Squid-Konfiguration

```
# NETWORK OPTIONS
# ----------------------------------------------------------------------------
#  TAG: http_port
#http_port 3128
Mittels des http_port stellen Sie ein, unter welcher Portnummer auf Ihrem Rechner  Squid zu erreichen ist (siehe Einführung).
# OPTIONS WHICH AFFECT THE CACHE SIZE
# ----------------------------------------------------------------------------
#  TAG: cache_mem       (bytes)
#cache_mem  8 MB
#  TAG: maximum_object_size     (bytes)
#maximum_object_size 4096 KB
Durch cache_mem wird festgelegt, wieviel Speicher für In-Transit-Objekte zur Verfügung steht. Dies sind alle Daten, die in Übertragung begriffen sind. Zeitweilig kann diese Größe überschritten werden, falls z.B eine tar.gz-Datei heruntergeladen wird, die größer als der cache_mem-Wert ist.
maximum_object_size legt die maximal Größe einer Datei fest, die noch im Cache  gspeichert wird. Beide Optionen sollten an Bedarf und Systemressourcen angepasst werden. Es macht z.B keinen Sinn, den gesamten Hauptspeicher als Größe anzugeben, zumal wenn  Squid auf dem Arbeitsrechner läuft.
# LOGFILE PATHNAMES AND CACHE DIRECTORIES
# ----------------------------------------------------------------------------
#  TAG: cache_dir
#cache_dir /usr/local/squid/cache 100 16 256
#  TAG: cache_access_log
#cache_access_log /usr/local/squid/logs/access.log
#  TAG: cache_log
#cache_log /usr/local/squid/logs/cache.log
#  TAG: cache_store_log
#cache_store_log /usr/local/squid/logs/store.log
#  TAG: cache_swap_log
#cache_swap_log
#  TAG: pid_filename
#pid_filename /usr/local/squid/logs/squid.pid
Falls eine extra Festplatte/Partition für die Daten zur Verfügung steht, empfiehlt es sich, die Logdateien ebenfalls dort abzulegen. Dementsprechend müssen die Pfade angepasst werden, z.B. /mnt/proxy/....
Die Datei swap.state darf unter keinen Umständen gelöscht werden, da darin die Informationen gespeichert werden, wo auf der Festplatte die Daten des  Caches abgelegt sind. Diese Datei wird beim Neustart von Squid verwendet, um wieder auf die gespeicherten Daten zugreifen zu können. In den anderen Datein sind Informationen, Zugriffe und Status verzeichnet.
#  TAG: ident_lookup    on|off
#ident_lookup off
Mittels dieser Option ist es möglich, eine Abfrage des Nutzernamens beim  Client durchzuführen und im Log zu speichern.
#  TAG: client_netmask
#client_netmask 255.255.255.255
Um einen entsprechenden Datenschutz für die Benutzer im Log zu erreichen, kann man die  IP-Nummern der Rechner ähnlich wie Telefonnummern auf einer Telekomrechnung um beliebige Stellen kürzen. Mittels client_netmask 255.255.255.0
erreicht man z.B., dass aus 194.162.83.24 194.162.83.0 wird und die letzten acht Bit der  IP-Adresse verloren gehen. Die wahre  IP-Nummer wird dabei einfach mit  client_netmask durch die logische und-Funktion verknüpft, bevor sie im Log gespeichert wird.
# OPTIONS FOR EXTERNAL SUPPORT PROGRAMS
# ----------------------------------------------------------------------------
#  TAG: dns_children
#dns_children 5
Die dns_children sind dazu da, die Nameserverabfragen zu übernehmen. Bei normaler Benutzung kann man diese Option unverändert lassen. Falls der Cache dafür gedacht ist vielen Leuten zu dienen, und diese über eine langsame Leitung angebunden sind, sollte die Anzahl eventuell erhöht werden. Die Programmierer empfehlen für einen sehr stark ausgelasteten Cache mindestens 10. Der Maximalwert beträgt 32. Man sollte aber bedenken, dass jeder weitere DNS-Prozess etwa 100kB Hauptspeicher belegt.
# OPTIONS FOR TUNING THE CACHE
# ----------------------------------------------------------------------------
#  TAG: reference_age
#reference_age 1 month
Beim Aufräumen des Caches werden alle Objekte entfernt, die ihr maximales Alter erreicht haben. Wenn reference_age auf einen Monat eingestellt ist, werden alle Objekte entfernt, auf die seit einem Monat nicht mehr zugegriffen wurde.
#  TAG: quick_abort_min (KB)
#  TAG: quick_abort_max (KB)
#  TAG: quick_abort_pct (percent)
#quick_abort_min 16 KB
#quick_abort_max 16 KB
#quick_abort_pct 95
Squid ist in der Lage, Dateien, deren Übertragung er begonnen hat, auch nach dem Beenden bzw. Stoppen des Browsers durch den Benutzer fertig zu laden, falls sie bestimmten Kriterien genügen. Falls weniger als quick_abort_min Kilobyte von der Übertragung übrig bleiben, wird diese fortgesetzt. Wenn mehr als quick_abort_max Kilobyte zu laden sind, wird der Transfer abgebrochen. Die letzte Bedingung quick_abort_pct legt fest, wieviel Prozent der Übertragung abgeschlossen sein müssen, um diese fortzusetzen.
Die quick_abort-Funktionalität hat Ihre Stärken und Schwächen. Durch die fortgesetzte Übertragung kann es, vor allem auf langsamen Leitungen wie Wählverbindungen, zu Engpässen und starker Verlängerung der Transferzeiten kommen. Andererseits sind dann vollständige Daten im Cache auch für andere Benutzer abrufbar. Der Standardnutzer sollte die quick_ abort-Funktion abstellen. Dies geschieht durch
quick_abort_min 0 KB
quick_abort_max 0 KB
quick_abort_pct 100
# TIMEOUTS
# ----------------------------------------------------------------------------
#  TAG: request_timeout
#request_timeout 30 seconds
Bei stark ausgelasteten Leitungen bietet es sich an, den  Timeout nach Bedarf anzupassen.
# ACCESS CONTROLS
# ----------------------------------------------------------------------------
#  TAG: acl
#Defaults:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535
acl CONNECT method CONNECT
#  TAG: http_access
#Default configuration:
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access deny all
Access Control Lists, kurz acl, werden nach folgendem Syntax definiert:
acl aclname acltyp string1 ...
acl aclname acltyp datei ...
In einer Datei sollte nur eine Regel pro Zeile eingetragen werden. Die unterschiedlichen  acltypen sind:
src
Fasst Herkunfts-IP-Adressen zusammen.
IP-Adresse/Netzmaske ... (Client-IP-Adresse)
Addr1-Addr2/Netzmaske ... (Bereich von Adressen)
dst
Fasst Ziel-IP-Adressen zusammen.
srcdomain
Herkunftsdomain.
dstdomain
Zieldomain.
srcdom_regex
Regulärer Ausdruck angewendet auf den  Client.
dstdom_regex
Regulärer Ausdruck angewendet auf den Server.
url_regex
Regulärer Ausdruck, der auf den ganzen  URL angewendet wird.
urlpath_regex
Regulärer Ausdruck, der auf den Pfad des  URL angewendet wird.
time
Tages und Zeitbereichsangabe Tag h1:min1-h2:min2. Die erste Zeitangabe muss kleiner als die zweite sein. Tag:
M
Montag
T
Dienstag
W
Mittwoch
H
Donnerstag
F
Freitag
A
Samstag
S
Sonntag
port
Portnummern
proto
Protokoll
method
Methoden wie GET, POST, ...
browser
regular expression
ident
Benutzername
http_access erlaubt oder sperrt den Zugriff auf  Squid durch Access-Lists. Zugriff auf den HTTP-Port:
http_access allow|deny [!]aclname
Wenn keine http_access-Zeile vorhanden ist, wird die Anfrage grundsätzlich erlaubt. Wenn keine http_access-Zeile auf einen Anfrage angewendet werden kann, wird das Gegenteil der letzten Regel in der Liste angewendet. Die Regeln werden eine nach der anderen von oben nach unten abgearbeitet, bis eine Regel zutrifft. Danach folgende Regeln werden nicht mehr berücksichtigt. Innerhalb einer  acl sind die Elemente mit oder und bei  http_access mit und verknüpft.
Nehmen wir einmal an, der Zugang zum  WWW soll für zwei Benutzergruppen reglementiert werden.
acl standard src 194.246.68.1-194.246.68.100/255.255.255. 194.246.68.102/255.255.255.255
acl privilegiert src 194.246.68.101/255.255.255.255 194.246.68.103/255.255.255.255
acl Mittagspause 12:00-13:00
http_access allow Mittagspause standard
http_access deny standard
http_access allow privilegiert
http_access deny all
Mit dieser Konfiguration werden die Standard-Nutzer nur zur Mittagspause freigeschaltet, während die privilegierten Nutzer jederzeit Zugriff besitzen. Alle diejenigen  IP-Nummern, die durch die Listen nicht abgedeckt werden, haben keinen Zugriff.
# ADMINISTRATIVE PARAMETERS
# ----------------------------------------------------------------------------
#  TAG: cache_mgr
#cache_mgr webmaster
Hier muss die E-Mail-Adresse desjenigen eingetragen werden, der die Administration von  Squid übernommen hat.
# MISCELLANEOUS
# ----------------------------------------------------------------------------
#  TAG: dns_testnames
#dns_testnames netscape.com internic.net nlanr.net microsoft.com
Mit den eingetragenen Domains wird die DNS-Abfrage überprüft. Sobald der erste erfolgreiche DNS-Lookup gelingt, wird der Test erfolgreich abgebrochen. Ansonsten wird nach einer gewissen Zeit Squid beendet (z.B falls die Leitung gerade nicht aufgebaut ist). Um den DNS-Test zu unterbinden, muss Squid mit squid -D gestartet werden.
#  TAG: append_domain
#append_domain .yourdomain.com
append_domain dient der Bequemlichkeit und ermöglicht es im Browser Rechnernamen des lokalen Netzes ohne Domainnamen anzugeben. Squid ergänzt diese automatisch um die Zeichenkette in  append_domain. Also z.B append_domain .unix-ag.uni-kl.de. Aus http://sushi wird somit http://sushi.unix-ag.uni-kl.de.
#  TAG: memory_pools    on|off
#memory_pools on
Wenn memory_pools aktiviert ist, behält Squid ungenutzten zugewiesenen Speicher für zukünftigen Gebrauch, anstatt ihn wieder freizugeben. Wenn der Rechner über wenig Speicher verfügt, sollte man memory_pools abschalten.
#  TAG: forwarded_for    on|off
#forwarded_for on
Standardmäßig leitet Squid die IP-Nummer oder den Namen eines Rechners, für den eine Anfrage bearbeitet wird, zum WWW-Server weiter.
forwarded_for off
#  TAG: http_anonymizer
#http_anonymizer off
Mittels http_anonymizer lässt sich konfigurieren, wieviele HTTP-Header gefiltert werden. Es gibt die drei Einstellungen off, standard und paranoid. Mit standard werden die wichtigsten Header unterdrückt, mit paranoid hingegen fast alle.
Unter Version 2.2 wurde diese Option dahingehend verändert, dass nun die einzelnen  Header, die erlaubt oder unterdrückt werden sollen, direkt angegeben werden können.
```

Squid starten

Nach den Änderungen an der Datei muss der Squid neu gestartet werden sofern er schon läuft. Dies geschieht am einfachsten mit dem Befehl / sbin/init.d/squid restart.
Damit Squid bei jedem Start Ihres Linux-Rechners automatisch gestartet wird, setzen Sie in der Datei /etc/rc.config den Wert von START_SQUID auf yes.

Logdateien rotieren

Um eine Rotation der Logdateien auszuführen, können Sie squid -k rotate verwenden.

Squid rekonfigurieren

Nach einer Änderung an der Konfiguration ist es möglich mittels squid -k reconfigure ein Neueinlesen einzuleiten.

Squid beenden

Benutzen Sie einfach squid -k shutdown, um Squid nach ungefähr einer halben Minute terminieren zu lassen.