# Windows Firewall Configuration Task Report

This document summarizes the steps taken to manage firewall rules on Windows using both GUI and PowerShell methods.

## Step 1 — Open Firewall Configuration Tool

Press Win + R, type 'wf.msc', and press Enter to open Windows Defender Firewall with Advanced Security.

## Step 2 — List Current Firewall Rules

GUI Method: Click Inbound Rules → view Name, Profile, Action, Protocol, Local Port.

PowerShell Method:

Get-NetFirewallRule -Direction Inbound | Format-Table DisplayName, Enabled, Action, Profile, Protocol, LocalPort

## Step 3 — Add a Rule to Block Inbound Traffic (Port 23 - Telnet)

GUI Method:

1. In Inbound Rules → New Rule…

2. Select Port → TCP → Specific local ports: 23

3. Choose Block the connection → apply to all profiles → Name it 'Block Telnet Port 23' → Finish

PowerShell Method:

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

## Step 4 — Test the Rule

Ensure Telnet client installed:

dism /online /Enable-Feature /FeatureName:TelnetClient

Test connection:

telnet 127.0.0.1 23

Expected: Connection should fail (firewall blocking the port).

## Step 6 — Remove Test Block Rule

GUI: Right-click rule 'Block Telnet Port 23' → Delete or Disable

PowerShell:

Remove-NetFirewallRule -DisplayName "Block Telnet Port 23"

## Summary

These steps demonstrate how to view, add, test, and remove firewall rules on Windows using GUI and PowerShell.