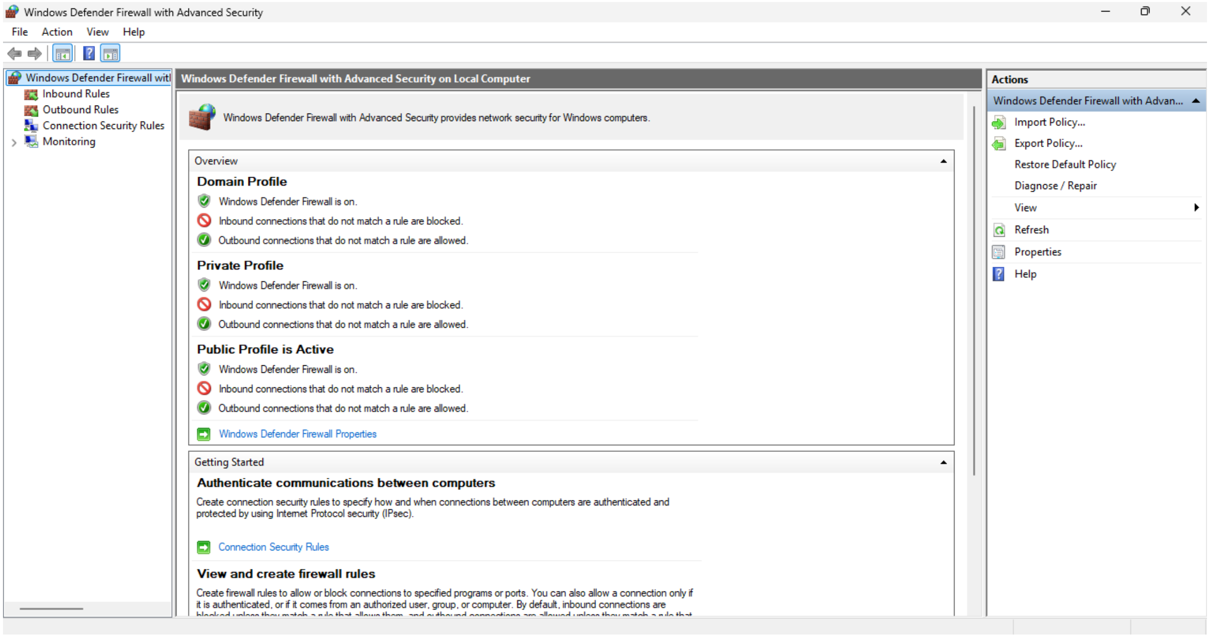
TASK 4



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

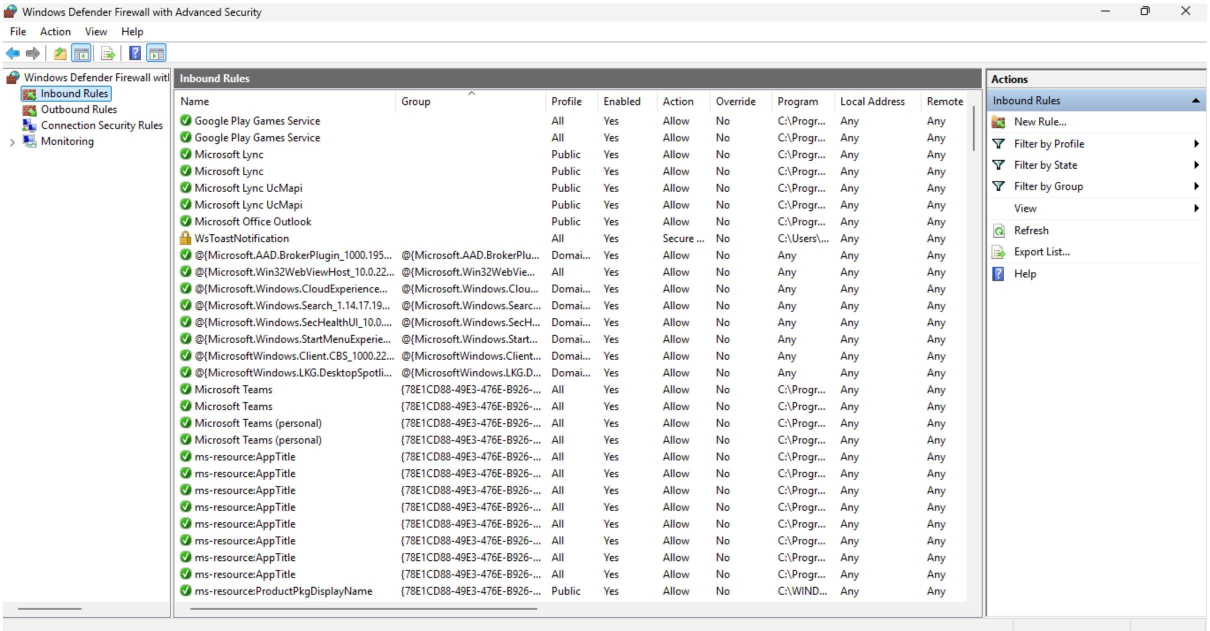
Authenticate communications between computers

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

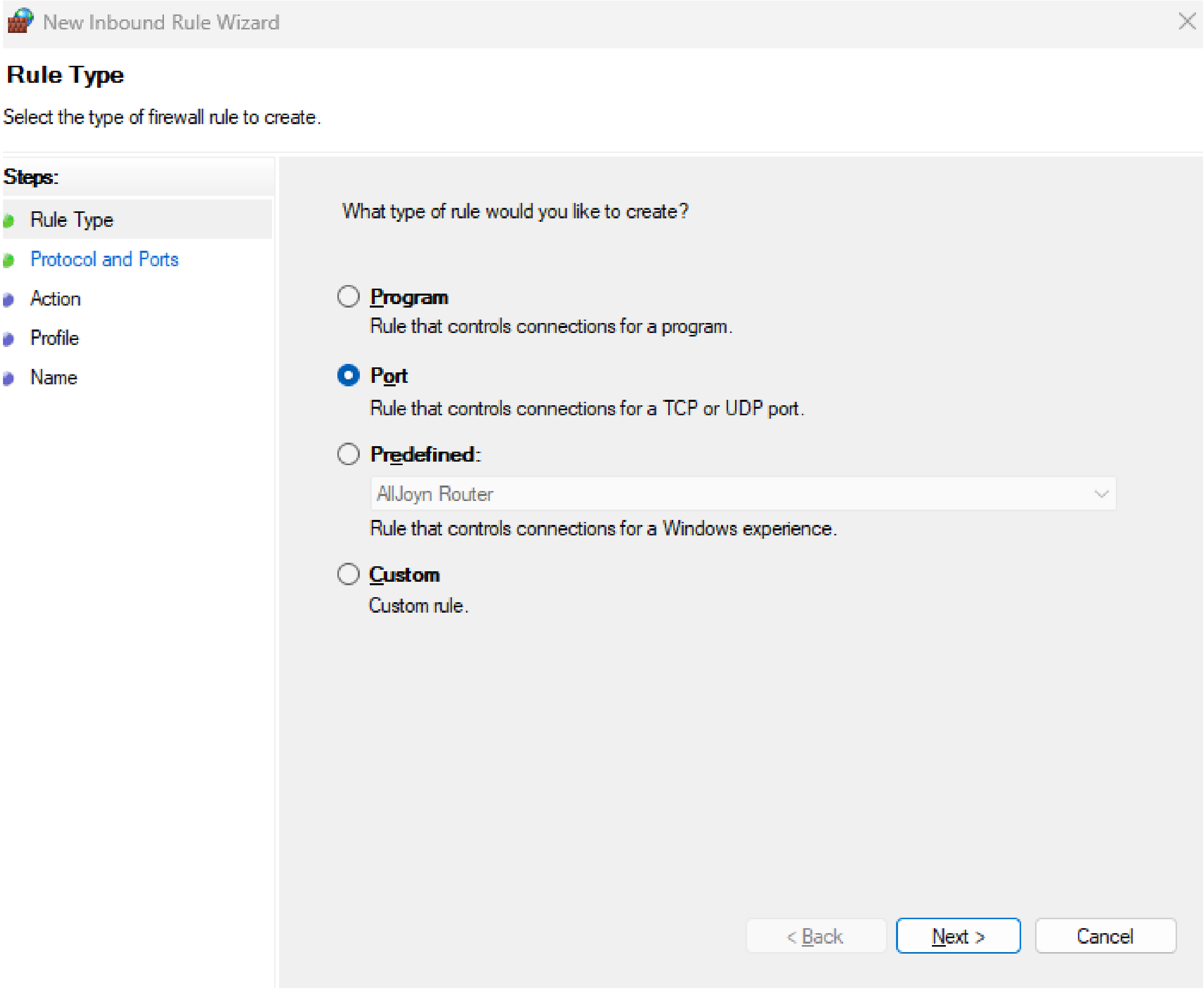
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
Google Play Games Service		All	Yes	Allow	No	C:\Progr...	Any	Any
Google Play Games Service		All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Lync		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Lync		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Lync UcMapi		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Lync UcMapi		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any
WsToastNotification		All	Yes	Secure ...	No	C:\Users\...	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Search_1.14.17.19...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.SecHealthUI_10.0....	@{Microsoft.Windows.SecH...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any
@{MicrosoftWindows.Client.CBS_1000.22...	@{MicrosoftWindows.Client...	Domai...	Yes	Allow	No	Any	Any	Any
@{MicrosoftWindows.LKG.DesktopSpotli...	@{MicrosoftWindows.LKG.D...	Domai...	Yes	Allow	No	Any	Any	Any
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

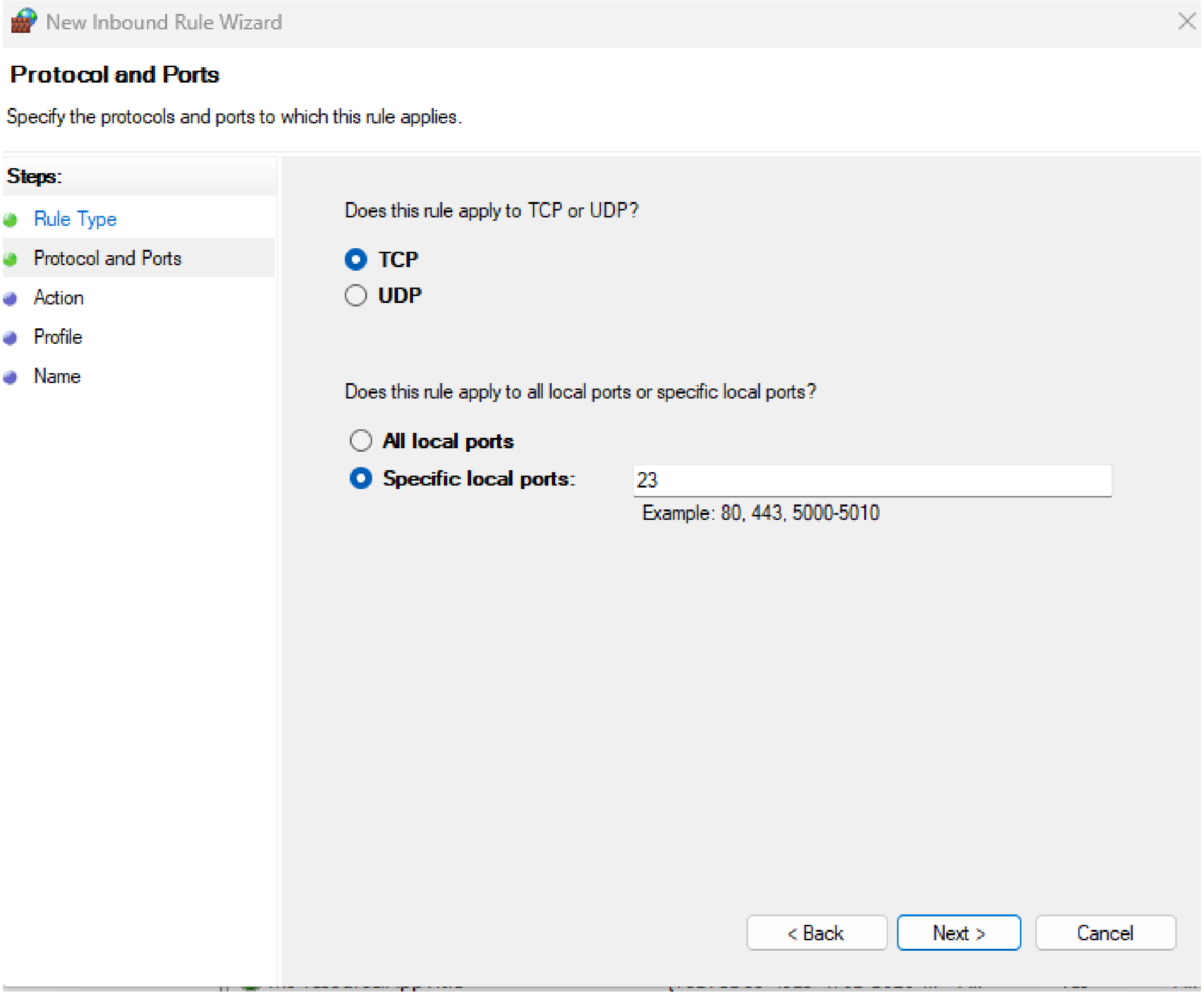
What type of rule would you like to create?

○ Program
Rule that controls connections for a program.

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

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

○ Custom
Custom rule.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

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

Does this rule apply to TCP or UDP?

● **TCP**

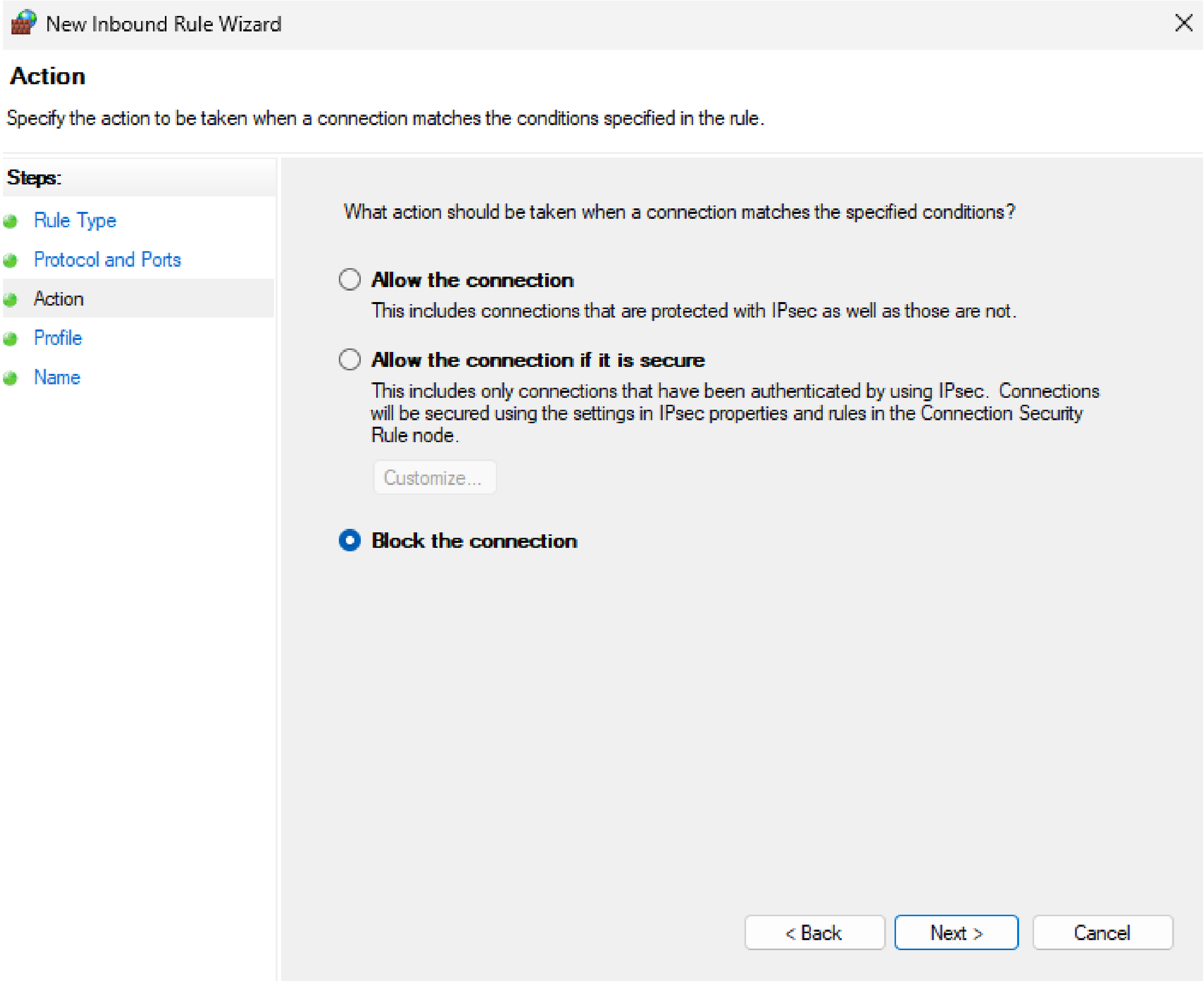
○ **UDP**

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

○ **All local ports**

● **Specific local ports:** 23

Example: 80, 443, 5000-5010



New Inbound Rule Wizard

Action

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

Steps:

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

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

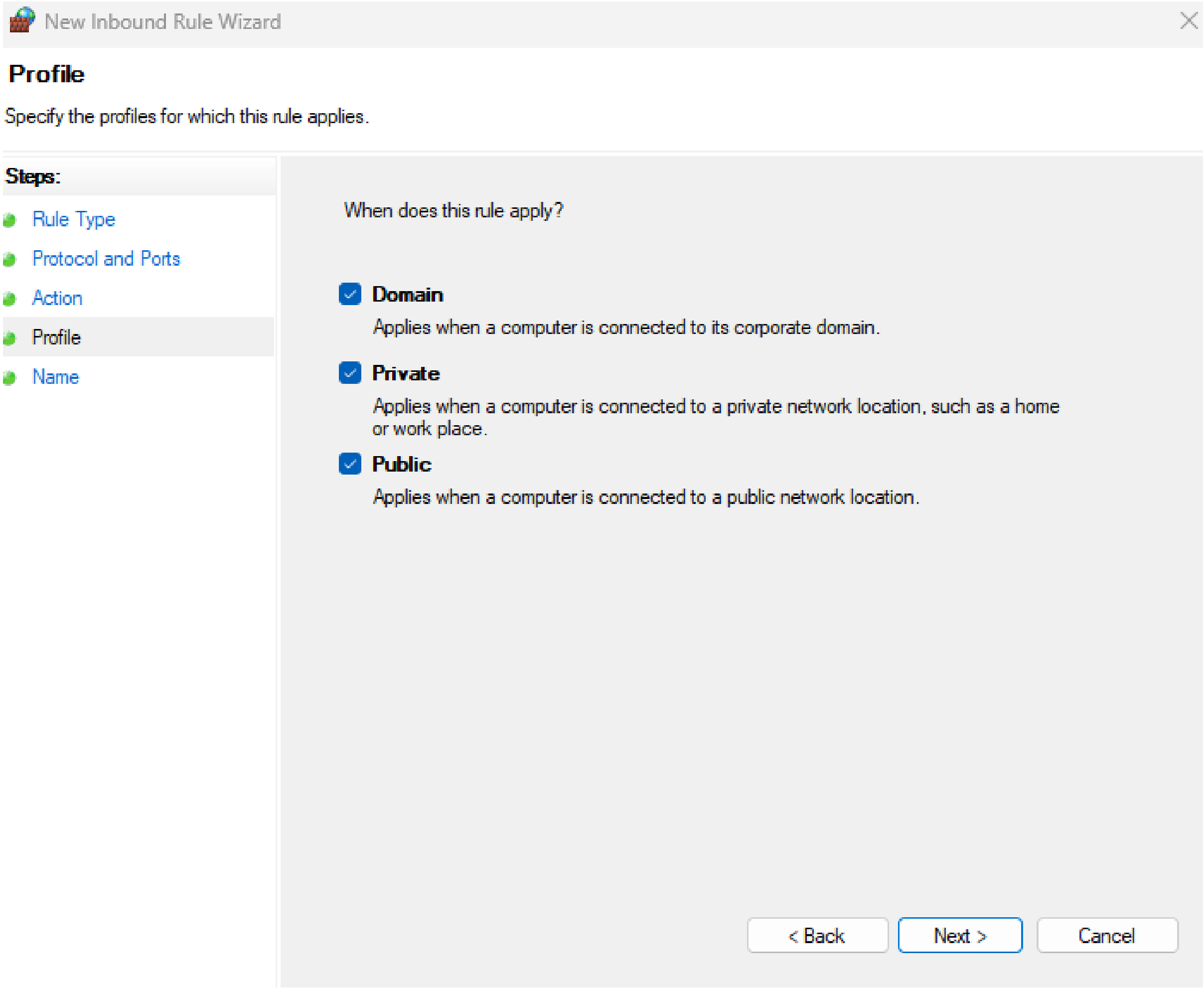
○ **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**



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**

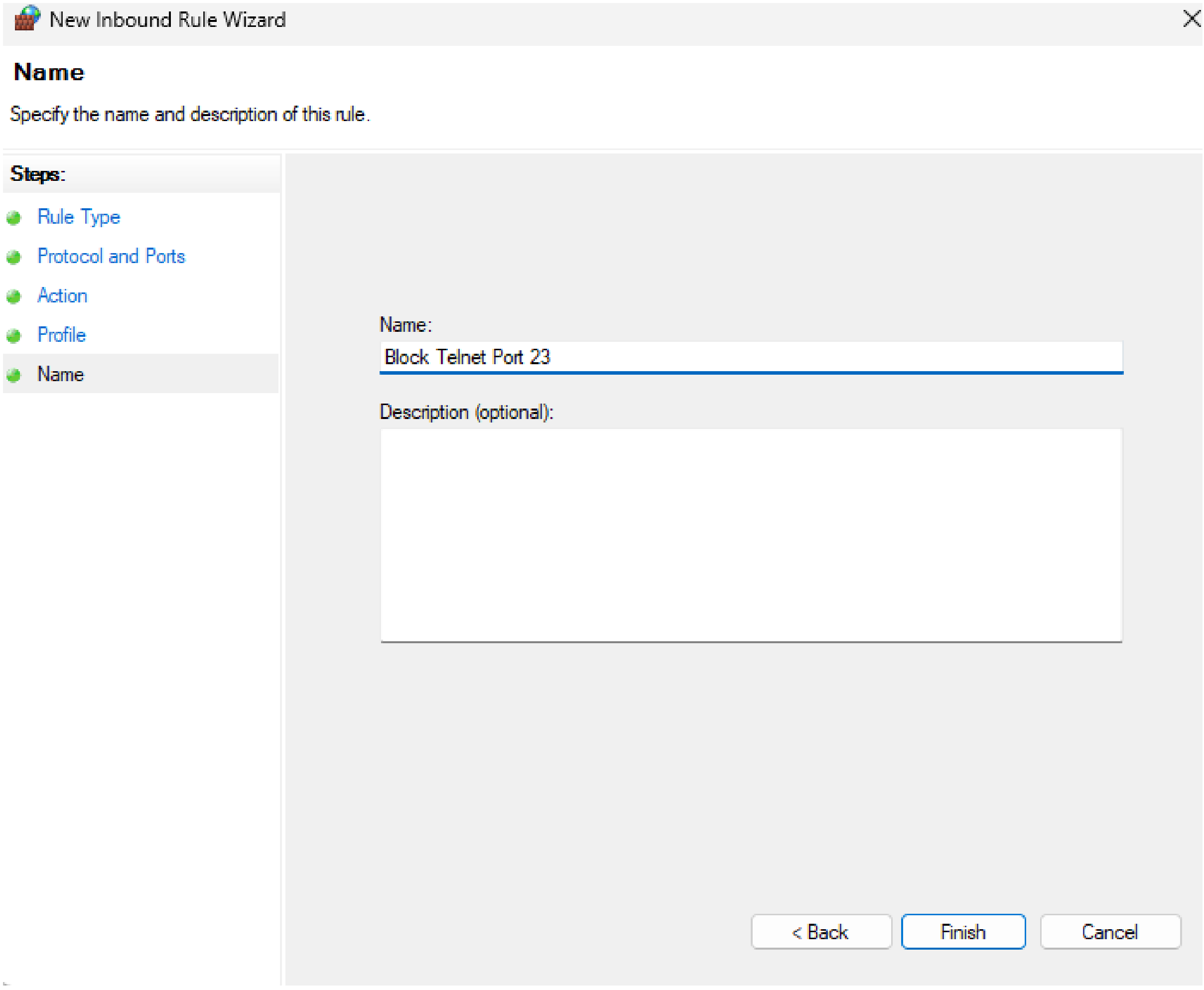
Applies when a computer is connected to its corporate domain.

☑ **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.

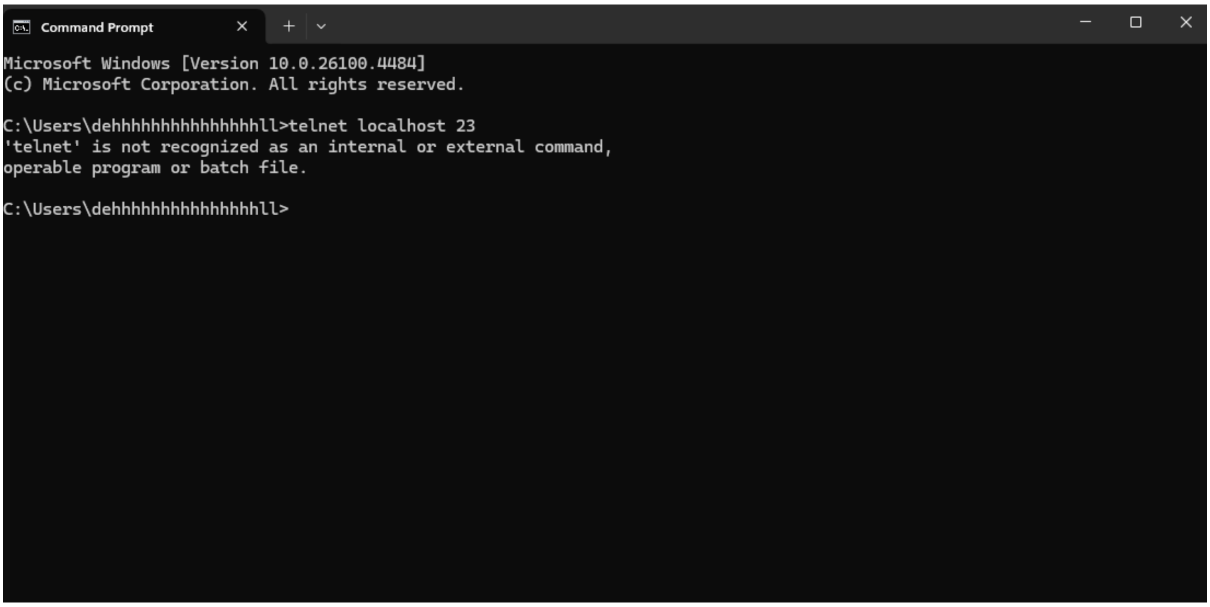


Name

Specify the name and description of this rule.

Name: Block Telnet Port 23

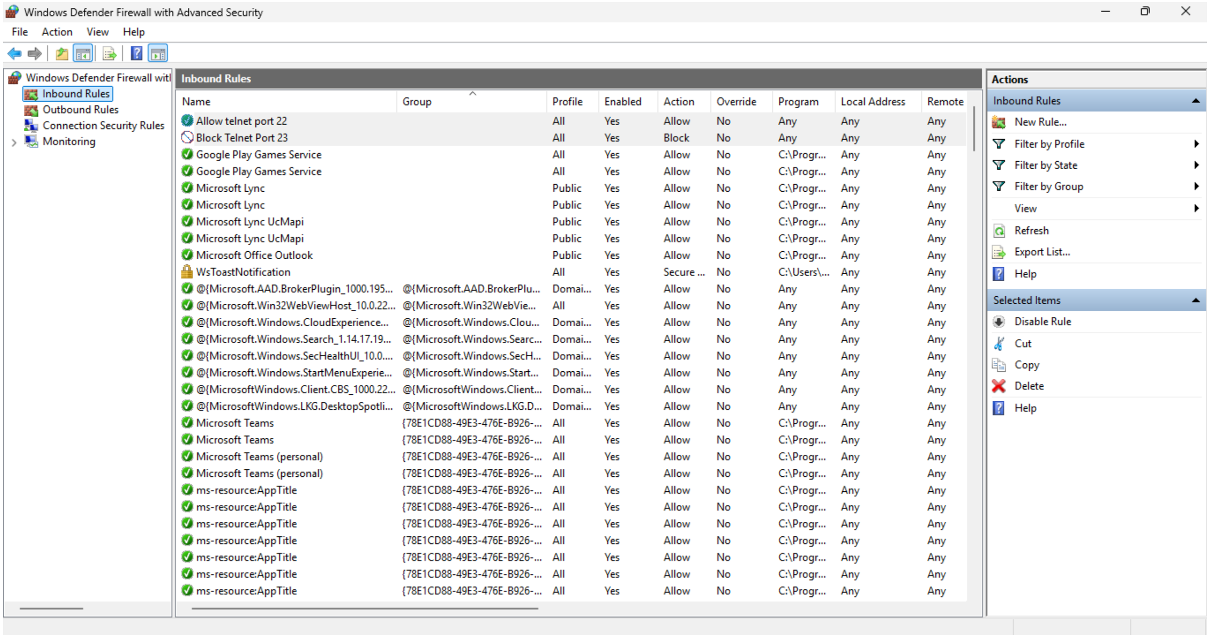
Description (optional):



```
Microsoft Windows [Version 10.0.26100.4484]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dehhhhhhhhhhhhhhhll>telnet localhost 23
'telnet' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\dehhhhhhhhhhhhhhhll>
```



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
Allow telnet port 22		All	Yes	Allow	No	Any	Any	Any
Block Telnet Port 23		All	Yes	Block	No	Any	Any	Any
Google Play Games Service		All	Yes	Allow	No	C:\Progr...	Any	Any
Google Play Games Service		All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Lync		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Lync		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Lync UcMapi		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Lync UcMapi		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any
WsToastNotification		All	Yes	Secure ...	No	C:\Users\...	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Search_1.14.17.19...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.SecHealthUI_10.0....	@{Microsoft.Windows.SecH...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any
@{MicrosoftWindows.Client.CBS_1000.22...	@{MicrosoftWindows.Client...	Domai...	Yes	Allow	No	Any	Any	Any
@{MicrosoftWindows.LKG.DesktopSpotli...	@{MicrosoftWindows.LKG.D...	Domai...	Yes	Allow	No	Any	Any	Any
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any

A firewall filters traffic by **examining network packets** and allowing or blocking them based on a set of predefined rules.

It checks factors like:

- **Source & destination IP address**
- **Port number**
- **Protocol type (TCP, UDP, etc.)**
- **Connection state** (for stateful firewalls)

If a packet matches an **allow** rule, it’s forwarded; if it matches a **deny/block** rule, it’s dropped.
This helps **control access**, **prevent unauthorized connections**, and **protect against threats**.