TP – Proxy

A quoi sert Proxy Squid

- Proxy Squid permet de :

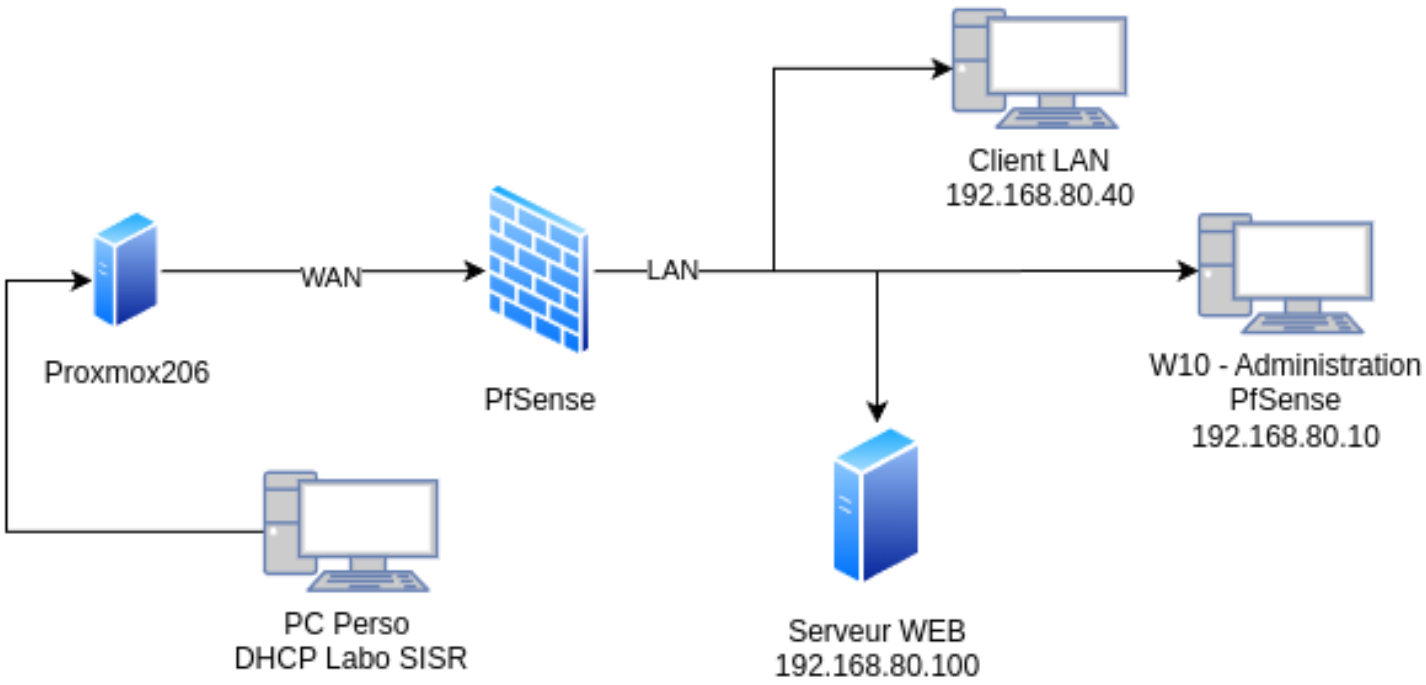
  - Filtrer les accès et bloquer certains sites ou catégories de site grâce à des **A**ccess **C**ontrol **L**ists (ACL) .

  - Intercepter le trafic HTTP/HTTPS avec le mode proxy transparent sans de configuration manuelle sur les postes clients.

  - Surveille et journalise les requête web en temps réel et génère des journaux détaillés afin d'analyser le trafic réseau.

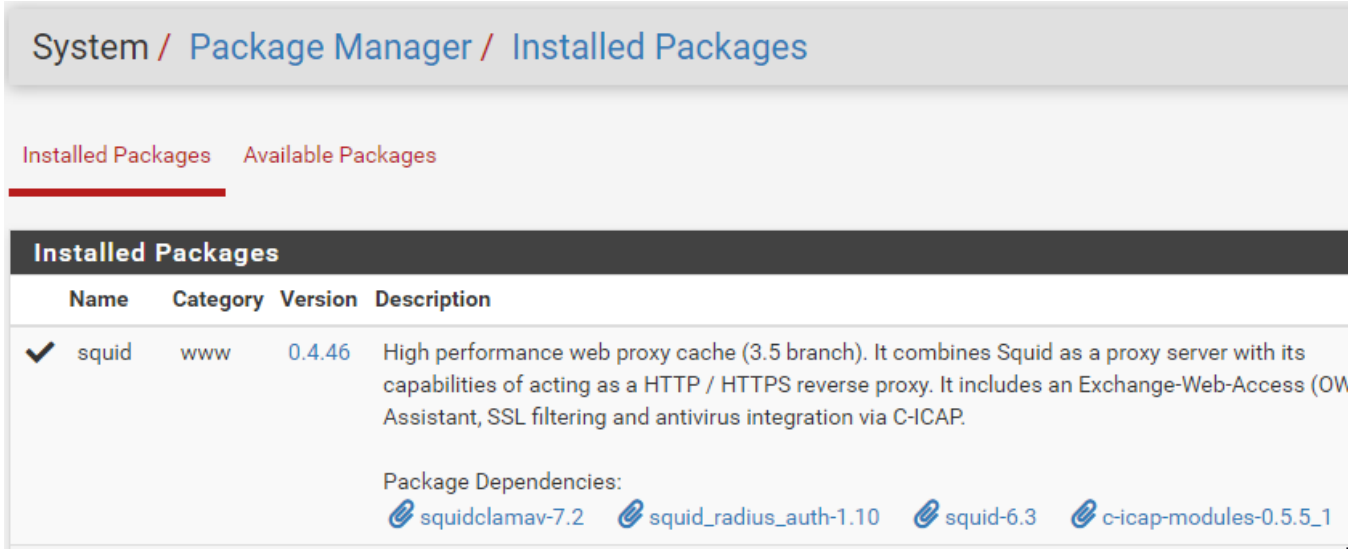
  - Contrôle d'accès avancé avec la possibilité de restreindre l'accès à internet selon des plages horaires, groupes d'utilisateurs ou adresses IP spécifiques, cela peut être utile pour encadré l'accès des employés.

Présentation de l'infrastructure



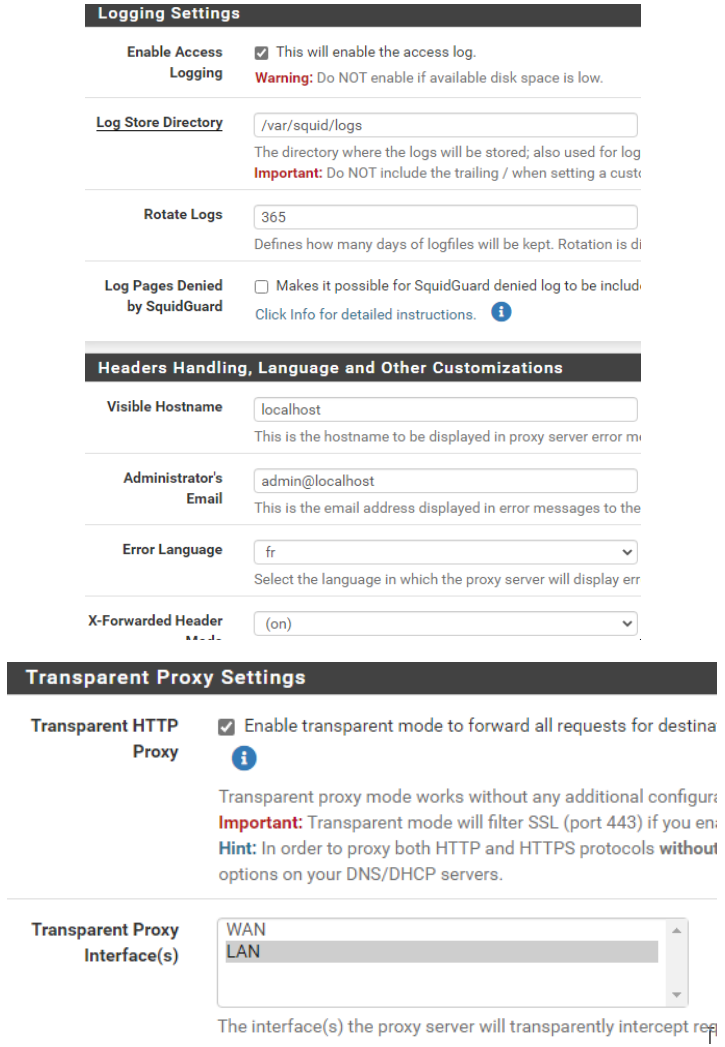
Installation de Proxy Squid

- Dans notre serveur PfSense en accès web, nous nous rendons dans **Système > Package Manager**, puis nous installons squid.
- Rendez vous dans l'onglet Services du PfSense pour la configuration de squid.
- Installation et configuration de PfSense : https://baptiste-mathius.github.io/img/BTS2/TP-B2-Pfsense.pdf



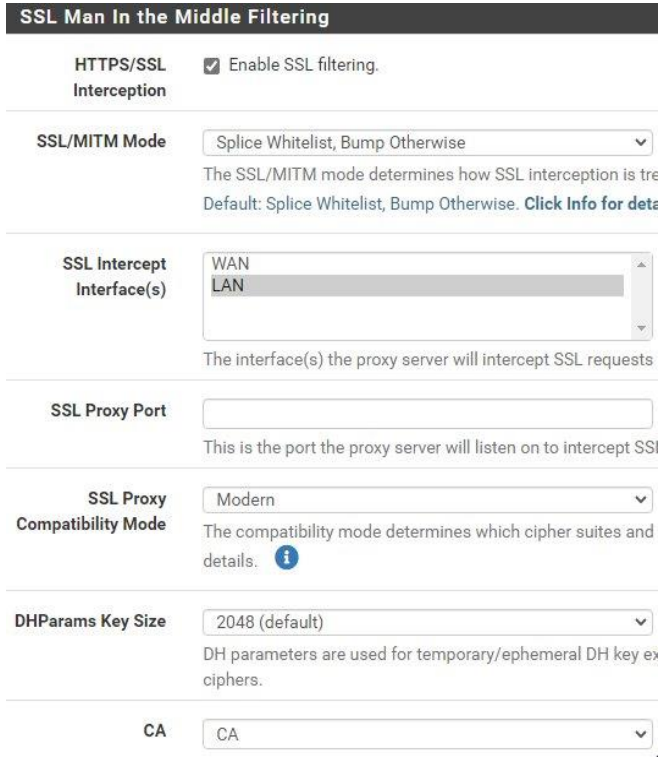
Configuration de Proxy Squid

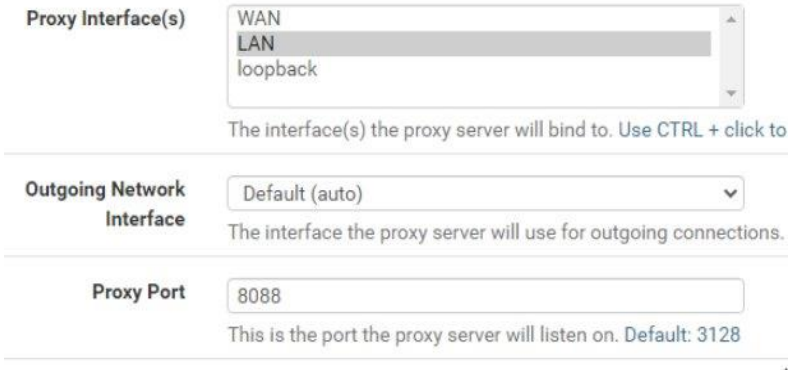
- Pour la configuration, nous nous rendons dans l'onglet **Service > Squid proxy server > general**.
- On coche enable squid proxy afin de démarrer le service.
- On coche également **enable access logging**, pour avoir un retour sur les logs dans le but d'analyser la suite de nos règles que nous allons mettre en place.



Configuration de Proxy Squid

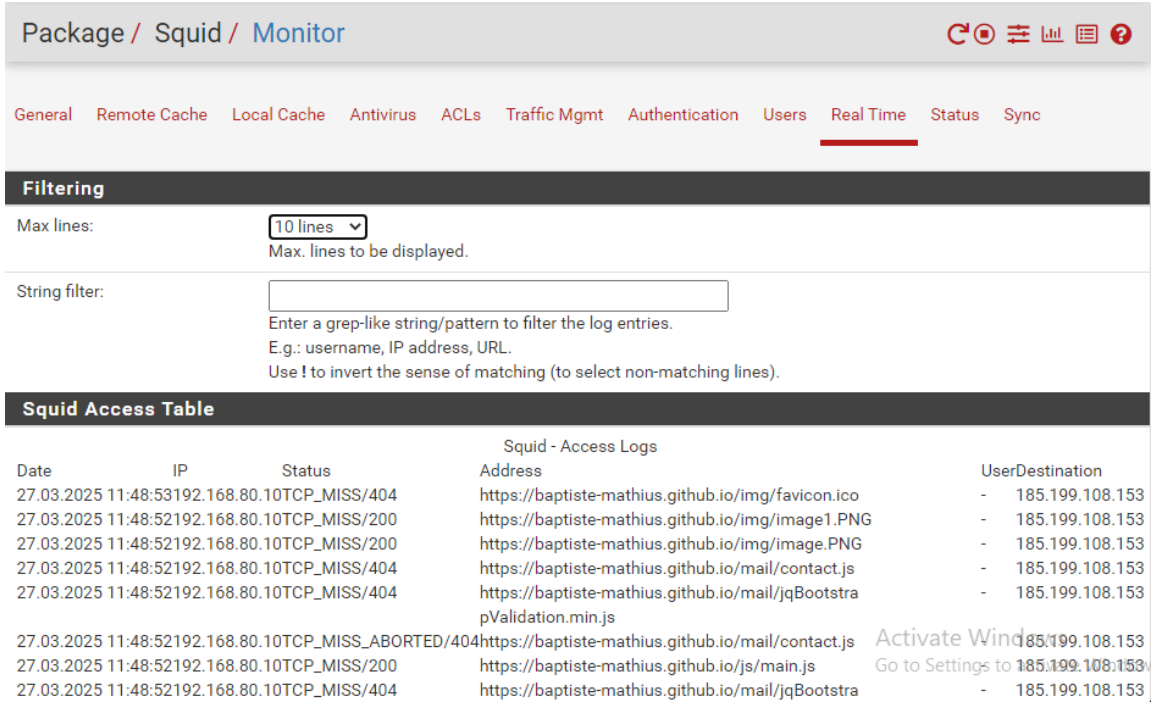
- Nous choisissons l'interface **LAN** pour le proxy puis les écoutes d'IP en IPv4 et nous mettons le **port 8088**.
- On active l'option HTTPS/SSL interception et nous ajoutons notre Certificat Autosigné sinon le service ne démarrera pas.
- On valide notre configuration en cliquant sur **save.**





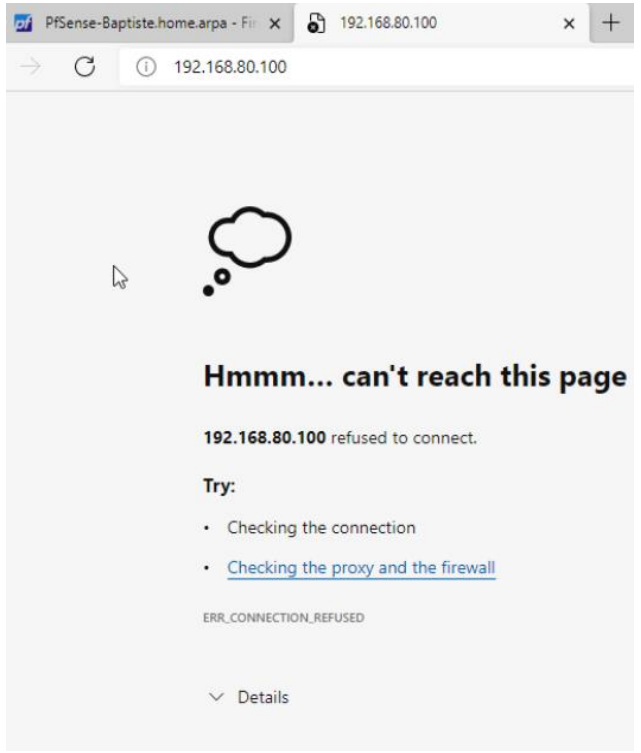
Test du Proxy

- Ensuite nous allons consulter différents sites comme un Web héberger sur une VM avec un apache et mon portfolio.
- Nous pouvons voir que l'adresse de mon portfolio remonte, notre Proxy est donc actif.
- Passons maintenant à la suite avec la sécurisation.



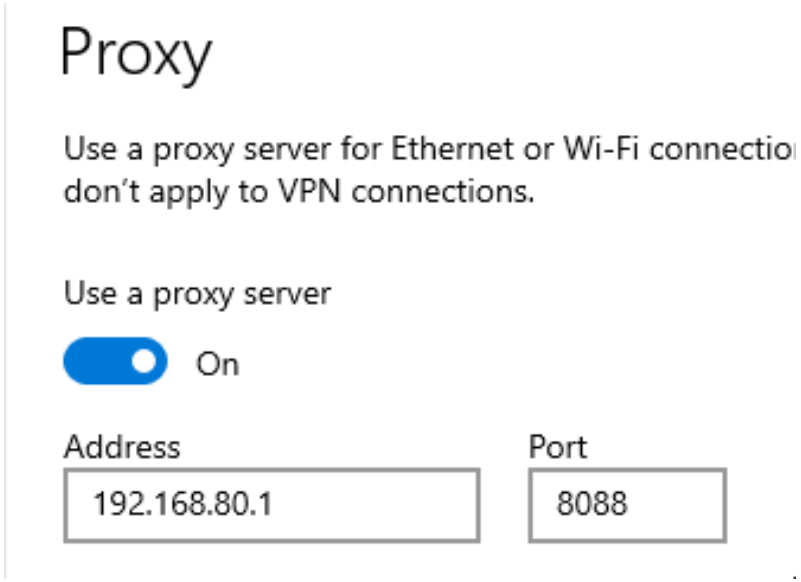
Blocage du Port 80

- On ajoute cette règle dans l'onglet Firewall / Rules / LAN, pour bloquer le port 80.
- Puis on test sur notre navigateur, nous voyons que la page est inaccessible.

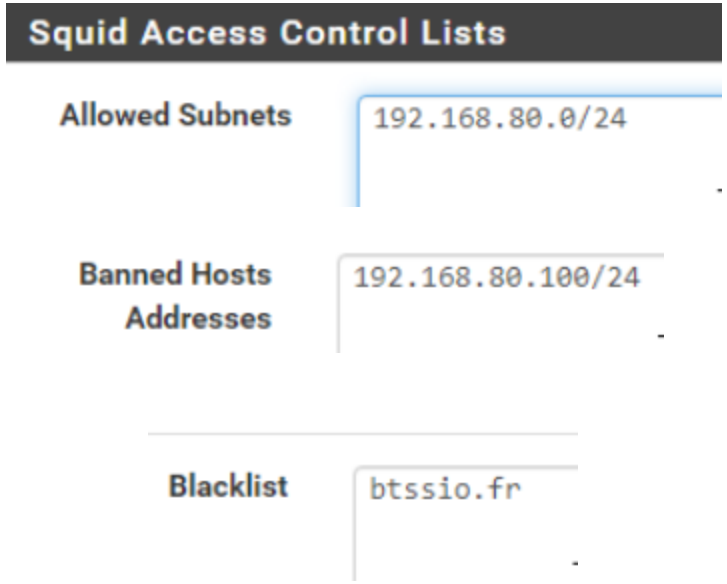


Redirection du client vers le proxy

- Nous allons maintenant rediriger notre machine cliente directement sur notre proxy.
- Il faut donc se rendre dans **settings, network & internet** puis on ajoute le proxy.



Restriction sur le proxy

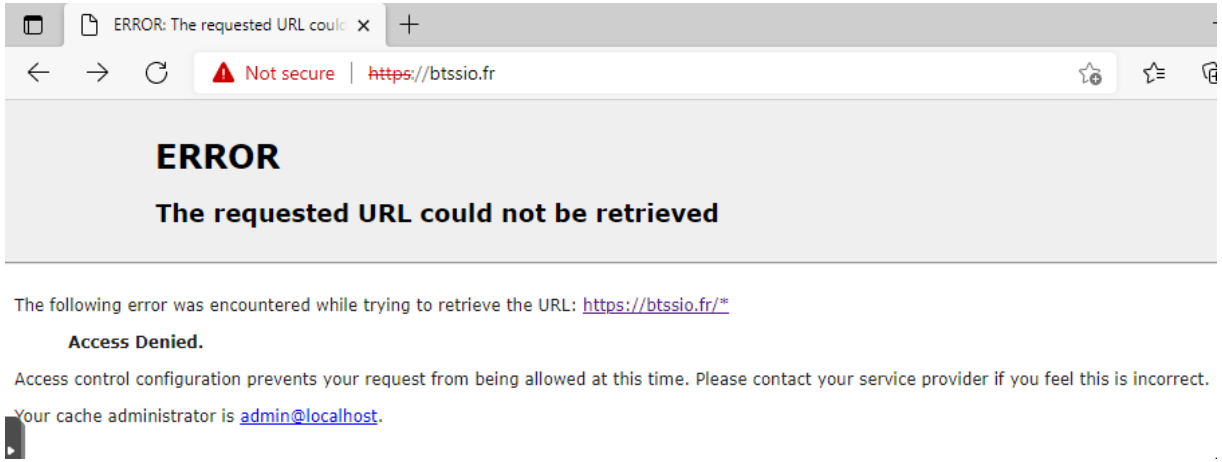


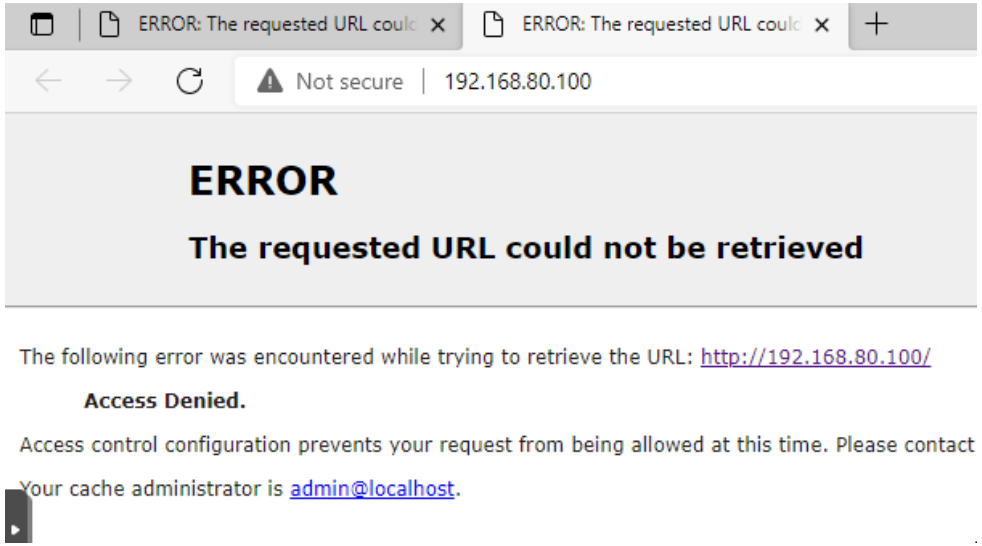
- Avec Proxy Squid, nous avons plusieurs possibilités :
- Nous allons donc autoriser nos adresses LAN et nous allons blacklist le moodle et notre serveur Web.
- Pour cela on se rend dans **Services -> Squid Proxy Server -> ACLs**

Allow subnets	adresses autorisées sur le proxy
Unrestricted IPs	accès non restreints
Banned hots addresses	bannir des adresses
Whitelist	liste blanche des IP/sites web consultables
Blacklist	liste noire des IP/Sites non consultables

Test et vérifications

- Passons sur notre client LAN et testons cela :





Analyse des logs proxy

- Dans le Real Time, nous voyons les log d'accès Squid, avec les status et les adresses consultées.
- Tout ce qui est consulté et qui n'est pas du réseau 192.168.80.0 ne peut pas être consulté.
- Nous pouvons voir que notre serveur web est blacklist donc il est inaccessible