Windows Firewall Configuration Guide

**Contents**

1. [Objective](#_bookmark0) 2
2. [Tools](#_bookmark1) 2
3. [Steps](#_bookmark2) 2
   1. [Opening the Firewall Configuration Tool](#_bookmark3) 2
   2. [Listing Current Firewall Rules](#_bookmark4) 2
   3. [Adding a Rule to Block Inbound Traffic on Port 23 (Telnet)](#_bookmark5) 2
   4. [Testing the Rule](#_bookmark6) 3
   5. [Adding a Rule to Allow SSH (Port 22)](#_bookmark7) 3
   6. [Removing the Test Block Rule](#_bookmark8) 4
   7. [Documenting Commands and GUI Steps](#_bookmark9) 4
4. [Deliverables](#_bookmark10) 4
5. [How Windows Firewall Filters Traffic](#_bookmark11) 4

# Objective

Configure and test basic firewall rules on Windows to allow or block network traffic, ensuring proper filtering of inbound connections.

# Tools

* **Windows Defender Firewall**: Built-in firewall management tool in Win- dows.
* **PowerShell**: For command-line configuration and testing.
* **GUI**: Windows Defender Firewall with Advanced Security for graphical con- figuration.

# Steps

## Opening the Firewall Configuration Tool

* + - **GUI**: Press Win + S, type “Windows Defender Firewall with Advanced Se- curity,” and open the application.
    - **PowerShell**: Open PowerShell as Administrator by running powershell

via Win + R.

## Listing Current Firewall Rules

* + - **GUI**: In the Windows Defender Firewall with Advanced Security window, click **Inbound Rules** or **Outbound Rules** in the left pane to view existing rules.
    - **PowerShell**: Execute the following command to list all firewall rules:

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

## Adding a Rule to Block Inbound Traffic on Port 23 (Telnet)

* + - **GUI**:
      1. In the Windows Defender Firewall with Advanced Security window, click **Inbound Rules** >**New Rule**.
      2. Select **Port** >Next.
      3. Choose **TCP**, enter 23 in “Specific local ports” >Next.
      4. Select **Block the connection** >Next.
      5. Apply to all profiles (Domain, Private, Public) >Next.
      6. Name the rule “Block Telnet Port 23” >Finish.
    - **PowerShell**: Run the following command:

New-NetFirewallRule -Name ”BlockTelnet” -DisplayName ”Block Telnet Port 23” -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block

## Testing the Rule

* + - Locally, test the connection to port 23 using PowerShell:

Test-NetConnection -ComputerName localhost -Port 23

Expected output: TcpTestSucceeded: False (indicating the connection is blocked).

* + - Alternatively, from a remote machine (if available), use:

telnet <your-machine-ip> 23

The connection should fail.

* + - **Deliverable**: Take a screenshot of the PowerShell output or Telnet failure message.

## Adding a Rule to Allow SSH (Port 22)

* + - Note: Windows does not run an SSH server by default. If OpenSSH Server is installed, allow port 22.
    - **GUI**:
      1. Follow the same steps as above, but select **Allow the connection** for port 22 (TCP).
      2. Name the rule “Allow SSH Port 22”.

#### PowerShell:

New-NetFirewallRule -Name ”AllowSSH” -DisplayName ”Allow SSH Port 22” -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow

## Removing the Test Block Rule

* + - **GUI**: In **Inbound Rules**, locate “Block Telnet Port 23,” right-click, and select

#### Delete.

#### PowerShell:

Remove-NetFirewallRule -Name ”BlockTelnet”

## Documenting Commands and GUI Steps

* + - Export firewall rules to a file:

netsh advfirewall export ”C:\firewall-rules.wfw”

* + - Save the following PowerShell commands in a .ps1 or text file:

# Block Telnet

New-NetFirewallRule -Name ”BlockTelnet” -DisplayName ”Block Telnet Port 23” -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block

# Allow SSH

New-NetFirewallRule -Name ”AllowSSH” -DisplayName ”Allow SSH Port 22” -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow

# Remove Telnet Rule

Remove-NetFirewallRule -Name ”BlockTelnet”

* + - **Deliverable**: Take a screenshot of the **Inbound Rules** list showing the “Block Telnet Port 23” and “Allow SSH Port 22” rules.

# Deliverables

* **Screenshot**: Capture the **Inbound Rules** list or PowerShell output showing the rules.
* **Configuration File**: Export firewall rules to C:-rules.wfw or save the PowerShell commands in a text file.
* **Test Output**: Screenshot of Test-NetConnection output showing port 23 blocked.

# How Windows Firewall Filters Traffic

The Windows Defender Firewall filters network traffic based on predefined rules that specify whether to allow or block packets. It inspects:

* **Source/Destination IP**: Identifies the sender or receiver.
* **Port Numbers**: Determines the service (e.g., port 23 for Telnet, 22 for SSH).
* **Protocol**: Filters based on TCP, UDP, or ICMP.
* **Direction**: Differentiates between inbound and outbound traffic.
* **Action**: Specifies whether to allow or block the packet.

The firewall evaluates packets against rules in order of priority, applying the first matching rule’s action. If no rule matches, the default policy is applied. Windows Firewall supports stateful inspection, tracking connection states to allow return traffic for established sessions.



