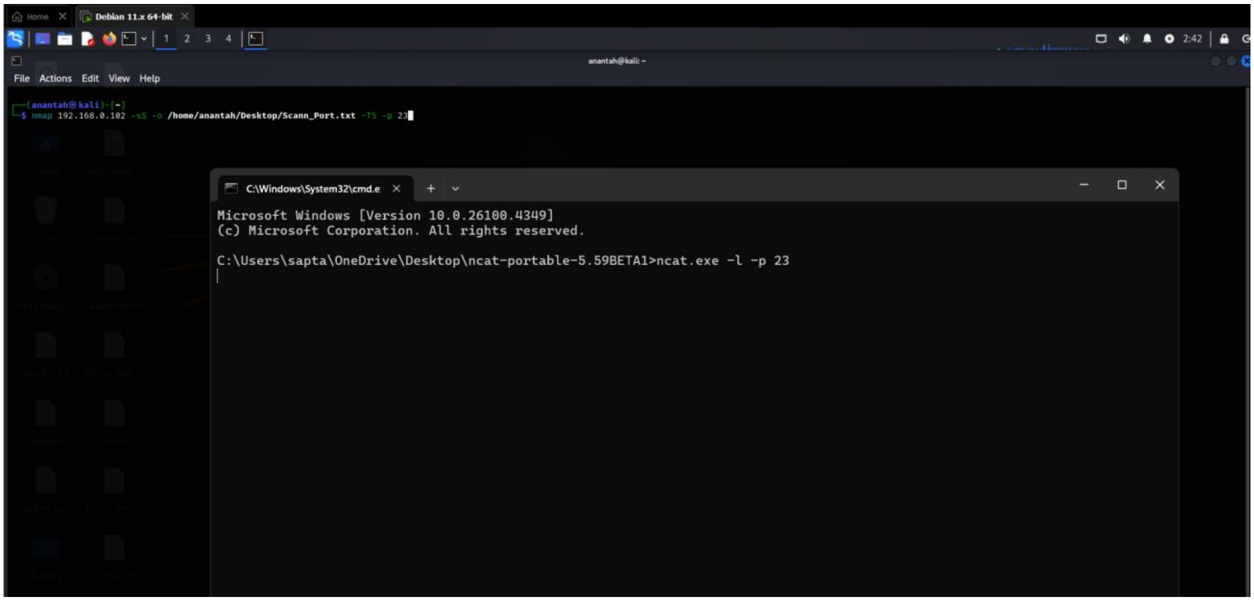
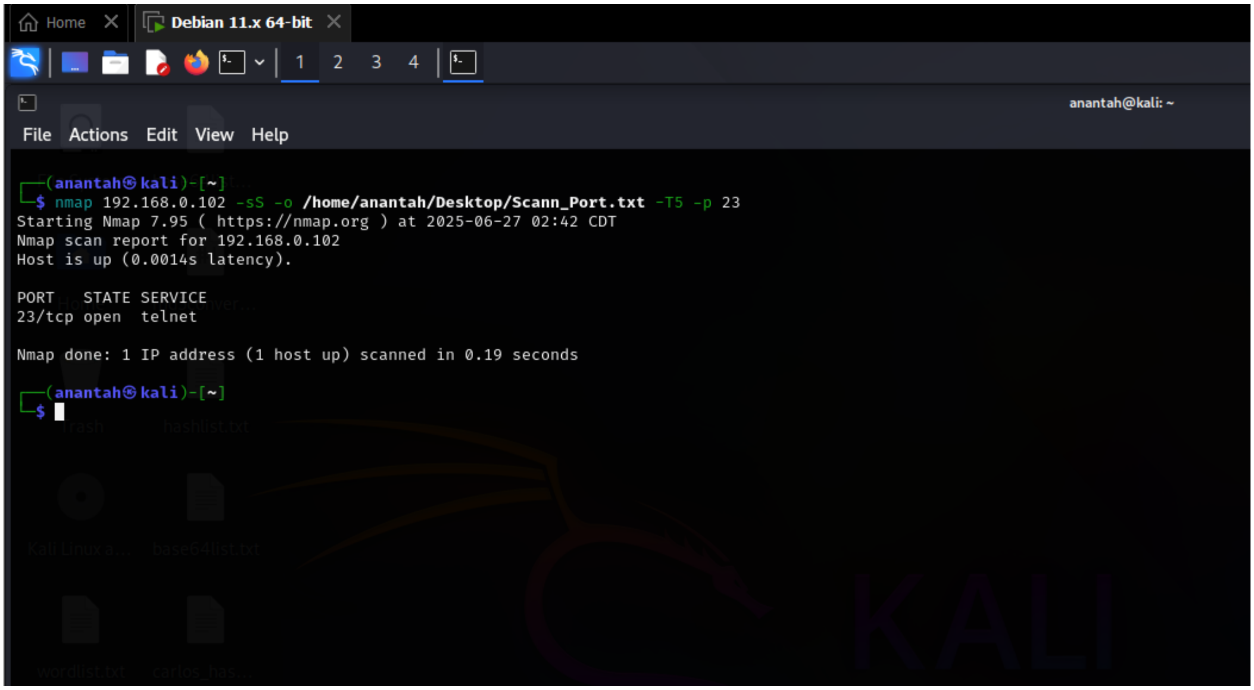
Task: Setup and Use a Firewall on Windows



```
┌──(anantah㉿kali)-[~]
└─$ nmap 192.168.0.102 -sS -o /home/anantah/Desktop/Scann_Port.txt -T5 -p 23
```

```
Microsoft Windows [Version 10.0.26100.4349]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23
```



```
┌──(anantah㉿kali)-[~]
└─$ nmap 192.168.0.102 -sS -o /home/anantah/Desktop/Scann_Port.txt -T5 -p 23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-27 02:42 CDT
Nmap scan report for 192.168.0.102
Host is up (0.0014s latency).

PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(anantah㉿kali)-[~]
└─$ 
```

As You can See My Telnet Port is shown As Open When I Scan.

Objective: Configure and test basic firewall rules to allow or block traffic.

Tools: Windows Firewall.

Deliverables: Screenshot/configuration file showing firewall rules applied.

Steps Followed:

1. Opened the Windows Defender Firewall with Advanced Security.

2. Navigated to 'Inbound Rules' > 'New Rule...' to create a new inbound rule.

3. Chose 'Port' as the rule type and specified TCP port 23 (Telnet).

4. Selected 'Block the connection' to block incoming traffic.

5. Applied the rule to all profiles (Domain, Private, Public).

6. Named the rule 'Block Telnet Port Incoming Traffic'.

7. Saved and applied the rule.

8. Verified that the rule appears in the Inbound Rules list and is enabled.

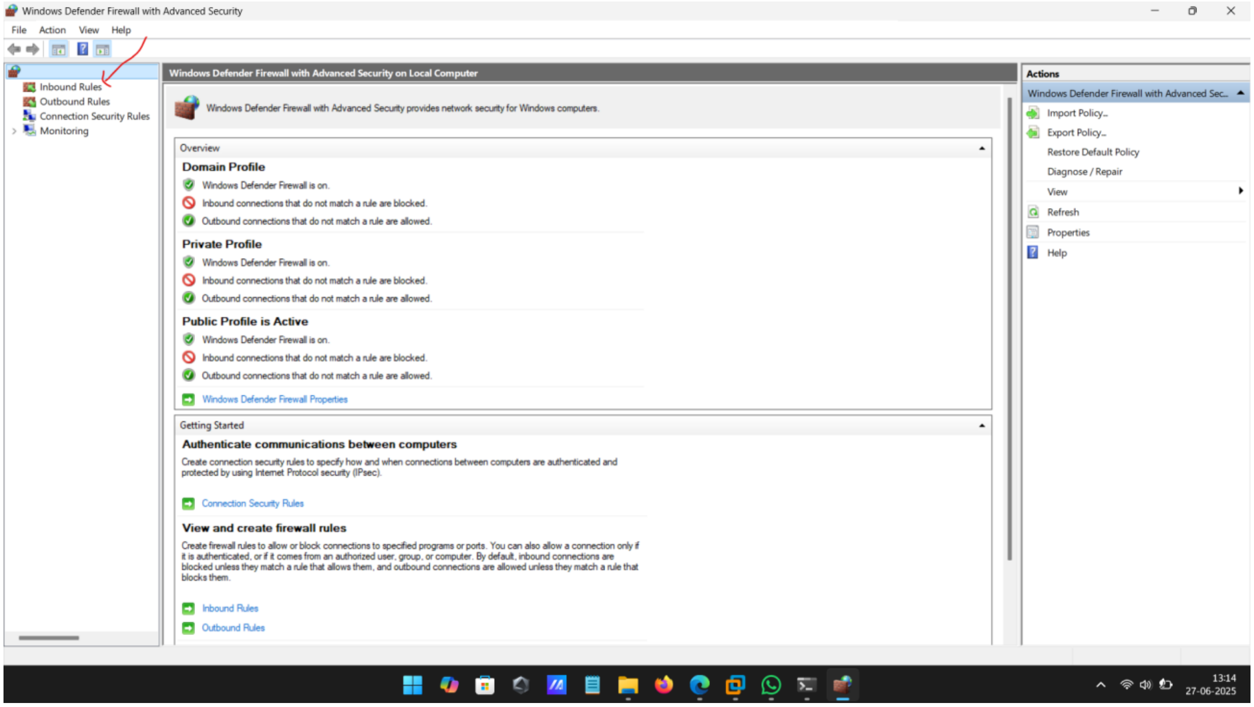
9. Attempted a Telnet connection to localhost on port 23, which failed - confirming the rule works.

10. This screenshot shows the final step where the rule was named and confirmed.

Summary:

The firewall was configured to block Telnet traffic on TCP port 23. Before applying the rule, the port was open to connections. After applying the rule, all incoming Telnet traffic was blocked, effectively filtering unwanted access.

Screenshot of the configuration process:



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).

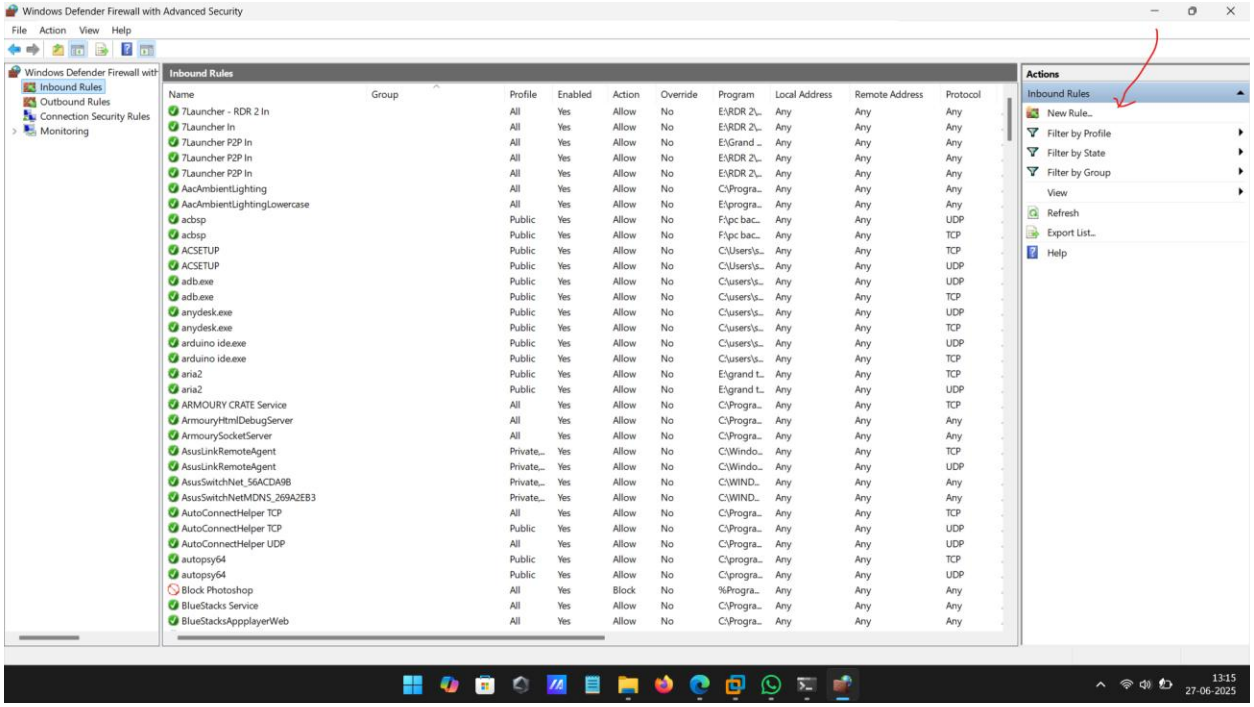
Connection Security Rules

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.

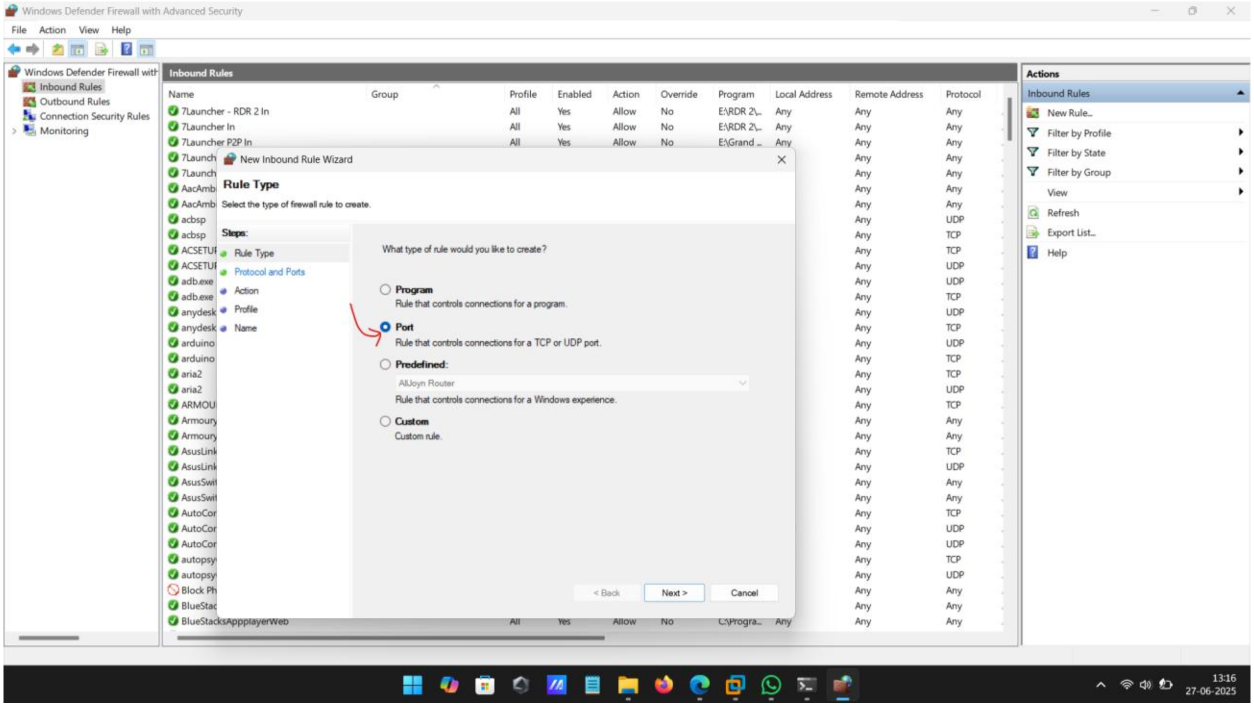
Inbound Rules

Outbound Rules



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
✓ 7Launcher - RDR 2 In		All	Yes	Allow	No	E:\RDR 2\...	Any	Any	Any
✓ 7Launcher In		All	Yes	Allow	No	E:\RDR 2\...	Any	Any	Any
✓ 7Launcher P2P In		All	Yes	Allow	No	E:\Grand ...	Any	Any	Any
✓ 7Launcher P2P In		All	Yes	Allow	No	E:\RDR 2\...	Any	Any	Any
✓ 7Launcher P2P In		All	Yes	Allow	No	E:\RDR 2\...	Any	Any	Any
✓ AacAmbientLighting		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
✓ AacAmbientLightingLowercase		All	Yes	Allow	No	E:\progra...	Any	Any	Any
✓ acbsp		Public	Yes	Allow	No	F:\pc bac...	Any	Any	UDP
✓ acbsp		Public	Yes	Allow	No	F:\pc bac...	Any	Any	TCP
✓ ACSETUP		Public	Yes	Allow	No	C:\Users\s...	Any	Any	TCP
✓ ACSETUP		Public	Yes	Allow	No	C:\Users\s...	Any	Any	UDP
✓ adb.exe		Public	Yes	Allow	No	C:\users\s...	Any	Any	UDP
✓ adb.exe		Public	Yes	Allow	No	C:\users\s...	Any	Any	TCP
✓ anydesk.exe		Public	Yes	Allow	No	C:\users\s...	Any	Any	UDP
✓ anydesk.exe		Public	Yes	Allow	No	C:\users\s...	Any	Any	TCP
✓ arduino ide.exe		Public	Yes	Allow	No	C:\users\s...	Any	Any	UDP
✓ arduino ide.exe		Public	Yes	Allow	No	C:\users\s...	Any	Any	TCP
✓ aria2		Public	Yes	Allow	No	E:\grand t...	Any	Any	TCP
✓ aria2		Public	Yes	Allow	No	E:\grand t...	Any	Any	UDP
✓ ARMOURY CRATE Service		All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
✓ ArmouryHtmlDebugServer		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
✓ ArmourySocketServer		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
✓ AsusLinkRemoteAgent		Private,...	Yes	Allow	No	C:\Windo...	Any	Any	TCP
✓ AsusLinkRemoteAgent		Private,...	Yes	Allow	No	C:\Windo...	Any	Any	UDP
✓ AsusSwitchNet_56ACDA9B		Private,...	Yes	Allow	No	C:\WIND...	Any	Any	Any
✓ AsusSwitchNetMDNS_269A2EB3		Private,...	Yes	Allow	No	C:\WIND...	Any	Any	Any
✓ AutoConnectHelper TCP		All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
✓ AutoConnectHelper TCP		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
✓ AutoConnectHelper UDP		All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
✓ autopsy64		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
✓ autopsy64		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
🚫 Block Photoshop		All	Yes	Block	No	%Progra...	Any	Any	Any
✓ BlueStacks Service		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
✓ BlueStacksAppplayerWeb		All	Yes	Allow	No	C:\Progra...	Any	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?

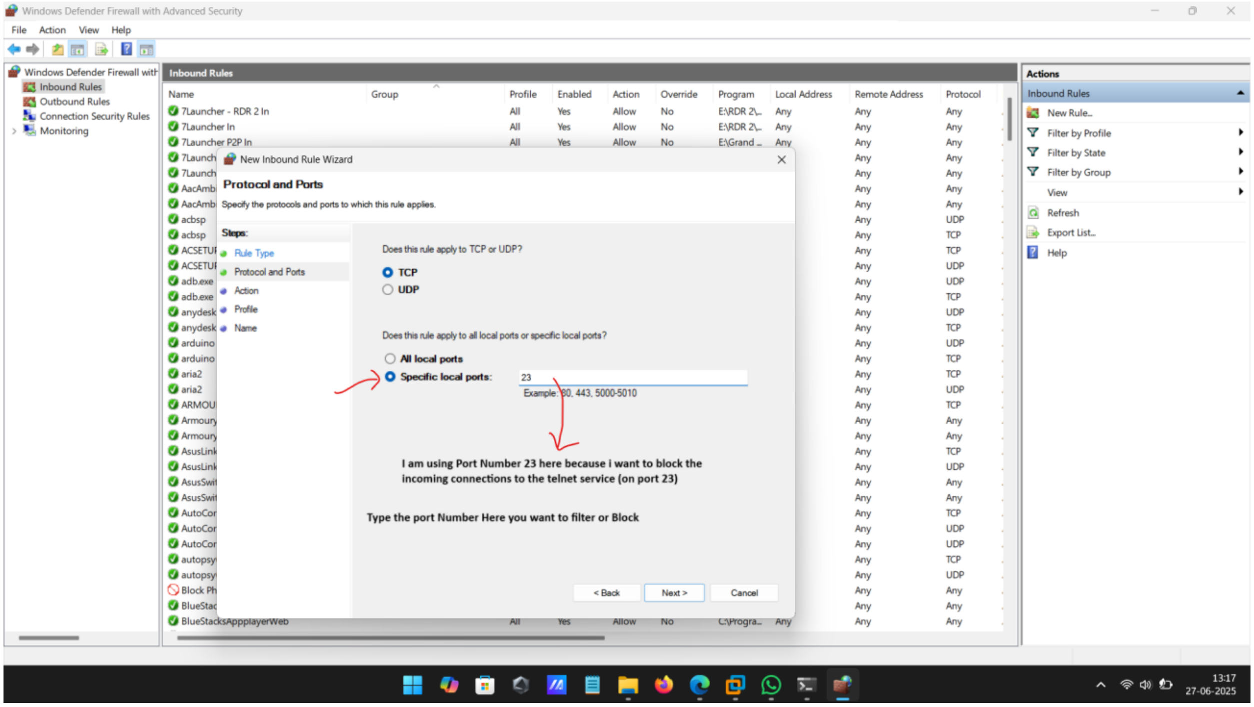
○ **Program**
Rule that controls connections for a program.

● **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.

< Back | Next > | Cancel



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**

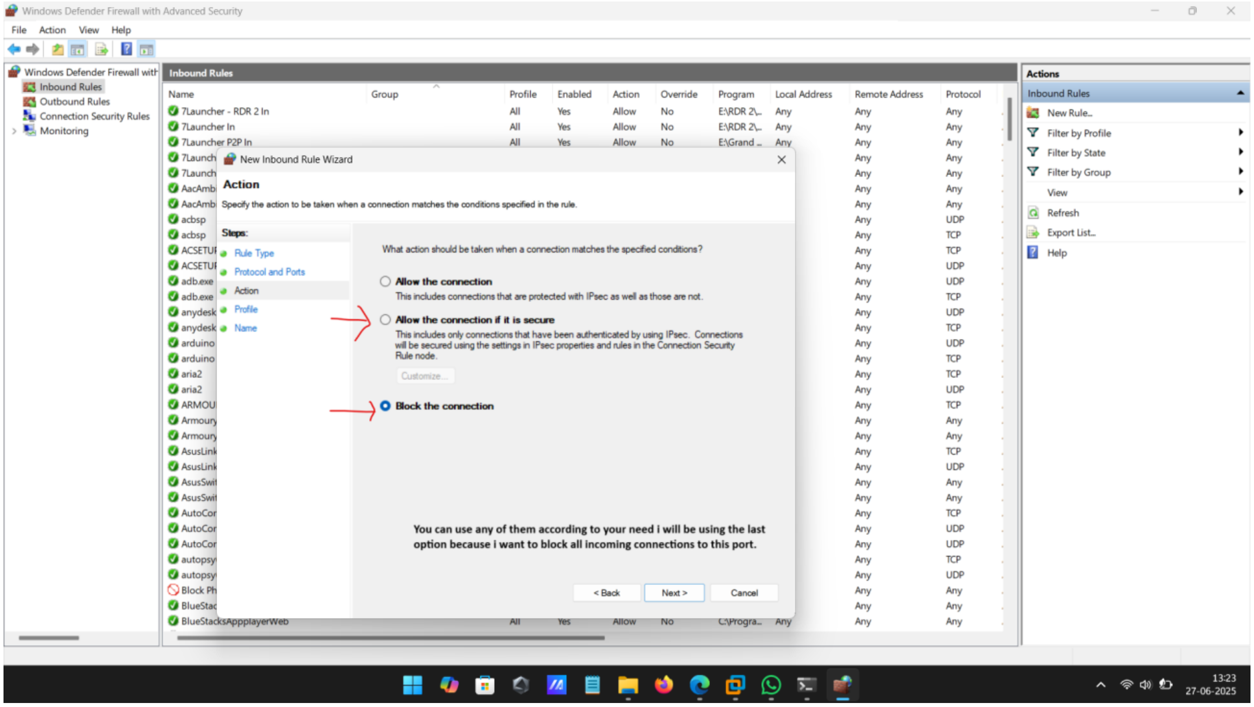
Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 23
Example: 80, 443, 5000-5010

I am using Port Number 23 here because i want to block the incoming connections to the telnet service (on port 23)

Type the port Number Here you want to filter or Block

< Back | Next > | Cancel



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

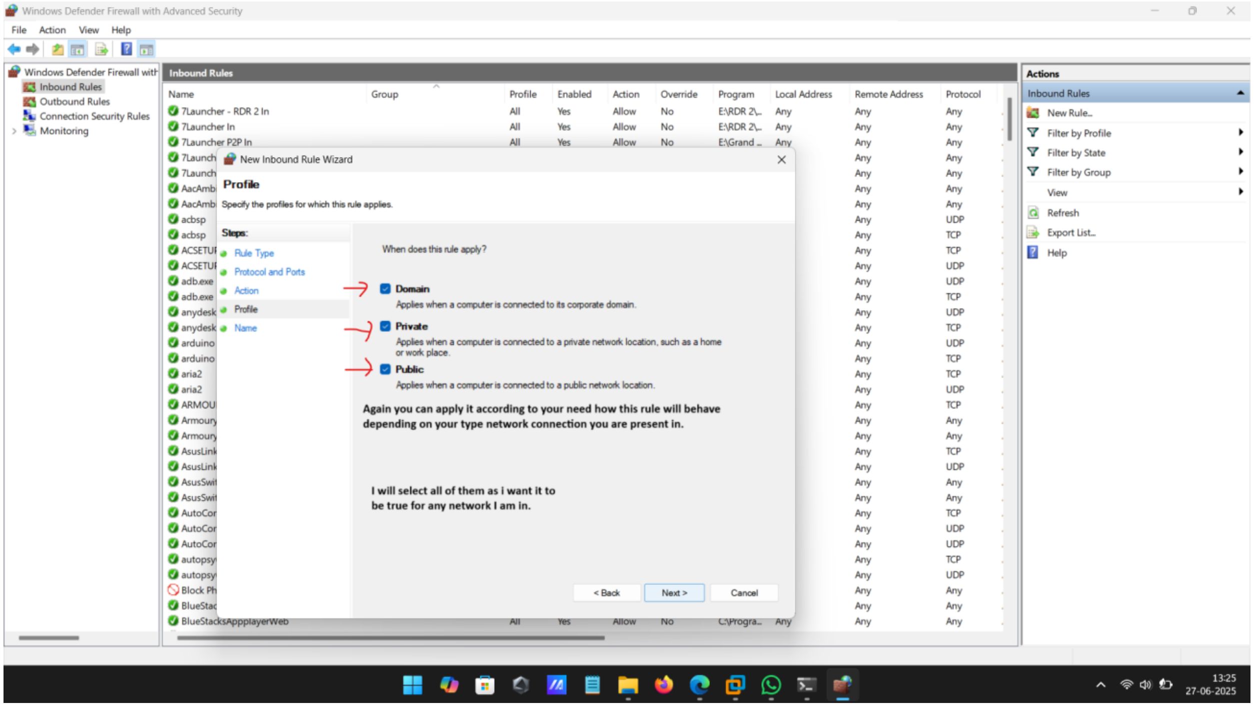
What action should be taken when a connection matches the specified conditions?

○ **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**

You can use any of them according to your need i will be using the last option because i want to block all incoming connections to this port.



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?

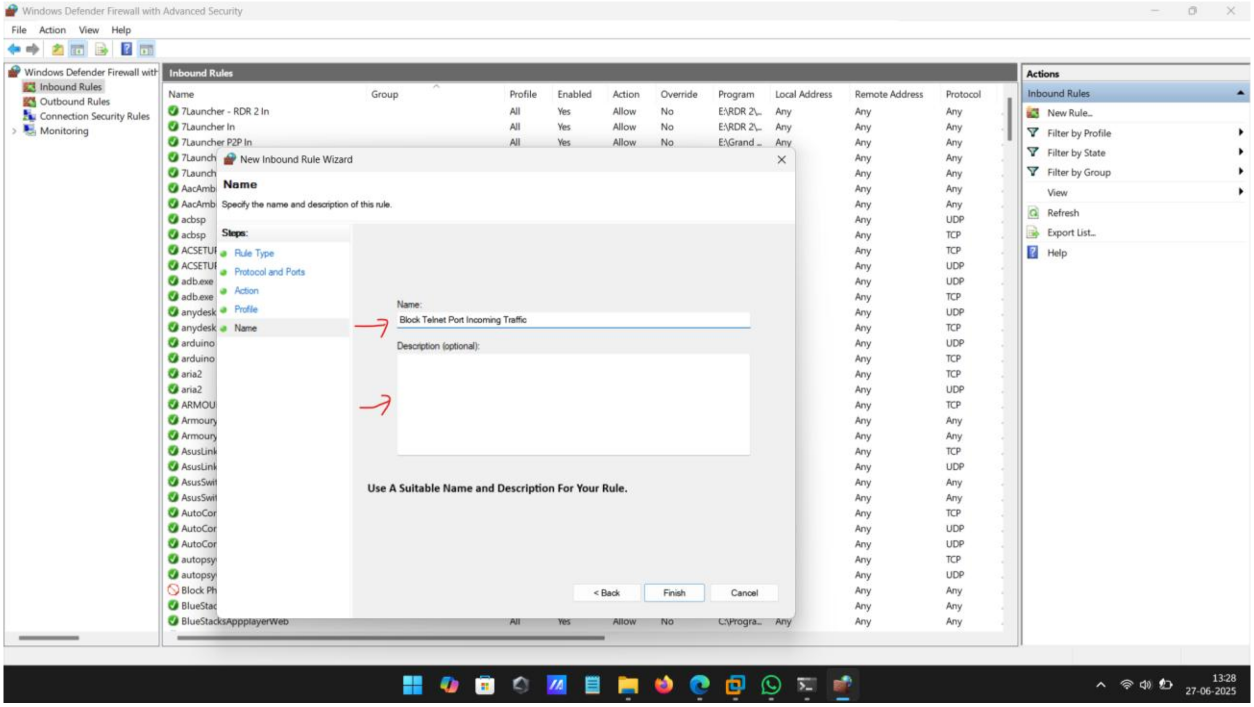
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **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.

Again you can apply it according to your need how this rule will behave depending on your type network connection you are present in.

I will select all of them as i want it to be true for any network I am in.



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
7Launcher - RDR 2 In		All	Yes	Allow	No	E:\RDR 2\...	Any	Any	Any
7Launcher In		All	Yes	Allow	No	E:\RDR 2\...	Any	Any	Any
7Launcher P2P In		All	Yes	Allow	No	E:\Grand ...	Any	Any	Any
7Launch								Any	Any
7Launch								Any	Any
AacAmb								Any	Any
AacAmb								Any	Any
acbsp								Any	UDP
acbsp								Any	TCP
ACSETUI								Any	TCP
ACSETUI								Any	UDP
adb.exe								Any	UDP
adb.exe								Any	TCP
anydesk								Any	UDP
anydesk								Any	TCP
arduino								Any	UDP
arduino								Any	TCP
aria2								Any	TCP
aria2								Any	UDP
ARMOU								Any	TCP
Armoury								Any	Any
Armoury								Any	Any
AsusLink								Any	TCP
AsusLink								Any	UDP
AsusSwi								Any	Any
AsusSwi								Any	Any
AutoCor								Any	TCP
AutoCor								Any	UDP
AutoCor								Any	UDP
autopsy								Any	TCP
autopsy								Any	UDP
Block Ph								Any	Any
BlueStac								Any	Any
BlueStacksAppplayerWeb		All	Yes	Allow	No	C:\Progra...	Any	Any	Any

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

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

Name:

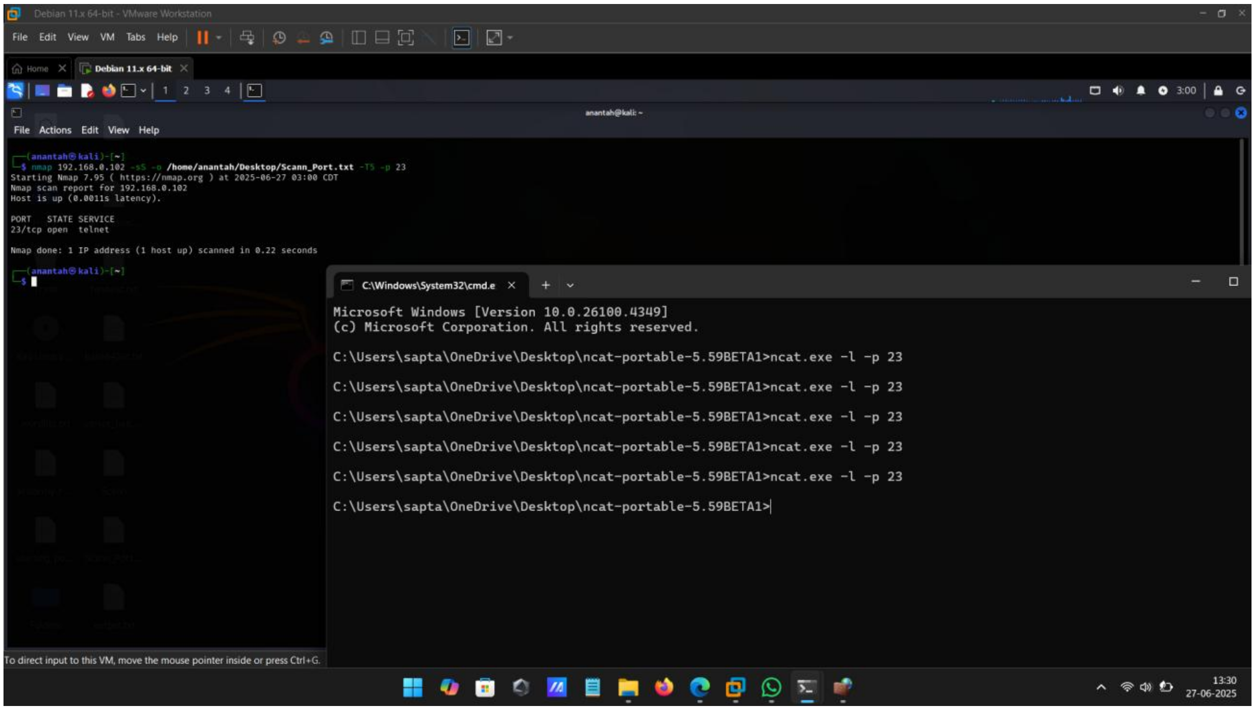
Block Telnet Port Incoming Traffic

Description (optional):

Use A Suitable Name and Description For Your Rule.

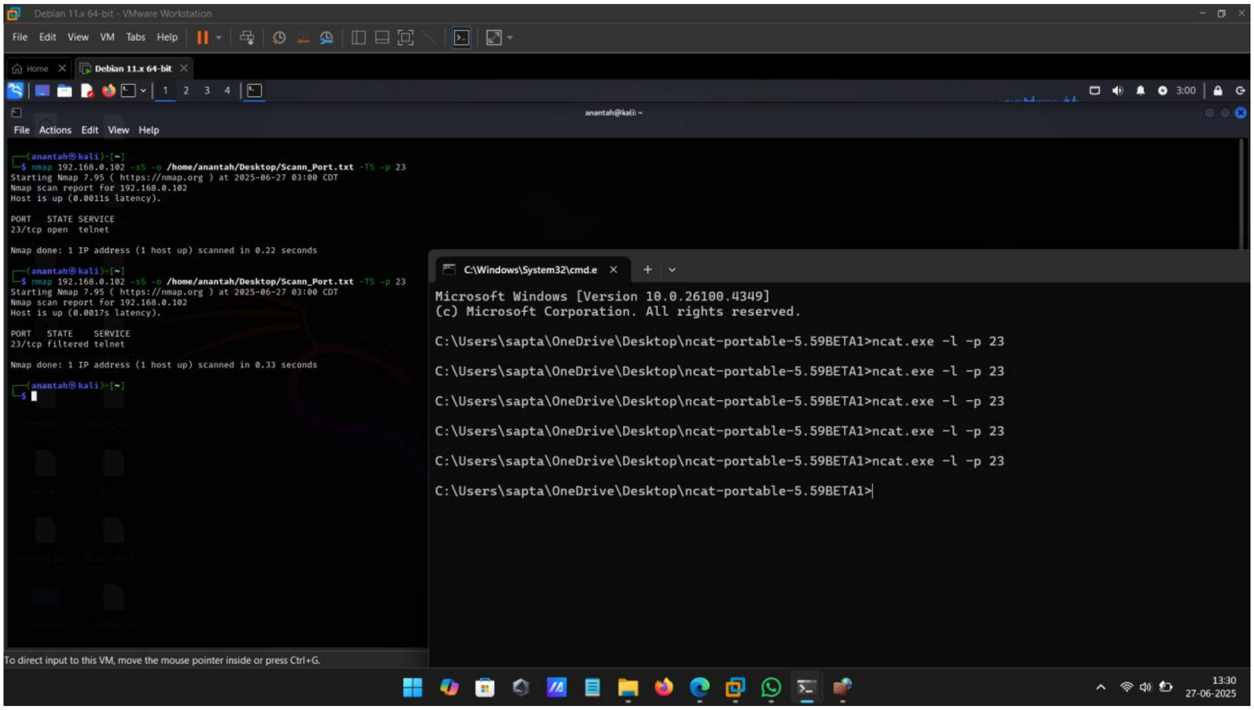
< Back | Finish | Cancel

After Configuration This What We can Observe :


Debian 11.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Debian 11.x 64-bit
File Actions Edit View Help
anantah@kali: ~
C:\Windows\System32\cmd.e
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:00
13:30
27-06-2025

```
┌──(anantah㉿kali)-[~]
└─$ nmap 192.168.0.102 -sS -o /home/anantah/Desktop/Scann_Port.txt -T5 -p 23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-27 03:00 CDT
Nmap scan report for 192.168.0.102
Host is up (0.0011s latency).

PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(anantah㉿kali)-[~]
└─$
```

```
Microsoft Windows [Version 10.0.26100.4349]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>
```


Debian 11.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Debian 11.x 64-bit
File Actions Edit View Help
anantah@kali: ~
C:\Windows\System32\cmd.e
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:00
13:30
27-06-2025

```
┌──(anantah㉿kali)-[~]
└─$ nmap 192.168.0.102 -sS -o /home/anantah/Desktop/Scann_Port.txt -T5 -p 23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-27 03:00 CDT
Nmap scan report for 192.168.0.102
Host is up (0.0011s latency).

PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(anantah㉿kali)-[~]
└─$ nmap 192.168.0.102 -sS -o /home/anantah/Desktop/Scann_Port.txt -T5 -p 23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-27 03:00 CDT
Nmap scan report for 192.168.0.102
Host is up (0.0017s latency).

PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

┌──(anantah㉿kali)-[~]
└─$
```

```
Microsoft Windows [Version 10.0.26100.4349]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>ncat.exe -l -p 23

C:\Users\sapta\OneDrive\Desktop\ncat-portable-5.59BETA1>
```

Observations: Any Incoming Traffic to port 23/tcp is blocked after applying the Firewall filter.