

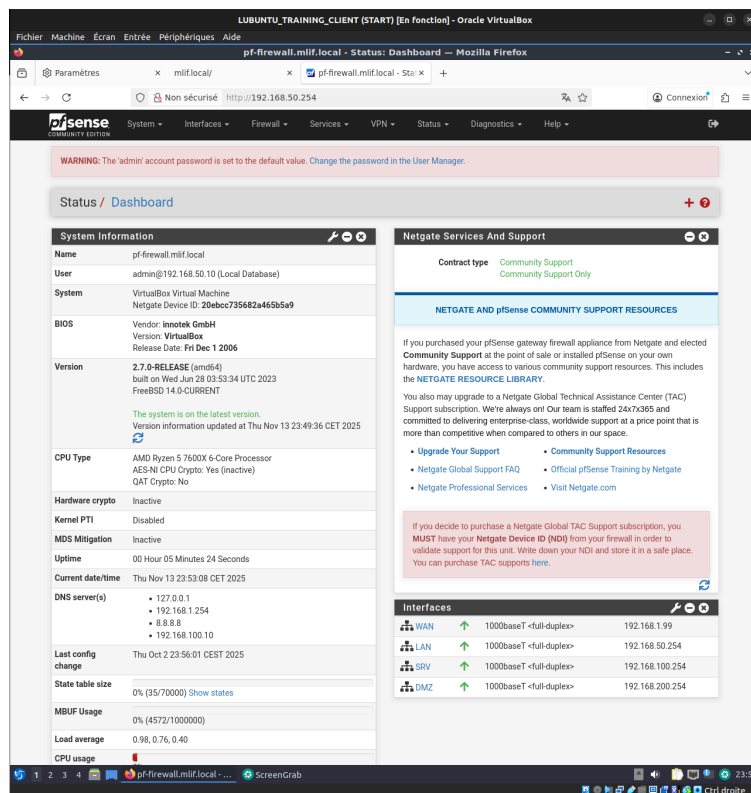
LAB3-B3-UTM (squid)

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

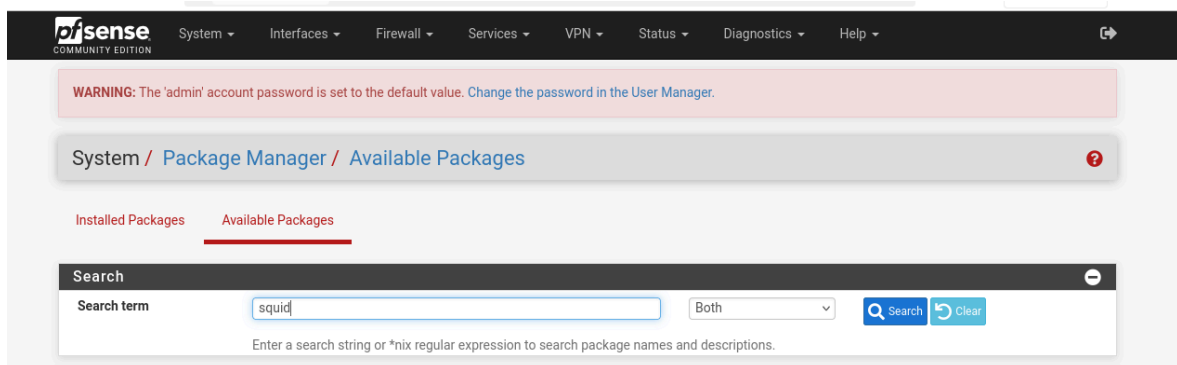
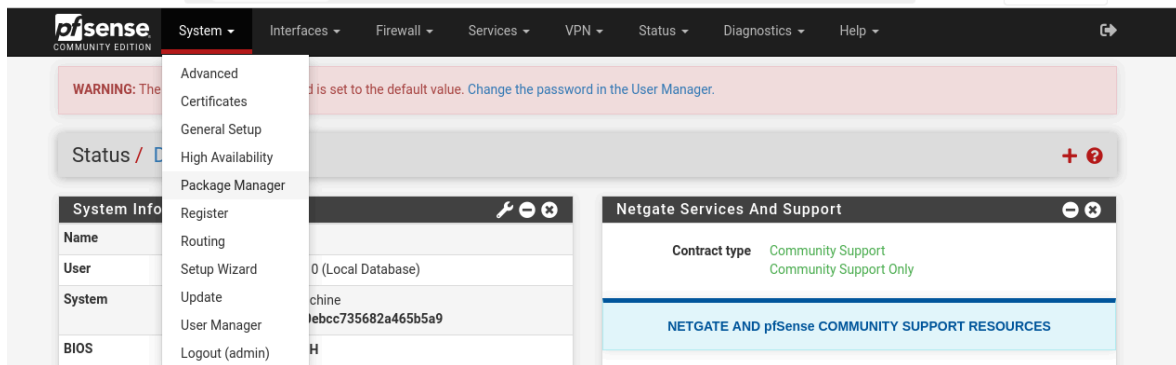


3.1°) Installation des packages squid et squidguard

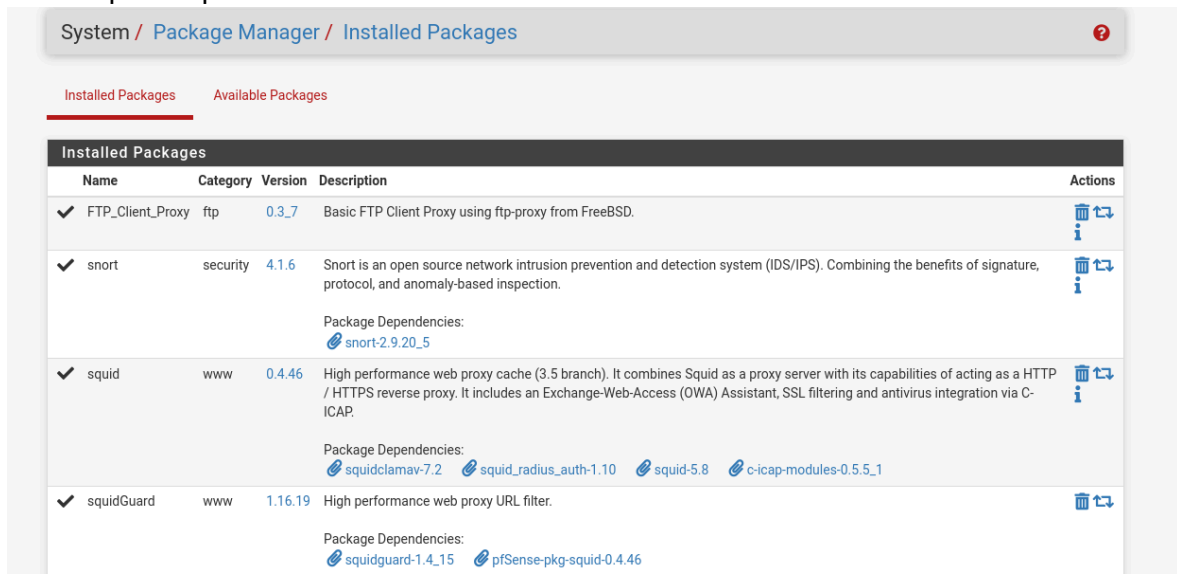
On vas maintenant procéder à l'installation des paquet squid et squidguard, pour cela il faut se rendre sur la DEBIAN_TRAINING_CLIENT, puis se connecter à la page de configuration du pare-feu :



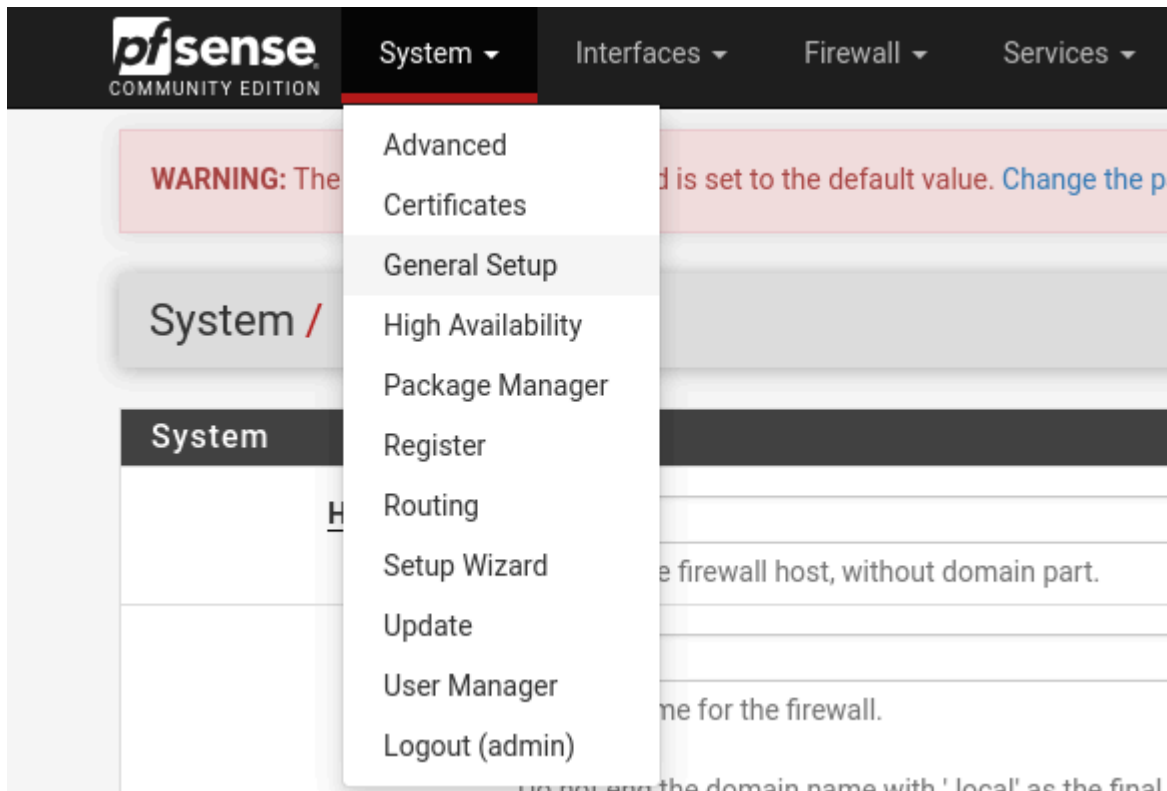
Une fois connecter se rendre dans **System Package > Manager Available Package > rechercher "squid"**



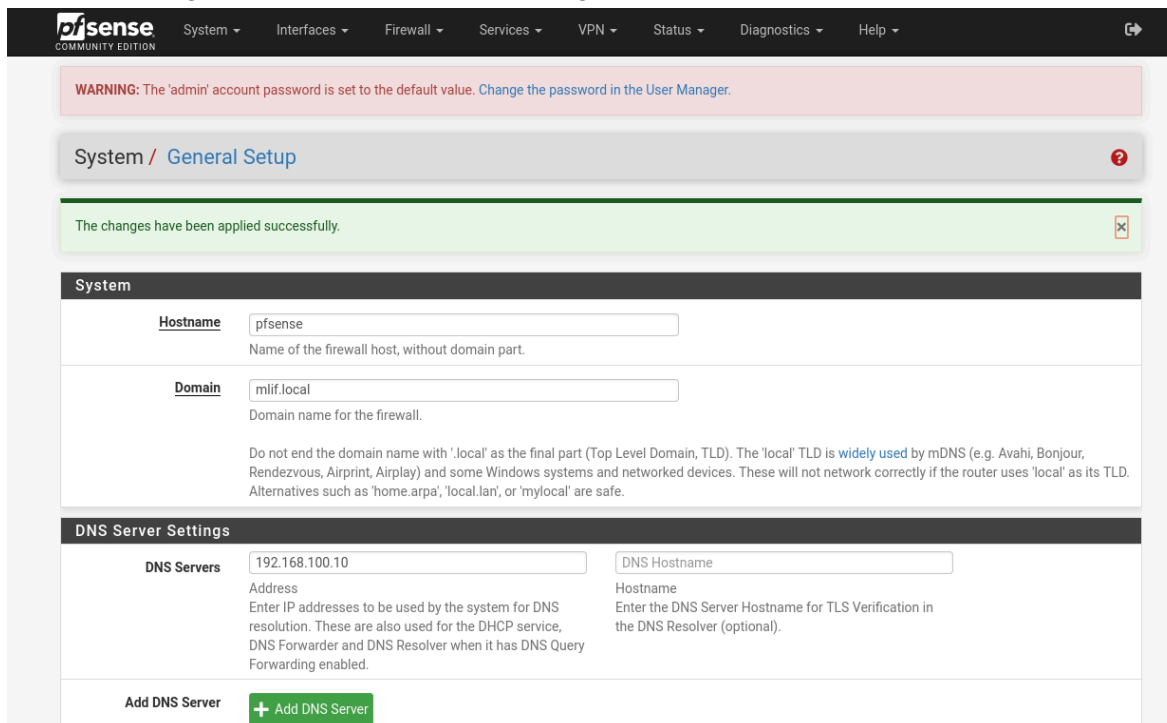
Une fois que je clique sur installer, je me rend sur la page " Installed Package" afin de vérifier que les packet se soit correctement installer :



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



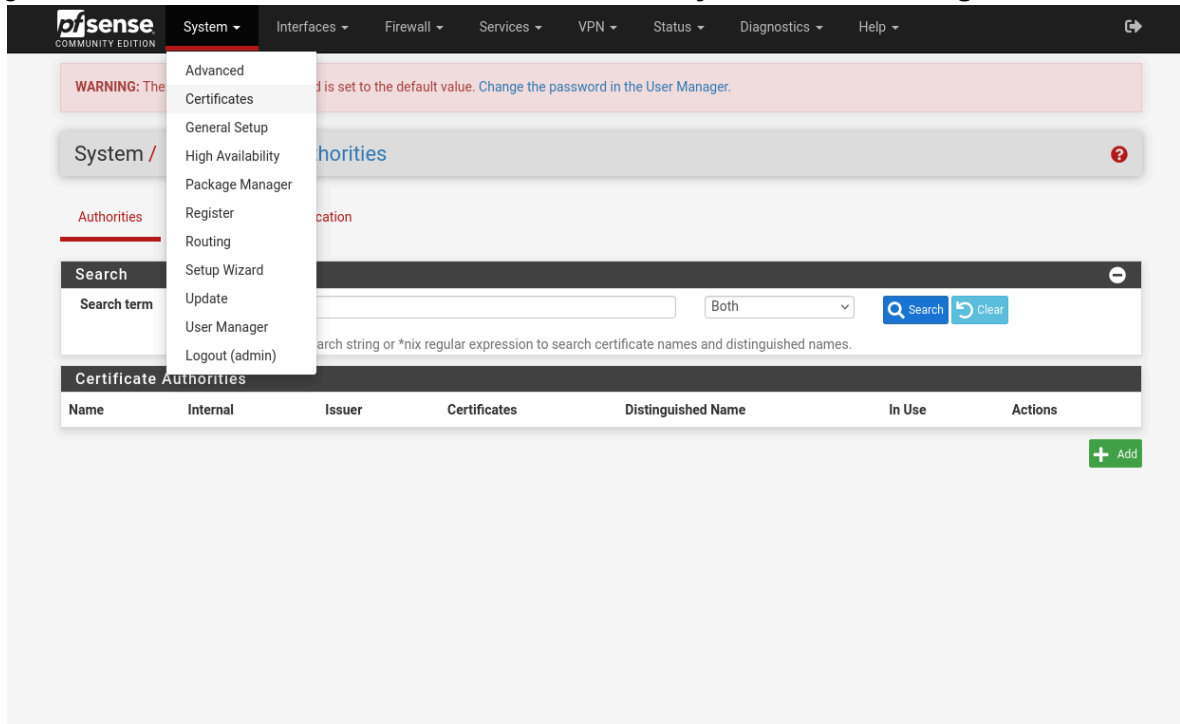
Dans cette onglet on vas procéder à la configuration du dns ainsi que du nom de l'hôte.



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” :

Create / Edit CA

Descriptive name
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ', "

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

Common Name
The following certificate authority subject components are optional and may be left blank.

Country Code

State or Province

City

Organization

Organizational Unit

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

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CAMLIF	✓	self-signed	0	ST=IDF, OU=CA, O=MLIF, L=PARIS, CN=internal-ca, C=FR ⓘ Valid From: Fri, 14 Nov 2025 00:10:12 +0100 Valid Until: Mon, 12 Nov 2035 00:10:12 +0100		

+ Add

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.

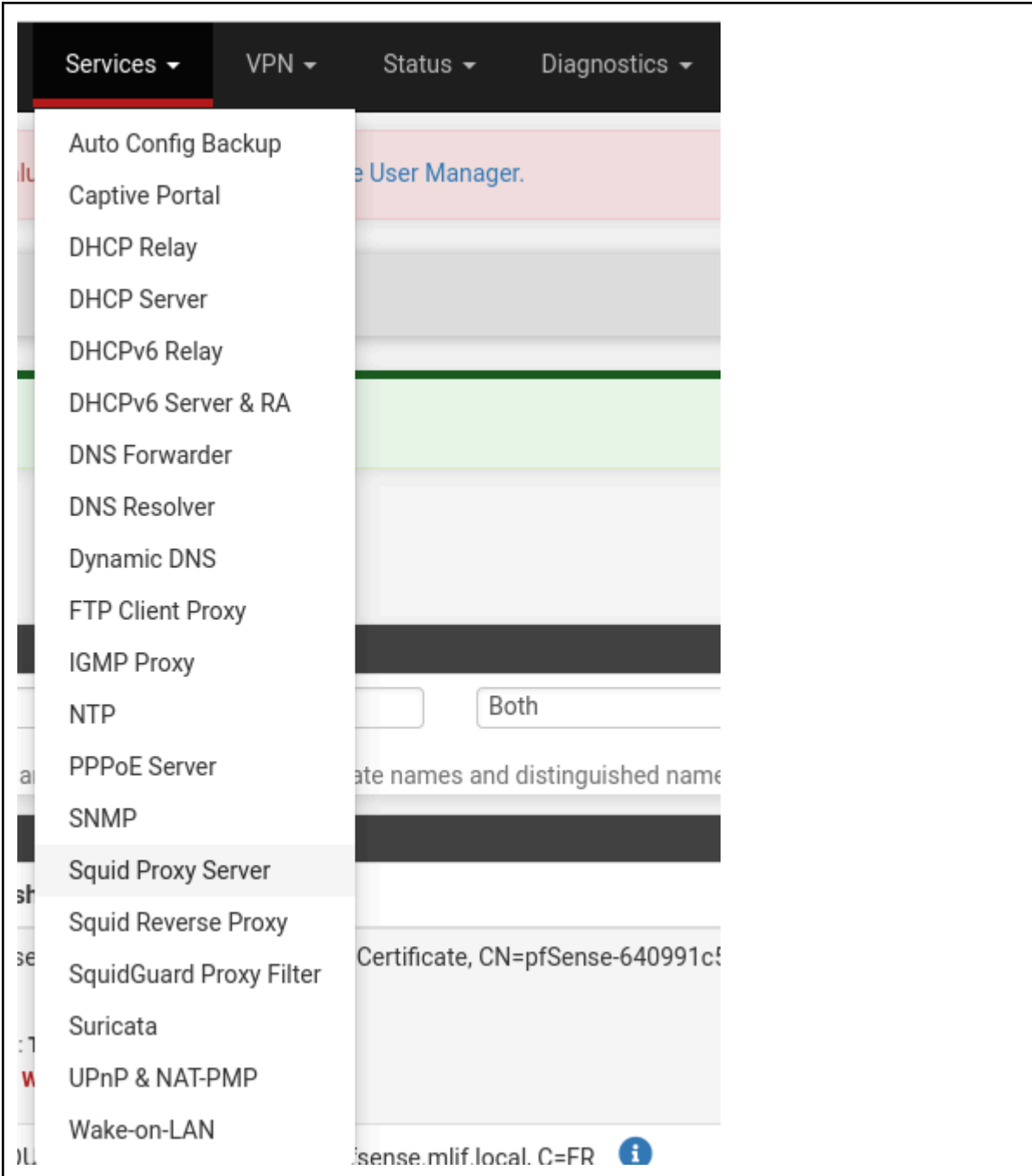
Il faudra laisser tout les paramètres par défaut sauf les paramètres suivant :

<u>Descriptive name</u>	<input type="text" value="Certificat du serveur MLIF"/>
	<small>The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '</small>
	<small>Server certificates should not have a lifetime over 398 days or some platforms may c</small>
<u>Common Name</u>	<input type="text" value="pfsense.mlif.local"/>
<u>Certificate Type</u>	<input type="text" value="Server Certificate"/>
	<small>Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.</small>

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**.



The image shows a screenshot of the pfSense web interface. At the top, there is a navigation bar with four tabs: "Services", "VPN", "Status", and "Diagnostics". The "Services" tab is currently selected and highlighted with a red underline. A dropdown menu is open from the "Services" tab, listing various services. The "Squid Proxy Server" option is highlighted in a light grey color. Other visible options in the menu include Auto Config Backup, Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server & RA, DNS Forwarder, DNS Resolver, Dynamic DNS, FTP Client Proxy, IGMP Proxy, NTP, PPPoE Server, SNMP, Squid Reverse Proxy, SquidGuard Proxy Filter, Suricata, UPnP & NAT-PMP, and Wake-on-LAN. The background of the interface is partially visible, showing a "User Manager" section and a "Both" button.

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

General Remote Cache **Local Cache** Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

Squid Cache General Settings

Disable Caching Disable caching completely.
This may be required if Squid is only used as a proxy to audit website access.

Cache Replacement Policy Heap LFUDA
The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. **Default:** heap LFUDA ⓘ

Low-Water Mark in % 90
The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm. ⓘ

High-Water Mark in % 95
The high-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm. ⓘ

Do Not Cache

Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line.

Enable Offline Mode Enable this option and the proxy server will never try to validate cached objects.
Offline mode gives access to more cached information than normally allowed (e.g., expired cached versions where the origin server should have been contacted otherwise).

External Cache Managers
Enter the IPs for the external **Cache Managers** to be granted access to this proxy. **Separate entries by semi-colons (;)**

Squid Hard Disk Cache Settings

Hard Disk Cache Size 100
Amount of disk space (in megabytes) to use for cached objects.

3.3.2°) Configuration générale

On va 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 :

Squid General Settings

Enable Squid Proxy Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Listen IP Version IPv4
Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP none
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.
Important: Don't forget to generate Local Cache on the secondary node and configure **XMLRPC Sync** for the settings synchronization.

Proxy Interface(s) WAN LAN SRV DMZ
The interface(s) the proxy server will bind to. **Use CTRL + click to select multiple interfaces.**

Outgoing Network Interface Default (auto)
The interface the proxy server will use for outgoing connections.

Proxy Port 3128
This is the port the proxy server will listen on. **Default: 3128**

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:

The screenshot shows the 'SSL Man In the Middle Filtering' configuration page. It includes the following settings:

- HTTPS/SSL Interception:** Enable SSL filtering.
- SSL/MITM Mode:** Splice All. A dropdown menu is shown with 'Splice All' selected. Below it, a note states: 'The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. Click Info for details.' with an information icon.
- SSL Intercept Interface(s):** A list box containing 'WAN', 'LAN', 'SRV', and 'DMZ'. Below it, a note states: 'The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.'
- SSL Proxy Port:** 3129. Below it, a note states: 'This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129'

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 :

The screenshot shows the 'CA' configuration section. It includes the following settings:

- CA:** CAMLIF. A dropdown menu is shown with 'CAMLIF' selected. Below it, a note states: 'Select Certificate Authority to use when SSL interception is enabled.' with an information icon.

3.3.4°) Proxy transparent via WPAD

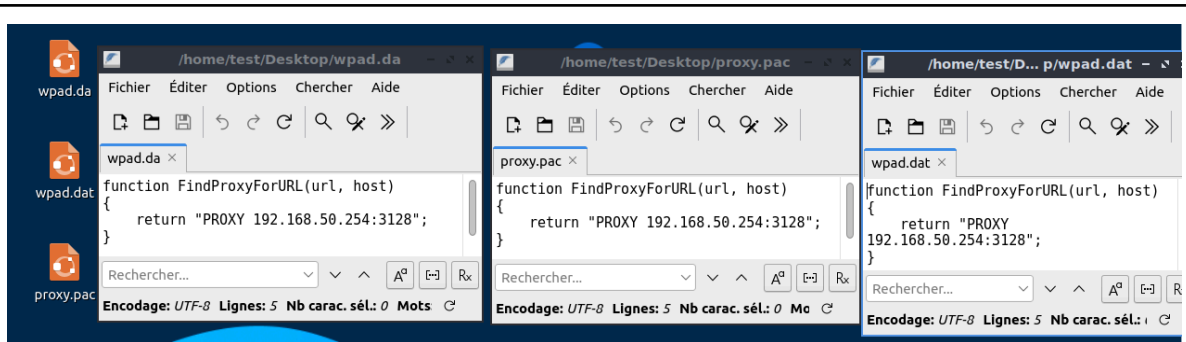
Nous devons maintenant configurer le proxy en **mode transparent**. Avec ce mode, les navigateurs des machines clientes n'auront plus besoin d'indiquer manuellement l'adresse du proxy : tout sera détecté automatiquement.

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 :

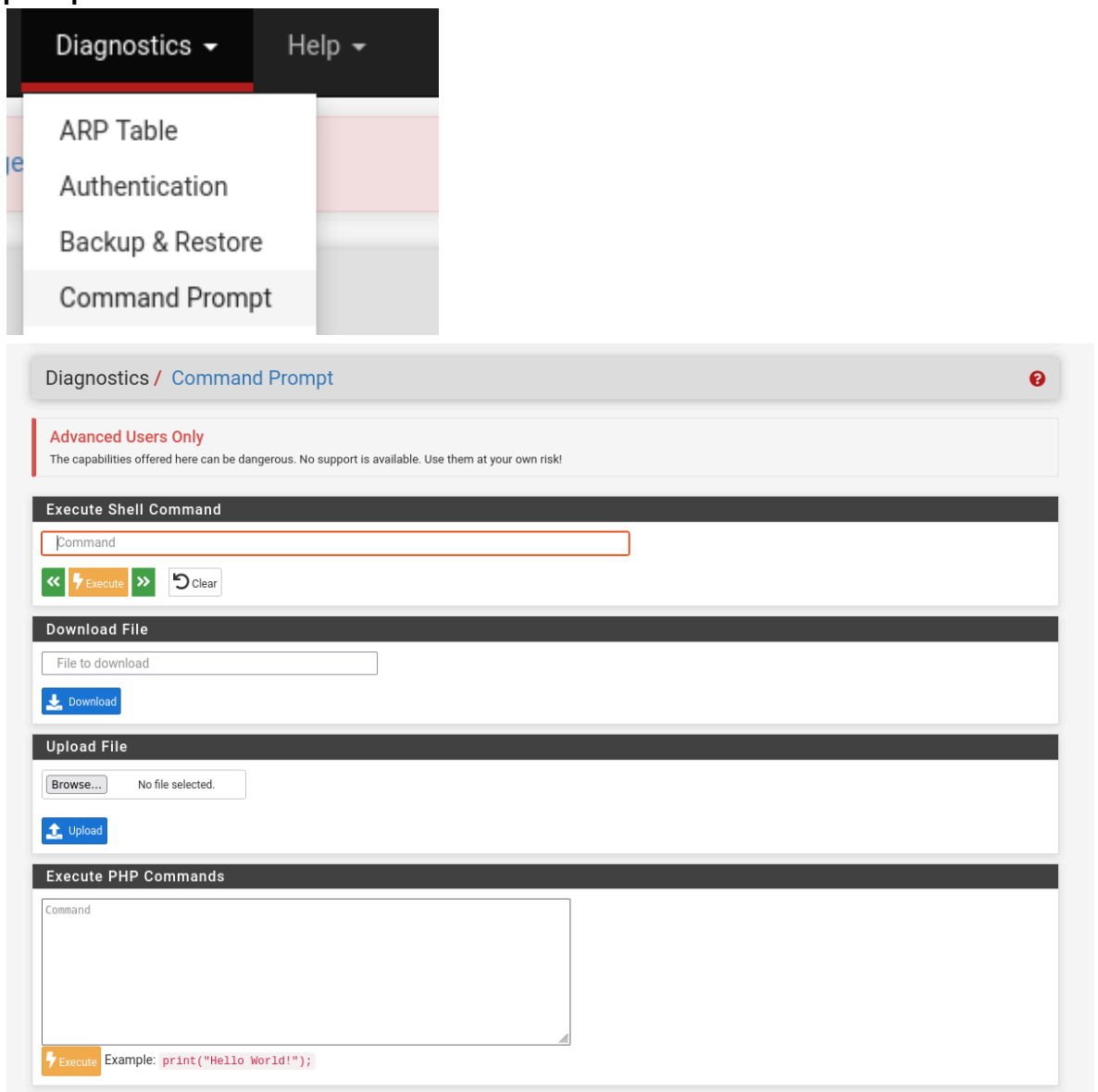
- wpad.dat ;
- wpad.da ;
- proxy.pac ;

Les 3 fichiers posséderont le même contenu :



Une fois les trois fichiers créés, il nous faudrait 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 :

Uploaded file to /tmp/wpad.dat.

Upload File

Browse...

wpad.da

Upload

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**" :

Execute Shell Command

```
mv /tmp/wpad.dat /usr/local/www
```

Execute Clear

Shell Output - mv /tmp/wpad.dat /usr/local/www

Execute Shell Command

Shell Output - mv /tmp/wpad.da /usr/local/www

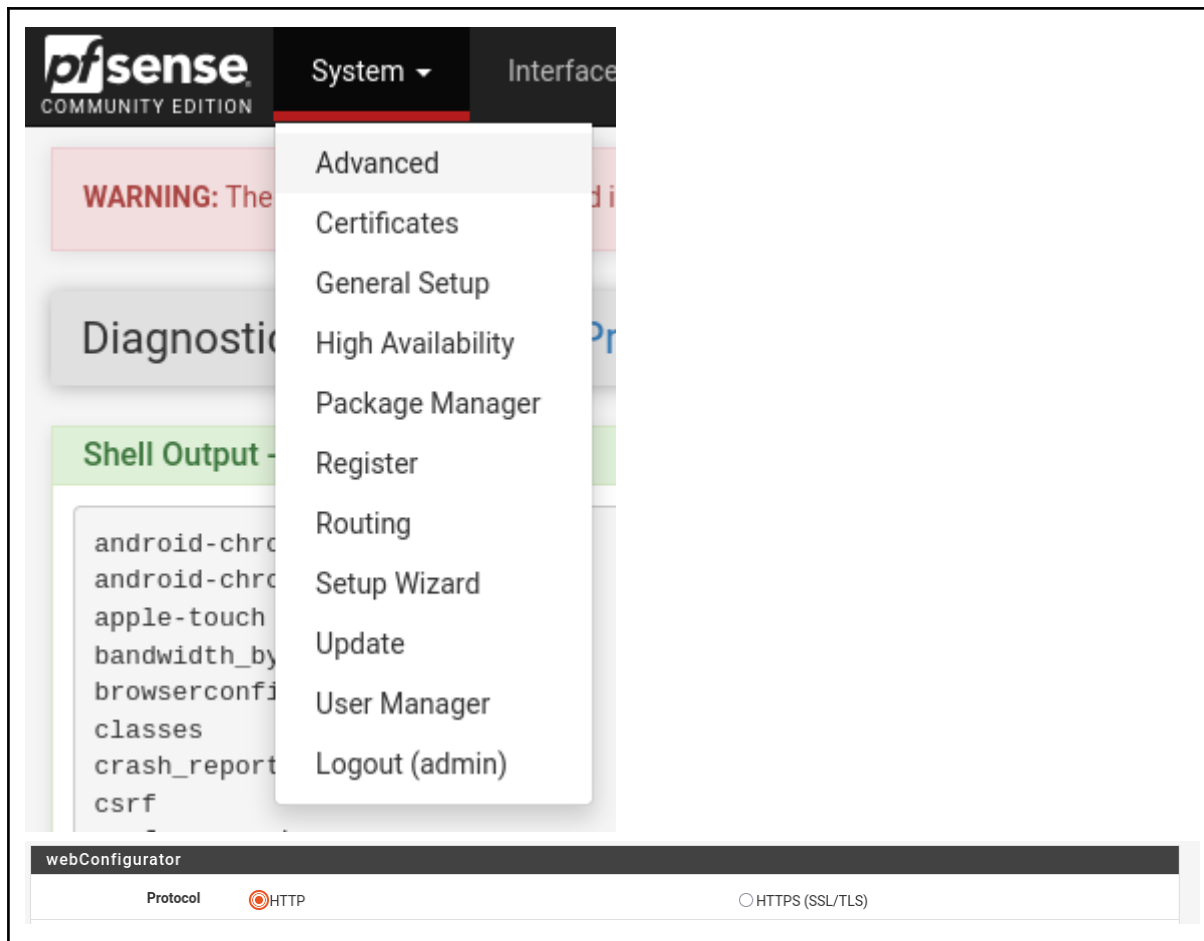
```
mv: rename /tmp/wpad.da to /usr/local/www/wpad.da: No such file or directory
```

Shell Output - mv /tmp/proxy.pac /usr/local/www

Execute Shell Command

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”**

```

GNU nano 7.2 /var/lib/bind/db.mlif.local
; BIND data file pour zone directe.
$TTL 604800
@ IN SOA messagelab.mlif.local. root.mlif.local. (
    11 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS messagelab.mlif.local.
@ IN MX 10 mail.mlif.local.
messagelab IN A 192.168.100.10
mail IN A 192.168.100.20
pfsense IN A 192.168.50.254
toip IN A 192.168.100.40
backup IN A 192.168.100.50
wpad IN A 192.168.50.254
cdp IN A 192.168.100.30
www IN A 192.168.200.5
srv-web-bis-ayoub IN A 192.168.200.52
srv-web-ayoub IN A 192.168.200.51

imap IN CNAME mail.mlif.local.
smtp IN CNAME mail.mlif.local.
sitea IN CNAME www.mlif.local.
siteb IN CNAME www.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 enregistre 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.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/2.07 MIB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
<input checked="" type="checkbox"/>	18/88.89 MIB	IPv4 *	*	*	*	*	*	none		
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

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 :

```
test@client-mlif: ~
Fichier Actions Éditer Vue Aide
test@client-mlif: ~
test@client-mlif:~$ wget www.cisco.com
--2025-11-14 01:08:18-- http://www.cisco.com/
Resolving www.cisco.com (www.cisco.com)... failed: Temporary failure in name resolution.
wget: unable to resolve host address 'www.cisco.com'
test@client-mlif:~$ wget www.free.com
--2025-11-14 01:12:21-- http://www.free.com/
Resolving www.free.com (www.free.com)... failed: Name or service not known.
wget: unable to resolve host address 'www.free.com'
```

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 :

Paramètres de connexion ×

Configuration du serveur proxy pour accéder à Internet

Pas de proxy

Détection automatique des paramètres de proxy pour ce réseau

Utiliser les paramètres proxy du système

Configuration manuelle du proxy

Proxy HTTP Port

Utiliser également ce proxy pour HTTPS

Proxy HTTPS Port

Hôte SOCKS Port

SOCKS v4 SOCKS v5

Adresse de configuration automatique du proxy

Actualiser

Pas de proxy pour

Exemples : .mozilla.org, .asso.fr, 192.168.1.0/24
Les connexions à localhost, 127.0.0.1/8 ou ::1 ne passent jamais par un proxy.

Ne pas me demander de m'authentifier si le mot de passe est enregistré

Utiliser un DNS distant lorsque SOCKS v4 est actif

Utiliser un DNS distant lorsque SOCKS v5 est actif

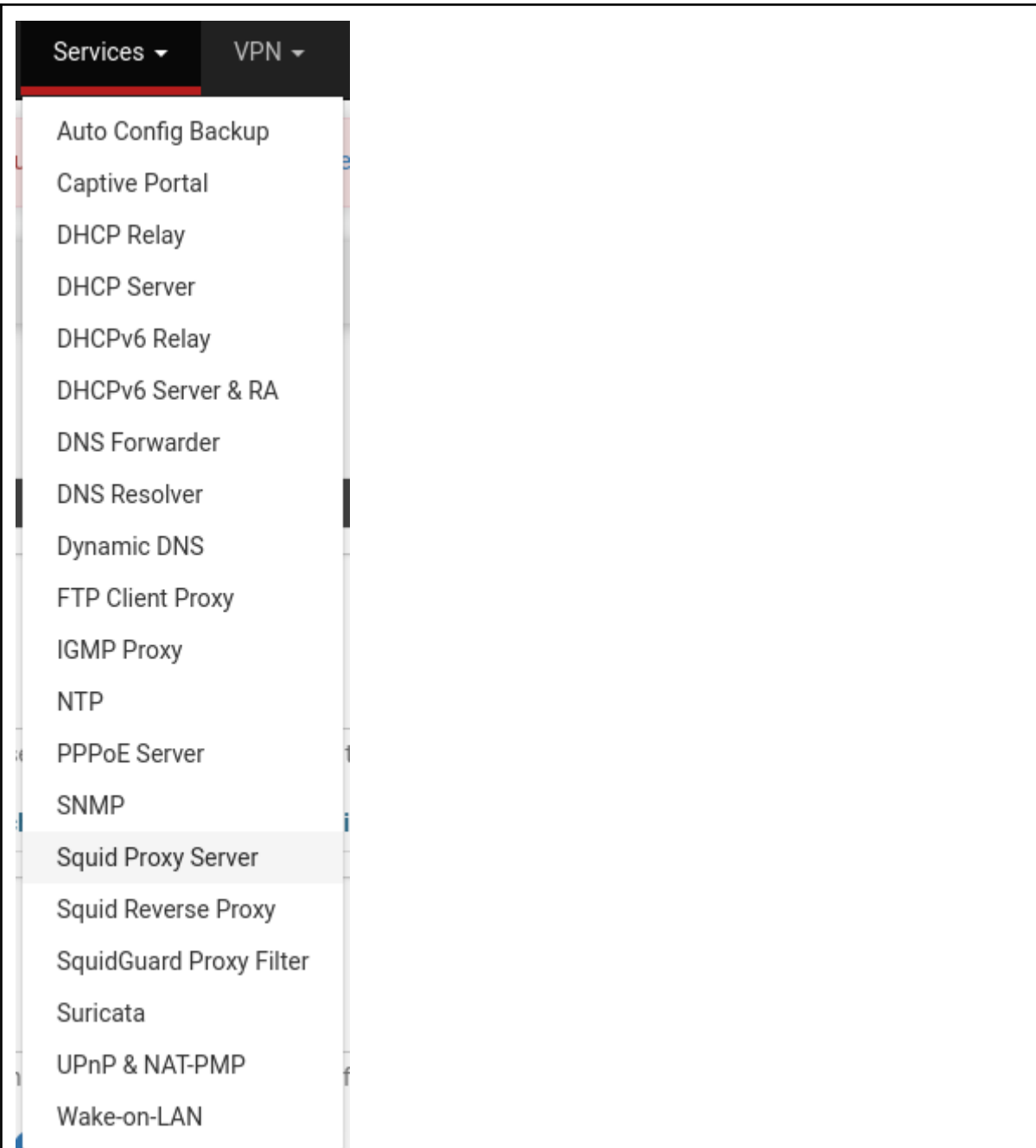
Annuler OK

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

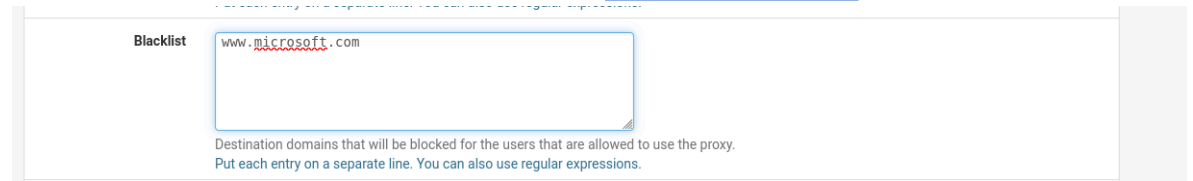
3.3.7°) Test de la configuration

Nous devons maintenant configurer Squid pour bloquer les sites du domaine microsoft.com.

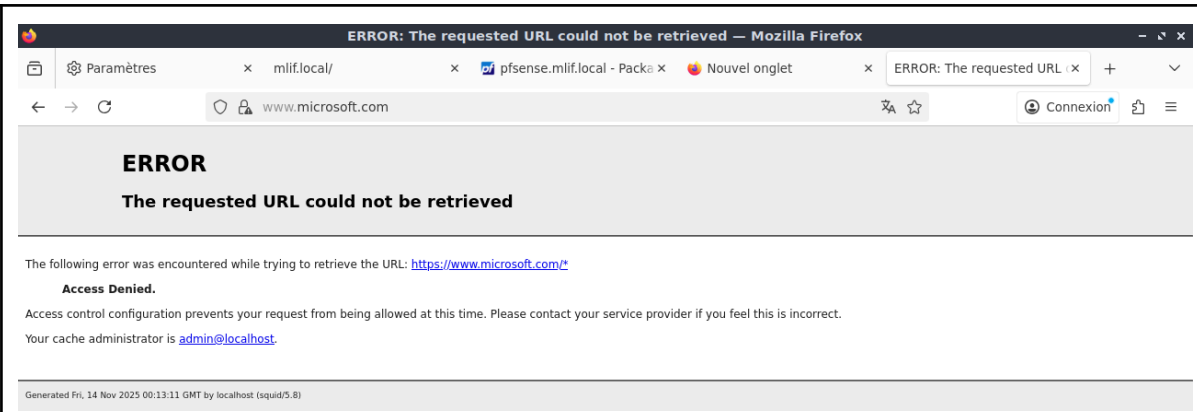
Pour cela, il suffit d'ouvrir l'onglet **ACLs dans Squid**, d'ajouter microsoft.com dans la zone Blacklist, puis de valider. Enfin, il faut fermer et rouvrir le navigateur pour appliquer le filtrage. Au chemin "**Service > Squid Proxy Server**"



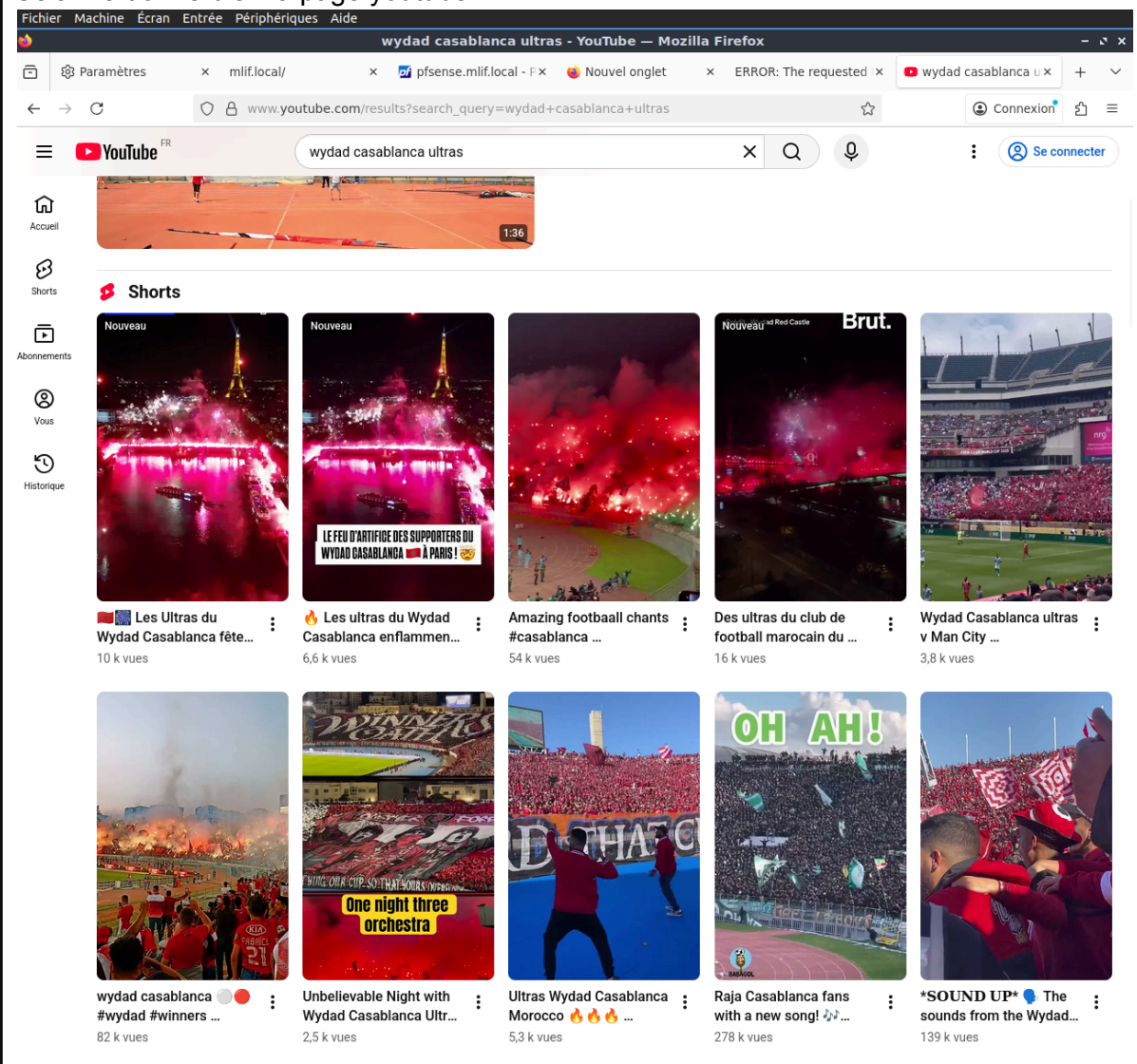
Puis dans blacklist entrer le site de microsoft "www.microsoft.com"



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](https://www.youtube.com)
Cela me donne bien la page youtube.



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

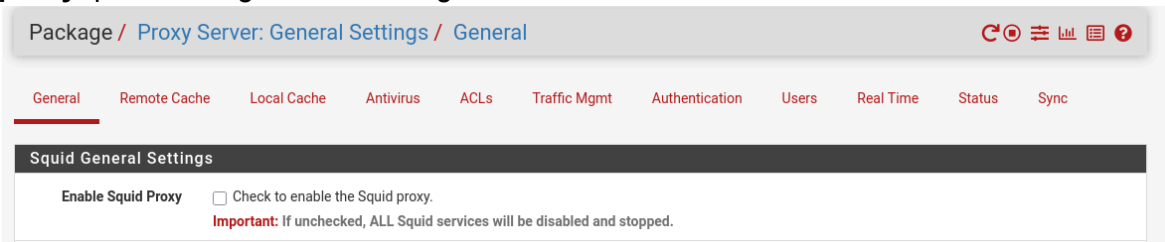


STOP 1 : Appelez moi pour que je puisse vérifier cette partie du travail

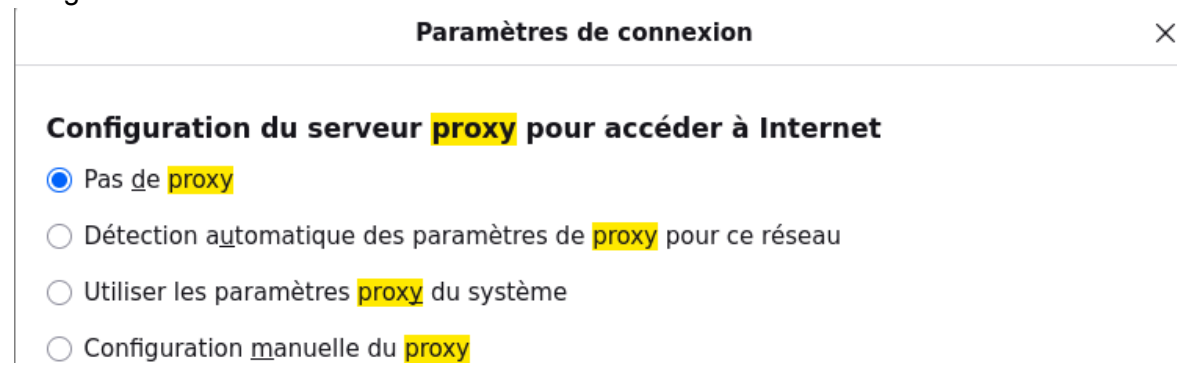
3.4°) Filtrage avancé avec squidguard

3.4.1°) Configuration de squidguard

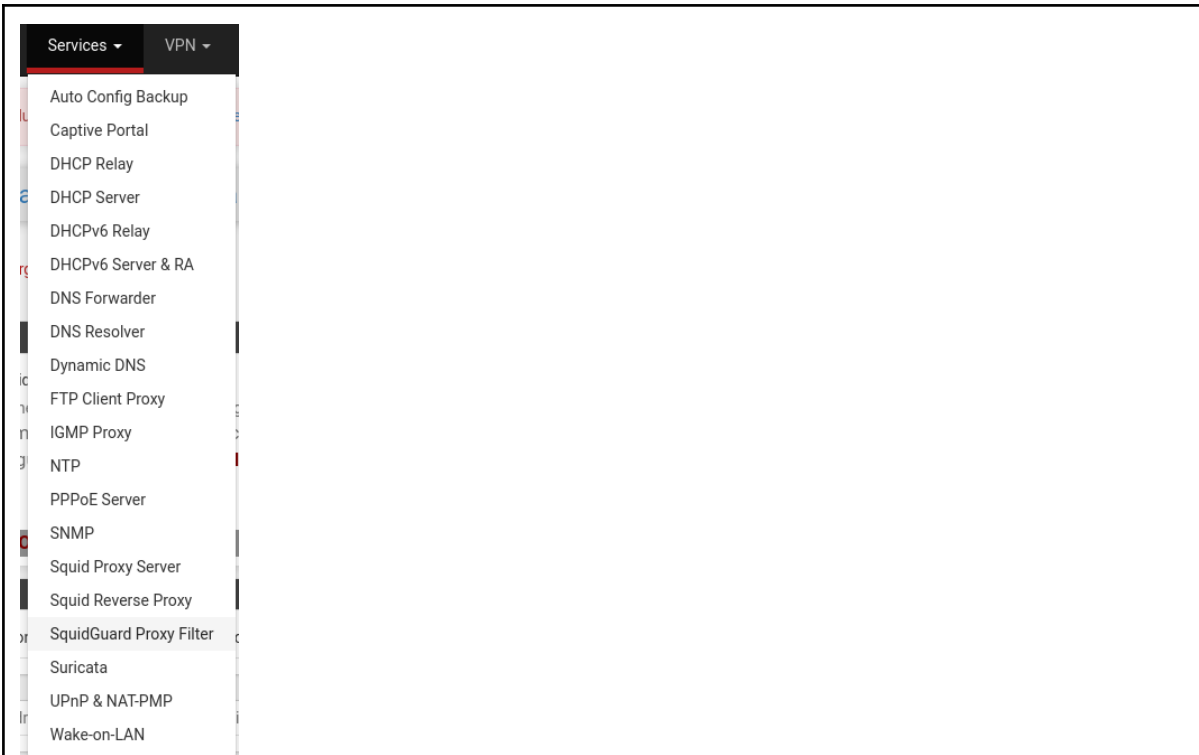
Depuis le navigateur d'administration, nous devons désactiver le service Squid. Pour cela, il suffit d'ouvrir **Services > Squid Proxy Server**, de **décocher l'option d'activation du proxy**, puis d'enregistrer les changements.



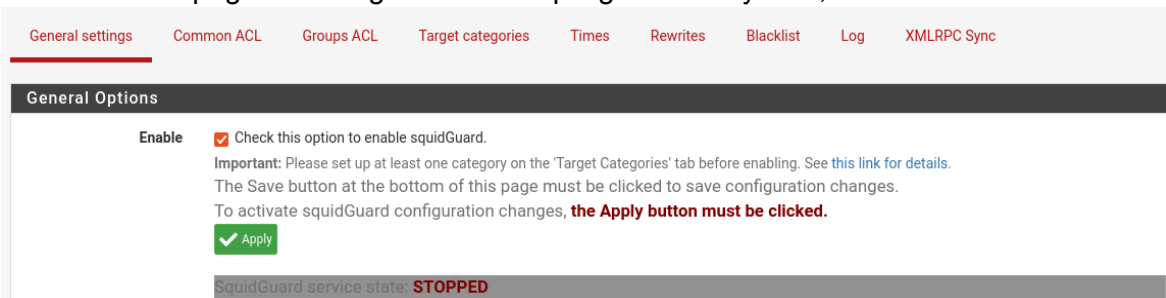
Nous devons ensuite modifier les paramètres du navigateur pour désactiver l'utilisation du proxy. Il suffit de sélectionner l'option Pas de proxy dans la configuration réseau du navigateur.



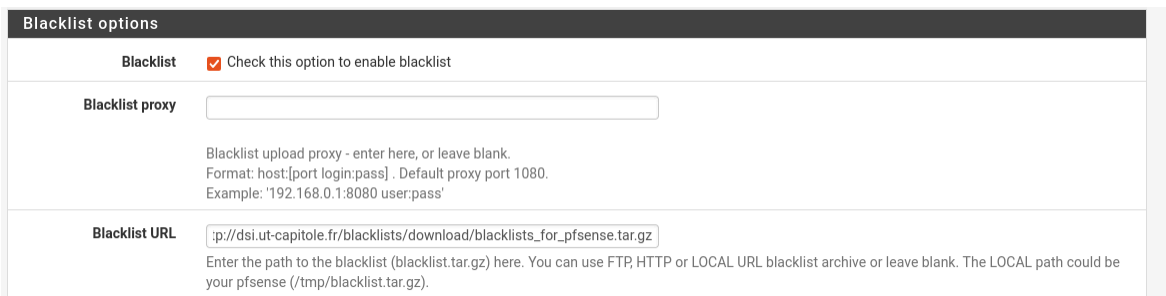
Nous devons maintenant activer le filtre SquidGuard. Pour cela, il suffit d'ouvrir **Services > SquidGuard Proxy Filter**, puis de **cocher l'option d'activation dans l'onglet General Settings**.



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 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.



WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / Suricata / Blocked Hosts

Sync IP Lists

Blocked Hosts Log View Settings

Save or Remove Hosts

All blocked hosts will be saved

All blocked hosts will be cleared

Save Settings

Save auto-refresh and view settings

Refresh

Default is ON

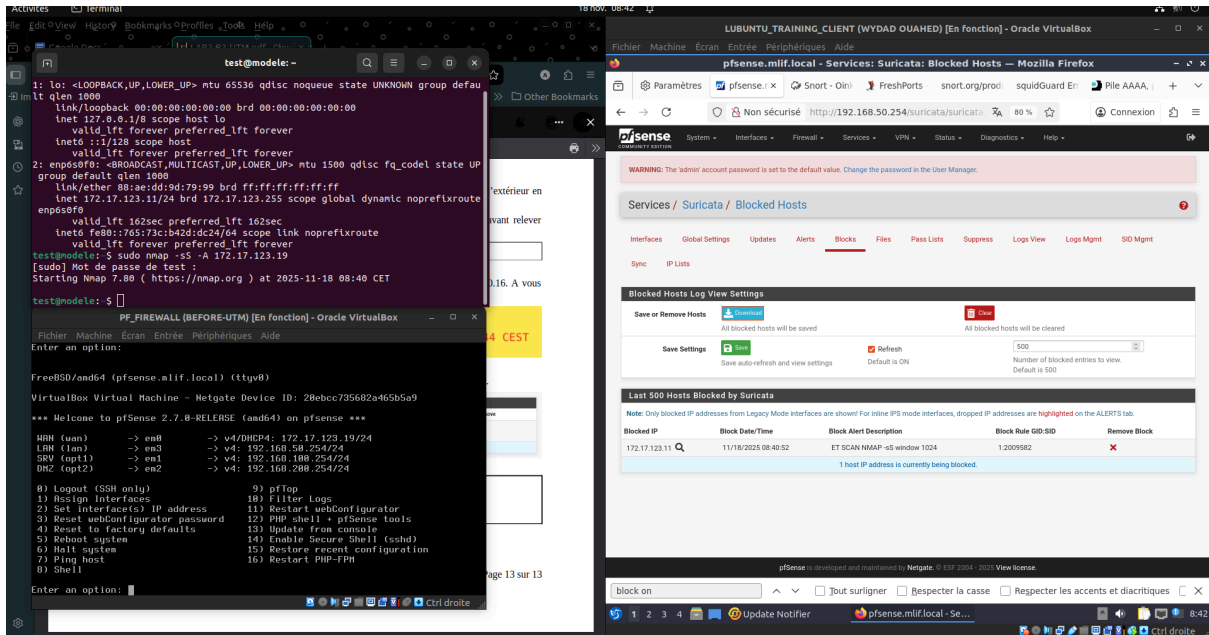
Number of blocked entries to view. Default is 500

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.



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.