

Gesamtverzeichnis Kurs Netzwerktechnik

Christian Zahler

PCNEWS	Seite	Abschnitt Netzwerktechnik	99	16	IP-Routing
103	31	Routing	98	22	Transfer Control Protocol
103	30	Internet Grundlagen	98	17	Internet Protocol
102	27	DNS Domain Name System	97	20	Verkabelung
101	19	Smartcards	96	25	Netzwerk-Hardware und Verkabelung
101	18	DHCP-Server	95	19	Datenübertragung in Netzwerken
100	17	Netzwerkanalyse	95	18	Netzwerk-Grundlagen

DNS-Abfrage länger dauert, lässt sich der Seiteninhalt nicht mehr scrollen und wird auch nicht mehr aktualisiert. Dies führt dazu, dass man während der manchmal recht langen Zeit gar nichts mit Netscape anfangen kann, da es nicht einmal möglich ist, bereits fertig dargestellte Seiten zu lesen. Zumindest wenn man mehrere Fenster übereinander, iconisiert oder auf einer anderen Seite des Windowmanager liegen hat. Hier kann Squid weiterhelfen, denn Netscape stellt seine Anfrage nun an den lokal gut zu erreichenden Squid-Server und ist von der DNS-Problematik befreit.

- Freischaltung bestimmter Rechner zu genau definierten Zeiten

Squid verfügt über sogenannte "Access Lists", kurz **acl**. In diese kann man Rechner, Subnetze, Protokolle, Ports, URLs etc. aufnehmen. Sobald eine acl definiert ist, kann diese benutzt werden, um den Zugang zu ermöglichen oder zu sperren. So ist es in einer Firma z.B. sehr einfach zu realisieren, dass die Rechner aller Mitarbeiter in der Mittagspause surfen können. Während der Arbeitszeit hingegen bleibt der Zugang denen vorbehalten, die ihn benötigen. Hierzu wird neben dem Webcache noch ein Firewall gebraucht der verhindert, dass alle Rechner freien Zugang in und aus dem Netz heraus besitzen.

Durch die Möglichkeit komplette URLs und reguläre Ausdrücke in acl-Listen aufzunehmen, können komplette WWW-Server gesperrt werden oder solche bei denen bestimmte Schlüsselwörter im URL auftreten.

- Nutzung eines Wählzugangs mit einer einzigen IP-Nummer zum Surfen mit mehreren Rechnern

Eine weiter schöne Einsatzmöglichkeit liegt darin, ohne sich mit IP-Masquerading befassen zu müssen, weiteren Rechnern den Zugang zum WWW bereitzustellen. Hierzu wird Squid einfach auf dem Rechner installiert der für den Verbindungsaufbau zuständig ist. Die Konfiguration für Squid ändert sich dadurch nicht.

- Einfache Überprüfung der heruntergeladenen Inhalte möglich

Durch die von Squid erstellten Logdateien lassen sich mittels diverser Skripte Übersichten erstellen, die einige interessante Statistiken erfassen. So können alle WWW-Server, auf die zugegriffen wurde, mit Anzahl, Menge und Art der Anfragen eingesehen werden. Eine aktuelle Liste dieser Skripte kann man auf der offiziellen Squid Webseite <http://squid.nlanr.net/> finden. Sie sind zumeist von Anwendern für private Zwecke geschrieben worden, daher nicht in das Squid-Paket integriert und müssen "von Hand" installiert werden.

- Zurückverfolgung der Übertragungen zu den einzelnen Rechnern möglich

- Anonymisieren der User nach innen und außen hin möglich

Sobald Squid WWW-Anfragen der User weiterleitet, wird ein "forwarded for xyz" in den HTTP-Header eingefügt. Diese Informationen kann der WWW-Server speichern und verarbeiten. Um zu verhindern, dass Nutzerprofile angelegt werden, kann die Konfiguration so umgestellt werden, dass diese Informationen nicht verschickt werden bzw. einen fest definierten Wert erhalten. Je nach Konfiguration speichert Squid in seinen eigenen Logdateien aber noch, für welche Rechner er die Daten herausgegeben hat. Dies kann für alle diejenigen wünschenswert sein, die auf eine Kontrolle bzw. einen Beleg angewiesen sind. Dabei sollten aber alle Aspekte des Datenschutzes beachtet werden. Falls man andererseits die Privatsphäre seiner Benutzer schützen will, kann dies durch eine entsprechende Konfiguration auch gewährleistet werden.

Nachteile von Squid

- Eventuell kommt es zur Auslieferung nicht mehr aktueller Daten

Squid teilt gespeicherte Daten in die zwei Klassen FRESH und STALE ein. Diese Einteilung wird mittels mehrere Regeln und dem Zeitpunkt der Übertragung sowie des Alters des Dokuments bestimmt. Solange ein Objekt FRESH ist, wird es bei einer erneuten Anfrage sofort aus dem Cache ausgeliefert. Ansonsten werden verschiedene Maßnahmen eingeleitet um zu überprüfen, ob das gespeicherte Objekt noch aktuell ist. Trotzdem kann es vorkommen, dass Objekte ausgeliefert werden, die nicht mehr dem letzten Stand entsprechen. Dies tritt vor allem bei Seiten ein, die sich täglich oder stündlich ändern. Wenn man den Verdacht hat, dass die dargestellte Seite nicht aktuell ist sollte man in Netscape, falls ein Reload erfolglos ist, mittels Shift-Reload einen neuen kompletten Download erzwingen.

- Eventuelle Probleme mit nur über Links zugänglichen Daten

Leider kann mit Shift-Reload kein neues Laden eines Links erzwungen werden. Diese Designschwäche des Browsers kann zu ärgerlichen Ergebnissen führen. Stellen Sie sich einmal vor, Sie wollen eine Liveübertragung eines Fußballspieles per Realaudio verfolgen. Die dazu nötige .ra-Datei ist über einen Link zugänglich und beim Anklicken wird das Realvideo-Plug-in aktiv. Weiterhin befindet sich vor der eigentlichen Übertragung ein Ankündigungstrailer unter diesem Link. Ist man nun etwas früh, hat man folgendes Problem: Der Trailer befindet sich im Cache und ist FRESH. Daher wird dieser, sobald man wieder auf den Link klickt, vom Ca-

che ausgeliefert, obwohl die Übertragung jetzt läuft. Da man kein neues Laden über den Browser erzwingen kann, befindet man sich in der Situation, dass es nur möglich ist die Übertragung zu verfolgen, wenn man für alle Fenster des Browsers den Cache abschaltet. Um dem Ganzen aus dem Weg zu gehen, muss man dem Cache mitteilen, welche Dateitypen er nicht cachen soll. In der Standardkonfiguration befinden sich nur cgi und ? in dieser Liste. Sie sollte also nach Bedarf um all die Dateitypen erweitert werden, die nur per Links zugänglich sind.

Systemvoraussetzungen

Für den Betrieb von Squid bieten sich alte Rechner wie ein 486er geradezu an. Mit wenigen Mitteln kann man aus seinem alten Rechner ein schönes Gateway machen, das gleichzeitig für Verbindungsaufbau, Firewall und den Webcache zuständig ist. Man sollte nur darauf achten, dass dem Rechner genügend Hauptspeicher zur Verfügung steht. In diesem Fall fehlen eventuell nur noch ein oder zwei Netzwerkkarten, die es heute aber auch schon sehr günstig gibt.

Wenn möglich, sollte man dem Rechner zwei Festplatten spendieren, eine für das System und die andere auf der die Daten von Squid liegen. Dies sollte unbedingt der Fall sein, wenn der Rechner häufig swapt, weil er zuwenig Hauptspeicher besitzt. Squid läuft auf quasi allen Unix-Betriebssystemen. Auf der Tagungs-CD-ROM ist ein Binary-RPM für Red Hat 5.2 enthalten, das Sie recht einfach als root mittels `rpm -i dateiname` installieren können. In der Delix DLD-Distribution, die sich auf der CD-ROM zum LinuxTag '99 befindet, ist das Paket leider nur in einer etwas älteren Version verfügbar. Für die Betreiber von anderen oder älteren Systemen ist auch ein Source-RPM vorhanden. Mit dessen Hilfe können Sie ein für Ihr System passendes Binary-RPM erzeugen.

Wichtigste Konfigurationsoptionen

Im folgenden Abschnitt finden Sie die wichtigsten Konfigurationsoptionen aus der Datei `etc/squid.conf`, mit deren Hilfe Sie Ihren Cache grundlegend konfigurieren können. Die folgenden Optionen sind dem Konfigurationsfile der Version 2.1 entnommen.

Dieser Text ist aus Platzgründen in die Webversion verlagert worden.

13.5 Quellen

www.tecchannel.de

http://www.zdnet.de/technik/artikel/swp/200006/proxy_01-wc.html