

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

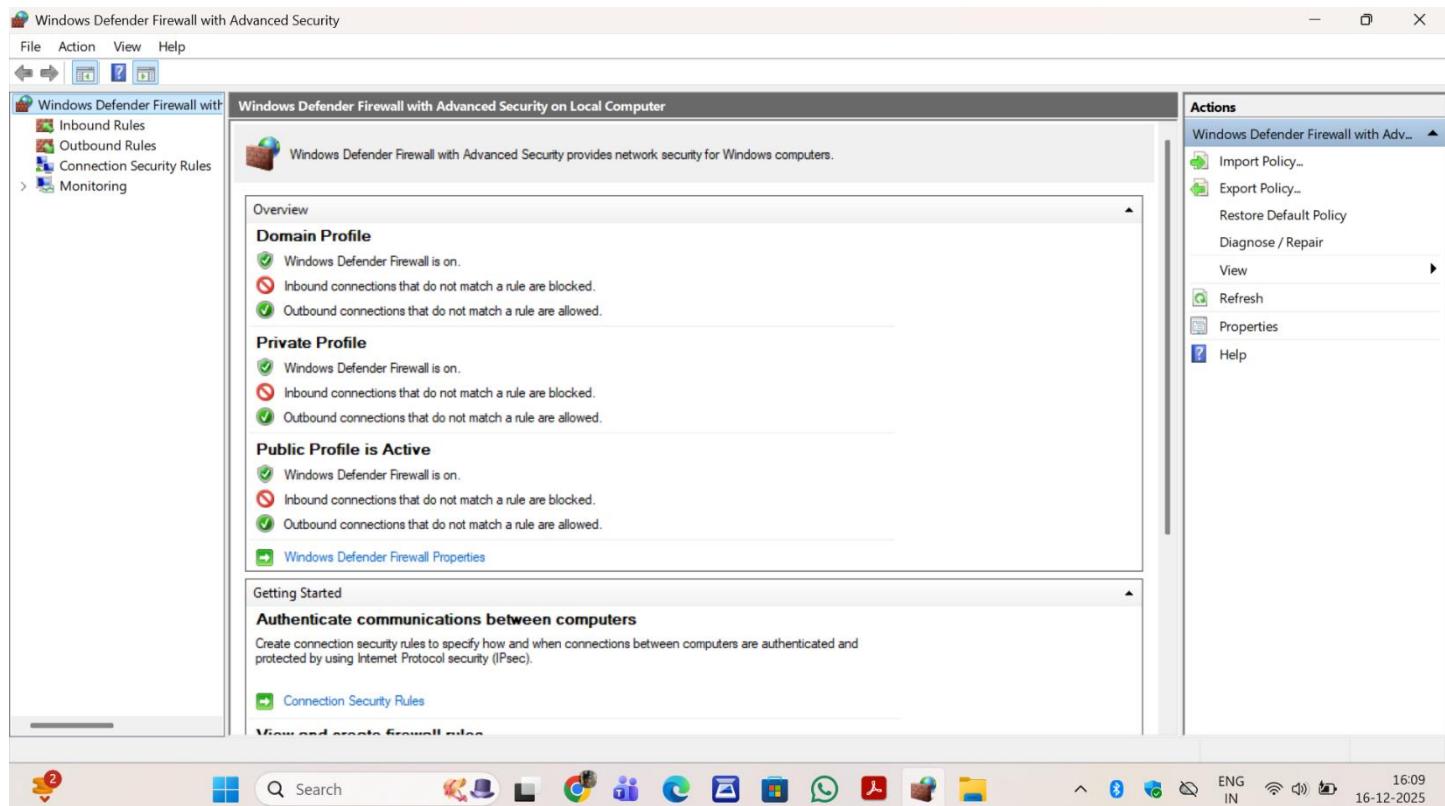
**Tools:** Windows Firewall

**Deliverables:** Screenshot/configuration file showing firewall rules applied.

- a. Open firewall configuration tool (Windows Firewall or terminal for UFW).

### Open Firewall Tool

- Press **Win + R**
- Type **wf.msc** → **Enter**



- b. List current firewall rules.

### List Current Rules

- Click Inbound Rules
- Existing rules are displayed

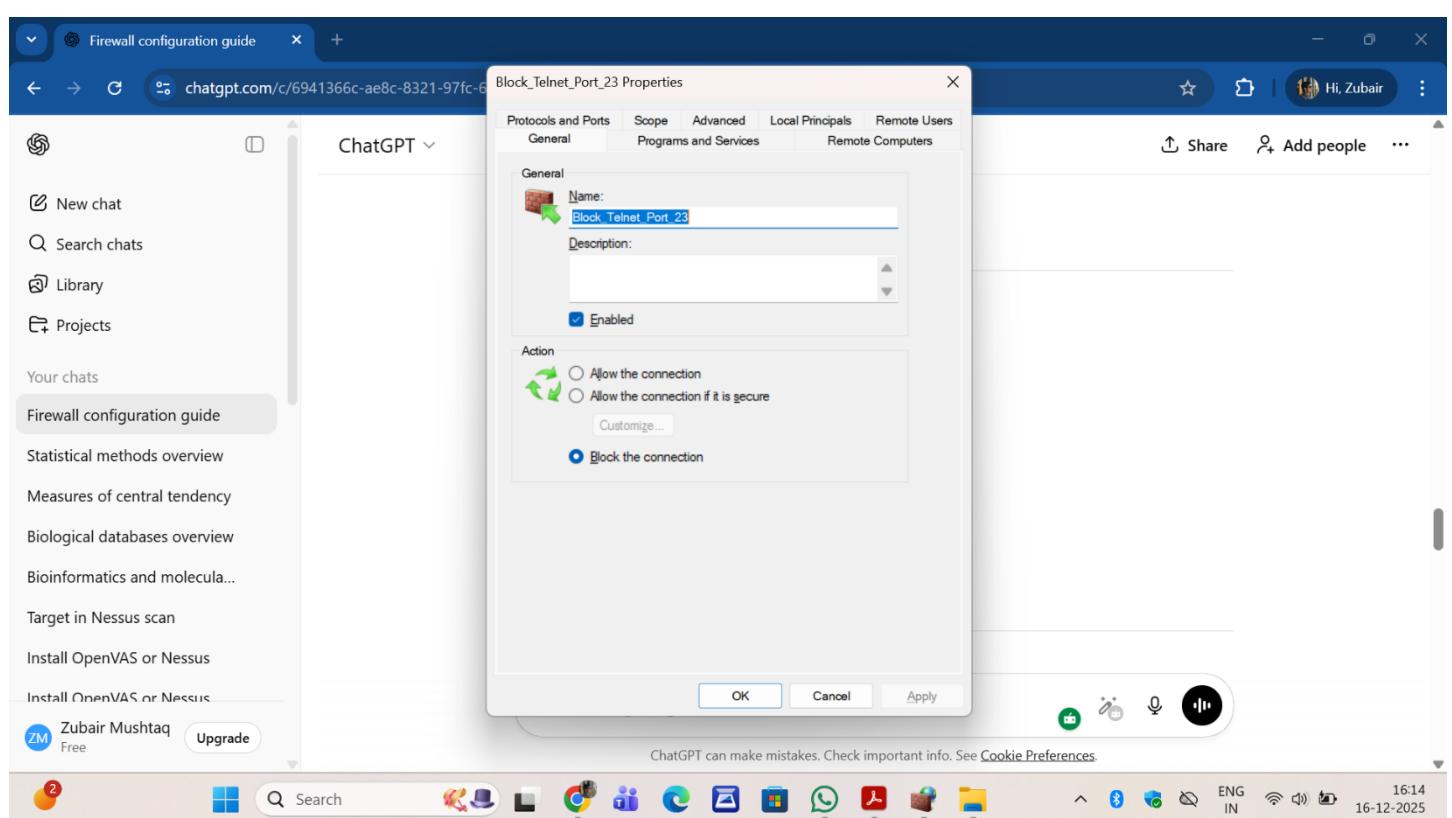
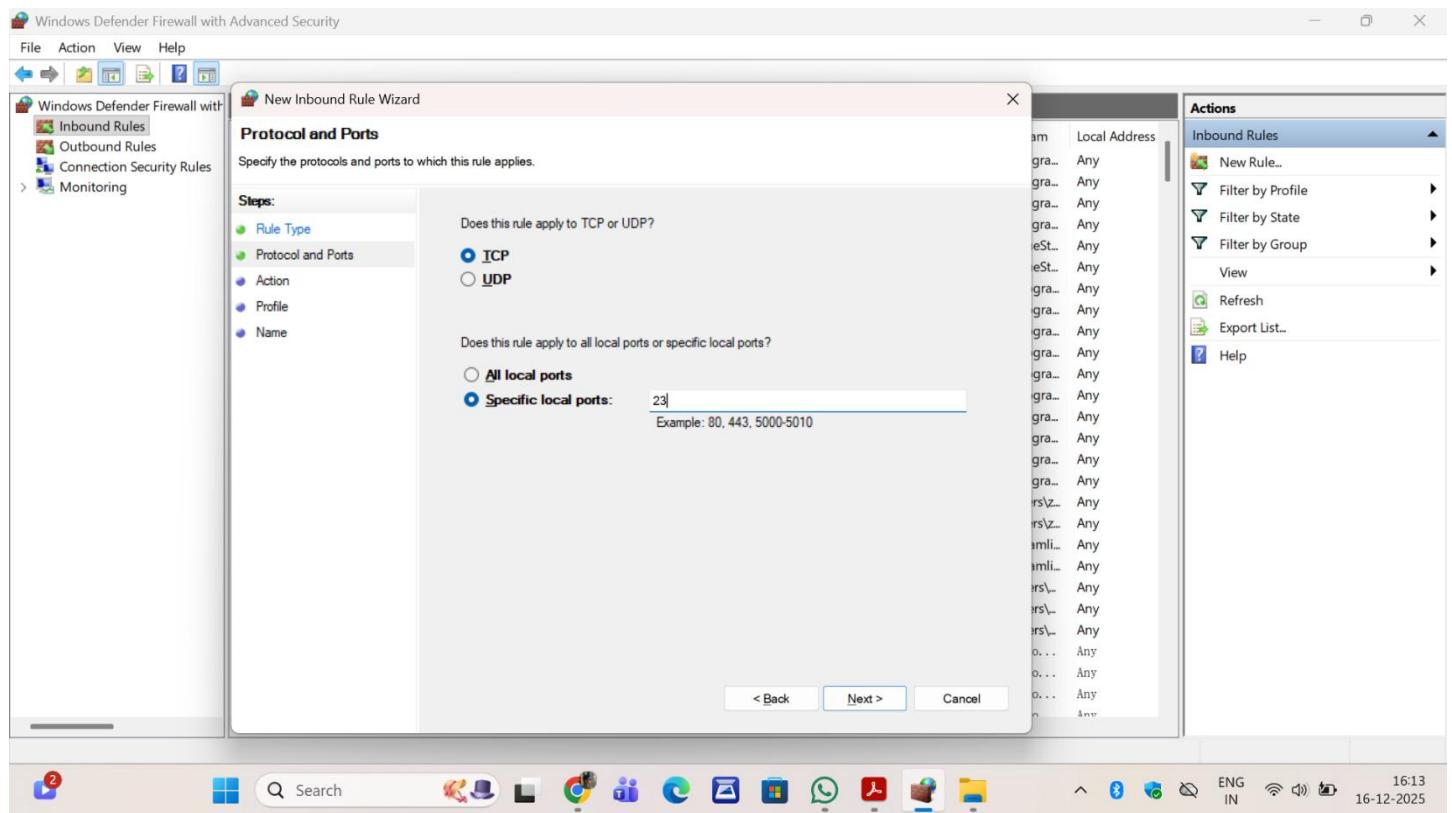
Screenshot of Windows Defender Firewall with Advanced Security showing the Inbound Rules list. The list contains numerous rules, many of which are for Steam and BlueStacks services. The Actions pane on the right shows options like 'New Rule...', 'Filter by Profile', and 'View'.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
360TSLiveUpd.exe		Public	Yes	Allow	No	C:\Progra...	Any
360TSLiveUpd.exe		Public	Yes	Allow	No	C:\Progra...	Any
BlueStacks Service		All	Yes	Allow	No	C:\Progra...	Any
BlueStacksAppLayerWeb		All	Yes	Allow	No	C:\Progra...	Any
BlueStacksWeb		All	Yes	Allow	No	D:\BlueSt...	Any
Cloud Game		All	Yes	Allow	No	D:\BlueSt...	Any
ivms-4200.devicemanagements		Public	Yes	Allow	No	C:\progra...	Any
ivms-4200.devicemanagements		Public	Yes	Allow	No	C:\progra...	Any
ivms-4200.video.c		Public	Yes	Allow	No	C:\progra...	Any
ivms-4200.video.c		Public	Yes	Allow	No	C:\progra...	Any
nginx		Public	Yes	Allow	No	C:\progra...	Any
nginx		All	Yes	Allow	No	C:\Progra...	Any
Steam		All	Yes	Allow	No	C:\Progra...	Any
Steam		All	Yes	Allow	No	C:\Progra...	Any
Steam Web Helper		All	Yes	Allow	No	C:\Progra...	Any
Steam Web Helper		All	Yes	Allow	No	C:\Progra...	Any
teams.exe		Public	Yes	Allow	No	C:\users\z...	Any
teams.exe		Public	Yes	Allow	No	C:\users\z...	Any
TslGame		Public	Yes	Allow	No	E:\steamli...	Any
TslGame		Public	Yes	Allow	No	E:\steamli...	Any
uTorrent Web		Public	Yes	Allow	No	C:\Users\z...	Any
uTorrent Web		Public	Yes	Allow	No	C:\Users\z...	Any
WsToastNotification		All	Yes	Secure ...	No	C:\Users\z...	Any
腾讯手游助手下载器组件		Public	Yes	Allow	No	D:\Pro... Any	
腾讯手游助手下载器组件		Private	Yes	Allow	No	D:\Pro... Any	
腾讯手游助手下载器组件		Public	Yes	Allow	No	D:\Pro... Any	
腾讯手游助手下载器组件		Domain	Yes	Allow	No	D:\Pro... Any	

c. Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).

1. **Inbound Rules → New Rule**
2. **Select Port**
3. **Select TCP → Port 23**
4. **Choose Block the connection**
5. **Apply to all profiles**
6. **Name rule: Block\_Telnet\_Port\_23**
7. **Click Finish**

Screenshot of Windows Defender Firewall with Advanced Security showing the 'New Inbound Rule Wizard' dialog. The 'Rule Type' step is selected, showing options for Program, Port, Predefined, and Custom. The 'Port' option is chosen, and the 'Protocol and Ports' section shows 'TCP' selected with port '23'. The Actions pane on the right is visible.



#### d. Test the rule by attempting to connect to that port locally or remotely.

Open Command Prompt:

```
telnet localhost 23
```

Connection should fail

```

Microsoft Windows [Version 10.0.26200.6901]
(c) Microsoft Corporation. All rights reserved.

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

C:\Users\ZubairMushtaqDar>

```

ChatGPT can make mistakes. Check important info. See [Cookie Preferences](#).

**e. Remove the test block rule to restore original state.**

1. Open Run → wf.msc
2. Click **Inbound Rules**
3. Locate the rule **Block\_Telnet\_Port\_23**
4. Right-click the rule → **Delete**
5. Confirm deletion

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
Allow SSH_22	All	Yes	Allow	No	Any	Any	
<b>Block_Telnet_Port_23</b>	All	Yes	Block	No	Any	Any	
360TSLiveUpd.exe	Yes	Allow	No	C:\Progra...	Any		
360TSLiveUpd.exe	Yes	Allow	No	C:\Progra...	Any		
BlueStacks Service	Yes	Allow	No	C:\Progra...	Any		
BlueStacksAppplayerWeb	Yes	Allow	No	C:\Progra...	Any		
BlueStacksWeb	Yes	Allow	No	D:\BlueSt...	Any		
Cloud Game	Yes	Allow	No	D:\BlueSt...	Any		
ivms-4200.devicemanagements	Yes	Allow	No	C:\progra...	Any		
ivms-4200.devicemanagements	Yes	Allow	No	C:\progra...	Any		
ivms-4200.video.c	Yes	Allow	No	C:\progra...	Any		
ivms-4200.video.c	Public	Yes	Allow	No	C:\progra...	Any	
nginx	Public	Yes	Allow	No	C:\progra...	Any	
nginx	Public	Yes	Allow	No	C:\progra...	Any	
Steam	Public	Yes	Allow	No	C:\Progra...	Any	
Steam	All	Yes	Allow	No	C:\Progra...	Any	
Steam Web Helper	All	Yes	Allow	No	C:\Progra...	Any	
Steam Web Helper	All	Yes	Allow	No	C:\Progra...	Any	
teams.exe	Public	Yes	Allow	No	C:\users\z...	Any	
teams.exe	Public	Yes	Allow	No	C:\users\z...	Any	
TslGame	Public	Yes	Allow	No	E:\steamli...	Any	
TslGame	Public	Yes	Allow	No	E:\steamli...	Any	
uTorrent Web	Public	Yes	Allow	No	C:\Users\z...	Any	
uTorrent Web	Public	Yes	Allow	No	C:\Users\z...	Any	
WsToastNotification	All	Yes	Secure ...	No	C:\Users\z...	Any	
腾讯手游助手下载器组件	Public	Yes	Allow	No	D:\Pro... Any		
腾讯手游助手下载器组件	Private	Yes	Allow	No	D:\Pro... Any		

**f. Summarize how firewall filters traffic.**

A firewall filters network traffic by applying predefined rules that allow or block data packets based on port numbers, protocols, IP addresses, and direction of traffic. This helps prevent unauthorized access while permitting legitimate communication.