Elevate_Labs_Task_4

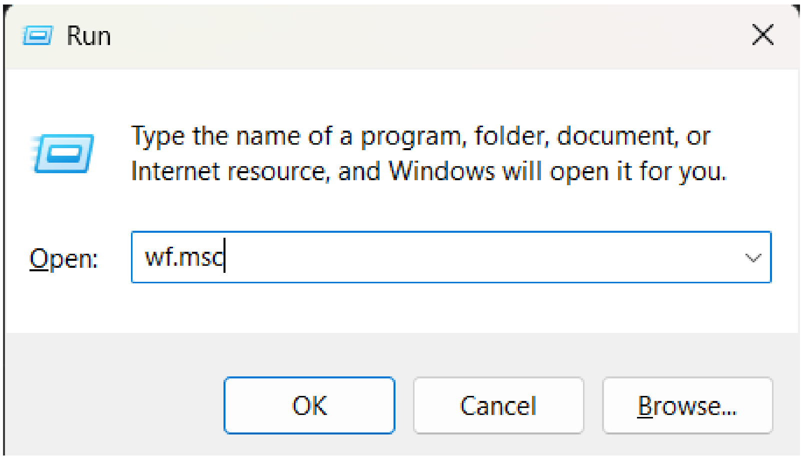
Rudra Srilakshmi

Task 4 : Setup and Use a Firewall on Windows/Linux

1.Open firewall configuration tool (Windows Firewall or terminal for UFW).

To open Windows Defender Firewall with Advanced Security Tool:

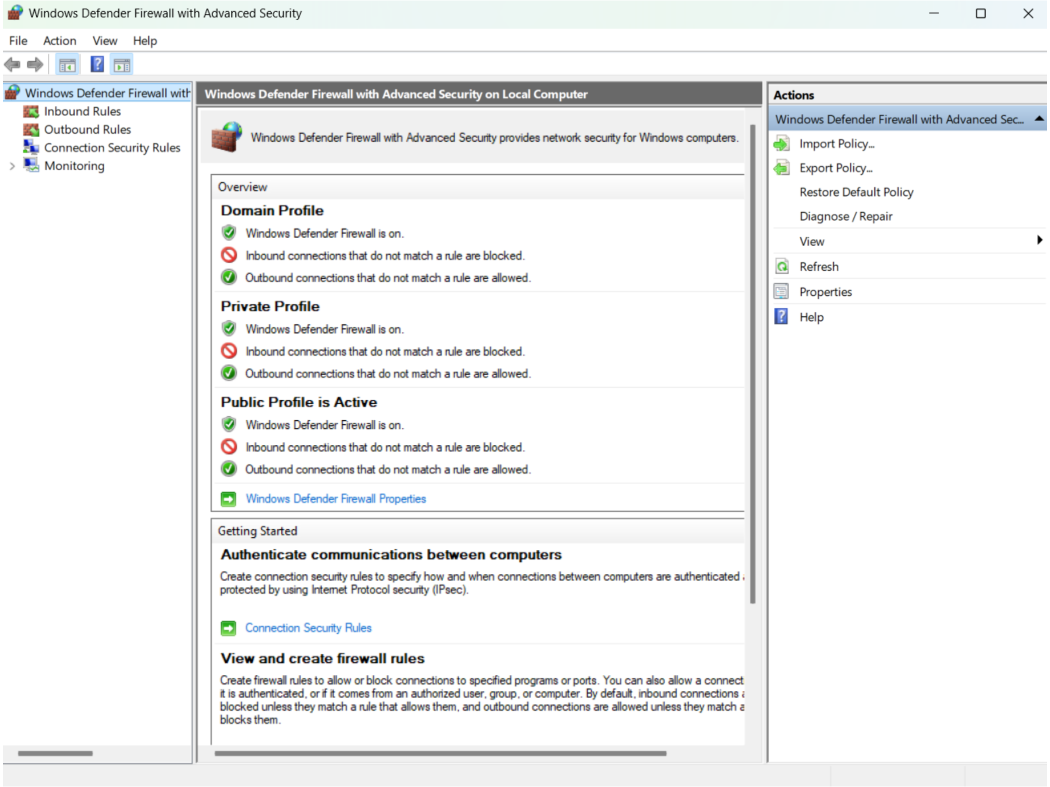
- Press Windows+R
- typed wf.msc then click on enter.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wf.msc

Windows Defender Firewall with Advanced Security tool interface:



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 a protected by using Internet Protocol security (IPsec).

Connection Security Rules

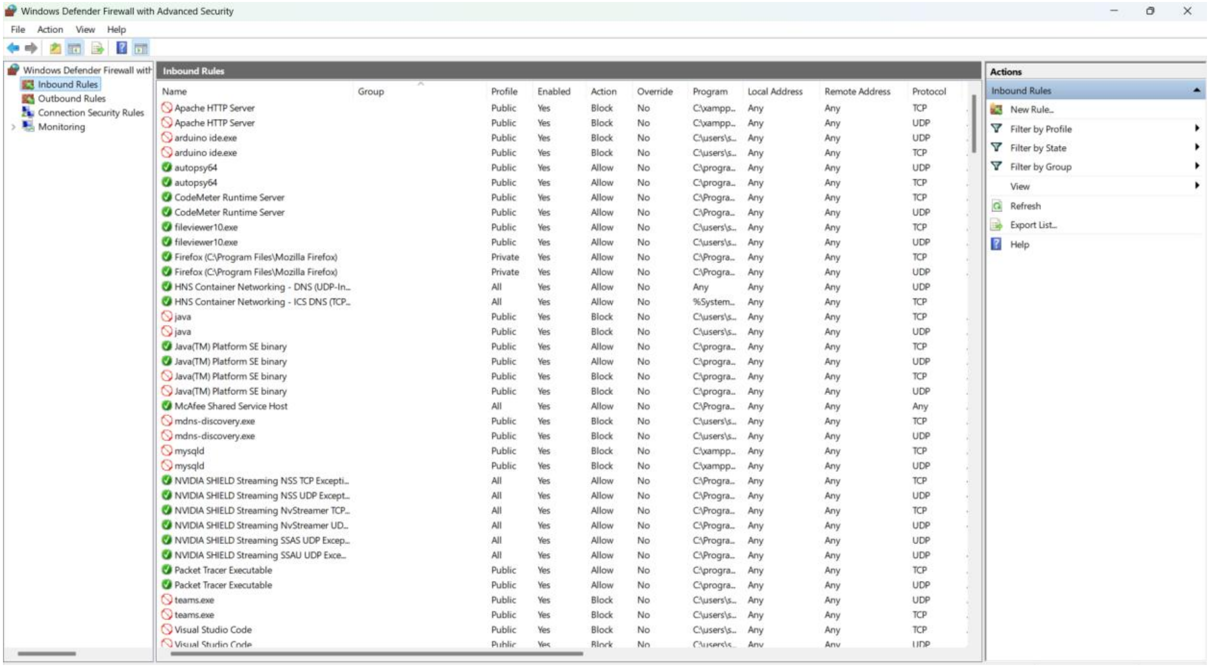
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connect it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections a blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a blocks them.

2.List current firewall rules.

In that, Navigate to Inbound Rules which is in the left pane.

This gives an overview of which services and ports are already allowed or blocked.



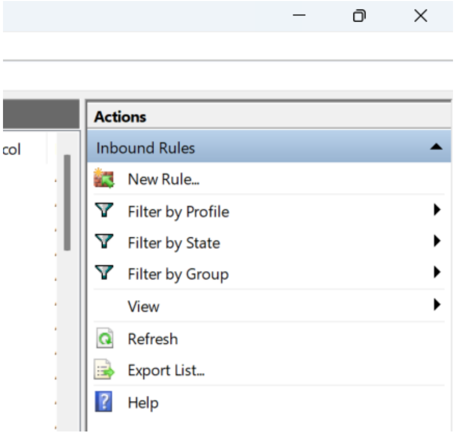
Inbound Rules

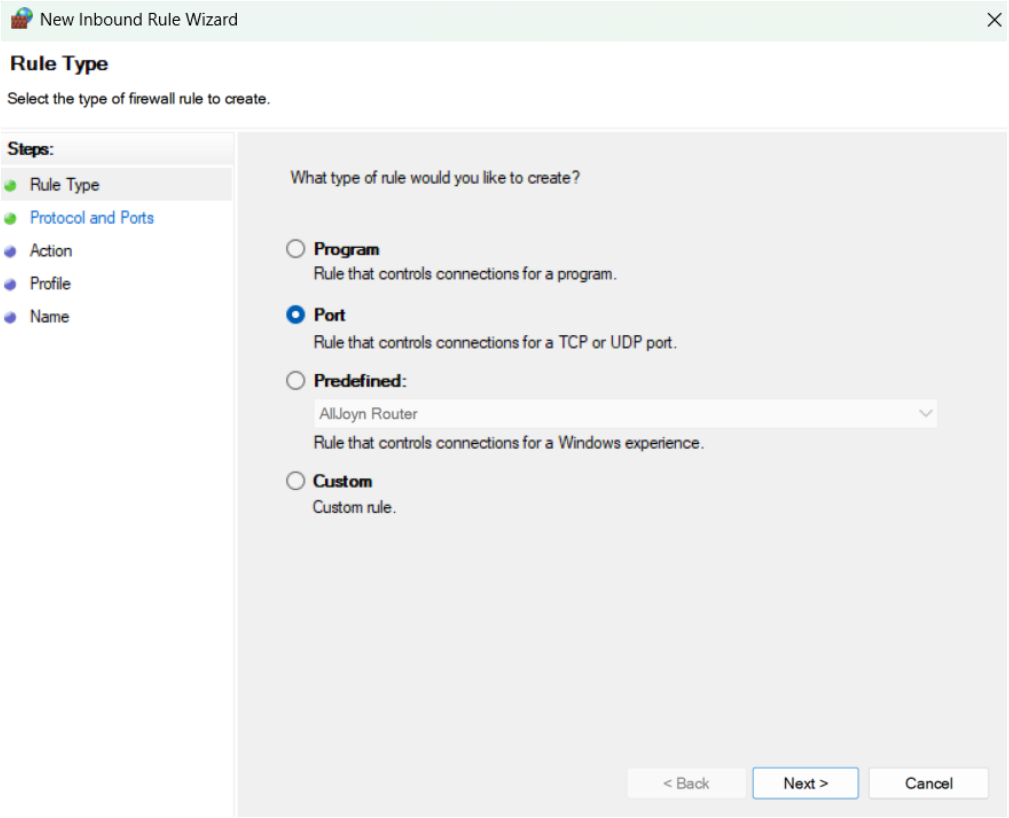
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Apache HTTP Server		Public	Yes	Block	No	C:\xampp…	Any	Any	TCP
Apache HTTP Server		Public	Yes	Block	No	C:\xampp…	Any	Any	UDP
arduino ide.exe		Public	Yes	Block	No	C:\users\s…	Any	Any	UDP
arduino ide.exe		Public	Yes	Block	No	C:\users\s…	Any	Any	TCP
autopsy64		Public	Yes	Allow	No	C:\progra…	Any	Any	UDP
autopsy64		Public	Yes	Allow	No	C:\progra…	Any	Any	TCP
CodeMeter Runtime Server		Public	Yes	Allow	No	C:\Progra…	Any	Any	TCP
CodeMeter Runtime Server		Public	Yes	Allow	No	C:\Progra…	Any	Any	UDP
fileviewer10.exe		Public	Yes	Allow	No	C:\users\s…	Any	Any	TCP
fileviewer10.exe		Public	Yes	Allow	No	C:\users\s…	Any	Any	UDP
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra…	Any	Any	TCP
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra…	Any	Any	UDP
HNS Container Networking - DNS (UDP-In…		All	Yes	Allow	No	Any	Any	Any	UDP
HNS Container Networking - ICS DNS (TCP…		All	Yes	Allow	No	%System…	Any	Any	TCP
java		Public	Yes	Block	No	C:\users\s…	Any	Any	TCP
java		Public	Yes	Block	No	C:\users\s…	Any	Any	UDP
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progra…	Any	Any	TCP
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progra…	Any	Any	UDP
Java(TM) Platform SE binary		Public	Yes	Block	No	C:\progra…	Any	Any	TCP
Java(TM) Platform SE binary		Public	Yes	Block	No	C:\progra…	Any	Any	UDP
McAfee Shared Service Host		All	Yes	Allow	No	C:\Progra…	Any	Any	Any
mdns-discovery.exe		Public	Yes	Block	No	C:\users\s…	Any	Any	TCP
mdns-discovery.exe		Public	Yes	Block	No	C:\users\s…	Any	Any	UDP
mysqld		Public	Yes	Block	No	C:\xampp…	Any	Any	TCP
mysqld		Public	Yes	Block	No	C:\xampp…	Any	Any	UDP
NVIDIA SHIELD Streaming NSS TCP Excepti…		All	Yes	Allow	No	C:\Progra…	Any	Any	TCP
NVIDIA SHIELD Streaming NSS UDP Except…		All	Yes	Allow	No	C:\Progra…	Any	Any	UDP
NVIDIA SHIELD Streaming NvStreamer TCP…		All	Yes	Allow	No	C:\Progra…	Any	Any	TCP
NVIDIA SHIELD Streaming NvStreamer UD…		All	Yes	Allow	No	C:\Progra…	Any	Any	UDP
NVIDIA SHIELD Streaming SSAS UDP Excep…		All	Yes	Allow	No	C:\Progra…	Any	Any	UDP
NVIDIA SHIELD Streaming SSAU UDP Exce…		All	Yes	Allow	No	C:\Progra…	Any	Any	UDP
Packet Tracer Executable		Public	Yes	Allow	No	C:\progra…	Any	Any	TCP
Packet Tracer Executable		Public	Yes	Allow	No	C:\progra…	Any	Any	UDP
teams.exe		Public	Yes	Block	No	C:\users\s…	Any	Any	UDP
teams.exe		Public	Yes	Block	No	C:\users\s…	Any	Any	TCP
Visual Studio Code		Public	Yes	Block	No	C:\users\s…	Any	Any	TCP
Visual Studio Code		Public	Yes	Block	No	C:\users\s…	Any	Any	UDP

3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).

Here, Telnet is an insecure protocol. Blocking port 23 simulates how a firewall can prevent unauthorized or risky traffic.

In Inbound Rules, clicked New Rule… on the right side and selected Port as the rule type.




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?

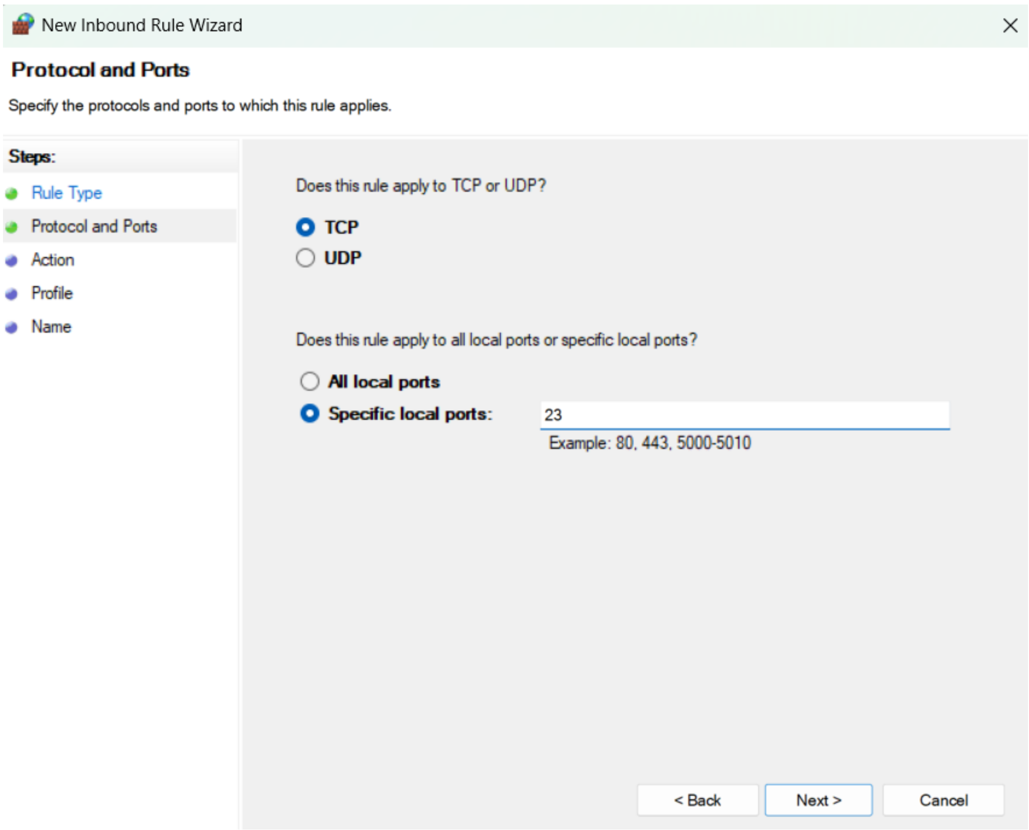
○ **Program**
Rule that controls connections for a program.

● **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.

Choose TCP, specified port 23, then selected Block the connection.



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**

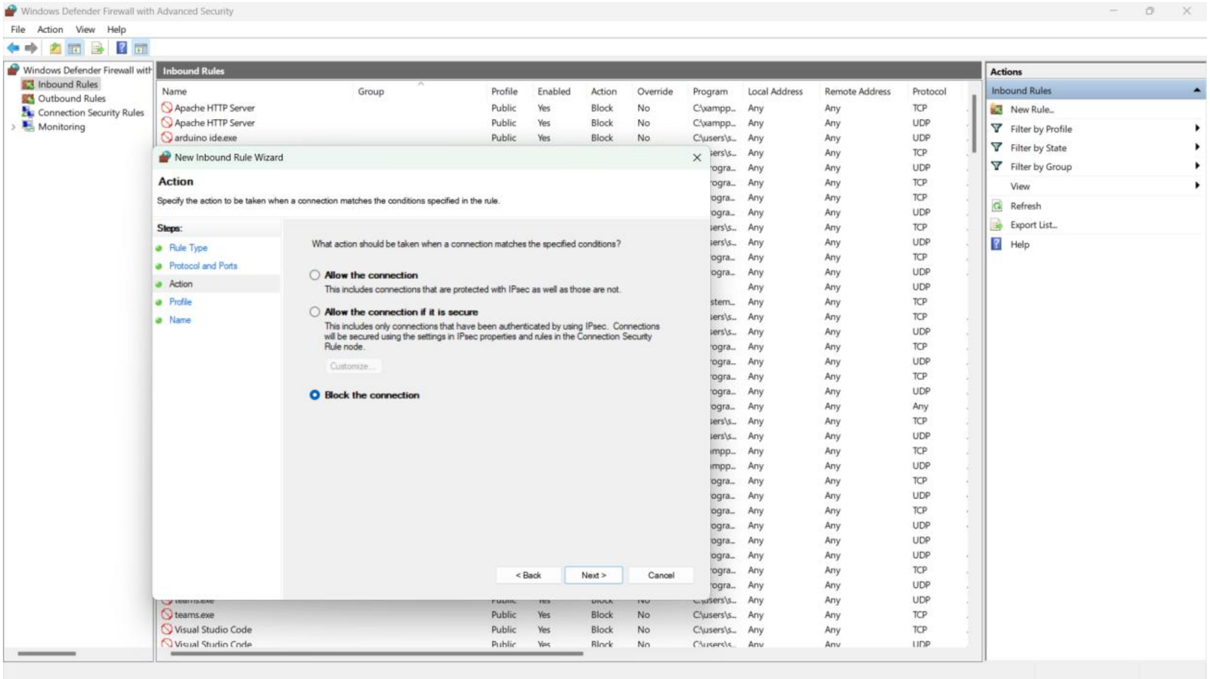
○ **UDP**

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

○ **All local ports**

● **Specific local ports:** 23

Example: 80, 443, 5000-5010



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Apache HTTP Server		Public	Yes	Block	No	C:\xampp...	Any	Any	TCP
Apache HTTP Server		Public	Yes	Block	No	C:\xampp...	Any	Any	UDP
arduino ide.exe		Public	Yes	Block	No	C:\users\s...	Any	Any	UDP
						ers\s...	Any	Any	TCP
						ogra...	Any	Any	UDP
						ogra...	Any	Any	TCP
						ogra...	Any	Any	TCP
						ogra...	Any	Any	UDP
						ers\s...	Any	Any	TCP
						ers\s...	Any	Any	UDP
						ogra...	Any	Any	TCP
						ogra...	Any	Any	UDP
							Any	Any	UDP
						stem...	Any	Any	TCP
						ers\s...	Any	Any	TCP
						ers\s...	Any	Any	UDP
						ogra...	Any	Any	TCP
						ogra...	Any	Any	UDP
						ogra...	Any	Any	TCP
						ogra...	Any	Any	UDP
						ogra...	Any	Any	Any
						ers\s...	Any	Any	TCP
						ers\s...	Any	Any	UDP
						mpp...	Any	Any	TCP
						mpp...	Any	Any	UDP
						ogra...	Any	Any	TCP
						ogra...	Any	Any	UDP
						ogra...	Any	Any	TCP
						ogra...	Any	Any	UDP
						ogra...	Any	Any	UDP
						ogra...	Any	Any	UDP
						ogra...	Any	Any	TCP
						ogra...	Any	Any	UDP
teams.exe		Public	Yes	Block	No	C:\users\s...	Any	Any	UDP
teams.exe		Public	Yes	Block	No	C:\users\s...	Any	Any	TCP
Visual Studio Code		Public	Yes	Block	No	C:\users\s...	Any	Any	TCP
Visual Studio Code		Public	Yes	Block	No	C:\users\s...	Any	Any	UDP

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**

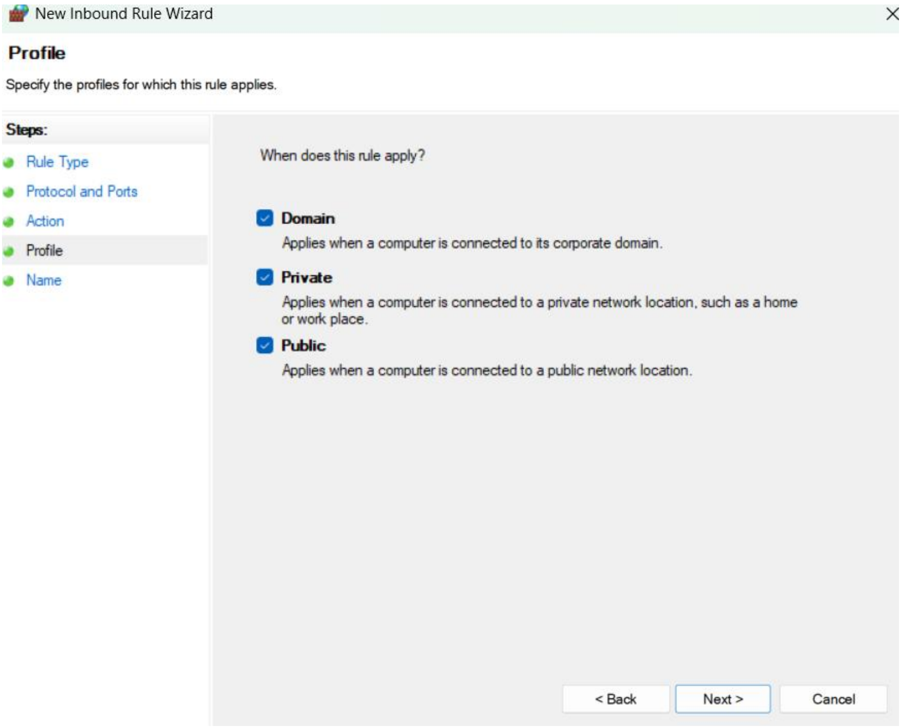
This includes connections that are protected with IPsec as well as those are not.

○ **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**

Applied the rule to Domain, Private, and Public profiles and Named the rule as Block Telnet Port 23.



New Inbound Rule Wizard

Profile

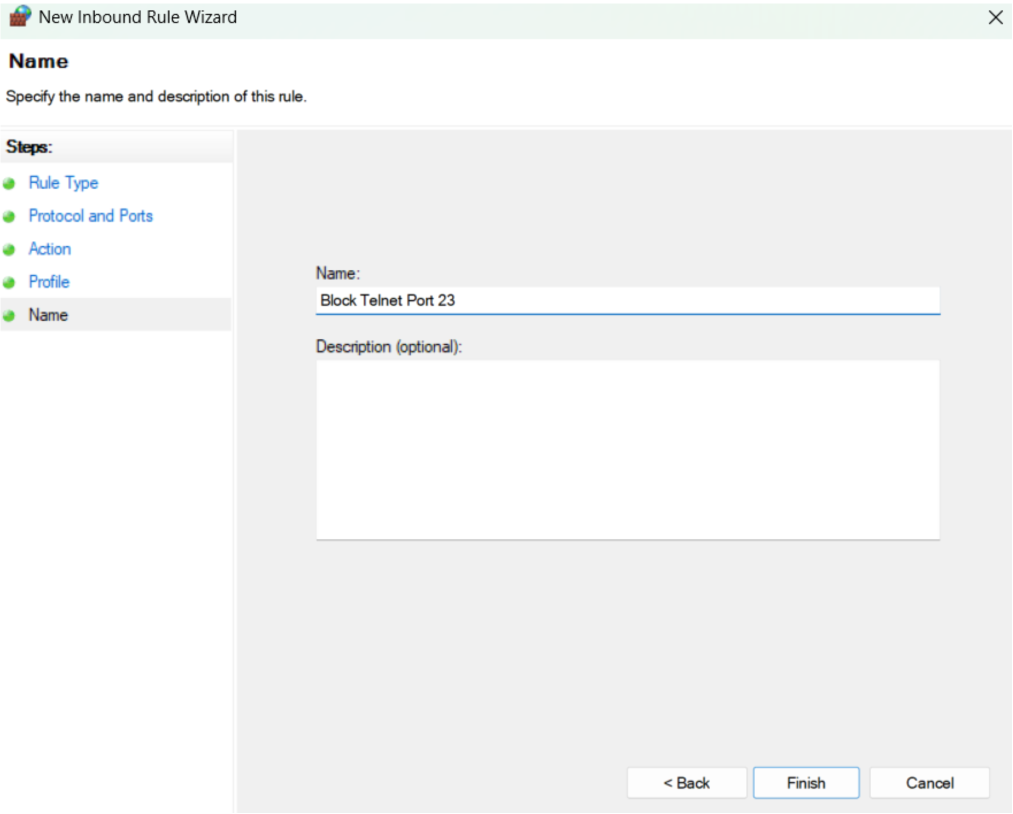
Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

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



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Name:
Block Telnet Port 23

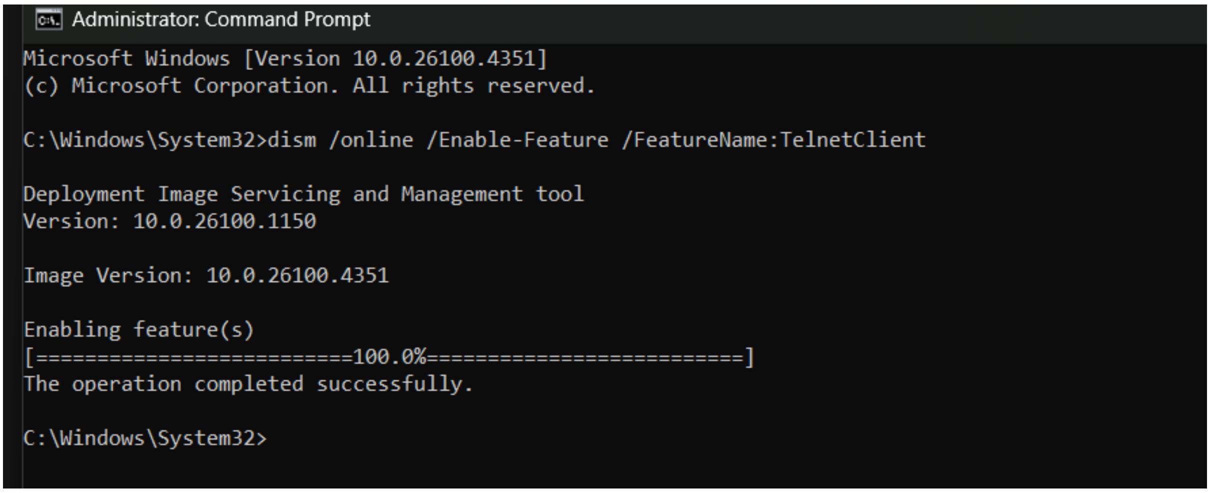
Description (optional):

4.Test the rule by attempting to connect to that port locally or remotely.

First, enabled the Telnet Client on Windows using the command,

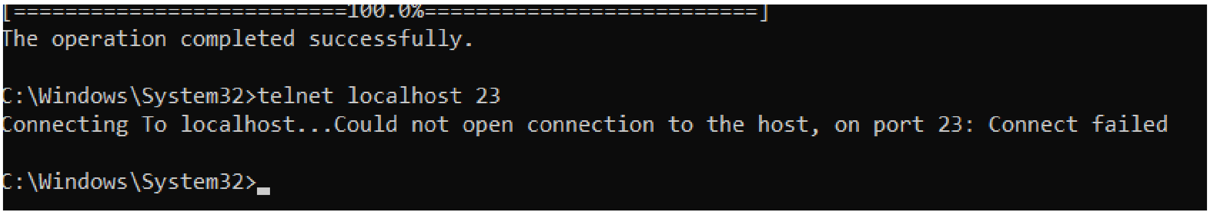
“dism /online /Enable-Feature /FeatureName:TelnetClient”

“telnet localhost 23”



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>dism /online /Enable-Feature /FeatureName:TelnetClient

Deployment Image Servicing and Management tool
Version: 10.0.26100.1150

Image Version: 10.0.26100.4351

Enabling feature(s)
[==========================100.0%==========================]
The operation completed successfully.

C:\Windows\System32>
```

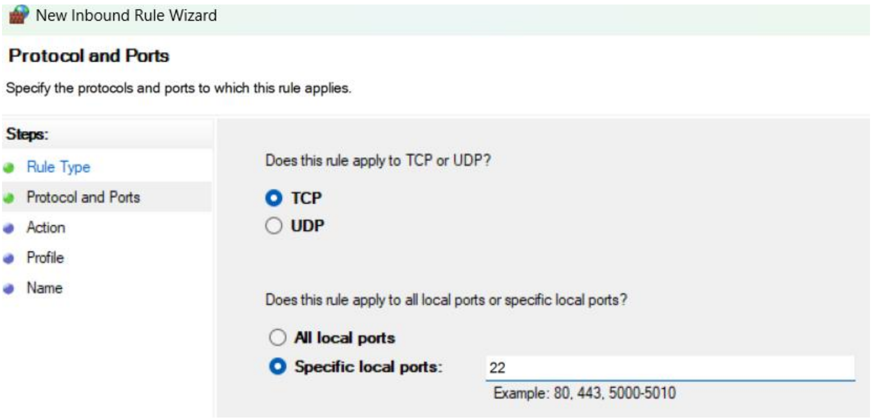


```
[==========================100.0%==========================]
The operation completed successfully.

C:\Windows\System32>telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed

C:\Windows\System32>
```

Here, Connection failed, confirms that the firewall successfully blocked port 23.

5.Add rule to allow SSH (port 22) if on Linux.

Even though SSH is not typically used on Windows, created an Allow rule for port 22 to simulate Linux-like behaviour.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

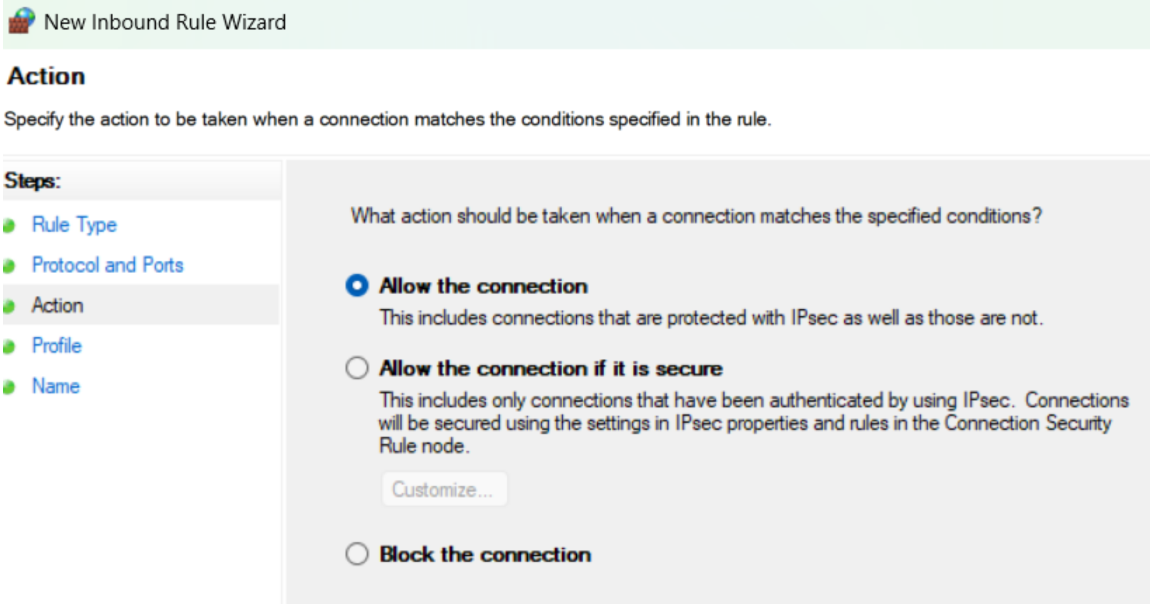
Does this rule apply to TCP or UDP?

● TCP
○ UDP

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

○ All local ports
● Specific local ports: 22

Example: 80, 443, 5000-5010



New Inbound Rule Wizard

Action

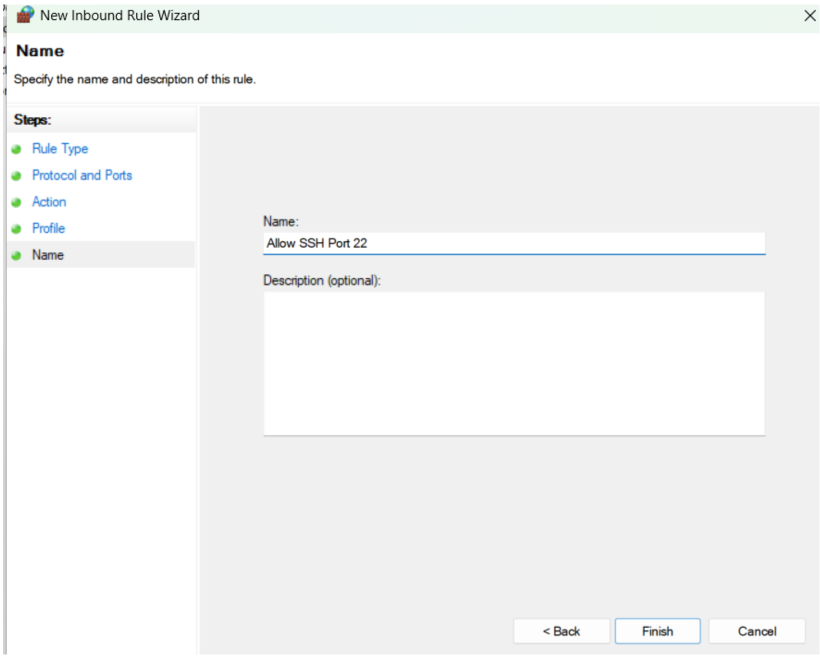
Specify the action to be taken when a connection matches the conditions specified in the rule.

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**



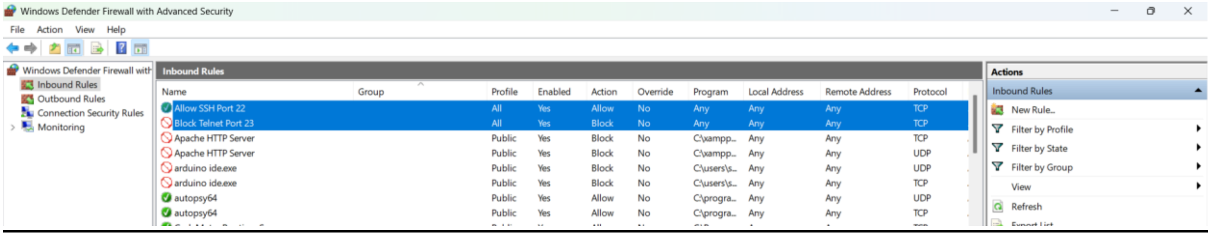
New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Name: Allow SSH Port 22

Description (optional):



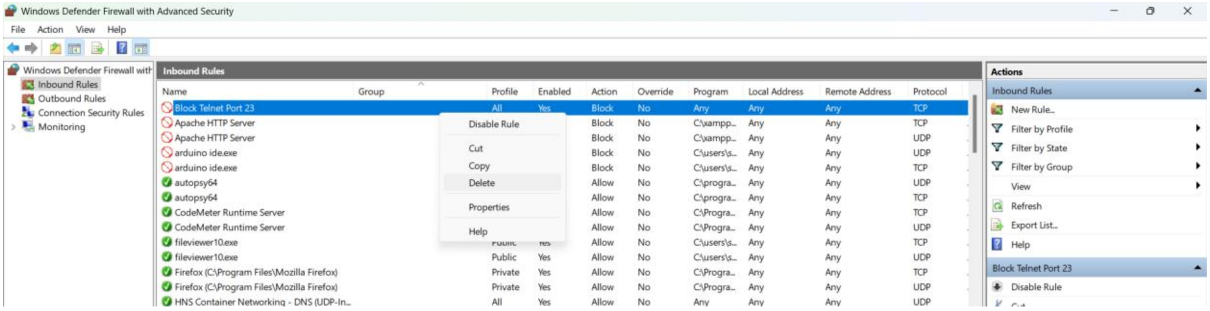
Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Allow SSH Port 22		All	Yes	Allow	No	Any	Any	Any	TCP
Block Telnet Port 23		All	Yes	Block	No	Any	Any	Any	TCP
Apache HTTP Server		Public	Yes	Block	No	C:\xampp...	Any	Any	TCP
Apache HTTP Server		Public	Yes	Block	No	C:\xampp...	Any	Any	UDP
arduino ide.exe		Public	Yes	Block	No	C:\users\s...	Any	Any	UDP
arduino ide.exe		Public	Yes	Block	No	C:\users\s...	Any	Any	TCP
autopsy64		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
autopsy64		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP

6.Remove the test block rule to restore original state.

To remove the blocking rule, right click on the rule and select delete



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Block Telnet Port 23		All	Yes	Block	No	Any	Any	Any	TCP
Apache HTTP Server				Block	No	C:\xampp...	Any	Any	TCP
Apache HTTP Server				Block	No	C:\xampp...	Any	Any	UDP
arduino ide.exe				Block	No	C:\users\s...	Any	Any	UDP
arduino ide.exe				Block	No	C:\users\s...	Any	Any	TCP
autopsy64				Allow	No	C:\progra...	Any	Any	UDP
autopsy64				Allow	No	C:\progra...	Any	Any	TCP
CodeMeter Runtime Server				Allow	No	C:\Progra...	Any	Any	TCP
CodeMeter Runtime Server				Allow	No	C:\Progra...	Any	Any	UDP
fileviewer10.exe		Public	Yes	Allow	No	C:\users\s...	Any	Any	TCP
fileviewer10.exe		Public	Yes	Allow	No	C:\users\s...	Any	Any	UDP
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any	Any	UDP
HNS Container Networking - DNS (UDP-In...		All	Yes	Allow	No	Any	Any	Any	UDP

7.Document commands or GUI steps used.

- Opened wf.msc to launch firewall.
- Navigated through Inbound Rules to create and delete rules.
- Used rule type “Port” to specify TCP ports.
- Chose actions: Block (for Telnet), Allow (for SSH simulation).

8.Summarize how firewall filters traffic.

Based on configured rules, A firewall is a system security mechanism that monitors and filters incoming and outgoing traffic.
It acts like a gatekeeper that checks whether data packets should be allowed or denied based on:

- Port numbers (e.g., 23 for Telnet, 22 for SSH)
- IP addresses
- Protocols (TCP/UDP)
- Applications or programs