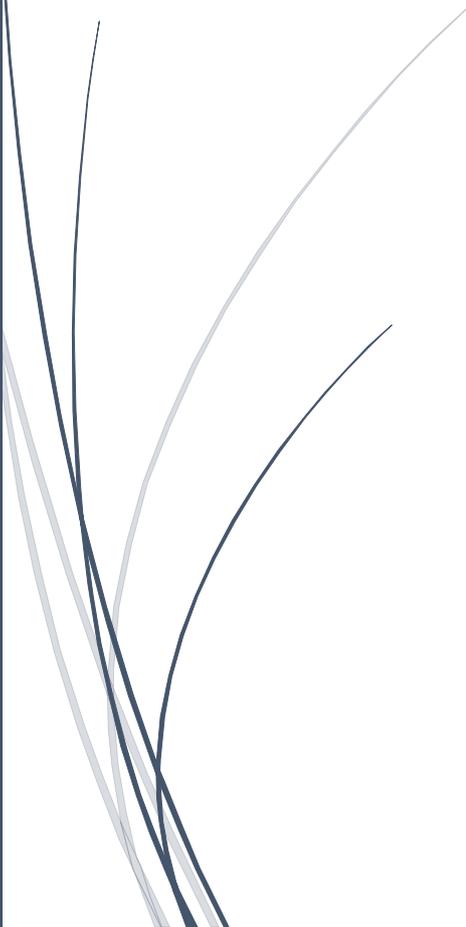


05/10/2015

Installation d'un proxy (SQUID

v1



Lecaudey Etienne

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

SOMMAIRE :

Table des matières

Table des matières	2
Objectifs :	3
<i>Information sur les versions:</i>	3
<i>Installation des services :</i>	3
<i>Configuration de base :</i>	3
Les contrôles d'accès (ACL) :	4
Authentification des utilisateurs	5
Touch /etc/squid3/squidusers	5
SquidGuard :	6
Analyseur de log Lightsquid :	7
Test du serveur proxy mandataire :	8

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Objectifs :

L'objectif de cette procédure est de procéder à l'installation du serveur proxy mandataire Squid et du filtrage à l'aide de SquidGuard.

Information sur les versions:

VM	Debian 8.1	Jessie	SQUID	192.168.1.126
SQUID	3.5			

Installation des services :

Avant toute Installation, il faut réaliser une mise à jour des paquets :

```
apt-get update
```

Puis on peut installer Squid et les autres paquets :

```
root@debian8:/# aptitude install squid3 apache2_
```

Configuration de base :

Lorsque Squid est installé, le proxy bloque toutes les connexions de base, nous devons le paramétrer pour pouvoir accéder aux pages internet

Pour commencer nous allons copier le fichier squid.conf pour en faire un backup :

```
root@debian8:/etc/squid3# cp squid.conf squid.conf.bak_
```

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Puis dans le fichier squid.conf nous allons enlever toutes les phrases commençant par « # » et par « \$ » :

```
root@debian8:/etc/squid3# cat squid.conf.bak | grep -v ^# | grep -v ^$ > squid.conf_
```

Ensuite à la fin du fichier squid.conf, rajoutez les lignes suivantes :

```
#utilisateur faisant les requêtes sur le serveur
cache_effective_user proxy
cache_effective_group proxy

#Emplacement de stockage des données et réglage des niveaux
cache_mem 16 MB
cache_dir ufs /var/spool/squid3 120 16 128
```

Pour la dernière ligne, les variables désigne :

- Ufs = type du système
- Emplacement du cache
- 120Mo = taille du cache

- 16= nombre de répertoire de niveau 1
- 128 = nombre de répertoire de niveau 2

Après ces premières configurations ; le serveur proxy mandataire bloque toujours les connexions.

Pour débloquer cette situation, nous allons voir les ACL

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Les contrôles d'accès (ACL) :

Pour Squid, les ACL permettent de définir des conditions sur les adresses IP, les ports, le contenu de certains textes, etc.

- Autoriser l'utilisation du proxy pour le réseau local

Ajouter la définition ACL pour votre réseau local juste avant la ligne `acl localhost` puis l'autorisation comme premier `http_access` :

#tout en haut du fichier

```
acl lan src 192.168.1.0/24
```

#Ajout du droit AU-DESSUS des autres `http_access`

```
http_access allow lan
```

L'ordre des ACL est très important

- Contrôle d'accès horaire

```
acl allowed_hosts src 192.168.1.12
acl limit_hour time 16:00-17:30
http_access allow allowed_hosts limithour_
```

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Authentification des utilisateurs

Touch /etc/squid3/squidusers

Htpasswd -b /etc/squid3/squidusers [user] [mot de passe]

Htpasswd -b /etc/squid3/squidusers [user] [mdp]

Ensuite, modifiez le fichier /etc/squid3/squid.conf :

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/squidusers
auth_param basic children 5
auth_param basic realm Squid proxy 2A
authenticate_ttl 1 hour
authenticate_ip_ttl 60 seconds
acl utilisateurs proxy_auth REQUIRED
acl lan src 192.168.1.0/24
acl SSL_ports port 443
```

```
acl CONNECT method CONNECT
http_access allow utilisateurs
http_access allow lan
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
```

Les options commençant par Authenticate spécifient le temps de connexion de l'utilisateur avant une nouvelle demande du mot de passe et l'intervalle de connexion pour des ordinateurs différents sur lesquels un même utilisateur peut se connecter.

Ensuite, nous devons donner les droits pour les fichiers basic_ncsa_auth avec :

```
chown proxy:shadow /usr/lib/squid3/basic_ncsa_auth_
```

```
chmod 2750 /usr/lib/squid3/basic_ncsa_auth_
```

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

SquidGuard :

SquidGuard permet de mettre en place des fonctions avancées de filtrage, par exemple en mettant en place une blacklist permettant de bloquer l'accès à certains sites web.

```
oot@debian8:/etc/squid3# aptitude install squidguard_
```

Pour mettre en place une blacklist, nous allons prendre celle de l'Université Toulouse 1 Capitole qui récence énormément de sites web sensible.

Pour cela, nous utilisons la commande suivante :

```
root@debian8:/etc/squid3# wget http://cri.univ-tlse1.fr/blacklists/download/blacklists.tar.gz_
```

Ensuite, dans le fichier /etc/squid/squidguard.conf

Tape ceci (en fonction de l'utilité) :

```
#emplacement du répertoire contenant les listes de blocages
dbhome /var/lib/squidguard/db/blacklists

#emplacement du répertoire de log de Squid
logdir /var/log/squid3

#Définition de la plage d'adresses IP du réseau local
src lan {
    ip 192.168.1.1-192.168.1.254
}

#Définition d'une catégorie de site
dest games {
    domainlist games/domains
    urllist games/urls
}

#définition de la zone locale
dest local {
}

#Définition de l'attitude a adopter pour le réseau local
#Blocage des sites de jeu
#autorisation des sites locaux
acl {
    lan {
        pass !games all
        redirect http://127.0.0.1/proxy.html
    }
    default {
        pass local none
    }
}
```

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Pour la capture d'écran ci-dessus, on interdit l'accès à une destination (les sites pour les jeux) et les acl dans le fichier de SquidGuard

Ensuite, dans le fichier /etc/squid3/squid.conf, on ajoute la ligne permettant de rediriger Squid vers SquidGuard et pour indiquer le nombre de processus engendré

```
#redirigier Squid vers SquidGuard
url_rewrite_program /usr/bin/squidGuard
url_rewrite_children 5

visible_hostname debian8
```

Ensuite, nous allons reconstruire la base de données de la liste noir pour SquidGuard après l'avoir dé-tarrer

```
root@debian8:/var/lib/squidguard/db# tar zxvf blacklists.tar.gz _
```

```
root@debian8:/var/lib/squidguard/db# squid guard -C all -d /var/lib/db_
```

Puis après nous allons donner les droits à l'utilisateur proxy du groupe proxy

```
root@debian8:/var/lib/squidguard/db# chown -Rf proxy:proxy /var/lib/squidguard/d
0_
```

Ensuite, nous devons créer une page HTML que l'utilisateur verra lorsqu'il ira sur un site bloqué par le proxy à placer dans /var/www/html

Maintenant nous allons redémarrer Squid :

```
root@debian8:/var/lib/squidguard/db# service squid3 restart_
```

Maintenant, nous tentons l'accès au site : www.game.fr



Connexion refusée, veuillez contacter votre administrateur réseau

Nous pouvons voir que le proxy Squid est en place et n'accepte pas la connexion au site.

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Analyseur de log Lightsquid :

Nous commençons par installer un paquet pour apache2 :

```
root@debian8:/# aptitude install libgd-gd2-perl
```

Puis, avec la commande WGET nous téléchargeons le paquet de Lightsquid et nous le mettons dans le /var/www/html

```
root@debian8:/var/www/html# wget http://sourceforge.net/projects/lightsquid/files/latest/download?source=files_
```

Le paquet sera installé mais n'aura pas un nom explicite donc nous le renommons puis on le décompresse

```
root@debian8:/var/www/html# ls
download?source=files proxy.html
root@debian8:/var/www/html# mv download\?source\=files lightSquid.tgz
root@debian8:/var/www/html# tar zxvf lightSquid.tgz
```

Maintenant, nous nous assurons que le mod perl et CGI sont activé :

```
root@debian8:/var/www/html# a2enmod cgi && a2enmod perl
```

Ensuite, nous rendons tous les scripts pl et cgi exécutable et changeons le propriétaire du répertoire Lightsquid :

```
root@debian8:/var/www/html# chmod -R ugo+x lightsquid/*.cgi
root@debian8:/var/www/html# chmod -R ugo+x lightsquid/*.pl
root@debian8:/var/www/html# chown -R www-data:www-data lightsquid/
```

Ensuite, nous devons configurer apache2 pour pouvoir lancer Light squid :

```
root@debian8:/# nano /etc/apache2/sites-available/000-default.conf
```

Et insérez entre les balises Virtual host :

```
<Directory "/var/www/html/lightsquid">
    AddHandler cgi-script.cgi
    AllowOverride All
    DirectoryIndex index.cgi
    Options +ExecCGI
</Directory>
```

Puis nous redémarrons Apache2 :

Service apache2 restart

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Ensuite, dans le fichier lightsquid.cfg (/var/www/html/lightsquid)

Nous devons remplacer la variable « \$logpath »

Par « \$logpath= »/var/log/squid3 »

Et \$lang= »eng » en \$lang= »fr »

Tester la configuration avec ./check-setup.pl

```
root@debian8:/var/www/html/lightsquid# ./check-setup.pl
```

Et si nous n'avons pas de message d'erreur, nous Parons le fichier de log de squid avec :

```
root@debian8:/var/www/html/lightsquid# ./lightparser.pl
```

Ensuite, tester l'accès à l'aide d'un navigateur : http://ip_du_serveur

Squid rapport d'accès utilisateur
Periode de travail: Oct 2015

Calendar											
2015											
01	02	03	04	05	06	07	08	09	10	11	12

Top Sites	Total	Groupe
ANNEE	ANNEE	ANNEE
MOIS	MOIS	MOIS

Date	Groupe	Utilisateurs	Quota Dépassé	Octets	Moyenne	Hit %
06 Oct 2015	grp	1	0	2.4 M	2.4 M	0.02%
05 Oct 2015	grp	3	2	45.2 M	15.1 M	0.02%
Total/Moyenne:		2	1	47.6 M	8.8 M	0.02%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

Nous pouvons voir que LightSquid est en place avec cette interface graphique

Ensuite, pour sécuriser l'accès à ces données qui sont sensibles, nous pouvons verrouiller l'accès grâce à Httaccs.

Configuration d'un navigateur par un script :

Pour configurer les navigateurs de manière à ce qu'ils utilisent le proxy, il y a deux méthodes :

- Faire le tour des PC et paramétrer un à un les navigateurs
- Utiliser un script de configuration

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Nous allons maintenant utiliser la deuxième solution, pour cela, nous allons créer un script qui sera écrit en JavaScript nommé proxy.pac, pour cela, nous nous plaçons dans /var/www/html

Et nous allons créer le fichier avec « nano »

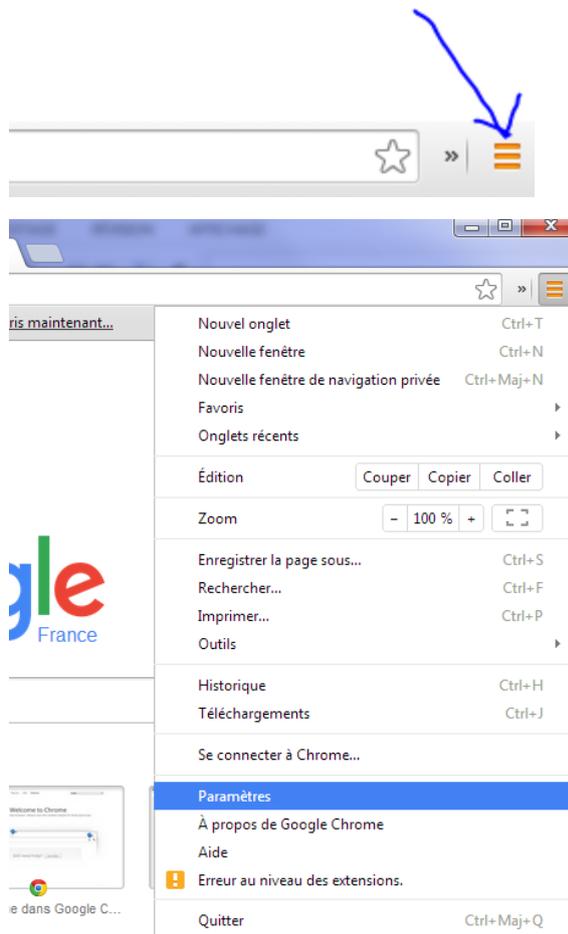
```
root@debian8:/var/www/html# nano proxy.pac_
```

Et écrivons cette commande :

```
GNU nano 2.2.6          Fichier : proxy.pac          Modifié
function FindProxyForUrl(url,host)    {
    return "PROXY 192.168.1.126:2128;DIRECT";
}
#Veillez à mettre l'adresse IP de votre proxy_
```

Puis, une fois le script écrit, nous devons l'insérer dans le navigateur

Nous devons aller dans le navigateur (Google chrome pour cette procédure)



Réseau

Google Chrome utilise les paramètres proxy du système pour se connecter au réseau.

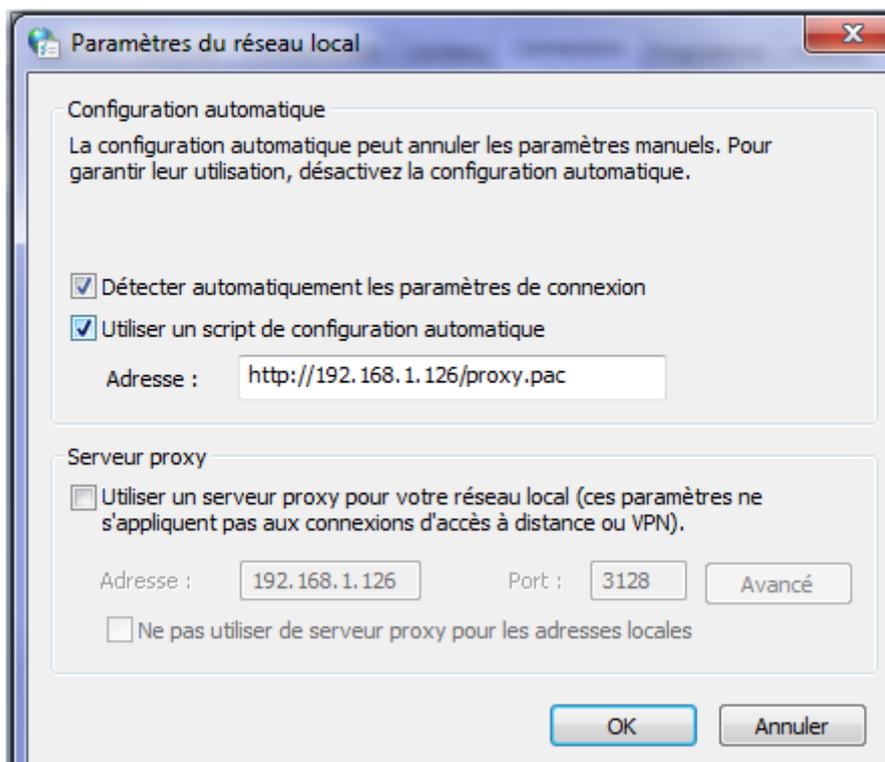
[Modifier les paramètres du proxy...](#)

Tutoriel 1.1 : Installation et configuration d'un proxy sous SQUID		
Lecaudey Etienne	Version 1.0	05/10/2015

Paramètres de réseau local

Les paramètres de réseau local ne s'appliquent pas aux connexions d'accès à distance. Cliquez sur Paramètres pour définir les options de numérotation.

Paramètres réseau



Avec la dernière image, nous avons le choix de soit :

Mettre un script ou mettre une IP fixe pour le proxy