```
# TP-PROXY.md
```

TP-PROXY Thomas GRZESINSKI

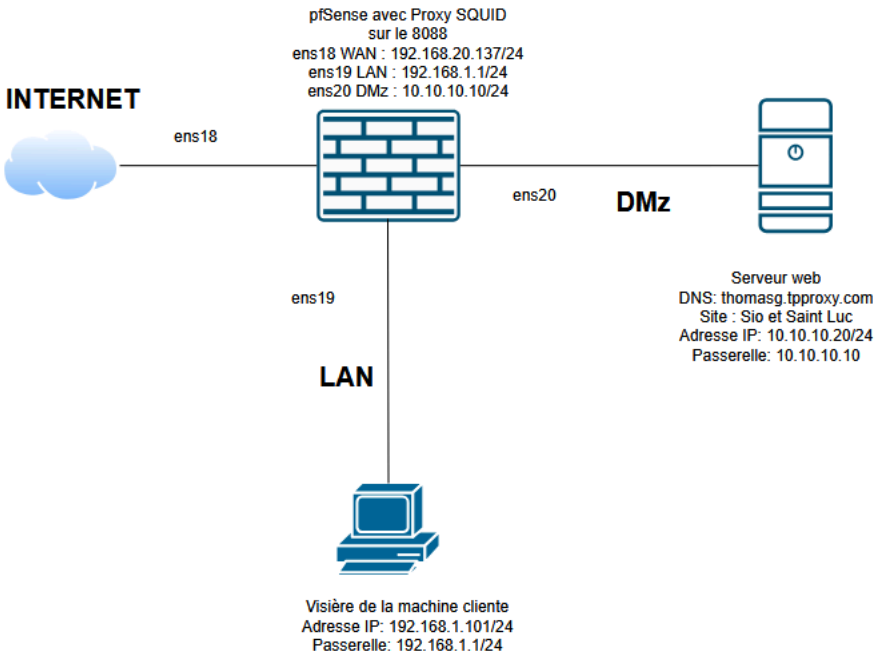
C’est quoi un proxy ?

- Un serveur proxy agit comme un intermédiaire entre un client et un serveur distant. Il permet de filtrer l’accès à certains sites, de mettre en cache les requêtes pour accélérer le chargement des pages, et de compresser les données afin d’optimiser la bande passante. Il assure également la journalisation des requêtes des utilisateurs, renforce l’anonymat en masquant l’adresse IP du client et contrôle les droits d’accès aux ressources. Nous allons donc maintenant utilisé proxy squid sur pfSense

c’est quoi Squid ?

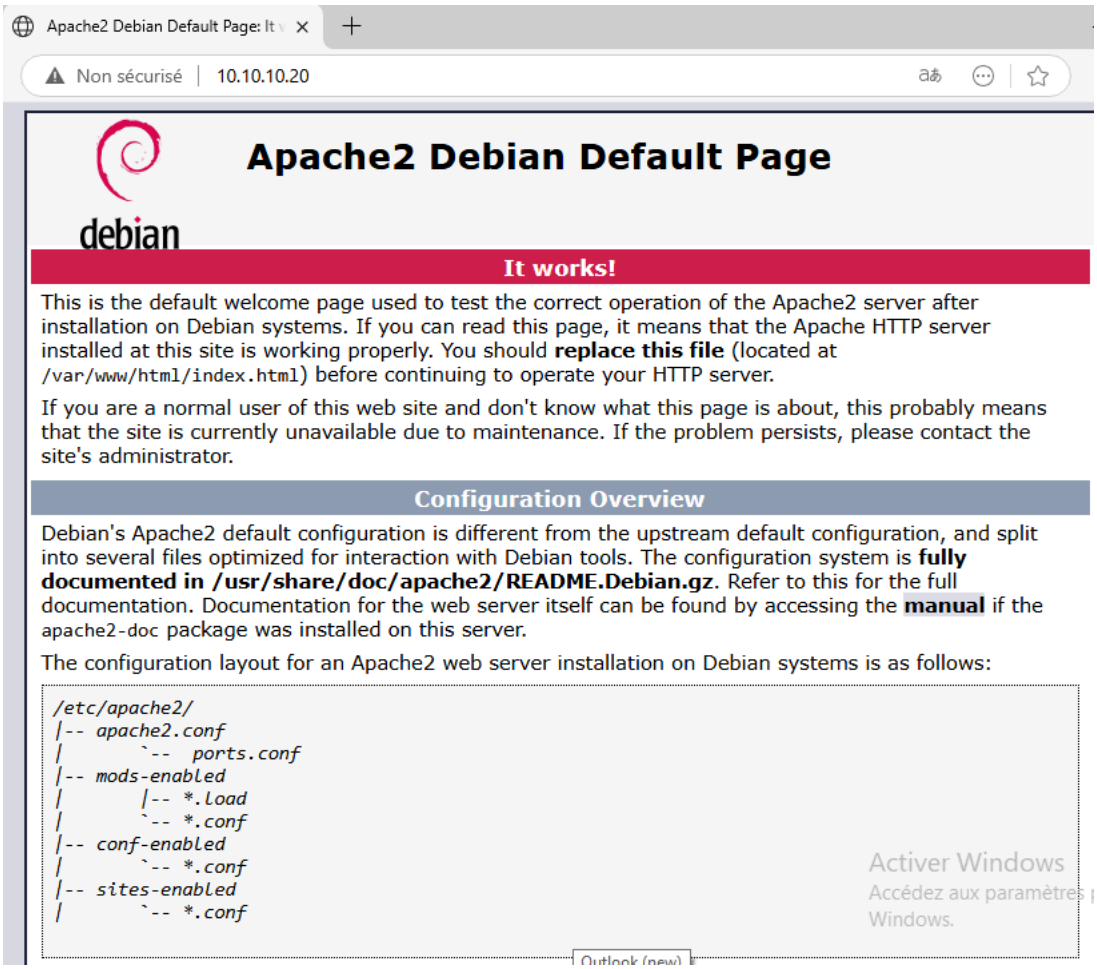
- Squid est un logiciel open-source qui permet de configurer un serveur proxy et un cache web afin d’accélérer la navigation, de sécuriser et de contrôler l’accès à Internet en filtrant les contenus et en optimisant l’utilisation de la bande passante.

Schéma de l’infrasstrucutre

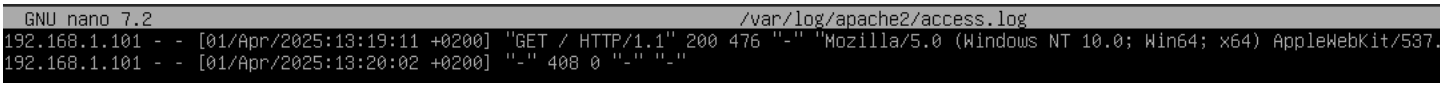


1 Mise en place de l’infrastrucutre web

- Tuto de la mise en place du pfSense sur mon portfolio : https://thomas-portfolio.fr/TP-pfSense.pdf
- Vérification que le client accède au serveur web :



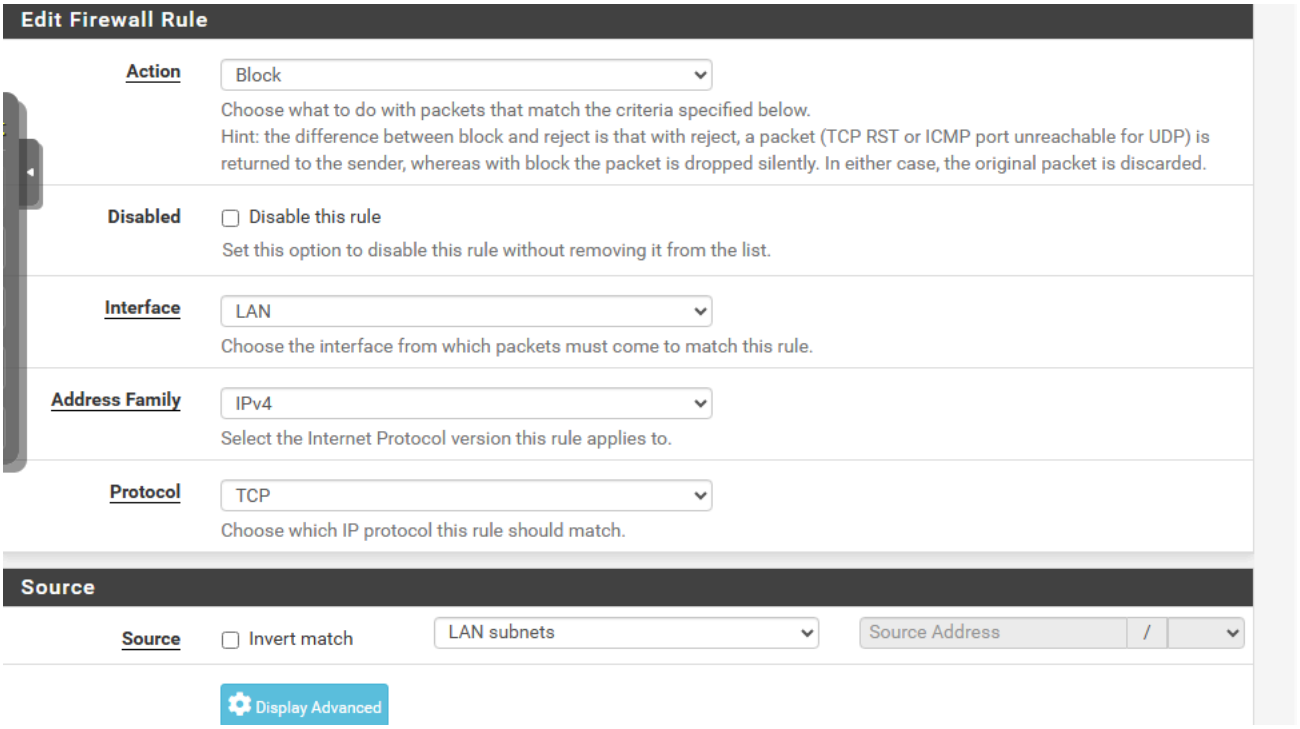
- Pour vérifié qui consulte notre serveur web, nous pouvons directement aller sur le serveur web et aller dans le fichier var/log/apache2/access.log

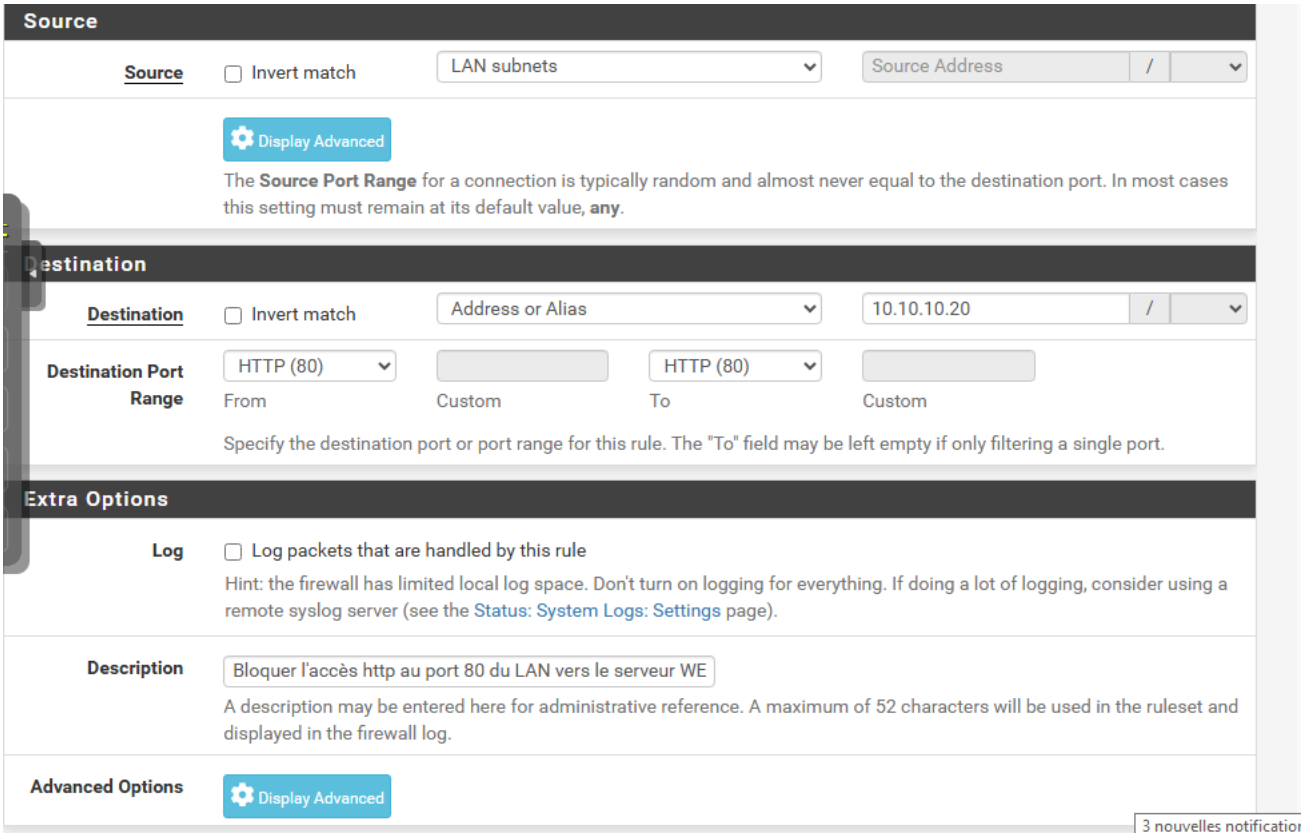


- On peut constater que notre machine windows cliente avec comme adresse IP 192.168.1.101 à bien consulté notre serveur web

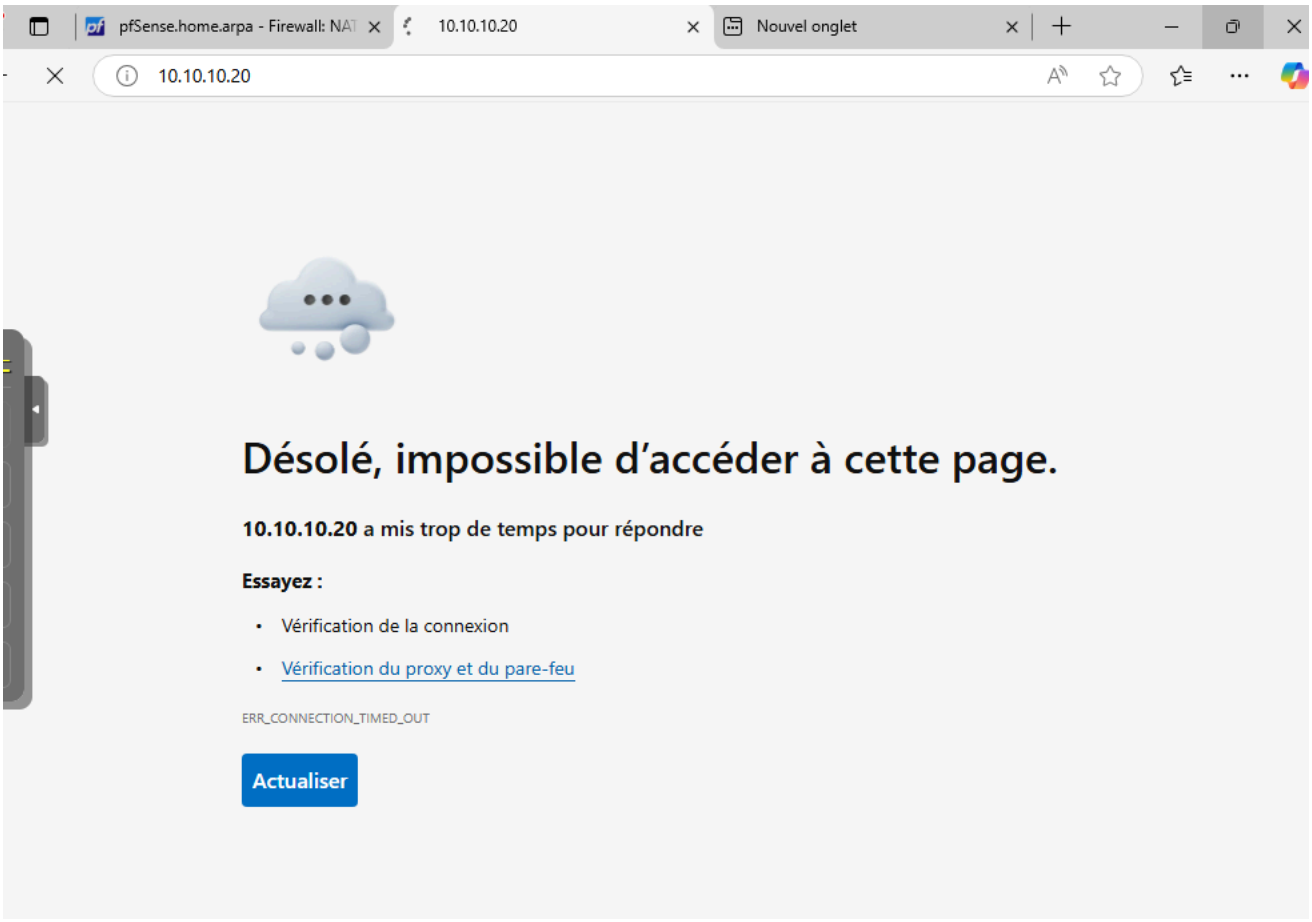
2 Refuser l’accès direct au web

- On voudrait que les requêtes sur le port 80 soit refusé
- Sur pfSense ajouter donc cette règle pour le LAN :





- Explication de la règle : Cette règle configurée sur l'interface LAN en mode « Block » pour le protocole TCP (IPv4), empêche toute machine du réseau local (LAN subnets) d'accéder à l'adresse 10.10.10.20 sur le port HTTP (80), bloquant ainsi la navigation web vers ce serveur depuis le LAN.
- vérification :



3 Finalisation de l'environnement web

- Nous allons maintenant mettre en place sur notre serveur web un service DNS pour facilité l'accés à nos SIo et Saint Luc
- Il vous faudra donc d'abord installer bind 9 sur votre serveur web
- C'est quoi bind9 ?
    - BIND 9 (Berkeley Internet Name Domain, version 9) est un logiciel de serveur DNS (Domain Name System) largement utilisé sur Linux. Il permet de traduire des noms de domaine en adresses IP et vice versa, jouant ainsi un rôle essentiel dans la résolution de noms sur Internet et les réseaux.
- Configuration de l'installation :
    - apt update && upgrade
    - apt-get install bind9 bind9utils bind9-doc
- Nous pouvons donc maintenant mettre en place notre DNS
- Il vous faudra modifier le fichier hostname devotre machine nano/etc/hostname pour changé le nom d'hôte de la machine, ce qui est essentiel pour l'identification de la machine du système sur le réseau, facilite la geestion des services et la lecture des lofs, et contribue à une meilleure origanisation de l'infrastructure. Je vais donc la nommé pour moi Thomasg.tpproxy.com

```
 GNU nano 7.2                                                /etc/hostname *
Thomasg.tpproxy.com_
```

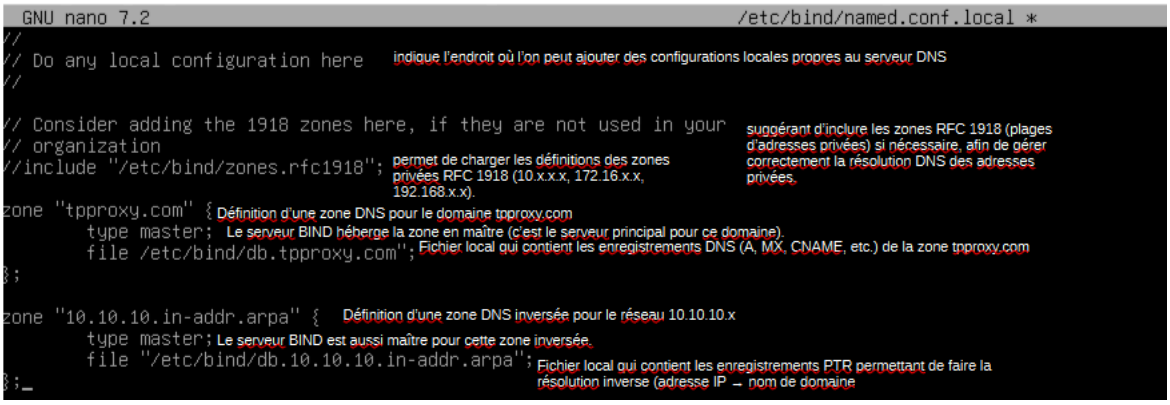
- Ensuite on associe l'ip de notre machine a notre DNS dans le fichier nano /etc/hosts

```
 GNU nano 7.2                                                  /etc/hosts *
127.0.0.1       localhost
127.0.1.1       ThomasG.tpproxy.com
10.10.10.20 ThomasG.tpproxy.com
```

- Enfin on associe le domaine et la zone de recherche DNS pour intégré la zone DNS dans le fichier /etc/resolv.conf

```
 GNU nano 7.2                                              /etc/resolv.conf *
domain sio.local
search sio.local
nameserver 185.156.80.7
nameserver 10.10.10.20
```

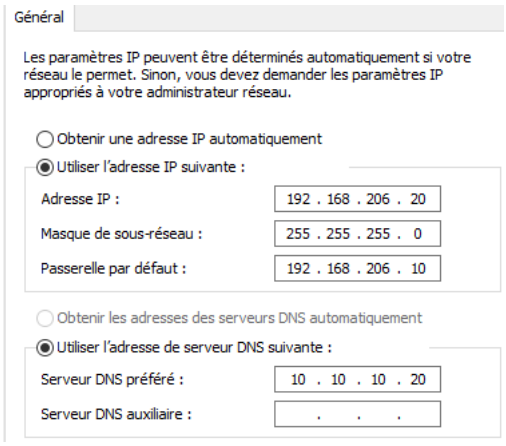
- Maintenant on doit déclarer notre zone DNS et sa zone inverse dans le fichier /etc/bind/named.conf.local * ce fichier sert à déclarer les zones DNS que le serveur BIND va gérer (zones directes et inversées), ainsi que des inclusions éventuelles pour d'autres configurations (comme les zones privées RFC 1918).



- Maintenant on doit donc créer la zone pour tpproxy.com et pour 10.10.10.in-addr.arpa
- Créer un fichier /etc/bind/db.tpproxy.com (pour mon cas il faudra adapter pour vous). Ce fichier de zone DNS contient tous les enregistrements DNS (tels que les enregistrements A, MX, NS, etc.) qui définissent comment les noms de ce domaine se traduisent en adresses IP et autres informations nécessaires. En d'autres termes, c'est lui qui dit à BIND comment répondre aux requêtes DNS pour tpproxy.com.

- Créer un fichier /etc/bind/db.10.10.10.in-addr.arpa . Ce fichier sert à la gestion de la zone DNS inversée pour le réseau 10.10.10.x. Il contient les enregistrements PTR qui permettent de résoudre, à partir d'une adresse IP, le nom de domaine associé. En d'autres termes, il facilite la résolution inverse, indispensable pour certains services et pour la vérification de l'authenticité des adresses sur le réseau.

- Créer un fichier index.html et un fichier index2.html pour avoir accès à nos différents sites
- Vérification de votre DNS :
- Sur votre machine cliente, accédez aux paramètres de votre carte réseau et configurez l'adresse IP de votre serveur web, qui joue également le rôle de serveur DNS.



- Faites un ping sur l'adresse IP et sur le nom de domaine et vous observerez une réponse

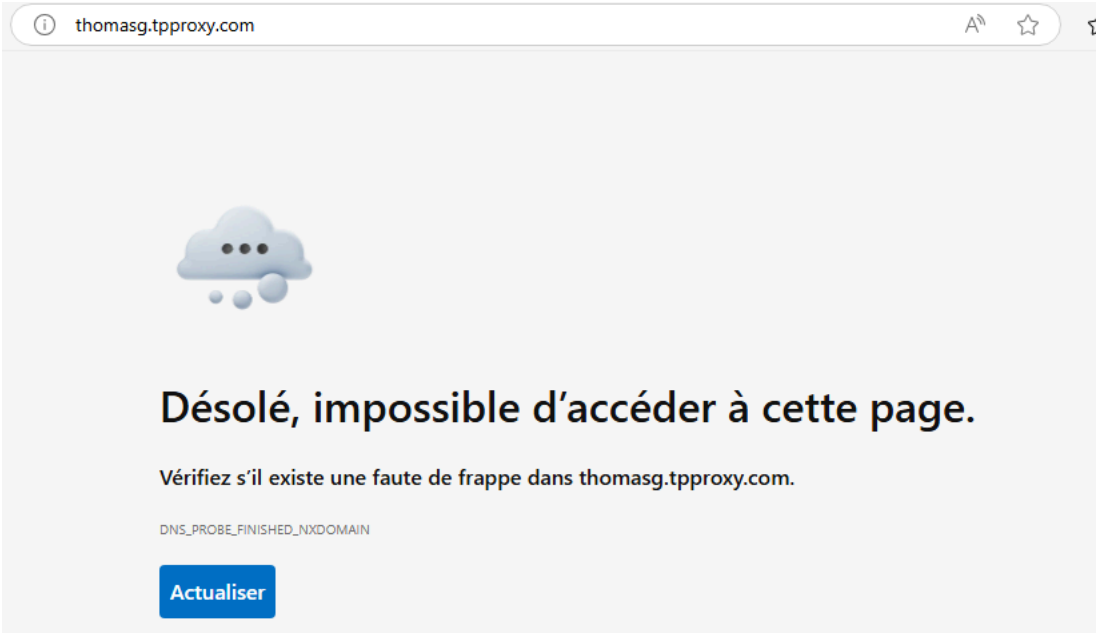
```
C:\Users\sio>ping 10.10.10.20

Envoi d'une requête 'Ping'  10.10.10.20 avec 32 octets de données :
Réponse de 10.10.10.20 : octets=32 temps=3 ms TTL=63
Réponse de 10.10.10.20 : octets=32 temps=2 ms TTL=63
Réponse de 10.10.10.20 : octets=32 temps=3 ms TTL=63
Réponse de 10.10.10.20 : octets=32 temps=2 ms TTL=63

Statistiques Ping pour 10.10.10.20:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms
```

```
C:\Users\sio>ping Thomasg.tpproxy.com

Envoi d'une requête 'ping' sur ThomasG.tpproxy.com [10.10.10.20] avec 32 octets de données :
Réponse de 10.10.10.20 : octets=32 temps=2 ms TTL=63
Réponse de 10.10.10.20 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.20 : octets=32 temps=2 ms TTL=63
Réponse de 10.10.10.20 : octets=32 temps=2 ms TTL=63

Statistiques Ping pour 10.10.10.20:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

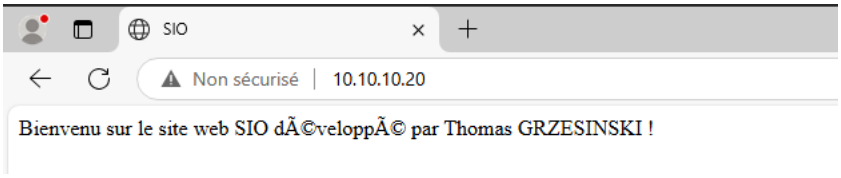
- Vous pouvez aussi faire un nslookup pour vérifier que le DNS fonctionne correctement mais aussi s'assuré que le serveur est joignable

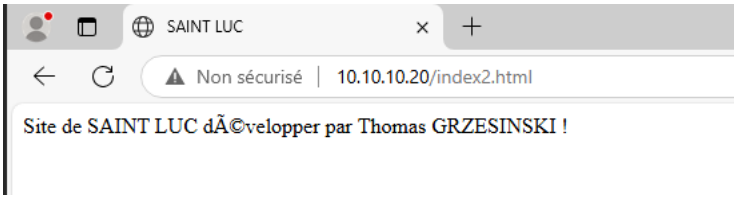
```
C:\Users\sio>nslookup Thomasg.tpproxy.com
Serveur :   UnKnown
Address:  10.10.10.20

Nom :    ThomasG.tpproxy.com
Addresses:  10.10.10.20
          192.168.1.20
```

- Parcontre nous ne pourrons pas aller sur notre site internet direcement avec lez DNS car notre proxy n'est pas configuré, et la règle sur le port 80 bloque l'accès



- Désactivez temporairement la règle qui bloque le port 80 le temps de voir si votre site web avec les fichiers sont bien opérationnelles :

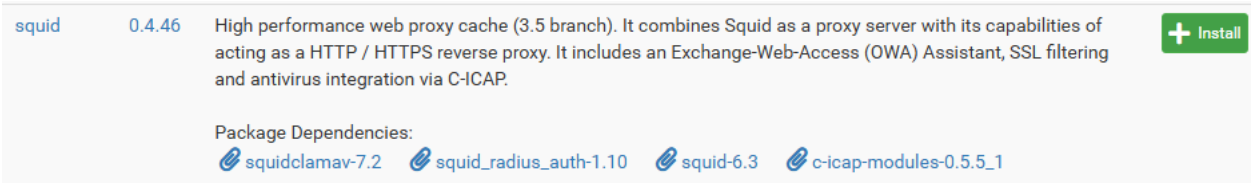




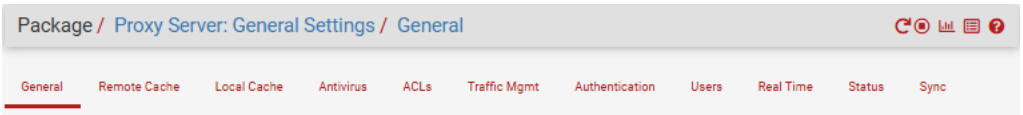
- Réactiver ensuite la règle

4 Installation de SQUID

- Nous allons donc maintenant installé notre proxy squid sur pfSense
- Sur pfSense aller dans System -> Package Manager -> Available Packages -> Recherché “Squid” et installé le



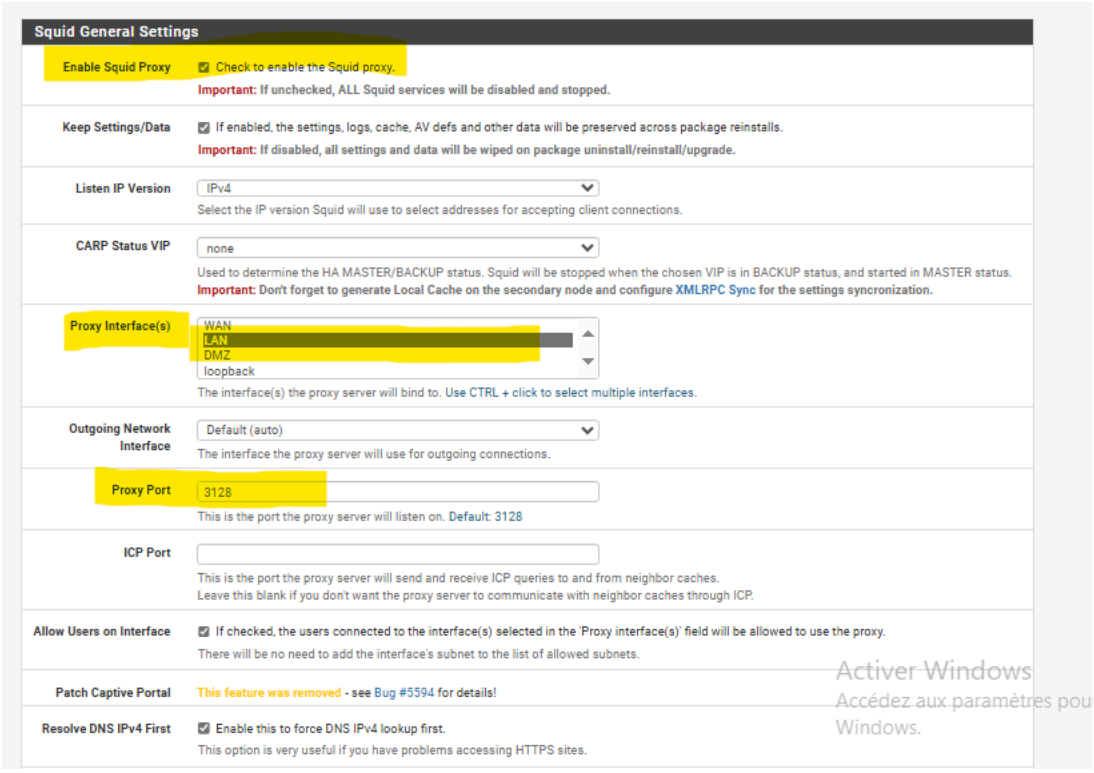
- Une fois que Squid est installé aller dans Services -> Squid Proxy Server
- Vous pouvez observez que de nombreuses options permettant la configuration du proxy server existent :



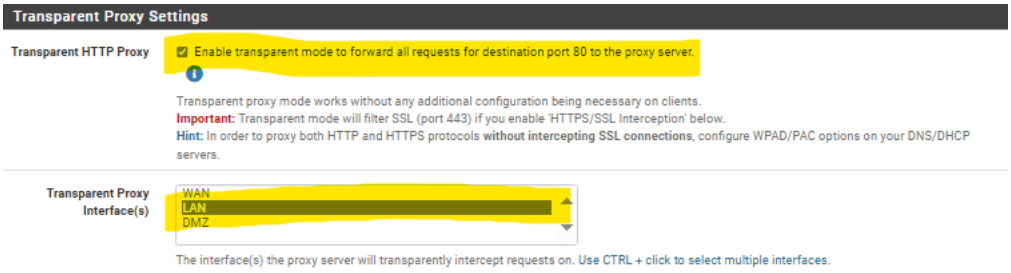
- Nous allons maintenant configuré notre proxy server afin qu’il puisse être fonctionnel

4.2 Confiugration de SQUID

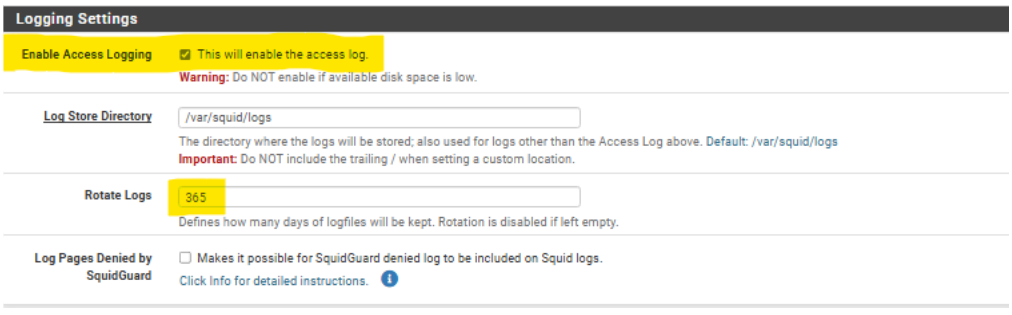
- Aller dans général, activé SQUID, précisé que nous voulons le proxy sur l’interface LAN et vérifier que le proxy écoute bien sur le port 3128 qui est le port par défaut de squid



- Ensuite vous devez cochez “Transparent HTTP Proxy”, pour activer le mode transparent pour le protocole HTTP (Le mode transparent pour le protocole HTTP, souvent utilisé avec un proxy transparent, permet d’intercepter et de rediriger automatiquement le trafic HTTP (port 80) sans que les clients aient besoin de configurer manuellement un proxy dans leur navigateur.)



- Coché ensuite :
  - Enable Access Logging : cochez l’option pour activer les journaux, ce qui va permettre de savoir qui fait quoi sur Internet.
  - Rotate Logs : pendant combien de jours souhaitez-vous conserver les logs ? Pour les établissements scolaires, c’est pendant 365 jours qu’il faut conserver les logs



- Vous pouvez ensuite cochez la case ” Suppress Squid Version” pour masquer la version de squid

- La configuration a été effectué à l’aide du tuto de IT Connect : https://www.it-connect.fr/proxy-transparent-mise-en-place-de-squid-sur-pfsense/

5 Mise en place du serveur proxy

- Avec la mise en place du proxy le client n’a pas accès au DNS du serveur web il va donc falloir le configuré pour autorisé son trafic
- Modifier tout d’abord le port 3128 du proxy en 8088 afin d’améliorer la sécurité de votre serveur et d’éviter les conflits avec d’autres services et de contourner d’éventuelles restrictions réseau

- Pour faire ceci aller dans General de votre Proxy server et modifier le proxy port

- Une fois ceci fais vous pouvez configuré votre client windows
- Sur votre machine cliente aller dans Paramètres -> Réseau et Internet -> Proxy
- Il vous faudra mettre en place l'adresse de votre proxy ici ce sera donc 192.168.1.1 comme nous sommes dans le LAN et donc le port 8088 pour intercepter les bonnes requêtes

- Mais quand vous allez entrez l'adresse IP ou le nom de domaine sur internet vous nepourrez toujours pas y accéder et c'est normal car nous n'avons pas configuré nos ACL

Une ACL c'est quoi ?

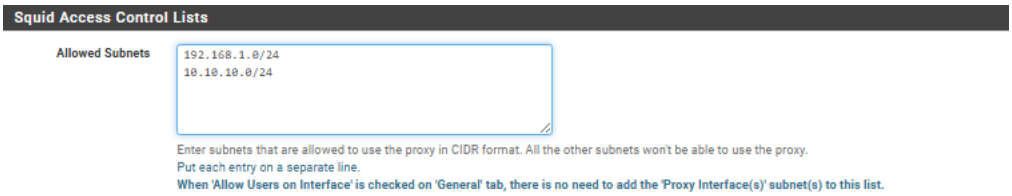
- Une CL (ou ACL - Access Control List) est une liste de contrôle d'accès utilisée pour définir des règles de filtrage et de restriction dans un système informatique, notamment dans un proxy comme Squid.
- Les ACLs permettent de :
  - Autoriser ou bloquer l'accès à certains sites web ou adresses IP.
  - Restreindre l'accès à Internet pour certains utilisateurs ou plages d'IP.
  - Définir des règles spécifiques (ex : bloquer les téléchargements, autoriser certains horaires, etc.).
- Sur pfSense le proxy SQUID propose directement en interface graphique les ACLs ce qui permet de simplifié la mise en place et la compréhension
- Pour la gestion des ACLs aller dans l'onglet "ACLs" dans le proxy et vous pouvez observer différente option possible
- Allowed Subnets qui permet de définir les plages d'adresses IP qui sont autorisées à accéder au proxy. Seules les machines appartenant à ces sous-réseaux pourront utiliser le proxy.
- Unrestricted IPs : Liste d'adresses IP qui ne sont soumises à aucune restriction. Ces IPs peuvent accéder à tout sans être affectées par les règles de filtrage.
- Banned Hosts Address : contient les adresses IP ou noms d'hôtes interdits d'accès. Toute requête provenant de ces adresses sera bloquée.
- Whitelist qui permet : liste d'adresses IP, de sites web ou de domaines toujours autorisés, même si d'autres règles de filtrage les bloqueraient normalement.
- Blacklist qui permet : liste de sites web ou de domaines interdits. Tout trafic vers ces adresses est bloqué.
- Block user Agents qui permet : empêche l'accès à certaines requêtes en fonction du User-Agent (exemple : empêcher l'accès aux navigateurs obsolètes ou à certains bots).
- Block MME Types (Reply Only) : Interdit le téléchargement de fichiers en fonction de leur type MIME (ex : bloquer les fichiers .exe, .mp3, .mp4, etc.)

ACl SafePorts : Liste des ports autorisés pour les connexions HTTP classiques

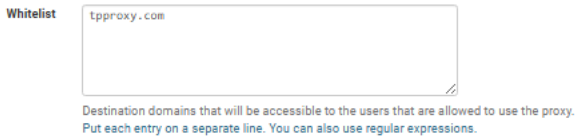
ACl SSLPorts : Liste des ports autorisés pour le trafic HTTPS (chiffré)

5.2 Configuration des ACLS

- Nous allons donc maintenant configurer 2 ACLs afin d'autoriser le DNS et l'adresse IP du serveur WEB
- Dans Allowed subnets on va donc autorisé le réseau de notre LAN et de la DMZ à être communiqué donc :

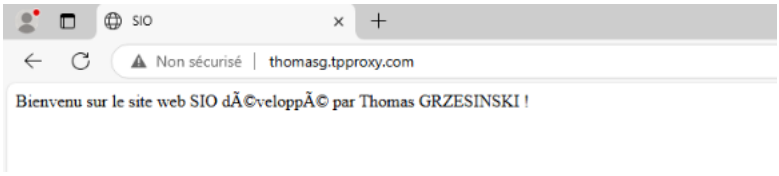


- Dans Whitelist on va donc configuré et autorisé notre domaine tpproxy.com :

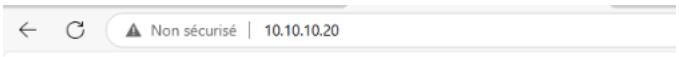


5.2 Vérification , Wireshark et logs

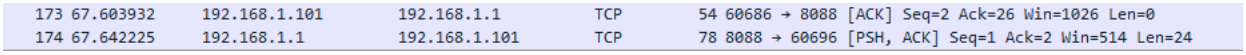
- Maintenant avec votre client configuré sur le proxy vous pouvez tenté d'accéder au DNS de votre serveur web mais aussi le faire directement avec son adresse IP :
- DNS :



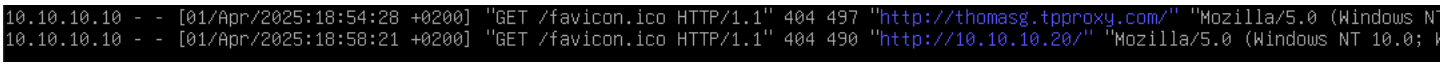
- Adresse IP :



- Vérification avec une capture de la trame de wireshark :

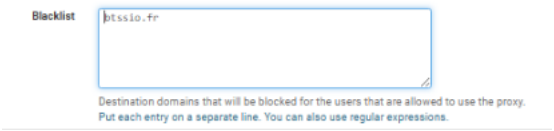


- Expliation des trames :
- Trame 173 :
  - Le client 192.168.1.101 envoie un paquet ACK au proxy 192.168.1.1 sur le port 8088. Dans ce paquet, le client accuse réception d'un segment de 26 octets envoyé précédemment par le proxy. Il utilise le port source 60686, qui est un port éphémère attribué dynamiquement par le système. Le client ne transmet pas de données dans ce paquet (longueur = 0), il signale simplement qu'il attend la suite de la communication.
- Trame 174 :
  - Le proxy 192.168.1.1 répond au client 192.168.1.101 avec un paquet PSH, ACK en provenance du port 8088 et à destination du port 60696 (port éphémère du client).Ce paquet contient 24 octets de données et utilise le drapeau PSH (Push), indiquant que ces données doivent être traitées immédiatement par le client. L'accusé de réception ACK signifie que le proxy a bien reçu le dernier message du client.
- Sur le serveur web dans le fichier nano /var/log/apache2/access.log on peut observer que le proxy a pris l'adresse DMZ du serveur proxy et indique bien la communication sur le DNS et l'adresse IP :

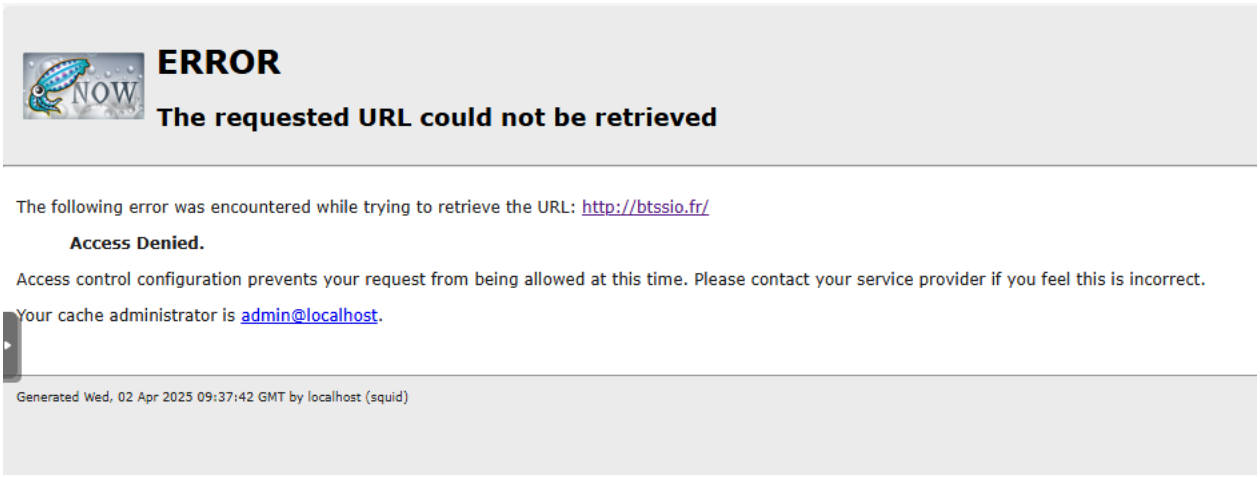


5.3 Bloqué un site internet

- Dans Blacklist vous pouvez entrer un domaine d'un site interet



- Vérification avec le client :



- Le message indique bien que l'accès au site web est refusé