Squid (Port 3128)

10/03/2024

Introduction :

Qu’est ce que Squid ?

Squid est un logiciel de serveur proxy open-source largement utilisé. Il agit comme une interface entre les utilisateurs et l'internet, en permettant le contrôle d'accès, la gestion de la bande passante, la mise en cache de contenu et d'autres fonctionnalités liées à la gestion des requêtes web.

Squid est souvent utilisé dans les réseaux informatiques pour améliorer la performance, économiser la bande passante et renforcer la sécurité.

En tant que proxy, Squid intercepte les demandes web des utilisateurs et les transmet au serveur distant, puis renvoie les réponses du serveur aux utilisateurs. Cela permet un certain nombre de fonctionnalités, telles que le filtrage du contenu, la mise en cache pour accélérer l'accès aux sites fréquemment consultés, et la limitation de la bande passante pour certaines applications.

Squid est principalement utilisé dans des environnements réseau tels que les entreprises, les écoles et les fournisseurs d'accès Internet pour optimiser la gestion des ressources réseau et améliorer l'expérience utilisateur.

Installation :

I) Tout d’abord, je commence par installer Squid

```
root@debian:~# apt install squid
```

```
root@debian:~# netstat -atn | grep 3128
tcp6       0      0 :::3128                 :::*                    LISTEN
```

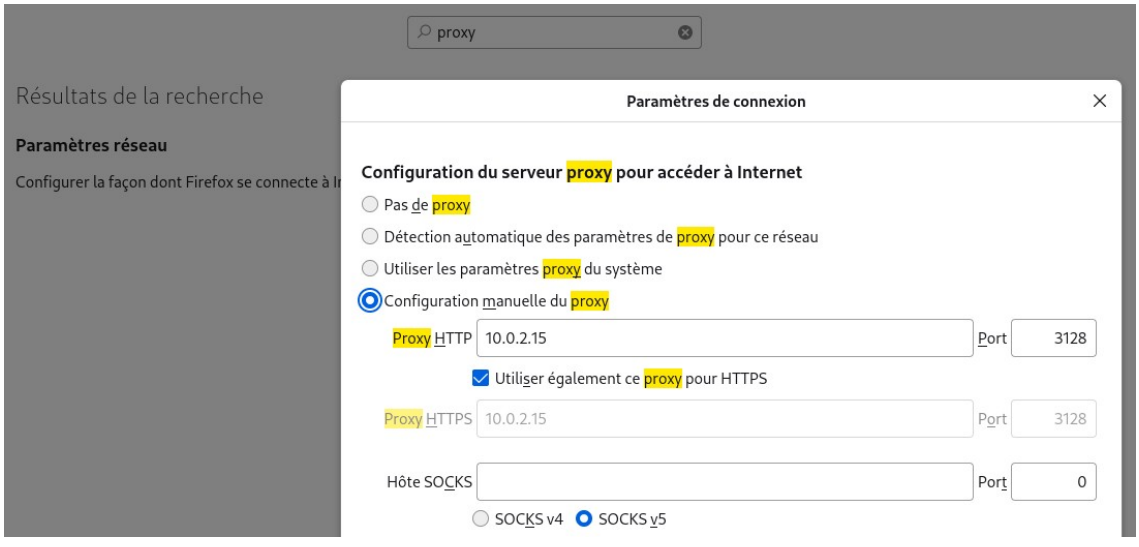
II) Je configure mon fichier squid.conf présent dans /etc/squid, le fichier est rempli de nombreux commentaires, pas forcément utiles, donc je commence par les supprimer grâce à vi

g/^#/d : Supprime toutes les lignes qui commence par #.
g/^$/d : Supprime les lignes vides.

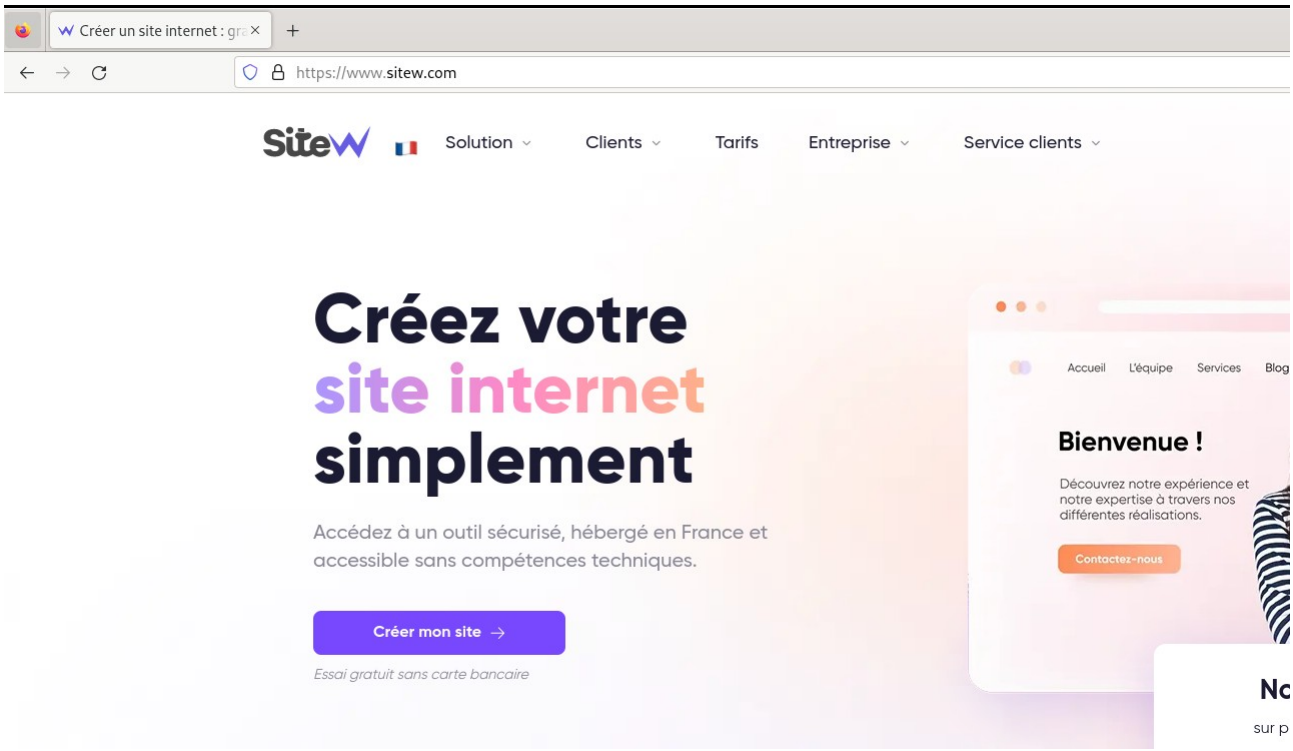
III) Désormais, mon fichier est propre. Je peux configurer le fichier en bloquant l'accès au site et configurer mes acls

```
  GNU nano 7.2                          squid.conf
acl monpost src 10.0.2.15/24
acl SSL_ports port 443

# ACL pour le site pratique.leparisien.fr en HTTP
acl siteblock_http dstdomain .pratique.leparisien.fr

#lien
url_rewrite_program /usr/bin/squidGuard

# Bloquer l'accès au site en HTTP
http_access deny siteblock_http
# Autoriser l'accès à monpost
http_access allow monpost

# Définition des autres ACL Safe_ports
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager

include /etc/squid/conf.d/*.conf

http_access allow localhost
```

IV) Ensuite, sur mon moteur de recherche, je viens mettre le proxy Squid dans les paramètres



V) Maintenant, testons un site au hasard et le site interdit

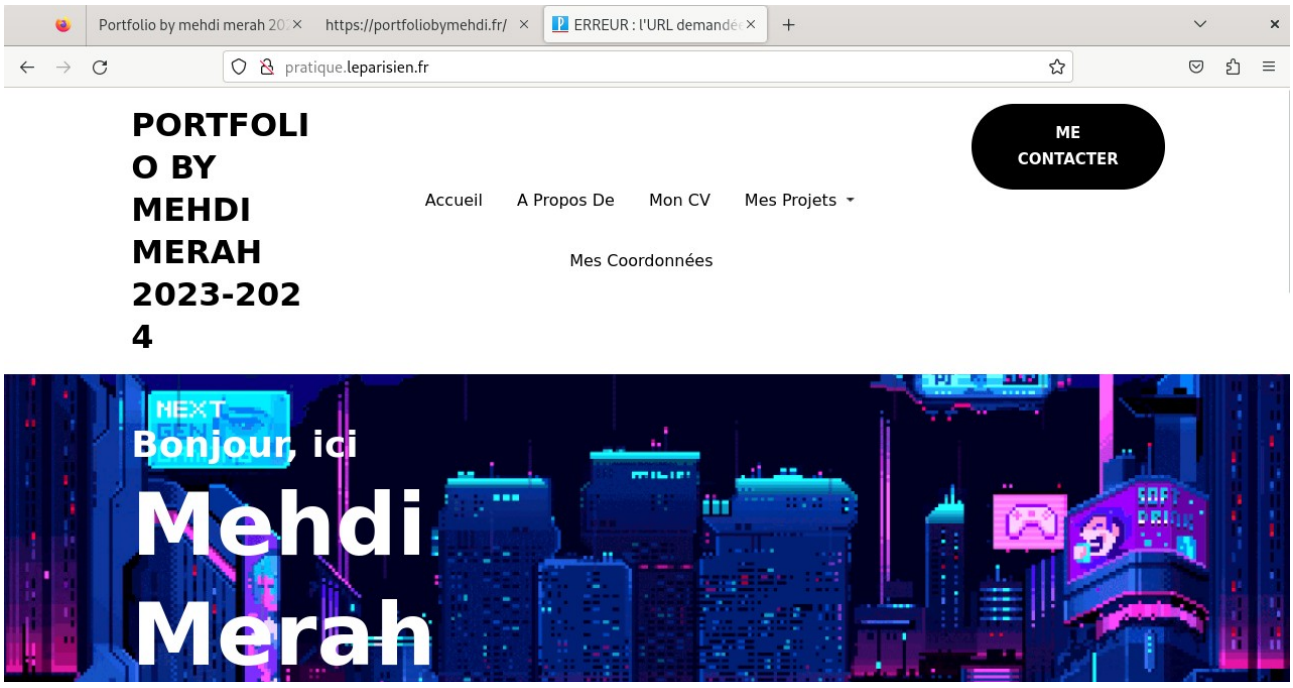


VI) Le site a bien était bloqué, je peux vérifier dans les logs de Squid

```
root@debian:/etc/squid# tail -f /var/log/squid/access.log
```

```
1707677229.557 115605 10.0.2.15 TCP_TUNNEL/200 4406 CONNECT eur-bid-hubvisor.adsrvr.org:443 - HIER_DIRECT/15.197.133.55 -
1707677232.558 175796 10.0.2.15 TCP_TUNNEL/200 12630 CONNECT ae.mmstat.com:443 - HIER_DIRECT/47.246.110.45 -
1707677233.132      0 10.0.2.15 TCP_DENIED/403 4764 GET http://pratique.leparisien.fr/glossaire/informatique/ordinateur/http-1330003116 - HIER_NONE/- text/html
1707677233.558 183461 10.0.2.15 TCP_TUNNEL/200 26891 CONNECT script.4dex.io:443 - HIER_DIRECT/104.26.9.169 -
1707677234.559 115808 10.0.2.15 TCP_TUNNEL/200 4656 CONNECT ad.yieldlab.net:443 - HIER_DIRECT/104.124.109.153 -
1707677236.205 188318 10.0.2.15 TCP_TUNNEL/200 45469 CONNECT assets.pinterest.com:443 - HIER_DIRECT/184.51.104.201 -
1707677236.405 188399 10.0.2.15 TCP_TUNNEL/200 38136 CONNECT www.leparisien.fr:443 - HIER_DIRECT/104.125.3.145 -
1707677238.048 187419 10.0.2.15 TCP_TUNNEL/200 63232 CONNECT images.outbrainimg.com:443 - HIER_DIRECT/23.212.157.240 -
1707677238.405 187737 10.0.2.15 TCP_TUNNEL/200 30377 CONNECT widgets.outbrain.com:443 - HIER_DIRECT/104.124.109.108 -
1707677238.927 120603 10.0.2.15 TCP_TUNNEL/200 6539 CONNECT hb.yahoo.net:443 - HIER_DIRECT/96.17.206.23 -
1707677239.207 121586 10.0.2.15 TCP_TUNNEL/200 85393 CONNECT libs.outbrain.com:443 - HIER_DIRECT/104.124.109.108 -
```

V) Je peux m’amuser à changer la page d’erreur par défaut de Squid en y insérant le code source de mon portfolio vi errorpage.css



Squidguard

10/03/2024

Introduction :

Qu’est ce que SquidGuard ?

SquidGuard est un module d'extension pour le serveur proxy Squid, souvent utilisé pour le filtrage du contenu web. Son rôle principal est d'ajouter des fonctionnalités de filtrage, de blocage et de redirection d'URL en complément de Squid.

SquidGuard offre une gestion avancée des politiques d'accès à Internet en permettant aux administrateurs de définir des règles spécifiques pour contrôler l'accès aux sites web.

Installation :

I) Je télécharge SquidGuard

```
root@debian:~# apt install squidguard
```

II) Je télécharge une blacklists trouvé sur internet

III) Ensuite je peux la décompresser grâce à la commande tar

```
root@debian:/home/exoldy/Téléchargements# tar -xzf blacklists.tar.gz
```

IV) Je déplace la blacklists dans le bon chemin

```
root@debian:/var/lib/squidguard/db# cp -R blacklists/* /var/lib/squidguard/db/
```

V) Ensuite, je configure le fichier squidguard.conf

```
  GNU nano 7.2                                                  /etc/squidguard/squidGuard.conf
dbhome /var/lib/squidguard/db

# Définition des catégories à bloquer
dest games {
    domainlist games/domains
    urllist games/url
    expressionlist games/expressions
}

# Définition des ACL pour bloquer l'accès
acl {
    monpost {
        pass !games_domains !porn !games_url all !all
        redirect https://portfoliobymehdi.fr
    }
}

# Inclure la blacklist
blacklist blacklist {
    domainlist blacklist/domains
    urllist blacklist/urls
}
```

VI) Puis, il faut rajouter la phrase suivante dans le fichier squid.conf

```
#lien
url_rewrite_program /usr/bin/squidGuard
```

VII) Désormais, on peut reload Squid

```
root@debian:/etc/squidguard# systemctl reload squid
root@debian:/etc/squidguard# systemctl status squid
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-03-10 20:59:06 CET; 1min 43s ago
       Docs: man:squid(8)
    Process: 6116 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
    Process: 6284 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
   Main PID: 6119 (squid)
      Tasks: 5 (limit: 4262)
     Memory: 19.2M
        CPU: 175ms
```