

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

 For Windows (Using Windows Defender Firewall)

1. Open Firewall Configuration Tool

Press Win + R, type wf.msc, and press Enter.

2. List Current Firewall Rules

In the left panel, click on:

Inbound Rules to see all rules allowing/blocking inbound traffic.

Outbound Rules to see outbound traffic rules.

3. Add Rule to Block Inbound Traffic on Port 23

Go to Inbound Rules > New Rule...

Choose Port > Click Next

Select TCP > Enter 23 in Specific local ports

Click Next > Select Block the connection

Click Next > Choose profiles (Domain, Private, Public)

Name it: Block Telnet Port 23 > Finish

4. Test the Rule

Open Command Prompt:

```
nginx
```

```
telnet localhost 23
```

If telnet is installed and running, the connection should fail due to the block.

5. Allow SSH (Port 22) – (Optional for Windows unless SSH server is running)

If needed, repeat step 3 but Allow the connection on port 22.

6. Remove the Test Rule

Go back to Inbound Rules

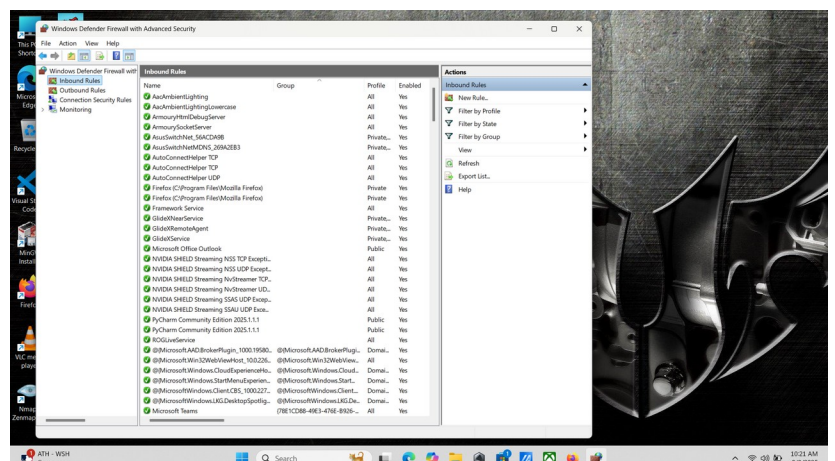
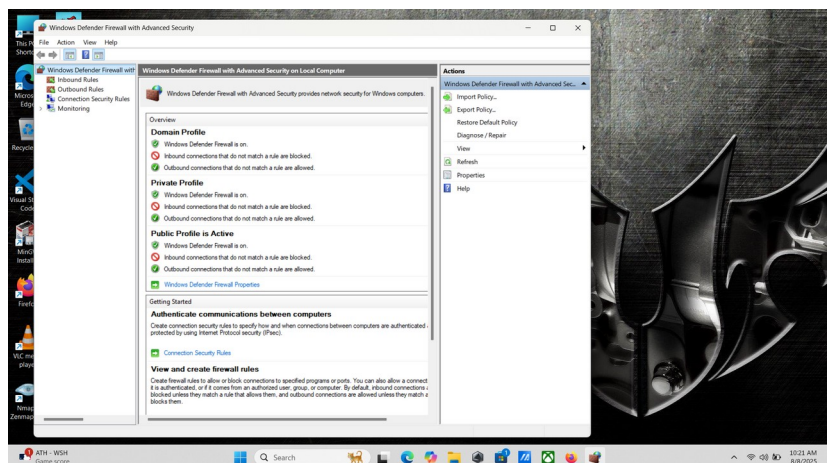
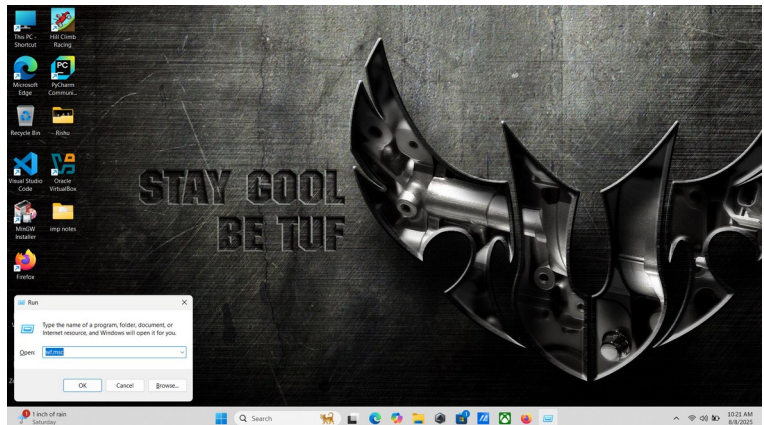
Find Block Telnet Port 23

Right-click > Delete

7. Documentation of GUI Steps Used

Open wf.msc

Inbound Rules → New Rule → Port → TCP port 23 → Block



To remove: Right-click rule → Delete

8. Firewall Summary (Windows)

The Windows Firewall filters inbound and outbound traffic based on rules.

It uses port, protocol, application, or IP address as rule criteria.

Default policy: block unsolicited inbound, allow outbound unless specified.

🔗 For Linux (Using UFW - Uncomplicated Firewall)

1. Open Terminal (UFW Tool)

bash

sudo ufw status verbose

2. List Current Rules

bash

sudo ufw status numbered

3. Add Rule to Block Inbound Traffic on Port 23

bash

sudo ufw deny 23

4. Test the Rule

Try to connect locally:

bash

telnet localhost 23

You should see a connection refused or timeout.

5. Add Rule to Allow SSH (Port 22)

bash

sudo ufw allow 22

6. Remove the Test Block Rule

bash

sudo ufw delete deny 23

7. Documentation of Commands Used

bash

Show firewall status

sudo ufw status numbered

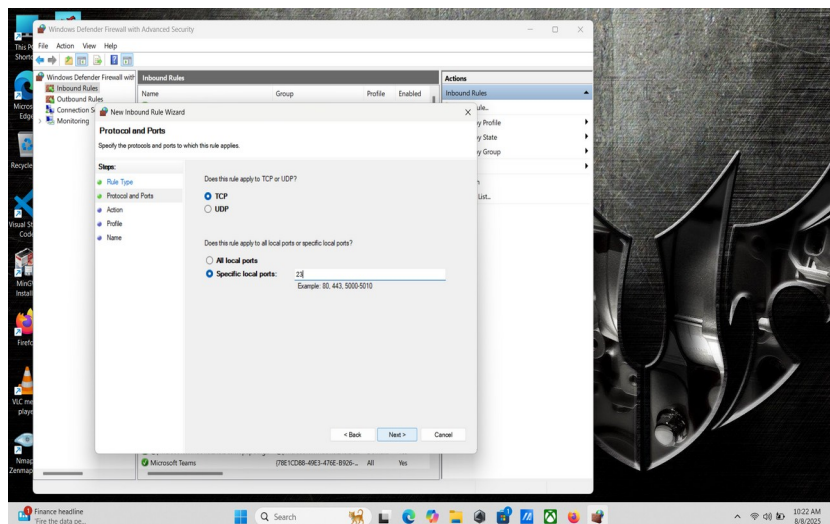
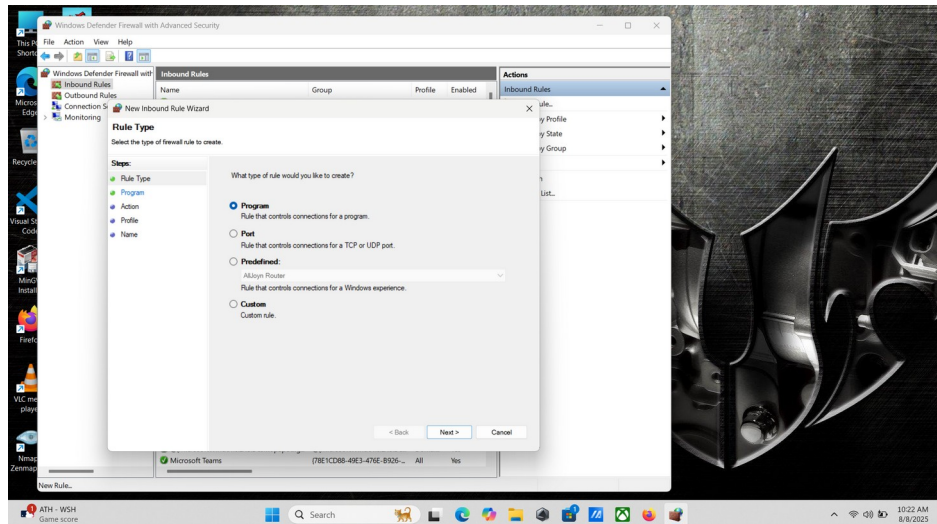
Block port 23 (Telnet)

sudo ufw deny 23

Allow port 22 (SSH)

sudo ufw allow 22

Delete block rule for port 23



```
sudo ufw delete deny 23
```

8. Firewall Summary (UFW/Linux)

UFW is a simplified front-end for iptables.

It filters traffic based on direction (in/out), protocol, port, or IP.

Default policy: deny incoming, allow outgoing unless rules override.

Let me know if you want a script for Linux or Windows PowerShell to automate this!

When, I'm running telnet localhost 23 command on windows terminal it's showing: The term telnet is not recognized as the name of a cmdlet, function, script file, or operable program

That error means the Telnet client is not installed on your Windows system. It's not enabled by default in modern versions of Windows.

✓ Here's how to enable Telnet on Windows:

✚ Option 1: Using Command Prompt (Admin)

Open Command Prompt as Administrator

(Right-click Start > "Command Prompt (Admin)" or "Windows Terminal (Admin)")

Run the following command:

```
cmd
```

```
dism /online /Enable-Feature /FeatureName:TelnetClient
```

Wait for the installation to complete (it takes a few seconds).

Now you can run:

```
cmd
```

```
telnet localhost 23
```

✚ Option 2: Using GUI (Control Panel)

Open Control Panel

Go to Programs > Programs and Features

Click Turn Windows features on or off (on the left pane)

Scroll down and check Telnet Client

Click OK to install it

Then Test Again:

After installation, open a new terminal and run:

```
cmd
```

telnet localhost 23

If port 23 is open, it will try to connect.

If port 23 is blocked or not listening, it will fail (which is the expected result if your firewall block rule is working).

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ps407> telnet localhost 23
telnet : The term 'telnet' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ telnet localhost 23
~
+ CategoryInfo          : ObjectNotFound: (telnet:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\ps407> dism /online /Enable-Feature /FeatureName:TelnetClient

Deployment Image Servicing and Management tool
Version: 10.0.26100.1150

Image Version: 10.0.26100.4652

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
PS C:\Users\ps407> telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed
PS C:\Users\ps407> telnet localhost telnet 23

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]
-a      Attempt automatic logon. Same as -l option except uses
        the currently logged on user's name.
-e      Escape character to enter telnet client prompt.
-f      File name for client side logging
-l      Specifies the user name to log in with on the remote system.
        Requires that the remote system support the TELNET ENVIRON option.
-t      Specifies terminal type.
        Supported term types are vt100, vt52, ansi and vtnt only.
host    Specifies the hostname or IP address of the remote computer
        to connect to.
port    Specifies a port number or service name.
PS C:\Users\ps407>
```