

SQUID

Proxy Libre pour Unix et Linux

1. Présentation :

SQUID est un proxy (serveur mandataire en français) cache sous linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs avec une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu du web, réduisant les temps d'accès et la bande passante consommée, il est possible aussi d'effectuer des contrôles de sites. Enfin il permet de partager une connexion à internet à l'aide SQUID, mais SQUID n'est pas un proxy POP, SMTP, NNTP (comme Samba par exemple).

SQUID est un logiciel de cette catégorie, qui autorise le proxy, le cache des protocoles HTTP, ftp, Gopher, etc. Il supporte également SSL, les contrôles d'accès, le cache de DNS et fournit une trace complète (log) de toutes les requêtes. SQUID est aussi disponible pour Windows NT.

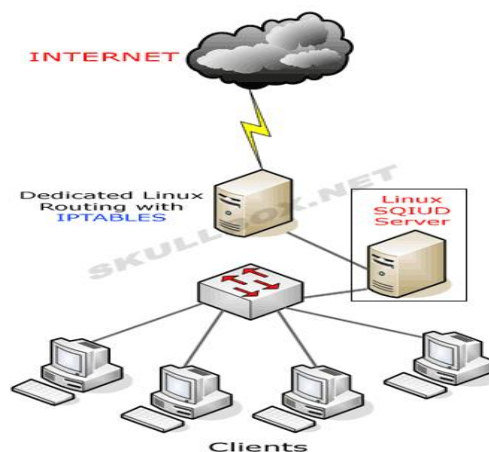


Figure1 : Mise en place du serveur proxy SQUID dans le réseau d'entreprise

2. Pré-requis et Installation :

Une minimale configuration matérielle est requise. Par exemple un Pentium III avec un disque de 10 Go et une RAM de 128 Mo.

**Pour l'installation on procède comme suit :

- 1- Téléchargez la dernière version de SQUID du site : www.squid-cache.org .
- 2- **Si vous avez maintenant les packages rpm il faudra utiliser cette commande :

```
rpm -ivh squid*.rpm
```

Il place alors les fichiers de log dans /var/log/squid, le fichier de configuration dans /etc/squid/squid.conf.

Ce dernier est le seul fichier de configuration de SQUID. Il faut donc ouvrir ce fichier pour effectuer les paramétrages correspondant à votre situation.

** En cas d'utilisation des tar, il faut les Décompressez-la en utilisant cette commande:

```
tar -zxvf squid-x.tar.gz
```

- 3- Compilez-la en utilisant cette commande :

```
./configure --enable-err-language=French
```

```
make all
```

```
make install
```

Un répertoire sera créé dans /usr/local/squid, il contient un répertoire bin qui contient lui même les répertoires cache, etc, logs... .

3. Les services de SQUID

3.1 Le cache

Le principe de cache est assez simple, prenons par exemple le réseau de l'INSAT. Ce dernier est composé d'une dizaine de postes équipés de cartes réseaux Ethernet à 100Mb/s. Ce réseau est relié via un routeur à internet en utilisant une ligne spécialisée. Nous lui avons affecté une plage d'adresses IP non routable (192.168.1.x).

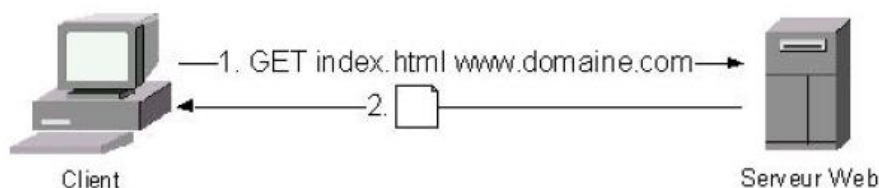
Avant la mise en place de notre proxy, toutes les personnes qui allaient sur internet, récupèrent par l'intermédiaire de leurs navigateurs les objets (html, images, ...) qu'ils avaient consultés, mais tous ces objets qui ont été téléchargé n'étaient pas accessible par les autres navigateurs (c'est-à-dire les autres utilisateurs du réseau), ce qui implique que les autres utilisateurs devraient eux aussi récupérer leurs propres objets. Ce qui réduit la consommation de bande sur notre ligne spécialisée et produit un gain de temps pour les utilisateurs internet. Bien sur le serveur proxy vérifie, avant de donner les objets qui possèdent sur son disque, s'il n'y a pas de version plus récente de l'objet demandé sur Internet. S'il y a une version plus récente il va la télécharger sinon il donne à l'utilisateur l'objet qui avait enregistré.

SQUID est capable de relayer les protocoles HTTP, FTP, SSL et Gopher.

****Observons, tout d'abord, l'accès à un site web sans passer par un proxy :**

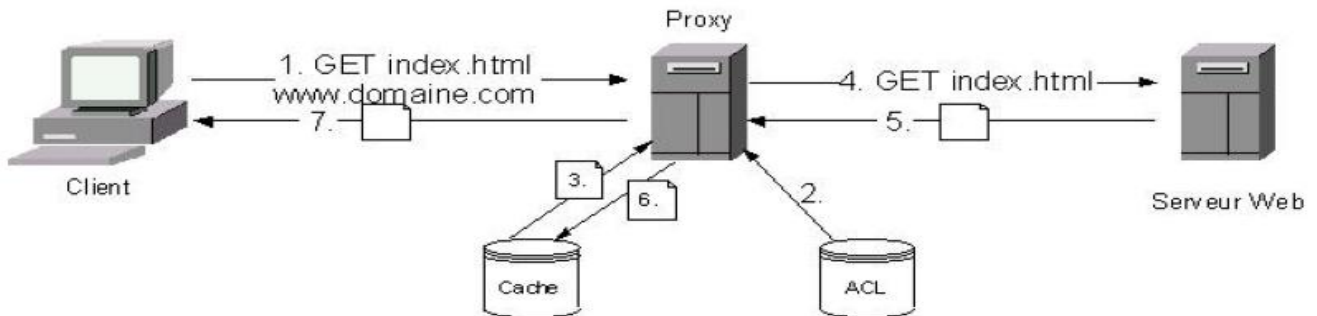
Le client demande directement au serveur Web de lui envoyer une page. Si un autre client du réseau demande la même page, le serveur Web est contacté à nouveau.

Figure 1. Accès web sans proxy



Avec un proxy, toutes les requêtes passent par un intermédiaire.

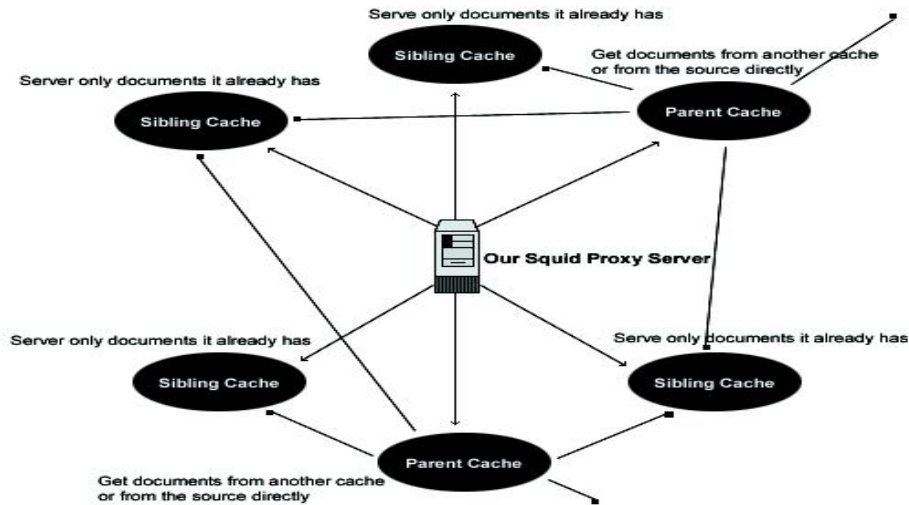
Figure 2. Accès web avec proxy



1. Le client demande une page.
2. La requête est interceptée par le proxy. Celui-ci vérifie ses ACLs. Si la requête est interdite, un message d'erreur (non représenté sur la figure) est envoyé au client.
3. Si la requête est autorisée, le proxy vérifie si la page est déjà dans son cache (autrement dit, si elle été demandée récemment). Si c'est le cas, elle est envoyée directement au client sans passer par le serveur web.
4. Si la page ne figure pas dans le cache, le proxy transmet la requête au serveur désiré.
5. Le serveur retourne la page.
6. Le proxy intègre cette page dans son cache.
7. Le client reçoit la page demandée.

3.2 Le support des protocoles liés aux caches

SQUID supporte beaucoup de protocoles liés aux caches: ICP, HTCP, CARP, Cache Digests, WCCP. Ces protocoles permettent les échanges entre les différents caches et ainsi favoriser les flux de données les plus proche du site plutôt que de solliciter un serveur qui sera peut-être plus éloigné et plus lent à répondre qu'un serveur cache.



3.3 Accélérateur pour le serveur http (Mode Reverse-Proxy)

Tout l'intérêt de ce service repose sur le cache de SQUID. Effectivement, une fois que celui-ci aura enregistré tous les objets possibles du serveur http, la plupart des requêtes des clients seront alors traitées par SQUID. Ainsi, le serveur http sera beaucoup moins sollicité. Par cette méthode, le serveur web ne sert plus alors qu'à traiter les pages dynamiques, CGI, l'enregistrement de formulaire, etc.

Il est possible de multiplier les "Proxy Accelerator" en les faisant communiquer via ICP : (Internet Cache Protocol, protocole de communication inter-cache). Cela permet encore d'augmenter la rapidité de réponse et le backup des données.

3.4 L'authentification :

SQUID permet d'authentifier les clients avant qu'ils accèdent à la ressource qu'ils demandent. L'authentification s'effectue pour les modes proxy et "httpd accelerator". Il devient alors de plus en plus avantageux d'utiliser SQUID en frontale d'un serveur web car ce dernier n'aura à assumer que les rôles primordiaux de service web dynamique. SQUID supporte beaucoup de protocoles liés à l'authentification (Basic, Digest, LDAP, NTLM, Radius, Mysql).



L'authentification est réalisée via des codes exécutables externes à SQUID, chaque protocole d'authentification ayant son propre code exécutable. Ces programmes d'authentification ont un format d'utilisation très simple : ils lisent sur STDIN les informations d'authentification sous la forme "login, MotDePasse" et retourne sur STDOUT "OK" ou "ERR" en fonction des informations introduites (correctes ou non).

3.5 Le filtrage : Autorisation d'accès par filtrage :

SQUID offre la possibilité de filtrer les requêtes des clients. Ainsi, il est possible de restreindre l'accès aux ressources en fonction de différents paramètres. Voici une liste de paramètre pouvant intervenir dans le rejet d'une requête répondant à l'un des critères :

- L'URL contient un mot interdit.
- L'adresse IP source/destination est interdite.
- Le domaine de source/destination est interdit ou contient un mot interdit.
- La date de la demande. Par exemple, SQUID peut interdire l'accès à Internet durant certaines heures (comme le soir entre 20h et 6h du matin).
- Le port de destination.
- Le protocole utilisé peut permettre de bloquer les transferts FTP par exemple.
- La méthode utilisée peut permettre d'empêcher les méthodes HTTP comme POST par exemple.
- Le type du navigateur utilisé peut permettre d'empêcher l'utilisation d'IE par exemple.
- Ce filtrage est basé sur des ACL. SQUID n'est capable de filtrer que les requêtes de ses clients, pas le contenu de ce qu'il relaye à ceux-ci (bien qu'un proxy filtrant le contenu de page revient à multiplier la charge d'administration par le nombre d'interdiction malencontreuse).

3.6 Réécriture des entêtes de requêtes:

Il est possible de réécrire les entêtes des requêtes des clients. Cela a pour utilité (par exemple) de rendre les demandes anonymes. Ceci se fait très simplement en indiquant dans la configuration de SQUID quels sont les champs HTTP autorisés et en précisant que tous les autres ne le sont pas. Il est aussi possible de remplacer le contenu d'un champ.

3.8 Le protocole SNMP:

SQUID offre la possibilité d'être géré à distance via SNMP. Ainsi, les données collectées via ce protocole pourront permettre à l'administrateur de visualiser l'état courant de son proxy, d'avoir des statistiques d'utilisation, des statistiques sur le cache, sur le temps processeur consommé, ...

Programmes associés :

- **WebMin:** est une page d'administration au format web, permettant de gérer son serveur linux ainsi que tous ses services (SQUID, DHCP, serveur web, utilisateurs ...etc.)
- **SquidGuard:** propose un filtrage puissant d'accès au web, en fonction des groupes d'utilisateurs, des listes de domaines et d'URL, des plages horaires,...
- **DansGuardian:** est un outil de filtrage de contenu similaire à SquidGuard.

DG sait interdire des sites en fonction du Domaine, URL, Utilisateur, IP client, extension de fichier, mot dans la page, score de mots dans la page, type MIME, RegExp (expression régulière), PICS.

DG gère aussi les listes blanches et les listes grises.

- **MRTG :** est un outil pour monitorer SQUID à distance via SNMP.
- **Prostat :** est un outil de statistiques afin d'évaluer le taux d'utilisation d'un cache SQUID.
- ...



S E C U R I N E T S
Club de la sécurité informatique
I N S A T

Autres proxy :

- Delegate : proxy / cache très souple à configurer gérant le protocole Socks.
- Oops : c'est un proxy / cache écrit pour la performance et la rapidité de configuration.
- Privoxy : c'est un proxy écrit pour "anonymiser" le surf de ses clients.