

Paket PROXY

Version 3.7.0-rev20394

Frank Meyer	Das fli4l-Team
E-Mail: frank@fli4l.de	E-Mail: team@fli4l.de

2. Dezember 2011

Inhaltsverzeichnis

1	Dokumentation des Paketes PROXY	3
1.1	PROXY - Verschiedene Proxy-Server	3
1.1.1	OPT_PRIVOX - Ein Werbung-filternder HTTP-Proxy	3
1.1.2	OPT_TOR - Ein anonymes Kommunikationssystem für das Internet . .	5
1.1.3	OPT_SS5 - Ein Socks4/5 Proxy	7
1.1.4	OPT_TRANSPROXY (EXPERIMENTELL) - Transparenter HTTP-Proxy	7
	Abbildungsverzeichnis	9
	Tabellenverzeichnis	10
	Index	11

1 Dokumentation des Paketes PROXY

1.1 PROXY - Verschiedene Proxy-Server

1.1.1 OPT_PRIVOX - Ein Werbung-filternder HTTP-Proxy

Privoxy wird auf der offiziellen Privoxy-Homepage (<http://www.privoxy.org/>) als "Privacy Enhancing Proxy" (= "privatsphärenerweiternder Proxy") beworben. Als sichtbarer und erwünschter Nebeneffekt ersetzt Privoxy Werbe-Banner und -Popups durch leere Bilder, verhindert das Speichern von ungewollten Cookies (kleine Datenpakete, mit denen eine Website einen bestimmten Surfer wiedererkennen kann) und verhindert die Anzeige von sogenannten Web-Bugs (das sind 1x1 Pixel große Bilder, die dazu benutzt werden, um das Surfverhalten von Benutzern auszuspähen).

Privoxy kann, während es läuft, ganz einfach über ein Webinterface konfiguriert und (de)aktiviert werden. Dieses Webinterface findet sich unter <http://config.privoxy.org/> oder <http://p.p/>.

Privoxy ist eine konsequente Weiterentwicklung des Internet Junkbusters, der bis Version 2.1.0 in diesem Paket (<http://www.junkbuster.com/>) enthalten war. Die wichtigste Neuerung ist, dass alle Regeln für die Filterung in der zentralen Datei `default.action` definiert werden. Diese befindet sich bei FLI4L im Verzeichnis `/etc/privoxy`. Der große Vorteil an dieser Methode ist, dass sich neue Versionen dieser Datei separat von <http://sourceforge.net/projects/ijbswa/files/> herunterladen lassen. So kann jeder FLI4L-Benutzer die Datei selbst auf dem neusten Stand halten, ohne auf Updates von FLI4L angewiesen zu sein. (Momentan befindet sich die Version 1.8 dieser Datei im Paket.)

Eine so
getätigte
Konfigu-
ration
überlebt
keinen
Neu-
start... (tobi)

PRIVOXY_MENU Fügt dem httpd-Menü einen Privoxy-Abschnitt hinzu.

PRIVOXY_N Gibt die Anzahl der Privoxy-Instanzen an, die gestartet werden sollen.

PRIVOXY_x_LISTEN Hier werden die IP-Adressen oder symbolischen Namen inklusive der Portnummer der Interfaces angegeben, auf denen Privoxy auf Verbindungen von Clients horchen soll. Es ist eine gute Idee, hier nur die Adressen der Interfaces anzugeben, denen man vertraut, da alle Rechner vollen Zugriff auf Privoxy haben (und auf den eventuell aktivierten Konfigurations-Editor). In der Regel ist die Vorgabe `IP_NET_1_IPADDR:8118` sinnvoll.

Auf hier angegebenen Adressen lauscht Privoxy und bietet seine Dienste an. 8118 ist der Standard-Port. Die Angabe hier muss man dann bei der Proxy-Konfiguration des jeweils verwendeten Internet-Browsers benutzen. Weitere Informationen zur Konfiguration von Internet Explorer und Netscape Navigator auf

<http://www.privoxy.org/>

Als Proxy beim jeweiligen Browser muss der fli4l-Rechner angegeben werden, also das, was man bei `HOSTNAME='fli4l'` angegeben hat bzw. dessen IP (z.B. 192.168.6.1), die

Genaue
URL

man bei `HOST_x_IP='192.168.6.1'` angegeben hat. Zusammen mit dieser Port-Angabe hier hat man dann alle nötigen Daten, um seinen Webbrowser für die Nutzung von Privoxy zu konfigurieren.

PRIVOXY_x_ALLOW_N Gibt die Anzahl der Listeneinträge an.

PRIVOXY_x_ALLOW_x Die Liste der Netze und/oder IP-Adressen für die der Paketfilter geöffnet wird. Sinnvoll ist hier auch wieder die Vorgabe `IP_NET_1`.

PRIVOXY_x_ACTIONDIR Diese Variable gibt den Ort an, an dem die Privoxy-Regelsätze (die Dateien *default.action* und *user.action*) auf dem Router liegen sollen. Der angegebene Pfad wird relativ zum Wurzelverzeichnis ausgewertet. Diese Variable kann für zwei Dinge verwendet werden:

Verlagern der Standardregeln auf permanenten Speicher Gibt man als Verzeichnis einen Ort ausserhalb der Ram-Disk an, werden die Standardregelsätze beim erstmaligen Booten dorthin kopiert und dann von diesem Ort aus genutzt. Änderungen an diesen Regelsätzen überleben dann ein Reboot des Routers. Zu beachten ist, dass nach einem Update des Privoxy-Paketes diese Regeln immer noch Verwendung finden und evtl. mit dem aktuellen Paket kommende neuere Regelsätze ignoriert werden.

Verwenden eigener Regelsätze Fli4l gestattet das Überschreiben der Standardregeln mit nutzerspezifischen Regeln. Dazu legt man im *config*-Verzeichnis ein Unterverzeichnis an (z.B. *etc/my_privoxy*; es darf nicht *etc/privoxy* heissen) und legt dort die eigenen Regeln ab.

Das Setzen dieser Variable ist optional.

PRIVOXY_x_HTTP_PROXY Möchte man zusätzlich zu Privoxy einen weiteren HTTP Proxy verwenden, der dann z.B. auch Webseiten zwischenspeichert, so kann man den hier angeben. Privoxy bedient sich dann dieses Proxys. So kann man die Vorteile mehrerer Proxys nutzen. Ein Eintrag könnte so aussehen:

```
PRIVOXY_1_HTTP_PROXY='mein.provider.de:8000'
```

Die Angabe ist optional.

PRIVOXY_x SOCKS_PROXY Möchte man zusätzlich zu Privoxy einen weiteren SOCKS Proxy verwenden, kann man den hier angeben. Um die Privatsphäre weiter zu erhöhen kann der Datenverkehr vom Privoxy beispielsweise durch das Tor Netzwerk geschickt werden. Für weitere Details zu Tor lesen Sie in der [Tor Dokumentation](#) (Seite 5) weiter. Ein Eintrag für die Nutzung von Tor könnte so aussehen:

```
PRIVOXY_x SOCKS_PROXY='127.0.0.1:9050'
```

Die Angabe ist optional.

PRIVOXY_x_TOGGLE Diese Option aktiviert die Möglichkeit, den Proxy über das Webinterface ein- bzw. auszuschalten. Wird Privoxy ausgeschaltet, wirkt er als einfacher Forwarding-Proxy und ändert den Inhalt der übertragenen Seiten in keinsten Weise. Es ist zu beachten, daß diese Einstellung für ALLE Benutzer des Proxys gilt, d.h. wenn ein Benutzer Privoxy abschaltet, ist Privoxy auch für die anderen Nutzer nur noch ein Weiterleitungs-Proxy.

PRIVOXY_x_CONFIG Diese Option ermöglicht den Benutzern des Proxys die interaktive Bearbeitung der Konfiguration über das Privoxy-Webinterface. Für weitere Details bitte ich auch hier, die Privoxy-Dokumentation zu konsultieren.

PRIVOXY_x_LOGDIR Mit dieser Option kann ein Logverzeichnis für Privoxy angegeben werden. Dies kann z.B. dann sinnvoll sein, wenn Website-Zugriffe der Benutzer geloggt werden sollen. Wird hier nichts angegeben (Standard), dann loggt nur die wichtigsten Meldungen auf die Konsole und ignoriert **PRIVOXY_LOGLEVEL**.

PRIVOXY_x_LOGLEVEL Diese Option gibt an, was Privoxy in die Logdatei schreiben soll. Folgende Werte sind möglich, sie können durch Leerstelle getrennt angegeben werden, man kann sie aber auch addieren.

Wert	Was wird geloggt?
1	Jeden Request (GET/POST/CONNECT) ausgeben.
2	Status jeder Verbindung ausgeben
4	I/O-Status anzeigen
8	Header-Parsing anzeigen
16	Alle Daten loggen
32	Force-Feature debuggen
64	reguläre Ausdrücke debuggen
128	schnelle Weiterleitungen debuggen
256	GIF De-Animation debuggen
512	Common Log Format (zur Logfile-Analyse)
1024	Popup-Kill-Funktion debuggen
2048	Zugriffe auf den eingebauten Webserver loggen
4096	Startmeldungen und Warnungen
8192	Nicht-fatale Fehler

Um eine Logdatei im Common Logfile Format zu erstellen, sollte NUR der Wert 512 angegeben werden, da sonst die Logdatei durch andere Meldungen "verschmutzt" wird und somit nicht mehr problemlos ausgewertet werden kann.

Privoxy bietet sehr viele Konfigurationsmöglichkeiten. Diese können aber aus verständlichen Gründen nicht alle durch die Konfigurations-Datei von fli4l abgedeckt werden. Sehr viele dieser Optionen können im Webinterface von Privoxy eingestellt werden. Genauere Infos über den Aufbau dieser Dateien gibt es auf der Privoxy-Homepage. Die Konfigurationsdateien von Privoxy liegen unter <FLI4L-Verzeichnis>/opt/etc/privoxy/. Es handelt sich hierbei um die Original-Dateien aus dem Privoxy-Paket, allerdings wurden, um Platz zu sparen, alle Kommentare entfernt.

1.1.2 OPT_TOR - Ein anonymes Kommunikationssystem für das Internet

Tor ist ein Werkzeug für eine Vielzahl von Organisationen und Menschen, die ihren Schutz und ihre Sicherheit im Internet verbessern wollen. Die Nutzung von Tor hilft Ihnen, das Browsen und Veröffentlichen im Web, Instantmessaging, IRC, SSH und anderen TCP basierende Anwendungen zu anonymisieren. Weiterhin bietet Tor eine Plattform auf der Softwareentwickler neue Anwendungen schaffen können die zu mehr Anonymität, Sicherheit und zum Schutz der Privatsphäre beitragen.

<https://www.torproject.org/index.html.de>

TOR_LISTEN_N

TOR_LISTEN_x Hier werden die IP-Adressen oder symbolischen Namen inklusive der Portnummer der Interfaces angegeben, auf denen Tor auf Verbindungen von Clients horchen soll. Es ist eine gute Idee, hier nur die Adressen der Interfaces anzugeben, denen man vertraut, da alle Rechner vollen Zugriff auf Tor haben (und auf den eventuell aktivierten Konfigurations-Editor). In der Regel ist die Vorgabe `IP_NET_1_IPADDR:9050` sinnvoll.

Auf hier angegebenen Adressen lauscht Tor und bietet seine Dienste an. 9050 ist der Standard-Port. Die Angabe hier muss man dann bei der Proxy-Konfiguration des jeweils verwendeten Programms benutzen.

Als Proxy beim jeweiligen Programm muss der fli4l-Rechner angegeben werden, also das, was man bei `HOSTNAME='fli4l'` angegeben hat bzw. dessen IP (z.B. 192.168.6.1), die man bei `HOST_x_IP='192.168.6.1'` angegeben hat. Zusammen mit dieser Port-Angabe hier hat man dann alle nötigen Daten, um sein Programm für die Nutzung von Tor zu konfigurieren.

TOR_ALLOW_N Gibt die Anzahl der Listeneinträge an.

TOR_ALLOW_x Die Liste der Netze und/oder IP-Adressen für die der Paketfilter geöffnet wird. Sinnvoll ist hier auch wieder die Vorgabe `IP_NET_1`.

TOR_CONTROL_PORT Hier kann angegeben werden auf welchem TCP Port Tor einen Kontrollzugang über das Tor Control Protocol öffnen soll. Die Angabe ist optional. Wird nichts angegeben wird diese Funktion deaktiviert.

TOR_CONTROL_PASSWORD Hier kann ein Passwort für den Kontrollzugang angegeben werden.

TOR_DATA_DIR Diese Angabe ist optional. Wird nichts angegeben, wird der Standardordner `/etc/tor` verwendet

TOR_HTTP_PROXY Soll Tor die Anfragen an einen HTTP-Proxy weiterleiten, kann man den hier angeben. Tor bedient sich dann dieses Proxys. So kann man die Vorteile mehrerer Proxys nutzen. Ein Eintrag könnte so aussehen:

```
TOR_HTTP_PROXY='mein.provider.de:8000'
```

Die Angabe ist optional.

TOR_HTTP_PROXY_AUTH Eine eventuell notwendige Authentifizierung für den Proxy kann hier in der Form `Benutzername:Passwort` eingetragen werden.

TOR_HTTPS_PROXY Hier kann ein HTTPS-Proxy eingetragen werden. Siehe dazu auch [TOR_HTTP_PROXY](#).

TOR_HTTPS_PROXY_AUTH Siehe dazu [TOR_HTTP_PROXY_AUTH](#).

TOR_LOGLEVEL Diese Option gibt an, was Tor in die Logdatei schreiben soll. Folgende Werte sind möglich: `debug`, `info`, `notice`, `warn` oder `err`. Die Werte `debug` und `info` sollten aus Sicherheitsgründen möglichst nicht verwendet werden.

TOR_LOGFILE Falls Tor statt ins syslog in eine Datei loggen soll, kann diese hier angegeben werden.

1.1.3 OPT_SS5 - Ein Socks4/5 Proxy

Für einige Programm wird ein Socks-Proxy benötigt. SS5 stellt diese Funktionalität bereit.

<http://ss5.sourceforge.net/>

SS5_LISTEN_N

SS5_LISTEN_x Hier werden die IP-Adressen oder symbolischen Namen inklusive der Portnummer der Interfaces angegeben, auf denen SS5 auf Verbindungen von Clients horchen soll. Es ist eine gute Idee, hier nur die Adressen der Interfaces anzugeben, denen man vertraut, da alle Rechner vollen Zugriff auf SS5 haben (und auf den eventuell aktivierten Konfigurations-Editor). In der Regel ist die Vorgabe `IP_NET_1_IPADDR:8050` sinnvoll.

Auf hier angegebenen Adressen lauscht SS5 und bietet seine Dienste an. 8050 ist der Standard-Port. Die Angabe hier muss man dann bei der Proxy-Konfiguration des jeweils verwendeten Programms benutzen.

Als Proxy beim jeweiligen Programm muss der fli4l-Rechner angegeben werden, also das, was man bei `HOSTNAME='fli4l'` angegeben hat bzw. dessen IP (z.B 192.168.6.1), die man bei `HOST_x_IP='192.168.6.1'` angegeben hat. Zusammen mit dieser Port-Angabe hier hat man dann alle nötigen Daten, um sein Programm für die Nutzung von SS5 zu konfigurieren.

SS5_ALLOW_N Gibt die Anzahl der Listeneinträge an.

SS5_ALLOW_x Die Liste der Netze und/oder IP-Adressen für die der Paketfilter geöffnet wird. Sinnvoll ist hier auch wieder die Vorgabe `IP_NET_1`.

1.1.4 OPT_TRANSPROXY (EXPERIMENTELL) - Transparenter HTTP-Proxy

Transproxy ist ein „transparenter“ Proxy, also ein Programm, dass es ermöglicht, alle HTTP-Abfragen, die über den Router laufen, abzufangen und an einen normalen HTTP-Proxy, z.B. Privoxy, weiterzuleiten. Um diese Funktionalität zu erreichen, muss der Paketfilter HTTP-Anfragen, die eigentlich ins Internet gehen sollen, an Transproxy weiterreichen, welcher diese weiter aufbereitet und an den anderen HTTP-Proxy weitergibt. iptables bietet zur Unterstützung dieser Funktion die Aktion „REDIRECT“:

```
PF_PREROUTING_1='tpr1:http IP_NET_1 REDIRECT:8081'
```

Diese Regel würde alle HTTP-Pakete aus dem ersten definierten Netz (normalerweise das interne LAN) an Transproxy auf Port 8081 weiterleiten.

TRANSPROXY_LISTEN_N

TRANSPROXY_LISTEN_x Hier werden die IP-Adressen oder symbolischen Namen inklusive der Portnummer der Interfaces angegeben, auf denen Transproxy auf Verbindungen von Clients horchen soll. Hier müssen alle Interfaces angegeben werden, für die im Paketfilter Pakete auf Transproxy umgelenkt werden. Mit der Vorgabeeinstellung `any:8081` hört Transproxy auf allen Interfaces.

TRANSPROXY_TARGET_IP

TRANSPROXY_TARGET_PORT Mit diesen Optionen wird festgelegt, an welchen Dienst eingehende HTTP-Anfragen umgeleitet werden. Dies kann ein beliebiger Standard-HTTP-Proxy (Squid, Privoxy, Apache, etc.) auf einem beliebigen anderen Rechner (oder auch auf fl4l selbst) sein. Hier ist darauf zu achten, dass der Proxy sich nicht im Bereich der durch den Paketfilter umgeleiteten HTTP-Anfragen befindet, da sonst eine Schleife entsteht.

TRANSPROXY_ALLOW_N

TRANSPROXY_ALLOW_x Die Liste der Netze und/oder IP-Adressen für die der Paketfilter geöffnet wird. Dies sollte die gleichen Netze abdecken, die auch im Paketfilter umgeleitet werden. Werden hier keine Bereiche angegeben, müssen die Angaben von Hand in der Paketfilter-Konfiguration vorgenommen werden.

Abbildungsverzeichnis

Tabellenverzeichnis

Index

OPT_PRIVOXY, [3](#)
OPT_SS5, [7](#)
OPT_TOR, [5](#)
OPT_TRANSPROXY, [7](#)

PRIVOXY_MENU, [3](#)
PRIVOXY_N, [3](#)
PRIVOXY_x_ACTIONDIR, [4](#)
PRIVOXY_x_ALLOW_N, [4](#)
PRIVOXY_x_ALLOW_x, [4](#)
PRIVOXY_x_CONFIG, [4](#)
PRIVOXY_x_HTTP_PROXY, [4](#)
PRIVOXY_x_LISTEN, [3](#)
PRIVOXY_x_LOGDIR, [5](#)
PRIVOXY_x_LOGLEVEL, [5](#)
PRIVOXY_x SOCKS_PROXY, [4](#)
PRIVOXY_x_TOGGLE, [4](#)

SS5_ALLOW_N, [7](#)
SS5_ALLOW_x, [7](#)
SS5_LISTEN_N, [7](#)
SS5_LISTEN_x, [7](#)

TOR_ALLOW_N, [6](#)
TOR_ALLOW_x, [6](#)
TOR_CONTROL_PASSWORD, [6](#)
TOR_CONTROL_PORT, [6](#)
TOR_DATA_DIR, [6](#)
TOR_HTTP_PROXY, [6](#)
TOR_HTTP_PROXY_AUTH, [6](#)
TOR_HTTPS_PROXY, [6](#)
TOR_HTTPS_PROXY_AUTH, [6](#)
TOR_LISTEN_N, [5](#)
TOR_LISTEN_x, [6](#)
TOR_LOGFILE, [6](#)
TOR_LOGLEVEL, [6](#)
TRANSPROXY_ALLOW_N, [8](#)
TRANSPROXY_ALLOW_x, [8](#)
TRANSPROXY_LISTEN_N, [7](#)
TRANSPROXY_LISTEN_x, [7](#)

TRANSPROXY_TARGET_IP, [7](#)
TRANSPROXY_TARGET_PORT, [7](#)