Serveur Proxy-Mandataire

Mise en place de Squid 3.5 sous Debian 8.1

Anatole Billet

05 octobre 2015
Version : 1.00

Serveur Proxy-Mandataire

Mise en place de Squid 3.5 sous Debian 8.1

Avant de commencer…

Objectif :

Ici, L'objectif est de mettre en place un serveur de Proxy ayant un rôle mandataire.

Prérequis :

Une machine sous Debian 8.1

Un client sous Windows pour réaliser les teste

Un navigateur acceptant le changement de serveur

Code couleur :

-Bleu pour les commandes Debian

-Vert pour les noms des fichiers de configurations

-Italic pour les descriptions et anecdotes.

Table des matières

1. Installation de Squid

Récupération du paquet :

Apt-get install squid3

Le port d'écoute par default de squid est le 3128 on le retrouve via la commande :

Netstat –ltp | grep squid

On peut voir via la commande :

Cat /etc/passwd | grep proxy

Cat /etc/group | grep proxy

Que l'utilisateur proxy et le groupe proxy on était créé.

2. Configuration de Squid

En paramétrant un navigateur pour le proxy on remarque que pour le moment celui-ci ne parviens pas à accéder à internet.

Cette ligne des fichiers de log nous donne la raison de ce blocage :

```
1444030101.357      0 192.168.1.68 TCP_DENIED/403 3730 CONNECT uib.ff.avast.com:
443 - HIER_NONE/- text/html
1444030101.734      0 192.168.1.68 TCP_DENIED/403 3614 CONNECT www.google.com:44
3 - HIER_NONE/- text/html
1444030101.781      0 192.168.1.68 TCP_DENIED/403 3730 CONNECT uib.ff.avast.com:
443 - HIER_NONE/- text/html
```

Le fichier de configuration de squid (**/etc/squid3/squid.conf**) est complexe, en effectuer une sauvegarde est important :

cp /etc/squid3/squid.conf /etc/squid3/squid.conf.old

Il possède également une énorme quantité de lignes commentées qui nous serons inutile dans notre cas, les supprimer permettra d'améliorer grandement la lisibilité du fichier :

Cat squid.conf.old | grep –v ^# | grep –v ^$ > squid .conf

Cette commande lit le fichier de sauvegarde et réécris sur le fichier d'origine seulement les lignes dé-commenter.

grep –v ^# ➔ enlever commentaires

grep –v ^$ ➔ enlever les lignes vides

On ajoute les lignes suivantes au fichier squid.conf :

```
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320

#utilisateur:
cache_effective-user proxy
cache_effective-group proxy
#Emplacement des données
cache_mem 16 MB
cache_dir ufs /var/spool/squid3 120 16 128
```

Ces lignes permettront d'indiquer l'emplacement du cache du serveur et d'activer celui des utilisateurs/groupes.

3. Les Contrôle d'accès

On créer une acl pour le réseau local dans le fichier de configuration et ce avant la définition de l'acl localhost et avant http-Access deny all :

```
acl Safe_ports port 777         # mul
acl CONNECT method CONNECT

acl lan src 192.168.1.0/24
http_access allow lan

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
```

L'ordre est important car les paramètres des fichiers sous Debian sont pris en compte de haut en bas.

3.2. Contrôle d'accès horaire

Ici un exemple d'accès horaire :

```
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

acl allowed_hosts src 192.168.1.122
acl limithour time 10:00-12:00
http_access allow allowed_hosts limithour

acl lan src 192.168.1.0/24
```

Ainsi, entre 10h et 12h l'utilisateur possédant l'adresse IP 192.168.1.122 ne pourras pas se connecter à internet via le serveur proxy.

4. Authentification des utilisateurs

Pour authentifier des utilisateurs on utilise la commande htaccess d'apache, nous devons donc installer apache2-utils :

Apt-get install apache2-utils

Puis, on ajoute les utilisateurs et leurs mots de passe :

Touch /etc/squid3/squidusers

Htpasswd –b /etc/squid3/squidusers toto root

Htpasswd –b /etc/squid3/squidusers tata root

Ensuite, on complète le fichier **squid.conf** pour que celui-ci prenne en compte les utilisateurs :

```
auth_param basic program /usr/squid3/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

http_access allow utilisateurs

http_access allow lan
```

On donne les droits d'accès au fichier de permission :

Chown proxy.shadow /usr/lib/squid3/basic_ncsa_auth

Chmod 2750 /usr/lib/squid3/basic_ncsa_auth

Redémarrer le service squid3 et tester la connexion.

5. SquidGuard

Squidguard est un logiciel de restriction d'accès de sites internet pour les utilisateurs du proxy.

Installation de SquidGuard :

Apt-get install squidguard

Il nous faut également, créer les fichiers **Black** et **white** dans **/etc/squid**

Retourner une nouvelle fois dans le fichier de configuration et ajoutez-y les lignes suivantes :

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

Black ou white en fonction de ce que vous désirez utiliser, un « ! » avant le nom du fichier lui donne l'effet inverse ainsi !white bloquera l'accès aux sites de la white-list

Intégration liste noire de L'université de Toulouse

Récupérer la liste noir sur votre Debian :

Wget http://cri.univ-tlse1.fr/blacklists/download/blacklists.tar.gz

Installer le tar via la commande :

Tar xzf blacklists.tar.gz

Et copier le répertoire extrait dans /var/lib/squidguard/db

Entrez ensuite les lignes suivantes au début de votre fichier de conf **squid.conf** :

```
url_rewrite_program /usr/bin/squidGuard
url_rewrite_children
```

Interdire par exemple les jeux en modifiant ainsi le **/etc/squid/squidguard/squidguard.conf** :

```
src lan {
        ip              192.168.1.10-192.168.1.100
}

dest games {
        domainlist      games/domains
        urllist         games/urls
}
acl {
        admin {
                pass    !games all
                redirect http://127.0.0.1/proxy.html
        }

        default {
                pass     local none
        }
}
```

Puis entrez la commande suivante pour reconstruire la base :

squidGuard –C all –d /var/lib/squidguard/db

On approprie les droits de la liste-noir au user proxy et son groupe :

Chown –Rf proxy.proxy /var/lib/squidguard/db

On peut finalement créer un un fichier nommée **proxy.html** dans **/var/www**

Redémarrer Squid et faites vos testes !

6. Analyseur de log Lightsquid

En premier lieu se rendre dans **/var/www/html** et télécharger lightsquid via la commande wget :

Wget http://sourceforge.net/projects/lightsquid/files/lightsquid/1.8/lightsquid-1.8.tgz

Puis procéder à sont extraction :

tar -xzf lightsquid.tgz

Ensuite rendre les scripts pl et cgi exécutables :

chmod +x *.cgi

chmod +x *.pl

Changer le propriétaire du dossier lightsquid en www-data :

chown –R www-data :www-data lightsquid-1.8

Configurer apache2 en modifiant comme ci-dessous le ficher **/etc/apache2/sites-available/000-default.conf** :

```
<Directory "/var/www/html/lightsquid-1.8">
        AddHandler cgi-script .cgi
        AllowOverride All
        DirectoryIndex index.cgi
        Options +ExecCGI
</Directory>
```

Puis personnaliser lightsquid :

nano /var/www/html/lightsquid-1.8/lightsquid.cfg

en modifiant les lignes :

$logpath= `/var/log/squid/' ;

$lang='fr' ;

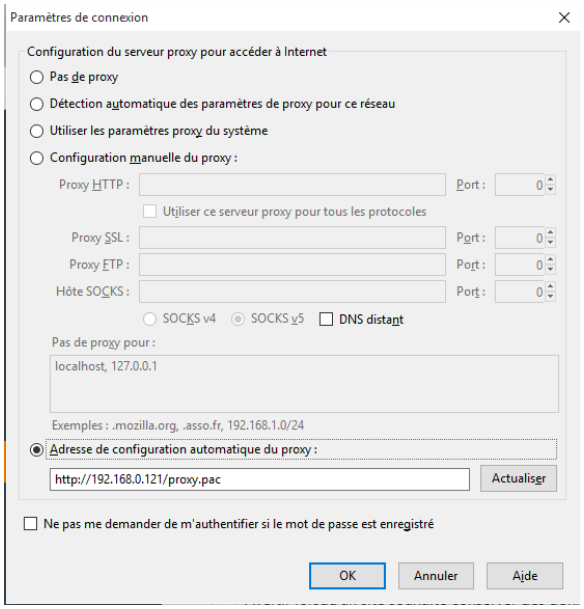
Voila votre interface de log web lightsquid est installer

7.Configuration d'un navigateur via script :

Créer le fichier **proxy.pac** dans /var/www/html/ et l'editer comme il suis :

```
function FindProxyForURL(url,host)
{
return "PROXY 192.168.0.121:3128;direct";
}
```

Il ne reste plus qu'a donner l'adresse du script a votre navigateur :



Vous savez maintenant mettre en place de façon complète un proxy sous Debian 8.1