

Reverse Proxy

Inhaltsverzeichnis

- [1 Funktionsweise](#)
- [2 Typische Einsatzbereiche](#)
- [3 Wichtige Hinweise](#)
- [4 Fazit](#)

Ein Reverse Proxy nimmt Anfragen aus dem Internet entgegen und leitet sie an interne Webserver oder Anwendungen weiter. Er dient der Lastverteilung, dem TLS-Abschluss, dem Caching und der Absicherung hinterliegender Dienste.

1 Funktionsweise

Clients sprechen nur den Reverse Proxy an. Dieser entscheidet anhand von Hostname, Pfad oder Regeln, welcher Backend-Dienst die Anfrage erhält, und gibt die Antwort wieder an den Client zurück.

- **TLS-Abschluss:** Zertifikate und HTTPS enden oft am Proxy.
- **Routing:** Weiterleitung an unterschiedliche Anwendungen hinter einer Domain.
- **Caching & Kompression:** Entlastung der Backend-Server.

2 Typische Einsatzbereiche

- Mehrere Dienste hinter einer öffentlichen IP oder Domain
- [Load Balancing](#) auf mehrere App-Server
- Schutz und Zentralisierung von Authentifizierung oder WAF-Regeln

3 Wichtige Hinweise

- Backend-Server sollten möglichst nicht direkt aus dem Internet erreichbar sein.
- Header wie X-Forwarded-For und X-Forwarded-Proto korrekt setzen und in Apps auswerten.
- Health-Checks und Timeouts verhindern, dass ausgefallene Backends Anfragen „hängen“ lassen.

4 Fazit

Ein Reverse Proxy ist die zentrale Eingangsschicht moderner Web- und Anwendungsinfrastrukturen: Er vereinfacht TLS, Routing und Absicherung, ohne dass jede Anwendung öffentlich exponiert werden muss.