Windows Firewall Configuration – GUI Steps

# 1. Open the Windows Firewall Configuration Tool

1. Press Win + S (search), type 'Windows Defender Firewall', and open it.  
2. Click 'Advanced settings' in the left panel to open 'Windows Defender Firewall with Advanced Security'.

# 2. List Current Firewall Rules

1. In the Advanced Security window, select 'Inbound Rules' to see all inbound rules.  
2. Select 'Outbound Rules' to see outbound rules.  
These lists display the current firewall rules.

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

1. In the left pane, click 'Inbound Rules'.  
2. In the right pane, click 'New Rule…'.  
3. Choose 'Port' and click Next.  
4. Select 'TCP', enter '23' in the Specific local ports field, click Next.  
5. Choose 'Block the connection' and click Next.  
6. Select when the rule applies (Domain, Private, Public) and click Next.  
7. Name the rule (e.g., 'Block Telnet') and click Finish.

# 4. Test the Rule

1. On the same computer, open PowerShell and run:  
 Test-NetConnection -Port 23 localhost  
 It should fail to connect.  
2. From another computer on the network, you can use a port scanner like nmap to confirm that port 23 is blocked.

# 5. Remove the Test Block Rule

1. Go back to 'Inbound Rules'.  
2. Find the rule named 'Block Telnet'.  
3. Right-click the rule and select 'Delete' to remove it.

# 6. Summary of Firewall Filtering

Windows Firewall is a stateful host-based firewall that filters inbound and outbound network traffic. By default, inbound connections are blocked unless a rule allows them, while outbound traffic is usually allowed. The firewall can filter by port, program, protocol, or network profile (Domain, Private, Public).