Reverse Proxy - what it is, how it works, and how to secure and scale your apps

Gridinsoft Help Center

What it is

A reverse proxy is a helper server that sits on the internet in front of your website or app. People connect to the proxy first, and it quietly passes the request to the real server in the background, then brings the answer back. Think of it like a bouncer and a concierge in one: it checks who is coming in, keeps the crowd organized, and helps things move faster. Many reverse proxies also handle HTTPS, speed things up with caching, and spread traffic across several back-end servers so nothing crashes during a rush.

Why it matters

Websites load faster and stay online during busy times. The real servers stay hidden, which makes attacks harder. One place to add security checks is easier than securing every single server.

How it works - quick tour

- Listens on the public web address and handles HTTPS.
- Looks at the request and decides which back-end server should answer.
- Can cache popular pages so they load instantly next time.
- Sends the reply back to the visitor like it came from the site itself.

Red flags

- People can reach your origin server directly by IP, skipping the proxy.
- Logins break because headers or links get mixed up after a change.
- Strange spikes of identical requests hint at someone trying to poison the cache.
- Health checks show one back-end doing all the work while others sit idle.

Prevent it

- Block direct access to the origin servers and force all traffic through the proxy.
- Turn on HTTPS, rate limits, and a basic web firewall if available.
- Only cache safe pages, not private areas like account settings.
- Keep an eye on uptime, response time, and error rates so you catch problems early.