Proxy

Olivier Hoarau (olivier.hoarau@funix.org)

V2.0 du 26 juillet 2006

1 Historique du document

V2.0 26.07.06 Adaptation pour installation de squid et squidguard sous ubuntu

V1.9 8.08.05 correction pour squidguard, passage à wwwoffle 2.8e

V1.8 28.01.05 rajout d'un petit script pour mettre à jour régulièrement la liste entretenue par l'université de Toulouse des sites tordus pour squidGuard

V1.7 28.11.04 Modification dans l'installation de SquidGuard, passage à wwwoffle 2.8d

V1.6 31.05.04 Modification/correction pour squid/squidGuard suite passage à Mandrake 10.0 official

V1.5 09.05.04 Présentation de squidguard pour filtrer les surfs, passage à wwwoffle 2.8b

V1.4 04.05.03 Passage Mandrake 9.1 changement de version de squid, passage à wwwoffle 2.7h

V1.3 24.12.02 Passage à Mandrake 9.0 (changement de version de squid), passage à wwwoffle 2.7g

V1.2 13.10.02 Passage à wwwoffle 2.7f

V1.1 09.06.02 Passage à la Mandrake 8.2, changement de version pour le package Squid et passage à la version 2.7b pour wwwoffle

V1.0 16.12.00 Création du document.

2 Préambule

Ce document présente les proxy squid couplé à SquidGuard et wwwoffle sous linux.
La dernière version de ce document est téléchargeable à l'URL http://www.funix.org. Ce document peut être reproduit et distribué librement dès lors qu'il n'est pas modifié et qu'il soit toujours fait mention de son origine et de son auteur, si vous avez l'intention de le modifier ou d'y apporter des rajouts, contactez l'auteur pour en faire profiter tout le monde.

Ce document ne peut pas être utilisé dans un but commercial sans le consentement de son auteur. Ce document vous est fourni "dans l'état" sans aucune garantie de toute sorte, l'auteur ne saurait être tenu responsable des quelconques misères qui pourraient vous arriver lors des manipulations décrites dans ce document.

3 Présentation

Un proxy (serveur mandataire en français) est un outil logiciel permettant de sauvegarder les pages les plus fréquemment visitées ou les dernières visitées pour qu'elles s'affichent plus rapidement. **SQUID** est le proxy le plus communément utilisé par les professionnels, il est plutôt destiné pour une connexion permanente avec beaucoup de machines, il a de plus besoin d'un serveur DNS pour fonctionner (ça peut être celui du FAI), si vous passez en mode off-line, vous ne pouvez plus accéder aux pages les plus fréquemment visitées ou aux dernières visitées même si elles ont été sauvegardées, de même vous ne pourrez accéder aux pages que vous mettez en ligne sur votre serveur Apache en intranet, en fait il peut être intéressant pour les utilisateurs d'ADSL.
SquidGuard couplé à Squid permet de rajouter un contrôle pour le surf à partir de listes prédéfinies, c'est particulièrement intéressant quand vous ne voulez pas que vos utilisateurs surfent n'importe où.

WWWOFFLE au contraire vous permet d'accéder en mode off-line à ces pages, il est plus destiné à un usage de type poste isolé (ou petit réseau isolé) avec une connexion intermittente.

4 Squid

4.1 Installation

ATTENTION squid a besoin d'un serveur DNS pour fonctionner, cela peut être le serveur DNS du FAI ou un serveur DNS local

Squid est disponible avec la Mandriva, package **squid-2.X-STABLE** qui requiert l'installation de **perl-Authen-Smb** (sous ubuntu package **squid**).

4.2 Configuration

Le fichier de configuration se trouve sous **/etc/squid** et a pour nom **squid.conf**, le fichier est très long, rassurez vous il n'y a que deux, trois trucs à rajouter ou à modifier pour que ça fonctionne.

Vous pouvez modifier la taille du répertoire de cache de **squid** en jouant sur le premier paramètre numérique de la variable **cache_dir**, ici il est limité à 40Mo.

cache_dir ufs /var/spool/squid 40 16 256

Par défaut les erreurs de **squid** sont mailés à l'utilisateur webmaster qu'il existe ou pas sur votre système, pour mettre un autre utilisateur, modifier la variable **cache_mgr**, pour ma part j'ai choisi l'utilisateur root comme destinataire.

cache_mgr root

Par défaut **squid** va chercher le nom du serveur DNS dans le fichier **/etc/resolv.conf** vous pouvez éventuellement définir des adresses IP de serveurs DNS avec la variable **dns_nameservers** comme ceci :

dns_nameservers 10.0.0.1 192.172.0.2

Dans le cas où il n'y a pas de d'adresse de serveur DNS dans votre fichier **resolv.conf** (cas d'attribution dynamique), je vous conseille de rajouter cette ligne **dns_nameservers** avec les adresses IP de votre fournisseur d'accès systématiquement sans quoi **squid** ne se lancera pas au démarrage (pour connaitre les adresses IP, il suffit de se connecter et d'éditer le fichier **/etc/resolv.conf**). Si vous avez un serveur DNS local, vous n'avez pas à activer cette ligne, dès lors que vous avez un fichier **resolv.conf** contenant au moins la ligne

nameserver 127.0.0.1

Pour éviter les longs time out du à la résolution d'adresse, modifiez la variable suivante

dns_timeout 2 minutes

Si vous voulez indiquer des secondes, mettre **seconds**

Maintenant on va définir les autorisations d'accès (**ACL Access Controls List**), on va définir le réseau qui a le droit d'accéder à votre système, ici c'est le réseau privé d'adresse 192.168.13.0.

acl allowed_hosts src 192.168.13.0/255.255.255.0

On définit maintenant les autorisations d'accés HTTP, on autorise uniquement les **allowed_hosts** qu'on a défini précédemment.

http_access allow allowed_hosts

Voilà ce que ça donne au final pour les autorisations d'accés :

#Recommended minimum configuration:
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 allowed_hosts src 192.168.13.0/255.255.255.0
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

(...)

#Recommended minimum configuration:
#
 # Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
 # Deny requests to unknown ports
http_access deny !Safe_ports
 # Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports

 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

 # And finally deny all other access to this proxy

http_access allow localhost
http_access allow allowed_hosts
http_reply_access allow all

Pour lancer **squid,** il suffit maintenant de taper **/etc/rc.d/init.d/squid start**

Si vous avez modifié **/etc/squid/squid.conf**, vous pouvez faire prendre en compte les modifs, en tapant:

sous mandriva

/etc/rc.d/init.d/squid restart

sous ubuntu

/etc/init.d/squid restart

Maintenant vous pouvez configurer vos postes clients, en configurant le browser pour qu'il se serve d'un proxy avec pour nom le nom de votre poste Linux (défini dans **c:/windows/hosts** pour Win9X) et pour port 3128 (port par défaut). Connectez vous sur le net, et normalement ça devrait marcher.

ATTENTION Squid a nécessairement besoin d'un serveur DNS pour pouvoir marcher, cela peut-être un serveur DNS local pour pouvoir accéder à votre site web intranet ou le(s) serveur(s) DNS du FAI.

Les clients peuvent maintenant être configurés pour utiliser votre serveur comme proxy (port par défaut 3128).

5 Installation de squidguard

5.1 Installation

Sur une Mandriva et (k)ubuntu le package se nomme **squidGuard**.

5.2 Configuration pour une Mandriva

A l'installation on a les messages suivants

Préparation... **##**
1:squidGuard **##**
warning: user apache does not exist - using root
warning: group apache does not exist - using root
warning: user apache does not exist - using root
warning: group apache does not exist - using root
#
WARNING !!! WARNING !!! WARNING !!! WARNING !!!

Modify the following line in the /etc/squid/squid.conf

redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

Maintenant sous **/etc/squid** on tape

cp squidGuard.conf.sample squidGuard.conf

C'est le fichier **/etc/squid/squidGuard.conf** qu'on modifiera un peu plus loin. Maintenant vous pouvez utiliser la liste noire des sites classées par catégorie (porno, violence, ...) fournie par le package **squidGuard** qui se trouve sous **/usr/share/squidGuard-1.2.0/db** ou récupérer des listes noires sur le net.

Dans le cas où on utilise une liste trouvée sur le net (il n'y a rien à faire si vous utilisez la liste fournie par la Mandriva). Cette URL http://www.squidguard.org/blacklist/ offre un certain nombre de listes. J'ai choisi celle entretenue par l'université de Toulouse. Pour voir comment mettre à jour régulièrement cette liste, voir plus bas dans le document. L'URL est la suivante http://cri.univ-tlse1.fr/documentations/cache/squidguard_en.html#contrib on y récupère un fichier **blacklists.tar.gz**.

Vous pouvez éventuellement préalablement sauvegarder les listes d'origine comme ceci

cp -Rf /usr/share/squidGuard-1.2.0/db/ /usr/share/squidGuard-1.2.0/mdk

on décompresse l'archive dans le répertoire **db** préalablement créé

tar xvfz blacklists.tar.gz --directory /usr/share/squidGuard-1.2.0/db
sudo tar xvfz blacklists.tar.gz --directory /var/lib/squidguard/db

On supprime quelques doublons originaux

cd /usr/share/squidGuard-1.2.0/db/
rm -Rf ads adult aggressive audio-video drugs forums gambling hacking mail porn proxy publicite redirector violence warez
cd /usr/share/squidGuard-1.2.0/db/blacklists
mv * ..
rmdir /usr/share/squidGuard-1.2.0/db/blacklists

En tant que root on met à jour la base en tapant

squidGuard -c /etc/squid/squidGuard.conf -C all -d /usr/share/squidGuard-1.2.0/db

Cela donne

2005-08-02 11:35:03 [3995] init iplist /usr/share/squidGuard-1.2.0/db/privilegedsource/ips
2005-08-02 11:35:03 [3995] sourceblock privilegedsource missing active content, set inactive
2005-08-02 11:35:03 [3995] init iplist /usr/share/squidGuard-1.2.0/db/bannedsource/ips
2005-08-02 11:35:03 [3995] sourceblock bannedsource missing active content, set inactive

2005-08-02 11:35:03 [3995] init iplist /usr/share/squidGuard-1.2.0/db/lansource/lan
2005-08-02 11:35:03 [3995] sourceblock lansource missing active content, set inactive
2005-08-02 11:35:03 [3995] init domainlist /usr/share/squidGuard-1.2.0/db/porn/domains
2005-08-02 11:35:25 [3995] create new dbfile /usr/share/squidGuard-1.2.0/db/porn/domains.db
2005-08-02 11:35:25 [3995] init urllist /usr/share/squidGuard-1.2.0/db/porn/urls
2005-08-02 11:35:25 [3995] create new dbfile /usr/share/squidGuard-1.2.0/db/porn/urls.db
2005-08-02 11:35:25 [3995] init expressionlist /usr/share/squidGuard-1.2.0/db/porn/expressions
2005-08-02 11:35:25 [3995] init domainlist /usr/share/squidGuard-1.2.0/db/adult/domains
(...)
2005-08-02 11:35:48 [3995] create new dbfile /usr/share/squidGuard-1.2.0/db/publicite/domains.db
2005-08-02 11:35:48 [3995] init urllist /usr/share/squidGuard-1.2.0/db/publicite/urls
2005-08-02 11:35:48 [3995] create new dbfile /usr/share/squidGuard-1.2.0/db/publicite/urls.db
2005-08-02 11:35:48 [3995] init expressionlist /usr/share/squidGuard-1.2.0/db/publicite/expressions
2005-08-02 11:35:48 [3995] init domainlist /usr/share/squidGuard-1.2.0/db/violence/domains
2005-08-02 11:35:48 [3995] create new dbfile /usr/share/squidGuard-1.2.0/db/violence/domains.db
2005-08-02 11:35:48 [3995] init urllist /usr/share/squidGuard-1.2.0/db/violence/urls
2005-08-02 11:35:48 [3995] create new dbfile /usr/share/squidGuard-1.2.0/db/violence/urls.db
2005-08-02 11:35:48 [3995] init expressionlist /usr/share/squidGuard-1.2.0/db/violence/expressions
2005-08-02 11:35:48 [3995] init domainlist /usr/share/squidGuard-1.2.0/db/banneddestination/domains
2005-08-02 11:35:48 [3995] domainlist empty, removed from memory
2005-08-02 11:35:48 [3995] init urllist /usr/share/squidGuard-1.2.0/db/banneddestination/urls
2005-08-02 11:35:48 [3995] urllist empty, removed from memory
2005-08-02 11:35:48 [3995] init expressionlist /usr/share/squidGuard-1.2.0/db/banneddestination/expressions
2005-08-02 11:35:48 [3995] init domainlist /usr/share/squidGuard-1.2.0/db/advertising/domains
2005-08-02 11:35:48 [3995] domainlist empty, removed from memory
2005-08-02 11:35:48 [3995] init urllist /usr/share/squidGuard-1.2.0/db/advertising/urls
2005-08-02 11:35:48 [3995] urllist empty, removed from memory
2005-08-02 11:35:48 [3995] squidGuard 1.2.0 started (1122975303.182)
2005-08-02 11:35:48 [3995] db update done
2005-08-02 11:35:48 [3995] squidGuard stopped (1122975348.995)

Maintenant sous **/usr/share/squidGuard-1.2.0/** on tape

chown -R squid:squid db

5.3 Configuration pour une ubuntu

La base de données des URLs craignos se trouve sous /var/lib/squidguard/db qui est totalement vide, il faut en récupérer une sur le net. On peut en trouver un certain nombre par ici Cette URL http://www.squidguard.org/blacklist/. J'ai choisi celle entretenue par l'université de Toulouse. Pour voir comment mettre à jour régulièrement cette liste, voir plus bas dans ce document. L'URL est la suivante http://cri.univ-tlse1.fr/documentations/cache/squidguard_en.html#contrib on y récupère un fichier **blacklists.tar.gz**.

on décompresse l'archive dans le répertoire db préalablement créé

sudo tar xvfz blacklists.tar.gz --directory /var/lib/squidguard/db

On place les répertoires au bon endroit

cd /var/lib/squidguard/db/blacklists
mv * ..
rmdir /var/lib/squidguard/db/blacklists

on met à jour la base en tapant

sudo squidGuard -c /etc/squid/squidGuard.conf -C all -d /var/lib/squidguard/db/

Cela donne

2006-07-24 18:43:34 [9859] sourceblock bannedsource missing active content, set inactive
2006-07-24 18:43:34 [9859] init domainlist /var/lib/squidguard/db/adult/domains
2006-07-24 18:44:04 [9859] create new dbfile /var/lib/squidguard/db/adult/domains.db
2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/adult/urls
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/adult/urls.db
2006-07-24 18:44:05 [9859] init expressionlist /var/lib/squidguard/db/adult/expressions
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/sexual_education/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/sexual_education/domains.db
2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/sexual_education/urls
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/sexual_education/urls.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/mixed_adult/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/mixed_adult/domains.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/mobile-phone/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/mobile-phone/domains.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/phishing/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/phishing/domains.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/dangerous_material/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/dangerous_material/domains.db
2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/dangerous_material/urls
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/dangerous_material/urls.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/audio-video/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/audio-video/domains.db
2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/audio-video/urls
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/audio-video/urls.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/cleaning/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/cleaning/domains.db
2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/cleaning/urls
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/cleaning/urls.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/forums/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/forums/domains.db
2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/forums/urls
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/forums/urls.db
2006-07-24 18:44:05 [9859] init expressionlist /var/lib/squidguard/db/forums/expressions
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/hacking/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/hacking/domains.db
2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/hacking/urls
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/hacking/urls.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/redirector/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/redirector/domains.db

2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/redirector/urls
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/redirector/urls.db
2006-07-24 18:44:05 [9859] init expressionlist /var/lib/squidguard/db/redirector/expressions
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/reaffected/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/reaffected/domains.db
2006-07-24 18:44:05 [9859] init domainlist /var/lib/squidguard/db/warez/domains
2006-07-24 18:44:05 [9859] create new dbfile /var/lib/squidguard/db/warez/domains.db
2006-07-24 18:44:05 [9859] init urllist /var/lib/squidguard/db/warez/urls
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/warez/urls.db
2006-07-24 18:44:06 [9859] init expressionlist /var/lib/squidguard/db/warez/expressions
2006-07-24 18:44:06 [9859] init domainlist /var/lib/squidguard/db/tricheur/domains
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/tricheur/domains.db
2006-07-24 18:44:06 [9859] init urllist /var/lib/squidguard/db/tricheur/urls
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/tricheur/urls.db
2006-07-24 18:44:06 [9859] init domainlist /var/lib/squidguard/db/agressif/domains
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/agressif/domains.db
2006-07-24 18:44:06 [9859] init urllist /var/lib/squidguard/db/agressif/urls
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/agressif/urls.db
2006-07-24 18:44:06 [9859] init expressionlist /var/lib/squidguard/db/agressif/expressions
2006-07-24 18:44:06 [9859] init domainlist /var/lib/squidguard/db/drogue/domains
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/drogue/domains.db
2006-07-24 18:44:06 [9859] init urllist /var/lib/squidguard/db/drogue/urls
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/drogue/urls.db
2006-07-24 18:44:06 [9859] init domainlist /var/lib/squidguard/db/gambling/domains
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/gambling/domains.db
2006-07-24 18:44:06 [9859] init urllist /var/lib/squidguard/db/gambling/urls
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/gambling/urls.db
2006-07-24 18:44:06 [9859] init domainlist /var/lib/squidguard/db/games/domains
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/games/domains.db
2006-07-24 18:44:06 [9859] init urllist /var/lib/squidguard/db/games/urls
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/games/urls.db
2006-07-24 18:44:06 [9859] init domainlist /var/lib/squidguard/db/publicite/domains
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/publicite/domains.db
2006-07-24 18:44:06 [9859] init urllist /var/lib/squidguard/db/publicite/urls
2006-07-24 18:44:06 [9859] create new dbfile /var/lib/squidguard/db/publicite/urls.db
2006-07-24 18:44:06 [9859] init expressionlist /var/lib/squidguard/db/publicite/expressions
2006-07-24 18:44:06 [9859] squidGuard 1.2.0 started (1153759414.809)
2006-07-24 18:44:06 [9859] db update done
2006-07-24 18:44:06 [9859] squidGuard stopped (1153759446.249)

Maintenant sous **/var/lib/squidguard/** on tape

chown -R proxy:proxy db

5.4 Suite de la configuration (pour Mandriva et ubuntu)

Voilà maintenant notre fichier de configuration **/etc/squid/squidGuard.conf**

```
#-----------------------------------------------------------------
#  SquidGuard CONFIGURATION FILE
#-----------------------------------------------------------------
```

```
# CONFIGURATION DIRECTORIES
dbhome /var/lib/squidguard/db
logdir /var/log/squidguard

# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

time workhours {
        weekly s 09:30-12:00 13:00-19:00
        weekly m 09:00-12:00 13:00-19:00
        weekly t 09:00-11:00 12:00-19:00
        weekly w 09:00-12:00 12:00-18:00
        weekly h 09:00-13:00 13:00-18:00
        weekly f 09:00-12:00 13:30-18:00
        weekly a 08:20-13:00 13:30-19:00
}

time heure-gamins {
        weekly smtwhfa 17:30 - 18:00
}
# SOURCE ADDRESSES:
src privilegedsource {
        #iplist privilegedsource/ips
        # liste des machines qui pourront se connecter avec tous les droits
         ip 192.168.1.11
}

src bannedsource {
        #iplist bannedsource/ips
}


src lansource {
        #iplist lansource/lan
        # liste des machines qui pourront se connecter avec droits limités
         ip 192.168.26.100 192.168.26.50 192.168.1.12
}

# DESTINATION CLASSES:
dest adult {
    domainlist adult/domains
    urllist adult/urls
    expressionlist  adult/expressions
    #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest sexual_education {
    domainlist sexual_education/domains
    urllist sexual_education/urls
    #redirect http://ohoarau.kervao.fr/interdit.htm
}
```

```
dest mixed_adult {
   domainlist mixed_adult/domains
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest mobile-phone {
   domainlist mobile-phone/domains
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest phishing {
   domainlist phishing/domains
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest dangerous_material {
   domainlist dangerous_material/domains
   urllist dangerous_material/urls
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest audio-video {
   domainlist audio-video/domains
   urllist audio-video/urls
   #redirect http://ohoarau.kervao.fr/interdit.htm
}


dest cleaning {
   domainlist cleaning/domains
   urllist cleaning/urls
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest forums {
   domainlist forums/domains
   urllist forums/urls
   expressionlist  forums/expressions
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest hacking {
   domainlist hacking/domains
   urllist hacking/urls
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest redirector {
   domainlist redirector/domains
   urllist redirector/urls
   expressionlist  redirector/expressions
```

```
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest reaffected {
   domainlist reaffected/domains
   #redirect http://ohoarau.kervao.fr/interdit.htm
}


dest warez {
   domainlist warez/domains
   urllist warez/urls
   expressionlist warez/expressions
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest tricheur {
   domainlist tricheur/domains
   urllist tricheur/urls
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest agressif {
   domainlist agressif/domains
   urllist agressif/urls
   expressionlist agressif/expressions
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest drogue {
   domainlist drogue/domains
   urllist drogue/urls
   #redirect http://ohoarau.kervao.fr/interdit.htm
}


dest gambling {
   domainlist gambling/domains
   urllist gambling/urls
   #redirect http://ohoarau.kervao.fr/interdit.htm
}

dest games {
   domainlist games/domains
   urllist games/urls
   #redirect http://ohoarau.kervao.fr/interdit.htm
}


dest publicite {
   domainlist publicite/domains
   urllist publicite/urls
   expressionlist  publicite/expressions
```

```
   #redirect http://ohoarau.kervao.fr/interdit.htm
}


# ACLs
acl {
      privilegedsource {
            # les machines privilégiés ont doit à tout sauf à la pub
            pass !publicite !phishing all
            redirect http://olivier.funix.org/images/temp/interdit.htm
      }

      bannedsource {
            pass none
            redirect http://olivier.funix.org/images/temp/interdit.htm
      }

      lansource {
            pass !adult !audio-video !agressif !cleaning !dangerous_material !drogue !forums !gambling !
games !hacking !mixed_adult !mobile-phone !publicite !reaffected !redi
rector !sexual_education !tricheur !warez all
            redirect http://olivier.funix.org/images/temp/interdit.htm
      }

      default {
            pass none
            redirect http://olivier.funix.org/images/temp/interdit.htm
      }
}
```

On modifie maintenant le fichier de configuration de **squid /etc/squid/squid.conf** pour faire appel à **squidGuard**

```
#  TAG: redirect_program
#       Specify the location of the executable for the URL redirector.
#       Since they can perform almost any function there isn't one included.
#       See the FAQ (section 15) for information on how to write one.
#       By default, a redirector is not used.
#
#Default:
# none
redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
```

On relance **squid**

sous mandriva

/etc/rc.d/init.d/squid restart

sous ubuntu

/etc/init.d/squid restart

C'est fini

Maintenant si vous voulez mettre en place une authentification basée sur vos utilisateurs, éditez le fichier **squid.conf** rajoutez les lignes

auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/users
auth_param basic children 5

Et au niveau des ACL

acl Users proxy_auth REQUIRED
http_access deny !Users

Créons le fichier **users**

touch /etc/squid/users

Puis pour chaque utilisateur

/usr/local/apache/bin/htpasswd -b /etc/squid/users olivier mot-de-passe-en-clair

Cela donne un fichier qui aura cette tête là

olivier:hSHTr8tdyLJh.
lena:LiIDffDc.jC4ow
...

A présent dans le fichier **squidGuard.conf** on pourra écrire

```
# SOURCE ADDRESSES:
src privilegedsource {
        #iplist privilegedsource/ips
        # liste des machines qui pourront se connecter avec tous les droits
        ip 192.168.13.100 192.168.13.50
        # utilisateurs privilégiés
        user olivier veronique
}

(...)

src lansource {
        #iplist lansource/lan
```

```
    # liste des machines qui pourront se connecter avec droits limités
    ip 192.168.13.100 192.168.13.50
    # utilisateurs droits restreints
    user benjamin julie
}
```

Relancez **squid**

sous mandriva

/etc/rc.d/init.d/squid restart

sous ubuntu

/etc/init.d/squid restart

A présent au lancement du navigateur une identification sera demandée.

Maintenant pour mettre à jour régulièrement la liste entretenue par l'université de Toulouse voilà un petit script à placer sous **/etc/cron.weekly** pour qu'il soit appelé toutes les semaines

script Mandriva

```
#!/bin/bash
# récupération du fichier blacklists.tar.gz
cd /tmp
ftp -n <<**
open ftp.univ-tlse1.fr
user anonymous toto@free.fr
binary
cd pub/unix/reseau/cache/squidguard_contrib
get blacklists.tar.gz
bye
**
# on met à jour le répertoire blacklist
tar zxvf /tmp/blacklists.tar.gz --directory /usr/share/squidGuard-1.2.0/db
cd /usr/share/squidGuard-1.2.0/db/blacklists
cp -Rf * ..
cd ..
rm -Rf /usr/share/squidGuard-1.2.0/db/blacklists
# on appelle squidGuard pour qu'il mette à jour la nouvelle liste
/usr/bin/squidGuard -c /etc/squid/squidGuard.conf -C all -d /usr/share/squidGuard-1.2.0/db
# changement du propriétaire
chown -R squid:squid /usr/share/squidGuard-1.2.0/db
# on relance squid
/etc/rc.d/init.d/squid restart
```

Le même adapté à une ubuntu

```
#!/bin/bash
```

```
# réupéation du fichier blacklist
cd /tmp
ftp -n <<**
open ftp.univ-tlse1.fr
user anonymous toto@free.fr
binary
cd pub/unix/reseau/cache/squidguard_contrib
get blacklists.tar.gz
bye
**

tar zxvf /tmp/blacklists.tar.gz --directory /var/lib/squidguard/db
cd /var/lib/squidguard/db/blacklists
cp -Rf * ..
cd ..
rm -Rf /var/lib/squidguard/db/blacklists
/usr/bin/squidGuard -c /etc/squid/squidGuard.conf -C all -d /var/lib/squidguard/db
chown -R proxy:proxy /var/lib/squidguard/db
/etc/init.d/squid restart
```

6 WWWOFFLE

6.1 Caractéristiques

Ces caractéristiques sont les suivantes:

En mode connecté :

- sauvegarde des pages pour une visualisation ultérieure
- sauvegarde de certaines pages qui ont été modifiées
- mise en place de contrôle d'accès sur certaines pages
- contrôle des pages qui ne doivent pas être sauvegardées

En mode non connecté :

- peut être configuré pour lancer une connexion pour les pages non sauvegardées
- sélection des pages à sauvegarder à la prochaine connexion
- contrôle des pages pouvant être visualisées en mode off-line

Pour info **wwwoffle** marche très bien aussi sous windows, pour plus d'info voir la page que je lui ai consacré sur www.funix.org.

6.2 Installation

On récupérera **wwwoffle** à l'**URL** www.gedanken.demon.co.uk/wwwoffle/ . L'archive se présente sous la forme d'un tarball **wwwoffle-2.8e.tgz** qu'on décompressera dans un répertoire de travail en tapant :

tar xvfz wwwoffle-2.8e.tgz

Cela va nous créer un répertoire **wwwoffle-2.8e**. Dans ce répertoire on tape

./configure --with-default-language=fr --with-confdir=/etc/wwwoffle

On indique ici qu'on veut utiliser le français comme langue par défaut, et que le fichier de conf se trouvera sous **/etc/wwoffle**

En tapant **./configure -help**, vous aurez les options nécessaires pour changer

-le port utilisé, par défaut c'est à **localhost:8080** (pour info **Squid** utilise le port 3128), il n'y a pas de raison de changer cela,
- le répertoire d'installation des exécutables **wwwoffle**, par défaut **/usr/local/bin** et **/usr/local/sbin,** à changer éventuellement,
- le répertoire où seront sauvegardées les pages, par défaut **/var/spool/wwwoffle** (attention à la taille de **/var**).

On tape maintenant :

make

NOTE Vous avez besoin du package **flex** pour compiler

Puis en tant que **root**

make install

ATTENTION: Si vous upgradez d'une ancienne version, il faudra taper dans le répertoire **wwwoffle-2.8e**

./conf/upgrade-config.pl /etc/wwwoffle/wwwoffle.conf

C'est pour upgrader le fichier de configuration existant, en fait chez moi ça n'a pas toujours marché au poil, il vaut mieux prendre le fichier de configuration exemple qu'on trouve sous **wwwoffle-2.8e/conf** et l'adapter à sa config.

6.3 Configuration basique

On va éditer le fichier **/etc/wwwoffle/wwwoffle.conf**. Pour modifier éventuellement le port d'**Apache** et de **wwwoffle**, vous avez la balise **StartUp**

```
StartUp
{
 bind-ipv4        = 0.0.0.0
#bind-ipv6        = ::

 http-port        = 8080
 wwwoffle-port    = 8081
```

Dans un premier temps on ne va pas modifier grand chose, si votre serveur s'appelle **obelix** et a pour adresse **192.168.13.11**, votre nom de domaine interne **breizland.bz** pour qu'il soit vu de votre réseau interne vous devez rajouter :

```
LocalHost
{
 localhost
 127.0.0.1
```

obelix.breizland.bz
192.168.13.11

::ffff:127.0.0.1

ip6-localhost
::1

Example
 # The server is on www.foo.com, with IP address 11.22.33.44.
 # www.foo.com
 # 11.22.33.44
}

Maintenant vous devez autoriser les machines de votre réseau local à accéder au proxy **wwwoffle** en rajoutant :

AllowedConnectHosts
{
***.breizland.bz**
Example
 # Only allow connections from hosts in the foo.com domain.
 # *.foo.com
}

Maintenant vous devez autoriser les machines de votre réseau local à accéder au proxy **wwwoffle** en rajoutant :

AllowedConnectHosts
{
***.breizland.bz**
Example
 # Only allow connections from hosts in the foo.com domain.
 # *.foo.com
}

Si vous avez des sites accessibles en intranet, vous pouvez spécifier qu'ils ne soient pas "cachées" (sauvegardées dans le cache). Si vos sites se terminent par votre nom de domaine interne, on mettra :

LocalNet
{
***.breizland.bz**
Example
 # The local domain is foo.com so don't cache any hosts in it.
 # *.foo.com
}

ATTENTION si vous passez par le proxy de votre FAI (nom **proxy.fai.fr**, port 3128 par exemple), vous devez modifier les lignes suivantes pour lire :

Proxy
{
<http://*> proxy = proxy.fai.fr:8080

Example
 # Use www.foo.com as a default http proxy server on port 8080
 # Except for the foo.com domain which has no proxy.
 # http://* = www.foo.com:8080
 # *://foo.com = none
}

Configurons maintenant le navigateur. Exemple avec **Netscape**, **Edition->Preférences->Avancées**, il faut d'abord désactiver le cache, sélectionner **Cache**, puis au niveau de **Comparer le cache avec celui du réseau**, choisissez **Jamais**. Toujours au niveau d'**Avancées** choisissez maintenant **Proxy**, puis **Configuration manuelle du proxy**, appuyez sur le bouton **Afficher**, pour les protocoles **proxy FTP**, **proxy Gopher**, **proxy HTTP**, **proxy de sécurité**, **proxy WAIS** mettez le nom du serveur **wwoffle** puis dans le champ port **8080**, laissez les autres champs par défaut puis **OK** et encore **OK**.

Pour **Konqueror**, **Configuration**, **Configurer Konqueror**, **Serveur mandataire (proxy)**, cocher **Utiliser un serveur de proximité**, cocher **Configuration manuelle** puis **Configuration**, au niveau du champ **HTTP** saisissez **http://votreserveurproxy**, **Port 8080**, cliquez sur le petit bouton à droite du champ **Port**, puis **OK**.

On va maintenant lancer le proxy en lui disant de relire son fichier de configuration :

wwwoffled -c /etc/wwwoffle/wwwoffle.conf

A noter les commentaires

wwwoffled[4535] Important: WWWOFFLE Demon Version 2.8b (with zlib,without ipv6) started.
wwwoffled[4535] Warning: Running with root user or group privileges is not recommended.

Voir plus bas, comment arranger cela. Connecter vous à Internet. Une fois connecté, tapez

wwwoffle -online

Surfer normalement, déconnectez vous, puis taper

wwwoffle -offline

A présent en mode off-line, surfer sur les quelques pages que vous venez de visiter, elles ont toutes été sauvegardées, cliquer maintenant sur une de ces pages sur un lien non visité, une page de **wwwoffle** s'affiche vous disant que la requête a été enregistrée, faites de mêmes pour quelques autres liens. Reconnectez vous, puis une fois connecté, tapez :

wwwoffle -online

Puis pour télécharger les pages que vous cherchiez à accéder en mode off-line:

wwwoffle -fetch

Les pages seront ainsi sauvegardées et vous pourrez à présent y accéder en mode off-line. Déconnectez vous (en n'oubliant pas le **wwwoffle -offline**) et réessayer.

NOTE Vous pouvez lancer le daemon en mode debug en tapant simplement :

wwwoffled -d 6

6.4 Configuration avancée

La configuration basique peut suffire dans la plupart des cas, on peut cependant aller plus loin. Si vous faites :

ps aux | grep wwwoffled

On se rencontre que c'est **root** le propriétaire du daemon, c'est un peu gênant dans la mesure où si **wwwoffled** est bugué quelqu'un peut se retrouver **root** sur le système, pour éviter cela, dans le fichier de configuration **wwwoffle.conf** au niveau des accolades **StartUp**, on dé commentera :

run-uid = daemon
run-gid = daemon

ATTENTION L'utilisateur **daemon** doit avoir les droits d'écriture sur **/var/spool/wwwoffle**.

On peut indiquer à **wwwoffle** lors de la récupération d'une page de ne pas récupérer les images, pour cela vous disposez d'options de récupération avec **FetchOptions**

FetchOptions
{
stylesheets = no
images = yes
frames = yes
scripts = no
objects = no
}

Les scripts correspondent au classe java par exemple. Pour autoriser certaines personnes à se connecter au serveur **wwwoffle**, vous disposez de **AllowedConnectUsers** avec la syntaxe du type :

olivier:motdepasse1
veronique:motdepasse2

S'il n'y a rien c'est que tout le monde est autorisé dès lors qu'on est sur une machine autorisée (**AllowedConnectHosts**)

AllowedConnectUsers
{

Example
 # Only allow connections from this one user.
 # andrew:password
}

On peut spécifier de ne pas sauvegarder certaines pages :

DontCache
{

 # pour ne pas sauvegarder les .gz et les .zip
***://*/*.gz**
***://*/*.zip**

 # pour ne pas sauvegarder les pages du domaine penthouse.com (!)
***://*.penthouse.com/**

Example
 # Don't cache any hosts in the barfoo.com domain.
 # *://*.barfoo.com/
 # Don't cache any gzipped or tar files.
 # *://*/*.gz
 # *://*/*.tar
 # Don't cache any files from /volatile in the foo.com domain.
 # *://*.foo.com/volatile/*
}

Pour que les utilisateurs ne puissent pas accéder à certaines pages sauvegardées quand on est offline :

DontRequestOffline
{

Example
 # Dont request any URLs at all when offline.
 # *://*/
}

Au niveau de **Purge**, on peut voir que par défaut les pages sont sauvegardées 28 jours pour changer cela, vous disposez de la variable **age** avec les variables w (week) pour semaine, m (month) pour mois et y (year) pour année. Exemple : age = 4w correspond à 4*7=28 jours, qui est d'ailleurs la valeur par défaut.

Pour faire le ménage pour que le cache ne dépasse pas 30Mo :

max-size = 30

Au niveau de **StartUp**, on peut spécifier un mot de passe, celui ci va servir à ce qu'uniquement les personnes le connaissant puissent modifier le fichier de config à partir d'un navigateur (voir paragraphe Utilisation).

password = mot-de-passe-en-clair

La syntaxe pour spécifier une **URL** est la suivante :

:// protocole quelconque, machine quelconque, port quelconque, chemin quelconque, arguments quelconques
***://*/<path>** protocole quelconque, machine quelconque, port quelconque, chemin spécifié, arguments quelconques (exemple ***://*/pub** comme **ftp://ftp.lip6.fr/pub** ou **http://www.yahoo.com/pub**)
***://*/*?** protocole quelconque, machine quelconque, port quelconque, chemin quelconque, pas d'arguments
***://<host>** protocole quelconque, hôte spécifié, port quelconque, chemin quelconque, arguments quelconques
<proto>:// protocole spécifié, hôte, port, chemin et arguments quelconques (exemple **http://** ou **ftp://**)
<proto>://<host> protocole et hôte spécifiés, chemin, port et arguments quelconques (exemple **http://www.yahoo.fr**)

6.5 Lancement automatisé

Si **squid** est votre proxy habituel, vous n'êtes pas obligé de le désactiver puisque les deux outils n'utilisent pas le même port. Si vous voulez néanmoins le désactiver pour cause de double emploi :

chkconfig --level 345 squid off

Pour un lancement automatique du daemon, on copiera le fichier **wwwoffled** se trouvant sous **./wwwoffle-2.8e/contrib/redhat1** sous **/etc/rc.d/init.d** :

cp ./wwwoffle-2.8e/contrib/redhat1/wwwoffled /etc/rc.d/init.d

Vérifier éventuellement les chemins dans ce fichier, puis pour un lancement automatique à l'état de marche 3, 4 et 5, il suffit de taper :

chkconfig --level 345 wwwoffled on

Et pour un arrêt aux autres ordres de marche

chkconfig --level 0126 wwwoffled off

Pour lancer le daemon il suffit alors de taper :

/etc/rc.d/init.d/wwwoffled start

Pour le stopper :

/etc/rc.d/init.d/wwwoffled stop

Pour le relancer :

/etc/rc.d/init.d/wwwoffled restart

Pour connaître son état (en marche ou arrêté)

/etc/rc.d/init.d/wwwoffled status

A chaque connexion on doit indiquer qu'on est online à wwwoffle, de même qu'on doit lui indiquer qu'on n'est plus online. Pour cela on dispose des fichiers **ip-up** et **ip-down** se trouvant sous **/etc/ppp** (sur une architecture de type **RedHat/Mandrake**). Dans le fichier **ip-up** on rajoutera :

 # On indique à wwwoffle qu'on passe en mode online
/usr/local/bin/wwwoffle -online -c /etc/wwwoffle/wwwoffle.conf

 # On récupère les pages qui ont été demandées pendant le mode offline
/usr/local/bin/wwwoffle -fetch -c /etc/wwwoffle/wwwoffle.conf &

Dans le fichier **ip-down** on rajoutera :

/usr/local/bin/wwwoffle -offline -c /etc/wwwoffle/wwwoffle.conf

A noter que pour le lancement du daemon et pour le passage online/offline il existe un ensemble de scripts pour les distribs de Linux les plus répandues sous **./wwwoffle-2.8e/contrib/redhat redhat1** et **redhat2**.

6.6 Utilisation

Vous disposez d'une page de consultation de **wwwoffle** à l'URL **http://obelix.breizland.bz:8080/Welcome.html** si **obelix** est le nom de votre serveur proxy et **breizland.bz** votre nom de domaine privé (**ATTENTION** saisissez exactement le même nom d'hôte que celui spécifié dans le fichier de config au niveau de **LocalHost**).

Une page de consultation en français apparaît. A partir de cette page vous avez dans l'ordre :

- la description du produit,
- l'index du cache, pour pouvoir entre autres :
  * voir la liste de toutes les pages **httpd** présentes en cache,
  * voir la liste des requêtes en attente,
  * voir la liste des pages à surveiller (voir si pages modifiées ou pas),
  * voir la liste des pages visitées à la dernière connexion,
- requête simple, pour spécifier une page à récupérer,
- suivi d'une page, pour spécifier une page à surveiller,
- contrôle interactif, pour administrer **wwwoffle** (édition du fichier de conf avec mot de passe),
- recherche dans le cache à partir de certains critères grâce à **ht://Dig** (qu'il faut installer),
- liens divers dont la FAQ de **wwwoffle**,
- e-mail de l'auteur en cas de problèmes (à rédiger en anglais) et listes de diffusion.

Vous avez la possibilité aussi de modifier en ligne le fichier de config.

Les clients peuvent maintenant être configurés pour utiliser votre serveur comme proxy (port par défaut 8080).