

Windows Firewall Configuration

1. Open Firewall Configuration Tool

GUI Method:

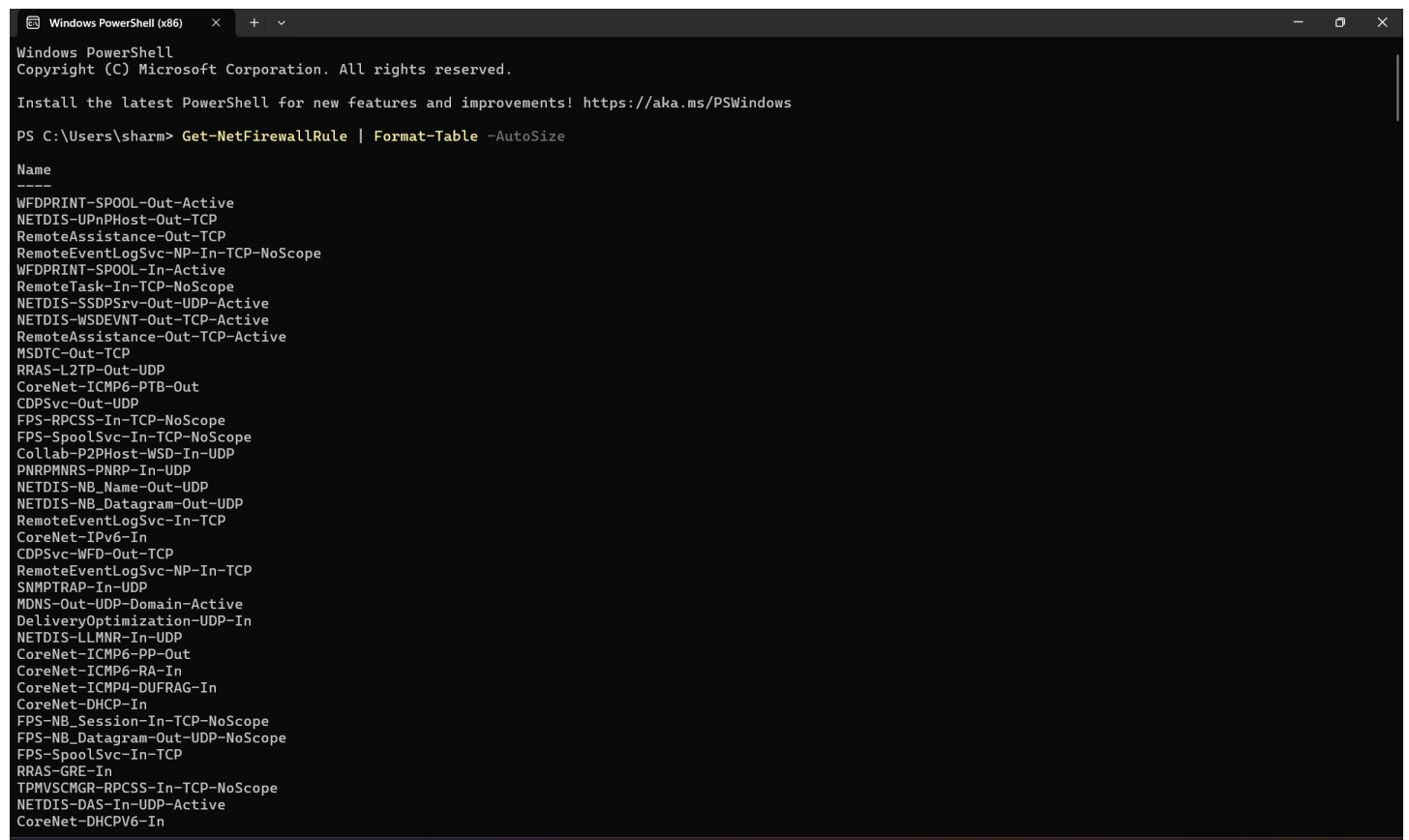
1. Press **Windows + R**, type `wf.msc`, and press **Enter**.
(This opens the Windows Defender Firewall with Advanced Security.)

Command-line (PowerShell) Method: `wf.msc`

2. List Current Firewall Rules

PowerShell: `Get-NetFirewallRule | Format-Table -AutoSize`

Or filter for inbound rules only: `Get-NetFirewallRule -Direction Inbound`



```
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\sharm> Get-NetFirewallRule | Format-Table -AutoSize

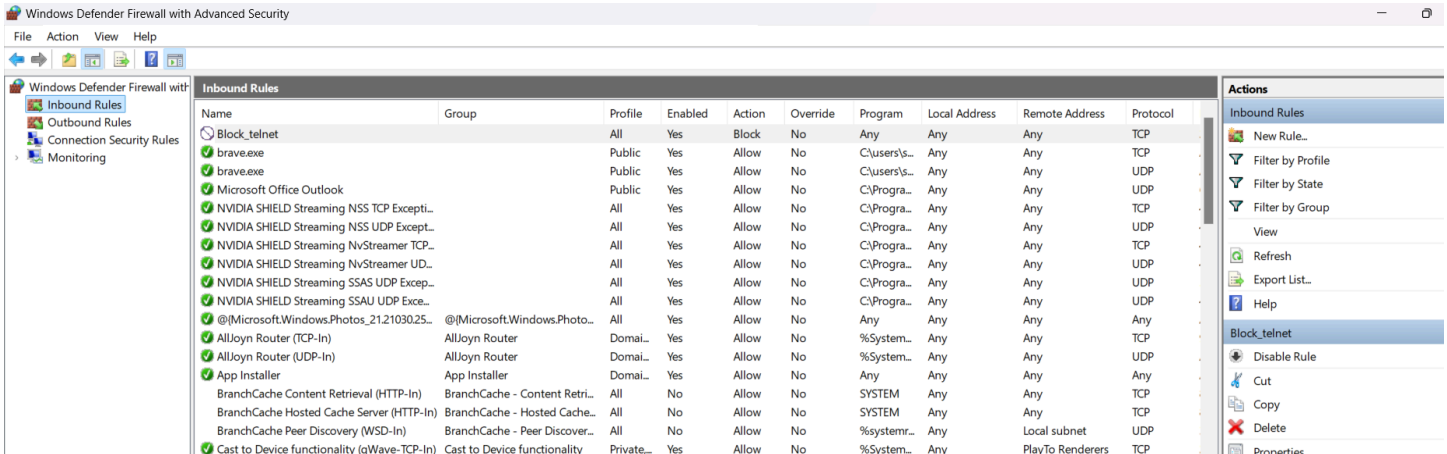
Name
----
WFDPRIINT-SPOOL-Out-Active
NETDIS-UPnPHost-Out-TCP
RemoteAssistance-Out-TCP
RemoteEventLogSvc-NP-In-TCP-NoScope
WFDPRIINT-SPOOL-In-Active
RemoteTask-In-TCP-NoScope
NETDIS-SSDPsrv-Out-UDP-Active
NETDIS-WSDEVNT-Out-TCP-Active
RemoteAssistance-Out-TCP-Active
MSDTC-Out-TCP
RRAS-L2TP-Out-UDP
CoreNet-ICMP6-PTB-Out
CDPSvc-Out-UDP
FPS-RPCSS-In-TCP-NoScope
FPS-SpoolSvc-In-TCP-NoScope
Collab-P2PHost-WSD-In-UDP
PNRPMNRS-PNRP-In-UDP
NETDIS-NB_Name-Out-UDP
NETDIS-NB_Datagram-Out-UDP
RemoteEventLogSvc-In-TCP
CoreNet-IPv6-In
CDPSvc-WFD-Out-TCP
RemoteEventLogSvc-NP-In-TCP
SNMPTRAP-In-UDP
MDNS-Out-UDP-Domain-Active
DeliveryOptimization-UDP-In
NETDIS-LLMNR-In-UDP
CoreNet-ICMP6-PP-Out
CoreNet-ICMP6-RA-In
CoreNet-ICMP4-DUFRAG-In
CoreNet-DHCP-In
FPS-NB_Session-In-TCP-NoScope
FPS-NB_Datagram-Out-UDP-NoScope
FPS-SpoolSvc-In-TCP
RRAS-GRE-In
TPMVSCMGR-RPCSS-In-TCP-NoScope
NETDIS-DAS-In-UDP-Active
CoreNet-DHCPV6-In
```

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

GUI Method:

1. In the left panel, click **Inbound Rules** → **New Rule**.
2. Choose **Port** → **Next**.
3. Select **TCP** and enter 23 → **Next**.

4. Select **Block the connection** → **Next**.
5. Apply to all profiles → **Next**.
6. Name it e.g. Block_Telnet → **Finish**.



PowerShell: New-NetFirewallRule -DisplayName "Block_Telnet" -Direction Inbound -LocalPort 23 -Protocol TCP -Action Block

4. Test the Rule

Local Test (PowerShell):

Test-NetConnection -ComputerName localhost -Port 23

Remote Test (From another system): telnet <your_IP> 23

```
Windows PowerShell (x86)
{5025BBDE-F549-42AB-92EA-2D9CBE3D0506} {04108D69-B37F-496C-B0EB-29EE1AD2762B}
Test-NetConnection :: ::1
Ping
Waiting for echo reply
{882345FB-61A8-4D0F-A171-3A1A38A14B21}
{28DE2F94-0663-4773-A882-771EF2195077}
{3566B0EC-B73E-4474-AB32-189EAC10B923}
{0950722E-5253-4C43-B19E-23F956C0D96C}
{C6B9D639-6D14-4609-96CF-08F4950D3941}
TCP Query User{90A67DDB-FF54-463B-B88C-D1A20A499916}C:\users\sharm\appda...
UDP Query User{2CB9F249-D0C9-4366-85AF-10D71F941D78}C:\users\sharm\appda...
{BE94D6E2-3C05-4437-985F-282649B522E9}
{627F130A-AB36-45BE-9BCB-4344EC38ABAD}
{724B7A81-6450-436D-9991-4E93722ADF67}
{553DC4A9-F186-4377-83F1-6B72F9F8179C}
{FA2719AF-0619-4FFD-9986-E48F9474EC76}
{F5B9614B-8A2F-4D9F-A080-54B6852D406A}
{ACAF42F8-EF30-4D6F-91FA-1FC47A7656C2}
{D1978B2F-5E00-4677-917A-980CF58E3E39}
{813C2EA5-2C86-4B6F-9BFB-BD3C7EBD9474}
{50D98239-4F5D-455D-BE83-C3D3271E1AFE}
{1CD2825E-EFBD-4D93-A436-AB0C037D344F}
{BEFBCFE4-D58E-4917-8A17-8E957CC00209}
{72A2122C-EBA6-4944-9296-DA0CDD31EE3E}
{A3D63AF5-6E9C-4285-B41C-99AB28DC4A2A}
{328FA984-329A-4C52-B2A3-B6C098C3F21D}
{D446022C-450C-4483-A0B7-F02C1BCC6E5A}
{35B2DCF7-C46D-4490-9B13-DB863924AE8C}
{B9442A1B-8BC4-4D12-AB2D-F1C2E81DB990}
{734FE027-F11A-4E9F-9D95-4F3564CEE5EA}
{4DC603EA-7C49-4DCA-BDDF-052C7FAA0DA9}
{34500C8C-1BDB-41EB-BF6A-6E67E9565E73}

PS C:\Users\sharm> Test-NetConnection -ComputerName localhost -Port 23
WARNING: TCP connect to (:::1 : 23) failed
WARNING: TCP connect to (127.0.0.1 : 23) failed
|
```

```
PS C:\Users\sharm> Test-NetConnection -ComputerName localhost -Port 23
WARNING: TCP connect to (:::1 : 23) failed
WARNING: TCP connect to (127.0.0.1 : 23) failed

ComputerName      : localhost
RemoteAddress     : :::1
RemotePort        : 23
InterfaceAlias    : Loopback Pseudo-Interface 1
SourceAddress     : :::1
PingSucceeded     : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded  : False
```

6. Remove the Test Block Rule

GUI:

- Go to **Inbound Rules**, find Block_Telnet, right-click → **Delete**.

PowerShell: Remove-NetFirewallRule -DisplayName "Block_Telnet"

How a Firewall Filters Traffic

A firewall works by applying a set of **rules** to decide whether to **allow**, **block**, or **limit** network traffic.

- **Packet Filtering:** Inspects packet headers (IP, port, protocol) to decide.
- **Stateful Inspection:** Tracks ongoing connections and applies rules based on connection state.
- **Application Filtering:** Controls traffic based on applications/services.
- **Profiles:** Rules can differ for private, public, and domain networks.

In our case:

- We blocked Telnet (port 23) inbound → prevented any device from establishing a connection.