Proxy Server

Was ist ein Proxy Server?

Das Wort Proxy bedeutet “im Namen eines anderen handeln”, und ein Proxy Server handelt im Namen des Benutzers. Ein Proxy Server (kurz: Proxy genannt) ist jeder Computer, der den Datenverkehr zwischen Netzwerken oder unterschiedlichen Übertragungs-Protokollen durchführt. Dieser Computer ist ein Zwischenserver, der Endbenutzer-Clients physikalisch vom Zielcomputer trennt, auf denen sie Informationen suchen. Je nach Anwendung, Unternehmensrichtlinien oder Anwendung bieten Proxy Server unterschiedliche Sicherheits-, Funktions- und Datenschutzstufen.

Bei der Verwendung eines Proxy Servers, läuft der Verkehr auf dem Weg vom Client zum Webserver über den Proxy. Die Informationen zur Anfrage kommen dann über denselben Proxy Server an den Client zurück. Es gibt jedoch Ausnahmen von dieser Regel. Der Server leitet die von der Website erhaltenen Daten an den Nutzer weiter.

Moderne Proxy Server leisten weit mehr als nur Webanfragen weiterzuleiten. Sie überwachen die Datensicherheit und Netzwerkleistung. Diese Server fungieren als Firewall und Webfilter, stellen gemeinsam genutzte Netzwerkverbindungen bereit und speichern Daten zwischen (cachen), um häufige Anfragen zu beschleunigen. Ein guter Proxy Server schützt Benutzer und das interne Netzwerk vor den schlechten Dingen, die versuchen, aus dem Internet in fremde Netzwerke einzudringen. Außerdem können Proxy Server ein hohes Maß an Privatsphäre bieten.

Was ist ein Circuit Level Proxy?

Der Generische Proxy (auch Circuit Level Proxy) besitzt einen spezifischen Filter-Algorithmus. So kann der Proxy als Firewall fungieren und bestimmte IP-Adressen oder Port für den Datenverkehr sperren. Dazu müssen noch nicht einmal Daten analysiert werden. Anders als sein Verwandter der Dedicated Proxy, manipuliert oder speichert der Generische Proxy Daten also nicht. Nach dem 7-schichtigen OSI-Modell operiert er auf der 3. und 4. Schicht, wo die Filterung von Adressen und Ports stattfindet.

Vorteile:

Schützt Adressen vor Offenlegung: Bei Proxies auf der Leitungsebene gibt es keine direkte Verbindung zwischen einem Anwendungsclient und einem Anwendungsserver. Proxy-Server verbergen die

Adressstruktur des Netzwerks und erschweren den Zugriff auf vertrauliche Informationen.

Bietet ein hohes Maß an Flexibilität: Wenn neue Internetdienste hinzugefügt werden, werden diese automatisch von Proxys unterstützt. Außerdem ist die Konfiguration von Clients für die Arbeit mit Proxys viel einfacher als Proxys auf Anwendungsebene. Anstatt jede Desktop-Anwendung neu zu konfigurieren, muss ein Client-Desktop nur einmal konfiguriert werden.

Ermöglicht umfassende Protokollierung: Systemadministratoren können den gesamten ein- und ausgehenden Datenverkehr in einem LAN protokollieren und analysieren.

Nachteile

Erfordert Client-Software: Client-Computer müssen so konfiguriert sein, dass alle TCP/IP-Daten über das Gateway auf Leitungsebene übertragen werden.

Bietet keine Sicherheit auf Anwendungsebene: Da die Server keine Kenntnis des zugrunde liegenden Anwendungsprotokolls haben, können sie anwendungsspezifische Informationen nicht so streng kontrollieren wie ein Gateway auf Anwendungsebene.

Wie funktioniert ein Proxy Server?

Ein Proxy Server (auch Dedicated Proxy) ist ein Dienstprogramm, das Anfragen zwischen einem Client und einem Server nach dem HTT-Protokoll vermittelt. Spricht man heute von einem Proxy, meint man damit in allen Fällen den Proxy Server. Ein Proxy fungiert im Datenverkehr zwischen Client und Server als Vermittler. Die vom Client gesendeten Anfragen werden vom Proxy Server an den Zielserver weiter geleitet. Die Rücksendung der Informationen erfolgt ebenfalls über den Proxy.

Für einen Proxy Server ist es möglich, die Kommunikation zu analysieren und deren Inhalt zu verändern. Der Zielserver kennt also die Identität des Clients nicht, falls der Verkehr über einen Proxy Server läuft. Ein gut arbeitender Proxy kann die Kommunikation zwischen Client und Server manipulieren. Ein Proxy kann auch Daten auf dem eigenen Server zwischenspeichern, um beispielsweise die Bearbeitungszeit zu verkürzen. Als Protokolle werden für die Datenübertragung neben dem HTTP-Protokoll auch HTTPS, SMTP und FTP Protokolle genutzt.

Was ist ein Forward Proxy?

Ein Forward Proxy Server sitzt zwischen dem Client und einem externen Netzwerk. Er wertet die ausgehenden Anforderungen aus und ergreift, falls nötig, Maßnahmen, bevor die Anforderung an die externe Ressource weitergeleitet wird.

Die meisten Proxy-Dienste, denen wir im Internet begegnen werden, sind Forward-Proxys. Virtual Private Networks und Webinhaltsfilter sind beides Beispiele für Forward-Proxys.

Was ist ein Reverse Proxy?

Ein Reverse Proxy Server befindet sich zwischen einem Netzwerk und mehreren anderen internen Ressourcen. Eine große Website kann Dutzende von Servern haben, die gemeinsam Anfragen von einer einzigen Domäne bedienen. Um dies zu erreichen, werden Client-Anfragen zu einer Maschine geleitet, die als Load Balancer fungieren. Je nach Auslastung gibt der Load Balancer den Datenverkehr dann an die einzelnen Server weiter. Reverse Proxies fungieren als Cache-Speicher und als Firewall, um die Netzsicherheit zu verbessern. Zu den beliebtesten Open Source Reverse Proxies gehören Varnish und Squid.

Nicht alle Proxies funktionieren gleich

Für Betreiber eines Proxy Servers ist es wichtig, zu wissen, welche Funktionen ein solcher Server bietet, um sicherzustellen, dass der Server für den Anwendungsfall geeignet ist.

Transparenter Proxy

Ein transparenter Proxy teilt Websites mit, dass es sich bei der Anfrage um einen Proxy-Server handelt. Er leitet die IP-Adresse des Anwenders weiter, um ihn beim Webserver zu identifizieren. Unternehmen, öffentliche Bibliotheken und Schulen verwenden häufig transparente Proxys für die Inhaltsfilterung: Sie lassen sich sowohl client- als auch serverseitig einfach einrichten.

Anonymer Proxy

Ein anonymer Proxy identifiziert sich selbst als Proxy, gibt jedoch die IP-Adresse des Anwenders nicht an die Website weiter. Dies hilft, Identitätsdiebstahl zu verhindern und die Surfgewohnheiten des Anwenders privat zu halten. Anonymer Server können auch verhindern, dass eine Website dem Anwender gezielte Marketinginhalte basierend auf seinem Standort liefert. Anonymes Surfen kann

verhindern, dass eine Website einige Techniken zur Anzeigenausrichtung verwendet, es gibt jedoch keine vollständige Garantie.

Aufgaben eines Proxys

Proxy werden in vielen Gebieten eingesetzt. Besonders für den Datenschutz verwenden auch immer mehr Privatnutzer einen Proxy Server. Die folgenden Dinge gehören zu den Aufgaben eines Proxys:

Schutz auf Seiten des Servers

Wird ein Proxy auf Serverseite genutzt, so kann er zum Schutz des Servers dienen. Dadurch können Clients den Zielserver nur über einen Proxy erreichen. Genauso ist auch der Proxy die erste Anlaufstelle für Angreifer, die eine Webseite hacken wollen.

Schutz des Nutzers

Bei der Nutzung öffentlicher Netzwerke besteht eine besondere Gefahr für den Datenschutz. Durch seine Funktion als Schnittstelle zwischen öffentlichen und privaten Netzen mildert der Proxy die Folgen. So verschickt ein Nutzer die Datenpakete nicht direkt an den Zielserver, sondern an den Proxy, der die Pakete weiterleitet. Der Proxy kann im Gegenzug kontrollieren, welche Pakete als Antwort an den Client zurückgeschickt werden und kann somit die Kommunikation kontrollieren.

Anonymes Surfen

Durch die Verwendung eines Proxys gelingt es den Client-Programmen, im Internet praktisch anonym zu bleiben. Die Identität und die wahre IP-Adresse des Nutzers bleibt weitgehend anonym. Software, wie zum Beispiel der Tor-Browser, dienen dazu, die Privatsphäre und den Datenschutz zu gewährleisten. Solche Anonymisierungsdienste lassen sich zum Beispiel nutzen, um Webserver, die für ein Netzwerk gesperrt wurden, über die Adresse des Dienstes zu erreichen.

Geoblocking umgehen

Manchmal sind ganze Webseiten oder bestimmte Inhalte aufgrund des Standortes des Nutzers gesperrt. In diesem Fall spricht man von Geoblocking. Dann kann ein Proxy Server dazu verwendet werden, um auf diese Inhalte zuzugreifen.

Datenanalyse und Protokollierung

Anders als zum Beispiel ein Gateway kann ein Proxy Server Daten protokollieren, speichern und analysieren. Eine statistische Auswertung der Server-Daten, kann außerdem zur Verbesserung der Performance dienen.

SEO-Küche Internet Marketing GmbH & Co. KG
Fraunhoferstr. 6, 83059 Kolbermoor
Telefon 08031 / 2575-100
Telefax 08031 / 2575-101
E-Mail: info@seo-kueche.de

SEO-Küche Internet Marketing GmbH & Co. KG,
HRA 11167 AG Traunstein
pers. Haftende Gesellschafterin:
SEO-Küche Verwaltungs GmbH, Kolbermoor, HRB 22414 AG Traunstein
Geschäftsführer: Christian Brunnenmayer, Patrick Keller, Oliver Lindner
Ust-IdNr.: DE 286 985 708, Steuer Nr. 156/174/08500

HypoVereinsbank
IBAN DE45 700202700015260147
BIC HYVEDEMMXXX