Summary of how firewall filters traffic

A firewall monitors network traffic and decides whether to allow or block it based on predefined rules.

These rules can filter traffic by:

1: Direction – inbound (coming into the device) or outbound (going out).

2: Protocol – such as TCP, UDP, or ICMP.

3: Port number – for example, port 23 for Telnet.

4: IP address or network – allowing or blocking specific sources/destinations.

When a packet matches a rule, the firewall takes the specified **action** (Allow, Block, or other policies).
In this task, we created a rule blocking TCP traffic on **port 23**, preventing Telnet connections to the system. This reduced potential attack surface by stopping unwanted service access.