and what can access your networks.

Home
Virus & threat protection
Firewall & network protection
App & browser control
Device security
Settings

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

Windows Community videos

Learn more about Firewall & network protection

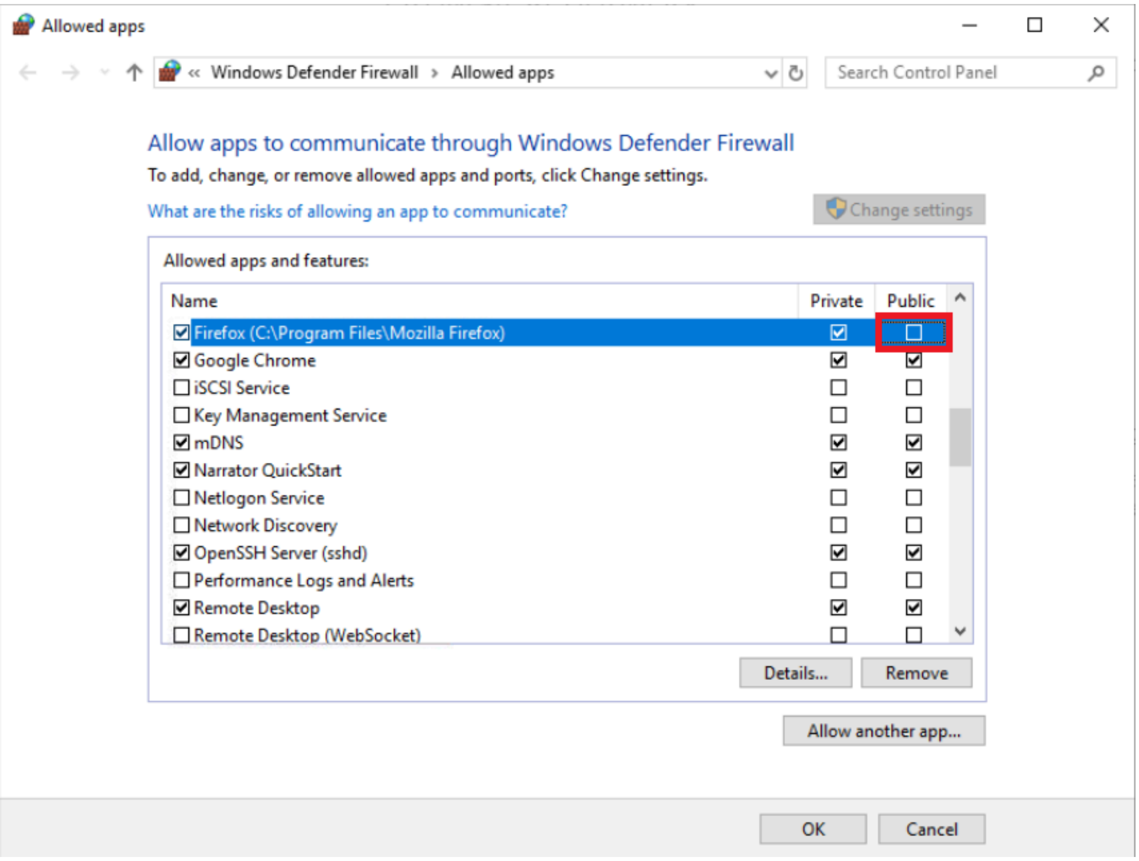
Who's protecting me?

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings
Privacy dashboard
Privacy Statement

5. Here you will see a list of allowed apps and features. Scroll down to Firefox (C:\Program Files\Mozilla Firefox). Notice that communication is permitted on the private, but not the public. Select the box to enable communication on the public network.



Allowed apps

Windows Defender Firewall › Allowed apps

Search Control Panel

Allow apps to communicate through Windows Defender Firewall

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

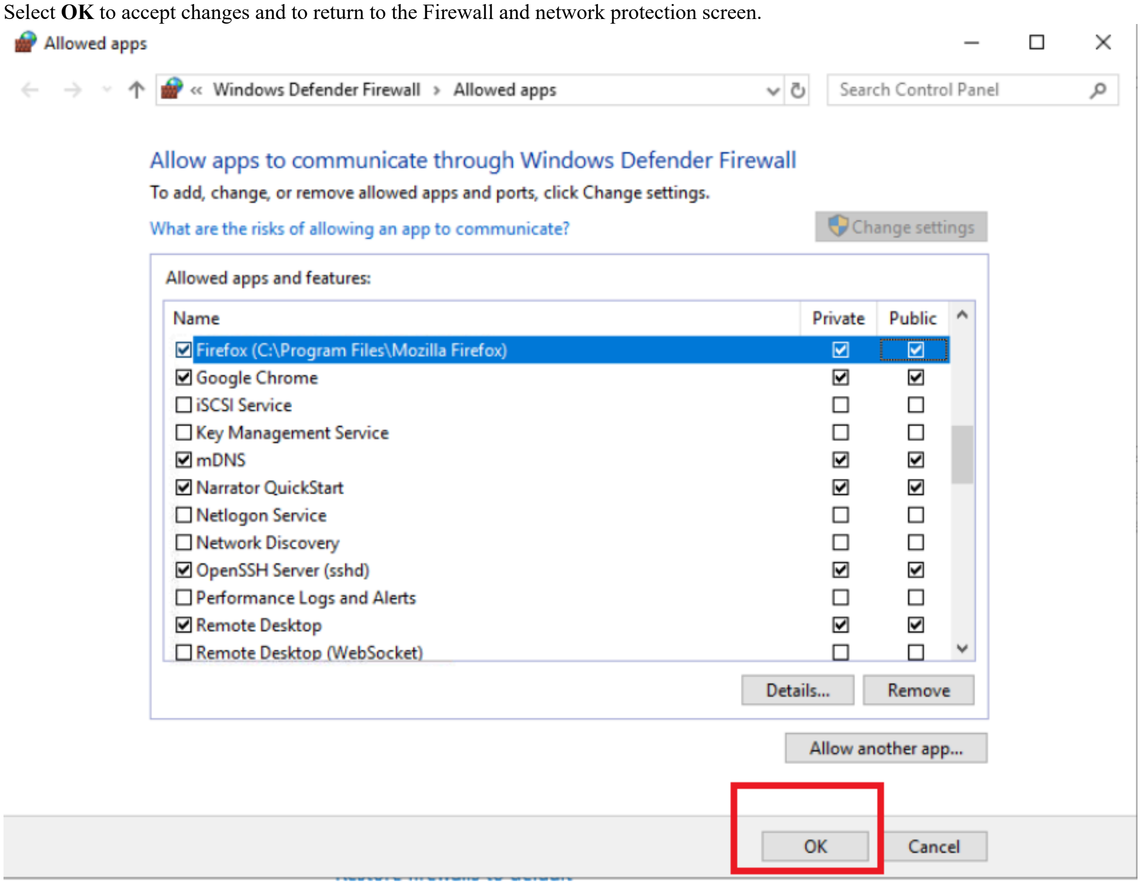
What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

Name	Private	Public
☑ Firefox (C:\Program Files\Mozilla Firefox)	☑	☐
☑ Google Chrome	☑	☑
☐ iSCSI Service	☐	☐
☐ Key Management Service	☐	☐
☑ mDNS	☑	☑
☑ Narrator QuickStart	☑	☑
☐ Netlogon Service	☐	☐
☐ Network Discovery	☐	☐
☑ OpenSSH Server (sshd)	☑	☑
☐ Performance Logs and Alerts	☐	☐
☑ Remote Desktop	☑	☑
☐ Remote Desktop (WebSocket)	☐	☐

6. Select **OK** to accept changes and to return to the Firewall and network protection screen.



Allowed apps

Windows Defender Firewall › Allowed apps

Search Control Panel

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?

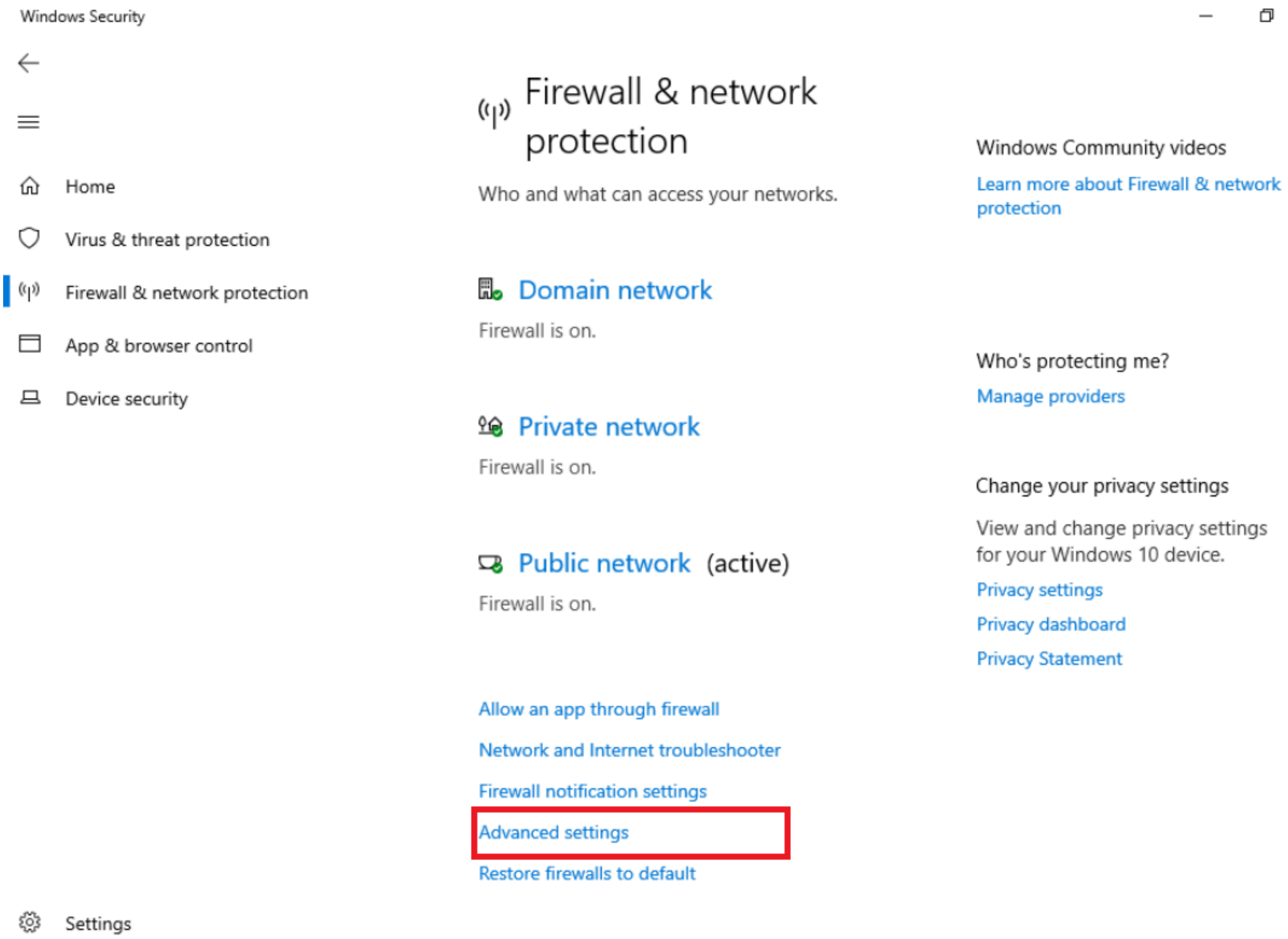
Change settings

Allowed apps and features:

Name	Private	Public
☑ Firefox (C:\Program Files\Mozilla Firefox)	☑	☑
☑ Google Chrome	☑	☑
☐ iSCSI Service	☐	☐
☐ Key Management Service	☐	☐
☑ mDNS	☑	☑
☑ Narrator QuickStart	☑	☑
☐ Netlogon Service	☐	☐
☐ Network Discovery	☐	☐
☑ OpenSSH Server (sshd)	☑	☑
☐ Performance Logs and Alerts	☐	☐
☑ Remote Desktop	☑	☑
☐ Remote Desktop (WebSocket)	☐	☐

Exercise 2: Enable Inbound Rules to Allow Remote Service Management

1. Select **Advanced settings** on the Firewall & network protection screen.



Windows Security
Home
Virus & threat protection
Firewall & network protection
App & browser control
Device 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

Windows Community videos

Learn more about Firewall & network protection

Who's protecting me?

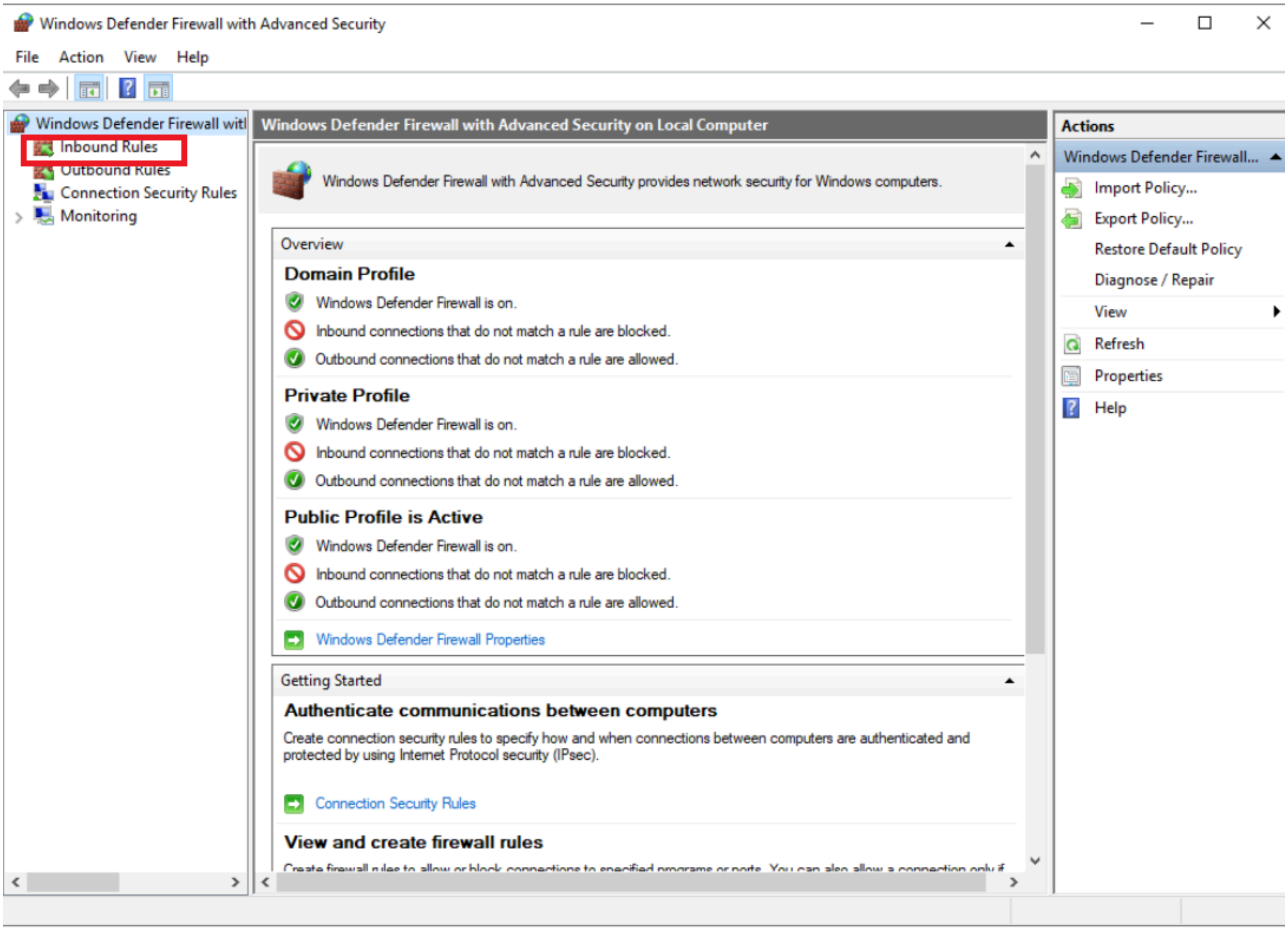
Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings
Privacy dashboard
Privacy Statement

2. Here you will see an **Overview** in the center panel. On the left side, you will see three different rule types:
   – Inbound rules
   – Outbound rules
   – Connection security rules

These rules can be configured to filter traffic based on computers, users, applications, ports, protocols, etc. Select **Inbound rules**.



Windows Defender Firewall with Advanced Security on Local Computer

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

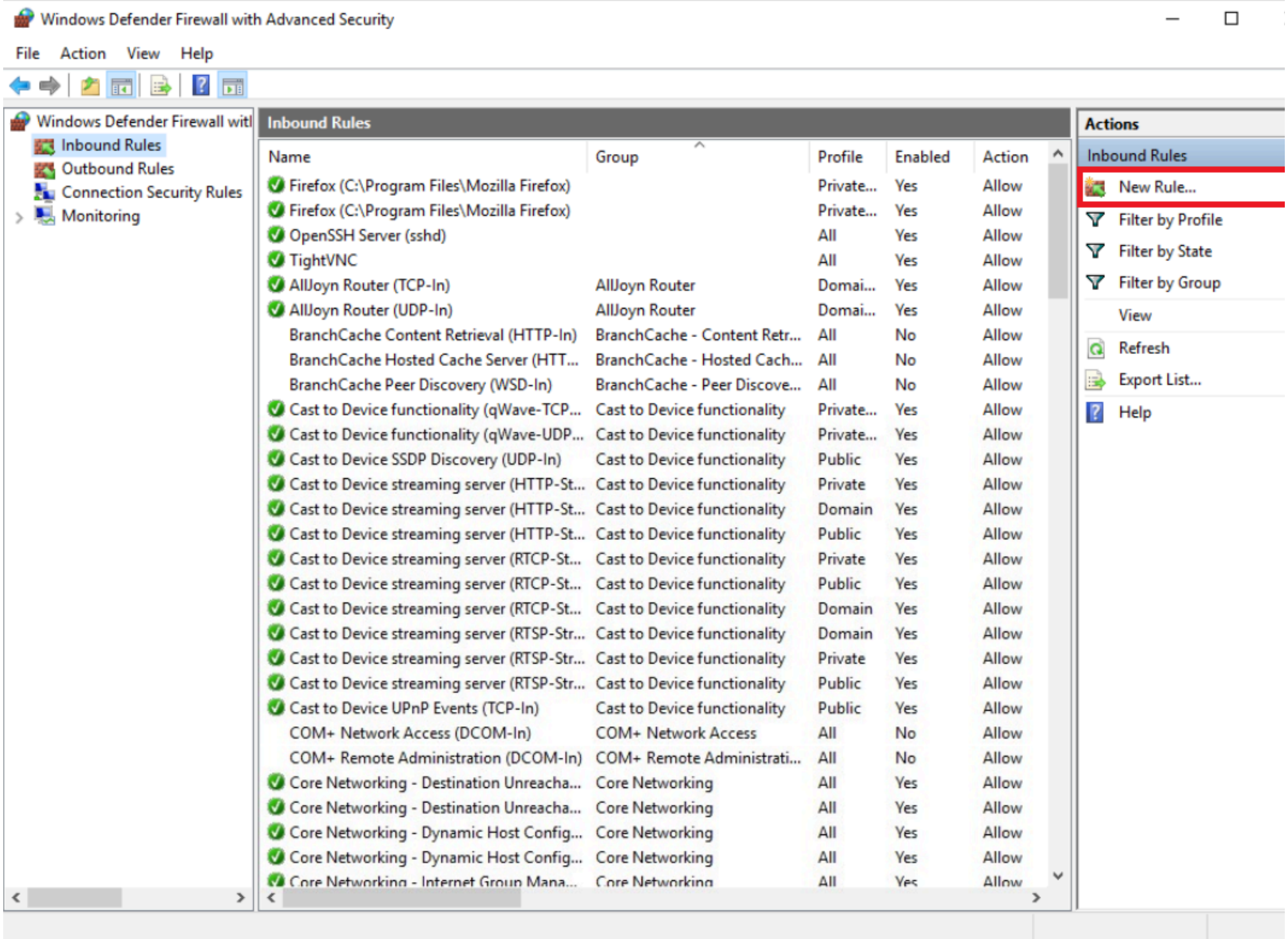
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

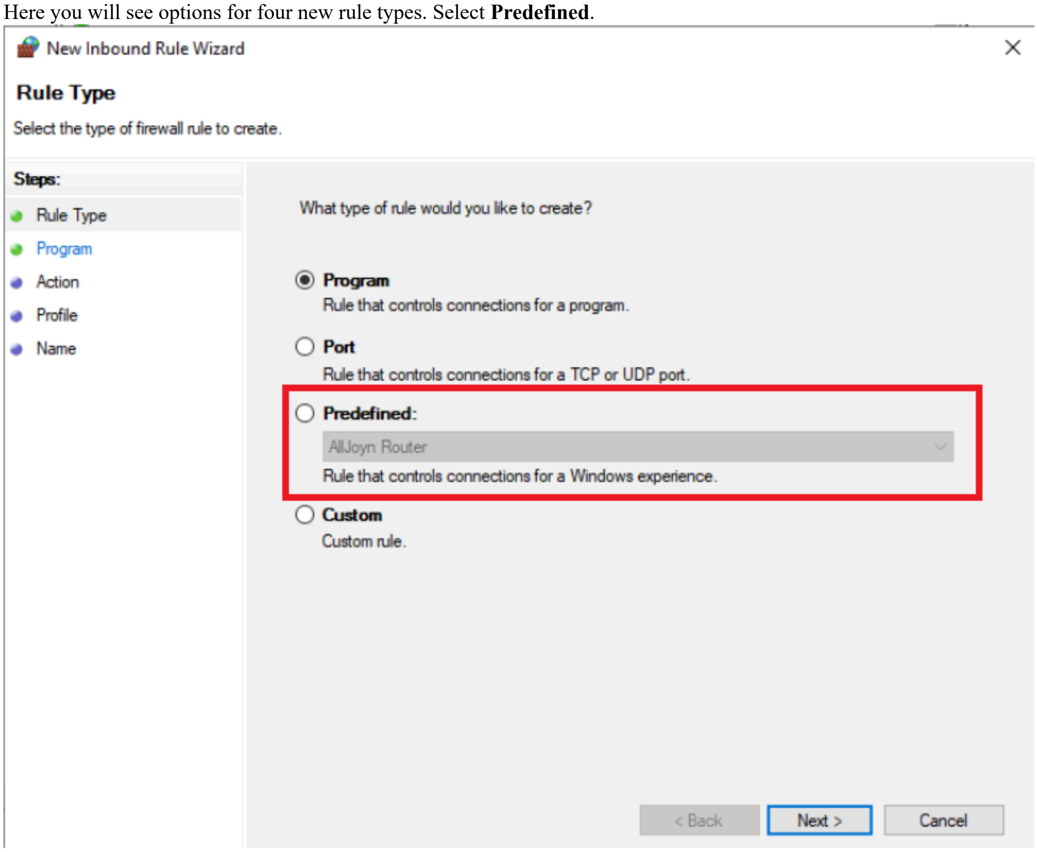
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if

3. Select **New Rule** in the right pane.



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
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes	Allow
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow

4. Here you will see options for four new rule types. Select **Predefined**.



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

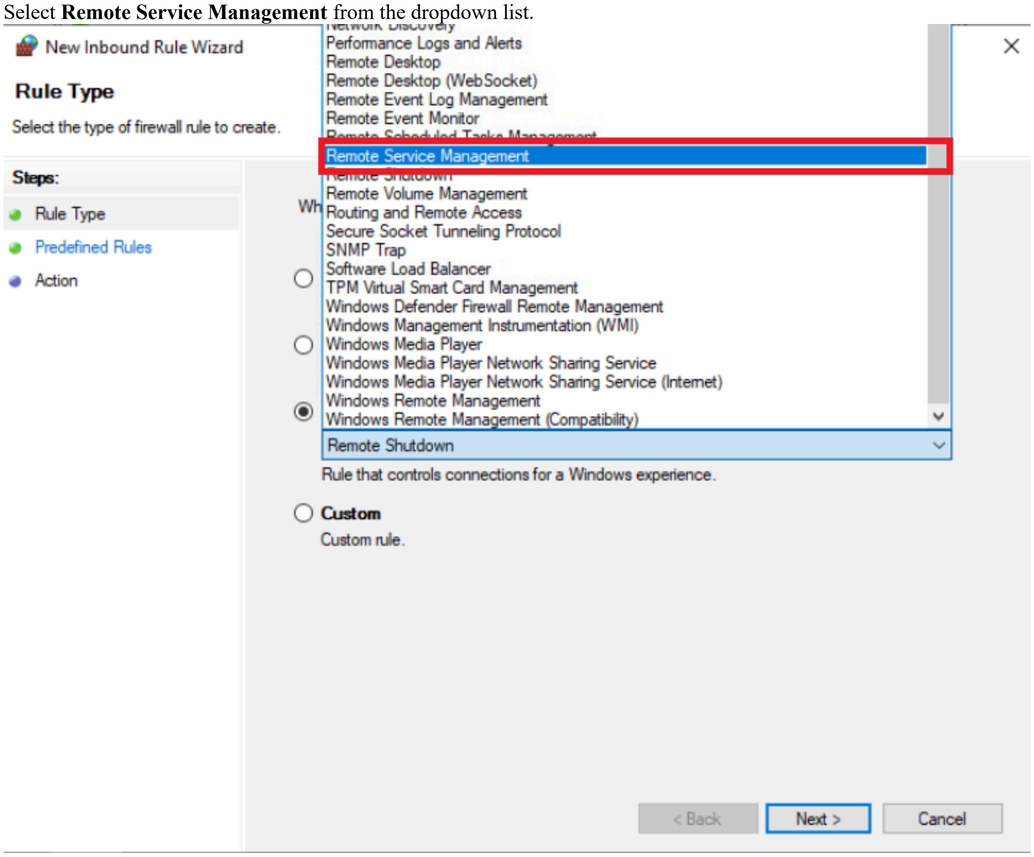
● **Program**
Rule that controls connections for a program.

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

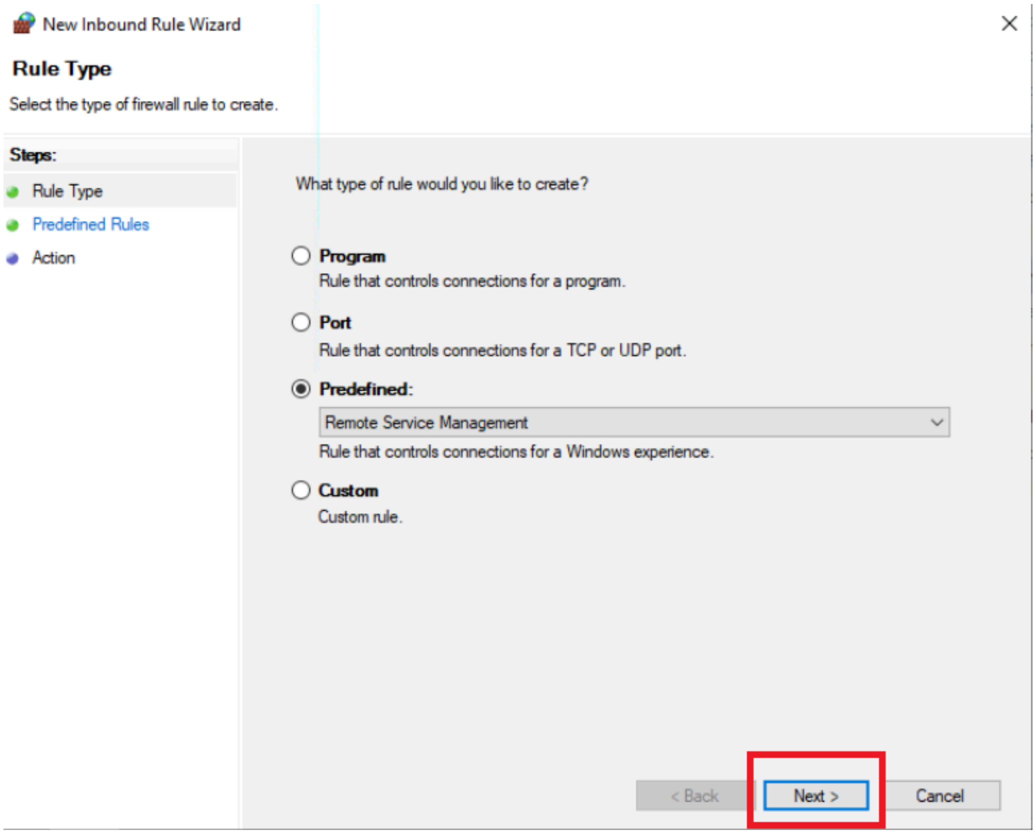
○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

5. Select **Remote Service Management** from the dropdown list.


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Predefined Rules
Action
Wh
Network Discovery
Performance Logs and Alerts
Remote Desktop
Remote Desktop (WebSocket)
Remote Event Log Management
Remote Event Monitor
Remote Scheduled Tasks Management
Remote Service Management
Remote Shutdown
Remote Volume Management
Routing and Remote Access
Secure Socket Tunneling Protocol
SNMP Trap
Software Load Balancer
TPM Virtual Smart Card Management
Windows Defender Firewall Remote Management
Windows Management Instrumentation (WMI)
Windows Media Player
Windows Media Player Network Sharing Service
Windows Media Player Network Sharing Service (Internet)
Windows Remote Management
Windows Remote Management (Compatibility)
Remote Shutdown
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

6. Select **Next** to continue.



What type of rule would you like to create?

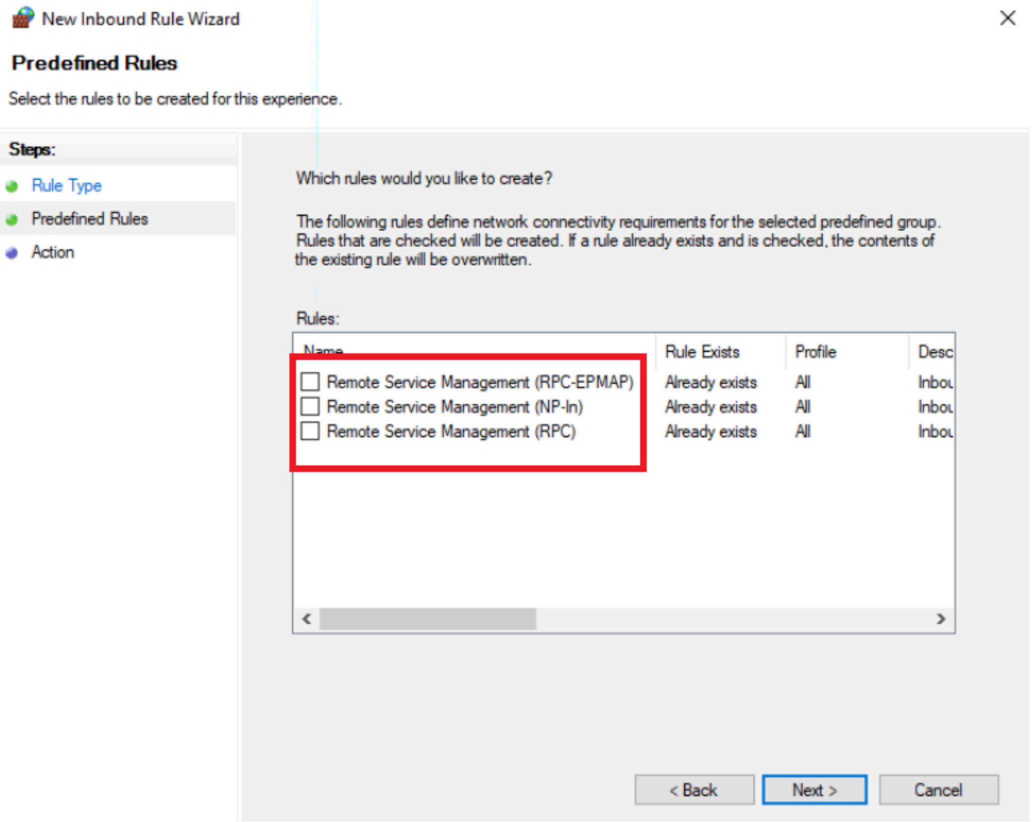
○ **Program**
Rule that controls connections for a program.

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

● **Predefined:**
Remote Service Management
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

7. Check the boxes for **Remote Service Management (RPC-EPMAP)**, **Remote Service Management (NP-IN)**, and **Remote Service Management (RPC)**.



Predefined Rules

Select the rules to be created for this experience.

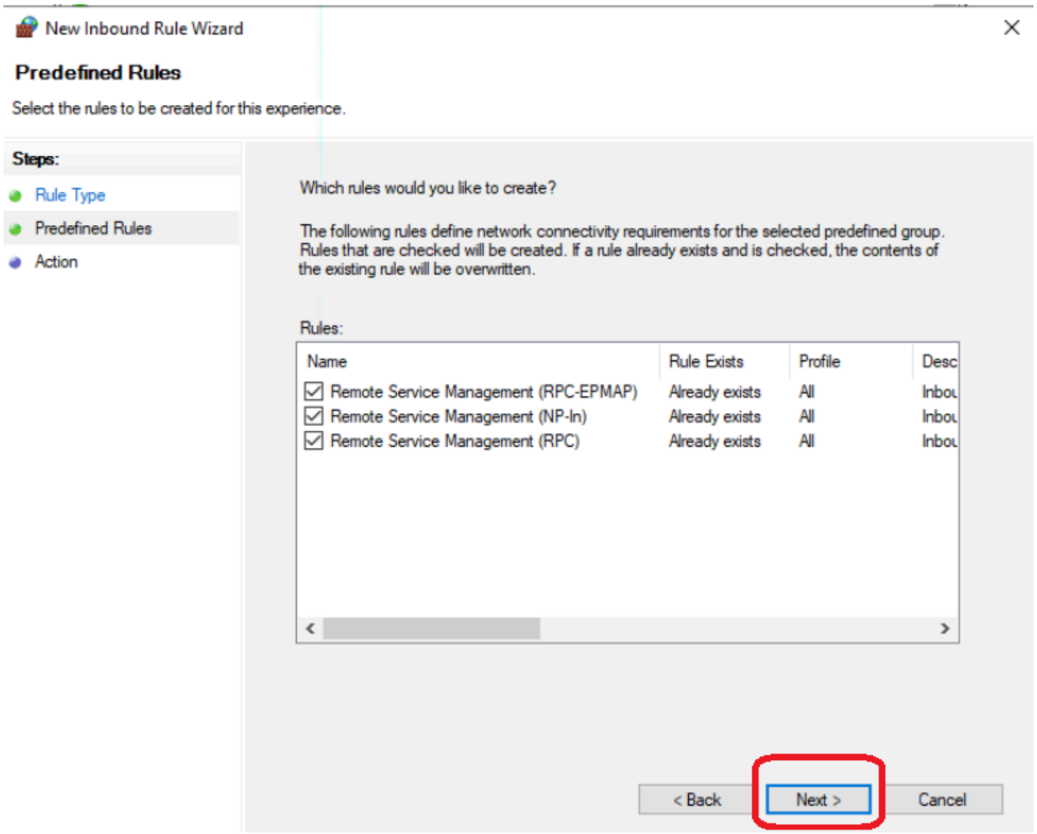
Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:

Name	Rule Exists	Profile	Desc
□ Remote Service Management (RPC-EPMAP)	Already exists	All	Inbou
□ Remote Service Management (NP-In)	Already exists	All	Inbou
□ Remote Service Management (RPC)	Already exists	All	Inbou

8. Select **Next** to continue.



Predefined Rules

Select the rules to be created for this experience.

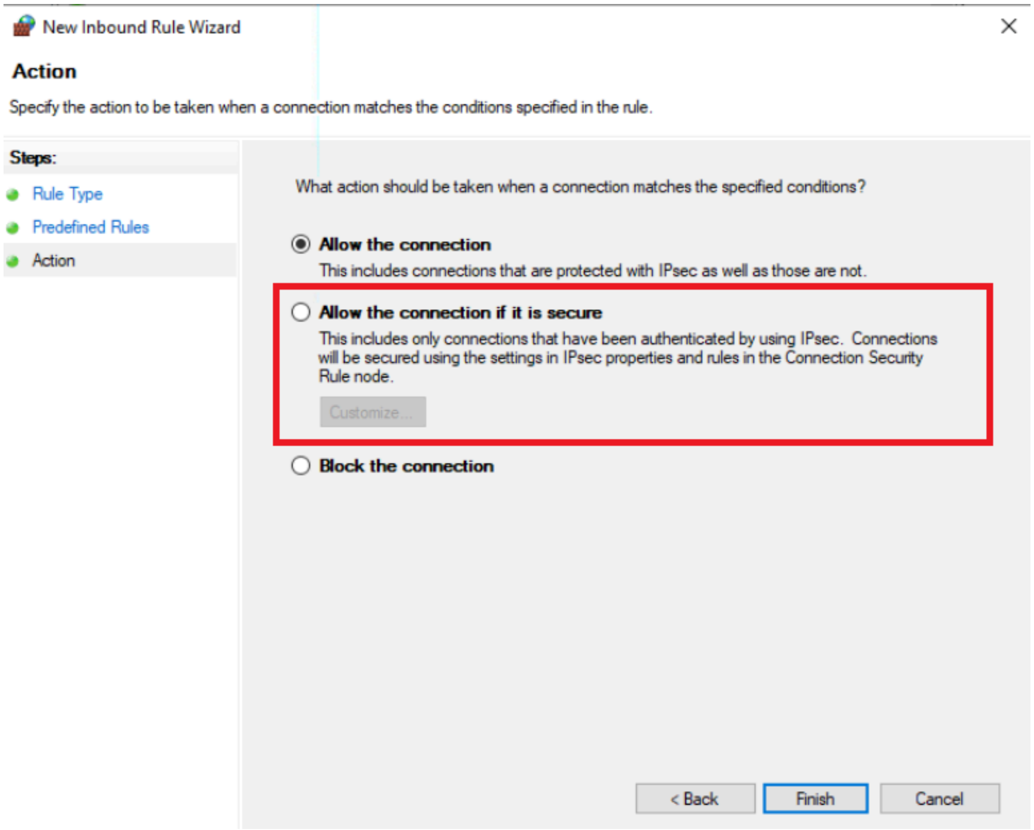
Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:

Name	Rule Exists	Profile	Desc
☑ Remote Service Management (RPC-EPMAP)	Already exists	All	Inbou
☑ Remote Service Management (NP-In)	Already exists	All	Inbou
☑ Remote Service Management (RPC)	Already exists	All	Inbou

9. Select **Allow the connection if it is secure**.



New Inbound Rule Wizard

Action

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

Steps:

- Rule Type
- Predefined Rules
- Action

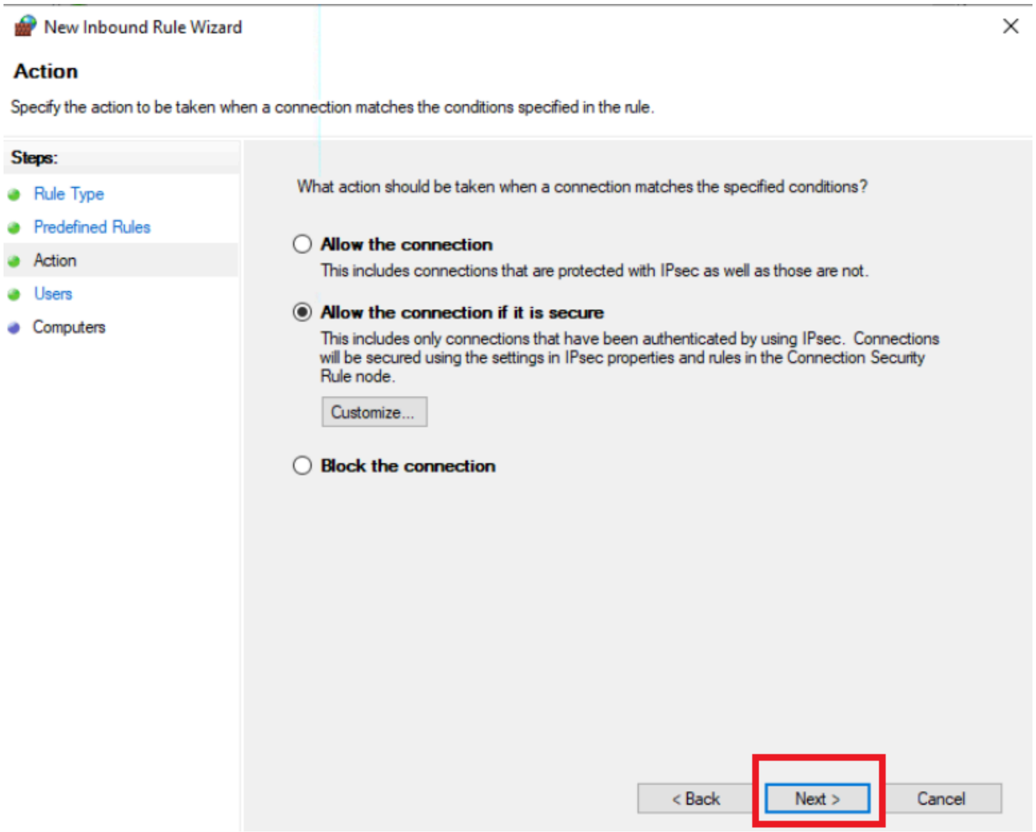
What action should be taken when a connection matches the specified conditions?

● **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**

10. Select **Next**.



New Inbound Rule Wizard

Action

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

Steps:

- Rule Type
- Predefined Rules
- Action
- Users
- Computers

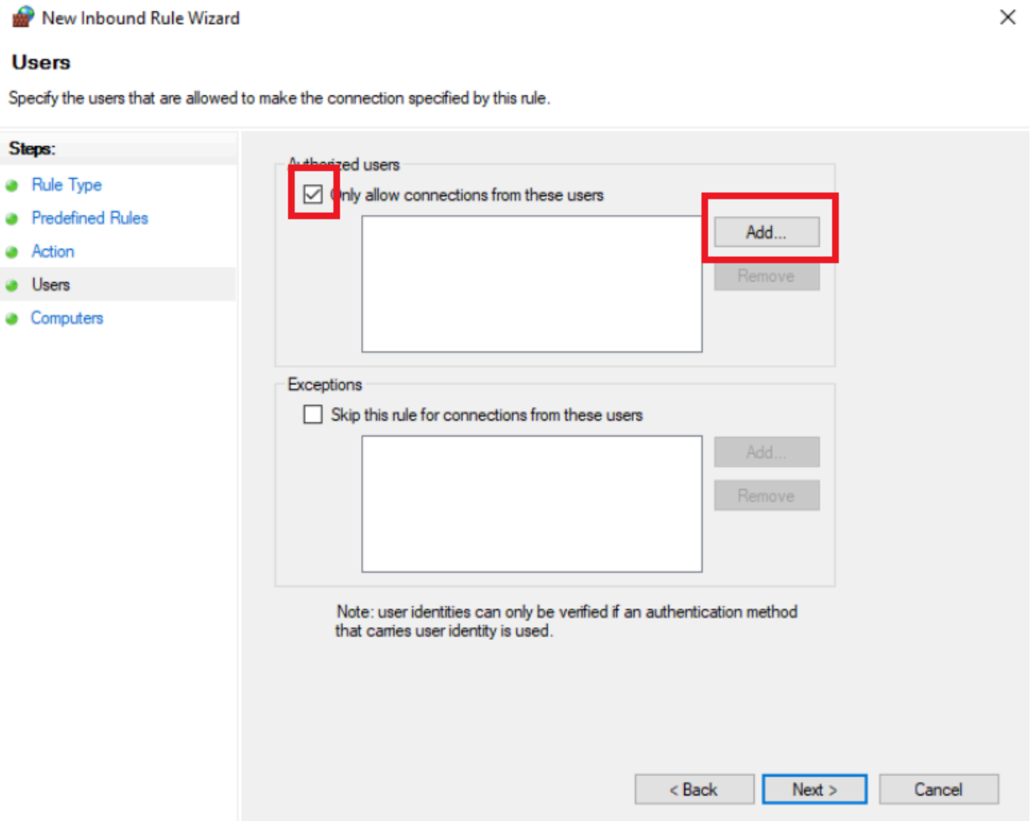
What action should be taken when a connection matches the specified conditions?

○ **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.

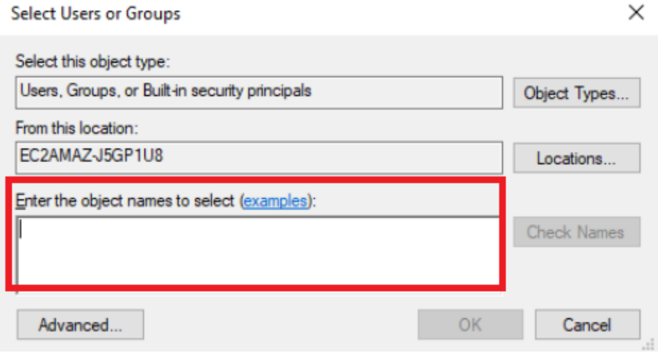
○ **Block the connection**

11. Verify that the box to **only allow connections from these users** has been checked. Select **Add** to add an authorized user.

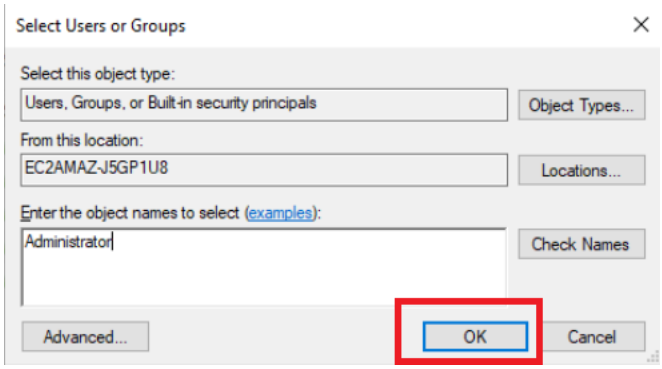


New Inbound Rule Wizard
Users
Specify the users that are allowed to make the connection specified by this rule.
Steps:
Rule Type
Predefined Rules
Action
Users
Computers
Authorized users
☑ Only allow connections from these users
Add...
Remove
Exceptions
□ Skip this rule for connections from these users
Add...
Remove
Note: user identities can only be verified if an authentication method that carries user identity is used.
< Back
Next >
Cancel

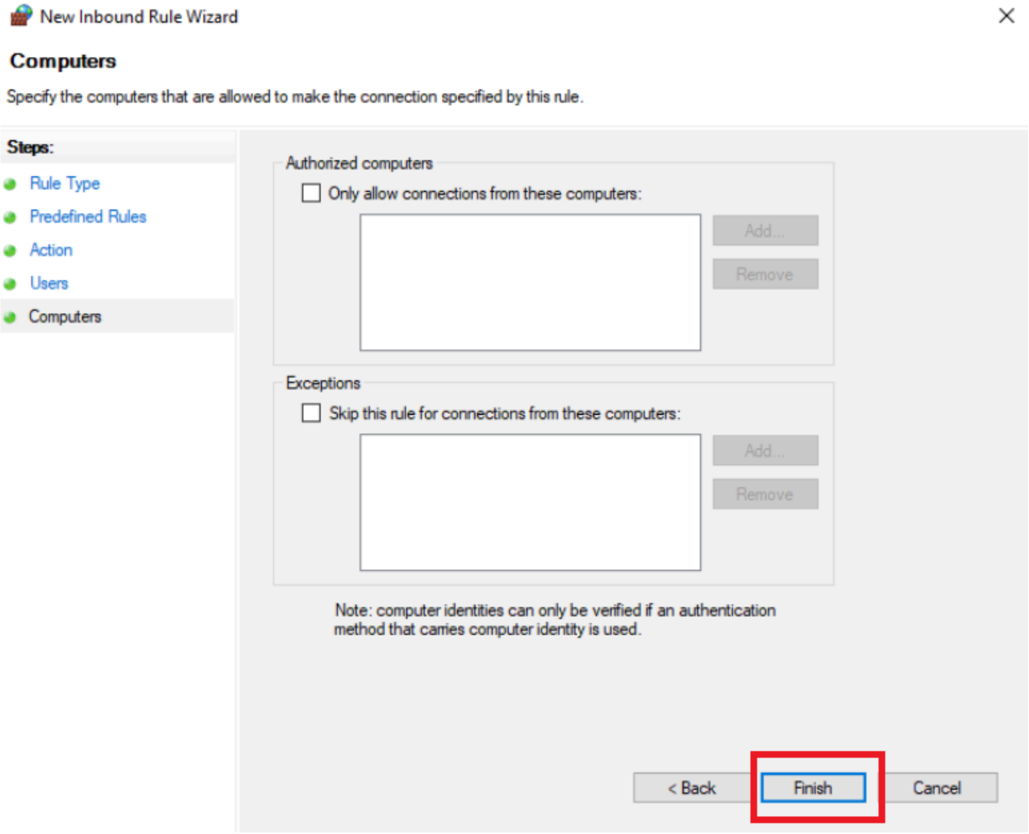
12. Enter "Administrator" into the **Enter the object names to select** box.



13. Select **OK**.



14. Click **Next** and Select **Finish**.

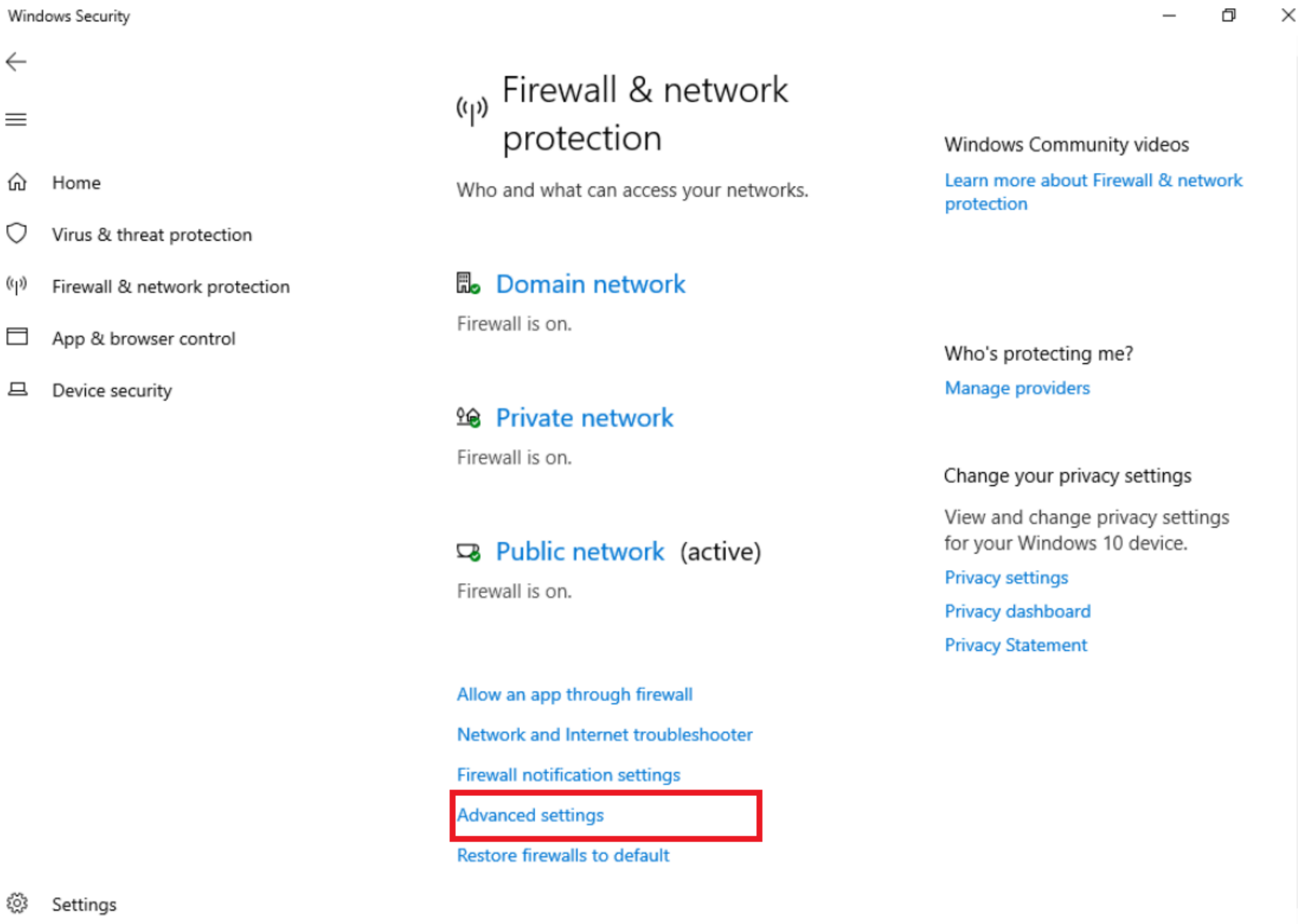


New Inbound Rule Wizard
Computers
Specify the computers that are allowed to make the connection specified by this rule.
Steps:
Rule Type
Predefined Rules
Action
Users
Computers
Authorized computers
□ Only allow connections from these computers:
Add...
Remove
Exceptions
□ Skip this rule for connections from these computers:
Add...
Remove
Note: computer identities can only be verified if an authentication method that carries computer identity is used.
< Back
Finish
Cancel

Exercise 3: 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



Windows Security

Home

Virus & threat protection

Firewall & network protection

App & browser control

Device 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

Windows Community videos

Learn more about Firewall & network protection

Who's protecting me?

Manage providers

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

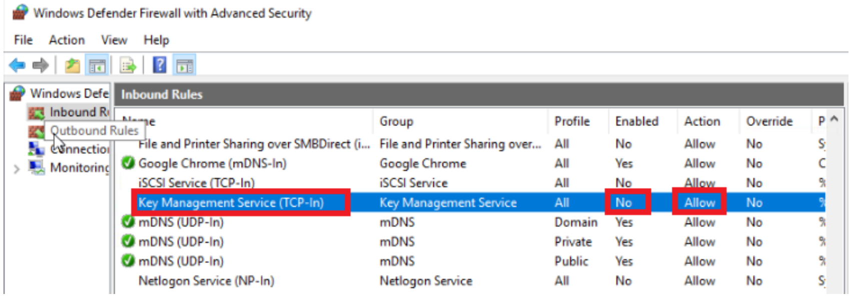
Privacy dashboard

Privacy Statement

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**.)

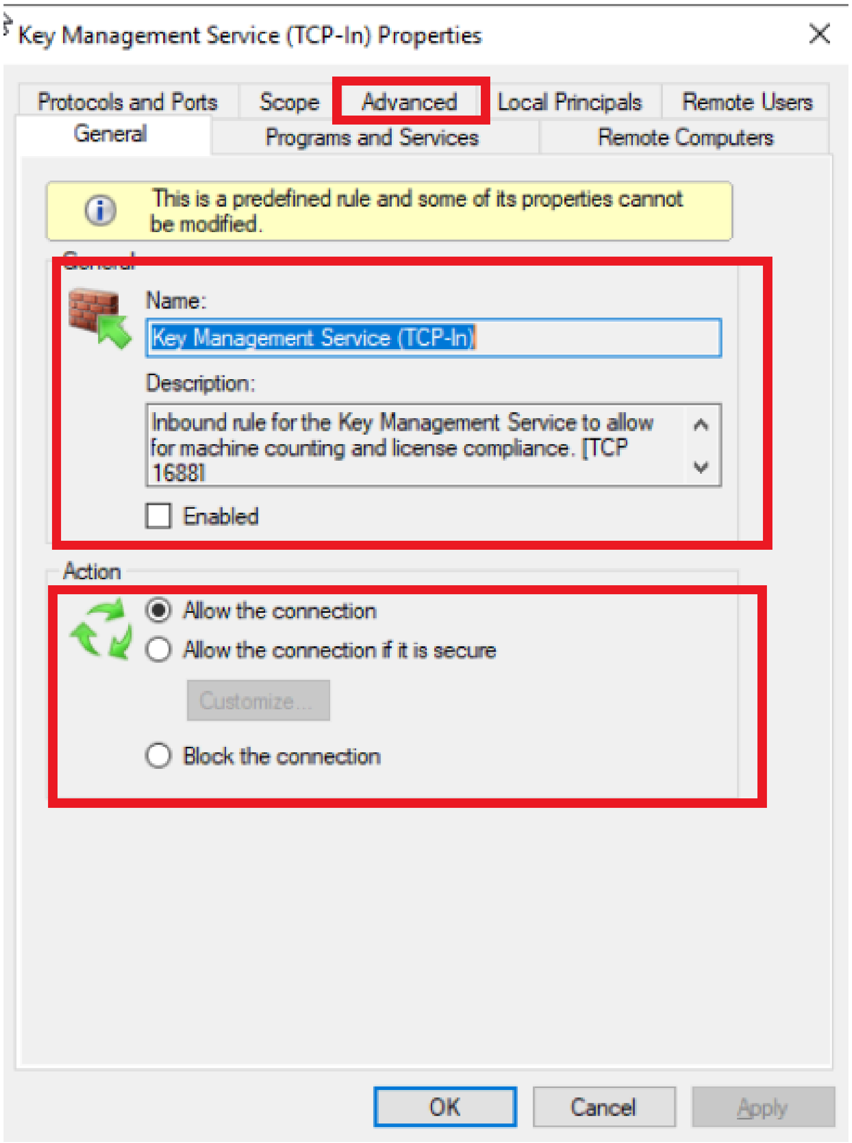
  Double-click this rule.



Inbound Rules

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.



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

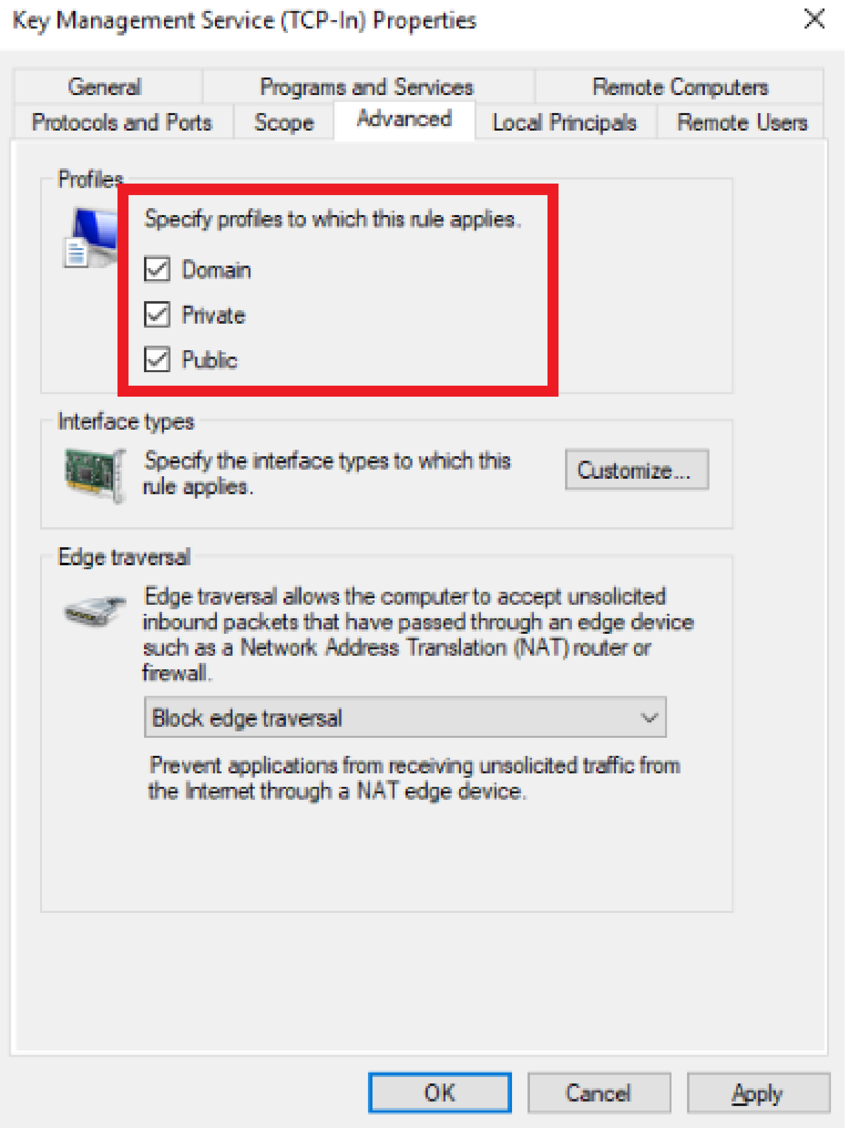
Action

● Allow the connection

○ Allow the connection if it is secure

○ Block the connection

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.

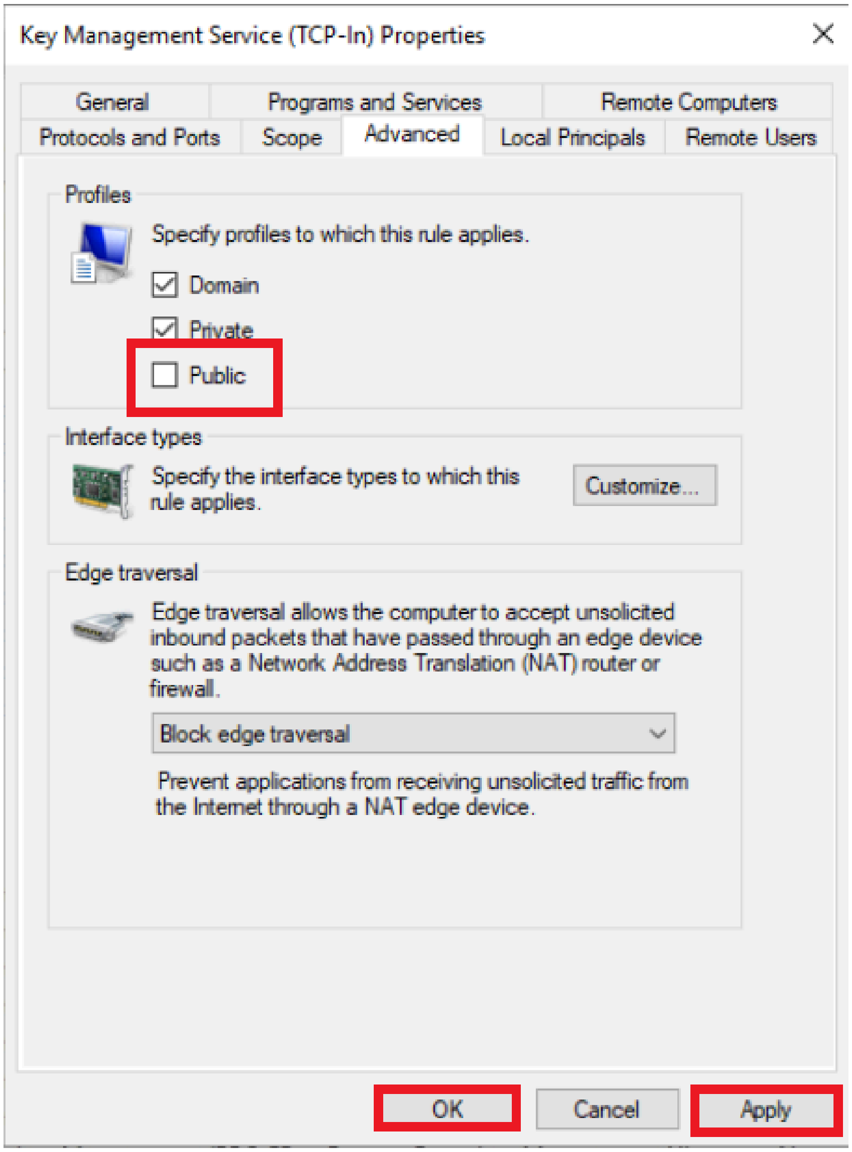
Edge traversal

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.

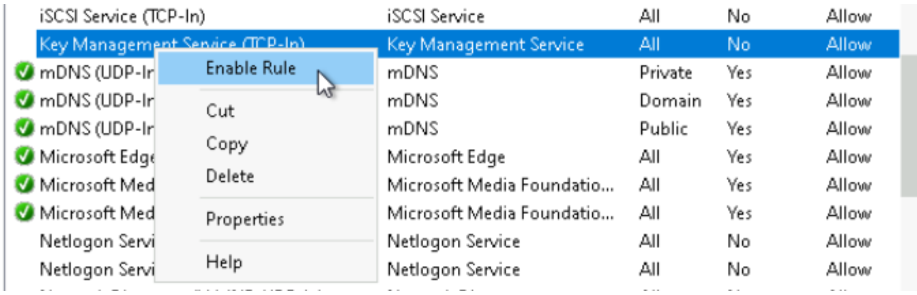
Edge traversal

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

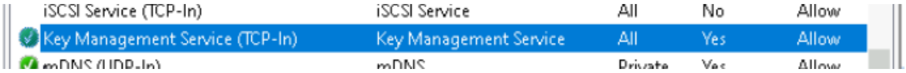
Prevent applications from receiving unsolicited traffic from the Internet through a NAT edge device.

6. Next, right click on Key Management Service(TCP-In) and select Enable Rule.



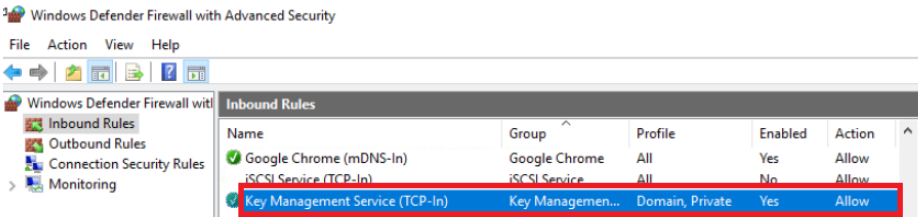
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
Key Management Service (TCP-In)	Key Management Service	All	No	Allow
✓ mDNS (UDP-In	mDNS	Private	Yes	Allow
✓ mDNS (UDP-In	mDNS	Domain	Yes	Allow
✓ mDNS (UDP-In	mDNS	Public	Yes	Allow
✓ Microsoft Edge	Microsoft Edge	All	Yes	Allow
✓ Microsoft Med	Microsoft Media Foundatio...	All	Yes	Allow
✓ Microsoft Med	Microsoft Media Foundatio...	All	Yes	Allow
Netlogon Servi	Netlogon Service	All	No	Allow
Netlogon Servi	Netlogon Service	All	No	Allow

This will be set as **Yes** which means now the communication with the domain and private network is allowed.



iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
✓ Key Management Service (TCP-In)	Key Management Service	All	Yes	Allow
✓ mDNS (UDP-In)	mDNS	Private	Yes	Allow

7. 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.

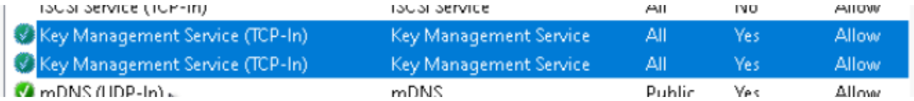


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Inbound Rules

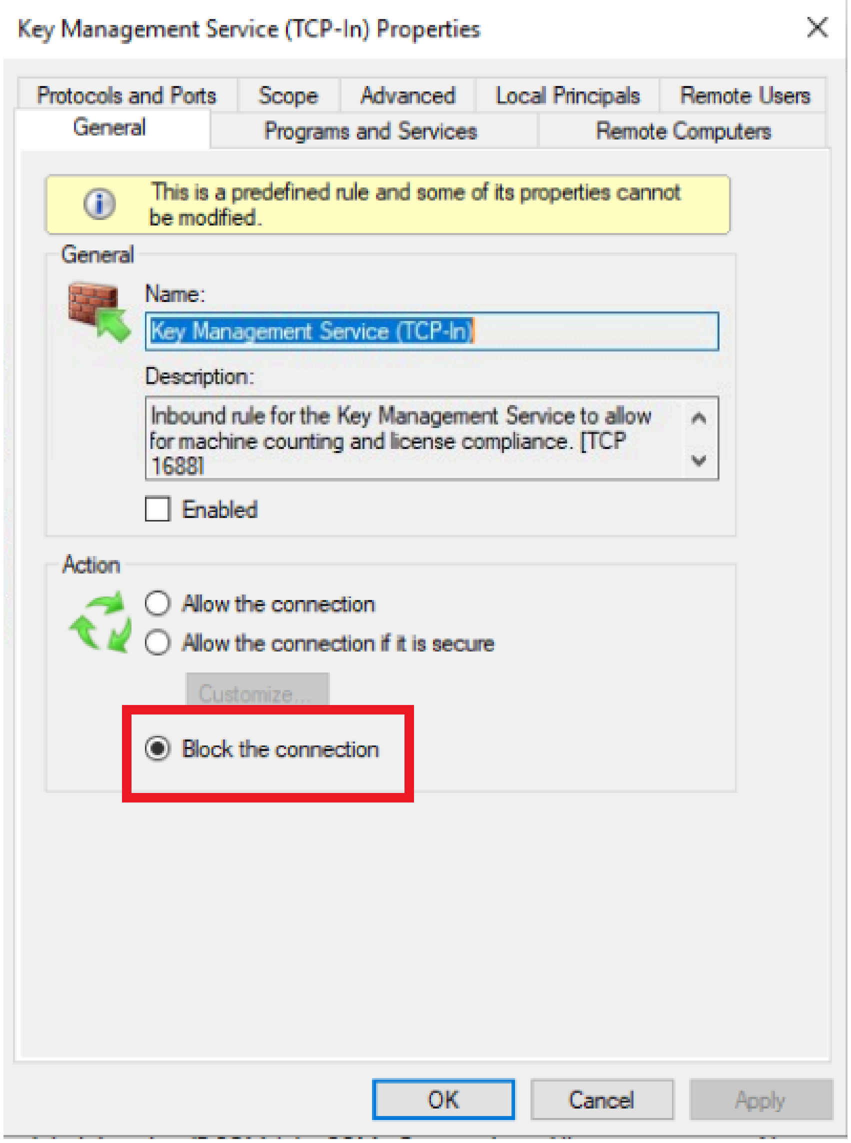
Name	Group	Profile	Enabled	Action
✓ Google Chrome (mDNS-In)	Google Chrome	All	Yes	Allow
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
✓ Key Management Service (TCP-In)	Key Managemen...	Domain, Private	Yes	Allow

8. 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.



iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
Key Management Service (TCP-In)	Key Management Service	All	Yes	Allow
Key Management Service (TCP-In)	Key Management Service	All	Yes	Allow
mDNS (UDP-In)	mDNS	Public	Yes	Allow

9. 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

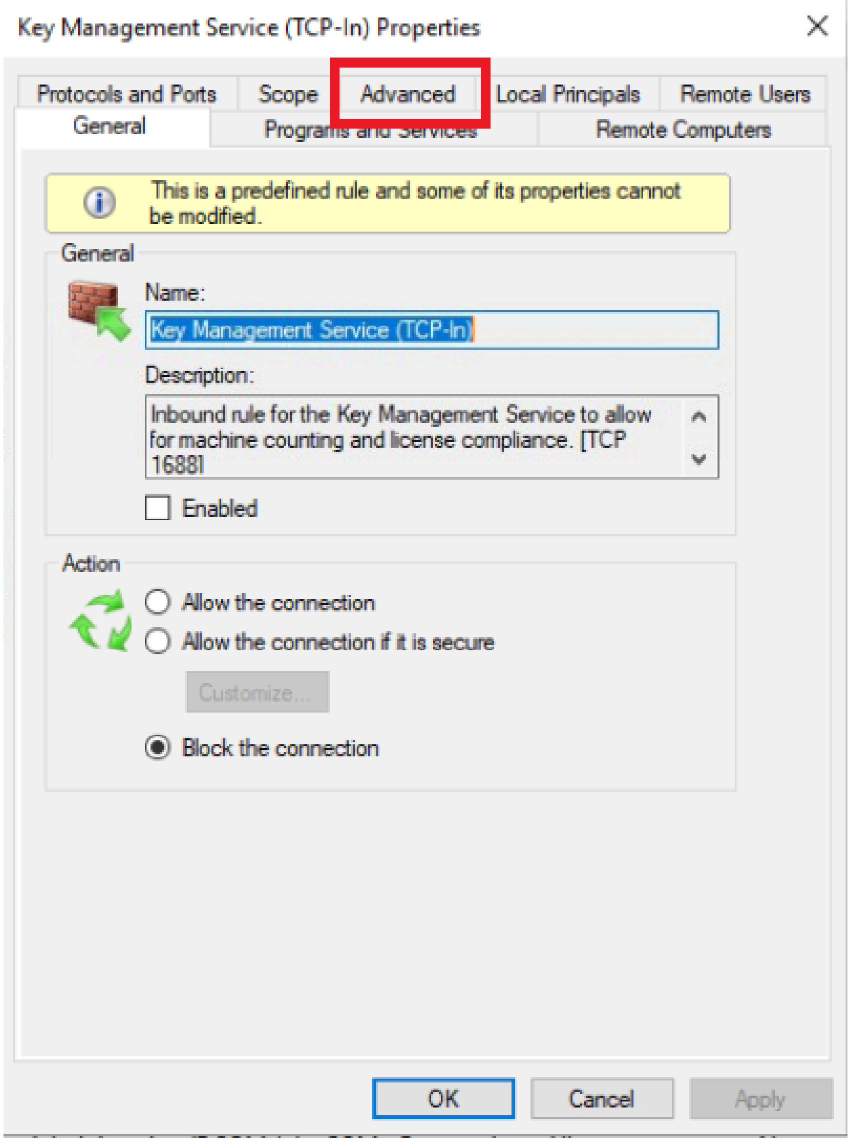
Action

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

10. Click the **Advanced** tab.



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

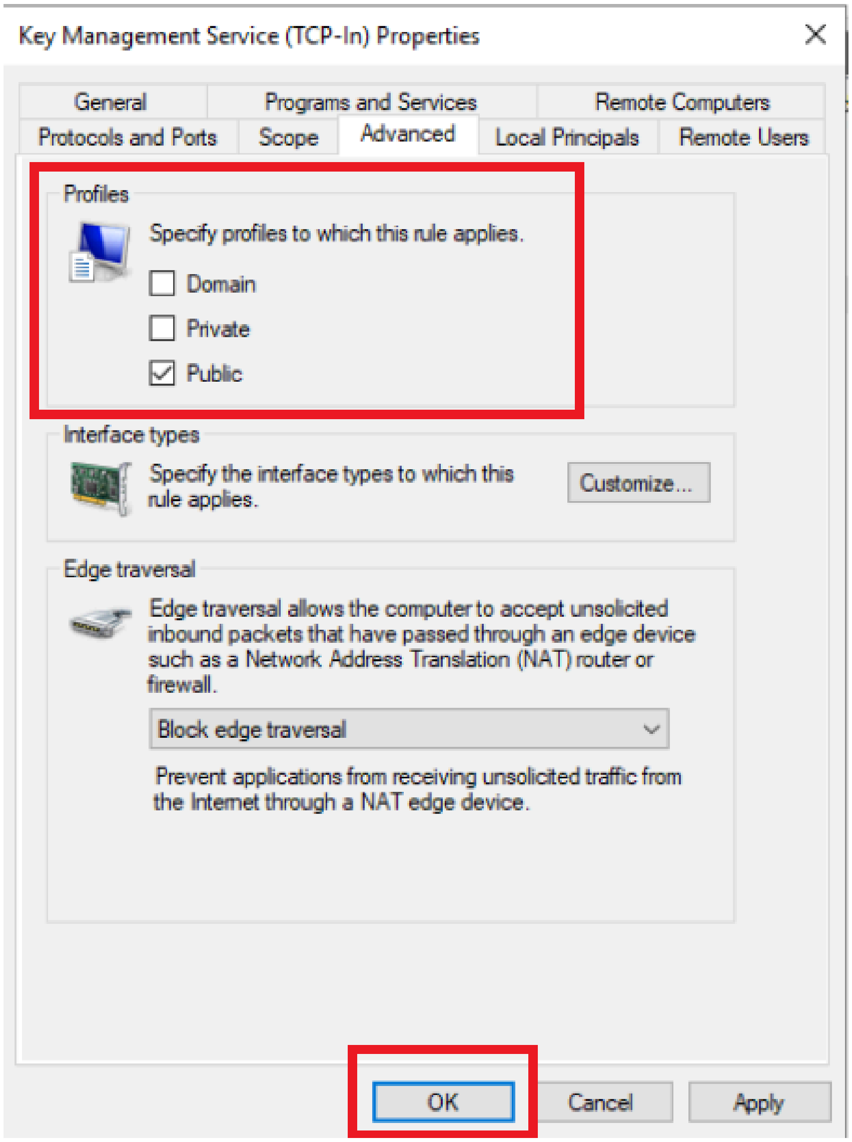
Action

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

11. 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.

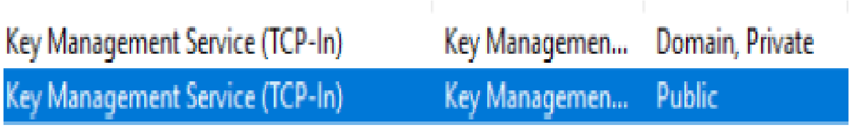
Edge traversal

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

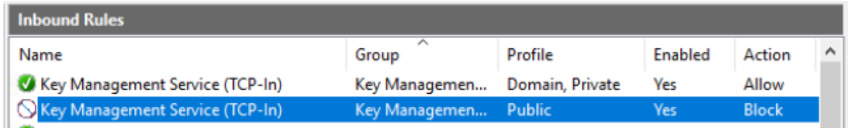
Prevent applications from receiving unsolicited traffic from the Internet through a NAT edge device.

12. 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

13. 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

Author(s)

Dee Dee Collette