Blocage de ChatGPT

mis à jour : 01-26
par Rémi Albertucci

Table des matières

I Contexte

Un professeur s'occupe d'une classe d'informatique à disposition des 3ième, notamment pour les certifications Pix mais aussi pour des cours.

Il n'interdit pas l'usage des IA et autres LLM, il leur apprend à s'en servir, et dans cette démarche il souhaite naturellement bloquer l'accès pendant les périodes d'examen.

Il est venu me demander comment faire pour bloquer momentanément ces sites, de manière facile et réversible.

Il faut donc une solution clé en main pour bloquer des sites, facile à utiliser et universelle, destinée à des élèves de 3ieme et non à des pentesters chevronnés.

II Solution proposée

Une solution simple semble s'imposer : Adguard, qui vient trier les requêtes au niveau DNS.

Une fois installé sur le réseau, on peut bloquer en un clic chatGPT ainsi que d'autres sites.

En le mettant en place dans un conteneur LXC, on peut aussi imaginer dupliquer le conteneur au besoin pour refaire le même blocage dans différentes salle facilement.
La seule contrainte étant qu'il faut rediriger le trafic DNS de la salle vers Adguard, et rediriger le trafic ensuite vers l'AD pour que les PC puissent s'identifier.

C'est une solution économe en ressources (1 coeur – 256Mb - 2Go suffisent), 100 % gratuite et facile à mettre en place/dupliquer.
Il sera de plus aisé de sauvegarder l'état et de restaurer ce conteneur au besoin.

III Mise en place

III.1 Conteneur LXC

Tout d'abord, il faut créer un conteneur LXC, ici Debian 13 (se référer à la documentation au besoin).

Comme dit précédemment, nous lui attribuerons le minimum de ressources :

- 2Go de stockage
- 1 coeur
- 256Mb de Ram

Le conteneur sera bien sûr relié réseau « Pédago ».
La configuration sera relativement simple :

- pas d'user
- accès ssh bloqué
- ip fixée

Pour couper ssh :

```
systemctl disable --now ssh
```

L'accès ne pourra se faire que depuis la console proxmox accessible depuis le réseau admin.

On fixe également l'ip de la machine, et pour faire deux façons : dire au routeur que cette adresse mac aura cette IP.
Ou faire en sorte que la machine virtuelle demande cette IP au routeur à chaque connexion.

La solution 1 est plus propre mais nécessite un accès qui est pour le moment en maintenance, nous allons donc fixer l'ip de la machine virtuelle depuis celle ci. Étant toujours allumée, le bail ne devrait pas expirer dans l'immédiat et on pourra modifier l'adressage de l'IP ultérieurement (même s'il n'est jamais bon de procrastiner !) :

```
nano /etc/network/interfaces
```

```
auto lo
        iface lo inet loopback

auto eth0
        iface eth0 inet static
        address XX.XX.XX.XX
```

```
        netmask 255.255.0.0
        gateway XX.XX.XX.XX
```

```
systemctl restart networking
reboot
```

On vérifie que ça ait fonctionné avec ip a et on continue vers l'installation d'adguard.

Pour installer automatiquement les mise à jour de sécurité :

```
sudo apt update
sudo apt install unattended-upgrades apt-
listchanges
sudo dpkg-reconfigure unattended-upgrades
```

III.2 Installation Adguard

Une fois notre conteneur LXC configuré :

```
apt update
apt upgrade -y
apt install curl ca-certificates -y
```

On peut ensuite créer un dossier adguard avec mkdir à l'endroit désiré et on se positionne dedans avec cd :

```
curl -s -S -L
https://static.adguard.com/adguardhome/re
lease/AdGuardHome_linux_amd64.tar.gz \
| tar xz
cd AdGuardHome
./AdGuardHome -s install
```

On peut alors se rendre à l'adresse http://IP-DE-LA-VM:3000 et attaquer la configuration via GUI.