Engineer

# Reverse Proxy

← Server, der Anfragen für einen Webdienst entgegennimmt

## Was es ist

Ein Reverse Proxy nimmt Anfragen für einen Webdienst entgegen. Der Browser verbindet sich mit der öffentlichen Adresse des Angebots. Dort empfängt der Proxy die Anfragen und leitet sie an den zuständigen Server weiter. Die Antwort gelangt über denselben Proxy zum Browser. Der Server hinter dem Proxy heißt Ursprungsserver. Er kann seinen Port wechseln oder in ein anderes internes Netz umziehen, während die Besucherinnen und Besucher weiterhin dieselbe Adresse verwenden. In der HTTP-Spezifikation heißt diese Rolle Gateway. Ein Forward Proxy sitzt auf der Seite des Clients und stellt ausgehende Verbindungen in dessen Auftrag her.

Auf einer Website kann der Pfad `/api/berichte/42` zum Berichtsdienst führen und die Startseite von einem anderen Server stammen. Für den Browser gehören beide Antworten zur gleichen öffentlichen Domain. Der Proxy kann entscheiden, an welchen Dienst er einen Pfad weitergibt. Können mehrere gleichwertige Server die Arbeit übernehmen, lässt sich außerdem die Last zwischen ihnen verteilen. Beide Aufgaben können im selben Produkt stecken. Schon ein einzelner Dienst hinter dem öffentlichen Eingang reicht für die erste Aufgabe.

Manche Produkte geben eine verschlüsselte TCP-Verbindung direkt weiter. In diesem Modus stehen ihnen die Verbindungsdaten und gegebenenfalls sichtbare Angaben beim TLS-Verbindungsaufbau zur Verfügung. Für ein Routing anhand des verschlüsselten HTTP-Pfads braucht die Komponente die entschlüsselte HTTP-Nachricht. In einer Skizze helfen deshalb zwei Markierungen: die Stelle, an der die TLS-Verbindung des Browsers endet, und der Anfang einer gegebenenfalls neu verschlüsselten Verbindung zum Ursprungsserver.

### Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist ein Reverse Proxy?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. WLAN, Firewalls und Fernzugriff werden so eingerichtet, dass Mitarbeitende von überall arbeiten können und nur Berechtigte Zugang erhalten.

**Unsere Leistungen entdecken** Kontakt aufnehmen →

### Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 30 Ubuntu-Linux-VPS-Instanzen verwaltet — 30 verwaltete Linux-Server mit geplantem Wiederherstellungsweg

**30 Ubuntu-Linux-VPS-Instanzen verwaltet** Kontakt aufnehmen →

## Warum es wichtig ist

Ein definierter Zugang macht verständlich, welche Dienste von außen erreichbar sind. Der Proxy kann das Zertifikat für den öffentlichen Namen verwalten. Die Anwendungen können in einem privaten Netz liegen. Außerdem lassen sich an dieser Stelle Regeln für Zugriffsprotokolle, Umleitungen und Größenlimits anwenden. Stimmen Sie Abweichungen auf den konkreten Pfad ab. Eine Schnittstelle für große Uploads hat andere Anforderungen als eine Statusseite. Bei einer laufenden Übertragung kann es sinnvoll sein, Teilantworten sofort weiterzugeben.

Wo der Proxy TLS beendet, kann sein Betreiber die weitergereichten Informationen verarbeiten. Dazu gehören unter Umständen Cookies, Suchbegriffe im Pfad und Inhalte, die der Browser mit der Anfrage sendet. Eine verschlüsselte Verbindung zum Ursprung schützt den zweiten Abschnitt während des Transports. Der Entschlüsselungspunkt bleibt Teil der Vertrauensgrenze. Klären Sie, wer den Proxy betreibt, wer Zugriff auf Protokolle erhält und wie lange diese Daten gespeichert werden.

Der zusätzliche Abschnitt verändert die Fehlersuche. Ein Gateway kann bei einer ungültigen Antwort des nächsten Servers den Status `502` liefern. Die Antwort `504` sagt, dass eine benötigte Antwort nicht rechtzeitig eingetroffen ist. Die Anwendung kann auch selbst eine Fehlerantwort erzeugen. Suchen Sie in beiden Protokollen nach demselben kontrollierten Aufruf. Gibt es am Ursprung keinen Eingang, sollten die Verbindungsdaten vom Proxy zum Ursprung Teil der Untersuchung sein.

## Wie es in der Praxis aussieht

Im Fallbeispiel zur Verwaltung der DNS-Zone als Code beschreibt Engineer ApS einen eingerichteten CDN-Proxy, der funktionierte und später abgeschaltet wurde. Im Proxybetrieb hätte das Netz des Anbieters die Adresse und die angefragte URL jedes Besuchers vor dem Unternehmen verarbeitet. Das Unternehmen gewichtete diesen Eingriff in die Privatsphäre höher als den zusätzlichen Schutz gegen Angriffe. Der dokumentierte, überprüfbare DNS-Bestand blieb bestehen. Das Beispiel zeigt, dass sich DNS-Betrieb und die Weiterleitung von Webanfragen getrennt beurteilen lassen.

Rufen Sie in einer Testumgebung `/health` und `/api/berichte/42?ansicht=kurz` auf. Prüfen Sie Methode und Pfad am Ursprung. Beobachten Sie im Browser den Status, das Ziel einer eventuellen Umleitung und das dort verwendete Schema. Ändern Sie anschließend die interne Adresse des Berichtsdienstes und wiederholen Sie beide Aufrufe am selben öffentlichen Namen. So sehen Sie, ob vorhandene Links nach einem kontrollierten Umzug weiter funktionieren.

Vor dem Einschalten eines gemeinsamen Caches sind zwei getrennte Testsitzungen mit unterschiedlichen Konten hilfreich. In jeder Antwort soll eine harmlose, eindeutige Markierung erscheinen. Prüfen Sie, dass beide Sitzungen ihren eigenen Inhalt behalten. Schalten Sie schließlich den Ursprungsdienst im Test gezielt aus. Erfassen Sie den Status aus Sicht des Browsers, die Wartezeit und den passenden Protokolleintrag. Damit erhalten Sie einen Vergleichswert für die Fehlersuche während des Betriebs.

## Wo es schiefgeht

Ein Client kann `Forwarded` oder `X-Forwarded-For` bereits in seiner Anfrage mitsenden. Die Anwendung braucht eine klare Liste der Zwischenstellen, deren Angaben sie annehmen darf. Entfernen oder ersetzen Sie unzuverlässige Werte am Übergang und beschränken Sie direkte Verbindungen zum Ursprung. Ergänzen Sie einen Test mit einer absichtlich falschen Adresse. Vergleichen Sie den protokollierten Wert mit der Adresse, auf deren Grundlage die Anwendung ihre Zugriffsregeln anwendet.

Eine Umleitung verrät häufig, dass Backend und Proxy verschiedene öffentliche Adressen voraussetzen. Der Browser kam über HTTPS, und die Anwendung hat einen Rücksprung mit HTTP oder mit einem internen Port gebaut. Geben Sie der Anwendung verifizierte Angaben zum öffentlich erreichbaren Schema und Host.

Prüfen Sie den kompletten Anmeldeablauf mit seinen Weiterleitungen und Cookies. Bei Regeln, die ein Pfadpräfix entfernen, gehört auch ein verschachtelter Pfad mit Parametern in den Test.

Ein neues Senden nach einem Timeout kann eine Zahlung doppelt auslösen. Die erste Anfrage kann am Ursprung verarbeitet worden sein, bevor der Proxy das Warten abbricht. Legen Sie vor automatischen Wiederholungen fest, wie die Anwendung mit wiederholten Aufrufen umgeht. Simulieren Sie eine kontrollierte Bearbeitung, bei der das Ergebnis gespeichert wird und die Antwort erst später folgt. So sehen Sie, welche Komponente abbricht und anhand welcher Kennung die Anwendung mehrere Versuche derselben Aktion erkennt.

## Weiterführende Lektüre

- RFC 9110 zu HTTP-Zwischenstellen definiert Proxy, Gateway und Tunnel.
- RFC 7239 zu Forwarded beschreibt das Feld und Fragen zu Sicherheit und Datenschutz.
- HTTP-Proxymodul von NGINX dokumentiert Pfadregeln, Header und Wartezeiten.
- Reverse-Proxy-Direktive von Caddy erklärt die Auswahl des Ursprungs und die übermittelten Header.
- Reverse-Proxy-Leitfaden des Apache HTTP Servers zeigt, wie der öffentliche Server mehrere Dienste erreichbar macht.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

**Preise ansehen** Kontakt aufnehmen →

# Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist ein Reverse Proxy?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

**Unsere Leistungen entdecken**

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

**Mit Sorgfalt und Liebe gestaltet von D.**

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

**Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.**

**Gedruckt von https://engineer.company/de/glossary/reverse-proxy/**