Q3. What is Firewall and types of firewalls?

Ans.

**Firewalls** are the devices that are used to prevent private networks from unauthorized access. A Firewall is a security solution for the computers or devices that are connected to a network, they can be either in form of hardware as well as in form of software. It monitors and controls the incoming and outgoing traffic (the amount of data moving across a computer network at any given time ).

The major purpose of the network firewall is to protect an inner network by separating it from the outer network. Inner Network can be simply called a network created inside an organization and a network that is not in the range of inner network can be considered as Outer Network.

**Types of Network Firewall :**

1. **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 (IP) addresses, protocols, and ports. This firewall is also known as a static firewall.
2. **Stateful Inspection Firewalls –**  
    It is also a type of packet filtering which is used to control how data packets move through a firewall. It is also called dynamic packet filtering. These firewalls can inspect that if the packet belongs to a particular session or not. It only permits communication if and only if, the session is perfectly established between two endpoints else it will block the communication.
3. **Application Layer Firewalls –**  
    These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.
4. **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 that we learned previously but on top of that, it includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.
5. **Circuit-level gateways –**  
   A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security and works between an Open Systems Interconnection (OSI) network model’s transport and application layers such as the session layer.
6. **Software Firewall –**  
   The software firewall is a type of computer software that runs on our computers. It protects our system from any external attacks such as unauthorized access, malicious attacks, etc. by notifying us about the danger that can occur if we open a particular mail or if we try to open a website that is not secure.
7. **Hardware Firewall –**  
    A hardware firewall is a physical appliance that is deployed to enforce a network boundary. All network links crossing this boundary pass-through this firewall, which enables it to perform an inspection of both inbound and outbound network traffic and enforce access controls and other security policies.
8. **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.