Engineer

Reverse proxy

← a server that receives requests for an origin server

What it is

A reverse proxy is a server that receives requests at a website's public address and forwards them to the service that can answer. A browser connects to the proxy, which sends a request upstream and relays the response. The browser can keep using the same domain even when the application moves to a different machine, port or internal address. The HTTP standard calls this role a gateway. The name describes which side it represents. The operator of the website puts it in front of the origin. A forward proxy is used by a client to contact destinations on the client's behalf.

Consider a page that loads a report from `/api/reports/42`. The browser requests the path on the same host that served the page. The proxy sends paths beginning with `/api/` to the application and serves the introduction from another upstream. Both services can change independently while the browser has one public address. In this arrangement the proxy receives HTTP messages. Some products can also pass encrypted TCP connections through to a backend. A listener doing that has access to connection information and the visible fields in a TLS handshake, when available. It needs to terminate TLS to inspect an encrypted HTTP path.

A reverse proxy can sit in front of one application. Distributing work among equivalent servers is load balancing and becomes relevant when several can answer the same request. Hosting several paths on one domain is routing and can work with one backend per path. Many products do both jobs. Drawing the public address, the routing rule and the point that changes the connection makes the design easier to review than listing product names alone.

Use the concept in a decision

Put “What is a reverse proxy?” to work in a real decision. We can help relate the concept to the system you are building or buying. Wi-Fi, firewalls and remote access set up so staff can work from anywhere and only the right people get in.

Explore our services Get in touch →

Test the assumptions behind the term

Use the explanation and linked work to frame questions for your project. We can examine the assumptions with you before a tool is chosen. Managed 30 Ubuntu Linux VPS instances — 30 Linux servers managed, with recovery planned for

Managed 30 Ubuntu Linux VPS instances Get in touch →

Why it matters

One front door gives a team a place to say which parts of a service callers can reach. If the public host exposes HTTPS, the proxy can manage its certificate and forward to backends on a private network. This gives operators a common place to handle access logs, request limits or redirect rules. Each choice has a scope. An upload endpoint may need a larger body limit than a status endpoint, and a streaming response may need buffering disabled. Shared defaults stay easier to reason about when the exceptions follow the needs of a specific route.

The proxy also becomes a participant in the site’s trust model. It sees decrypted content when it terminates TLS, which can include session cookies, search paths and sensitive request bodies. Proxy-to-origin encryption can protect the next connection in transit. The operator of the terminator can still see the content it forwards. Choose who runs that component, who can read its logs and how long the logs are retained before making promises about where visitor information travels.

An extra hop changes how to investigate an outage. A `502` can indicate an invalid upstream response and a `504` means a gateway waited too long for an upstream response. An application can also originate its own error status. Take the response, the proxy event and the application log for the same test request. If the upstream never saw it, investigating the application’s handler is unlikely to explain the break.

What it looks like in practice

Engineer ApS’s DNS reconciliation case records a working CDN proxy that the company turned off. The site had been routed through the provider’s content network. The provider could then handle each visitor’s address and requested URL before the company received the request. The published case explains why

the company prioritized that privacy boundary over the attack protection the extra service offered. The DNS zone remained versioned and auditable. This example is a decision about who handles a request, and shows why DNS hosting and proxying deserve separate consideration.

For a small application, start with two named test requests. Send `/health` and `/api/reports/42?view=summary` to a staging hostname. Record the method and path seen at the application, the final status in the browser and the scheme and host in any redirect. Repeat the report request after changing the upstream address while keeping the public URL constant. This checks routing and redirect construction as well as proving that clients can follow the intended public contract during a move.

Try a larger request body and two concurrent browser sessions with different accounts before enabling any cache. Give each session a harmless, distinct marker that appears only on its own response. Confirm the proxy and origin agree about which responses can be stored in a shared cache. With the backend stopped, make one intentional request and check the resulting status, elapsed time and logs. This creates useful evidence during an allowed failure instead of waiting to discover how the path behaves in production.

Where it goes wrong

The application may trust an address supplied by the visitor. A request can include a `Forwarded` or `X-Forwarded-For` header before it reaches the proxy. Decide which intermediaries are trusted, overwrite or remove untrusted values at the boundary and restrict the origin to the expected peers. Agree with the application’s runtime on how many trusted hops it should use. Include a test containing a deliberately false address. Check both the application’s decision and its recorded address with public and permitted internal requests.

A second frequent failure appears as a redirect loop or a link to an internal port. The browser used HTTPS to reach the edge, and the application inferred HTTP from its immediate connection. Give the application a verified external scheme and host and test its generated redirects, callback links and cookies. Also check whether the route is intended to preserve or strip its prefix. A check on `/` alone can leave a problem on a nested path undiscovered.

Finally, an upstream timeout can tempt a proxy to try the request again. During a failed purchase submission, a missing response does not reveal whether the purchase was written. Have the application define the behavior for repeats before allowing automatic retries of operations that change state. Test the boundary with a backend that deliberately delays replying after processing a controlled request. Set a time budget and document which component ends the attempt.

Further reading

- RFC 9110, HTTP intermediaries explains the HTTP roles of proxies, gateways and tunnels.
- RFC 7239, Forwarded documents the forwarding header and its security and privacy implications.
- NGINX HTTP proxy module specifies request routing, header settings, buffering and timeouts.
- Caddy reverse_proxy directive describes upstream selection, forwarded headers and transport settings.
- Apache HTTP Server reverse proxy guide shows how the front server and its backends share work.

Glossary

Choose for your actual constraints

Bring the deployment path, the operational risks and the people on call. We can scope a change with checks, a recovery route and clear ownership.

See what it costs Get in touch →

Make the terminology practical

Ask how “What is a reverse proxy?” applies to your organisation. A concrete example from your current system is enough to start the discussion.

Explore our services

welcome@engineer.company +45 50 10 61 84 Copenhagen, Denmark

Take this page with you

Contact card

Carefully Crafted With Love by D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – present · Engineer ApS · All rights reserved.

Printed from https://engineer.company/glossary/reverse-proxy/