Proxies

Ram is ill and decides not to go to college today. But it is a very important class and the attendance will be affecting the final grade. Ram thinks of an idea and asks his friend Shyam to mark Ram's attendance by signing against Ram's name on the attendance sheet. Shyam does the same. When the teacher asks the students to sign against their names to mark the attendance, Shyam signs against his and Ram's name according to the plan. This is an example of proxy and Shyam is acting as a proxy here. Because Shyam acted like Ram and signed on his behalf of him.

Definition:

The proxy server provides a gateway between the user and the Internet. The server is called a "proxy" because it runs between the end-user and the websites you visit online. We use an IP address when your computer connects to the Internet.

A proxy server, also known as a "proxy" or "application-level gateway", acts as a local network (for example, all computers in a business or building) and a large network (for example, the Internet.

Types of Proxy:

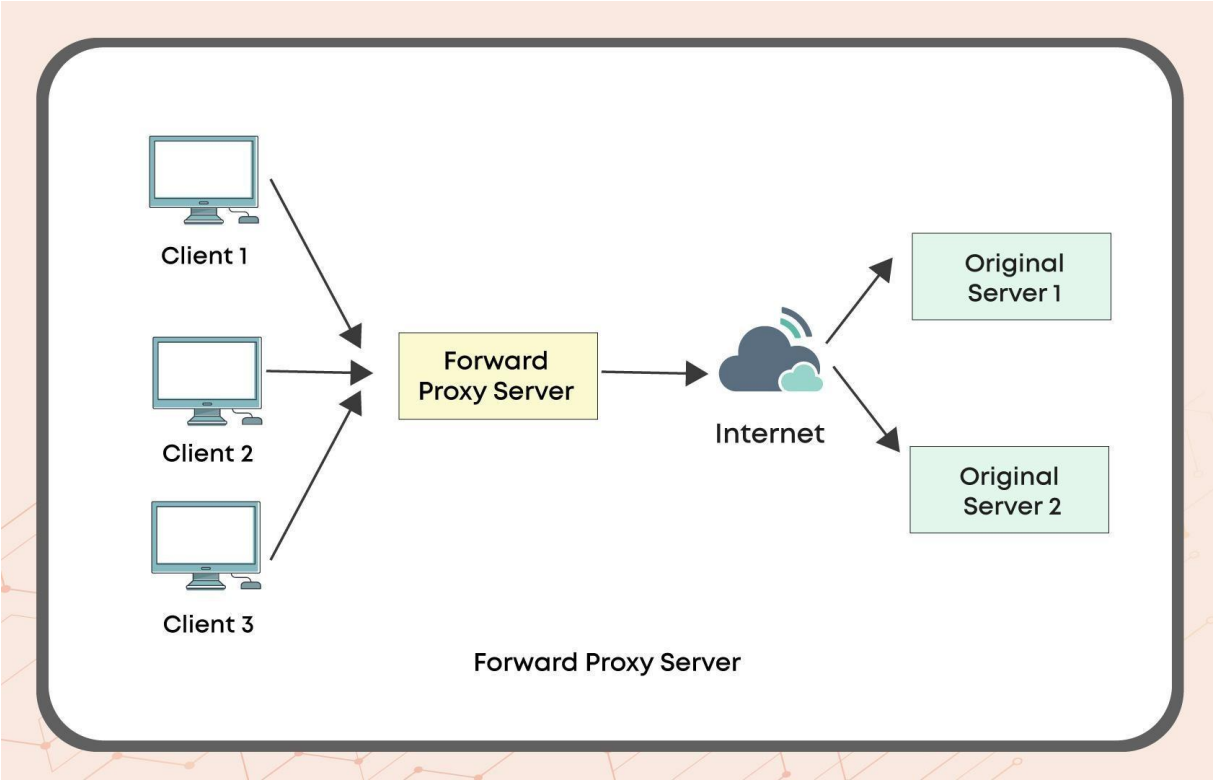
1. **Forward Proxy:** Forward proxy is the most common form of proxy server, which is generally used to pass requests from an isolated private network to the Internet through a firewall. Using a forward proxy, you can deny or allow requests from isolated networks or intranets to pass through the firewall. When one of these clients tries to connect to a file transfer server on the Internet, its request must first go through a forwarding proxy.

   According to the forwarding proxy settings, the request can be allowed or denied. If allowed, the request will be forwarded to the firewall and then to the file transfer server. From the perspective of the file transfer server, it is the proxy server that makes the request, not the client. Therefore, when the server responds, it directs its response to the proxy. But when the forwarding agent receives a response, it recognizes it as a response to a previous request. It then sends the response to the requesting client. Because the proxy server can track requests, responses, their origin and destination, different clients can send multiple requests to different servers through a forwarding proxy, and

the proxy will act as an intermediary for all these requests. Likewise, some requests will be allowed, while other requests will be denied.

Functions of forwarding proxy:

1. To provide protection to the client by filtering the outgoing requests and incoming responses
2. Enforcing “terms of use” of a network
3. Caching external site content for a better user experience



2. **Reverse Proxy:** Reverse proxies are servers located in front of web servers and forward client requests (such as web browsers) to these web servers. Reverse proxies are often used to help improve security, performance, and reliability.

   The reverse proxy server is present before one or more web servers, intercepting requests from clients. This is different from the forward proxy, which is located in front of the client. With a reverse proxy, when a client sends a request to the origin server of the website, these requests will be intercepted by the reverse proxy server at the edge of the network. Then the

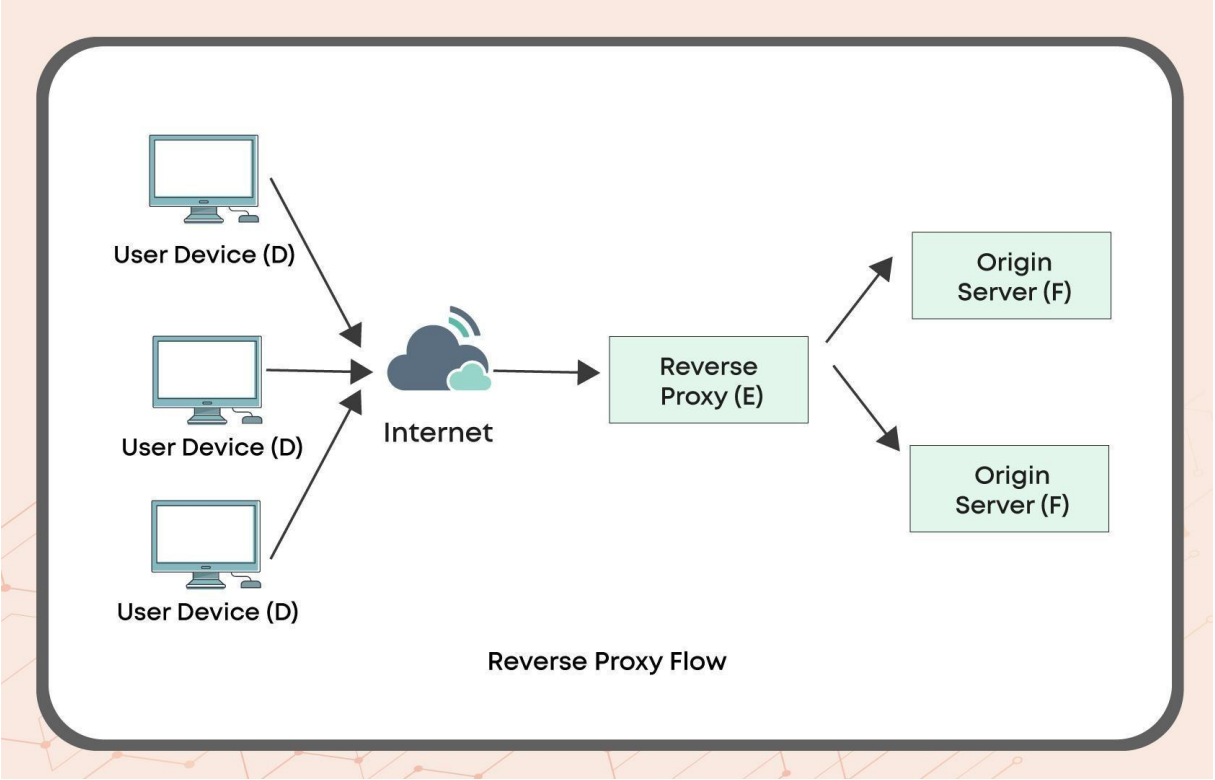
the reverse proxy server will send the request and receive the response from the original server.

The difference between a direct proxy and a reverse proxy is subtle but important. A simplified way of summarizing is to say that the forwarding proxy is in front of the client and to ensure that no origin server communicates directly with that particular client. On the other hand, the reverse proxy is located in front of the actual server to make sure that there exists no communication between the client with the actual server.

In the case of the content delivery network (CDN), requests are handled using Reverse proxy. Reverse proxies are servers located in front of web servers and forward client requests (such as web browsers) to these web servers. Reverse proxies are often used to help improve security, performance, and reliability. CDN uses a reverse proxy to establish secure network connections and provide load balancing for the servers.

Functions of Reverse Proxy:

1. Provide load balancing for the server
2. Prevention from malicious attacks such as Denial of Services
3. Allows administrators to swap the backend servers without disturbing the traffic.



Applications of Reverse Proxy:

API Gateway:

API Gateway is an API management tool located between the client and the collection of back-end services. The API gateway is implemented using the reverse proxy to accept all application programming interface (API) calls, and add the various services required to implement them and return the appropriate results. For the clients, an API gateway can hide the details of how the application is divided into microservices.

Functions of API Gateway:

1. It can authenticate an incoming API call
2. API Gateway can function as a Load Balancer(equal distribution of load) and keep track of requests sent to different nodes of the network
3. API Gateway can also behave as a single point of entry for the external API