Configuring and Testing Basic Firewall Rules (using Windows GUI)

1. Objective

To configure, test, and manage basic firewall rules using the Windows Defender Firewall with Advanced Security GUI, demonstrating how inbound traffic can be allowed or blocked based on specific ports.

2. Tools Used

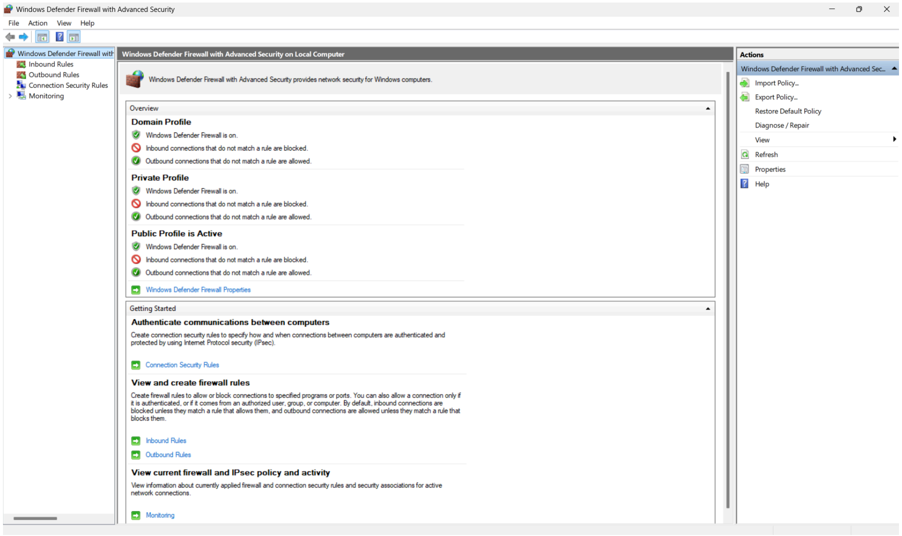
- **Operating System**: Windows 10
- **Tool**: Windows Defender Firewall with Advanced Security (GUI)
- **Ports Tested**:
  - Port 23 (Telnet) → Blocked
  - Port 22 (SSH) → Allowed

3. Activities Performed

Step 1: Open Firewall Configuration

- Opened the Run dialog (**Win + R**) → typed wf.msc → pressed Enter.
- This launched **Windows Defender Firewall with Advanced Security**.

Observation: Firewall management console opened successfully.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Advanced Sec...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

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

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for active network connections.

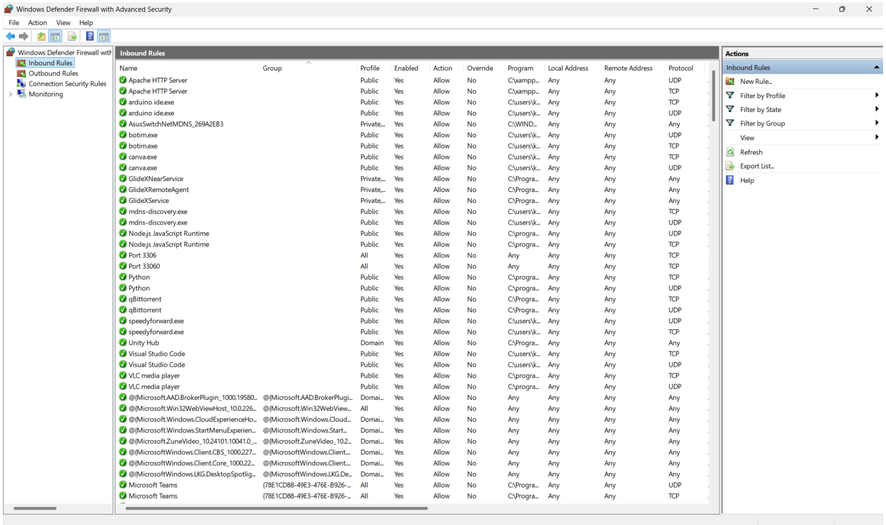
Monitoring

Step 2: Listed Current Rules

- Navigated to **Inbound Rules** in the left panel.

- Reviewed existing firewall rules controlling inbound connections.

Observation: Several default rules (e.g., Remote Desktop, File and Printer Sharing) were visible.



Windows Defender Firewall with Advanced Security

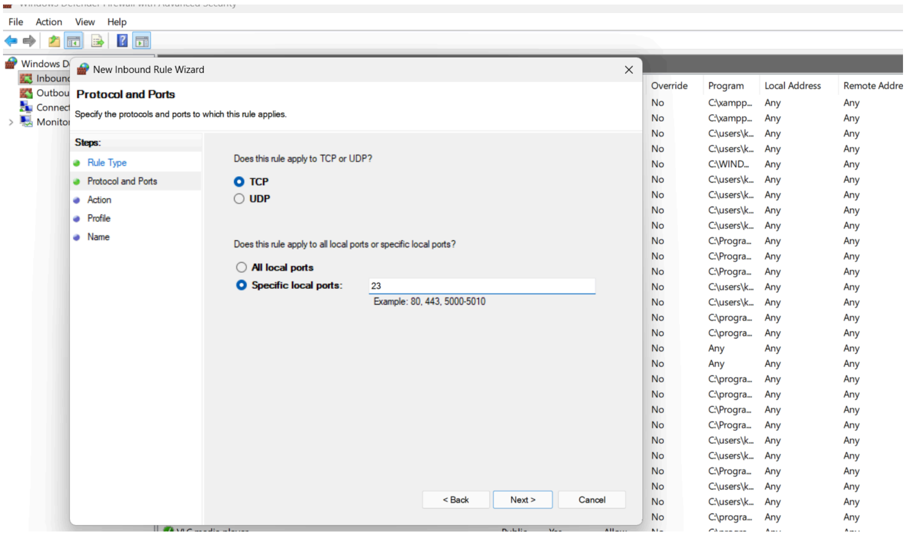
Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	UDP
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	TCP
arduino ide.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
arduino ide.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
AsusSwitchNetMDNS_269A2EB3		Private,...	Yes	Allow	No	C:\WIND...	Any	Any	Any
botim.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
botim.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
canva.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
canva.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
GlideXNearService		Private,...	Yes	Allow	No	C:\Progra...	Any	Any	Any
GlideXRemoteAgent		Private,...	Yes	Allow	No	C:\Progra...	Any	Any	Any
GlideXService		Private,...	Yes	Allow	No	C:\Progra...	Any	Any	Any
mdns-discovery.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
mdns-discovery.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Port 3306		All	Yes	Allow	No	Any	Any	Any	TCP
Port 33060		All	Yes	Allow	No	Any	Any	Any	TCP
Python		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Python		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
qBittorrent		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
qBittorrent		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
speedyforward.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
speedyforward.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
Unity Hub		Domain	Yes	Allow	No	C:\Progra...	Any	Any	Any
Visual Studio Code		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
Visual Studio Code		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
VLC media player		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
VLC media player		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
@{Microsoft.AAD.BrokerPlugin_1000.19580...	@{Microsoft.AAD.BrokerPlugi...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.226...	@{Microsoft.Win32WebView...	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.CloudExperienceHo...	@{Microsoft.Windows.Cloud...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.StartMenuExperien...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.ZuneVideo_10.24101.10041.0_...	@{Microsoft.ZuneVideo_10.2...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Client.CBS_1000.227...	@{MicrosoftWindows.Client....	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Client.Core_1000.22...	@{MicrosoftWindows.Client....	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.DesktopSpotlig...	@{MicrosoftWindows.LKG.De...	Domai...	Yes	Allow	No	Any	Any	Any	Any
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP

Step 3: Created a Block Rule for Telnet (Port 23)

- Chose **New Rule...** → Selected **Port** → Next.
- Selected **TCP** and entered port 23.
- Chose **Block the connection**.
- Applied to **Domain, Private, Public**.
- Named the rule **Block_Telnet**.

Observation: The rule appeared in the Inbound Rules list with action **Block**.



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

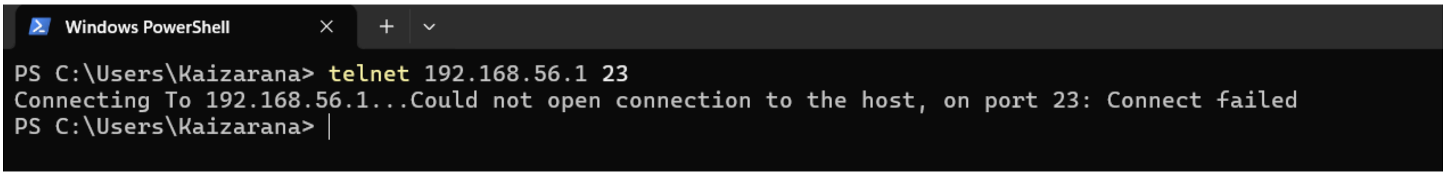
Example: 80, 443, 5000-5010

Override	Program	Local Address	Remote Addre
No	C:\xampp...	Any	Any
No	C:\xampp...	Any	Any
No	C:\users\k...	Any	Any
No	C:\users\k...	Any	Any
No	C:\WIND...	Any	Any
No	C:\users\k...	Any	Any
No	C:\users\k...	Any	Any
No	C:\users\k...	Any	Any
No	C:\users\k...	Any	Any
No	C:\Progra...	Any	Any
No	C:\Progra...	Any	Any
No	C:\Progra...	Any	Any
No	C:\users\k...	Any	Any
No	C:\users\k...	Any	Any
No	C:\progra...	Any	Any
No	C:\progra...	Any	Any
No	Any	Any	Any
No	Any	Any	Any
No	C:\progra...	Any	Any
No	C:\progra...	Any	Any
No	C:\Progra...	Any	Any
No	C:\Progra...	Any	Any
No	C:\users\k...	Any	Any
No	C:\users\k...	Any	Any
No	C:\Progra...	Any	Any
No	C:\users\k...	Any	Any
No	C:\users\k...	Any	Any
No	C:\progra...	Any	Any

Step 4: Tested the Block Rule

- Attempted to connect to port 23.
- Connection attempt was unsuccessful, confirming the rule worked.

Observation: Inbound Telnet traffic was blocked as expected.

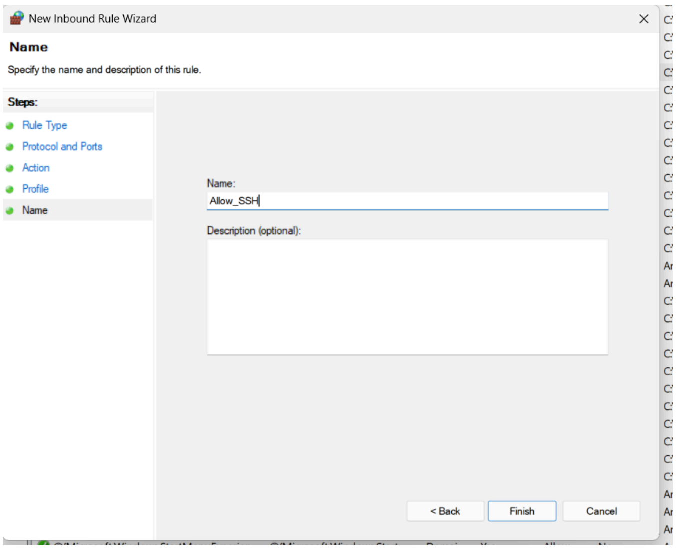


```
PS C:\Users\Kaizarana> telnet 192.168.56.1 23
Connecting To 192.168.56.1...Could not open connection to the host, on port 23: Connect failed
PS C:\Users\Kaizarana> |
```

Step 5: Added an Allow Rule for SSH (Port 22)

- Chose **New Rule...** → Selected **Port** → Next.
- Selected **TCP** and entered port 22.
- Chose **Allow the connection**.
- Applied to **Domain, Private, Public**.
- Named the rule **Allow_SSH**.

Observation: The rule appeared in the Inbound Rules list with action **Allow**.



Name

Specify the name and description of this rule.

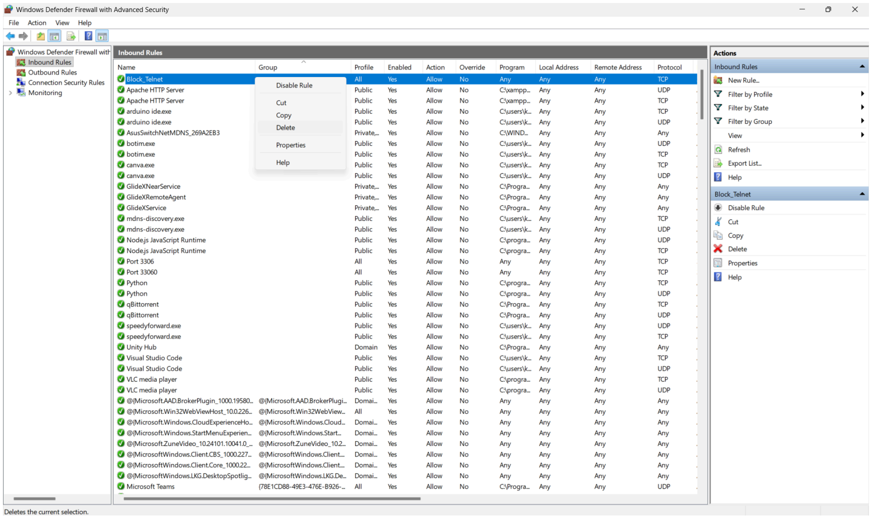
Name: Allow_SSH

Description (optional):

Step 6: Removed the Block Rule

- Located **Block_Telnet** in Inbound Rules.
- Right-clicked → chose **Delete**.

Observation: The Block_Telnet rule was removed, restoring the firewall to its previous state.



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Block_Telnet		All	Yes	Allow	No	Any	Any	Any	TCP
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	UDP
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	TCP
arduino ide.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
arduino ide.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
AsusSwitchNetMDNS_269A2EB3		Private,...	Yes	Allow	No	C:\WIND...	Any	Any	Any
botim.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
botim.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
canva.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
canva.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
GlideXNearService		Private,...	Yes	Allow	No	C:\Progra...	Any	Any	Any
GlideXRemoteAgent		Private,...	Yes	Allow	No	C:\Progra...	Any	Any	Any
GlideXService		Private,...	Yes	Allow	No	C:\Progra...	Any	Any	Any
mdns-discovery.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
mdns-discovery.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Port 3306		All	Yes	Allow	No	Any	Any	Any	TCP
Port 33060		All	Yes	Allow	No	Any	Any	Any	TCP
Python		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Python		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
qBittorrent		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
qBittorrent		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
speedyforward.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
speedyforward.exe		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
Unity Hub		Domain	Yes	Allow	No	C:\Progra...	Any	Any	Any
Visual Studio Code		Public	Yes	Allow	No	C:\users\k...	Any	Any	TCP
Visual Studio Code		Public	Yes	Allow	No	C:\users\k...	Any	Any	UDP
VLC media player		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
VLC media player		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
@{Microsoft.AAD.BrokerPlugin_1000.19580...	@{Microsoft.AAD.BrokerPlugi...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.226...	@{Microsoft.Win32WebView...	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.CloudExperienceHo...	@{Microsoft.Windows.Cloud...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.StartMenuExperien...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.ZuneVideo_10.24101.10041.0_...	@{Microsoft.ZuneVideo_10.2...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Client.CBS_1000.227...	@{MicrosoftWindows.Client....	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Client.Core_1000.22...	@{MicrosoftWindows.Client....	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.DesktopSpotlig...	@{MicrosoftWindows.LKG.De...	Domai...	Yes	Allow	No	Any	Any	Any	Any
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP

Deletes the current selection.

4. Summary of Results

- **Block_Telnet rule** successfully denied inbound connections on port 23.
- **Allow_SSH rule** explicitly permitted inbound connections on port 22.
- Rules were created, tested, and removed entirely using the GUI.

5. Conclusion

This exercise demonstrated how Windows Firewall filters traffic based on port and protocol. Using the GUI, inbound traffic can be easily managed with specific rules. Blocking port 23 showed how insecure services like Telnet can be restricted, while allowing port 22 demonstrated enabling secure remote access (SSH).

The exercise confirmed the firewall's role in **system hardening and network security**, ensuring only authorized connections are permitted while blocking unwanted traffic.