

A dark blue vertical bar runs down the left side of the page. A blue arrow points to the right from this bar, containing the date.

8/8/2025

Configure Firewall and Test Rules

(LINUX, WINDOWS)

Several thin, curved lines in dark blue and light grey originate from the bottom left and sweep upwards and to the right.

Sejal Rathwa

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.

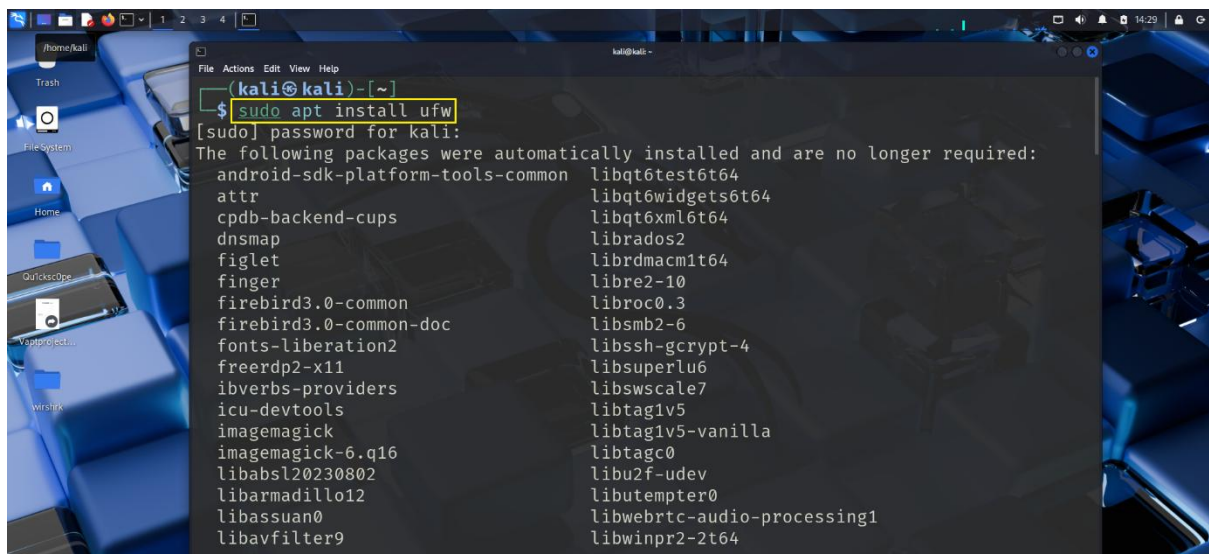
Here's a step-by-step guide to configure and test firewall rules on both Windows and Linux (UFW), depending on your system. Choose the section that matches your OS.

FOR LINUX (UFW - Uncomplicated Firewall)

Make sure UFW is installed and enabled:

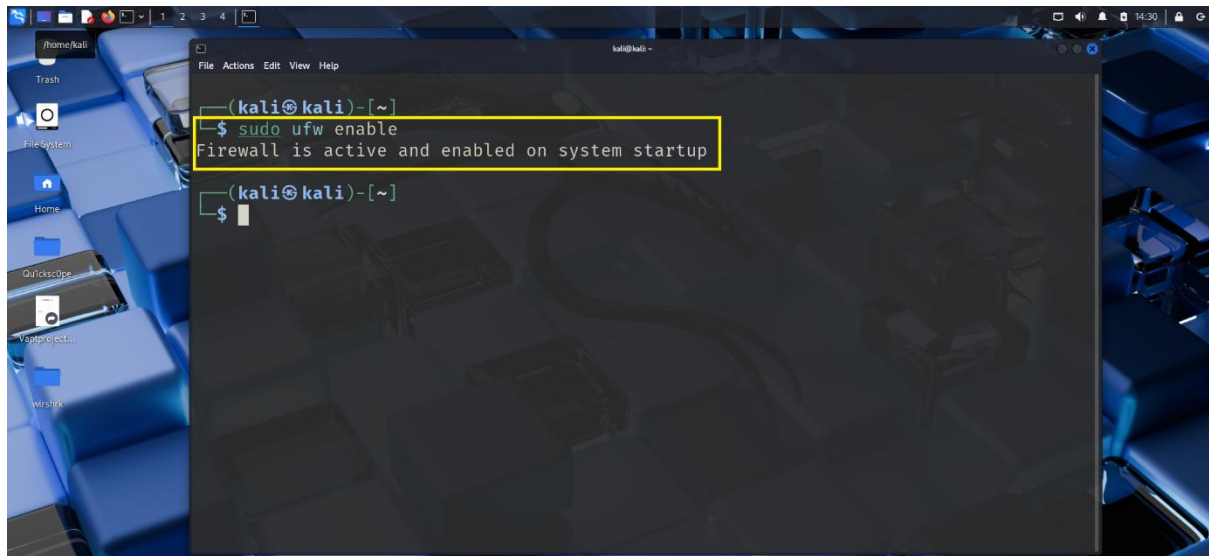
Run cmd

`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`



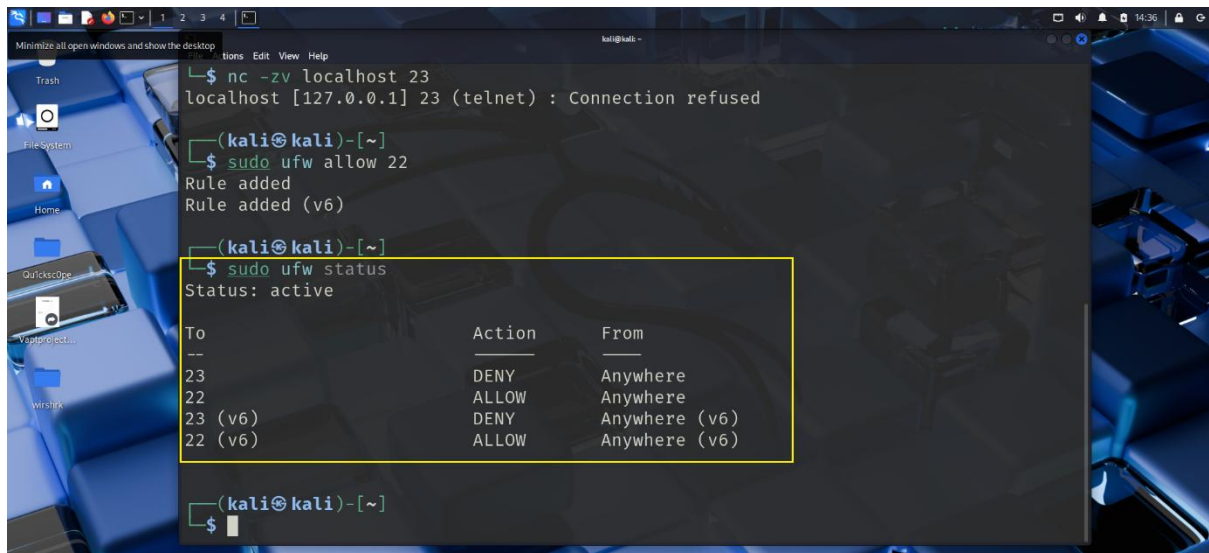
1. Open Firewall Configuration Tool

UFW is used via the terminal. No GUI needed.

2. List Current Firewall Rules

Run cmd

sudo ufw status numbered



A terminal window on a Kali Linux desktop. The user runs `nc -zv localhost 23`, which returns "localhost [127.0.0.1] 23 (telnet) : Connection refused". Then, they run `sudo ufw allow 22`, which outputs "Rule added" and "Rule added (v6)". Next, they run `sudo ufw status`, which outputs "Status: active". Finally, they run `sudo ufw status numbered`, which displays a table of rules. The table has three columns: "To", "Action", and "From". The rules are: 23 (DENY, Anywhere), 22 (ALLOW, Anywhere), 23 (v6) (DENY, Anywhere (v6)), and 22 (v6) (ALLOW, Anywhere (v6)).

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

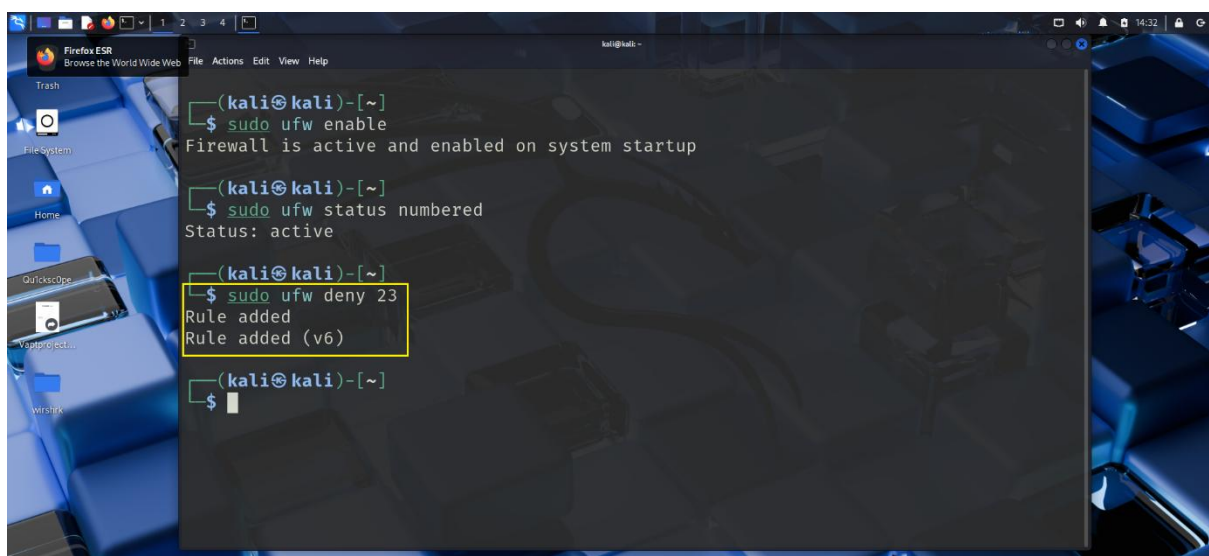
To           Action      From
--           -
23           DENY       Anywhere
22           ALLOW      Anywhere
23 (v6)     DENY       Anywhere (v6)
22 (v6)     ALLOW      Anywhere (v6)

(kali㉿kali)-[~]
└─$
```

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

Run cmd

sudo ufw deny 23



A terminal window on a Kali Linux desktop. The user runs `sudo ufw enable`, which outputs "Firewall is active and enabled on system startup". Then, they run `sudo ufw status numbered`, which outputs "Status: active". Next, they run `sudo ufw deny 23`, which outputs "Rule added" and "Rule added (v6)".

```
(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

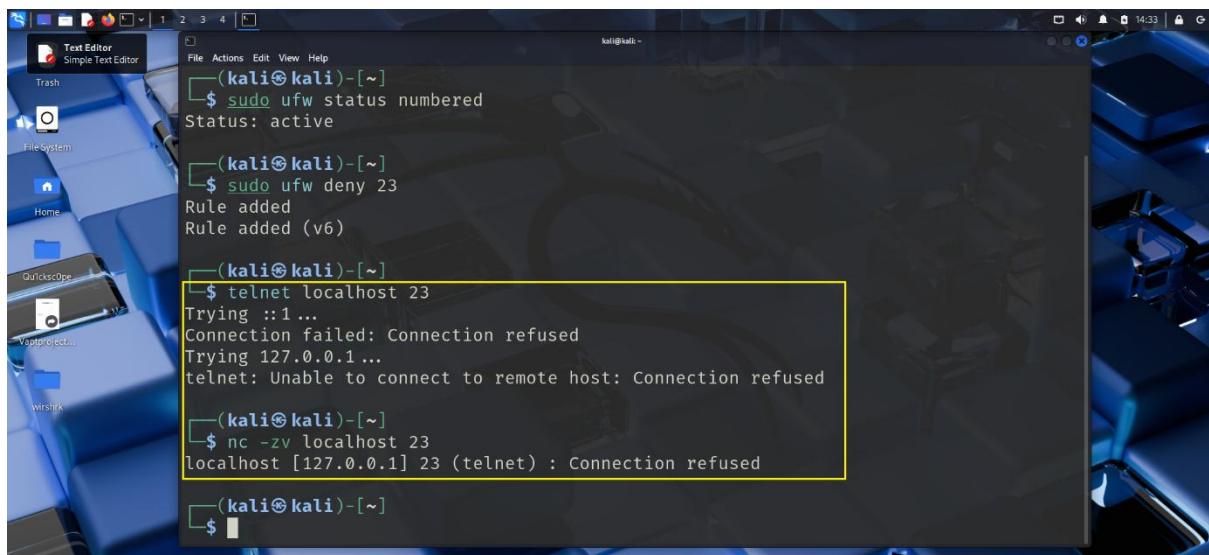
telnet localhost 23

Or use nc (netcat):

Run cmd

nc -zv localhost 23

Can see a connection refused or timeout.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

```
(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)-[~]
$
```

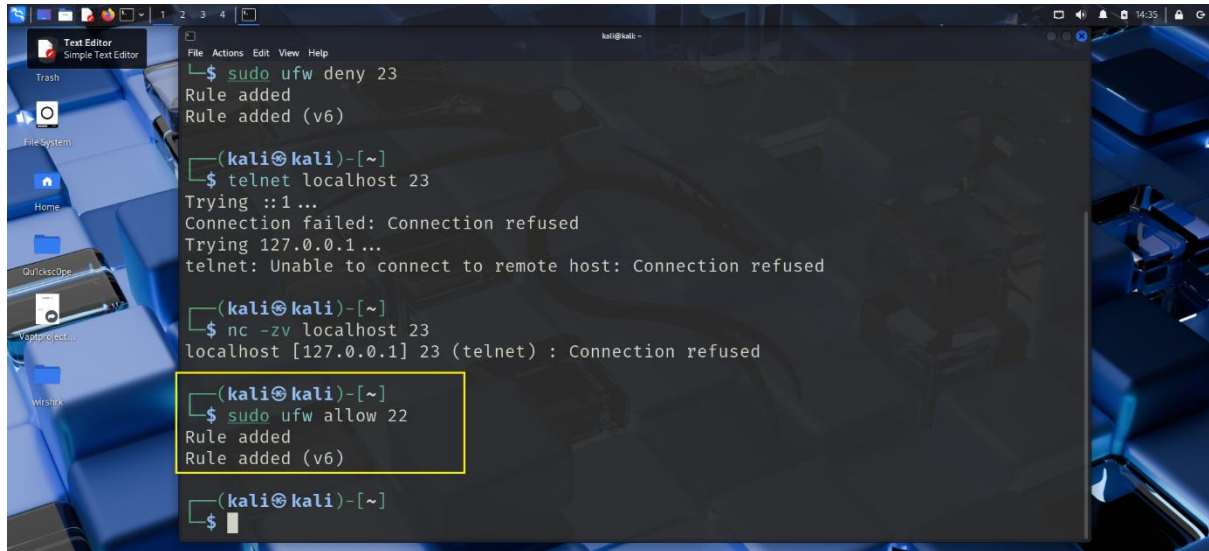
The terminal window is titled "kali@kali: ~" and has a menu bar with "File", "Actions", "Edit", "View", and "Help". The desktop background is a blue and black abstract image. On the left side, there is a sidebar with icons for "Trash", "File System", "Home", "Outlook", "VaporProject...", and "Wirstark".

5. Add Rule to Allow SSH (Port 22)

Run cmd

```
sudo ufw allow 22
```

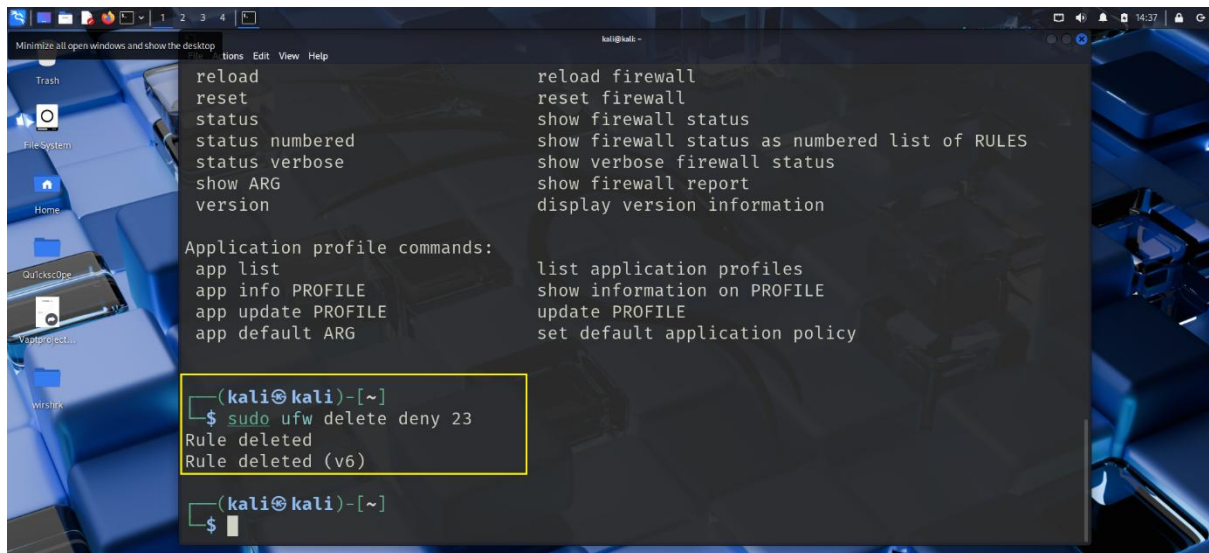
This is important if you're using SSH to manage the system remotely.



6. Remove the Block Rule (Restore Original State)

Run cmd

`sudo ufw delete deny 23`



A terminal window on a Kali Linux desktop. The terminal shows a list of UFW commands and their descriptions. Below this, application profile commands are listed. The main part of the terminal shows the execution of `sudo ufw delete deny 23`, which results in "Rule deleted" and "Rule deleted (v6)".

```
reload
reset
status
status numbered
status verbose
show ARG
version

Application profile commands:
app list
app info PROFILE
app update PROFILE
app default ARG

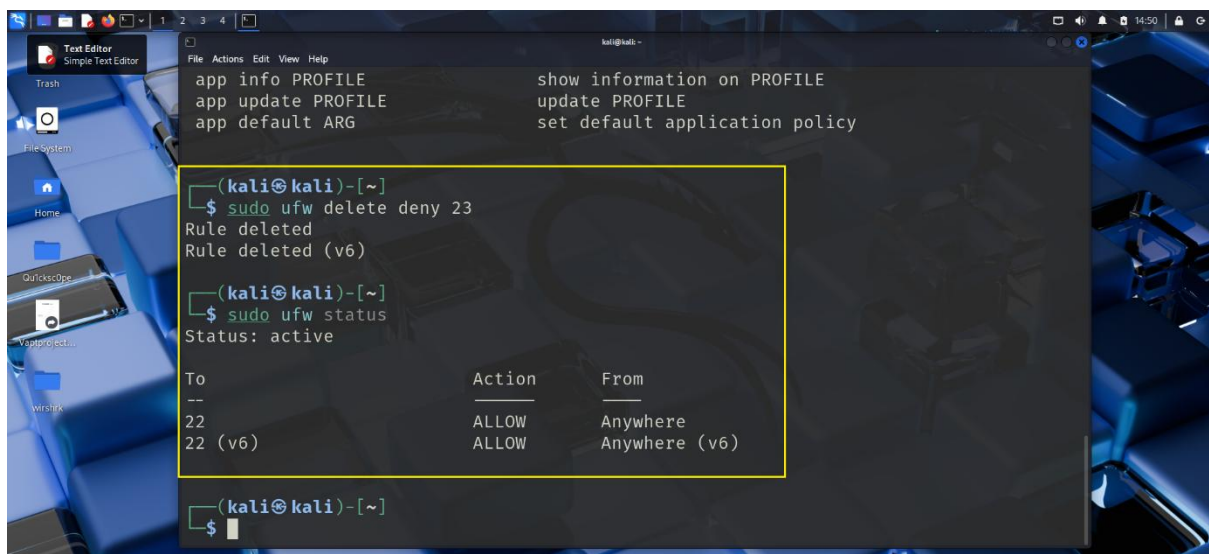
reload firewall
reset firewall
show firewall status
show firewall status as numbered list of RULES
show verbose firewall status
show firewall report
display version information

list application profiles
show information on PROFILE
update PROFILE
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.



A terminal window on a Kali Linux desktop. The terminal shows the execution of `sudo ufw delete deny 23`, which results in "Rule deleted" and "Rule deleted (v6)". Below this, the command `sudo ufw status` is executed, showing the status as "active". A table of rules is displayed, showing rule 22 (v6) with an "ALLOW" action and "Anywhere (v6)" as the source.

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

(kali@kali)-[~]
$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)

(kali@kali)-[~]
$ sudo ufw status
Status: active

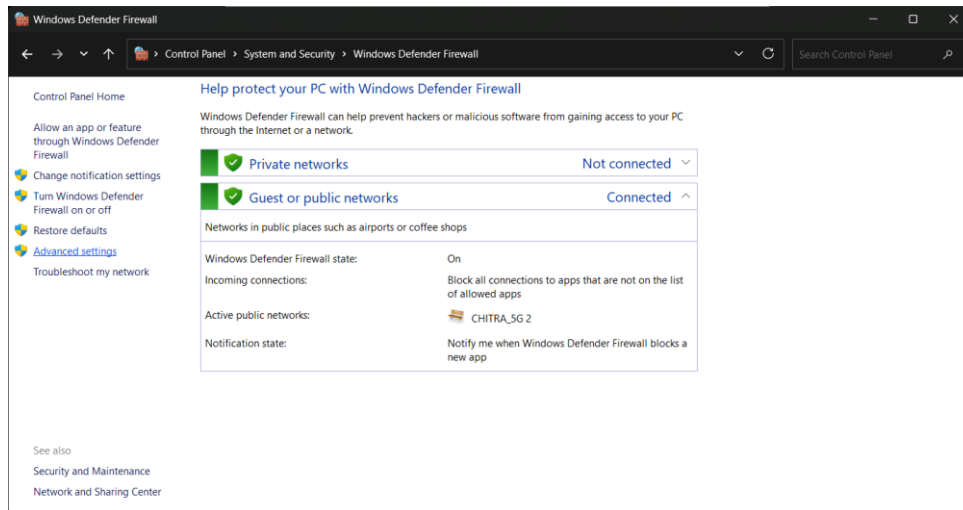
To Action From
--
22 ALLOW Anywhere
22 (v6) ALLOW Anywhere (v6)

(kali@kali)-[~]
$
```

FOR WINDOWS (Windows Defender Firewall)

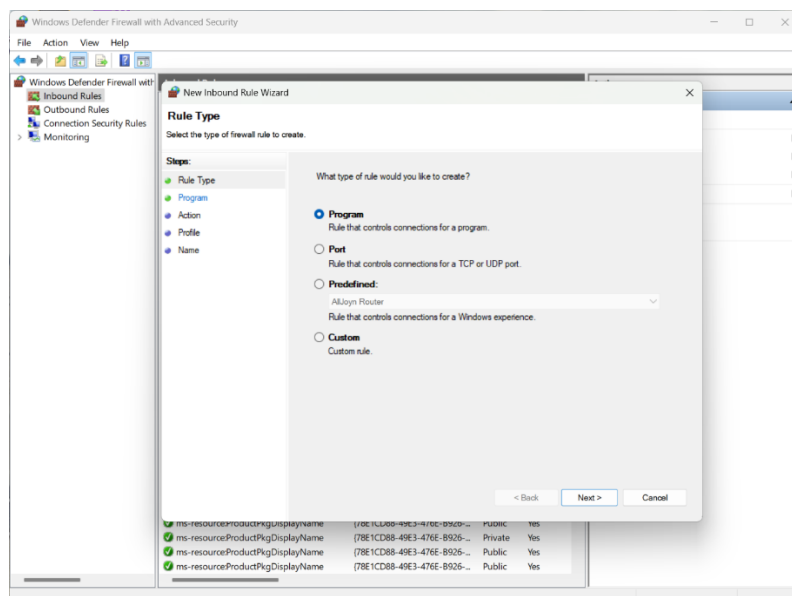
1. Open Firewall Configuration Tool

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



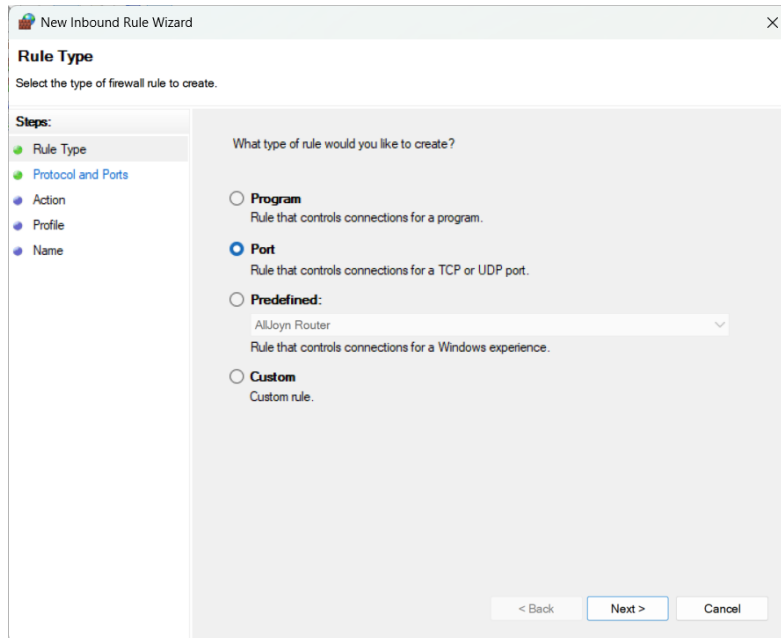
2. List Current Firewall Rules

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



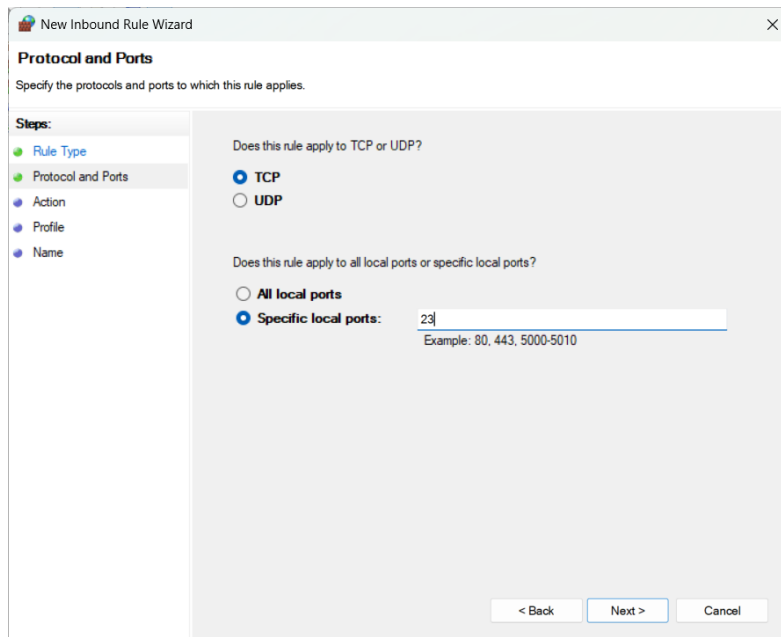
3. Block Inbound Traffic on Port 23

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



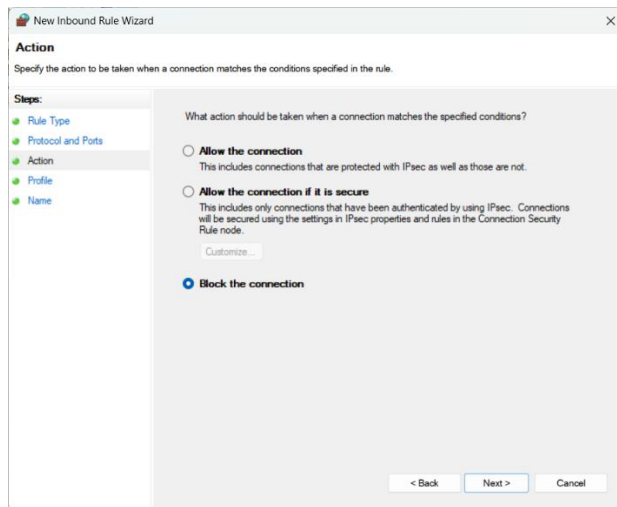
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Rule Type' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'What type of rule would you like to create?' and offers four options: 'Program' (Rule that controls connections for a program.), 'Port' (selected, Rule that controls connections for a TCP or UDP port.), 'Predefined:' (with a dropdown menu showing 'AllJoyn Router' and the description 'Rule that controls connections for a Windows experience.'), and 'Custom' (Custom rule.). At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

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



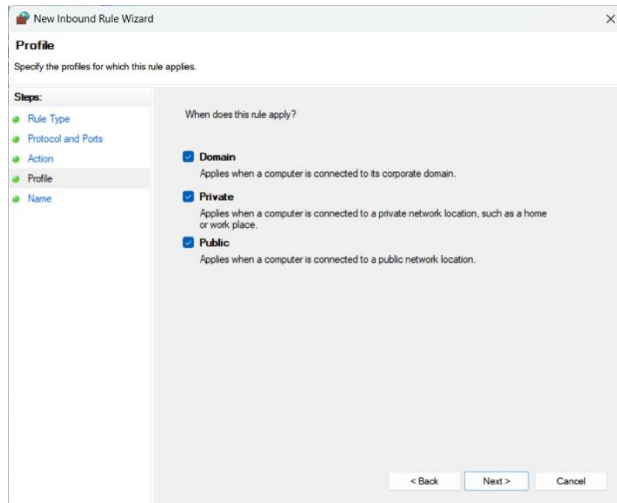
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, the 'Steps' pane shows 'Rule Type' and 'Protocol and Ports' as completed steps, followed by 'Action', 'Profile', and 'Name'. The main area asks 'Does this rule apply to TCP or UDP?' with 'TCP' selected. Below, it asks 'Does this rule apply to all local ports or specific local ports?' with 'Specific local ports:' selected. A text box contains '23' with an example 'Example: 80, 443, 5000-5010' below it. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

- Action: **Block the connection**



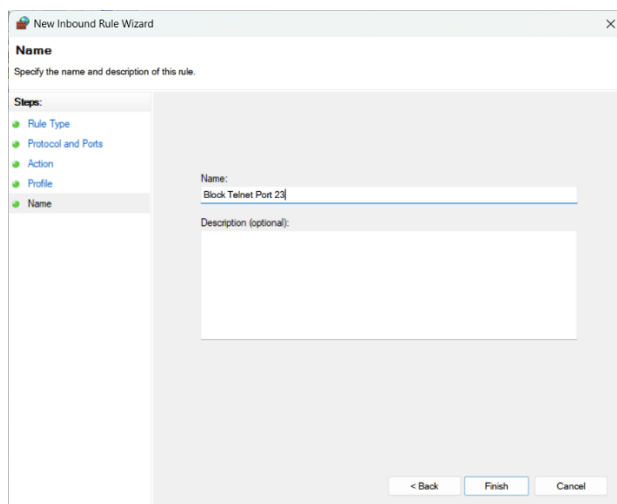
The 'New Inbound Rule Wizard' window is shown at the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (unselected), 'Allow the connection if it is secure' (unselected), and 'Block the connection' (selected). Below the 'Allow the connection if it is secure' option is a 'Customize...' link. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

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



The 'New Inbound Rule Wizard' window is shown at the 'Profile' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area asks 'When does this rule apply?'. There are three checked checkboxes: '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.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

- Name it: Block Telnet Port 23



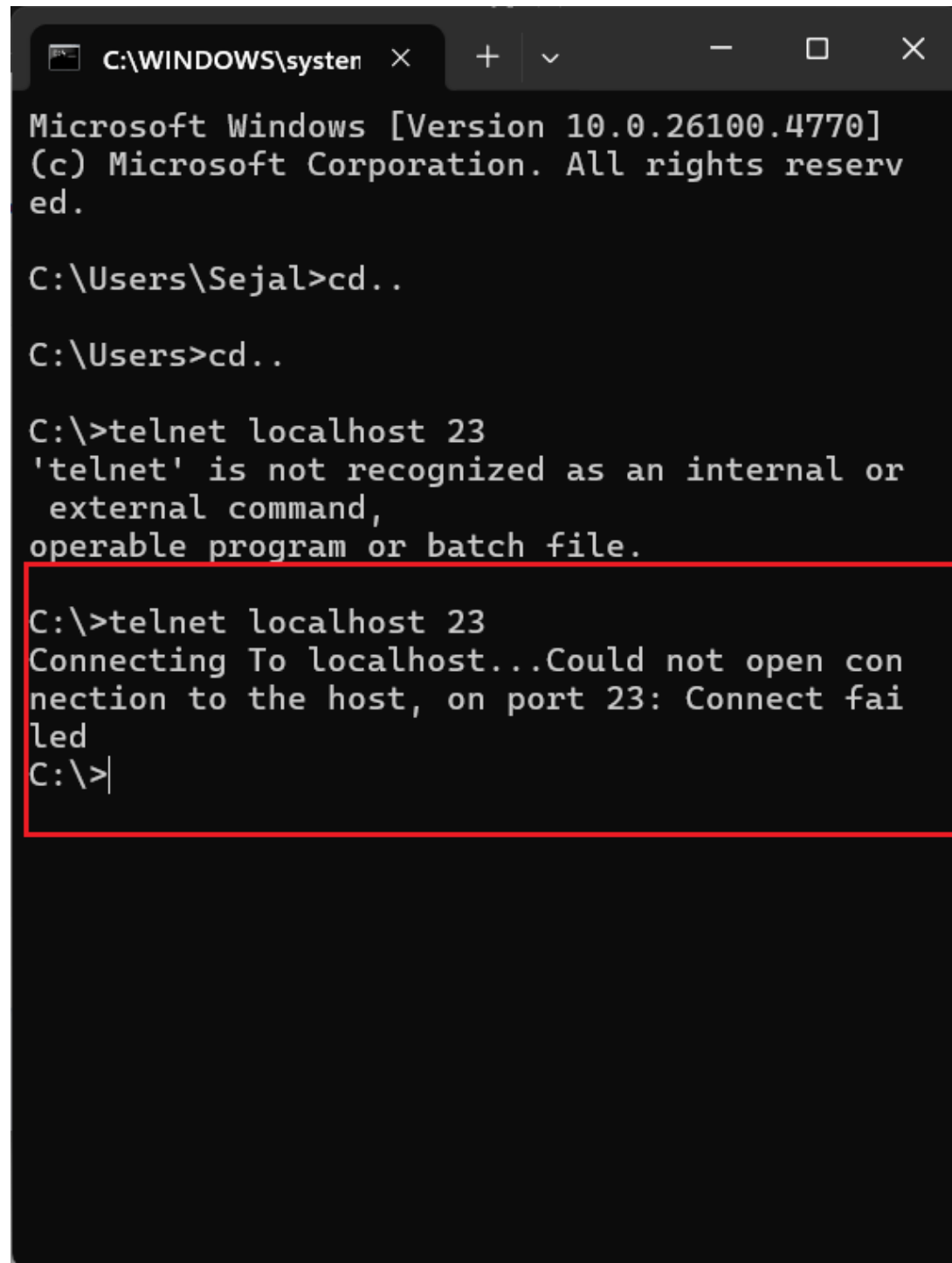
The 'New Inbound Rule Wizard' window is shown at the 'Name' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area asks 'Specify the name and description of this rule.'. There is a 'Name:' label followed by a text box containing 'Block Telnet Port 23'. Below it is a 'Description (optional):' label followed by a larger text box. At the bottom are '< Back', 'Finish', and 'Cancel' buttons.

4. Test the Rule

Use Telnet client:

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

telnet localhost 23

A screenshot of a Windows Command Prompt window. The title bar shows the path 'C:\WINDOWS\system' and standard window controls. The command history shows the user navigating from 'C:\Users\Sejal' to 'C:\Users' and then to 'C:\'. The first attempt to run 'telnet localhost 23' results in an error: "'telnet' is not recognized as an internal or external command, operable program or batch file." The second attempt, which is highlighted with a red rectangular box, shows the command being entered, followed by the output: 'Connecting To localhost...Could not open connection to the host, on port 23: Connect failed', and then the prompt returns to 'C:\>|'.

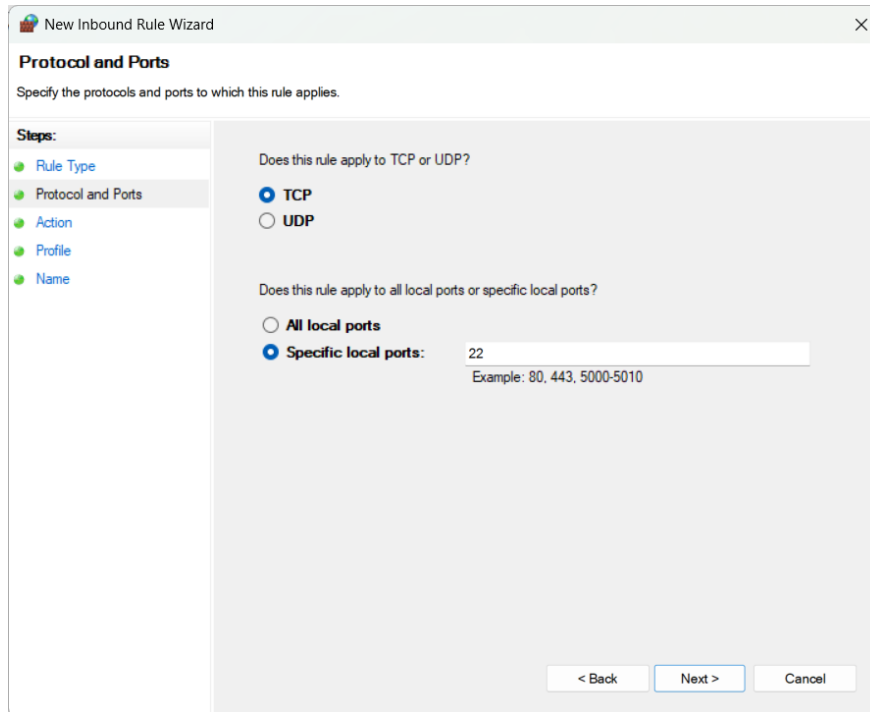
```
C:\WINDOWS\system > cd ..
C:\Users\Sejal> cd ..
C:\Users> cd ..
C:\> telnet localhost 23
'telnet' is not recognized as an internal or
external command,
operable program or batch file.
C:\> telnet localhost 23
Connecting To localhost...Could not open con
nection to the host, on port 23: Connect fai
led
C:\>|
```

Get a failure to connect.

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

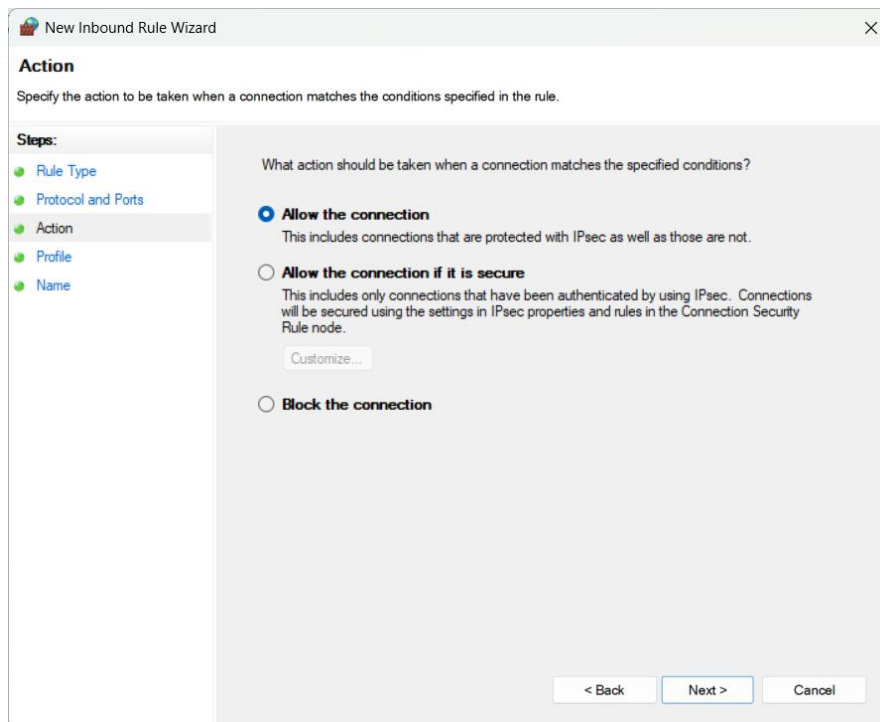
Not typically used unless you're running OpenSSH server. If so:

- Go to Inbound Rules > New Rule...



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window title is 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' pane lists 'Rule Type', 'Protocol and Ports' (selected), 'Action', 'Profile', and 'Name'. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports:' (selected). The 'Specific local ports:' field contains the value '22' and an example 'Example: 80, 443, 5000-5010'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

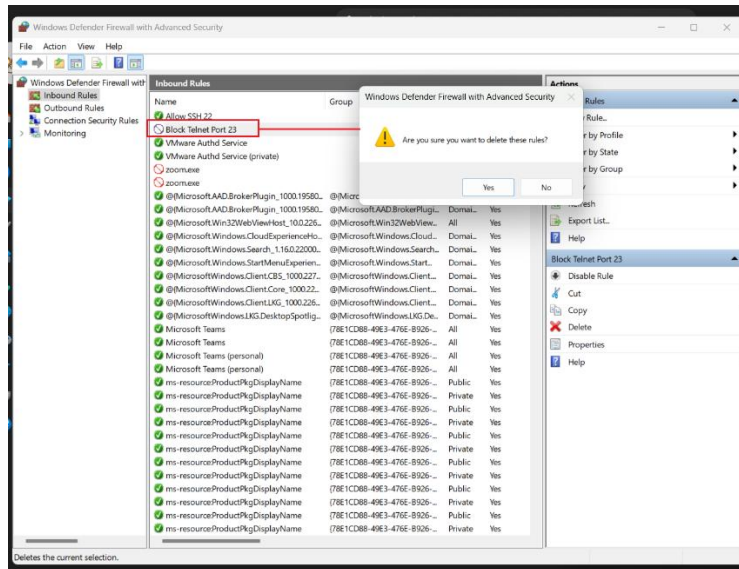
- Port: 22 > Allow the connection



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The window title is 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps' pane lists 'Rule Type', 'Protocol and Ports', 'Action' (selected), 'Profile', and 'Name'. The main area contains the question 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those that are not.' The 'Allow the connection if it is secure' option has a description: '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.' and a 'Customize...' button. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

6. Remove the Test Rule

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



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