

0.1 [Squid] Plugin SquidGuard

SquidGuard est un filtre, un redirecteur et un plugin de contrôle d'accès pour Squid. Dans la suite, je suppose que vous avez installé et configuré Squid comme indiqué ICI¹.

0.1.1 1. Installation de squidGuard depuis les sources

0.1.2 1.1 Pré-requis

Pour fonctionner SquidGuard 1.2.x a besoin de BerkeleyDB version 3.3 téléchargeable sur www.sleepycat.com². La version BerkeleyDB 4.2.x n'est pas compatible avec squidGuard 1.2.x. BerkeleyDB version 3.3 s'installe comme suite :

```
$ tar zxvf db-3.3.tar.gz
$ cd db-3.3/buid_unix
$ ../dist/configure && make
$ su
# make install
```

Renseignez /etc/ld.so.conf :

```
# echo "/usr/local/BerkeleyDB.3.3/lib" » /etc/ld.so.conf
# ldconfig -v
```

Finissez par :

```
# cd /usr/local
# ln -nsf BerkeleyDB.3.3 BerkeleyDB
```

0.1.3 1.2 Installation de SquidGuard

Pour installer SquidGuard il suffit de taper dans un terminal :

```
# mkdir /var/lib/squidGuard
# mkdir /var/lib/squidGuard/db
# touch /etc/squid/squidGuard.conf
# exit
$ tar zxvf squidGuard-1.2.x.tar.gz
$ cd squidGuard-1.2.x
$ ./configure --prefix=/usr --with-db-lib=/usr/local/BerkeleyDB/lib --with-sg-config=/etc/squid/squidGuard.conf
    --with-sg-logdir=/var/log/squid --with-sg-dbhome=/var/lib/squidGuard/db
$ make
$ su
# make install
```

¹<http://www.trustonme.net/didactels/294.html>

²<http://www.sleepycat.com>

0.1.4 2. Installation de squidGuard depuis les paquets

- **Debian**
apt-get install squidGuard
- **Mandriva**
urpmi squidGuard
- **Gentoo**
emerge squidGuard

0.1.5 3. Installation de la Blacklist

Téléchargez la blacklist de votre choix parmi celles-ci :

- blacklist officielle³
- blacklist française⁴

Si ça vous intéresse, j'utilise la blacklist française. Une fois la blacklist téléchargée, installez-la comme suite :

```
# tar zxvf blacklist.tar.gz -C /var/lib/squidGuard/db/  
# cd /var/lib/squidGuard/db/  
# mv blacklist/* .  
# rm -rf blacklist
```

0.1.6 4. Configurez SquidGuard

Le fichier de configuration de SquidGuard est /etc/squid/squidGuard.conf. J'en fournis un exemple, correspondant au réseau suivant :

- Adresses de type : 192.168.0.x
- Adresse du serveur proxy : 192.168.0.1
- Nom du serveur proxy : serveur
- Port d'écoute de Squid : 3128.
- Stations autorisées à utiliser Internet : 192.168.0.50 et de 192.168.0.100 à 192.168.0.125

```
# /etc/squid/squidGuard.conf  
dbhome /var/lib/squidGuard/db  
logdir /var/log/squid  
# Definition des sources :  
src admin {  
  ip 192.168.0.1  
}  
src poste {  
  ip 192.168.0.50  
}  
src multipostes {
```

³<http://www.squidguard.org/blacklist/>

⁴ftp://ftp.univ-tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz

```
ip 192.168.0.100-192.168.0.125
}
# Definition de la base de données de filtrage utilisée
dest adult {
domainlist adult/domains
urllist adult/urls
}
dest publicite {
domainlist publicite/domains
urllist publicite/urls
}
dest warez {
domainlist warez/domains
urllist warez/urls
}
dest porn {
domainlist porn/domains
urllist porn/urls
}
# Definition des ACL
acl {
admin {
pass all
}
poste {
pass !porn !adult !publicite !warez all
redirect http ://mon_serveur/interdiction.html
}
multipostes {
pass !porn !adult !publicite !warez all
redirect http ://mon_serveur/interdiction.html
}
default {
pass none
redirect http ://mon_serveur/interdiction.html
}
}
# pour admin tout est autorisé, pour poste et multipostes
  tout est autorisé sauf porn adult publicite et warez
# "redirect http ://mon_serveur/interdiction.html" correspond
  à la redirection du client en cas d'accès refusé.
# FIN /etc/squid/squidGuard.conf #
```

Il existe d'autres possibilités de filtrage et d'acl comme la gestion des plages horaires et des domaines (voir <http://www.squidguard.org/config>⁵)

0.1.7 5. Mise en place

SquidGuard comme Squid doit être lancé par un utilisateur différent de root, par mesure de sécurité. Pour cela, en tant que root, créez les groupe et utilisateur "proxy" s'ils n'existent pas, par :

```
# groupadd proxy
# useradd -g proxy -d /etc/squid -s /bin/bash proxy
# passwd proxy
```

Il ne vous reste plus qu'à attribuer les bonnes permissions aux répertoires :

```
# chown -R proxy.proxy /var/lib/squidGuard /etc/squid /usr/bin/squidGuard /usr/bin/squid
/var/log/squid /var/spool/squid
```

Créez la base de données de filtrage par :

```
# squidGuard -C all
```

Editez le fichier /etc/squid/squid.conf et décommentez la ligne :

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

Redémarrez squid qui initialisera automatiquement squidGuard.

0.1.8 6. Les logs

Les logs de Squid et SquidGuard sont dans /var/log/squid, pour les consulter en direct, tapez en root dans un terminal :

```
# tail -f /var/log/squid/access.log
```

et

```
# tail -f /var/log/squid/squidGuard.log
```

⁵<http://www.squidguard.org/config>