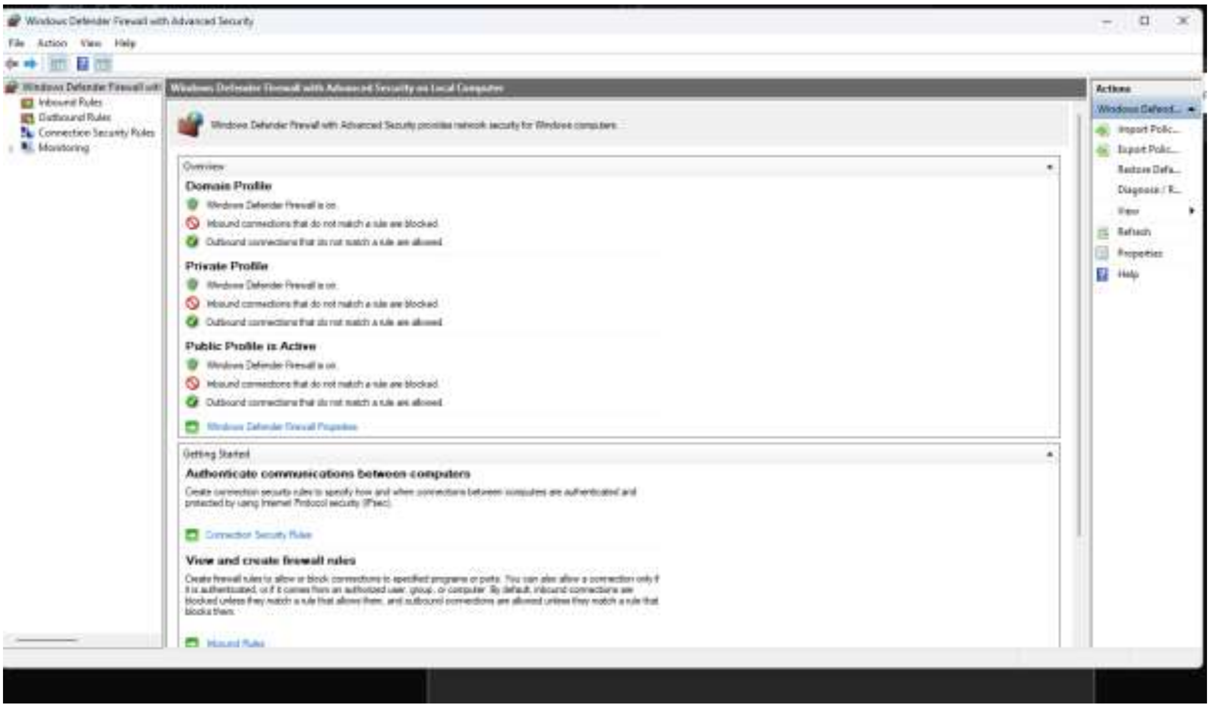
Task 4 –

Configure a firewall on local system.

First open the wf.msc firewall configuration in start menu



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

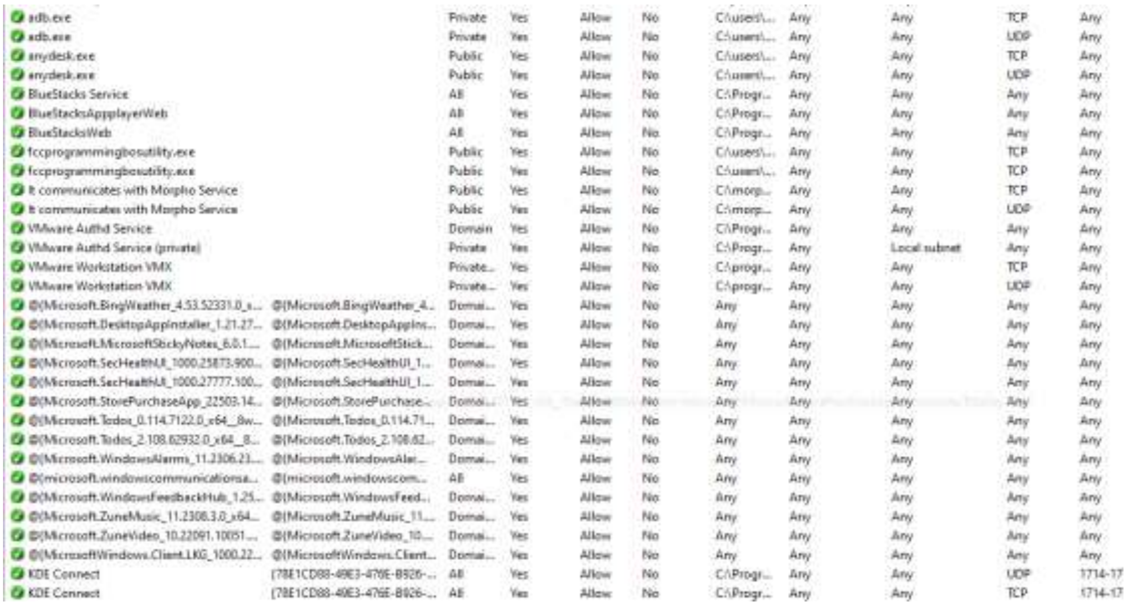
View and create firewall rules

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 blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

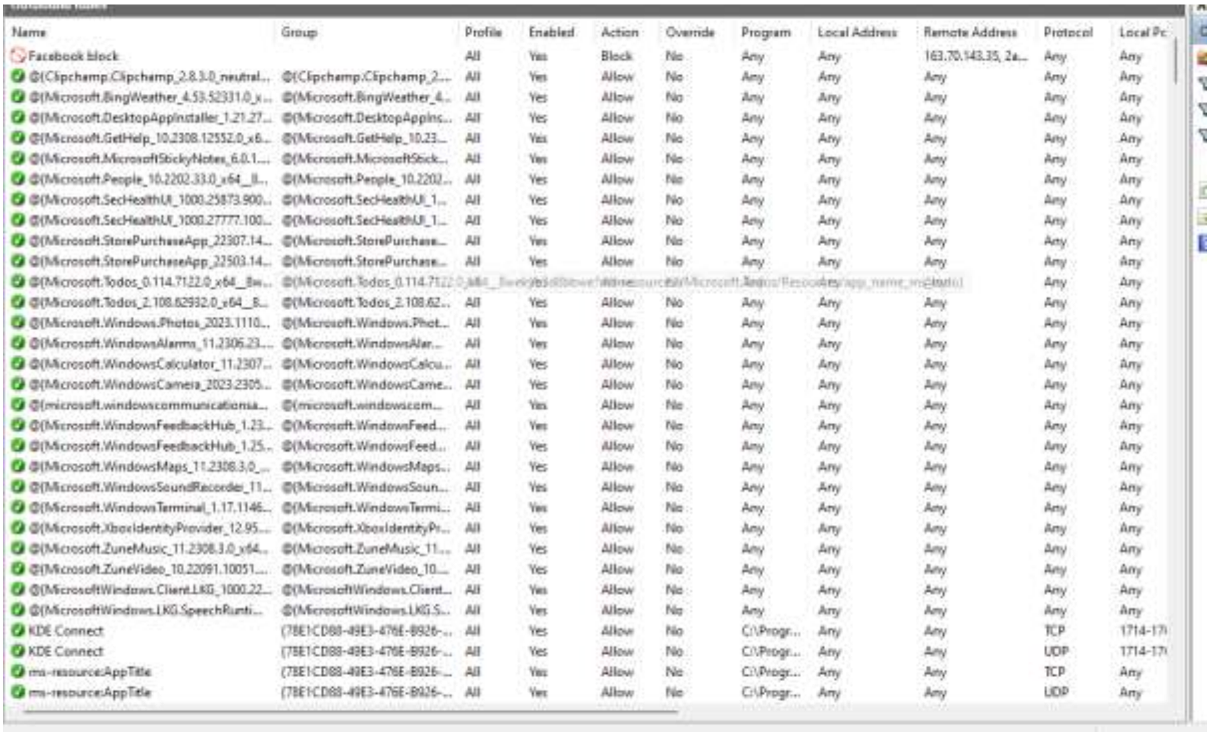
Now 2 rules are showing on left hand side.

Inbound rule



adb.exe		Private	Yes	Allow	No	C:\users\...	Any	Any	TCP	Any
adb.exe		Private	Yes	Allow	No	C:\users\...	Any	Any	UDP	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	TCP	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	UDP	Any
BlueStacks Service		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any
BlueStacksAppplayerWeb		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any
BlueStacksWeb		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any
fccprogrammingbosutility.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	TCP	Any
fccprogrammingbosutility.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	TCP	Any
It communicates with Morpho Service		Public	Yes	Allow	No	C:\morp...	Any	Any	TCP	Any
It communicates with Morpho Service		Public	Yes	Allow	No	C:\morp...	Any	Any	UDP	Any
VMware Authd Service		Domain	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any
VMware Authd Service (private)		Private	Yes	Allow	No	C:\Progr...	Any	Local subnet	Any	Any
VMware Workstation VMX		Private...	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any
VMware Workstation VMX		Private...	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any
@{Microsoft.BingWeather_4.53.52331.0_x...	@{Microsoft.BingWeather_4...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.DesktopAppInstaller_1.21.27...	@{Microsoft.DesktopAppIns...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.MicrosoftStickyNotes_6.0.1...	@{Microsoft.MicrosoftStick...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.SecHealthUI_1000.25873.900...	@{Microsoft.SecHealthUI_1...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.SecHealthUI_1000.27777.100...	@{Microsoft.SecHealthUI_1...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.StorePurchaseApp_22503.14...	@{Microsoft.StorePurchase...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.Todos_0.114.7122.0_x64__8w...	@{Microsoft.Todos_0.114.71...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.Todos_2.108.62932.0_x64__8...	@{Microsoft.Todos_2.108.62...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsAlarms_11.2306.23...	@{Microsoft.WindowsAlar...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsFeedbackHub_1.25...	@{Microsoft.WindowsFeed...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.ZuneMusic_11.2308.3.0_x64...	@{Microsoft.ZuneMusic_11...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.ZuneVideo_10.22091.10051...	@{Microsoft.ZuneVideo_10...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
@{MicrosoftWindows.Client.LKG_1000.22...	@{MicrosoftWindows.Client...	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
KDE Connect	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	1714-17
KDE Connect	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	1714-17

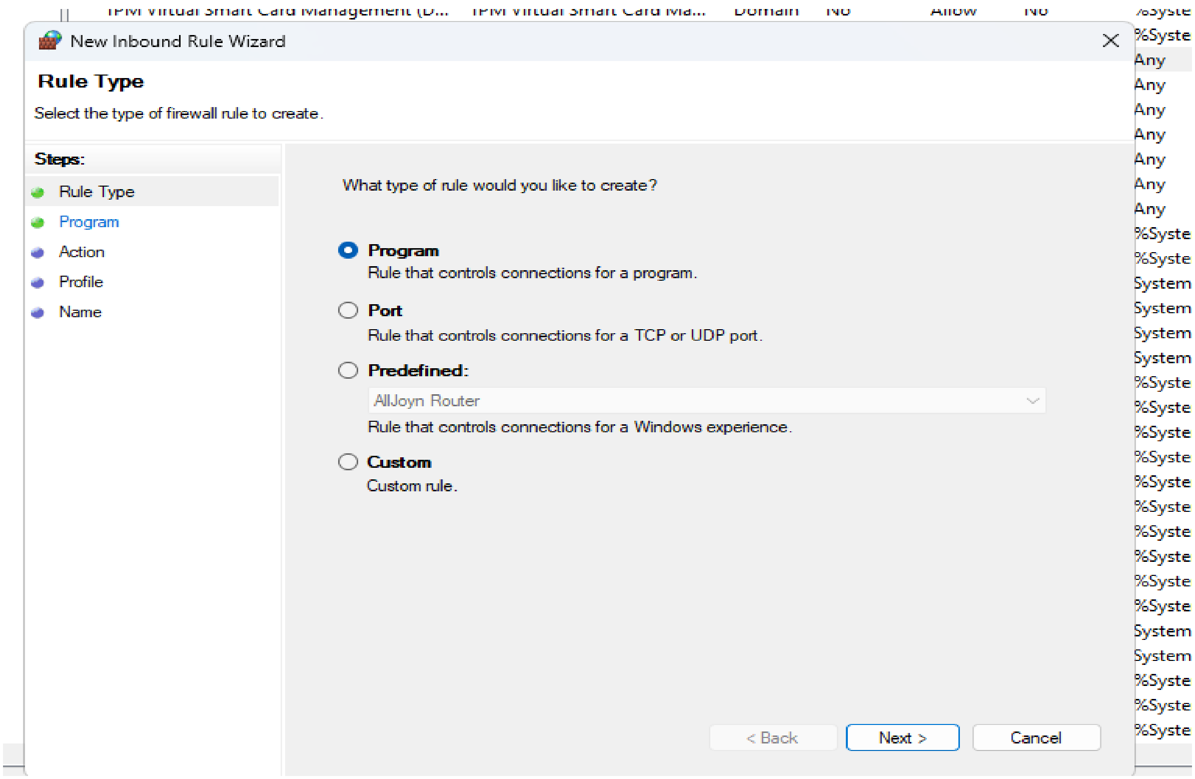
Outbound Rules -



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Po
Facebook block		All	Yes	Block	No	Any	Any	163.70.143.35, 2a...	Any	Any
@{Clipchamp.Clipchamp_2.8.3.0_neutral...	@{Clipchamp.Clipchamp_2...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.BingWeather_4.53.52331.0_x...	@{Microsoft.BingWeather_4...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.DesktopAppInstaller_1.21.27...	@{Microsoft.DesktopAppIns...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.GetHelp_10.2308.12552.0_x6...	@{Microsoft.GetHelp_10.23...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.MicrosoftStickyNotes_6.0.1....	@{Microsoft.MicrosoftStick...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.People_10.2202.33.0_x64__8...	@{Microsoft.People_10.2202...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.SecHealthUI_1000.25873.900...	@{Microsoft.SecHealthUI_1...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.SecHealthUI_1000.27777.100...	@{Microsoft.SecHealthUI_1...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.StorePurchaseApp_22307.14...	@{Microsoft.StorePurchase...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.StorePurchaseApp_22503.14...	@{Microsoft.StorePurchase...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.Todos_0.114.7122.0_x64__8w...	@{Microsoft.Todos_0.114.7122.0_x64__8wekyb3d8bbwe?ms-resource://Microsoft.Todos/Resources/app_name_ms_todo}								Any	Any
@{Microsoft.Todos_2.108.62932.0_x64__8...	@{Microsoft.Todos_2.108.62...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.Windows.Photos_2023.1110...	@{Microsoft.Windows.Phot...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsAlarms_11.2306.23....	@{Microsoft.WindowsAlar...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsCalculator_11.2307...	@{Microsoft.WindowsCalcu...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsCamera_2023.2305...	@{Microsoft.WindowsCame...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsFeedbackHub_1.23...	@{Microsoft.WindowsFeed...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsFeedbackHub_1.25...	@{Microsoft.WindowsFeed...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsMaps_11.2308.3.0_...	@{Microsoft.WindowsMaps...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsSoundRecorder_11...	@{Microsoft.WindowsSoun...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.WindowsTerminal_1.17.1146...	@{Microsoft.WindowsTermi...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.XboxIdentityProvider_12.95...	@{Microsoft.XboxIdentityPr...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.ZuneMusic_11.2308.3.0_x64...	@{Microsoft.ZuneMusic_11...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{Microsoft.ZuneVideo_10.22091.10051....	@{Microsoft.ZuneVideo_10....	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{MicrosoftWindows.Client.LKG_1000.22...	@{MicrosoftWindows.Client...	All	Yes	Allow	No	Any	Any	Any	Any	Any
@{MicrosoftWindows.LKG.SpeechRunti...	@{MicrosoftWindows.LKG.S...	All	Yes	Allow	No	Any	Any	Any	Any	Any
KDE Connect	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	1714-17
KDE Connect	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	1714-17
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any

Now configure a rule for blocking telnet protocol

For new rule



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

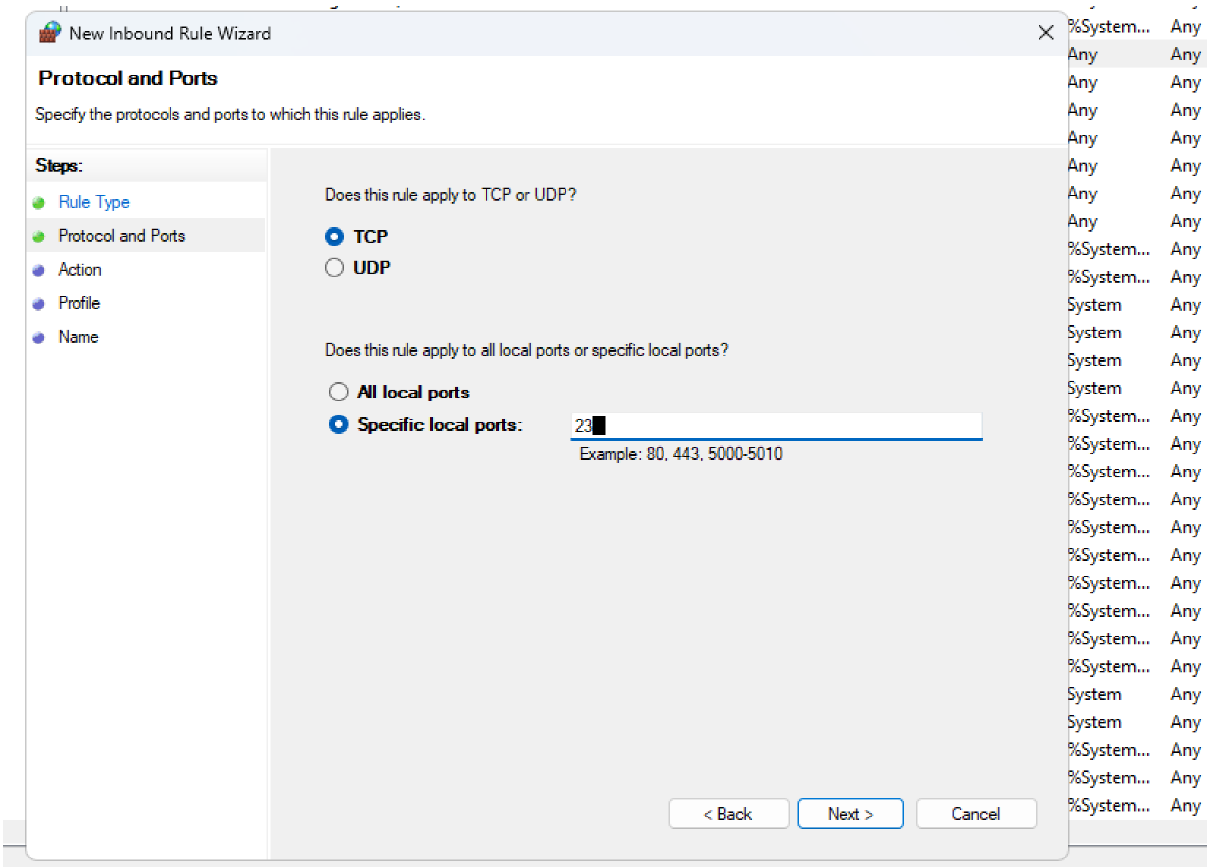
What type of rule would you like to create?

● **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.



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

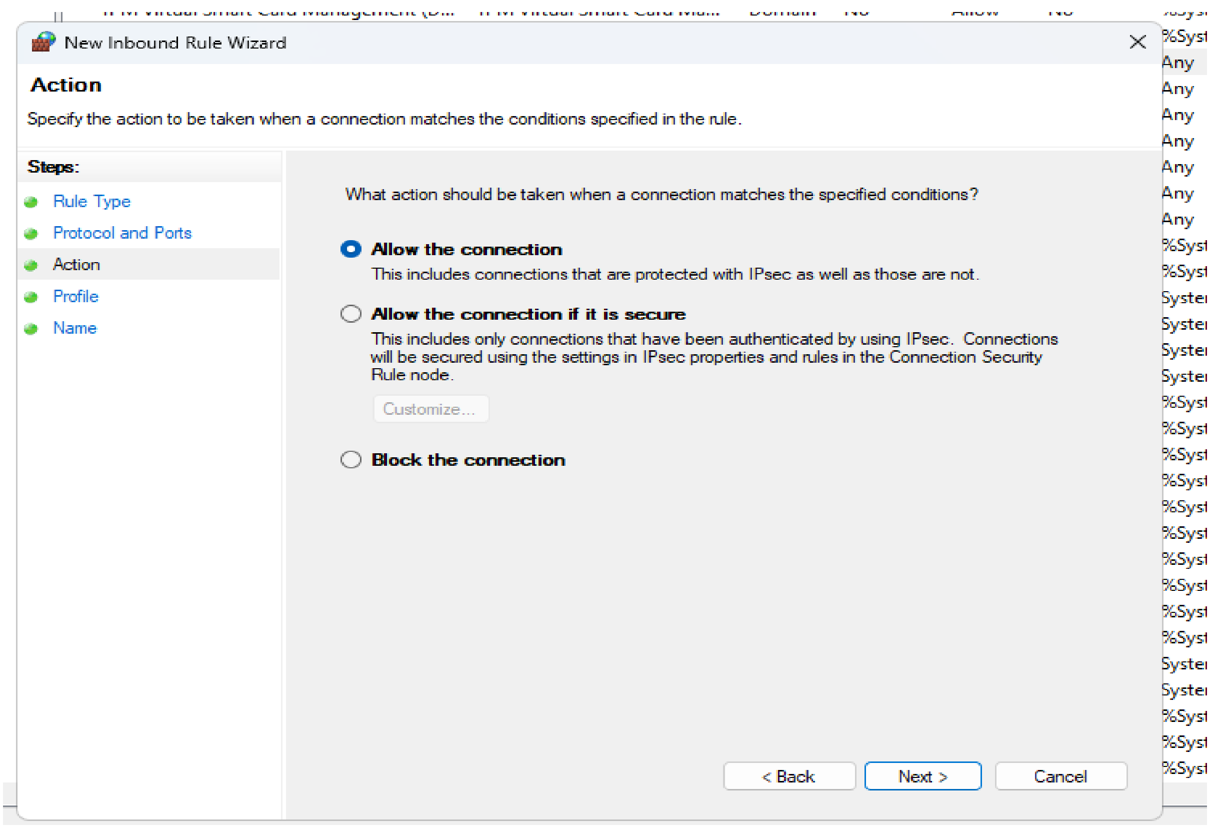
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 23

Example: 80, 443, 5000-5010

Now block all connections



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

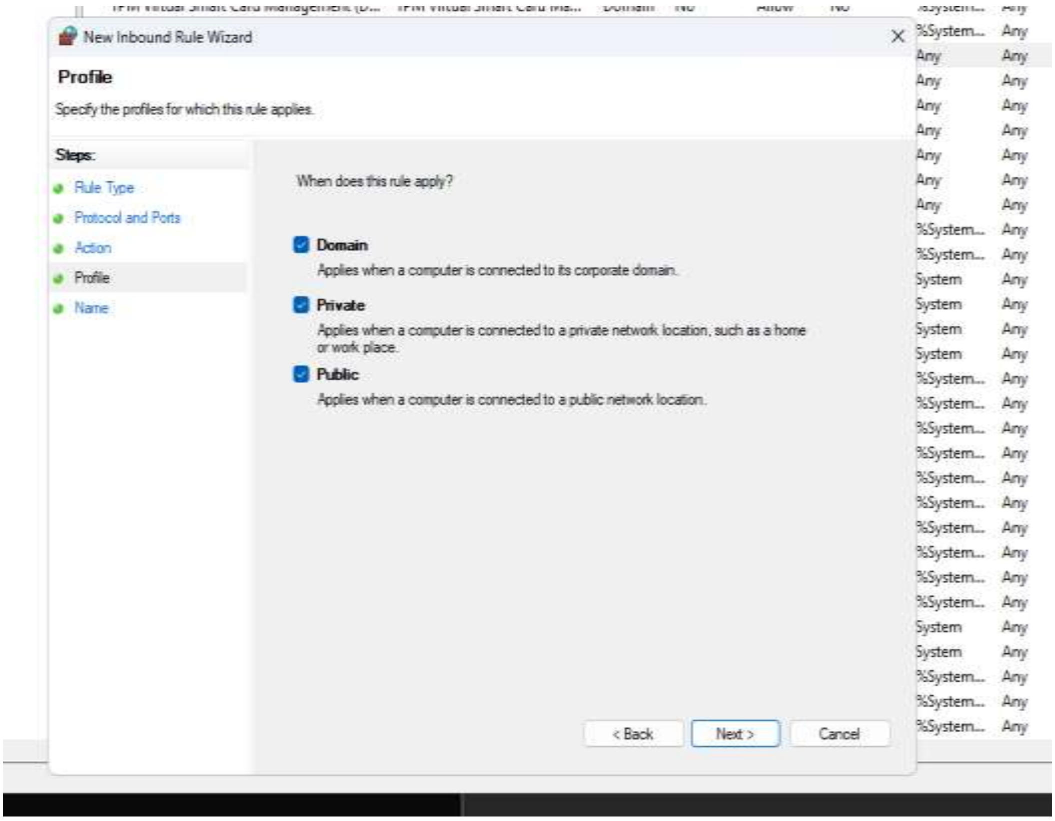
What action should be taken when a connection matches the specified conditions?

● **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**

For all domain now block



Profile

Specify the profiles for which this rule applies.

Steps:

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

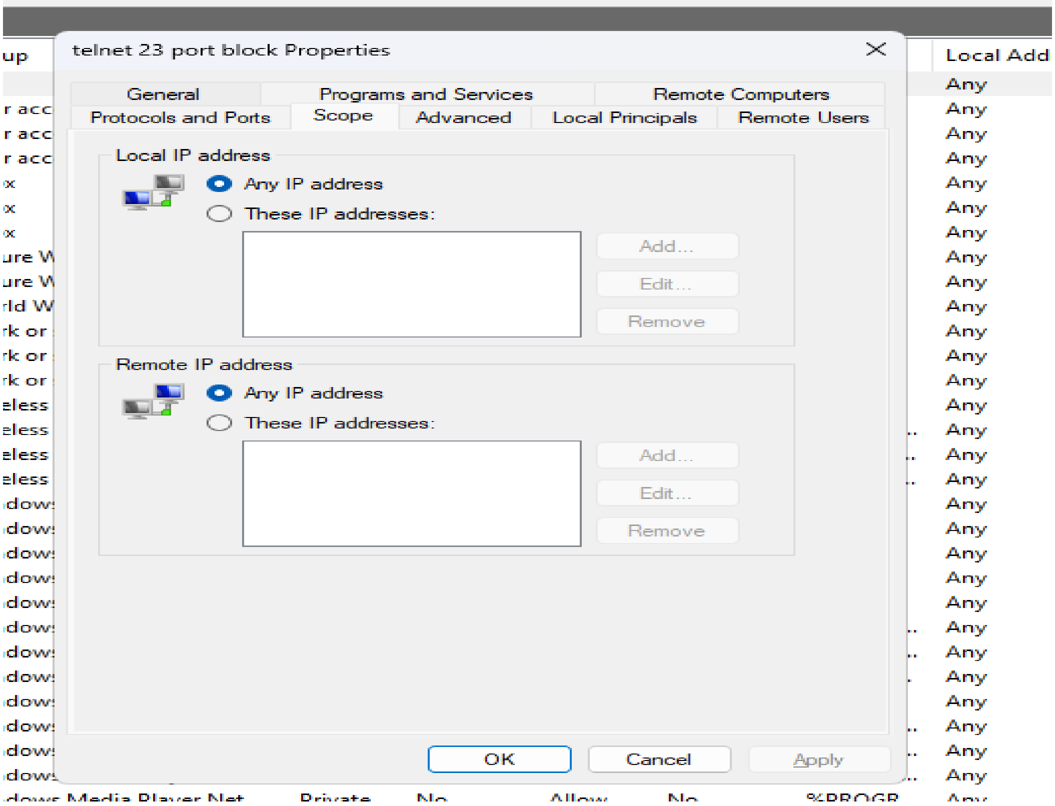
When does this rule apply?

☑ **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.

We can define the particular ip address for accessing or blocking connection



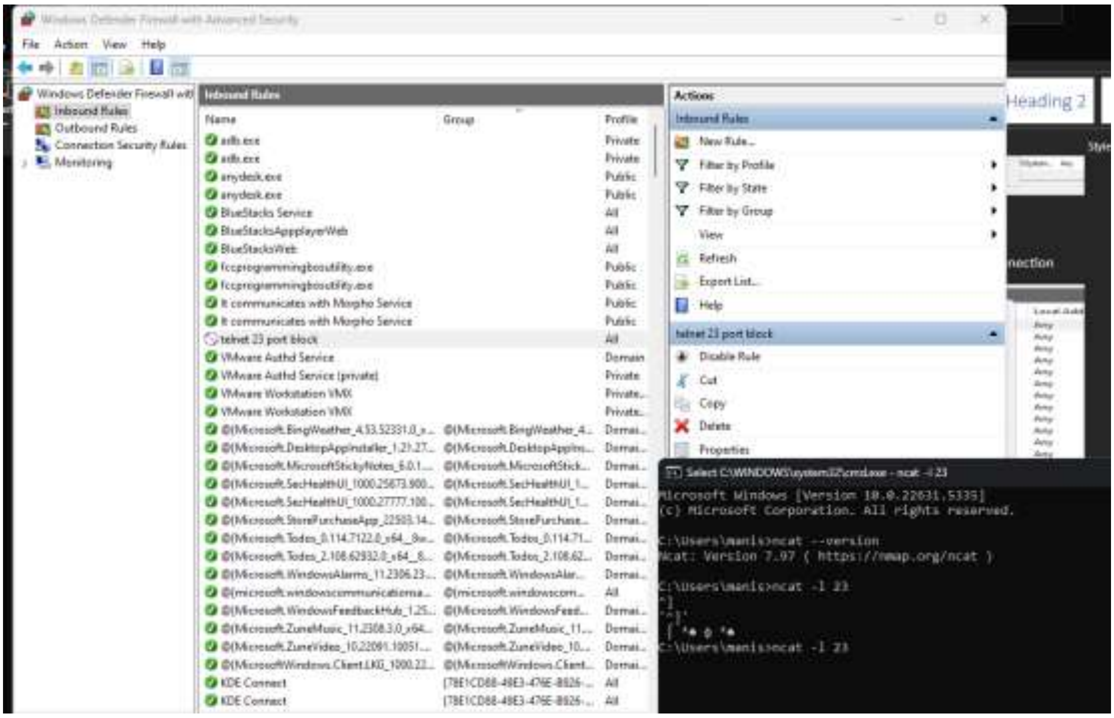
Local IP address

● Any IP address
○ These IP addresses:

Remote IP address

● Any IP address
○ These IP addresses:

Now testing with blocked 23 port

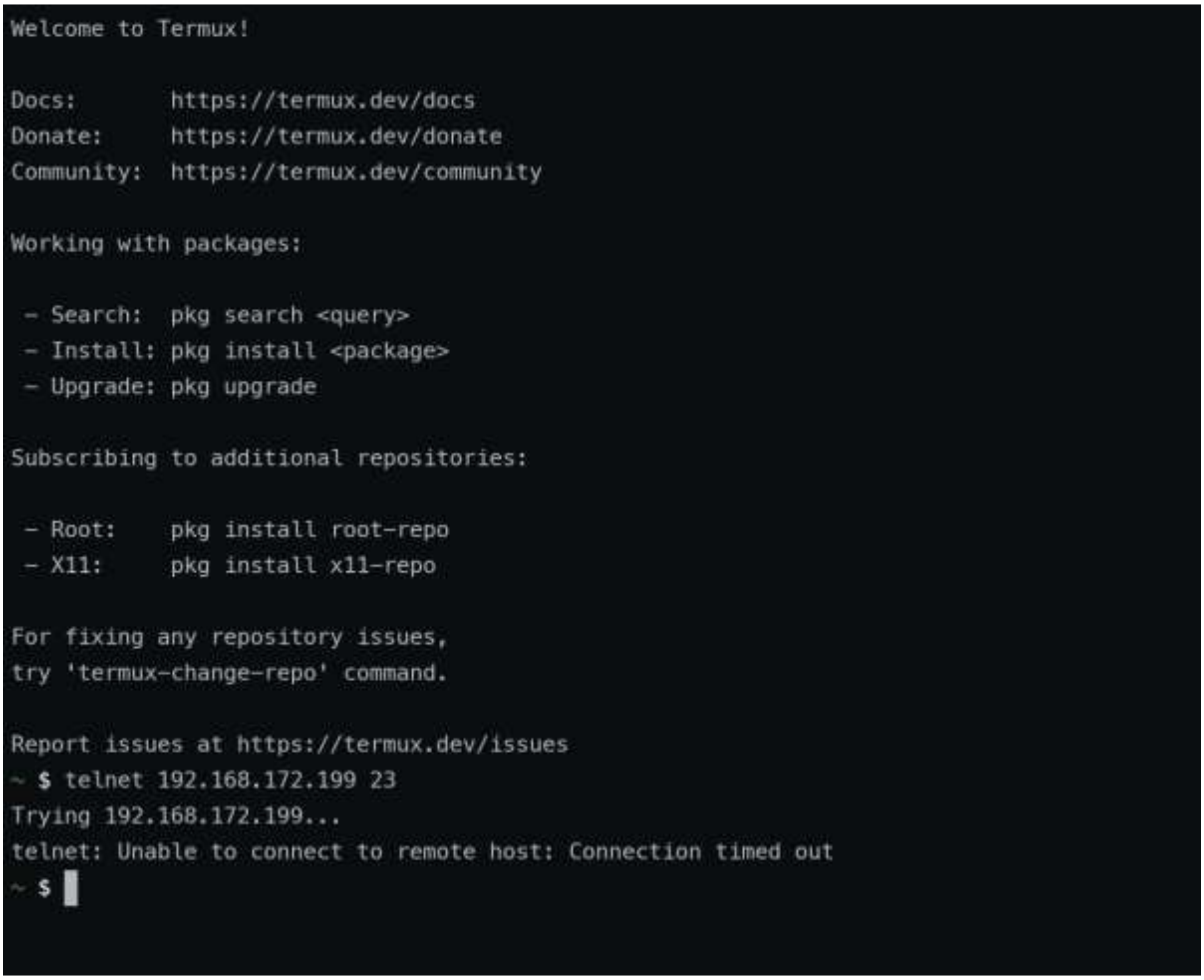


Inbound Rules

Name	Group	Profile
adb.exe		Private
adb.exe		Private
anydesk.exe		Public
anydesk.exe		Public
BlueStacks Service		All
BlueStacksAppplayerWeb		All
BlueStacksWeb		All
fccprogrammingbeautifity.exe		Public
fccprogrammingbeautifity.exe		Public
It communicates with Morpho Service		Public
It communicates with Morpho Service		Public
telnet 23 port block		All
VMware Authd Service		Domain
VMware Authd Service (private)		Private
VMware Workstation VMX		Private...
VMware Workstation VMX		Private...
@{Microsoft.BingWeather_4.53.52331.0_x...	@{Microsoft.BingWeather_4...	Domai...
@{Microsoft.DesktopAppInstaller_1.21.27...	@{Microsoft.DesktopAppIns...	Domai...
@{Microsoft.MicrosoftStickyNotes_6.0.1....	@{Microsoft.MicrosoftStick...	Domai...
@{Microsoft.SecHealthUI_1000.25873.900...	@{Microsoft.SecHealthUI_1...	Domai...
@{Microsoft.SecHealthUI_1000.27777.100...	@{Microsoft.SecHealthUI_1...	Domai...
@{Microsoft.StorePurchaseApp_22503.14...	@{Microsoft.StorePurchase...	Domai...
@{Microsoft.Todos_0.114.7122.0_x64__8w...	@{Microsoft.Todos_0.114.71...	Domai...
@{Microsoft.Todos_2.108.62932.0_x64__8...	@{Microsoft.Todos_2.108.62...	Domai...
@{Microsoft.WindowsAlarms_11.2306.23-...	@{Microsoft.WindowsAlar...	Domai...
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All
@{Microsoft.WindowsFeedbackHub_1.25...	@{Microsoft.WindowsFeed...	Domai...
@{Microsoft.ZuneMusic_11.2308.3.0_x64...	@{Microsoft.ZuneMusic_11...	Domai...
@{Microsoft.ZuneVideo_10.22091.10051....	@{Microsoft.ZuneVideo_10...	Domai...
@{MicrosoftWindows.Client.LKG_1000.22...	@{MicrosoftWindows.Client...	Domai...
KDE Connect	{78E1CD88-49E3-476E-8926-...	All
KDE Connect	{78E1CD88-49E3-476E-8926-...	All

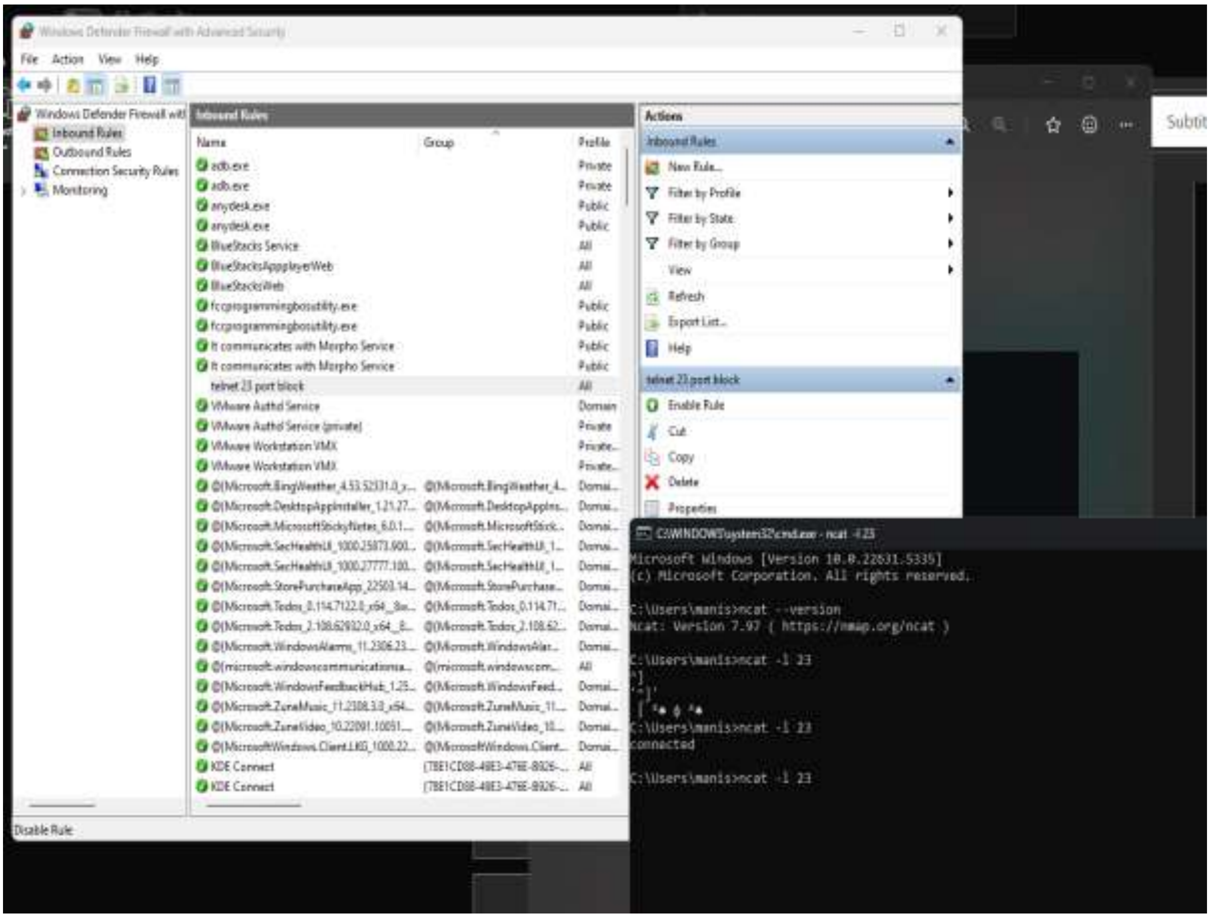
Select C:\WINDOWS\system32\cmd.exe - ncat -l 23

```
Microsoft Windows [Version 10.0.22631.5335]
(c) Microsoft Corporation. All rights reserved.

C:\Users\manis>ncat --version
Ncat: Version 7.97 ( https://nmap.org/ncat )

C:\Users\manis>ncat -l 23
^]
'^]'
 [ *● ◎ *●
C:\Users\manis>ncat -l 23
```



```
Welcome to Termux!

Docs:       https://termux.dev/docs
Donate:     https://termux.dev/donate
Community:  https://termux.dev/community

Working with packages:

 - Search:  pkg search <query>
 - Install: pkg install <package>
 - Upgrade: pkg upgrade

Subscribing to additional repositories:

 - Root:    pkg install root-repo
 - X11:     pkg install x11-repo

For fixing any repository issues,
try 'termux-change-repo' command.

Report issues at https://termux.dev/issues
~ $ telnet 192.168.172.199 23
Trying 192.168.172.199...
telnet: Unable to connect to remote host: Connection timed out
~ $ 
```

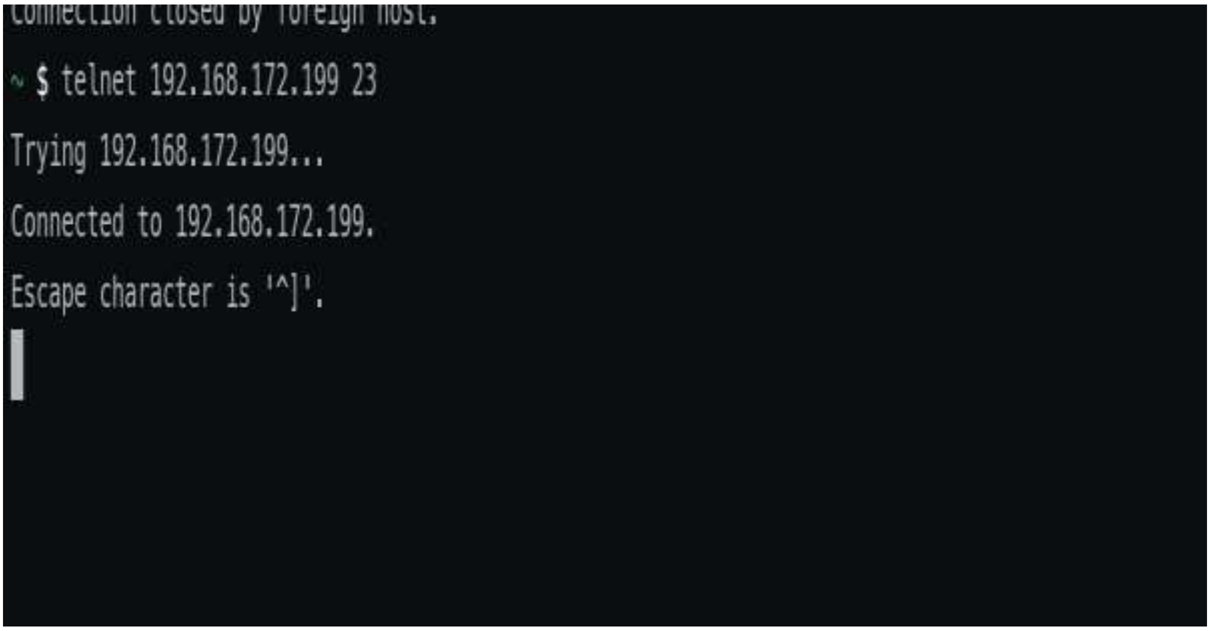
Now disable firewall and try to connect 23 port



Inbound Rules

Name	Group	Profile
adb.exe		Private
adb.exe		Private
anydesk.exe		Public
anydesk.exe		Public
BlueStacks Service		All
BlueStacksAppplayerWeb		All
BlueStacksWeb		All
fccprogrammingbosutility.exe		Public
fccprogrammingbosutility.exe		Public
It communicates with Morpho Service		Public
It communicates with Morpho Service		Public
telnet 23 port block		All
VMware Authd Service		Domain
VMware Authd Service (private)		Private
VMware Workstation VMX		Private...
VMware Workstation VMX		Private...
@{Microsoft.BingWeather_4.53.52331.0_x...	@{Microsoft.BingWeather_4...	Domai...
@{Microsoft.DesktopAppInstaller_1.21.27...	@{Microsoft.DesktopAppIns...	Domai...
@{Microsoft.MicrosoftStickyNotes_6.0.1...	@{Microsoft.MicrosoftStick...	Domai...
@{Microsoft.SecHealthUI_1000.25873.900...	@{Microsoft.SecHealthUI_1...	Domai...
@{Microsoft.SecHealthUI_1000.27777.100...	@{Microsoft.SecHealthUI_1...	Domai...
@{Microsoft.StorePurchaseApp_22503.14...	@{Microsoft.StorePurchase...	Domai...
@{Microsoft.Todos_0.114.7122.0_x64__8w...	@{Microsoft.Todos_0.114.71...	Domai...
@{Microsoft.Todos_2.108.62932.0_x64__8...	@{Microsoft.Todos_2.108.62...	Domai...
@{Microsoft.WindowsAlarms_11.2306.23...	@{Microsoft.WindowsAlar...	Domai...
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All
@{Microsoft.WindowsFeedbackHub_1.25...	@{Microsoft.WindowsFeed...	Domai...
@{Microsoft.ZuneMusic_11.2308.3.0_x64...	@{Microsoft.ZuneMusic_11...	Domai...
@{Microsoft.ZuneVideo_10.22091.10051...	@{Microsoft.ZuneVideo_10...	Domai...
@{MicrosoftWindows.Client.LKG_1000.22...	@{MicrosoftWindows.Client...	Domai...
KDE Connect	{7BE1CD88-48E3-47EE-8926-...	All
KDE Connect	{7BE1CD88-48E3-47EE-8926-...	All

```
Microsoft Windows [Version 10.0.22631.5335]
(c) Microsoft Corporation. All rights reserved.

C:\Users\manis>ncat --version
Ncat: Version 7.97 ( https://nmap.org/ncat )

C:\Users\manis>ncat -l 23
^]
'^]'
 [ *♠ ♦ *♠
C:\Users\manis>ncat -l 23
connected

C:\Users\manis>ncat -l 23
```



```
Connection closed by foreign host.
~ $ telnet 192.168.172.199 23
Trying 192.168.172.199...
Connected to 192.168.172.199.
Escape character is '^]'.
▌
```

Above image showing connected with 23 port connection established

A firewall acts as a security guard for a network, positioned between a trusted internal network (like your home or office network) and an untrusted external network (like the internet). Its primary function is to **monitor and filter incoming and outgoing network traffic based on a predefined set of security rules**, allowing non-threatening traffic to pass through and blocking dangerous traffic.

Here's a breakdown of how firewalls filter traffic:

1. Rule Examination: Every data packet attempting to traverse the firewall is evaluated against a set of established rules. These rules are configured by network administrators and dictate what traffic is allowed or blocked based on various criteria. If a packet doesn't comply with any of the rules, it's typically discarded.

2. Key Filtering Mechanisms:

- **Packet Filtering (Stateless Inspection):** This is the most basic and oldest form of firewall filtering.
    - It inspects individual data packets in isolation, looking at information in the packet's header, such as:
        - **Source and Destination IP addresses:** Where the packet originated and where it's trying to go.
        - **Source and Destination Port numbers:** These specify the application or service the traffic is associated with (e.g., port 80 for HTTP web traffic, port 22 for SSH).
        - **Protocols:** The type of communication protocol being used (e.g., TCP, UDP, ICMP).
    - Based on these header details and the predefined rules, the firewall decides to allow or block the packet.
    - **Limitation:** It doesn't remember past packets or the context of a connection, making it less secure against more sophisticated attacks.
- **Stateful Inspection (Dynamic Packet Filtering):** This is a more advanced and common method.
    - It builds upon packet filtering by maintaining a "state table" or "connection table" that tracks active network connections.
    - When an outgoing packet is sent, the firewall records its details. When an incoming response arrives, the firewall checks if it matches an active session in its state table.

    - Only packets that correspond to a valid, previously established outgoing connection are allowed through. This significantly enhances security by preventing unsolicited incoming connections.
    - **Benefit:** More secure than basic packet filtering as it understands the context of a conversation.
- **Proxy Service (Application-Level Gateway):**
    - A proxy firewall acts as an intermediary between the internal network and the external network.
    - Instead of allowing direct communication, the proxy intercepts requests from internal users, establishes its own connection to the external destination, fetches the data, inspects it, and then relays it to the user.
    - Similarly, for incoming traffic, the proxy receives it first, inspects it, and then forwards it to the internal system if it's deemed safe.
    - **Benefit:** Provides an extra layer of isolation, preventing direct access to internal systems and allowing for deeper inspection of application-level content.
- **Next-Generation Firewalls (NGFWs):**
    - These are modern, multi-layered firewalls that combine the capabilities of packet filtering, stateful inspection, and proxy services with additional advanced features.
    - They can perform **deep packet inspection (DPI)**, which examines the actual payload (content) of packets for specific patterns, signatures, or anomalies indicative of malicious behavior (like malware or specific keywords).
    - NGFWs often integrate with intrusion prevention systems (IPS), antivirus software, and other security tools for comprehensive threat protection.
    - They can also control traffic based on specific applications, users, or even content categories.

3. Decision Execution and Logging: After evaluating a packet against its rules and applying the relevant filtering mechanism, the firewall makes a decision:

- **Allow:** The packet is permitted to pass through to its intended destination.
- **Block (Reject):** The packet is dropped, and an "unreachable error" message might be sent back to the sender.
- **Drop:** The packet is silently discarded without any notification to the sender.

Firewalls also typically maintain a log of their actions, recording details of accepted and rejected packets. This logging provides administrators with valuable insights into network traffic patterns, potential threats, and helps in troubleshooting.

4. Continuous Updates: Firewall rules are not static. Administrators regularly update and refine these rules based on emerging threats, changing network requirements, and security policies to maintain optimal network security. Modern firewalls can also use AI-driven security operations platforms to adapt to new threats.

In essence, a firewall acts as a customizable gatekeeper, meticulously inspecting every piece of data that tries to enter or leave a network, ensuring that only authorized and safe traffic is allowed to flow.