

SQUID

I- Squid, c'est quoi?

Squid est un serveur proxy-cache, c'est à dire, qu'il stocke les données fréquemment consultées sur les pages Web (notamment les images) sur un serveur cache du réseau local pour éviter de les télécharger à chaque connexion. De même, il peut mettre en mémoire cache les requêtes DNS.

Il permet ainsi de réduire et d'optimiser l'usage de la bande passante vers Internet et du réseau en général, d'ouvrir Internet aux machines situées derrière un pare feu, de restreindre les ressources web utilisables, de contrôler l'utilisation.

II- Comment ca marche?

Squid est un daemon, il tourne donc en tâche de fond. Il écoute en permanence un port (d'origine le 3128).

Squid cache les pages visitées, ce qui permet de les charger plus vite lors d'une nouvelle visite, car les images ne sont pas rechargées depuis internet, mais depuis le serveur, donc en local.

Lorsqu'une page est demandée, Squid vérifie si les informations de la page sont plus récentes que celles qu'il possède en cache. Si c'est le cas, il met à jour son cache et envoie les informations à l'utilisateur, sinon il envoie directement les informations à l'utilisateur.

III- Où trouver des informations?

Différents sites traitent de ce sujet.

A commencer par le site officiel de squid: <http://www.squid-cache.org/>

L'article sur Wikipédia: <http://fr.wikipedia.org/wiki/Squid>

Sur les sites et forums des différentes distributions.

Autres liens:

<http://www.malekal.com/squid.php>

<http://stielec.ac-aix-marseille.fr/cours/caleca/squid/>

Dans ce document, nous utiliserons une distribution Ubuntu et un serveur Squid 2.6.STABLE14.

IV- Installation

Utilisez la commande d'installation de paquetage:

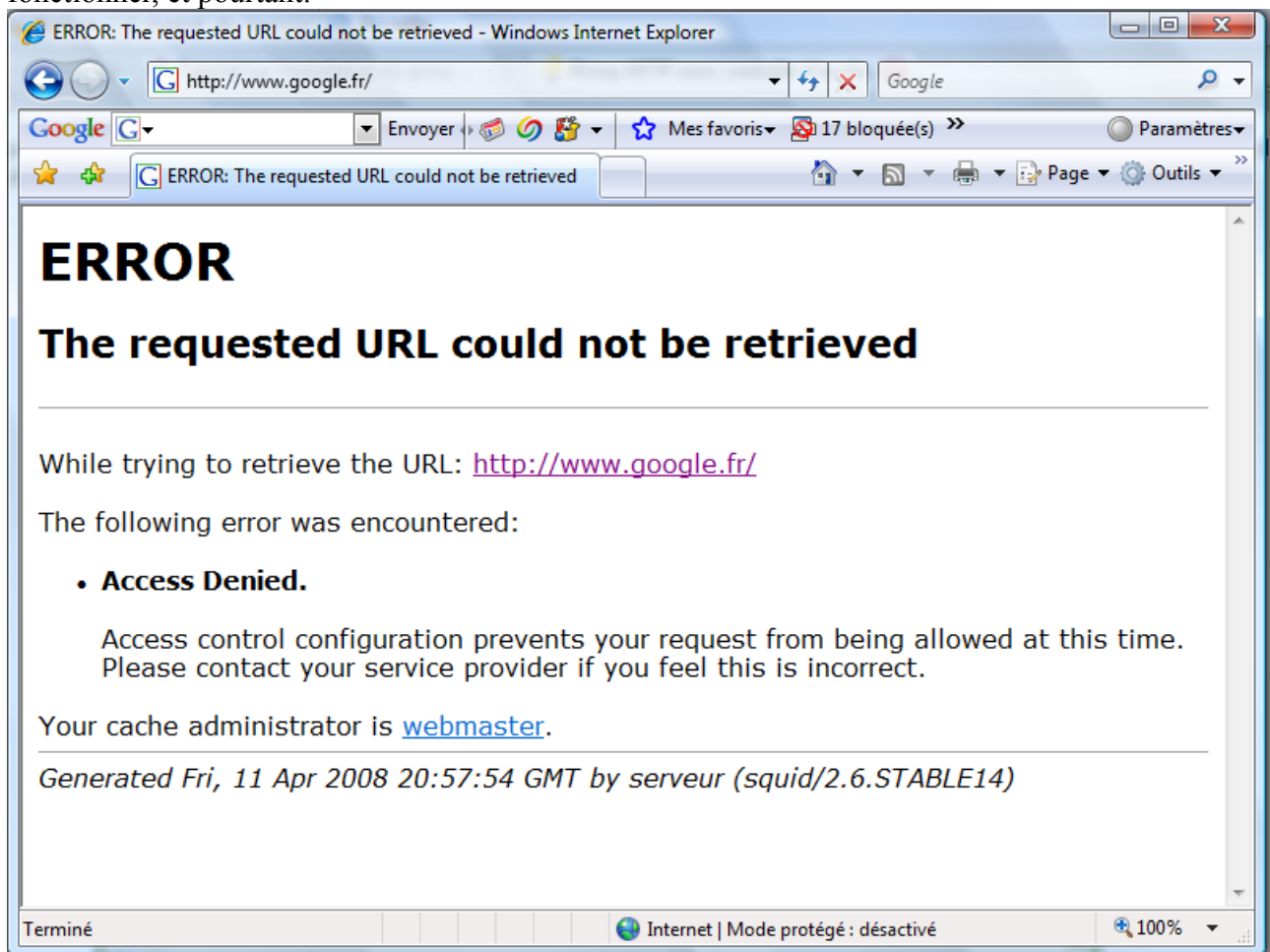
```
toto@serveur:~$ sudo apt-get install squid
```

Le daemon est lancé automatiquement:

```
toto@serveur:~$ ps aux | grep squid
root      11208  0.0  0.1  4780  652 ?        Ss   Apr04   0:00 /usr/sbin/squid -D -sYC
proxy    11210  0.0  3.1 18480 16184 ?        S    Apr04   0:11 (squid) -D -sYC
```

Donc Squid fonctionne.

Il suffit d'entrer paramètres du proxy dans les options du navigateur internet et tout devrait fonctionner, et pourtant:



Cela ne fonctionne pas car d'origine Squid interdit toutes les connexions.

V- Configuration de base

Le fichier de configuration se trouve dans le dossier:

```
toto@serveur:~$ cd /etc/squid/
```

Il faut éditer le fichier de configuration de manière à autoriser le réseaux local à accéder à internet:

```
toto@serveur:/etc/squid$ sudo vi squid.conf
```

Squid est un proxy très complet, son fichier de configuration est donc plein d'explications et donc très long (environ 4500 lignes).

Pour une configuration de base, il faut autoriser le réseaux local à accéder à internet.

Nous garderons la configuration d'origine pour ce qui concerne le port utilisé et le stockage, mais nous verrons où et comment cela est configuré.

- Vérifier le port sur lequel écoute le serveur, dans la section « Network options »:

```
# NETWORK OPTIONS
# -----
# TAG: http_port
# Squid normally listens to port 3128
http_port 3128
```

- Ensuite une section important, celle où l'on configure les autorisations d'accès « Access controls »:

Tout d'abord, les ACL (Access Control List, Liste de Contrôle d'Accès), ce sont des listes d'adresses aux quelles on peut ensuite autoriser ou non différents accès.

On y trouve toutes les listes d'origine:

```
# ACCESS CONTROLS
# -----
# TAG: acl
#
#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 to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 # https
acl SSL_ports port 563 # snews
acl SSL_ports port 873 # rsync
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
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 Safe_ports port 631 # cups
acl Safe_ports port 873 # rsync
acl Safe_ports port 901 # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
```

A la suite de ces liste, on va créer un nouvelle ACL pour notre réseau:

```
acl mon_reseau src 192.168.1.0/24
```

Le premier champ sert à dire que ce qui suit est une ACL.

Le second champ est le nom de l'ACL, ici « mon-reseau »

Ensuite, « src » signifie que les requêtes viendront des adresses qui font partie du réseau défini après.

Ensuite il faut donner les autorisation aux ACL:

ATTENTION: L'ordre des ACL n'a aucune importance. En revanche, l'ordre dans lequel les autorisations d'accès sont données est très important.

La liste d'origine:

```
# TAG: http_access
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access deny to localhost
```

Puis l'autorisation de notre ACL:

```
http_access allow mon_reseau
```

Et on fini par interdire tout le reste, pour plus de sécurité:

```
http_access allow localhost
http_access deny all
```

- Dans la section « Administrative parameters », il faut configurer:

```
# TAG: visible_hostname
#Default:
visible_hostname serveur
```

Remplacer « serveur » par le nom que vous souhaitez donner à votre proxy.

- Pour configurer le cache, il faut modifier les paramètres dans la section « Options which affect the cache size ».

On peut y configurer l'espace réserver au stockage, la taille maximum/minimum des objets stockés.

- Dans la section « Logfile pathnames and cache directories » se trouve la configuration des dossiers des logs et du cache ainsi que leurs emplacements.

VI- Autres possibilités

Dans la configuration de Squid:

- Par les ACL, il est possible de gérer les jours et heures de connexions.
- Il est possible de créer des utilisateurs avec mot de passe, ce qui permet d'identifier les utilisateurs et de voir dans les logs qui visite quel site et d'interdire l'accès à des personnes qui ne sont pas autorisées.
- Avec une redirection du port 80 vers le port d'écoute du proxy, on oblige les utilisateurs à utiliser le proxy de manière transparente, mais ceci est incompatible avec le point précédent.

Autres programmes:

SquidGuard est un « add-on » de Squid.

Il permet notamment la gestion des accès à certaines URL en fonction de différents paramètres.

Il permet donc un filtrage plus fin des accès à internet.