Windows Firewall Configuration Task

Objective

Configure and test basic firewall rules on a Windows machine to allow or block network traffic.

Tools Used

- **Windows Defender Firewall with Advanced Security** (GUI, accessed via `wf.msc`)
- **Command Prompt**
- **Telnet Client** (for testing blocked ports)

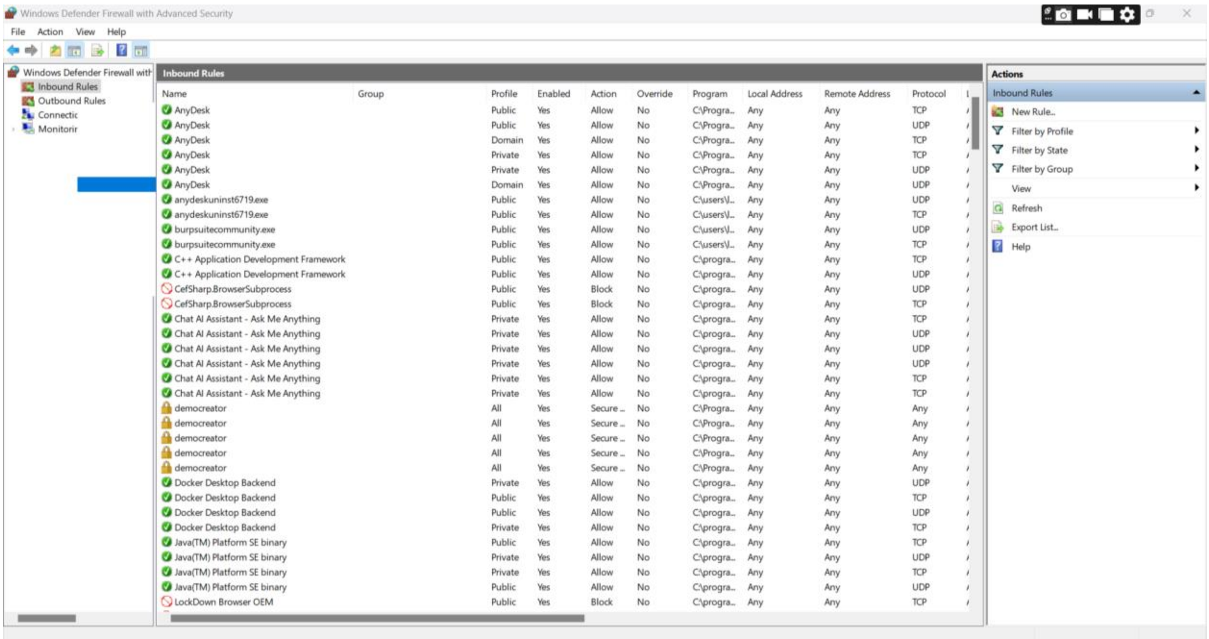
Steps Performed

1. Open Windows Firewall Configuration Tool

- Pressed `Win + R`, typed `wf.msc`, and pressed `Enter`.
- This opened the **Windows Defender Firewall with Advanced Security** window.

2. List Current Firewall Rules

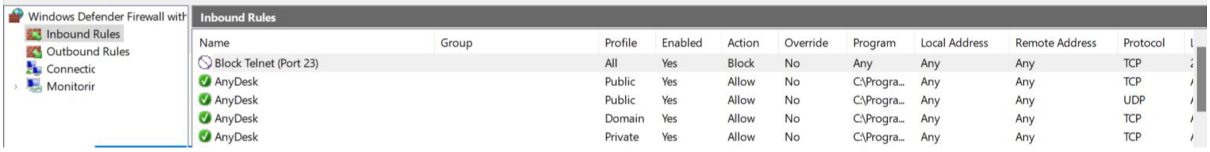
- Navigated to **Inbound Rules** on the left pane.
- Reviewed the current active rules applied to incoming network traffic.



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
AnyDesk		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk		Domain	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Private	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Private	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk		Domain	Yes	Allow	No	C:\Progra...	Any	Any	UDP
anydeskuninst6719.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	UDP
anydeskuninst6719.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	TCP
burpsuitecommunity.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	UDP
burpsuitecommunity.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	TCP
C++ Application Development Framework		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
C++ Application Development Framework		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
CefSharp.BrowserSubprocess		Public	Yes	Block	No	C:\progra...	Any	Any	UDP
CefSharp.BrowserSubprocess		Public	Yes	Block	No	C:\progra...	Any	Any	TCP
Chat AI Assistant - Ask Me Anything		Private	Yes	Allow	No	C:\progra...	Any	Any	TCP
Chat AI Assistant - Ask Me Anything		Private	Yes	Allow	No	C:\progra...	Any	Any	UDP
Chat AI Assistant - Ask Me Anything		Private	Yes	Allow	No	C:\progra...	Any	Any	UDP
Chat AI Assistant - Ask Me Anything		Private	Yes	Allow	No	C:\progra...	Any	Any	UDP
Chat AI Assistant - Ask Me Anything		Private	Yes	Allow	No	C:\progra...	Any	Any	TCP
Chat AI Assistant - Ask Me Anything		Private	Yes	Allow	No	C:\progra...	Any	Any	TCP
democreator		All	Yes	Secure ...	No	C:\Progra...	Any	Any	Any
democreator		All	Yes	Secure ...	No	C:\Progra...	Any	Any	Any
democreator		All	Yes	Secure ...	No	C:\Progra...	Any	Any	Any
democreator		All	Yes	Secure ...	No	C:\Progra...	Any	Any	Any
democreator		All	Yes	Secure ...	No	C:\Progra...	Any	Any	Any
Docker Desktop Backend		Private	Yes	Allow	No	C:\progra...	Any	Any	UDP
Docker Desktop Backend		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Docker Desktop Backend		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
Docker Desktop Backend		Private	Yes	Allow	No	C:\progra...	Any	Any	TCP
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Java(TM) Platform SE binary		Private	Yes	Allow	No	C:\progra...	Any	Any	UDP
Java(TM) Platform SE binary		Private	Yes	Allow	No	C:\progra...	Any	Any	TCP
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
LockDown Browser OEM		Public	Yes	Block	No	C:\progra...	Any	Any	TCP

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

- In **Inbound Rules**, clicked **New Rule...** on the right panel.
- Selected **Port** and clicked **Next**.
- Selected **TCP**, entered `23` in the specific local ports box.
- Chose **Block the connection**.
- Applied the rule to all profiles: Domain, Private, and Public.
- Named the rule **Block Telnet (Port 23)**.
- Finished and confirmed the new rule was listed.

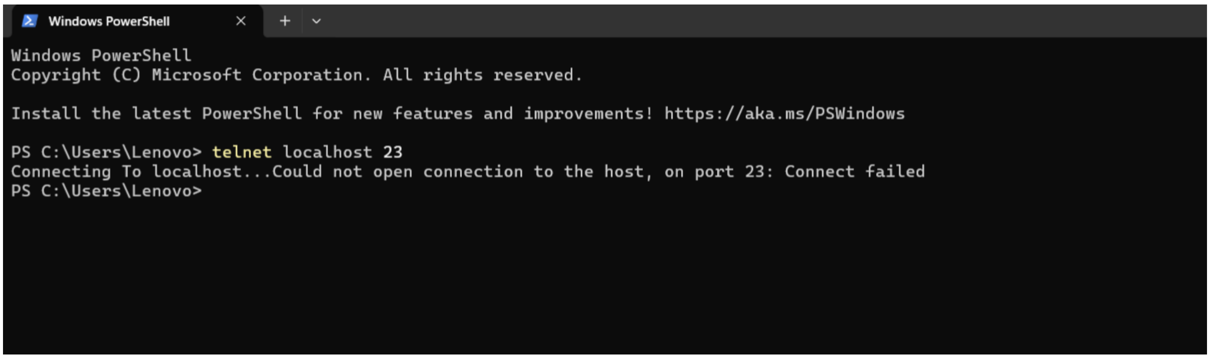


Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Block Telnet (Port 23)		All	Yes	Block	No	Any	Any	Any	TCP
AnyDesk		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk		Domain	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Private	Yes	Allow	No	C:\Progra...	Any	Any	TCP

4. Test the Block Rule

- Opened **Command Prompt**.

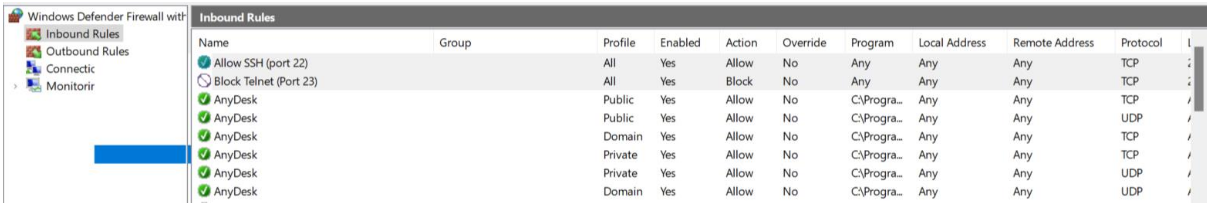


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

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

- The connection failed, confirming the block rule was effective.

5. Add Rule to Allow SSH Port 22

- Created another new inbound rule.
- Selected **Port**, TCP, and entered `22`.
- Chose **Allow the connection**.
- Applied to all profiles.
- Named the rule **Allow SSH (Port 22)**.
- Verified the rule appeared in the inbound rules list.

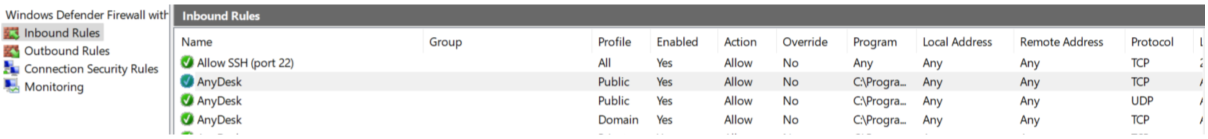


Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Allow SSH (port 22)		All	Yes	Allow	No	Any	Any	Any	TCP
Block Telnet (Port 23)		All	Yes	Block	No	Any	Any	Any	TCP
AnyDesk		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk		Domain	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Private	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Private	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk		Domain	Yes	Allow	No	C:\Progra...	Any	Any	UDP

6. Remove the Block Rule on Port 23

- Located the **Block Telnet (Port 23)** rule in inbound rules.
- Right-clicked and selected **Delete**.
- Confirmed removal to restore original firewall state.
- Took a final screenshot showing the rule no longer exists.



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Allow SSH (port 22)		All	Yes	Allow	No	Any	Any	Any	TCP
AnyDesk		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk		Domain	Yes	Allow	No	C:\Progra...	Any	Any	TCP

How Windows Firewall Filters Traffic

Windows Firewall filters network traffic based on a set of rules that specify:

- Protocol (TCP or UDP)
- Port number or program
- Direction (inbound or outbound)
- Action (allow or block)
- Network profile (Domain, Private, Public)

When a blocking rule is applied, the firewall silently drops matching packets, preventing unauthorized access. Allow rules permit traffic to pass, enabling legitimate network connections.

Outcome and Learning

- Demonstrated ability to manage Windows Firewall via GUI.
- Successfully blocked and allowed specific ports.
- Verified firewall rules through testing with Telnet.
- Learned how firewall rules control network traffic flow.