ADRAR FORMATION

Mis en place d'un Proxy

MARAVAL Liam
07/10/2024

Ce document sera décomposé en plusieurs chapitres :

1.Contexte : Définition des besoins ainsi que le choix des solutions en réponse à la demande client.
2.Configuration technique : Procédure technique de mise en place des solutions
3. Conclusion
4. Annexes

Table des matières

1. Contexte

1.1 Demandes du client

Nous avons été sollicités par l'ADRAR pour concevoir et déployer une solution de Proxy destinée à sécuriser les accès Internet sur leur site.
La gestion des droits d'accès à certains sites se fera en fonction du groupe LDAP auquel appartient l'utilisateur pour le personnel du centre de formation et des stagiaires.

En plus de la gestion des droits, nous sommes chargés de mettre en place une solution de conservation des accès Internet comme le prévoit la loi pour tout organisme fournissant un accès Internet public.

Les utilisateurs seront répartis dans 3 groupes :

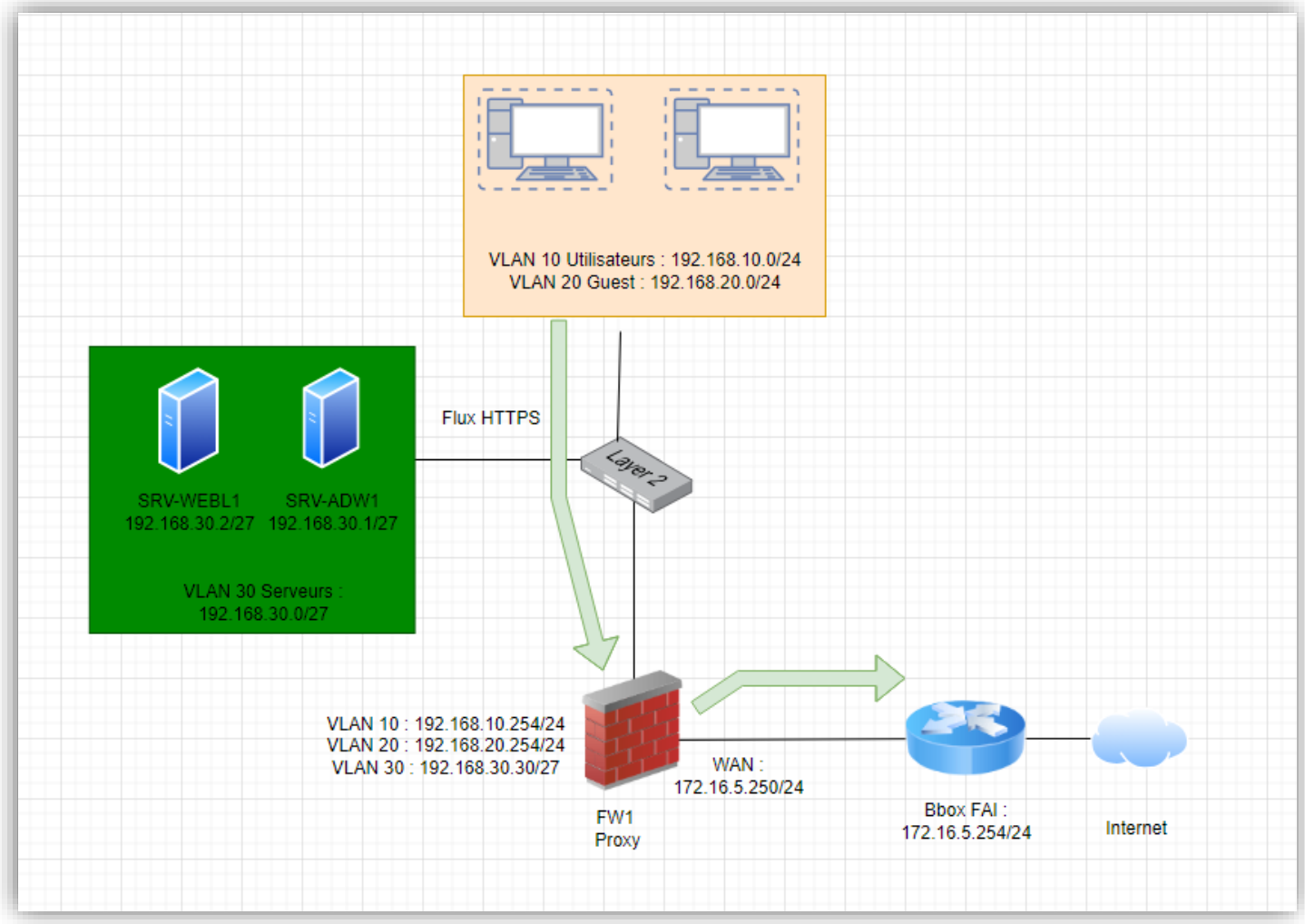
- Administration : pour les employés de l'ADRAR
- Formation : pour les stagiaires
- Guest : pour des utilisateurs externes
  - Le personnel administratif aura accès à tous les sites internet, sauf ceux inclus dans la blacklist « Adultes » ains que « Shopping » de UT1.
  - Les stagiaires n'auront pas accès aux sites : réseaux sociaux + jeux + sites pour adultes de la blacklist UT1.
  - Les Guest devront passer par un portail captif en se connectant à un navigateur Web, et n'auront accès qu'à un nombre de sites limités

Voici l'infrastructure en place actuellement :

- 3 Réseaux distincts :
  - Un réseau **« Utilisateurs »**
  - Un réseau **« Guest »**
  - Un réseau **« Serveurs »**
- Un serveur AD avec un domaine adrar.local
- Un serveur DHCP
- Un pare feu Pfsense

1.2 Evolution de l'infrastructure

Pour mieux comprendre la mise en place de la nouvelle infrastructure, veuillez-vous référer au nouveau schéma effectué :

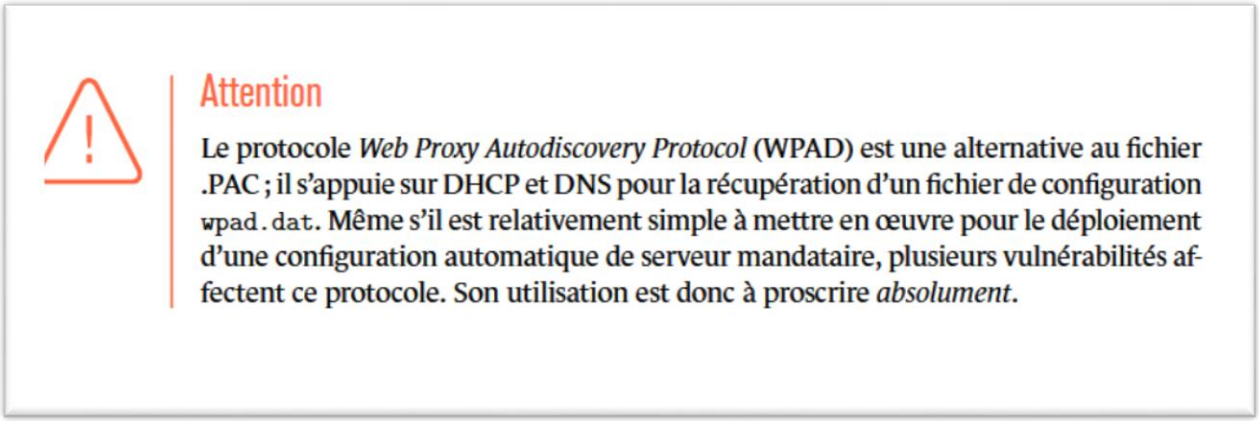


Afin de répondre à la demande de l'ADRAR, nous allons déployer un Proxy sur le PfSense déjà en place.
Ce service remplira plusieurs fonctions essentielles :

- Agir en tant qu'intermédiaire entre les requêtes Web clientes et les serveurs Web externes
- Anonymiser les IP clientes
- Effectuer un filtrage des flux Web
- Mettre en cache les données afin d'améliorer les performances
- Journaliser les activités via des fichiers de logs.

Pour répondre aux exigences de sécurité et de protection des données des utilisateurs conformément au RGPD, le proxy sera configuré de manière stricte et explicite.
De plus, nous souhaitons améliorer la sécurité en mettant en place du filtrage Web via des groupes AD, ce qui peux être implémenté uniquement via un Proxy explicite.

Afin de déployer notre configuration, une GPO sera mise en place sur notre Active Directory pour forcer l'utilisation du Proxy dans le navigateur Firefox, celui-ci étant imposé sur les postes utilisateurs.
Nous avons choisi cette solution car le déploiement des configurations via DHCP/DNS et WPAD n'est pas envisageable car proscrit par l'ANSSI (lien du document en Annexes).



Pour rappel, une charte informatique devra être à faire signer pour les utilisateurs avec une rubrique les informant de l'utilisation du proxy.

Concernant les filtrages web, celui-ci va s'effectuer en fonction des groupes d'appartenance des utilisateurs.

Pour ce faire, nous allons configurer une liaison avec l'AD.
Squid effectuera des requêtes LDAP afin de vérifier l'appartenance au groupe de l'utilisateurs et lui appliquer les règles de filtrage via des ACLs définies le service.

En ce qui concerne la gestion des utilisateurs Guest, nous avons opté pour la mise en place d'un portail captif.
L'authentification se fera par vouchers et les utilisateurs seront placés dans un VLAN isolé et sécurisé. Cependant ils ne passeront pas par le Proxy pour des raisons techniques, de réglementation et de sécurité (plus de détails dans la partie **1.4 Sécurisation des accès**)

1.3 Choix de la solution

Concernant le choix de la solution, nous avons opté pour **« Squid ».**
Plus précisément 3 plugins seront installés sur Pfsense :

- **Squid Proxy Filter** : Qui servira à configurer le proxy dans ces paramètres générales (Port du proxy, définition du cache ect…)
- **SquidGuard** : qui servira pour mettre en place le filtrage d'URL via la blacklist ainsi qu'à configurer les ACLs pour les filtrages en fonction du groupe Active Directory
- **LightSquid** : Qui va servir comme outil d'analyse de notre Proxy afin de voir les logs par utilisateur, l'utilisation du cache, les sites les plus visités ect…

Nous avons retenu cette solution pour plusieurs raisons :

- Intégration complète dans Pfsense via les plugins
- Solution éprouvée et fiable
- Documentation et communauté très présentes
- Solution complète permettant un paramétrage poussé de notre proxy
- Solution offrant de bonnes performances

1.4 Sécurisation des accès

A des fins de sécurité, le port par défaut du Proxy sera modifié.

Concernant les filtrages des flux Web nous allons télécharger une blacklist **« UT1 »** qui regroupe des sites Web par catégorie.
Celle-ci va nous permettre de rejeter tout trafic inapproprié ou présentant un risque pour SI.

Afin de répondre aux normes de la législation, nous allons aussi mettre en place une conservation des logs utilisateurs pour une durée de 180 jours.

Concernant la demande de l'ADRAR pour le filtrage des Guest via le proxy, celle-ci est difficilement applicable.
L'architecture et les contraintes de Pfsense nous obligeraient à ajouter un deuxième pare feu et à configurer un proxy en mode transparent avec le SSL Bump activé.
En effet, les postes des utilisateurs externes ne faisant pas partie du domaine, nous ne pouvons pas pousser notre GPO sur leurs postes.

Comme mentionné en début de document, le fonctionnement en mode transparent avec le SSL Bump pose problème si l'on veut respecter la confidentialité des données et notamment le RPGD.
Voici les points essentiels bloquants :

- Capture non approuvé de données personnelles des utilisateurs (articles 5 et 6 du RGPD).
- Absence de consentement explicite (article 7 RGPD).
- Non-respect de la confidentialité des communications chiffrées.
- Amendes RGPD en cas de non-conformité
- Surveillance pouvant être perçue comme intrusive par les visiteurs et donc nuire à l'image de l'entreprise.

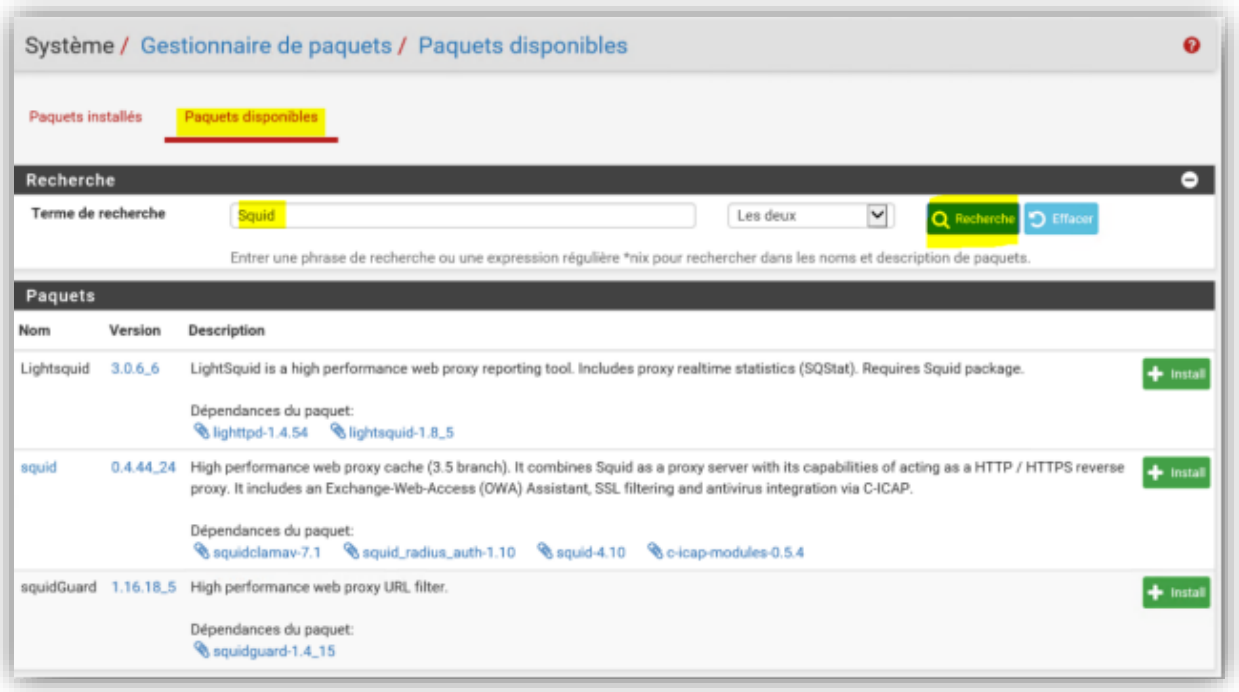
La solution serait d'intégrer des CGU au portail captif pour informer les utilisateurs externes de l'utilisation d'un proxy mais Pfsense ne le permet pas.
C'est donc pour ces raisons que nous avons opté pour la solution d'un portail captif avec authentification via vouchers (avec rétention des logs pendant 180 jours également) et du VLAN isolé.

Cependant, si un souhait est formulé par l'ADRAR d'imposer un proxy transparent pour les Guest, nous pourrons l'ajouter.
Un document officiel informant de l'utilisation du Proxy devra être à faire signer pour chaque utilisateur nécessitant d'une connexion « Guest ».
La partie configuration technique sera identique à celle dans le chapitre **2.Configuration technique** pour le deuxième pare-feu, il suffira de cocher deux cases supplémentaires pour activer le mode transparent et le SSL Bump.

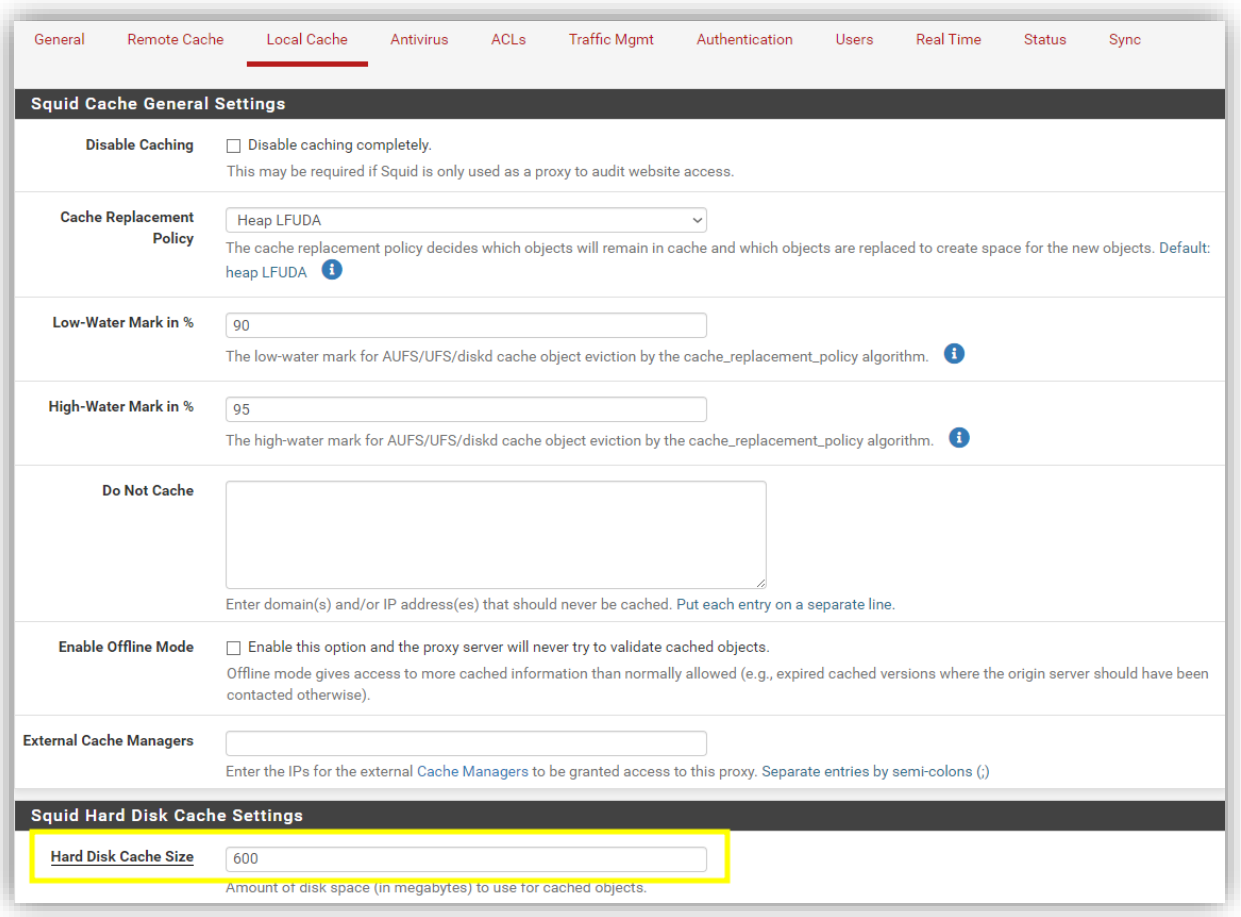
2. Configuration technique

2.1 Configuration de Squid

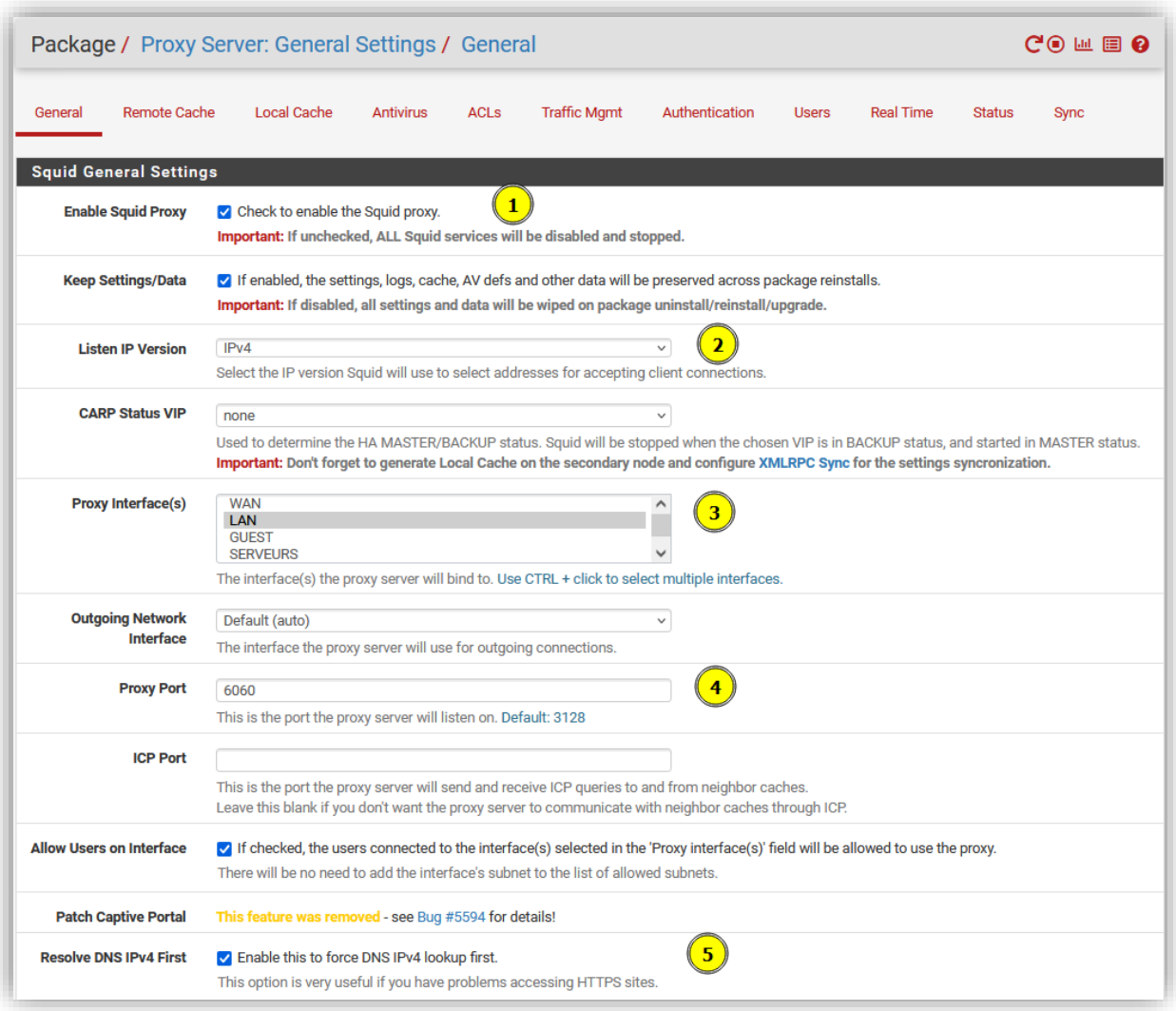
Dans un 1er temps, nous allons installer les différents plugins Squid :



Nous allons maintenant configurer le cache de notre Proxy que nous mettrons à 600Mo (la taille du cache sera revue à la hausse celle-ci étant configurée à600 Mo à des fins de tests, il sera recommandé de l'augmenter entre 20Go et 50Go en fonction de son utilisation) :

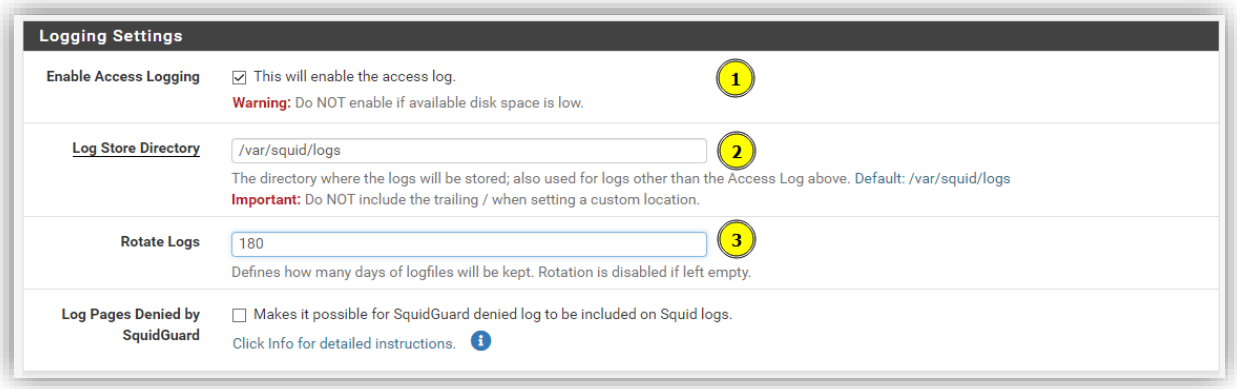


Nous pouvons maintenant continuer les configurations générales de notre proxy dans la rubrique **« Services »** puis **« Squid Proxy Server »** :

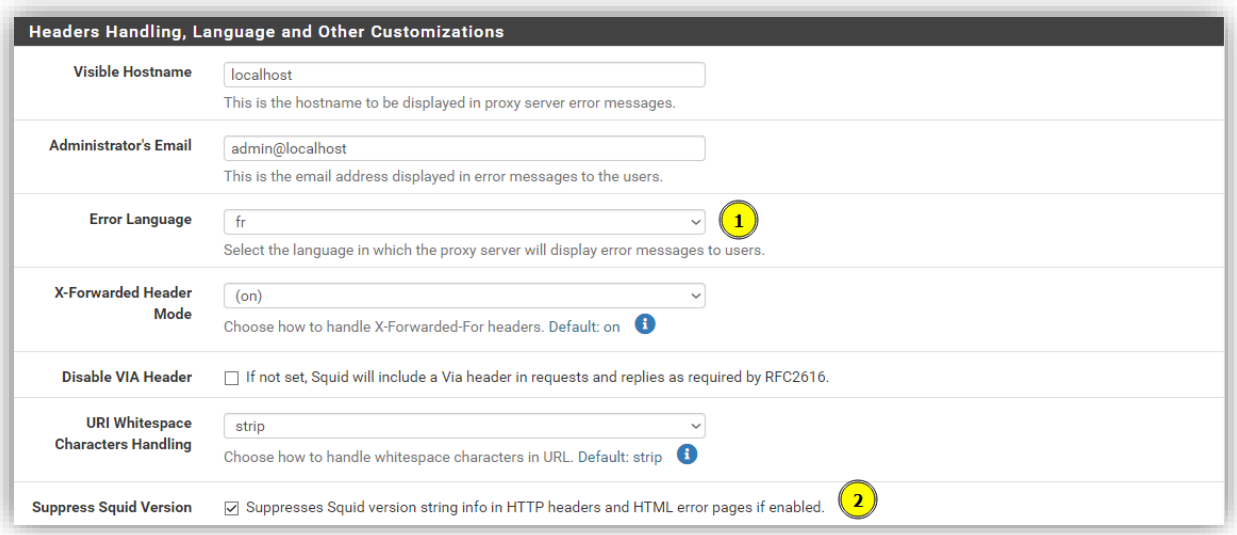


1. Activer le Proxy Squid
2. Version IPV4 pour l'écoute de notre Proxy
3. Interfaces d'utilisation de notre Proxy
4. Port du Proxy
5. Activer la résolution IPv4 en premier

Nous continuons ensuite la configuration en descendant sur la page :

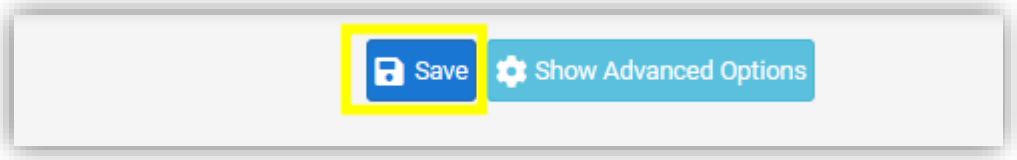


1. Activer les logs sur le proxy
2. Répertoire de stockage des logs
3. Durée de conservation des logs



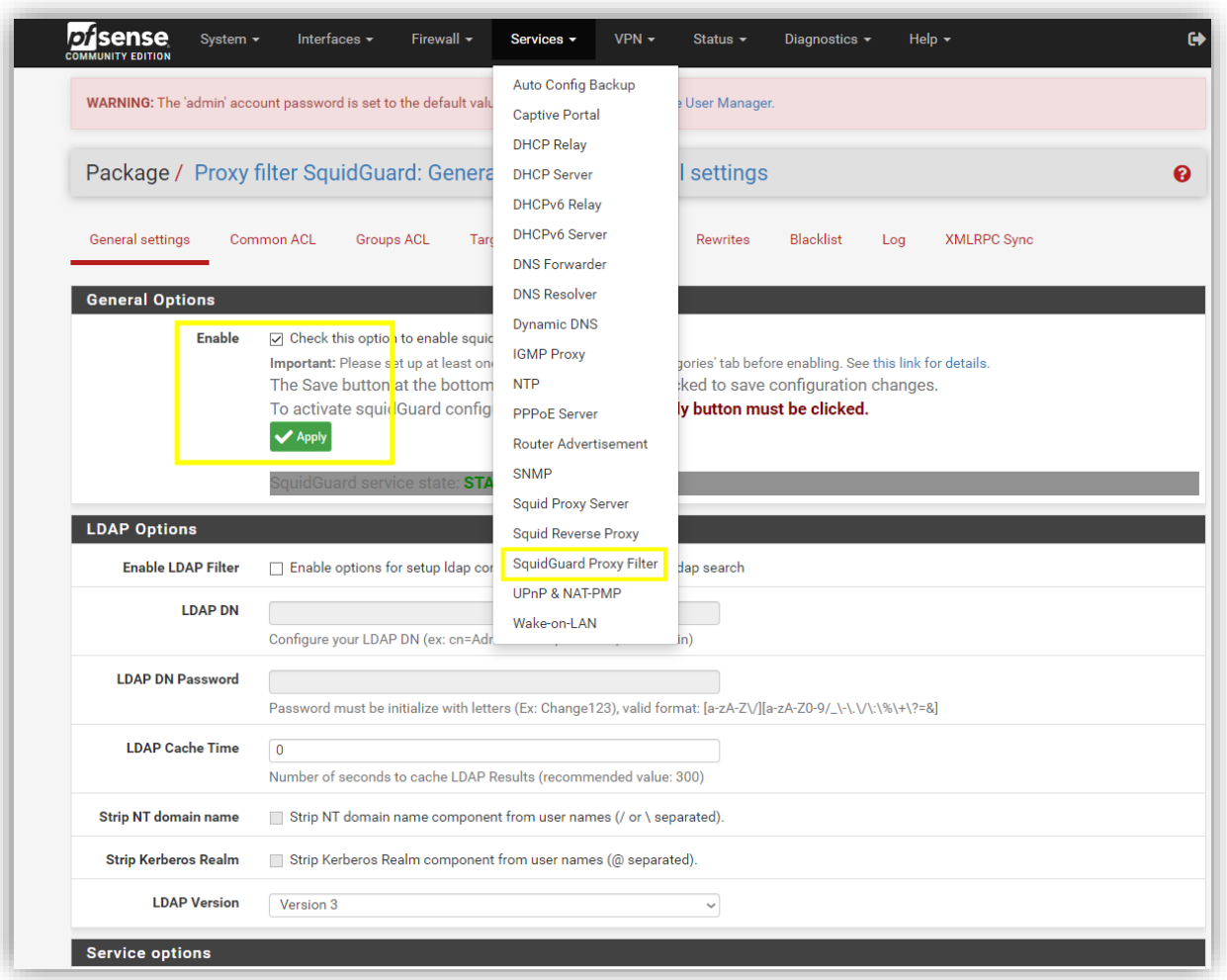
1. Langue affichée pour les erreurs
2. Masque les informations de la version du serveur Squid dans les en tête HTTP

Puis nous sauvegardons la configuration :

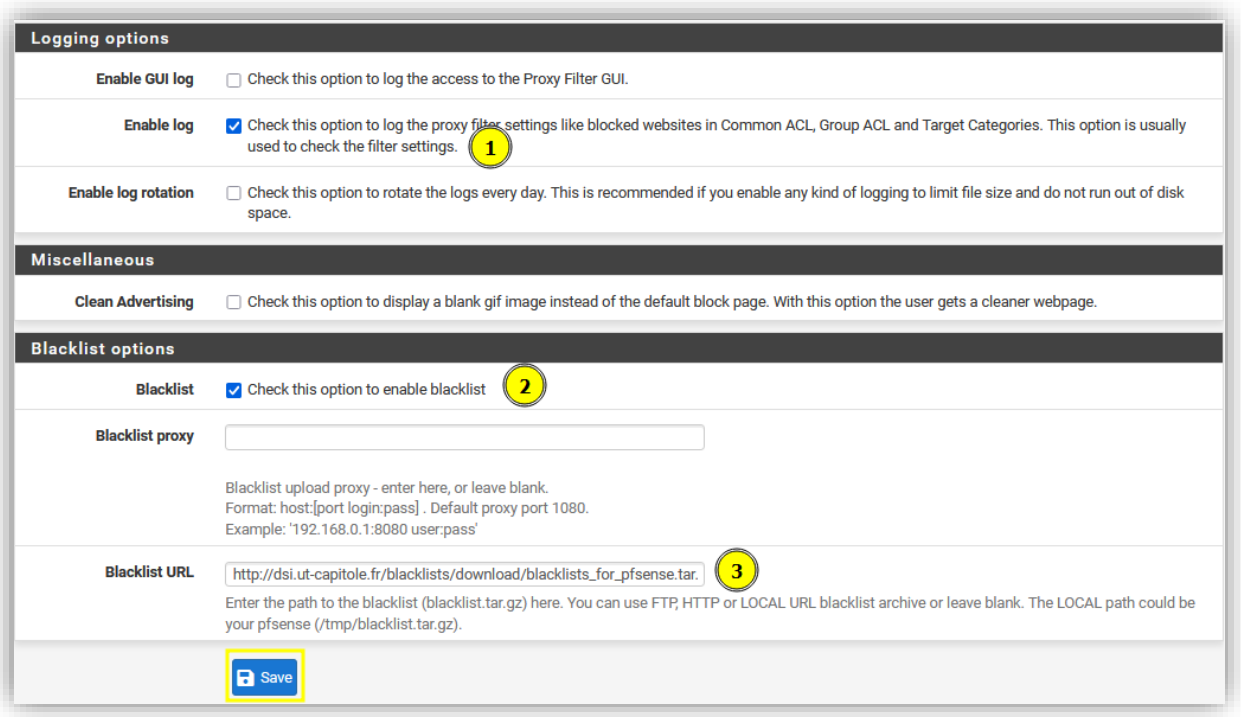


2.2 Configuration du SquidGuard

Nous commençons par activer **« SquidGuard Proxy Filter »** :

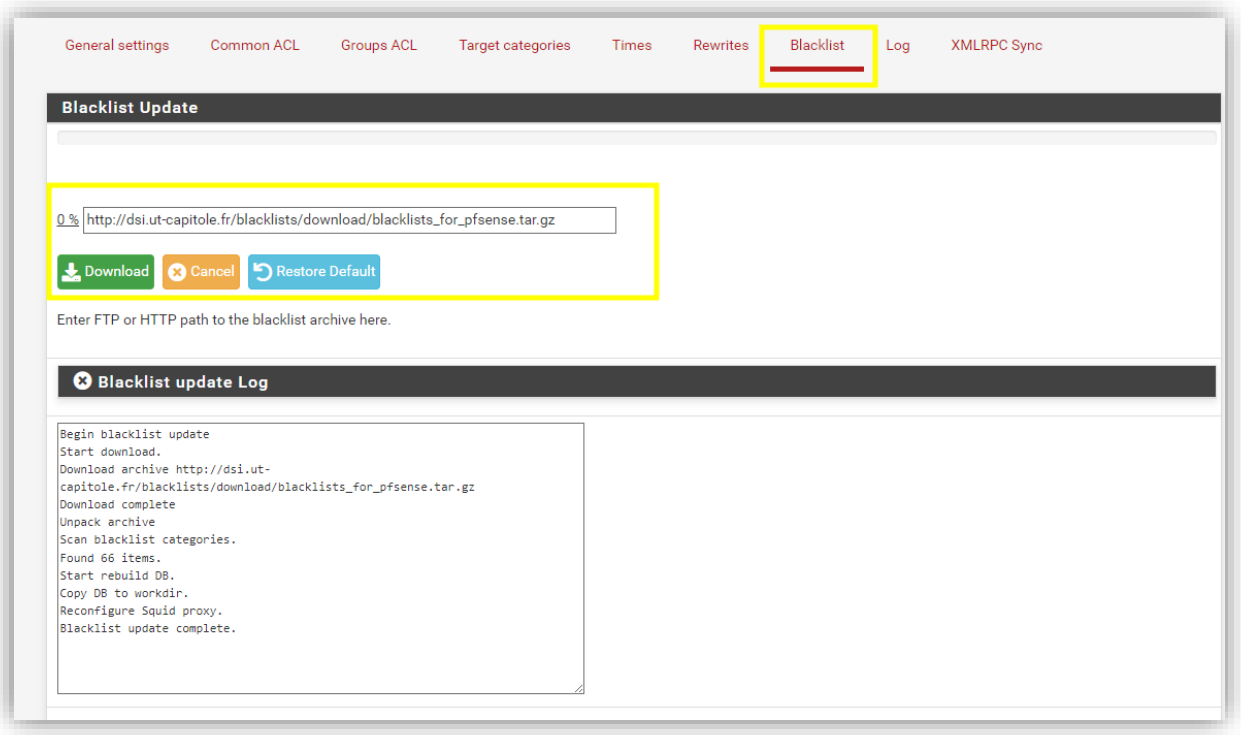


Maintenant, nous activons les logs dans **SquidGuard** et renseignons notre blacklist :

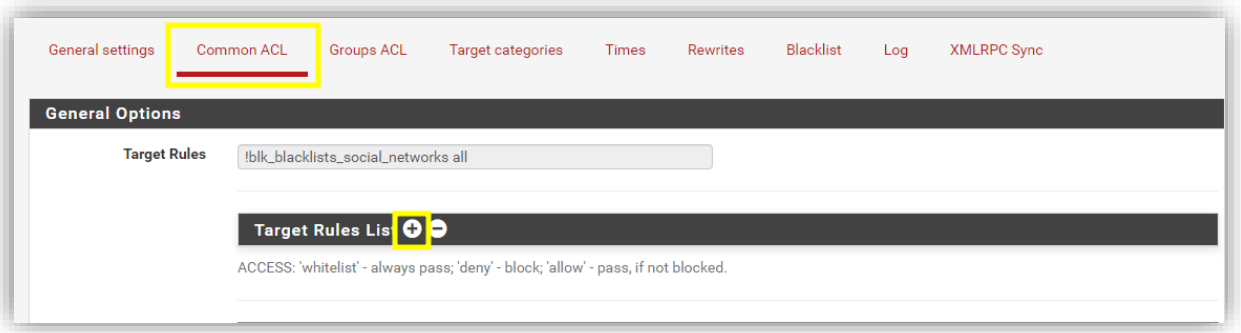


1. Activer les logs
2. Activer la blacklist
3. URL de la blacklist

Il faut désormais se rendre dans le menu Blacklist, et allons renseigner l'URL de notre UT1 et ensuite cliquer sur Download pour charger toutes les catégories définies dans celles-ci :



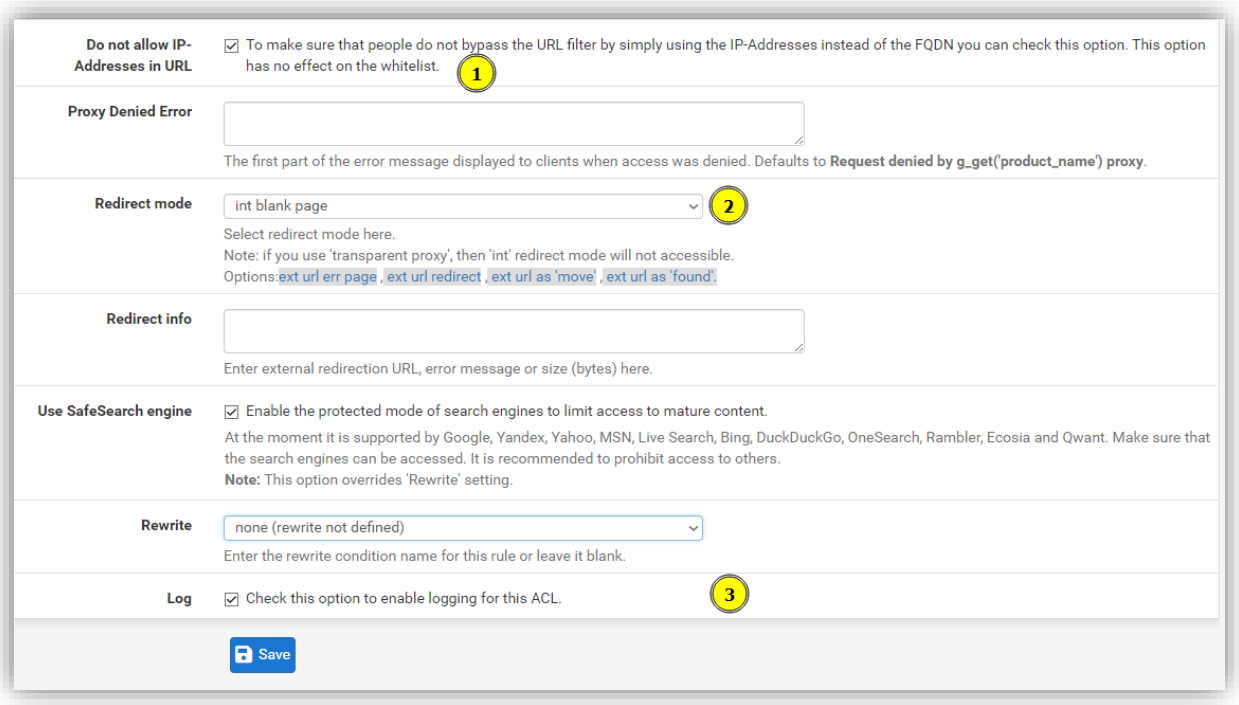
Nous allons maintenant dans le menu Common ACL, cliquons sur le + pour déplier les catégories.



Nous accédons à toutes les catégories téléchargées dans la blacklist.
Nous autorisons le **« Default access »** pour que toutes les catégories soient autorisées par défaut.

Ensuite, nous affinons la sécurité en interdisant chaque catégorie voulu. (Voici un exemple pour les réseaux sociaux) :

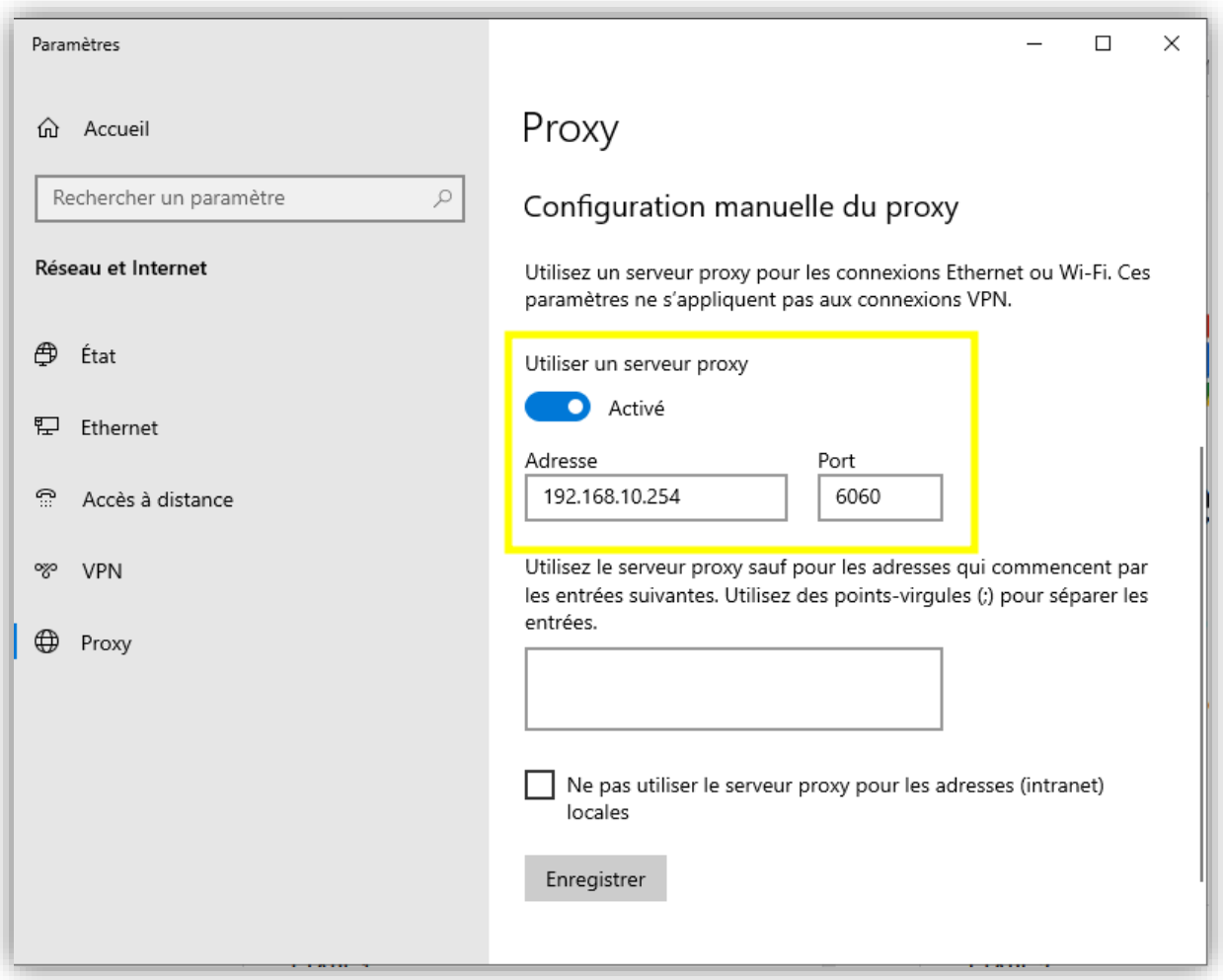
Nous continuons maintenant la configuration de notre ACL par défaut :



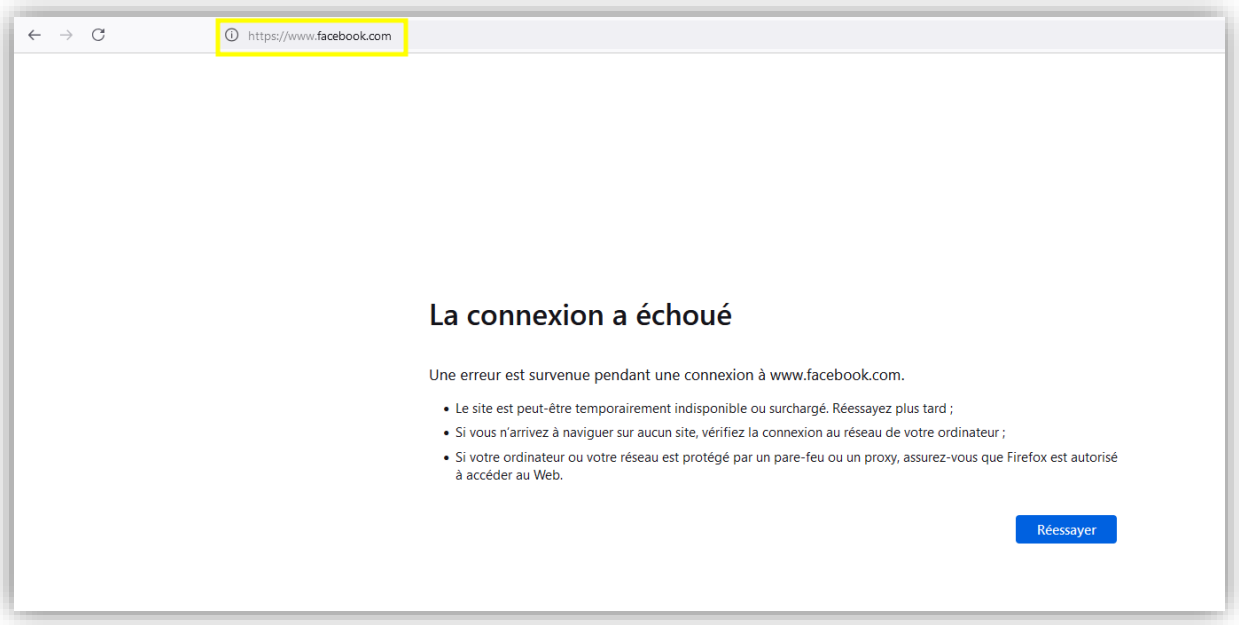
1. Ne pas autoriser l'accès au site via l'IP
2. Message d'erreur affiché lors d'une connexion refusée
3. Active les logs pour cette ACL

2.3 Test client du Proxy

Nous effectuons maintenant notre test sur une machine cliente.
Nous allons dans le menu de configuration de proxy de Windows et renseignons les paramètres suivant :

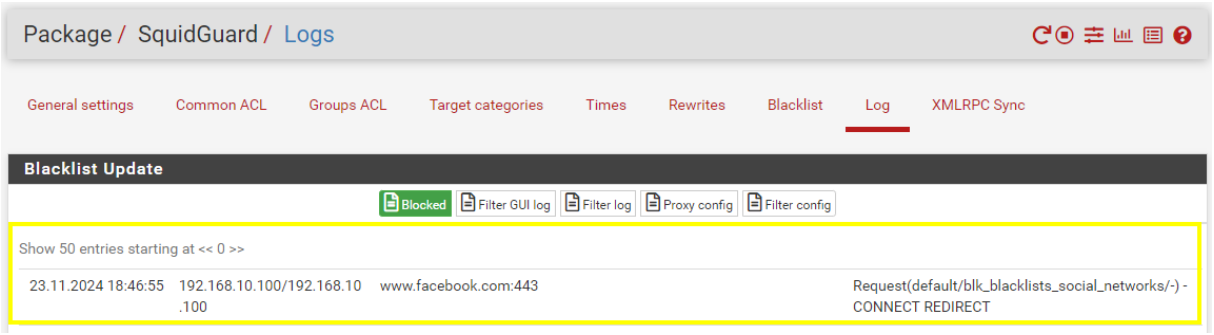


Nous essayons maintenant d'accéder à « Facebook » qui fais partie de la catégorie « réseaux sociaux » bloquée dans notre ACL par default :



Nous essayons avec Wikipédia qui fais partie des sites autorisés :

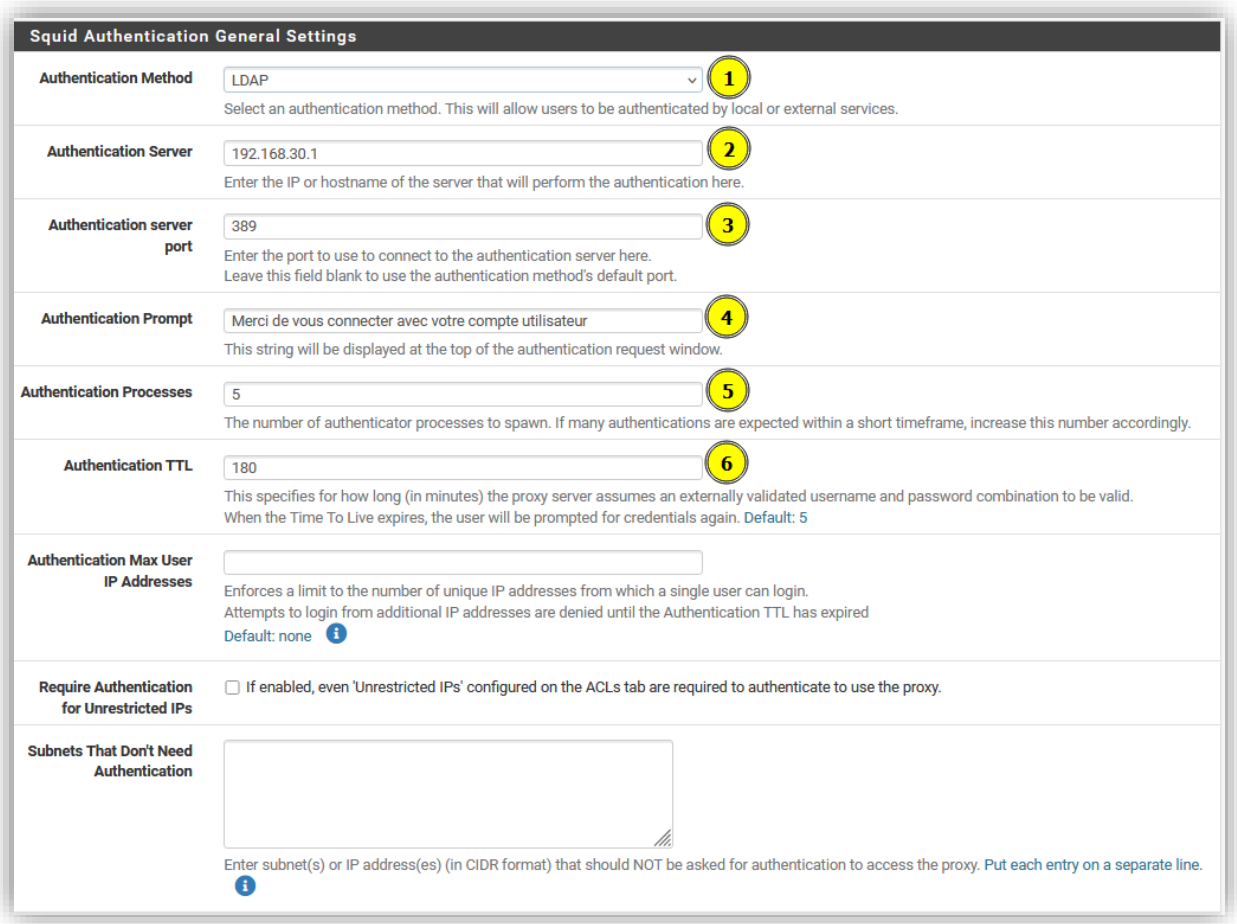
Nous vérifions également les logs dans notre service **« SquidGuard »** :



2.4 Configuration du filtrage Web par compte AD

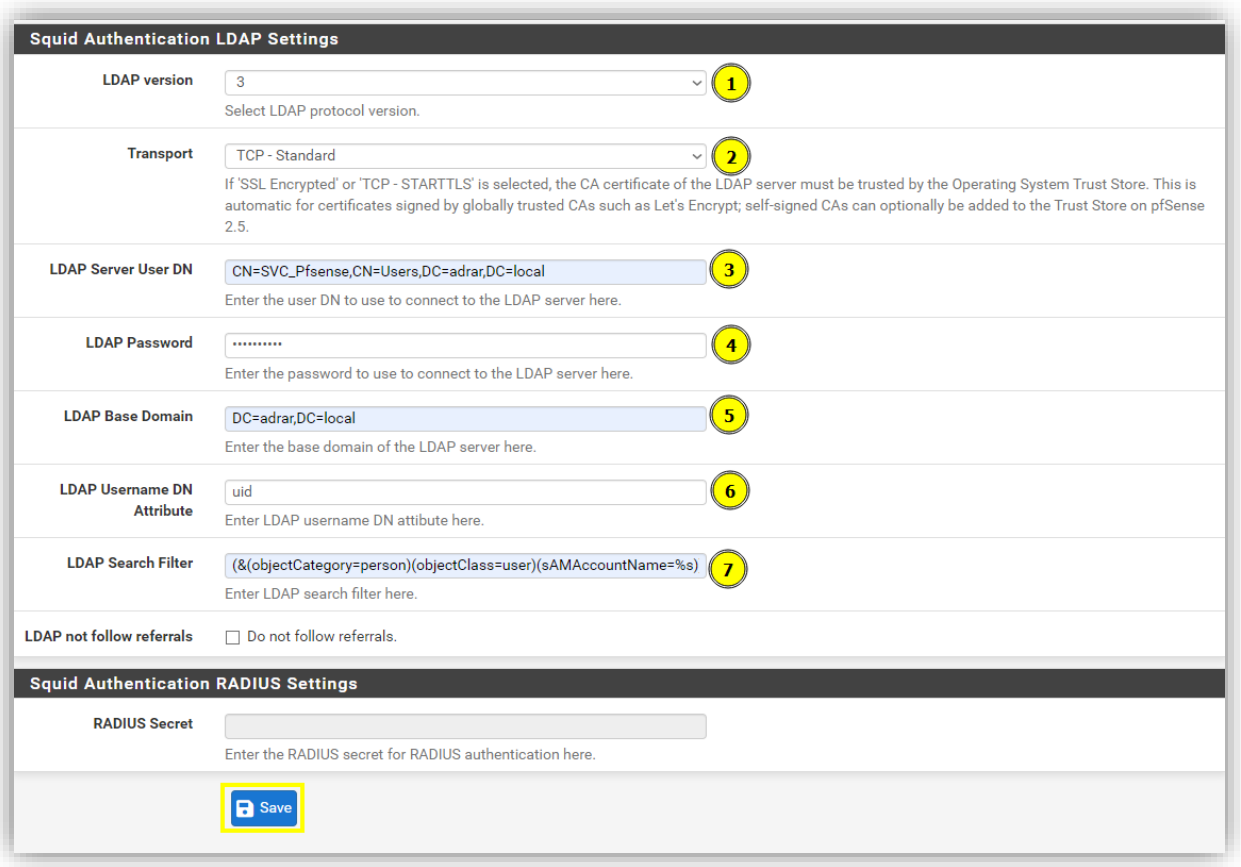
Maintenant, nous allons pouvoir mettre en place le filtrage par groupe AD.

Nous allons donc dans le menu **« Authentification »** de notre **« Squid Proxy Server »** et renseignons les éléments suivants :



1. Méthode d'authentification au proxy via le LDAP
2. IP de notre contrôleur de domaine
3. Port d'écoute de notre LDAP
4. Message à afficher aux utilisateurs pour l'authentification
5. Nombre de processus d'authentification simultanés autorisés
6. Durée de validité de l'authentification (en minutes)

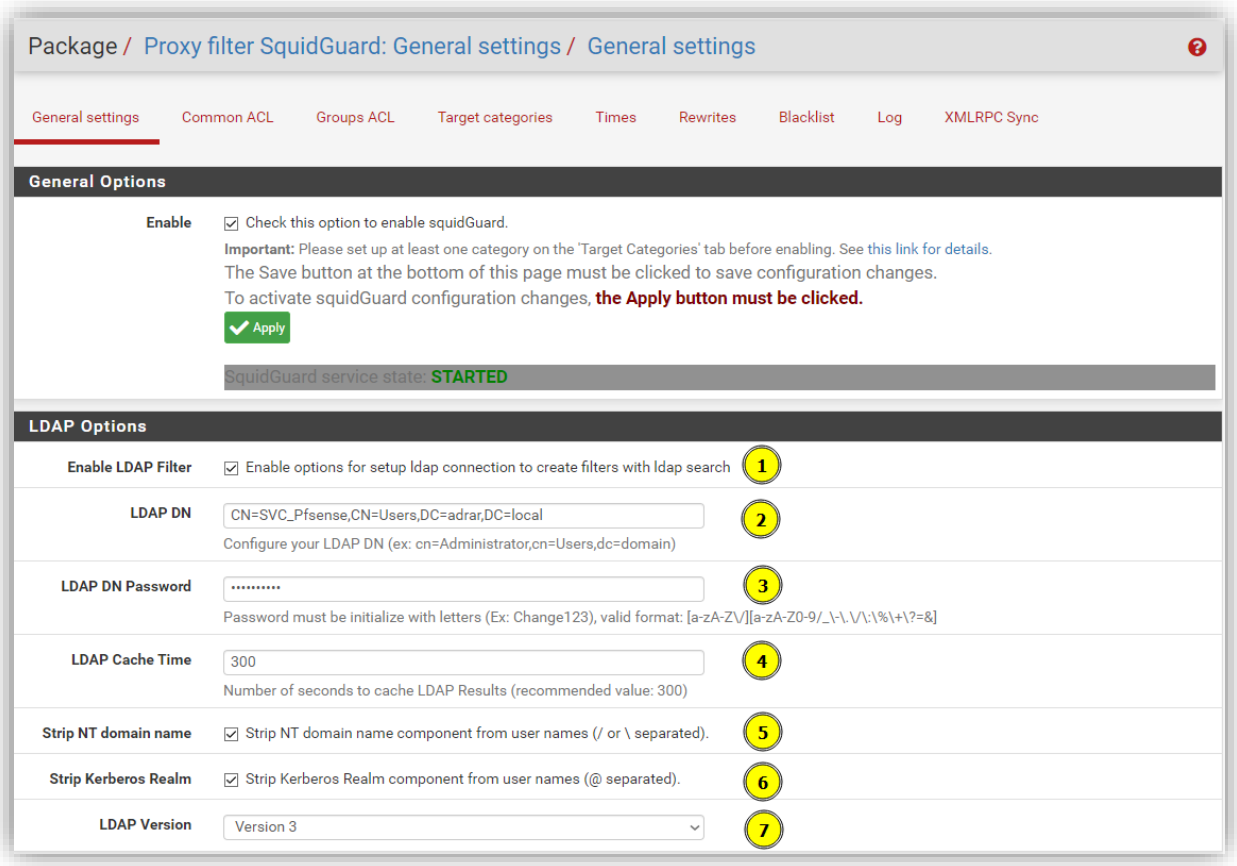
Nous continuons en renseignant les paramètres LDAP :



1. Version de LDAP utilisée
2. Protocole de transport utilisé TCP
3. DN de notre compte de service pour la lecture LDAP
4. Mot de passe associé au compte
5. Base DN du domaine
6. Attribut DN des utilisateurs
7. Filtre de recherche LDAP pour trouver des utilisateurs

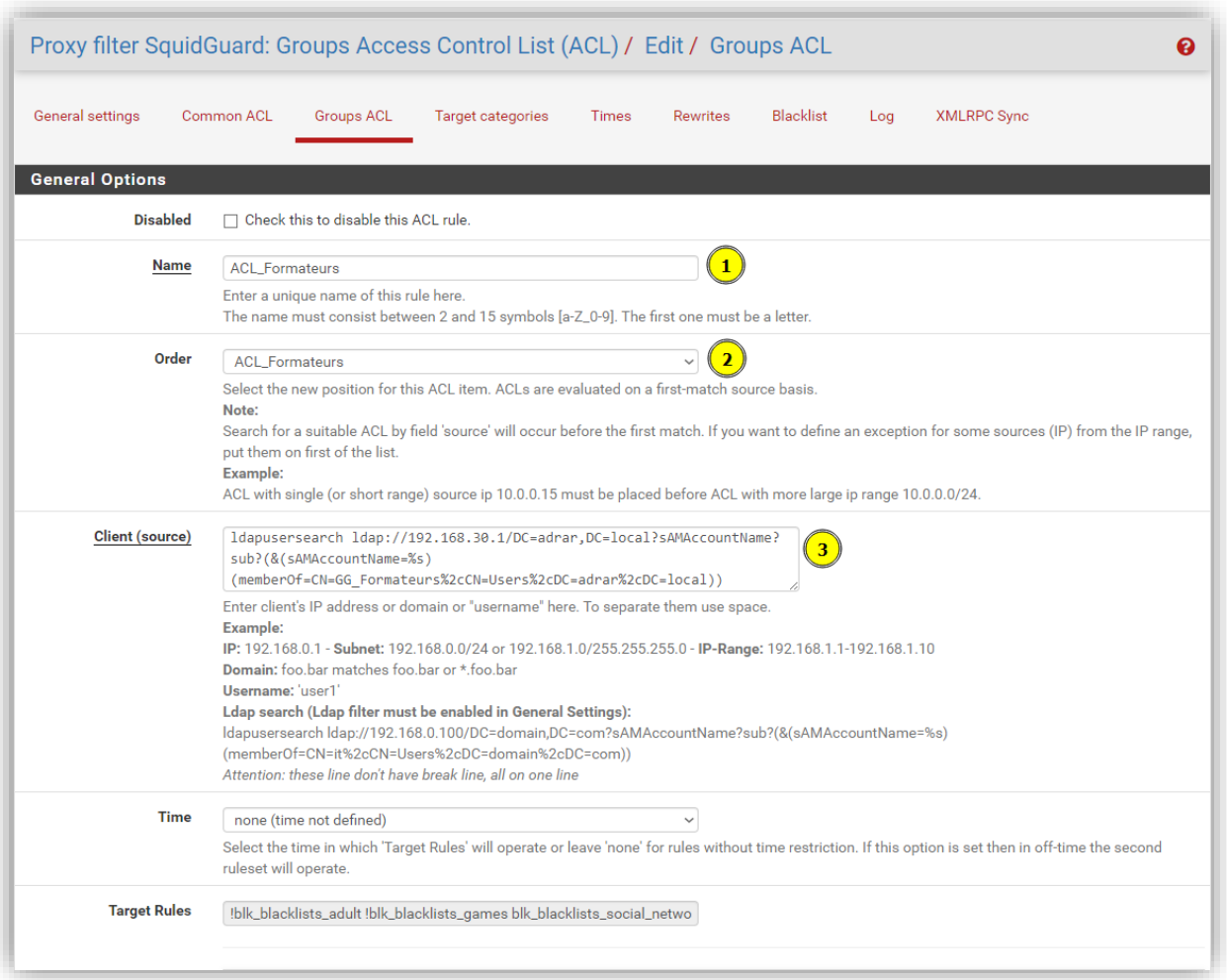
Une fois nos configurations effectuées nous cliquons sur **« Save »** pour enregistrer.

Dans la rubrique **« General Settings »** de **« SquidGuard »** nous allons renseigner les éléments suivants :



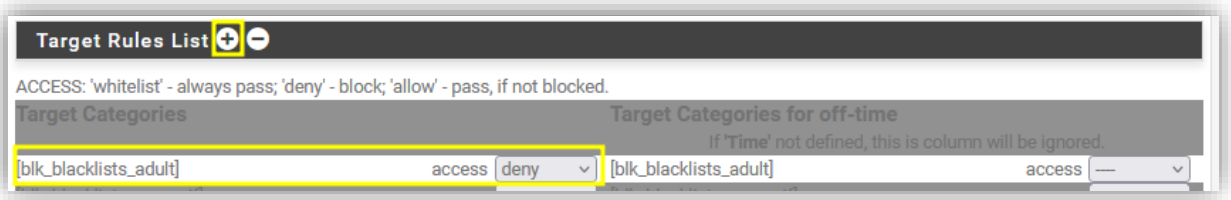
1. Activer le filtrage via LDAP
2. DN du compte de service
3. Mot de passe associé au compte
4. Durée de la mise en cache
5. Supprime le / ou \ des noms d'utilisateur pour l'authentification
6. Supprime le @NomDeDomaine pour l'authentification utilisateurs
7. Version de LDAP utilisée

Nous allons maintenant effectuer nos règles de filtrage par groupe LDAP.
Pour cela, nous allons dans le menu **« Groups ACL »** :

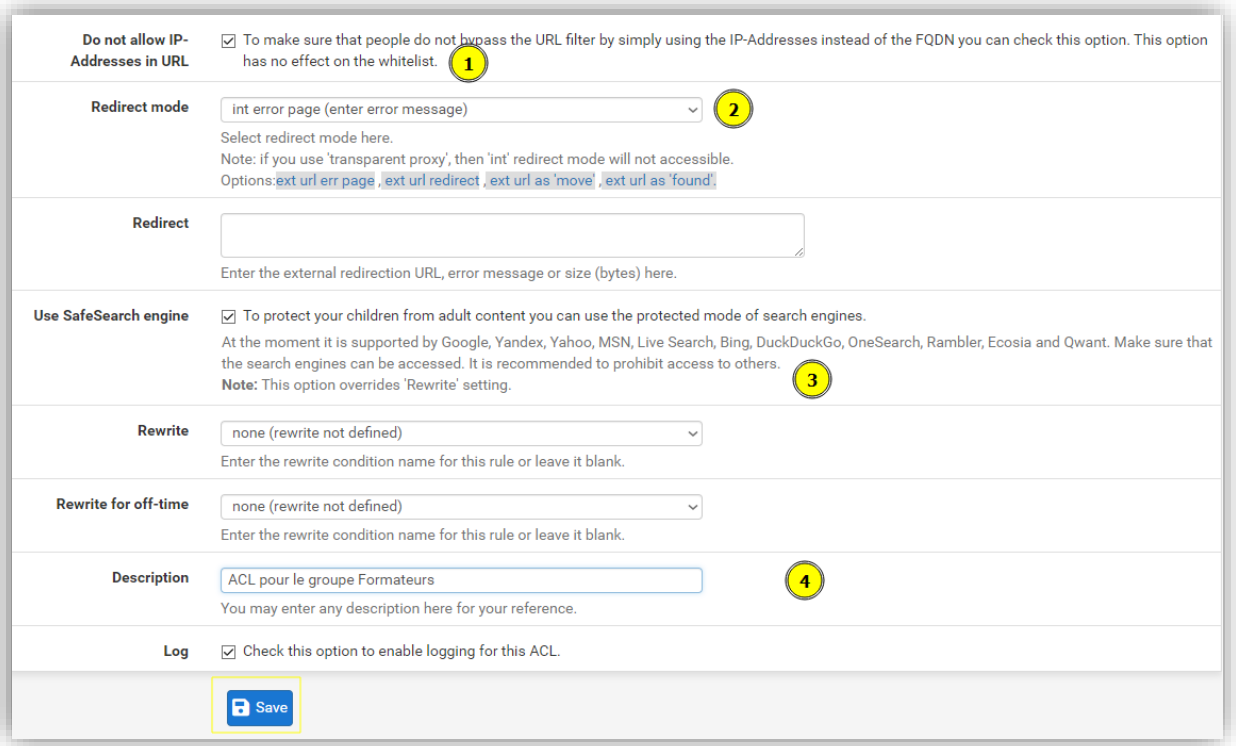


1. Nom de note ACL
2. Ordre d'exécutions de l'ACL
3. Requêtes afin de filtrer l'ACL sur le groupe LDAP nommé **« GG_Formateurs »**

Une fois cela fait, nous allons définir les filtrages web à effectuer.
Nous cliquons sur le « **+** » dans **« Target Rules List »** de la même façon que précédemment afin d'autoriser ou non certaines catégories. Voici un exemple :



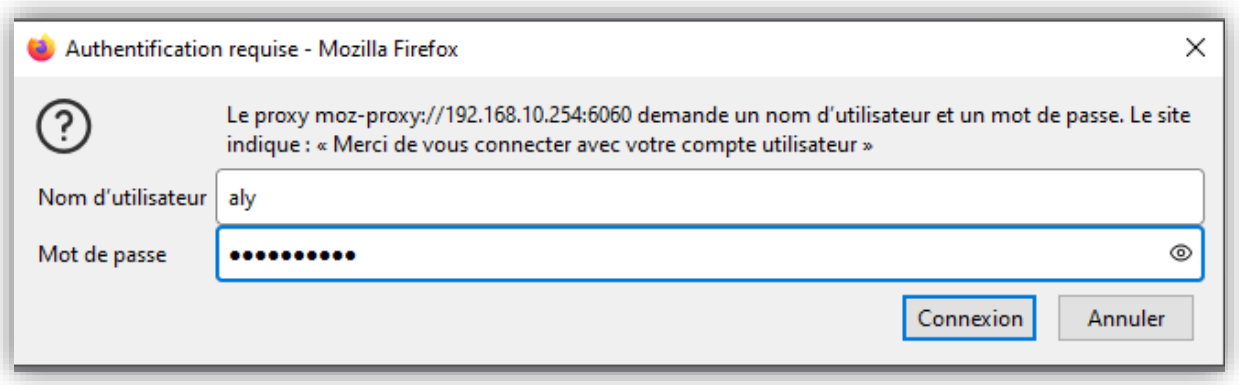
Nous continuons ensuite la configuration :



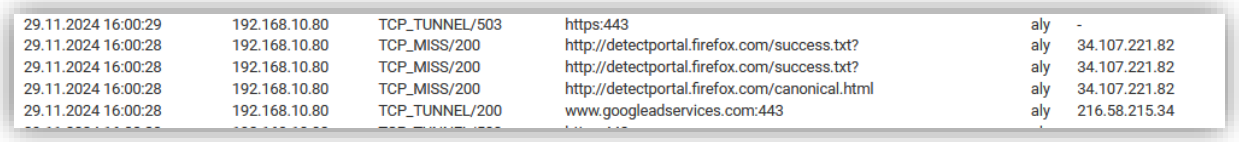
1. Ne pas autoriser l'accès au site via des IP
2. Message affiché lors d'une connexion refusée
3. Utiliser SafeSearch pour les recherches sur les navigateurs
4. Description de l'ACL

Nous sauvegardons la configuration et effectuons un test via un poste client.

Dès l'ouverture du navigateur, un message apparait demandant les identifiants d'accès au proxy.



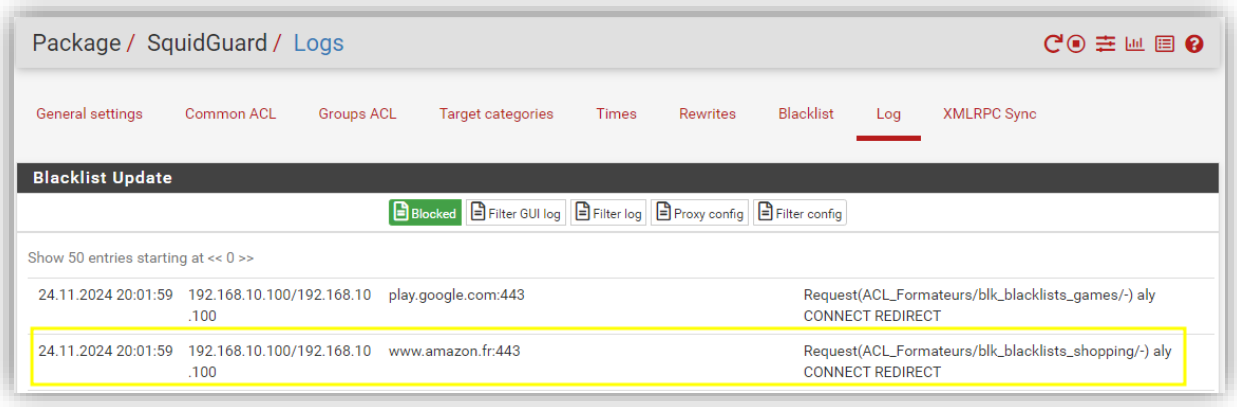
Nous regardons les logs et voyons l'utilisateur authentifié



29.11.2024 16:00:29	192.168.10.80	TCP_TUNNEL/503	https:443	aly	-
29.11.2024 16:00:28	192.168.10.80	TCP_MISS/200	http://detectportal.firefox.com/success.txt?	aly	34.107.221.82
29.11.2024 16:00:28	192.168.10.80	TCP_MISS/200	http://detectportal.firefox.com/success.txt?	aly	34.107.221.82
29.11.2024 16:00:28	192.168.10.80	TCP_MISS/200	http://detectportal.firefox.com/canonical.html	aly	34.107.221.82
29.11.2024 16:00:28	192.168.10.80	TCP_TUNNEL/200	www.googleadservices.com:443	aly	216.58.215.34

Une fois renseigné, nous essayons d'accéder à la Amazon qui fait partie de la rubrique Shopping qui est interdite pour ce groupe.

Le site est bien bloqué par le proxy.
Nous vérifions dans les logs en regardant le nom de l'ACL qui bloque le trafic Web :

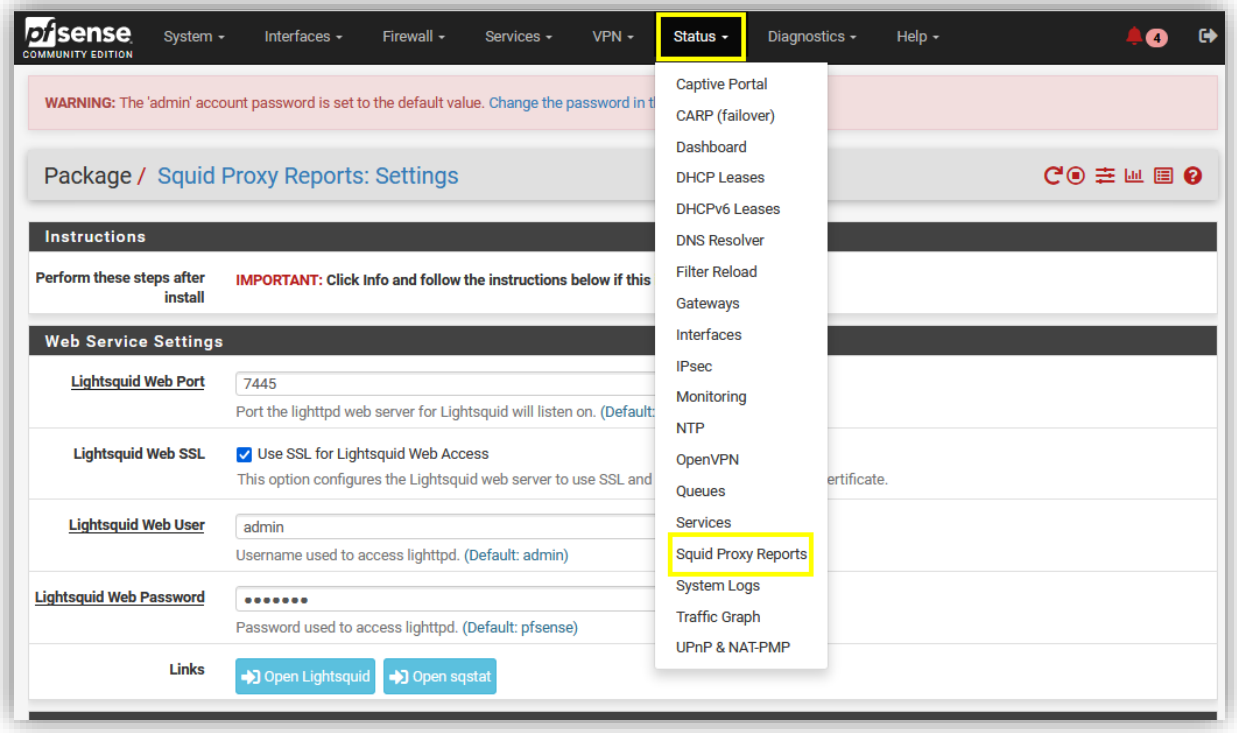


Nous allons effectuer les mêmes configurations pour créer les ACLs pour le filtrage des groupes **« GG_Stagiaires »** et **« GG_Guest »**

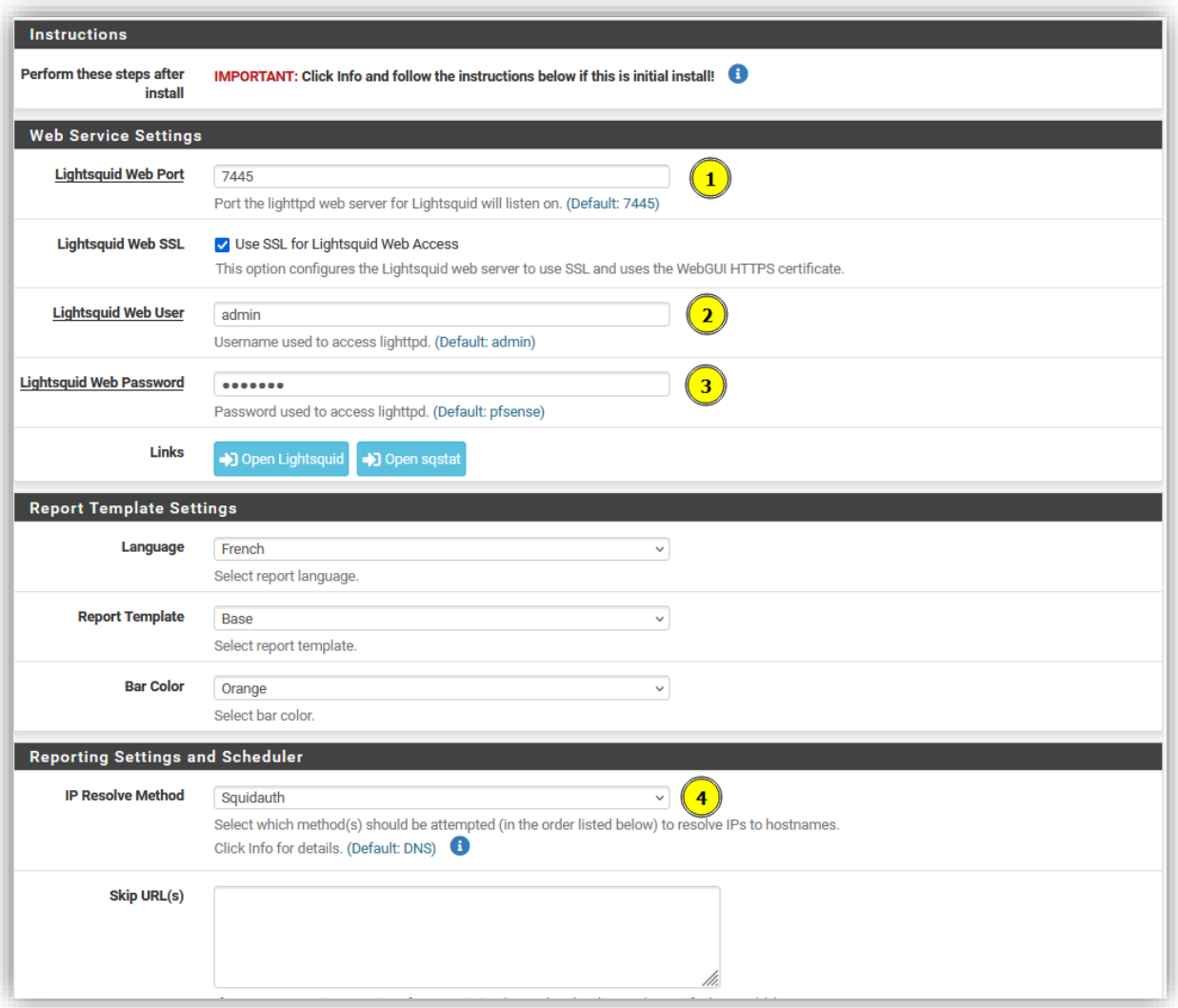
2.5 Configuration de LightSquid

Maintenant nous allons pouvoir configurer LightSquid qui nous servira principalement afin d'avoir des statistiques sur l'utilisation de notre Proxy

Pour le configurer nous allons dans le menu suivant :



Nous renseignons les paramètres suivants pour accéder à la page de LightSquid :

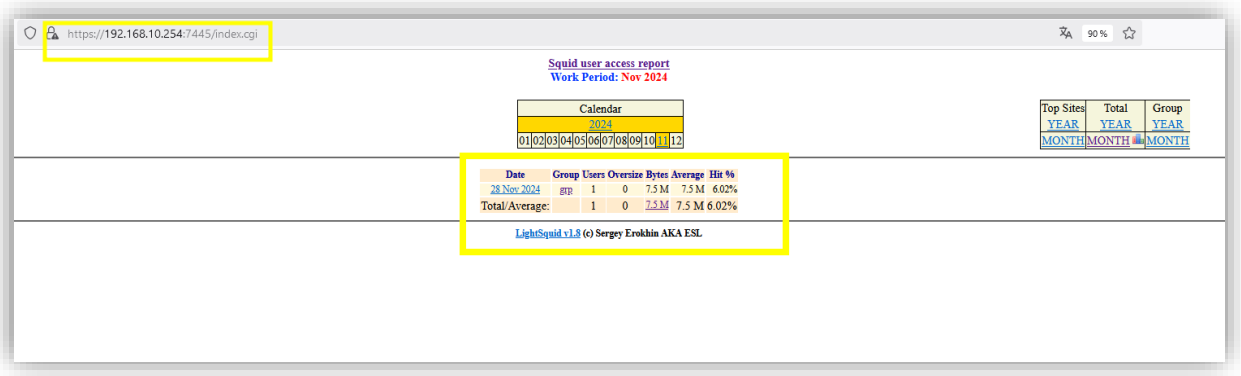


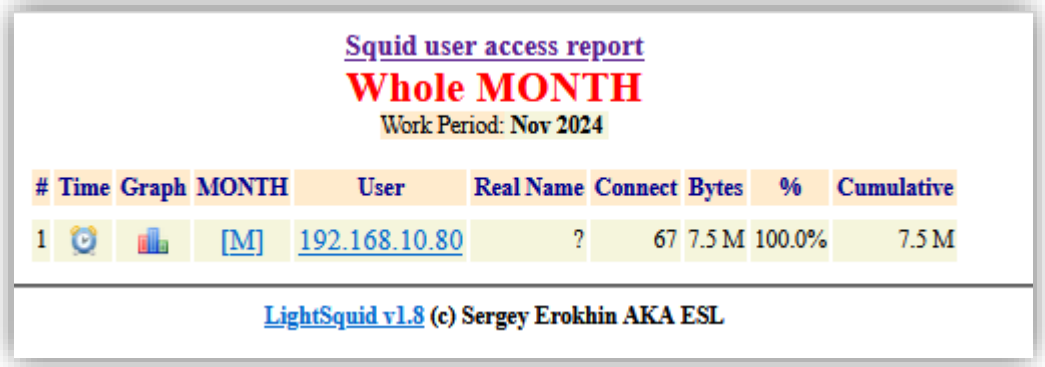
1. Port d'écoute
2. Utilisateur pour se connecter
3. Mot de passe du compte
4. Méthode de résolution des noms via Squid

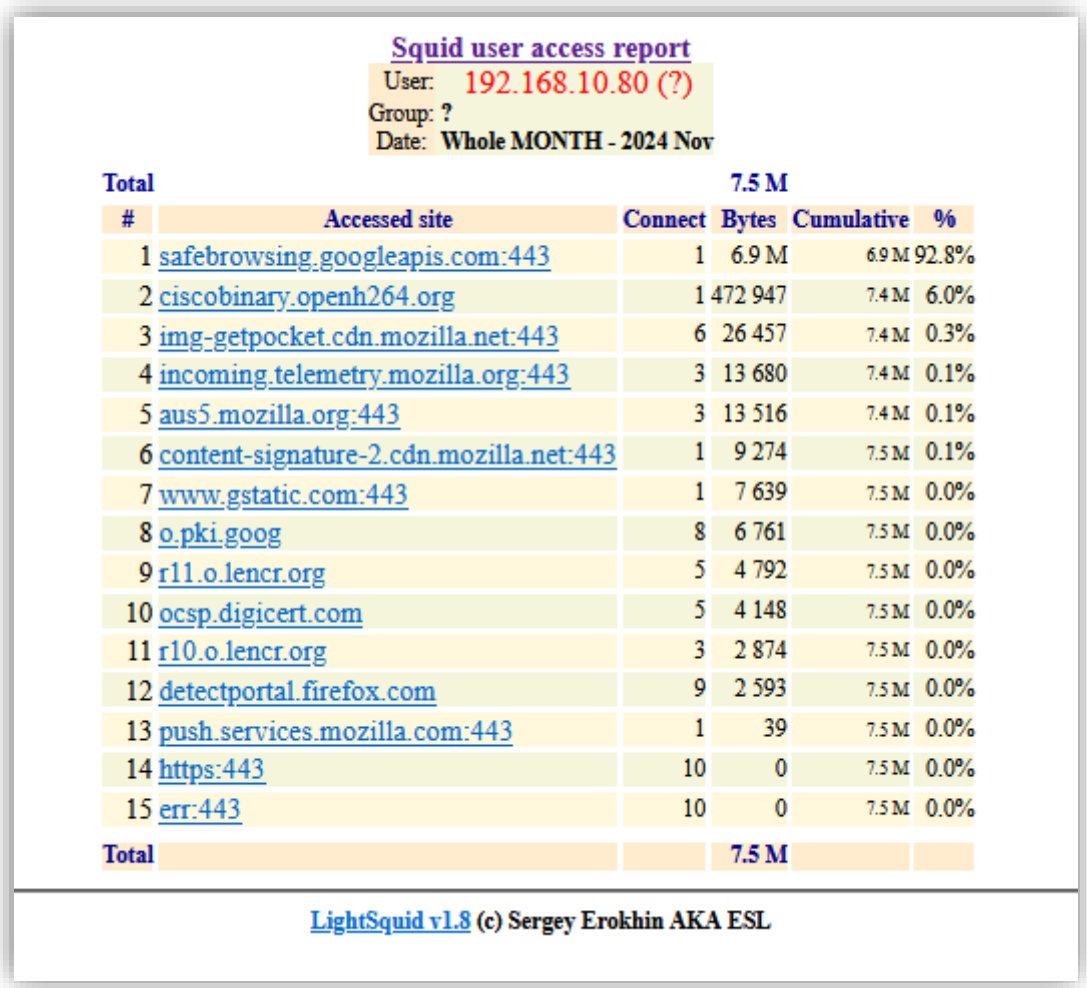
Nous accédons à la page via l'IP de notre Firewall et le port défini précédemment.

Pour se connecter, nous utilisons le login défini précédemment.

Sur cette page, nous pouvons avoir un détail des connexions selon la date et la machine, des graphiques, des tops sites, du temps passé etc…







Squid user access report

User: 192.168.10.80 (?)
Group: ?
Date: Whole MONTH - 2024 Nov

Total 7.5 M

#	Accessed site	Connect	Bytes	Cumulative	%
1	safebrowsing.googleapis.com:443	1	6.9 M	6.9 M	92.8%
2	ciscobinary.openh264.org	1	472 947	7.4 M	6.0%
3	img-getpocket.cdn.mozilla.net:443	6	26 457	7.4 M	0.3%
4	incoming.telemetry.mozilla.org:443	3	13 680	7.4 M	0.1%
5	aus5.mozilla.org:443	3	13 516	7.4 M	0.1%
6	content-signature-2.cdn.mozilla.net:443	1	9 274	7.5 M	0.1%
7	www.gstatic.com:443	1	7 639	7.5 M	0.0%
8	o.pki.goog	8	6 761	7.5 M	0.0%
9	r11.o.lencr.org	5	4 792	7.5 M	0.0%
10	ocsp.digicert.com	5	4 148	7.5 M	0.0%
11	r10.o.lencr.org	3	2 874	7.5 M	0.0%
12	detectportal.firefox.com	9	2 593	7.5 M	0.0%
13	push.services.mozilla.com:443	1	39	7.5 M	0.0%
14	https:443	10	0	7.5 M	0.0%
15	err:443	10	0	7.5 M	0.0%
Total			**7.5 M**		

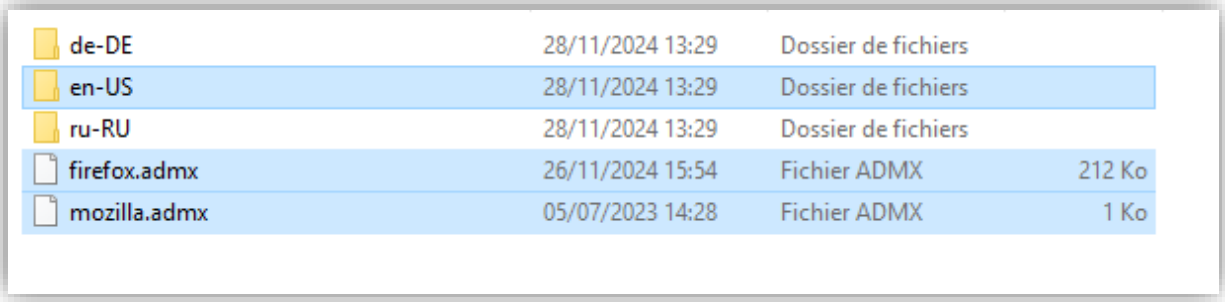
LightSquid v1.8 (c) Sergey Erokhin AKA ESL

2.6 Déploiement des configuration Proxy par GPO

Pour déployer nos configurations Proxy sur nos machines clientes, nous allons mettre en place une GPO.

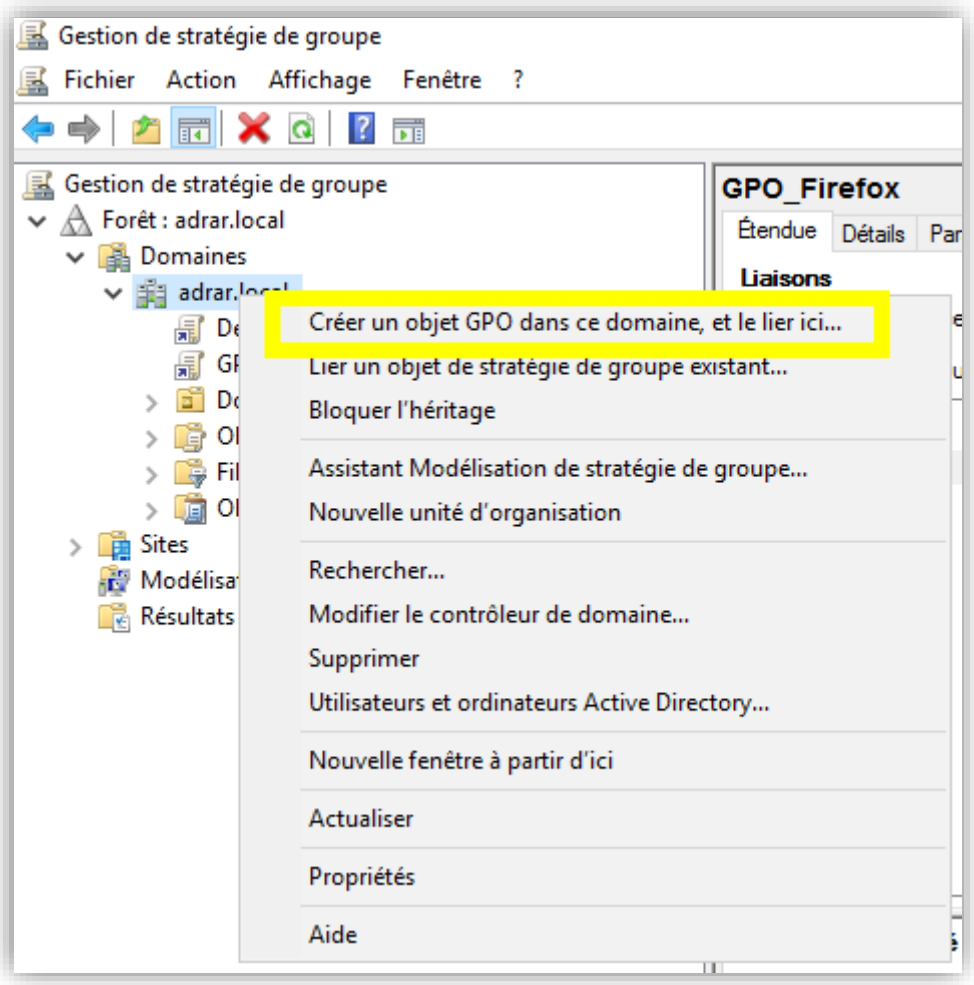
Nous commençons par télécharger les fichiers **« admx »** pour Firefox car c'est ce navigateur utilisé sur nos postes clients.

Une fois cela fait nous copions les fichiers et dossiers dans **« C:\Windows\PlicyDefinitions »** sur le contrôleur de domaine :

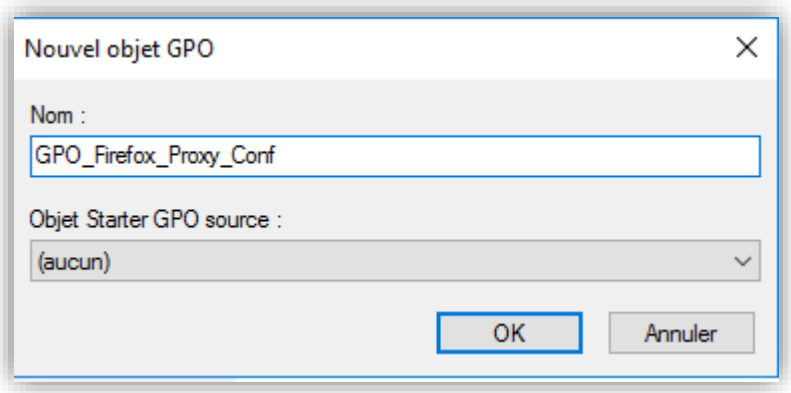


de-DE	28/11/2024 13:29	Dossier de fichiers	
en-US	28/11/2024 13:29	Dossier de fichiers	
ru-RU	28/11/2024 13:29	Dossier de fichiers	
firefox.admx	26/11/2024 15:54	Fichier ADMX	212 Ko
mozilla.admx	05/07/2023 14:28	Fichier ADMX	1 Ko

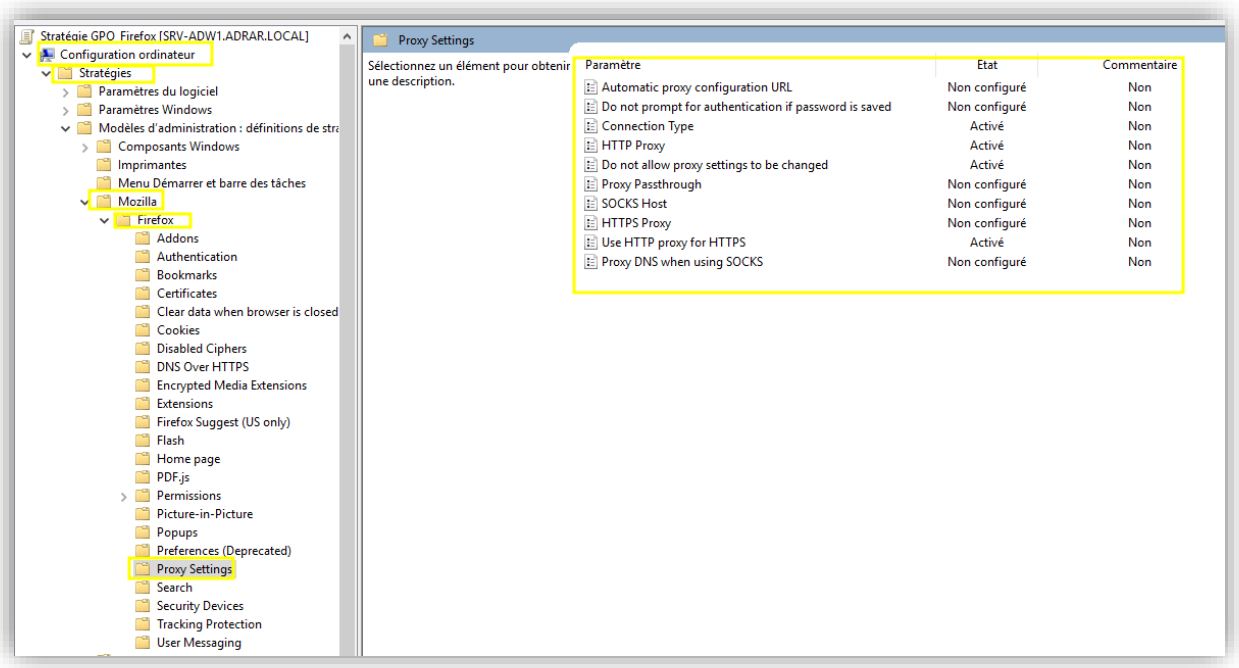
Nous ouvrons la console GPO et créons une nouvelle règle :



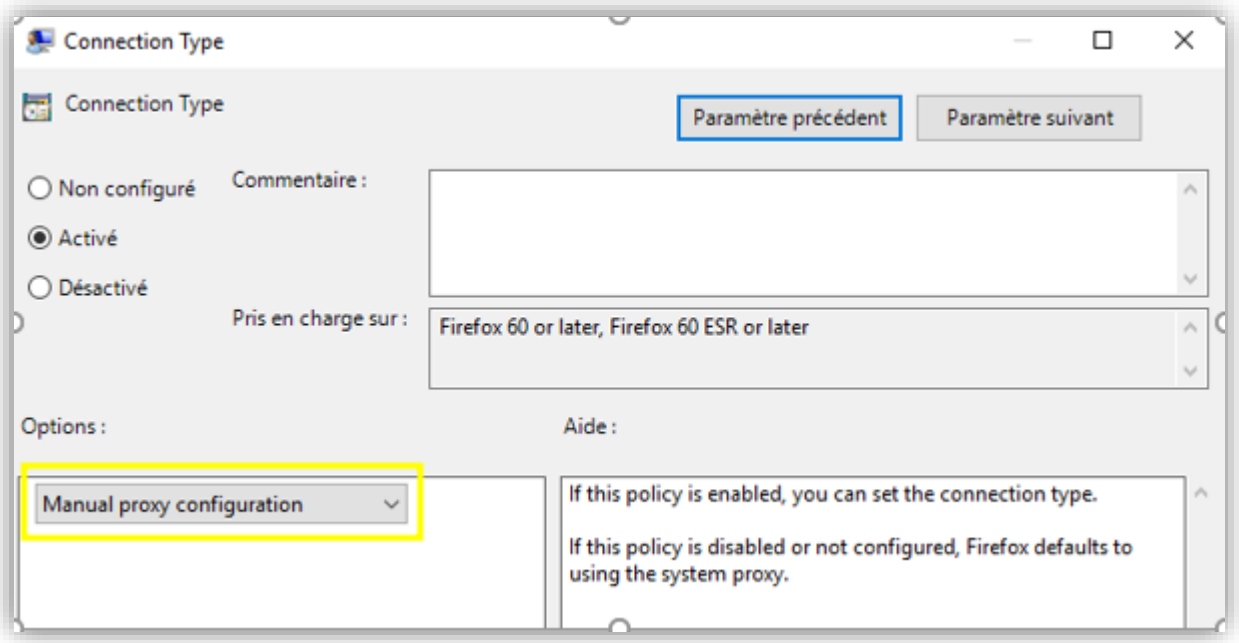
Nous nommons notre GPO



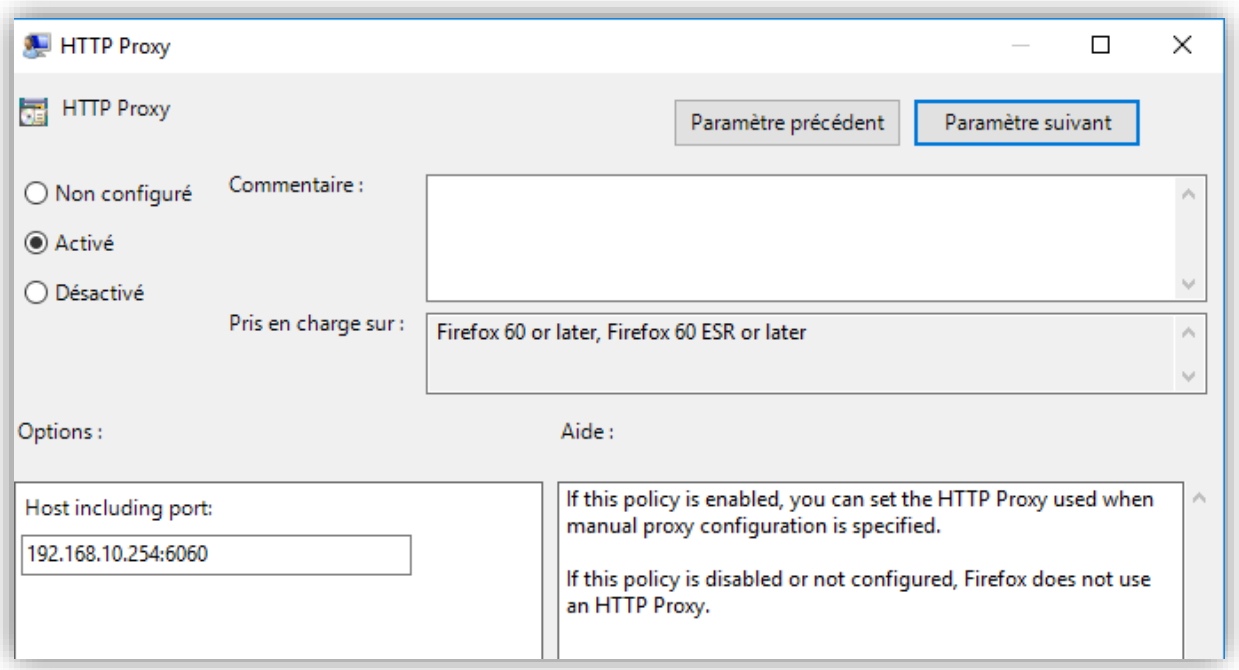
Nous allons dans la rubrique suivante et allons configurer différentes options :



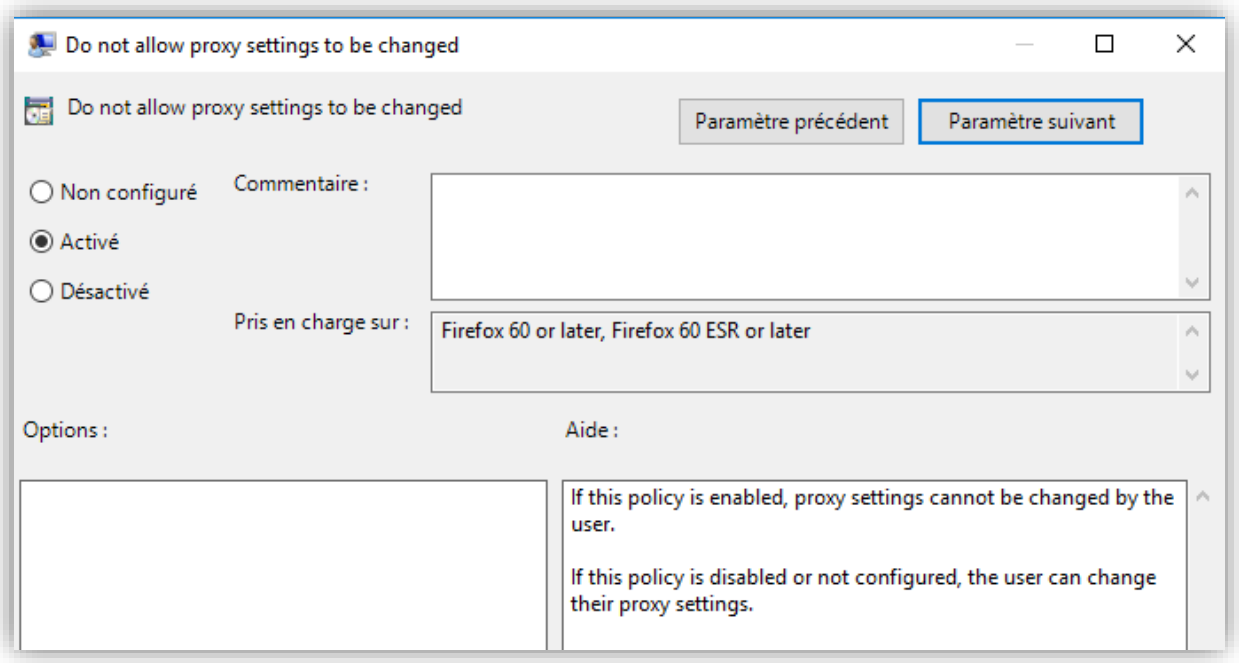
Dans **« Connection Type »** nous allons définir **« Manual Proxy configuration »** pour pousser la configuration de notre proxy sur le navigateur manuellement :



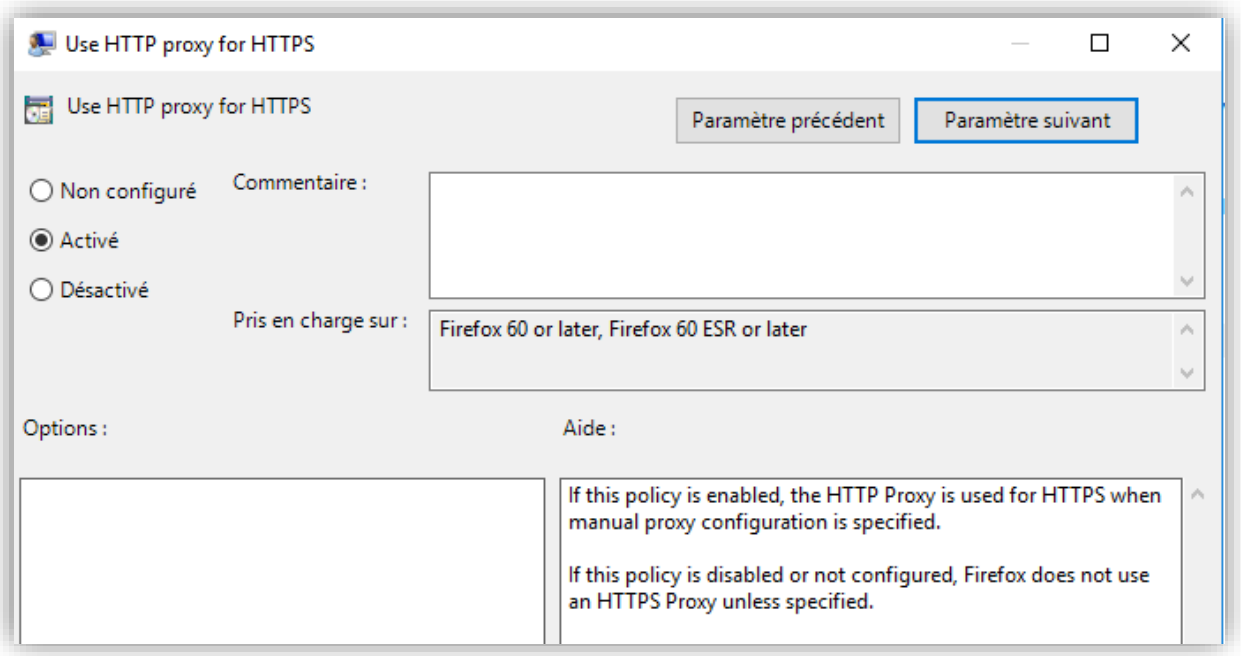
Dans ce paramètre, nous définissons l'IP et le port de notre Proxy :



Ici nous interdisons la modification des paramètres de Proxy

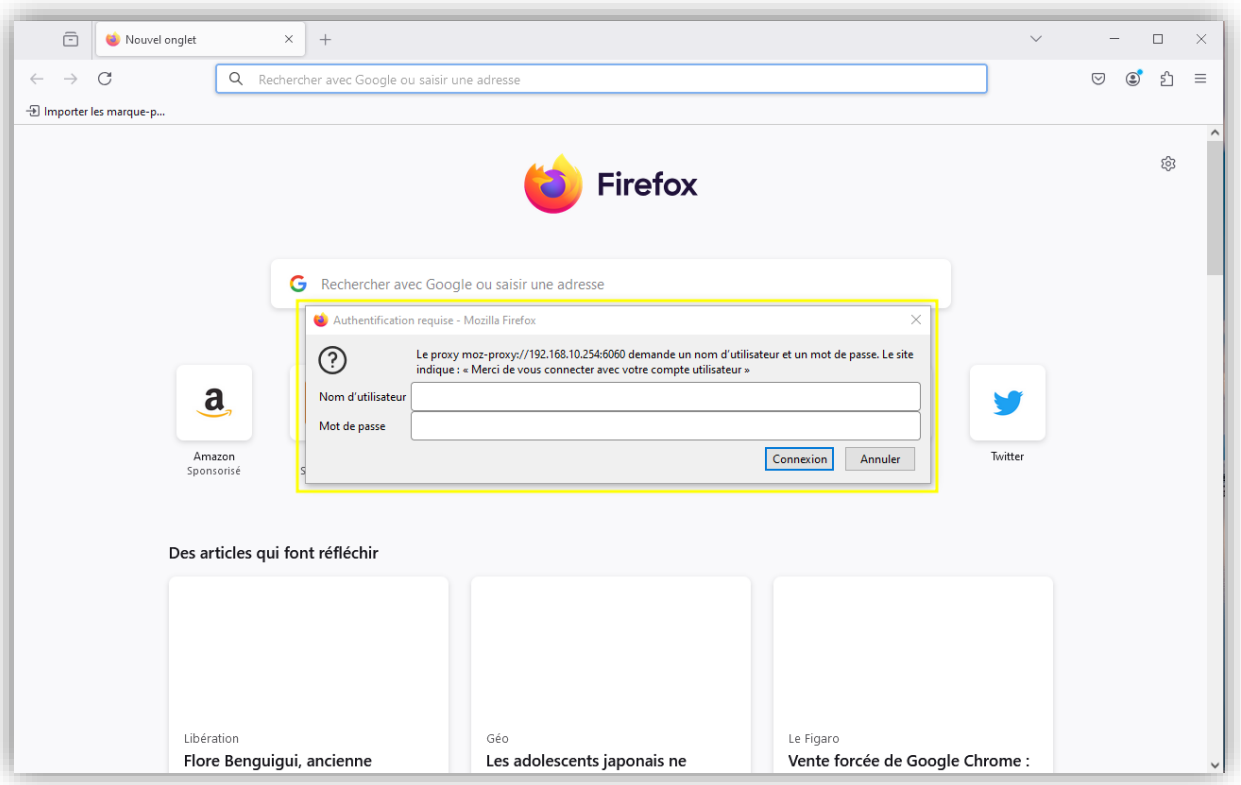


Ici, nous indiquons d'utiliser les mêmes configurations Proxy pour HTTP et HTTPS

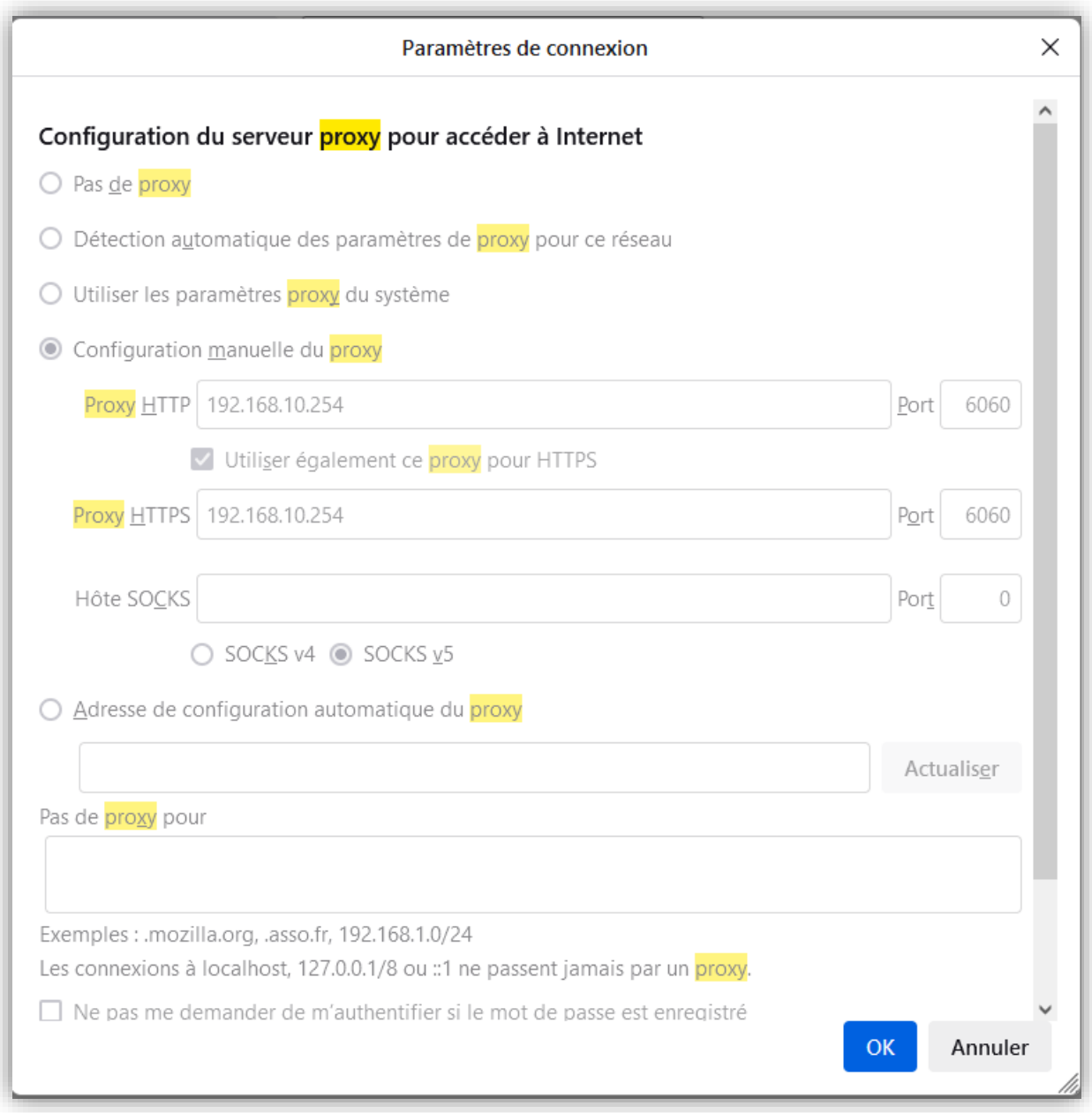


Nous pouvons maintenant effectuer notre test de validation de la GPO.

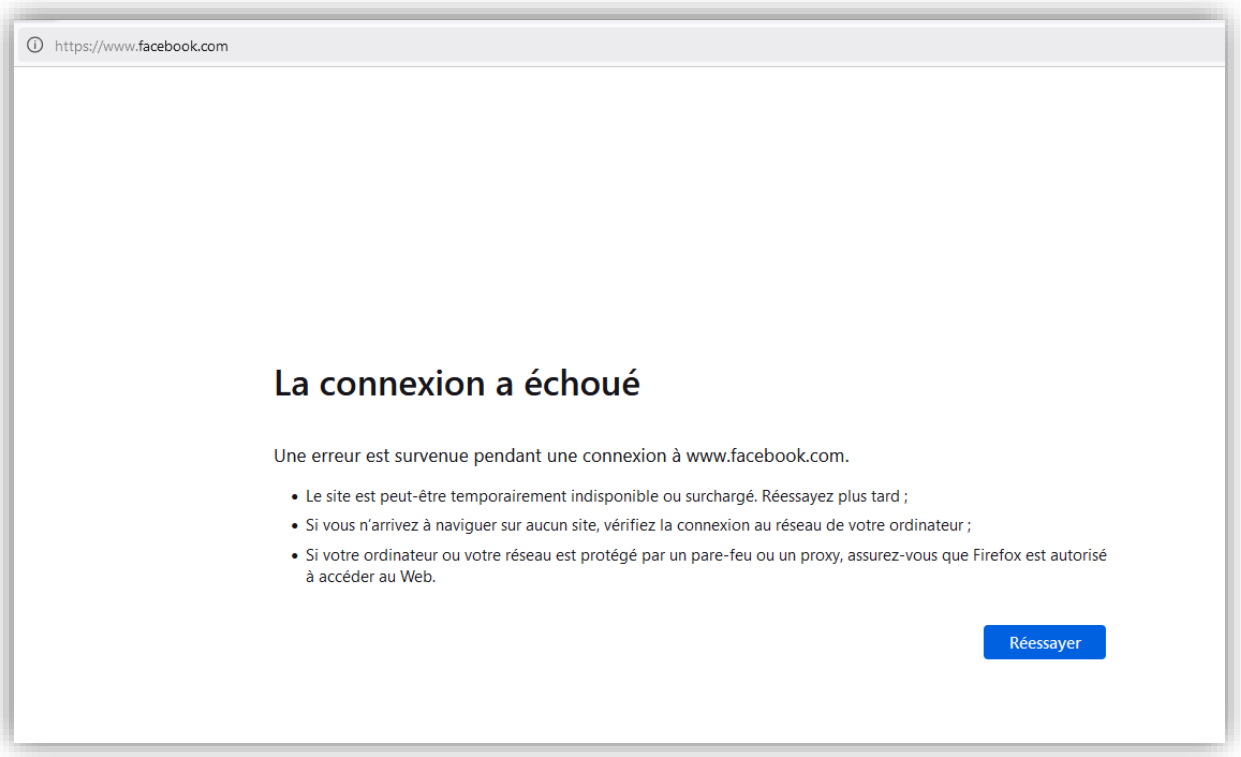
La page de connexion apparait sur le navigateur dès l’ouverture du navigateur sur le poste utilisateur :



Dans les paramètres de Proxy de Firefox, nous voyons la configuration que nous ne pouvons modifier :



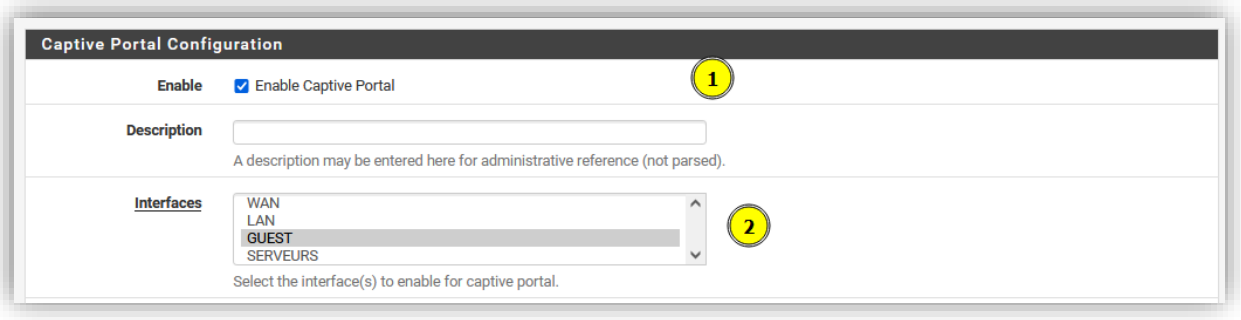
Puis nous validons le bon fonctionnement du filtrage Web :



Dans nos logs, nous voyons bien le refus par « **ACL_Stagiaires »** :

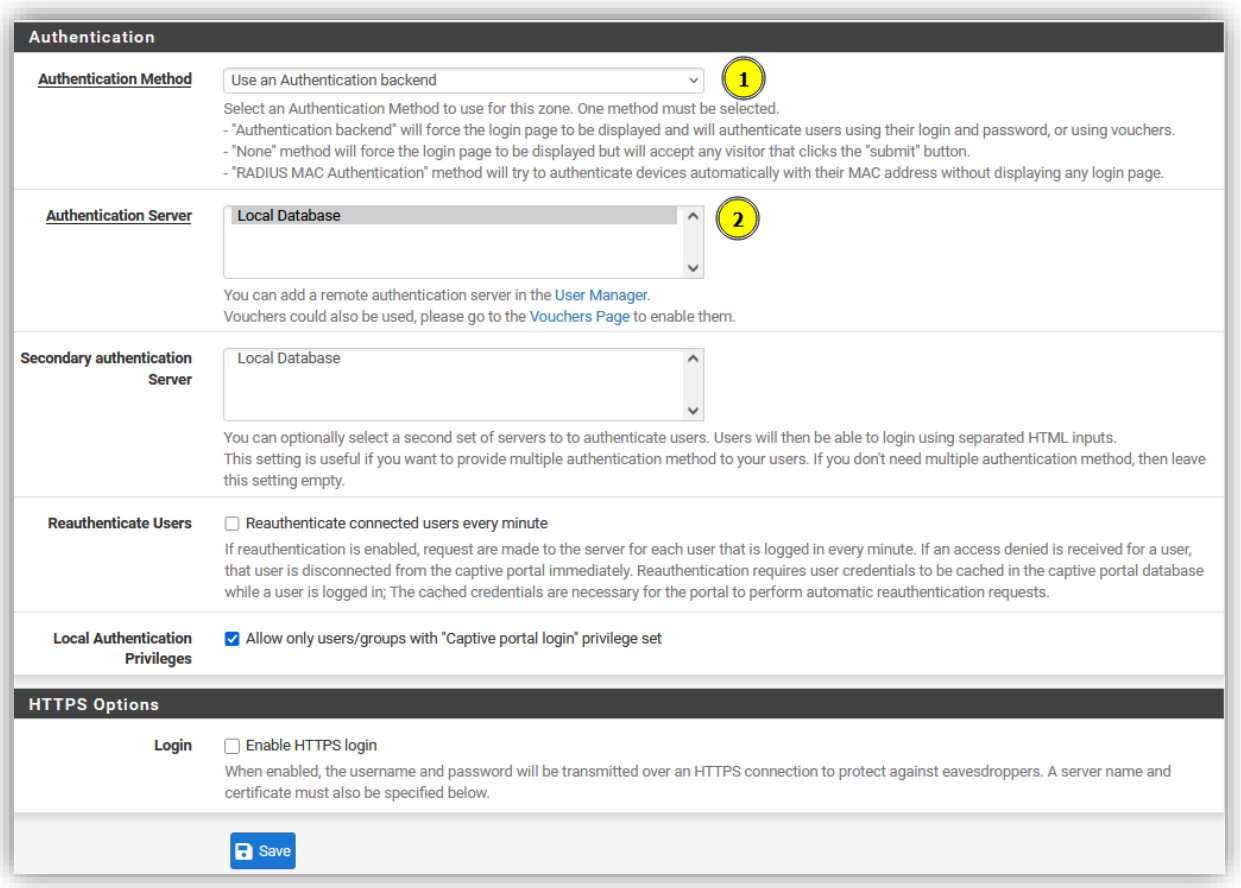
2.7 Configuration du portail captif pour les Guest

Nous commençons la configuration du portail captif dans le menu **« Services »** puis **« Captive Portal »** :



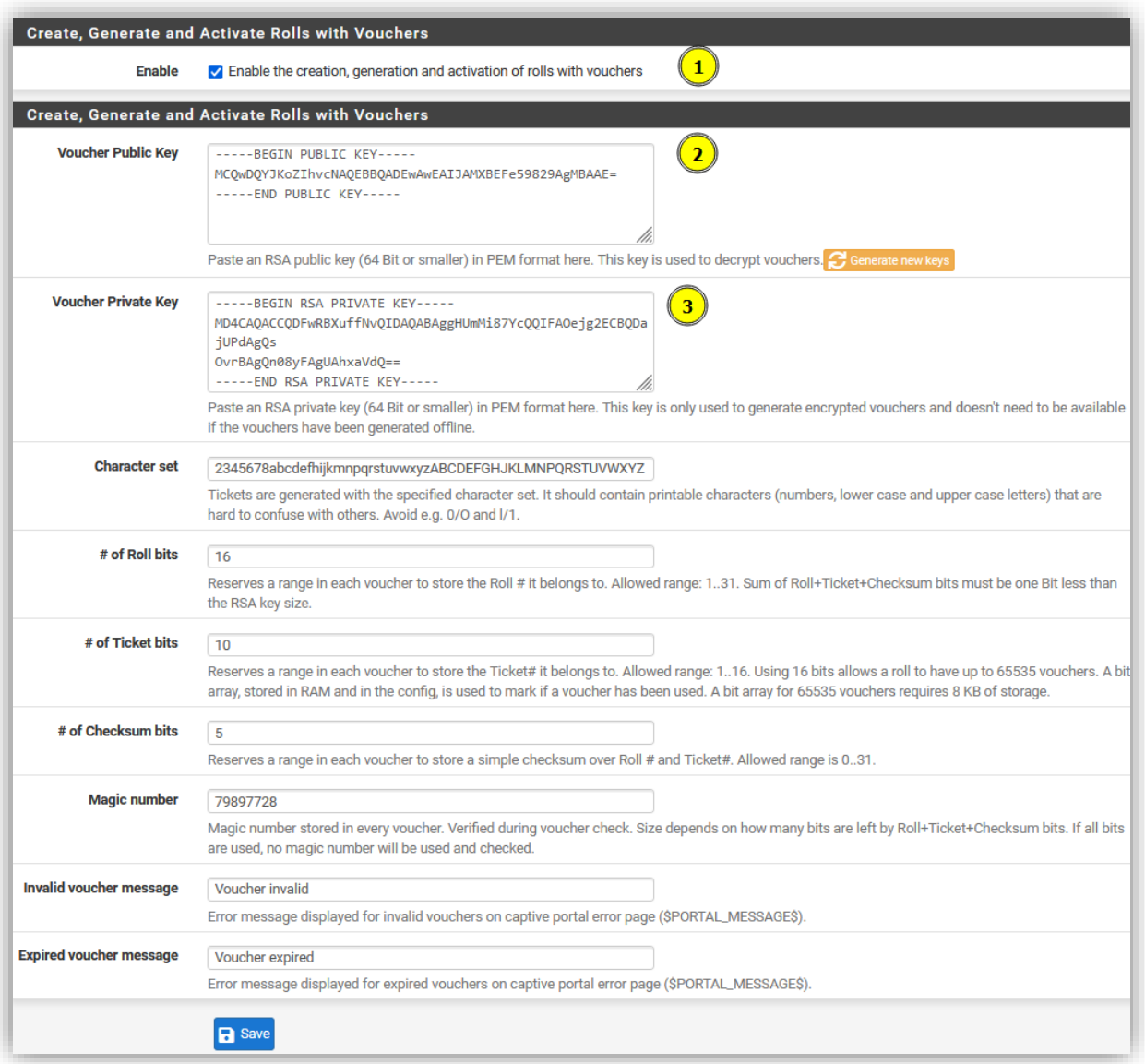
1. Activer le portail captif
2. Interface d'assignation du portail captif à l'interface Guest

Plus bas dans la page nous renseignons les paramètres suivants :



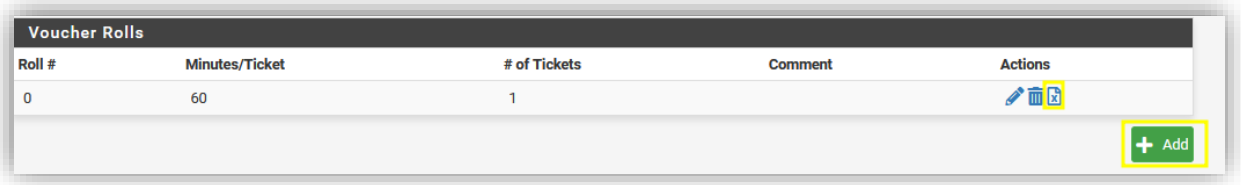
1. Authentification via une page demandant un login ou voucher
2. Authentification via la base locale (le serveur voucher étant le pare feu)

Nous pouvons désormais configurer le serveur vouchers :

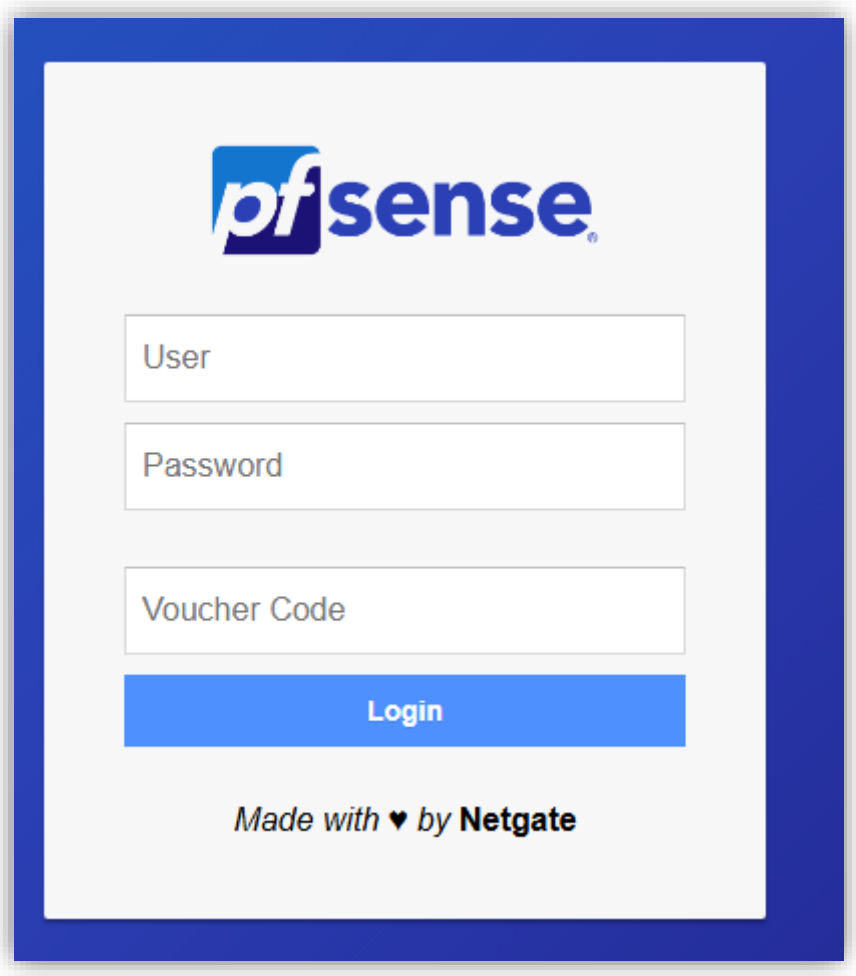


1. Activer le serveur vouchers
2. Clé privée pour déchiffrer les vouchers
3. Clé publique pour chiffrer les vouchers

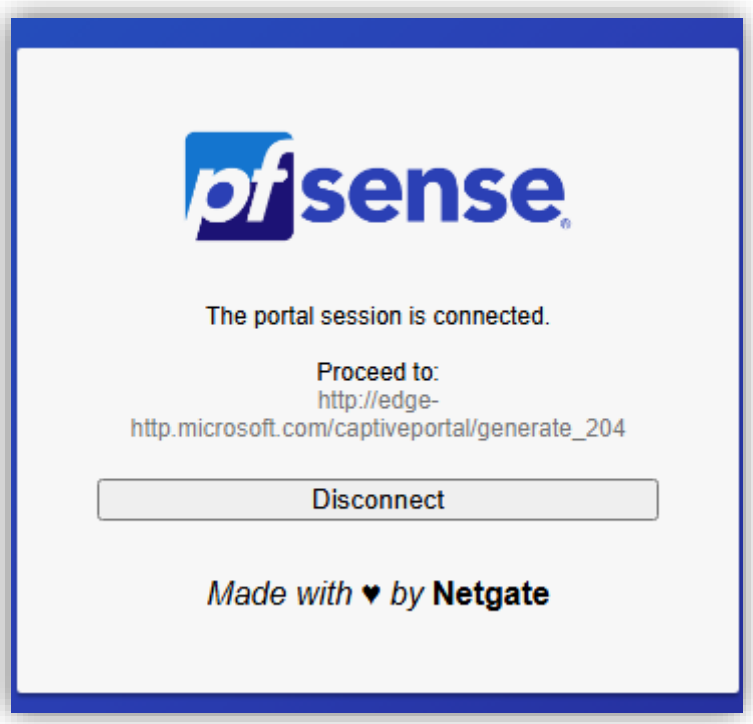
Nous générons un voucher via le bouton **« Add »** et l'exportons en CSV pour récupérer le login



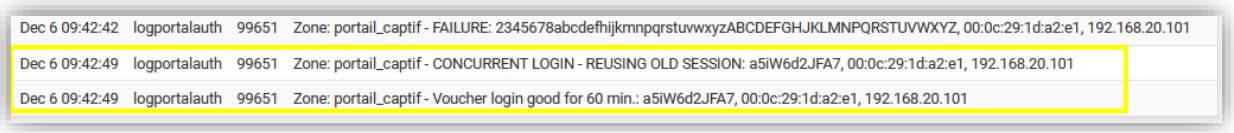
Nous allons tester maintenant notre solution.
Une fois connecté au réseau **« Guest »,** nous lançons le navigateur Firefox et voyons cette page :

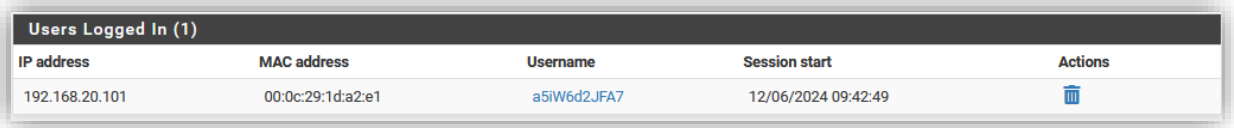


Nous renseignons les codes vouchers générés précédemment et nous constatons l'authentification acceptée :



Nous retrouvons les logs de connexion dans notre pare feu afin d'avoir les détails de la session en cours :





3. Conclusion

En réponse aux besoins d’ADRAR, nous avons conçu et mis en place une solution de Proxy basée sur Pfsense avec Squid et ses extensions, permettant de sécuriser et de contrôler efficacement les accès Internet. Cette infrastructure offre :

- Filtrage Web avancé : Une gestion personnalisée des accès basée sur les groupes LDAP (Formateurs, Stagiaires) pour une navigation adaptée et sécurisée.
- Portail captif : authentification via vouchers pour les visiteurs et limitation des accès via un VLAN Guest étanche et sécurisé.
- Journalisation conforme : Conservation des logs utilisateurs pour une durée de 180 jours, respectant les obligations légales.
- Sécurité renforcée : Proxy explicite sans SSL bump pour une meilleure conformité RGPD.

Cette solution fiable, évolutive et intégrée garantit la sécurité et l’efficacité des flux Internet tout en répondant aux exigences réglementaires.

4. Annexes

Documentation ANSSI sur la mise en place d'un Proxy : https://cyber.gouv.fr/sites/default/files/2012/01/anssi-guide-passerelle_internet_securisee-v2.pdf

Documentation RGPD : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Installation et paramétrage de Pfsense : https://www.it-connect.fr/installation-de-pfsense%EF%BB%BF/

Configuration de Squid et Squid Guard sur Pfsense : https://www.it-connect.fr/pfsense-et-squid-ajouter-le-filtrage-par-categories-avec-squid-guard/

Configuration de LightSquid : https://www.pc2s.fr/pfsense-proxy-transparent-filtrage-web-url-squid-squidguard/

Configuration du portail captif Pfsense : https://www.comparitech.com/blog/vpn-privacy/captive-portal-pfsense/

Configuration des vouchers sur Pfsense : https://docs.netgate.com/pfsense/en/latest/captiveportal/vouchers.html