

REPUBLIQUE DU SENEGAL



Un Peuple - Un But - Une Foi



Ministère de l'enseignement supérieur et de la recherche

\*\*\*\*\*

Université Alioune Diop de Bambe

\*\*\*\*\*

UFR : Sciences Appliquées et Technologie de L'Information et de la communication

\*\*\*\*\*

Filière : Système ; Réseaux & Télécommunications (SRT)

**INSTALLATION ET CONFIGURATION D'UN SERVEUR PROXY SQUID**  
**SÉCURISÉ**

Présenté Par :

- ❖ Aminata Dieye
- ❖ Fatou Mbengue
- ❖ Hawa Dembélé
- ❖ Awa Lo

Professeur : Monsieur Diatta

Année académique : 2021 / 2022

# Tables des matières

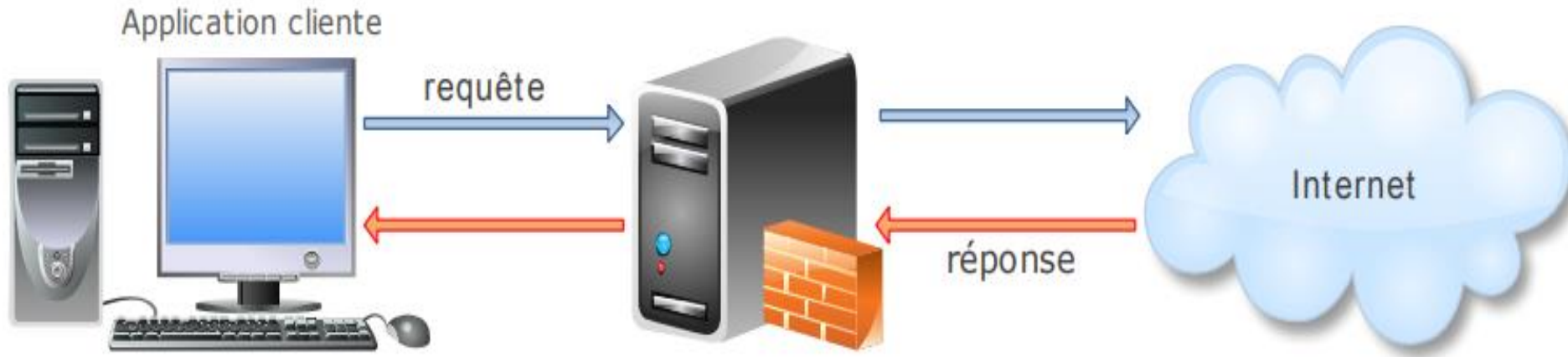
- ▶ **Introduction**
- ▶ **I. FONCTIONNEMENT ET ROLES**
  - ▶ 1. Fonctionnement
  - ▶ 2. Rôles
- ▶ **II. INSTALLATION ET CONFIGURATION DU SERVEUR SQUID**
  - ▶ 1) Installation
  - ▶ 2) Configuration
  - ▶ 3) Contrôle d'accès
- ▶ **III. CONFIGURATION DU CLIENT**
- ▶ **IV. AUTHENTIFICATION NCSA AVEC SQUID**
- ▶ **V. SQUIDGUARD**
- ▶ **Conclusion**

# INTRODUCTION

Un serveur proxy aussi appelé serveur mandataire, est à l'origine d'une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy http Tel que squid qui est capable d'utiliser les protocoles FTP, HTTP, HTTPS. C'est un logiciel libre sous la licence GNU GPL.

# 1. FONCTIONNEMENT ET ROLES

## 3. Fonctionnement



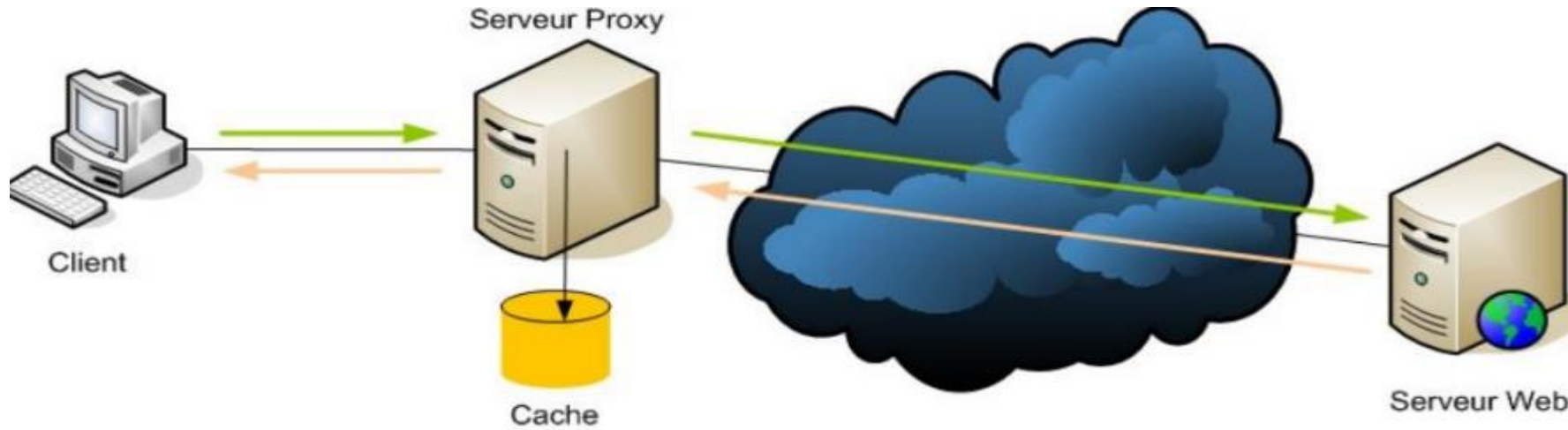
Lorsque vous vous connectez à l'internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy. Celui-ci émet une requête en votre nom, récupère la réponse du serveur web et vous transmet les données de la page Web afin que vous puissiez l'afficher dans votre navigateur.

## Suite Fonctionnement

- Lorsque le serveur proxy transmet vos requêtes Web, il peut réaliser des modifications sur les données que vous avez envoyées tout en vous faisant parvenir les informations que vous attendez. Un serveur proxy peut modifier votre adresse IP, Il peut chiffrer vos données, ce qui les rend invisibles. Et enfin, un serveur proxy peut bloquer l'accès à certaines pages Web en se basant sur leurs adresses IP.

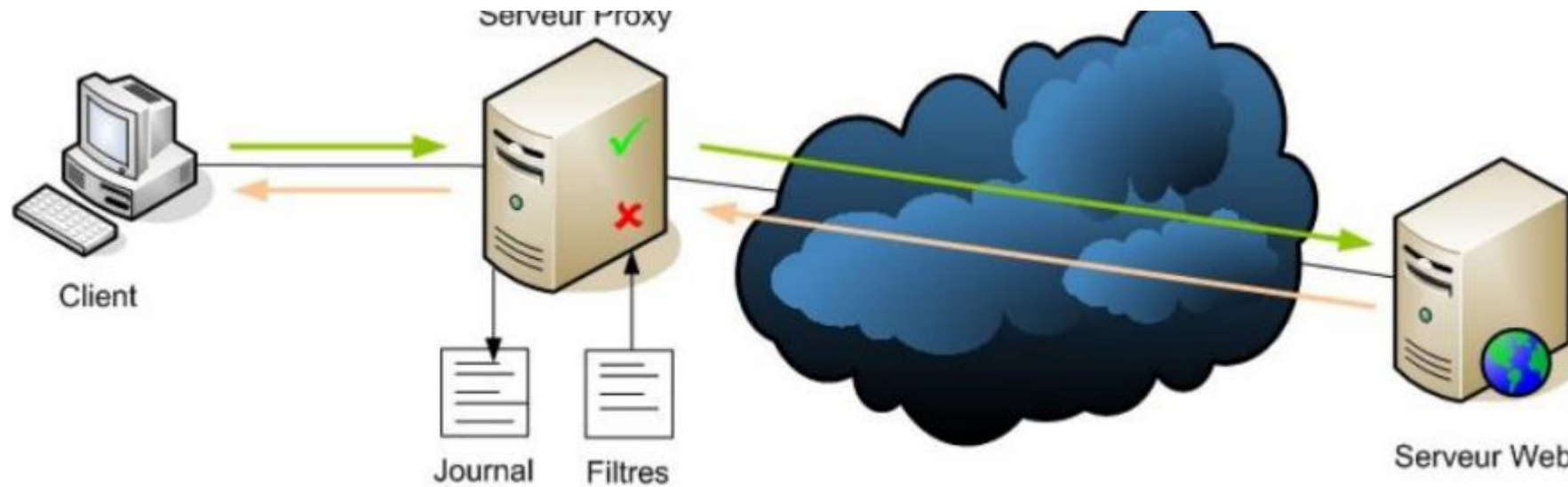
## 4. Rôles

### ➤ LE CACHE :



La plupart des proxys assurent ainsi une fonction de cache, c'est-à-dire la capacité à garder en mémoire (en "cache") les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir leur fournir le plus rapidement possible.

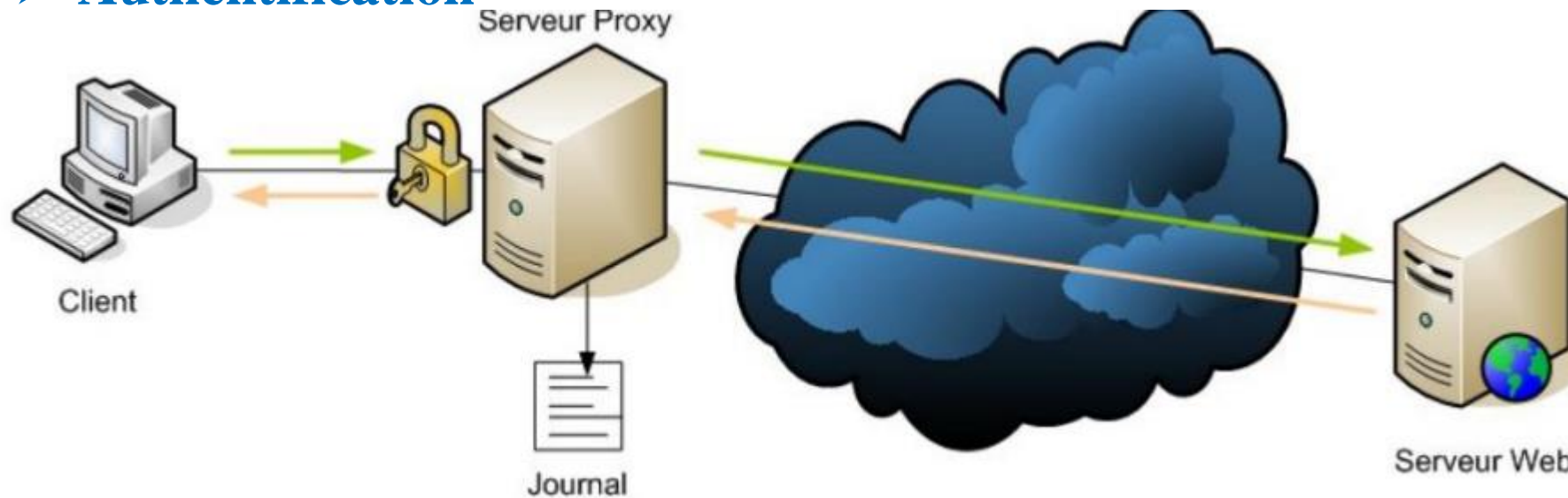
## ► LE Filtrage



- D'autre part, grâce à l'utilisation d'un proxy, il est possible d'assurer un suivi des connexions via la constitution de journaux d'activité (logs) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet. Il est ainsi possible de filtrer les connexions à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs.



## ➤ Authentification



il est parfois possible d'utiliser le proxy pour authentifier les utilisateurs, c'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés.



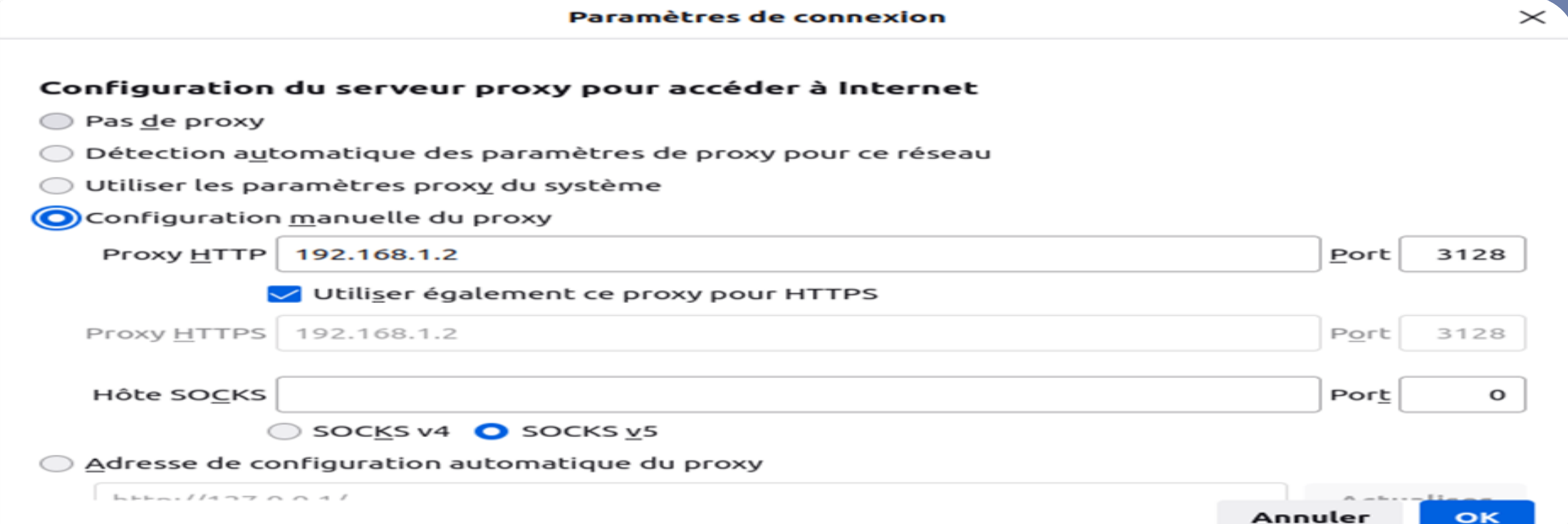
## II. INSTALLATION ET CONFIGURATION DU SERVEUR SQUID

### 4) Installation

- ▶ Le téléchargement des paquets se fait avec la commande `apt-get install squid`
- ▶ Pour voir l'état du processus squid on tape la commande `sudo service squid status`
- ▶ Ensuite on tue le processus en faisant `sudo pkill-9 squid`
- ▶ Enfin on désactive squid avec `sudo service squid stop`

## 5) Configuration

Le nom du fichier de configuration s'appelle squid.conf et se trouve dans /etc/squid. Il est important de faire une copie de la configuration avant toute modification pour cela il faut se placer dans le fichier squid grâce à la commande `cd /etc/squid` et taper la commande `sudo cp squid.conf squid.conf.originale`. Avant d'éditer le fichier de configuration nous allons d'abord choisir de configurer manuellement le serveur proxy.



The screenshot shows a window titled "Paramètres de connexion" with a close button (X) in the top right corner. The window contains the following configuration options:

- 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:  Port:
- ☒ Utiliser également ce proxy pour HTTPS
- Proxy HTTPS:  Port:
- Hôte SOCKS:  Port:
- ☐ SOCKS v4 ☒ SOCKS v5
- ☐ Adresse de configuration automatique du proxy:

At the bottom right, there are two buttons: "Annuler" (grey) and "OK" (blue).

- Dans le fichier de configuration on a indiqué le nom de notre machine dans TAG : `visible_hostname`




```
6044 # TAG: visible_hostname
```

```
6045 visible_hostname hawa-HP-EliteBook-820-G1
```

```
6046 # If you want to present a special hostname in error messages, etc,
```

```
6047 # define this. Otherwise, the return value of gethostname()
```

```
6048 # will be used. If you have multiple caches in a cluster and
```



```
6049 # get errors about IP-forwarding you must set them to have individual
```

```
6050 # names with this setting.
```

```
6051 #Default:
```

- On commente toutes les lignes contenant ACL localnet sauf la ligne contenant notre adresse réseau.

```
1199 #acl localnet src 169.254.0.0/16      # RFC 3927 link-local (directly plugged) machines
1200 #acl localnet src 172.16.0.0/12        # RFC 1918 local private network (LAN)
1201 #acl localnet src 192.168.1.0/24       # RFC 1918 local private network (LAN)
1202 #acl localnet src fc00::/7             # RFC 4193 local private network range
1203 #acl localnet src fe80::/10            # RFC 4291 link-local (directly plugged) machines
1204
```

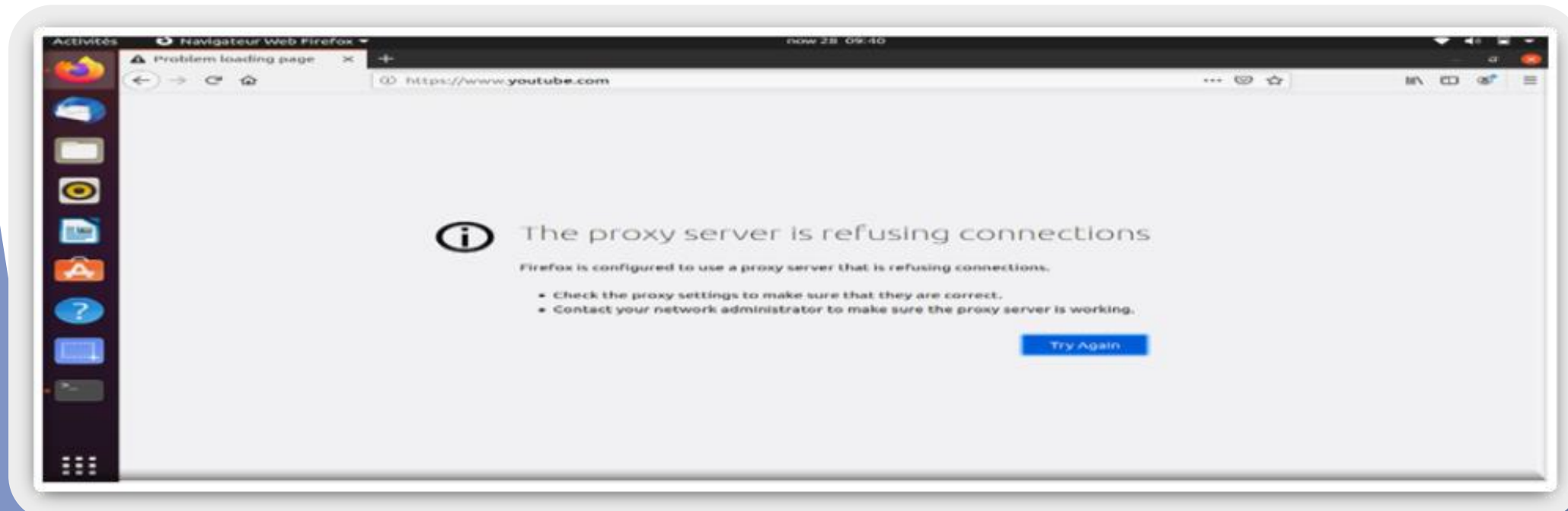
```
1421 # from where browsing should be allowed
1422 http_access allow localnet
1423 http_access allow localhost
1424
1425 # And finally deny all other access to this proxy
```

- ▶ Par défaut tous les sites sont bloqués au niveau du fichier de configuration

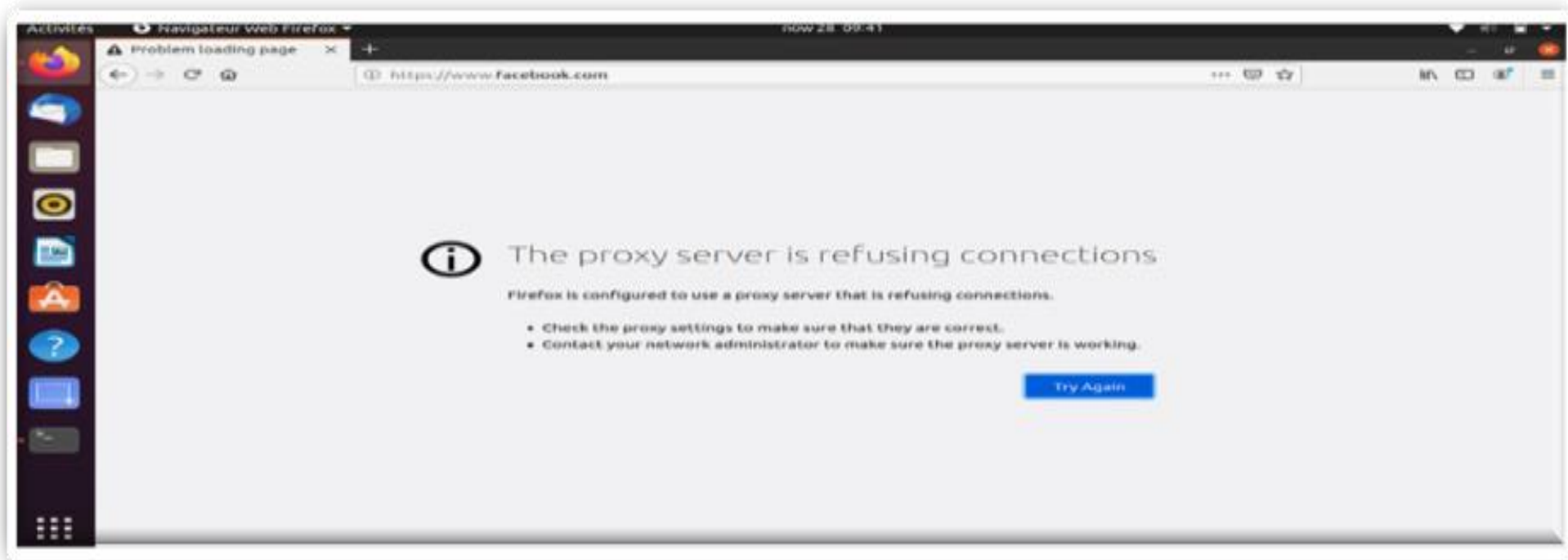
```
1410 http_access allow localhost
1411
1412 # And finally deny all other access to this proxy
1413 http_access deny all
1414
1415 # TAG: adapted_http_access
1416 #      Allowing or Denying access based on defined access lists
```

EN guise d'exemple nous avons essayé d'accéder à des sites tel que YouTube, Facebook, et Yahoo.

- YouTube

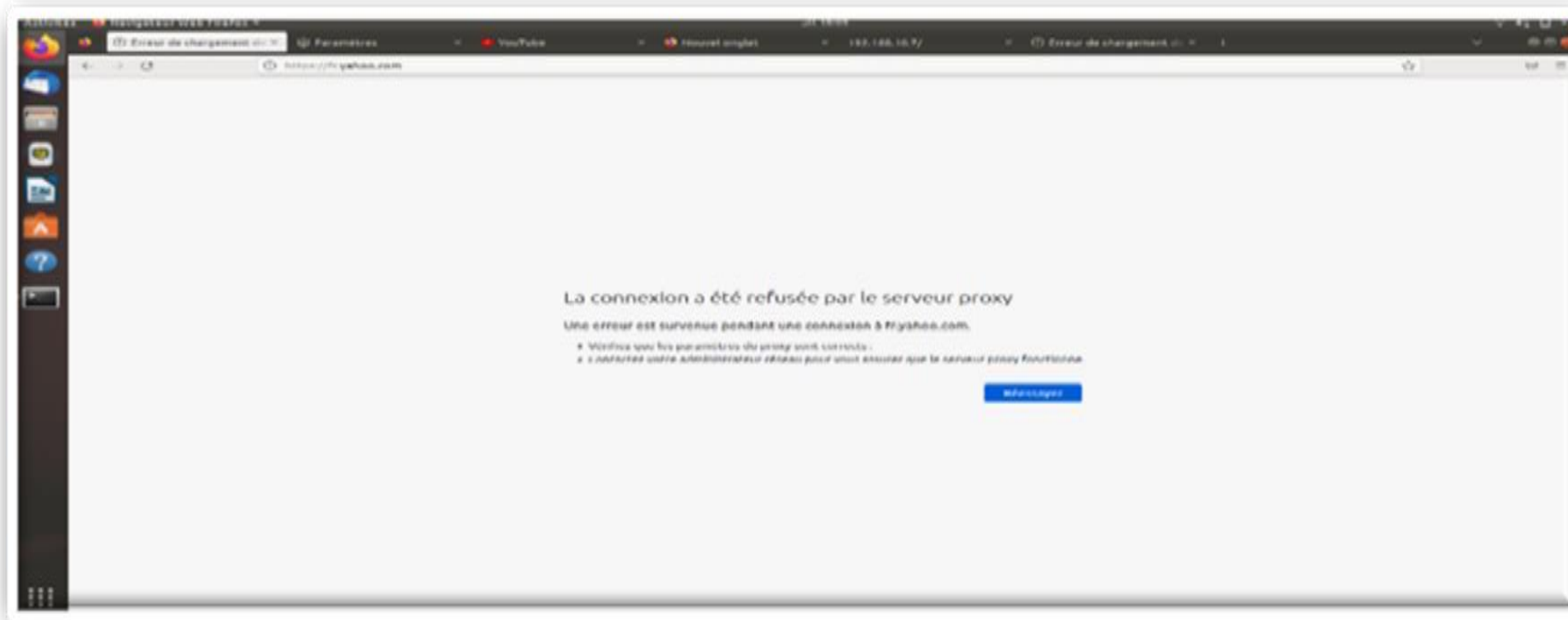


- Facebook



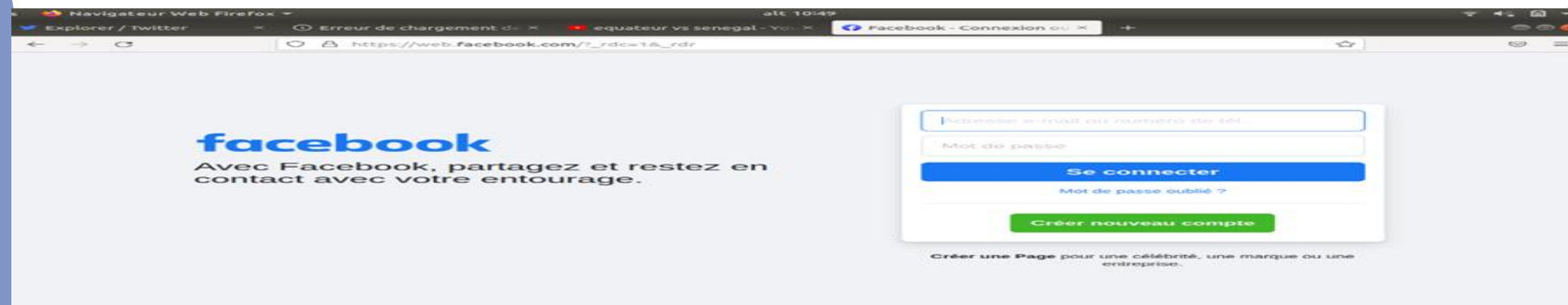


- Yahoo

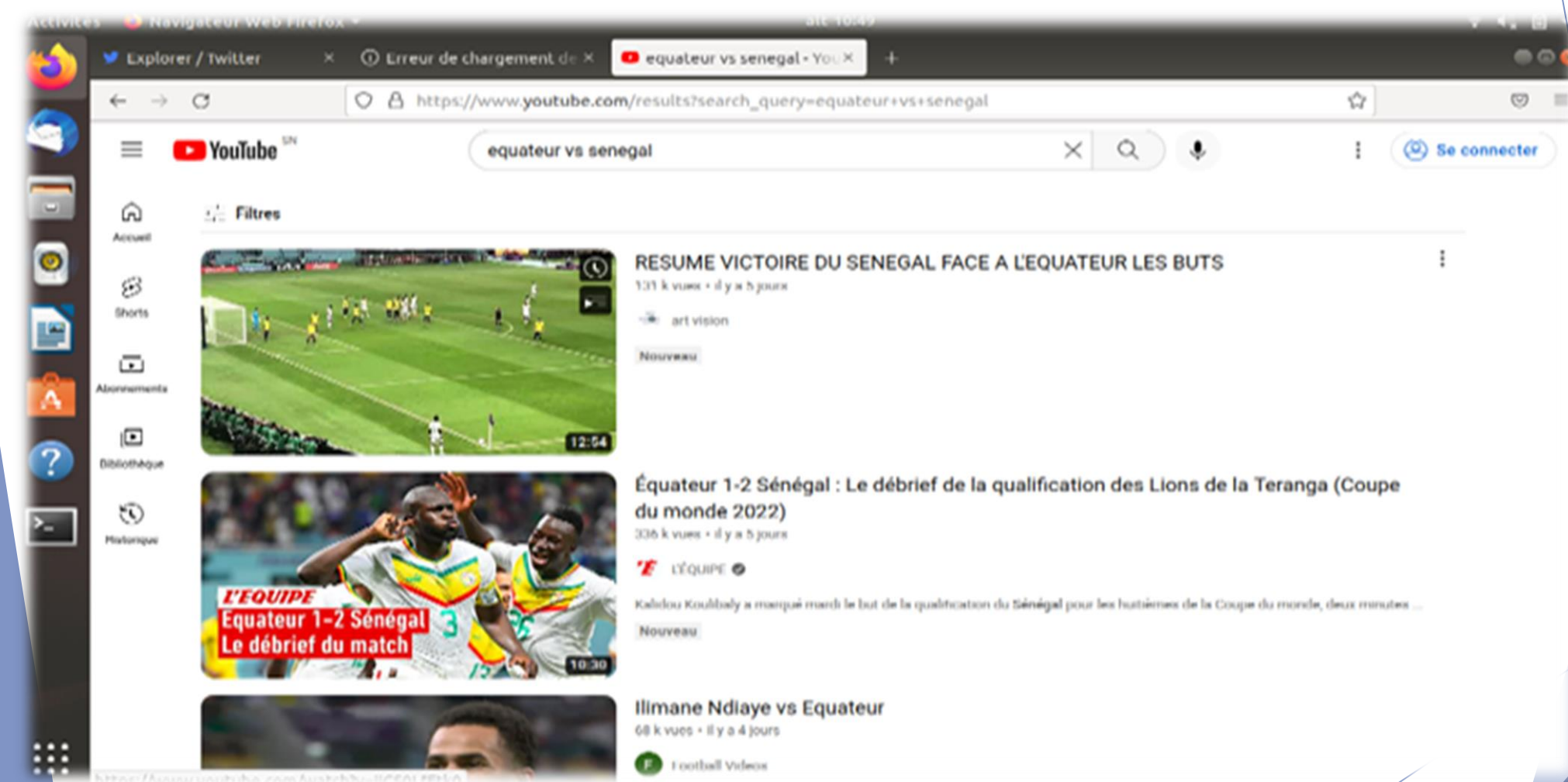




Maintenant on décommente la ligne contenant deny all, de ce fait tous les sites sont à nouveau autorisés





- YouTube



## 6) Contrôle d'accès

- ▶ Les ACL (Access Control Lists) permettent de définir des conditions sur les IPs, les ports, le contenu de certains textes, etc. nous donnerons des exemples ci-dessous ; cela ne signifie pas du tout que ce soient les seuls disponibles.

- *Autoriser l'accès A Internet A Certaines Machines*



```
849 # acl aclname src ip-address/mask ... # clients ip address [fast]
849 acl myclients src 192.168.1.0/24
850 # acl aclname src addr1-addr2/mask ... # range of addresses [fast]
851 acl myclient1 src 192.168.1.3
852 acl myclient2 src 192.168.1.4
853 acl myclient3 src 192.168.1.5
854 acl myclient4 src 192.168.1.6
855 acl localsrv dstdomain 192.168.1.2
```

```
1420 # And finally deny all other access to this proxy
1421 http_access allow all
1422 http_access allow myclients
1423 http_access allow myclient1
1424 http_access allow myclient2
1425 http_access allow myclient3
1426 http_access allow myclient4
1427 # TAG: adapted http_access
1428 # Allowing or Denying access based on defined access lists
1429 #
1430 # Essentially identical to http_access, but runs after redirectors
```

## ➤ Restreindre l'accès Selon Les Heures Et Jour

```
Ouvrir  *squid.conf  Enregistrer  -  ⌵
/etc/squid

921 #      # cache_peer_access mycache.mydomain.net allow asexample
922 #      # cache_peer_access mycache.mydomain.net deny all
923 #
924 #      acl aclname peername myPeer ...
925 #      acl aclname peername_regex [-i] regex-pattern ...
926 #      # [fast]
927 #      # match against a named cache_peer entry
928 #      # set unique name= on cache_peer lines for reliable use.
929 #
930 #      acl aclname time [day-abbrevs] [h1:m1-h2:m2]
931 #      acl regular_day time MTWHFA 07:00-20:00
932 #      acl morning_time 07:00-12:00
933 #      acl lunch time 12:01-17:00
934 #      acl night time 17:01-20:00
935 #      # [fast]
936 #      # day-abbrevs:
937 #      #   S - Sunday
938 #      #   M - Monday
939 #      #   T - Tuesday
940 #      #   W - Wednesday
941 #      #   H - Thursday
942 #      #   F - Friday
943 #      #   A - Saturday
944 #      # h1:m1 must be less than h2:m2
```

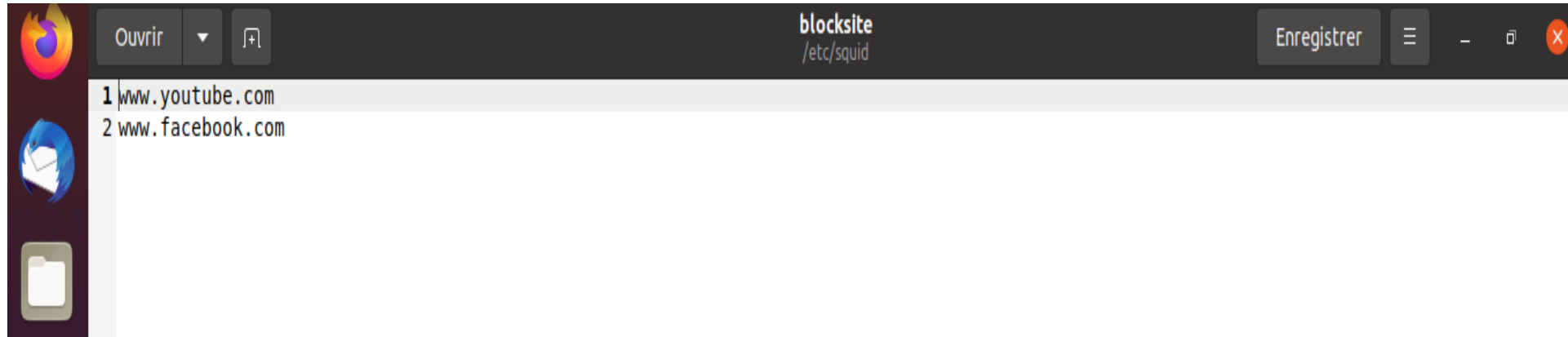
### ➤ autoriser certains client a utiliser le cache a des heures précis

La règle ci-dessus donne l'accès à la machine myclient1 aux heures du matin et du soir ; mais myclient2 n'accède qu'au heures du matin, myclient3 et myclient4 n'accèdent, respectivement, qu'à l'après midi et au soir.

```
1434 http_access allow myclient1 morning night
1435 http_access allow myclient2 morning
1436 http_access allow myclient2 night
1437 http_access allow myclient3 lunch
1438 http_access allow myclient4 night
```

## ➤ Interdire les site

On crée un fichier blocksite dans le répertoire /etc /squid



Puis on bloque les sites contenus dans blocksite

```
414 #acl localnet src 127.0.0.1
415 acl blocksite dstdomain "/etc/squid/blocksite"
416 http_access deny blocksite
417 #http_access deny all
418
419 # Example rule allowing access from your local networks.
420 # Adapt localnet in the ACL section to list your (internal) IP networks
```



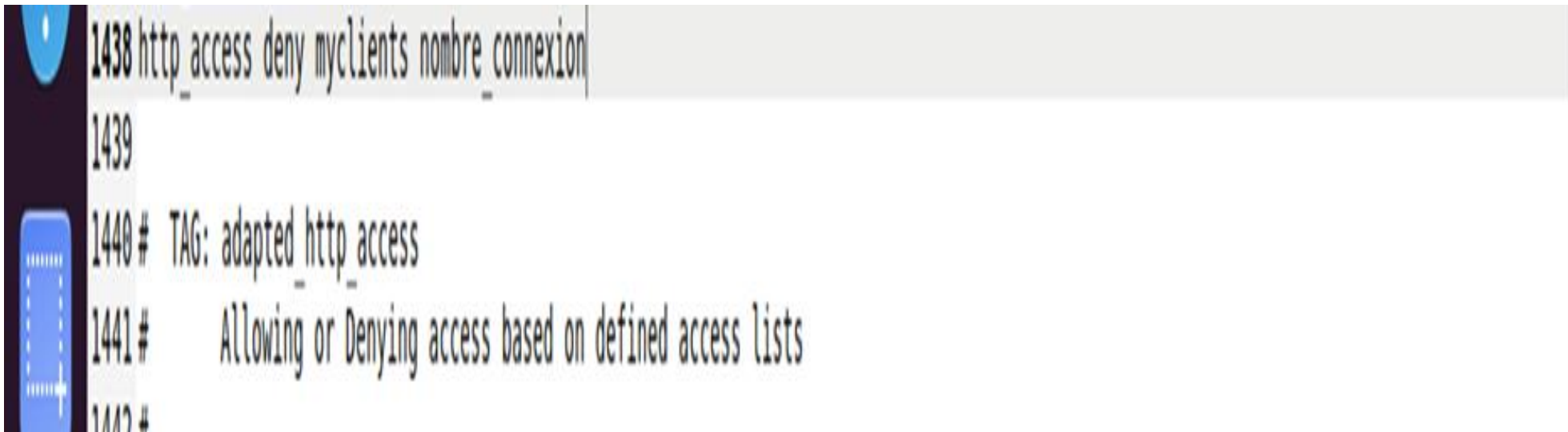
## ➤ Limitation Du Nombre De Connexion d'une Machine

Squid peut limiter le nombre de connexions d'une machine cliente grâce à l'élément maxconn.

```
8349
8350 # TAG: client_db    on|off
8351 #   If you want to disable collecting per-client statistics,
8352 #   turn off client_db here.
8353 #Default:
8354 client_db on
8355
```

```
1005 # #
1006 # #   acl snmppublic snmp_community public
1007 #
1008 #   acl nombre_connexion maxconn 10
1009 #   # This will be matched when the client's IP address has
1010 #   # more than <number> TCP connections established. [fast]
```

- L'ACL maxconn utilise la comparaison "inférieur à". Elle s'active lorsque le nombre de connexion est plus grand que la valeur donnée. C'est pourquoi elle n'est pas utilisée avec la

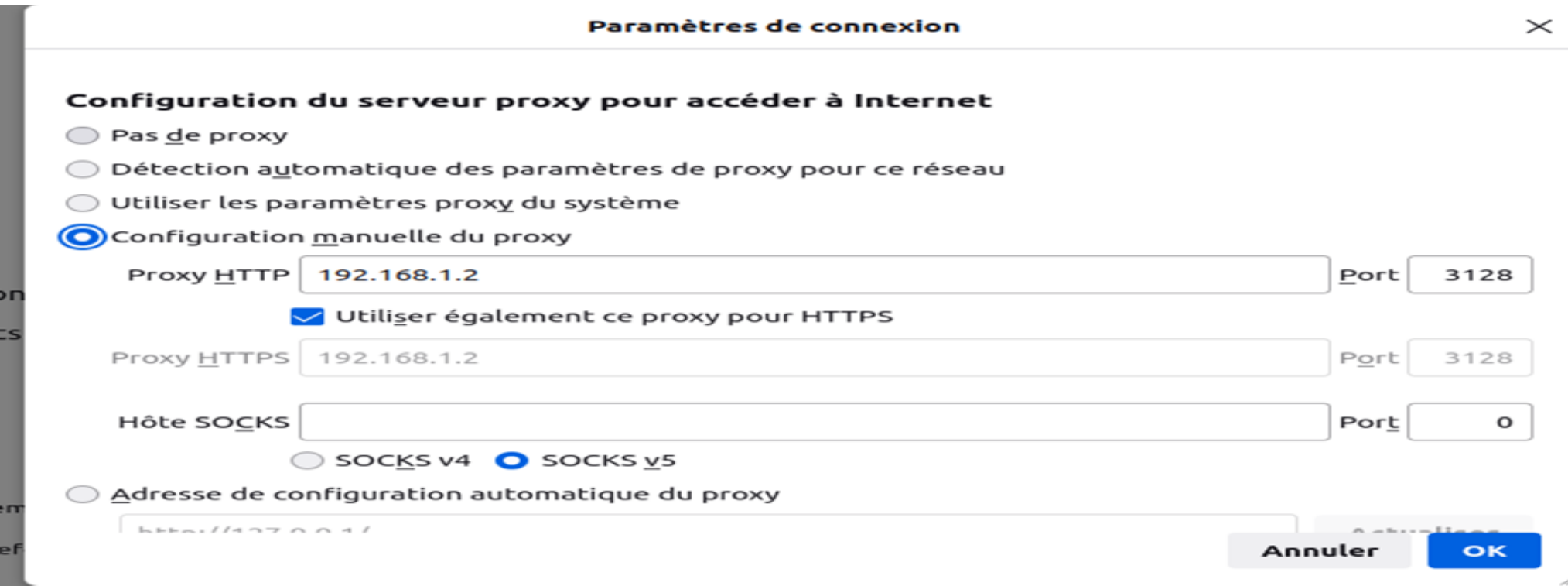
A screenshot of a network configuration interface, likely from a Mikrotik WinBox. The interface shows a list of configuration steps for setting up an ACL. The first step, labeled '1438', is 'http\_access deny myclients nombre\_connexion'. The second step, labeled '1439', is empty. The third step, labeled '1440 #', is 'TAG: adapted\_http\_access'. The fourth step, labeled '1441 #', is 'Allowing or Denying access based on defined access lists'. The fifth step, labeled '1442 #', is empty. The interface has a blue sidebar on the left with icons for various network functions.

```
1438 http_access deny myclients nombre_connexion|
1439
1440 # TAG: adapted_http_access
1441 #   Allowing or Denying access based on defined access lists
1442 #
```



### III. CONFIGURATION DU CLIENT

► Puisque le service fourni utilise un port particulier du serveur, les machines clientes doivent bien sûr être configurées en conséquence. Nous supposons que ces machines sont déjà connectées sur le réseau local (avec une adresse IP valide) et sont capables d'établir un 'Ping' vers le serveur Linux.



The screenshot shows a window titled "Paramètres de connexion" with a close button (X) in the top right corner. The main heading is "Configuration du serveur proxy pour accéder à Internet". There are four radio button options: "Pas de proxy", "Détection automatique des paramètres de proxy pour ce réseau", "Utiliser les paramètres proxy du système", and "Configuration manuelle du proxy". The "Configuration manuelle du proxy" option is selected. Below this, there are three sections for proxy configuration. The first section is for HTTP proxy, with a text box containing "192.168.1.2" and a "Port" box containing "3128". A checkbox labeled "Utiliser également ce proxy pour HTTPS" is checked. The second section is for HTTPS proxy, with a text box containing "192.168.1.2" and a "Port" box containing "3128". The third section is for SOCKS proxy, with a text box for "Hôte SOCKS" and a "Port" box containing "0". Below the SOCKS host box, there are two radio button options: "SOCKS v4" and "SOCKS v5", with "SOCKS v5" selected. At the bottom, there is an unchecked radio button for "Adresse de configuration automatique du proxy" with a text box containing "http://127.0.0.1/". At the bottom right, there are two buttons: "Annuler" and "OK".

**Paramètres de connexion** X

**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  Port

☒ Utiliser également ce proxy pour HTTPS

Proxy HTTPS  Port

Hôte SOCKS  Port

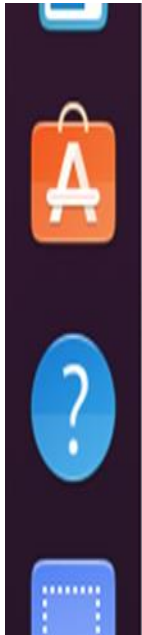
☐ SOCKS v4 ☒ SOCKS v5

☐ Adresse de configuration automatique du proxy

Annuler OK

## IV. AUTHENTIFICATION NCSA AVEC SQUID

- L'Authentification NCSA(National center for supercomputing Applications) permet de faire le contrôle sur les utilisateurs Pour utiliser l'authentification NCSA (pop-up d'authentification), il faut au préalable installer le paquet apache2-utils avec la commande `apt-get install apache2-utils` Cette commande est nécessaire pour utiliser `htpasswd` qui est une commande qui permet d'ajouter des utilisateurs.



```
1414
1415
1416 auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/users
1417 auth_param basic children 10
1418 auth_param basic realm merci de vous identifier sur notre proxy
1419 auth_param basic credentialsttl 3 hours
1420
1421 acl users proxy_auth REQUIRED
1422
1423 http_access deny !users
1424
```

- ▶ Dans le fichier squid.conf, dans la partie TAG : auth\_param décommenter les lignes :
- ▶ Auth\_param basic program /usr/lib/squid/ncsa\_auth /etc/squid/users pour
- ▶ Autoriser l'authentification ncsa sur le fichier users.

- ▶ `Auth_param realm Squid proxy-caching web server` : texte qui apparaîtra
- ▶ Dans la demande d'authentification.
- ▶ `Auth_param credentialsttl 3 hours` : durée de vie de l'authentification.
- ▶ `Auth_param children 10` : nombre d'utilisateur autorisé à s'authentifier

rajouter les lignes suivantes :

```
Acl users proxy_auth REQUIRED
```

```
http_access deny !users
```

- ▶ Ajouter des utilisateurs avec la commande `htpasswd -b /etc/squid/ users <nom de l'utilisateur>`

The SHA algorithm does not use a salt and is less secure than the MD5 algorithm.

```
root@hawa-HP-EliteBook-820-G1:/etc/squid# htpasswd -b users fatou fatou
```

Updating password for user fatou

```
root@hawa-HP-EliteBook-820-G1:/etc/squid# htpasswd -b users amina amina
```

Updating password for user amina

```
root@hawa-HP-EliteBook-820-G1:/etc/squid# htpasswd -b users awa awa
```

Updating password for user awa

```
root@hawa-HP-EliteBook-820-G1:/etc/squid# htpasswd -b users hawa hawa
```

Adding password for user hawa

```
root@hawa-HP-EliteBook-820-G1:/etc/squid#
```

- On ajoute un acl pour les utilisateurs créés dans squid.conf

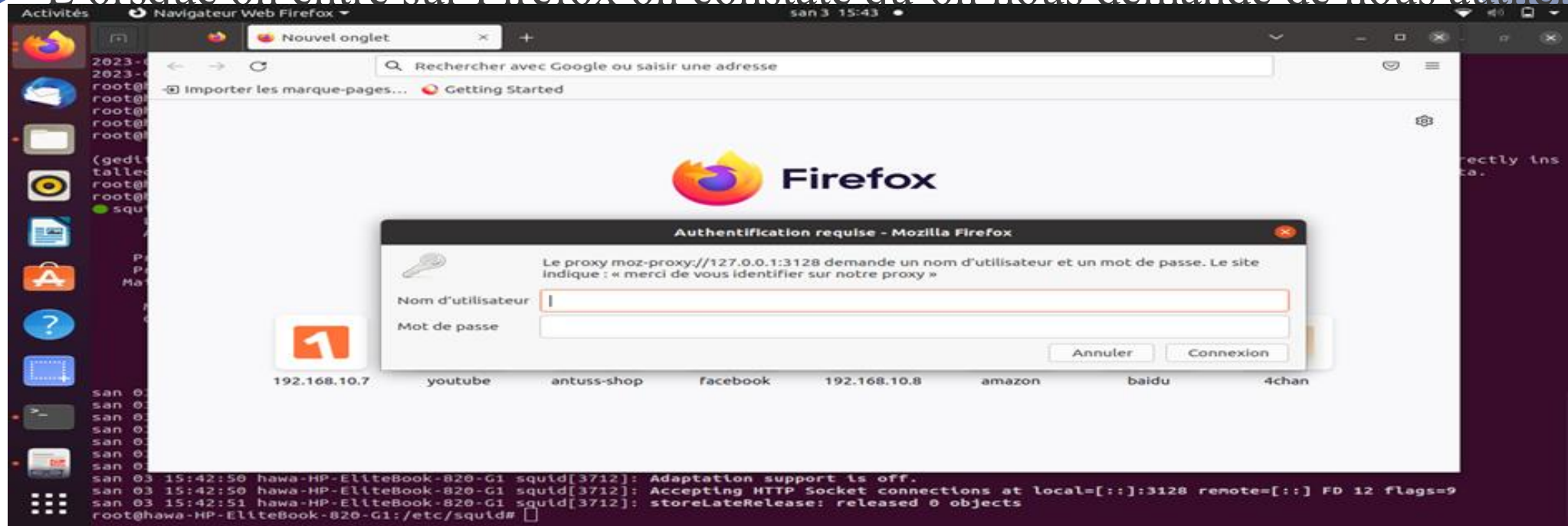
```
1418 auth_param basic realm merci de vous identifier sur notre proxy
1419 auth_param basic credentialsttl 3 hours
1420
1421 acl users proxy_auth REQUIRED
1422
1423 http_access deny !users
1424
```

- On ajoute http\_access allow localnet users

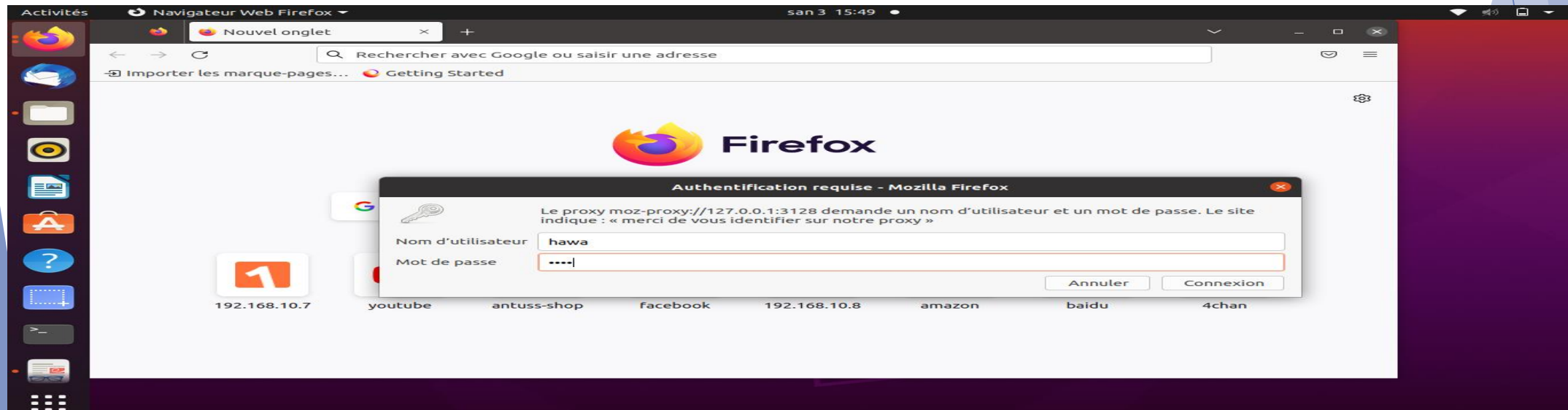
```
1439 http_access allow myclient4 night
1440 http_access deny myclients nombre_connexion
1441 http_access allow localnet users
1442
1443 # TAG: adapted_http_access
1444 #     Allowing or Denying access based on defined access lists
```



- Lorsque on entre sur Firefox on constate qu'on nous demande de nous authentifier



- Hawa étant l'un des utilisateurs , elle peut ainsi se connecter a l'aide de son mot de passe





# *squidGuard*

- ▶ Squidguard est un plug-in de Squid. Il permet de filtrer les pages consultées par les utilisateurs.
- ▶ On peut définir des groupes d'utilisateurs à partir de leurs logins (authentification réalisée par
- ▶ Squid) ou d'adresses IP sources (fixe, réseau, ou à partir d'un fichier de la base de données).

# *SquidGuard*

- ▶ SquidGuard propose un filtrage très puissant d'accès au web, en fonction :
- ▶ De groupes d'utilisateurs, définis de diverses manières. Ici, nous nous baserons sur des IPs ou des groupes d'IPs, mais il est possible d'utiliser l'identification des utilisateurs mise en place sur Squid ;
- ▶ de listes de domaines et d'URL qui serviront à définir soit des cibles autorisées, soit des cibles interdites ;
- ▶ de plages horaires pendant lesquelles l'accès sera autorisé ou interdit

# INSTALLATION

- ▶ Installation de SquidGuard: `apt-get install squidguard`
- ▶ Dans un premier temps, il faut ajouter la ligne suivante dans le fichier de configuration de Squid pour qu'il prenne en compte SquidGuard : `url_rewrite_program /usr/bin/squidGuard`
- ▶ Le fichier de configuration squidguard se trouve comme pour squid dans le répertoire `/etc/squid/` il se nomme `squidGuard.conf`
- ▶ Squidguard utilise des blacklists dans lesquels se trouvent tous les sites interdits par catégorie. Ils sont mise à jour régulièrement et téléchargeable sur le site <http://cri.univ-tlse1.fr/blacklists/>

# *CONFIGURATION*

- ▶ on télécharge les blacklists avec la commande
- ▶ Wget <http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz>
- ▶ On décompacte, un repertoire blacklists est alors crée
- ▶ Tar zxvf blacklists.tar.gz
- ▶ On crée un lien symbolique pour garder la notion de dest :
- ▶ In -s blacklists dest

# squidGuard

```
Activités Terminal des 10 10:55
root@hawa-HP-EliteBook-820-G1: /etc/squid

root@hawa-HP-EliteBook-820-G1:/etc/squidguard# cd /var/lib/squidguard/db
root@hawa-HP-EliteBook-820-G1:/var/lib/squidguard/db# wget http://dsl.ut-capitole.fr/blacklists/download/blacklists.tar.gz
--2022-12-10 10:22:55-- http://dsl.ut-capitole.fr/blacklists/download/blacklists.tar.gz
Résolution de dsl.ut-capitole.fr (dsl.ut-capitole.fr)_ 193.49.48.249
Connexion à dsl.ut-capitole.fr (dsl.ut-capitole.fr)[193.49.48.249]:80_ connecté.
requête HTTP transmise, en attente de la réponse_ 200 OK
Taille : 28704549 (27M) [application/x-gzip]
Enregistre : «blacklists.tar.gz»

blacklists.tar.gz 100%[=====] 27,37M 2,57MB/s ds 11s
2022-12-10 10:23:08 (2,40 MB/s) - «blacklists.tar.gz» enregistré [28704549/28704549]

root@hawa-HP-EliteBook-820-G1:/var/lib/squidguard/db# tar zxvf blacklists.tar.gz
blacklists/README
blacklists/global_usage
blacklists/cc-by-sa-4-0.pdf
blacklists/LICENSE.pdf
blacklists/adult/
blacklists/adult/domains
blacklists/adult/expressions
blacklists/adult/urls
blacklists/adult/usage
blacklists/adult/very_restrictive_expression
blacklists/adult/domains.9309
blacklists/adult/domains.24733
blacklists/agressif/
blacklists/agressif/domains
blacklists/agressif/expressions
blacklists/agressif/urls
blacklists/agressif/usage
blacklists/arjel/
blacklists/arjel/domains
blacklists/arjel/usage
blacklists/astrology/
blacklists/astrology/domains
blacklists/astrology/urls
blacklists/astrology/usage
blacklists/audio-video/
```



► Configuration du fichier squidGuard.conf avec gedit /etc/squidguard/squidGuard.conf



```
29
30 #src foo-clients {
31 #     ip          172.16.2.32-172.16.2.100 172.16.2.100 172.16.2.200
32 #}
33
34 src myclients {
35     ip          192.168.1.0/24
36 }
37
38 #
39 # DESTINATION CLASSES:
40 #
41 # [see also in file dest-snippet.txt]
42
43 dest adult {
44     domainlist dest/adult/domains
45     urllist dest/adult/urls
46     redirect http://192.168.1.2
47 }
48
49
50 dest publicite {
51     domainlist dest/publicite/domains
52     urllist dest/publicite/urls
53     redirect http://192.168.1.2
54 }
55
56 dest violence {
57     domainlist dest/violence/domains
58     urllist dest/violence/urls
59     redirect http://192.168.1.2
60 }
61
62 #dest adult {
63 #     domainlist      BL/adult/domains
64 #     urllist         BL/adult/urls
65 #     expressionlist  BL/adult/expressions
66 #     redirect http://admin.foo-bar.de/cgi-bin/blocked.cgi?clientaddr=%fclientname=%fclientuser=%fclientgroup=%ftargetaounkfturl=%fu
```



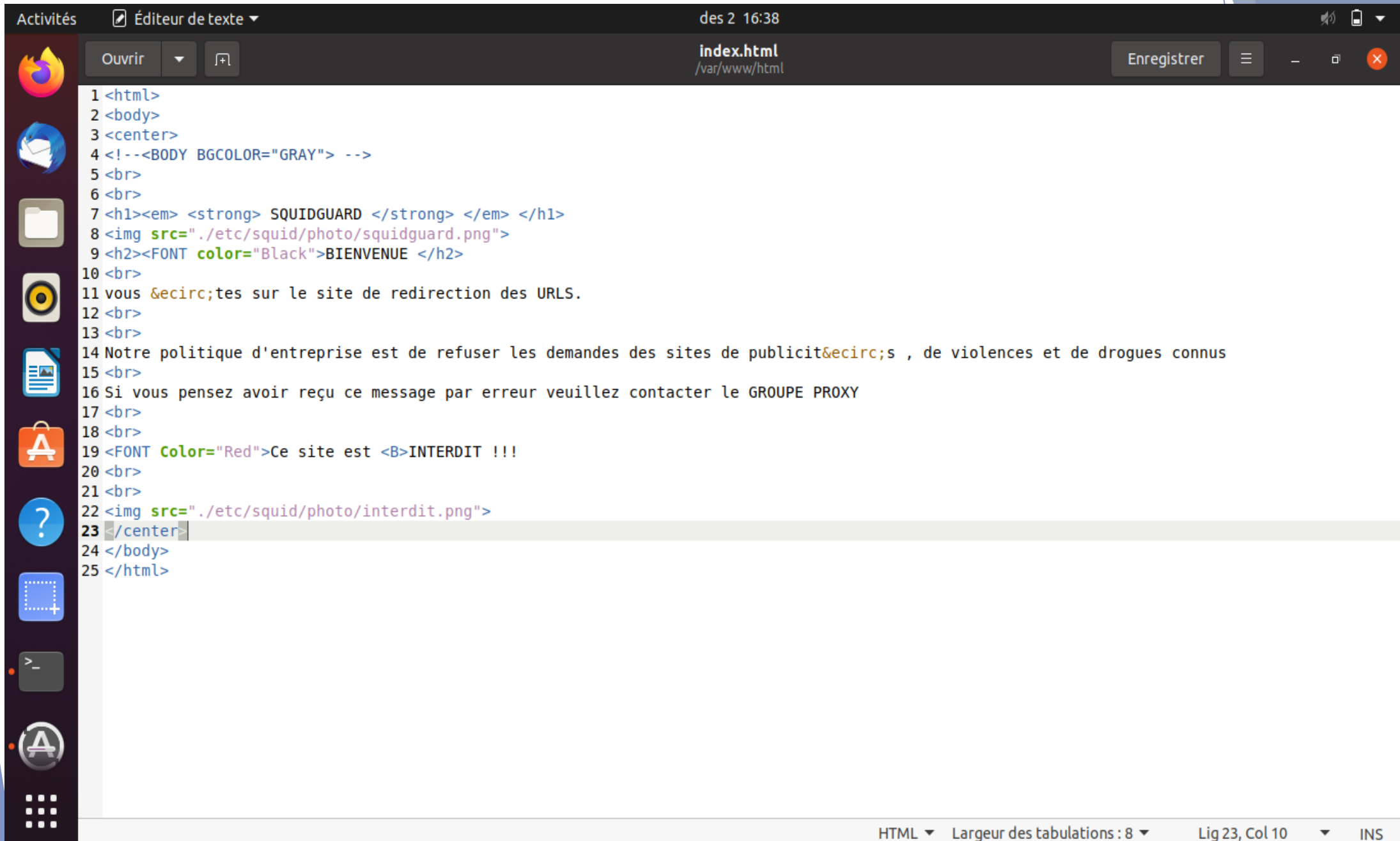
```
56 dest violence {
57     domainlist dest/violence/domains
58     urllist dest/violence/urls
59     redirect http://192.168.1.2
60 }
61
62 #dest adult {
63 #     domainlist      BL/adult/domains
64 #     urllist          BL/adult/urls
65 #     expressionlist  BL/adult/expressions
66 #     redirect http://admin.foo.bar.de/cgi-bin/blocked.cgi?clientaddr=%a&clientname=%n&clientuser=%i&clientgroup=%s&targetgroup=%t&url=%u
67 #}
68
69 #
70 # ACL RULES:
71 #
72
73 acl {
74 #admin {
75 #     pass    any
76 # }
77
78 #     foo-clients within workhours {
79 #         pass    good !in-addr !porn any
80 #     } else {
81 #         pass any
82 #     }
83
84 #     bar-clients {
85 #         pass    local none
86 #     }
87
88 #     default {
89 #         pass    !adult !publicite !violence all
90 #         redirect http://192.168.1.2
91 #     }
92 }
```

Squid peut interdire l'accès à un site ou des sites qui contiennent tel ou tel mot : adult, violence, publicité, de ce fait à chaque fois que nous lançons des requêtes sur des sites qui sont en rapport avec ces mots, celui-ci sera inaccessible et les redirigera vers notre page web dont l'adresse IP est : 192.168.1.2

Personnalisation de la page de redirection : Pour créer une page de redirection, il faut utiliser apache. On installe apache avec la commande `apt-get install apache2`



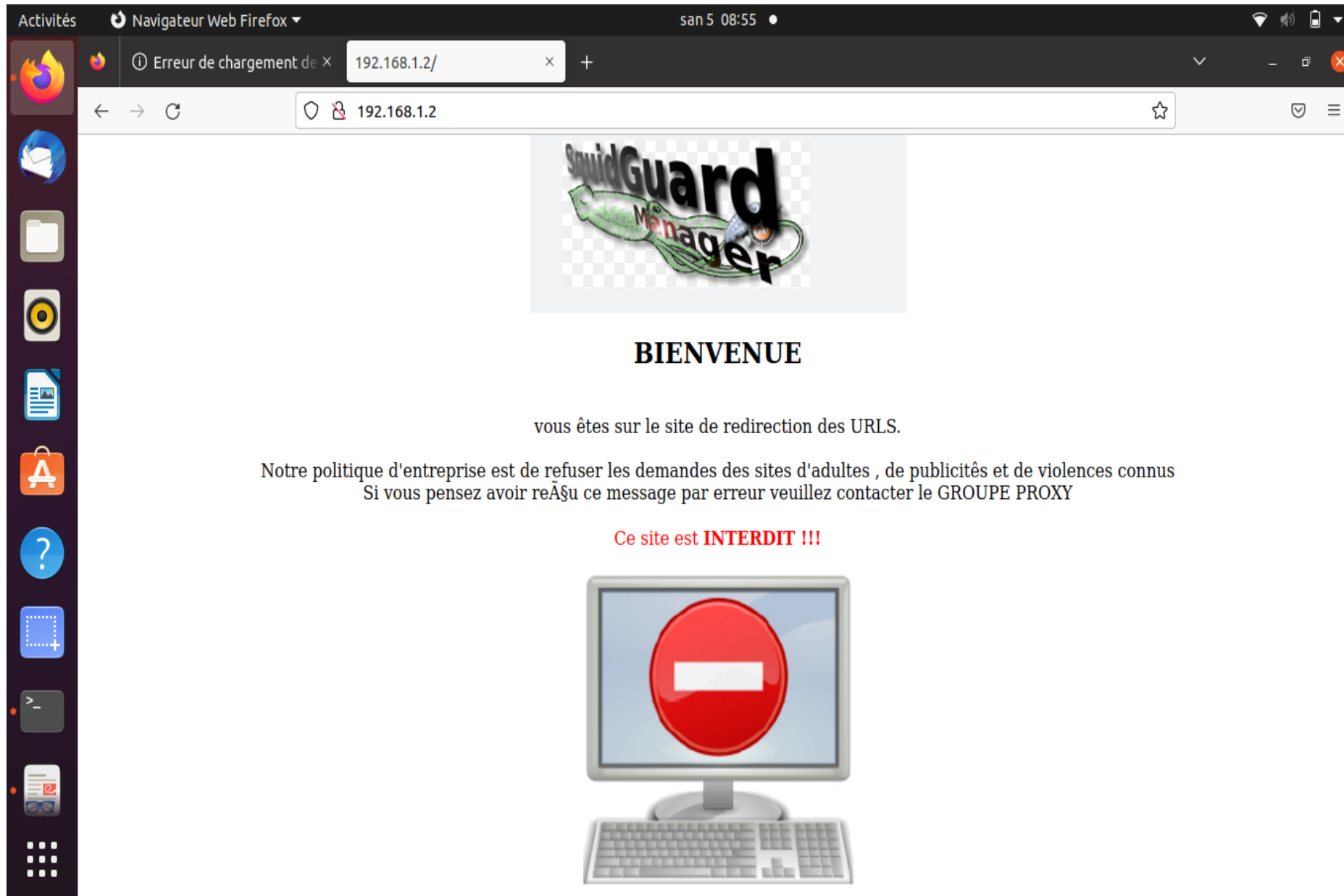
- On Modifie la page web par défaut d'apache2 : Il faut modifier le fichier index.html qui se trouve dans /var/www/html



```
1 <html>
2 <body>
3 <center>
4 <!--<BODY BGCOLOR="GRAY"> -->
5 <br>
6 <br>
7 <h1><em> <strong> SQUIDGUARD </strong> </em> </h1>
8 
9 <h2><FONT color="Black">BIENVENUE </h2>
10 <br>
11 vous &ecirc;tes sur le site de redirection des URLs.
12 <br>
13 <br>
14 Notre politique d'entreprise est de refuser les demandes des sites de publicit&ecirc;s , de violences et de drogues connus
15 <br>
16 Si vous pensez avoir reçu ce message par erreur veuillez contacter le GROUPE PROXY
17 <br>
18 <br>
19 <FONT color="Red">Ce site est <B>INTERDIT !!!
20 <br>
21 <br>
22 
23 </center>
24 </body>
25 </html>
```

HTML ▾ Largeur des tabulations : 8 ▾ Lig 23, Col 10 ▾ INS

- La page de redirection est la suivante :



- ▶ Pour accélérer le traitement (mais en réduisant considérablement le nombre de domaines filtres) :
- ▶ `cd dest/adult`
- ▶ `cp domains domains.originel`
- ▶ `echo "playboy.com" >domains`
- ▶ `chown proxy:proxy domains`

```
talled or GVfs metadata are not supported on this platform. In the latter case, you should configure Ieptl with --disable-gvfs-metadata.
root@hawa-HP-EliteBook-820-G1:/etc/squid# cd /var/lib/squidguard/db
root@hawa-HP-EliteBook-820-G1:/var/lib/squidguard/db# cd dest/adult
root@hawa-HP-EliteBook-820-G1:/var/lib/squidguard/db/dest/adult# echo "playboy.com" >domains
root@hawa-HP-EliteBook-820-G1:/var/lib/squidguard/db/dest/adult# chown proxy:proxy domains
root@hawa-HP-EliteBook-820-G1:/var/lib/squidguard/db/dest/adult# service squid restart
root@hawa-HP-EliteBook-820-G1:/var/lib/squidguard/db/dest/adult# service squid status
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-01-05 09:53:56 GMT; 5s ago
     Docs: man:squid(8)
  Process: 6595 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
  Process: 6598 ExecStart=/usr/sbin/squid -sYC (code=exited, status=0/SUCCESS)
 Main PID: 6599 (squid)
    Tasks: 4 (limit: 4491)
   Memory: 15.3M
    CGroup: /system.slice/squid.service
            └─6599 /usr/sbin/squid -sYC
              └─6601 (squid-1) --kid squid-1 -sYC
                └─6602 (logfile-daemon) /var/log/squid/access.log
                  └─6603 (pinger)

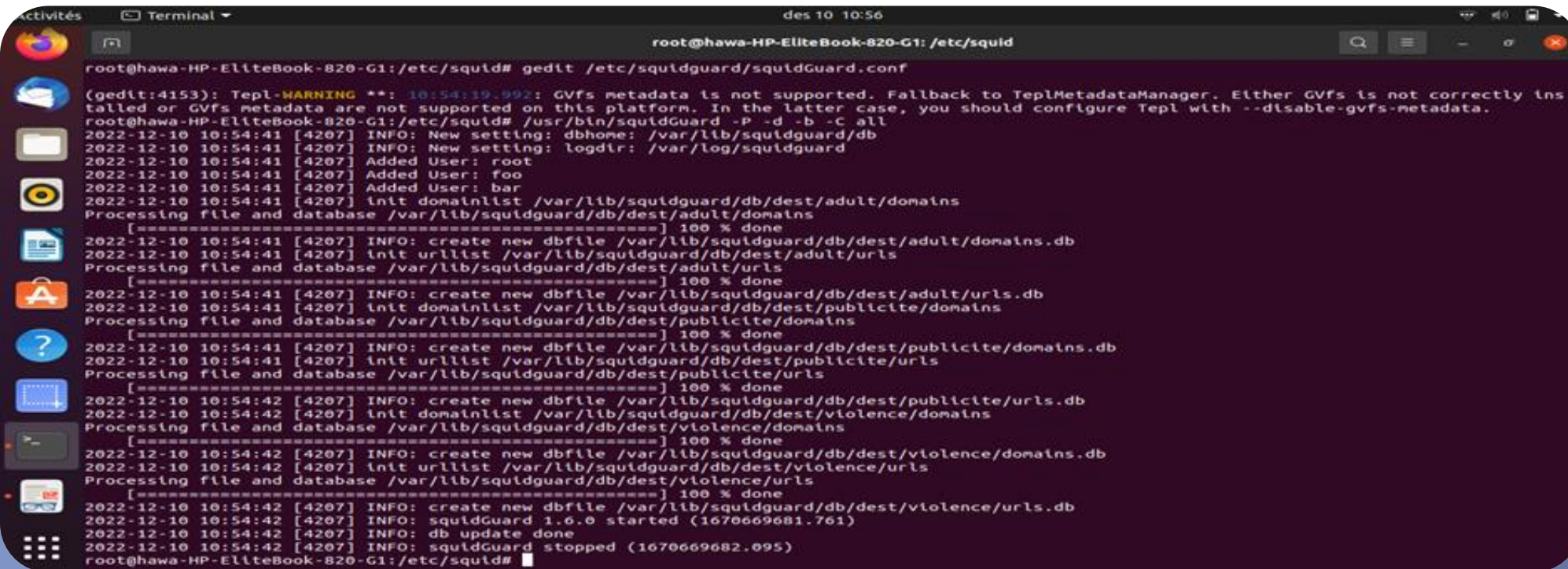
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: Max Swap size: 0 KB
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: Using Least Load store dir selection
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: Set Current Directory to /var/spool/squid
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: Finished loading MIME types and icons.
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: HTCP Disabled.
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: Pinger socket opened on FD 14
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: Squid plugin modules loaded: 0
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: Adaptation support is off.
san 05 09:53:56 hawa-HP-EliteBook-820-G1 squid[6601]: Accepting HTTP Socket connections at local=[::]:3128 remote=[::] FD 12 flags=9
san 05 09:53:57 hawa-HP-EliteBook-820-G1 squid[6601]: storeLateRelease: released 0 objects
root@hawa-HP-EliteBook-820-G1:/var/lib/squidguard/db/dest/adult#
```

# *squidward*

- ▶ La structure des fichiers textes contenant la liste est créée. Squidguard peut fonctionner tel quel (il recompilera les bases en mémoire au démarrage), mais cela ralentira considérablement tout démarrage ou redémarrage.
- ▶ Il faut donc créer (compiler) les bases de données avant le lancement.
- ▶ Il faudra prendre la précaution d'arrêter le squid avant, si on veut que la compilation soit rapide.
- ▶ Arrêter le squid avec : `service squid stop`

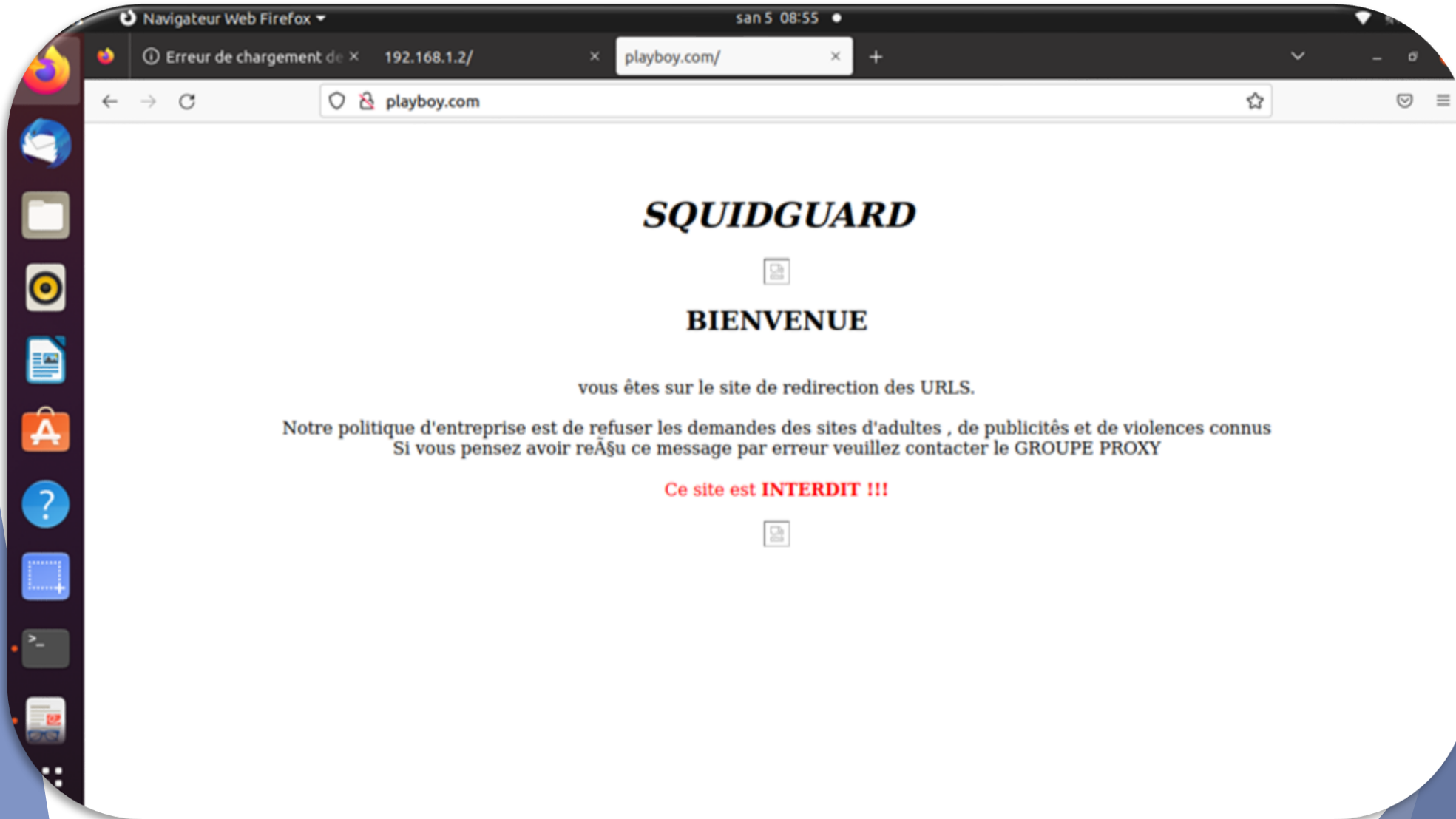


- ▶ Le régénérer avec : `/usr/bin/squidGuard -P -d -b -C all`
- ▶ Comme la commande a été faite par root, les fichiers domains.db et urls.db lui appartiennent, il faut changer le propriétaire.
- ▶ `chown -R proxy:proxy /var/lib/squidguard/db`
- ▶ On peut alors relancer le squid.
- ▶ `service squid start`



```
root@hawa-HP-EliteBook-820-G1:/etc/squid# gedit /etc/squidguard/squidGuard.conf
(gedit:4153): Tepl-WARNING **: 10:54:19.992: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
root@hawa-HP-EliteBook-820-G1:/etc/squid# /usr/bin/squidGuard -P -d -b -C all
2022-12-10 10:54:41 [4207] INFO: New setting: dbhome: /var/lib/squidguard/db
2022-12-10 10:54:41 [4207] INFO: New setting: logdir: /var/log/squidguard
2022-12-10 10:54:41 [4207] Added User: root
2022-12-10 10:54:41 [4207] Added User: foo
2022-12-10 10:54:41 [4207] Added User: bar
2022-12-10 10:54:41 [4207] Init domainlist /var/lib/squidguard/db/dest/adult/domains
Processing file and database /var/lib/squidguard/db/dest/adult/domains
[=====] 100 % done
2022-12-10 10:54:41 [4207] INFO: create new dbfile /var/lib/squidguard/db/dest/adult/domains.db
2022-12-10 10:54:41 [4207] Init urllist /var/lib/squidguard/db/dest/adult/urls
Processing file and database /var/lib/squidguard/db/dest/adult/urls
[=====] 100 % done
2022-12-10 10:54:41 [4207] INFO: create new dbfile /var/lib/squidguard/db/dest/adult/urls.db
2022-12-10 10:54:41 [4207] Init domainlist /var/lib/squidguard/db/dest/publicite/domains
Processing file and database /var/lib/squidguard/db/dest/publicite/domains
[=====] 100 % done
2022-12-10 10:54:41 [4207] INFO: create new dbfile /var/lib/squidguard/db/dest/publicite/domains.db
2022-12-10 10:54:41 [4207] Init urllist /var/lib/squidguard/db/dest/publicite/urls
Processing file and database /var/lib/squidguard/db/dest/publicite/urls
[=====] 100 % done
2022-12-10 10:54:42 [4207] INFO: create new dbfile /var/lib/squidguard/db/dest/publicite/urls.db
2022-12-10 10:54:42 [4207] Init domainlist /var/lib/squidguard/db/dest/violence/domains
Processing file and database /var/lib/squidguard/db/dest/violence/domains
[=====] 100 % done
2022-12-10 10:54:42 [4207] INFO: create new dbfile /var/lib/squidguard/db/dest/violence/domains.db
2022-12-10 10:54:42 [4207] Init urllist /var/lib/squidguard/db/dest/violence/urls
Processing file and database /var/lib/squidguard/db/dest/violence/urls
[=====] 100 % done
2022-12-10 10:54:42 [4207] INFO: create new dbfile /var/lib/squidguard/db/dest/violence/urls.db
2022-12-10 10:54:42 [4207] INFO: squidGuard 1.6.0 started (1670669681.761)
2022-12-10 10:54:42 [4207] INFO: db update done
2022-12-10 10:54:42 [4207] INFO: squidGuard stopped (1670669682.095)
root@hawa-HP-EliteBook-820-G1:/etc/squid#
```

- ▶ Reste alors a tester, a partir du navigateur l'url <http://www.playboy.com> qui va se transformer en <http://192.168.1.2>





# Conclusion

Le serveur proxy assure plusieurs rôles tel que le filtre, le cache, la facilitation des réseaux partagés... néanmoins l'utilisation d'un VPN est aujourd'hui une option nettement plus intéressante. Non seulement cela garantit une sécurité accrue, mais les connexions sont aussi beaucoup plus rapides. De plus, vous disposez toujours d'un kill-switch si quelque chose est compromis.

**MERCI D'AVOIR SUIVI**  
**MAINTENANT NOUS ALLONS EN**  
**VENIR AU TEST**