**TP1 : Le serveur proxy avec squid et squidgard**

**Environnement de travail :**

* Preparer une machine virtuelle Linux Debian 11
* Taille : 80 Go
* RAM : 2000 Go

***Installer les paquets suivants :***

* Squid
* Squidguard
* Apache2-utils
* Lightsquid
* Openssl

Créer les repertoires :

mkdir -p /apps/squid/cache

mkdir –p /apps/squid/log

mkdir -p/apps/squid/lib

Un utilisateur proxy sera le controleur de notre processus squid, il faut lui attribuer les droits aux fichiers et repertoires que nous avons crées precedemment

Il suffit de changer le propriétaire car un utilisateur est crée dès qu’on démarre le service et s’enregistre dans le cache, pour des raisons de sécurité, il ne pourra rien lancer.

* Chown r  proxy :proxy suivi du noms des repertoires crées

Nous devons installer un fichier de blacklists en version compressé, nous allons recuperer la ressource via la commande wget

Wget <http://dsi.int.capitole.fr/blacklists/blacklists.tar.gzz> chemin : /apps/squid/lib

Sur le repertoire apps/squid/lib, on fait une compression du fichier :

* tar -xvzf blacklists.tar.gz

**2. Configuration du squid**

Stoppez le service squid

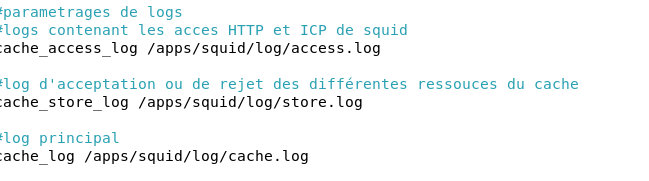
Deplacer le repertoire /etc/squid/squid.conf dans le /repertoire/home

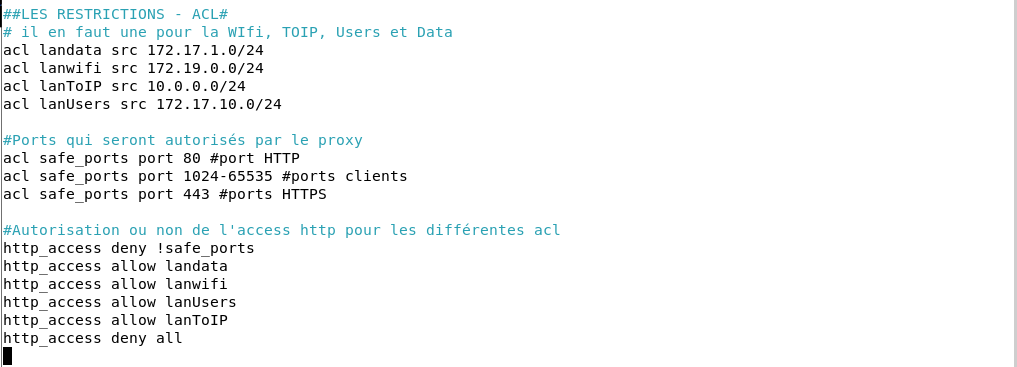
mv /etc/squid/squid.conf /home

Créer a nouveau le fichier de configuration squid dans le repertoire de l’utilisateur

Editer le fichier squid.conf





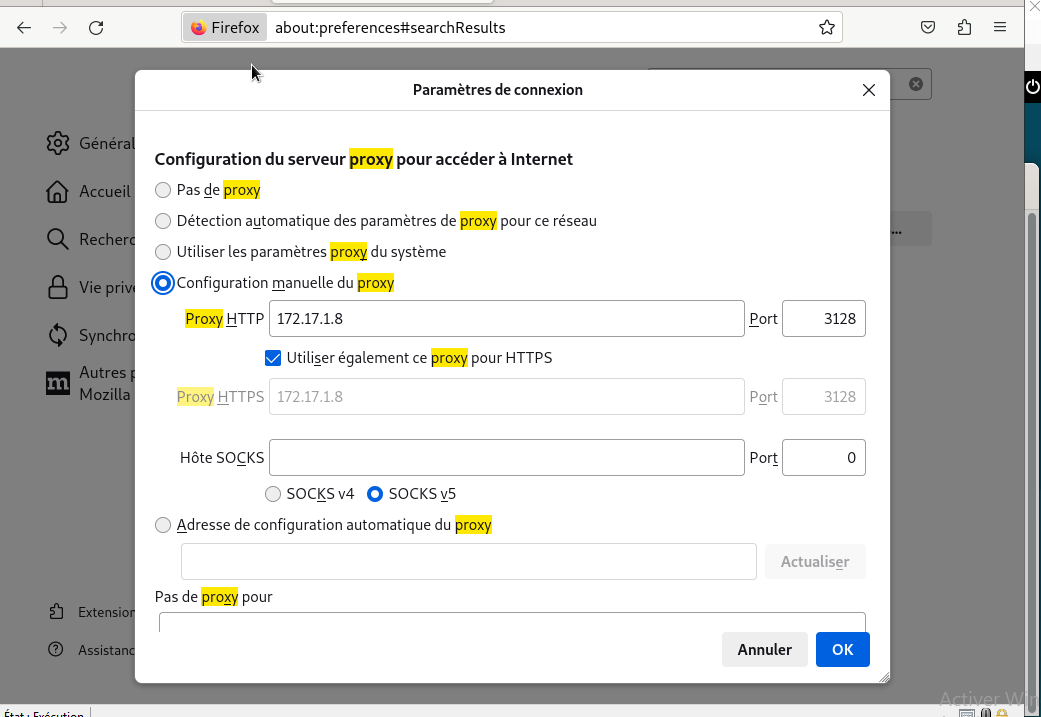


Ps –axf | grep squid(nom du service)

Reperez le temps

(reperez les processus squid)

**Configuration du parametrage proxy**



Précédemment, on a ajouté une règle déclarant que le client ne puisse pas faire des requetes http dans le champ « Autorisation ou non de l’accès http pour les différentes acl «

Chemin pointant vers les différents fichiers du repertoire home



3. Configuration squidGuard

Nous allons installer un logiciel qui va permettre l’interdiction de site Web en fonction d’une Blacklist

Parametrage du serveur

**ETAPES DE LA CONFIGURATION DU FICHIER SQUIDGUARD-**

1. Verifier si les domaines sont bien exactes
2. Adresser les sources par vlan

Puis se positionner sur chaque domain si il est bien existant via la blacklist :



#Destination interdites via l’utilisation des blacklists

Parametrage des acl pour chaque source autorisant ou non les acces à certaine destination



Avant de relancez squid, il faut lui signaler de démarre sqiuidguard, on ajoute alors dans /etc/squid/squid.conf :



Nous allons faciliter l’indexation des bases de données de squidGuard, ouvrez le log de squidguard :

**Tail –f /apps/squidguard/squidGuard.log**

Comment verifier si les interdictions ont bien été appliquées :

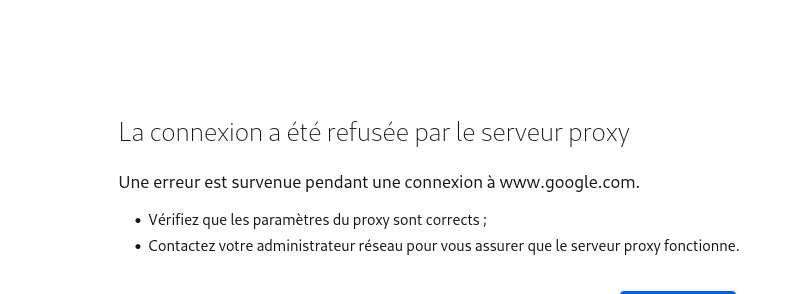
**Tail –f /apps/squid/log/access.log**

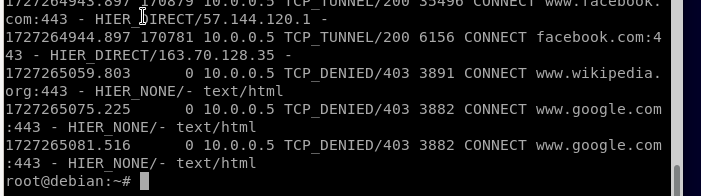
Test du Clt(vlan10) vers les réseaux :



Test du Clt (TOIP) sur le Web :







Plus de contraintes sous squid et squidGuard

Ajoutez une contrainte d’horaire en utilisant les ressources de type time sous Squid

On autorise les connexions du lan WIFI que sur les jours ouvrables de la semaine de 9 :00-20 :00

**Format de la ressource (time ) :**

**Liste des jours :**

**M-Monday T-Tuesday –W-Wednesday H-Thursday F-Friday A-Saturday S-Sunday**

Creation de la ressource (time) :

\*

**Il faut desormais authentifier les utilisateurs du reseau :**

