

## Compte rendu Proxy

### Etape 1 :

Installer les paquetages suivants : [squid](#), [squidguard](#), [apache2-utils](#), [lightsquid](#)

### Etape 2 :

Créer les répertoires suivants : `/apps/squid/cache`, `/apps/squid/log`, `/apps/squid/lib`

```
root@debian:/# mkdir /apps/squid/cache
root@debian:/# mkdir /apps/squid/log
root@debian:/# mkdir /apps/squid/lib
root@debian:/#
```

Donnez tous les droits à proxy sur les répertoires précédents

```
root@debian:/# chown -R proxy:proxy /apps/squid/cache
root@debian:/# chown -R proxy:proxy /apps/squid/log/
root@debian:/# chown -R proxy:proxy /apps/squid/lib
root@debian:/#
```

### Etape 3 :

Sur le site [dsi.ut-capitole.fr/blacklists/](http://dsi.ut-capitole.fr/blacklists/) un fichier de blacklist en version compressée est disponible.

Décompresser le et copier le dans `apps/squid/lib`

```
root@debian:/tmp/tempo# wget http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz
--2022-11-05 10:33:15-- http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz
Resolving dsi.ut-capitole.fr (dsi.ut-capitole.fr)... 193.49.48.249
Connecting to dsi.ut-capitole.fr (dsi.ut-capitole.fr)|193.49.48.249|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31180329 (30M) [application/x-gzip]
Saving to: 'blacklists.tar.gz'

blacklists.tar.gz  100%[=====>] 29.74M  2.18MB/s   in 19s
2022-11-05 10:33:34 (1.57 MB/s) - 'blacklists.tar.gz' saved [31180329/31180329]

root@debian:/tmp/tempo#
root@debian:/tmp/tempo# tar -xzf blacklists.tar.gz
root@debian:/tmp/tempo# cp -R blacklists/* /apps/squid/lib
root@debian:/tmp/tempo#
```

```

root@debian:/apps/squid/lib# cd /tmp/tempo
root@debian:/tmp/tempo# ls
blacklists  blacklists.tar.gz
root@debian:/tmp/tempo# cp blacklists /apps/squid/lib/
cp: -r not specified; omitting directory 'blacklists'
root@debian:/tmp/tempo# cp -r blacklists /apps/squid/lib/
root@debian:/tmp/tempo# cd /apps/squid/lib
root@debian:/apps/squid/lib# ls
ads                celebrity          drugs              lingerie           publicite          sta
adult              chat              educational_games liste_blanche      radio             str
aggressive         child             examen_pix         liste_bu           README            str
agressif           cleaning          exceptions_liste_bu mail              reaffected        tra
arjel              cooking           filehosting        malware            redirector        tri
associations_religieuses cryptojacking      financial          manga              remote-control    upd
astrology           dangerous_material forums             marketingware     sect              vic
audio-video         dating            gambling           mixed_adult       sexual_education  vpr
bank                ddos              games              mobile-phone      shopping          war
bitcoin             dialer            global_usage       phishing           shortener         web
blacklists          doh               hacking            porn               social_networks
blog                download          jobsearch          Active Windows    special
cc-by-sa-4-0.pdf    drogue            LICENSE.pdf        proxy              sports

```

Etape 4 :

Donner l'intégralité des droits sur ces blacklists à proxy

```

root@debian:/apps/squid/lib# chown -R proxy:proxy /apps/squid/lib/blacklists/
root@debian:/apps/squid/lib#

```

## II) Configuration du squid

Stoppez squid

Puis Sauvegardez /etc/squid/squid.conf en squid.old puis effacez et recréez le fichier de configuration /etc/squid /squid.conf

```

root@debian:/apps/squid/lib# cp /etc/squid/squid.conf /etc/squid/squid.old
root@debian:/apps/squid/lib# cd /etc/squid
root@debian:/etc/squid# ls
conf.d  errorpage.css  squid.conf  squid.configuration  squid.old
root@debian:/etc/squid# nano squid.conf
root@debian:/etc/squid#

```

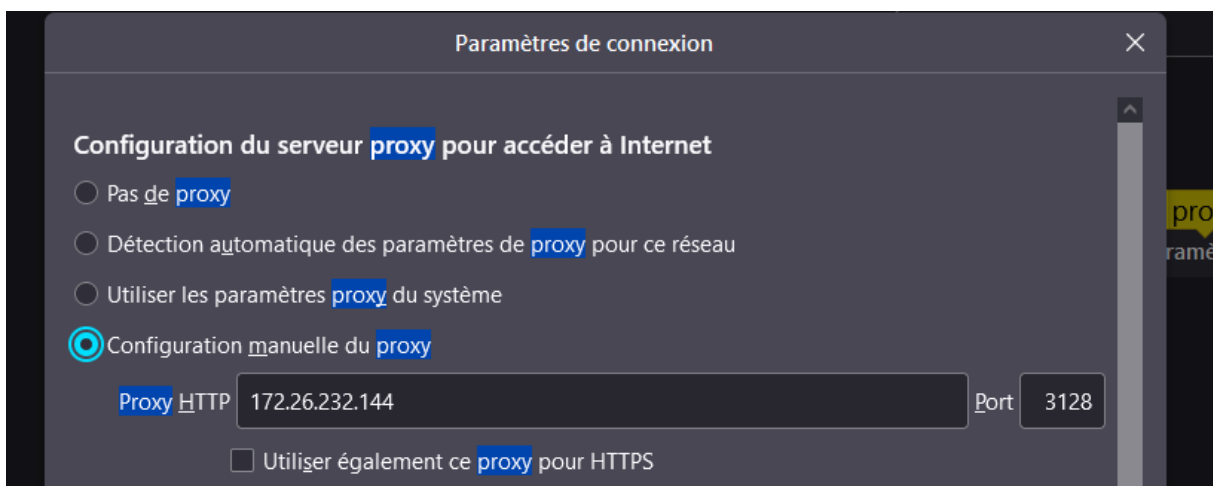
En suivant le modèle ci-dessous adaptez-le aux réseaux de votre contexte

```
GNU nano 3.2 /etc/squid/squid.conf
#Paramétrage du serveur
#Port sur lequel squid écoute
http_port 3128

#nom que renvoy squid quand il est interrogé de l'extérieur
visible_hostname BookticProxy
#taille de mémoire RAM réservée au cache ne pas dépasser 70 à 80 % de la RAM totale
cache_mem 200 MB
# Paramétrage du cache, UFS(Unix File System), chemin,
# taille totale du cache en MB, Nombre de répertoires de premier et de second niveau
cache_dir ufs /apps/squid/cache 1000 16 256
#taille maxi d'un objet gardé en cache
maximum_object_size 10 MB
#identifiant du processus squid
pid_filename /var/run/squid.pid
#Affichage des pages d'erreur en français
error_directory/usr/share/squid/errors/French
#Paramétrages de logs
#log contenant les accès HTTP et ICP de squid
cache_access_log /apps/squid/log/access.log
#log d'acceptation ou de rejet des différentes ressources du cache
cache_store_log /apps/squid/log/store.log
#log principal
cache_log /apps/squid/log/cache.log
###LES RESTRICTIONS - ACL### # ajoutez autant d'acl que de réseau à traiter...# il en faut une pour le Wifi, la ToIP, Users et Data
acl landata src 172.17.0.0/24
acl lanwifi src 172.19.0.0/24
### Ports qui seront autorisés par le proxy
acl safe_ports port 80
acl safe_ports port 1024-65535
acl safe_ports port 443
#Autorisations ou non de l'accès http pour les différentes acl
# A compléter avec les acls ajoutées plus haut
http_access deny !safe_ports
http_access allow landata
http_access allow lanwifi
http_access deny all
```

Générez les répertoires et fichiers de cache avec la commande : `squid -z`

Configurez un navigateur pour qu'il aille sur le web via mon proxy



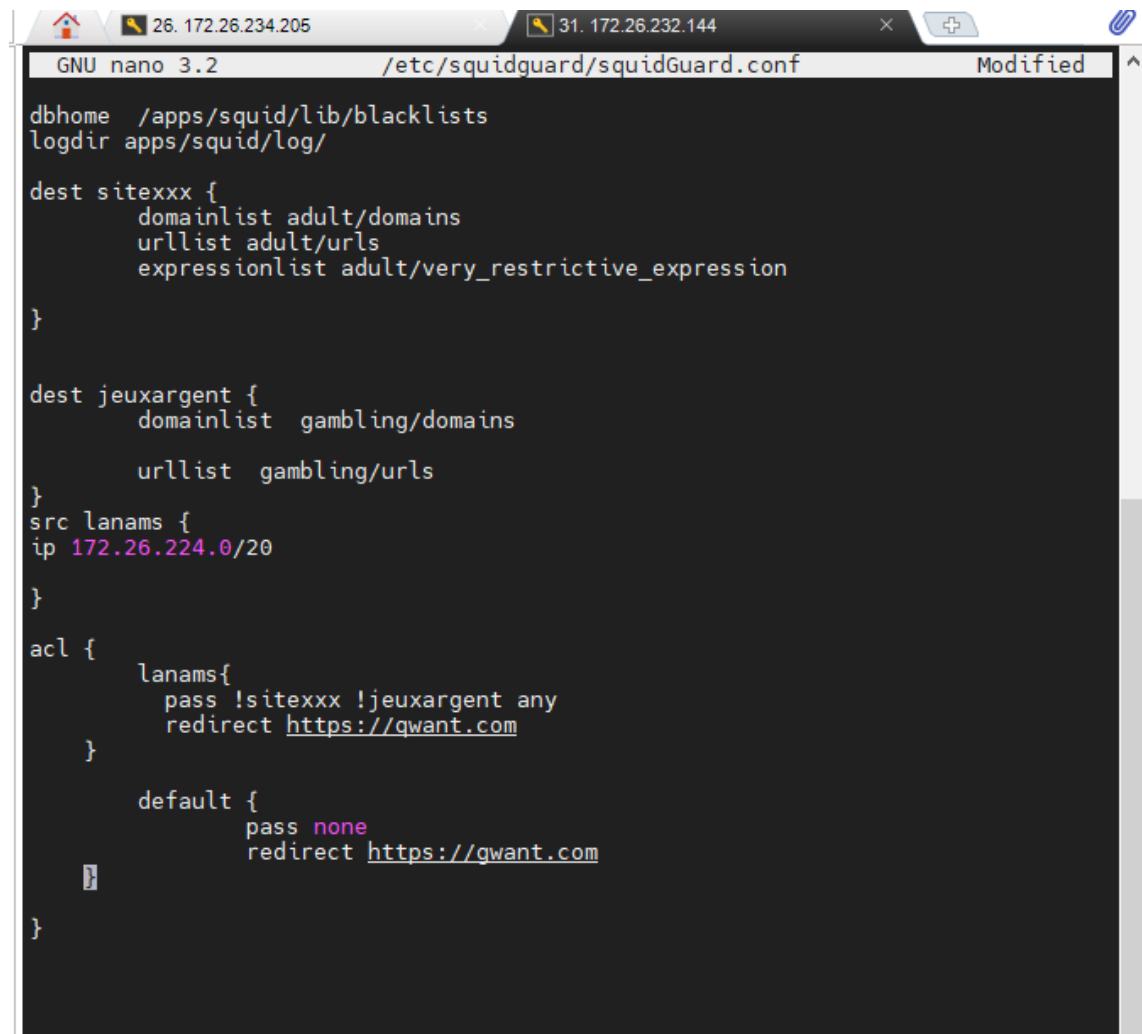
```
root@debian:/etc/squid# service squid start
root@debian:/etc/squid# service squid start
root@debian:/etc/squid# tail -f /apps/squid/l
lib/ log/
root@debian:/etc/squid# tail -f /apps/squid/log/cache.log
2022/11/05 11:56:25| FATAL: Squid is already running: Found fresh instance PID file (/var/run/squid.pid) with PID 11
exception location: Instance.cc(121) ThrowIfAlreadyRunningWith
```

## Configuration de squidGuard

Nous allons maintenant améliorer la sécurité de squid en lui ajoutant un logiciel qui va permettre l'interdiction de site Web en fonction de blacklists. Il permet bien d'autres options mais nous nous concentrerons sur celles ci. L'utilisation des blacklists nécessite une observation préalable de l'arborescence existante pour chaque groupe d'interdiction (voir ci-après).

Prenez soin de déplacer le fichier /etc/squidguard/squidGuard.conf existant pour en avoir un vierge comme on l'a fait pour squid.conf. Ecrivez, ensuite, ce fichier (/etc/squidguard/squidGuard.conf) à partir du modèle suivant

```
root@debian:/etc/squid# cp -r /etc/squidguard/squidGuard.conf /etc/squidguard/squidGuard.old
root@debian:/etc/squid# cd /etc/squidguard/
root@debian:/etc/squidguard# ls
squidGuard.conf  squidGuard.conf.default  squidGuard.old
root@debian:/etc/squidguard#
```



```
GNU nano 3.2 /etc/squidguard/squidGuard.conf Modified
dbhome /apps/squid/lib/blacklists
logdir apps/squid/log/

dest sitexxx {
    domainlist adult/domains
    urllist adult/urls
    expressionlist adult/very_restrictive_expression
}

dest jeuxargent {
    domainlist gambling/domains
    urllist gambling/urls
}
src lanams {
ip 172.26.224.0/20
}

acl {
    lanams{
        pass !sitexxx !jeuxargent any
        redirect https://qwant.com
    }

    default {
        pass none
        redirect https://qwant.com
    }
}
```

Avant de relancez squid. Il faut lui signaler de démarrer squidguard, on ajoute alors dans squid.conf

```
#Autorisations ou non de l'accès http pour les différentes acl
# A compléter avec les acls ajoutées plus haut.
http_access deny !safe_ports
http_access allow lanams
http_access deny all

ur_rewrite_program/usr/bin/squidGuard-c/etc/squidguard/squidGuard.conf

url_rewrite_children 5
```

Test final après l'attribution des droits aux nouveaux fichiers :

```
root@debian:/etc/squidguard# chown -R proxy:proxy /etc/squidguard/squidGuard.conf
root@debian:/etc/squidguard# chown -R proxy:proxy /etc/squid/squid.conf
root@debian:/etc/squidguard#
```

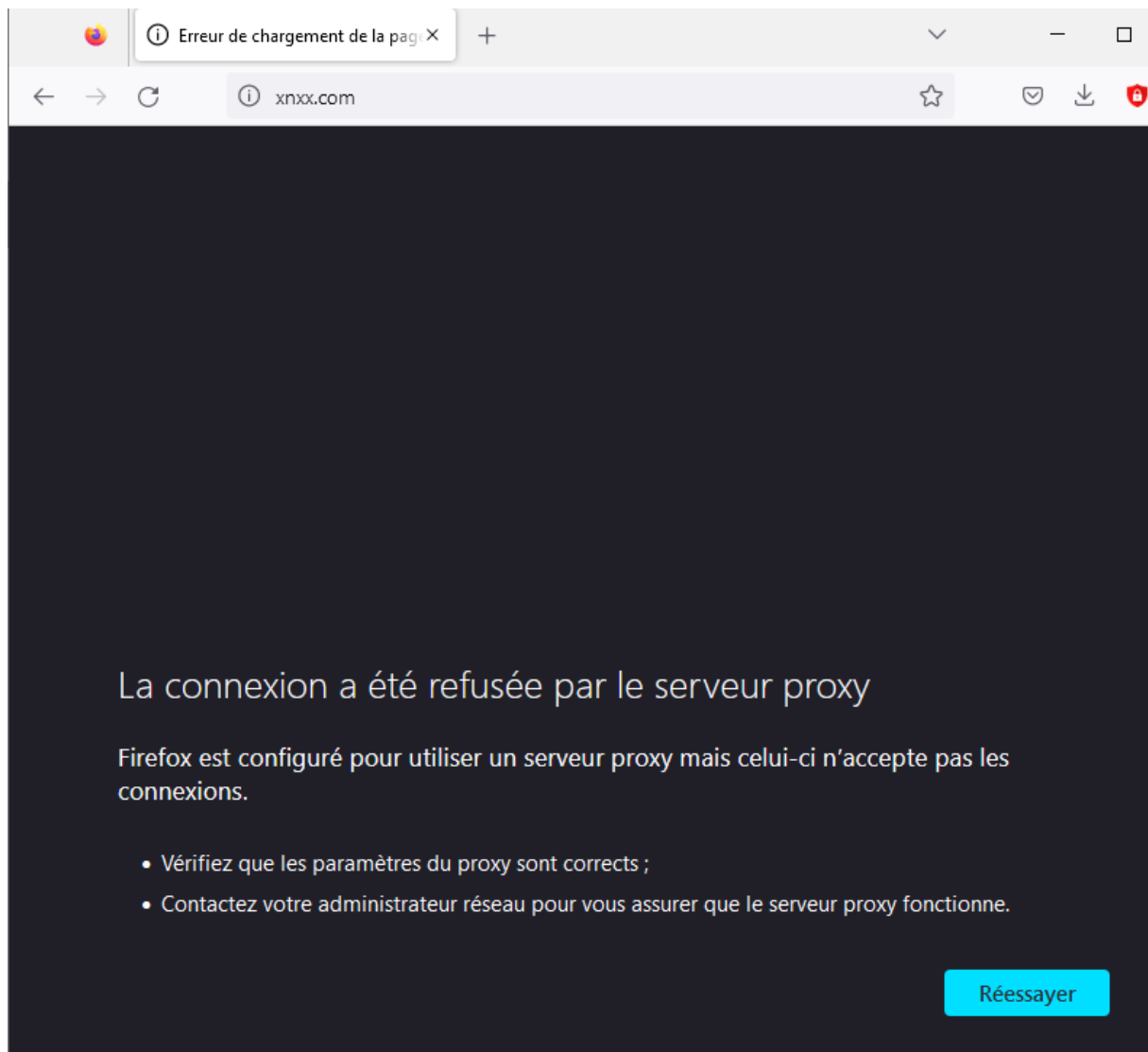
```
root@debian:/etc/squidguard# chown -R proxy:proxy /apps/squid/lib/blacklists/
```

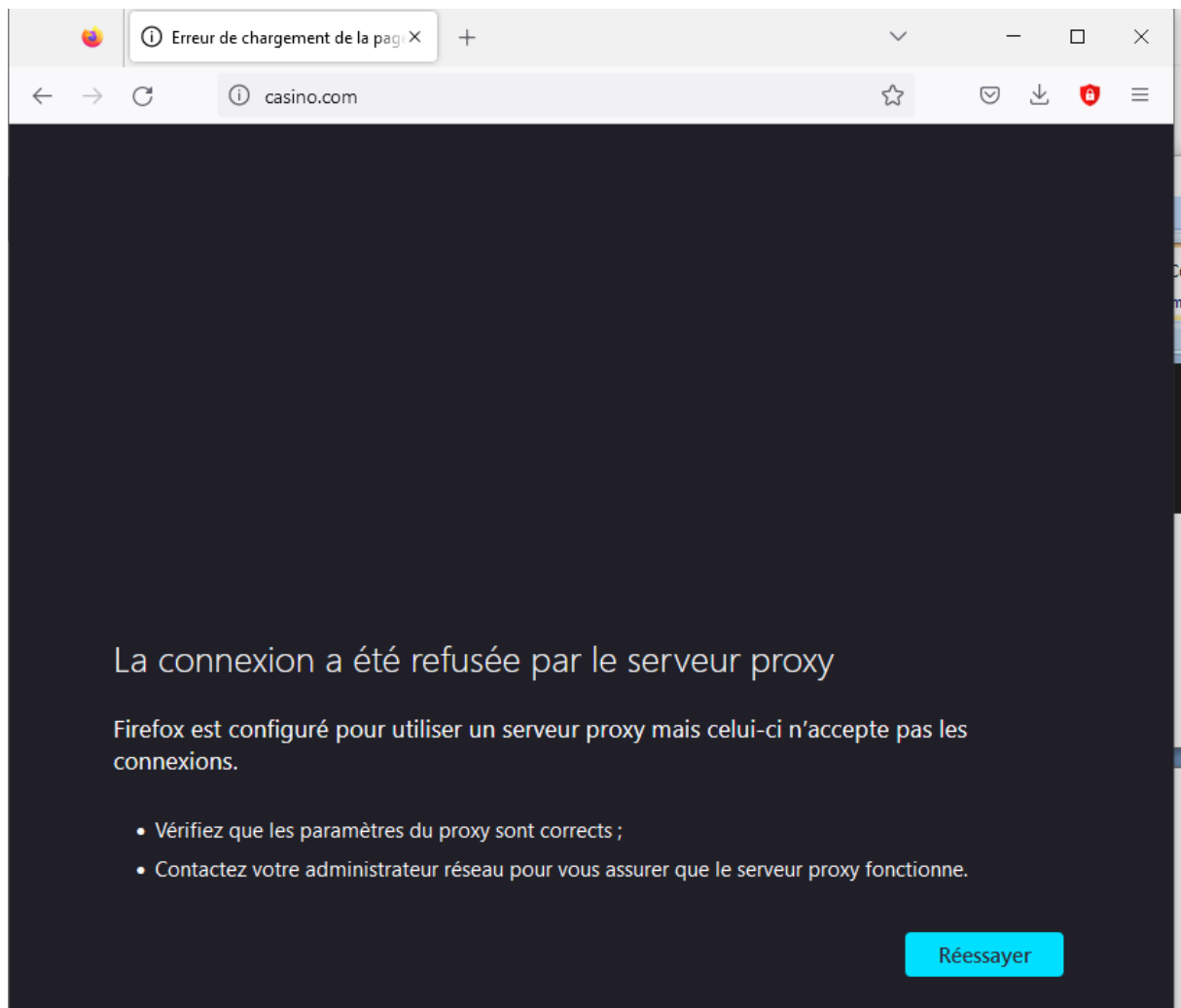
```

/bin/bash
/bin/bash 126x20
bash: IP: command not found
root@debian:/etc/squidguard# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:01:1e:18 brd ff:ff:ff:ff:ff:ff
    inet 172.26.232.144/20 brd 172.26.239.255 scope global dynamic eth0
        valid_lft 78022sec preferred_lft 78022sec
    inet6 fe80::215:5dff:fe01:1e18/64 scope link
        valid_lft forever preferred_lft forever
root@debian:/etc/squidguard# chown -R proxy:proxy /apps/squid/lib/blacklists/
root@debian:/etc/squidguard# squidGuard -C all
^C
root@debian:/etc/squidguard# systemctl restart squid
root@debian:/etc/squidguard# squidGuard -C all

/bin/bash 126x20
2022-11-06 13:31:33 [3305] init domainlist /apps/squid/lib/blacklists/adult/domains
2022-11-06 13:31:33 [3305] INFO: loading dbfile /apps/squid/lib/blacklists/adult/domains.db
2022-11-06 13:31:33 [3305] FATAL: Error db_open: Permission denied
2022-11-06 13:31:33 [3305] ERROR: Going into emergency mode
2022-11-06 13:37:21 [3315] INFO: New setting: dbhome: /apps/squid/lib/blacklists
2022-11-06 13:37:21 [3315] INFO: New setting: logdir: apps/squid/log/
2022-11-06 13:37:21 [3315] init domainlist /apps/squid/lib/blacklists/adult/domains
^C
root@debian:/etc/squidguard# tail -f /var/log/squidguard/squidGuard.log
2022-11-06 13:38:22 [3329] INFO: loading dbfile /apps/squid/lib/blacklists/adult/urls.db
2022-11-06 13:38:22 [3329] init expressionlist /apps/squid/lib/blacklists/adult/very_restrictive_express
2022-11-06 13:38:22 [3329] init domainlist /apps/squid/lib/blacklists/gambling/domains
2022-11-06 13:38:22 [3329] INFO: loading dbfile /apps/squid/lib/blacklists/gambling/domains.db
2022-11-06 13:38:22 [3329] init urllist /apps/squid/lib/blacklists/gambling/urls
2022-11-06 13:38:22 [3329] INFO: loading dbfile /apps/squid/lib/blacklists/gambling/urls.db
2022-11-06 13:38:22 [3329] (squidGuard): can't write to logfile apps/squid/log//apps/squid/log//squidGu
2022-11-06 13:38:28 [3330] INFO: New setting: dbhome: /apps/squid/lib/blacklists
2022-11-06 13:38:28 [3330] INFO: New setting: logdir: apps/squid/log/
2022-11-06 13:38:28 [3330] init domainlist /apps/squid/lib/blacklists/adult/domains
Active Windows
Accédez aux paramètres pour activer Windows.

État : Exécution
```





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