# Squid
# & SquidGuard

Sommaire:

## Versions utilisées

Fedora core 4
Squid 2.5.STABLE11-2.FC4
squidguard-1.2.0-2.2

## Configuration de Squid

Si ce n'est pas fait, créer un utilisateur et un groupe **squid.**
Si ce n'est pas le cas changez les droits pour le dossier de cache de squid (suivant la version il n'est pas toujours au même endroit)

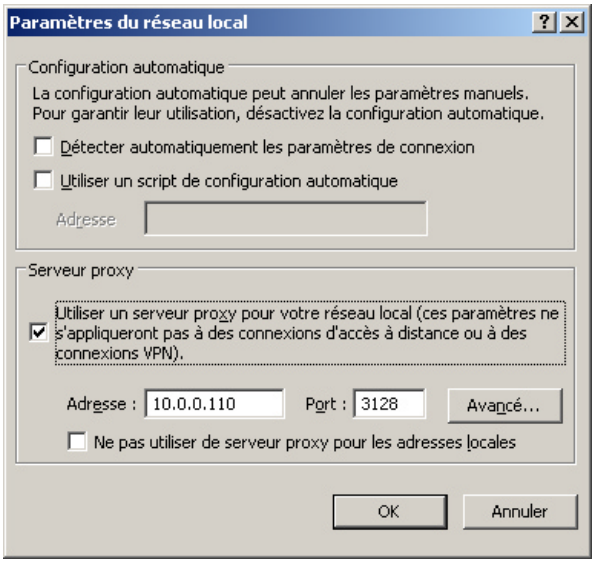
```
>#  chown  squid  /var/spool/squid
>#  chgrp  squid  /var/spool/squid
```

Lancer Squid avec les options par défaut et vérifier sont fonctionnement avec un client internet

```
>#  service  squid  start
```

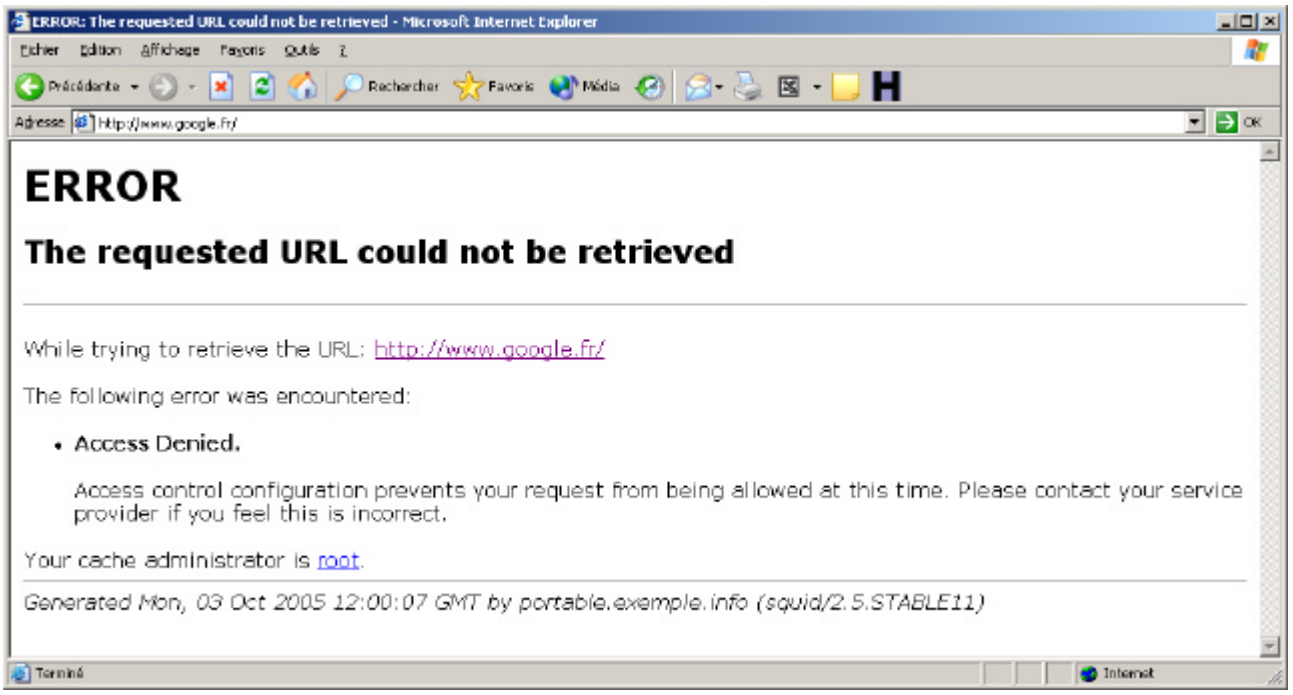
Lors du premier lancement le cache est initialisé (attention ce n'est pas vrai avec toutes les versions)

Sur le poste client, dans Internet Explorer allez dans le menu Outils \ options Internet onglet Connexions \ Paramètres du réseau local
entrez l'adresse du serveur proxy et le port (3128 par défaut pour squid)
Cliquez sur avancé pour activer la case **Utiliser le même serveur proxy pour tous les protocoles**




Dans Firefox allez dans Outils \Options Onglet Général Paramètres de connexion. Faites de même (Adresse Ip du serveur et port 3128).

Essayez ensuite de vous connecter à un de vos sites préférés. Vous devez obtenir un message de ce type.



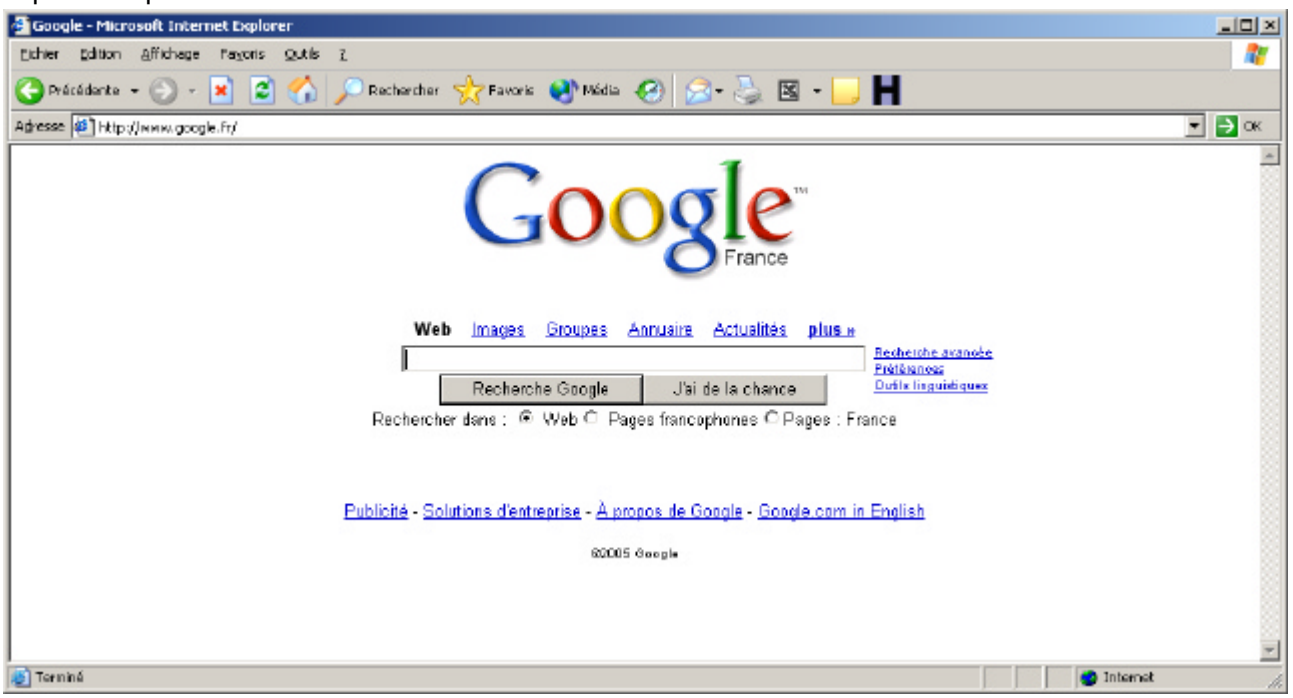

Squid fonctionne bien. Il faut maintenant le configurer pour pouvoir surfer.
Editez le fichier `/etc/squid/squid.conf`
Les commentaires ont été supprimé pour plus de clarté (plus de 3400 lignes par défaut)

```
#---------------Debut fichier configuration Squid---------------
http_port 3128 # port d'écouter par défaut
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
cache_effective_user squid # nom de l'utilisateur
```

```
cache_effective_group squid # et du groupe par défaut
cache_dir ufs /var/spool/squid 1024 16 256  # taille du cache
refresh_pattern ^ftp:         1440  20%   10080
refresh_pattern ^gopher:      1440  0%    1440
refresh_pattern .       0     20%   4320
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 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
acl monreseau src 10.0.0.1-10.0.0.200 #la plage d'adresse de votre réseau
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access allow monresau # la règle pour autoriser le surf pour votre réseau
http_access deny all
icp_access allow all
#-----------------Fin fichier configuration squid---------------
```

Attention l'ordre des ACL est très importante, bien mettre votre acl pour votre réseau avant l'acl `http_access deny all` sinon cela ne fonctionne pas.
Les lignes ajoutées / modifiées sont en gris

Redémarrer le service squid
`>#  service squid restart`
et vérifiez que vous surfez




Si tout va bien, vous arrivez sur la page demandée. Bien que l'on puisse créer des règles (acl) dans squid, il est préférable de passer par un programme externe comme SquidGuard, notamment pour des raisons de performance.

## SquidGuard

Si vous ne l'avez pas encore, récupérez le programme Suidguard avec yum par exemple.

```
>#  yum install squidguard
```

Après l'installation vous devez avoir
`/etc/squid/squidGuard.conf`
et un répertoire `/var/lib/squidGuard/db`, normalement vide (sur ma FC4 il n'existait pas)

### *Configuration*

Le fichier est dans /etc/squid/squidguard.conf

```
dbhome /var/lib/squidguard/db #emplacement des bases
logdir /var/log/squidguard
source reseau { #nom de votre réseau avec la plage d'adresse
      ip          10.0.0.1-10.0.0.200
}
acl {
      reseau { #par défaut on laisse tout passer pour le moment
            pass any
            redirect http://127.0.0.1/erreursquid.html
      }
      default {
            redirect http://127.0.0.1/erreursquid .html
            pass none
      }
}
```

Pour utiliser la directive redirect il vous faut un serveur web (type apache)
Créez une page web et placez là sur votre serveur (/var/www/html/ par défaut).
Vous pouvez aussi utiliser les scripts cgi fourni avec squidguard.

S'il le faut, changez les droits pour le dossier de squidguard

```
>#  chown squid /var/lib/squidguard/db
>#  chgrp squid /var/ lib/squidguard/db
>#  chmod 760 /var/ lib/squidguard/db
```

Il faut ajouter à la fin du fichier squid.conf la ligne suivante

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

Relancez le service squid et le service httpd (pour le serveur web). Vous devez normalement toujours surfer.

## *Intégration des black listes*

récupérez les sur :
ftp://ftp.univ-tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz
Décompactez le et placez les fichiers dans le dossier db de squidguard. Pour ne pas alourdir la charge du serveur j'ai supprimé tout les fichiers 'expressions' des différents dossiers quand ils existaient.
On va maintenant pouvoir intégrer les 'black listes' dans le fichier de configuration de squidguard.

```
#---------début fichier configuration squidguard -----------
dbhome /var/lib/squidguard/db
logdir /var/log/squidguard

source reseau {
      ip          10.0.0.1-10.0.0.200
}
destination porno {
    urllist adult/urls
    domainlist    adult/domains
}
destination agressif {
    urllist agressif/urls
    domainlist    agressif/domains
}
destination drogue {
    urllist drogue/urls
    domainlist    drogue/domains
}
acl {
      reseau {
            pass !porno !agressif !drogue
            redirect http://127.0.0.1/index.html
      }
      default {
            redirect http://127.0.0.1/index.html
            pass none
      }
```

```
Squid &SquidGuard
}
#-------------fin fichier configuration squidguard--------------------
```

Je n'ai pas utilisé tout les groupes, mais le principe est le même. Faites très attention aux fautes de frappe.

## *Initialisation des bases*

Lancez la commande suivante

```
>#  squidGuard -C all
```

Cela peut être vraiment très long et lorsque qu'il y a une erreur de syntaxe il ne le signal pas, le process ne s'arrête pas non plus. Pour le vérifier faites

```
>#  ps aux
```

Si dans la colonne STATS vous voyez un S ou S+ c'est qu'il y a un problème, arrêtez le process (Ctrl + c), vérifiez vos fichier de configuration et recommencez.

Il doit y avoir dans chaque dossier des fichiers avec l'extension .db

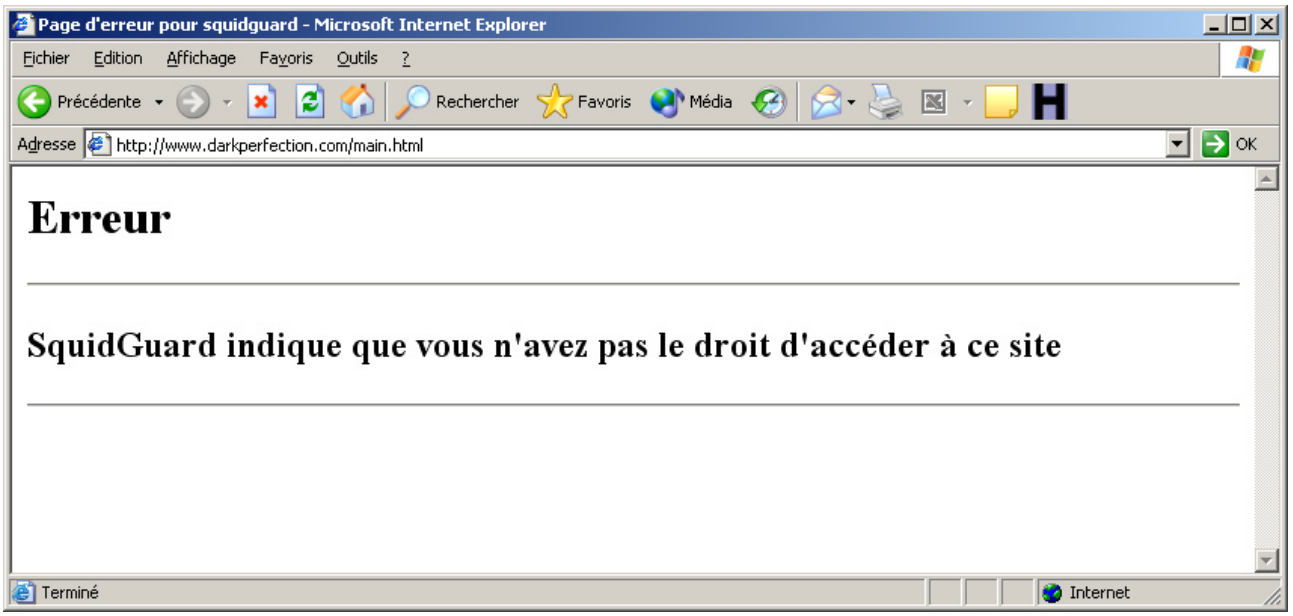
Si vous avez fait les opérations avec l'utilisateur root il y des chances que les droits aient changé, refaites

```
>#  chown -R squid /var/lib/squidguard/db
>#  chgrp -R squid /var/ lib/squidguard/db
>#  chmod -R 760 /var/ lib/squidguard/db
```

Relancez squid

Vous pouvez bien sur éditer les urls et domains pour les adapter à votre usage (et aussi en créer des nouveaux). Normalement les bases sont resynchronisées si vous relancez le service Squid

Vérifiez que effectivement certains sites ne sont plus accessible




La page créée pour Squidguard est alors affichée à la place de celle de squid.