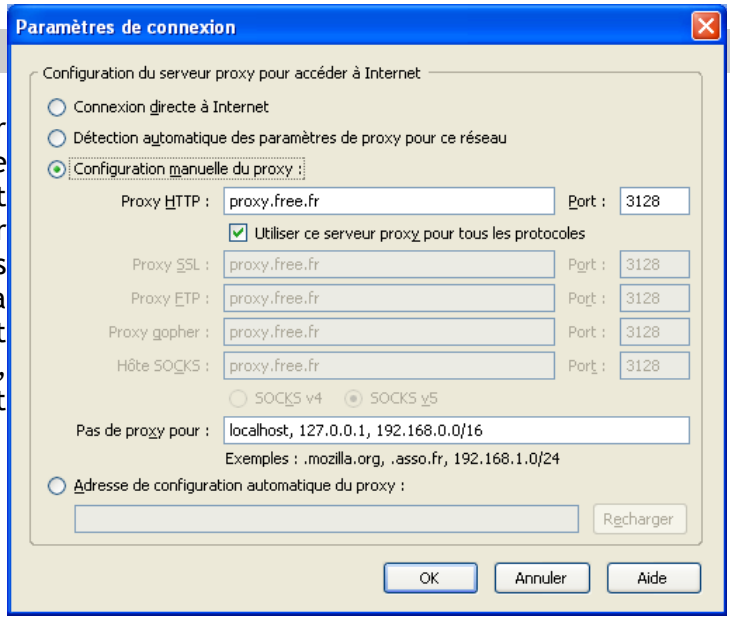
Nicolas Dewaele
nico@nicodewaele.info
www.nicodewaele.info

Serveur Proxy : Squid et SquidGuard

I- Comprendre les fonctions du Proxy :

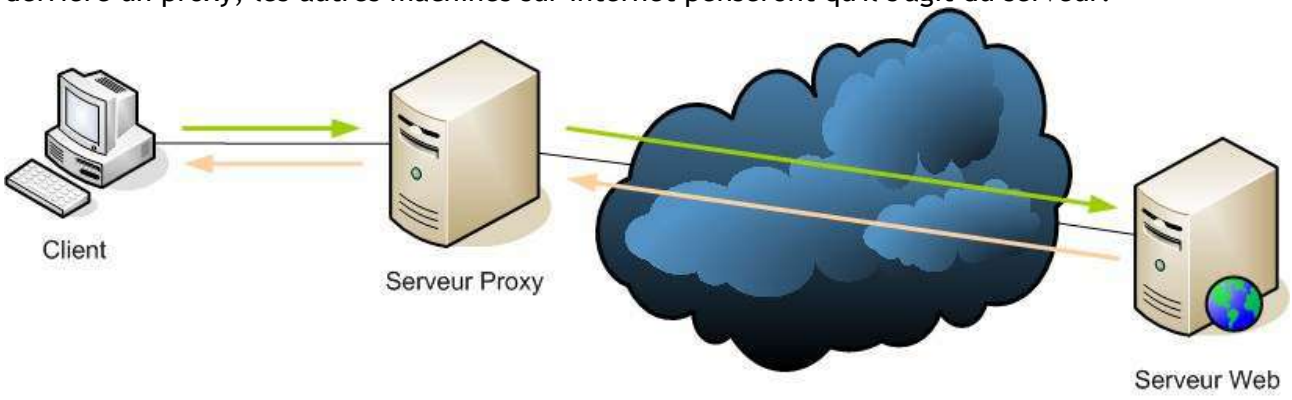
Le serveur mandataire :



Dans un réseau local, on peut avoir envie de mettre une machine qui fasse l'intermédiaire entre notre réseau et Internet. Le serveur proxy (ou serveur mandataire) permet de d'envoyer les requêtes et de recevoir les réponses à la place de ses clients. Ces requêtes peuvent être des requêtes de divers protocoles, les plus utilisées étant le HTTP, HTTPS et FTP, SSL.

- Un client envoie sa requête
- Le proxy la récupère et la renvoie
- Le serveur répond au proxy
- Le proxy renvoie la réponse au client.

L'avantage du proxy est que les clients deviennent invisible pour l'Internet. Si un client est derrière un proxy, les autres machines sur Internet penseront qu'il s'agit du serveur.

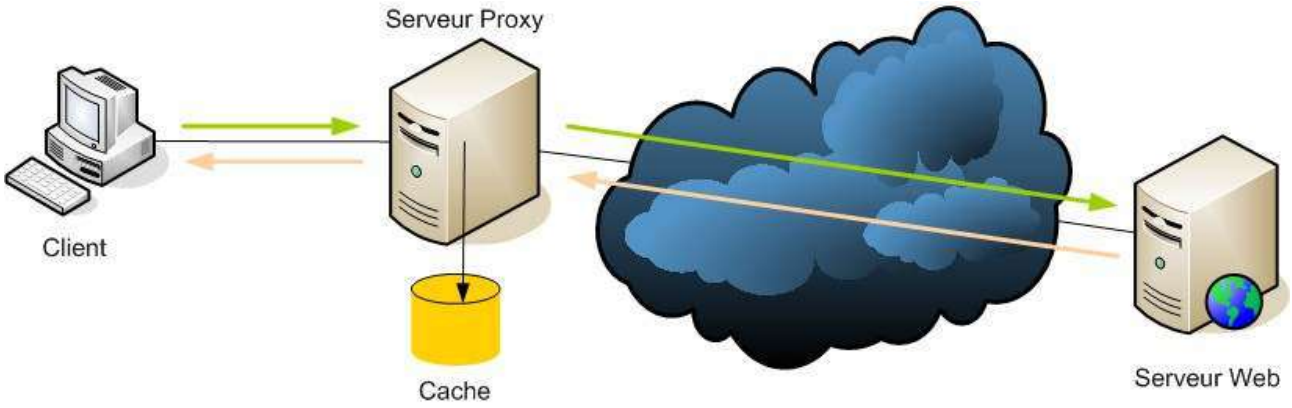


En tant que clients Web, votre fournisseur d'accès vous offre de passer par son proxy pour aller sur Internet. Cela a comme avantage pour vous d'être anonyme, puisqu'il fait chaque requête à votre place.

Le proxy à également d'autres rôles détaillés aux paragraphes suivants.

Nicolas Dewaele
nico@nicodewaele.info
www.nicodewaele.info

Le cache :

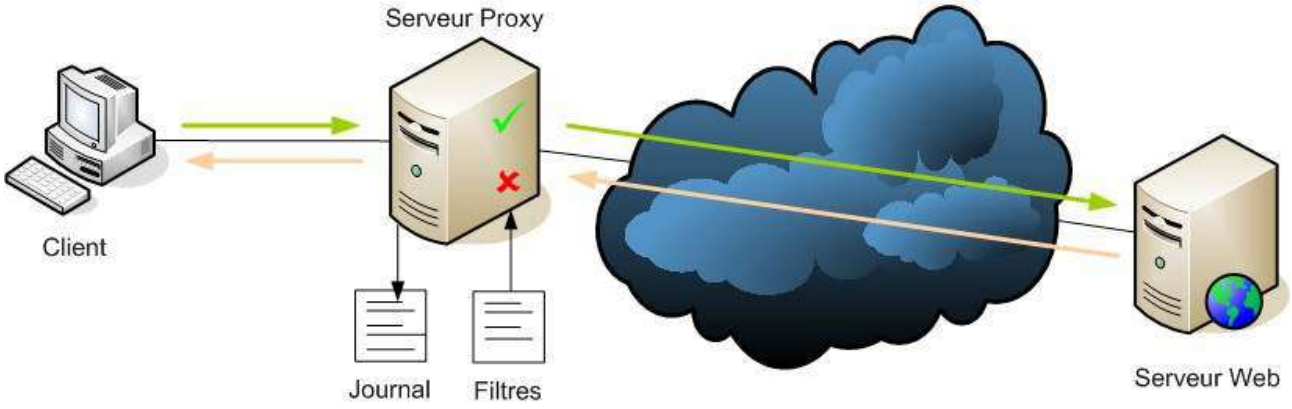


Le cache permet de stocker un certain nombre de fichiers pendant que vous naviguez sur Internet pour permettre d'afficher la page plus rapidement si vous retournez sur le même site une autre fois.

En général, les navigateurs Web (Mozilla, Internet Explorer, ...) utilisent un cache (ils prennent une certaine place sur le disque dur pour stocker ces fichiers).

Un serveur cache-proxy permet de faire la même chose à un plus grand niveau: Il est dédié au stockage des fichiers et pages Internet les plus visitées. Toutes les machines qui passent à travers le proxy lui font stocker des pages et fichiers Internet, du coup les sites les plus visités par les gens utilisant le réseaux sont plus rapides à télécharger.

Le filtrage :



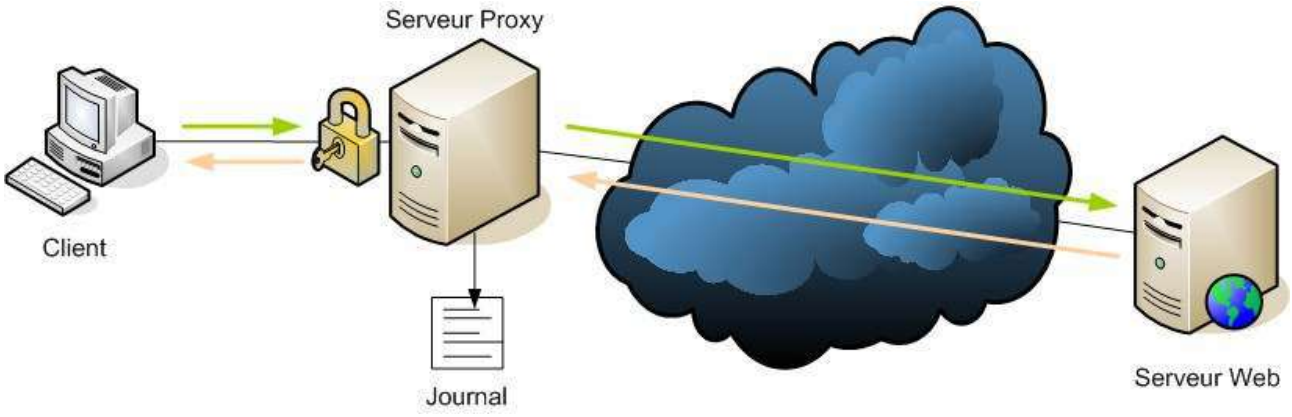
Le serveur proxy peut également servir à suivre toutes les entrées et sorties en créant des **journaux d'activités (logs)** qui enregistrent chaque requête que font les clients.

Au niveau des clients on peut lister un certain nombre de sites autorisés (**liste blanche**) ou des sites qui ne le sont pas (**liste noire**).

Au niveau des serveurs, l'analyse des réponses en fonction de certains critères s'appelle le **filtrage de contenu** (mots clés, adresses IP, noms de domaines, ...).

Nicolas Dewaele
nico@nicodewaele.info
www.nicodewaele.info

L'authentification :



Puisque le serveur Proxy se trouve entre le réseau local et Internet, il peut très bien décider de qui a le droit de se connecter sur Internet en imposant que le client s'authentifie pour se connecter (login et mot de passe).

Reverse Proxy :

Le proxy inversé ne sert pas de relais aux clients de son lan mais à ceux qui viennent d'Internet et ont besoin d'avoir accès à certains serveurs internes.

II- Squid :

Le serveur Proxy le plus utilisé par les fournisseurs d'accès et les administrateurs de réseaux locaux s'appelle Squid. Il fonctionne sous Unix.

Installation:

Si vous fonctionnez sur un Linux basé sur une Debian (Debian, Knoppix, Mepis, ...) vous n'avez qu'à utiliser la commande apt :

apt-get install squid

La commande apt se charge de tout faire: téléchargement, installation et configuration.

Avant de commencer:

Le fichier de configuration de squid s'appelle squid.conf et se trouve dans /etc/squid

Sauvegardez le fichier d'origine en faisant: cp squid.conf squid.conf.original Pour démarrer le service, vous pouvez taper la commande:

```
/etc/init.d/squid start
```

Nicolas Dewaele
nico@nicodewaele.info
www.nicodewaele.info

Pour vérifier que le serveur est en fonctionnement: ps ax | grep squid

Si vous avez une réponse c'est que ça tourne.

Pour vérifier que ça marche, vous devez configurer un client (Internet Explorer, Mozilla ou Konqueror) en mettant dans les options comme serveur proxy votre adresse IP et le bon port (par défaut 3128).

III- Configuration: /etc/squid/squid.conf

Le fichier squid.conf fonctionne de la même manière que les autres fichiers de configuration, on entre des directives et les options qui vont avec.

Les lignes commençant par # sont des commentaires.

Il y a une quantité de directives à configurer, pour faire simple, voici seulement quelques directives à connaître :

```
######################### # SQUID.CONF # #########################

# CONFIGURATION GENERALE

# Numéro de port http sur lequel les clients se connectent. Souvent 8080
# On peut aussi préciser sur quelle @IP

http_port 192.168.0.101:3128

# Nom DNS du proxy
visible_hostname proxy.mynetcourse.info
```

```
# CONCERNANT LE CACHE :

# Mémoire vive allouée à Squid
cache_mem 20 MB

# Quand le cache est rempli à 90% il se vide jusqu'à 75% de sa capacité
cache_swap_low 75

cache_swap_high 90

# Interdire de stocker en cache des objets de plus de 8M
maximum_object_size 8192 KB

# Répertoire où stocker le cache, la taille maxi du répert (ici 200 M)
# et le nombre de sous répertoires de premier et de deuxième niveau
#(16 rep dans lesquels 256 sous-rep)
cache_dir ufs /cache1 200 16 256

# Journal des requêtes
cache_access_log /var/log/squid/access.log
# Journal de Squid
```

```
cache_log /var/log/squid/cache.log

# Ne pas enregistrer les écritures et suppr de fichiers dans un journal
cache_store_log none

# Adresse de l'administrateur du proxy
cache_mgr admin@mynetcourse.info

# Utilisateur et groupe qui utilisent Squid
cache_effective_user proxy
cache_effective_group proxy

# Pour réécrire les logs toutes les 2 semaines
logfile_rotate 2
```

Pour pouvoir formater le répertoire du cache, tapez la commande

```
squid -z
```

pour cela le répertoire doit exister et être accessible en écriture par l'utilisateur proxy.

Autorisations par les ACL :

Les ACL (Access Control List) sont des listes de machines, de réseaux auxquelles on affecte un certain nombres de droits. Elles sont utilisées pour dire que telle machine ou tel réseau à le droit ou pas de faire telles choses.

Elles se configurent en deux temps:

• D'abord la **déclaration des ACL** avec la directive acl : acl <nom> src/dest groupe-de-machines
• Ensuite, on donne des **droits sur l'acl** que l'on a déclaré avec par exemple la directive http_access qui donne des droits sur les requêtes http.

Voici quelques exemples de listes d'accès:

```
### Déclaration de diverses ACL ###

# Cette liste concerne tous les accès provenant du réseau 192.168.0.0
acl lan1 src 192.168.0.0/255.255.255.0

# Cette liste concerne tous les accès à destination du réseau 10.0.0.0
acl servers dest 10.0.0.0/255.0.0.0

# Cette liste concerne tous les accès à destination du domaine yahoo.fr
acl yahoo dst www.yahoo.fr

# Cette liste concerne des mots-clés
acl interdit url_regex sex
acl interdit url_regex drogue
acl interdit url_regex violence

# Cette liste concerne toutes les machines non listées ci-dessus
acl autres src 0.0.0.0/0.0.0.0
```

Nicolas Dewaele
nico@nicodewaele.info
www.nicodewaele.info

Voici quelques droits associés aux ACL de la page précédente :

```
### Droits de requêtes http pour les acl déclarées au-dessus ###
http_access deny interdit
http_access allow lan1
http_access deny servers
http_access deny all

# ... Il est possible d'imaginer beaucoup d'autres restrictions
```

Les ACL font office de firewall mais s'appliquant uniquement aux protocoles gérés par le proxy (HTTP, FTP, HTTPS).

> Comme pour un pare-feu, l'ordre des règles a une importance,
> les règles sont lues de haut en bas.

Authentification :

Vous allez devoir créer des utilisateurs avec leurs mots de passe. Pour créer l'utilisateur toto avec le mot de passe motdepasse, utilisez la commande:

```
htpasswd -cb /etc/squid/users toto motdepasse
```

L'option -c est utilisée pour la création du fichier. Ne la mettez que si vous créez le fichier.

Testez votre fichier de mot de passe en tapant la commande:

```
/usr/lib/squid/ncsa_auth /etc/squid/users
     toto motdepasse
     OK
```

CTRL + C pour sortir.

Pour demander à l'utilisateur d'être authentifié pour pouvoir utiliser le Proxy, vous devez rajouter une acl comme ceci dans squid.conf :

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/users
acl restriction proxy_auth REQUIRED
http_access allow restriction
http_access deny !restriction
```

Nicolas Dewaele
nico@nicodewaele.info
www.nicodewaele.info

IV- SquidGuard :

SquidGuard est un filtre, un redirecteur et un plugin de contrôle d'accès pour Squid. Il va notamment permettre d'appliquer sur un proxy une liste noire de sites ou mots clés interdits.

Installation:

Nous allons installer le plugin de squid (squidGuard) :

```
apt-get install squidguard
```

Cette installation crée un fichier de configuration de squidGuard
/etc/squid/squidGuard.conf

Nous allons télécharger une liste de sites classés par catégories :
ftp://ftp.univ-tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz

Puis extraire cette liste (tar.gz) dans le répertoire /var/lib/

Configuration :

SquidGuard permet à Squid de limiter l'accès aux sites de façon assez poussée et complémentaire à ce que peut faire squid tout seul:

Vous devez éditer le fichier /etc/squid/squidGuard.conf

```
### Configuration générale:

# Répertoire contenant les bases de données des sites interdits
dbhome /var/lib/blacklists
# Répertoire des logs
logdir /var/log/squid
```

```
### Plages horaires
time workhours {
      # Du lundi au vendredi de 8h30 à 18h30
      weekly mtwhf 08:30-18:30
      # Le samedi de 8h30 à 13h
      weekly a 08:30-13:00
}
```

```
### Définition des sources :
# Poste de l'administrateur
src admin {
      ip 192.168.0.1
]
# Poste de toto
src toto {
      ip 192.168.0.50
```

Nicolas Dewaele
nico@nicodewaele.info
www.nicodewaele.info

```
}
# Postes de la salle Lady
src sallelady {
      ip 192.168.0.100-192.168.0.125
}
### Déclaration des destinations (bases de données de sites interdits)

# Base de donnée sites pour adultes (dont liste de domaines et liste
d'URL)
dest adult {
      domainlist adult/domains
      urllist adult/urls
}

# Base de donnée sites de pub (dont liste de domaines et liste d'URL)
dest publicite {
      domainlist publicite/domains
      urllist publicite/urls
}

# Base de donnée sites de warez (dont liste de domaines et liste d'URL)
dest warez {
      domainlist warez/domains
      urllist warez/urls
}

# Base de donnée sites pornographiques (dont liste de domaines et liste
d'URL)
dest porn {
      domainlist porn/domains
      urllist porn/urls
}
```

```
### Application des listes d'accès (ACL) : Elles font le lien entre
### un groupe de machines et une ou plusieurs bases de données.
acl {
      admin {
            # L'administrateur à le droit de tout voir
            pass all
      }

      toto {
            # Toto ne peut voir les sites pornographiques
            # ni ceux destinés aux adultes mais peut voir les autres
            pass !porn !adult all
            # Si il va sur un site interdit, il est redirigé vers ce site
            redirect http://www.mynetcourse.info/interdit.html
      }

      sallevon {
            pass !porn !adult !publicite !warez all
            redirect http://www.mynetcourse.info/interdit.html
      }
```

Nicolas Dewaele
nico@nicodewaele.info
www.nicodewaele.info

```
default {
        # Les autres n'ont rien le droit de voir
        pass none
        redirect http://www.mynetcourse.info/interdit.html
}
```

Derniers paramétrages :

Pour activer vos listes de sites interdits, tapez la commande:

```
squidGuard -C all
```

Enfin il faut dire à Squid d'utiliser SquidGuard, en ajoutant cette ligne au début du fichier **/etc/squid/squid.conf**:

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

V- Sites Internet sur le sujet :

Comprendre le rôle du proxy :

http://www.ac-creteil.fr/reseaux/internetlinetlproxy/default.htm

Tout savoir sur Squid :

http://www.ac-creteil.fr/reseaux/internetlinetiproxy/Squid/default.htm
http://squid.visolve.com/squid/configuration_manual.htm
http://www.linux-france.org/prj/edu/archinet/systeme/c7156.html

Configuration de Squid et SquidGuard :

http://christian.caleca.free.fr/squid/
http://www.niemueller.de/webmin/modules/squidguard/
http://www.trustnome.net/didactels/295.html