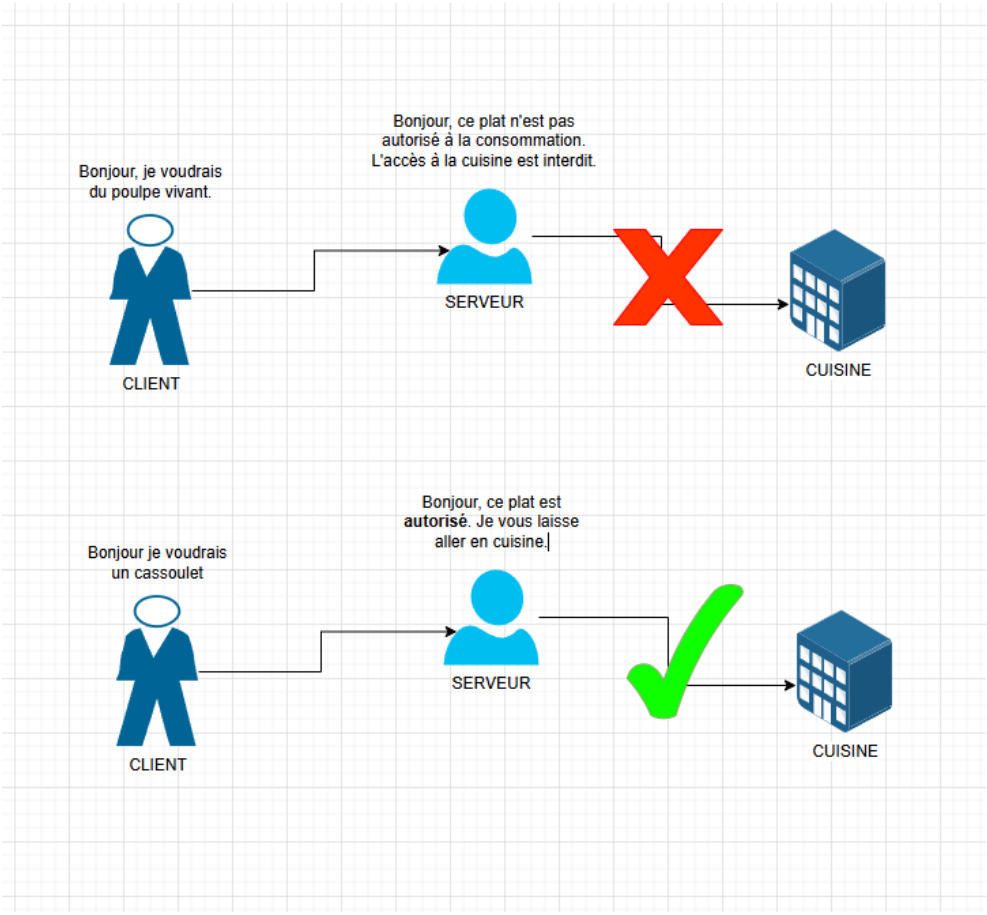
TP-Proxy (proxy-squid) Luca BONA

Un Proxy ?? Comment ca marche ?

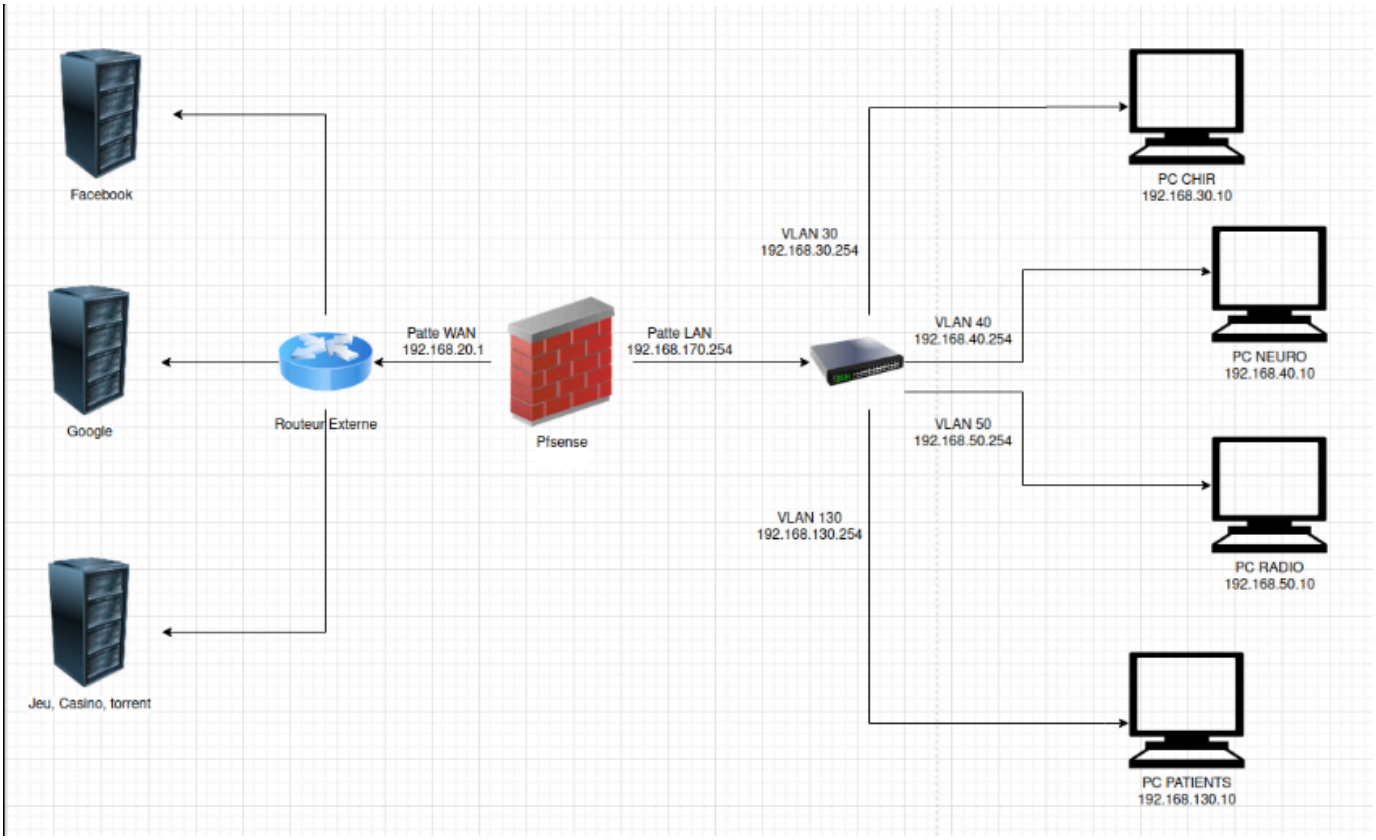
L'idée est simple : au lieu que chaque ordinateur demande directement une page à Internet, ils vont tous passer par un "secrétaire" (le **Proxy Squid**) qui vérifiera si la demande est autorisée et s'il n'a pas déjà la réponse en mémoire.

> **Le Proxy en une image : Imaginez un restaurant où les clients (les PC) doivent aller en cuisine préparer eux-mêmes leurs plats. Avant ça ils donnent leur commande à un serveur (le Proxy).**
>
> 1. Si le client demande un plat interdit (site bloqué), le serveur refuse car il est interdit de commander ce plat.
> 2. Si le client demande un plat déjà prêt, donc qui n'est pas interdit, le serveur laisse les clients aller dans la cuisine



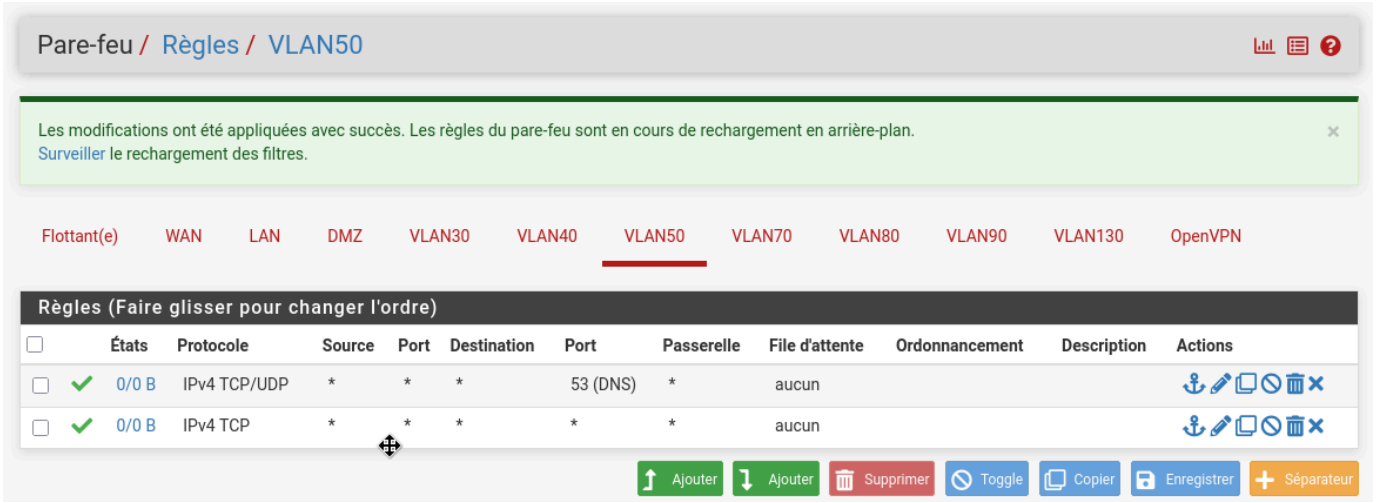
1. Mise en place de l'infra

Ici c'est mon contexte, j'utilise un boitier netget avec pfsense, un firewall opensource. J'utilise aussi de l'intervlan pour mes differents service



2. Premier contact avec pfSense

Dans mon contexte je n'avais pas de connexion a internet depuis mon LAN,
j'ai donc tout mis en oeuvre pour pouvoir faire ce tp, j'ai simplement creer des vlans qui sont identique a ceux de mon switch. La passerelle n'est plus donnée par mon switch, mais par pfsense. Tout les pc utilise la passerelle du vlan qui leur est attitrer, ici 192.168.X.254/24



Avant d'installer quoi que ce soit, vérifions que notre machine "parle" bien à Internet.

- **Accès :** `https://10.0.0.1` (admin / pfsense)
- **Vérification :** Menu `Diagnostics > Ping` -> Testez `8.8.8.8`.
- **Vérification :** Menu `Diagnostics > Ping` -> Testez `google.com`.
- **Vérification :** Menu `Diagnostics > Etat > WAN`

Réponses attendues

- **Q1 (Version) :** 23.09.1-RELEASE.

Résultat

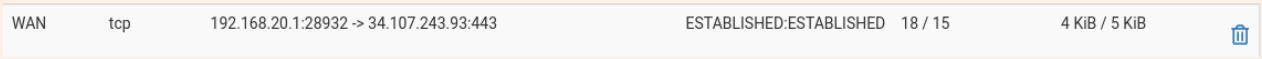
```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=117 time=5.652 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=5.509 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=5.533 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 5.509/5.565/5.652/0.062 ms
```

Résultat

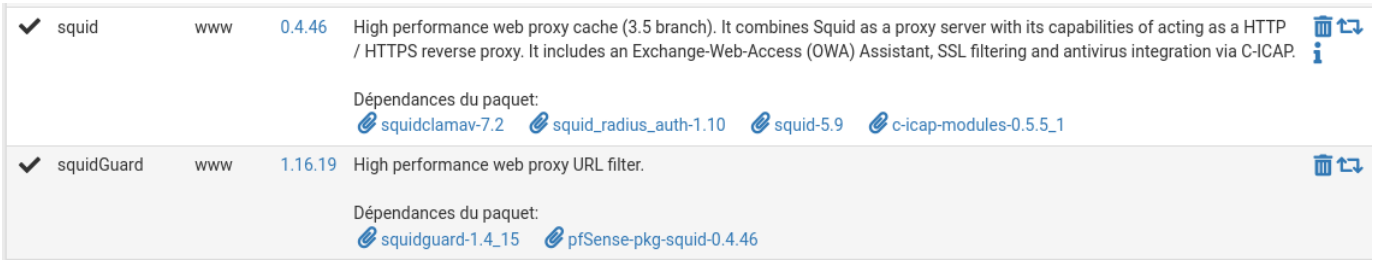
```
PING google.com (142.251.142.14): 56 data bytes
64 bytes from 142.251.142.14: icmp_seq=0 ttl=117 time=5.887 ms
64 bytes from 142.251.142.14: icmp_seq=1 ttl=117 time=5.832 ms
64 bytes from 142.251.142.14: icmp_seq=2 ttl=117 time=5.969 ms

--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 5.832/5.896/5.969/0.056 ms
```



3. Installation du package Squid

1. Allez dans `System > Package Manager > Available Packages`.
2. Cherchez **Squid** et cliquez sur **Install**.



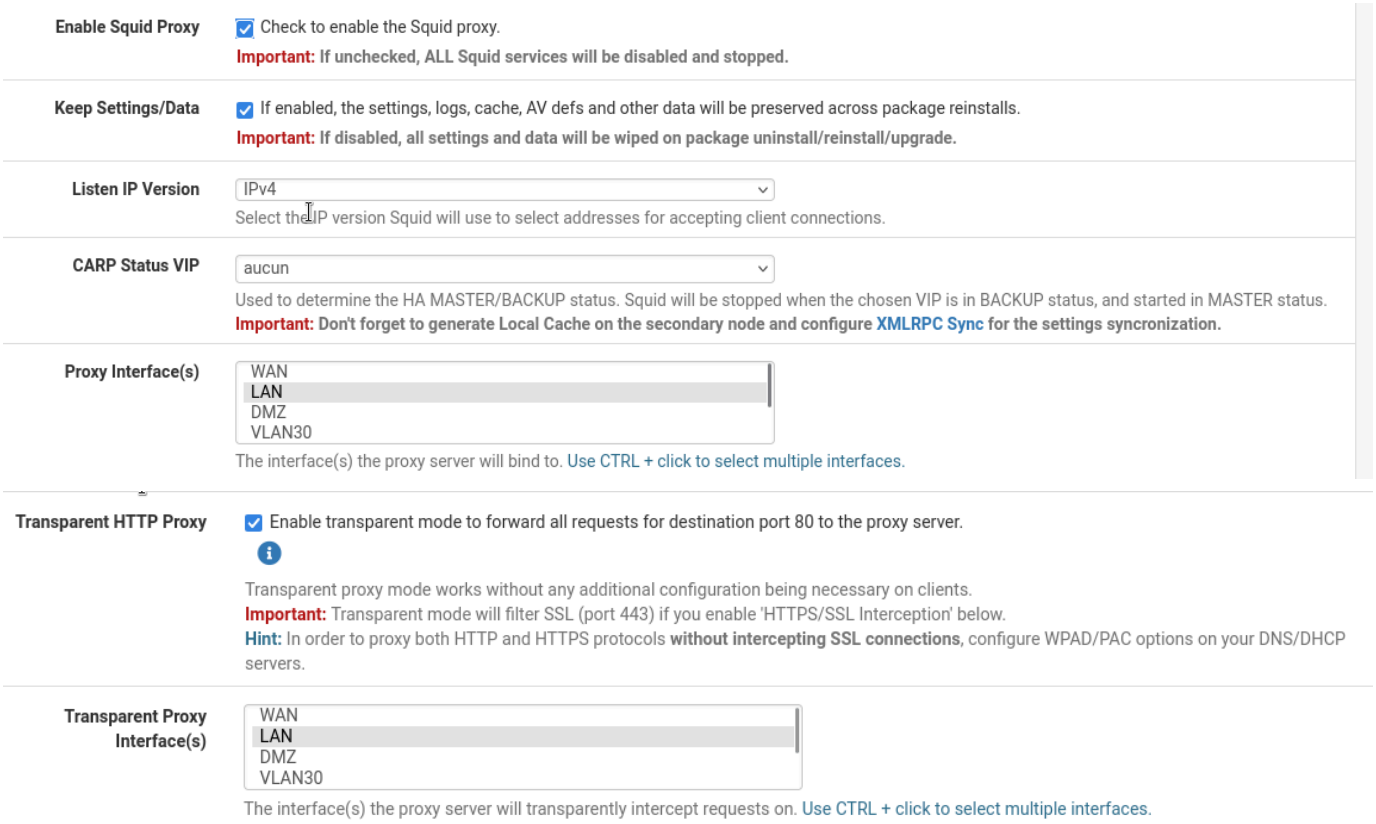
À savoir On utilise souvent **SquidGuard** en complément. Si Squid est le moteur, SquidGuard est le cerveau qui contient des listes de millions de sites classés par catégories (sport, jeux, etc.). Mais il y'a aussi SARG - Squid Analysis Report Generator. **Son rôle :** Il transforme les milliers de lignes de textes bruts (les "logs") en **tableaux et graphiques HTML** faciles à lire.

4. Configuration générale de Squid

Rendez-vous dans `Services > Squid Proxy Server > General`. C'est ici qu'on allume la machine et qu'on lui donne ses ordres de base.

🖊 Réglages à appliquer

- **Enable Squid Proxy** : ✅ (On appuie sur l'interrupteur).
- **Proxy Interface(s)** : Choisissez **LAN**. C'est le côté "intérieur" de votre réseau, là où sont vos utilisateurs.
- **Proxy Port** : `3128`. C'est le numéro de la porte par laquelle les données vont entrer dans le proxy.
- **Transparent HTTP Proxy** : ✅ **Coché**. C'est le mode "ni vu ni connu" : les PC sont filtrés sans même le savoir.
- **HTTPS/SSL Interception** : ❌ **Décoché**. On ne touche pas encore au cadenas des sites sécurisés (c'est complexe, on verra ça en bonus).
- **Visible Hostname** : `proxy.netsecure.lan` (Le petit nom de votre serveur).



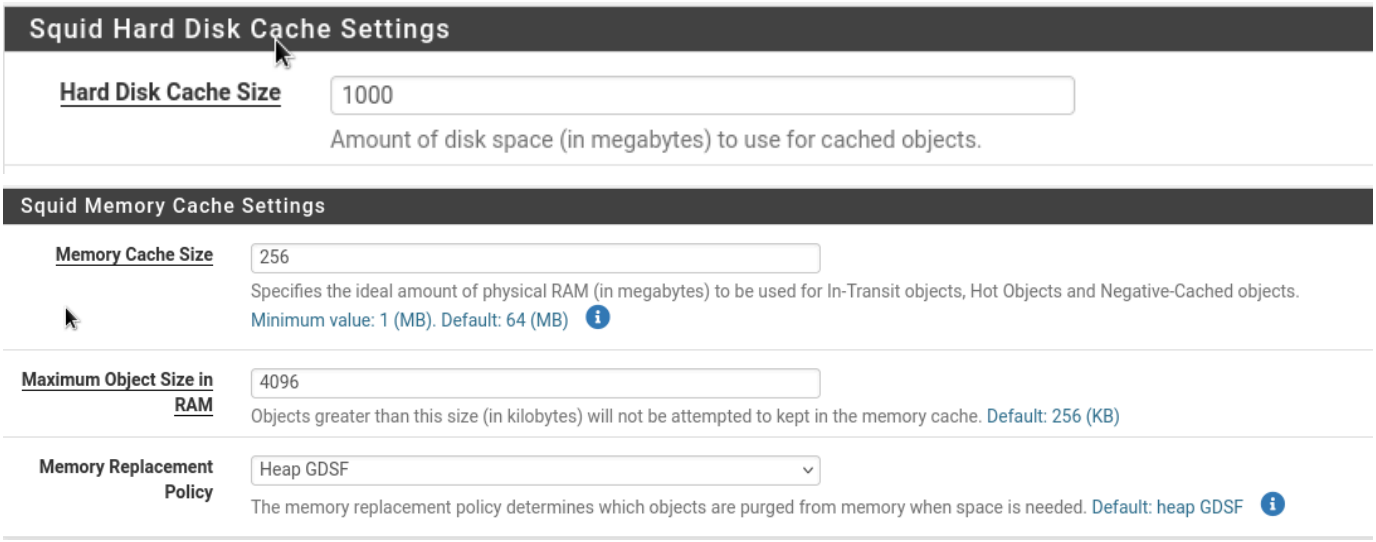
5. Configuration du Cache (La mémoire locale)

Le **Cache**, c'est la bibliothèque de votre proxy. Au lieu de retourner sur Internet (lent) chercher la même image 50 fois, Squid en garde une copie dans son "placard" (rapide).

🖊 Paramètres du Cache Local Rendez-vous dans : `Services > Squid Proxy Server > Local Cache`

- **Hard Disk Cache Size (MB)** : `1000` *(C'est la taille de votre placard sur le disque dur : 1 Go ici).*

- **Hard Disk Cache Location** : `/var/squid/cache` *(L'adresse précise du dossier de stockage dans pfSense).*
- **Memory Cache Size (MB)** : `256` *(C'est la RAM. C'est encore plus rapide que le disque, mais plus petit).*
- **Maximum Object Size (KB)** : `4096` *(La taille max d'un fichier qu'on accepte de garder. On évite de stocker des films entiers !).*
- **Minimum Object Size (KB)** : `0` *(On accepte de garder même les tout petits fichiers comme les icônes).*



6. Filtrage : Qui a le droit de voir quoi ?

6.1 Les Listes (ACL)

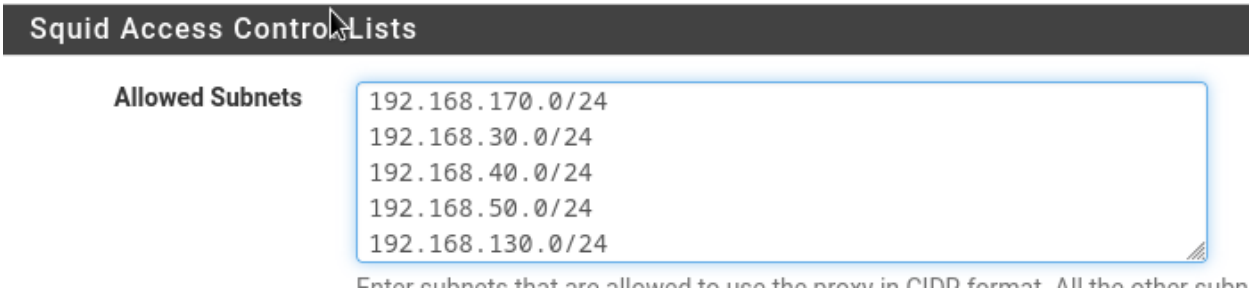
Rendez-vous dans l'onglet **ACLs**.

Type	Analogie
Whitelist	La liste des invités VIP (Autorisés d'office).
Blacklist	La liste des personnes bannies de la boîte de nuit.

> **⚠ Le point stratégique**
>
> En mettant `.facebook.com` (avec un point devant), vous bloquez la maison mère ET toutes les dépendances (`messenger.facebook.com` , etc.). C'est un filet de sécurité total.

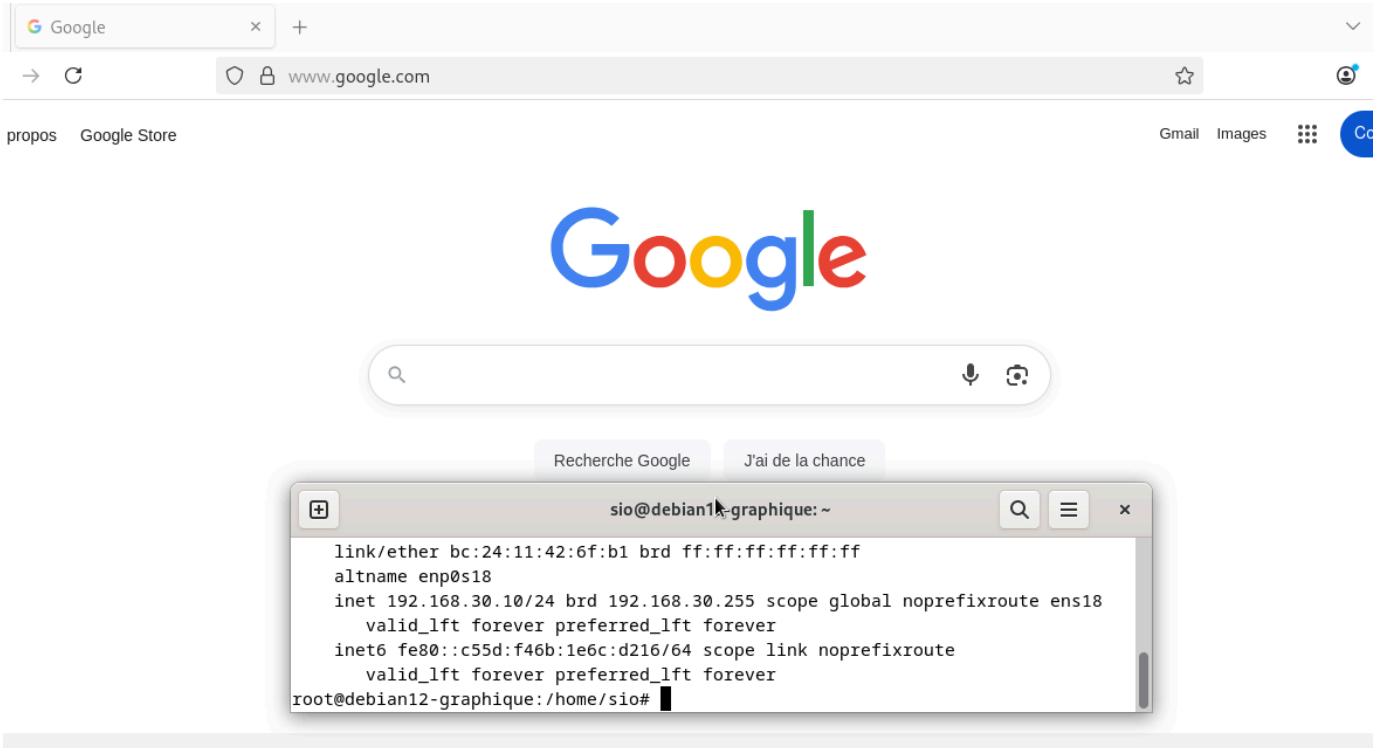
6.2 Les Expressions Régulières (Regex)

C'est le filtrage par "mot-clé". Si l'URL contient "casino" ou "torrent", le proxy coupe le sifflet à la connexion, peu importe le nom du site.



6.3 Les Tests

Client CHIR ->



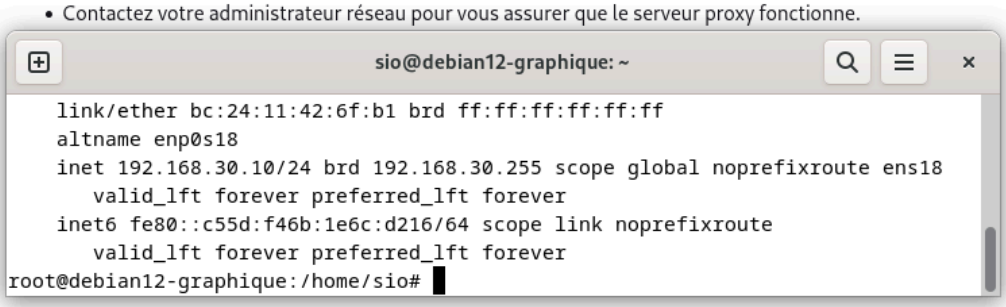
www.tiktok.com

La connexion a été refusée par le serveur proxy

Firefox est configuré pour utiliser un serveur proxy mais celui-ci n'accepte pas les connexions.

Code d'erreur : 403 Forbidden

- Vérifiez que les paramètres du proxy sont corrects ;
- Contactez votre administrateur réseau pour vous assurer que le serveur proxy fonctionne.



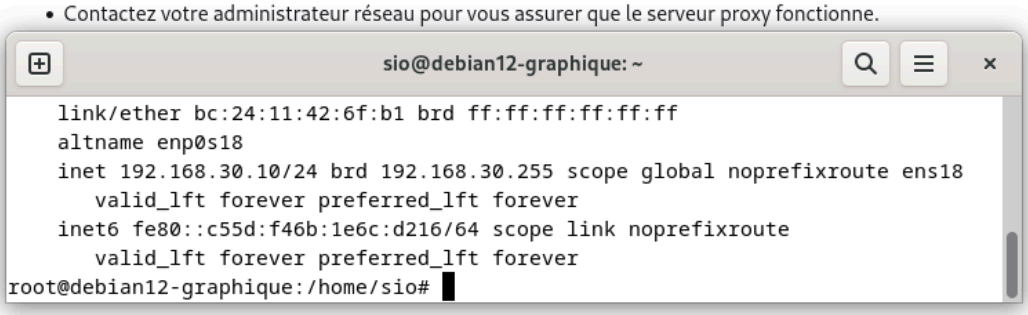
www.facebook.com

La connexion a été refusée par le serveur proxy

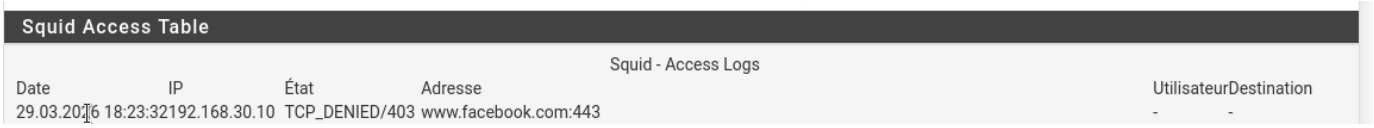
Firefox est configuré pour utiliser un serveur proxy mais celui-ci n'accepte pas les connexions.

Code d'erreur : 403 Forbidden

- Vérifiez que les paramètres du proxy sont corrects ;
- Contactez votre administrateur réseau pour vous assurer que le serveur proxy fonctionne.



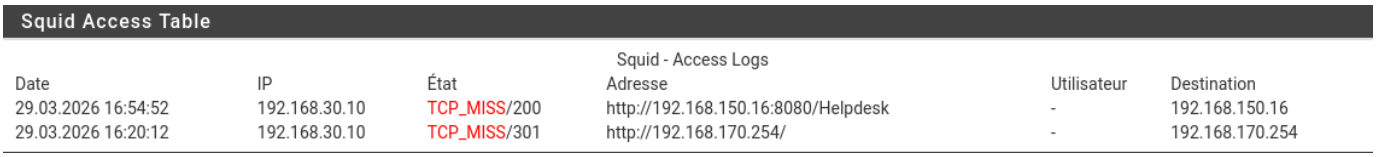
6.4 Les logs



TCP_DENIED = **"Accès refusé"**.

- Le client demande un site
- Le proxy vérifie ses règles de sécurité (ACL).
- Il voit que c'est **interdit** par l'administrateur.
- Il bloque la connexion et renvoie une erreur (souvent `403 Forbidden`).

C'est ce qui arrive quand un site est **filtré** ou si tu n'as pas les bons **identifiants**.



TCP_MISS = **"Pas en stock"**.

- Le client demande un fichier.
- Le proxy regarde dans son cache : **il ne l'a pas**.
- Le proxy va le chercher sur **Internet**.
- Il le donne au client et en garde une copie.

C'est ce qui arrive lors de la **toute première visite** d'un site.

TCP_HIT = **"Déjà en stock"**.

1. Le client demande un fichier (ex: une image).
2. Le proxy regarde dans sa mémoire : **il l'a déjà**.
3. Il la donne **immédiatement** au client.
4. Il n'a **pas besoin** d'aller sur Internet.

7. Scénario 2 et 3 - Restriction horaire/Personnaliser la page d'erreur Squid

➡ Scénario 2 — Mettre en place une restriction horaire

- Dans l'onglet **ACLs**, repérez la section **'Blacklist'** et notez qu'il est possible d'associer un planning (schedule) aux règles.
- Créer un planning **'Heures_Travail'** : `Firewall > Schedules > Add` — Lundi à Vendredi, 08h00 à 18h00.
- Appliquer ce planning à la **blacklist des réseaux sociaux** : les sites ne sont bloqués que pendant les heures de travail.
- Tester en modifiant temporairement les horaires du planning pour simuler un accès hors heures ouvrées.
- Vérifier que l'accès est autorisé en dehors des horaires définis et consulter les journaux pour confirmer.

➖ Scénario 3 — Personnaliser la page d'erreur Squid

- Accéder à la configuration avancée : `Services > Squid Proxy Server > General > onglet Advanced`.
- Dans la section **'Custom Error Pages'**, repérer le champ permettant d'injecter du HTML personnalisé.
- Rédiger une page **HTML simple** indiquant : le nom de l'entreprise (**NetSecure SAS**), la raison du blocage, le contact du responsable informatique et la politique d'utilisation.
- Appliquer la configuration et tester depuis un client en accédant à un site bloqué.
- Vérifier que la **page personnalisée** s'affiche correctement à la place du message d'erreur Squid par défaut.

Cependant avec les indications qui m'ont été données, il n'est pas possible de créer tout ceci.

Pourquoi le HTTPS bloque ta page

C'est une limite mathématique du chiffrement **SSL/TLS**.

- **Le mécanisme :** Quand tu vas sur un site HTTPS, une "poignée de main" (handshake) sécurisée se crée entre ton PC et le serveur (ex: Google). Le Proxy Squid est au milieu, mais il ne possède pas la clé privée de Google.
- **Le blocage :** Quand Squid décide de bloquer le site, il doit envoyer ton code HTML. Mais le navigateur, lui, attend des données chiffrées par Google. Comme le code HTML de ta page `NetSecure SAS` est en texte clair, le navigateur voit que le "paquet" ne correspond pas à ce qu'il attendait.
- **La réaction :** Le navigateur coupe tout et affiche `ERR_CONNECTION_CLOSED` ou `PR_END_OF_FILE_ERROR`. Votre page personnalisée est littéralement jetée à la poubelle par le navigateur pour des raisons de sécurité.

**Sources

- **Documentation officielle Squid :** Dans la section *Features/HTTPS*, il est précisé que sans "SSL Bump" (interception), Squid ne peut pas envoyer de message d'erreur HTTP au client.
- **Forum pfSense :** De nombreux fils de discussion expliquent que "Custom Error Pages do not work for HTTPS sites" (Les pages d'erreur ne marchent pas pour le HTTPS).

Pourquoi l'horaire est "compliqué" sans SquidGuard

Techniquement, **Squid sait gérer le temps**, mais l'interface graphique (GUI) de pfSense/OPNsense est souvent limitée.

- **Squid "Pur" :** Utilise des lignes de commande appelées `acl time`. On peut écrire `acl travail time M T W T F 08:00-18:00`.
- **Le problème du TP :** L'onglet **Blacklist** qu'on utilise dans l'interface graphique est souvent une fonction "simplifiée". Elle applique une liste globale de domaines. Dans 90 % des versions de l'interface pfSense, il n'y a **pas de case à cocher** "Planning" directement dans cet onglet Blacklist.
- **Pourquoi SquidGuard:** SquidGuard a été créé spécifiquement pour ajouter cette interface visuelle de gestion du temps aux listes de blocage.

Sources :

- **Squid Wiki (ACLs) :** La doc sur les *Time-based ACLs* montre que cela se fait par lignes de code (config file), pas par une simple case dans un menu Blacklist.