Windows 11 Firewall Setup and Testing Guide

**Contents**

1. [Introduction](#_bookmark0) 2
2. [Steps to Configure and Test Firewall on Windows 11](#_bookmark1) 2
   1. [Open Firewall](#_bookmark2) 2
   2. [List Current Rules](#_bookmark3) 2
   3. [Add a Rule to Block a Port (e.g., Telnet = Port 23)](#_bookmark4) 2
   4. [Test the Rule](#_bookmark5) 3
   5. [Allow a Rule (Optional – Example: Port 22 for SSH)](#_bookmark6) 3
   6. [Remove the Test Rule](#_bookmark7) 3
   7. [Deliverables](#_bookmark8) 3
3. [Summary](#_bookmark9) 4
4. [Outcome](#_bookmark10) 4

# Introduction

This guide provides step-by-step instructions for configuring and testing firewall rules on Windows 11 using the Windows Defender Firewall with Advanced Se- curity. By setting up rules to block or allow specific network traffic, you can en- hance your system’s security. This document covers opening the firewall, man- aging rules, testing configurations, and documenting the process.

# Steps to Configure and Test Firewall on Windows 11

## Open Firewall

blue-square **Steps:**

1. Press Win + R, type wf.msc, and press Enter to open “Windows Defender Firewall with Advanced Security”.
2. point-right If the window opens, your firewall is installed and running.

## List Current Rules

blue-square **Steps:**

1. In the left pane, click **Inbound Rules** to view the list of existing rules.
2. Similarly, click **Outbound Rules** to view outbound rules.

## Add a Rule to Block a Port (e.g., Telnet = Port 23)

blue-square **Steps:**

1. In the right pane, click **New Rule…**.
2. Choose **Port** >Click **Next**.
3. Select **TCP** >In “Specific local ports” type: 23 >Click **Next**.
4. Select **Block the connection** >Click **Next**.
5. Choose when to apply (Domain, Private, Public) >Keep all checked >Click **Next**.
6. Name the rule (e.g., Block Telnet 23) >Click **Finish**. point-right Traffic on Port 23 is now blocked.

## Test the Rule

blue-square **Steps:**

1. Attempt to connect via Telnet on port 23 (locally or remotely). The connection should fail.
2. Note: The Telnet client can be installed via Windows Features if not already enabled.

## Allow a Rule (Optional – Example: Port 22 for SSH)

blue-square **Steps:**

1. In **Inbound Rules**, click **New Rule…**.
2. Select **Port** >**TCP** >Enter 22.
3. Select **Allow the connection**.
4. Apply to Domain, Private, Public >Click **Next**.
5. Name the rule (e.g., Allow SSH 22) >Click **Finish**.

## Remove the Test Rule

blue-square **Steps:**

1. Go to **Inbound Rules**.
2. Locate the Block Telnet 23 rule >Right-click >**Delete**.
3. This restores the firewall to its original state.

## Deliverables

blue-square **Required Screenshots:**

1. **Inbound Rules** list before adding the new rule.
2. The “New Rule Wizard” during rule creation.
3. The Block Telnet 23 rule in the **Inbound Rules** list.
4. The **Inbound Rules** list after deleting the rule.

# Summary

blue-square **How the Firewall Works:**

**Overview.** The Windows Defender Firewall filters network traffic using rules that either **Allow** or **Block** packets based on:

* **Protocol** (e.g., TCP, UDP)
* **Port number** (e.g., 23 for Telnet, 22 for SSH)

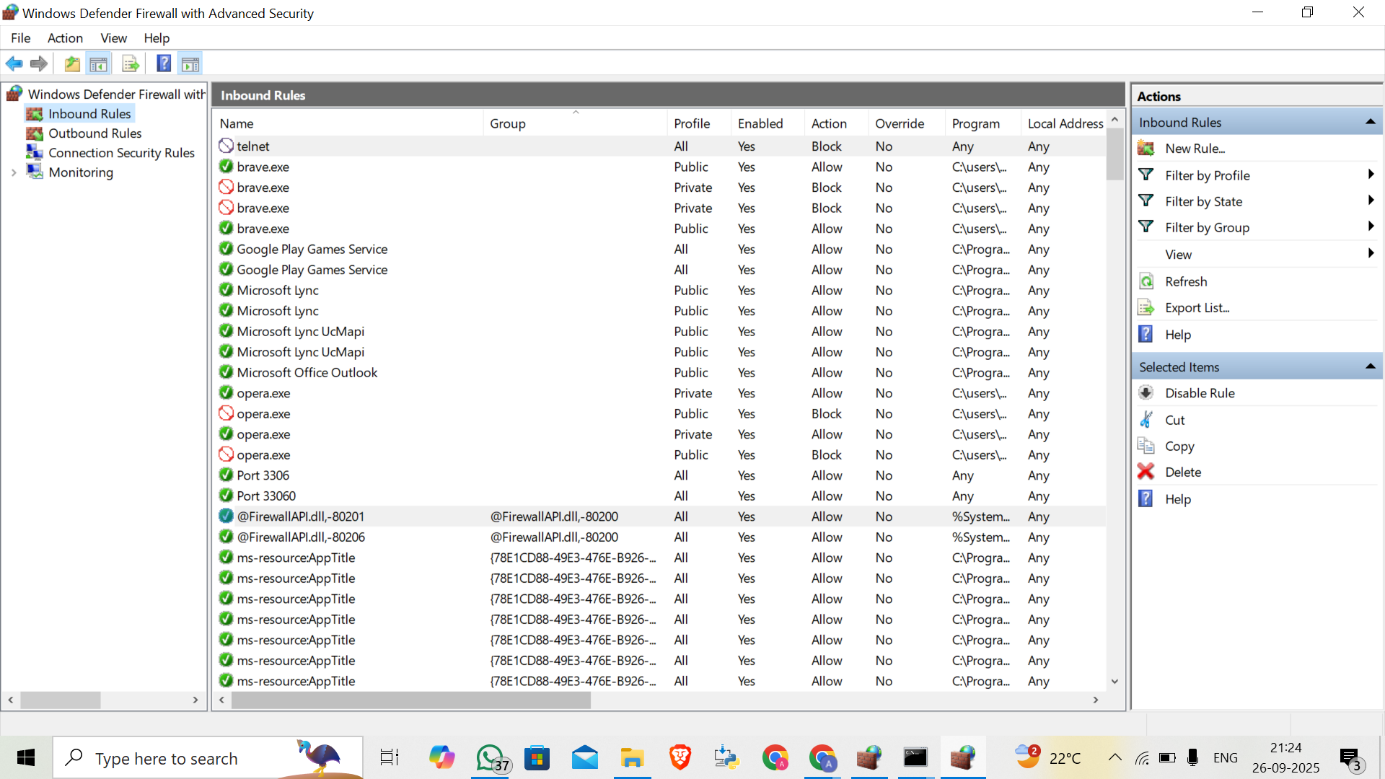
#### Application

* **Network profile** (Domain, Private, Public)

**Purpose.** Firewall rules protect your system by controlling incoming and out- going traffic, preventing unauthorized access, and ensuring only trusted connections are allowed.

# Outcome

check-mark-button You have gained essential skills for managing the Windows 11 firewall, enabling you to con



A screenshot of a computer

AI-generated content may be incorrect.

figure and test rules to secure network traffic.