Proxy (Rechnernetz)

Quelle: de.wikipedia.org

Wird der Proxy als Netzwerkkomponente eingesetzt, bleibt einerseits die wahre Adresse des einen Kommunikationspartners dem anderen Kommunikationspartner gegenüber komplett verborgen, was eine gewisse Anonymität schafft. Als (mögliches) Verbindungsglied zwischen unterschiedlichen Netzwerken realisiert er andererseits eine Verbindung zwischen den Kommunikationspartnern selbst dann, wenn deren Adressen zueinander inkompatibel sind und eine direkte Verbindung nicht möglich wäre.

Im Unterschied zu einer einfachen Adressumsetzung (NAT) ist ein Proxy-Server dabei in der Lage, die Kommunikation selbst zu führen und zu beeinflussen, statt die Pakete ungesehen durchzureichen. Auf ein bestimmtes Kommunikationsprotokoll spezialisiert, wie z.B. HTTP oder FTP, kann er die Daten zusammenhängend analysieren, Anfragen filtern und bei Bedarf beliebige Anpassungen vornehmen, aber auch entscheiden, ob und in welcher Form die Antwort des Ziels an den tatsächlichen Client weitergereicht wird. Mitunter dient er dazu, bestimmte Antworten zwischenzuspeichern, damit sie bei wiederkehrenden Anfragen schneller abrufbar sind, ohne sie erneut vom Ziel anfordern zu müssen. Auf einem einzigen Gerät kommen oft mehrere *Dedicated Proxys* parallel zum Einsatz, um unterschiedliche Protokolle bedienen zu können.

Ein **Generischer Proxy** findet als protokollunabhängiger Filter auf einer Firewall Anwendung. Er realisiert dort ein port- und adressbasiertes Filtermodul, welches zudem eine (mögliche) Authentifizierung für den Verbindungsaufbau unterstützt. Daneben kann er für eine einfache Weiterleitung genutzt werden, indem er auf einem Port eines Netzwerkadapters lauscht und die Daten auf einen anderen Netzwerkadapter und Port weitergibt. Dabei ist er nicht in der Lage, die Kommunikation einzusehen, sie selbst zu führen und zu beeinflussen, da er das Kommunikationsprotokoll nicht kennt.

Technisch gesehen arbeitet ein typischer Proxy als in den Verkehr eingreifender Kommunikationspartner auf der OSI-Schicht 7, wobei die Verbindungen auf beiden Seiten terminiert werden (es handelt sich somit um zwei eigenständige Verbindungen), statt die Pakete wie ein NAT-Gerät einfach durchzureichen.

Sichtbarkeiten

Ein **konventioneller Proxy** tritt beiden Seiten selbst als vermeintlicher Kommunikationspartner gegenüber. Er wird von ihnen also bewusst angesprochen (adressiert). Hier bittet der Client den Proxy, stellvertretend für ihn die Kommunikation mit dem Zielsystem zu übernehmen. So wird z.B. der Internetbrowser derart konfiguriert, dass er sämtliche Internetanfragen nicht direkt zur Zieladresse schickt, sondern als Anforderung formuliert zum Proxy sendet.

Daneben gibt es den **transparenten Proxy** als spezielle Netzwerkkomponente, der sich einer der beiden Seiten gegenüber transparent (nahezu unsichtbar) verhält. Diese Seite adressiert direkt das Ziel und nicht den Proxy. Durch eine entsprechend konfigurierte Infrastruktur des Netzes wird die betreffende Anfrage dort automatisch über den Proxy geleitet, ohne dass der Absender dies bemerkt oder gar beeinflussen kann. Für die andere Seite aber stellt der Proxy weiterhin den zu adressierenden Kommunikationspartner dar, der stellvertretend für den tatsächlichen Kommunikationspartner angesprochen wird.

Somit tritt ein Proxy generell für wenigstens eine der beiden Seiten selbst als vermeintlicher Kommunikationspartner in Erscheinung.

Lage

Ein Proxy als *separate* Netzwerkkomponente befindet sich physisch zwischen dem Quell- und Zielsystem. Innerhalb eines IP-Netzes nimmt er eine Konvertierung der IP-Adresse vor, sobald die Pakete durch das Netz hindurch auf ihrem Weg zum Ziel den Proxy passieren. Dadurch lassen sich die wahre IP-Adresse des tatsächlichen Kommunikationspartners verbergen und einzelne Teilnehmer eines Netzes oder gar ganze Netzwerke selbst dann miteinander verbinden, wenn sie adressierungstechnisch inkompatibel zueinander sind.

Der *lokale Proxy* läuft dagegen direkt auf dem Quell- oder Zielsystem und befindet sich logisch

(jedoch nicht physisch) zwischen dem zu kontaktierenden Netzwerkdienst und dem anfragenden Client. Er wird meist als Filter oder Konverter eingesetzt. Da er vor Ort in Aktion tritt, also noch bevor die Pakete in das Netz geleitet werden (lokaler Proxy auf dem Quellsystem), oder nachdem die Pakete das Zielsystem erreicht haben (lokaler Proxy auf dem Zielsystem), ist dieser Proxy nicht in der Lage, die wahre IP-Adresse des Kommunikationssystems zu verbergen. Das unterscheidet ihn maßgeblich von anderen Proxys eines IP-Netzwerkes. Allerdings kann ein lokaler Proxy auf dem Quellsystem durchaus dabei behilflich sein, die Netzwerkanfrage automatisiert über einen externen Proxy zu schicken, wobei der lokale Proxy diese Art der Umleitung dann verwaltet und somit seinen Teil zur Anonymisierung der eigenen IP-Adresse beiträgt.

Mögliche Funktionen eines Proxys

Schutz der Clients

Der Proxy kann eine Schnittstelle zwischen dem privaten Netz und dem öffentlichen Netz bilden. Der Zugriff von Clients auf Webserver ist dann nur über den Proxy möglich, der die Verbindung aktiv kontrollieren kann.

Schutz der Server

Ein Proxyserver kann allgemein dazu verwendet werden, den eigentlichen Server in ein geschütztes Netz zu stellen, wodurch er vom externen Netz aus nur durch den Proxy erreichbar wird. Auf diese Weise versucht man den Server vor Angriffen zu schützen. Die Proxy-Software ist weniger komplex und bietet daher weniger Angriffspunkte.

Bandbreitenkontrolle

Der Proxy teilt verschiedenen Benutzern und Gruppen je nach Auslastung unterschiedliche Ressourcen zu. Der Proxy-Server Squid beherrscht dieses Verfahren, wobei er ebenso zum Schutz des Servers beitragen kann und Methoden unterstützt, die zu besserer Verfügbarkeit beitragen.

Verfügbarkeit

Über einen Proxyverbund lassen sich mit relativ geringem Aufwand Lastverteilung und Verfügbarkeit erreichen.

Inhaltliche Kontrolle häufig verwendeter Protokolle

Ein Proxy kann Softwaremodule enthalten, die auf ein bestimmtes Kommunikationsprotokoll spezialisiert sind. Diese sind dann in der Lage, die Pakete des jeweiligen Protokolls zu analysieren und dabei als Verbindungs- und Befehlsfilter zu fungieren.

Funktionserweiterung eines Netzwerkdienstes

Ein Reverse-Proxy kann den üblichen Funktionsumfang eines Dienstes erweitern, indem er dank der Analyse des Protokolls z.B. spezielle Statistiken erstellt, die der Dienst normalerweise nicht anbietet. Da er in der Lage ist, Anfragen selbst zu beantworten, sind beliebige weitere funktionelle Erweiterungen denkbar.

Protokollierung

Viele Proxys erlauben es, Verbindungen, die über sie laufen, zu protokollieren. Das ermöglicht statistische Auswertungen und Erkennen ungewollter Verbindungen.

Translating Proxy

Manche Proxys übersetzen ein Protokoll in ein anderes. Diese heissen dann Gateway, Transport, Agent.

Der lokale Proxy

Auch bei einer lokal auf dem Quell- oder Zielsystem installierten Proxysoftware wird intern eine Adresskonvertierung vorgenommen. Das ist Teil ihrer internen Arbeitsweise und kann sich auf

eine Umleitung des Ports beschränken, bezieht sich oft aber auf eine Umsetzung zu localhost (der so genannten Loopback-Schnittstelle 127.0.0.1).

Dedicated Proxy (Proxy-Server)

Ein Dedicated Proxy ist ein Dienstprogramm, das im Datenverkehr zwischen dem anfragenden Client und dem Zielsystem vermittelt. Er ist auf das Kommunikationsprotokoll spezialisiert, welches der Dienst verwendet, und kann daher die Kommunikation analysieren und bei Bedarf deren Inhalt manipulieren. Darüber hinaus ist er in der Lage, eigenständig Anfragen an den Kommunikationspartner zu senden und mitunter als Zwischenspeicher zu fungieren (also von sich aus auf eine Anfrage zu antworten, ohne sie erneut vom tatsächlichen Zielsystem anfordern zu müssen).

Zwischenspeicher (Cache)

Der Proxy kann gestellte Anfragen bzw. deren Ergebnis speichern. Wird die gleiche Anfrage erneut gestellt, kann diese aus dem Speicher beantwortet werden, ohne zuerst den Webserver zu fragen. Der Proxy stellt sicher, dass die von ihm ausgelieferten Informationen nicht allzu veraltet sind. Eine vollständige Aktualität wird in der Regel nicht gewährleistet. Durch das Zwischenspeichern können Anfragen schneller beantwortet werden und es wird gleichzeitig die Netzlast verringert. Beispielsweise vermittelt ein derartiger Proxy einer Firma den gesamten Datenverkehr der Computer der Mitarbeiter mit dem Internet.

Ausfiltern von Werbung

Werbung kann erhebliche Mengen an Datenverkehr erzeugen – viele Werbeflächen laden sich z.B. regelmässig neu. Was für den Privatanwender an einer ADSL-Leitung unproblematisch ist, kann beispielsweise für ein Netz von mehreren Dutzend Anwendern an dieser Leitung zum Problem werden.

Transparenter Proxy

Ein „Transparenter Proxy“ besteht grundsätzlich aus zwei Komponenten. Zunächst werden am Router die gewünschten Ports der Protokolle abgegriffen (beispielsweise über Iptables unter Einsatz eines Redirects) und dann an einen Proxy weitergeleitet. Für den Anwender ist die Verbindung über einen transparenten Proxy in der Benutzung nicht von einer direkten Verbindung über den Router zu unterscheiden. Das Vorhandensein eines transparenten Proxys bietet daher den Nutzen, dass eine Konfiguration der Proxyeinstellungen am einzelnen PC unterbleiben kann.

Reverse Proxy

Ein Proxy tritt im Falle des Reverse Proxys als vermeintliches Zielsystem in Erscheinung, wobei die Adressumsetzung dann in der entgegengesetzten Richtung vorgenommen wird und so dem Client die wahre Adresse des Zielsystems verborgen bleibt. Während ein typischer Proxy dafür verwendet werden kann, mehreren Clients seines internen (privaten – in sich geschlossenen) Netzes den Zugriff auf ein externes Netz zu gewähren, funktioniert ein Reverse Proxy genau andersherum.

Reverse Proxy als Weiterleitungsmodul einer Firewall

Die Reverse Proxys einer Firewall bieten zunächst die gleiche Funktionalität wie Port Forwarding und ermöglichen so einen von außen initiierten Verbindungsaufbau zu einem hinter der Weiterleitung liegenden Server des internen Netzes. Sobald sie als Dedicated Proxy arbeiten, können sie das Netzwerkprotokoll verstehen und sind dann zudem in der Lage, die Daten der Netzwerkpakete zu analysieren und zu bearbeiten. So können sie z.B. einen Virenscan vornehmen oder Regeln realisieren, die sich auf die Paketinhalte beziehen.

Demgegenüber gibt es auch Reverse Proxys, die nicht Bestandteil der Firewallsoftware sind und dennoch das Ziel verfolgen, aus dem externen Netz heraus auf einen internen Rechner zugreifen zu können, ohne jedoch die Firewall manuell entsprechend konfigurieren zu müssen. Dazu baut der interne Rechner zunächst eine Verbindung zu einem bestimmten externen Rechner auf, wodurch der externe Rechner über die Firewall hinweg mit dem internen Rechner kommunizieren kann. Läuft auf dem externen Rechner ein Reverse Proxy, so können nun auch

beliebige andere Rechner aus dem externen Netz auf den internen Rechner hinter der Firewall zugreifen, indem sie ihre Anfragen an den Reverse Proxy des externen Rechners schicken (der Reverse Proxy leitet die Anfragen an den internen Rechner weiter).

Reverse Proxy für eine Performance-Optimierung

Eine gänzlich andere Aufgabe kann ein Reverse Proxy erfüllen, der die Anfragen für einen Dienst entgegennimmt, um die Geschwindigkeit bzw. Zugriffsrate auf den Dienst zu verbessern oder funktionell zu erweitern. Er kann lokal auf dem Zielsystem installiert sein, oder auf einer separaten Hardware laufen, und arbeitet beispielsweise als HTTP-Accelerator, auch Surrogate Proxy genannt. Verbindungen aus dem Internet an einen Webserver werden durch den Proxy bearbeitet, der die Anfragen selbst beantwortet, sofern sie in dem eigenen Cache stehen, oder andernfalls an die nachgeordneten Dienste oder an einen entfernten Server weiterleitet.

Weitere Einsatzszenarien eines Reverse Proxys

Es gibt mehrere Gründe für den Einsatz eines Reverse Proxys:

Netzsicherheit

Der Reverse Proxy stellt ein weiteres Glied in der Sicherheitskette dar und trägt so zur Sicherheit der Webserver bei.

Single Sign-on

Der Reverse Proxy kann die Benutzer-Authentifizierung für mehrere Webserver übernehmen. Dadurch braucht sich der Benutzer nur einmal anzumelden, um die Dienste mehrerer Server zu nutzen.

Transparenter Proxy

Hier wird an den Clients nichts konfiguriert; sie richten ihre Anfragen an das Ziel auf die Ports 80 (HTTP), als ob sie eine direkte Verbindung zum Internet hätten. Die Infrastruktur des Netzes sorgt dafür, dass ihre Anfragen an den Proxy geleitet werden.