8/8/2025

Configure Firewall and Test Rules

(LINUX, WINDOWS)

@SRCybersecurity

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

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

Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

Deliverables: Screenshot/configuration file showing firewall rules applied.

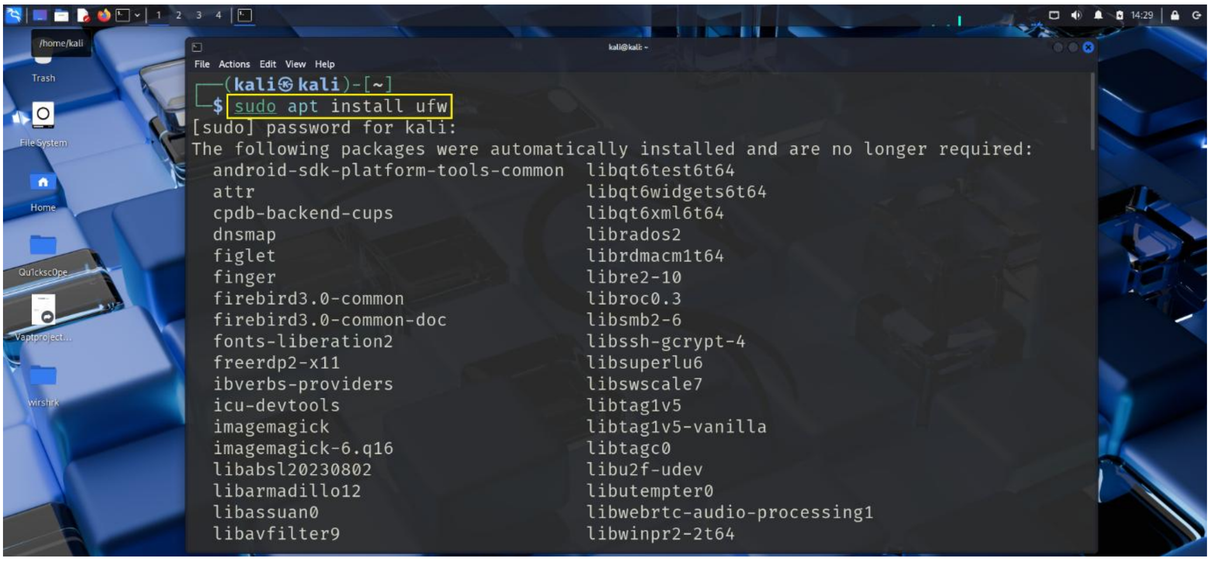
Here's a step-by-step guide to configure and test firewall rules on both Windows and Linux (UFW), depending on your system. Choose the section that matches your OS.

FOR LINUX (UFW - Uncomplicated Firewall)

Make sure UFW is installed and enabled:

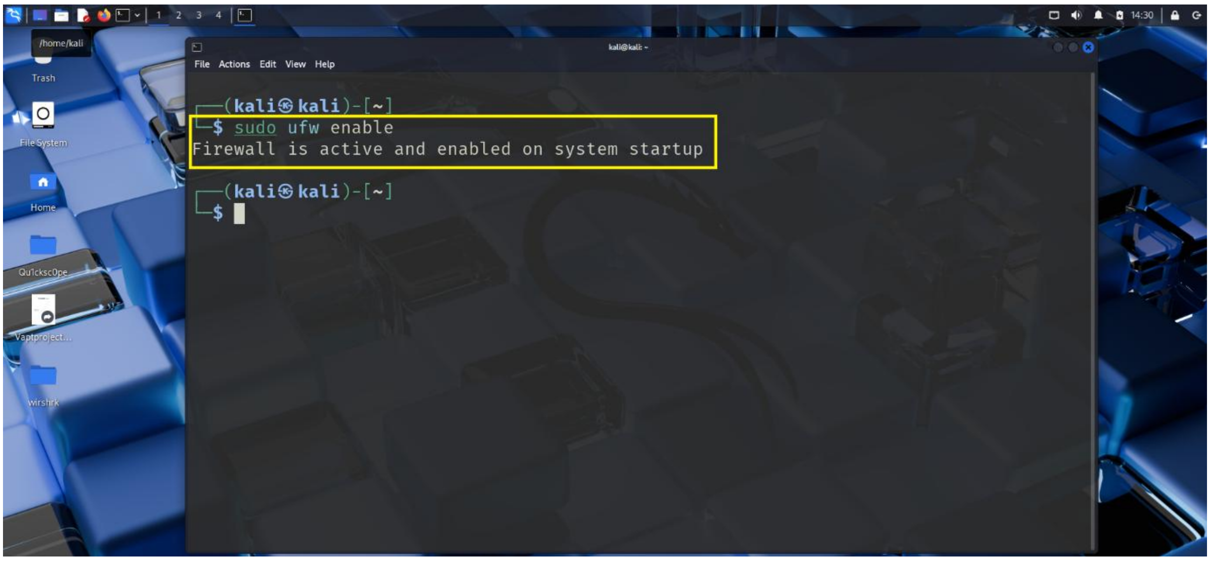
Run cmd

sudo apt install ufw



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install ufw
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  android-sdk-platform-tools-common  libqt6test6t64
  attr                               libqt6widgets6t64
  cpdb-backend-cups                  libqt6xml6t64
  dnsmap                             librados2
  figlet                             librdmacm1t64
  finger                             libre2-10
  firebird3.0-common                 libroc0.3
  firebird3.0-common-doc             libsmb2-6
  fonts-liberation2                  libssh-gcrypt-4
  freerdp2-x11                       libsuperlu6
  ibverbs-providers                  libswscale7
  icu-devtools                       libtag1v5
  imagemagick                        libtag1v5-vanilla
  imagemagick-6.q16                  libtagc0
  libabsl20230802                    libu2f-udev
  libarmadillo12                     libutempter0
  libassuan0                         libwebrtc-audio-processing1
  libavfilter9                       libwinpr2-2t64
```

sudo ufw enable



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(kali㉿kali)-[~]
└─$ 
```

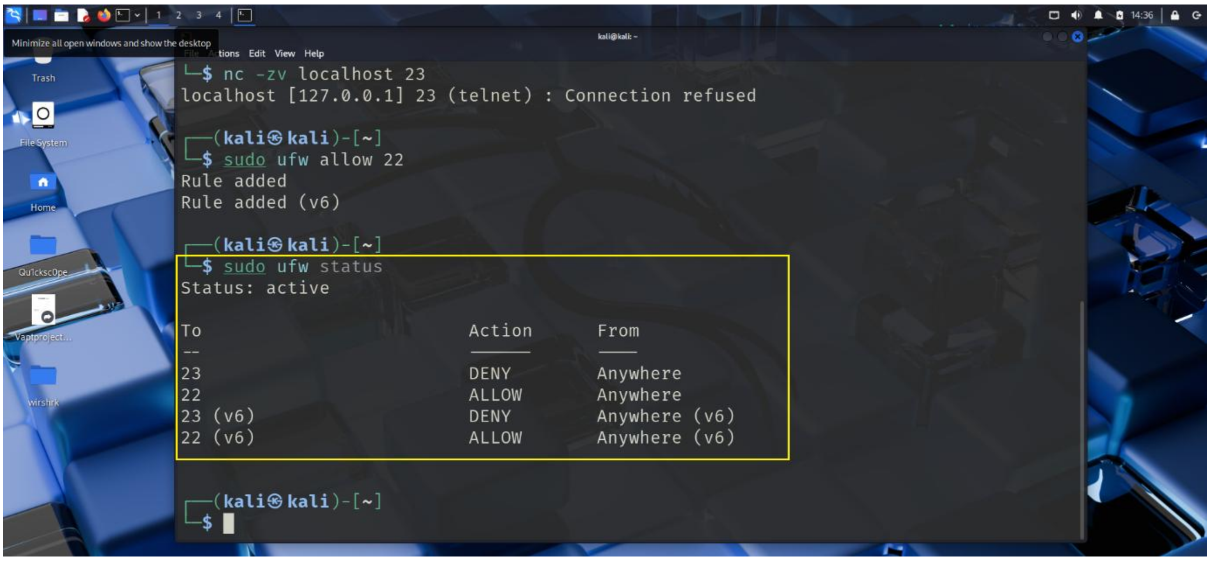
1. Open Firewall Configuration Tool

UFW is used via the terminal. No GUI needed.

2. List Current Firewall Rules

Rum cmd

sudo ufw status numbered



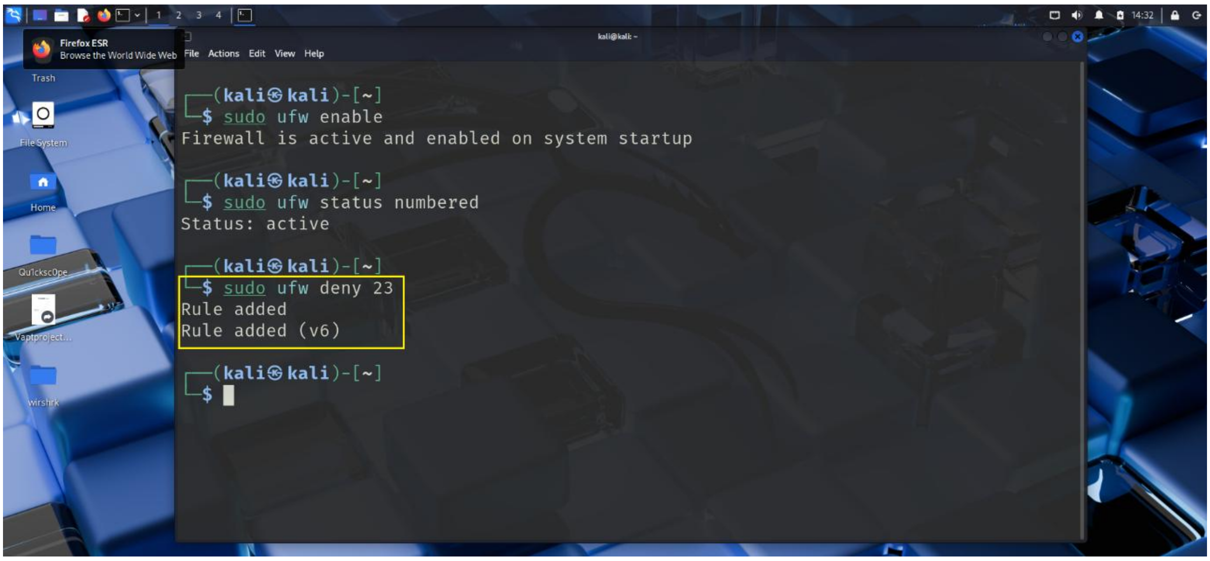
```
└─$ nc -zv localhost 23
localhost [127.0.0.1] 23 (telnet) : Connection refused

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         DENY        Anywhere
22                         ALLOW       Anywhere
23 (v6)                    DENY        Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)

┌──(kali㉿kali)-[~]
└─$ 
```

Minimize all open windows and show the desktop
Trash
File System
Home
Qu!cksc0pe
Vaptproject...
wirshrk
File Actions Edit View Help
kali@kali: ~
14:36

3. Add Rule to Block Inbound Traffic on Port 23 (Telnet)

Run cmd

sudo ufw deny 23



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered
Status: active

┌──(kali㉿kali)-[~]
└─$ sudo ufw deny 23
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ 
```

4. Test the Rule

You can test with:

- Telnet client:

Run cmd

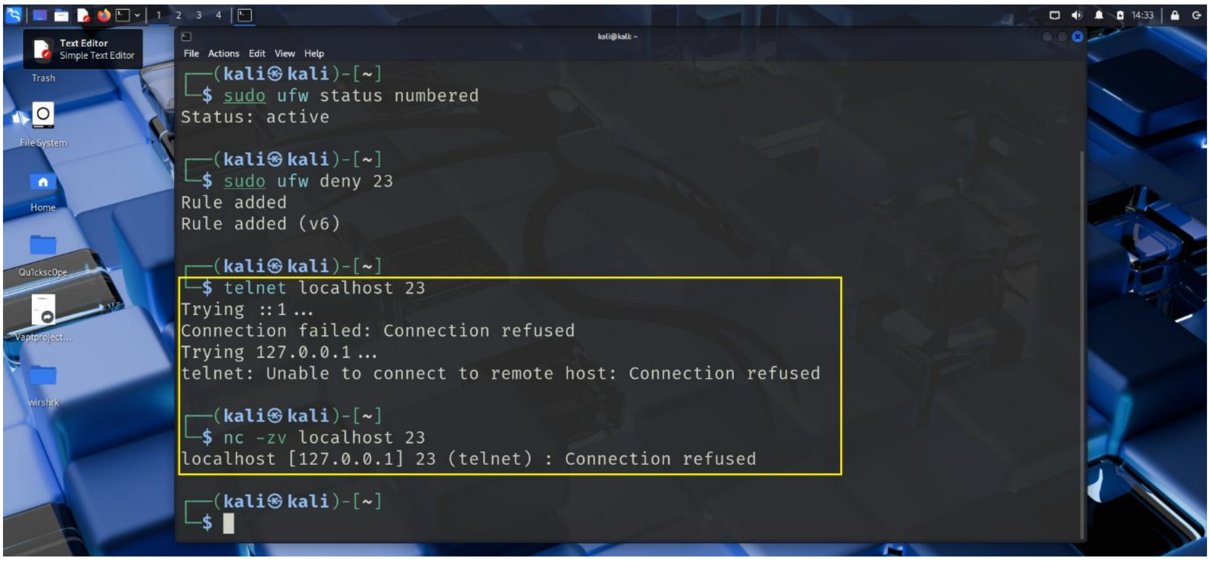
telnet localhost 23

Or use nc (netcat):

Run cmd

nc -zv localhost 23

Can see a connection refused or timeout.



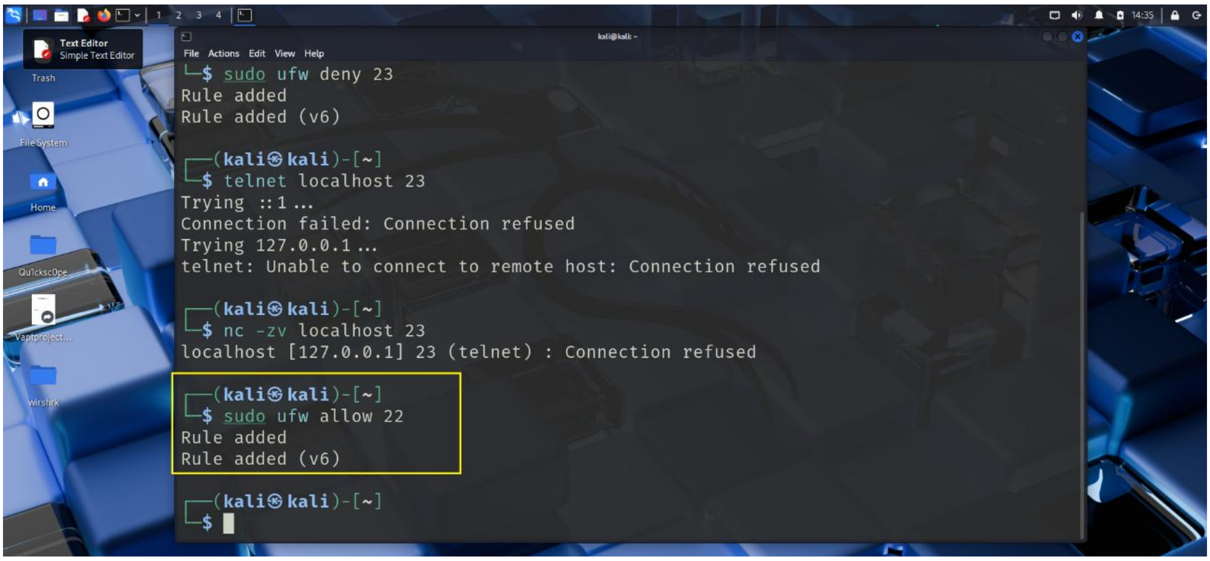
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered
Status: active

┌──(kali㉿kali)-[~]
└─$ sudo ufw deny 23
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

┌──(kali㉿kali)-[~]
└─$ nc -zv localhost 23
localhost [127.0.0.1] 23 (telnet) : Connection refused

┌──(kali㉿kali)-[~]
└─$ 
```

5. Add Rule to Allow SSH (Port 22)

Run cmd

sudo ufw allow 22

This is important if you're using SSH to manage the system remotely.

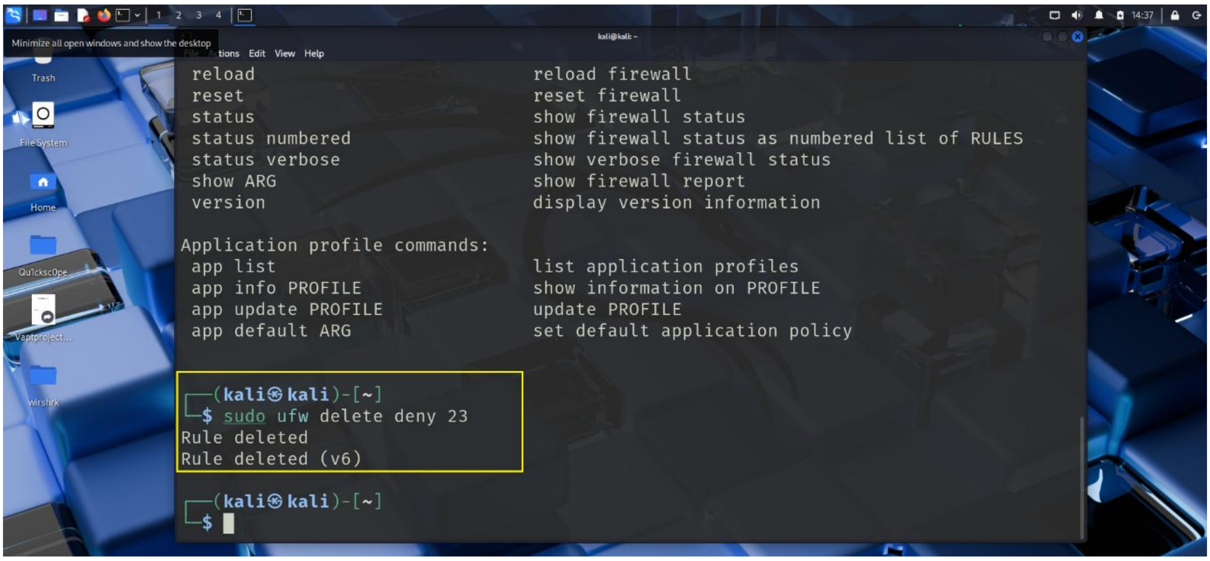


```
└─$ sudo ufw deny 23
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

┌──(kali㉿kali)-[~]
└─$ nc -zv localhost 23
localhost [127.0.0.1] 23 (telnet) : Connection refused

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ 
```

6. Remove the Block Rule (Restore Original State)

Rum cmd

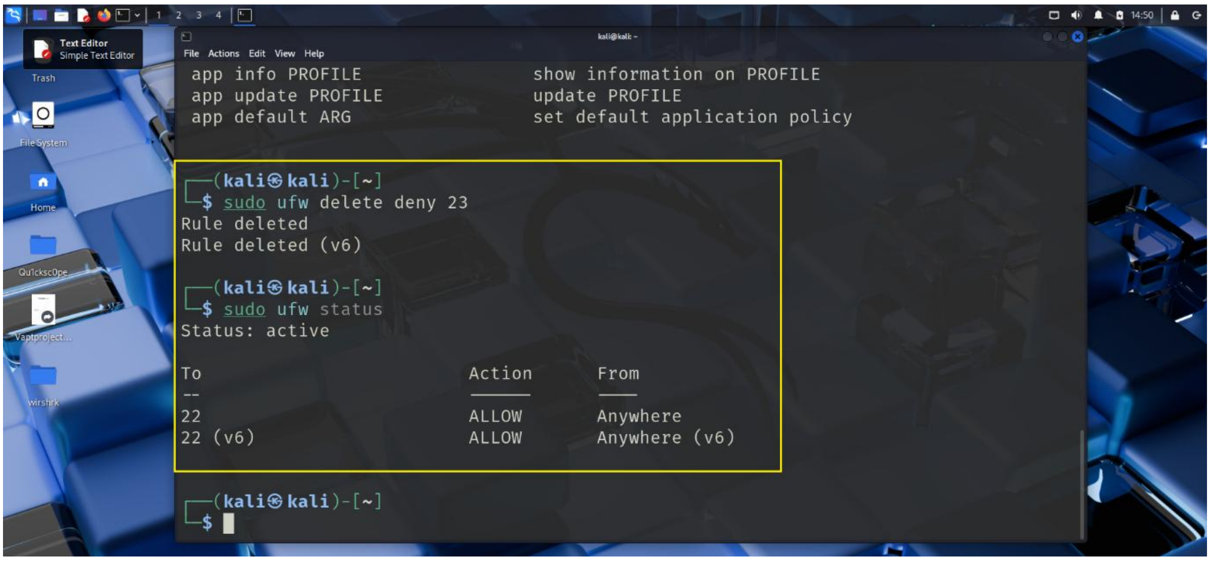
sudo ufw delete deny 23



Minimize all open windows and show the desktop
Trash
File System
Home
QuIcksc0pe
Vaptproject...
wirshrk
kali@kali: ~
File Actions Edit View Help

```
   reload                         reload firewall
   reset                          reset firewall
   status                         show firewall status
   status numbered                show firewall status as numbered list of RULES
   status verbose                 show verbose firewall status
   show ARG                       show firewall report
   version                        display version information

Application profile commands:
   app list                       list application profiles
   app info PROFILE               show information on PROFILE
   app update PROFILE             update PROFILE
   app default ARG                set default application policy

┌──(kali㉿kali)-[~]
└─$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)

┌──(kali㉿kali)-[~]
└─$ █
```

Use sudo ufw status numbered to find the rule number if needed.

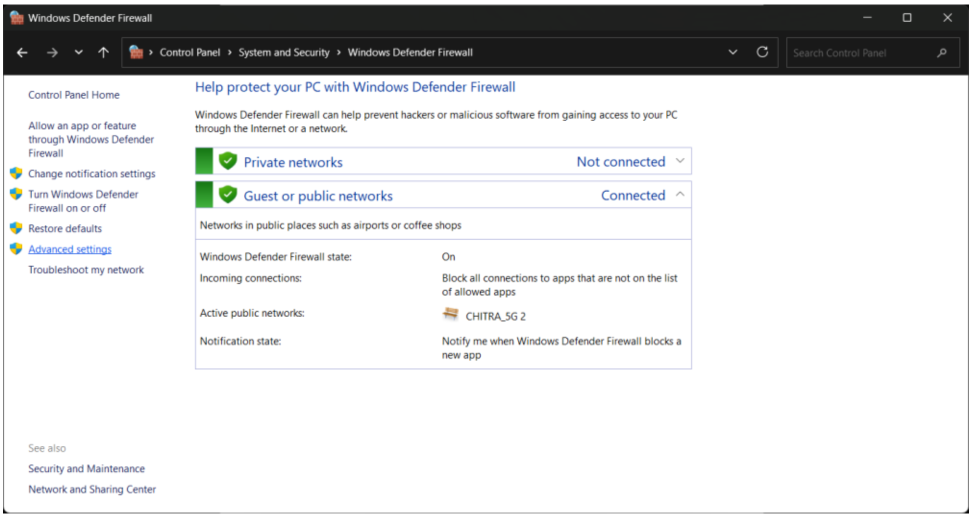


```
   app info PROFILE               show information on PROFILE
   app update PROFILE             update PROFILE
   app default ARG                set default application policy

┌──(kali㉿kali)-[~]
└─$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)

┌──(kali㉿kali)-[~]
└─$ █
```

FOR WINDOWS (Windows Defender Firewall)

1. Open Firewall Configuration Tool

- Go to Control Panel > System and Security > Windows Defender Firewall.
- Or search: "Windows Defender Firewall with Advanced Security".



Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

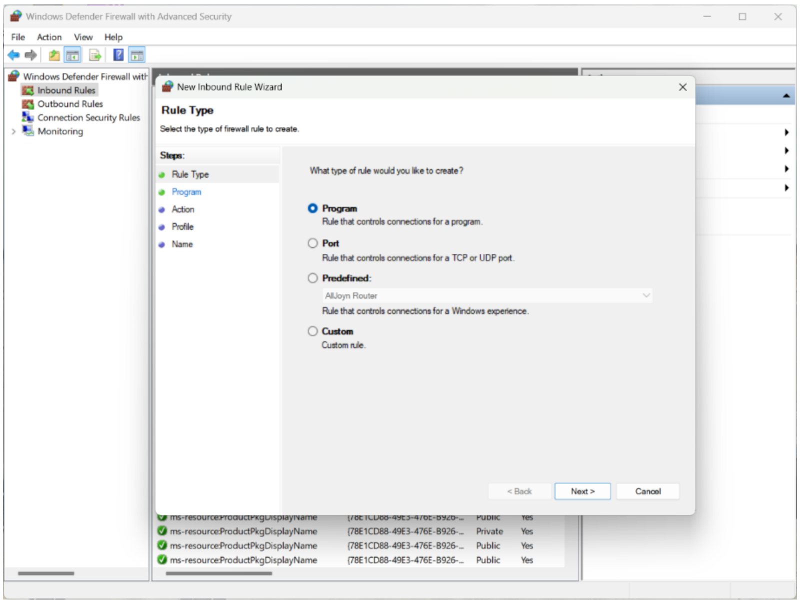
Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	CHITRA_5G 2
Notification state:	Notify me when Windows Defender Firewall blocks a new app

2. List Current Firewall Rules

- In the **Advanced Settings** panel, check:
  - Inbound Rules
  - Outbound Rules



Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
< Back
Next >
Cancel

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.

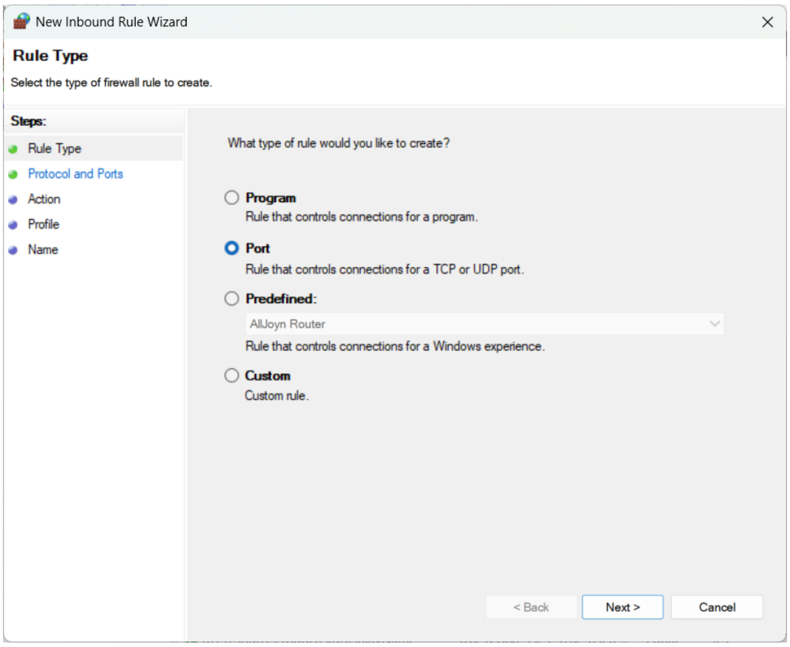
○ Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.

ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes

3. Block Inbound Traffic on Port 23

- In **Inbound Rules**, click **New Rule...**
- Select **Port** > Click **Next**



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

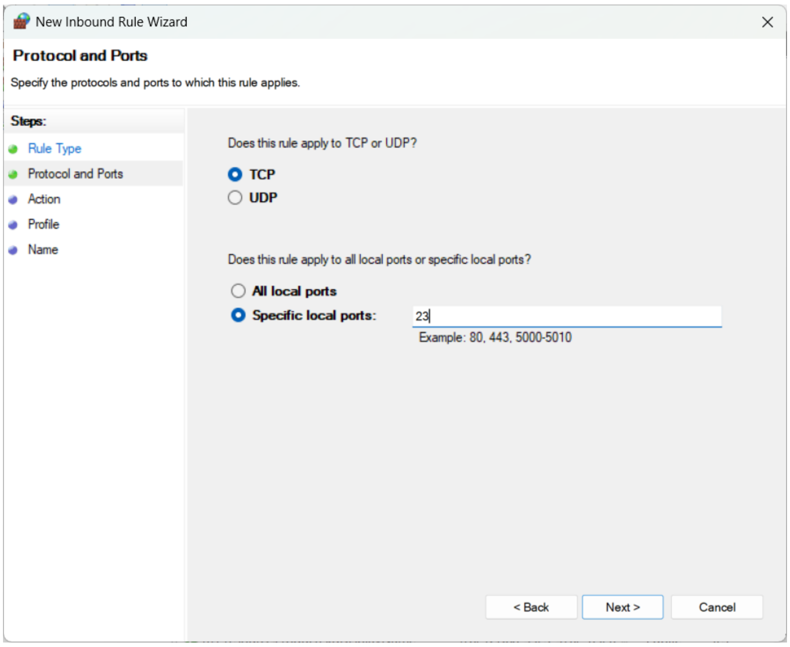
○ **Program**
Rule that controls connections for a program.

● **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.

- Choose **TCP** > Specific local ports: 23



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

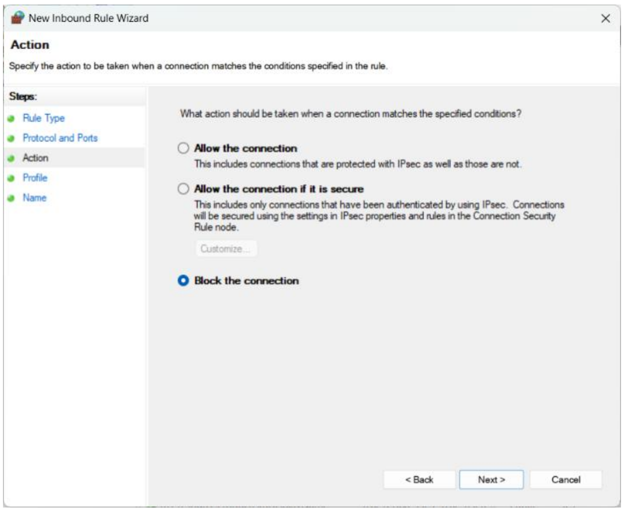
Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

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

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

- Action: **Block the connection**



Action

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

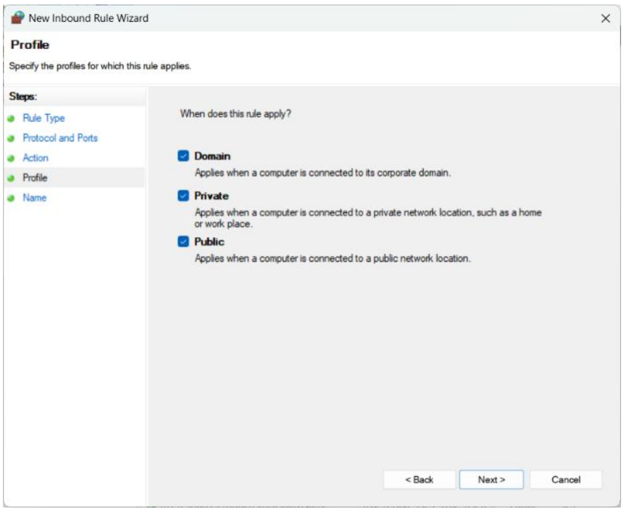
What action should be taken when a connection matches the specified conditions?

○ **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**

- Apply to all profiles (Domain, Private, Public)



Profile

Specify the profiles for which this rule applies.

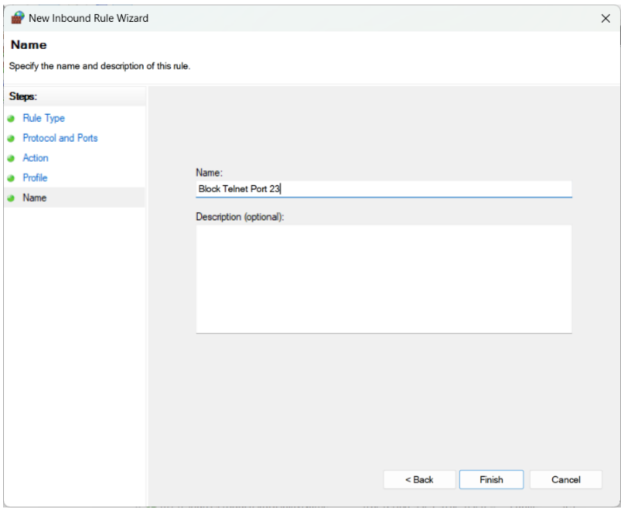
When does this rule apply?

☑ **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.

- Name it: Block Telnet Port 23



Name

Specify the name and description of this rule.

Name:
Block Telnet Port 23

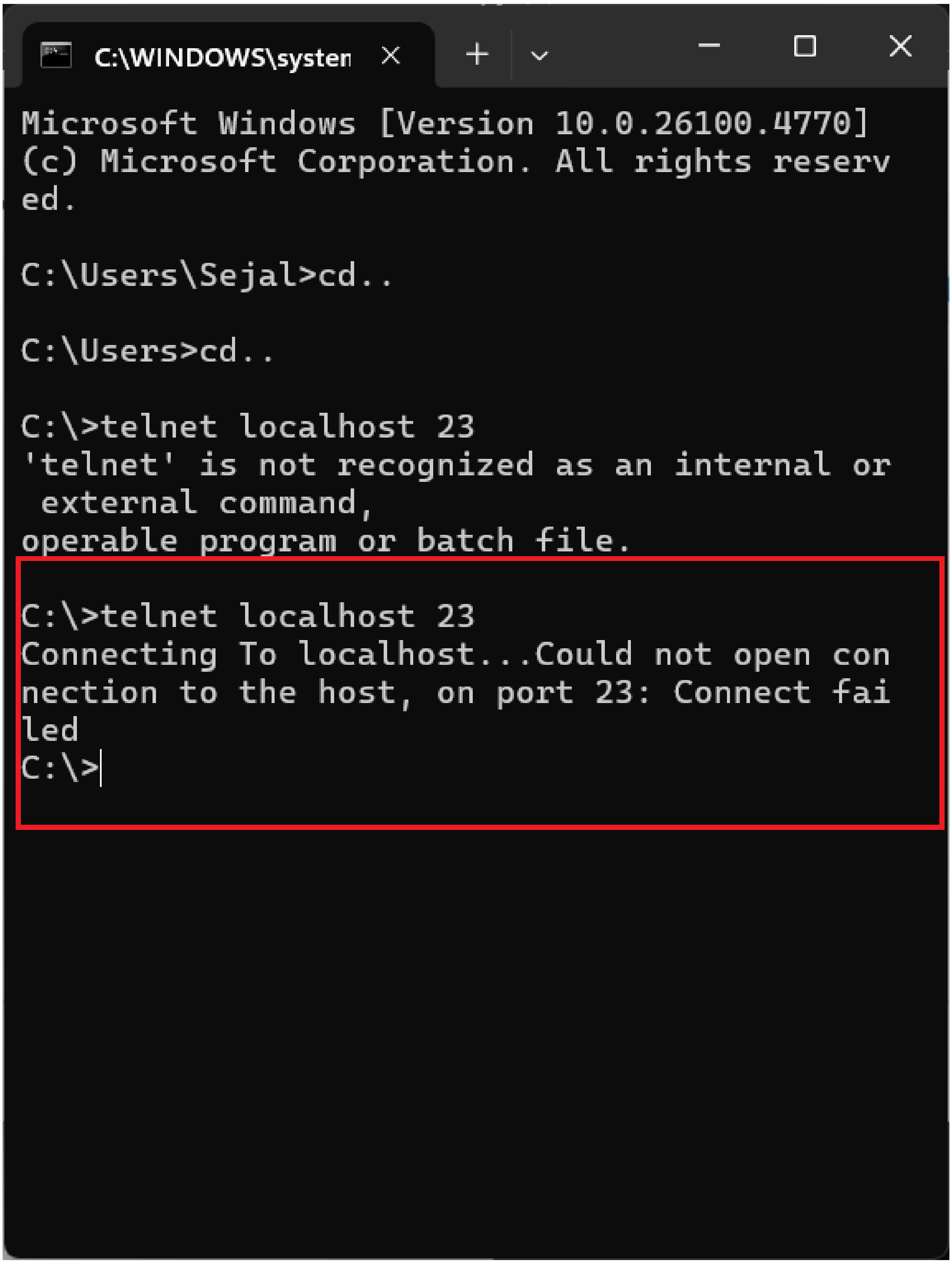
Description (optional):

4. Test the Rule

Use Telnet client:

1. Install from Optional Features if not present.
2. Run cmd

   telnet localhost 23



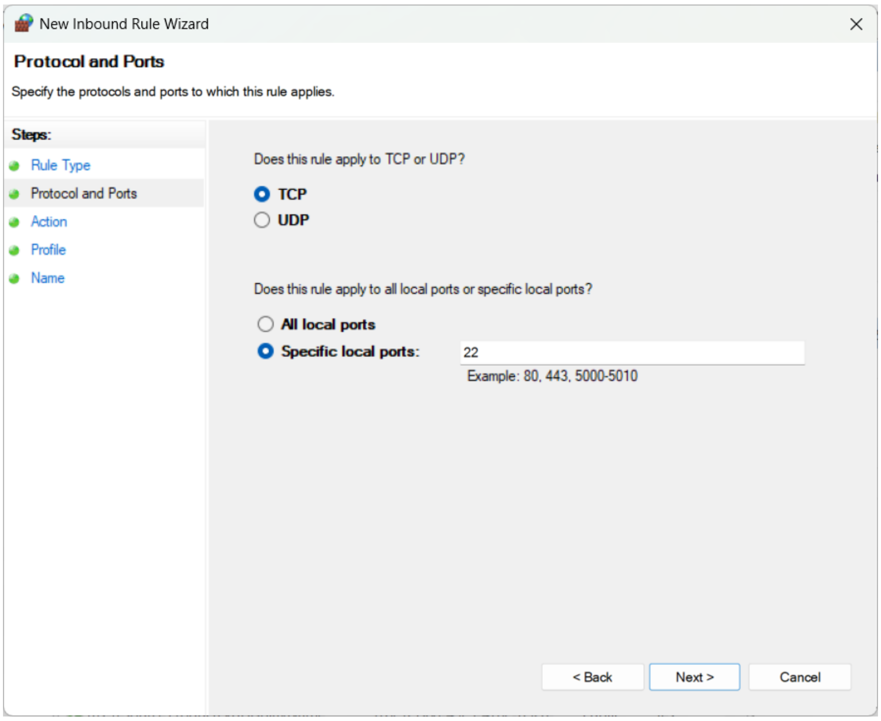
```
Microsoft Windows [Version 10.0.26100.4770]
(c) Microsoft Corporation. All rights reserv
ed.

C:\Users\Sejal>cd..

C:\Users>cd..

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

C:\>telnet localhost 23
Connecting To localhost...Could not open con
nection to the host, on port 23: Connect fai
led
C:\>
```

Get a failure to connect.

5. Allow SSH (Port 22) *(Optional for Windows)*

Not typically used unless you're running OpenSSH server. If so:

- Go to Inbound Rules > New 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?

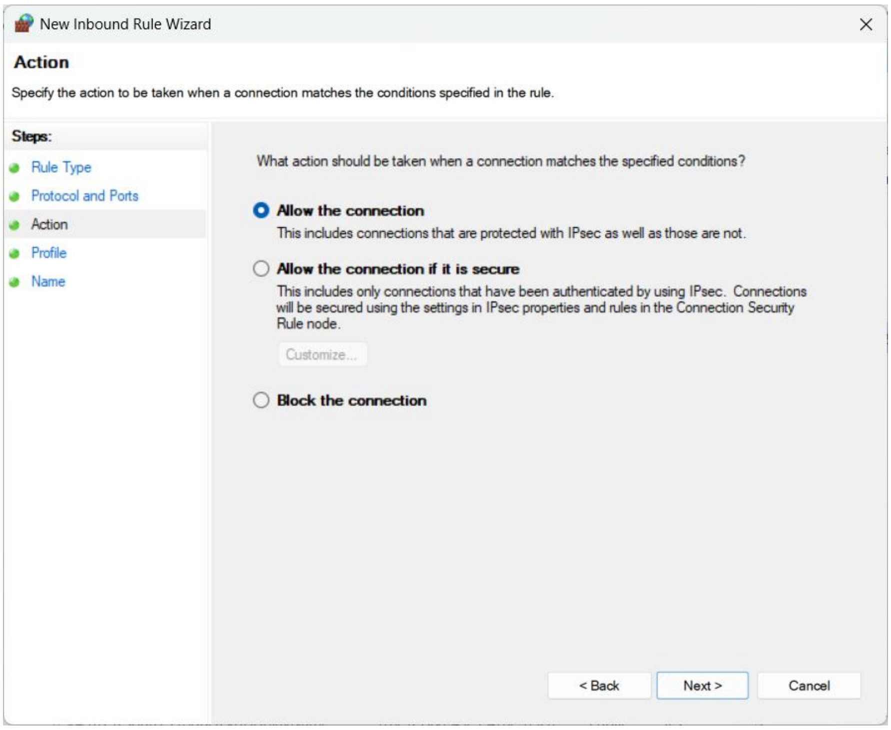
● TCP
○ UDP

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

○ All local ports
● Specific local ports: 22

Example: 80, 443, 5000-5010

- Port: 22 > Allow the connection



New Inbound Rule Wizard

Action

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

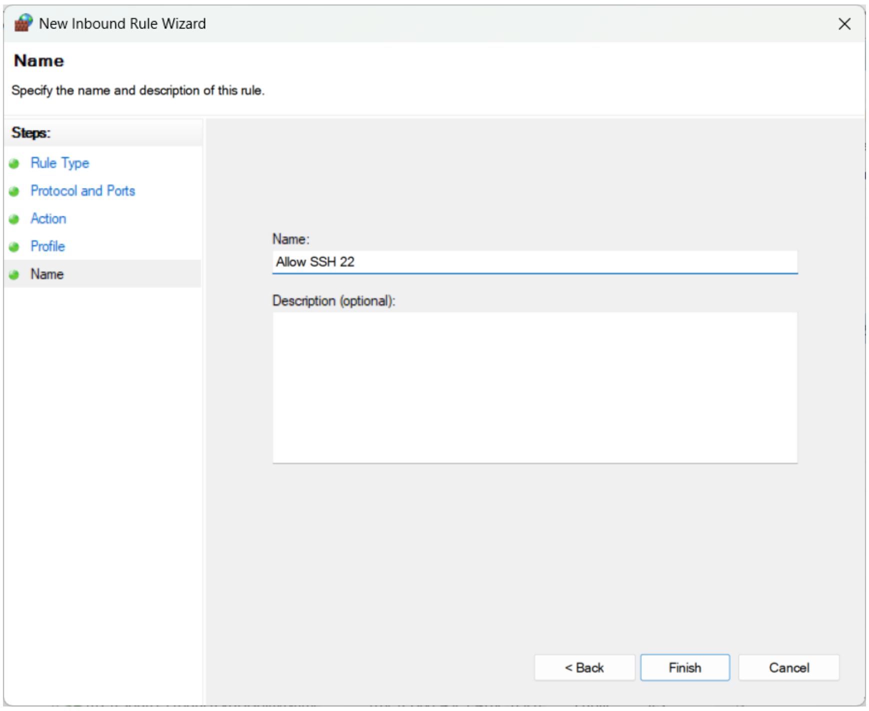
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

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

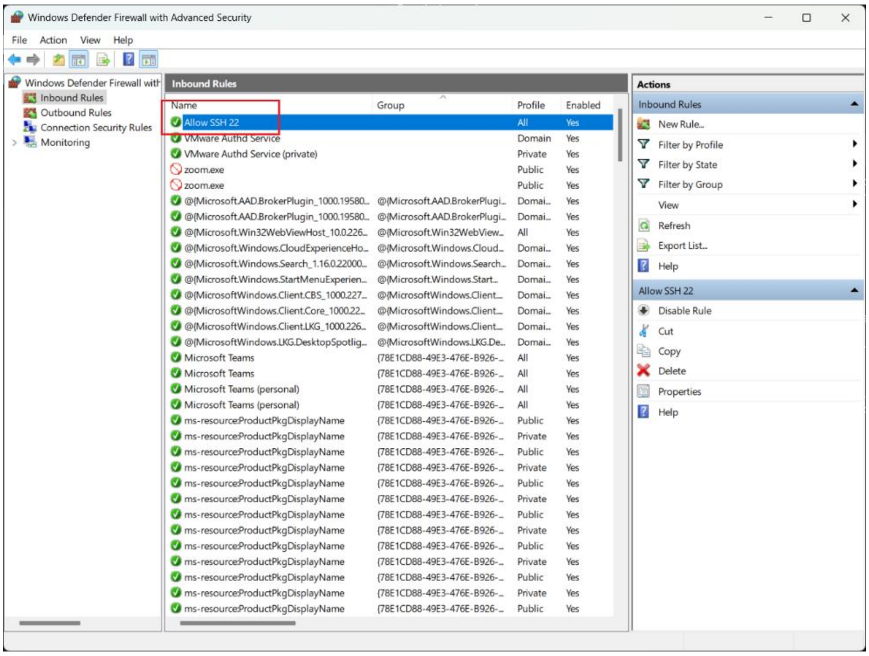
Name

Specify the name and description of this rule.

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

Name: Allow SSH 22

Description (optional):



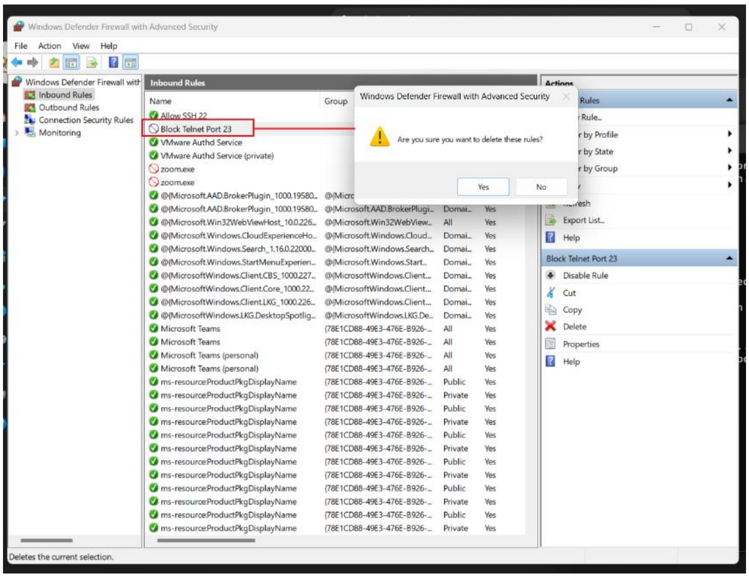
Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled
Allow SSH 22		All	Yes
VMware Authd Service		Domain	Yes
VMware Authd Service (private)		Private	Yes
zoom.exe		Public	Yes
zoom.exe		Public	Yes
@{Microsoft.AAD.BrokerPlugin_1000.19580...	@{Microsoft.AAD.BrokerPlugi...	Domai...	Yes
@{Microsoft.AAD.BrokerPlugin_1000.19580...	@{Microsoft.AAD.BrokerPlugi...	Domai...	Yes
@{Microsoft.Win32WebViewHost_10.0.226...	@{Microsoft.Win32WebView...	All	Yes
@{Microsoft.Windows.CloudExperienceHo...	@{Microsoft.Windows.Cloud...	Domai...	Yes
@{Microsoft.Windows.Search_1.16.0.22000...	@{Microsoft.Windows.Search...	Domai...	Yes
@{Microsoft.Windows.StartMenuExperien...	@{Microsoft.Windows.Start...	Domai...	Yes
@{MicrosoftWindows.Client.CBS_1000.227...	@{MicrosoftWindows.Client...	Domai...	Yes
@{MicrosoftWindows.Client.Core_1000.22...	@{MicrosoftWindows.Client...	Domai...	Yes
@{MicrosoftWindows.Client.LKG_1000.226...	@{MicrosoftWindows.Client...	Domai...	Yes
@{MicrosoftWindows.LKG.DesktopSpotlig...	@{MicrosoftWindows.LKG.De...	Domai...	Yes
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes

6. Remove the Test Rule

- Go to Inbound Rules
- Find Block Telnet Port 23, right-click > Delete



Windows Defender Firewall with Advanced Security

Are you sure you want to delete these rules?

Name	Group		
Allow SSH 22			
Block Telnet Port 23			
VMware Authd Service			
VMware Authd Service (private)			
zoom.exe			
zoom.exe			
@{Microsoft.AAD.BrokerPlugin_1000.19580...	@{Micro		
@{Microsoft.AAD.BrokerPlugin_1000.19580...	@{Microsoft.AAD.BrokerPlugi...	Domai...	Yes
@{Microsoft.Win32WebViewHost_10.0.226...	@{Microsoft.Win32WebView...	All	Yes
@{Microsoft.Windows.CloudExperienceHo...	@{Microsoft.Windows.Cloud...	Domai...	Yes
@{Microsoft.Windows.Search_1.16.0.22000...	@{Microsoft.Windows.Search...	Domai...	Yes
@{Microsoft.Windows.StartMenuExperien...	@{Microsoft.Windows.Start...	Domai...	Yes
@{MicrosoftWindows.Client.CBS_1000.227...	@{MicrosoftWindows.Client...	Domai...	Yes
@{MicrosoftWindows.Client.Core_1000.22...	@{MicrosoftWindows.Client...	Domai...	Yes
@{MicrosoftWindows.Client.LKG_1000.226...	@{MicrosoftWindows.Client...	Domai...	Yes
@{MicrosoftWindows.LKG.DesktopSpotlig...	@{MicrosoftWindows.LKG.De...	Domai...	Yes
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes

Deletes the current selection.

Summary: How Firewall Filters Traffic

Firewall in Linux

Firewalls monitor and control incoming and outgoing network traffic based on predefined rules. They:

- Allow or deny packets based on IP address, port, or protocol.
- Protect systems from unauthorized access.
- Act as a barrier between trusted and untrusted networks.

Firewall in Windows

Windows Firewall filters traffic using rules based on:

- Port numbers
- Application names
- Network profiles

It ensures that only authorized traffic can reach or leave your device, improving security.

THANK YOU

END