Summary: How a Firewall Filters Traffic

A firewall filters network traffic by inspecting incoming and outgoing data packets and comparing them against a set of predefined security rules. These rules are based on parameters such as **IP address**, **port number**, **protocol (TCP/UDP)**, and **direction of traffic (inbound or outbound)**. If a packet matches an **allow rule**, it is permitted to pass; if it matches a **deny/block rule**, it is dropped or rejected. Traffic that does not match any explicit allow rule is usually blocked by default. This rule-based filtering mechanism helps prevent unauthorized access, reduces exposure to network attacks, and protects systems from malicious traffic.