Firewall

https://personalfirewall.comodo.com/how-firewall-works.html
https://www.forcepoint.com/cyber-edu/firewall

Firewall monitors and controls network traffic in and out of a computer. Firewalls use **3 types of filtering mechanisms**:

Packet filtering: The data is transmitted through packets of information. Firewall is to analyses whether these packets of information are unwanted or suspected of malicious activity.

Proxy: A proxy Firewall is on a dedicated computer and can appear to be the recipient and responder, shielding the IP Address of the computer actually doing the communication.

Stateful Inspection: A firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. Stateful inspection is also known as dynamic packet filtering.

Firewall rules are requirements that can be customized. **Creating or disabling the filter rules can be done considering the following conditions**

IP Addresses

Suspicious IP addresses can be blocked.

Domain names

Permit only specified domain names to be accessible over your systems and servers, such as .edu or .mil.

Protocols

The access level of protocols like SMTP, IP, ICMP, FTP, UDP, Telnet or SNMP.

Ports

You can close entry ports that may be susceptible to hackers or malicious program and disconnect the ports of servers that have been connected to the Internet.
This helps user or the administrator to maintain a disciplined flow of data.

Keyword

A Firewall can check on the flow of data to determine if it matches keywords used to block unwanted information flowing in.

How Does a Firewall Work?

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).