Proxy

Installer une debian 10 avec 1go de RAM et 40 go de stockage
Le mettre dans le vlan 60 pour le début
Faire une apt update et un apt urgrade pour installer toutes les mises à jour
Installer les paquets suivant :

-apt install squid
- apt install squidguard
-apt install apache2-utils
-apt install lightsquid

-créer les répertoires suivants :

-mkdir -p /apps/squid/cache
-mkdir -p /apps/squid/log
-mkdir -p /apps/squid/lib

-donner tous les droit à ces chemins :

- chown -R proxy:proxy /apps/squid/cache
- chown -R proxy:proxy /apps/squid/log
- chown -R proxy:proxy /apps/squid/lib

Installer ssh : apt install ssh
Récupérer le dossier blacklists : scp sio@heimdall.sio.jjr:/applis/www/squid/blacklists.tar.gz /apps/squid/lib
avec pour mot de passe : siojjr
Décompresser ce fichier : tar xfz /apps/squid/lib/ blacklists.tar.gz
Puis lui donner tous les droits : chown -R proxy:proxy /apps/squid/lib/blacklists

Pour configurer squid :
Arrêter squid : systemctl stop squid pour voir si squid est activer ou non : systemctl status squid
Faire un copie du /etc/squid/squid.conf : cp /etc/squid/squid.conf /etc/squid/squid.old
Effacer ce qu'il y a dans /etc/squid/squid.conf : echo < > /etc/squid/squid.conf
Puis écrire les lignes suivantes dans le fichier /etc/squid/squid.conf :

```
#Paramétrage du serveur
#Port sur lequel squid écoute
http_port 3128

#nom que renvoi squid quand il est interroger de l'extérieur
visible_hostname proxyjk

#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

#Pramétrage de logs

#log contenant les acces 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
```

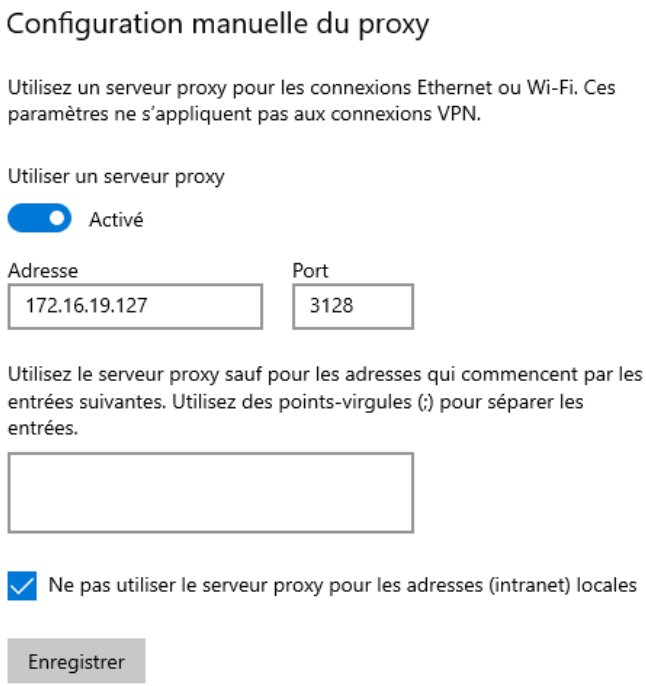
```
cache_log /apps/squid/log/cache.log

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

### Ports qui seront autorisé par le proxy
acl safe_ports port 80
 #port HTTP
acl safe_ports port 1024-65535
 #port client
acl safe_ports port 443
 #port HTTPS

#Autorisations ou no de l'accès http pour les différences acl
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 systemctl restart squid pour redémarrer squid
Aller dans les paramètre du proxy sur notre page internet (chrome, firefox), dans le même vlan, et ajouter l'adresse Ip du serveur proxy et son port :



Faire la commande tail -f /apps/squid/log/cache.log pour afficher cache.log en direct

Faire la commande tail -f /apps/squid/log/access.log pour afficher access.log en direct

```
root@proxyjk:~# tail -f /apps/squid/log/access.log
1665046229.117      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.118      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.120      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.121      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.131      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.132      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.134      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.143      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.167      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046229.206      0 172.16.19.127 TCP_DENIED/403 3921 CONNECT content-signature-2.cdn.mozilla.net:443 - HIER_NO
NE/- text/html
1665046262.195      0 172.16.19.127 TCP_DENIED/403 3900 CONNECT contile.services.mozilla.com:443 - HIER_NONE/- te
xt/html
```

Configuration de squidguard

Faire une copie du /etc/squid/squid.conf : cp /etc/squidgard/squidGuard.conf /etc/squidgard/ squidGuard.conf

Effacer ce qu'il y a dans /etc/squid/squid.conf : echo < > /etc/squidgard/squidGuard.conf

Puis écrire les lignes suivantes dans le dossier /etc/squidguard/squidGuard.conf :

Ajouter les lignes suivantes dans le fichier /etc/squid/squid.conf :

Faire systemctl restart squid

Faire squidGuard -C all -d pour bloqué les sites indésirables

Ensuite il ne faudra pas oublier de donner les droits au fichier squidguard :

-chown -R proxy /etc/squidguard/squid/squidGuard.conf