Proxy

Squid

Révision 1
04/12/25
Nombre de Pages :8

Antoine Pontier 2025

Introduction

Ce document est le compte rendu de l’installation du proxy squid

Sommaire

1. Mise en place

1.1 Installation

Squid est un serveur proxy capable de gérer les protocoles FTP, HTTP et HTTPS. Il est généralement utilisé pour le filtrage d'URL. Le serveur est installé sur une VM vide Debian 13 via Apt avec d'autres paquets.

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

Squid aura sa blacklist et ses logs dans le dossier « /apps/squid/ » qu'il faudra créer et rendre l'utilisateur squid, crée par l'installation, propriétaire de ces dossiers

```
mkdir -p /apps/squid/log
mkdir -p /apps/squid/lib
mkdir -p /apps/squid/cache
chown -R proxy:proxy /apps/squid
```

Il faut une base de domaine à bloquer, l'université Toulouse capitole fourni en licence CC-BY-SA 4.0 que nous allons utiliser (https://dsi.ut-capitole.fr/blacklists/)

```
cd /apps/squid/lib/
wget \
ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz
tar -xzvf blacklists.tar.gz
chown -R proxy:proxy /apps/squid
```

Puis il faut modifier le fichier de configuration tout en préservant l'ancien

```
cd /etc/squid/
cp ./squid.conf ./squid.old
rm ./squid.conf
nano squid.conf
```

Le nouveau fichier de configuration doit ressembler à celui ci-dessous qui permet le bloquage de tout requête en dehors des réseau définit mais qui pour le moment ne fait rien d'autre

```
#Serveur
#Port
http_port 3128

#Nom exterieur
visible_hostname BookticapProxy

#Cache mémoire
cache_mem 1024 MB
```

```
#Cache stocké
#type|où|taille max|répertoires primaires|secondaires
cache_dir ufs /apps/squid/cache 2000 16 256

#Identifiant de processus
pid_filename /var/run/squid.pid

#Logs
#log des accès http et icp
cache_access_log /apps/squid/log/access.log

#log decisions proxy
cache_store_log /apps/squid/log/store.log

#log principal
cache_log /apps/squid/log/cache.log

error_directory /usr/share/squid/errors/French
#ACL
#réseaux
acl landata src 172.17.1.0/24
acl lanuser src 172.17.10.0/24
acl lanwifi src 172.19.0.0/24
acl lantoip src 10.0.0.0/24
acl landmz src 172.18.0.240/28

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

#access
http_access deny !safe_ports
http_access allow landata
http_access allow lanuser
http_access allow lanwifi
http_access allow lantoip
http_access allow landmz
http_access deny all
```

1.2 Filtrage

Les listes de filtrage sont placée dans le fichier de configuration de squid

```
#Serveur
#Port
http_port 3128

#Nom exterieur
visible_hostname BookticapProxy

#Cache mémoire
cache_mem 1024 MB

#Cache stocké
#type|où|taille max|répertoires primaires|secondaires
cache_dir ufs /apps/squid/cache 2000 16 256

#Identifiant de processus
pid_filename /var/run/squid.pid

#Logs
#log des accès http et icp
cache_access_log /apps/squid/log/access.log

#log decisions proxy
cache_store_log /apps/squid/log/store.log

#log principal
cache_log /apps/squid/log/cache.log

error_directory /usr/share/squid/errors/French
#ACL
#réseaux
acl landata src 172.17.1.0/24
acl lanuser src 172.17.10.0/24
acl lanwifi src 172.19.0.0/24
acl lantoip src 10.0.0.0/24
acl landmz src 172.18.0.240/28

#ports
acl safe_ports port 80
acl safe_ports port 443
acl safe_ports port 1024-65535
```

```
#sites
acl sitetest dstdomain '/apps/squid/lib/blacklists/test/domains'
acl sitevpn dstdomain '/apps/squid/lib/blacklists/vpn/domains'

#access
http_access deny !safe_ports
http_access deny sitetest
http_access deny sitevpn
#http_access allow landata
#http_access allow lanuser
#http_access allow lanwifi
#http_access allow lantoip
#http_access allow landmz
http_access allow all
```

2. Problèmes

2.1 Squidguard

Originellement nous devions utiliser le plugin Squidguard pour effectuer le blocage mais le plugin n'est plus supporté depuis plus de 3 ans et il est en court de remplacement dans la future version de squid (7). Squidguard est un redirecteur d'url qui traitais à la place de squid la fonction de vérification du contenu, pour l'installer il faut ajouter ces lignes au fichier de configuration de Squid et retirer les lignes de filtrage du Chapitre 1.2 :

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

et modifier le fichier de config de Squidguard pour lui fournir les instructions :

```
#Serveur
dbhome /apps/squid/lib/blacklists
logdir /apps/squid/log/

#Sources
src landata {
      ip 172.17.1.0/24
}

#Sites
dest sitetest {
      domainlist test/domains
}
dest sitevpn {
      domainlist vpn/domains
}

#ACL
acl {
      landata {
            pass !sitevpn !sitetest all
      }
      default {
            pass none
      }
}
```

Normalement après un redémarrage tout devrais fonctionner sur le papier, or après diagnostique sur les machines virtuelles Squidguard n'interprète pas les requêtes de squid

2.2 Type de filtrage

Squid ne peux filtrer que du trafic FTP, HTTP et HTTPS. Tout les autres types de connexions passent pas à travers ce qui est voulu.

Mais un des problème est que on peux offusquer une connexion par ces protocoles ce qui pose un problème car par défaut Squid n’inspecte pas le contenu de ce trafic ce qui fait que le DoH et les connexions Tor avec pont passent à travers