**Week 4: Firewalls, IDS, and IPS**

**Objective:** Set up and manage network defense mechanisms.

**Task#05:** **Write a short explanation of how a Proxy Server and Reverse Proxy work with examples.**

**Solution:**

A **Proxy Server** (or Forward Proxy) acts as an intermediary for clients requesting resources from other servers. It sits between a client and the internet. When a client makes a request, it goes to the proxy, which then forwards the request to the destination server. The response then comes back to the proxy, which forwards it to the client.

* **Example:** Imagine a company network where all employee internet requests first go through a proxy server. This proxy can then filter content, cache frequently accessed websites to speed up browsing, or log internet activity. The websites you visit only see the proxy's IP address, not your individual computer's IP.

A **Reverse Proxy** acts as an intermediary for servers, protecting and distributing requests coming from clients on the internet. It sits in front of one or more web servers. When a client makes a request to a website, the request goes to the reverse proxy first, which then forwards it to the appropriate backend web server. The response comes back through the reverse proxy to the client.

* **Example:** A large e-commerce website might use a reverse proxy. When you visit their site, your request hits the reverse proxy. The reverse proxy can then distribute the load across multiple backend web servers (load balancing), provide SSL termination (handling encryption), or serve cached content directly, all while hiding the actual internal server architecture from you.