Kindersicherung mit SquidGuard

WALTER JUSTEN, SENIOR SYSTEM ENGINEER

Mit SquidGuard gibt es eine Zusatzsoftware für den Squid-Proxy, mit der das Filtern von Zugriffen über den Squid-Proxy in das Internet ermöglicht wird. Eine Anwendungsmöglichkeit im privaten Umfeld kann der Schutz vor nicht jugendfreien Webinhalten sein, im Arbeitsumfeld das Unterbinden des Surfens auf privaten Seiten.

SquidGuard bietet die Möglichkeit, anhand definierter URLs oder Strings angeforderte Internetseiten zu filtern und nach definierten Regeln zu sperren oder auf andere Internetseiten umzuleiten. Eine einfache und grundlegende Konfiguration sehen wir uns hier an.
Bei SquidGuard handelt es sich um eine eigenständige Software. Sie setzt auf das Redirector-Interface des Squid-Proxy auf. Ein Patchen des Squid ist daher nicht nötig und eine bereits bestehende Proxy-Installation kann daher unverändert genutzt werden. Zum Einsatz kommt eine solche Lösung in der Regel, um das Abrufen nicht erlaubter Seiten zu verhindern. Je nach Einsatzgebiet kann es sich dabei um pornographische oder kriminelle Inhalte handeln. Denkbar wäre ebenso das Verhindern eines MP3-Downloads, um die Bandbreite des Internet-Zugangs nicht zu gefährden.

Installation

Voraussetzung ist natürlich eine funktionierende Installation von Squid. Hat man kein fertiges Paket von SquidGuard und muß man die Software aus den Quellen kompilieren, sind außer den SquidGuard-Sourcen noch die Quelltexte der Berkeley DB Library mindestens in der Version 2.X nötig.
Die Berkeley DB Library ist aktuell in der Version 4.x erhältlich. Sie bereitet aber Probleme beim Kompilieren von SquidGuard. Daher wurde für diesen Beitrag die Version 2.7.7 verwendet. Die Quellen der Library und von SquidGuard befindet sich auf der CD-ROM zu dieser freeX.
Erst müssen die Sourcen entpackt werden, im Anschluß werden sie kompiliert und installiert. Begonnen werden muß mit der Berkeley DB Library:

```
# tar -xzvf db-2.7.7.tar.gz
# cd db-2.7.7/build_unix
# CC=gcc
# export CC
# ../dist/configure
# make
# make install
```

Daraufhin kann SquidGuard kompiliert und installiert werden:

```
# tar -xvzf squidGuard-1.2.0.tar.gz
# cd squidGuard-1.2.0
# ./configure --with-db=/usr/local/
# BerkeleyDB
# make
# make install
```

In der Voreinstellung werden die Bibliotheken und SquidGuard selbst unter »/usr/local« installiert.
Zur Grundkonfiguration von SquidGuard gehört eine minimale »squidguard.conf«. Sie wird in der Voreinstellung unter »/usr/local/squidGuard/squidGuard.conf« erwartet. Es kann aber beim Start eine alternative Konfigurationsdatei angegeben werden:

```
squidGuard -c <Pfad>/sguidGuard.conf
```

Eine minimale Konfiguration, die noch keinen Einfluß auf den Squid-Proxy hat und nur das Log und das Datenbankverzeichnis für SquidGuard angibt, könnte den folgenden Inhalt haben:

```
logdir /usr/local/squidGuard/log
dbhome /usr/local/squidGuard/db
  acl {
    default {
    pass all
  }
}
```

Quellen und Ziele

Bevor SquidGuard genutzt werden kann, muß der Redirector-Funktion des Squid mitgeteilt werden, daß sie SquidGuard nutzen soll. Dazu muß die Konfigurationsdatei des Proxy, die Datei »squid.conf«, angepaßt werden. Ein Eintrag bei *redirect-program* könnte für die Beispielkonfiguration das folgende Aussehen haben:

```
redirect_program \
 /usr/local/bin/squidGuard -c \
 /usr/local/squidGuard/squidGuard.conf
```

Außerdem wird hier auch die Anzahl der Redirector-Prozesse angegeben, die gestartet werden sollen:

```
redirect_children 5
```

Nach dem Neustart des Squid sollte er nun die eingestellte Anzahl SquidGuard-Prozesse starten und sie über seine Redirector Funktion ansprechen.
Möchte man Ziele nicht für alle User oder Gruppen sperren, sollten entsprechend verschiedene Quellen angelegt werden. Eine Quellgruppe

kann unter anderem eine IP-Adresse oder ein bestimmter Bereich von IP-Adressen sein oder auch Domains oder einzelne User umfassen:

```
src erwachsene {
  ip      192.168.3.5 192.168.3.6
  domain  home.meinedomain.de
  user    root
}
src kinder {
  ip        192.168.4.0/24
  domain    home2.meinedomain.de
}
```

Außerdem lassen sich verschiedene Ziele bestimmen. Eine Liste der Zieladressen wird jeweils für den entsprechenden Typ im db-Verzeichnis erwartet. Sie befindet sich im Pfad, der am Anfang in der Konfiguration gesetzt wurde.

```
dest sex {
  domainlist sex/domains
  urllist    sex/urls
}

dest musik {
  expressionlist musik/expressions
}
```

Für das Beispiel sollte sich dann im Directory »/usr/local/squidGuard/db« die Unterverzeichnisse »sex« und »musik« befinden. »sex« enthält die Dateien »domainlist« mit einer Auflistung von Domains und die Datei »urllist« mit einer Auflistung von Webseiten.

Regelwerk

In der Datei »expressions« im Verzeichnis »musik« sollten dann Buchstabenfolgen wie zum Beispiel »mp3« oder ähnliches zu finden sein.

```
# vi expressions
mp3
realaudio
```

Hat man die Quellen und Ziele definiert, ist es möglich, anhand derer Regeln beziehungsweise Access Control Lists zu erstellen. Um der Quelle »kinder« das Ziel »sex« zu sperren und dabei eine Umleitung auf eine Verbots- beziehungsweise Hinweisseite zu erzwingen, könnte eine Regel wie folgt aussehen.

```
acl {
  kinder {
    pass !sex all
    redirect http://www.meinedomain.de\
/verboten.html
  }
  default {
    pass all
  }
}
```

```
logdir /usr/local/squidGuard/log
dbhome /usr/local/squidGuard/db

src erwachsene {
  ip       192.168.3.5 192.168.3.6
  domain   home.meinedomain.de
  user     root
}
src kinder {
  ip       192.168.4.0/24
  domain   home2.meinedomain.de
}
dest sex {
  domainlist sex/domains
  urllist    sex/urls
  log        sex.log
}

dest musik {
  expressionlist musik/expressions
}

acl {
  kinder {
    pass !sex all
    redirect http://www.meinedomain.de/verboten.html
  }
  default {
    pass all
  }
}
```

Listing 1: Die »squidGuard.conf« auf einen Blick

Um verbotene Zugriffe später überprüfen zu können, bietet SquidGuard auch einen Login-Mechanismus für diese Zugriffe an:

```
log sex.log
```

Wobei das Log in den in der Konfigurationsdatei definierten Logpfad geschrieben wird. Die Definition zum Loggen der Zugriffe muß im Destination-Teil der Konfigurationsdatei erfolgen.

Weitere Konfigurationen

Außer der bis hierher recht einfachen Konfiguration bietet SquidGuard weitere Möglichkeiten. So ist unter anderem auch das Filtern nur an gewissen Tagen oder Uhrzeiten konfigurierbar. Außerdem ist es möglich, statt einer Umleitung auf eine bestimmte URL auch die angeforderte URL mittels der Funktion *rewrite* umzuschreiben. Auch lassen sich der ersatzweise anzuzeigenden Internetseite mit Hilfe von *redirect* verschiedene Parameter übergeben, unter anderem Daten wie die IP-Adresse des Anfragenden oder der Ziel-Domain. Auch gibt es im Internet bereits einige fertige Datenbanken mit Blacklists zum Download, die in SquidGuard verwendet werden können. ◆

Weitere Infos:

Squid Proxy: »http://www.squid-cache.org/«

Squid Guard: »http://www.squidguard.org/«

Berkeley DB Library: »http://www.sleepycat.com/«

Internet Filter: »http://www.bn-paf.de/filter/index_de.html«