

1. List of current firewall rule
 - Inbound rules
 - Out bound rules
 - Connection security rules

2. Add a rule to block inbound traffic on a specific port
 - Open Windows Defender Firewall and go to Advanced Security
 - Firewall → Advanced Settings
 - Inbound Rules → New Rule
 - Select Port
 - Choose TCP
 - Enter Port: 23
 - Select Block the connection
 - Apply on Domain, Private, Public
 - Name the rule:-Block Telnet

Port number:- 23

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
block telnet	All	Yes	Block	No	Any	Any	Any	
Microsoft Office Groove	Public	Yes	Allow	No	C:\Prog...	Any	Any	
Microsoft Office OneNote	Public	Yes	Allow	No	C:\Prog...	Any	Any	
Microsoft Office OneNote	Public	Yes	Allow	No	C:\Prog...	Any	Any	
Microsoft Office Outlook	Public	Yes	Allow	No	C:\Prog...	Any	Any	
Microsoft Office Outlook	Public	Yes	Allow	No	C:\Prog...	Any	Any	
Port 3306	All	Yes	Allow	No	Any	Any	Any	
Port 3306	All	Yes	Allow	No	Any	Any	Any	
@FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes	Allow	No	%System...	Any	Local su...
@FirewallAPI.dll,-80206	@FirewallAPI.dll,-80200	All	Yes	Allow	No	%System...	Any	Local su...
ms-resource:ProductPkg DisplayName	(78E1CD88-49E3-476E-B926...)	Private	Yes	Allow	No	C:\Wind...	Any	
ms-resource:ProductPkg DisplayName	(78E1CD88-49E3-476E-B926...)	Private	Yes	Allow	No	C:\Wind...	Any	
ms-resource:ProductPkg DisplayName	(78E1CD88-49E3-476E-B926...)	Public	Yes	Allow	No	C:\Wind...	Any	
ms-resource:ProductPkg DisplayName	(78E1CD88-49E3-476E-B926...)	Public	Yes	Allow	No	C:\Wind...	Any	
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any
App Installer	App Installer	Domai...	Yes	Allow	No	Any	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discov...	All	No	Allow	No	%system...	Any	Local su...
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo R...
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo R...
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow	No	System	Any	Local su...
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local su...
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo R...
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local su...
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	PlayTo R...
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	Any

Actions

- Inbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Selected Rule: Block telnet

- Disable Rule
- Cut
- Copy
- Delete
- Properties
- Help

Activate Windows

To settings to activate Windows.

Port number:-80

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has options: Inbound Rules, Outbound Rules, Connection Security Rules, and Monitoring. The main area is titled 'Inbound Rules' and lists various rules. One rule is highlighted: 'block unencrypted web traffic'. The right sidebar is titled 'Actions' and includes options like New Rule..., Filter by Profile, Refresh, Export List..., Help, Disable Rule, Cut, Copy, Delete, Properties, and a question mark icon.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
block unencrypted web traffic		All	Yes	Block	No	Any	Any	Any
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Prog...	Any	Any
Microsoft Office Groove		Public	Yes	Allow	No	C:\Prog...	Any	Any
Microsoft Office OneNote		Public	Yes	Allow	No	C:\Prog...	Any	Any
Microsoft Office OneNote		Public	Yes	Allow	No	C:\Prog...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Prog...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Prog...	Any	Any
Port 3306		All	Yes	Allow	No	Any	Any	Any
Port 33060		All	Yes	Allow	No	Any	Any	Any
@FirewallAPI.dll.-80201	@FirewallAPI.dll.-80200	All	Yes	Allow	No	%System...	Any	Local su
@FirewallAPI.dll.-80206	@FirewallAPI.dll.-80200	All	Yes	Allow	No	%System...	Any	Local su
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926...}	Private	Yes	Allow	No	C:\Wind...	Any	Any
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926...}	Public	Yes	Allow	No	C:\Wind...	Any	Any
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926...}	Public	Yes	Allow	No	C:\Wind...	Any	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any
App Installer	App Installer	Domain	Yes	Allow	No	Any	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%System...	Any	Local su
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo R
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo R
Cast to Device SSDP Discovery (UPD-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local su
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow	No	System	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo R
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local's
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any

3. Testing the rule by using Nmap :- tcp/23 closed

The screenshot shows the Zenmap interface. The target is set to 10.1.3.77. The command entered is nmap -p 23 10.1.3.77. The results tab shows the following output:

```
Starting Nmap 7.99 ( https://nmap.org ) at 2025-11-24 11:22 +0530
Nmap scan report for 10.1.3.77.
Host is up (0.00s latency).

PORT      STATE SERVICE
23/tcp    closed telnet

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

At the bottom right, there is an 'Activate Windows' watermark: 'Activate Windows Go to Settings to activate Windows.'

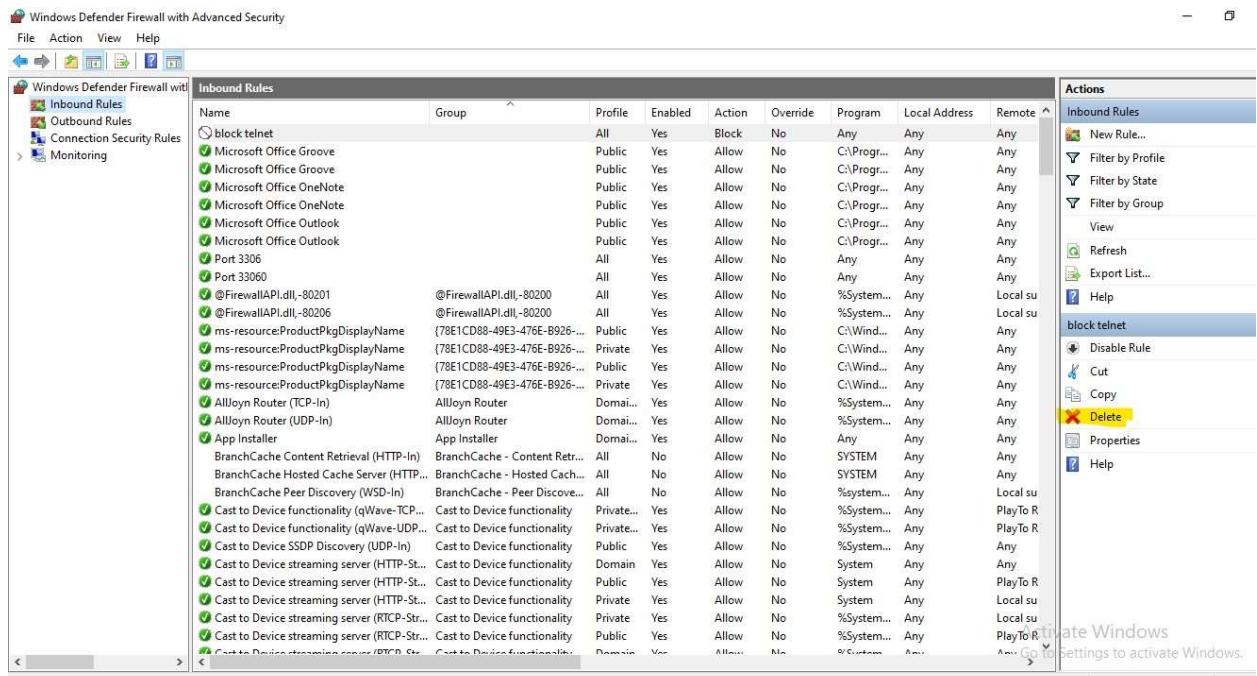
(PowerShell Test-NetConnection -ComputerName localhost -Port 23

Expected Output:

- TcpTestSucceeded : False → port is blocked
- TcpTestSucceeded : True → port is open/allowed)

4. .Removing the test block rule to restore original state :-

- Advanced Settings → Inbound Rules
- Right-click Block Telnet → Delete



5. summary

A firewall controls network traffic by comparing each packet against security rules (based on IPs, ports, protocols, and direction) and then allowing or blocking it accordingly.