**8.1 Firewalls:**

Firewalls can be either physical or logical, either hardware or software. Hardware provides more performance at cost, and software are better to protect individual hosts.

Packet filtering firewalls examine packets to find its destination and contents, and will accept or reject based on received NIC, its direction. Uses ACLs to control traffic as it moves through the network. Offers high performance and low overhead as it only analyzes the first part of a packet.

Circuit level gateways make packet decisions based on Session layer. Application level firewalls analyze packets sent by applications themselves, and can limit access to HTTP, URLs requested, users, or groups. These firewalls are also known as proxy servers, that sit between internet and the clients in to monitor and manage connections made by clients. Reverse proxy servers work to accept information from the client, and direct them to the servers that are requested; they work in conjunction with servers, whereas proxy servers work with clients.

UTM(Unified Threat Management) devices put many different services like Firewalls, ad-blocking, spam-guard, VPN, load-balancing as well as many other security services. This creates a single point of failure, but also allows for easier management of security for network administration.