

Fiche   
Proxy HTTP - squid

Département d’informatique  
Collège de Maisonneuve  
3800 est, rue Sherbrooke,  
Montréal (Québec) H1X 2A2  
514.251-7131 poste 4800

Document proposé par Louis Savard, M. Ing. TI  
Dernière révision : Novembre 2019

Table des matières

[Proxy HTTP 3](#_Toc24526105)

[Installation du service 3](#_Toc24526106)

[Configuration du proxy 3](#_Toc24526107)

[Visualisation du fichier de configuration 3](#_Toc24526108)

[Test de la connectivité du serveur proxy 3](#_Toc24526109)

[Vérification de la syntaxe du fichier */etc/squid/squid.conf* 5](#_Toc24526110)

[Définition des droits d'accès 5](#_Toc24526111)

[Démarrage du proxy 7](#_Toc24526112)

[Ajout de règles de filtrage 7](#_Toc24526113)

[Modification de la mise en cache de squid 7](#_Toc24526114)

[Informations supplémentaires 9](#_Toc24526115)

[Document adapté des sites web 9](#_Toc24526116)

[Annexe 01   
Authentification des utilisateurs pour pouvoir accéder à squid 10](#_Toc24526117)

[Exercices 11](#_Toc24526118)

# Proxy HTTP

squid est un serveur mandataire (proxy) et un serveur mandataire inverse capable d'utiliser les protocoles FTP, HTTP, Gopher, et HTTPS.   
Contrairement aux serveurs proxy classiques, un serveur squid gère toutes les requêtes en un seul processus d'entrée/sortie, non bloquant.

squid garde les meta-données et plus particulièrement les données les plus fréquemment utilisées en mémoire. Il conserve aussi en mémoire les requêtes DNS, ainsi que les requêtes ayant échoué.   
Les requêtes DNS sont toutefois non bloquantes.

Les données mémorisées peuvent être rangées en hiérarchies ou en mailles afin d’utiliser moins de bande passante.

## Installation du service

Pour installer squid, on utilise la commande …   
# sudo apt install squid

Pour vérifier si le service est démarré …

# sudo ps aux | grep squid  
ou  
# sudo service --status-all  
# sudo systemctl list-units --type=service

## Configuration du proxy

Par défaut Squid est configuré et fonctionnel. Cependant, on peut apporter quelques modifications afin de l'optimiser ou mieux l'adapter à certains environnements.  
La configuration de squid se fait en éditant le fichier /etc/squid/squid.conf.

### Visualisation du fichier de configuration

# sudo cat /etc/squid/squid.conf

Il peut être intéressant de faire une sauvegarde du fichier original de configuration avant d’y effectuer des modifications.  
# sudo cp /etc/squid/squid.conf{,.original}

Pour épurer le fichier de configuration …  
# sudo cd /etc/squid  
# sudo cat squid.conf.original | egrep -v -e '^[[:blank:]]\*#|^$' > squid.conf  
ou   
# sudo egrep -v -e '^[[:blank:]]\*#|^$' squid.conf

Pour éditer ce fichier …   
# sudo nano /etc/squid/squid.conf

### Test de la connectivité du serveur proxy

À partir de là, le proxy devrait fonctionner. Il suffit de configurer les différents fureteurs pour qu'ils l'utilisent.

**Remarque** …  
Par défaut, le proxy squid est exécuté sur le port 3128. Il suffit de modifier le port si tel n’est pas le cas.  
  
On peut utiliser pour ce faire une simple requête curl …  
# curl -x http://<Adresse IP du serveur>:<port> -L <http://google.com># curl -x http://localhost:3128 -L http://google.com

**Exemple de fichier de configuration de base */etc/squid/squid.conf***

|  |
| --- |
| acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN) acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN) acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN) acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN) acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN) acl localnet src fc00::/7 # RFC 4193 local private network range acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines  acl SSL\_ports port 443 # https 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 CONNECT method CONNECT  http\_access deny !Safe\_ports http\_access deny CONNECT !SSL\_ports http\_access allow localhost manager http\_access deny manager  include /etc/squid/conf.d/\*  http\_access allow localhost http\_access deny all http\_port 3128  coredump\_dir /var/spool/squid  refresh\_pattern ^ftp: 1440 20% 10080 refresh\_pattern ^gopher: 1440 0% 1440 refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0 refresh\_pattern . |

**Nom du proxy**squid a besoin de connaître le nom de l’hôte sur lequel il est installé afin d’afficher ce nom de d’hôte dans les messages d’erreur ...   
Pour ce faire, on repère la ligne **visible\_hostname** (si elle elle existe) et la remplace par le nom du serveur …   
**# …  
visible\_hostname ProxyWebMaisonneuve  
# …**

**Choix du port**  
Par défaut, le serveur proxy sera en écoute sur le port 3128.  
Pour choisir un autre port, on repère la ligne …  
**http\_port 3128**  
et on modifier le numéro de port … curl -  
**# …**  
**http\_port 3177**  
**# …**

**Choix de l'interface**Par défaut le serveur proxy sera en écoute sur toutes les interfaces.   
Pour des raisons de sécurité, il ne faut le mettre en écoute que sur son réseau local …  
Par exemple, si l’interface réseau reliée au réseau local possède l'adresse IP 206.167.46.112 …   
**# …  
http\_port 206.167.46.112.1.0:3177  
# …**

### Vérification de la syntaxe du fichier */etc/squid/squid.conf*

Avant d'essayer de démarrer squid, il est préférable de vérifier que le fichier squid.conf a du sens.   
Cela est facile à faire. Il suffit de lancer la commande …  
# sudo squid -k parse

La sortie indique clairement si le fichier est correct ou non.   
En cas d’erreur, la sortie va en préciser la nature.

### Définition des droits d'accès

Les restrictions indiquent quoi faire lorsque ces conditions sont vérifiées.   
On autorise ou on interdit en fonction d'une ACL ou d'un groupe d'ACLs, le sens de « restriction » est donc à prendre avec un peu de recul, une restriction pouvant être une autorisation.

La première restriction vérifiée est la bonne, d'où l'importance de l'ordre dans lequel elles sont placées.   
Les autres restrictions seront alors systématiquement ignorées.

**Autorisation des hôtes du réseau local**

Sans faire une analyse détaillée, on voit que dans la configuration par défaut, seul *localhost* peut utiliser le proxy (**http\_access allow localhost**).   
Si cette condition n'est pas respectée, la règle suivante étant **http\_access deny all**, personne ne passera.   
Il faut donc faire intervenir la notion de réseau local.

Bien entendu, l'idée de faire plutôt Allow all est une mauvaise idée.   
Si le proxy possède un interface réseau connecté vers Internet (s'il est installé sur la passerelle par exemple), on risque d’avoir un proxy ouvert, avec tous les usages pervers que l'on peut en faire.  
C’est pourquoi par défaut, personne n'est autorisé à se connecter au serveur proxy, sauf l’hôte lui-même.

Afin de modifier cet état, il faut créer une liste d'autorisations.   
Par exemple, on va définir un groupe englobant tout le réseau local.

Dans un premier temps, on va commenter toutes les lignes en début de fichier commençant par …  
**# acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)  
…**

On va définir par la suite son réseau local …  
**# …  
acl localnet src 206.167.46.0/24 # réseau local (LAN)  
# …**

On repère la ligne du fichier commençant par **http\_access allow localhost** et on modifie la ligne comme suit …  
**# …  
http\_access allow localnet  
# …**

**Note** …  
localnet est un nom arbitraire.

**Méthode alternative**  
Si tous les clients qui utiliseront le proxy ont une adresse IP statique, l'option la plus simple consiste à créer une liste de contrôle d'accès qui inclut les adresses IP autorisées.

Au lieu d'ajouter les adresses IP dans le fichier de configuration principal, il est possible de créer un nouveau fichier d'inclusion qui stockera les adresses IP …  
# nano /etc/squid/ips\_autorisees.txt  
**206.167.46.101**  
**# Toutes les autres adresses IP autorisées**

Une fois cela fait, on ouvre le fichier de configuration principal et on crée une nouvelle ACL nommée ips\_aotoriseeset et on autorise l'accès à cette ACL à l'aide de la directive http\_access …  
**# …acl ips\_autorisees src "/etc/squid/ips\_autorisees.txt"  
# …  
# …**  
**http\_access allow ips\_autorisees  
# …**  
  
# On interdit l’accès à toutes les autres adresses au proxy   
**# …  
http\_access deny all  
# …**

**Rappel** …  
L'**ordre des** **règles http\_access** est important.   
Il est important de s’assurer d’ajouter la bonne ligne avant que http\_access refuse tout.

La **directive http\_access** fonctionne de la même manière que les règles de pare-feu.   
squid lit les règles de haut en bas et, lorsqu'une règle correspond, les règles qui suivent ne sont pas traitées.

**Autorisation des ports non standards**

Par défaut, squid n'autorise le trafic HTTP(S) que sur certains ports (TCP 80, TCP 443, ...).   
Il existe une liste (lignes commençant par acl Safe\_ports port …) de ports autorisés.  
Cela peut poser un problème pour certains sites web utilisant d'autres ports (comme un site de l’intranet).   
(Exemple … http://maisonneuve.info:8080/images/logo.png serait bloqué par squid).

Pour ajouter un port autorisé …  
# …  
acl Safe\_ports port 8080 # Serveur web interne  
# …

Une autre méthode permettant d’éviter ce blocage, serait de commenter la ligne visant à débloquer tous les ports non sécures.

On identifie la ligne …  
**http\_access deny !Safe\_ports**et on la commente …  
# …  
# http\_access deny !Safe\_ports  
# …

**Remarque** …  
Il est aussi possible d’ajouter d’autres ports sur le même modèle de la liste.

### Démarrage du proxy

On redémarre squid pour qu'il prenne en compte la configuration modifiée …  
# sudo systemctl reload squid  
ou  
# sudo systemctl restart squid

### Ajout de règles de filtrage

Il est possible d’interdire tous les accès avec la règle …  
**# …  
http\_access deny all  
# …**

**Mise en place d'ACL simple**

Il est possible d’Interdire l'accès à un serveur particulier (facebook.com par exemple) …  
**# …  
acl facebook dstdomain facebook.com  
# …**

Il faut par la suite indiquer à qui cette restriction s'impose …  
**# …  
http\_access deny nocalnet facebook  
# …**

Afin de bloquer une listre de sites à l’aide d’un ficher, il faut ajouter ces lignes …  
**# …  
acl liste\_url dstdomain "/etc/squid/liste-sites.txt"  
http\_access deny liste\_url  
# …**

On doit par la suite créer le **fichier /etc/squid/liste-sites.txt** et y ajouter les sites web èa bloquer …  
**.youtube.com  
.facebook.com**

**Définition d’une période de temps d'utilisation**  
Afin d’imposer des restrictions basées sur une période de temps, on peut créer une acl …  
**# …  
acl jour time 08:00-17:30  
# …**

Une période de temps nommé jour est définie de 8h00 à 17h30.

Il faut par la suite indiquer à qui (l’objet) cette restriction s'impose …  
**# …  
http\_access allow localnet jour  
# …**

En dehors de cette étendue, le proxy refusera la connexion.

### Modification de la mise en cache de squid

**Mise en cache de page web**

Par défaut, le tampon de squid est activé, ce qui permet d'accélérer le chargement de certaines pages.   
La taille par défaut est de 100 Mo (situé dans /var/spool/squid).

Pour modifier sa taille, on édite le fichier /etc/squid/squid.conf …  
**# …  
cache\_dir ufs /var/spool/squid 100 16 256  
# …**

On peut modifier la valeur 100 par ce que l’on veut (par exemple 200 pour 200 Mo.

Dans l’exemple précédent …

* **100**  
  La quantité d'espace disque à utiliser en Mo pour le répertoire de mise en cache ;
* **16**  
  Les sous-répertoires de premier niveau qui seront créés dans le répertoire de cache ;
* **256**  
   Le nombre de sous-répertoires de deuxième niveau qui seront créés sous chaque répertoire de premier niveau.

Afin de modifier la taille maximum de mémoire vive utilisée pour stocker le tampon …  
**# …  
cache\_mem 16 MB  
# …**

Pour modifier la taille maximum des objets stockés dans le tampon …  
**# …  
maximum\_object\_size 15 MB  
# …**

**Mise en cache DNS**

Par defaut, squid est configuré pour garder 6 heures le tampon DNS dont il a pu résoudre le nom et 5 minutes celui dont il n'a pas pu résoudre le nom DNS.

Modification du temps de tampon pour la résolution de nom positive …  
**# …  
positive\_dns\_ttl 8 hours  
# …**

Modification du temps de tampon pour la résolution de nom négative …  
**# …  
negative\_dns\_ttl 4 minutes  
# …**

### Informations supplémentaires

**Journalisation du service**Les journaux du proxy sont situés dans /var/log/squid/access.log.

**Redémarrage du service squid**Un redémarrage de squid peut être long. Par défaut ce délai est de 30 secondes.

Afin de modifier ce temps, on peut indiquer à squid d'attendre 4 secondes avant de fermer les connexions existantes lors de l’arrêt ou du redémarrage.  
**# …  
shutdown\_lifetime 4 secondes  
# …**

**Messages d'erreur en français**Dans la partie TAG: error\_directory, modifier ou ajouter la ligne comme suit …  
**# …  
error\_directory /usr/share/squid/errors/French  
# …**

**Fonctions et modules supplémentaires**squid possède plein d'options et modules …

* **préfetch** (pour précharger les pages et ainsi accélérer la navigation) ;
* **filtres** antivirus, antipopups, … ;
* **contrôle** d'accès au proxy par login et mot de passe ;
* **contrôle** d'accès en fonction des heures ;
* …

squid est aussi paramétrable avec **webmin**.

### Document adapté des sites web

* <http://www.commentcamarche.net/faq/6323-installer-un-serveur-proxy-http-squid>
* <http://www.linux-france.org/prj/edu/archinet/systeme/ch41.html>
* <http://fr.wikipedia.org/wiki/Squid_(logiciel)>
* <http://www.linuxpedia.fr/doku.php/expert/proxy-squid>
* <http://irp.nain-t.net/doku.php/220squid:020_squid>
* <http://irp.nain-t.net/doku.php/220squid:020_squid>

# 

# Annexe 01 Authentification des utilisateurs pour pouvoir accéder à squid

Pour mettre en place le système d’authentification, squid utilise la méthode htpasswd disponible avec le paquet apache2-utils, il faut donc dans un premier temps installer ce paquet …  
# sudo apt install apache2-utils

Ensuite, il faut créer un fichier où seront déclarés les utilisateurs et leur mot de passe …  
# sudo nano /etc/squid/utilisateurs

On peut désormais déclarer des utilisateurs dans ce fichier grâce à la commande suivante …  
# sudo htpasswd –b /etc/squid/utilisateurs <Nom utilisateur> <Mot de passe>

Exemple …  
htpasswd –b /etc/squid/utilisateurs tux bingo

Le fichier utilisateurs s’est donc remplit sous la forme : <Nom utilisateur:Mot de passe>

**Remarque** …  
Le mot de passe est chiffré.

Avant d’indiquer à Squid qu’il doit utiliser ce système d’authentification, il faut valider voir si celui fonctionne …  
# sudo /usr/lib/squid/ncsa\_auth /etc/squid/utilisateurs  
Il faut saisir le nom de l’utilisateur suivi de son mot de passe (séparé par un espace)  
tux bingo

Si on a saisi les bonnes informations, le programme devrait vous retourner **OK**, sinon **Err**.

Il ne reste plus qu’à indiquer à quid qu’il doit utiliser ce programme d’authentification en modifiant le fichier /etc/squid/squid.conf …  
**# On déclare le programme qui gère l'authentification :  
auth\_param basic program /usr/lib/squid/ncsa\_auth /etc/squid/utilisateurs  
  
# Grâce à cette ACL, le Proxy demandera une authentification  
acl utilisateurs proxy\_auth REQUIRED**

**# Refuser l'accès à tous les utilisateurs sauf ceux du fichier Utilisateurs  
http\_access deny !utilisateurs**

Il faut redémarrer le service squid.   
# sudo systemctl restart|relaod squid

**Méthode alternative**

squid peut utiliser différentes méthodes d’identification, notamment l’authentification de base Samba, LDAP et HTTP pour les utilisateurs authentifiés.

Il est donc possible de configurer squid afin qu’il utilise l’authentification de base.   
C'est une méthode d'authentification simple intégrée au protocole HTTP.

L'utilitaire openssl permet de générer les mots de passe et ajouter la paire nom d'utilisateur:mot de passe au fichier /etc/squid/htpasswd à l'aide de la commande tee …  
# printf "USERNAME:$(openssl passwd -crypt <Mot de passe>)\n" | sudo tee -a /etc/squid/htpasswd

Pour créer un utilisateur nommé buster avec le mot de passe qwerty12345 …  
# printf "buster:$(openssl passwd -crypt 'qwerty12345')\n" | sudo tee -a /etc/squid/htpasswd  
Warning: truncating password to 8 characters  
buster:I6g7UmtUyYA9c

L'étape suivante consiste à activer l'authentification de base HTTP.   
On accède au fichier de configuration et on ajoute …  
**# …  
auth\_param basic program /usr/lib/squid3/basic\_ncsa\_auth /etc/squid/htpasswd  
auth\_param basic realm proxy  
acl authenticated proxy\_auth REQUIRED  
# ...**

**# …  
http\_access allow authenticated  
# ...**

# Exercices

**Question 01**Qu'entendez-vous par serveur proxy ?   
Quelle est l'utilisation d’un serveur proxy web dans les réseaux informatiques??

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |

**Question 02**Quel est le port par défaut de squid et comment modifier son port d’exploitation ?

|  |
| --- |
|  |
|  |
|  |
|  |

**Question 03**Vous travaillez pour une entreprise dont la gestion vous demande de bloquer certains domaines à l’aide d’un serveur proxy squid.   
Comment allez-vous faire ?

|  |
| --- |
|  |
|  |
|  |
|  |

**Question 04**squid peut être utilisé en tant que démon de cache Web.  
Qu’est-ce que cela signifie ?  
Est-il possible d'effacer son cache ? Comment ?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Question 05**Un de vos client vous demande s’il est possible de limier le temps d'accès au Web pour l’ensemble de ses employés.  
Comment pouvez-vous réaliser ce scénario ?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Question 06**Squid stocke les données dans quel format de fichier ?  
Décrivez ce type de format.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Question 07**Il est possible de configurer squid afin qu’il autorise seulement certains utilisateurs.  
Quel utilitaire d’Apache lui permet de le faire ?  
Donnez les principales étapes de configuration.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |