Parefeu Pfsense

Sommaire

Objectif

Prérequis

Procédure de mise en place du Firewall pfSense

1. Installation de pfSense

Télécharger l'image ISO

Rendez-vous sur : https://www.pfsense.org/download/.
Sélectionnez la version 2.7 en 64 bits.

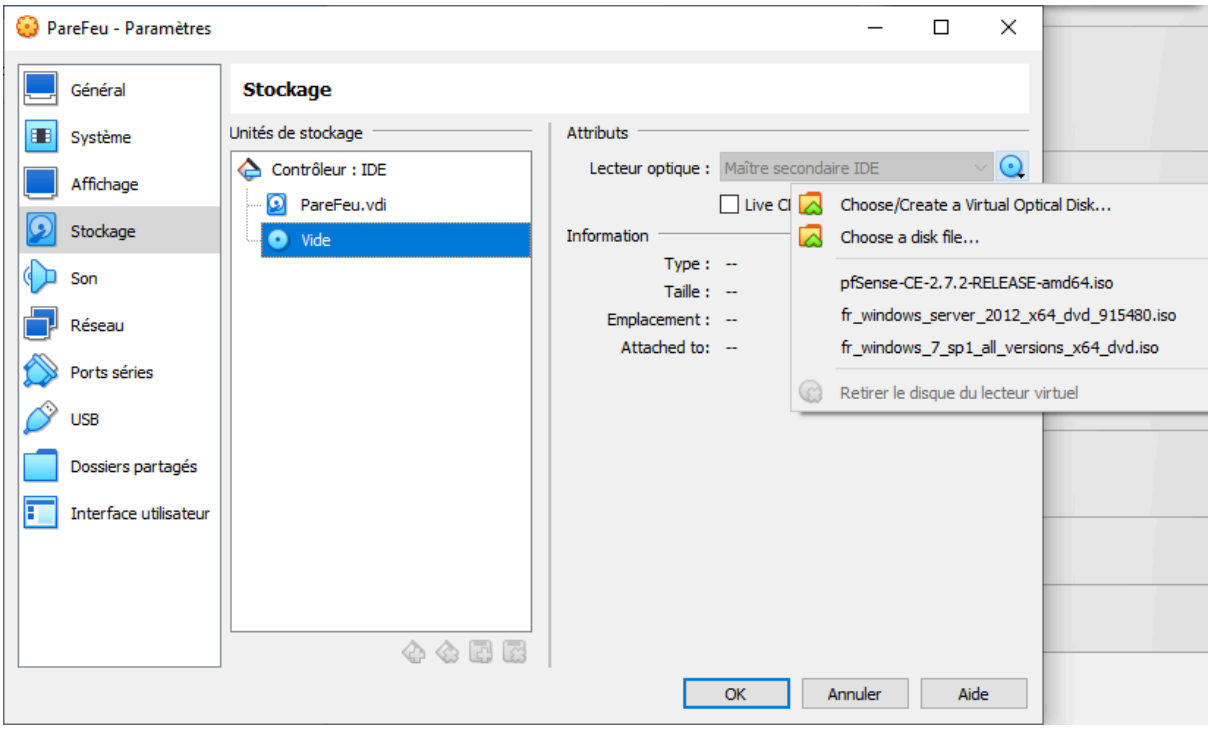
Création de la machine virtuelle (VM) sur VirtualBox

Ouvrir VirtualBox et cliquer sur Nouvelle machine.
Type : BSD
Version : FreeBSD (64-bit)
Attribuer 2 Go de RAM et 10 Go de disque dur (VHD ou VDI, en mode dynamique).
Ajouter deux cartes réseau :

Carte 1 : Mode Bridge (connectée au WAN).
Carte 2 : Mode Réseau privé hôte (LAN).

Installation de pfSense

Démarrer la VM avec l'ISO pfSense.
Suivre les étapes d'installation en gardant les paramètres par défaut.
Éteindre la VM et retirer l'iso :

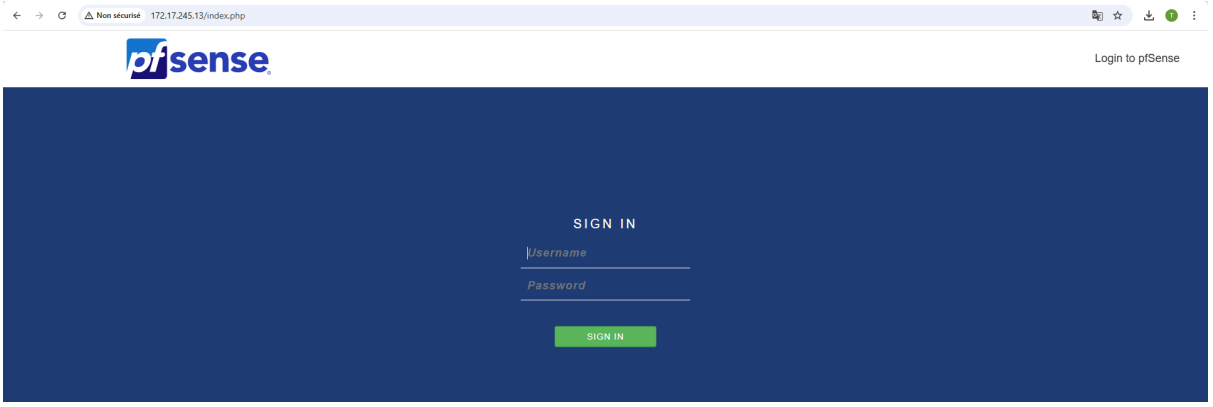


Après redémarrage, configurer les interfaces réseau :
WAN : 172.17.245.13/16
LAN : 192.168.1.254/24
Désactiver DHCP et IPv6 sur l'interface LAN.

2. Configuration via l'interface Web

Connexion à l'interface

Depuis un poste du réseau LAN, ouvrez un navigateur et entrez :
http://172.17.245.13 **ou seulment 172.17.245.13**



Si ça ne fonctionne pas :
entrez en mode commande shell

Pour se connecter :

Utilisateur : admin
Mot de passe : pfsense

Suivre l'assistant de configuration :

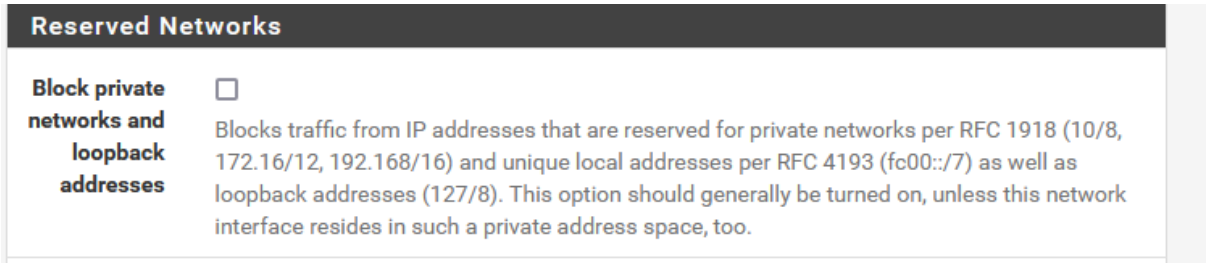
Nom d'hôte : redline.local
DNS : 8.8.8.8
Serveur NTP : 0.fr.pool.ntp.org

Pensez à modifier le mot de passe administrateur.

3. Configuration du firewall

Vérifier le NAT

Accéder à Firewall > NAT > Outbound.
Vérifier que le NAT automatique est activé pour translater le LAN vers le WAN.
Autoriser le ping sur WAN



Aller dans Firewall > Rules > WAN.
Désactiver la règle qui bloque tout le trafic privé.

Créez une règle qui autorise uniquement le réseau 172.17.0.0/16 à faire des pings et activez les logs :

Ajouter une règle bloquant tout le reste :

Tester avec un ping depuis un client du réseau WAN.

✗	Mar 11 13:37:14	WAN	Default deny rule IPv4 (1000000103)	172.17.12.30:138	172.17.255.255:138
✓	Mar 11 13:37:19	WAN	USER_RULE (1741626246)	172.17.13.11	172.17.245.13
✗	Mar 11 13:37:24	WAN	Default deny rule IPv4 (1000000103)	172.17.12.30:138	172.17.255.255:138
✗	Mar 11 13:37:25	LAN	Default deny rule IPv4 (1000000103)	192.168.1.252	192.168.1.254
✗	Mar 11 13:37:30	LAN	Default deny rule IPv4 (1000000103)	192.168.1.252	192.168.1.254
✗	Mar 11 13:37:35	LAN	Default deny rule IPv4 (1000000103)	192.168.1.252	192.168.1.254
✗	Mar 11 13:37:40	LAN	Default deny rule IPv4 (1000000103)	192.168.1.252	192.168.1.254

4. Mise en place du filtrage Web

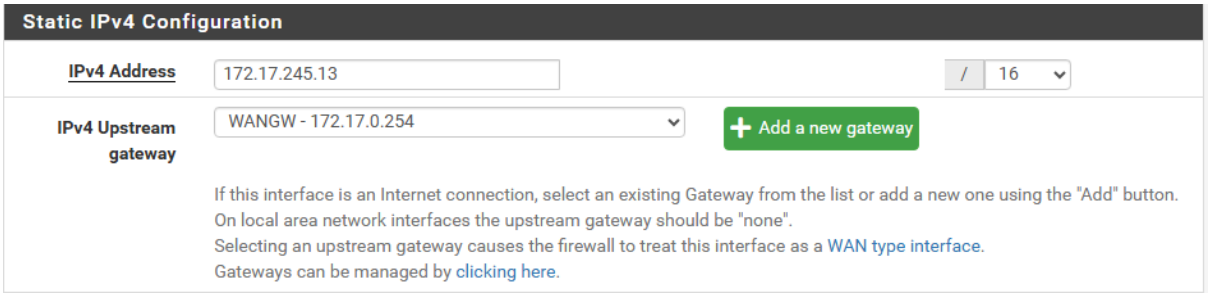
4.1. Installation de Squid (Proxy)

Installation des paquets

Aller dans System > Package Manager > Available Packages.
Installer Squid, SquidGuard et LightSquid.
Configuration de Squid

Si ça marche pas :

Mettre la passerelle dans l'interface web :



Taper cette command dans la vm pfsense :

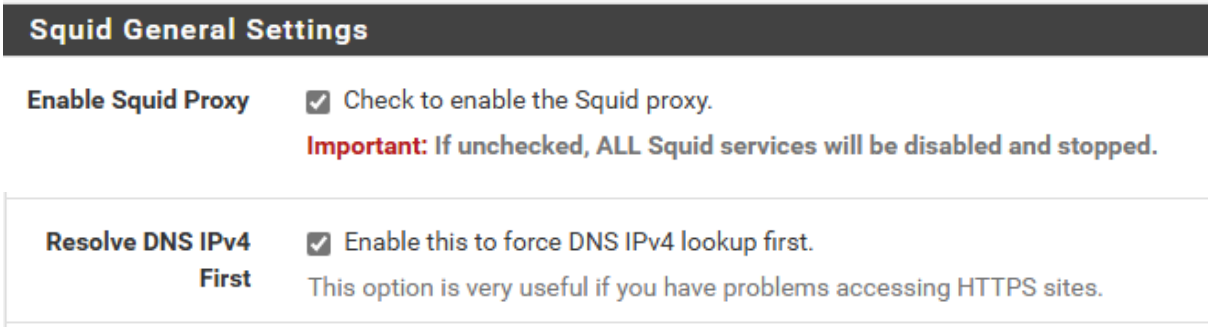
```
pkg-static install -fy pkg pfSense-repo pfSense-upgrade
```

Aller dans System > Cert Manager.
Donnez un nom au certificat (CSI CA), ne changez rien d'autre.

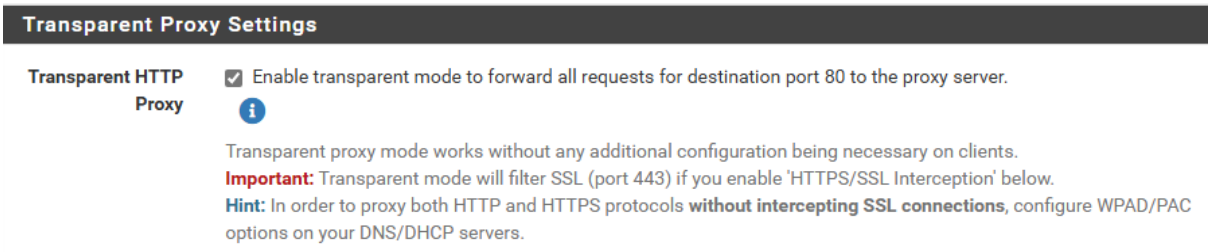
Accéder à Services > Squid Proxy Server.
Configurez Squid (Local Cache)

- Heap LFUDA, low 90% et high 95%
- Taille du cache 500
- Cache System ufs
- Level 1 directories 16
- Cache location /var/squid/cache
- Memory 64

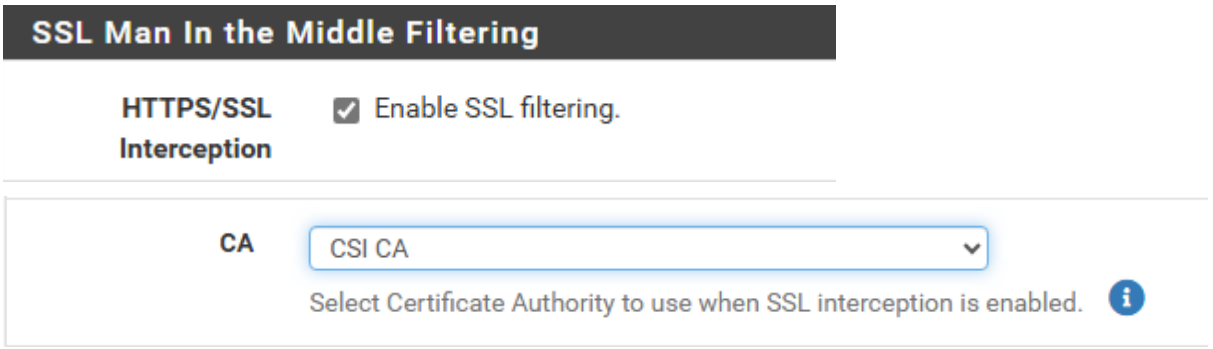
Dans l'onglet « Général », activez « Enable Squid Proxy » et « Resolve DNS Ipv4 fisrt » :



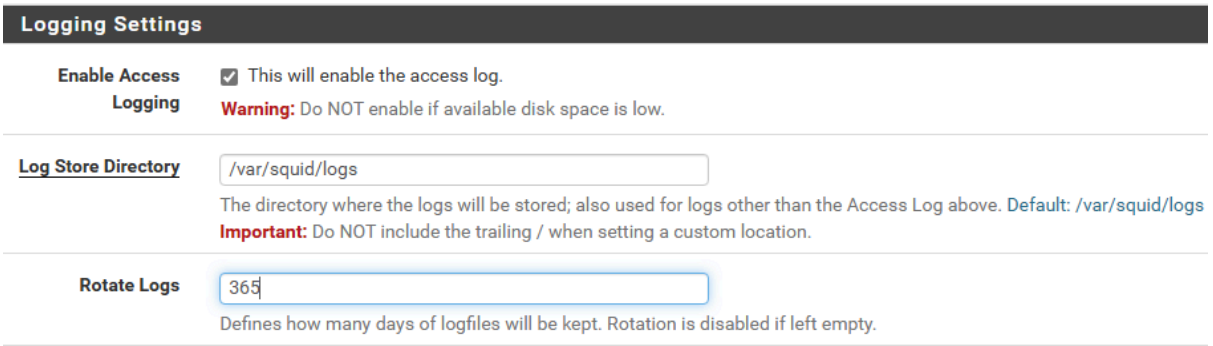
Activez le proxy transparent (interface LAN)



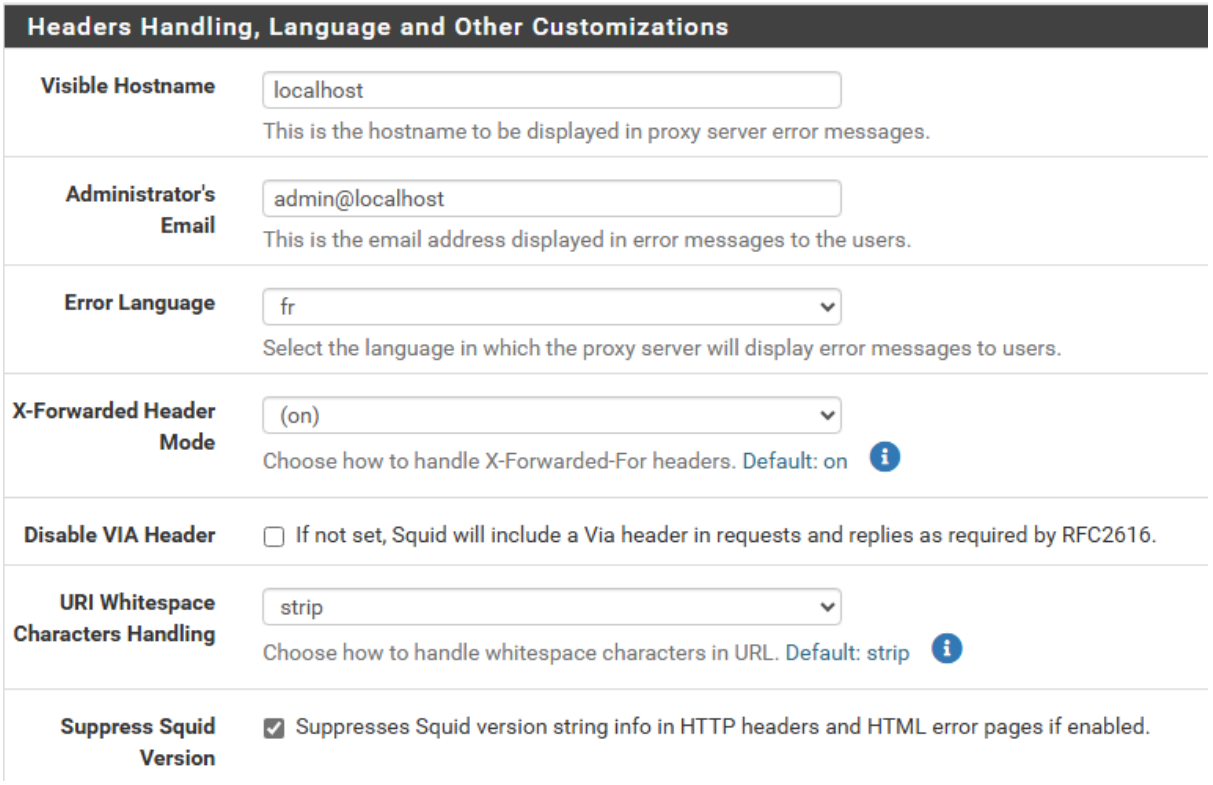
Activez "HTTPS/SSL Interception SSL filtering" , sélectionner "Splice All" et le Certificat précédemment créé "CSI CA".



Activez "Enable Access Logging" et définir combien de jours les logs seront conservés (365 jours).



Sélectionnez “fr” pour “Error language” et Activer “Suppress Squid Version”

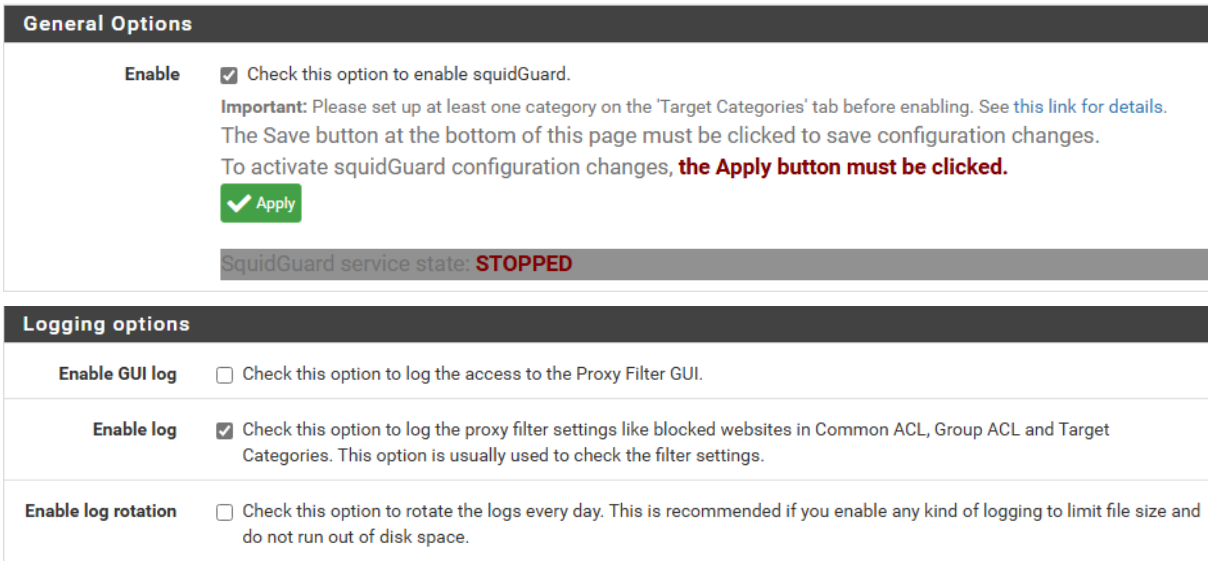


Cliquez sur “Save” pour enregistrer toutes les modifications effectuées dans Squid

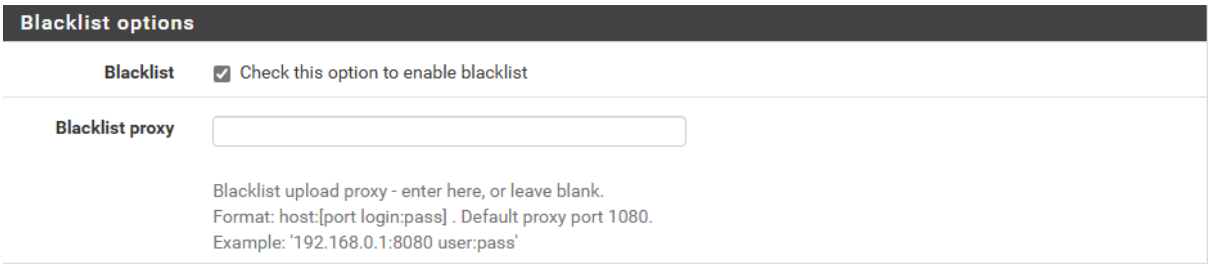
4.2. Configuration de SquidGuard (Filtrage de contenu)

Activer SquidGuard

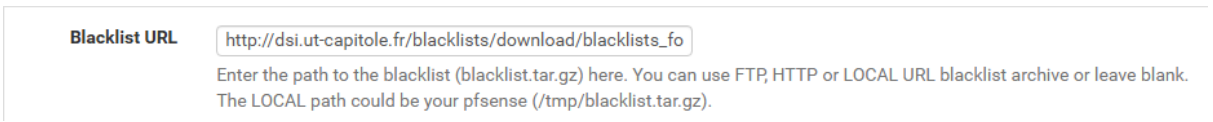
Aller dans Services > SquidGuard Proxy Filter.
Activer Enable SquidGuard et Enable Log.



Ajouter une liste noire

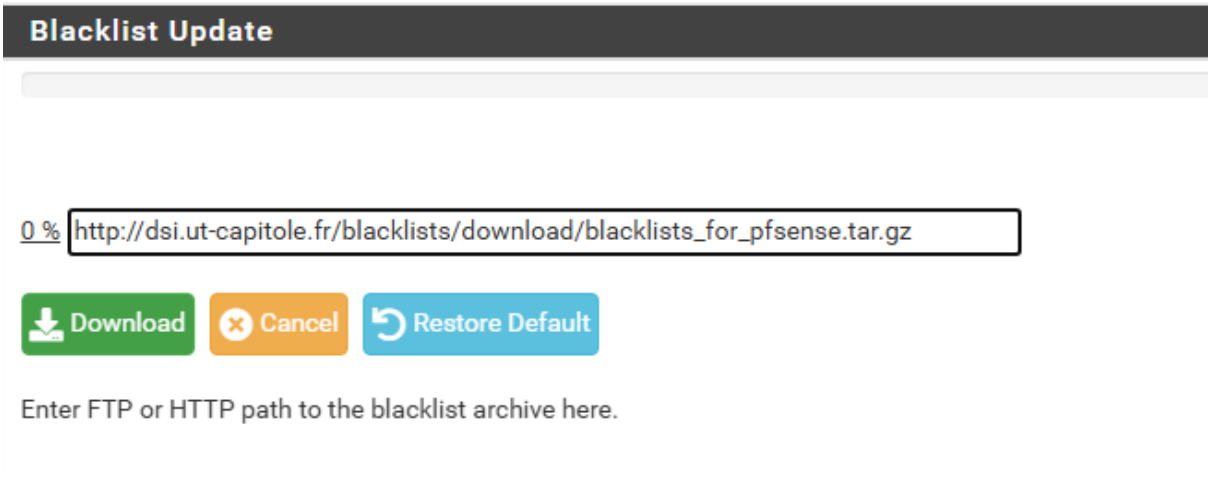


Dans l'onglet Blacklist, insérer l'URL :
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz



cliquez sur "Save"

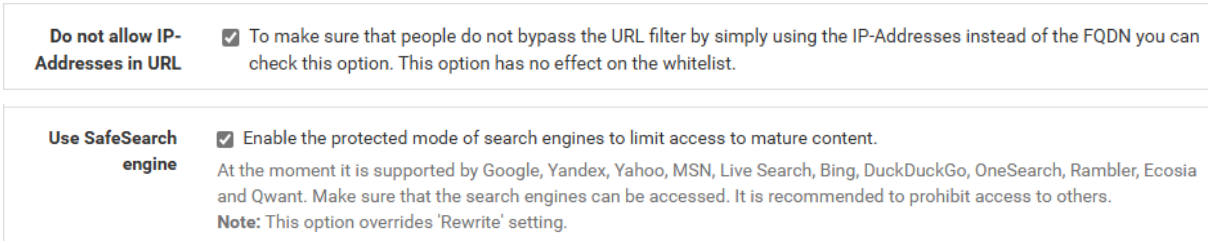
Dans l'onglet "Blacklist" : Cliquer sur "Download" pour télécharger les listes de filtrage.



Dans l'onglet 'Common ACL", cliquez, dans "Target Rules List" sur le " + "

Sélectionner les catégories à bloquer ou à autoriser (Sélectionner "Allow" pour Default access [all])

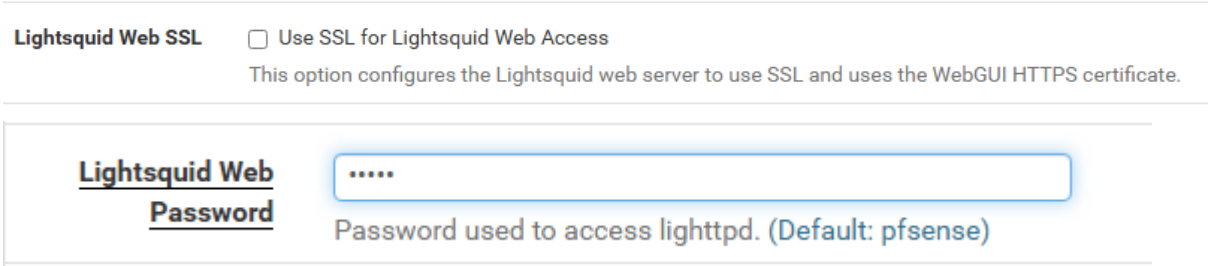
Cochez "Do not allow IP addresses in URL" et "Use SafeSearch engine" puis cliquer "Save".



4.3. Activation des logs LightSquid

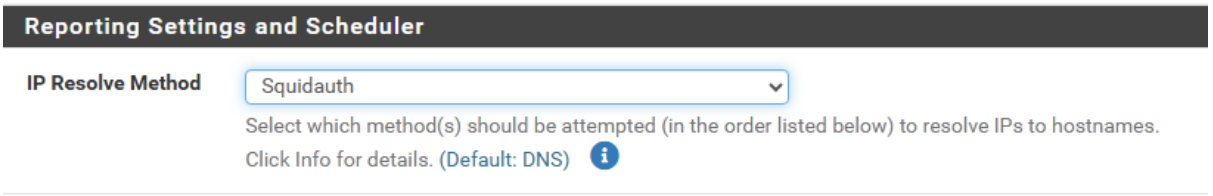
Configurer LightSquid

Accéder à Status > Squid Proxy Reports.
Décochez "LightSquid Web SSL" pour une connexion Web en HTTP et définissez le mot de passe de l'utilisateur admin.



Sélectionnez le language French

Sélectionnez “SquidAuth” pour “IP Resolve Method” et “60min” pour “Refresh Scheduler” puis cliquez “Save” et “Refresh Full”.



AIDE

1. Annexe

2. Commandes utiles

- Pour examiner les erreurs système et les événements. : journalctl -xe
- Fichier pour voir les logs : cat /var/log/syslog
- voir les 25 dernière ligne d’un fichier : tail -n 25 /var/log/syslog
- Voir le début d’un fichier : head /var/log/syslog
- Voir l’état du service : systemctl status *nom du service*