Firewall Configuration & Traffic Control Guide

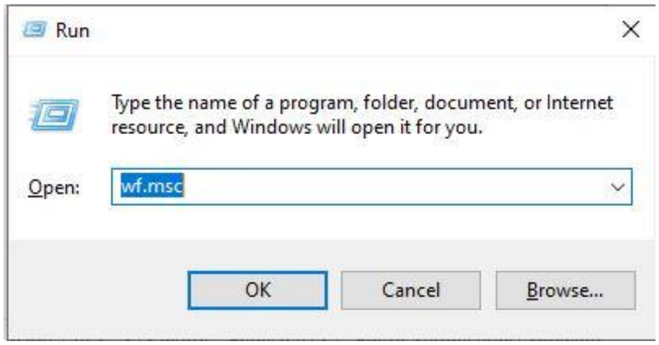
Overview

This document provides step-by-step guidance on configuring firewalls using both Windows and Linux systems. It includes how to block/allow ports, test rules, and understand firewall behavior.

Firewall Configuration on Windows

1. Open Firewall Configuration Tool

- Press Windows + R, type 'wf.msc', and press Enter.
- Or use PowerShell: Get-NetFirewallRule



Run

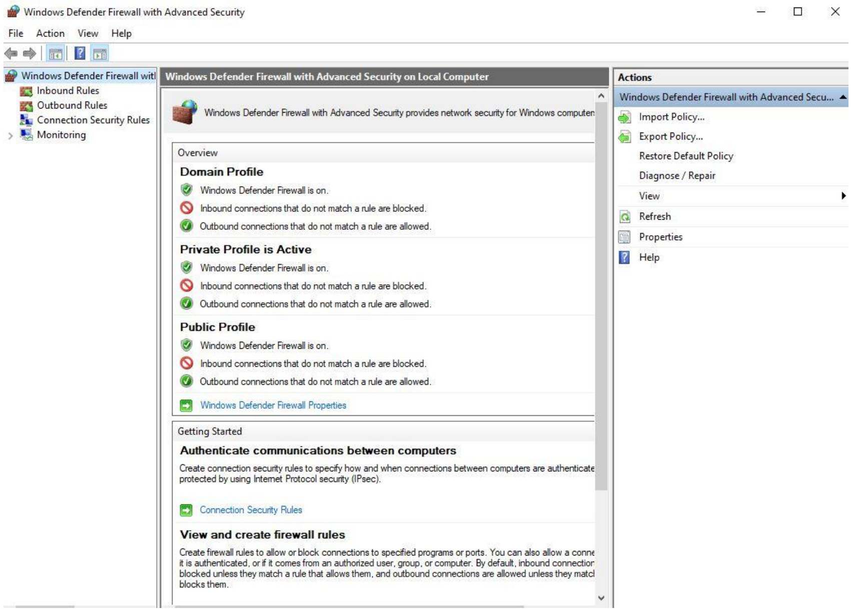
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wf.msc

2. List Current Firewall Rules

PowerShell:

```
Get-NetFirewallRule | Format-Table Name, Direction, Action, Enabled
```



Windows Defender Firewall with Advanced Security

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computer

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 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.

Public 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.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticate protected by using Internet Protocol security (IPsec).

Connection Security Rules

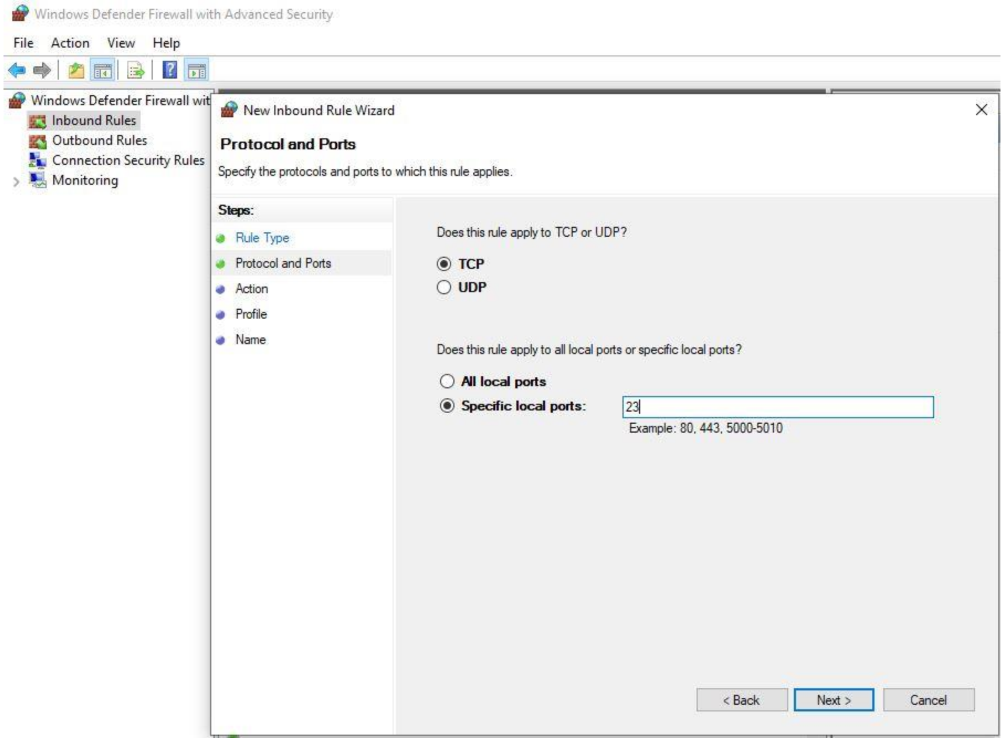
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a conne it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connection blocked unless they match a rule that allows them, and outbound connections are allowed unless they matcl blocks them.

3. Block Inbound Traffic on Port 23 (Telnet)

PowerShell:

```
New-NetFirewallRule -DisplayName "Block Telnet Port 23" -Direction Inbound -LocalPort 23 -Protocol TCP -Action Block
```



Windows Defender Firewall with Advanced Security

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

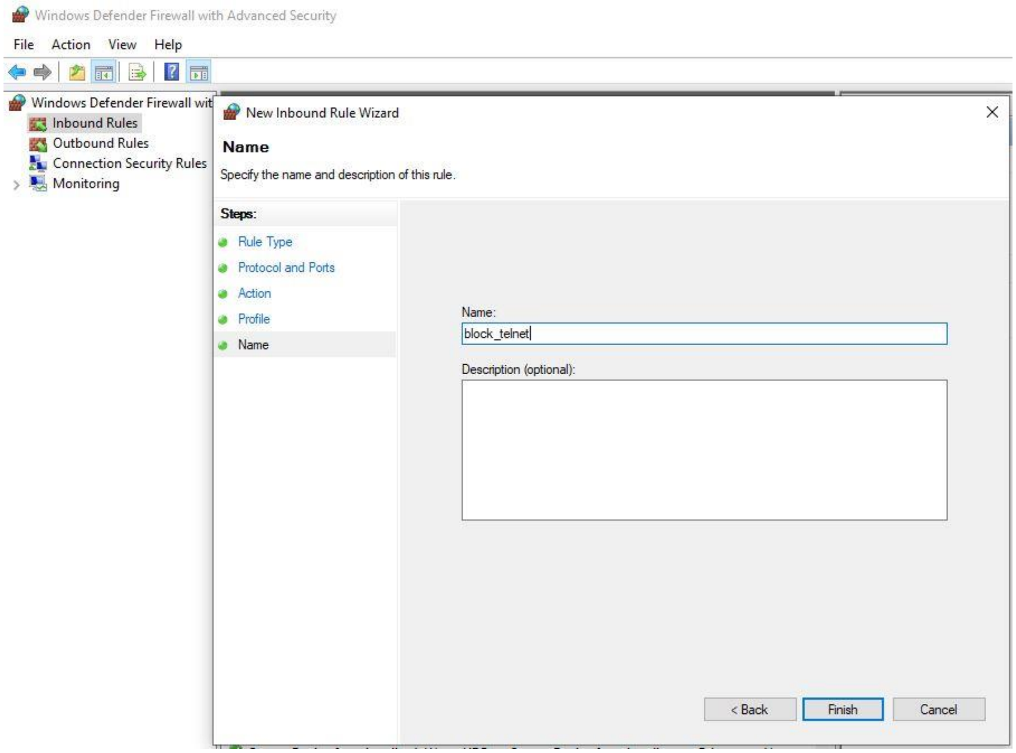
Does this rule apply to TCP or UDP?

● 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



Name

Specify the name and description of this rule.

Name: block_telnet

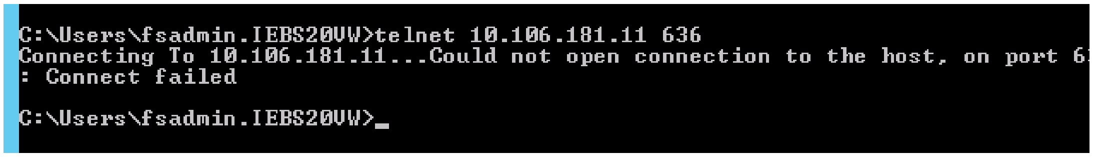
Description (optional):

4. Test the Rule

Open Command Prompt and run:

telnet 127.0.0.1 23

Note: Enable Telnet Client via 'optionalfeatures' if needed.



```
C:\Users\fsadmin.IEBS20VW>telnet 10.106.181.11 636
Connecting To 10.106.181.11...Could not open connection to the host, on port 6
: Connect failed

C:\Users\fsadmin.IEBS20VW>_
```

5. Allow SSH (Port 22)

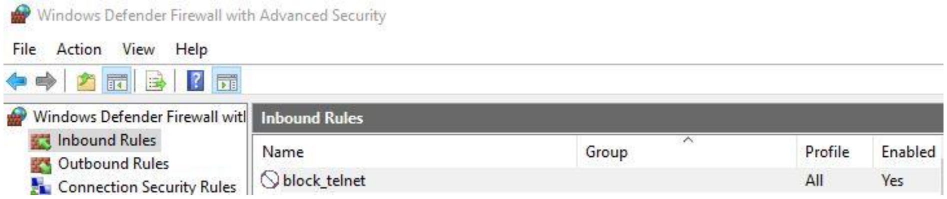
PowerShell:

New-NetFirewallRule -DisplayName "Allow SSH Port 22" -Direction Inbound -LocalPort 22 -Protocol TCP -Action Allow

6. Remove Block Rule

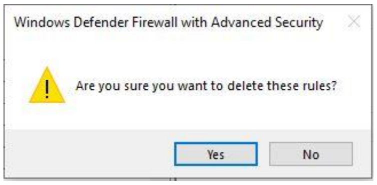
PowerShell:

Remove-NetFirewallRule -DisplayName "Block Telnet Port 23"


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules

Inbound Rules

Name	Group	Profile	Enabled
block_telnet		All	Yes



Windows Defender Firewall with Advanced Security

Are you sure you want to delete these rules?

Firewall Behavior Summary

Firewalls filter traffic by controlling incoming and outgoing network connections based on:
- Port number (e.g., 22 for SSH, 80 for HTTP)
- Protocol (TCP/UDP)
- IP address or range
- Application/process
This helps secure the system against unauthorized access and network-based attacks.