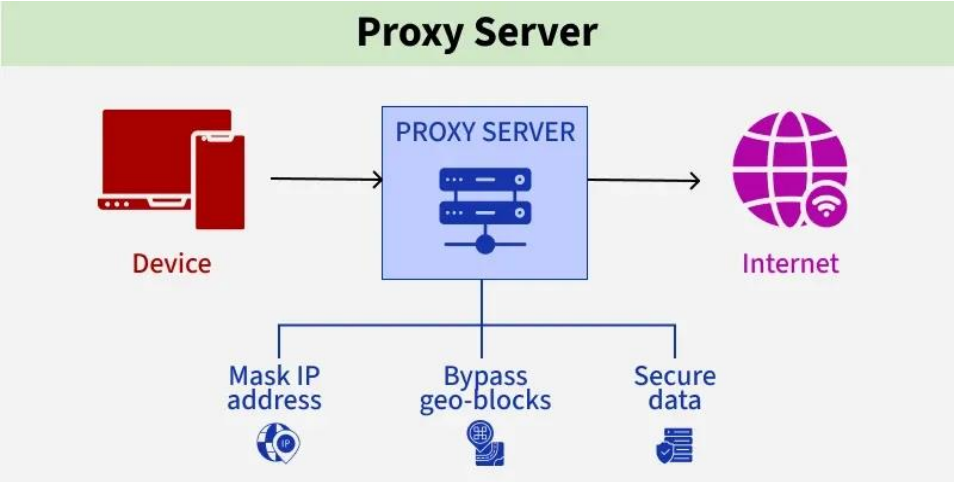
What is Proxy Server?

A proxy server acts as a gateway between your device and the internet, masking your IP address and enhancing online privacy. But what exactly does it do, and why is it critical for businesses, developers, and everyday users?



For example, **Smartproxy** has been offering unique solutions for online anonymity and web data collection since 2018. It has a 55M+ residential proxy pool that opens horizons for block-free web scraping and geo-targeting. They provide access to 195+ locations worldwide, including city-level and 50 US states targeting You can check out Smartproxy's official website to uncover more of its unique features.

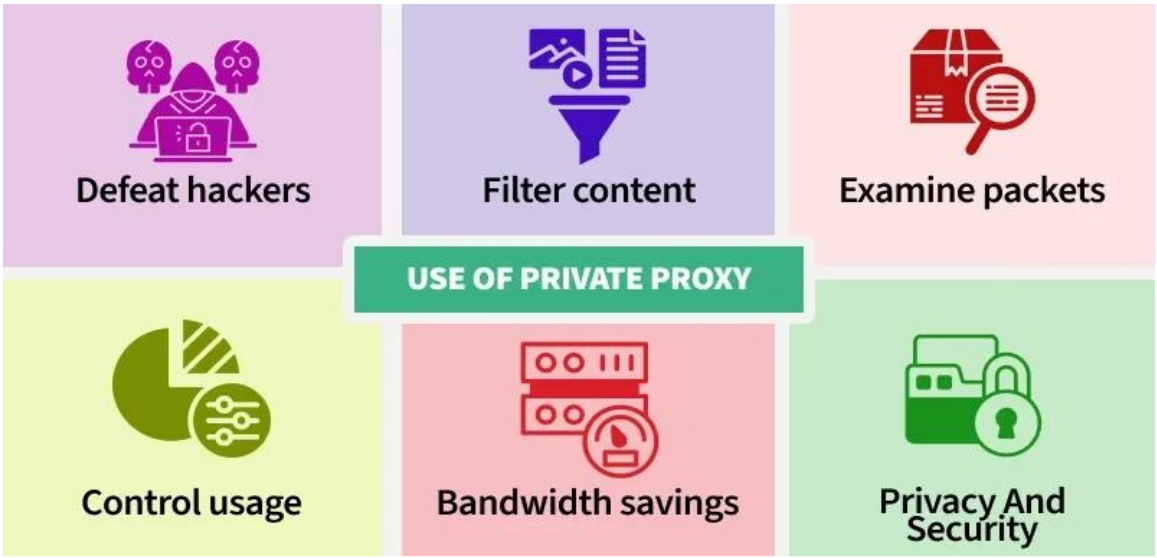
The proxy server also prevents the identification of the client's IP address when the client makes any request to any other servers.

- **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 remain 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 a specific application such as HTTP or FTP. For example, organizations can use a proxy to observe the traffic of their employees to get the work efficiently done. It can also be used to keep a check on any kindba of highly confidential data leakage. Some can also use it to increase their website rank.

Why to Use Private Proxy

These benefits make private proxies essential for enhancing security, privacy, and network control in both personal and organizational use.



- **Defeat Hackers:** To protect an organization's data from malicious use, passwords are used and different architects are set up, 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.

- **Filtering of Content:** By caching the content of the websites, Proxy helps in fast access to the data that has been accessed very often.

- **Examine Packet Headers and Payloads:** Payloads and packet headers of the requests made by the user nodes in the internal server to access social websites can be easily tracked and restricted.

- **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.

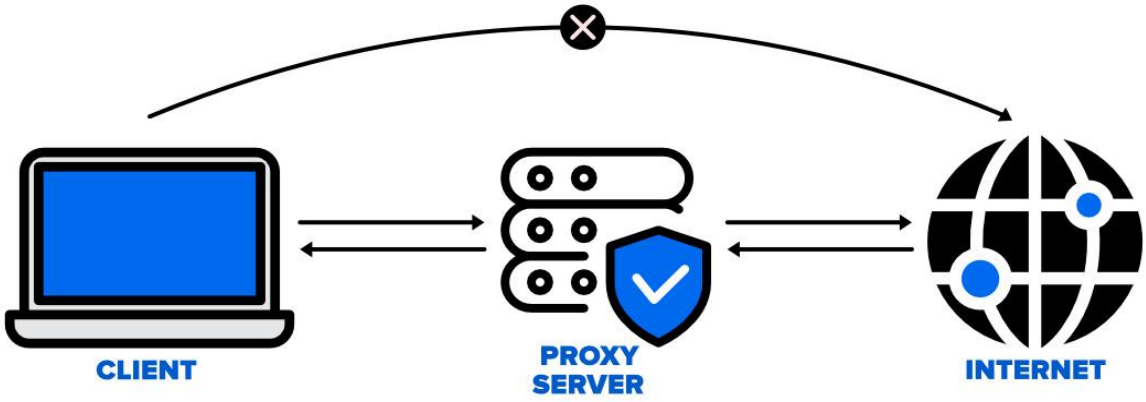
- **Bandwidth savings and improved speeds:** Proxy helps organizations to get better overall network performance with a good proxy server.

- **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.

- **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

Explore the different types of proxy servers—residential, datacenter, mobile, and more. Learn how each works, and ideal use cases for privacy, security, and data tasks.



Reverse Proxy Server

A reverse proxy does the opposite of forward proxy. A forward proxy acts on behalf of clients (or requesting hosts). Forward proxies can hide the identities of clients whereas reverse proxies can hide the identities of servers.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. Reverse proxies have several use cases, a few are:

- **Load balancing:** distribute the load to several web servers.
- **Cache static content:** offload the web servers by caching static content like pictures, HTML pages.
- **Compression:** compress and optimize content to speed up load time..

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.

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.

Highly Anonymity Proxy

This proxy server does not allow the original IP address and it as a proxy server to be detected.

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 .

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.

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.

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.

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.

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.

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.

Rotating Proxy

A rotating proxy assign a new or different IP address to each user that connects to proxy. As users connect, the unique address is assign to it.

How Proxy Server Work?

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.

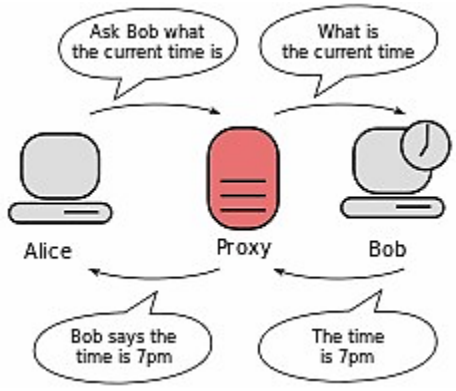
- You open a website in your browser.
- Instead of going directly to the site, your request first goes to the proxy server.
- The proxy reads your request and sends it to the website on your behalf.
- The website sends the response back to the **proxy** (not directly to you).
- The proxy checks the response for security issues (like malware).
- If everything looks fine, the proxy sends the data to your browser.

What is the reason of using Proxy Server?

There are some reasons why everyone should proxy server because it provide following advantages including privacy, web scraping, fast speed, saves bandwidth etc.


7 Reasons to use a proxy server
Improving Your Privacy
Accessing Geo-restricted Content
Improving Your Online Security
Blocking Access to Unwanted Websites
Web Scraping
Improving Your SEO Monitoring and Research
Providing Faster Speed and Saving Bandwidth


Proxy server
This can cache content, do webfiltering, or just make you anonymous
You
Destination
Internet
IP: 1.1.1.1
IP 2.2.2.2
This website Will think you are IP: 2.2.2.2 Making you anonymous


Ask Bob what the current time is
What is the current time
Alice
Proxy
Bob
Bob says the time is 7pm
The time is 7pm

A proxy server acts as an intermediary between a user and the internet, forwarding requests to websites and hiding the user's IP address. While some proxies offer basic privacy, others, often called anonymizers, are specifically designed to provide a higher degree of anonymity by masking the user's identity and location more effectively. Anonymizers may also offer encryption to further protect user data.
Here's a breakdown of the key differences:
Proxy Server:

- **Function:**

  Acts as a gateway between the user and the internet, forwarding requests and potentially hiding the user's IP address.

- **Anonymity:**

May offer basic privacy by hiding the IP address, but doesn't always encrypt traffic or fully mask the user's identity.

- **Examples:**

Can be used for various purposes, including accessing blocked websites, filtering content, and improving performance.

-

Anonymizer:

- **Function:**

Specifically designed to provide a higher level of anonymity by hiding the user's IP address and other identifying information.

- **Anonymity:**

Typically offers encryption and routes traffic through multiple servers to make it more difficult to trace the user's activity.

- **Examples:**

Can be used for privacy, bypassing censorship, and accessing information without revealing one's identity.

-

Key Differences Summarized:

Feature	Proxy Server	Anonymizer
Purpose	General internet access, privacy	Enhanced privacy, anonymity
Anonymity	Basic, may not be complete	Higher level, more robust
Encryption	Not always enabled	Often enabled
Traffic Routing	May be direct or indirect	Usually through multiple servers
Complexity	Can be simple to complex	Often more complex
Examples	Firewalls, web filters	Tor network, VPNs

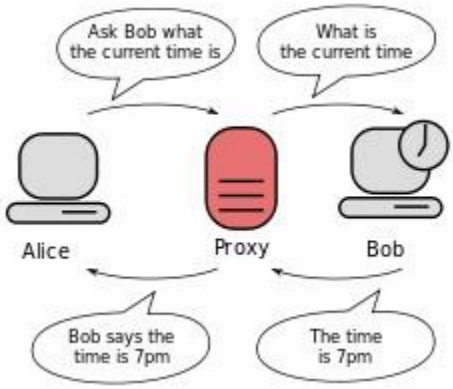
In essence, while all anonymizers are proxy servers, not all proxy servers are anonymizers. Anonymizers are a specialized type of proxy server focused on providing a higher degree of anonymity and privacy

Notes 2

Proxy Servers and Anonymizers

Proxy Server

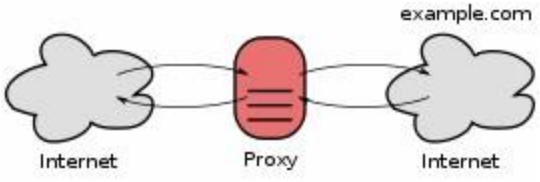
It is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some services, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing anonymity.



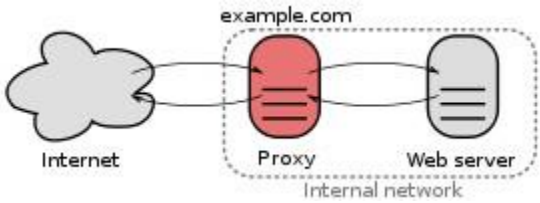
Types of proxy – A proxy server may reside on the user's local computer, or at various points between the user's computer and destination servers on the Internet.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.
- A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).
- A reverse proxy is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.

Open proxies – An open proxy is a forwarding proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet. An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of 'tricking' the client into revealing itself regardless of the proxy being used.



Reverse proxies – A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more proxy servers which handle the request. The response from the proxy server is returned as if it came directly from the original server, leaving the client no knowledge of the origin servers. Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.



There are several reasons for installing reverse proxy servers

- Encryption / SSL acceleration: when secure web sites are created, SSL encryption is often not done by the web server itself, but by a reverse proxy that is equipped with SSL acceleration hardware. See Secure Sockets Layer. Furthermore, a host can provide a single "SSL proxy" to provide SSL encryption for an arbitrary number of hosts; removing the need for a separate SSL Server Certificate for each host, with the downside that all hosts behind the SSL proxy have to share a common DNS name or IP address for SSL connections. This problem can partly be overcome by using the SubjectAltName feature of X.509 certificates.
- Load balancing: the reverse proxy can distribute the load to several web servers, each web server serving its own application area. In such a case, the reverse proxy may need to rewrite the URLs in each web page (translation from externally known URLs to the internal locations).
- Serve/cache static content: A reverse proxy can offload the web servers by caching static content like pictures and other static graphical content.
- Compression: the proxy server can optimize and compress the content to speed up the load time.
- Spoon feeding: reduces resource usage caused by slow clients on the web servers by caching the content the web server sent and slowly "spoon feeding" it to the client. This especially benefits dynamically generated pages.
- Security: the proxy server is an additional layer of defense and can protect against some OS and Web Server specific attacks. However, it does not provide any protection from attacks against the web application or service itself, which is generally considered the larger threat.

- Extranet Publishing: a reverse proxy server facing the Internet can be used to communicate to a firewall server internal to an organization, providing extranet access to some functions while keeping the servers behind the firewalls. If used in this way, security measures should be considered to protect the rest of your infrastructure in case this server is compromised, as its web application is exposed to attack from the Internet.

If the destination server filters content based on the origin of the request, the use of a proxy can circumvent this filter. For example, a server using IP-based geolocation to restrict its service to a certain country can be accessed using a proxy located in that country to access the service.

Web proxies are the most common means of bypassing government censorship, although no more than 3% of Internet users use any circumvention tools. In some cases users can circumvent proxies which filter using blacklists using services designed to proxy information from a non-blacklisted location.

Proxies can be installed in order to eavesdrop upon the data-flow between client machines and the web. All content sent or accessed – including passwords submitted and cookies used – can be captured and analyzed by the proxy operator. For this reason, passwords to online services (such as webmail and banking) should always be exchanged over a cryptographically secured connection, such as SSL. By chaining proxies which do not reveal data about the original requester, it is possible to obfuscate activities from the eyes of the user's destination. However, more traces will be left on the intermediate hops, which could be used or offered up to trace the user's activities. If the policies and administrators of these other proxies are unknown, the user may fall victim to a false sense of security just because those details are out of sight and mind. In what is more of an inconvenience than a risk, proxy users may find themselves being blocked from certain Web sites, as numerous forums and Web sites block IP addresses from proxies known to have spammed or trolled the site. Proxy bouncing can be used to maintain your privacy.

Anonymizer

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.

There are many reasons for using anonymizers. Anonymizers help minimize risk. They can be used to prevent identity theft, or to protect search histories from public disclosure. Some countries apply heavy censorship on the internet. Anonymizers can help in allowing free access to all of the internet content, but cannot help against persecution for accessing the Anonymizer website itself. Furthermore, as information itself about Anonymizer websites are banned in these countries, users are wary that they may be falling into a government-set trap.

Anonymizers are also used by people who wish to receive objective information with the growing target marketing on the internet and targeted information. For example, large news outlets such as CNN target the viewers according to region and give different information to

different populations. Websites such as YouTube obtain information about the last videos viewed on a computer, and propose "recommended" videos accordingly, and most of the online targeted marketing is done by showing advertisements according to that region. Anonymizers are used for avoiding this kind of targeting and getting a more objective view of information.

Types

- Protocol specific anonymizers – Sometimes anonymizers are implemented to work only with one particular protocol. The advantage is that no extra software is needed. The operation occurs in this manner: A connection is made by the user to the anonymizer. Commands to the anonymizer are included inside a typical message. The anonymizer then makes a connection to the resource specified by the inbound command and relays the message with the command stripped out. An example of a protocol-specific anonymizer is an anonymous remailer for e-mail. Also of note are web proxies, and bouncers for FTP and IRC.
- Protocol independent anonymizers – Protocol independence can be achieved by creating a tunnel to an anonymizer. The technology to do so varies. Protocols used by anonymizer services may include SOCKS, PPTP, or OpenVPN. In this case either the desired application must support the tunneling protocol, or a piece of software must be installed to force all connections through the tunnel. Web browsers, FTP and IRC clients often support SOCKS for example, unlike telnet.