



Installation
Configuration

Serveur proxy

Objectif : mettre en place un serveur proxy afin de sécuriser l'accès à internet et pouvoir contrôler l'accès à certains sites.

DEBIAN SQUID : 192.168.1.90/24

DEBIAN DNS : 192.168.1.91/24

Installer le serveur DNS :

Installer le paquet : **apt-get install bind9**

Ensuite, il faut éditer le fichier **named.conf.local** dans **/etc/bind/**:

A la base, le fichier de configuration est totalement vide. C'est ici qu'il faut renseigner les zones.

```
GNU nano 2.2.6      Fichier : named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
_
```

Création de la zone de recherche directe :

```
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "sio2.local" IN {
type master;
file "/var/cache/bind/db.sio2.local";
};
_
```

Ensuite il faut compléter la zone inversée de la même façon.

```
zone "1.168.192.in-addr.arpa" IN {
type master;
file "/var/cache/bind/rev.sio2.local";
};_
```

On vérifie ensuite nos zones pour voir s'il n'y a pas d'erreur présente avec la commande **named-checkconf /chemincomplet**.

```
root@Vincent:/etc/bind# named-checkconf /etc/bind/named.conf.local
root@Vincent:/etc/bind# _
```

Ensuite, il faut créer les deux autres fichiers de configuration qui sont **db.nomdomaine.local** et **rev.nomdomaine.local** :

Pour ce faire, il faut aller de le dossier **/var/cache/bind** :

On crée le fichier de zone de recherche directe qui se nommera **db.sio2.local**.

```
root@Vincent:/var/cache/bind# touch db.sio2.local
```

Dans ce fichier, il faut renseigner les enregistrements suivants avec la bonne syntaxe :

```
$TTL 86400
@ IN SOA vincent.sio2.local. vincentfournier.gmail.com (
2014111801
3600
180
3600
60 )
@ IN NS vincent.sio2.local.
vincent.sio2.local. IN A 192.168.1.91
proxy.sio2.local. IN A 192.168.1.90
```

Ensuite, on teste si la zone créée fonctionne bien avec la commande **named-checkzone sio2.local /var/cache/bind/db.sio2.local**.

```
root@Vincent:/var/cache/bind# named-checkzone sio2.local /var/cache/bind/db.sio2.local
zone sio2.local/IN: loaded serial 2014111801
OK
root@Vincent:/var/cache/bind# _
```

Puis, on crée le fichier de zone inversée dans le même dossier que précédemment :

```
root@Vincent:/var/cache/bind# touch rev.sio2.local_
```

Il faut renseigner les champs suivants dans le fichier de zone de recherche inversée :

```
$TTL 86400
@ IN SOA vincent.sio2.local. vincentfournier@gmail.com (
2014111801
3600
180
3600
60 )
@ IN NS vincent.sio2.local.
91 IN PTR vincent.sio2.local.
90 IN PTR proxy.sio2.local.
```

Il faut ensuite modifier le fichier **resolv.conf** et mettre son adresse IP pour résoudre.

```
root@debian:~# nano /etc/resolv.conf_
```

On redémarre ensuite le service **bind** :

```
root@Vincent:/var/cache/bind# service bind9 restart
```

On télécharge les paquets **dnsutils** pour tester notre DNS. (Si la commande **nslookup** ne fonctionne pas).

Puis on test le serveur DNS à l'aide de la commande **nslookup** :

```
root@Vincent:~# nslookup
> 192.168.1.90
Server:          127.0.0.1
Address:         127.0.0.1#53

90.1.168.192.in-addr.arpa      name = proxy.sio2.local.1.168.192.in-addr.arpa.
> proxy.sio2.local
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   proxy.sio2.local
Address: 192.168.1.90
> _
> _
```

On peut voir que le DNS fonctionne en zone directe et inversé pour le serveur proxy d'adresse **192.168.1.90** et de nom **proxy.sio2.local**.

Notre serveur DNS est en état de fonctionnement.

Installation du serveur Proxy (Squid) :

Il faut télécharger le paquet squid avec la commande **apt-get install squid3**.

Le fichier de configuration de Squid se situe dans **etc/squid3/squid.conf**.

Pour ce fichier, il faudra en premier créer une sauvegarde 2 et une sauvegarde 3 du fichier car on va toucher au fichier initial et à la première sauvegarde (**cp squid.conf squid2.conf**).

En premier, il faudra rentrer la commande suivante qui permet d'expurger les lignes de commentaire.

```
root@debian:/etc/squid3# cat squid2.conf | grep -v ^# | grep -v ^$ > squid.conf_
```

On voit donc ensuite que le fichier n'as plus de commentaires:

```
GNU nano 2.2.6      Fichier : squid.conf
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1
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
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost

[ Lecture de 27 lignes ]
^G Aide      ^O Écrire   ^R Lire fich.^V Page préc.^K Couper     ^C Pos. cur.
^X Quitter   ^J Justifier ^W Chercher  ^V Page suiv.^U Coller    ^T Orthograp.
```

Pour vérifier que le serveur écoute bien sur le port 3128, on tape la commande **lsof -i:3128** :

```
root@debian:/var/spool/squid3# lsof -i:3128
COMMAND PID  USER  FD   TYPE    DEVICE  SIZE/OFF  NODE NAME
squid3  2926 proxy  15u  IPv6    7430      0t0      TCP *:3128 (LISTEN)
root@debian:/var/spool/squid3# _
```

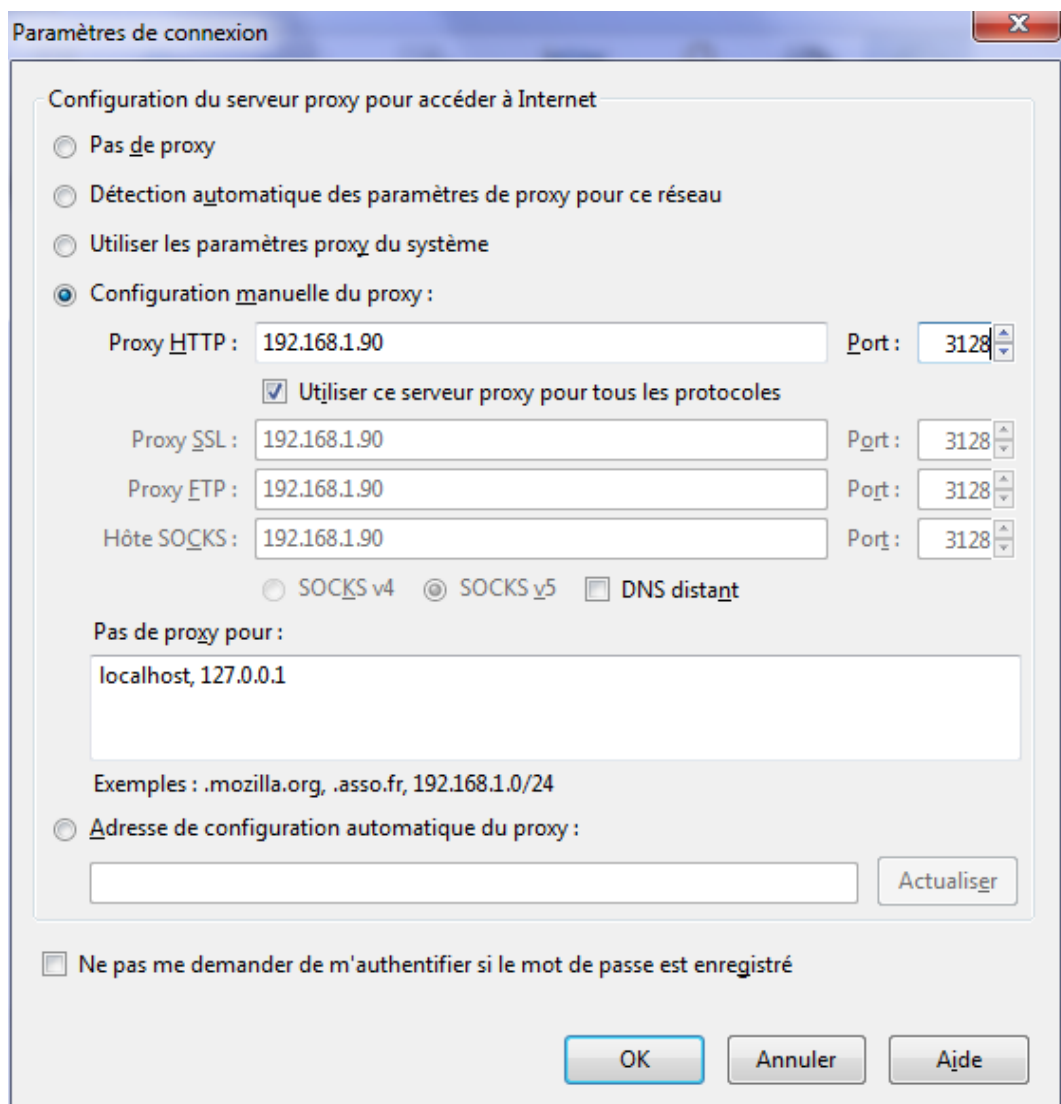
Ensuite, il faut aller dans le fichier de configuration dans **/etc/squid/squid.conf** et marquer les lignes suivantes:

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

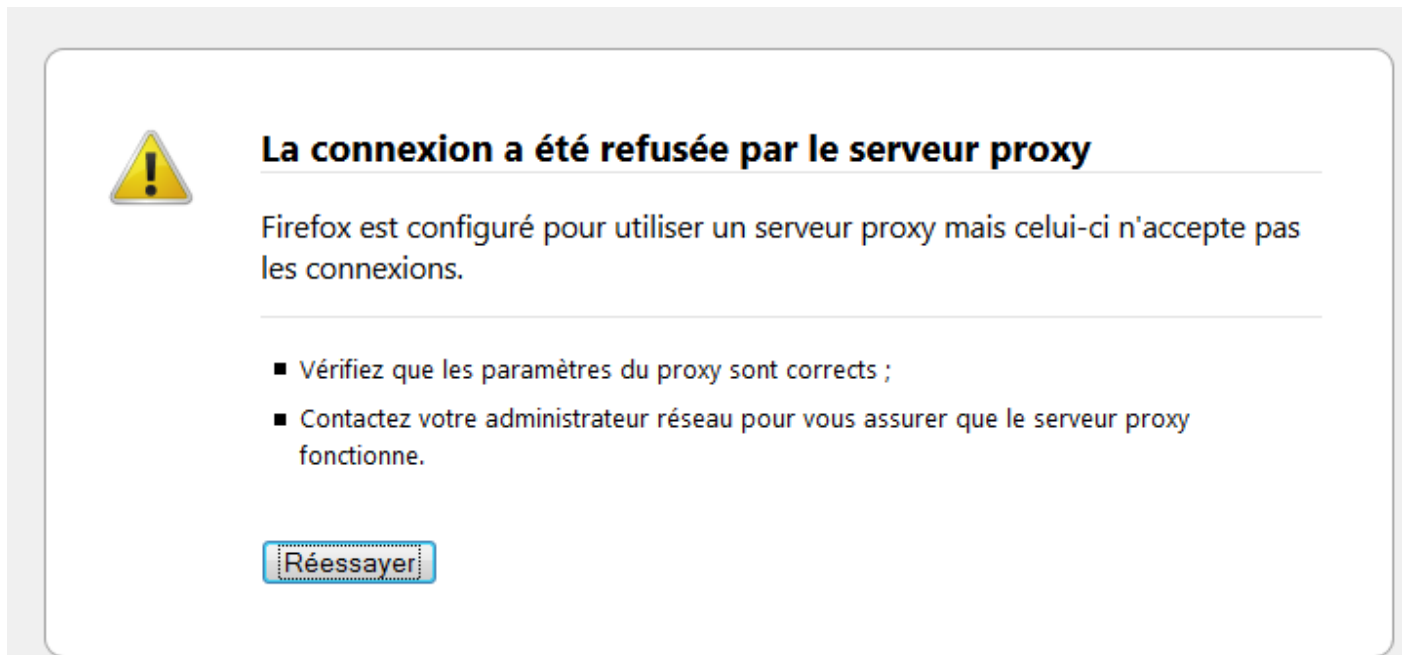
#Emplacement de stockage des données et réglage des niveaux
cache_mem 16 MB
cache_dir ufs /var/spool/squid3 120 16 128
```

La dernière ligne du fichier de configuration permet de créer un fichier **swap.state** qui est le fichier cache de Squid.

Test proxy sur Firefox:



On peut constater qu'aucune page internet n'est contactable :



La connexion a été refusée par le serveur proxy

Firefox est configuré pour utiliser un serveur proxy mais celui-ci n'accepte pas les connexions.

- Vérifiez que les paramètres du proxy sont corrects ;
- Contactez votre administrateur réseau pour vous assurer que le serveur proxy fonctionne.

Réessayer

Cette erreur est normale car nous n'avons pas encore configuré squid pour permettre l'accès à internet depuis le réseau local.

Installation ACL:

On va donc installer les ACL pour permettre les droits d'accès à internet. On tape la commande :
apt-get install acl

Autorisation de l'utilisation du proxy pour le réseau local

Ajouter les lignes de commandes ci-dessous au fichier de configuration `/etc/squid3/squid.conf` juste avant la ligne `acl localhost` pour autoriser le proxy sur le réseau local :

```
acl lan src 192.168.1.0/24
# Ajout du droit AU-DESSUS des autres http_access
http_access allow lan_
```

* Les lignes `acl` permettent d'autoriser ou de refuser des accès, tandis que les lignes `http_access` définissent les `acl` afin de les appliquer.

* L'ordre des `acl` est très important, il faut mettre les plus restrictives en premier.

* Lorsque l'on se déplace dans le fichier log situé dans `/var/log/squid3/access.log`, on peut voir tous les sites auquel on a accédé.

Puis, sur la machine cliente, il faut configurer le proxy.

Authentification des utilisateurs

Pour utiliser l'authentification des utilisateurs, il faut installer un serveur apache avec la commande `apt-get install apache2` puis ensuite créer un fichier "squidusers" dans le répertoire /etc/squid3 :

```
root@debian:/etc/squid3# touch squidusers
root@debian:/etc/squid3# ls
errorpage.css  msntauth.conf  squid2.conf  squid3.conf  squid.conf  squidusers
root@debian:/etc/squid3# _
```

Ensuite, on ajoute avec la commande `htpasswd` le nom des utilisateurs et leurs mot de passe:

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

Ensuite, si l'on vérifie le fichier squidusers, on voit que les mots de passe sont cryptés en md5:

```
GNU nano 2.2.6 Fichier : squidusers
tintin:$apr1$/jVFwHYL$mMqcEcpwbuADnhJug5XC7.
milou:$apr1$w9cjQZ1B$6Jk0YnYqP898F97uq16U6/
```

Ensuite, il faut rajouter des lignes dans le fichier de configuration de squid:

```
GNU nano 2.2.6 Fichier : squid.conf Mo
#a mettre au tout début du fichier (authentification):
auth_param basic program /usr/lib/squid3/ncsa_auth /etc/squid3/squidusers
auth_param basic children 5
auth_param basic realm Squid proxy 2A
authentucate_ttl 1 hour
authenticate_ip_ttl 60 seconds
```

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

```
#autorisation authentification
http_access allow utilisateurs_
```

```
#Ajout du droit au dessus des autres http_access
http_access allow lan
```

```
acl manager proto cache_object
```

```
#suite acl authentification
acl utilisateurs proxy_auth REQUIRED
```

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

```
#Ajout du droit au dessus des autres http_access
http_access allow lan_
```


* La ligne children permet de démarrer 5 processus et la ligne realm squid permet de donner un nom à la boîte de dialogue de la page d'authentification de squid.

* Lors de l'accès à internet, les proxy nous demandera dorénavant un nom d'utilisateur et un mot de passe afin d'accéder à la page:

Installer SquidGuard:

En premier, il faut installer le paquet squidguard:

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

Puis, il faut récupérer les sources de la blacklist avec la commande wget:

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

Ensuite, on décompresse l'archive:

```
root@debian:~# ls
blacklists.tar.gz
root@debian:~# tar xzvf blacklists.tar.gz
```

Puis on déplace la blacklist avec la commande move (mv) vers le répertoire /var/lib/squidguard/db:

```
root@debian:~# mv blacklists /var/lib/squidguard/db
root@debian:~# cd /var/lib/squidguard/db
root@debian:/var/lib/squidguard/db# ls
blacklists
```

Ensuite on va dans le dossier blacklist:

```
root@debian:~# cd blacklists
root@debian:~/blacklists# _
```

Puis on vérifie si les fichiers ont bien été copiés avec la commande ls:

```
root@debian:~/blacklists# ls
ads                cooking            lingerie           reaffected
adult             dangerous_material liste_bu           redirector
aggressive        dating            mail              remote-control
agressif          drogue            malware           sect
arjel             drugs             manga             sexual_education
astrology         educational_games marketingware      shopping
audio-video       filehosting       mixed_adult       social_networks
bank              financial         mobile-phone      sports
bitcoin           forums            phishing          strict_redirector
blog              gambling          porn              strong_redirector
cc-by-sa-4-0.pdf  games            press             translation
celebrity         global_usage      proxy             tricheur
chat              hacking           publicite         violence
child             jobsearch        radio             warez
cleaning          LICENSE.pdf       README            webmail
root@debian:~/blacklists# _
```

Ensuite, il faut rajouter deux lignes dans le fichier de configuration de squid afin de rediriger squid vers squidguard : (/etc/squid3/squid.conf)

```
url_rewrite_program /usr/bin/squidGuard
url_rewrite_children 5_
```


Ensuite, éditer le fichier /etc/squidguard/squidGuard.conf puis modifier les lignes suivantes pour définir un réseau, une destination interdite et les ACL :

- dbhome /var/lib/squidguard/db/blacklists
- logdir /var/log/squid3

```
#
# CONFIG FILE FOR SQUIDGUARD
#
# Caution: do NOT use comments inside { }
#
dbhome /var/lib/squidguard/db/blacklists
logdir /var/log/squid3_
```

- Ajouter src lan comme ci-dessous :

```
#
# SOURCE ADDRESSES:
#
src lan {
    ip 192.168.1.113
}
src admin {
    ip          1.2.3.4  1.2.3.5
    user        root foo bar
    within      workhours
```

- Ajouter dest games comme ci-dessous :

```
#
# DESTINATION CLASSES:
#
dest games {
    domainlist games/domains
    urllist games/urls
}
dest good {
```

- Ajouter dans acl, le lan :

```
#
# ACL RULES:
#
acl {
    lan {
        pass !games all
        redirect http://192.168.1.113/proxy.html
    }
    admin {
        pass any
    }
}
```

Ensuite, il faut reconstruire la base de la liste noire pour squidguard ! Taper cette commande :
- squidGuard -C all -d /var/lib/squidguard/db/blacklists/

```
root@debian:/etc/squidguard# squidGuard -C all -d /var/lib/squidguard/db/blacklists/
2014-09-26 14:44:08 [4805] INFO: New setting: dbhome: /var/lib/squidguard/db/blacklists
2014-09-26 14:44:08 [4805] INFO: New setting: logdir: /var/log/squid3
2014-09-26 14:44:08 [4805] Added User: root
2014-09-26 14:44:08 [4805] Added User: foo
2014-09-26 14:44:08 [4805] Added User: bar
2014-09-26 14:44:08 [4805] init domainlist /var/lib/squidguard/db/blacklists/games/domains
2014-09-26 14:44:08 [4805] INFO: create new dbfile /var/lib/squidguard/db/blacklists/games/domains.db
2014-09-26 14:44:08 [4805] init urllist /var/lib/squidguard/db/blacklists/games/urls
2014-09-26 14:44:08 [4805] INFO: create new dbfile /var/lib/squidguard/db/blacklists/games/urls.db
2014-09-26 14:44:08 [4805] destblock good missing active content, set inactive
2014-09-26 14:44:08 [4805] destblock local missing active content, set inactive
2014-09-26 14:44:08 [4805] destblock porn missing active content, set inactive
2014-09-26 14:44:08 [4805] INFO: squidGuard 1.5 started (1411735448.510)
2014-09-26 14:44:08 [4805] INFO: db update done
2014-09-26 14:44:08 [4805] INFO: squidGuard stopped (1411735448.549)
```

Maintenant, taper la commande ci-dessous pour attribuer la propriété de l'ensemble des fichiers de la liste noire à l'utilisateur proxy du groupe proxy :

```
root@debian:/etc/squidguard# chown -Rf proxy:proxy /var/lib/squidguard/db
```

On va créer deux fichiers dans /etc/squid nommer **black** & **white**.

```
root@proxy:/etc/squid3# touch black
root@proxy:/etc/squid3# touch white
root@proxy:/etc/squid3# _
```

On redémarre ensuite le service. Commande: **service squidguard restart**.

Installer Apache sur le serveur:

Commande: **apt-get install apache2**

Créer une page proxy.html avec un message d'interdiction placé dans **/var/www**:

```
root@debian:/var/www# nano proxy.html_
```

```
<html><h1>Le proxy à bloquer ce site contacter votre administrateur
```

Redémarrage du service apache: **service apache2 restart** et **service squid3 restart**.

Configuration d'un navigateur via un script:

On crée le fichier **proxy.pac** afin de créer un script de connexion automatique au proxy. Ce fichier sera stocké dans **/var/www**:

Pour terminer, on rentre les nouveaux paramètres de proxy sur la machine cliente:

```
GNU nano 2.2.6          Fichier : proxy.pac
function FindProxyForURL(ur1,host)
{
return "PROXY 192.168.1.113:3128;DIRECT";
}
```

