TP PROXY SQUID/SQUIDGUARD

En premier temps installer tout les paquets suivant afin de mettre en place le serveur :

- squid
- squidguard
- apache2-utils
- lightsquid
- openssl

Puis crée les répertoires suivant mkdir -p :

- /apps/squid/cache
- /apps/squid/log
- /apps/squid/lib

Donner les droits à l'utilisateur proxy :

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

Ensuite faire un SCP pour récupérer le certificat Ile-de-France et la blacklist avec la commande suivante :

```
root@debian:~# scp sio@margaux.sio.jjr:/home/sio/*.* /apps/squid/lib
sio@margaux.sio.jjr's password:
RIDF_CA.crt                                   100% 2116   348.0KB/s   00:00
blacklists.tar.gz                             100%   24MB   5.5MB/s   00:04
```

Une fois la blacklist récupéré il faut décompresser le fichier tar.gz avec la commande le permettant : tar -xvzf blacklists.tar.gz -C /apps/squid/lib

—---------- 2 - Configuration de Squid :

Stopper squid en premier lieu : systemctl stop squid

Puis sauvegarder le fichier squid.conf en squid.old, et effacer, recréer et réécrire le fichier squid.conf :

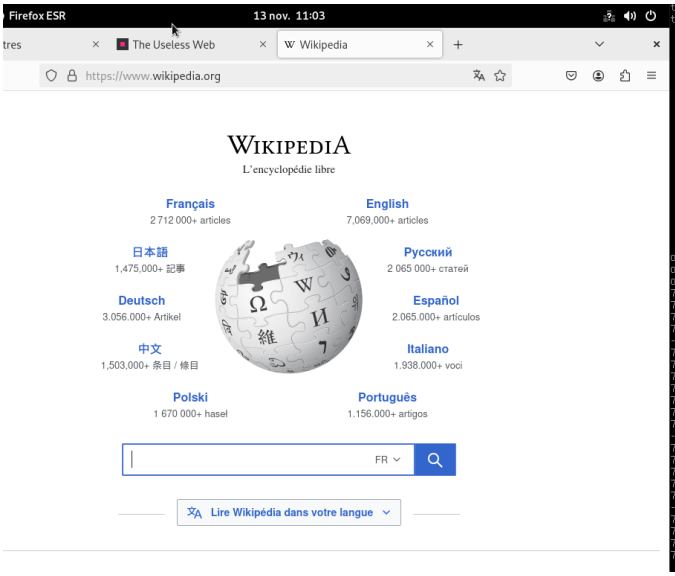
```
root@debian:/etc/squid# ls
conf.d  errorpage.css  squid.conf  squid.old
root@debian:/etc/squid#
```

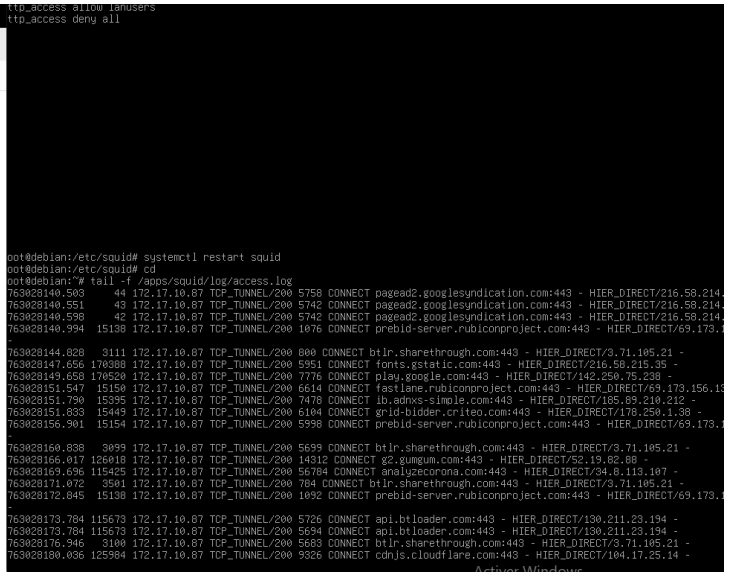
Voici le fichier squid.conf réécrit :

```
http_port 3128
visible_hostname BookticProxy
cache_mem 200 MB
cache_dir ufs /apps/squid/cache 1000 16 256
maximum_object_size 10 MB
pid_filename /var/run/squid.pid
error_directory /usr/share/squid/errors/French

cache_access_log /apps/squid/log/access.log
cache_store_log /apps/squid/log/store.log
cache_log /apps/squid/log/cache.log

acl landata src 172.17.1.0/24
acl lanwifi src 172.19.0.0/24
acl lanusers src 172.17.10.0/24
acl lantoip src 10.0.0.0/24

acl safe_ports port 80
acl safe_ports port 1024-65535
acl safe_ports port 443

http_access deny !safe_ports
http_access allow landata
http_access allow lanwifi
http_access allow lantoip
http_access allow lanusers
http_access deny all
```

faire un squid -z pour afficher les caches

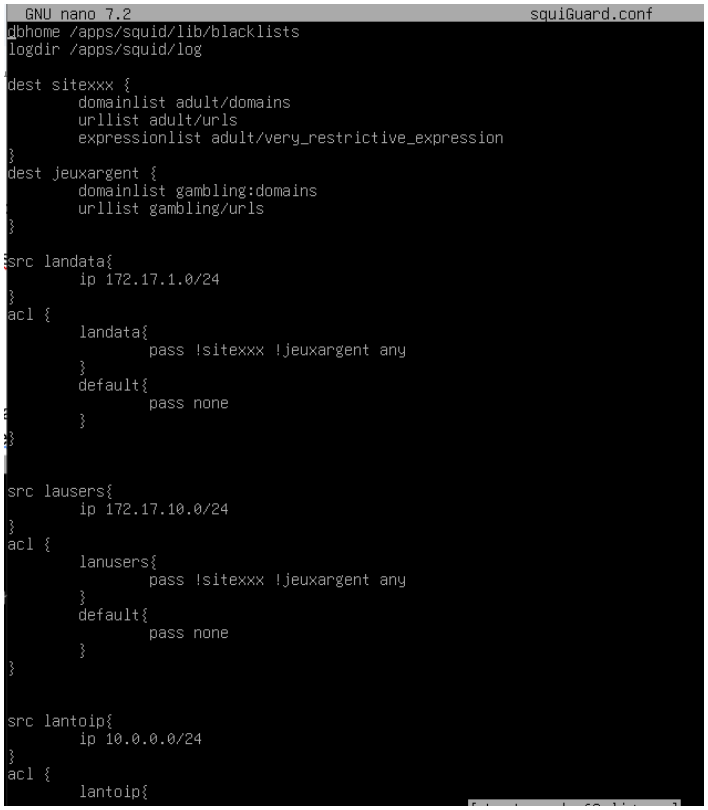
Puis faire un tail -f /apps/squid/log/access.log pour voir les logs en direct et nous allons sur un client externe au proxy pour voir si nous arrivons à entrer sur un site, ici nous pouvons nous naviguer sur wikipédia et les logs nous le confirme :





—---------- 3 - Configuration de squidGuarde :

Comme pour le fichier squid.conf, copier le fichier squidgarde.conf et le supprimer pour le réécrire sur un fichier vierge : voici le fichier et ses paramètre:



```
  GNU nano 7.2                                          squiGuard.conf
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 landata{
        ip 172.17.1.0/24
}
acl {
        landata{
                pass !sitexxx !jeuxargent any
        }
        default{
                pass none
        }
}


src lausers{
        ip 172.17.10.0/24
}
acl {
        lanusers{
                pass !sitexxx !jeuxargent any
        }
        default{
                pass none
        }
}


src lantoip{
        ip 10.0.0.0/24
}
acl {
        lantoip{
```

Avant de relancer squid nous allons signaler qu'il faut démarrer squidguarde donc on fait un nano /etc/squid/squid.conf et on ajoute les deux dernière ligne du fichier conf :

```
  GNU nano 7.2                                                  squid.conf *
http_port 3128
visible_hostname BookticProxy
cache_mem 200 MB
cache_dir ufs /apps/squid/cache 1000 16 256
maximum_object_size 10 MB
pid_filename /var/run/squid.pid
error_directory /usr/share/squid/errors/French

cache_access_log /apps/squid/log/access.log
cache_store_log /apps/squid/log/store.log
cache_log /apps/squid/log/cache.log

acl landata src 172.17.1.0/24
acl lanwifi src 172.19.0.0/24
acl lanusers src 172.17.10.0/24
acl lantoip src 10.0.0.0/24

acl safe_ports port 80
acl safe_ports port 1024-65535
acl safe_ports port 443

http_access deny !safe_ports
http_access allow landata
http_access allow lanwifi
http_access allow lantoip
http_access allow lanusers
http_access deny all

url_rewrite_rpogram /usr/bin/squidGuard -c /etc/squid3/squidGuarde.conf
url_rewrite_children 5
```

Ensuite ouvrir les logs de squidguard avec la commande nano ***/var/log/squidguard/squidGuard.log****, juste apres lancer la commande* ***squidGuard -C all*** *:*

Ici on voit bien que tout se passe comme convenu et qu'aucune erreur n'est affichées :

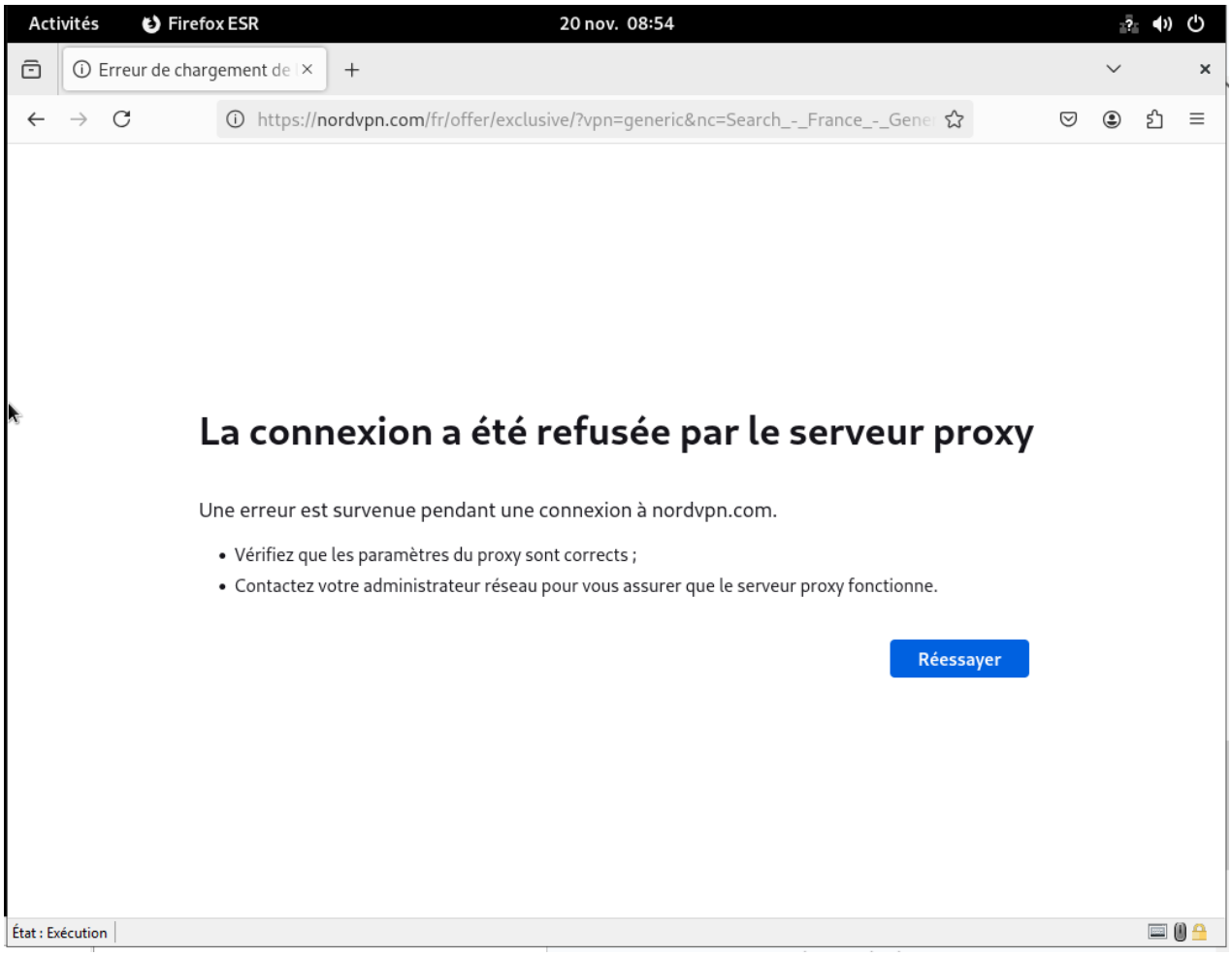
```
root@debian:/var/log/squidguard# tail -f squidGuard.log
2025-11-19 14:19:09 [992] INFO: New setting: logdir: /apps/squid/log
2025-11-19 14:19:09 [992] init domainlist /apps/squid/lib/blacklists/adult/domains
2025-11-19 14:19:44 [992] INFO: create new dbfile /apps/squid/lib/blacklists/adult/domains.db
2025-11-19 14:19:49 [992] init urllist /apps/squid/lib/blacklists/adult/urls
2025-11-19 14:19:49 [992] INFO: create new dbfile /apps/squid/lib/blacklists/adult/urls.db
2025-11-19 14:19:49 [992] init expressionlist /apps/squid/lib/blacklists/adult/very_restrictive_expression
2025-11-19 14:19:49 [992] init domainlist /apps/squid/lib/blacklists/gambling/domains
2025-11-19 14:19:49 [992] INFO: create new dbfile /apps/squid/lib/blacklists/gambling/domains.db
2025-11-19 14:19:49 [992] init urllist /apps/squid/lib/blacklists/gambling/urls
2025-11-19 14:19:49 [992] INFO: create new dbfile /apps/squid/lib/blacklists/gambling/urls.db
```

Le VPN n'étant plus mis a jour i maintenu par le plugin squidguard nous allons trouver une autre méthode pour passer par squid directement au lieu du plugin squidguard pour cela nous allons configurer les acl et les http manuellement à l'aide de la blacklists voici un exemple pour les sites de VPN :

Entrer dans le fichier nano /etc/squid/squid.conf et ajouter un acl et des http pour le réseau local lan

```
  GNU nano 7.2                                          /etc/squid/squid.conf
http_port 3128
visible_hostname BookticamProxy
cache_mem 200 MB
cache_dir ufs /apps/squid/cache 1000 16 256
maximum_object_size 10 MB
pid_filename /var/run/squid.pid
error_directory /usr/share/squid/errors/French

cache_access_log /apps/squid/log/access.log
cache_store_log /apps/squid/log/store.log
cache_log /apps/squid/log/cache.log

acl landata src 172.17.1.0/24
acl lanusers src 172.17.10.0/24
acl lanwifi src 172.19.0.0/24
acl lanToIP src 10.0.0.0/24
acl vpn dstdomain "/apps/squid/lib/blacklists/vpn/domains"


acl blacklists dstdomain
acl safe_ports port 80
acl safe_ports port 1024-65535
acl safe_ports port 443

http_access deny !safe_ports
http_access deny vpn lanusers
#http_access allow landata
http_access allow lanusers
#http_access allow lanwifi
#http_access allow lanToip
http_access deny all

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

On voit donc que notre fichier conf est bien configuré et que les sites vpn sont bloqué ici NordVPN :



En bonus nous allons ajouter des contraintes d'heures et de dates:

```
 GNU nano 7.2                                          /etc/squid/squid.conf *
http_port 3128
visible_hostname BookticamProxy
cache_mem 200 MB
cache_dir ufs /apps/squid/cache 1000 16 256
maximum_object_size 10 MB
pid_filename /var/run/squid.pid
error_directory /usr/share/squid/errors/French

cache_access_log /apps/squid/log/access.log
cache_store_log /apps/squid/log/store.log
cache_log /apps/squid/log/cache.log

acl landata src 172.17.1.0/24
acl lanusers src 172.17.10.0/24
acl lanwifi src 172.19.0.0/24
acl lanToIP src 10.0.0.0/24

acl vpn dstdomain "/apps/squid/lib/blacklists/vpn/domains"
acl manga dstdomain "/apps/squid/lib/blacklists/maga/domains"
acl heures_bureau time M T W H F A 08:00-18:00
acl safe_ports port 80
acl safe_ports port 1024-65535
acl safe_ports port 443

http_access deny !safe_ports
http_access deny vpn lanusers
http_acces deny manga lanusers
http_acces deny heures_bureau lanusers _
#http_access allow landata
http_access allow lanusers
#http_access allow lanwifi
#http_access allow lanToip
http_access deny all

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

Ici nous pouvons voir que vous avons rajouté des contraintes d'heures et de jour

```
acl heures_bureau time M T W H F A 08:00-18:00
```

on autorise les connexions seulement certain jour de la semaine de 8h a 18h :

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

```
http_acces deny heures_bureau lanusers
#http_access allow landata
```

ici on explique que à ses jours et horaires le lan users ne peut pas se connecter au sites que nous n'avons pas autorisé.