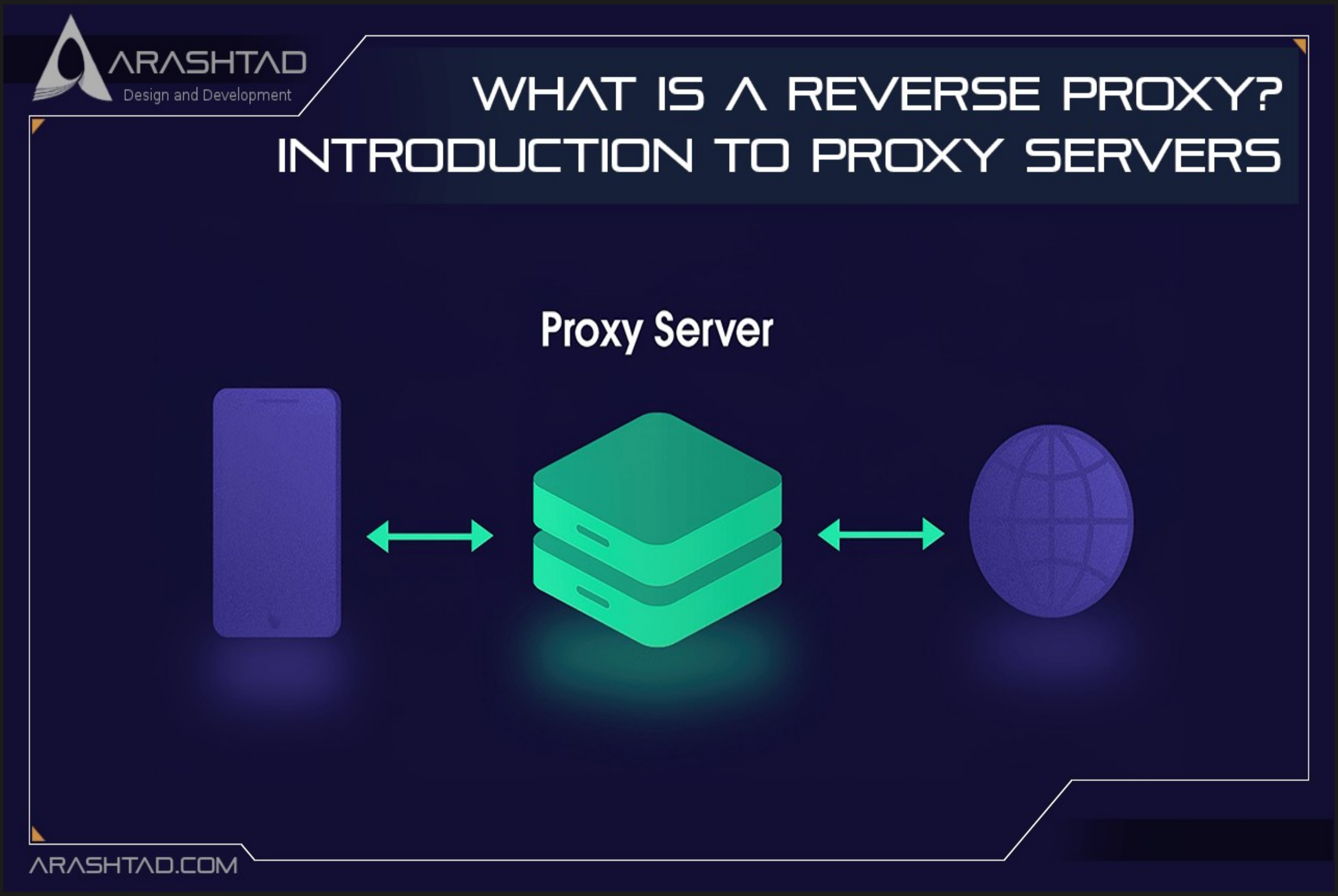
Title	WHAT IS A REVERSE PROXY? INTRODUCTION TO PROXY SERVERS?
Description	Designing 3D web pages using Three.js
Date	Aug 2022
Author	Arashtad
Author URI	https://arashtad.com

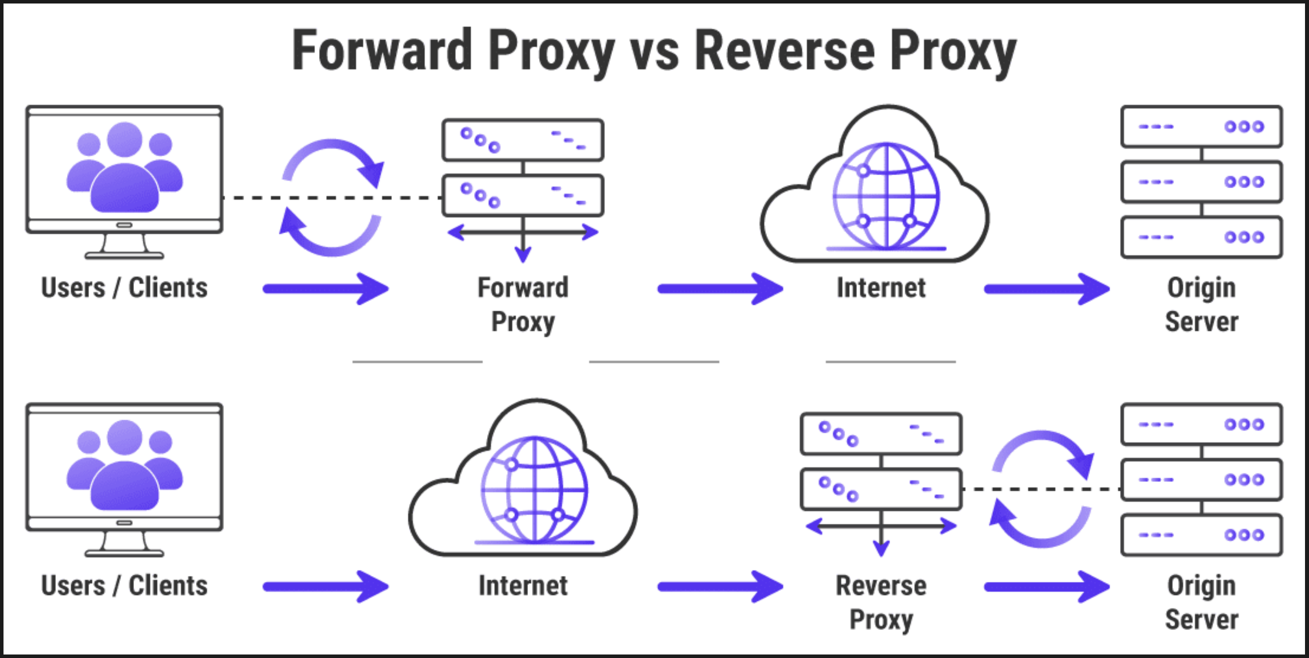


A reverse proxy is a server that is placed on the server side and directs the requests from the clients to the main servers. In the large databases we usually have multiple severs that need a kind of a management to direct the coming requests to the appropriate server that contains the proper data for the client’s request. Reverse proxies are typically implemented to help increase security, performance and reliability.

In this article we will first see what a proxy server is and then take a look at the different kinds of proxy servers. Afterward, we will focus on the reverse proxy, its pros and cons and see when and and where we need to use the proxy servers. If you are new to IT and want to learn more about the web servers and different articles on these subjects, feel free to take a look at our blog and read the different documents that we have provided about the web servers.

WHAT IS A PROXY SERVER?

Often times, when we talk about a proxy server, we are referring to the forward proxy server. A forward proxy also known as web proxy is placed in front of a group of a client machines. When those computers make requests to sites and services on the Internet, the proxy server intercepts those requests and then communicates with web servers on behalf of those clients, like a middleman. Below, you can see the forward proxy in comparison with the reverse proxy.



In a standard Internet communication, the client computer would reach out directly to the origin server, meaning that the client sends requests to the origin server and the origin server responds to the client. When a forward proxy is in place, The client will instead send requests to it (the forward proxy), which will then forward the request to the origin server. The origin server will then send a response to the forward proxy, which will forward the response back to the client's computer.

Why would anyone add this extra middleman to their Internet activity? There are a few reasons one might want to use a forward proxy:

1. To avoid governmental or institutional browsing restrictions: Some governments, schools, and other organizations use firewalls to give their users access to a limited version of the Internet. A forward proxy can be used to get around these restrictions,

as they let the user connect to the proxy rather than directly to the sites they are visiting.

2. For filtering certain contents: Conversely, there are circumstances in which proxies are set up to block a group of users from accessing to contents or sites. For example, a school network might be configured to connect to the web through a proxy which enables content filtering rules, refusing to forward responses from Facebook and other social media sites.

3. To be anonymous online: There are times when users want to protect their identity. In some cases, regular Internet users simply desire increased anonymity online, but in other cases, Internet users live in places where the government can impose serious consequences to political dissidents. Criticizing the government in a web forum or on social media can lead to fines or imprisonment for these users. If one of these dissidents uses a forward proxy to connect to a website where they post politically sensitive comments, the IP address used to post the comments will be harder to trace back to the dissident. Only the IP address of the proxy server will be visible.

HOW DOES A REVERSE PROXY WORK?

As mentioned earlier at the beginning of the article, the reverse proxy server is placed on the server side and intercepts the requests from the clients. This is different from a forward proxy, where the proxy sits in front of the clients. With a reverse proxy, when clients send requests to the origin server of a website, those requests are intercepted at the network edge by the reverse proxy server. The reverse proxy server will then send requests to and receive responses from the origin server.

If we want to compare the forward proxy server with the reverse proxy server, we should put it this way; a forward proxy sits in front of a client and ensures that no origin server ever communicates directly with that specific client. On the other hand, a reverse proxy sits in front of an origin server and ensures that no client ever communicates directly with that origin server.

WHY DO WE USE THE REVERSE PROXY?

There are multiple reasons as to why we use the reverse proxy server:

1. Load balancing and Global Server Load Balancing (GSLB): A website with millions of users everyday from all around the globe a certain country, may not be able to

handle all of its incoming site traffic with a single origin server. Instead, the site can be distributed among a pool of different servers, all handling requests for the same site. In this case, a reverse proxy can provide a load balancing solution which will distribute the incoming traffic evenly among the different servers to prevent any single server from becoming overloaded. In the event that a server fails completely, other servers can step up to handle the traffic.

2. Security: With a reverse proxy in front of the origin servers, a website or a web service will never have to reveal the IP address of the its origin web servers and this can protect it from the attackers who want to leverage a targeted attack against them, such as a DDoS attack. Instead the attackers will only be able to target the reverse proxy, such as Cloudflare's CDN, which will have tighter security and more resources to fend off a cyber attack.

3. SSL encryption: Encrypting and decrypting SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) communications for each client could be computationally inefficient and cost effective if done with an origin server. A reverse proxy can be configured to decrypt all incoming requests and encrypt all outgoing responses, freeing up valuable resources on the origin server.

4. caching: Caching is the process of storing copies of files in a cache, or temporary storage location, so that they can be accessed more quickly. A reverse proxy can also cache content, resulting in faster performance. For instance, if a user in London visits a reverse-proxied website with web servers in Silicon valley, the user might actually connect to a local reverse proxy server in London, which will then have to communicate with an origin server in Silicon valley. The proxy server can then cache (or temporarily save) the response data. Subsequent London users who browse the site will then get the locally cached version from the London reverse proxy server, resulting in much faster performance.

CONCLUSION

In this article, we have got familiar with the two types of the proxy servers including the forward and reverse proxy servers. The proxy servers are mostly referred to the forward type. However, the reverse proxy servers are also very common these days considering that we have so many websites with many users and a high traffic. Not to mention that so many important web services and websites need a security layer for encryption and decryption. Moreover, caching makes the use of the origin servers much more efficient using the reverse proxy servers.

ARASHTAD TEAM

We have a strong 3D modeling and 3D web development team in Arashtad group, ready to design high quality productions in case of 3D websites, 3D games and metaverses. We are also an experienced team in Blockchain development. If you have an idea for a project like this, please don't hesitate to contact us on Arashtad.com. Also, you can see some samples of our previous projects at https://demo.arashtad.com.