

Pacquetage PROXY

Version 3.7.0-rev20394

Frank Meyer L'équipe fli4l
courriel : frank@fli4l.de courriel : team@fli4l.de

2 décembre 2011

Table des matières

1	Documentation du paquetage PROXY	3
1.1	PROXY - Différent Serveur-Proxy	3
1.1.1	OPT_PRIVOX - Filtrage de la publicité avec un Proxy-HTTP	3
1.1.2	OPT_TOR - Système de communication anonyme pour Internet	5
1.1.3	OPT_SS5 - Proxy Socks 4/5	7
1.1.4	OPT_TRANSPROXY (EXPÉRIMENTAL) - Proxy-HTTP Transparent	7
	Table des figures	9
	Liste des tableaux	10
	Index	11

1 Documentation du paquetage PROXY

1.1 PROXY - Différent Serveur-Proxy

1.1.1 OPT_PRIVOXY - Filtrage de la publicité avec un Proxy-HTTP

Privoxy "Privacy Enhancing Proxy" ("filtrage avancé, pour la protection de la vie privée") voir le site Web officiel de Privoxy (<http://www.privoxy.org/>). Privoxy filtre le contenu des pages web sur votre navigateur, en remplaçant par des images vides les bannières publicitaires et les Popups, Il gère les cookies dans une mémoire cache (petit paquet de données avec lesquels un site web peut reconnaître certain surfer) et empêche l'affichage de ce que l'on appelle bugs-Web (ce sont de grandes images 1x1 pixels, qui sont utilisées, pour espionner le comportement des utilisateurs sur le Net).

Pendant que Privoxy fonctionne, vous pouvez tout simplement configurer et activer les paramètres par l'intermédiaire de l'interface Web. L'interface Web se trouve à l'adresse <http://config.privoxy.org/> ou en abrégée <http://p.p/>.

Privoxy Internet Junkbusters à eu une évolution conséquente à partir de la version 2.1.0, voir le site Web (<http://www.junkbuster.com/>). L'innovation la plus importante, est que toutes les règles de filtrage sont centralisées dans un fichier `default.action`. Celui-ci se trouve dans le répertoire FLI4L /`etc/privoxy`. Le grand avantage de cette méthode c'est que les nouvelles versions de ce fichier peuvent être télécharger séparément à cette adresse <http://sourceforge.net/projects/ijbswa/files/>.

Ainsi, chaque utilisateur FLI4L peut tenir ce fichier à jour, sans mettre à jour le routeur-FLI4L. (Actuellement, la version 1.8 de ce fichier est dans ce paquetage)

PRIVOXY_MENU Avec cette variable, vous pouvez ajouter la section Privoxy au menu-httpd.

PRIVOXY_N Vous indiquez dans cette variable le nombre de Privoxy qui doit être enregistré pour chaque interface.

PRIVOXY_x_LISTEN Vous indiquez dans cette variable, l'adresse-IP ou le nom symbolique, y compris le numéro de Port de l'interface, sur lequel le Privoxy doit écouter les connexions des clients. C'est une bonne idée d'indiquer ici, seulement les adresses des interfaces que l'on fait confiance, car tous les ordinateurs auront un accès complet à travers le Privoxy (avec bien sur le navigateur configuré et activé). En règle générale il est judicieux d'indiquer, la valeur par défaut qui est `IP_NET_1_IPADDR :8118`

Avec l'adresse indiquée ici, le Privoxy écoute et offre ses services. Le port par défaut est 8118. Vous devez utiliser cette information pour configurer le proxy dans votre navigateur. Pour plus de détail sur la configuration d'Internet Explorer et de Netscape Navigator, voir le site Web :

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

Vous devez enregistrer dans chaque navigateur, en tant que proxy l'ordinateur-fli4l, vous allez donc prendre le nom de la variable `HOSTNAME='fli4l'` ou l'adresse-IP (par ex. 192.168.6.1) de la variable `HOST_x_IP='192.168.6.1'` qui est dans le fichier config de fli4l.

Une configuration ainsi activer ne survit pas à un redémarrage du routeur fli4l... (tobig)

URL précise

Avec le Port par défaut, on a ici tous les paramètres nécessaires, pour configurer votre navigateur Web, pour l'utilisation du Privoxy.

PRIVOXY_x_ALLOW_N Vous indiquez dans cette variable le nombre d'adresse réseau à installer.

PRIVOXY_x_ALLOW_x Vous indiquez dans cette variable l'adresse réseau ou l'adresse-IP pour le quelle le filtrage de paquets doit être ouvert. Normalement il est logique d'indiquer ici le paramètre `IP_NET_1`.

PRIVOXY_x_ACTIONDIR Avec cette variable vous indiquez l'emplacement, ou vous pouvez paramétrer l'ensemble des règles Privoxy, (avec les fichiers *default.action* et *user.action*) sur le routeur. Le chemin d'accès spécifié est évaluée par rapport au répertoire racine. Cette variable peut être utilisé pour deux choses différentes :

Le déplacement de l'Ensemble des règles de la mémoire permanente Si vous spécifiez un répertoire dans un emplacement autre que le disque-RAM, au démarrage de `fi4l` l'ensemble des règles défini par défaut sera copié et utilisé à partir de cet emplacement. Les modifications apportées à ces ensembles de règles survivront à un redémarrage du routeur. On doit aussi tenir compte du fait qu'après une mise à jour du paquetage Privoxy, ces règles seront toujours utilisées donc l'ensemble des règles du paquetage de mise à jour sera simplement ignoré.

l'utilisation de vos propres ensembles de règles L'utilisateur `fi4l` permet d'écrire des règles spécifiques à la place des règles standard. Vous devez dans cette variable indiquer votre propre sous-répertoire qui sera dans le répertoire *config* (par exemple *etc/mon_privoxy*, par contre vous ne devez pas indiquer *etc/privoxy*) ensuite vous placez dans ce sous-répertoire vos propres règles.

Le paramétrage de cette variable est optionnel.

PRIVOXY_x_HTTP_PROXY Si vous voulez utiliser en plus du Privoxy un autre Proxy HTTP, c'est-à-dire utiliser également des pages Web en cache, vous pouvez paramétrer cette variable. Le Privoxy utilise alors ce proxy. Avec cette variable vous avez l'avantage utilisé plusieurs Proxys. Le paramètre peut ressembler à cela :

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

Ce paramètre est optionnel.

PRIVOXY_x SOCKS_PROXY Si vous voulez utiliser en plus du Privoxy un autre Proxy SOCKS. Pour augmenter la surveillance privée de la transmission de données du Privoxy, par exemple, envoyé les données par le réseau Tor, vous pouvez paramétrer cette variable. Pour plus de détails sur Tor, reportez-vous à la [Documentation Tor](#) (Page 5). Le paramètre pour l'utiliser Tor peut ressembler à cela :

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

Ce paramètre est optionnel.

PRIVOXY_x_TOGGLE Avec cette variable vous pouvez arrêter le proxy par l'interface Web. Si le Privoxy est mis hors circuit, il réagira simplement comme Proxy-Forwarding et ne modifiera plus le contenu des pages Web transférées. Vous devez considérer, que ce réglage vaut pour TOUS les utilisateurs du Proxy, c.-à-d. que si un utilisateur arrête Privoxy, le Privoxy sera coupé pour tous les autres utilisateurs Web qui transfert par Proxy.

PRIVOXY_x_CONFIG Avec cette variable, les utilisateurs ont la possibilité de configurer le proxy par l'interface web. Pour plus de détails, je vous demande de consulter la documentation Privoxy qui est ici.

PRIVOXY_x_LOGDIR Dans cette variable vous pouvez indiquer le répertoire du fichier log (ou journal) pour le privoxy. Cela peut être utile, par ex. lorsque l'utilisateur veut enregistrer les accès des sites Web. Si rien n'est spécifié (par défaut), les principaux messages sont enregistrés sur la console et la variable **PRIVOXY_LOGLEVEL** est ignorée.

PRIVOXY_x_LOGLEVEL On indique dans cette variable les valeurs, pour que Privoxy puisse enregistrer les événements dans le fichier log. Il est possible d'ajouter plusieurs valeurs à la suite, vous devez les séparer par un espace. Les valeurs suivantes peuvent être ajoutées.

Valeur	ce qui sera enregistré ?
1	Chaque Requête (GET/POST/CONNECT).
2	Le statut de chaque connexion
4	Le statut-I/O
8	Header-Parsing
16	Toutes les données
32	Debug force-feature
64	Debug regular expression filters
128	Debug redirects
256	Debug GIF animation
512	Common Log Format (Analyse fichier-log)
1024	Debug kill pop-ups
2048	CGI (server web) user interface
4096	Startup banner and warnings
8192	Non-fatal errors

Pour produire un fichier log (journal) avec Common Log Format, vous devez indiquer SEULEMENT la valeur 512, si vous indiquez d'autres valeurs le fichier log sera "pollué" par d'autres enregistrements et on aura des problèmes pour l'analyser.

Privoxy offre de très nombreuses options de configurations. Cependant pour des raisons compréhensibles nous ne pouvons pas développer toutes ces options dans le fichier de configuration de fli4l. Beaucoup de ces options peuvent être paramétrées sur l'interface Web de Privoxy. Vous trouverez des infos plus précises pour la configuration de ces fichiers sur la page d'accueil de Privoxy. Les fichiers de configuration de Privoxy se trouvent dans le répertoire <FLI4L-Version>/opt/etc/privoxy/. Ce sont des fichiers originaux du Paket-Privoxy, toutefois, pour gagner de la place, tous les commentaires ont été supprimés.

1.1.2 OPT_TOR - Système de communication anonyme pour Internet

Tor est l'outil d'un grand nombre d'organismes et de simples citoyens, qui veulent améliorer leur protection et leur sécurité sur Internet. L'utilisation de Tor vous aide à être anonymes lors de la navigation et de la publication sur le Web, messagerie instantanée, IRC, SSH et autres applications basées sur TCP. En outre, Tor fournit une plate-forme sur laquelle les développeurs de logiciels peuvent créer de nouvelles applications pour plus d'anonymat, sur la sécurité et la protection de la vie privée.

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

TOR_LISTEN_N

TOR_LISTEN_x Dans la première variable, vous indiquez le nombre d'adresse réseau, dans la deuxième variable vous indiquez l'adresse-IP ou le nom symbolique, y compris le numéro de Port de l'interface, sur lequel Tor doit écouter les connexions des Clients. C'est une bonne idée, d'indiquer ici seulement les adresses des interfaces que l'on fait confiance, car tous les ordinateurs auront un accès complet à travers Tor (avec bien sur le navigateur configuré et activé). En règle générale il est judicieux d'indiquer, la valeur par défaut qui est `IP_NET_1_IPADDR :9050`

Avec l'adresse indiquée ici, Tor écoute et offre ses services. Le port par défaut est 9050. Vous devez utiliser cette information pour configurer le proxy dans votre navigateur.

Vous devez indiquer dans chaque navigateur en tant que proxy l'ordinateur-fli4l, vous allez donc prendre le nom de la variable `HOSTNAME='fli4l'` ou l'adresse-IP (par ex. 192.168.6.1) de la variable `HOST_x_IP='192.168.6.1'` qui est dans le fichier config de fli4l. Avec le Port par défaut, on a ici tous les paramètres nécessaires, pour configurer votre navigateur Web, pour l'utilisation de Tor.

TOR_ALLOW_N Vous indiquez dans cette variable le nombre d'adresse réseau à installer.

TOR_ALLOW_x Vous indiquez dans cette variable l'adresse réseau ou l'adresse-IP pour le quelle le filtrage de paquets doit être ouvert. Normalement il est logique d'indiquer ici le paramètre `IP_NET_1`.

TOR_CONTROL_PORT Vous indiquez dans cette variable, le port TCP que Tor doit utiliser, pour le contrôle d'accès via le protocole Tor. Cette variable est optionnelle, si rien n'ai indiqué cette fonction sera désactivée.

TOR_CONTROL_PASSWORD Vous spécifier dans cette variable, un mot de passe pour le contrôle d'accès.

TOR_DATA_DIR Cette variable est optionnelle. Si rien n'est indiqué, le dossier par défaut `/etc/tor` est utilisé.

TOR_HTTP_PROXY Si vous voulez utiliser en plus de Tor un autre Proxy http, Tor pourra alors utiliser ce proxy. Avec cette variable vous avez l'avantage utilisé plusieurs Proxys. Le paramètre peut ressembler à cela :

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

Ce paramètre est optionnel.

TOR_HTTP_PROXY_AUTH Une authentification peut-être nécessaire, vous devez la spécifier dans cette variable. Ainsi le mandataire sera enregistré sous la forme Nom d'utilisateur :Mot de passe.

TOR_HTTPS_PROXY Vous pouvez enregistrer dans cette variable, un Proxy-HTTPS. Voir [TOR_HTTP_PROXY](#).

TOR_HTTPS_PROXY_AUTH Voir pour ce sujet [TOR_HTTP_PROXY_AUTH](#).

TOR_LOGLEVEL On indique dans cette variable les valeurs pour que Tor puisse enregistrer les événements dans le fichier log. Les valeurs suivantes sont possibles : debug, info, notice, warn ou err. Les valeurs debug et info ne devraient pas si possible être utilisées, pour des raisons de sécurité.

TOR_LOGFILE Si vous voulez utiliser un autre système que syslog pour enregistrer les événements de Tor, vous devez l'indiquer dans cette variable.

1.1.3 OPT_SS5 - Proxy Socks 4/5

Il est nécessaire d'installer le Proxy-Socks pour certains programmes, nous mettons à disposition ici le protocole SS5. Voir le site Web.

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

SS5_LISTEN_N

SS5_LISTEN_x Dans la première variable vous indiquez le nombre d'adresse réseau, dans la deuxième variable vous indiquez l'adresse-IP ou le nom symbolique, y compris le numéro de Port de l'interface, sur lequel SS5 doit écouter les connexions des Clients. C'est une bonne idée, d'indiquer ici seulement les adresses des interfaces que l'on fait confiance, car tous les ordinateurs auront un accès complet à travers SS5 (avec bien sur le navigateur configuré et activé). En règle générale il est judicieux d'indiquer, la valeur par défaut qui est `IP_NET_1_IPADDR :8050`

Avec l'adresse indiquée ici, SS5 écoute et offre ses services. Le port par défaut est 8050. Vous devez utiliser cette information pour configurer le proxy dans votre navigateurs.

Vous devez indiquer dans chaque navigateur en tant que proxy l'ordinateur-fli4l, vous allez donc prendre le nom de la variable `HOSTNAME='fli4l'` ou l'adresse-IP (par ex. 192.168.6.1) de la variable `HOST_x_IP='192.168.6.1'` qui est dans le fichier config de fli4l. Avec le Port par défaut, on a ici tous les paramètres nécessaires, pour configurer votre navigateur Web, pour l'utilisation de SS5.

SS5_ALLOW_N Vous indiquez dans cette variable le nombre d'adresse réseau à installer.

SS5_ALLOW_x Vous indiquez dans cette variable l'adresse réseau ou l'adresse-IP pour laquelle le filtrage de paquets doit être ouvert. Normalement il est logique d'indiquer ici le paramètre `IP_NET_1`.

1.1.4 OPT_TRANSPROXY (EXPÉRIMENTAL) - Proxy-HTTP Transparent

Transproxy est un proxy "transparent", c'est une application qui permet, d'intercepter toutes les requêtes-HTTP qui passent par le routeur et de les transmettre à un Proxy-HTTP normal, par ex. au Privoxy. Pour parvenir à cette fonctionnalité, le filtre de paquets des requêtes HTTP qui doit aller sur Internet, passent par le transproxy celui-ci les traite et les transmet à un Proxy-HTTP. Iptables supporte cette fonction en utilisant le paramètre "REDIRECT" :

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

Cette règle transmet tous les paquets-HTTP du premier réseau défini (normalement c'est le LAN interne) au transproxy par le port 8081.

TRANSPROXY_LISTEN_N

TRANSPROXY_LISTEN_x Vous indiquez ici, les adresses IP ou les noms symboliques, ainsi que le numéro de port des interfaces, sur lesquels Transproxy doit écouter les connexions des clients. Si Toutes les interfaces spécifiées ici, utilise déjà un filtrage de paquets, Transproxy sera gêné par les paquets qui provient de ce filtrage. Avec la configuration par défaut `any :8081` Transproxy écouterait toutes les interfaces.

TRANSPROXY_TARGET_IP

TRANSPROXY_TARGET_PORT Grâce à cette option vous définissez le service pour lequel les requêtes HTTP doivent être redirigé. Cela peut être n'importe quel proxy standard HTTP (Squid, Privoxy, Apache, etc) et sur n'importe quel ordinateur (ou sur lui-même). Faire attention, que le Proxy ne se trouve pas dans le domaine du filtrage de paquet, dans lequel les requêtes http seront redirigées. Autrement un bouclage d'adresse apparaîtra.

TRANSPROXY_ALLOW_N

TRANSPROXY_ALLOW_x Liste des réseaux et/ou des adresses IP pour le filtrage de paquets ouvert. Cela devrait couvrir mêmes les réseaux, qui sont redirigés par le filtrage de paquets. Si aucun domaine n'est indiqué ici, vous devez indiquer les informations manuellement dans la configuration du filtrage de paquets.

Table des figures

Liste des tableaux

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, [5](#)
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](#)