Table des matières :

Avant-Propos

Compétences :

- A1.1.1 Analyse du cahier des charges d'un service à produire
- A1.2.4 Déterminer des tests nécessaires à la validation d'un service (3)
- A4.1.9 Rédaction d'une documentation technique

Le terme proxy se traduit littéralement par le mot procuration mais on lui préfère celui de mandat. Un serveur proxy se définit donc comme un serveur mandataire réalisant à votre place des requêtes réseaux protocolaires comme par exemple http ou encore FTP.

Principalement un serveur proxy sert :

- A mettre en cache des éléments (images, pages HTML)
- A filtrer des données.

Un proxy agit selon deux modes différents, serveur ou transparent :

- En mode serveur, une modification se fera dans les paramètres de connexion du navigateur des postes clients afin d'indiquer l'adresse du serveur et le port sur lequel il doit s'y connecter.
- En mode transparent, aucune modification n'est nécessaire sur le poste client mais il ne peut plus y avoir alors demande d'authentification utilisateur.

Objectif :

Dans cette procédure, nous allons montrer comment installer et configurer un serveur Proxy-Mandataire sous Debian.

OS	Distribution	Version
Debian	Linux	8.5

1. Installation de Squid :

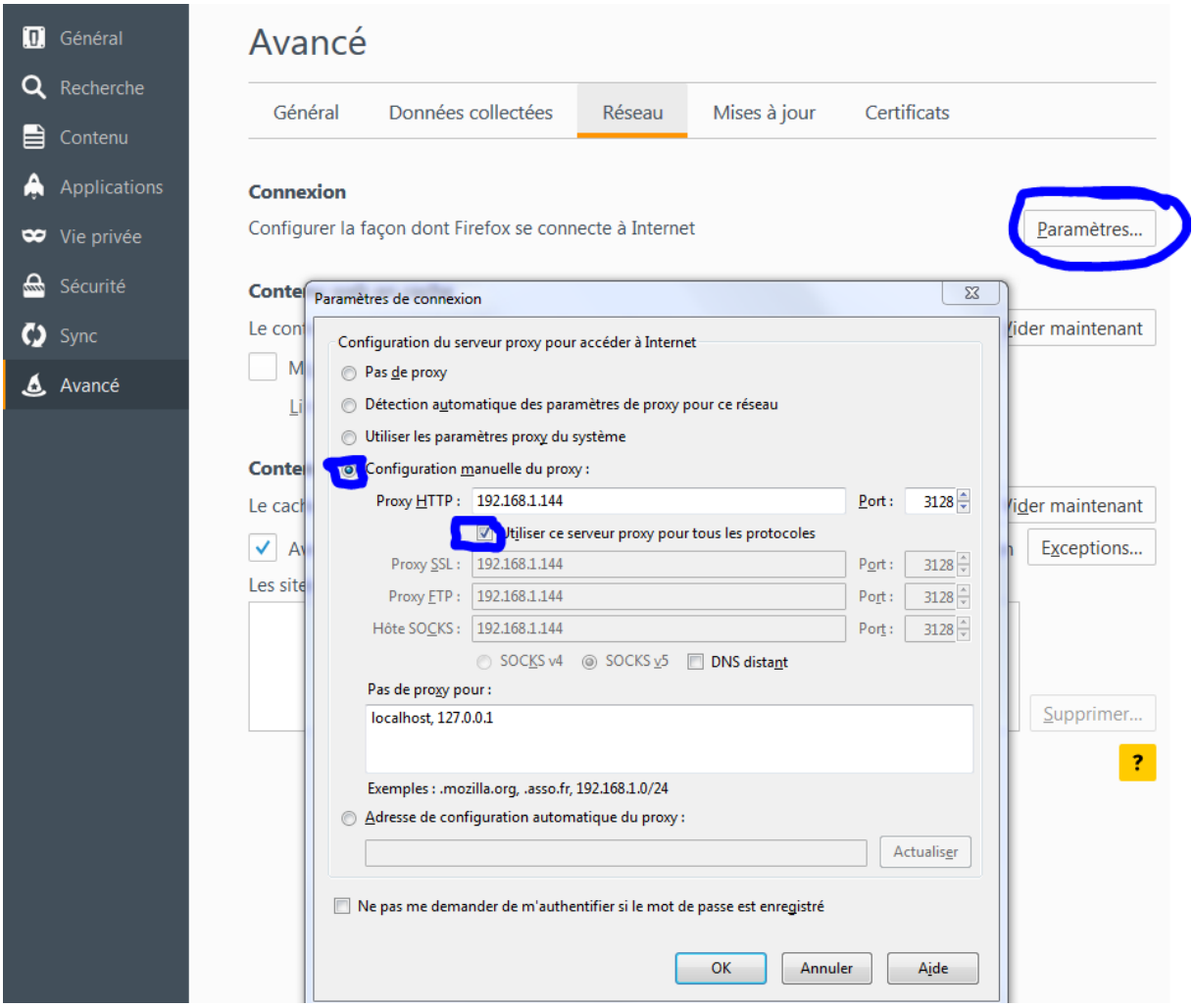
apt update

apt upgrade

Apt install squid3

Pour vérifier les groupes d'utilisateur : « cat /etc/passwd »

2. Configuration de base :



On remarque que internet ne marche plus.

On peut consulter le fichier de log pour constater notre erreur. On peut aussi utiliser la commande « tail »

```
root@debian8:~# cat /var/log/squid3/access.log_
```

```
1473662401.101      0 192.168.1.60 TCP_DENIED/403 3611 CONNECT www.google.fr:443
 - HIER_NONE/- text/html
```

On effectue ensuite une copie du fichier squid.conf

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

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

On rajoute les lignes de commandes suivantes dans le fichier squid.conf

```
# 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
visible_hostname<nom d'hôte>_
```

On peut mettre un nom d'hote :

```
  GNU nano 2.2.6               Fichier : squid.conf

refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320

# 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
visible_hostname PROXY_Mariette
```

On redémarre le service squid

```
root@debian8:/etc/squid3# systemctl restart squid3
_
```

On peut ensuite aller consulter les messages

```
root@debian8:/etc/squid3# cd /var/spool/squid3/
root@debian8:/var/spool/squid3# ls
00  01  02  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F  swap.state
```

3. Les contrôles d'accès :

On vérifie que notre distribution supporte les ACL

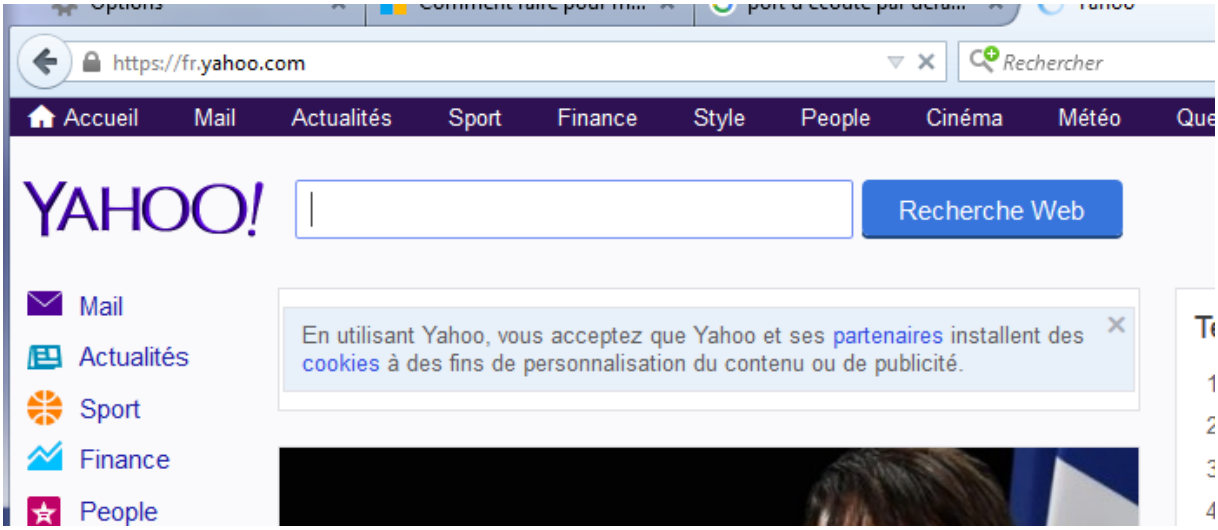
« cat /boot/config_version_noyau | grep ACL »

```
root@debian8:/var/spool/squid3# cat /boot/config-3.16.0-4-amd64 | grep ACL
```

On retourne dans le fihcier squid.conf

```
  GNU nano 2.2.6               Fichier : squid.conf

acl lan src 192.168.1.0/24
acl SSL_ports port 443
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
# Ajout du droit AU-DESSUS des autres http_access
http_access allow lan
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
```

On test une recherche sur internet pour vérifier que sa marche :



On a modifié les commandes ACL et http_access

ACL est là pour crée la règle

http_access pour appliquer la règle

Contrôle d'accès horaire :

On peut alors autoriser une machines a se connecter

```
  GNU nano 2.2.6               Fichier : squid.conf

acl lan src 192.168.1.0/24
acl allowed_hosts src 192.168.1.60
acl limithour time 09:00-17:30

acl SSL_ports port 443
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
# Ajout du droit AU-DESSUS des autres http_access
# http_access allow lan
http_access allow allowed_hosts limithour
http_access allow lan
```

On autorise l'adresse ip 192.168.1.60 entre 9h et 17h30

4. Authentification des utilisateurs :

```
root@debian8:/etc/squid3# touch /etc/squid3/squidusers_
```

Avant d'installer apache2-utils, on fait un apt upadte et apt upgrade. On install apache2-utils.

```
root@debian8:/etc/squid3# apt-get install apache2-utils_
```

```
root@debian8:/etc/squid3# htpasswd -b /etc/squid3/squidusers tintin reporter
Adding password for user tintin
root@debian8:/etc/squid3# htpasswd -b /etc/squid3/squidusers milou chien
Adding password for user milou
```

Le mot de passe est le dernier mot « reporter » et « chien »

On modifie ensuite le fichier /etc/squid3/squid.conf

```
  GNU nano 2.2.6               Fichier : squid.conf                    Modifié

# A mettre au tout début du fichier
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
```

```
# a mettre l'ACL juste avant celle sur le lan
acl utilisateurs proxy_auth REQUIRED
```

```
#mettre l'autorisation avant les autres http_access
http_access allow utilisateurs_
http_access allow allowed_hosts limithour
```

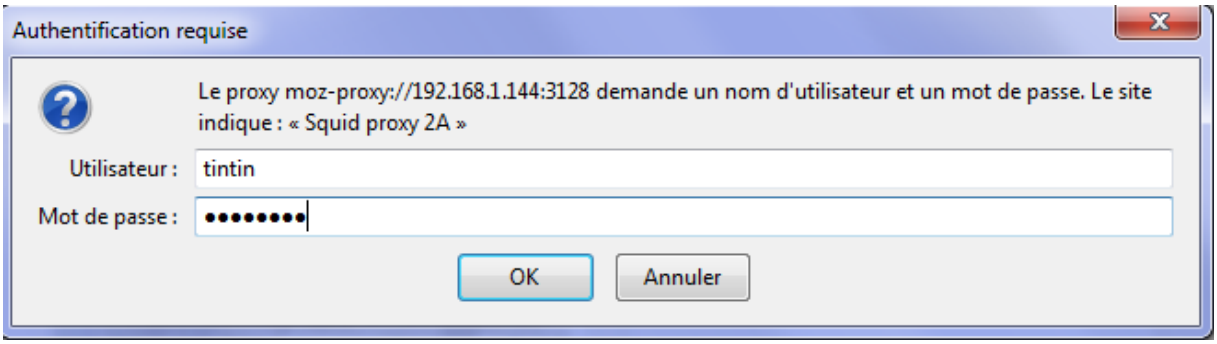
On redémarre ensuite le service

```
root@debian8:/etc/squid3# systemctl restart squid3
```

On donne ensuite la liste des permissions

```
root@debian8:~# chown proxy:shadow /usr/lib/squid3/basic_ncsa_auth
```

```
root@debian8:~# chmod 2750 /usr/lib/squid3/basic_ncsa_auth
```



5. SquidGuard :

Comment bloquer l'accès a un site

On installe SquidGuard

```
root@debian8:~# apt-get install squidguard_
```

On crée ensuite deux fichiers :

```
root@debian8:/etc/squid3# nano white_
```

```
root@debian8:/etc/squid3# nano black_
```

On va ensuite indiquer l'endroit des fichiers et de ces regles dans le fichier squid.conf

```
acl whitelist dstdomain "/etc/squid3/white"
acl blacklist dstdomain "/etc/squid3/black"
```

On peut aller mettre les pages a bloquer dans la liste black et redemarrer les services :

```
root@debian8:/etc/squid3# systemctl restart squid3_
```

On peut essayer avec une liste de liste a bloquer :

```
  GNU nano 2.2.6                Fichier : black

www.google.com
www.youtube.com
fr.yahoo.com
```

On redémarre les services de squid.

On va ensuite récupère une liste noir du site de Toulouse :

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

Et ensuite l'extraire

```
root@debian8:~# tar -xvf blacklists.tar.gz _
```

Apres avoir extrait le fichier, il faut le déplacer dans un autre dossier

```
root@debian8:/etc/squid3# mv blacklists/ /var/lib/squidguard/db.
```

Il faut ensuite modifier le fichier squid.conf

```
# la ligne pour redirifer Squid vers squidGuard
url_rewrite_program /usr/bin/squidGuard
url_rewrite_children 5_
```

Il faut ensuite définir le réseau, la destination interdit et les ACL dans le fichier squidguard :

```
root@debian8:/etc/squidguard# nano squidGuard.conf_
```

```
dbhome /var/lib/squidguard/db
logdir /var/log/squid3
```

```
src lan {
 ip 192.168.1.60_
}
```

```
dest games {
 domainlist games/domains
 urllist games/urls
}
```

```
acl {
        lan {
         pass !games all
         redirect http://192.168.1.144/proxy.html
        }
        default {
         pass local none
        }
```

Il faut ensuite redémarre le service

```
root@debian8:/etc/squidguard# systemctl restart squid3
```

Reconstruire la base de la liste noire pour squidguard

```
root@debian8:~# squidGuard -C all -d /var/lib/squidguard/db.
```

Attribuez la propriété de l'ensemble des fichiers de la liste noir a l'utilisateur proxy du groupe proxy

```
root@debian8:~# chown -Rf proxy.proxy /var/lib/squidguard/db.
```

Apres avoir mis les autorisations du dessus ;

Il suffit de crée une parge html

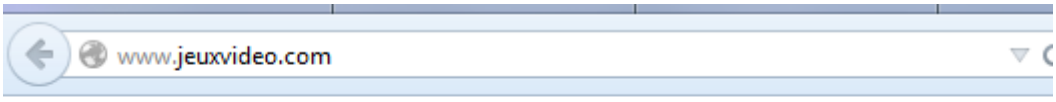
```
root@debian8:/var/www/html# nano proxy.html
```

```
<h1> TRAVAIL, AU LIEU DE JOUER <h1>
```

Puis de redémarrer les services squid

```
root@debian8:/var/www/html# systemctl restart squid3
```

RESULTAT FINAL



TRAVAIL, AU LIEU DE JOUER

On peut aussi consulter les sites précédents consultés.

```
1473758481.800     27 192.168.1.60 TCP_SWAPFAIL_MISS/200 407 GET http://www.jeux
video.com/ tintin HIER_DIRECT/192.168.1.144 text/html
```

6. Analyseur de log Lightsquid :

Lightsquid est un analyseur de log SQUID open source écrit en perl permettant d'afficher sous forme de page web l'usage du proxy.

```
..
root@debian8:/var/www/html# apt-get install libgd-gd2-perl_
```

On télécharge maintenant lightsquid

```
root@debian8:~# wget http://downloads.sourceforge.net/project/lightsquid/lightsq
uid/1.8/lightsquid-1.8.tgz?r=https%3A%2F%2Fsourceforge.net%2Fprojects%2Flightsqu
id%2Ffiles%2Flightsquid%2F&ts=1474027414&use_mirror=netix
```

On le met dans le dossier /var/www/html

```
root@debian8:/var/www/html# ls
index.html  nfe102   proxy.html  sisr  totortweb.html       web
lightsquid  non.jpg  rt2a        slam  totortweb.html.save
```

```
root@debian8:/var/www/html# tar -xzf lightsquid-1.8.tgz _
```

```
root@debian8:/var/www/html# cd lightsquid-1.8/_
```

Rends les scripts pl et cgi exécutables

```
root@debian8:/var/www/html/lightsquid-1.8# chmod ugo+x *.pl
root@debian8:/var/www/html/lightsquid-1.8# chmod ugo+x *.cgi
```

Changer le propriétaire du répertoire Lightsuid

```
root@debian8:/var/www/html# chown www-data lightsquid-1.8
```

On active le module

```
root@debian8:/var/www/html/lightsquid-1.8# a2enmod cgi
AH00548: NameVirtualHost has no effect and will be removed in the next
etc/apache2/sites-enabled/sites-sio.conf:1
Your MPM seems to be threaded. Selecting cgid instead of cgi.
Enabling module cgid.
To activate the new configuration, you need to run:
  service apache2 restart
root@debian8:/var/www/html/lightsquid-1.8# service apache2  restart _
```

On faut ensuite aller configurer le fichier default d'apache

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

```
 GNU nano 2.2.6          Fichier : 000-default.conf

        # For most configuration files from conf-available/
        # enabled or disabled at a global level, it is poss
        # include a line for only one particular virtual ho
        # following line enables the CGI configuration for
        # after it has been globally disabled with "a2disco
        #Include conf-available/serve-cgi-bin.conf

        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory "var/www/html/lightsquid">
                AddHandler cgi-script .cgi
                AllowOverride All
                DirectoryIndex index.cgi
                Options +ExecCGI
        </Directory>
```

On change le nom du dossier pour qu'il soit en coordonnante avec le fichier précédant.

```
root@debian8:/var/www/html# mv lightsquid-1.8 lightsquid
```

```
root@debian8:/var/www/html/lightsquid# nano lightsquid.cfg _
```

```
# -------------------- WEB VARIABLES  ----------------------

#language
#see `lang` folder (avaible: bg,eng,fr,hu,it,pt_br,ru,sp)
$lang                ="fr";_
```

```
#path to access.log
$logpath             ="/var/log/squid3";
#path to `ip2name` folder
```

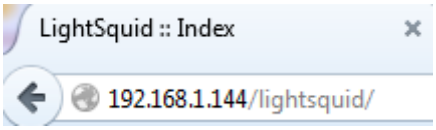
On test l'installation par une commande :

```
root@debian8:/var/www/html/lightsquid# ./check-setup.pl
LightSquid Config Checker, (c) 2005-9 Sergey Erokhin GNU GPL

LogPath    : /var/log/squid3
reportpath: /var/www/html/lightsquid/report
Lang       : /var/www/html/lightsquid/lang/fr
Template   : /var/www/html/lightsquid/tpl/base
Ip2Name    : /var/www/html/lightsquid/ip2name/ip2name.simple


all check passed, now try access to cgi part in browser
```

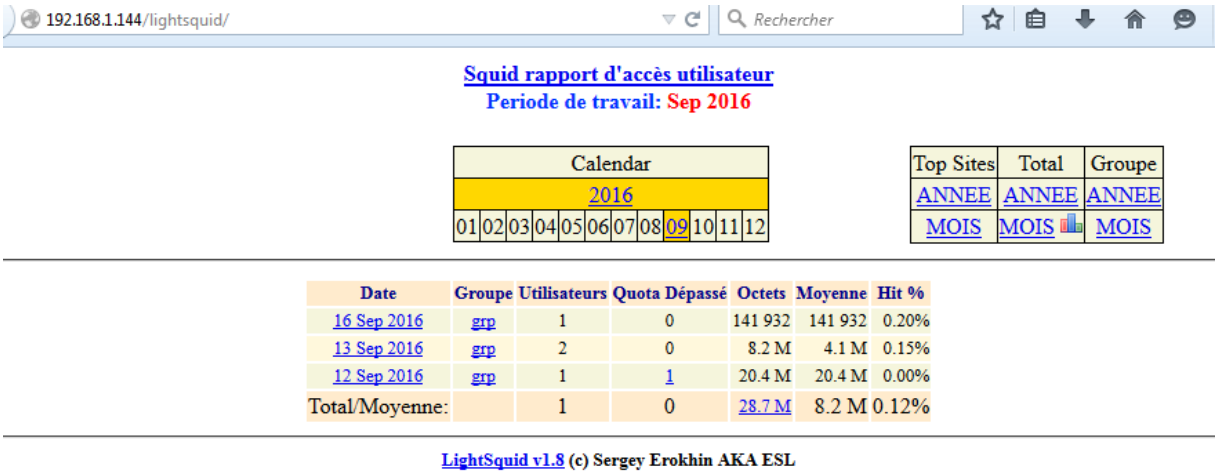
```
root@debian8:/var/www/html/lightsquid# ./lightparser.pl
```

```
root@debian8:/var/www/html/lightsquid# service apache2 restart
```

On test ensuite dans un navigateur.

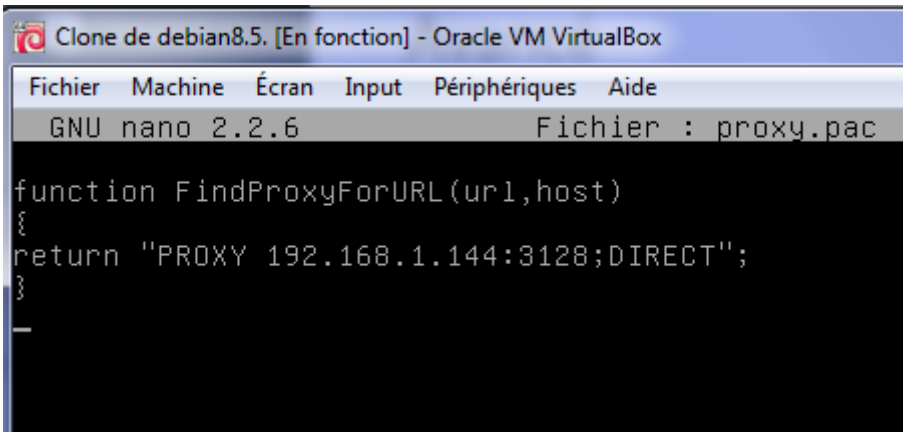


Resultat final :



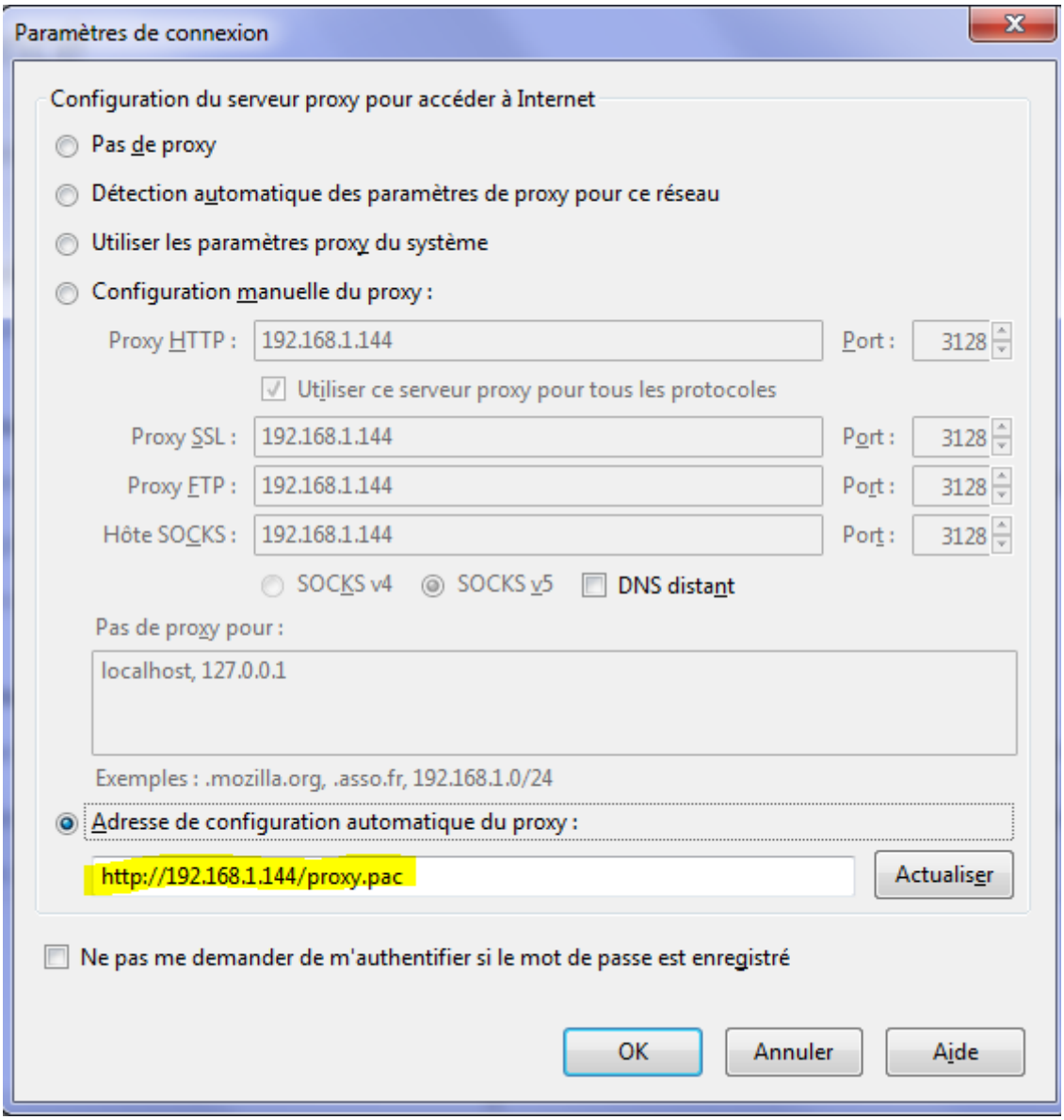
7. Configuration d'un navigateur via un script :

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




```
root@debian8:/var/www/html# service apache2 restart
```

Enfin il faut aller régler le proxy en mode automatique :


Paramètres de connexion
Configuration du serveur proxy pour accéder à Internet
Pas de proxy
Détection automatique des paramètres de proxy pour ce réseau
Utiliser les paramètres proxy du système
Configuration manuelle du proxy :
Proxy HTTP : 192.168.1.144 Port : 3128
Utiliser ce serveur proxy pour tous les protocoles
Proxy SSL : 192.168.1.144 Port : 3128
Proxy FTP : 192.168.1.144 Port : 3128
Hôte SOCKS : 192.168.1.144 Port : 3128
SOCKS v4 SOCKS v5 DNS distant
Pas de proxy pour :
localhost, 127.0.0.1
Exemples : .mozilla.org, .asso.fr, 192.168.1.0/24
Adresse de configuration automatique du proxy :
http://192.168.1.144/proxy.pac
Actualiser
Ne pas me demander de m'authentifier si le mot de passe est enregistré
OK
Annuler
Aide