**Proxy Servers**

**Introduction**

A proxy server acts as an intermediary between a client (such as a web browser) and a target server (like a web server). The client sends requests to the proxy server, which then forwards those requests to the destination server. Once the destination server responds, the proxy relays the response back to the client. Proxies are used to perform tasks like caching, content filtering, security, anonymity, and traffic routing.

**Forward Proxy**

A forward proxy is placed between the **client** and the **internet**. It forwards client requests to the target server on behalf of the client. The use of forward proxy are as follows

**Content Filtering**

A forward proxy can block access to specified websites or content, helping organizations enforce browsing policies and restrict access to inappropriate material.

**Anonymity and Privacy**

By masking the client's IP address, a forward proxy enables users to browse the internet anonymously, enhancing privacy and protecting identity.

**Network Security**

A forward proxy filters outgoing traffic to prevent malicious sites from accessing the internal network, offering an extra layer of protection against cyber threats.

**Bypassing Geo-restrictions**

Forward proxies enable users to access region-blocked content by routing traffic through a server in a different geographic location.

**Caching**

A forward proxy can store copies of frequently accessed resources (like web pages, images, or videos) locally. When another user requests the same resource, the proxy can serve the cached version instead of fetching it from the internet again, thus saving bandwidth and improving response times.

### **Logging User Activity**

### Forward proxies can track and log every request made by users. This includes recording details like IP addresses, websites visited, timestamps, and other metadata.

**Reverse Proxy**

A reverse proxy is placed in front of one or more **web servers** and handles requests on their behalf, forwarding client requests to the appropriate server. The client is unaware of the existence of the backend servers. The use of reverse proxy are as follows

**Load Balancing**

A reverse proxy distributes incoming traffic across multiple servers, ensuring no single server is overwhelmed, which improves performance and reliability of websites or applications.

**Security and Anonymity**

A reverse proxy hides the identity and internal structure of the backend servers, providing an additional layer of security by protecting the servers from direct exposure to the internet.

**SSL Termination**

A reverse proxy can handle SSL/TLS encryption and decryption, offloading this resource-intensive process from backend servers to improve their performance.

**Caching**

A reverse proxy can cache content, such as web pages or images, to reduce server load and speed up response times for users accessing the same resources.

**Traffic Distribution and Optimization**

A reverse proxy can direct traffic based on different criteria (e.g., server load, user location), optimizing resource utilization and ensuring better user experience.