Proxy Server

Proxy server refers to a server that acts as an intermediary between the request made by clients, and a particular server for some services or requests for some resources. There are different types of proxy servers available that are put into use according to the purpose of a request made by the clients to the servers. The basic purpose of Proxy servers is to protect the direct connection of Internet clients and internet resources. The proxy server also prevents the identification of the client's IP address when the client makes any request is made to any other servers.

- **Internet Client and Internet resources:** For internet clients, Proxy servers also act as a shield for an internal network against the request coming from a client to access the data stored on the server. It makes the original IP address of the node remains hidden while accessing data from that server.
- **Protects true host identity:** In this method, outgoing traffic appears to come from the proxy server rather than internet navigation. It must be configured to the specific application such as HTTPs or FTP. For example, organizations can use a proxy to observe the traffic of its employees to get the work efficiently done. It can also be used to keep a check on any kind of highly confidential data leakage. Some can also use it to increase their websites rank.

Need of Private Proxy:

1. **Defeat Hackers:** To protect organizations data from malicious use, passwords are used and different architects are setup, but still, there may be a possibility that this information can be hacked in case the IP address is accessible easily. To prevent such kind of misuse of Data Proxy servers are set up to prevent tracking of original IP addresses instead data is shown to come from a different IP address.
2. **Filtering of Content:** By caching the content of the websites, Proxy helps in fast access to the data that has been accessed very often.

3. **Examine Packet headers and Payloads:** Payloads and packet headers of the requests made by the user nodes in the internal server to access to social websites can be easily tracked and restricted.
4. **To control internet usage of employees and children:** In this, the Proxy server is used to control and monitor how their employees or kids use the internet. Organizations use it, to deny access to a specific website and instead redirecting you with a nice note asking you to refrain from looking at said sites on the company network.
5. **Bandwidth savings and improved speeds:** Proxy helps organizations to get better overall network performance with a good proxy server.
6. **Privacy Benefits:** Proxy servers are used to browse the internet more privately. It will change the IP address and identify the information the web request contains.
7. **Security:** Proxy server is used to encrypt your web requests to keep prying eyes from reading your transactions as it provides top-level security.

Types of Proxy Server

1. **Reverse Proxy Server:** The job of a reverse proxy server to listen to the request made by the client and redirect to the particular web server which is present on different servers. Example – Listen for TCP port 80 website connections which are normally placed in a demilitarized zone (DMZ) zone for publicly accessible services but it also protects the true identity of the host. Moreover, it is transparent to external users as external users will not be able to identify the actual number of internal servers. So, it is the prime duty of reverse proxy to redirect the flow depending upon the configurations of internal servers. The request that is made to pass through the private network protected by firewalls will need a proxy server that is not abiding by any of the local policies. Such types of requests from the clients are completed using reverse proxy servers. This is also used to restrict the access of the clients to the confidential data residing on the particular servers.
2. **Web Proxy Server:** Web Proxy forwards the HTTP requests, only URL is passed instead of a path. The request is sent to particular the proxy server responds. Examples, Apache, HAP Proxy.

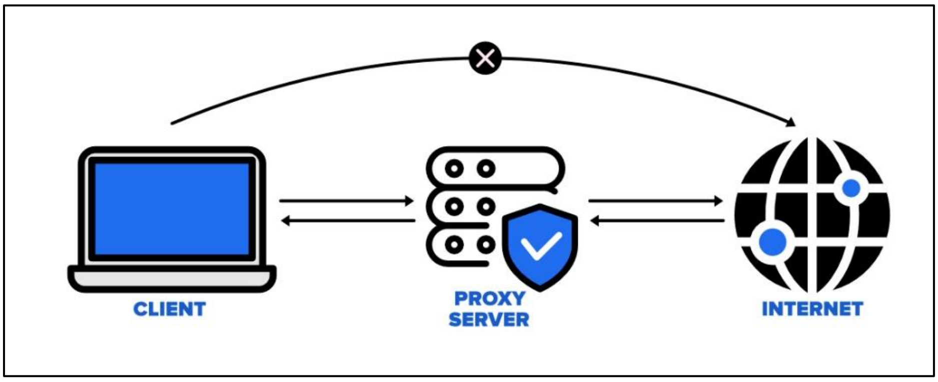
3. **Anonymous Proxy Server:** This type of proxy server does not make an original IP address instead these servers are detectable still provides rational anonymity to the client device.
4. **Highly Anonymity Proxy:** This proxy server does not allow the original IP address and it as a proxy server to be detected.
5. **Transparent Proxy:** This type of proxy server is unable to provide any anonymity to the client, instead, the original IP address can be easily detected using this proxy. But it is put into use to act as a cache for the websites. A transparent proxy when combined with gateway results in a proxy server where the connection requests are sent by the client , then IP are redirected. Redirection will occurs without the client IP address configuration. HTTP headers present on the server-side can easily detect its redirection .
6. **CGI Proxy:** CGI proxy server developed to make the websites more accessible. It accepts the requests to target URLs using a web form and after processing its result will be returned to the web browser. It is less popular due to some privacy policies like VPNs but it still receives a lot of requests also. Its usage got reduced due to excessive traffic that can be caused to the website after passing the local filtration and thus leads to damage to the organization.
7. **Suffix Proxy:** Suffix proxy server basically appends the name of the proxy to the URL. This type of proxy doesn't preserve any higher level of anonymity. It is used for bypassing the web filters. It is easy to use and can be easily implemented but is used less due to the more number of web filter present in it.
8. **Distorting Proxy:** Proxy servers are preferred to generate an incorrect original IP address of clients once being detected as a proxy server. To maintain the confidentiality of the Client IP address HTTP headers are used.
9. **Tor Onion Proxy:** This server aims at online anonymity to the user's personal information. It is used to route the traffic through various networks present worldwide to arise difficulty in tracking the users' address and prevent the attack of any anonymous activities. It makes it difficult for any person who is trying to track the original address. In this type of routing, the information is encrypted in a multi-folds layer. At the destination, each layer

is decrypted one by one to prevent the information to scramble and receive original content. This software is open-source and free of cost to use.

10. **12P Anonymous Proxy:** It uses encryption to hide all the communications at various levels. This encrypted data is then relayed through various network routers present at different locations and thus I2P is a fully distributed proxy. This software is free of cost and open source to use, It also resists the censorship.
11. **DNS Proxy:** DNS proxy take requests in the form of DNS queries and forward them to the Domain server where it can also be cached, moreover flow of request can also be redirected.

Working of Proxy Server

Every computer has its unique IP address which it uses to communicate with another node. Similarly, the proxy server has its IP address that your computer knows. When a web request is sent, your request goes to the proxy server first. The Proxy sends a request on your behalf to the internet and then collect the data and make it available to you. A proxy can change your IP address So, the webserver will be unable to fetch your location in the world. It protects data from getting hacked too. Moreover, it can block some web pages also



Disadvantages of Proxy Server

1. **Proxy Server Risks:** Free installation does not invest much in backend hardware or encryption. It will result in performance issues and potential data security issues. If you install a “free” proxy server, treat very carefully, some of those might steal your credit card numbers.

2. **Browsing history log:** The proxy server stores your original IP address and web request information is possibly unencrypted form and saved locally. Always check if your proxy server logs and saves that data – and what kind of retention or law enforcement cooperation policies they follow while saving data.
3. **No encryption:** No encryption means you are sending your requests as plain text. Anyone will be able to pull usernames and passwords and account information easily. Keep a check that proxy provides full encryption whenever you use it.

Difference between Firewall and Proxy Server

1. Firewall :

Firewall is software program that prevents unauthorized access to or from a private network. All data packets in it are entering or dropping network passes through the firewall and after checking whether the firewall allows it or not. All traffic must pass through the firewall and only authorized traffic must pass. It is a system located between two networks where it implements an access control policy between those networks. It works on network layer of the OSI model and uses encryption to encrypt the data before transmission.

2. Proxy Server :

Proxy Server is a server that acts as a gateway or intermediary between any device and the rest of the internet. A proxy accepts and forwards connection requests, then returns data for those requests. It uses the anonymous network id instead of actual IP address of client (means it hides the IP address of client), so that the actual IP address of client couldn't be reveal.

Difference between Firewall and Proxy Server :

SR.NO	Firewall	Proxy Server
1	Firewall can monitor and filter all the incoming and outgoing traffic on a given local network.	Proxy server connects an external client with a server to communicate with each other.
2	It blocks connections from unauthorised network.	It facilitates connections over network.
3	It filters data by monitoring IP packets that are traversed.	It filters the client-side requests that are made to connect to the network.

SR.NO	Firewall	Proxy Server
4	It involves network and transport layer data.	It work on application layer data.
5	It exist as an interface between a public and private network.	It can exist with public networks on both sides.
6	It is used to protect an internal network against attacks .	It is used for anonymity and to bypass restrictions.
7	The overhead generated in firewall is more as compared to a proxy server.	The overhead generated in proxy server is less as compared to a firewall.
8	It works on the packet level.	It works on application protocol level.