# Firewall Configuration Task – Linux (UFW) and Windows

## Option A: Linux – Using UFW (Uncomplicated Firewall)

### 1. Open Firewall Configuration Tool

Open terminal and run:  
  
sudo ufw enable

### 2. List Current Firewall Rules

sudo ufw status verbose

### 3. Add Rule to Block Inbound Traffic on Port 23 (Telnet)

sudo ufw deny 23

### 4. Test the Rule

Install Telnet if not installed:  
  
sudo apt install telnet  
  
Then test:  
  
telnet localhost 23  
  
Expected: Connection refused

### 5. Add Rule to Allow SSH (Port 22)

sudo ufw allow 22

### 6. Remove the Test Block Rule

sudo ufw delete deny 23

### 7. Documented Commands Used

sudo ufw enable  
sudo ufw status verbose  
sudo ufw deny 23  
telnet localhost 23  
sudo ufw allow 22  
sudo ufw delete deny 23

### 8. Summary: How Firewall Filters Traffic

A firewall controls the flow of traffic into and out of a system based on defined rules. It filters inbound and outbound connections by port, protocol, or IP. For example, blocking port 23 prevents Telnet access, while allowing port 22 ensures SSH remains available. This helps protect the system from unauthorized access or exploitation.

## Option B: Windows – Using Windows Firewall

### 1. Open Firewall Configuration Tool

Search 'Windows Defender Firewall' and click 'Advanced Settings'.

### 2. List Current Firewall Rules

Go to 'Inbound Rules' or run in PowerShell:  
  
Get-NetFirewallRule | Where-Object { $\_.Enabled -eq 'True' }

### 3. Add Rule to Block Port 23

In 'Inbound Rules' → New Rule → Port → TCP → Specific port: 23 → Block the connection → Apply to all profiles → Name it: 'Block Telnet'

### 4. Test the Rule

Enable Telnet:  
Control Panel → Programs → Turn Windows features on or off → Enable 'Telnet Client'  
  
Then run:  
  
telnet localhost 23  
  
Expected: Failed connection

### 5. Add Rule to Allow SSH (Port 22)

Same steps as above, but use Port 22 and select 'Allow the connection'.

### 6. Remove Block Rule

Find 'Block Telnet' in 'Inbound Rules', right-click and select 'Delete'.

### 7. Documented GUI Steps

Windows Firewall → Advanced Settings → Inbound Rules → New Rule → Port → TCP → Port 23 → Block  
Add rule for Port 22 → Allow  
Delete the test rule after testing

### 8. Summary: How Firewall Filters Traffic

Windows Firewall monitors and controls incoming and outgoing network traffic. Rules define which ports or applications are allowed or blocked. Blocking port 23 disables Telnet, enhancing security. Allowing port 22 ensures SSH connections are permitted.