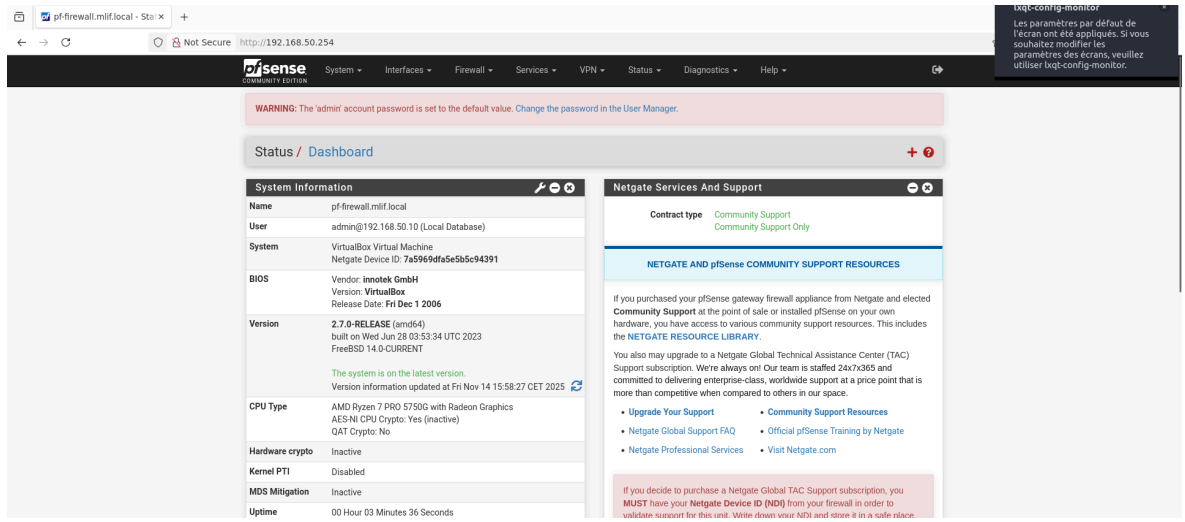
Faire un snapshot de votre machine PF_FIREWALL nommé BEFORE-UTM.
Ensuite, démarrer les machines suivantes du contexte de la MLIF :
• PF_FIREWALL ;
• DEBIAN_TRAINING_CLIENT;
• DEBIAN_TRAINING_SERVEUR ;
Sur la machine DEBIAN_TRAINING_CLIENT :
Ouvrir le navigateur et se connecter au pare-feu. (login : admin/admin)



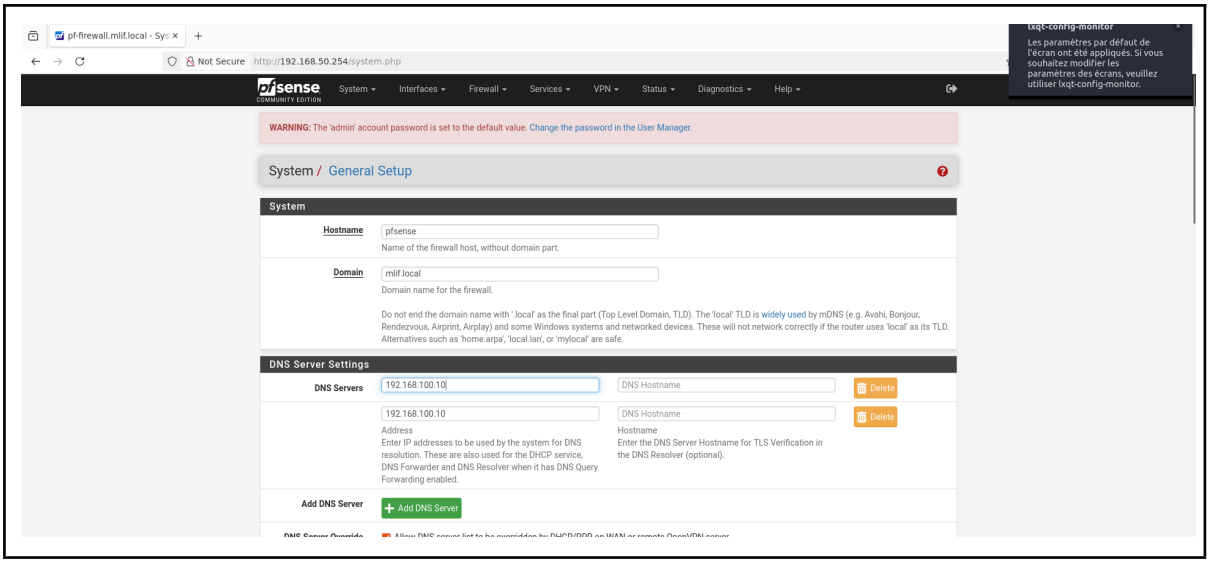
Ensuite cliquer sur System puis sur Package Manager.
Dans le gestionnaire de packages, cliquer sur l'onglet Available Package. Saisir la chaîne de caractère squid dans la barre de recherche. Enfin, cliquer sur le bouton vert pour installer squid.

squid est déjà installé

Ensuite, procéder de même en installant le logiciel squidguard. Ce logiciel permet de gérer des catégories de sites web à bloquer afin de faciliter le travail de l'administrateur.

squidguard est déjà installé

Aller ensuite dans le menu System puis dans General Setup et mettre les deux valeurs suivantes :
• Hostname : pfsense ;
• Domain : mlif.local ;
• DNS Servers : 192.168.100.10.

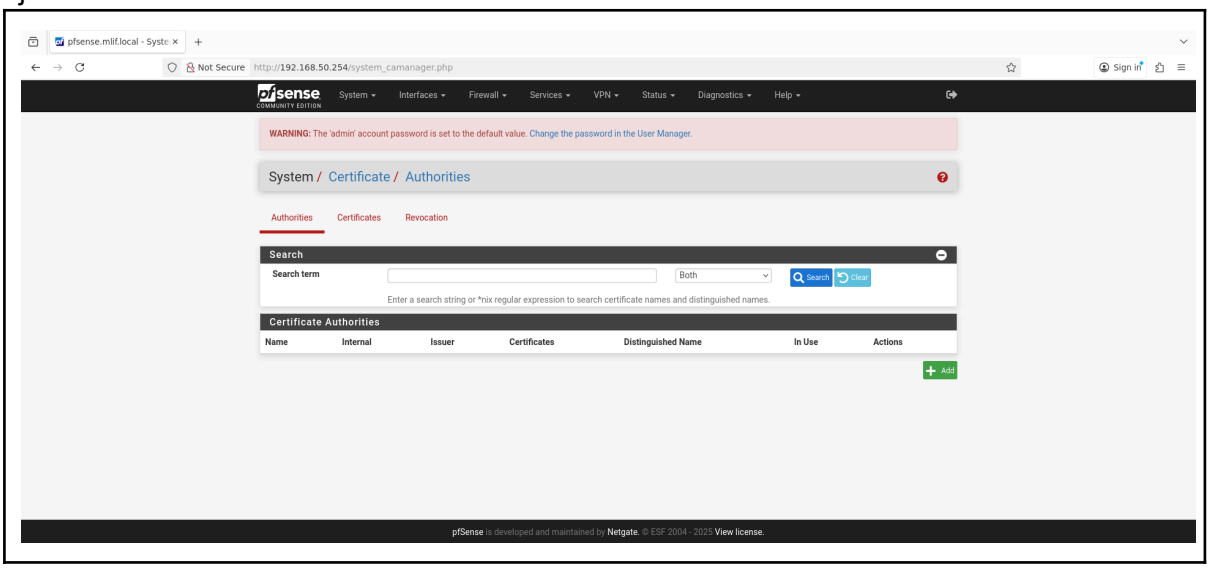


Sur la machine DEBIAN_TRAINING_CLIENT :

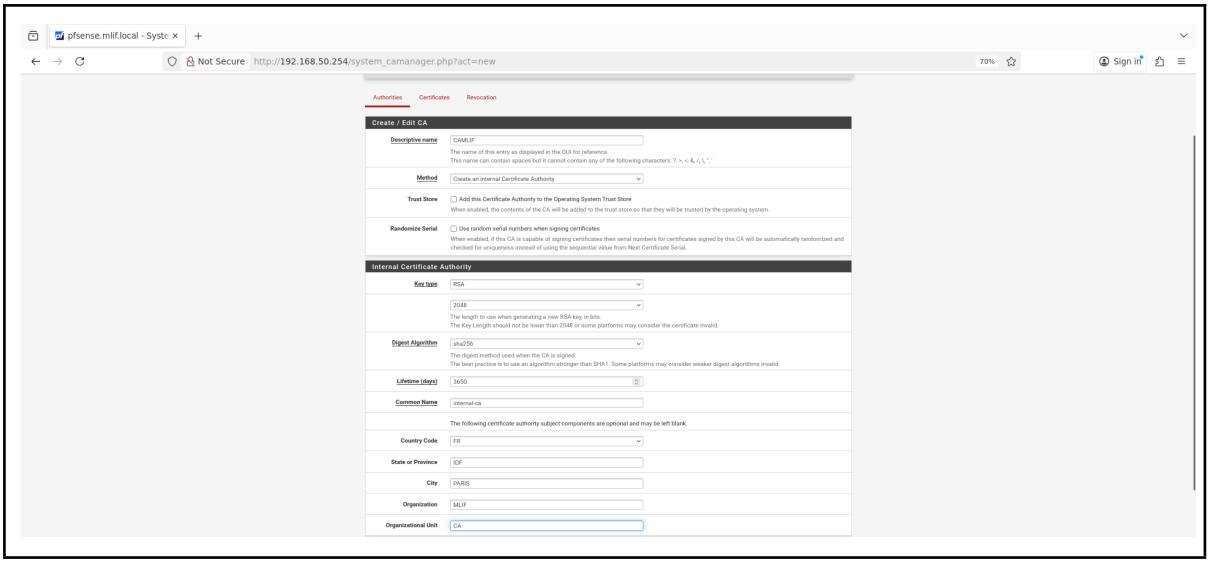
Toujours sur le pare-feu via le navigateur de la machine cliente.

3.2.1°) Création du certificat de l'autorité de certification

Cliquer sur System puis sur Cert.Manager. Dans l'onglet CAs, cliquer sur le bouton Add pour ajouter un certificat.



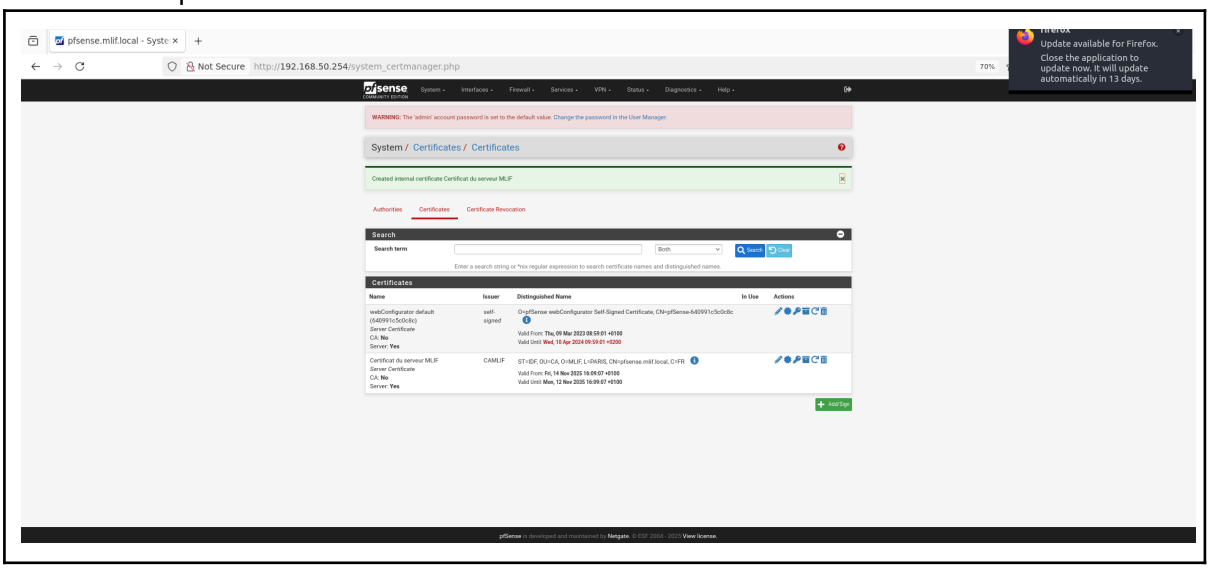
Nommer le certificat CAMLIF puis remplir les champs du formulaire en laissant les valeurs par défaut sauf pour les valeurs suivantes :



Il faut ensuite créer un certificat spécifique au serveur signé par notre autorité de certification. Pour cela,cliquer sur l'onglet Certificates puis sur le bouton Add/Sign. Ensuite, remplir les champs du formulaire en laissant les valeurs par défaut sauf pour les valeurs suivantes :

• Descriptive Name : Certificat du serveur MLIF ;
• Common Name : pfsense.mlif.local.
• Certificate type : Server Certificate.

Valider en cliquant sur le bouton Save.



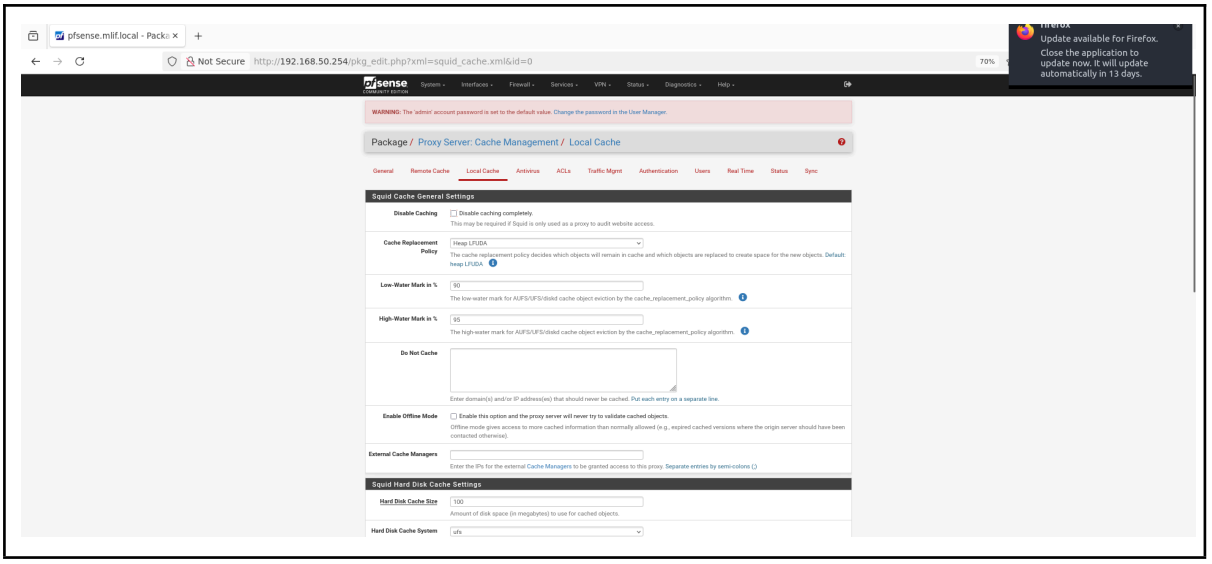
3.3.1°) Configuration du cache de squid

Sur la machine DEBIAN_TRAINING_CLIENT :

Toujours concernant le pare-feu via le navigateur de la machine cliente.

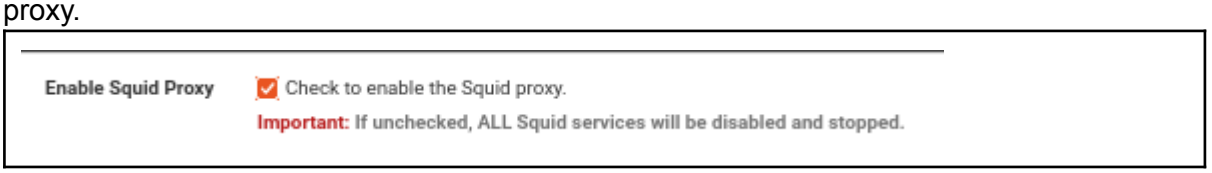
Cliquer sur Services puis sur Squid Proxy Server.

Ensuite, cliquer sur l'onglet Local Cache. Dans cet onglet, laisser les valeurs par défaut et valider en cliquant sur le bouton Save.



3.3.2°) Configuration générale

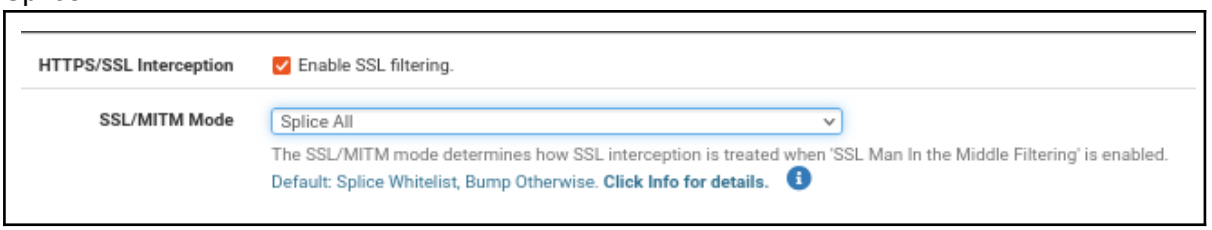
Puis, cliquer sur l'onglet General et activer le proxy en cochant Check to enable the Squid proxy.



Ensuite, sélectionner l'interface CLIENTS. (LAN) Laisser les autres valeurs par défaut.

3.3.3°) Configuration du filtrage SSL

Enfin, pour activer le filtrage SSL, il faut cocher l'option correspondante et choisir l'option Splice All.



Pour l'interception SSL, il faut faire référence au certificat du serveur configuré précédemment.

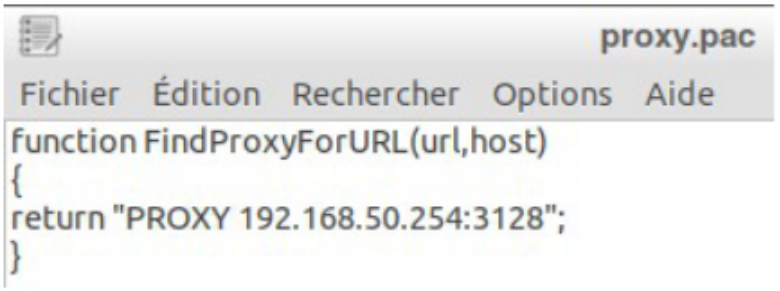


Depuis la machine DEBIAN_TRAINING_CLIENT :

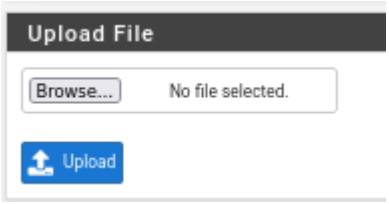
Créer trois fichiers sur votre bureau nommés respectivement :

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

Remplir ces trois fichiers avec le même contenu suivant :



Ensuite, il faut uploader ces trois fichiers sur votre serveur dans l'emplacement suivant : /usr/local/www.
Pour cela, cliquer sur Diagnostics puis sur Command Prompt depuis le navigateur qui pilote pfsense.



Sélectionner les trois fichiers précédents et valider en cliquant sur le bouton Upload. Les trois fichiers se trouvent enregistrés dans le répertoire /tmp. Il convient alors de les déplacer avec la commande mv vers le bon répertoire. Pour cela, exécuter les commandes suivantes via l'interpréteur de commandes :

- mv /tmp/wpad.dat /usr/local/www ;
- mv /tmp/wpad.da /usr/local/www ;
- mv /tmp/proxy.pac /usr/local/www

mv /tmp/proxy.pac /usr/local/www/proxy.pac mettre ca sinon yaura des souci



Enfin, il faut configurer l'accès web de votre pare-feu en HTTP seulement. Cette configuration est très dangereuse d'un point de vue sécurité. Nous procédons ainsi pour des raisons de simplicité de démonstration. Normalement, il aurait fallu créer une instance HTTP faisant référence au WPAD en dehors du pare-feu et ce uniquement dans ce but car cette dernière option ne nécessite pas d'authentification et n'est pas secrète mais à destination de tous les navigateurs.
Pour cela, cliquer sur System Puis sur Advanced. Ensuite, cocher Protocol HTTP et valider



Depuis la machine DEBIAN_TRAINING_SERVEUR:
Il faut ensuite ajouter une entrée dans la zone directe de notre serveur DNS. L'entrée à ajouter est la
suivante :

nano /var/lib/bind/db.mlif.local

```
wpad            IN      A       192.168.50.254
```

Tester en faisant un nslookup wpad.mlif.local. Ne pas oublier d'incrémenter le numéro de version du fichier.

```
root@messagelab:~# nslookup wpad.mlif.local
Server:         192.168.100.10
Address:        192.168.100.10#53

Name:   wpad.mlif.local
Address: 192.168.50.254
```

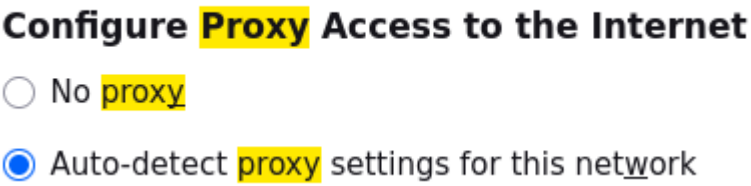
Depuis la machine DEBIAN_TRAINING_CLIENT :
Depuis le navigateur qui pilote la pare-feu, désactiver la règle de filtrage qui autorise l'accès à internet à tous les clients. Ainsi, tous les clients non authentifiés ne passant pas par le proxy ne pourront pas avoir accès à Internet.
La règle à désactiver, issue du LABO de filtrage, est la suivante :



Tester depuis un terminal de votre machine cliente la commande suivante :

```
test@client-mlif:~$ wget www.cisco.com
URL transformed to HTTPS due to an HSTS policy
--2025-11-14 16:32:19--  https://www.cisco.com/
Resolving www.cisco.com (www.cisco.com)... 104.116.98.2, 2a02:26f0:9100:f90::b33, 2a02:26f0:
9100:f94::b33
Connecting to www.cisco.com (www.cisco.com)|104.116.98.2|:443... connected.
OpenSSL: error:0A00010B:SSL routines::wrong version number
Unable to establish SSL connection.
```

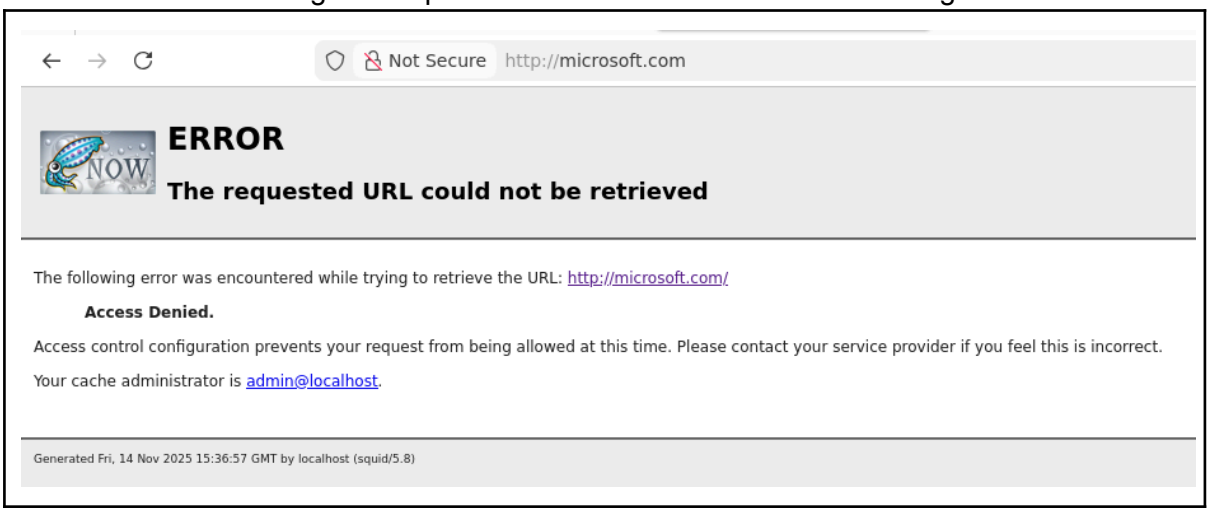
Vous devriez obtenir un échec ce qui est normal car cette commande n'est pas configurée pour passer par le proxy.
Pour terminer, le navigateur de la machine cliente doit être configurer pour détecter automatiquement les paramètres du proxy. Cette option se configure dans les préférences du navigateur :



Configurer squid pour bloquer les sites associés au nom de domaine microsoft.com. Pour cela, dans la configuration de squid, cliquer sur l'onglet ACLs et dans la zone de texte nommée Blacklist saisir microsoft.com.



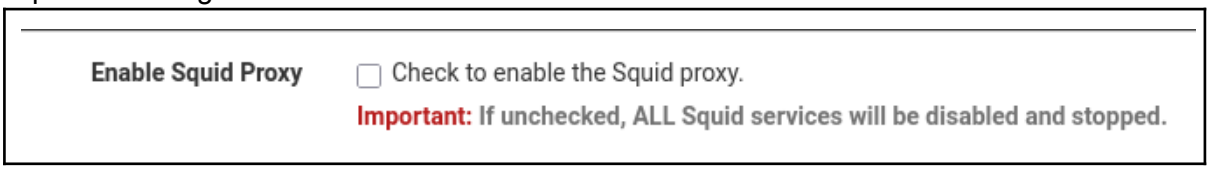
Valider la nouvelle configuration puis fermer et ouvrir de nouveau le navigateur



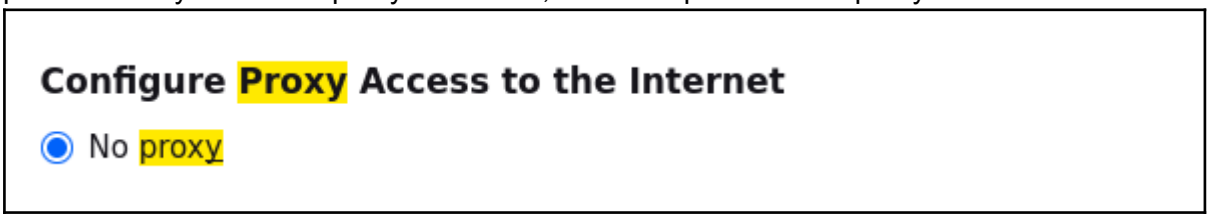
Tous les autres sites doivent être accessibles.
Si tout est bon, votre proxy est opérationnel. Il est transparent et filtre le HTTPS.
Il faut que quand on enlève le proxy, les sites ne soient pas accessibles

STOP 1

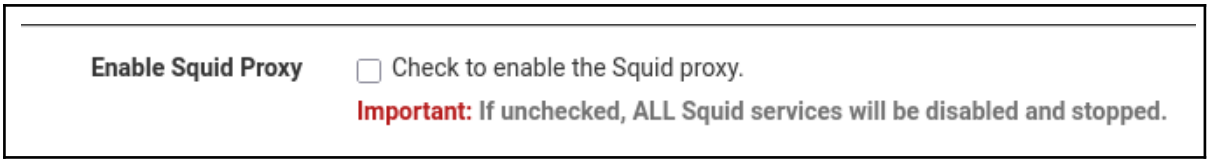
Depuis la machine DEBIAN_TRAINING_CLIENT :
Depuis le navigateur qui pilote la pare-feu, commencer par désactiver le service squid en cliquant sur Services puis sur Squid Proxy Server. Ensuite décocher la case d'activation de Squid et sauvegarder.



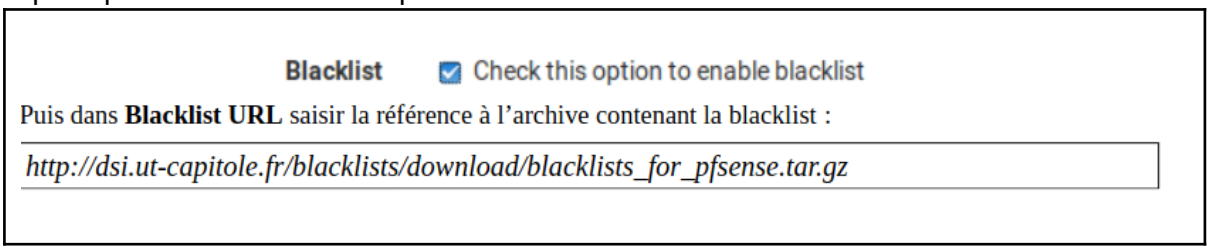
Ensuite modifier la configuration des paramètres du navigateur pour désactiver les paramètres systèmes du proxy. Pour cela, cocher l'option Pas de proxy.



Ensuite, cliquer sur Services puis sur SquidGuard Proxy Filter. Puis, dans l'onglet General Settings, cocher la case permettant d'activer squidguard.



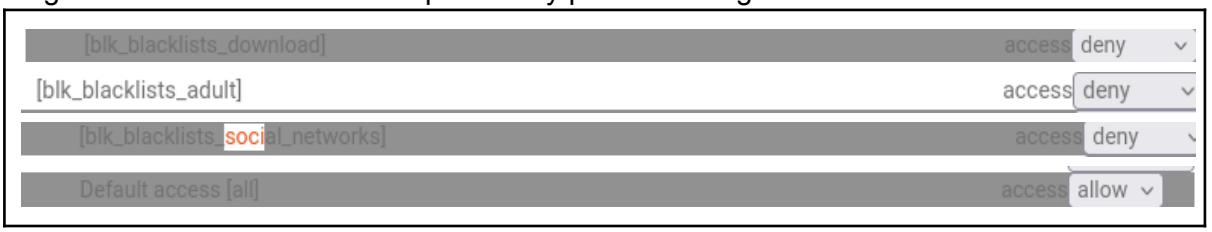
Toujours dans cet onglet, en bas de la page, dans la rubrique Blacklist Options, cocher l'option permettant d'activer l'option de blacklist.

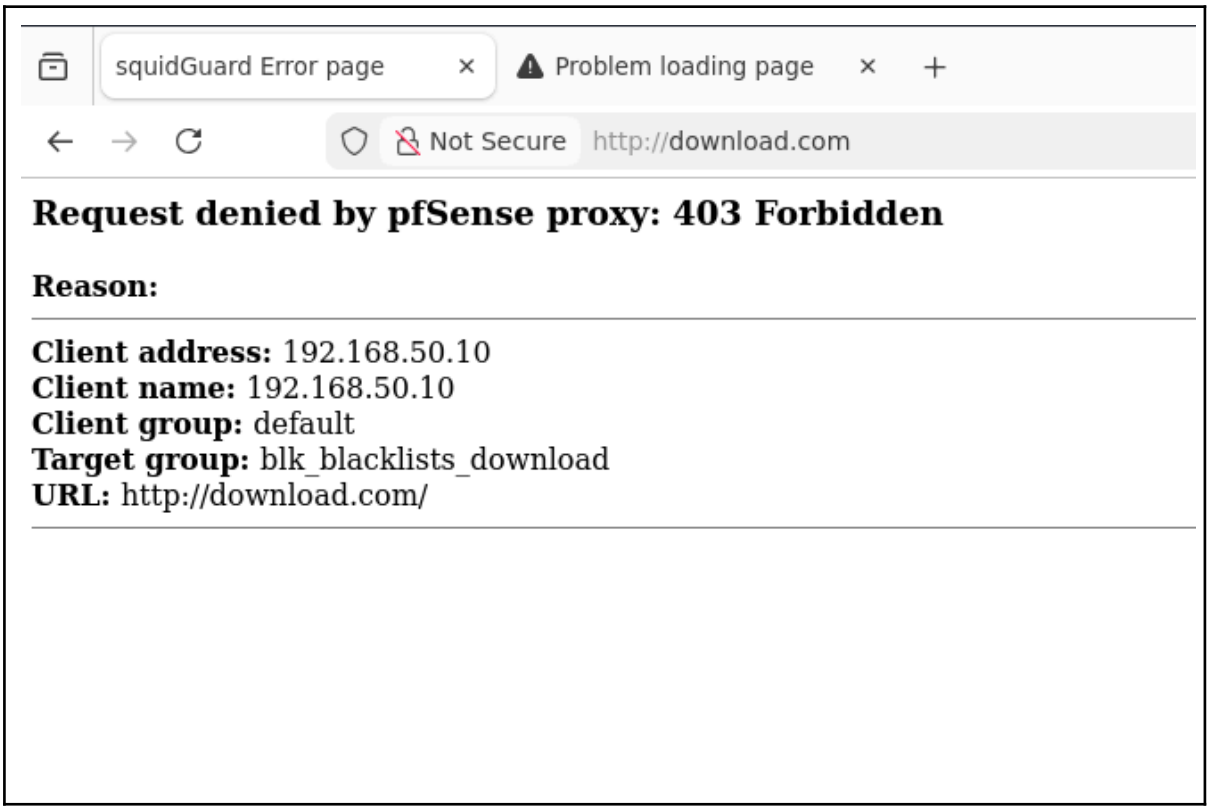


Entrer l'url ici :



Une fois terminé, se rendre sur l'onglet Common ACL et cliquer sur le bouton (+) dans Target Rules List sélectionner l'option deny pour les catégories suivantes :





Le message n'est pas le même pour facebook c'est normal

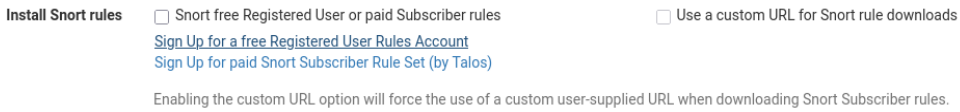
STOP 2

Via le navigateur qui pilote pfsense, commencer par installer le logiciel snort en le cherchant dans les packages. (PENSER À REMETTRE LES REGLES DE FILTRAGES)

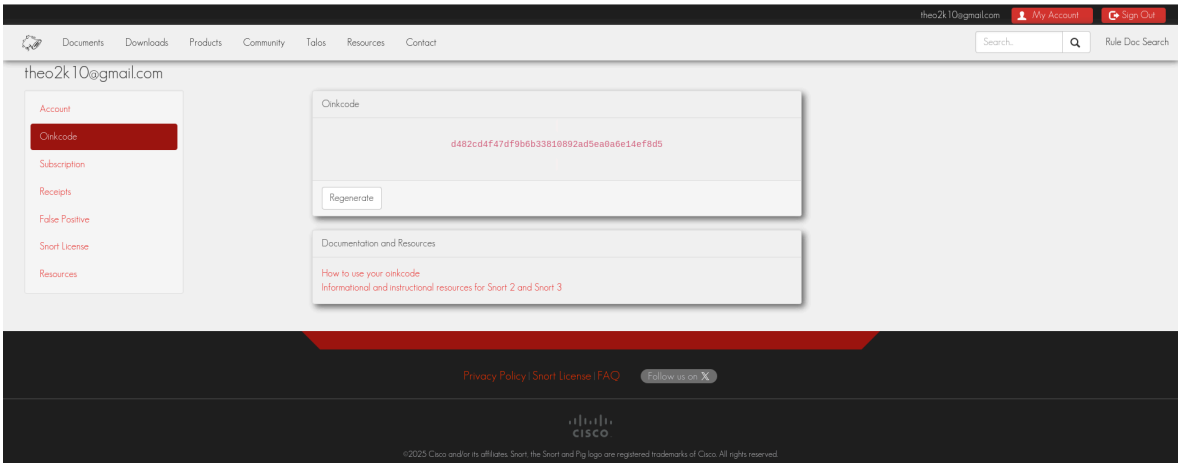


On va utiliser surikata dans notre cas

Depuis la machine DEBIAN_TRAINING_CLIENT :
Cliquer sur Services puis sur Snort. Ensuite, se rendre dans l'onglet Global Settings. A ce niveau là, il faut créer un compte sur le site officiel de snort afin de disposer d'un Oinkcode.



Une fois le compte fait, il faut valider par email puis aller en haut à droite sur son profil puis cliquer sur Oinkcode :

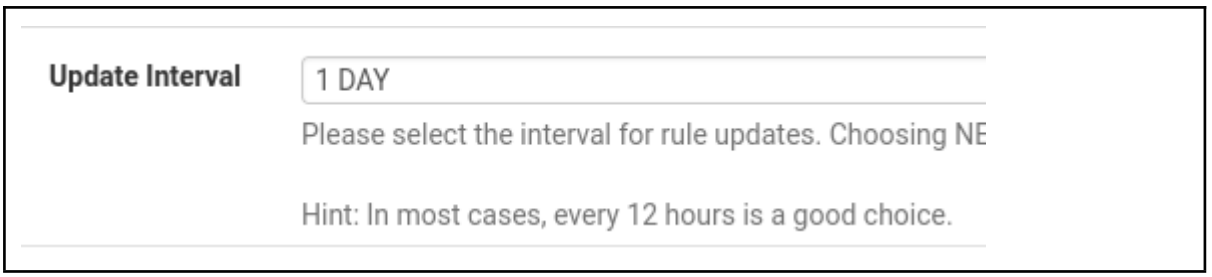


SURICATA NA PAS BESOIN DE CE CODE

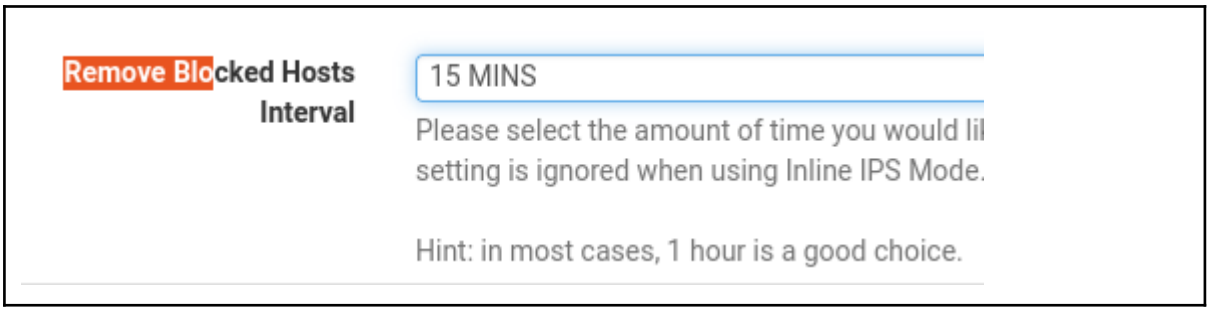
Cocher aussi les cases suivantes :
• Enable ET Open ;
• Enable OpenAppID ;
• Enable RULES OpenAppID ;
• Hide Deprecated Rules Category.

avec suricata, on peut que activer et open et hide deprecated rules category

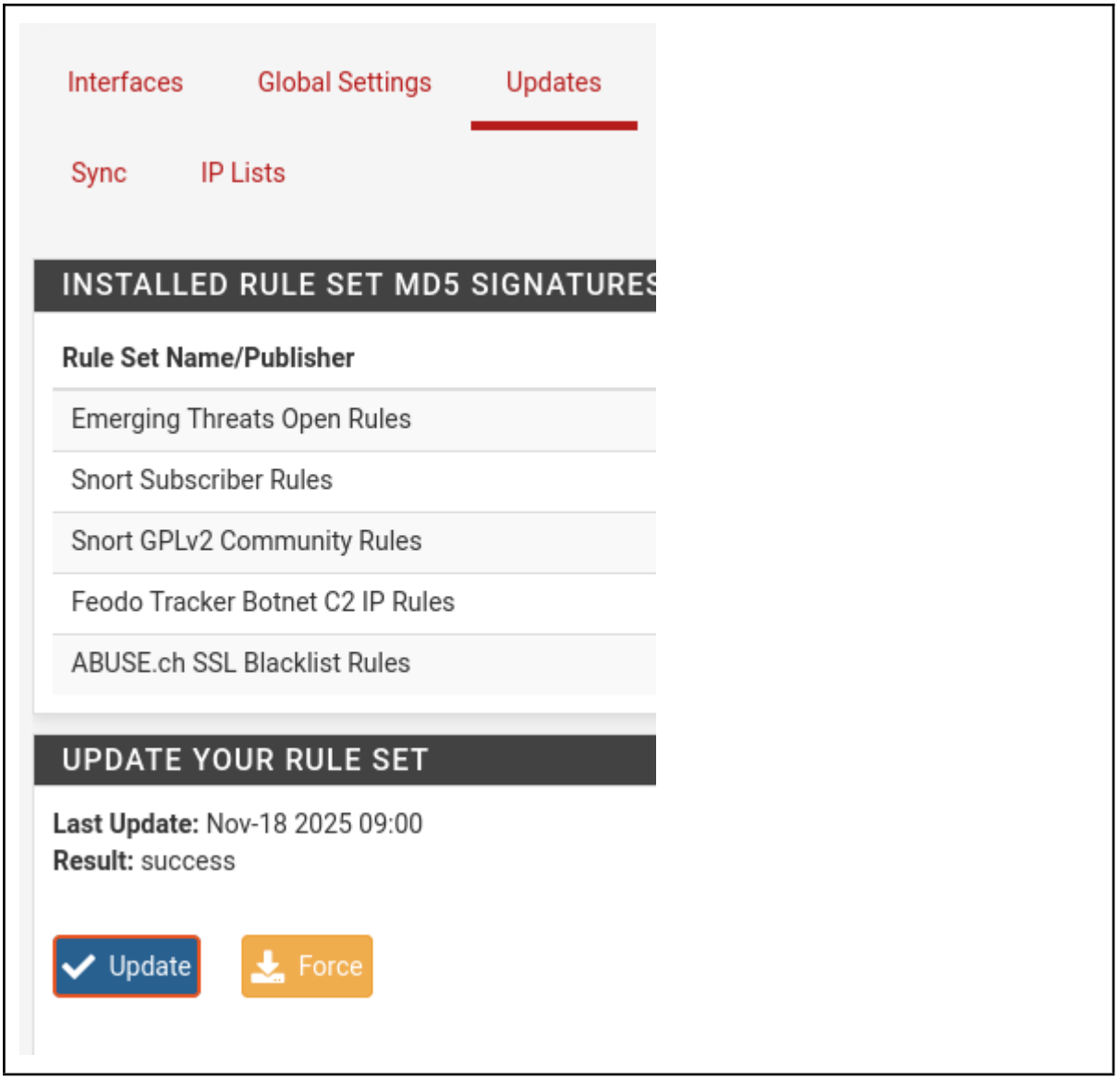
Update interval 1 day :



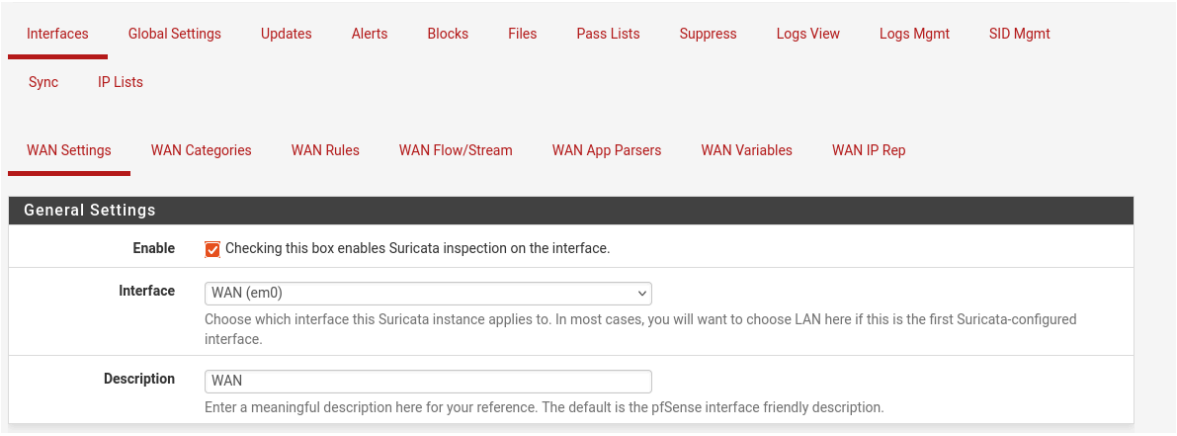
Ensuite, :



Et après on va update les rules :

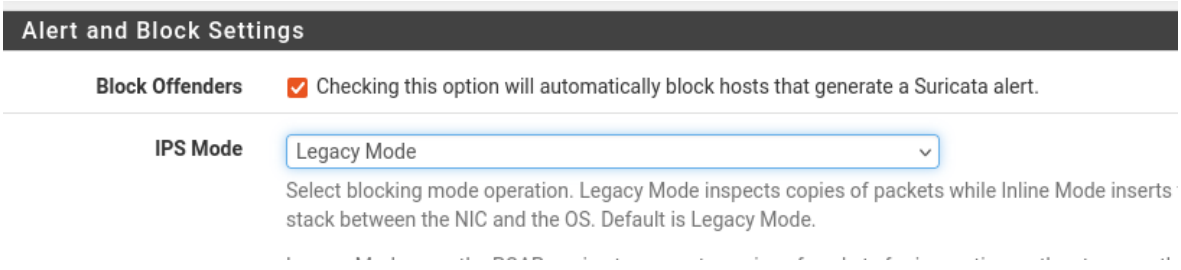


Ensuite, cliquer sur l'onglet Snort Interfaces puis sur le bouton Add. Nous allons configurer une protection de l'interface WAN afin de prévenir les attaques extérieures. Nous pourrions faire de même avec les attaques internes en configurant une protection de l'interface CLIENTS par exemple.
Dans la liste déroulante, choisir l'interface WAN.
De nouveaux onglets sont disponibles.



Les nouveaux onglets portent maintenant le nom de l'interface WAN.
Dans l'onglet Wan Preprocs, activer la case à cocher Auto Rules Disable. Puis, toujours dans cet onglet,dans la rubrique Application ID Detection, cocher la case Enable. Et dans la rubrique Portscan Detection,activer aussi la case Enable. Cliquer enfin sur le bouton Save en base de la page.
Revenir ensuite dans l'onglet WAN settings et cocher la case Block Offenders afin de configurer snort en mode IPS.

On ne peut que activer cette option avec suricata (dans l'onglet general):



Depuis la machine physique du lycée :
Afin de tester la fonction IPS de snort, nous allons tenter un scan de port avec nmap depuis l'extérieur en ciblant l'interface WAN.
Depuis la machine physique, lancer un scan sur l'interface WAN du pare-feu. Il faut auparavant relever
l'adresse IP de cette interface. Puis, depuis un terminal, lancer la commande suivante :

```
nmap -sS -A <adresse-ip-interface-wan>
```

```
root@archa:/home/test# nmap -sS -A 172.17.123.79
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-18 09:10 CET
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 172.17.123.79
Host is up (0.00024s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  (generic dns response: REFUSED)
1 service unrecognized despite returning data. If you know the service/version, please submit the followi
SF-Port53-TCP:V=7.80%I=7%D=11/18%Time=691C29F7%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0")%r(DNSStatus
SF:RequestTCP,E,"\0\x0c\0\0\x90\x05\0\0\0\0\0\0\0");
MAC Address: 08:00:27:5B:A9:60 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.24 ms 172.17.123.79

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.10 seconds
```



emerging-scan.rules

WAN Categories

Penser à activer cette option dans

172.17.123.23 11/18/2025 09:20:00 ET SCAN Suspicious inbound to mySQL port 3306