Mise en place d'un proxy avec: Privoxy - Squid - Tor

Je vous propose un petit didacticiel sur l'installation d'un serveur proxy, en vous servant d'un vieil ordinateur sur lequel vous installerez ubtuntu server.

Pour quoi faire ?

Le proxy, servira a filtrer les pages webs consultées en http (seulement!). Il apportera trois fonctions importantes:

- Possibilité de transiter une partie du trafic par le réseau tor
- Possibilité de bloquer certaines pages, et de pouvoir modifier certains contenus
- Possibilité de mettre en cache certaines données, telles que les images, ou les données DNS.

Tout cela, entre autre dans un soucis, de sécuriser votre navigation (attention à tor cependant !), et de retrouver un minimum de vie privée (Mais on est malheureusement loin de la perfection).

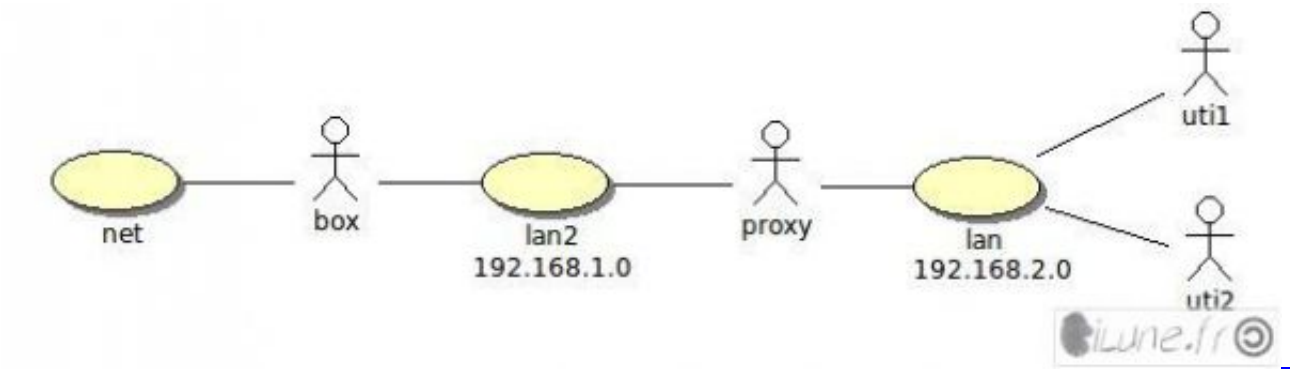
A noter

Je ne détaillerai pas les étapes de l'installation de ubuntu server, seulement, le paramètrage du proxy.

A noter, que vous rencontrerez surement des erreurs, et que il est important que vous compreniez les données indiquée pour pouvoir les adapter à vos besoins et votre configuration (!!!).

Enfin, je ne me préoccupe pas des problèmes des droits d'accès etc, je vous laisse le gérer en fonction. J'apporterai des modification au document de temps à autre, pour corriger ou améliorer certaines parties.

J'ai réalisé un petit schéma (pas normé du tout) pour donner une idée de ce que l'on veut faire:



Materiel requis

Pour mettre en place le proxy, il vous faudra:

- Un vieux PC (Pas forcément besoin d'un écran à part pour l'installation) avec deux interfaces réseaux (wifi déconseillé). Vous pouvez acheter une carte Réseau USB externe, si vous n'avez qu'une carte réseau, ou en rajouter une.
- Un switch pour connecter les différents PC du réseau interne au proxy.
- Des cables RJ45 pour relier tout ce beau monde
- Bien sûr un accès internet, et au moins un pc utilisateur

Et c'est tout ! Un peu de place pour mettre tout ça et ça sera bon
. (Bien sûr pour bien faire n'oubliez pas qu'un ondulateur n'est pas un grand luxe)

Installation de la souris pour la console : paquet gpm

```
sudo apt-get install gpm
```

Installation de fluxbox si on veut une petite interface graphique

```
Sudo apt-get install xorg
sudo apt-get install fluxbox
startx
```

Paramétrage IP de eth0 et eth1

Pour pouvoir faire fonctionner les deux connexions sur le proxy, il faut paramètrer les deux interfaces de l'ordinateur, ici eth0 et eth1.

On va donc modifier le fichier de configuration dans **/etc/network/interface,** Remplacer DHCP (ip automatique) par static et on renseigne les paramètres de configuration pour les deux réseau selon le besoin.

```
auto eth0
iface eth0 inet static
        address 192.168.1.2
        netmask 255.255.255.0
 network 192.168.1.0
        gateway 192.168.1.1

auto eth1
iface eth1 inet static
        address 192.168.2.1
        netmask 255.255.255.0
 network 192.168.2.0
```

Redémarrer le réseau pour appliquer les changements :

```
sudo /etc/init.d/networking restart
```

Et surement le proxy:

```
sudo reboot
```

Afficher les paramètres réseaux courants:

```
ifconfig -a
```

Installation de SSH

Pour se simplifier la vie, et ne pas bouger constamment entre le proxy et notre ordinateur, on va installer SSH, qui nous permet de nous connecter au proxy et d'y faire les opérations qu'on veut sans bouger de notre chaise
 !

De plus SSH contrairement à telnet crypte ses connexions, donc c'est ++ mieux d'un point de vue sécurité


```
Sudo apt-get install openssh-server
```

Une fois installé, pour vous connecter il vous suffit de renseigner cette commande sur votre console:

```
ssh @
```

Vous pouvez également utiliser SSH pour copier des fichiers de votre ordinateur au proxy:

```
scp  @ipadress>:
```

Installation de Ntop

Ntop est un logiciel qui permet d'enregistrer le trafic passant sur un serveur. Il dispose d'une interface web, et sera donc très bien pour un proxy.

```
sudo apt-get install ntop
```

Définir le password d'administration pour ntop

ntop --set-admin-password

Démarrer ntop

sudo /etc/init.d/ntop start

Consulter ntop

http://192.168.2.1:3000

!!! ATTENTION A FOXY PROXY (le désactiver pour consulter ntop) [erreur : Please enable make sure that the ntop html/ directory is properly installed]

Repertoire de configuration

/var/lib/ntop

Supprimer

sudo apt-get remove --purge ntop

(parfois, en cas de problème plus simple de le supprimer et le réinstaller)

Privoxy, Squid, Tor: Installation

Bien, nous avons notre espace de travail en place, il est temps de passer au sérieux, à savoir l'installation de privoxy, squid, et tor
 !!!

Privoxy

C'est un proxy qui a pour rôle de bloquer des domaines, des liens, et dispose d'une fonction pour filtrer le contenu des pages chargés, voir même de le remplacer ! (et c'est là son grand avantage).

Squid

C'est un proxy cache, c'est à dire qu'il conserve les fichiers que vous consultez sur le net dans l'ordinateur, et les restitue si vous les redemandez. Il peut avoir d'autres fonctions comme ici où il sert à rediriger les requètes vers un des deux privoxy (oui vous comprendrez après)

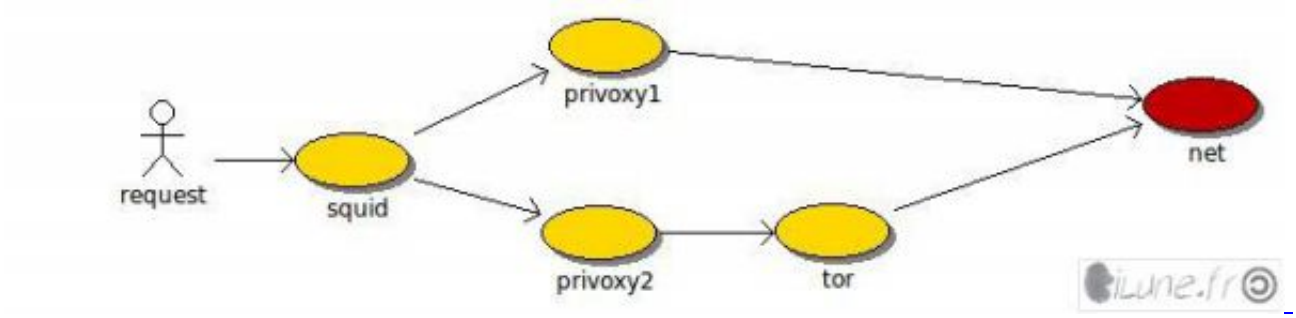
Tor

Tor est un réseau avant tout, qui permet d'anonymiser vos connexions en passant par d'autres particuliers... Ainsi ça empèche de savoir qui est qui.

Gros problème à être conscient: Utiliser Tor signifie être conscient que ses données peuvent être lues par quelqu'un d'autre (même si ce quelqu'un ne sait pas que c'est vous), étant donné que vous allez passer par les ordinateurs d'inconnus, qui si ils se placent en fin de parcours, peuvent lire les flux facilement.

Autre problème: Tor est lent ! C'est la raison que nous ne l'utilierons que pour certains cas particuliers.

Nous allons mettre en place ce schéma:



On installe privoxy:

```
sudo apt-get install privoxy
```

On installe squid

```
sudo apt-get install squid
```

On installe Tor

Pour tor, c'est un peu plus compliqué (rhoo à peine
)

Déjà il faut rajouter le dépôt tor en rajoutant une ligne dans le fichier `/etc/apt/sources.list:`

deb http://deb.torproject.org/torproject.org main

Vous remplacez par la votre (*cherchez pas bien loin, regardez les lignes au dessus*
)

Vous tappez ensuite (un par un)

```
sudo gpg --keyserver keys.gnupg.net --recv 886DDD89
```

```
sudo gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -
```

Si tout s'est bien passé, vous pouvez enfin renseigner les commandes d'installation:

```
apt-get update
apt-get install tor tor-geoipdb
```

Et voila !!


Ça y est, les trois logiciels sont installés ! C'est fini ? Et non, il va falloir paramètrer tout ça !


Attend ! Comment on test ?

Et oui !


Je vous conseille d'installer foxyproxy (le plugin firefox) pour pouvoir switcher entre les ports d'écoute en fonction du proxy testé.

Mais il vous faudra également pour que ça fonctionne dire au proxy, qu'il va servire de proxy... Sinon rien ne marchera
 ! Pour cela, vous entrerez dans une console (à chaque fois que ça redemarre) cette ligne:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
#changez eth0 par le nom de votre interface correspondant à internet.
sudo iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQU
ERADE
```

Paramétrage de Tor

On commence par la fin, pour effectuer les paramètrages (les derniers noeuds en lien avec le net). Ça permet entre autre de pouvoir tester tout ça
 .

Pour ceux que ça interesse, il n'y a peu d'articles qui expliquent comment paramétrer Tor, mais vous en avez un autre ici: https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/CentralizedTorServer et ici: http://doc.ubuntu-fr.org/tor

Donc on va commencer par tor.

Le fichier de configuration principal de tor se trouve dans le dossier /etc/tor/torrc.

Nous ne changerons peu de choses dedans.
Tout d'abord vérifier ses ports d'écoutes:

```
SocksPort 9050 # what port to open for local application connections
SocksListenAddress 127.0.0.1 # accept connections only from localhost
```

Vous noterez que j'ai laissé l'écoute en 127.0.0.1, puisque nous n'accéderons pas directement à tor. (C'est privoxy qui lui transférera les paquests)

Bien, vous pouvez changer ensuite l'emplacement de vos logs.

```
Log notice file /[folter]/notices.log
Log debug file /[folder]/debug.log
```

Voila, ces paramètres devraient suffire.
Suivant
 !

Paramétrage de Privoxy

N.B.: Quand j'ai fait ma config, je me suis beaucoup inspiré de cet article http://artisan.karma-lab.net/node/1204 *- Il peut y avoir donc des ressemblances, de plus il est très bien rédigé (mieux que moi)*

Bien, alors il y a un peu de travail...


Nous voulons avoir deux privoxy, l'un qui renvoie sur tor, et l'autre qui renvoie directement sur le net !

Pour cela nous utiliserons deux ports d'écoute, 8118 (par défaut) et 8119.

Pour simplifier nous doublerons après avoir paramétrer le premier (qui redirige sur le net).

config

Le fichier de configuration de privoxy se trouve dans /etc/privoxy.

Donc on modifie l'adresse et le port d'écoute:

listen-address 192.168.2.1:8118

On autorise l'accès à privoxy via notre réseau interne

permit-access 192.168.2.0/24

On rajoute un fichier user.filter, pour y renseigner nos propres filtres

filterfile user.filter

On peut changer le dossier de logs

logdir /[reperoire]/privoxy

On indique ce qu'on veut que privoxy log

```
debug     1 # Log the destination for each request Privoxy let through.
debug     512 # Common Log Format
debug   1024 # Log the destination for requests Privoxy didn't let through, and the reason why.
debug   4096 # Startup banner and warnings
debug   8192 # Non-fatal errors
```

On lui dit qu'il peut utiliser de la mémoire pour traiter les files

buffer-limit 50000

Voila pour les principales configurations.


Rajouter la deuxième instance de privoxy

Celle qui redirigera les requêtes vers Tor !!!


Pour cela on repasse à notre console:

```
#on double notre fichier config
sudo cp -a /etc/privoxy/config /etc/privoxy/config2
#on double les fichiers systèmes
sudo cp /etc/init.d/privoxy /etc/init.d/privoxy2
sudo cp /usr/sbin/privoxy /usr/sbin/privoxy2
```

On edit le deuxième lanceur

Ouvrez le fichier /etc/init.d/privoxy2 et changez le nom par privoxy2:

NAME=privoxy2

Changez le fichier de configuration

CONFIGFILE=/etc/privoxy/config2

Le tour est presque joué !

On modifie le fichier config

Notre deuxième fichier de configuration utilisera les mêmes filtres (filter.user) et actions (action.user) que le premier. Ainsi en modifiant un fichier d'action ou de filtre, on modifie pour les deux instances de privoxy !
 (ouiiii c'est beau l'informatique)

Bon alors première chose à changer, le port d'écoute:

listen-address 192.168.10.1:8119

Le fichier de log

logfile logfile2

Et le forward donc vers notre tor

forward-socks5 / 127.0.0.1:9050 .

(par oublier le point à la fin)

Et c'est bon !

Supeeer !!! Fini avec privoxy !!! Heu non pas du tout
 !

Le fichier action

Et oui, bon alors ça peut faire redondance avec squid, mais privoxy est plus orienté blocage de site que squid...

Vous noterez que il y a un défault.action, et un user.action (pour nous) !!!

Je ne m'attarde pas trop sur la syntaxte de chaque élément, consultez la doc officielle pour plus d'information http://www.privoxy.org/user-manual/actions-file.html#ACTIONS ou cet article très bien fait http://artisan.karma-lab.net/node/1204

Le block

Alors, la balise block parle assez bien... Ça bloque les sites et url que vous aimez pas.

Je vous présente ma petite liste... (mais oui j'aime tout le monde)

```
#BLOCK

{ +block{bad} }
# Régies publicitaires/ Plate-formes d'annonce
.netavenir.com
.turn.com
.bluestreak.com
.criteo.com
.blogbang.com/demo/js/blogbang_ad.php\?id=
/.*\/microsoft_adcenterconversion\.js
*.*.marketingsolutions.yahoo.com/*
```

```
.googleadservices.com/*
.fmpub.net
pubsrv.allopass.com/*
.comclick.com
.regieci.com
.allo-audience.fr
.audientia.net
.clickintext.com
.clickintext.net
.intellitxt.com
payperpost.com
.counter.com
.hitbox.com
.doubleclick.net
.cashcount.com
.cryotrades.com
.adxpansion.com
.quantserve.com
.livejasmin.com
.partypoker.fr
.el-cigarette.net
.email-match.com
.visio-rose.com
.shopoon.fr
.adserverpub.com
.banstex.com
.surftraffic.net
.super-ads.fr
.avenir-affiliation.fr
.128b.com
.trafficrevenue.net
.veoxa.com
.scorecardresearch.com

# Les enregistreurs/relecteurs
.clicktale.*                                    # clicktale.com/faq.html
cetrk.com/*                                     # crazyegg.com/overview
*.robotreplay.com/*                             # robotreplay.com/
/.*/clickheat.js

  # médiamêtrie/traçage
.estat.com                                      # .estat.com/service/servi
ces_form.html
.sitemeter.com                                  # .sitemeter.com/
.w3counter.com                                  # .w3counter.com/
.reinvigorate.net                                # eport.reinvigorate.net/
snoop
/.*\/webanalytics                                # france.webanalytics.be/
.opentracker.net                                # www.opentracker.net/inde
x.jsp
.weborama.*                                      # weborama.com/
.quantserve.com                                  # .quantcast.com/
```

```
.performancing.com                          # performancing.com/tracke
r
.ToutLeMondeEnBlogue.com                    # .toutlemondeenblogue.com
/index.aspx
stats.wordpress.com                          # .wordpress.com
*.technorati.com/*                          # .technorati.com
embed.technorati.com/linkcount              #
/.*xiti.js                                  # .xiti.com/
*.getclicky.com/*                            # .getclicky.com/help/
*.iminr.com/*                                # .iminr.com/
.netprofitblueprint.com/*                    # .netprofitblueprint.com
/capture.html (assez opaque celui-la...)
.converdge.com                              # .converdge.com/features
.cybermonitor.com
my.blogitexpress.com/.*\.js                  # .blogitexpress.com/
.atoomic.com/js/*                         # .atoomic.com/
.clustrmaps.com/counter/*
.trackalyzer.com
log.tf1.fr
.amung.us
.getclicky.com
.go2web20.net
.appspot.com
.wikio.fr
.woopra.com
.woopra-ns.com
.progressiveline.com

  # Page ranking
.free-pagerank.com/fcgi-bin/alive_js.fcgi.*
external.wikio.fr/blogs/top/getrank
.pagerank.fr/pagerank-actuel.gif

  # Loggers un peu trop traçeurs
.mybloglog.com                              # .mybloglog.com/
.rpxnow.com

  # traçage des flux (feeds)
    feedjit.com/*                                 # feedjit.com/

  # Spécial Google
/.*utm.js                                    # variante d'urchin
/.*stat.*\.js                                # un filtrage générique
/.*\/urchin.js                              # variante d'urchin
/.*s_code.js                                # variate d'urchin
/.*google-analyticator.*                    # le plugin pour wordpress
.google.com/coop/cse/brand?form=cse-search-box.*
.google.com/cse/intl/fr/images/google_custom.*\.gif
.google.com/coop/cse/brand.*
.google.com/recaptcha.*
.recaptcha.net
.safebrowsing-cache.google.com/safebrowsing.*
```

```
.google.*/csi\?v=.*
.clients*.google.*
.google.*/extern_.*
/.*googleanalytics.js
.google.fr/.*google_custom_search_watermark\.gif
.google.com/afsonline/show_afs_search\.js
.ajax.googleapis.com
.google.fr/cse/brand.*
.googleapis.com
.themes.googleusercontent.com
.maps.google.com

.dailymotion.com/flash/dmplayerv.*/plugins/GoogleAnalytics\.swf.*

#voila
.search.*.voila.*

#Pour bloquer les points exe
#/.*\.exe$

#facebook
#.static.ak.connect.facebook.com/connect\.php.*
#.facebook.com/ajax/presence.*
#.facebook.com/ajax/chat/buddy_list\.php.*
#.static.ak.fbcdn.net/images/connect_favicon\.png
#.static.ak.facebook.com/images/connect_sprite\.png
#.api.facebook.com/static/.*
#.static.ak.fbcdn.net/images/connect_.*
#.static.ak.facebook.com/images/connect_.*
#.static.ak.fbcdn.net/connect\.php/css/share-button-css
.facebook.com/plugins/like\.php.*
.facebook.com/plugins/likebox\.php*
#.static.ak.fbcdn.net/connect\.php.*
#.static.ak.fbcdn.net/rsrc.php.*
#.error.facebook.com/common/scribe_endpoint.php.*
#.facebook.com/.*&width=.*&connections=.*&stream=.*&header=.*&height=.
*
.facebook.com/plugins/activity\.php.*
#.connect.facebook.net/.*/all\.js
#.static.ak.fbcdn.net/connect/xd_proxy.php.*

#FACEBOOK2

.facebook.com/ajax/connect/activity_widget\.php.*

#SPECIAL MOI (domaine void)
.void

#autres
.fnacmusic.com
.fnac.com
.easyvoyage.com
```

```
.easyvols.org
.assuremieux.com
.gymglish.com
.static.inplay.tubemogul.com/tm-web/globe\.ogg
.load.tubemogul.com
.addthiscdn.com
.mediagra.com
.trafficholder.com
```

```
#chelous
.twimg.com
.yacast.net
.primenets.net
.cedexis.com
.chartbeat.com
.chartbeat.net
.primenets.net
.gstatic.com
.sd1.fr

#sais plus pourquoi
.addthis.com
.nsimg.net
.camads.net

#dangereux
.doublepimp.com

#yahoo
.pipes.yahoo.com
.yimg.com

#twitter
.backtype.com
```

Bon alors c'est un peu brouillon, j'ai peut être bloqué des choses à ne pas bloquer, vous en faites ce que vous voulez hein  ! A noter, que facebook étant présent à l'état de plugin sur beaucoup de pages (dont la mienne huh ), je voulais d'abord dans un premier temps tout bloquer, et au final, j'ai adopté une meilleur stratégie... J'ai tout autorisé, et j'ai juste filtré les domaines facebook sur les pages autres que facebook... (voir plus loin).

A noter également, que je n'utilise aucune fonctionnalité de google excepté la recherche, si ce n'est pas votre cas il est possible que vous ayez quelques ennuis...
 (commentez les lignes de google). Notez aussi que recaptcha a été racheté par google, c'est la raison pour laquel c'est bloqué. Je pense que je rebasculerai surement ce filtrage sur squid plus tard en le faisant passer par tor.. Mais vous étonnez pas si vous les voyez plus
 !

Bon voila, j'ai tendance à bloquer tout ce qui passe et qui est suspect
 !

Les filtres prédéfinis

Alors là c'est vraiment selon chacun, privoxy a mis en place des filtres que vous pouvez implémenter ou pas (ou déplémenter parfois).

Voici la liste: http://www.privoxy.org/user-manual/filter-file.html#PREDEFINED-FILTERS

En plus des filtres prédéfinis, vous avez diverses autres options comme changer votre entête navigateur.

Voici ce que j'ai mis:

```
#Là j'ai un peu pompé sur artisan karma ^^
{ +hide-user-agent{Mozilla/5.0 (TV; U; Oric Atmos 6502c; en-
US; rv:r91.6) Gecko/19870508 TranDOS Firefox/4.1} }
/

{ +hide-referrer{forge} }
/

#Marche moyen, je préfère utiliser redirect remover, le plugin firefox
#{ +fast-redirects{check-decoded-url} }
#/

{ +filter{js-annoyances} }
/

{ +filter{navigatorversion} }
/

{ +filter{webbugs}}
/

{ +filter{jumping-windows} }
/

{ +filter{frameset-borders} }
/
```

```
{ +filter{quicktime-kioskmode} }
/

{ +client-header-filter{hide-tor-exit-notation} }
/
```

VOS filtres

N.B.: Vous pouvez également consulter la documentation officielle sur ce sujet:
http://www.privoxy.org/user-manual/filter-file.html#AEN4814

Et là est toute la puissance de privoxy... C'est sa capacité à modifier le contenu des pages à la volée !!!!

Vous vous rappelez je vous avez demandé de rajouter une ligne user.filter dans le fichier de configuration ? Comment ça non ?


Bon je vous le dit
 , donc, vous avez dit à privoxy que vous vouliez faire vos propres filtres comme un grand (ou une grande hein)!! (ou rajouter les miens
).

Bon alors, les filtres de privoxy, sont assez casse tête en fait.
Au vu de la précédente section vous avez compris que pour dire que vous utilisiez un filtre, il fallait le rajouter en plus dans le fichier user.action

{ +filter{le_nom_de_mon_filtre} }

Donc ouvrez le fichier user.filter, pour commencer.

Pour déclarer un nouveau filtre, c'est simple vous renseignez:

FILTER:

Ensuite vous indiquez les remplacement que vous voulez effectuer. Privoxy utilise les expresssions régulières. Une règle se compose de 4 parties, séparées par un séparateur (nous prendrons @ par soucis de simplcité)

[partie1]@[partie2]@[partie3]@[partie4]

1. La partie 1 est souvent juste un s (surement pour string)
2. La partie 2 comprend l'expression régulière que vous recherchez
3. La partie 3 comprend ce que vous voulez mettre à la place
4. La partie 4 comprend des options de remplacement
    1. **x**: Pas sûr d'avoir bien compris, alors je vous laisse la version anglaise (rigolez pas hein )

in this job turns on extended syntax, and allows for e.g. the liberal use of (non-interpreted!) whitespace for nicer formatting.

2. **g**: Global, grosso modo, fera le remplacement plusieurs fois si nécessaire.
3. **s**: Permet de faire la recherche sur plusieurs lignes.
4. **U**: Aucune idée, mais ça sert !

Pour ma part, ce que je fais, je crée un fichier, avec ce les occurances que je veux remplacer, et je vérifie si ça fonctionne comme je le veux. Je suis pas un spécialiste des expressions régulières (voir wikipedia http://fr.wikipedia.org/wiki/Expression_rationnelle), mais voila quelques filtres que j'ai fait qui pourraient vous interesser potentiellement.

Donc le fameux facebook (filtre désactivé pour les domaines facebook):

x

```
FILTER:facebook_all
s@facebook\.com@facebook.com.void@g

FILTER:facebook_all2
s@fbcdn\.net@bdcdn.net.void@g
```

SImple, remplace facebook.com par facebook.com.void... Les liens pointent alors vers le domaine void ! Que j'ai d'ailleurs bloqué
😎 !

Un script dans un document.write ??

Grosso modo, c'est du javascript qui écris une autre balise javascript... Ça peut arriver dans des scripts tout à fait normaux, mais j'ai été embêté par un script qui s'amusait à écrire et écrire comme ça n'importe comment jusqu'à ce que la page prenne 1 Go en mémoire... Pour moi ça se fait pas, et ce filtre ne m'empêche pas de nagiguer alors ça va !

```
FILTER:scriptindocwrite
s@(.*)\)(.*)(.*)@

Bad iframe here (check7) =>$2
```

```
$6
@ig


FILTER:iframes6
s@Heuuu
acl shoutcast rep_header X-HTTP09-First-Line ^ICY.[0-9]
upgrade_http0.9 deny shoutcast

# Apache to signal ETag correctly on such responses=>Heeuuu
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache

# You can add up to 20 additional "extension" methods here.
extension_methods REPORT MERGE MKACTIVITY CHECKOUT

###Les repertoires
hosts_file /etc/hosts
coredump_dir /var/spool/squid
##le nom du proxy...
visible_hostname not_your_business
#Ici vous spécifier l'emplacement où sera enregistré le cache... (moi
j'ai tout groupir)
#cache_dir ufs /home/[user]/squid/cache 1000 16 256

#La mémoire, demandez moi pas la différence
memory_pools_limit 256 MB

### Cache
#On interdit de mettre en cache les extentions sans caches définis dan
s les ACL plus haut
cache deny  extention_no_cache
### MULTIPLE CACHE
#Et oui, vous avez vu squid redirige soit vers privoxy un soit vers pr
ivoxy2. Il a donc deux caches différents.
#On indique qu'il a quelqu'un derrière, il doit pas renvoyer directeme
nt le paquet sur le net
prefer_direct off

never_direct deny SSL_ports
#never_direct allow all

#Bon, on dit donc qu'il a deux parents (qu'il fait suivre en fait). pr
ivoxy1 et 2. On indique leurs ports (8118 et 8119)
cache_peer 192.168.2.1 parent 8118 0 no-query name=privoxy1
cache_peer 192.168.2.1 parent 8119 0 no-query name=privoxy2

#Ensuite on filtre avec pour chaque règle, on indique deny et allow po
ur chaque privoxy
#Domain tor, var vers privoxy2 (tor)
cache_peer_access privoxy1 deny domain_tor
cache_peer_access privoxy2 allow domain_tor
```

```
#Les POST sont interdits à tor (confidentialité)
cache_peer_access privoxy2 deny method_post
cache_peer_access privoxy1 allow method_post

#Les extentions définies
cache_peer_access privoxy2 deny files_NO_tor
cache_peer_access privoxy1 allow files_NO_tor

cache_peer_access privoxy1 deny files_to_tor
cache_peer_access privoxy2 allow files_to_tor

#Enfin par défaut on utilise privoxy1
cache_peer_access privoxy1 allow Safe_ports
```

Voila, ce fichier, devrait contenir tout ce dont vous avez besoin...

Pensez à définir les emplacement pour les logs et l'endroit où seront mis en cache les fichiers (cache_dir). Changez surtout pas l'ordre (squid aime pas ça du tout du tout).

Si vous avez un doute sur un item, reportez vous ici http://www.squid-cache.org/Doc/config/, et pour la mise en hiérarchie c'est ici http://wiki.squid-cache.org/Features/CacheHierarchy.

Concernant la redirection

Justement puisqu'on en parle, donc, vous voyez à la fin du fichier de configuration, les règles qui seront utilisés pour savoir si on passe par tor ou pas, l'ordre est très important. Vous voyez que pour ma part, j'ai défini

- en priorité les domaines
- puis si pas dans les domaines si c'est un post (si vous postez des données dont les mots de passe)=> pas de tor,
- puis on regarde les extentions (on filtre selon le type de donnée)
- et enfin on passe par le privoxy1... (par défaut, pas de tor)

Vous aurez bien sûr noté que pour ma part, google, yahoo et facebook sont passées tout les trois à la sauce Tor (et pour cause, ce sont ceux qui nous pistent le plus).

Vous pouvez rajouter vos propres règles, notamment ce qui n'est pas utilisé ici, les expressions régulières ! (oubliez pas on défini les ACL au début, et on indique leur traitement à la fin).

Noubliez pas non plus de supprimer ou modifier mes règles selon vos besoins... Si vous utilisez google professionellement parlant, vaut peut être mieux l'enlever de la liste par exemple (oubliez pas, que tor est un danger, autant qu'un précieux outil)

Exemple d'utilisation des ACL dans squid

si vous voulez appliquer une action spécifique aux url contenant le mot clé chat ou forum, vous définirez l'acl ainsi:

```
acl forum url_regex chat forum
```

Selon les besoins vous pouvez utiliser l'acl pour

Interdire

```
#a placer avec les autres, et avant les allow !
http_access deny forum
```

Interdire la mise en cache

```
cache deny forum
```

Rediriger vers Tor (privoxy2)

```
cache_peer_access privoxy1 deny forum
cache_peer_access privoxy2 allow forum
```

Enfin... Automatiser tout ça !

Et oui, c'est un proxy, alors automatiser un minimum le lancement de tout ça, c'est pas de trop... de plus

nous avons pas parlé de IPTABLES pour cette raison, car cela va être scripté !

Script de lancement du proxy

Donc, créez un dossier sur votre poste utilisateur de contrôle que vous nommerez pack, ou pack_server.

dedans, vous allez créer ces fichiers:

- launch_privoxy_tor_squid
- stop_server
- clear_log
- globa_iptables
- globa_proxy_start

C'est quoi ?


Ce sont les différents éléments qui composeront votre script de lancement de proxy ! J'ai préféré séparer les éléments pour permettre de bien séparer chaque élément.

Pour le fichier launch_privoxy_tor_squid

```
#! /bin/sh
PATH2="/home/[user]/packstart/"
filter="iptables -t filter"
nat="iptables -t nat"

#stop server
$PATH2"stop_server"
#clear log
$PATH2"clear_log"
#iptables
$PATH2"globa_iptables"

#Redirect 80 vers squid
sudo $nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-
port 3128

#start
$PATH2"globa_proxy_start"
echo *****START TOR
sudo /etc/init.d/tor start
echo *****START PRIVOXY2
sudo /etc/init.d/privoxy2 start
echo *****START PRIVOXY
sudo /etc/init.d/privoxy start
echo *****START SQUID
sudo service squid start
```

```
####ON AFFICHE L ETAT

sudo $nat -L
sudo $filter -L
echo "********************"
sudo service squid status
sudo /etc/init.d/privoxy status
sudo /etc/init.d/privoxy2 status
tail -f /[path]/squid_access.log
```

(pensez bien à remplacer les répertoires par vos valeurs !)

Fichier stop_server

```
#! /bin/sh
PATH=/sbin:/usr/sbin:/bin:/usr/bin
sudo service squid stop
sudo /etc/init.d/privoxy stop
sudo /etc/init.d/privoxy2 stop
sudo /etc/init.d/tor stop
#sudo /etc/init.d/apache2 stop
sudo /etc/init.d/ntop stop
sudo /etc/init.d/networking stop
```

Ce script arrête tout les services, ainsi que l'interface réseau... On arrête tout ou pas hein !


Fichier clear_log

```
#! /bin/sh
PATH=/sbin:/usr/sbin:/bin:/usr/bin
```

```
sudo rm -f "/[path]/privoxy/logfile"
sudo rm -f "/[path]/privoxy/logfile2"
#tor
sudo rm -f "/[path]/tor/notices.log"
sudo rm -f "/[path]/tor/debug.log"
#squid log
sudo rm -f "/[path]/squid_access.log"
echo "EFFACEMENT DU CACHE SQUID"
#Ma méthode consiste à effacer tout le cache, puis à recréer en 777, c
'est pas une bonne chose, mais ça m'a gonflé les droits pour le coup
sudo rm -f -r -v "/[path]/squid"
sudo mkdir "/[path]/squid"
sudo chmod 555 "/[path]/squid"
sudo touch "/[path]/squid/squid_access.log"
sudo touch "/[path]/squid/store.log"
sudo touch "/[path]/squid/cache.log"
sudo chmod -R 777 "/[path]/squid"
#on recrée la structure du cache
sudo squid -z
```

Je suis moyennement contant de ma méthode de suppression du cache... Pour le moment ça marche comme ça...

Fichier globa_iptables

```
#! /bin/sh
PATH=/sbin:/usr/sbin:/bin:/usr/bin
echo ON REINITIALISE IPTABLES
filter="iptables -t filter"
nat="iptables -t nat"

sudo iptables -F
sudo $nat -F
sudo $filter -F
/sbin/iptables -X

#passerelle: chez moi l'interface 0 (eth0) correspond au côté internet
sudo iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQU
ERADE

####FILTRES

#On drop les scans XMAS et NULL. (lignes trouvées sur la doc ubuntu)
```

```
sudo iptables -A INPUT -p tcp --tcp-
flags FIN,URG,PSH FIN,URG,PSH -j DROP

sudo iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP

sudo iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
sudo iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

#PORTS INUTILISES
sudo iptables -A INPUT -p tcp  --dport 5 -j  DROP #ALL
sudo iptables -A INPUT -p tcp  --dport 7 -j  DROP #ALL
sudo iptables -A INPUT -p tcp  --dport 23 -j  DROP #ALL
# Permettre à une connexion ouverte de recevoir du trafic en entrée.

sudo iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT

# Permettre à une connexion ouverte de recevoir du trafic en sortie.

sudo iptables -A OUTPUT -m state ! --state INVALID -j ACCEPT

# On accepte la boucle locale en entrée.

sudo iptables -I INPUT -i lo -j ACCEPT

# On accepte tout le trafic entrant.=>Pour faire simple ici
sudo iptables -P INPUT ACCEPT

# On accepte tout le trafic sortant.=>Pour faire simple ici

sudo iptables -P OUTPUT ACCEPT

# On accepte le forward.=>Pour faire simple ici

sudo iptables -P FORWARD ACCEPT

#interfaces admin
#ntop
sudo iptables -A INPUT -p tcp -i eth0 --dport 3000 -j DROP  #internet
sudo iptables -A INPUT -p tcp -i eth1 --dport 3000 -j ACCEPT

#privoxy
sudo iptables -A INPUT -p tcp -i eth0 --dport 8118 -j DROP #internet
sudo iptables -A INPUT -p tcp -i eth1 --dport 8118 -j ACCEPT

#privoxy2
sudo iptables -A INPUT -p tcp -i eth0 --dport 8119 -j DROP #internet
sudo iptables -A INPUT -p tcp -i eth1 --dport 8119 -j ACCEPT

#squid
sudo iptables -A INPUT -p tcp -i eth0 --dport 3128 -j DROP #internet
sudo iptables -A INPUT -p tcp -i eth1 --dport 3128 -j ACCEPT
```

```
####SSH
sudo iptables -A INPUT -p tcp -i eth0 --dport 22 -j DROP #internet
sudo iptables -A INPUT -p tcp -i eth1 --dport 22 -j ACCEPT

####FTP
sudo iptables -A INPUT -p tcp -i eth0 --dport 21 -j DROP #internet

###TOR
#tor ORport =>what port to advertise for incoming Tor connections.
sudo iptables -A INPUT -p tcp -i eth1 --dport 9001 -j DROP
sudo iptables -A INPUT -p tcp -i eth0 --dport 9001 -j ACCEPT #internet

#tor=>  open for local application connections
sudo iptables -A INPUT --dport 9050 DROP
sudo iptables -A INPUT -s 127.0.0.1 --dport 9050 ACCEPT

#tor mirror directory information for others. =>DirPort 9030
sudo iptables -A INPUT -p tcp -i eth1 --dport 9030 -j DROP
sudo iptables -A INPUT -p tcp -i eth0 --dport 9030 -j ACCEPT #internet
```

Si vous connaissez bien iptables, je vous laisse faire votre sauce, ma configuration n'offre qu'une protection minimale !


Fichier globa_proxy_start

```
#! /bin/sh
PATH=/sbin:/usr/sbin:/bin:/usr/bin
echo ON RELANCE LE PROXY
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
sudo /etc/init.d/networking start
sudo /etc/init.d/ntop start
```

Vous remarquerez qu'il y a peu de lignes... En fait c'est voulu, ça vous permettra de pouvoir créer un fichier pour ne lancer que privoxy par exemple ou que squid, etc...
 =>Le lancement de ces "particularités" se fait dans le fichier principal

Pensez à bien préciser que ces fichiers sont des executables (chmod +x).

Réfléchissez bien à ce que vous voulez faire de vos logs, mon script de démarage n'est pas forcément une référence, libre à vous de le modifier ou de faire le votre, voir à interdir les logs...

Problèmes

Dans les problèmes que vous pourriez rencontrer en voici quelques uns (surtout lors de l'ajout d'un nouvel ordi sous votre réseau):

Problème d'ip ?

Comme notre serveur n'a pas installé de DHCP, il faudra configurer chaque ordinateur pour lui indiquer son ip et sa passerelles.

(Voir début de l'article les paramètres à faire dans /etc/network/interfaces)

Problème de Noms de domaines ?

Comme le serveur ne gère pas le DNS, il se peut que vous ayez un soucis de ce côté (Constaté après coup). Pour vos ordinateurs clients sous ubuntu, il faudra que vous configuriez le fichier /etc/resolv.conf pour lui indiquer d'utiliser votre box comme serveur DNS. (Même si elle n'est pas dans le même réseau ça fonctionne chez moi).

```
# Generated by NetworkManager
nameserver 192.168.1.1
```

Sous windows, vous devez pouvoir spécifier l'adresse du serveur DNS dans les propriétés de connexion, sinon vous pouvez éventuellement indiquer au navigateur web que vous utilisez un proxy (au port 80), ça fonctionne.

Je pense que je modifierai le tutoriel dans un second temps pour rajouter le DHCP et le serveur DNS.

C'est fini !

Déjà ?


Mais si c'est possible que ça marche tout ce fatra, chez moi ça marche
 !

Bon j'espère que ça vous aura aidé un peu !

A noter que tout ce document est sous license LGPL, ne le copiez pas sur votre page en prétendant que c'est vous qui l'avez fait, sinon je mords
 ! J'ai passé au moins 6 heures à tout rédiger et une semaine à mettre en place le serveur chez moi en faisant des recherches, pour trouver les informations que je vous retransmet!