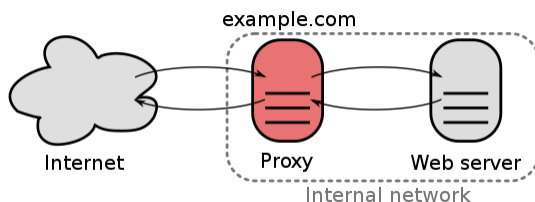


# Reverse proxy

In [computer networks](#), a **reverse proxy** is the application that sits in front of back-end applications and forwards client (e.g. browser) requests to those applications. Reverse proxies help increase scalability, performance, resilience and security. The resources returned to the client appear as if they originated from the web server itself.<sup>[1]</sup>



*Example scenario: A client on the Internet (cloud on the left) makes a request to a **reverse proxy** server (red oval in the middle). The proxy inspects the request, determines that it is valid and that it does not have the requested resource in its own cache. It then forwards the request to some internal web server (oval on the right). The internal server delivers the requested resource back to the proxy, which in turn delivers it to the client. The client on the Internet is unaware of the internal network, and cannot tell whether it is communicating with a proxy or directly with a web server.*

Large websites and [content delivery networks](#) use reverse proxies, together with other techniques, to [balance the load](#) between internal servers. Reverse proxies can keep a [cache](#) of static content, which further reduces the load on these internal servers and the internal network. It is also common for reverse proxies to add features such as [compression](#) or [TLS encryption](#) to the communication channel between the client and the reverse proxy.<sup>[2]</sup>

Reverse proxies are typically owned or managed by the [web service](#), and they are accessed by clients from the public Internet. In contrast, a [forward proxy](#) is typically managed by a client (or their company) who is restricted to a private, internal network, except that the client can ask the forward proxy to retrieve resources from the public Internet on behalf of the client.

Reverse proxy servers are implemented in popular [open-source web servers](#) such as [Apache](#), [Nginx](#), and [Caddy](#). This software can inspect HTTP headers, which, for example, allows it to present a single [IP address](#) to the Internet while relaying requests to different internal servers based on the [domain name](#) of the HTTP request. Dedicated reverse proxy servers such as the open source software [HAProxy](#) and [Squid](#) are used by some of the biggest websites on the Internet.

## Uses

---

- Reverse proxies can hide the existence and characteristics of [origin servers](#).
- [Application firewall](#) features can protect against common web-based attacks, like a [denial-of-service attack \(DoS\)](#) or distributed denial-of-service attacks (DDoS). Without a reverse proxy, removing malware or initiating [takedowns](#), for example, can be difficult.
- In the case of [secure websites](#), a web server may not perform [TLS encryption](#) itself, but instead offload the task to a reverse proxy that may be equipped with [TLS acceleration](#) hardware. (See [TLS termination proxy](#).)
- A reverse proxy can [distribute the load](#) from incoming requests to several servers, with each server supporting its own application area. In the case of reverse proxying [web servers](#), the reverse proxy may have to rewrite the [URL](#) in each incoming request in order to match the relevant internal location of the requested resource.
- A reverse proxy can reduce load on its origin servers by [caching static content](#) and [dynamic content](#), known as [web acceleration](#). Proxy caches of this sort can often satisfy a considerable number of website requests, greatly reducing the load on the origin server(s).
- A reverse proxy can optimize content by [compressing](#) it in order to speed up loading times.
- In a technique named "spoon-feeding",<sup>[3]</sup> a dynamically generated page can be produced all at once and served to the reverse proxy, which can then return it to the client a little bit at a time. The program that generates the page need not remain open, thus releasing server resources during the possibly extended time the client requires to complete the transfer.

- Reverse proxies can operate wherever multiple web-servers must be accessible via a single public IP address. The web servers listen on different ports in the same machine, with the same local IP address or, possibly, on different machines with different local IP addresses. The reverse proxy analyzes each incoming request and delivers it to the right server within the [local area network](#).
- Reverse proxies can perform [A/B testing](#) and [multivariate testing](#) without placing JavaScript tags or code into pages.
- A reverse proxy can add access authentication to a web server that does not have any authentication. [\[4\]\[5\]](#)

## Risks

---

- A reverse proxy can track all IP addresses making requests through it and it can also read and modify any non-encrypted traffic. Thus it can log passwords or inject malware, and might do so if compromised or run by a malicious party.
- When the transit traffic is encrypted and the reverse proxy needs to filter/cache/compress or otherwise modify or improve the traffic, the proxy first must decrypt and re-encrypt communications. This requires the proxy to possess the TLS certificate and its corresponding private key, extending the number of systems that can have access to non-encrypted data and making it a more valuable target for attackers.
- The vast majority of external [data breaches](#) happen either when hackers succeed in abusing an existing reverse proxy that was intentionally deployed by an organisation, or when hackers succeed in [converting](#) an existing Internet-facing server into a reverse proxy server. Compromised or converted systems allow external attackers to specify where they want their attacks proxied to, enabling their access to internal networks and systems.
- Applications that were developed for the internal use of a company are not typically hardened to public standards and are not necessarily designed to withstand all hacking attempts. When an organisation allows external access to such internal applications via a reverse proxy, they might unintentionally increase their own attack surface and invite hackers.
- If a reverse proxy is not configured to filter attacks or it does not receive daily updates to keep its attack signature database up to date, a [zero-day](#) vulnerability can pass through unfiltered, enabling attackers to gain control of the system(s) that are behind the reverse proxy server.

- Using the reverse proxy of a third party (e.g. [Cloudflare](#), Imperva) places the entire [triad of confidentiality, integrity and availability](#) in the hands of the third party who operates the proxy.
- If a reverse proxy is fronting many different domains, its outage (e.g. by a misconfiguration or DDoS attack) could bring down all fronted domains.<sup>[6]</sup>
- Reverse proxies can also become a [single point of failure](#) if there is no other way to access the back end server.

## See also

---

- [Network address translation](#)

## References

---

1. *"Forward and reverse proxies"* ([http://httpd.apache.org/docs/current/mod/mod\\_proxy.html](http://httpd.apache.org/docs/current/mod/mod_proxy.html)) . The Apache Software Foundation. Retrieved 26 August 2018.
2. *"Proxy servers and tunneling"* ([https://developer.mozilla.org/en-US/docs/Web/HTTP/Proxy\\_servers\\_and\\_tunneling](https://developer.mozilla.org/en-US/docs/Web/HTTP/Proxy_servers_and_tunneling)) . MDN Web Docs. Retrieved 6 December 2020.
3. *"squid-cache wiki entry on "SpoonFeeding" "* (<http://wiki.squid-cache.org/SpoonFeeding>) . Francesco Chemolli. Retrieved 9 February 2011.
4. *"Possible to add basic HTTP access authentication via HAProxy?"* (<http://serverfault.com/questions/239749/possible-to-add-basic-http-access-authentication-via-haproxy>) . serverfault.com.
5. Server, Caddy Web. *"forward\_auth (Caddyfile directive) - Caddy Documentation"* ([https://caddyserver.com/docs/caddyfile/directives/forward\\_auth#examples](https://caddyserver.com/docs/caddyfile/directives/forward_auth#examples)) . caddyserver.com. Retrieved 22 May 2022.
6. *"Cloudflare outage knocks out major sites and services, including Discord"* (<https://finance.yahoo.com/news/cloudflare-outage-knocks-major-sites-170213763.html>) . finance.yahoo.com. Retrieved 14 December 2020.

Retrieved from

["https://en.wikipedia.org/w/index.php?](https://en.wikipedia.org/w/index.php?)

title=Reverse\_proxy&oldid=1114110462"

---

Last edited 3 months ago by Guy Harris

WIKIPEDIA

---