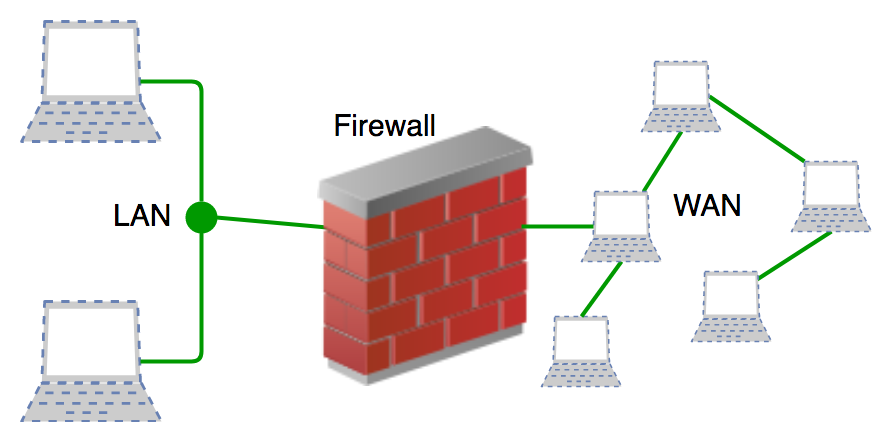
**What is Firewall?**

* A firewall is a type of network security device that filters incoming and outgoing network traffic with security policies that have previously been set up inside an organization.
* A firewall is essentially the wall that separates a private internal network from the open Internet at its very basic level.

1. **Accept:** allow the traffic
2. **Reject:** block the traffic but reply with an “unreachable error”
3. **Drop:**block the traffic with no reply

**Diagram:**



**1. Inter-Firewall**

**Definition:**

* **Inter-Firewall** refers to firewalls that sit **between two networks or systems** to control traffic.
* This firewall configuration typically separates **two networks** (e.g., LAN and WAN) or network zones (e.g., DMZ and internal networks).

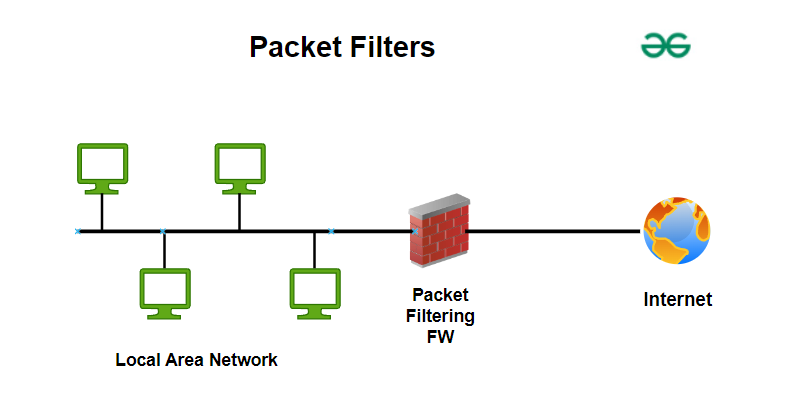
**Key Features:**

* Filters traffic **between two specific network segments**.
* Controls inbound and outbound traffic **within an enterprise network**.
* Implements security policies to **restrict unauthorized access** between zones.

**Example:**

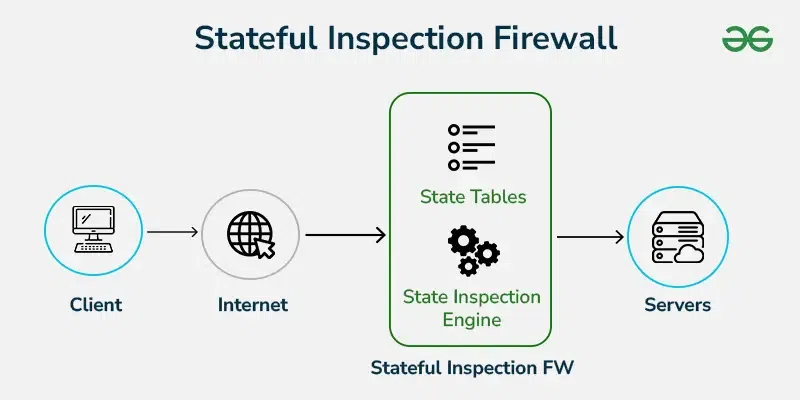
**Packet Filters**

It is a technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination [Internet Protocol](https://www.geeksforgeeks.org/what-is-an-ip-address/) (IP) addresses, protocols, and ports.  This firewall is also known as a static firewall.



**Stateful Inspection Firewalls**

* It is also a type of packet filtering that is used to control how data packets move through a firewall.
* It is also called dynamic packet filtering.



**2. Trans-Firewall**

**Definition:**

* **Trans-Firewall** refers to firewalls that control traffic **across multiple firewalls** or **through different security layers**.
* It typically involves **crossing multiple firewalls** as traffic moves through different network boundaries.

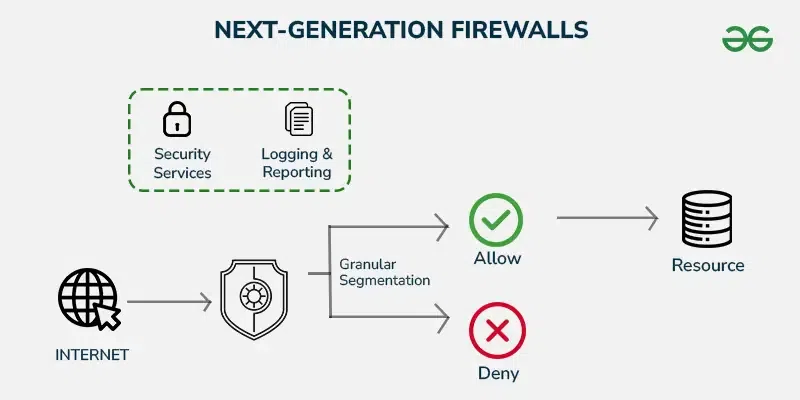
**Key Features:**

* Used in environments with **multi-layer security** (e.g., enterprise networks, cloud architectures).
* Controls traffic that transits across **different firewall instances or layers**.
* Provides an added layer of **granular security control** in multi-zone networks.

### ****Next-generation Firewalls :****

These firewalls are called intelligent firewalls.

These firewalls can perform all the tasks that are performed by the other types of firewalls, it includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered [threat](https://www.geeksforgeeks.org/difference-between-threat-and-attack/)intelligence.



**Cloud Firewall**

These are software-based, cloud-deployed network devices. This cloud-based firewall protects a private network from any unwanted access. Unlike traditional firewalls, a cloud firewall filters data at the cloud level.

**Advantages of Firewalls**

1. **Security:** Protects your network from unauthorized access and cyber threats.
2. **Traffic Monitoring:** Monitors incoming and outgoing network traffic.
3. **Access Control:** Restricts access to sensitive data and systems.
4. **Prevents Attacks:** Blocks malicious attacks like viruses, malware, and hackers.
5. **Network Segmentation:** Divides your network into secure segments, limiting the spread of attacks.

**Disadvantages of Firewalls:**

1. **Costly:** They can be expensive to buy and maintain.
2. **Slows Down Network:** Can make your network run slower.
3. **Complicated Setup:** Setting them up can be tricky and time-consuming.
4. **Not Foolproof:** Doesn't protect against all types of attacks.
5. **False Security:**  Might give you a false sense of being fully protected.

**Applications of Firewalls**

1. **Home Networks:** Protects personal devices and sensitive information.
2. **Business Networks:** Secures company data and prevents unauthorized access.
3. **Data Centers:** Safeguards large amounts of sensitive data and critical infrastructure.
4. **Cloud Services:** Ensures secure access to cloud-based applications and data.