11. What is Firewall? Explain its various types with advantages and disadvantages of each.
Ans.
A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.
There are five key types of firewalls that use different mechanisms to identify and filter out malicious traffic:
1. packet filtering firewall
2. circuit-level gateway
3. application-level gateway (aka proxy firewall)
4. stateful inspection firewall
5. next-generation firewall (NGFW)

1. Packet Filtering
Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets; rather they compare each packet received to a set of established criteria. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.
Advantages:
- Simple and efficient at filtering traffic based on predefined rules.
- Minimal impact on network performance.

Disadvantages:
- Limited ability to inspect traffic beyond the packet header, making it vulnerable to certain attacks.
- Complex rules can be difficult to manage and maintain.

2. Circuit Level Gateway
Using another relatively quick way to identify malicious content, circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered trusted.
Advantages:
- Only processes requested transactions; all other traffic is rejected
- Easy to set up and manage

3. Application Level Gateway
This kind of device -- technically a proxy and sometimes referred to as a proxy firewall -- functions as the only entry point to and exit point from the network. Application-level gateways filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by other characteristics, such as the HTTP request string.
Advantages:
- Offers deep packet inspection at the application layer, allowing for granular control.
- Can identify and block specific applications and services.

Disadvantages:
- Can be resource-intensive and may impact network performance.
- Complex to configure and maintain.

4. Stateful inspection

State-aware devices not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.

Advantages:

- Examines the state of active connections, providing better security.
- Can make decisions based on the state of a connection (e.g., allowing response packets for established connections).

Disadvantages:

- More resource-intensive compared to packet filtering firewalls.
- Still limited in its ability to inspect application-layer content.

5. Next Generation

A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection (DPI), as well as other network security systems, such as an IDS/IPS, malware filtering and antivirus.

Advantages:

- Combines traditional firewall capabilities with advanced features like intrusion prevention, antivirus, and application awareness.
- Provides more comprehensive security in a single device.

Disadvantages:

- Can be costly, both in terms of hardware and licensing.
- May require specialized expertise to configure and manage effectively.