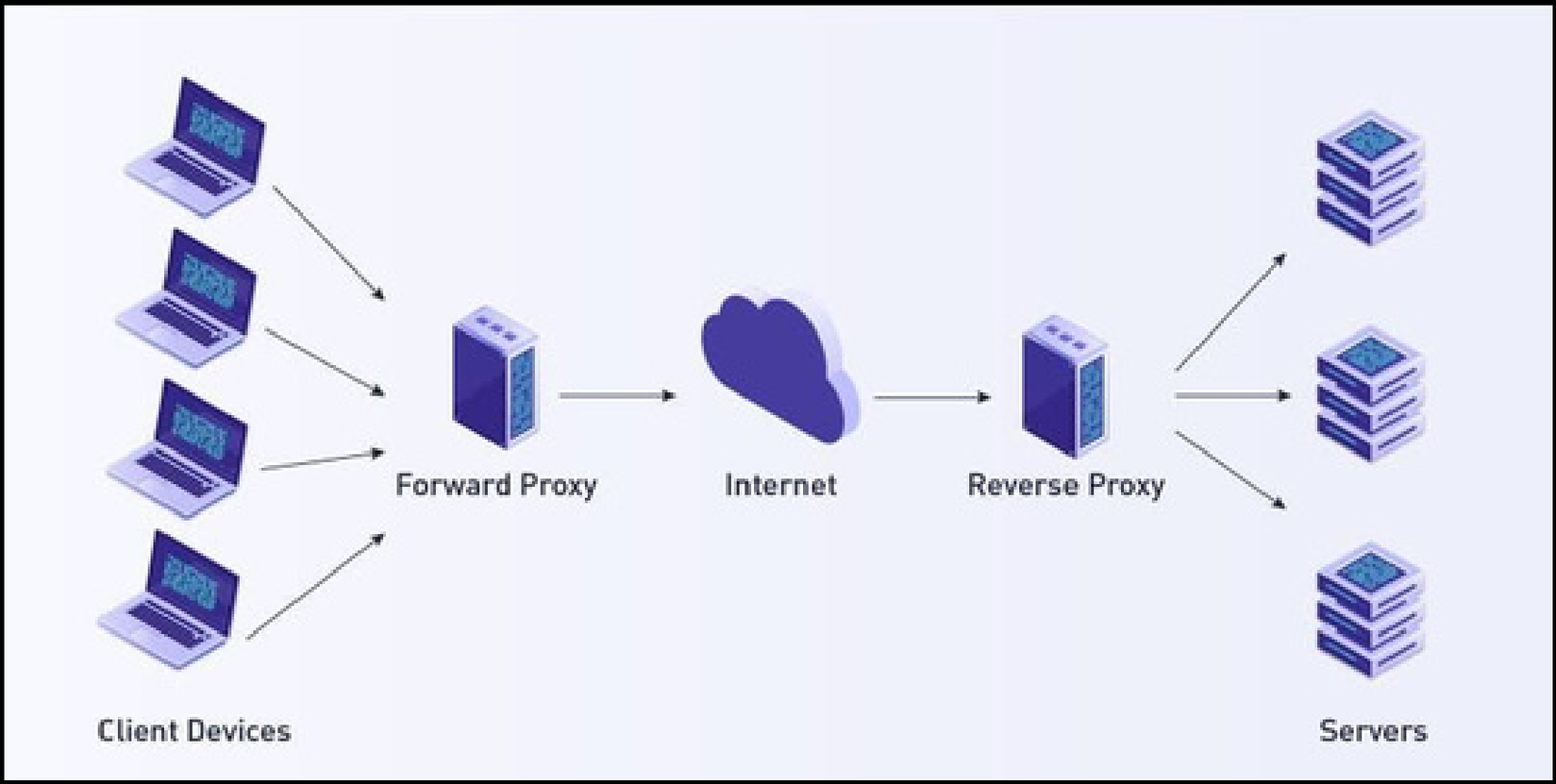
Forward Proxy Vs Reverse Proxy Vs Transparent Proxy Vs Load Balancing Vs VPN

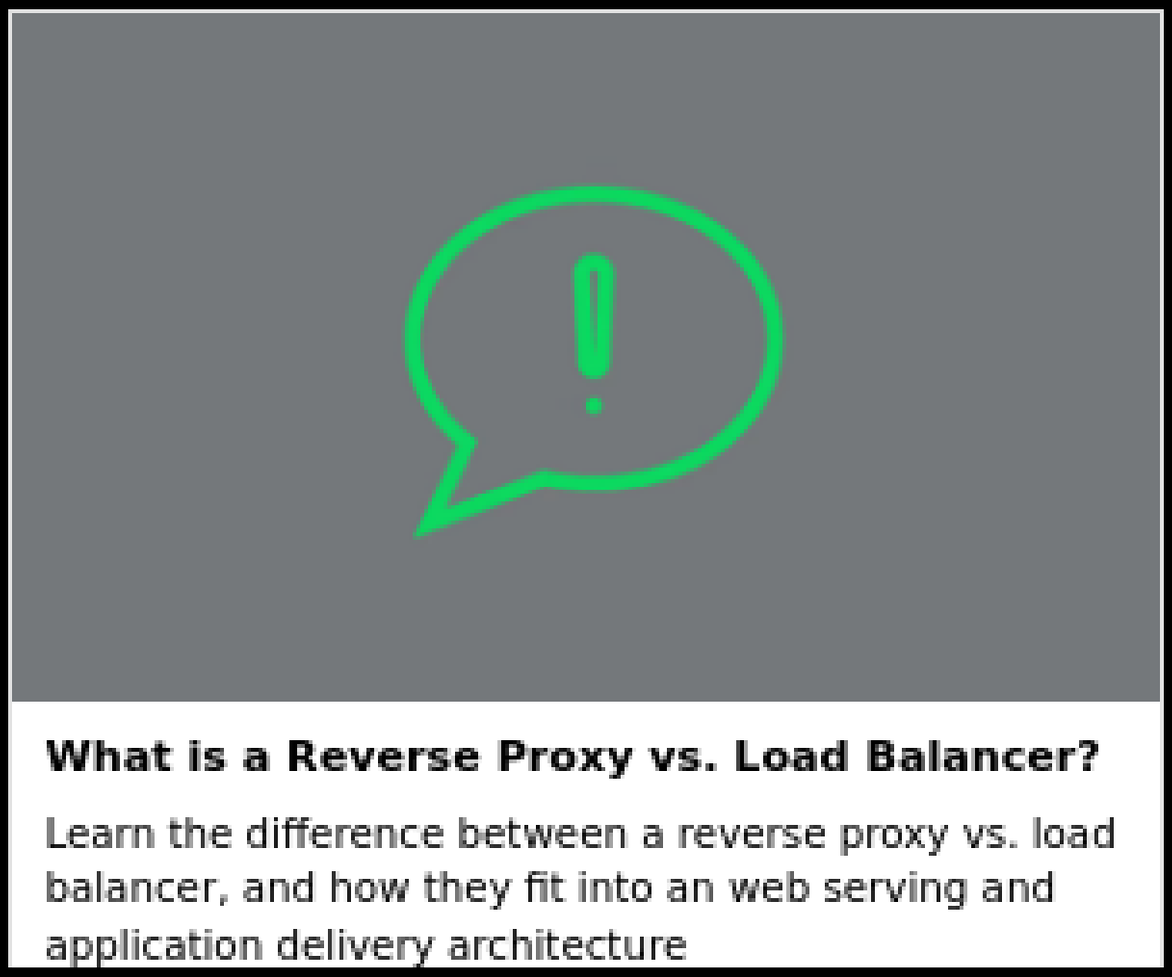


A proxy server, sometimes referred to as a forward proxy, is a server that routes traffic between client(s) and another system, usually external to the network. By doing so, it can regulate traffic according to preset policies, convert and mask client IP addresses, enforce security protocols, and block unknown traffic.

A reverse proxy is a type of proxy server. Unlike a traditional proxy server, which is used to protect clients, a reverse proxy is used to protect servers. A reverse proxy is a server that accepts a request from a client, forwards the request to another one of many other servers, and returns the results from the server that actually processed the request to the client as if the proxy server had processed the request itself. The client only communicates directly with the reverse proxy server and it does not know that some other server actually processed its request.

The key difference between a reverse proxy and a forward proxy is that a forward proxy enables computers isolated on a private network to connect to the public internet, while a reverse proxy enables computers on the internet to access a private subnet.

A load balancer distributes incoming client requests among a group of servers, in each case returning the response from the selected server to the appropriate client.



A reverse proxy accepts a request from a client, forwards it to a server that can fulfill it, and returns the server’s response to the client.

A load balancer distributes incoming client requests among a group of servers, in each case returning the response from the selected server to the appropriate client.

But they sound pretty similar, right? Both types of application sit between clients and servers, accepting requests from the former and delivering responses from the latter.

Load balancers are most commonly deployed when a site needs multiple servers because the volume of requests is too much for a single server to handle efficiently. Deploying multiple servers also eliminates a single point of failure, making the website more reliable. Most commonly, the servers all host the same content, and the load balancer's job is to distribute the workload in a way that makes the best use of each server's capacity, prevents overload on any server, and results in the fastest possible response to the client.

Whereas deploying a load balancer makes sense only when you have multiple servers, it often makes sense to deploy a reverse proxy even with just one web server or application server

Making use of reverse proxy has following advantages:

- **Increased security :** Many reverse proxy servers include features that help protect backend servers from distributed denial-of-service (DDoS) attacks, for example by rejecting traffic from particular client IP addresses (denylisting), or limiting the number of connections accepted from each client.
- **Increased scalability and flexibility :** Because clients see only the reverse proxy's IP address, you are free to change the configuration of your backend infrastructure. This is particularly useful In a load-balanced environment, where you can scale the number of servers up and down to match fluctuations in traffic volume.
- **Compression :** Compressing server responses before returning them to the client (for instance, with gzip) reduces the amount of bandwidth they require, which speeds their transit over the network.
- **SSL termination** : By decrypting incoming requests and encrypting server responses, the reverse proxy frees up resources on backend servers which they can then devote to their main purpose, serving content.
- **Caching :** Before returning the backend server's response to the client, the reverse proxy stores a copy of it locally. When the client (or any client) makes the same request, the reverse proxy can provide the response itself from the cache instead of forwarding the request to the backend server.

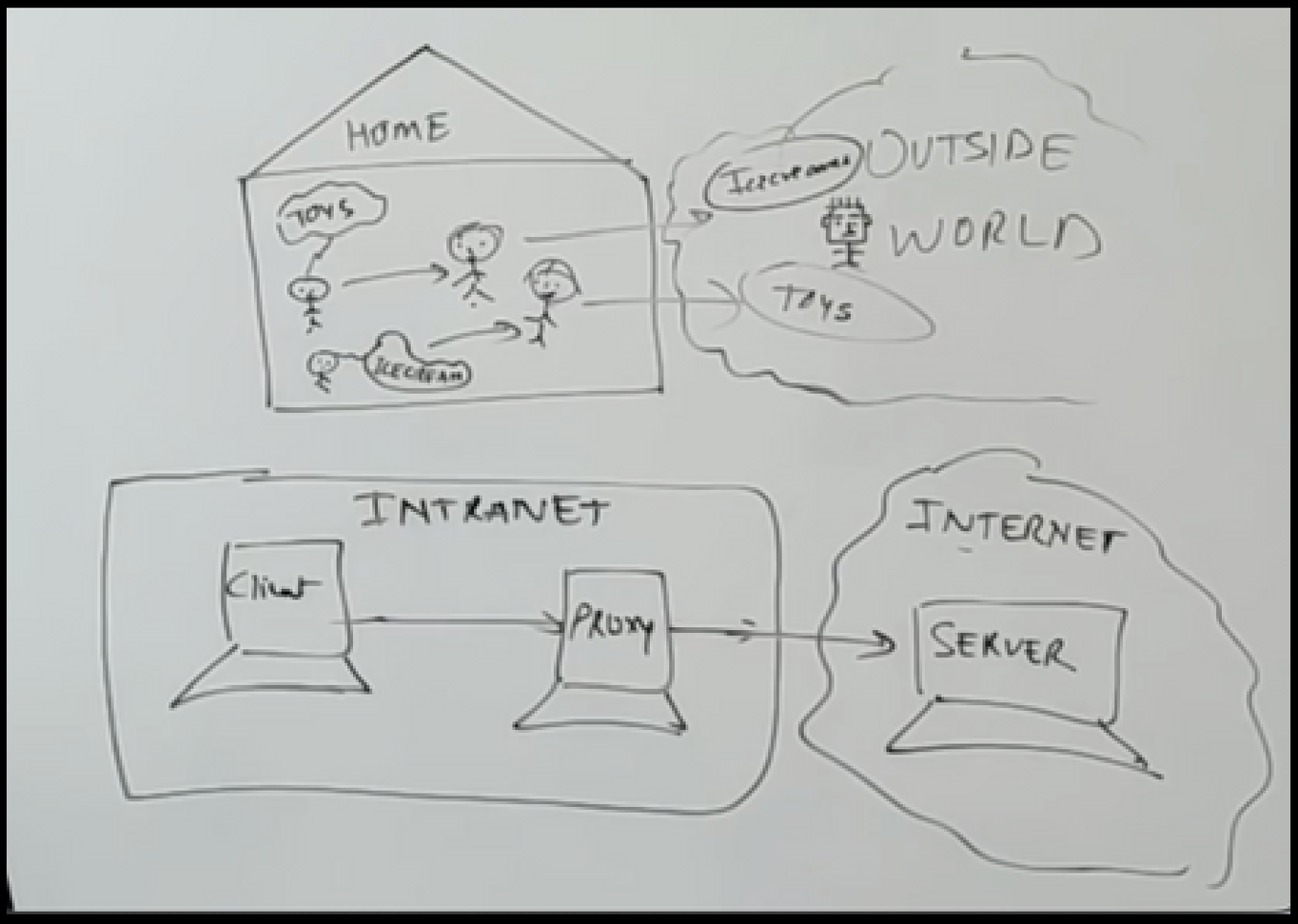
Real Life Examples :

In our childhood, our parents used to fulfil the requirements.

Proxy is an act which someone else does on your behalf.

In U.K. there's a concept called proxy voting. If you can't vote someone else can go and vote on your behalf.

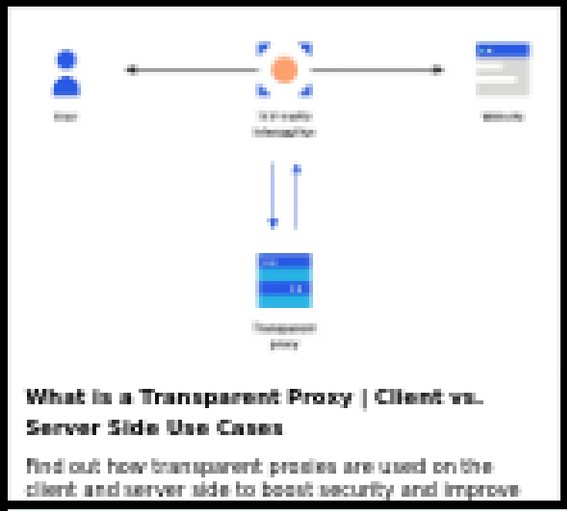
In college also , students do proxy attendance.



Forward Proxy acts as a filter or firewall. It used for better management. It also helps for caching and security. We can store static page at the proxy server. We don't need to hit the internet (n/w) again. It saves us the bandwidth.
Reverse proxy can act as a load balancer. Server IP's will be masked

VPNs are Virtual Private Servers that encrypt all of a users' web activity and device IP addresses. Typically, they come in the form of either an app or a browser extension.

The main difference between a VPN proxy and a VPN is encryption. VPNs hide not only your private IP address but all your web activity, such as the websites you visit, using encryption. Proxy servers, on the other hand, will only change your IP address, but they won't encrypt your online activities.



A **transparent proxy**, also known as an **inline proxy, intercepting proxy** or **forced proxy**, is a server that intercepts the connection between an end-user or device and the internet. It is called "transparent" because it does so without modifying requests and responses. Squid Transparent Proxy Server is a popular open source transparent proxy tool.

Uses for Transparent Proxy on Client Side Authentication Content Filtering Gateway Proxies Traffic Monitoring Caching

Feature	Proxy	VPN
Cost	Usually free	Usually paid
Number of uses	1	Unlimited
Encrypt IP address	Yes	Yes
Encrypt web activity	No	Yes
Sells user data	Yes	No
Coverage	1 website or app	All websites and apps
Compatible with streaming and gaming	Yes	Yes
Can be used to bypass geo-restrictions	Yes	Yes
Slows down browsing speeds	Yes	Yes