

```
File Actions Edit View Help
(kotto@kali)-[~]
$ sudo mkdir -p /usr/share/squid/errors/fr/
[sudo] password for kotto:
(kotto@kali)-[~]
$ sudo nano /usr/share/squid/errors/fr/SITE_BLOQUE.htm
l

(kotto@kali)-[~]
$ sudo nano /etc/squid/squid.conf

(kotto@kali)-[~]
$ sudo systemctl restart squid

(kotto@kali)-[~]
$
```

```
(kotto@kali)-[~]
$ cat /etc/squid/squid.conf | grep sites_bloques

acl sites_interdits dstdomain "/etc/squid/sites_bloques.txt"
```

- `cat /etc/squid/squid.conf` :
  - Cela **affiche tout le contenu** du fichier de configuration principal de Squid (`squid.conf`).
- `|` (pipe) :
  - Cela **envoie le résultat** de la commande précédente (le contenu du fichier) **vers** une autre commande.
- `grep sites_bloques` :
  - Cela **cherche uniquement** les lignes qui contiennent le mot `sites_bloques`.

---

## □ En résumé :

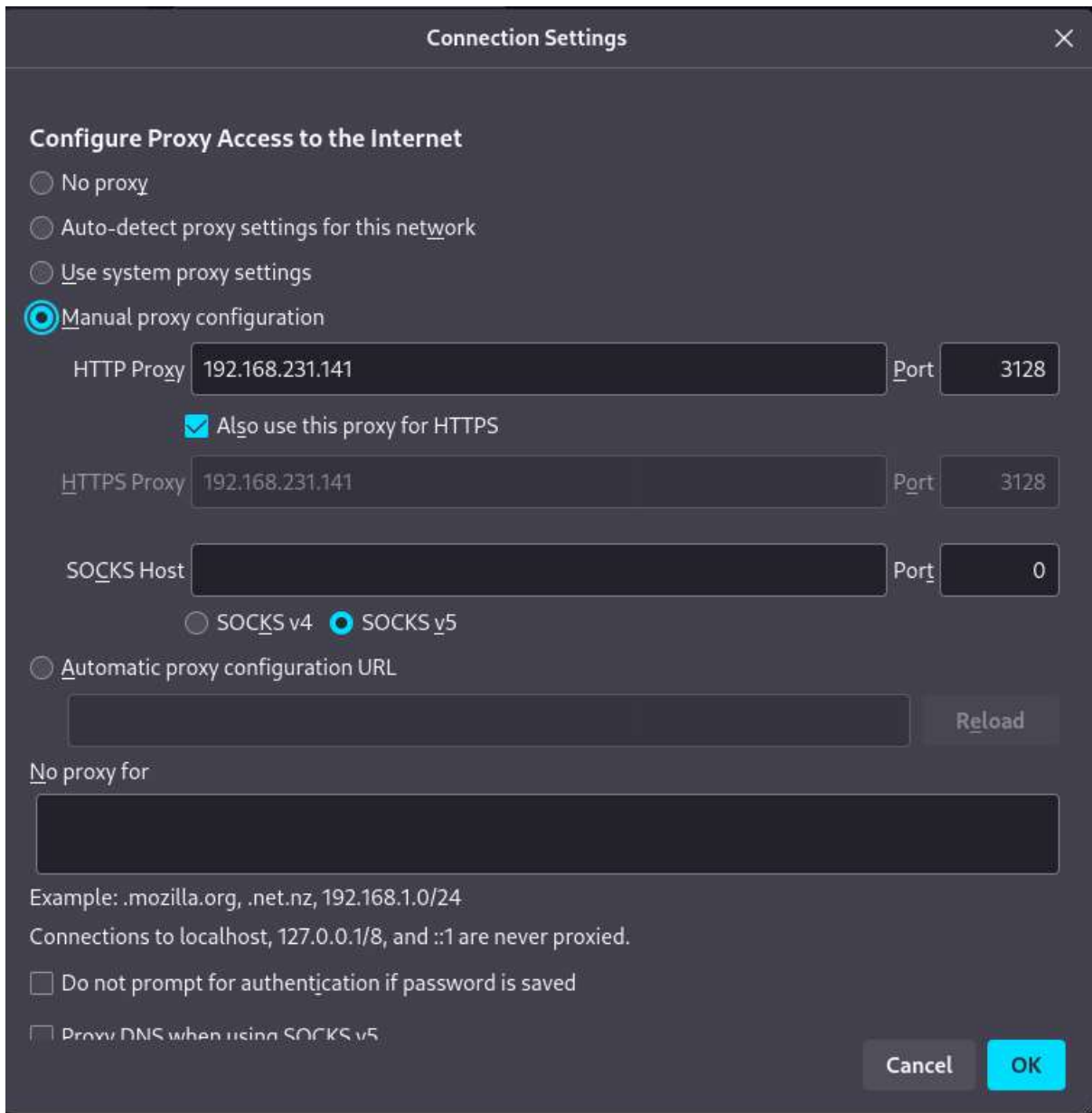
Cette commande sert à **vérifier rapidement** si ton fichier `squid.conf` est bien configuré pour utiliser ton fichier de sites bloqués (`sites_bloques.txt`).

```
(kotto@kali)-[~]
$ cat /etc/squid/sites_bloques.txt

pornhup.com
youtube.com
tiktok.com
```

- `cat` = "**concatenate**" → c'est une commande Linux qui sert principalement à **afficher le contenu d'un fichier** directement dans le terminal.
- `/etc/squid/sites_bloques.txt` = c'est le chemin vers **ton fichier** où tu as listé les sites à bloquer.

Donc, **cette commande affiche à l'écran la liste des sites interdits** que tu as enregistrée dans `sites_bloques.txt`, sans l'ouvrir avec un éditeur de texte.



Connection Settings

**Configure Proxy Access to the Internet**

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy  Port

☒ Also use this proxy for HTTPS

HTTPS Proxy  Port

SOCKS Host  Port

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

Cancel OK

```
(kotto@kali)-[~]
$ sudo systemctl start squid

(kotto@kali)-[~]
$ sudo systemctl status squid

● squid.service - Squid Web Proxy Server
   Loaded: loaded (/usr/lib/systemd/system/squid.service; disabled; preset>
   Active: active (running) since Mon 2025-04-28 11:48:41 CEST; 19s ago
   Invocation: 87890e68c7cf45c8acc40ded71bfebb5
     Docs: man:squid(8)
   Process: 21809 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited>
  Main PID: 21813 (squid)
    Tasks: 4 (limit: 3472)
   Memory: 24.6M (peak: 25M)
      CPU: 457ms
   CGroup: /system.slice/squid.service
           └─21813 /usr/sbin/squid --foreground -sYC
             └─21821 "(squid-1)" --kid squid-1 --foreground -sYC
               └─21825 "(logfile-daemon)" /var/log/squid/access.log
                 └─21826 "(pinger)"
```

- **systemctl** : C'est l'outil qui gère les **services** (programmes qui tournent en arrière-plan) sur Linux.
- **status squid** : Demande à **systemctl** de **montrer l'état** du service **Squid**.

---

## ☐ Ce que tu dois voir :

- **active (running)** → Squid fonctionne correctement ✓
- **inactive (dead)** → Squid est arrêté ✗

Cette commande sert à vérifier si Squid est bien en train de tourner sur ta machine.

```
(kotto@kali)-[~]
$ sudo apt install squid -y

[sudo] password for kotto:
squid is already the newest version (6.13-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2133

(kotto@kali)-[~]
$ sudo apt install squid -y

[sudo] password for kotto: █
```

Cette commande **installe le logiciel Squid** sur ta machine **sans te demander de confirmation**, en mode rapide.

C'est une des **premières étapes indispensables** pour transformer ta machine en **serveur proxy**.

```
kotto@kali: ~  
File Actions Edit View Help  
valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq sta  
te UP group default qlen 1000  
    link/ether 00:0c:29:71:52:5d brd ff:ff:ff:ff:ff:ff  
    inet 192.168.231.141/24 brd 192.168.231.255 scope global dyn  
amic noprefixroute eth0  
        valid_lft 1446sec preferred_lft 1446sec  
    inet6 fe80::20c:29ff:fe71:525d/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
  
(kotto@kali)-[~]  
$ ^[[200~sudo tail -f /var/log/squid/access.log  
zsh: bad pattern: ^[[200~sudo  
  
(kotto@kali)-[~]  
$ ~sudo tail -f /var/log/squid/access.log  
  
Command '~sudo' not found, did you mean:  
  command 'sudo' from deb sudo  
  command 'sudo' from deb sudo-ldap  
Try: sudo apt install <deb name>  
  
(kotto@kali)-[~]  
$ sudo tail -f /var/log/squid/access.log  
  
[sudo] password for kotto:  
1744727145.637 15482 127.0.0.1 TCP_MISS/200 1582 GET http://exa  
mple.com/ - HIER_DIRECT/96.7.128.198 text/html  
^C  
  
(kotto@kali)-[~]  
$ sudo nano /etc/squid/sites_bloques.txt  
  
(kotto@kali)-[~]  
$ sudo nano /etc/squid/squid.conf  
  
(kotto@kali)-[~]  
$ sudo systemctl restart squid  
  
(kotto@kali)-[~]  
$
```

- Affichage des informations réseau :

- Tu montres que ta machine Kali utilise l'interface `eth0`.
- Ton adresse IP est `192.168.231.141`.
- Cela confirme que ta machine proxy est bien connectée au réseau.

- Tentative d'affichage des logs Squid :

- Première tentative : erreur (`~sudo` n'existe pas) → faute de frappe.
- Deuxième tentative correcte :

```
bash  
CopierModifier  
sudo tail -f /var/log/squid/access.log
```

- Résultat : une connexion a été faite via le proxy (127.0.0.1) pour accéder à `http://example.com/`. → **Ton proxy fonctionne** et capture bien les requêtes !

- **Modification des fichiers de Squid :**

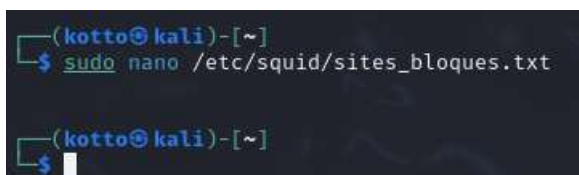
- Tu ouvres **le fichier** `/etc/squid/sites_bloques.txt` → pour ajouter les sites à bloquer.
- Tu ouvres **le fichier** `/etc/squid/squid.conf` → pour configurer Squid afin de prendre en compte le blocage.

- **Redémarrage du service Squid :**

- Tu exécutes :

```
bash
CopierModifier
sudo systemctl restart squid
```

- Cela applique toutes les modifications que tu as faites.



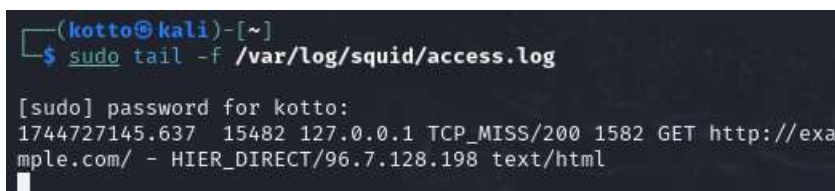
```
(kotto@kali)-[~]
$ sudo nano /etc/squid/sites_bloques.txt

(kotto@kali)-[~]
$
```

La création du fichier `/etc/squid/sites_bloques.txt` est une étape essentielle pour **gérer facilement les sites que tu veux interdire** via ton proxy Squid.

Grâce à ce fichier :

- Tu peux **centraliser la liste** des sites à bloquer.
- Tu peux **ajouter, modifier ou supprimer** des sites **très rapidement**, sans avoir à réécrire toute la configuration de Squid.
- Cela rend ton proxy **plus flexible** et **plus facile à administrer**.



```
(kotto@kali)-[~]
$ sudo tail -f /var/log/squid/access.log

[sudo] password for kotto:
1744727145.637 15482 127.0.0.1 TCP_MISS/200 1582 GET http://example.com/ - HIER_DIRECT/96.7.128.198 text/html
```