Squid Proxy sur Debian 10 Linux

Une machine linux qui servira de serveur proxy
Notre ip :172.18.60.135

Installation de Squid :

apt update
apt install squid

vérifier la version de squid :
squid chache : Version 4.6

Pour trouver le port tcp de squid :
Lsof –i –P

Normalement le port est :3128

Le proxy créer un utilisateur et un groupe du nom de proxy.

Premier test :

Nous allons utiliser firefox pour pouvoir configurer un proxy dessus.

Sur firefox :
Options
Configuation manuelle du proxy

Puis cocher utiliser également ce proxy pour FTP et HTTPS.

Configuration de squid :

Nous allons créer une copie du fichier /etc/squid/squid.conf puis le purger.
cp squid.conf squid.conf.backup
cat squid.conf.backup | grep -v ^# | grep -v ^$ > squid.conf

Puis on ajoute à la fin du fichier 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/squid 120 16 128

 # algorithme utilisé pour gérer le remplacement des objets stockés en cache
cache_replacement_policy heap LFUDA

 # pourcentage dusage du cache à partir duquel squid commence à supprimer des objets
cache_swap_low 80

 # pourcentage dusage du cache à partir duquel squid devient plus agressif
cache_swap_high 90

Contrôle d'accès :

On vérifie notre fichier acl qu'il accepte bien toute les demandes :
cat /boot/config-4 .19.0-10-amd64 | grep ACL

on ajoute notre réseau dans /etc/squid/squid.conf :

acl monlan src 172.18.0.0/16
http_access allow monlan

on ajoute une option pour autoriser en fonction de l'horaire :

acl llimithour time 09 :00-18 :00
http_access allow mon limithour

Accès par authentification :
On vas créer un fichier pour y mettre nos utilisateurs :
Touch /etc/squid/squidusers

Pour utiliser la commande htpasswd :
apt install apache2

on ajoute les lignes de configuration suivante :
#A mettre au tout début du fichier
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid/squidusers
auth_param basic children 2
auth_param basic credentialsttl 3 hours
auth_param basic realm Squid proxy SIO2A
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'aurisation avant les autres http_access
http_access allow utilisateurs

On vas configurer SquidGuard .

apt install squidguard
cd /var/lib/squidguard/db
wget http://cri.univ-tlse1.fr/blacklists/download/blacklists.tar.gz

on décompresse :
tar –xzf blacklists.tar.gz

pour indiquer squidgard à squid on ajoute dans le fichier squid.conf à la fin :

redirect_program /usr/bin/squidGuard –c /etc/squidguard/squidGuard.conf
redirect_children 10

on va changer les règles de /etc/squidguard/squidguard.conf :

```
#| CONFIG FILE FOR SQUIDGUARD

# Caution: do NOT use comments inside { }


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

# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

time workhours {
        weekly mtwhf 08:00 - 16:30
        date *-*-01  08:00 - 16:30
}


# SOURCE ADDRESSES:


src admin {
        ip      172.18.60.135/255.255.255.0

}

src clients {
        ip      172.18.0.0/255.255.0.0
}


# DESTINATION CLASSES:


dest adult {
        domainlist      adult/domains
        urllist         adult/urls
        expressionlist  adult/expressions
#       redirect http://admin.foo.bar.de/cgi-bin/blocked.cgi?cl
}
```

```
dest agressif {
        domainlist agressif/domains
        expressionlist agressif/expressions
        urllist agressif/urls
}

dest bank{
        domainlist bank/domains
}


dest blog {
        domainlist blog/domains
        urllist blog/urls
}

dest celebrity {
        domainlist celebrity/domains
        urllist celebrity/urls
}


dest chat {
        domainlist chat/domains
        urllist chat/urls
}

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

# ACL RULES:


acl {
        admin {
                pass     any
        }

        default {
                #pass    local none
                pass !games !adult !chat !celebrity !blog !bank !agressif all
                redirect http://localhost/proxy.html
        }
}
```

Puis on reconstruit la liste noir avec la commande :
squidGuard -C all -d /var/lib/squidguard/db/blacklists

nous allons créer une page proxy.html pour rediriger les utilisateurs :
nano /var/www/html/squidguard/proxy.html

<!DOCTYPE html>
<html lang="fr">
<head>

```
        <meta charset="UTF-8">
        <title>Proxy Squid</title>
</head>
 <body>
        <h1>L'accès à ce site n'est pas autorisé !</h1>
</body>
 </html>
```

On change la configuration de apache2 :
nano /etc/apache2/sites-available/000-default.conf
puis :
DocumentRoot /var/www/html/squidguard

Et on recharge apache2 :
systemctl reload apache2

on change les droit de notre blacklist pour les donner a notre utilisateurs proxy :
chown -R proxy.proxy /var/lib/squidguard/db/blacklists
systemctl reload squid

on vérifie que cela fonctionne correctement :
tail /var/log/squidguard/squidGuard.log

puis on peut tester avec l'adresse game.fr par exemple..

(si jamais on n'as un problème on peut rentrer c'est commande ci-dessous :
chown -R root.root /var/lib/squidguard
systemctl reload squid
chown -R proxy.proxy /var/lib/squidguard/db/blacklists
systemctl reload squid
cela peut fonctionner)

Si on veut dévelloper notre projet on peut alors utiliser SquidAnalyzer.

SquidAnalyzer est un analyseur de logs c'est-à-dire qu'il permet grâce à une interface web de regarder plus finement les transactions.

Pour forcer notre proxy il faut mettre en place un proxy transparant et un routeur qui nous servira de parefeu qui n'autorise que l'adresse du proxy à communiquer avec internet. Notre routeur devras faire le lien entre le réseau/parefeu et internet.

Pour cela on ajoute une ligne dans /etc/squid/squid.conf :
http_port : 3128 transparent
et ensuite mettre en place un parefeu.

Installer un parefeu

Pour installer un pare-feu nous allons utiliser de l'iptables à l'aide de 2 script.
Parefeu_off.sh et Parefeu_on.sh.

Parefeu_off.sh :

```
ifwan=eth0

iptables -F
iptables -t nat -F

iptables -P OUTPUT ACCEPT
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT

iptables -t nat -A POSTROUTING -o $ifwan -j MASQUERADE
iptables -t nat -A POSTROUTING -o $ifwanall -j MASQUERADE
```

Parefeu_on.sh :

```
ifwan=eth2
iflan=eth0
proxy=172.18.60.135

iptables -F
iptables -t nat –F

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

iptables -t nat -A POSTROUTING -o $ifwan -j MASQUERADE
```

Autorise les requêtes http à passer au travers du routeur :

```
iptables -A FORWARD -i $proxy -p tcp --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -o $proxy -p tcp --sport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Autorise les requêtes https à passer au travers du routeur :

```
iptables -A FORWARD -i $proxy -p tcp --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -o $proxy -p tcp --sport 443 -m state --state ESTABLISHED,RELATED -j ACCEPT
```