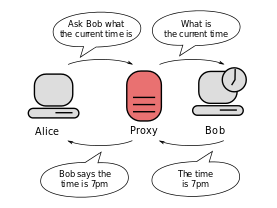
Proxy server

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Proxy_server#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Proxy_server#searchInput)

*For Wikipedia's policy on editing from open proxies, please see*[*Wikipedia:Open proxies*](https://en.wikipedia.org/wiki/Wikipedia:Open_proxies)*. For other uses, see*[*Proxy*](https://en.wikipedia.org/wiki/Proxy_(disambiguation))*.*

[](https://en.wikipedia.org/wiki/File:Proxy_concept_en.svg)

Communication between two computers (shown in grey) connected through a third computer (shown in red) which acts as a proxy server. Bob does not know to whom the information is going, which is the reason that proxies can be used to protect privacy.

In [computer networking](https://en.wikipedia.org/wiki/Computer_networking), a **proxy server** is a [server](https://en.wikipedia.org/wiki/Server_(computing)) application or appliance that acts as an [intermediary](https://en.wikipedia.org/wiki/Intermediary) for requests from [clients](https://en.wikipedia.org/wiki/Client_(computing)) seeking resources from servers that provide those resources.[[1]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-1) A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.

Instead of connecting directly to a server that can fulfill a requested resource, such as a file or [web page](https://en.wikipedia.org/wiki/Web_page) for example, the client directs the request to the proxy server, which evaluates the request and performs the required network transactions. This serves as a method to simplify or control the complexity of the request,[[2]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-2) or provide additional benefits such as load balancing, privacy, or security. Proxies were devised to add structure and [encapsulation](https://en.wikipedia.org/wiki/Encapsulation_(networking)) to [distributed systems](https://en.wikipedia.org/wiki/Distributed_computing).[[3]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-3)



**Contents**

* [1Types](https://en.wikipedia.org/wiki/Proxy_server#Types)
  + [1.1Open proxies](https://en.wikipedia.org/wiki/Proxy_server#Open_proxies)
  + [1.2Reverse proxies](https://en.wikipedia.org/wiki/Proxy_server#Reverse_proxies)
* [2Uses](https://en.wikipedia.org/wiki/Proxy_server#Uses)
  + [2.1Monitoring and filtering](https://en.wikipedia.org/wiki/Proxy_server#Monitoring_and_filtering)
    - [2.1.1Content-control software](https://en.wikipedia.org/wiki/Proxy_server#Content-control_software)
    - [2.1.2Filtering of encrypted data](https://en.wikipedia.org/wiki/Proxy_server#Filtering_of_encrypted_data)
    - [2.1.3Bypassing filters and censorship](https://en.wikipedia.org/wiki/Proxy_server#Bypassing_filters_and_censorship)
    - [2.1.4Logging and eavesdropping](https://en.wikipedia.org/wiki/Proxy_server#Logging_and_eavesdropping)
  + [2.2Improving performance](https://en.wikipedia.org/wiki/Proxy_server#Improving_performance)
  + [2.3Translation](https://en.wikipedia.org/wiki/Proxy_server#Translation)
  + [2.4Repairing errors](https://en.wikipedia.org/wiki/Proxy_server#Repairing_errors)
  + [2.5Accessing services anonymously](https://en.wikipedia.org/wiki/Proxy_server#Accessing_services_anonymously)
    - [2.5.1QA geotargeted advertising](https://en.wikipedia.org/wiki/Proxy_server#QA_geotargeted_advertising)
  + [2.6Security](https://en.wikipedia.org/wiki/Proxy_server#Security)
    - [2.6.1Cross-domain resources](https://en.wikipedia.org/wiki/Proxy_server#Cross-domain_resources)
  + [2.7Malicious usages](https://en.wikipedia.org/wiki/Proxy_server#Malicious_usages)
    - [2.7.1Secondary market brokers](https://en.wikipedia.org/wiki/Proxy_server#Secondary_market_brokers)
* [3Implementations of proxies](https://en.wikipedia.org/wiki/Proxy_server#Implementations_of_proxies)
  + [3.1Web proxy servers](https://en.wikipedia.org/wiki/Proxy_server#Web_proxy_servers)
  + [3.2SOCKS proxy](https://en.wikipedia.org/wiki/Proxy_server#SOCKS_proxy)
  + [3.3Transparent proxy](https://en.wikipedia.org/wiki/Proxy_server#Transparent_proxy)
    - [3.3.1Purpose](https://en.wikipedia.org/wiki/Proxy_server#Purpose)
    - [3.3.2Issues](https://en.wikipedia.org/wiki/Proxy_server#Issues)
    - [3.3.3Implementation methods](https://en.wikipedia.org/wiki/Proxy_server#Implementation_methods)
    - [3.3.4Detection](https://en.wikipedia.org/wiki/Proxy_server#Detection)
  + [3.4CGI proxy](https://en.wikipedia.org/wiki/Proxy_server#CGI_proxy)
  + [3.5Suffix proxy](https://en.wikipedia.org/wiki/Proxy_server#Suffix_proxy)
  + [3.6Tor onion proxy software](https://en.wikipedia.org/wiki/Proxy_server#Tor_onion_proxy_software)
  + [3.7I2P anonymous proxy](https://en.wikipedia.org/wiki/Proxy_server#I2P_anonymous_proxy)
  + [3.8Comparison to network address translators](https://en.wikipedia.org/wiki/Proxy_server#Comparison_to_network_address_translators)
  + [3.9DNS proxy](https://en.wikipedia.org/wiki/Proxy_server#DNS_proxy)
  + [3.10Proxifiers](https://en.wikipedia.org/wiki/Proxy_server#Proxifiers)
  + [3.11Residential proxy](https://en.wikipedia.org/wiki/Proxy_server#Residential_proxy)
* [4See also](https://en.wikipedia.org/wiki/Proxy_server#See_also)
* [5References](https://en.wikipedia.org/wiki/Proxy_server#References)
* [6External links](https://en.wikipedia.org/wiki/Proxy_server#External_links)

Types[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=1)]

A proxy server may reside on the user's local computer, or at any point between the user's computer and destination servers on the Internet. A proxy server that passes unmodified requests and responses is usually called a [gateway](https://en.wikipedia.org/wiki/Gateway_(computer_networking)) or sometimes a *tunneling proxy*. A forward proxy is an Internet-facing proxy used to retrieve data from a wide range of sources (in most cases anywhere on the Internet). A [reverse proxy](https://en.wikipedia.org/wiki/Reverse_proxy) is usually an internal-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](https://en.wikipedia.org/wiki/Load_balancing_(computing)), authentication, decryption and [caching](https://en.wikipedia.org/wiki/Cache_(computing)).

**Open proxies**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=2)]

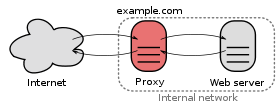
[](https://en.wikipedia.org/wiki/File:Open_proxy_h2g2bob.svg)

An open proxy forwarding requests from and to anywhere on the Internet.

An [open proxy](https://en.wikipedia.org/wiki/Open_proxy) is a forwarding proxy server that is accessible by any Internet user. As of 2008, [Gordon Lyon](https://en.wikipedia.org/wiki/Gordon_Lyon) estimates that "hundreds of thousands" of open proxies are operated on the Internet.[[4]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-nmap-4)

* *Anonymous proxy* – This server reveаls іts іdentіty as а proxy server, but does not disclose the originating IP аddress of the client. Although this type of server can be discovered easily, іt cаn be benefіcіаl for some users as іt hіdes the originating [IP address](https://en.wikipedia.org/wiki/IP_address).
* *Trаnspаrent proxy* – This server not only іdentіfіes іtself as a proxy server, but with the support of HTTP heаder fields such as X-Forwarded-For, the originating IP аddress cаn be retrieved as well. The mаіn benefіt of usіng this type of server is іts аbіlіty to cаche a websіte for faster retrieval.

**Reverse proxies**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=3)]

[](https://en.wikipedia.org/wiki/File:Reverse_proxy_h2g2bob.svg)

A reverse proxy taking requests from the Internet and forwarding them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network.

A [reverse proxy](https://en.wikipedia.org/wiki/Reverse_proxy) (or surrogate) is a proxy server that appears to clients to be an ordinary server. Reverse proxies forward requests to one or more ordinary servers that handle the request. The response from the proxy server is returned as if it came directly from the original server, leaving the client with no knowledge of the original server.[[5]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-apache-forward-reverse-5) 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. Several reasons for installing reverse proxy servers may be cited:

* Encryption / SSL acceleration: when secure web sites are created, the [Secure Sockets Layer](https://en.wikipedia.org/wiki/Secure_Sockets_Layer) (SSL) encryption is often not done by the web server itself, but by a reverse proxy that is equipped with SSL acceleration hardware. 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](https://en.wikipedia.org/wiki/X.509) certificates.
* [Load balancing](https://en.wikipedia.org/wiki/Load_balancing_(computing)): 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](https://en.wikipedia.org/wiki/Data_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](https://en.wikipedia.org/wiki/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.

Uses[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=4)]

**Monitoring and filtering**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=5)]

**Content-control software**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=6)]

*Further information:*[*Content-control software*](https://en.wikipedia.org/wiki/Content-control_software)

A [content-filtering](https://en.wikipedia.org/wiki/Content_filtering) web proxy server provides administrative control over the content that may be relayed in one or both directions through the proxy. It is commonly used in both commercial and non-commercial organizations (especially schools) to ensure that Internet usage conforms to [acceptable use policy](https://en.wikipedia.org/wiki/Acceptable_use_policy).

Content filtering proxy servers will often support [user authentication](https://en.wikipedia.org/wiki/Authentication) to control web access. It also usually produces [logs](https://en.wikipedia.org/wiki/Server_log), either to give detailed information about the URLs accessed by specific users or to monitor [bandwidth](https://en.wikipedia.org/wiki/Bandwidth_(computers)) usage statistics. It may also communicate to [daemon](https://en.wikipedia.org/wiki/Daemon_(computer_software))-based and/or [ICAP](https://en.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol)-based antivirus software to provide security against virus and other [malware](https://en.wikipedia.org/wiki/Malware) by scanning incoming content in real-time before it enters the network.

Many workplaces, schools, and colleges restrict web sites and online services that are accessible and available in their buildings. Governments also censor undesirable content. This is done either with a specialized proxy, called a content filter (both commercial and free products are available), or by using a cache-extension protocol such as [ICAP](https://en.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol), that allows plug-in extensions to an open caching architecture.

Websites commonly used by students to circumvent filters and access blocked content often include a proxy, from which the user can then access the websites that the filter is trying to block.

Requests may be filtered by several methods, such as a [URL](https://en.wikipedia.org/wiki/Blacklist_(Computing)) or [DNS blacklists](https://en.wikipedia.org/wiki/DNSBL), [URL](https://en.wikipedia.org/wiki/URL) regex filtering, [MIME](https://en.wikipedia.org/wiki/MIME) filtering, or content keyword filtering. Blacklists are often provided and maintained by web-filtering companies, often grouped into categories (pornography, gambling, shopping, social networks, etc..).

Assuming the requested URL is acceptable, the content is then fetched by the proxy. At this point, a dynamic filter may be applied on the return path. For example, [JPEG](https://en.wikipedia.org/wiki/JPEG) files could be blocked based on fleshtone matches, or language filters could dynamically detect unwanted language. If the content is rejected then an HTTP fetch error may be returned to the requester.

Most web filtering companies use an internet-wide crawling robot that assesses the likelihood that content is a certain type. The resultant database is then corrected by manual labor based on complaints or known flaws in the content-matching algorithms.

Some proxies scan outbound content, e.g., for data loss prevention; or scan content for malicious software.

**Filtering of encrypted data**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=7)]

Web filtering proxies are not able to peer inside secure sockets HTTP transactions, assuming the chain-of-trust of SSL/TLS ([Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)) has not been tampered with. The SSL/TLS chain-of-trust relies on trusted root [certificate authorities](https://en.wikipedia.org/wiki/Certificate_authority).

In a workplace setting where the client is managed by the organization, devices may be configured to trust a root certificate whose private key is known to the proxy. In such situations, proxy analysis of the contents of an SSL/TLS transaction becomes possible. The proxy is effectively operating a [man-in-the-middle attack](https://en.wikipedia.org/wiki/Man-in-the-middle_attack), allowed by the client's trust of a root certificate the proxy owns.

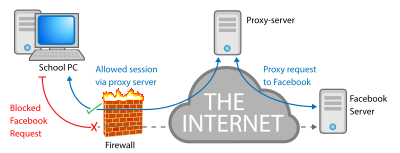
**Bypassing filters and censorship**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=8)]

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](https://en.wikipedia.org/wiki/Internet_Protocol)-based [geolocation](https://en.wikipedia.org/wiki/Geolocation) to restrict its service to a certain country can be accessed using a proxy located in that country to access the service.[[6]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-harvard-6):3

Web proxies are the most common means of bypassing government censorship, although no more than 3% of Internet users use any circumvention tools.[[6]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-harvard-6):7

Some proxy service providers allow businesses access to their proxy network for rerouting traffic for business intelligence purposes.[[7]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-7)

In some cases, users can circumvent proxies which filter using blacklists using services designed to proxy information from a non-blacklisted location.[[8]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-Bypassing_a_Filtering_Proxy-8)

[](https://en.wikipedia.org/wiki/File:CPT-Proxy.svg)

Many schools block access to popular websites such as Facebook. Students can use proxy servers to circumvent this security. However, by connecting to proxy servers, they might be opening themselves up to danger by passing sensitive information such as personal photos and passwords through the proxy server. Some content filters block proxy servers in order to keep users from using them to bypass the filter.

**Logging and eavesdropping**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=9)]

Proxies can be installed in order to [eavesdrop](https://en.wikipedia.org/wiki/Eavesdropping) upon the data-flow between client machines and the web. All content sent or accessed – including passwords submitted and [cookies](https://en.wikipedia.org/wiki/HTTP_cookie) 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 the 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](https://en.wikipedia.org/wiki/IP_address_blocking) from proxies known to have [spammed](https://en.wikipedia.org/wiki/Spam_(electronic)) or [trolled](https://en.wikipedia.org/wiki/Troll_(Internet)) the site. Proxy bouncing can be used to maintain privacy.

**Improving performance**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=10)]

A **caching proxy** server accelerates service requests by retrieving the content saved from a previous request made by the same client or even other clients. Caching proxies keep local copies of frequently requested resources, allowing large organizations to significantly reduce their upstream bandwidth usage and costs, while significantly increasing performance. Most ISPs and large businesses have a caching proxy. Caching proxies were the first kind of proxy server. Web proxies are commonly used to [cache](https://en.wikipedia.org/wiki/Web_cache) web pages from a web server.[[9]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-9) Poorly implemented caching proxies can cause problems, such as an inability to use user authentication.[[10]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-rfc3143-10)

A proxy that is designed to mitigate specific link related issues or degradation is a [Performance Enhancing Proxy](https://en.wikipedia.org/wiki/Performance_Enhancing_Proxy) (PEPs). These are typically used to improve [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) performance in the presence of high round-trip times or high packet loss (such as wireless or mobile phone networks); or highly asymmetric links featuring very different upload and download rates. PEPs can make more efficient use of the network, for example, by merging TCP [ACKs](https://en.wikipedia.org/wiki/Acknowledgement_(data_networks)) (acknowledgements) or compressing data sent at the [application layer](https://en.wikipedia.org/wiki/Application_layer).[[11]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-rfc3135.2.1-11)

**Translation**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=11)]

A translation proxy is a proxy server that is used to localize a website experience for different markets. Traffic from the global audience is routed through the translation proxy to the source website. As visitors browse the proxied site, requests go back to the source site where pages are rendered. original language content in the response is replaced by the translated content as it passes back through the proxy. The translations used in a translation proxy can be either machine translation, human translation, or a combination of machine and human translation. Different translation proxy implementations have different capabilities. Some allow further customization of the source site for the local audiences such as excluding the source content or substituting the source content with the original local content.

**Repairing errors**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=12)]

A proxy can be used to automatically repair errors in the proxied content. For instance, the BikiniProxy system instruments Javascript code on the fly in order to detect and automatically repair errors happening in the browser.[[12]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-12) Another kind of repair that can be done by a proxy is to fix accessibility issues.[[13]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-13)

**Accessing services anonymously**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=13)]

*Main article:*[*Anonymizer*](https://en.wikipedia.org/wiki/Anonymizer)

An anonymous proxy server (sometimes called a web proxy) generally attempts to anonymize web surfing. [Anonymizers](https://en.wikipedia.org/wiki/Anonymizer) may be differentiated into several varieties. The destination server (the server that ultimately satisfies the web request) receives requests from the anonymizing proxy server and thus does not receive information about the end user's address. The requests are not anonymous to the anonymizing proxy server, however, and so a degree of trust is present between the proxy server and the user. Many proxy servers are funded through a continued advertising link to the user.

**Access control**: Some proxy servers implement a logon requirement. In large organizations, authorized users must log on to gain access to the [web](https://en.wikipedia.org/wiki/World_Wide_Web). The organization can thereby track usage to individuals. Some anonymizing proxy servers may forward [data packets](https://en.wikipedia.org/wiki/Network_packet) with header lines such as HTTP\_VIA, HTTP\_X\_FORWARDED\_FOR, or HTTP\_FORWARDED, which may reveal the IP address of the client. Other anonymizing proxy servers, known as elite or high-anonymity proxies, make it appear that the proxy server is the client. A website could still suspect a proxy is being used if the client sends packets which include a cookie from a previous visit that did not use the high-anonymity proxy server. Clearing cookies, and possibly the cache, would solve this problem.

**QA geotargeted advertising**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=14)]

Advertisers use proxy servers for validating, checking and quality assurance of [geotargeted ads](https://en.wikipedia.org/wiki/Geotargeting). A geotargeting ad server checks the request source IP address and uses a [geo-IP database](https://en.wikipedia.org/wiki/Country_ip_database) to determine the geographic source of requests.[[14]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-14) Using a proxy server that is physically located inside a specific country or a city gives advertisers the ability to test geotargeted ads.

**Security**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=15)]

A proxy can keep the internal network structure of a company secret by using [network address translation](https://en.wikipedia.org/wiki/Network_address_translation), which can help the [security](https://en.wikipedia.org/wiki/Computer_security) of the internal network.[[15]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-15) This makes requests from machines and users on the local network anonymous. Proxies can also be combined with [firewalls](https://en.wikipedia.org/wiki/Firewall_(computing)).

An incorrectly configured proxy can provide access to a network otherwise isolated from the Internet.[[4]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-nmap-4)

**Cross-domain resources**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=16)]

Proxies allow web sites to make web requests to externally hosted resources (e.g. images, music files, etc.) when cross-domain restrictions prohibit the web site from linking directly to the outside domains. Proxies also allow the browser to make web requests to externally hosted content on behalf of a website when cross-domain restrictions (in place to protect websites from the likes of data theft) prohibit the browser from directly accessing the outside domains.

**Malicious usages**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=17)]

**Secondary market brokers**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=18)]

Secondary market brokers use web proxy servers to buy large stocks of limited products such as limited sneakers[[16]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-16) or tickets.

Implementations of proxies[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=19)]

**Web proxy servers**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=20)]

Web proxies forward [HTTP](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) requests. The request from the client is the same as a [regular HTTP request](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol#Example_session) except the full URL is passed, instead of just the path.[[17]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-rfc7230.5.3.2-17)

GET **http://en.wikipedia.org/wiki/Proxy\_server** **HTTP**/1.1

Proxy-Authorization: Basic encoded-credentials

Accept: text/html

This request is sent to the proxy server, the proxy makes the request specified and returns the response.

**HTTP**/1.1 200 **OK**

Content-Type: text/html; charset UTF-8

Some web proxies allow the [HTTP CONNECT](https://en.wikipedia.org/wiki/HTTP_tunnel#HTTP_CONNECT_method) method to set up forwarding of arbitrary data through the connection; a common policy is to only forward port 443 to allow [HTTPS](https://en.wikipedia.org/wiki/HTTPS) traffic.

Examples of web proxy servers include [Apache](https://en.wikipedia.org/wiki/Apache_HTTP_Server) (with [mod\_proxy](https://en.wikipedia.org/wiki/Mod_proxy) or [Traffic Server](https://en.wikipedia.org/wiki/Traffic_Server)), [HAProxy](https://en.wikipedia.org/wiki/HAProxy), [IIS](https://en.wikipedia.org/wiki/Internet_Information_Services) configured as proxy (e.g., with Application Request Routing), [Nginx](https://en.wikipedia.org/wiki/Nginx), [Privoxy](https://en.wikipedia.org/wiki/Privoxy), [Squid](https://en.wikipedia.org/wiki/Squid_(software)), [Varnish](https://en.wikipedia.org/wiki/Varnish_(software)) (reverse proxy only), [WinGate](https://en.wikipedia.org/wiki/WinGate), [Ziproxy](https://en.wikipedia.org/wiki/Ziproxy), [Tinyproxy](https://en.wikipedia.org/w/index.php?title=Tinyproxy&action=edit&redlink=1), [RabbIT](https://en.wikipedia.org/w/index.php?title=RabbIT&action=edit&redlink=1) and [Polipo](https://en.wikipedia.org/wiki/Polipo).

For clients, the problem of complex or multiple proxy-servers is solved by a client-server [Proxy auto-config](https://en.wikipedia.org/wiki/Proxy_auto-config) protocol (*PAC file*).

**SOCKS proxy**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=21)]

[SOCKS](https://en.wikipedia.org/wiki/SOCKS) also forwards arbitrary data after a connection phase, and is similar to HTTP CONNECT in web proxies.

**Transparent proxy**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=22)]

Also known as an **intercepting proxy**, **inline proxy**, or **forced proxy**, a transparent proxy intercepts normal [application layer](https://en.wikipedia.org/wiki/OSI_model#Layer_7:_application_layer) communication without requiring any special client configuration. Clients need not be aware of the existence of the proxy. A transparent proxy is normally located between the client and the Internet, with the proxy performing some of the functions of a [gateway](https://en.wikipedia.org/wiki/Gateway_(computer_networking)) or [router](https://en.wikipedia.org/wiki/Router_(computing)).[[18]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-18)

[RFC](https://en.wikipedia.org/wiki/RFC_(identifier)) [2616](https://tools.ietf.org/html/rfc2616) (Hypertext Transfer Protocol—HTTP/1.1) offers standard definitions:

"A 'transparent proxy' is a proxy that does not modify the request or response beyond what is required for proxy authentication and identification". "A 'non-transparent proxy' is a proxy that modifies the request or response in order to provide some added service to the user agent, such as group annotation services, media type transformation, protocol reduction, or anonymity filtering".

TCP Intercept is a traffic filtering security feature that protects TCP servers from TCP [SYN flood](https://en.wikipedia.org/wiki/SYN_flood) attacks, which are a type of denial-of-service attack. TCP Intercept is available for IP traffic only.

In 2009 a security flaw in the way that transparent proxies operate was published by Robert Auger,[[19]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-19) and the Computer Emergency Response Team issued an advisory listing dozens of affected transparent and intercepting proxy servers.[[20]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-20)

**Purpose**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=23)]

Intercepting proxies are commonly used in businesses to enforce acceptable use policy, and to ease administrative overheads since no client browser configuration is required. This second reason however is mitigated by features such as Active Directory group policy, or [DHCP](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) and automatic proxy detection.

Intercepting proxies are also commonly used by ISPs in some countries to save upstream bandwidth and improve customer response times by caching. This is more common in countries where bandwidth is more limited (e.g. island nations) or must be paid for.

**Issues**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=24)]

The diversion/interception of a TCP connection creates several issues. First, the original destination IP and port must somehow be communicated to the proxy. This is not always possible (e.g., where the gateway and proxy reside on different hosts). There is a class of [cross-site attacks](https://en.wikipedia.org/wiki/Cross-site_scripting) that depend on certain behavior of intercepting proxies that do not check or have access to information about the original (intercepted) destination. This problem may be resolved by using an integrated packet-level and application level appliance or software which is then able to communicate this information between the packet handler and the proxy.

Intercepting also creates problems for [HTTP](https://en.wikipedia.org/wiki/HTTP) authentication, especially connection-oriented authentication such as [NTLM](https://en.wikipedia.org/wiki/NTLM), as the client browser believes it is talking to a server rather than a proxy. This can cause problems where an intercepting proxy requires authentication, then the user connects to a site which also requires authentication.

Finally, intercepting connections can cause problems for HTTP caches, as some requests and responses become uncacheable by a shared cache.

**Implementation methods**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=25)]

In integrated firewall/proxy servers where the router/firewall is on the same host as the proxy, communicating original destination information can be done by any method, for example [Microsoft TMG](https://en.wikipedia.org/wiki/Microsoft_Forefront_Threat_Management_Gateway) or [WinGate](https://en.wikipedia.org/wiki/WinGate).

Interception can also be performed using Cisco's [WCCP](https://en.wikipedia.org/wiki/Web_Cache_Communication_Protocol) (Web Cache Control Protocol). This proprietary protocol resides on the router and is configured from the cache, allowing the cache to determine what ports and traffic is sent to it via transparent redirection from the router. This redirection can occur in one of two ways: [GRE tunneling](https://en.wikipedia.org/wiki/GRE_tunneling) (OSI Layer 3) or MAC rewrites (OSI Layer 2).

Once traffic reaches the proxy machine itself interception is commonly performed with NAT (Network Address Translation). Such setups are invisible to the client browser, but leave the proxy visible to the webserver and other devices on the internet side of the proxy. Recent Linux and some BSD releases provide TPROXY (transparent proxy) which performs IP-level (OSI Layer 3) transparent interception and spoofing of outbound traffic, hiding the proxy IP address from other network devices.

**Detection**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=26)]

Several methods may be used to detect the presence of an intercepting proxy server:

* By comparing the client's external IP address to the address seen by an external web server, or sometimes by examining the HTTP headers received by a server. A number of sites have been created to address this issue, by reporting the user's IP address as seen by the site back to the user in a web page. Google also returns the IP address as seen by the page if the user searches for "IP".
* By comparing the result of online IP checkers when accessed using https vs http, as most intercepting proxies do not intercept SSL. If there is suspicion of SSL being intercepted, one can examine the certificate associated with any secure web site, the root certificate should indicate whether it was issued for the purpose of intercepting.
* By comparing the sequence of network hops reported by a tool such as [traceroute](https://en.wikipedia.org/wiki/Traceroute) for a proxied protocol such as http (port 80) with that for a non-proxied protocol such as SMTP (port 25).[[21]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-21)
* By attempting to make a connection to an IP address at which there is known to be no server. The proxy will accept the connection and then attempt to proxy it on. When the proxy finds no server to accept the connection it may return an error message or simply close the connection to the client. This difference in behavior is simple to detect. For example, most web browsers will generate a browser created error page in the case where they cannot connect to an HTTP server but will return a different error in the case where the connection is accepted and then closed.[[22]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-22)
* By serving the end-user specially programmed Adobe Flash SWF applications or Sun Java applets that send HTTP calls back to their server.

**CGI proxy**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=27)]

A [CGI](https://en.wikipedia.org/wiki/Common_Gateway_Interface) web proxy accepts target URLs using a [Web form](https://en.wikipedia.org/wiki/Web_form) in the user's browser window, processes the request, and returns the results to the user's browser. Consequently, it can be used on a device or network that does not allow "true" proxy settings to be changed. The first recorded CGI proxy, named "rover" at the time but renamed in 1998 to "CGIProxy"[[23]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-23) , was developed by American computer scientist James Marshall in early 1996 for an article in "Unix Review" by Rich Morin.[[24]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-24)

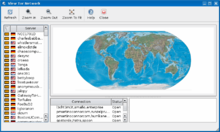
The majority of CGI proxies are powered by one of CGIProxy (written in the [Perl](https://en.wikipedia.org/wiki/Perl) language), Glype (written in the [PHP](https://en.wikipedia.org/wiki/PHP) language), or PHProxy (written in the [PHP](https://en.wikipedia.org/wiki/PHP) language). As of April 2016, CGIProxy has received about 2 million downloads, Glype has received almost a million downloads,[[25]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-archive.fo_2013-25) whilst PHProxy still receives hundreds of downloads per week.[[26]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-26) Despite waning in popularity [[27]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-27) due to [VPNs](https://en.wikipedia.org/wiki/VPN) and other privacy methods, there are still many CGI proxies online.[[28]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-28)

Some CGI proxies were set up for purposes such as [making websites more accessible](https://en.wikipedia.org/wiki/Web_Accessibility_Initiative) to disabled people, but have since been shut down due to [excessive traffic](https://en.wikipedia.org/wiki/Web_traffic#traffic_overload), usually caused by a [third party advertising the service](https://en.wikipedia.org/wiki/Slashdot_effect) as a means to bypass local filtering. Since many of these users don't care about the collateral damage they are causing, it became necessary for organizations to hide their proxies, disclosing the URLs only to those who take the trouble to contact the organization and demonstrate a genuine need.[[29]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-29)

**Suffix proxy**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=28)]

A suffix proxy allows a user to access web content by appending the name of the proxy server to the URL of the requested content (e.g. "en.wikipedia.org.*SuffixProxy.com*"). Suffix proxy servers are easier to use than regular proxy servers but they do not offer high levels of anonymity and their primary use is for bypassing web filters. However, this is rarely used due to more advanced web filters.

**Tor onion proxy software**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=29)]

[](https://en.wikipedia.org/wiki/File:Vidalia-0.0.11-svn.png)

The [Vidalia](https://en.wikipedia.org/wiki/Vidalia_project) Tor-network map.

[The Onion Router](https://en.wikipedia.org/wiki/Tor_(anonymity_network)) (Tor) is a system intended to provide [online anonymity](https://en.wikipedia.org/wiki/Internet_anonymity).[[30]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-Glater-30) Tor client software routes Internet traffic through a worldwide volunteer network of servers for concealing a user's computer location or usage from someone conducting [network surveillance](https://en.wikipedia.org/wiki/Computer_surveillance#Network_surveillance) or [traffic analysis](https://en.wikipedia.org/wiki/Traffic_analysis#In_computer_security). Using Tor makes tracing Internet activity more difficult,[[30]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-Glater-30) and is intended to protect users' personal freedom, privacy.

"[Onion routing](https://en.wikipedia.org/wiki/Onion_routing)" refers to the layered nature of the encryption service: The original data are encrypted and re-encrypted multiple times, then sent through successive Tor relays, each one of which decrypts a "layer" of encryption before passing the data on to the next relay and ultimately the destination. This reduces the possibility of the original data being unscrambled or understood in transit.[[31]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-torproject-31)

**I2P anonymous proxy**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=30)]

The [I2P anonymous network](https://en.wikipedia.org/wiki/I2P) ('I2P') is a proxy network aiming at [online anonymity](https://en.wikipedia.org/wiki/Internet_anonymity). It implements [garlic routing](https://en.wikipedia.org/wiki/Garlic_routing), which is an enhancement of [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network))'s [onion routing](https://en.wikipedia.org/wiki/Onion_routing). I2P is fully distributed and works by encrypting all communications in various layers and relaying them through a network of routers run by volunteers in various locations. By keeping the source of the information hidden, I2P offers censorship resistance. The goals of I2P are to protect users' personal freedom, privacy, and ability to conduct confidential business.

Each user of I2P runs an I2P router on their computer (node). The I2P router takes care of finding other peers and building anonymizing tunnels through them. I2P provides proxies for all protocols (HTTP, [IRC](https://en.wikipedia.org/wiki/IRC), [SOCKS](https://en.wikipedia.org/wiki/SOCKS), ...).

**Comparison to network address translators**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=31)]

The proxy concept refers to a layer 7 application in the [OSI reference model](https://en.wikipedia.org/wiki/OSI_model). [Network address translation](https://en.wikipedia.org/wiki/Network_address_translation) (NAT) is similar to a proxy, but operates in layer 3.

In the client configuration of layer-3 NAT, configuring the gateway is sufficient. However, for the client configuration of a layer 7 proxy, the destination of the packets that the client generates must always be the proxy server (layer 7), then the proxy server reads each packet and finds out the true destination.

Because NAT operates at layer-3, it is less resource-intensive than the layer-7 proxy, but also less flexible. As we compare these two technologies, we might encounter a terminology known as 'transparent firewall'. **Transparent firewall** means that the proxy uses the layer-7 proxy advantages without the knowledge of the client. The client presumes that the gateway is a NAT in layer 3, and it does not have any idea about the inside of the packet, but through this method, the layer-3 packets are sent to the layer-7 proxy for investigation.

**DNS proxy**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=32)]

A [DNS](https://en.wikipedia.org/wiki/Domain_Name_System) proxy server takes DNS queries from a (usually local) network and forwards them to an Internet Domain Name Server. It may also cache DNS records.

**Proxifiers**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=33)]

Some client programs "SOCKS-ify" requests,[[32]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-32) which allows adaptation of any networked software to connect to external networks via certain types of proxy servers (mostly SOCKS).

**Residential proxy**[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=34)]

A residential proxy is an intermediary that uses a real IP address provided by an Internet Service Provider (ISP) with physical devices such as mobiles and computers of end-users. Instead of connecting directly to a server, residential proxy users connect to the target through residential IP addresses.[[33]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-33) The target then identifies them as organic internet users. It doesn’t let any tracking tool identify the reallocation of the user. Any residential proxy can send any number of concurrent requests and IP addresses are directly related to a specific region.[[34]](https://en.wikipedia.org/wiki/Proxy_server#cite_note-34)

See also[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=35)]

* [Darknet](https://en.wikipedia.org/wiki/Darknet)
* [SMTP proxy](https://en.wikipedia.org/wiki/SMTP_proxy)
* [Web accelerator](https://en.wikipedia.org/wiki/Web_accelerator) which discusses host-based HTTP acceleration
* [Web cache](https://en.wikipedia.org/wiki/Web_cache)
* [Application firewall](https://en.wikipedia.org/wiki/Application_firewall)
* [Captive portal](https://en.wikipedia.org/wiki/Captive_portal)
* [Distributed Checksum Clearinghouse](https://en.wikipedia.org/wiki/Distributed_Checksum_Clearinghouse)
* [Internet privacy](https://en.wikipedia.org/wiki/Internet_privacy)
* [Proxy list](https://en.wikipedia.org/wiki/Proxy_list)
* [SOCKS](https://en.wikipedia.org/wiki/SOCKS) an alternative firewall traversal protocol supported by many applications

References[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=36)]

* 1. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-1) [World-Wide Web Proxies](http://courses.cs.vt.edu/~cs4244/spring.09/documents/Proxies.pdf), [Ari Luotonen](https://en.wikipedia.org/wiki/Ari_Luotonen), April 1994
  2. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-2) "[A Survey of Techniques for Improving Efficiency of Mobile Web Browsing](https://www.researchgate.net/publication/329502453_A_Survey_of_Techniques_for_Improving_Efficiency_of_Mobile_Web_Browsing)", Concurrency and Computation: Practice and Experience, 2018
  3. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-3) [[1]](https://hal.inria.fr/inria-00444651/document), Marc Shapiro. Structure and Encapsulation in Distributed Systems: the Proxy Principle. Int. Conf. on Distr. Comp. Sys. (ICDCS), 1986, Cambridge, MA, USA, United States. pp.198--204, 1986, Int. Conf. on Distr. Comp. Sys. (ICDCS).
  4. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-nmap_4-0) [***b***](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-nmap_4-1) [*Lyon, Gordon*](https://en.wikipedia.org/wiki/Gordon_Lyon)*(2008). Nmap network scanning. US: Insecure. p. 270.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-9799587-1-7*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-9799587-1-7)*.*
  5. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-apache-forward-reverse_5-0) [*"Forward and Reverse Proxies"*](http://httpd.apache.org/docs/2.0/mod/mod_proxy.html#forwardreverse)*. httpd mod\_proxy. Apache. Retrieved 20 December 2010.*
  6. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-harvard_6-0) [***b***](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-harvard_6-1) [*"2010 Circumvention Tool Usage Report"*](http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf)*(PDF). The Berkman Center for Internet & Society at Harvard University. October 2010.*
  7. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-7) [*"How to Check if Website is Down or Working Worldwide"*](https://www.hostinger.co.uk/tutorials/website/how-to-check-if-website-is-working-worldwide/)*. Hostinger. 19 November 2019. Retrieved 14 December 2019.*
  8. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-Bypassing_a_Filtering_Proxy_8-0) [*"Using a Ninjaproxy to get through a filtered proxy"*](https://web.archive.org/web/20160309075844/http:/sitevana.com/webtech)*. advanced filtering mechanics. TSNP. Archived from*[*the original*](http://sitevana.com/webtech/)*on 9 March 2016. Retrieved 17 September 2011.*
  9. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-9) *Thomas, Keir (2006).*[*Beginning Ubuntu Linux: From Novice to Professional*](https://archive.org/details/beginningubuntul00keir)*. Apress.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-1-59059-627-2*](https://en.wikipedia.org/wiki/Special:BookSources/978-1-59059-627-2)*. A proxy server helps speed up Internet access by storing frequently accessed pages*
  10. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-rfc3143_10-0) *I. Cooper; J. Dilley (June 2001).*[*Known HTTP Proxy/Caching Problems*](https://tools.ietf.org/html/rfc3143)*.*[*IETF*](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force)*.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.17487/RFC3143*](https://doi.org/10.17487%2FRFC3143)*.*[*RFC*](https://en.wikipedia.org/wiki/RFC_(identifier))[*3143*](https://tools.ietf.org/html/rfc3143)*. Retrieved 17 May 2019.*
  11. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-rfc3135.2.1_11-0) [*"Layering"*](https://tools.ietf.org/html/rfc3135#section-2.1)*.*[*Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations*](https://tools.ietf.org/html/rfc3135)*.*[*IETF*](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force)*. June 2001. p. 4. sec. 2.1.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.17487/RFC3135*](https://doi.org/10.17487%2FRFC3135)*.*[*RFC*](https://en.wikipedia.org/wiki/RFC_(identifier))[*3135*](https://tools.ietf.org/html/rfc3135)*. Retrieved 21 February 2014.*
  12. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-12) *Durieux, T.; Hamadi, Y.; Monperrus, M. (2018).*[*Fully Automated HTML and Javascript Rewriting for Constructing a Self-Healing Web Proxy*](https://hal.archives-ouvertes.fr/hal-01746141/document)*. 2018 IEEE 29th International Symposium on Software Reliability Engineering (ISSRE). pp. 1–12.*[*arXiv*](https://en.wikipedia.org/wiki/ArXiv_(identifier))*:*[*1803.08725*](https://arxiv.org/abs/1803.08725)*.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/ISSRE.2018.00012*](https://doi.org/10.1109%2FISSRE.2018.00012)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-1-5386-8321-7*](https://en.wikipedia.org/wiki/Special:BookSources/978-1-5386-8321-7)*.*
  13. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-13) *Zhang, Xiaoyi; Ross, Anne Spencer; Caspi, Anat; Fogarty, James; Wobbrock, Jacob O. (2017). Interaction Proxies for Runtime Repair and Enhancement of Mobile Application Accessibility. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. pp. 6024–6037.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/3025453.3025846*](https://doi.org/10.1145%2F3025453.3025846)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*9781450346559*](https://en.wikipedia.org/wiki/Special:BookSources/9781450346559)*.*
  14. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-14) [*"Hot Tactics For Geo-Targeted Ads on Google & Bing"*](http://searchengineland.com/hot-tactics-for-geo-targeted-ads-on-google-bing-smx-east-173213)*. Retrieved 7 February 2014.*
  15. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-15) [*"Firewall and Proxy Server HOWTO"*](http://tldp.org/HOWTO/Firewall-HOWTO-11.html)*. tldp.org. Retrieved 4 September 2011. The proxy server is, above all, a security device.*
  16. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-16) [*"Sneaker Bot Supreme Proxy"*](https://www.geosurf.com/sneaker-residential-ips-proxy/)*. GeoSurf. Retrieved 24 September 2017.*
  17. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-rfc7230.5.3.2_17-0) [*"absolute-form"*](https://tools.ietf.org/html/rfc7230#section-5.3.2)*.*[*HTTP/1.1 Message Syntax and Routing*](https://tools.ietf.org/html/rfc7230)*.*[*IETF*](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force)*. June 2014. p. 41. sec. 5.3.2.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.17487/RFC7230*](https://doi.org/10.17487%2FRFC7230)*.*[*RFC*](https://en.wikipedia.org/wiki/RFC_(identifier))[*7230*](https://tools.ietf.org/html/rfc7230)*. Retrieved 4 November 2017. a client MUST send the target URI in absolute-form as the request-target*
  18. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-18) [*"Transparent Proxy Definition"*](https://web.archive.org/web/20130301235707/http:/www.ukproxyserver.org/transparent-proxy/)*. ukproxyserver.org. 1 February 2011. Archived from*[*the original*](http://www.ukproxyserver.org/transparent-proxy/)*on 1 March 2013. Retrieved 14 February 2013.*
  19. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-19) [*"Socket Capable Browser Plugins Result in Transparent Proxy Abuse"*](http://www.thesecuritypractice.com/the_security_practice/2009/03/socket-capable-browser-plugins-result-in-transparent-proxy-abuse.html)*. The Security Practice. 9 March 2009. Retrieved 14 August 2010.*
  20. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-20) [*"Vulnerability Note VU#435052"*](http://www.kb.cert.org/vuls/id/435052)*.*[*US CERT*](https://en.wikipedia.org/wiki/United_States_Computer_Emergency_Readiness_Team)*. 23 February 2009. Retrieved 14 August 2010.*
  21. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-21) [*"Subversion Dev: Transparent Proxy detection (was Re: Introduction\_"*](http://svn.haxx.se/dev/archive-2003-02/0257.shtml)*. Tracetop.sourceforge.net. Retrieved 16 November2014.*
  22. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-22) *Wessels, Duane (2004).*[*Squid The Definitive Guide*](https://archive.org/details/squiddefinitiveg00wess_703)*. O'Reilly. pp.*[*130*](https://archive.org/details/squiddefinitiveg00wess_703/page/n151)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-596-00162-9*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-596-00162-9)*.*
  23. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-23) *Marshall, James.*[*"CGIProxy"*](https://www.jmarshall.com/tools/cgiproxy/)*. Retrieved 12 November 2018.*
  24. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-24) [*"The Limits of Control"*](http://www.cfcl.com/rdm/Pubs/tin/P/199606.shtml)*. June 1996. Retrieved 12 November2018.*
  25. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-archive.fo_2013_25-0) [*"Glype® Proxy Script"*](https://archive.today/20130103162849/http:/www.glype.com/)*. glype.com. Archived from*[*the original*](https://www.glype.com/)*on 3 January 2013. Retrieved 17 May 2019.*
  26. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-26) [*"PHProxy"*](https://sourceforge.net/projects/poxy/)*. SourceForge.*
  27. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-27) [*"Google Trends"*](https://www.google.com/trends/explore?date=all&q=glype+proxy)*. Google Trends.*
  28. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-28) [*"Proxy Stats :: Get Proxi.es"*](http://getproxi.es/proxy-stats/)*. getproxi.es.*
  29. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-29) *Estrada-Jiménez, José (March 2017). "Online advertising: Analysis of privacy threats and protection approaches". Computer Communications.****100****: 32–51.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1016/j.comcom.2016.12.016*](https://doi.org/10.1016%2Fj.comcom.2016.12.016)*.*[*hdl*](https://en.wikipedia.org/wiki/Hdl_(identifier))*:*[*2117/99742*](https://hdl.handle.net/2117%2F99742)*.*
  30. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-Glater_30-0) [***b***](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-Glater_30-1) *Glater, Jonathan (25 January 2006).*[*"Privacy for People Who Don't Show Their Navels"*](https://www.nytimes.com/2006/01/25/technology/techspecial2/25privacy.html?_r=1)*. The New York Times. Retrieved 4 August 2011.*
  31. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-torproject_31-0) *The Tor Project.*[*"Tor: anonymity online"*](https://www.torproject.org/)*. Retrieved 9 January2011.*
  32. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-32) *Zwicky, Elizabeth D.; Cooper, Simon; Chapman, D. Brent (2000).*[*Building Internet Firewalls*](https://archive.org/details/buildinginternet00zwic/page/235)*(2nd ed.). p.*[*235*](https://archive.org/details/buildinginternet00zwic/page/235)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-1-56592-871-8*](https://en.wikipedia.org/wiki/Special:BookSources/978-1-56592-871-8)*.*
  33. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-33) [*"What are Residential Proxies?"*](https://oxylabs.io/blog/residential-proxies)*. oxylabs.io. Retrieved 29 May2020.*
  34. [**^**](https://en.wikipedia.org/wiki/Proxy_server#cite_ref-34) *Smith, Vincent (2019).*[*Go Web Scraping Quick Start Guide: Implement the power of Go to scrape and crawl data from the web*](https://books.google.co.in/books?id=jQGGDwAAQBAJ&pg=PA76&dq=Residential+proxy&hl=en&sa=X&ved=0ahUKEwiI_t_a2tnpAhVaAXIKHZ0PCzkQ6AEIJzAA#v=onepage&q=Residential%20proxy&f=false)*. Packt Publishing Ltd.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-1-78961-294-3*](https://en.wikipedia.org/wiki/Special:BookSources/978-1-78961-294-3)*.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=Proxy_server&action=edit&section=37)]

* [Proxy software and scripts](https://curlie.org/Computers/Internet/Proxying_and_Filtering/Products_and_Tools/Software) at [Curlie](https://en.wikipedia.org/wiki/Curlie)
* [Free web-based proxy services](https://curlie.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/CGI_Proxy) at [Curlie](https://en.wikipedia.org/wiki/Curlie)
* [Free http proxy servers](https://curlie.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists) at [Curlie](https://en.wikipedia.org/wiki/Curlie)