Proxy - Server

Ein Proxy-Server (kurz: Proxy) kann als intelligenter NAT-Router verstanden werden. Ein NAT-Router reicht Anfragen vieler Clients aus einem lokalen/privaten Netz (LAN/PAN) in das öffentliche Netz (Internet) weiter. Die Antworten kann er anhand seiner NAT-Tabelle (Schicht 3-4) wieder den richtigen Client weiterleiten. Ein Proxy arbeitet ähnlich, allerdings mit dem Unterschied, dass ein Proxy nicht nur auf Port und IP-Adressen achtet, sondern auch auf die Protokollinhalte auf den höheren Schichten 5-7. Im Folgenden werden die Aufgabengebiete eines Proxy-Servers exemplarisch dargestellt.

Ein Proxy hat u.a. folgende Aufgabengebiet:

1. Datentransferreduktion
2. Kontrolle des Traffics
3. Zugangsbeschränkung im Sinne einer Application-Firewall (s. Einführung in Firewalls)
4. Inhaltliche Aufbereitung der Daten
5. Lastverteilung
6. Protokollierung des Traffics
7. Gateway-Funktion

Datentransferreduktion

Sofern der gesamte Traffic über einen Proxy geführt wird, kann dieser so konfiguriert werden, dass bereits angeforderte Dateien zwischengespeichert werden und bei nochmaliger Anforderung direkt vom Proxy statt aus dem Internet geliefert wird. Wenn also häufig dieselben Dateien heruntergeladen werden müssen, spart ein Proxy Übertragungskapazitäten auf der WAN[1)]-Schnittstelle. Ein mögliches Problem kann sein, dass die zwischengespeicherten Dateien sich häufig ändern und ggf. aus dem Cache eine ältere Version bereitgestellt wird.

Vorteile:

- Reduktion der Übertragungsraten

Nachteile:

- Potentiell können veraltete Daten geliefert werden

Kontrolle des Traffics

Da der Proxy-Server alle ein- und ausgehenden Pakete filtert, kann er auch dazu eingesetzt werden Clients in ihrer Übertragungsrate einzuschränken. Werden zu viele Daten gesendet, so werden auf dem Proxy oberhalb einer festgesetzten Rate alle Pakete verworfen.

Zugangsbeschränkung im Sinne einer Application-Firewall

Ein weiteres Einsatzgebiet für Proxy-Server ist die Kontrolle des Traffics für bestimmte Protokolle. Man

kann einen Proxy damit auch als Application Firewall verstehen. Das Filtern auf Applikationsebene ist relativ komplex, da hier nicht nur einfache Kriterien wie Port oder IP-Adressen zur Entscheidung herangezogen werden. Viel mehr wird innerhalb eines Protokolls höherer Schicht (z.B. HTTP) eine Entscheidung getroffen, ob die Pakete passieren dürfen oder nicht. Es gibt prinzipbedingt nicht für jedes Protokoll eine Proxy-Umsetzung. Dies wäre sehr aufwendig. Häufig wird in den Firmen ein Proxy dazu verwendet den Zugriff auf bestimmte URL zu unterbinden. Problematisch kann es werden, wenn diverse Protokolle geschachtelt werden z.B. wenn eine HTTP-Anfrage über eine verschlüsselte-Verbindung (z.B. SSL) laufen soll. Da der Proxy zwischen dem Client und dem Server liegt, könnten hier Man-in-the-Middle-Attacken durchgeführt werden oder Passwörter abgegriffen werden. Um dies zu verhindern sind gesonderte Maßnahmen vorzusehen.

Vorteile:

- Kontrolle der nutzbaren Inhalte

Nachteile:

- Probleme bei bestimmten Protokollen bzw. Schachtelung von Protokollen (z.B. HTTP über SSH)

Inhaltliche Aufbereitung der Daten

Bei dieser Art Einsatz eines Proxys werden Datenpakete inhaltlich geändert. Z.B. können URL-Parameter ersetzt, hinzugefügt oder entfernt werden. Für den Client geschieht dies vollkommen transparent, da der Proxy dies für beide Richtungen durchführen kann.

Lastverteilung

Ein Proxy kann auch zur Lastverteilung eingesetzt werden. Wenn beispielsweise ein HTTP-Server nicht ausreicht, um die Anfrage abzuarbeiten, können weitere Server hinzugenommen werden. Um den Clients nicht unterschiedliche Ziele nennen zu müssen, wird ein Ziel genutzt (hier der Proxy) und dieser verteilt die eigentlichen Anfragen weiter an die HTTP-Server. Hier muss allerdings darauf geachtet werden, dass der Proxy über hinreichend Leistung verfügt, um die gesamte Anzahl an Anfragen verteilen zu können.

Protokollierung des Traffics

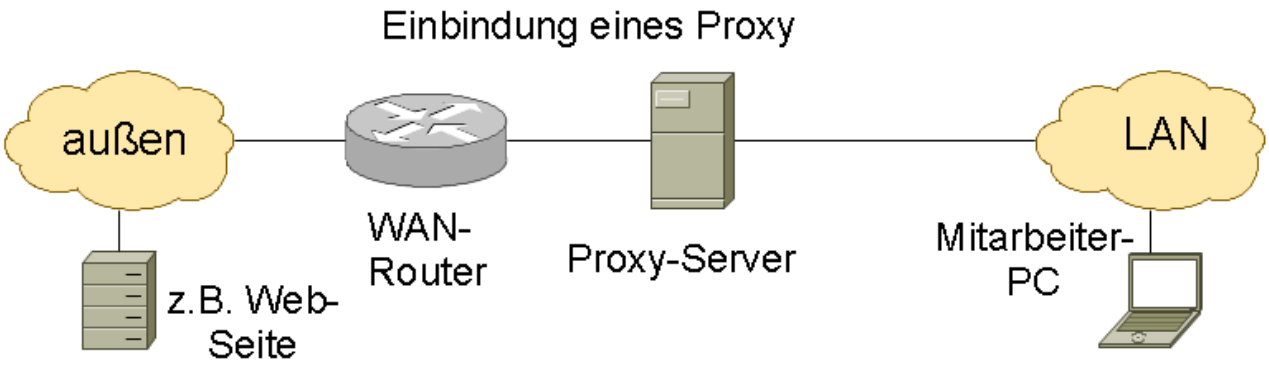
Da im Normalfall der gesamte Traffic über den Proxy läuft, kann dieser sehr gut als Protokollierungswerkzeug eingesetzt werden. Hier sind auf jeden Fall Datenschutzrichtlinien einzuhalten. Es Bedarf ggf. der Zustimmung des Datenschutzbeauftragten, wenn Verbindungsinformationen gespeichert werden sollen. Meist ist auch eine Anonymisierung notwendig.

Gateway-Funktion

Wenn ein Proxy als Gateway eingesetzt wird, dann findet eine Übersetzung von einem Protokoll (z.B. HTTP) in ein anderes Protokoll (z.B. FTP) statt. Dies ist sehr aufwendig und bedarf in der Regel einen Spezial-Proxy. Ein Gateway ist allgemein eine Netzkomponente, die Protokolle (z.B. HTTP zu FTP) oder auch Technologien (z.B. Ethernet zu TokenRing) konvertieren kann.

Integration in die Netzumgebung

Die folgende Abbildung zeigt eine mögliche Integration in eine Netzumgebung.



[1)]

WAN: wide area network