Proxy Server

Stand: 15.08.2022

Jeder Internetzugang besitzt eine eigene IP-Adresse, die beim Aufrufen einer Website an den dazugehörigen Server übermittelt wird. Sie gibt Auskunft über den Endpunkt, von dem aus ein User auf das Internet zugreift. Quasi wie ein digitales Klingelschild.

Wenn ein User diesen **direkten Rückschluss** auf seine IP-Adresse aus einem bestimmten Grund verhindern möchte oder der Zugriff damit nicht möglich ist, nutzt er Proxy-Server, die als Schnittstelle agieren. Aber sie bieten noch weitere Möglichkeiten.

Was ist ein Proxy-Server?

Proxy-Server sind **eigenständig arbeitende Programme**, die sich bei Bedarf zwischen die Kommunikation von zwei Rechnersystemen schalten. Sie agieren wie **Vermittler**, die den Datenaustausch steuern. Alle Anfragen gehen in dem Moment bei ihnen ein. Sie übergeben sie im Anschluss an die Zieladresse.

Greift ein Nutzer von seinem heimischen Laptop aus über einen Proxy-Server auf eine Internetseite zu, landet seine IP-Adresse im ersten Schritt bei ihm. Von dort aus wird die Person mit der **IP-Adresse des Servers** auf die gewünschte Website weitergeleitet. Die anvisierte Zielseite kann dabei nicht unterscheiden, ob die IP-Adresse zu einem natürlichen User oder einem Proxy-Server gehört.

Je nach Wirkrichtung verhindert der Proxy-Server die Übertragung von Seiten des Servers oder von Seiten des Users, um die jeweils andere Instanz zu schützen. Daher fungieren sie entweder als **Forward-Proxy** oder **Reverse-Proxy.**

Forward-Proxys helfen dabei, dass keine potenziell gefährlichen Daten aus dem Internet auf das **Endgerät des Nutzers** gelangen. Sie leiten jede Useranfrage, die über sie eingeht, um, sodass sie im Umkehrschluss die angeforderten Daten übertragen bekommen. Das private Netzwerk ist deswegen nicht an der direkten Kommunikation beteiligt. Die Daten leitet der Server erst nach einer Kontrolle weiter.

Daneben können Proxys auch **Webserver** vor schädlichen Zugriffen bewahren. **Reverse-Proxys** fangen die Anfragen von Online-Clients ab und geben sie erst an den Server weiter, nachdem sie sie überprüft haben.

Unterscheidung zwischen sichtbarem und transparentem Proxy

Die Verwendung eines Proxy-Servers ist nicht unbedingt in jedem Fall von beiden Kommunikationspunkten aus bekannt. **Transparente Proxys** agieren oft **unbemerkt** im Hintergrund. Sobald eine der beiden Seiten keine Kenntnis darüber hat, tritt dieser Fall ein. Der Nutzer oder die Website versuchen, die Daten unmittelbar zu senden, allerdings greift der Proxy dabei ein und leitet die Kommunikation um.

Verwenden die Beteiligten **gezielt** einen Proxy zur Kommunikation, ist das ein **sichtbarer Proxy**. Wie der Name schon vermuten lässt, tritt das Programm dabei in den Vordergrund und steuert die Anfrage.

Dedizierter vs. generische Proxy-Server

Neben der Unterscheidung, wie wahrnehmbar der Proxy agiert, unterscheiden sich verschiedene Proxy-Typen ebenfalls hinsichtlich ihrer **Flexibilität**. Bei der Übertragung von Daten zieht das Programm unterschiedliche Protokolle heran, je nachdem, ob beispielsweise Hypertext oder ganze Dateien transportiert werden sollen.

Ist ein Proxy-Server für ein **bestimmtes Protokoll** verantwortlich, handelt es sich um einen **dedizierten Proxy-Server**. **Generische Proxy-Server** hingegen kümmern sich um **mehrere Protokolle**, unter anderem SMTP- oder HTTP-Protokolle. Pro Netzwerk können daher einige dezidierte Proxy-Server aktiv sein, die sich um verschiedene Aufgabenbereiche kümmern.

Gründe für die Nutzung eines Proxy-Servers

Der Vorteil eines Proxy-Servers ist, dass **keine direkte Kommunikation** zwischen einem Endgerät und einer Website oder zwei Netzwerken stattfindet. Alle Datensätze, aus jeglicher Richtung, stehen dabei nicht im direkten Austausch, sondern der Proxy-Server kann diese bei Bedarf filtern. Dadurch setzen Nutzer sie zu unterschiedlichen Zwecken ein:

- Zwischenstation, die keine schädlichen Daten weitergibt
- schnellerer Abruf von gleichen Datensätzen
- anonyme Anfragen von beiden Seiten möglich

Funktionen

Proxy-Server erfüllen durch ihre Vielseitigkeit gleich mehrere Funktionen. Generell dienen sie als Schnittstelle zwischen Heimnetzwerken und öffentlichen Netzwerken. Außerdem kontrollieren sie die **Netzwerkbandbreite**, indem sie sie sinnvoll auf die vorhandenen Leitungen aufteilen. Dadurch entstehen keine Engpässe. Mithilfe eines Cache **entlasten** sie sie zusätzlich, da die Daten nicht bei jedem Abruf vom Server übergeben werden müssen. Eine der Hauptaufgaben ist der **Schutz** vor Netzwerkangriffen.

In allen Fällen dienen zwischengeschaltete Proxy-Server dazu, einzelnen Nutzern den **Zugriff** auf ein Netzwerk zu erlauben oder ihnen bestimmte Ressourcen zur Verfügung zu stellen.

Oftmals übernehmen Proxy-Server in der Praxis ebenfalls eine **Protokollierungsfunktion**, um die Aktivitäten innerhalb eines Netzwerks zu registrieren. Viele Internetnutzer greifen zudem auf Proxy-Server zurück, um die eigene IP-Adresse zu anonymisieren. Dadurch kann ihr Zugriff auf eine Website nicht von Tracking-Services erfasst werden.

Der Einsatz von **dedizierten Proxys** im Internet **vermindert die Serverlast** und macht Datenpakete leichter verfügbar. Darüber hinaus können diese Server zur Filterung und Sperrung von Inhalten in öffentlichen Netzwerken verwendet werden.

Arten und Anwendungsgebiete

Proxy-Server können sowohl im Internet als auch in eigenen Netzwerken eine Vermittlungsfunktion übernehmen. Darüber hinaus lassen sich unterschiedliche Arten bestimmen: Wird ein Proxy-Server als Teil eines Netzwerks verwendet, spricht man von einem **Netzwerk-Proxy**. Dieser transportiert Daten innerhalb eines Netzwerks von einem Sender zu einem Empfänger, ohne dass dabei die IP-Adresse des Senders übermittelt wird. So lassen sich Daten auch übertragen, wenn die Netzwerkadressen der Kommunikationspartner nicht kompatibel sind.

Ein **dedizierter Proxy** agiert nicht nur als Kommunikationsvermittler zwischen zwei Netzwerken oder Computern, sondern **beeinflusst** die Art der Kommunikation aktiv. Die zu übermittelnden Datenpakete kann er beispielsweise **verändern, filtern oder speichern**. Diese Zwischenspeicherung von Daten findet sich vor allem bei Dedicated Proxys im Internet, denn so sind Datenpakete bei einer erneuten Anfrage schneller verfügbar. Für die Übermittlung greift der Server dabei auf HTTP-Protokolle oder FTP-Protokolle zurück.

Proxy-Server, die auf einer **Firewall** installiert werden, werden **Circuit Level Proxy** genannt. In diesem Fall übernimmt der Server eine Filterfunktion in Hinblick auf die Zugriffe über bestimmte Adressen oder Ports. Deswegen kann beispielsweise erst auf eine Webseite zugegriffen werden, nachdem eine Authentifizierung stattgefunden hat. Circuit Level Proxy fallen in die Kategorie der **generischen Proxys.**

Einfluss auf die SEO

In Hinblick auf die Suchmaschinenoptimierung (SEO) **profitieren** Webseitenbetreiber von Proxy-Servern. Der Vorteil für Betreiber liegt darin, dass der **Grund** für häufige Seitenaufrufe durch die Programme von Suchmaschinen nicht erkannt werden kann. **Automatisierte Seitenaufrufe** spielen dabei vor allem in Hinblick auf die Platzierung einer Website in den SERPs eine Rolle.

Allerdings werden Proxy-Server auch im Rahmen der **Black Hat SEO** eingesetzt, um durch die Anwendung unlauterer Praktiken wie **Spam** die **Platzierung** einer Website in den **organischen Suchtreffern** kurzfristig zu verbessern. Durch die erhöhte Traffic-Rate erkennt der Algorithmus die Website fälschlicherweise als aktuell besonders relevant an.

Darüber hinaus können Websites mithilfe der **Manipulation der IP-Adresse** durch einen Reverse-IP-Proxy unterschiedliche Kennungen zugewiesen bekommen, obwohl alle Domains auf demselben Server liegen.

Greifen Personen über einen Proxy-Server auf eine Webseite zu, kann dieser Zugriff später **nicht** zu der entsprechenden Person **nachverfolgt** werden, da nur die IP-Adresse des Proxy-Servers im Logfile gespeichert wird. Infolgedessen erschweren die Programme die Analyse sowie Auswertung von Websitezugriffen.