**Firewall :(Implementation and importance )**

=> A firewall is a [network security](https://en.wikipedia.org/wiki/Network_security" \o "Network security) system that [monitors](https://en.wikipedia.org/wiki/Network_monitoring" \o "Network monitoring) and controls incoming and outgoing [network traffic](https://en.wikipedia.org/wiki/Network_traffic" \o "Network traffic) based on predetermined security rules. It typically establishes a barrier between a trusted internal network and untrustworthy external network, such as the [Internet](https://en.wikipedia.org/wiki/Internet" \o "Internet).

Using a wall of code a firewalls always acts as the first line of defense in [network security](https://learn.g2.com/network-security" \t "https://learn.g2.com/_blank) by virtually limiting the damage that a cyber attack can cause.It isolate your computer from the Internet while inspecting the data packet as it arrives on either side of the firewall. Then, it determines where it should be allowed to pass or be blocked.

The incoming traffic is analyzed based on predetermined rules and is carefully filtered from unsecured or malicious sources to prevent an attack. The firewall is responsible for checking the source and destination [IP address](https://learn.g2.com/ip-address" \t "https://learn.g2.com/_blank) on all packets, while filtering out packets sent from a malicious source.

In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely.

Firewall are basically of three types:- packet filtering , stateful, and application layer.

Packet filtering or stateless firewalls work by inspecting individual packets in isolation. As such, they are unaware of connection state and can only allow or deny packets based on individual packet headers.

Stateful firewalls are able to determine the connection state of packets, which makes them much more flexible than stateless firewalls. They work by collecting related packets until the connection state can be determined before any firewall rules are applied to the traffic.

Application firewalls go one step further by analyzing the data being transmitted, which allows network traffic to be matched against firewall rules that are specific to individual services or applications. These are also known as proxy-based firewalls.

In addition to firewall software, firewall functionality can also be provided by hardware devices, such as routers or firewall appliances to protect a PC or network system from malware threats or cyber attacks.