Firewall Configuration & Testing – Windows

1. Commands / GUI Steps Used

Step 1 – Open Windows Firewall (GUI)
- Press Windows + R, type: control firewall.cpl
- Press Enter → Opens Windows Defender Firewall.
- Click Advanced Settings to open Windows Defender Firewall with Advanced Security.

Step 2 – View Current Rules
- In the left pane, click Inbound Rules.
- Scroll to see all existing rules.

Step 3 – Block Inbound Traffic on Port 23 (Telnet)
GUI:
- Inbound Rules → New Rule… (right panel)
- Select Port → Next
- Select TCP → Specific local ports: 23 → Next
- Select Block the connection → Next
- Apply to Domain, Private, Public → Next
- Name: Block Telnet → Finish

PowerShell:
```
New-NetFirewallRule -DisplayName "Block Telnet" -Direction Inbound
-LocalPort 23 -Protocol TCP -Action Block
```

Step 4 – Test the Rule
Install Telnet Client:
```
dism /online /Enable-Feature /FeatureName:TelnetClient
```
Test:
```
telnet localhost 23
```
Expected result: Could not open connection to the host, on port 23: Connect failed

Step 5 – Allow SSH (Port 22)
GUI:
- Inbound Rules → New Rule…
- Select Port → Next
- Select TCP → Specific local ports: 22 → Next
- Select Allow the connection → Next
- Apply to profiles → Next
- Name: Allow SSH → Finish

PowerShell:
```
New-NetFirewallRule -DisplayName "Allow SSH" -Direction Inbound
-LocalPort 22 -Protocol TCP -Action Allow
```

Step 6 – Remove the Telnet Block Rule
GUI:
- In Inbound Rules, find Block Telnet.
- Right-click → Delete (or Disable).

PowerShell:
```
Remove-NetFirewallRule -DisplayName "Block Telnet"
```

2. Summary – How Firewall Filters Traffic

A firewall acts as a network security filter. It inspects packets entering or leaving your system and applies rules to decide whether to allow or block them.
Filtering can be based on:
- Port numbers (e.g., block 23, allow 22)
- Protocols (TCP/UDP/ICMP)
- Direction (Inbound or Outbound)
- Application-specific rules
- Network profile (Domain, Private, Public)

Windows Defender Firewall enforces these rules before traffic reaches the application, helping prevent unauthorized access or exploitation.