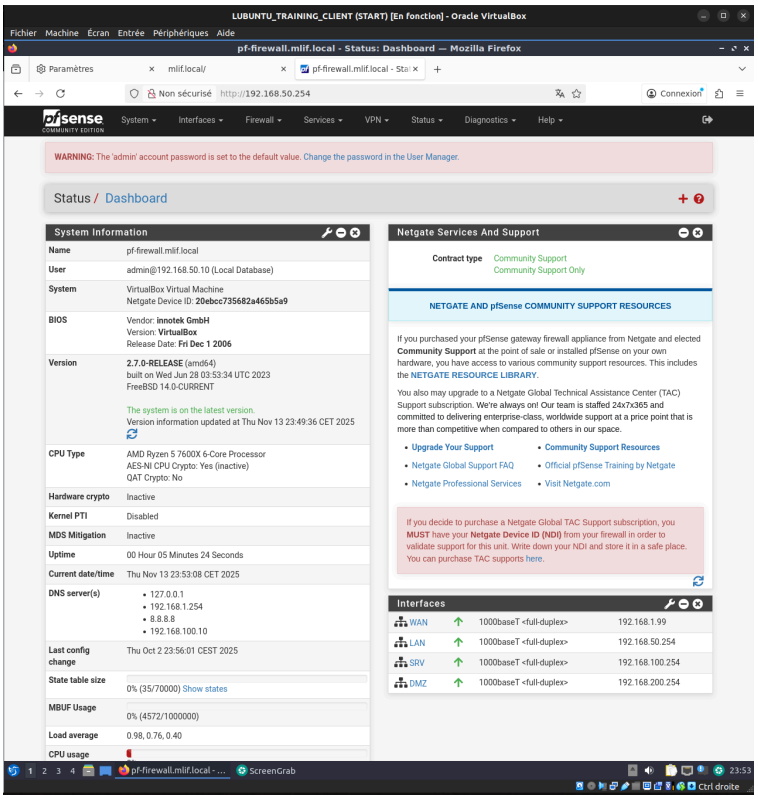
LAB3-B3-UTM (squid)

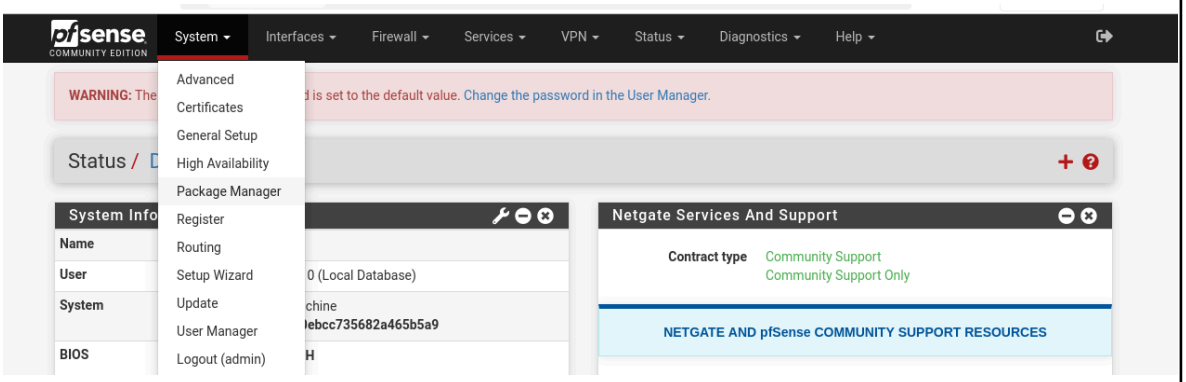
On commence par lancer les 3 machine nécessaire à la réalisation du tp :

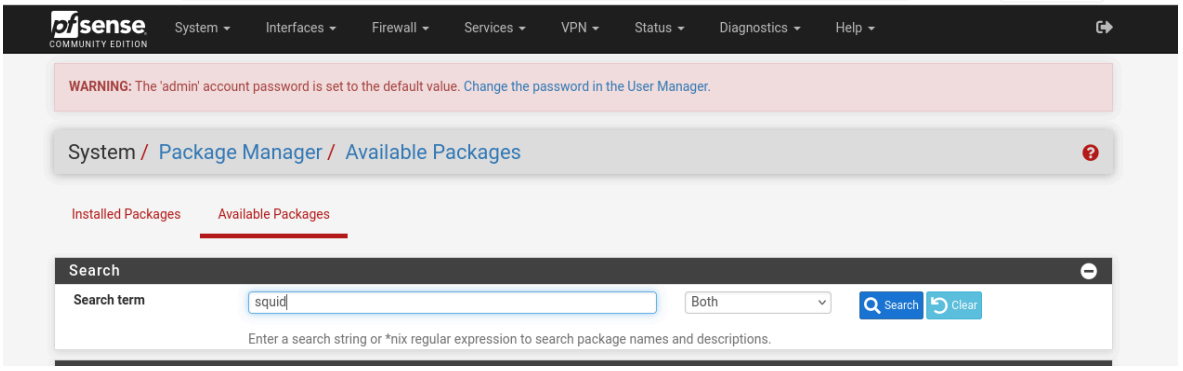
3.1°) Installation des packages squid et squidguard

On vas maintenant procéder à l'installation des paquet squid et squidguard, pour cela il faut se rendre sur la DEBIAN_TRAINING_CLIENT, puis se connecter à la page de configuration du pare-feu :

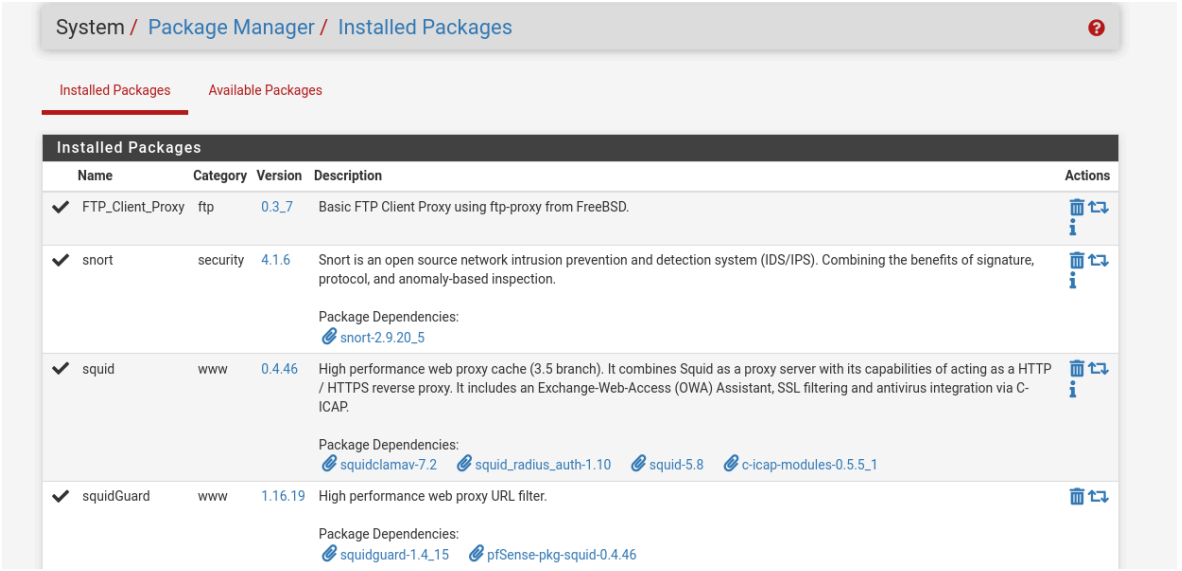


Une fois connecter se rendre dans **System Package** > **Manager Available Package > rechercher “squid”**

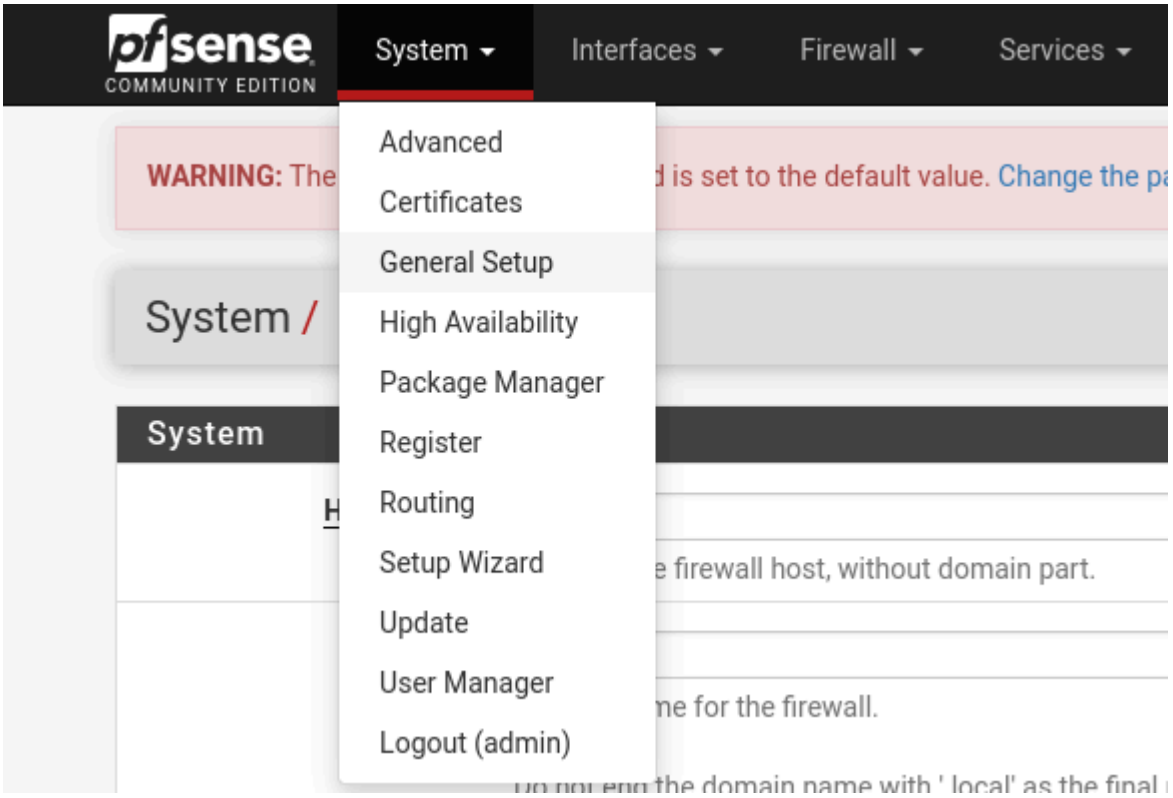




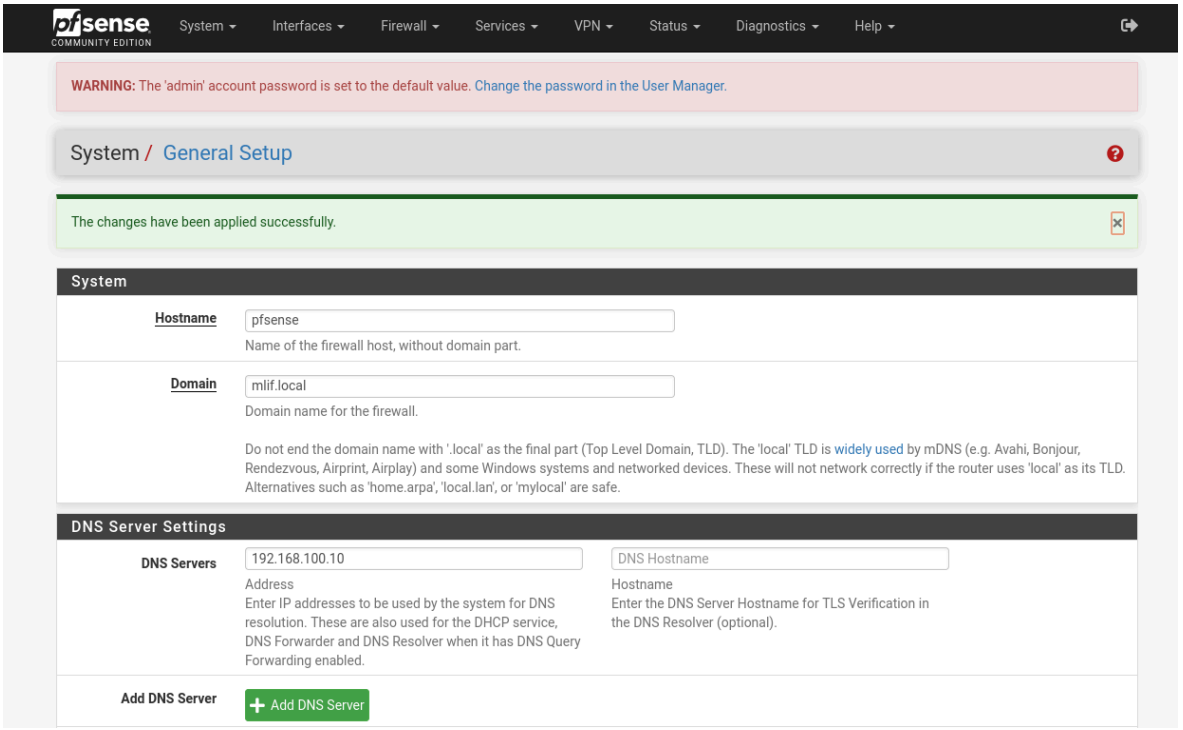
Une fois que je clique sur installer, je me rend sur la page “ Installed Package” afin de vérifier que les packet se soit correctement installer :



Une fois l'instalation terminés on va passer à la configuration pour cela ce rendre dans :
System > general setup



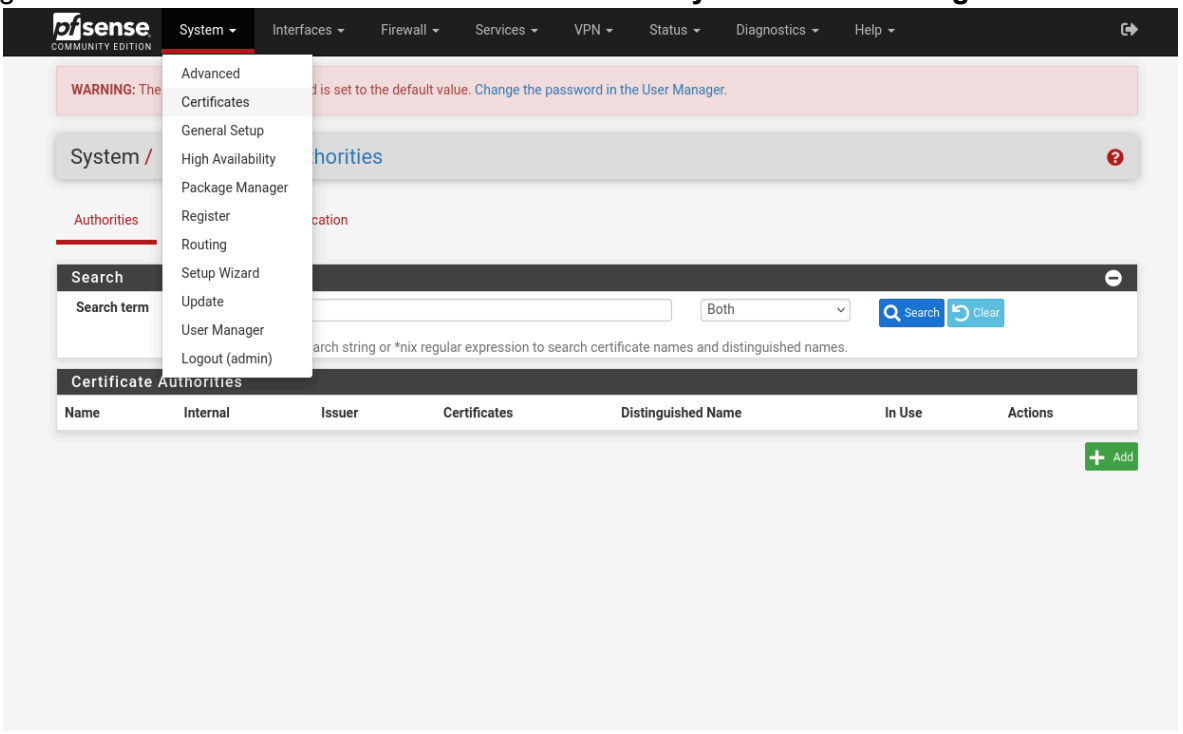
Dans cette onglet on vas procéder à la configuration du dns ainsi que du nom de l'hôte.



Une fois cette configuration effectuée, on peut save les changements.

3.2°) Création des certificats

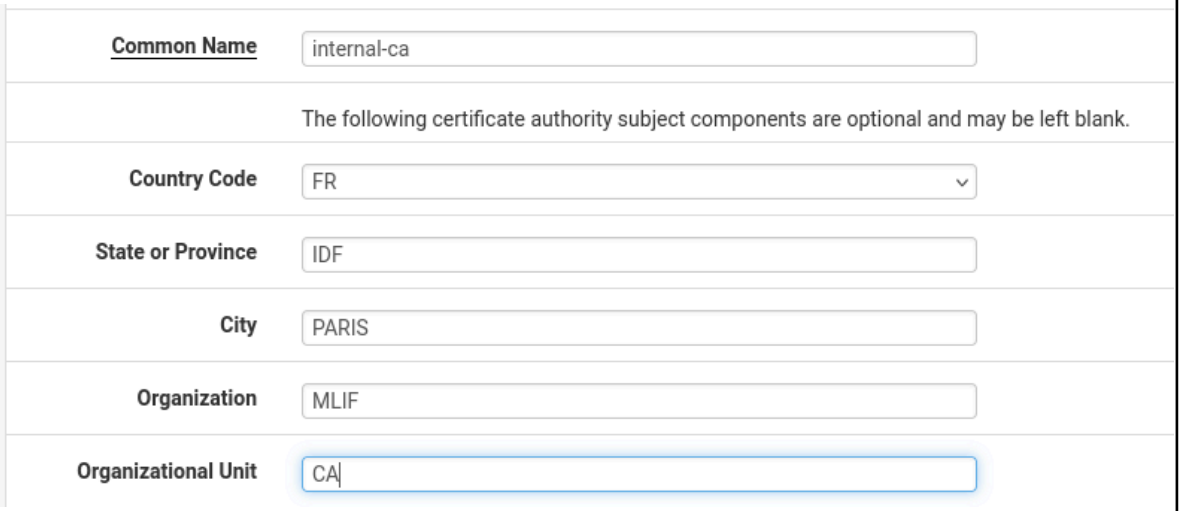
Comme nous devons aussi bloquer des sites HTTPS, il faut dans un premier temps générer les certificats. Pour ce faire se rendre dans **System > Cert.Manager.**



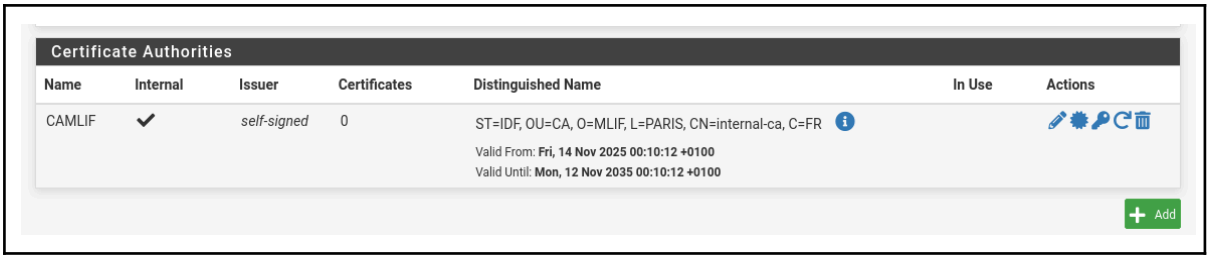
Dans authorities (anciennement CA) cliquer sur **“add” :**

- Renommer le certificat **“CAMLIF” :**

- Laisser tout les paramètre par défaut sauf les paramètres suivants :



Sur la page principale on peut maintenant voir que le certificat as bien été crée et ce pour une durée de 10 ans !!! *



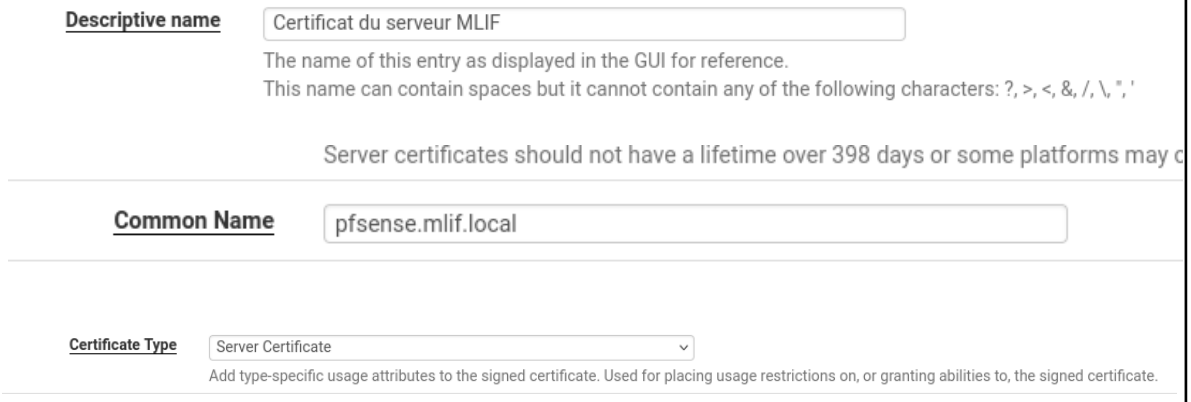
3.2.2°) Création du certificat du serveur

On va maintenant passer à la création du certificat coté serveur.

En effet, nous devons maintenant créer un **certificat spécifique au serveur**, signé par l'autorité de certification que nous venons de générer.

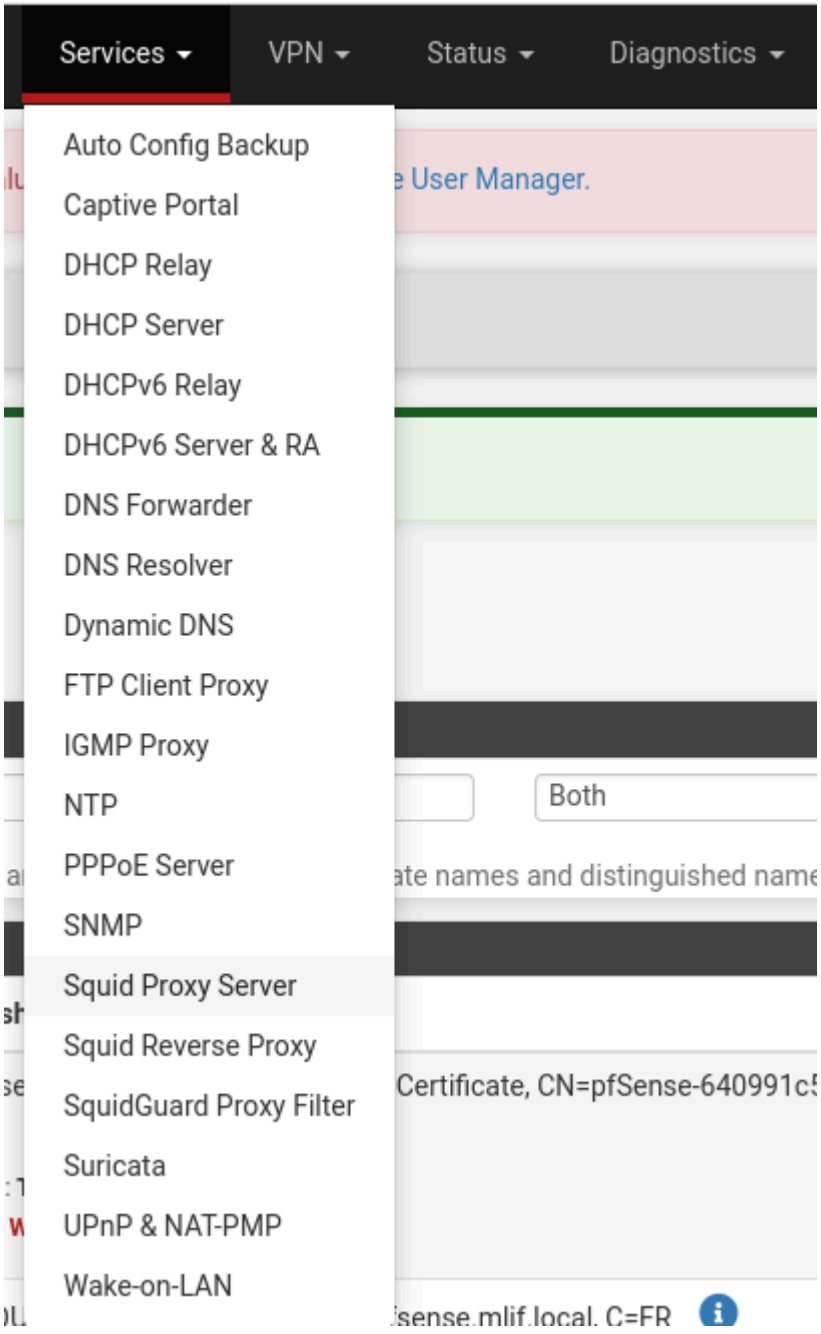
Pour cela, il suffit d'ouvrir l'onglet **Certificates > Add/Sign** afin de créer le nouveau certificat serveur.

Il faudra laisser tout les paramètres par défaut sauf les paramètres suivant :

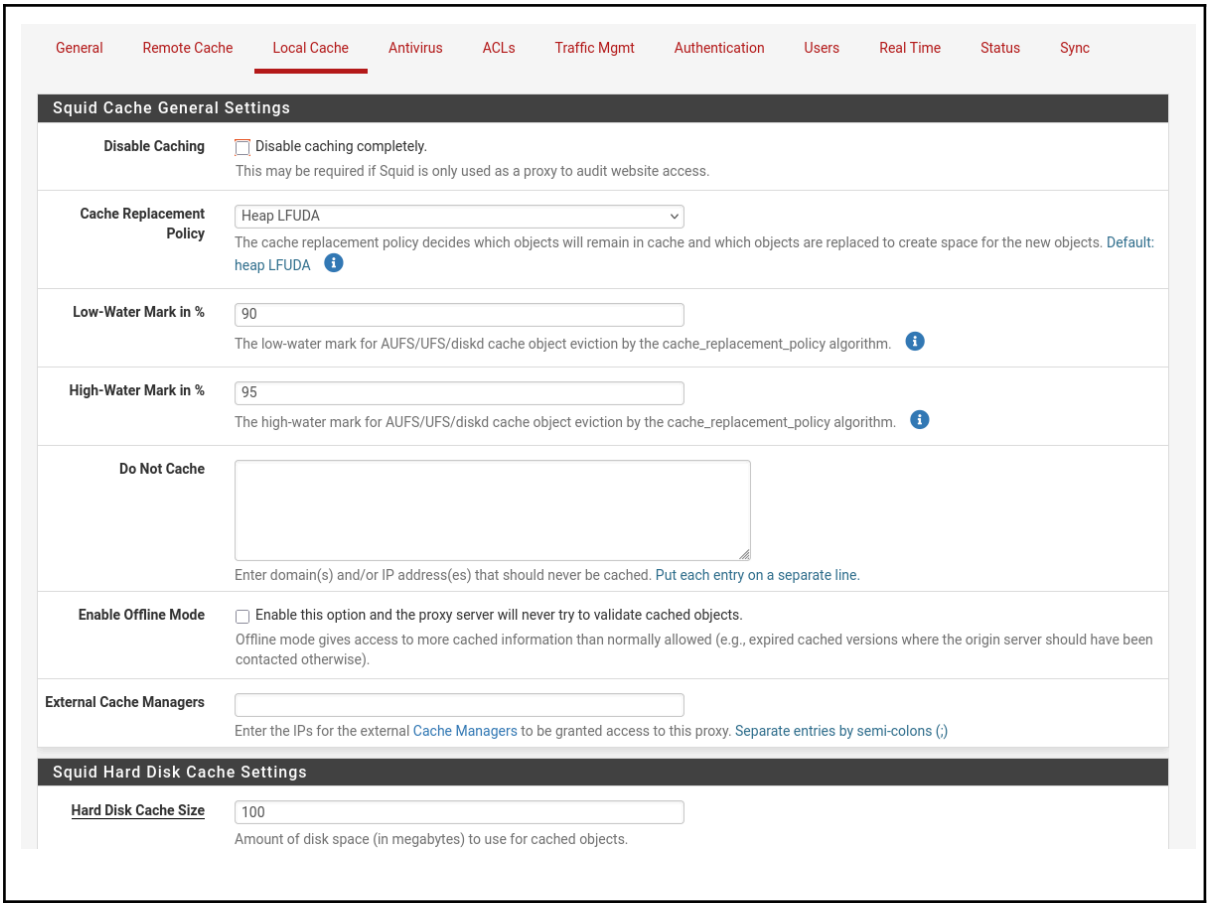


3.3°) Configuration de squid

Nous devons maintenant configurer le **cache de Squid**.
Encore sur le pare-feu accessible depuis la machine cliente on doit se rendre sur **Services > Squid Proxy Server**.

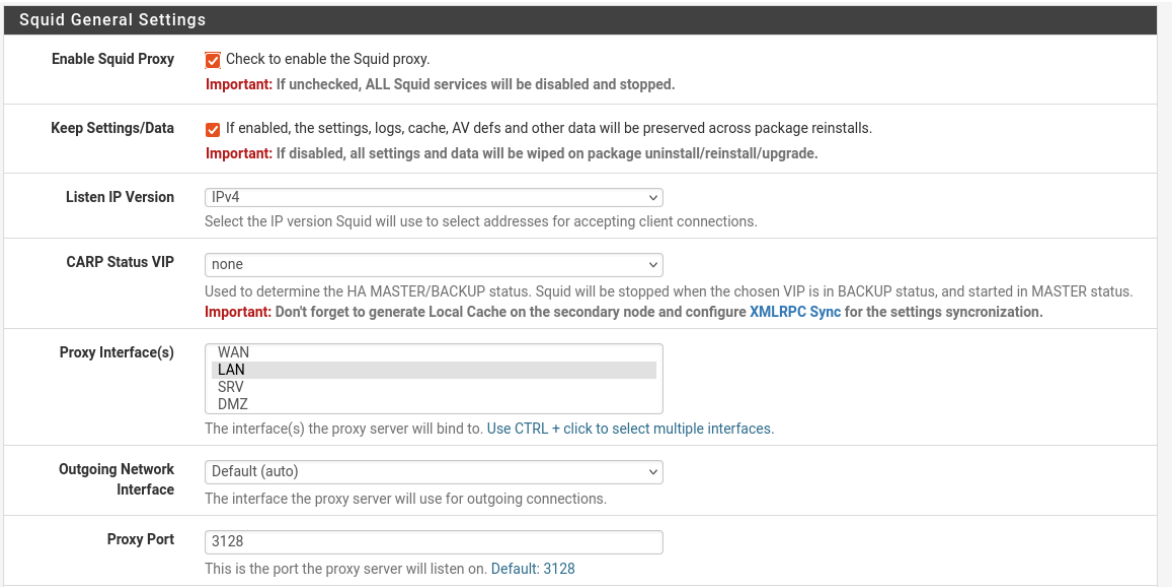


Une fois ici ce rendre sur l'onglet **"Local Cache"**, y laisser toutes les valeurs par défaut et cliquer uniquement sur **"SAVE"** :



3.3.2°) Configuration générale

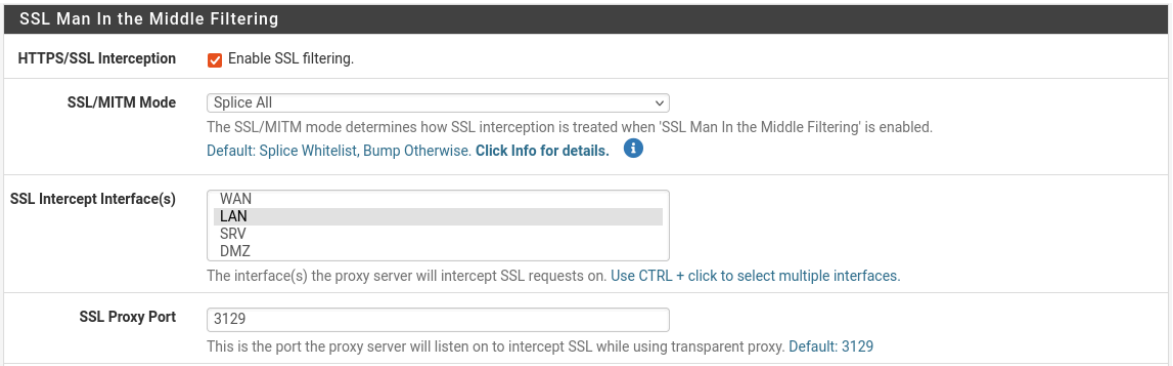
On vas maintenant procéder à la configuration général de squid, sur le même onglet du proxy server cliquer sur **“GENERAL”**, laisser toute les valeurs par défaut à l’exception des valeurs suivante :



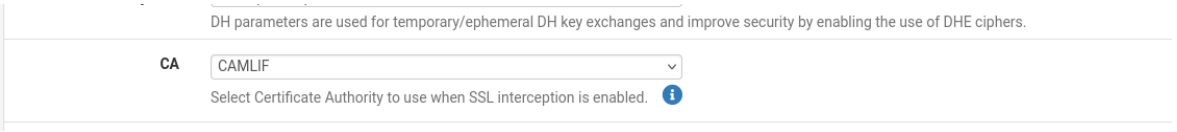
3.3.3°) Configuration du filtrage SSL (*Secure Sockets Layer*)

Tout d'abord petite définition, le SSL c'est quoi ? *Secure Sockets Layer* est un protocole de sécurisation des communications sur Internet. C'est lui qui permet d'établir une connexion **chiffrée** entre un client (par exemple ton navigateur) et un serveur (un site web). Aujourd'hui, SSL a été remplacé par son successeur **TLS**, mais on continue d'utiliser le terme "SSL" par habitude, notamment dans les outils comme Squid.

Ceci étant dit, on reste sur la même page et on descend un peu afin d'activer le filtrage SSL:



Il est nécessaire d'indiquer à Squid le **certificat serveur** que nous avons configuré précédemment, afin qu'il puisse déchiffrer puis réencrypter le trafic HTTPS.
Un tout petit peu plus bas dans la catégorie **"CA"**, sélectionner le certificat fraîchement créé :



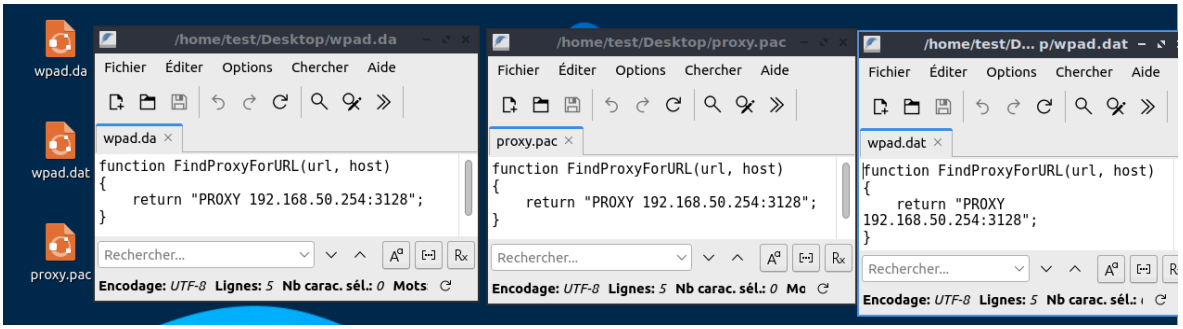
3.3.4°) Proxy transparent via WPAD

Nous devons maintenant configurer le proxy en **mode transparent**. Avec ce mode, les navigateurs des machines clientes n'auront plus besoin d'indiquer manuellement l'adresse du proxy : tout sera détecté automatiquement.
Pour cela, nous allons utiliser la méthode **WPAD** (*Web Proxy Auto-Discovery*), un protocole qui permet aux postes clients de trouver automatiquement l'URL du fichier de configuration du proxy.

Toujours depuis la machine DEBIAN_TRAINING_CLIENT, crée 3 fichiers sur le bureau nommée :

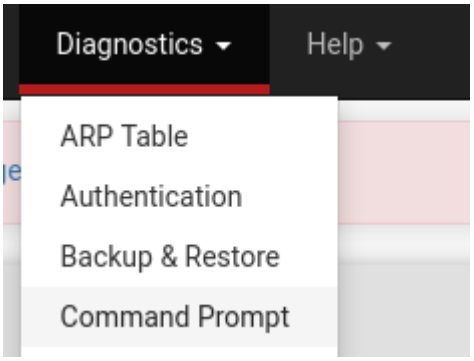
- wpad.dat ;
- wpad.da ;
- proxy.pac ;

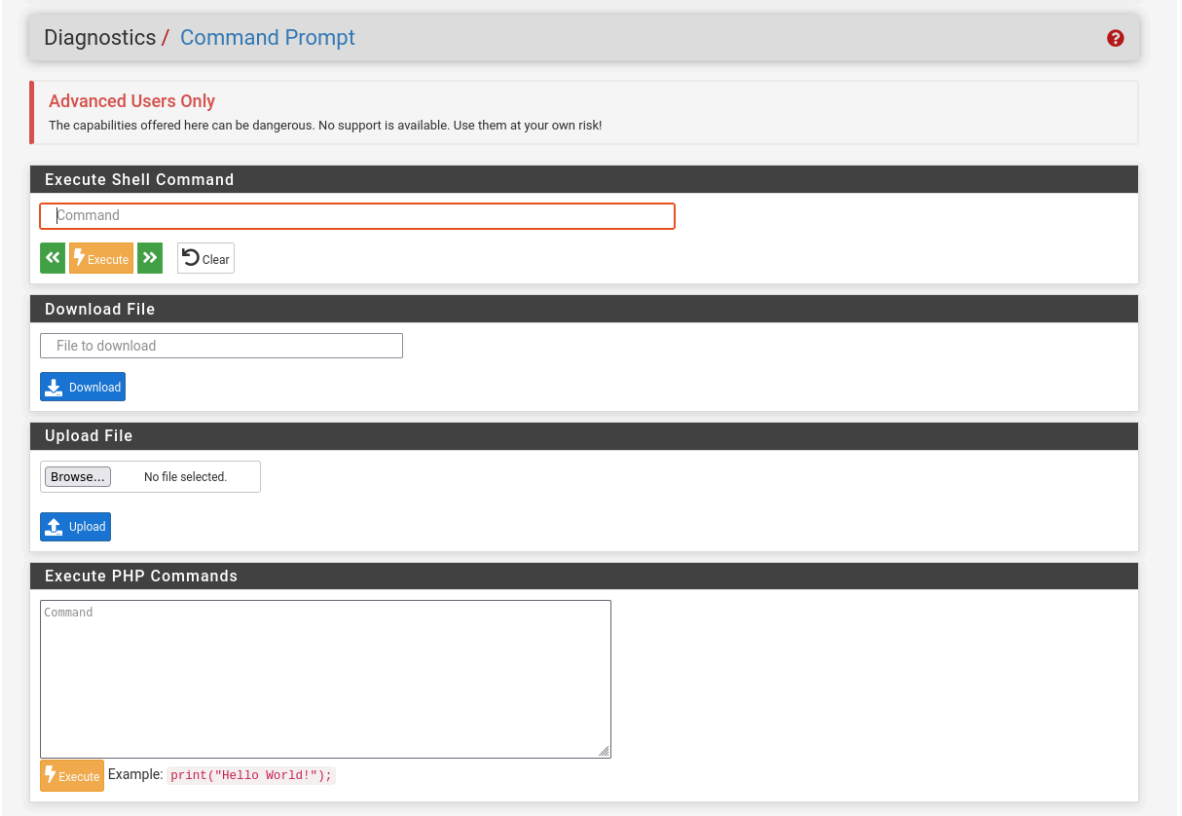
Les 3 fichiers posséderont le même contenu :



Une fois les trois fichiers créés, il nous faudrais les uploader sur notre serveur à l'adresse **/usr/local/www.**

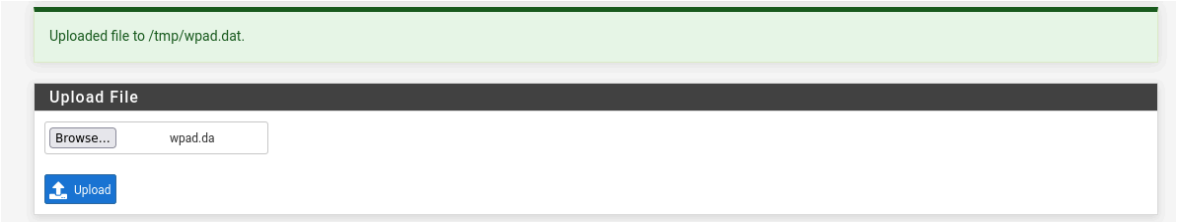
Pour ce faire il nous faudra se rendre dans l'onglet **"Diagnostics"** puis **"Command prompt"**



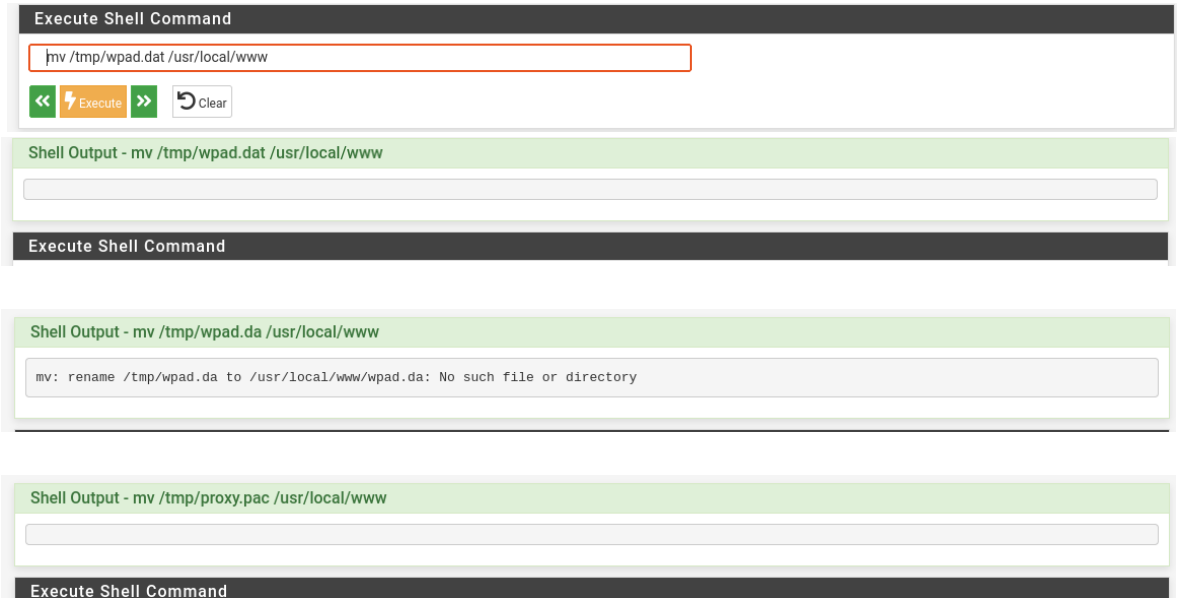


Une fois sur cette page, nous devons envoyer nos fichiers depuis la machine cliente vers le pare-feu. Nous devons donc les **uploader**.

Dans la section **"Upload File"**, nous devons donc sélectionner les 3 fichiers fraîchement créés :

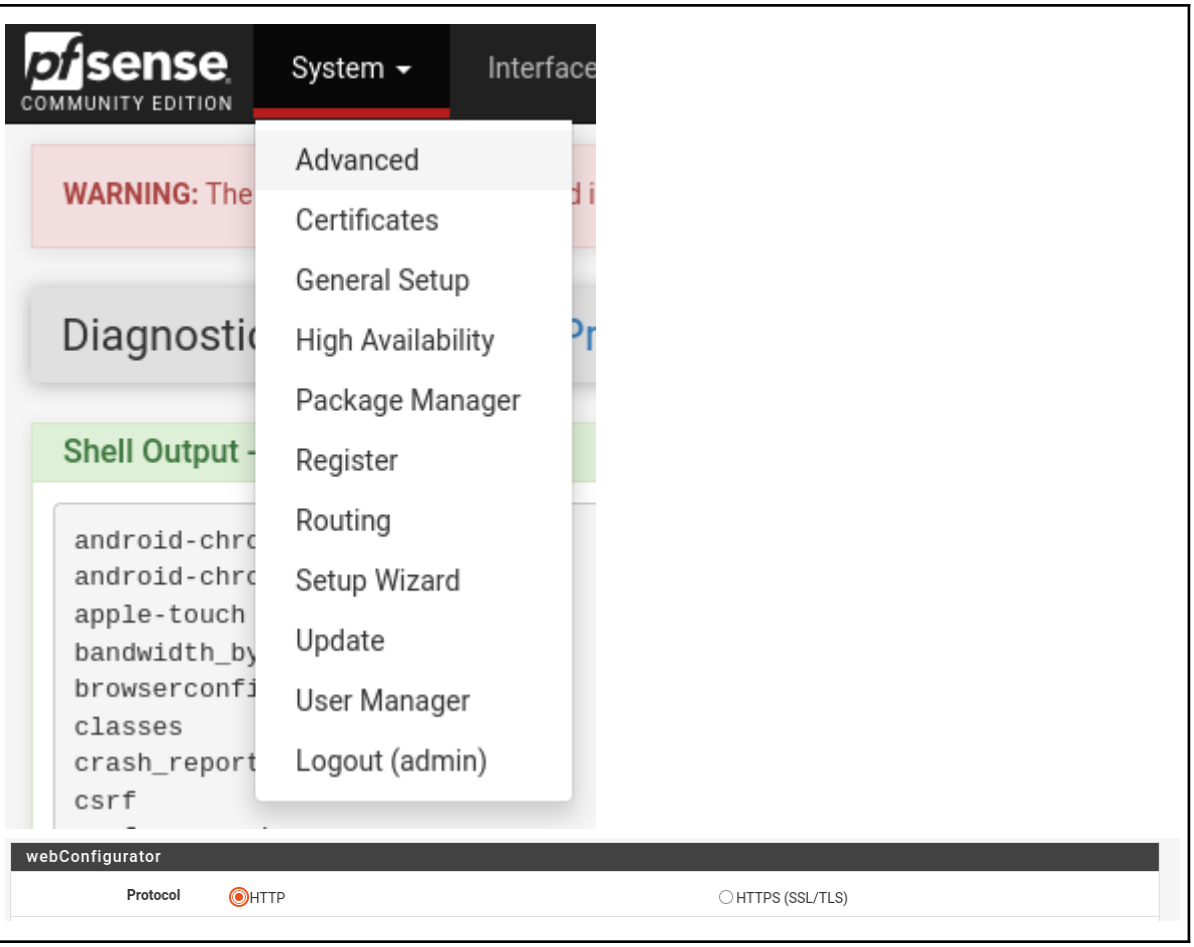


Une fois les fichiers uploadés on obtiendra ce message là. Les fichiers se trouvent maintenant dans un répertoire temporaire nous devons les déplacer dans le répertoire **/usr/local/www.** Dans l'exécuteur de commande **"Execute Shell Command”**, nous allons les déplacer à l’aide de la commande **“mv” :**



Nous devons maintenant configurer l’accès à l’interface web du pare-feu en HTTP uniquement. Même si cette méthode est peu sécurisée, elle est utilisée ici pour faciliter la démonstration. En pratique, il serait préférable de déployer une instance HTTP externe dédiée au WPAD, car ce service n’a pas besoin d’authentification et doit être accessible à tous les navigateurs.

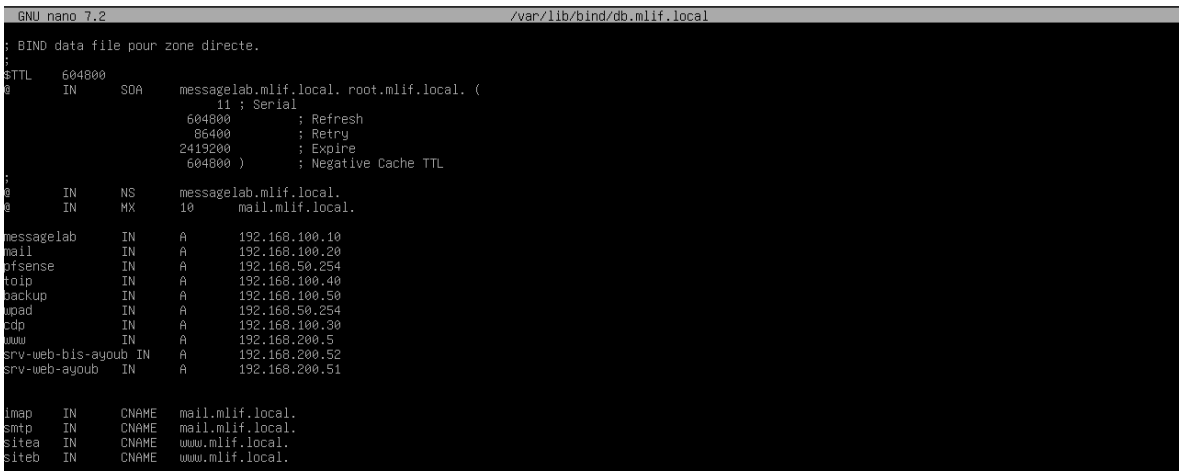
Pour effectuer cette modification, il suffit d’ouvrir **System > Advanced**, puis de sélectionner le protocole **HTTP** avant de valider les changements.



Depuis la machine DEBIAN_TRAINING_SERVEUR:

Nous devons ensuite ajouter une nouvelle entrée dans la zone directe de notre serveur DNS. Afin de permettre la résolution de nom.

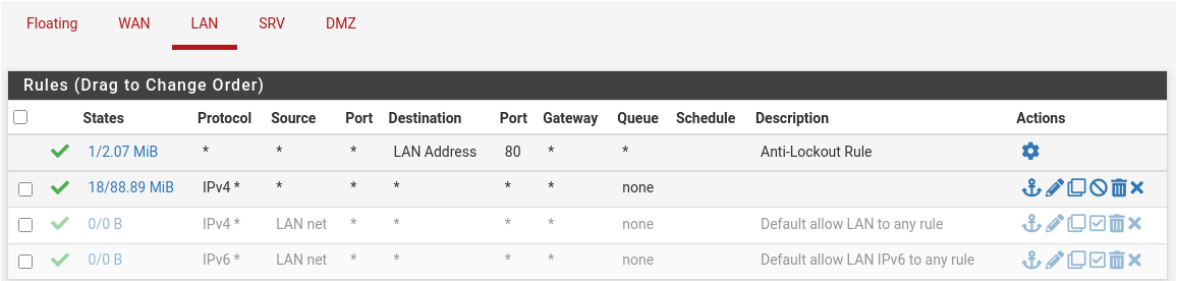
Pour cela se rendre dans le fichier de zone directe de notre DNS, il se trouve à l'adresse : **"/var/lib/bind/db.mlif.local"**



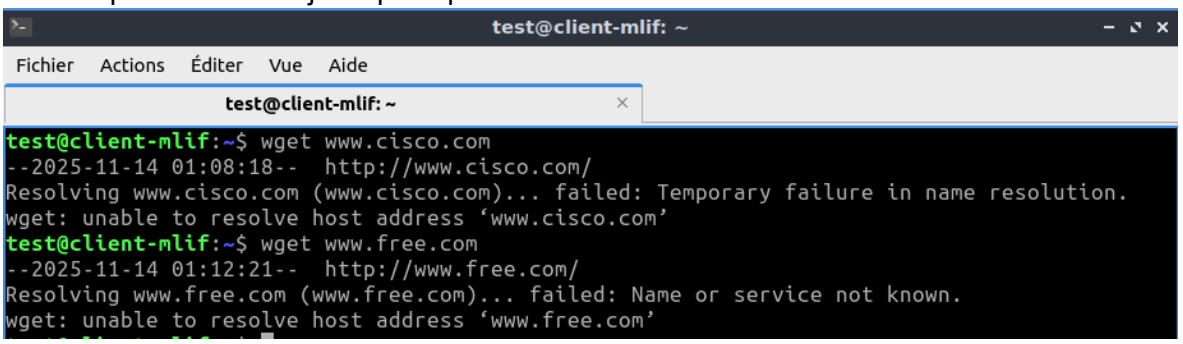
On voit bien que la ligne wpad pointant vers la passerelle de notre pare-feu est créée, on incrémente alors le numéro de série de version puis on enregistrer les modifications.

3.3.5°) Configuration du pare-feu

Nous devons ensuite désactiver, depuis le navigateur d'administration, la règle qui autorise l'accès Internet à tous les clients. Cela garantit que seuls les postes passant par le proxy pourront accéder au Web et donc correctement configurés . Tous les autres clients non authentifiés ou ne respectant pas la configuration proxy seront automatiquement bloqués.



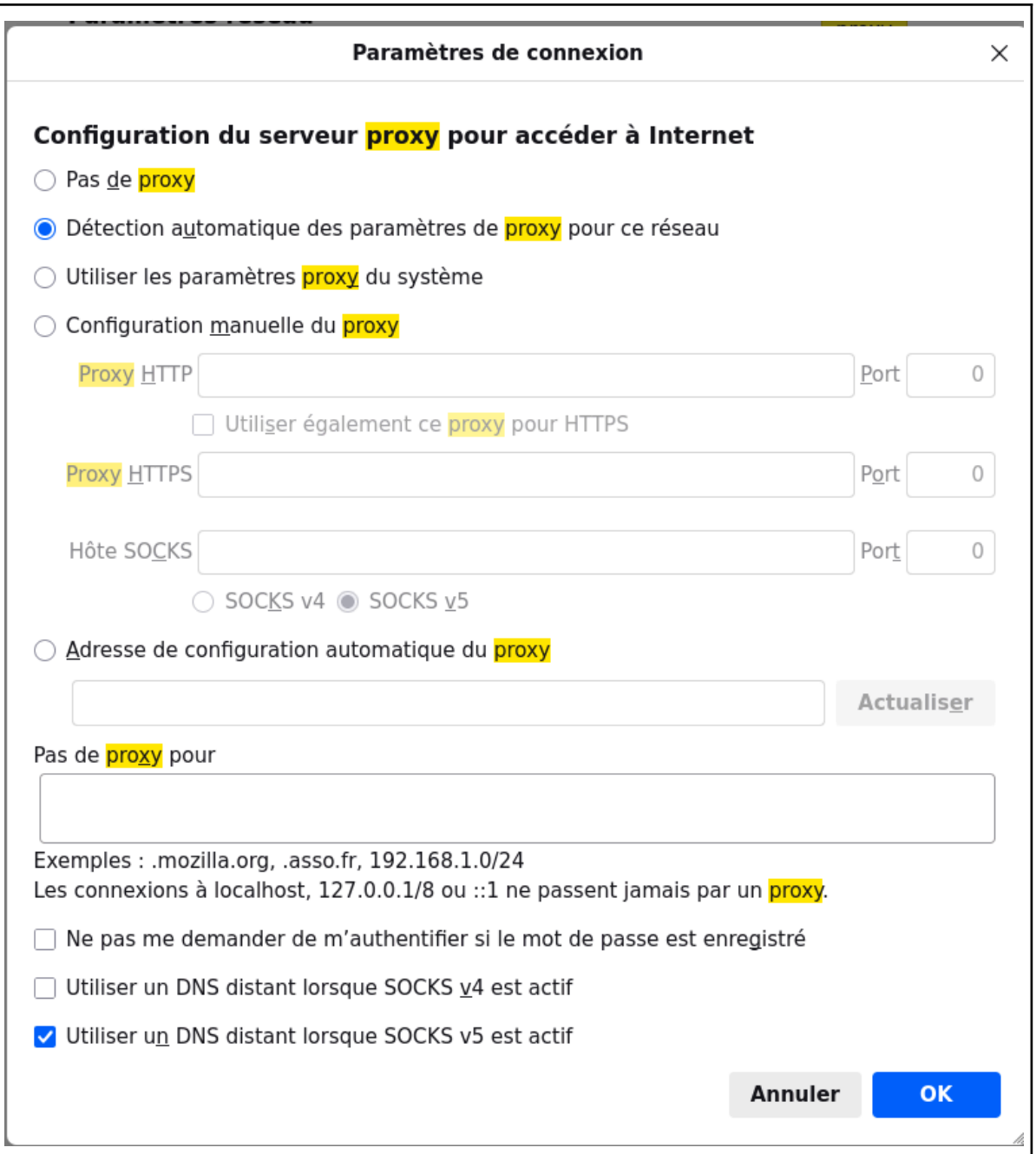
Je desactive donc la regle en ipv4 et en ipv6 qui permet la connexion de tous les clients au web. Pour verifier que cela fonctionne bien je sauvegarde les modifications et je test avec un "wget www.cisco.com" si un echec s'affiche cela signifie que je n'ai pas accès au web ce qui était mon objectif principale :



j'ai effectué 2 tests pour être sur de l'echec.

3.3.6°) Configuration du navigateur

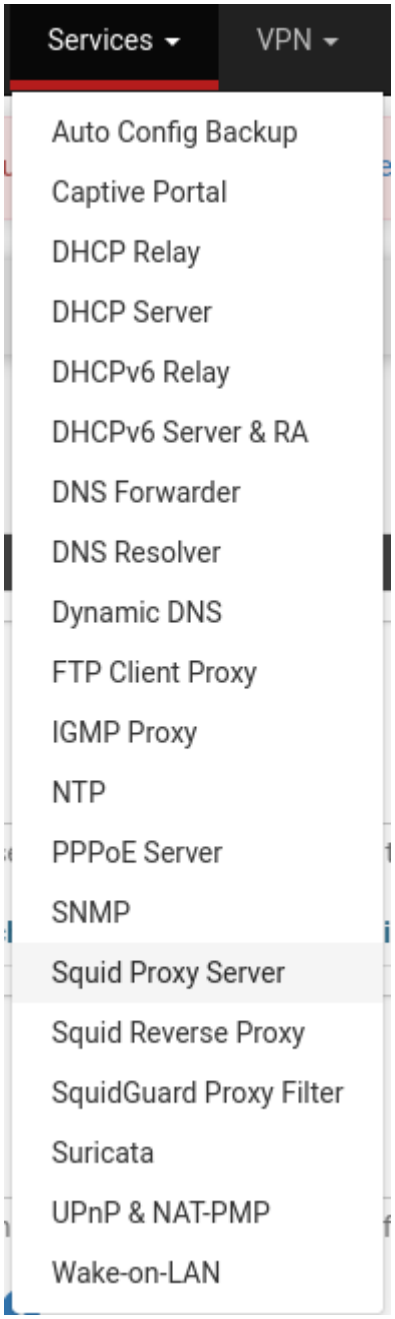
Pour terminer, le navigateur de la machine cliente doit être configuré pour détecter automatiquement les paramètres du proxy. Cette option se configure dans les préférences du navigateur :



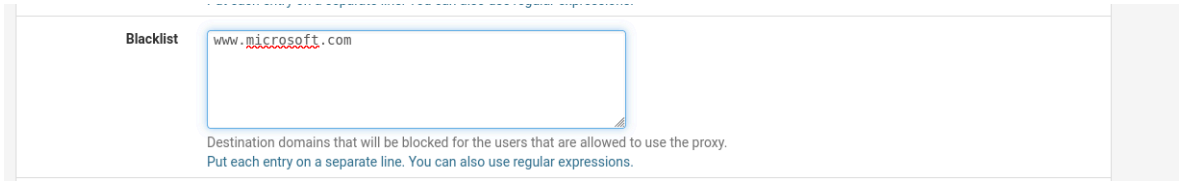
je bascule le paramètre sur " Détection automatique des paramètres de proxy pour ce réseau".

3.3.7°) Test de la configuration

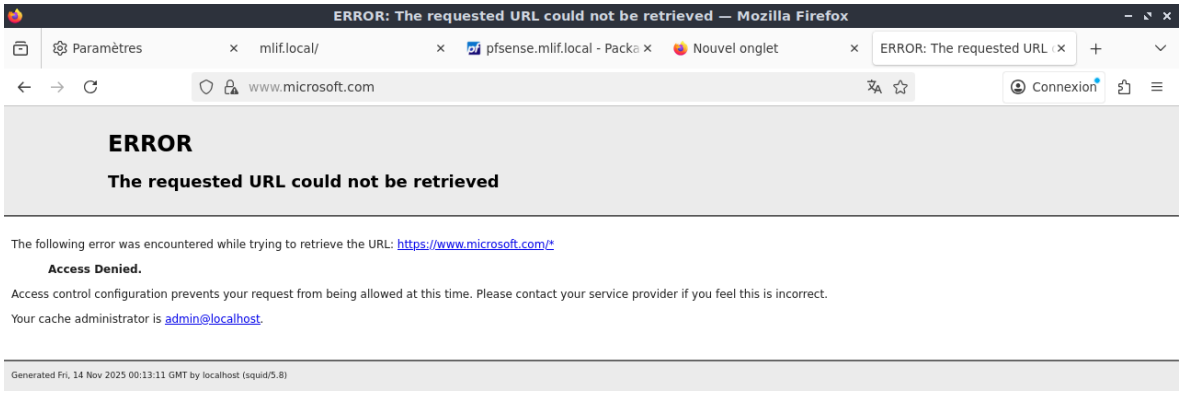
Nous devons maintenant configurer Squid pour bloquer les sites du domaine microsoft.com.
Pour cela, il suffit d'ouvrir l'onglet **ACLs dans Squid**, d'ajouter microsoft.com dans la zone Blacklist, puis de valider. Enfin, il faut fermer et rouvrir le navigateur pour appliquer le filtrage. Au chemin **"Service > Squid Proxy Server"**



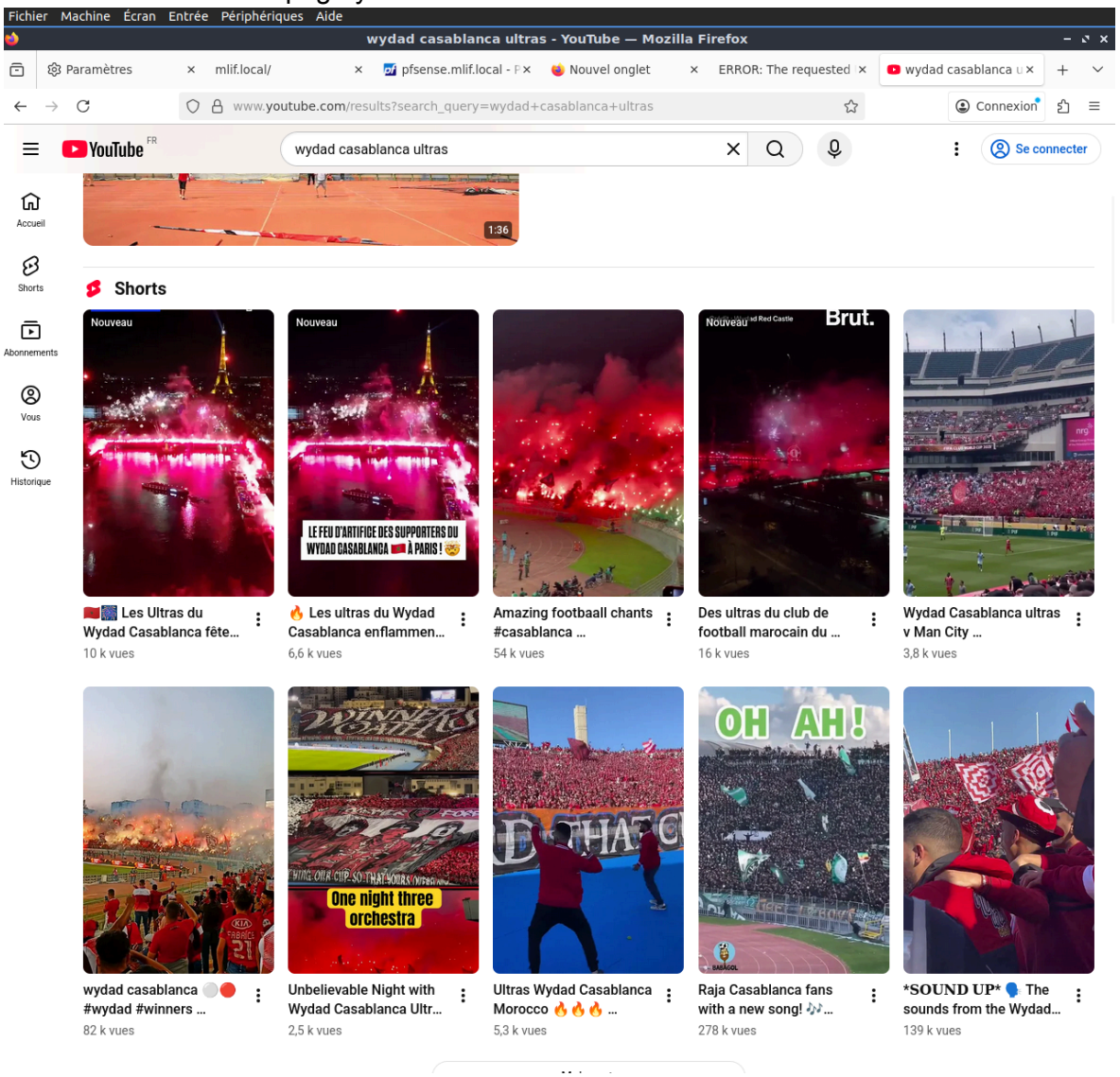
Puis dans blacklist entrer le site de microsoft “www.microsoft.com”



Maintenant si je test une de rentrer le site je dois être refusé :



à l'inverse les autres site fonctionne, je tente par exemple une connection à youtube.com
Cela me donne bien la page youtube.

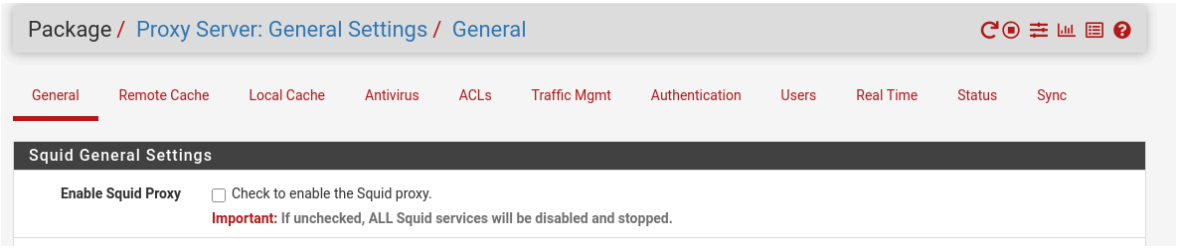


C'est bien ce qui se passe donc le proxy joue bien sont rôle.

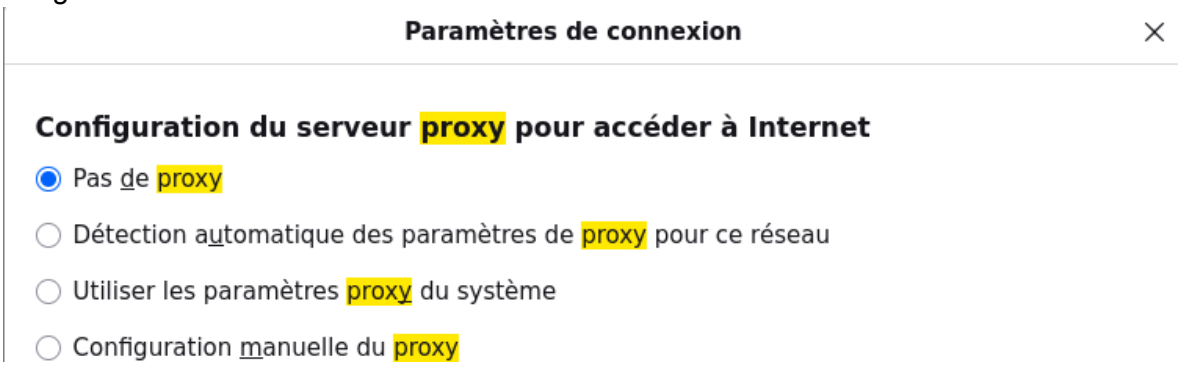
STOP 1 : Appelez moi pour que je puisse vérifier cette partie du travail

3.4°) Filtrage avancé avec squidguard
3.4.1°) Configuration de squidguard

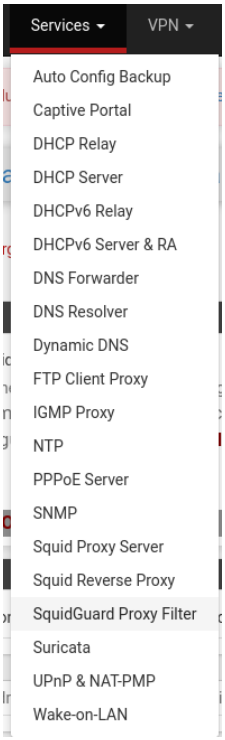
Depuis le navigateur d'administration, nous devons désactiver le service Squid. Pour cela, il suffit d'ouvrir **Services > Squid Proxy Server**, **de décocher l'option d'activation du proxy**, puis d'enregistrer les changements.



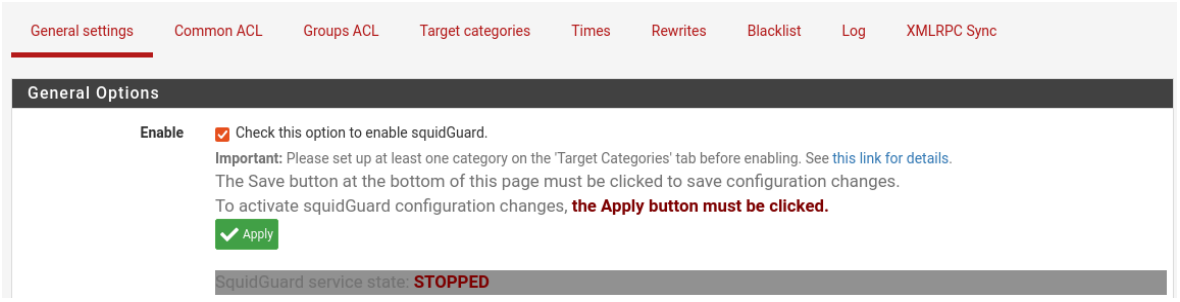
Nous devons ensuite modifier les paramètres du navigateur pour désactiver l'utilisation du proxy. Il suffit de sélectionner l'option Pas de proxy dans la configuration réseau du navigateur.



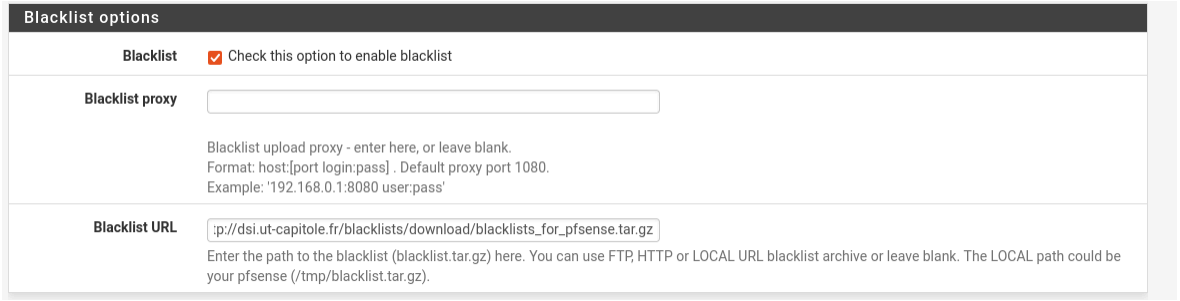
Nous devons maintenant activer le filtre SquidGuard. Pour cela, il suffit d'ouvrir **Services > SquidGuard Proxy Filter**, puis de c**ocher l'option d'activation dans l'onglet General Settings.**



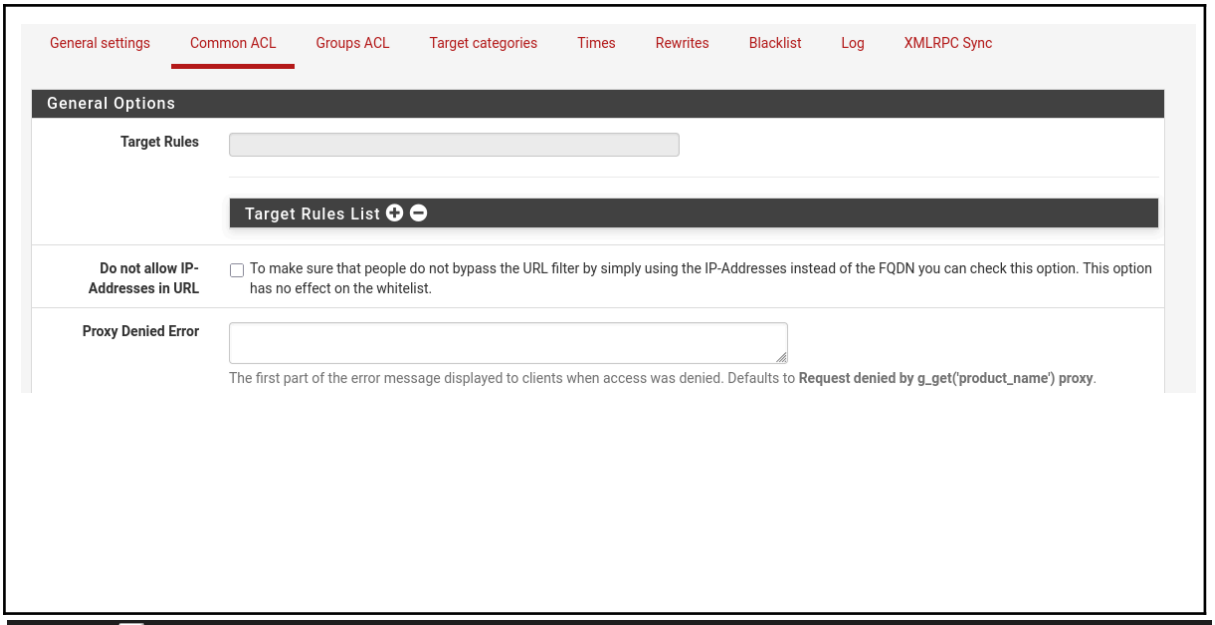
Une fois sur la page de configuration de Squidguard Proxy filter, il faudra l'activer

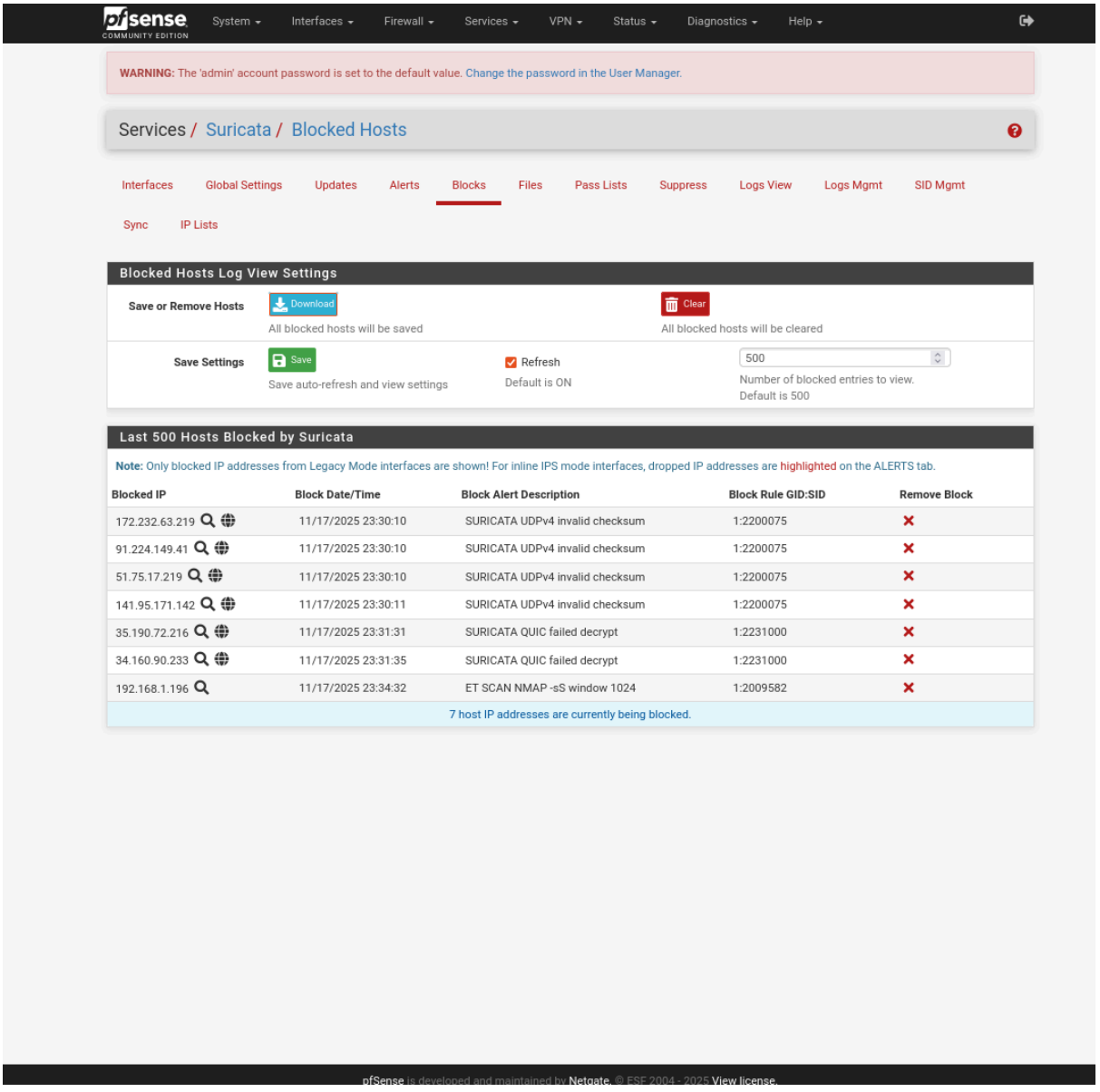


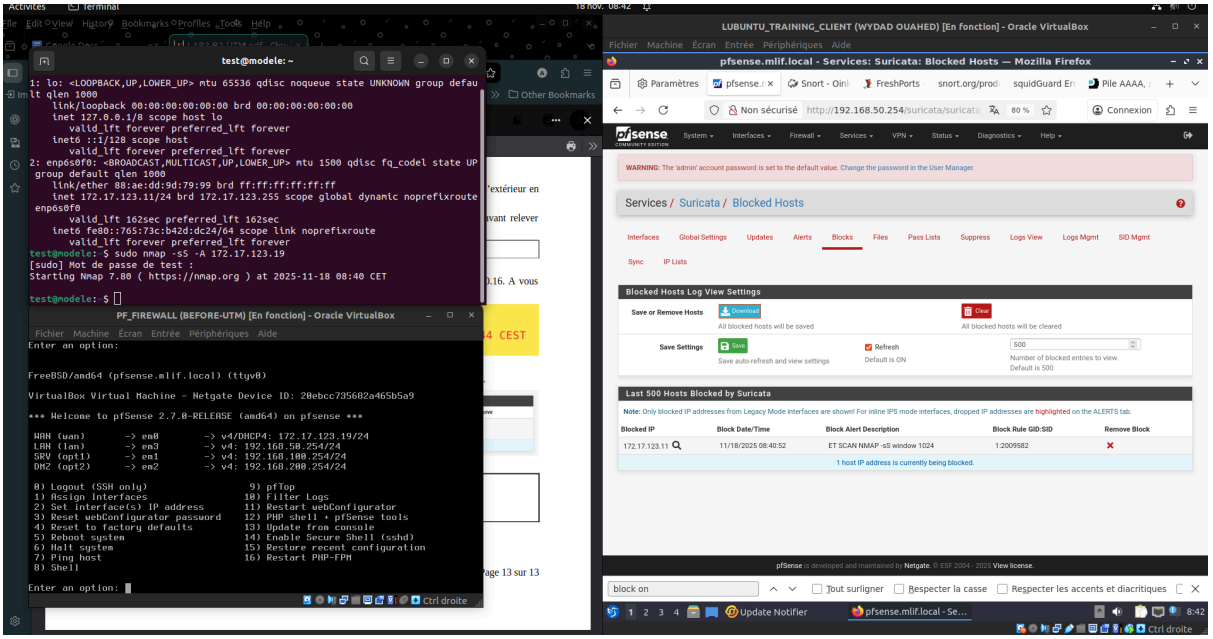
Une fois activé nous allons descendre un peu afin d'activer le blacklist et de renseigner l'adresse URL de l'archive contenant la blacklist :



On va maintenant se rendre sur **l'onglet Common ACL** et **cliquer sur le bouton (+)** dans **Target Rules List.**


General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
General Options
Target Rules
Target Rules List
Do not allow IP-Addresses in URL
To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.
Proxy Denied Error
The first part of the error message displayed to clients when access was denied. Defaults to Request denied by g_get('product_name') proxy.


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / Suricata / Blocked Hosts
Interfaces
Global Settings
Updates
Alerts
Blocks
Files
Pass Lists
Suppress
Logs View
Logs Mgmt
SID Mgmt
Sync
IP Lists
Blocked Hosts Log View Settings
Save or Remove Hosts
Download
All blocked hosts will be saved
Clear
All blocked hosts will be cleared
Save Settings
Save
Save auto-refresh and view settings
Refresh
Default is ON
500
Number of blocked entries to view.
Default is 500
Last 500 Hosts Blocked by Suricata
Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.
Blocked IP
Block Date/Time
Block Alert Description
Block Rule GID:SID
Remove Block
172.232.63.219
11/17/2025 23:30:10
SURICATA UDPv4 invalid checksum
1:2200075
91.224.149.41
11/17/2025 23:30:10
SURICATA UDPv4 invalid checksum
1:2200075
51.75.17.219
11/17/2025 23:30:10
SURICATA UDPv4 invalid checksum
1:2200075
141.95.171.142
11/17/2025 23:30:11
SURICATA UDPv4 invalid checksum
1:2200075
35.190.72.216
11/17/2025 23:31:31
SURICATA QUIC failed decrypt
1:2231000
34.160.90.233
11/17/2025 23:31:35
SURICATA QUIC failed decrypt
1:2231000
192.168.1.196
11/17/2025 23:34:32
ET SCAN NMAP -sS window 1024
1:2009582
7 host IP addresses are currently being blocked.
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.



Je vais maintenant pour approfondir mettre en place un serveur captif afin d'afficher un pop up demandant de se connecter à un compte de l'ad afin d'avoir l'accès.