Firewall Configuration and Testing Guide

Overview

This guide demonstrates how to configure and test basic firewall rules using Windows Firewall and UFW (Uncomplicated Firewall) on Linux to control network traffic.

How Firewalls Work

Firewalls act as a barrier between trusted internal networks and untrusted external networks. They filter traffic based on predetermined security rules, examining:

- **Source/Destination IP addresses**
- **Port numbers**
- **Protocols (TCP/UDP)**
- **Traffic direction (inbound/outbound)**

Part 1: Windows Firewall Configuration

Step 1: Access Windows Firewall

Method 1 - GUI:

1. Press Win + R, type wf.msc, press Enter
2. Or go to Control Panel → System and Security → Windows Defender Firewall → Advanced settings

Method 2 - Command Line (Run as Administrator):

```
# Open Command Prompt as Administrator

netsh advfirewall firewall
```

Step 2: List Current Firewall Rules

GUI Method:

- In Windows Firewall with Advanced Security, click "Inbound Rules" or "Outbound Rules"

Command Line Method:

```
# List all inbound rules

netsh advfirewall firewall show rule dir=in


# List all outbound rules
```

```
netsh advfirewall firewall show rule dir=out


# Show firewall profiles status
netsh advfirewall show allprofiles
```

Step 3: Block Telnet Traffic (Port 23)

GUI Method:

1. Right-click "Inbound Rules" → "New Rule"
2. Select "Port" → Next
3. Select "TCP" and "Specific local ports: 23"
4. Select "Block the connection"
5. Apply to all profiles (Domain, Private, Public)
6. Name: "Block Telnet Port 23"

Command Line Method:

```
# Block inbound Telnet traffic on port 23
netsh advfirewall firewall add rule name="Block Telnet Port 23" dir=in action=block protocol=TCP localport=23


# Verify the rule was created
netsh advfirewall firewall show rule name="Block Telnet Port 23"
```

Step 4: Test the Firewall Rule

cmd

```
# Test from local machine
telnet localhost 23


# Test with netstat to see if port is listening
netstat -an | findstr :23


# Use PowerShell to test port connectivity
Test-NetConnection -ComputerName localhost -Port 23
```

Step 5: Allow SSH Traffic (Port 22) - If Needed

```
# Allow inbound SSH traffic

netsh advfirewall firewall add rule name="Allow SSH Port 22" dir=in action=allow protocol=TCP localport=22


# Allow outbound SSH traffic

netsh advfirewall firewall add rule name="Allow SSH Port 22 Out" dir=out action=allow protocol=TCP localport=22
```

Step 6: Remove Test Rules

GUI Method:

1. Find the rule in Inbound Rules
2. Right-click → Delete

Command Line Method:

```
# Remove the block rule

netsh advfirewall firewall delete rule name="Block Telnet Port 23"


# Verify removal

netsh advfirewall firewall show rule name="Block Telnet Port 23"
```