Mise en place proxy squid

J’installe le paquet squid

Le fichier de conf est /etc /squid /squid.conf

Je modifie le nom du fichier par défaut en mettant squid.conf.old

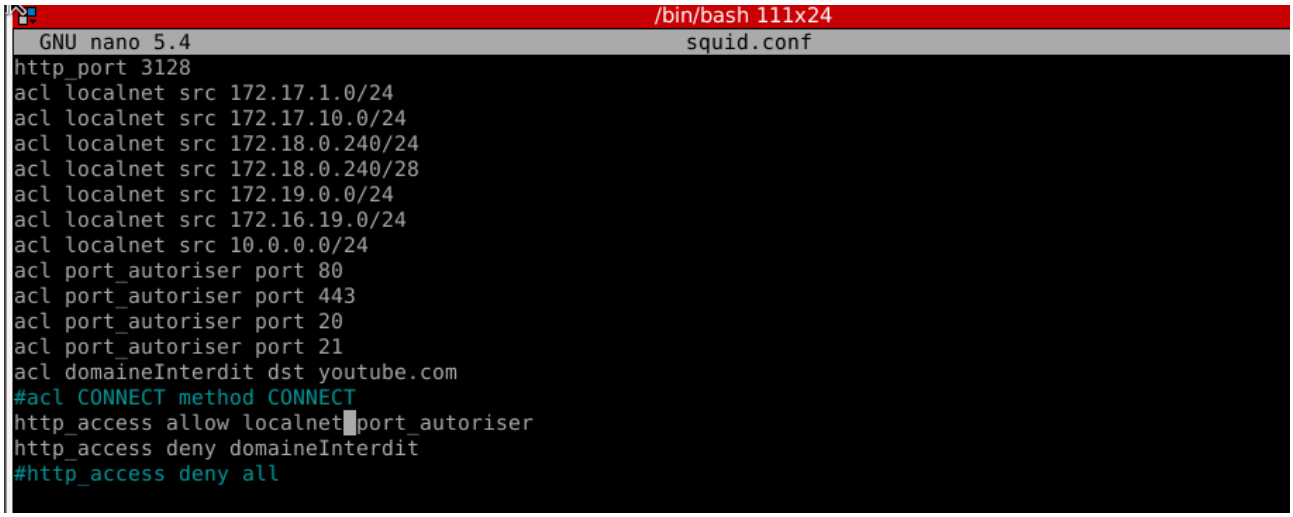
Et je crée un nouveau fichier de conf

Je commence à configurer le proxy je met une ACL qui englobe les adresses des réseaux des différents vlan

Quand on définit une ACL plusieurs réseaux c’est comme les ports sa doit avoir le meme nom au niveau de l’ACL pour pas surcharger la commande http_allow

Donc mon acl qui contiendra tous mes lan s’appellera localnet

et les ports autoriser s’appelleront ports autoriser



J’autorise tous les réseaux avec la directive http_access allow je les autorise de se connecter mais que à destination des ports autorisé

Et je refuse l’accès à d’autre réseau

Je vais sur Firefox paramètre proxy et je mets mon proxy et son port

Ensuite je fais une recherche banale comme wikipedia.org et je regarde les logs

Ça fonctionne parfaitement

```
1631791724.994    406 172.17.1.3 TCP_TUNNEL/200 5427 CONNECT upload.wikimedia.org:443 - HIER_DIRECT/91.198.174.
208 -
1631791725.664   1076 172.17.1.3 TCP_TUNNEL/200 1807 CONNECT upload.wikimedia.org:443 - HIER_DIRECT/91.198.174.
208 -
1631791734.676 170800 172.17.1.3 TCP_TUNNEL/200 6495 CONNECT 42s.s.m28n.net:443 - HIER_DIRECT/95.179.137.167 -
1631791734.676 171399 172.17.1.3 TCP_TUNNEL/200 5127 CONNECT api.n.m28.io:443 - HIER_DIRECT/104.26.10.242 -
1631791735.686 171809 172.17.1.3 TCP_TUNNEL/200 6495 CONNECT fv.s.m28n.net:443 - HIER_DIRECT/45.77.197.201 -
1631791738.504  11011 172.17.1.3 TCP_TUNNEL/200 1964 CONNECT webbouncer-live-v8-0.agario.miniclippt.com:443 - H
IER_DIRECT/54.191.127.113 -
1631791741.479  61014 172.17.1.3 TCP_TUNNEL/200 3792 CONNECT incoming.telemetry.mozilla.org:443 - HIER_DIRECT/5
4.190.205.249 -
1631791742.480  61849 172.17.1.3 TCP_TUNNEL/200 3792 CONNECT incoming.telemetry.mozilla.org:443 - HIER_DIRECT/5
4.190.205.249 -
1631791742.480  61857 172.17.1.3 TCP_TUNNEL/200 3792 CONNECT incoming.telemetry.mozilla.org:443 - HIER_DIRECT/5
4.190.205.249 -
1631791743.967  63501 172.17.1.3 TCP_TUNNEL/200 4062 CONNECT incoming.telemetry.mozilla.org:443 - HIER_DIRECT/5
4.190.205.249 -
1631791755.013 185716 172.17.1.3 TCP_TUNNEL/200 217706 CONNECT 4fi.s.m28n.net:443 - HIER_DIRECT/78.141.221.54 -
1631791755.013 177715 172.17.1.3 TCP_TUNNEL/200 196522 CONNECT 4fi.s.m28n.net:443 - HIER_DIRECT/78.141.221.54 -
1631791767.032    547 172.17.1.3 TCP_TUNNEL/200 731 CONNECT 42s.s.m28n.net:443 - HIER_DIRECT/95.179.137.167 -
1631791767.074    326 172.17.1.3 TCP_TUNNEL/200 349 CONNECT fv.s.m28n.net:443 - HIER_DIRECT/45.77.197.201 -
1631791774.486    299 172.17.1.3 TCP_TUNNEL/200 3964 CONNECT incoming.telemetry.mozilla.org:443 - HIER_DIRECT/3
5.244.247.133 -
root@debianAdel:/etc/squid#
```

Aussi j’avais une fenêtre agario ouverte à la pause qui est aussi dans les logs plus bas

Je vais bloquer maintenant le domaine youtube.com

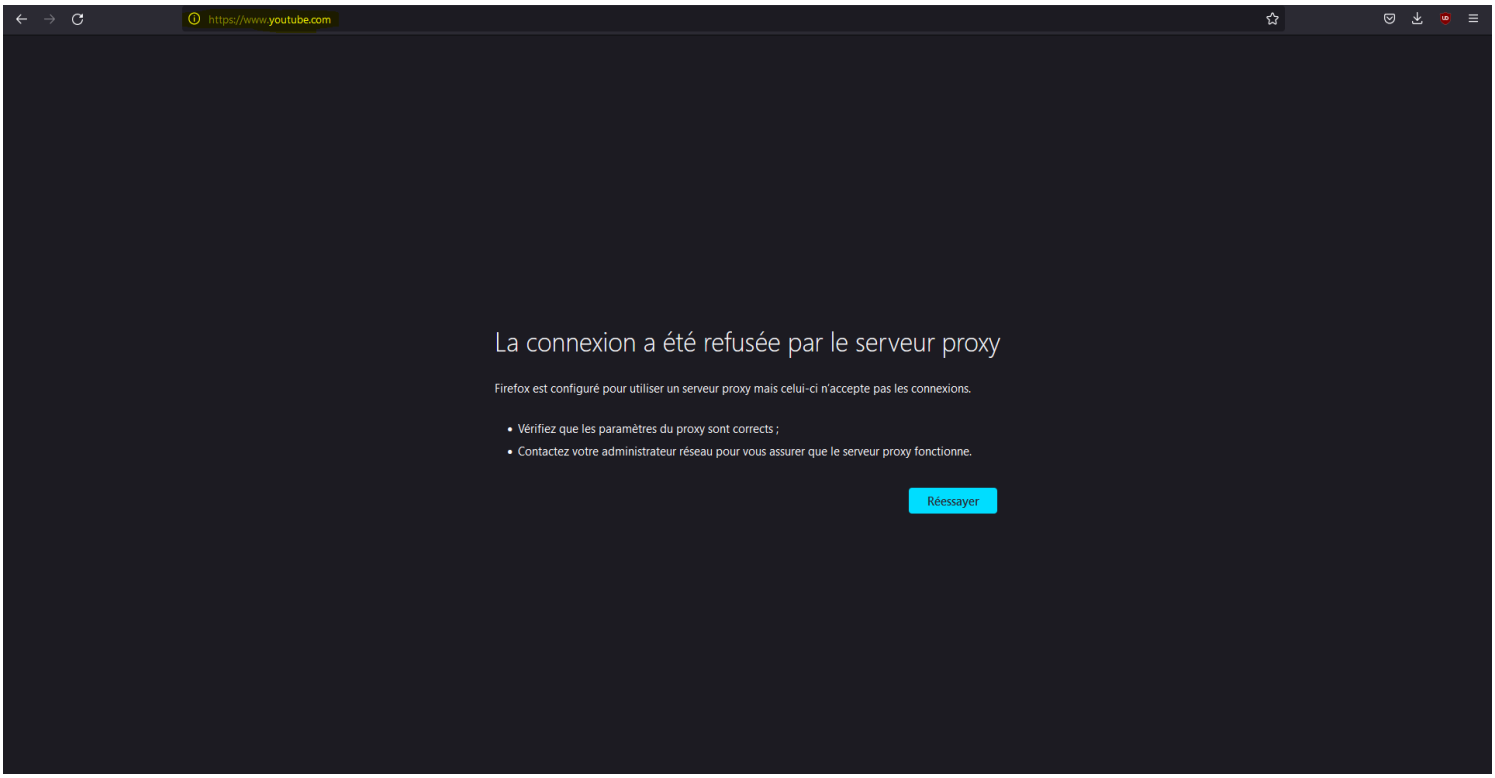
En paramétrant une ACL comme ceci

acl domaineInterdit dsl youtube.com

http_access deny domaineInterdit

```
/bin/bash 111x24
  GNU nano 5.4                                  squid.conf
http_port 3128
acl localnet src 172.17.1.0/24
acl localnet src 172.17.10.0/24
acl localnet src 172.18.0.240/24
acl localnet src 172.18.0.240/28
acl localnet src 172.19.0.0/24
acl localnet src 172.16.19.0/24
acl localnet src 10.0.0.0/24
acl port_autoriser port 80
acl port_autoriser port 443
acl port_autoriser port 20
acl port_autoriser port 21
acl domaineInterdit dst youtube.com
#acl CONNECT method CONNECT
http_access allow localnet port_autoriser
http_access deny domaineInterdit
#http_access deny all
```

Ça fonctionne parfaitement



Je rajoute une authentification sur le proxy

Sa sera la même que sur un serveur web j'installe le paquet apache2-utils

```
http_port 3128
#Authentification squid
#Ici je dis que je fais une authentification NCSA avec les utilisateurs dans le fichier /etc/squid/user
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid/user
#On autorise que 5 connexions simultanées
auth_param basic children 5
#Le texte à afficher lorsque la fenetre d'authentification apparait
auth_param basic realm Authentifiez vous !
#La connexion durera 2 heures apres il faudra ce re-authentifier
auth_param basic credentialsttl 2 hours
#Je crée une ACL qui contiendra l'obliagtion de l'authentification proxy
acl user proxy_auth REQUIRED

acl localnet src 172.17.1.0/24
acl localnet src 172.17.10.0/24
acl localnet src 172.18.0.240/24
acl localnet src 172.18.0.240/28
acl localnet src 172.19.0.0/24
acl localnet src 172.16.19.0/24
acl localnet src 10.0.0.0/24
acl port_autoriser port 80
acl port_autoriser port 443
acl port_autoriser port 20
acl port_autoriser port 21
acl domaineInterdit dst youtube.com
#acl CONNECT method CONNECT
http_access deny domaineInterdit
#Et ici je rajoute user à la fin pour forcer l'authentification proxy
http_access allow localnet port_autoriser user
#http_access deny all
```

Les commentaires dans la photo explique toutes les étapes

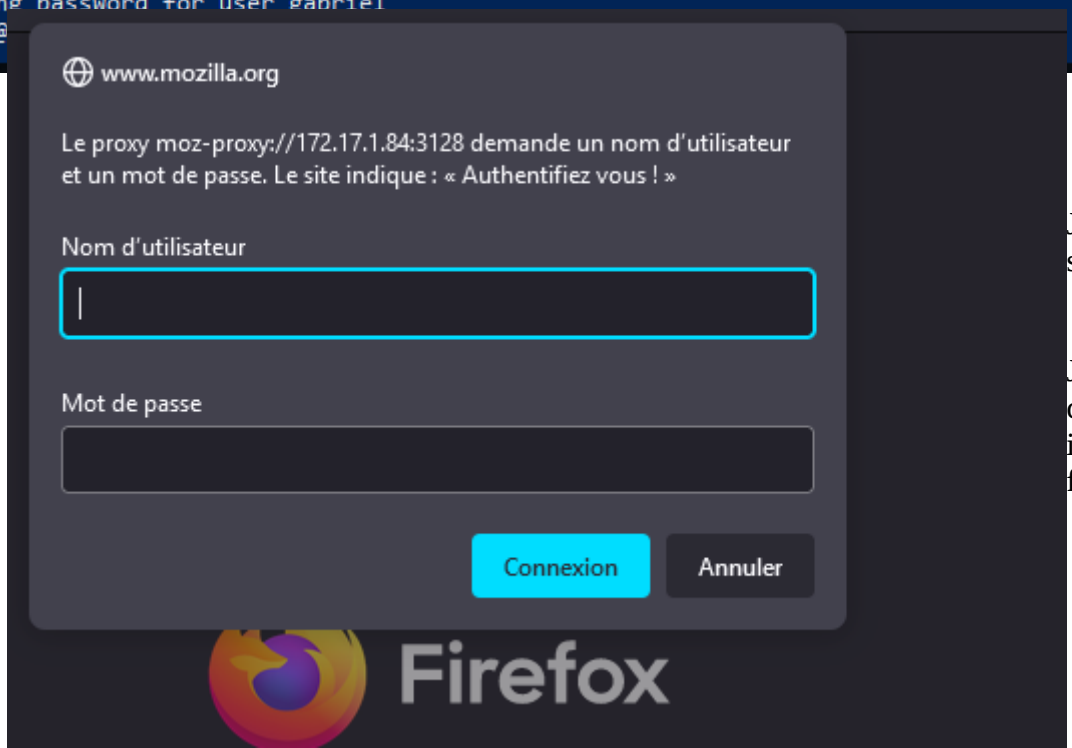
Ensuite je tappe dans le terminal

htpasswd -m *etc*/squid/user <nomUser>

Sa me demandera un mdp je saisis un mdp

le mdp sera siojjr

```
root@debianAdel:/etc/squid# htpasswd -m /etc/squid/user adel
New password:
Re-type new password:
Adding password for user adel
root@debianAdel:/etc/squid# htpasswd -m /etc/squid/user gabriel
New password:
Re-type new password:
Adding password for user gabriel
root@
```



Je relance le serveur squid

J'essaye de me connecter à internet et sa fonctionne

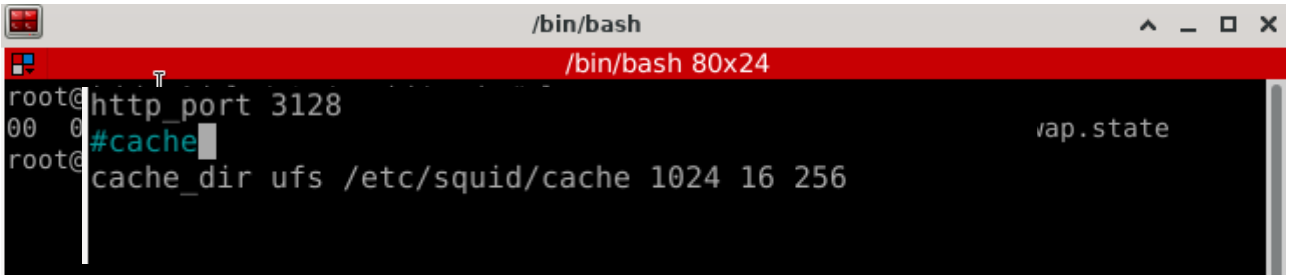
Je vais maintenant mettre au point la fonctionnalité cache du proxy

je vais créer un répertoire cache dans /etc /squid

-Je dois donner les droits corrects sur le répertoire cache

-Ensuite je remarre le proxy

-Je vais dans le proxy cache et plein de répertoire ont été créer



Ufs = c'est le type de disk

Ensuite on place le répertoire cache

Ensuite taille en MO

Puis nombre de réponse et ce qui suit à la fin nombre de sous-réponse

Ensuite je fais tail -f *var/log/squid/access.log*

Et si je vois apparaître TCP MISS /200 quand je me connecte à un nouveau site sa veut dire que le site n'été pas dans le cache et il y a été ajouter

```
^C
root@debianAdel:/etc/squid/cache# tail -f /var/log/squid/
access.log       access.log.2.gz  cache.log.1
access.log.1     cache.log        cache.log.2.gz
root@debianAdel:/etc/squid/cache# tail -f /var/log/squid/access.log
1632466356.918      0 172.17.1.3 NONE/000 0 NONE error:transaction-end-before-headers - HIER_NONE/- -
1632466357.921     49 172.17.1.3 TCP_TUNNEL/200 6277 CONNECT safebrowsing.googleapis.com:443 adel HIER_DIRECT/2
16.58.204.138 -
1632466357.934     12 172.17.1.3 TCP_DENIED/403 4063 CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1632466357.972     99 172.17.1.3 TCP_TUNNEL/200 5518 CONNECT realtime.jeu.video:443 adel HIER_DIRECT/51.158.127
.205 -
1632466358.038     44 172.17.1.3 TCP_TUNNEL/200 4376 CONNECT ssl.gstatic.com:443 adel HIER_DIRECT/142.250.75.22
7 -
1632466358.981      0 172.17.1.3 TCP_DENIED/403 4063 CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1632466358.983      0 172.17.1.3 TCP_DENIED/403 4063 CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1632466360.712     97 172.17.1.3 TCP_MISS/200 1108 POST http://ocsp.sca1b.amazontrust.com/ adel HIER_DIRECT/13.
225.29.204 application/ocsp-response
1632466361.513      8 172.17.1.3 TCP_MISS/200 931 POST http://ocsp.digicert.com/ adel HIER_DIRECT/93.184.220.29
 application/ocsp-response
1632466361.825     81 172.17.1.3 TCP_MISS/200 1108 POST http://ocsp.sca1b.amazontrust.com/ adel HIER_DIRECT/13.
225.29.204 application/ocsp-response
1632466381.829  20357 172.17.1.3 TCP_TUNNEL/200 4327 CONNECT usher.ttvnw.net:443 adel HIER_DIRECT/192.108.239.2
54 -
```

J'ai modifié le chemin du cache dans /var /spool /squid

Ensuite je regarde quelques fichiers dans ce répertoire

Je vais dans le répertoire 00 /00

Ensuite j'affiche les fichiers qu'il y'a dedans

```
/bin/bash 112x38
root@debianAdel:/var/spool/squid/00/00# ls
00000001  00000004  00000006  00000008  0000000A  0000000C  0000000E  00000010
00000003  00000005  00000007  00000009  0000000B  0000000D  0000000F
root@debianAdel:/var/spool/squid/00/00#
```

Le

```
root@debianAdel:/var/spool/squid/00/00# cat 00000009
?.???f??g??     ,z?Raz?Ra????????e??D@8http://igm.univ-mlv.fr/~dr/XPOSE2003/Squid/ch01s02.html
?;HTTP/1.1 200 OK
Date: Tue, 28 Sep 2021 07:08:42 GMT
Server: Apache
Last-Modified: Wed, 26 Jul 2006 18:58:45 GMT
ETag: "2a2c8be-3acd-41980ab29e340"
Accept-Ranges: bytes
Content-Length: 15053
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-15"><title>Pr?sentation de Squi
d</title><meta name="generator" content="DocBook XSL Stylesheets V1.64.1"><link rel="home" href="index.html" tit
le="Yet another Squid pr?sentation !!"><link rel="up" href="ch01.html" title="Chapter?1.?Pr?sentation"><link rel
="previous" href="ch01.html" title="Chapter?1.?Pr?sentation"><link rel="next" href="ch02.html" title="Chapter?2.
?Installation de Squid"></head><body bgcolor="d6e7ef" text="black" link="#0000FF" vlink="#840084" alink="#0000FF
"><div class="navheader"><table width="100%" summary="Navigation header"><tr><td align="left"><img src="logo_I20
0085.gif"></td><th align="center"><h2><u>Pr?sentation de Squid</u></h2></th><td align="right"><img src="logoSqui
d85.gif"></td></tr><tr><td width="20%" align="left"><a accesskey="p" href="ch01.html">Prev</a>?</td><th width="6
0%" align="center">Chapter?1.?Pr?sentation</th><td width="20%" align="right">?<a accesskey="n" href="ch02.html">
Next</a></td></tr></table><hr></div><div class="sect1" lang="en"><div class="titlepage"><div><div><h2 class="tit
```

fichier contient une des pages que j'ai consulter précédemment donc sa veut dire que les pages sont correctement mises dans le cache

Je rajoute une authentification sur le proxy

Sa sera la même que sur un serveur web j'installe le paquet apache2-utils

```
http_port 3128
#Authentification squid
#Ici je dis que je fais une authentification NCSA avec les utilisateurs dans le fichier /etc/squid/user
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid/user
#On autorise que 5 connexions simultanées
auth_param basic children 5
#Le texte à afficher lorsque la fenetre d'authentification apparait
auth_param basic realm Authentifiez vous !
#La connexion durera 2 heures apres il faudra ce re-authentifier
auth_param basic credentialsttl 2 hours
#Je crée une ACL qui contiendra l'obliagtion de l'authentification proxy
acl user proxy_auth REQUIRED

acl localnet src 172.17.1.0/24
acl localnet src 172.17.10.0/24
acl localnet src 172.18.0.240/24
acl localnet src 172.18.0.240/28
acl localnet src 172.19.0.0/24
acl localnet src 172.16.19.0/24
acl localnet src 10.0.0.0/24
acl port_autoriser port 80
acl port_autoriser port 443
acl port_autoriser port 20
acl port_autoriser port 21
acl domaineInterdit dst youtube.com
#acl CONNECT method CONNECT
http_access deny domaineInterdit
#Et ici je rajoute user à la fin pour forcer l'authentification proxy
http_access allow localnet port_autoriser user
#http_access deny all
```

Les commentaires dans la photo explique toute les étapes

Ensuite je tape dans le terminal

htpasswd -m *etc*/squid/user <nomUser>

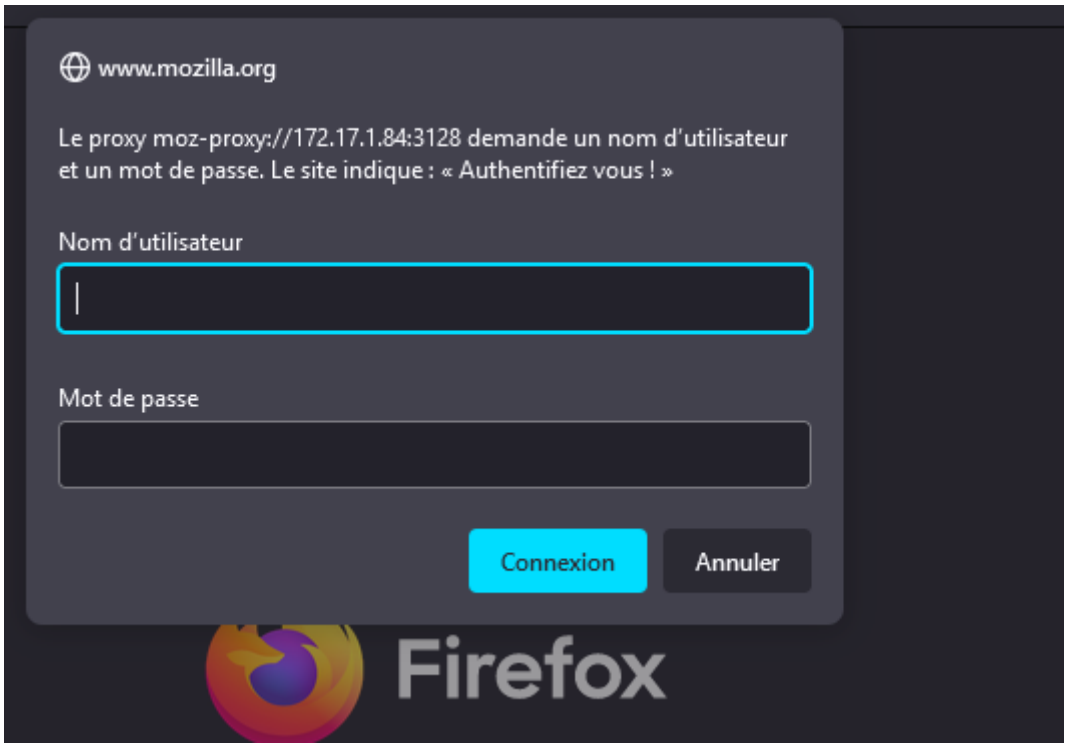
Sa me demandera un mdp je saisis un mdp

Le mdp sera siojjr

```
root@debianAdel:/etc/squid# htpasswd -m /etc/squid/user adel
New password:
Re-type new password:
Adding password for user adel
root@debianAdel:/etc/squid# htpasswd -m /etc/squid/user gabriel
New password:
Re-type new password:
Adding password for user gabriel
root@debianAdel:/etc/squid#
```

Je relance le serveur squid

J’essaye de me connecter à internet et sa fonctionne



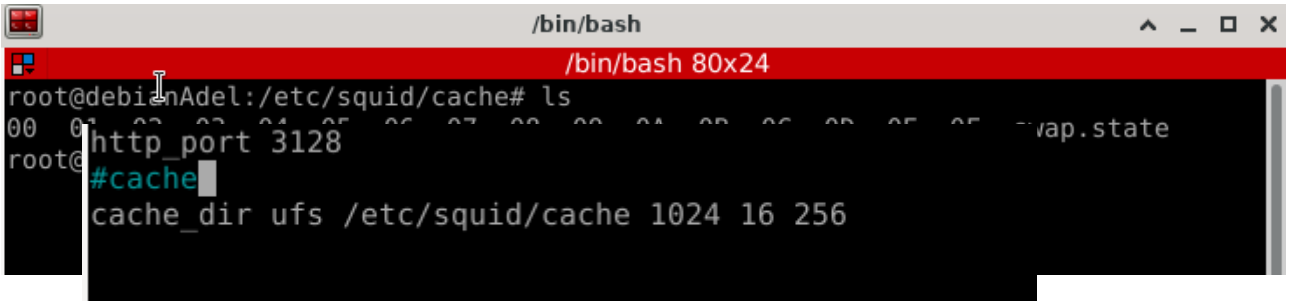
Je vais maintenant mettre au point la fonctionnalité cache du proxy

Je vais créer un répertoire cache dans /etc /squid

-Je dois donner les droits corrects sur le répertoire cache

-Ensuite je remarre le proxy

-Je vais dans le proxy cache et plein de répertoire ont été créer



Ufs = c’est le type de disk

Ensuite on place le répertoire cache

Ensuite taille en MO

Puis nombre de réponse et ce qui suit à la fin nombre de sous-réponse

Ensuite je fais tail -f *var/log/squid/access.log*

Et si je vois apparaître TCP MISS /200 quand je me connecte à un nouveau site sa veut dire que le site n’été pas dans le cache et il y a été ajouter

```
^C
root@debianAdel:/etc/squid/cache# tail -f /var/log/squid/
access.log       access.log.2.gz  cache.log.1
access.log.1     cache.log        cache.log.2.gz
root@debianAdel:/etc/squid/cache# tail -f /var/log/squid/access.log
1632466356.918      0 172.17.1.3 NONE/000 0 NONE error:transaction-end-before-headers - HIER_NONE/- -
1632466357.921     49 172.17.1.3 TCP_TUNNEL/200 6277 CONNECT safebrowsing.googleapis.com:443 adel HIER_DIRECT/2
16.58.204.138 -
1632466357.934     12 172.17.1.3 TCP_DENIED/403 4063 CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1632466357.972     99 172.17.1.3 TCP_TUNNEL/200 5518 CONNECT realtime.jeu.video:443 adel HIER_DIRECT/51.158.127
.205 -
1632466358.038     44 172.17.1.3 TCP_TUNNEL/200 4376 CONNECT ssl.gstatic.com:443 adel HIER_DIRECT/142.250.75.22
7 -
1632466358.981      0 172.17.1.3 TCP_DENIED/403 4063 CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1632466358.983      0 172.17.1.3 TCP_DENIED/403 4063 CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1632466360.712     97 172.17.1.3 TCP_MISS/200 1108 POST http://ocsp.sca1b.amazontrust.com/ adel HIER_DIRECT/13.
225.29.204 application/ocsp-response
1632466361.513      8 172.17.1.3 TCP_MISS/200 931 POST http://ocsp.digicert.com/ adel HIER_DIRECT/93.184.220.29
 application/ocsp-response
1632466361.825     81 172.17.1.3 TCP_MISS/200 1108 POST http://ocsp.sca1b.amazontrust.com/ adel HIER_DIRECT/13.
225.29.204 application/ocsp-response
1632466381.829  20357 172.17.1.3 TCP_TUNNEL/200 4327 CONNECT usher.ttvnw.net:443 adel HIER_DIRECT/192.108.239.2
54 -
```

J’ai modifié mon fichier de configuration pour définir une ACL par vlan pour me mettre de mieux filtrer les différents réseaux indépendamment des autres

```
http_port 3128
visible_hostname smtp.booktic.info
#cache
cache_dir ufs /var/spool/squid 5000 16 256
#cache_dir ufs /etc/squid/cache 5000 16 256
#cache_effective_group root
#cache_log /etc/squid/
#Authentification squid
#Ici je dis que je fais une authentification NCSA avec les utilisateurs dans le fichier /etc/squid/user
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid/user
#On autorise que 5 connexions simultanées
auth_param basic children 5
#Le texte à afficher lorsque la fenetre d'authentification apparait
auth_param basic realm Authentifiez vous !
#La connexion durera 2 heures apres il faudra ce re-authentifier
auth_param basic credentialsttl 2 hours
#Je crée une ACL qui contiendra l'obliagtion de l'authentification proxy
acl user proxy_auth REQUIRED

acl vlandata src 172.17.1.0/24
acl vlanusers src 172.17.10.0/24
#acl localnet src 172.18.0.240/24
acl vlanadmin src 172.18.0.240/28
acl wifi src 172.19.0.0/24
acl vlanwan src 172.16.19.0/24
acl vlantoip src 10.0.0.0/24

acl port_autoriser port 80
acl port_autoriser port 443
acl port_autoriser port 1120
acl port_autoriser port 3427
acl port_autoriser port 3306
acl port_autoriser port 1119
acl port_autoriser port 8085
acl port_autoriser port 8080
acl port_autoriser port 20
acl port_autoriser port 21
#acl domaineInterdit dst youtube.com
#acl CONNECT method CONNECT
#http_access deny domaineInterdit
#Et ici je rajoute user à la fin pour forcer l'authentification proxy
#http_access allow localnet wifi  vlandata port_autoriser
http_access allow wifi
http_access allow vlandata
http_access allow port_autoriser
http_access allow vlanusers
http_access allow vlanadmin
http_access allow vlanwan
http_access allow vlantoip
http_access deny all
```

Je rajoute cette acl : acl safe_ports port 1024-65535 #ports client
Pour autoriser les ports clients

Filtrage des url avec squidguard

Je rajoute ces deux directives qui vont me permettre d'interdire tout téléchargement de fichier mp3 ou mp4 je peux aussi interdit avec cette regex tous les fichiers .img ou .png comme ceci
Acl url_img regex -i \.img$

$ = Pour préciser que c'est la fin de la chaine de caractère

acl url_mp url_regex -i \.mp*$
http_access deny url_mp

```
acl url_mp url regex -i \.mp*$
acl url_img url regex -i \.img$


acl port_autoriser port 80
acl port_autoriser port 443
acl port_autoriser port 1120
acl port_autoriser port 3427
acl port_autoriser port 3306
acl port_autoriser port 1119
acl port_autoriser port 8085
acl port_autoriser port 8080
acl port_autoriser port 20
acl port_autoriser port 21
#acl domaineInterdit dst youtube
#acl CONNECT method CONNECT
#http_access deny domaineInterdi
#Et ici je rajoute user à la fin
#http_access allow localnet wifi
http_access allow wifi
http_access allow vlandata
http_access allow port_autoriser
http_access allow vlanusers
http_access allow vlanadmin
http_access allow vlanwan
http_access allow vlantoip
http_access deny url_mp
http_access deny url_img
```

Ne pas oublier de mettre un tiret du 8 entre url et regex et aussi ne pas mettre (*) après mp mais mettre (3 ou 4) parce que sinon ça ne fonctionne pas après avoir redémarrer si j'essaye de télécharger un fichier mp4 il ne ce télécharge pas

Mise en place de squidguard

D'abord j'installe le paquet squidguard

Je précise le répertoire ou il ya tous les fichiers contenant les domaines bloquer

```
dbhome /app/squid/lib/blacklists
logdir /var/log/squidguard
```

Je crée tous ces répertoires /apps/squid/lib
Ensuite je télécharge la blacklist du « dsi.ut-capitole.fr »
Je la décompresse dans le répertoire lib que je viens de créer

Je vais dans /etc/squidguard/squidguard.conf
Ensuite dans dbhome je mets ceci : dbhome /apps/squid/lib/blacklists

Je paramètre un bloc pour interdire les jeux d'argents

```
dest jeuxargent {
        domainlist gambling/domains
        urllist    gambling/urls
}
```

Ensuite dans les sources je mets tous mes réseaux
Un bloc par réseau

Ici j'ai configuré la source le réseau du vlan 10 et l'acl qui va avec pour les jeux d'argent

```
src vlandata {
       ip   172.17.1.0/24
}

src bar-clients {
       ip             172.16.4.0/26
}
acl{
       landata{
       pass !jeuxargent any
}
       default{
       pass none
       redirect https://qwant.com
}
}
```

Dans acl mettre vlan data pas landata
#Il y'a un ordre à respecter il faut mettre les acl après avoir définis les destinations l'ordre est source > destination > acl

Je configure squid pour que lorsqu'il démarre il lance squidguard et lui renvoie les url demander par les users

```
url_rewrite_program /usr/bin/squidGuard -c /etc/squidguard/squidGuard.conf
url_rewrite_children 5
```

<u>Fonctionnement de squidguard :</u>

Squidguard est un plugin pour squid, squid après avoir appliquer son traitement va renvoyer l'url vers squidGuard et ce dernier va vérifier si l'url est conforme à sa liste de site bloquer si c'st conforme il autorisera le passage si ce n'est pas conforme il interdira le passage et redirigera le client

Ensuite exécuter squidGuard -C all et regarder les logs de squidguard pour voir s'il y'a un problème dans la config

Ensuite il faut regarder les log de squidguard et vérifier qu'il y'a au redémarrage du proxy squid ce message « ready to request »

```
2021-12-09 11:48:22 [41397] init urllist /app/squid/lib/blacklists/gambling/urls
2021-12-09 11:48:22 [41397] INFO: loading dbfile /app/squid/lib/blacklists/gambling/urls.db
2021-12-09 11:48:22 [41397] destblock good missing active content, set inactive
2021-12-09 11:48:22 [41397] destblock local missing active content, set inactive
2021-12-09 11:48:22 [41397] destblock porn missing active content, set inactive
2021-12-09 11:48:22 [41397] INFO: squidGuard 1.6.0 started (1639046902.105)
2021-12-09 11:48:22 [41397] INFO: squidGuard ready for requests (1639046902.106)
```

Je test maintenant ma règle en allant sur betclic un site de paris sportif :

Je rajoute maintenant tous les autres réseaux dans squidGuard :

```
src vlandata {
        ip    172.17.1.0/24
}

src vlanusers {
        ip    172.17.10.0/24
}

src vlanadmin {
        ip    172.18.0.240/28
}

src vlanwifi {
        ip    172.19.0.0/24
}

src vlantoip {
        ip    10.0.0.0/24
}
```

Je définis les destinations redirector strong_redirector et strict_redirector :

```
dest jeuxargent {
        domainlist gambling/domains
        urllist    gambling/urls
}

dest drugs {
        domainlist drugs/domains
        urllist    drugs/urls
}
dest redirection {
        domainlist redirector/domains
        urllist  redirector/urls
}

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

dest strong_redirection {
        domainlist strong_redirector/domains
        urllist  strong_redirector/urls
}
```

Interdire l’accès au vlan 70 (TOIP)

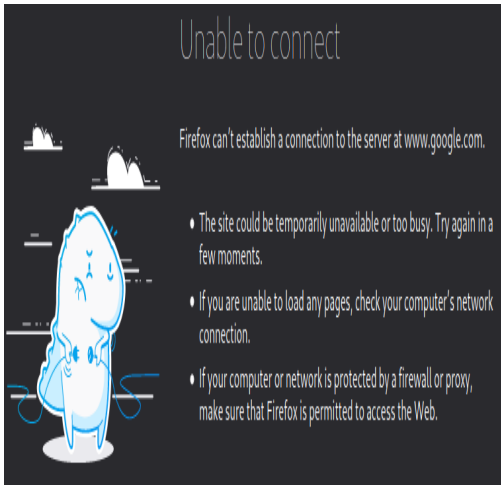
J’ai juste à mettre http_access deny vlantoip

```
#Interdire la sortie au vlan 70
http_access deny vlantoip
```

Je redémarre

Il n’avait pas de relais dhcp dans le vlan 70 je l’ai mis c’était sa le piège

Voilà je n’arrive pas à me connecter depuis le vlan 70, l’acl fonctionne correctement



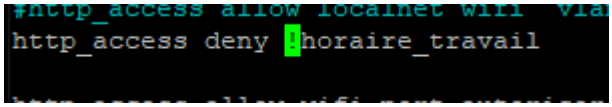
ACL pour autoriser l’accès à des heures précise :

Sa sera des acl de type « time » les jours sont en anglais je vais faire une acl qui autorise les connexions de 8h30 à 19h30 du lundi au vendre

```
#Acl pour autoriser la connexion que du lundu au vendredi de 8h30 a 19h30

acl horaire_travail time M-F 08:30-19:30
```

Je mets cette directive http_access pour interdire tout trafic qui n’est pas dans le laps de temps préciser



Il est 15h25 pour tester l’acl je modifier la limite à 15h00 au lieu de 19h30

L’acl fonctionne mais squid fonctionne comme un pare feu il faut mettre les règles les plus restrictives avant les plus générales pour qu’elles ne se font pas englober par les autres règles
Pour la partie utilisateurs du réseau wifi etc c’est déjà fait