GUI Steps Used:

Windows (GUI Method for Firewall)

1️ Open Control Panel → System and Security → Windows Defender Firewall → Advanced Settings.

2️ Go to Inbound Rules → Click New Rule.

3️ Select Port → Enter the port (e.g., 23 for Telnet).

4️ Choose Block the connection → Select profiles → Name the rule (e.g., "Block Telnet").

5️ To remove the rule, right-click the rule → Delete.

**How Firewall Filters Traffic:**

A **firewall** is like a security guard that checks all network traffic (packets) against a set of **rules**.  
 These rules are based on:

* **Direction** (Inbound or Outbound)
* **Protocol** (TCP, UDP, etc.)
* **Port number** (e.g., 23 for Telnet, 22 for SSH)
* **Action** (Allow, Block, or Deny)

When traffic **matches a rule**:

* If **allowed**, traffic passes through.
* If **denied/blocked**, the connection is refused or dropped.

Example in this task:

* Rule to **block port 23** means no Telnet connections can be made.
* Rule to **allow port 22** ensures you can still access SSH remotely.

Firewalls are **critical for security**:

* They prevent unauthorized access.
* They protect against attacks like port scanning, brute-forcing, and malware.