Engineer

Proxy

Server, der eine Anfrage in Ihrem Namen weiterleitet

Was es ist

Ein Proxy ist ein Programm zwischen einem Client und dem Server, den dieser erreichen will. Es nimmt die Anfrage des Clients an, stellt eine eigene Anfrage an den nächsten Rechner und gibt die Antwort zurück. Der Client spricht mit dem Proxy, der Proxy mit dem Server; die beiden Enden teilen sich daher nie eine Verbindung. Es gibt mehrere Arten von Proxys. Bei jeder Art hilft die Frage, wer den Proxy dort platziert hat.

Die HTTP-Spezifikation selbst, RFC 9110, benennt drei übliche Vermittler. Ein Proxy im engen Sinn ist vom Client gewählt, meist über eine lokale Einstellung im Browser oder eine Umgebungsvariable. Ein Gateway, im RFC auch Reverse Proxy genannt, sitzt auf der Serverseite: Gegenüber jedem, der eine Verbindung herstellt, verhält es sich wie der Ursprungsserver, während es jede Anfrage nach innen an einen oder mehrere dahinterliegende Server weiterleitet. Ein Tunnel reicht Bytes ungelesen zwischen zwei Verbindungen weiter und nimmt nach dem Öffnen nicht mehr selbst am Gespräch teil. Ein Client fordert ihn mit der Methode CONNECT unter Angabe von Host und Port an und baut anschließend durch ihn eine TLS-Verbindung zwischen den Endpunkten auf. Der RFC ergänzt eine vierte, von niemandem gewählte Art: den Interception Proxy, oft transparenter Proxy genannt. Er leitet am Netzwerkrand ausgehenden Verkehr auf Port 80 um, wie es öffentliche Zugangspunkte und Unternehmensfirewalls tun.

Jeder Vermittlungsschritt ist eine eigene Verbindung. Im Diagramm des RFC stehen drei Vermittler zwischen Browser und Ursprungsserver, also gibt es vier Verbindungen. Einstellungen wie keep-alive oder ein Zeitlimit gelten jeweils für eine davon. HTTP fordert zudem, dass ein Proxy sich zu erkennen gibt: Er muss jeder weitergeleiteten Nachricht ein Via-Headerfeld hinzufügen. So wird eine Schleife oder ein unerwarteter Vermittler in einem Trace sichtbar.

HTTP ist nur eine Schicht. Ein SOCKS-Proxy, dessen Version 5 im RFC 1928 vom März 1996 beschrieben ist, reicht TCP-Verbindungen und UDP-Datagramme weiter, ohne ihren Inhalt zu lesen. Jedes Protokoll kann ihn daher verwenden. Tor ist ein bekanntes Beispiel: Standardmäßig lauscht es auf Port 9050 auf SOCKS-Verbindungen lokaler Anwendungen.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist ein 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

Wer den Proxy betreibt, kann den Verkehr lesen. Bei unverschlüsseltem HTTP umfasst das jeden Header und jeden Nachrichtenrumpf. Durch einen CONNECT-Tunnel sieht er Hostnamen und Port; der Rest ist TLS zwischen Client und Server. Ein Reverse Proxy, der TLS terminiert, sieht alles im Klartext. Das ist seine Aufgabe, denn zur Weiterleitung muss er die Anfrage lesen. Den Reverse Proxy eines anderen Unternehmens vor eine Website zu setzen, wie es ein Content Delivery Network tut, gibt diesem Unternehmen deshalb die Adresse jedes Besuchers und jede URL, bevor die Website sie selbst sieht. Für einen angegriffenen Shop kann das die richtige Abwägung sein. Es bleibt eine Datenschutzentscheidung, die auf der Datenschutzseite stehen sollte.

Die zweite Folge betrifft die Informationen, die der Server erhält. RFC 7239 beschreibt den Verlust deutlich: Hinter einem Proxy scheinen Anfragen von dessen Adresse zu kommen. Ein Log, ein Ratenlimit, eine Sperrliste oder eine auf die Clientadresse gestützte Erlaubnisliste sieht dann für alle dieselbe Adresse. Die übliche Korrektur ist ein Header, der die ursprüngliche Adresse weiterträgt: das standardisierte Feld Forwarded aus RFC 7239 oder das ältere X-Forwarded-For. Welcher Kopie dieses Headers vertraut werden darf, ist der Ausgangspunkt der meisten Probleme.

Drittens verändert ein Proxy die Bedeutung eines Fehlers. Ein 502 Bad Gateway oder 504 Gateway Timeout stammt von einem Vermittler und bezieht sich auf den dahinterliegenden Server: Der Proxy erhielt eine ungültige Antwort oder keine rechtzeitige. Ein 407 bedeutet, dass der Proxy selbst Zugangsdaten verlangt, bevor er etwas weiterleitet. Zu wissen, welcher Rechner den Fehler erzeugte, ist die halbe Diagnose.

Viertens verwenden viele Proxys Caches. RFC 9111 nennt einen Cache, der Antworten für mehr als einen Nutzer speichert, einen gemeinsamen Cache, meist Teil eines Vermittlers. Er macht die Auslieferung einer Website schneller und billiger. Zugleich kann dort eine für eine Person bestimmte Antwort eine andere erreichen.

Wie es in der Praxis aussieht

Im August 2026 überführte das Unternehmen seine DNS-Zone mit etwa zwanzig Einträgen ins Repository und glich sie mit der Cloudflare-API ab. Den Webverkehr durch das CDN des Anbieters als Reverse Proxy zu leiten war Teil der Arbeit. Anschließend wurde ein funktionierender CDN-Proxy vor der Website aus Datenschutzgründen wieder abgebaut. Der Einwand galt seiner Position: Die Adresse jedes Lesers und jeder angefragte Pfad würden zuerst einen Dritten erreichen. Für ein Unternehmen, das seinen Lesern sagt, niemand beobachte sie, wog das schwerer als der damit erkaufte Angriffsschutz.

Im folgenden Monat Leser aus dem ohnehin vorhandenen Zugriffsprotokoll des Webservers zu zählen bedeutete, mit Proxys umzugehen, die das Unternehmen nicht selbst betreibt. Das Zugriffsprotokoll verwirft sieben Header, die eine Clientadresse weitergeben, bevor es eine Zeile schreibt. Der Log-Encoder kopiert Header unverändert. Ohne diesen Schritt wäre daher die unmaskierte Adresse eines Lesers hinter einem Unternehmensproxy unter einem Headernamen gespeichert worden, den die Maskierungsregel nicht abdeckte.

Als die Website im selben Monat einen Onion-Spiegel in Tor erhielt, wurde der eigene Proxyport des Tor-Daemons für ausgehenden Verkehr in seiner Konfiguration deaktiviert. Der Onion-Dienst wird über Circuits erreicht, die der Daemon nach außen aufbaut. Die Veröffentlichung dieses Spiegels erfordert deshalb keinen gesonderten eingehenden Internetport. Da sein SOCKS-Listener deaktiviert ist, bietet dieser Tor-Daemon lokalen Anwendungen keinen ausgehenden Proxy an.

Wo es schiefgeht

Jede Anfrage im Log kommt von derselben Adresse. Die Anwendung steht hinter einem Reverse Proxy und zeichnet die Adresse der empfangenen Verbindung auf, also die des Proxys. Ein Ratenlimit drosselt dann alle gleichzeitig. Eine Sperre eines Werkzeugs zur Angriffserkennung sperrt den Proxy und damit alle Nutzer. Lassen Sie den Proxy die Clientadresse in einem Header weitergeben und konfigurieren Sie die Anwendung so, dass sie diesen Header nur bei Verbindungen von der Adresse des Proxys selbst liest. In nginx ist das die Direktive set_real_ip_from des realip-Moduls; die meisten Webframeworks haben eine entsprechende Einstellung für vertrauenswürdige Proxys.

Ein Client wählt seine Adresse selbst, indem er einen Header sendet. Die Anwendung liest X-Forwarded-For bei jeder Anfrage, auch bei direkt eintreffenden Anfragen und solchen, die bereits einen gefälschten Headerwert enthalten. RFC 7239 hält ausdrücklich fest, dass jeder Knoten unterwegs das Feld ändern kann, einschließlich des Clients. Vertrauen Sie nur den von Ihrem eigenen Proxy hinzugefügten Einträgen, von rechts gezählt. Binden Sie die Anwendung an Loopback oder ein privates Netzwerk, damit der Proxy der einzige Zugang bleibt.

Das vermeintlich anonymisierte Log enthält vollständige Adressen. Die Clientadresse ist in dem überprüften Feld maskiert, reist aber zugleich in Forwarded, X-Forwarded-For, X-Real-IP und ähnlichen Headern mit. Ein Logger, der die empfangenen Header unverändert aufzeichnet, speichert diese Adressen vollständig. Listen Sie jeden Header auf, der eine Adresse tragen kann, entfernen oder maskieren Sie ihn beim Schreiben der Zeile, senden Sie dann eine Testanfrage und lesen Sie die Zeile auf dem Datenträger.

Seiten liefern 502 oder 504, während das Backendprotokoll schweigt. Der Fehler stammt vom Proxy. Ein 502 bedeutet eine ungültige Antwort: Das Backend war ausgefallen, lauschte auf einem anderen Port oder sprach unverschlüsseltes HTTP, wo der Proxy TLS erwartete, oder umgekehrt. Ein 504 bedeutet, dass das Backend länger als das Lesezeitlimit des Proxys brauchte, das nginx standardmäßig auf 60 Sekunden setzt. Lesen Sie zuerst das Fehlerprotokoll des Proxys: Es nennt die versuchte Upstream-Adresse. Erhöhen Sie ein Zeitlimit nur für nachweislich langsame Routen.

Ein Nutzer sieht die Seite eines anderen. Ein gemeinsamer Cache in einem Proxy oder Content Delivery Network speicherte eine persönliche Antwort, etwa eine mit einem Sitzungscookie zurückgegebene Kontoseite, und lieferte sie an die nächste Person mit derselben URL aus. Kennzeichnen Sie jede nutzerspezifische Antwort mit Cache-Control: private. Laut RFC 9111 darf ein gemeinsamer Cache sie dann nicht speichern. Verwenden Sie no-store, wenn nirgendwo eine Kopie verbleiben soll, und prüfen Sie die tatsächlich vom Proxy zurückgegebenen Header.

Weiterführende Lektüre

- RFC 9110, Abschnitt 3.7: Vermittler — die Definitionen von Proxy, Gateway, Tunnel und Interception Proxy.
- RFC 9110, Abschnitt 9.3.6: CONNECT — wie ein Client einen Proxy um einen Tunnel zu Host und Port bittet.
- RFC 7239: Forwarded-HTTP-Erweiterung — der standardisierte Header für die ursprüngliche Clientadresse mit den dabei zu beachtenden Einschränkungen.
- RFC 9111: HTTP-Caching — gemeinsame und private Caches und die Direktiven, die sie trennen.
- RFC 1928: SOCKS-Protokoll Version 5 — der protokollunabhängige Proxy, der TCP-Verbindungen und UDP-Datagramme weiterreicht.

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 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/proxy/