Mise en place pare-feu avec proxy web

Table des matières

Le système Ipfire permet de mettre en place une solution proxy pour contrôler notamment le trafic internet et bloquer l'accès à certains sites ou mots clés.

La gestion du service est accessible depuis l'onglet ***Réseau*** du webconfigurator (ce service doit aussi pouvoir être géré directement depuis le terminal du pare-feu).

1. Activer le proxy web :

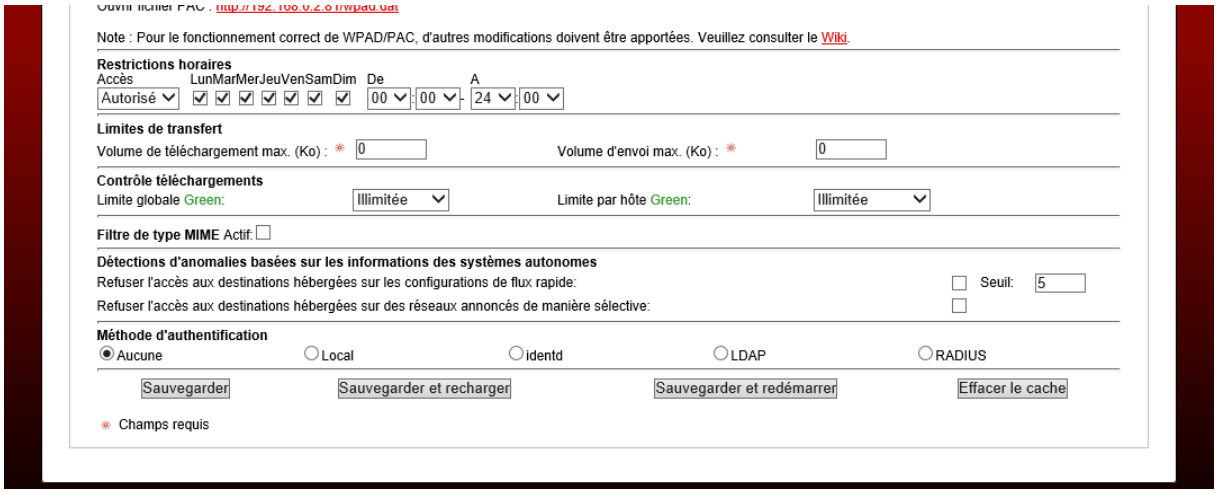
Pour activer le service de proxy web, vous devez activer (en mode normal ou transparent) le service depuis l'interface web.

Le port par défaut est 800 pour le proxy et 3128 pour le proxy transparent (les ports sont personnalisables).

Activez le filtre URL ainsi que la mise à jour accélérateur, changez la langue des messages en fr.

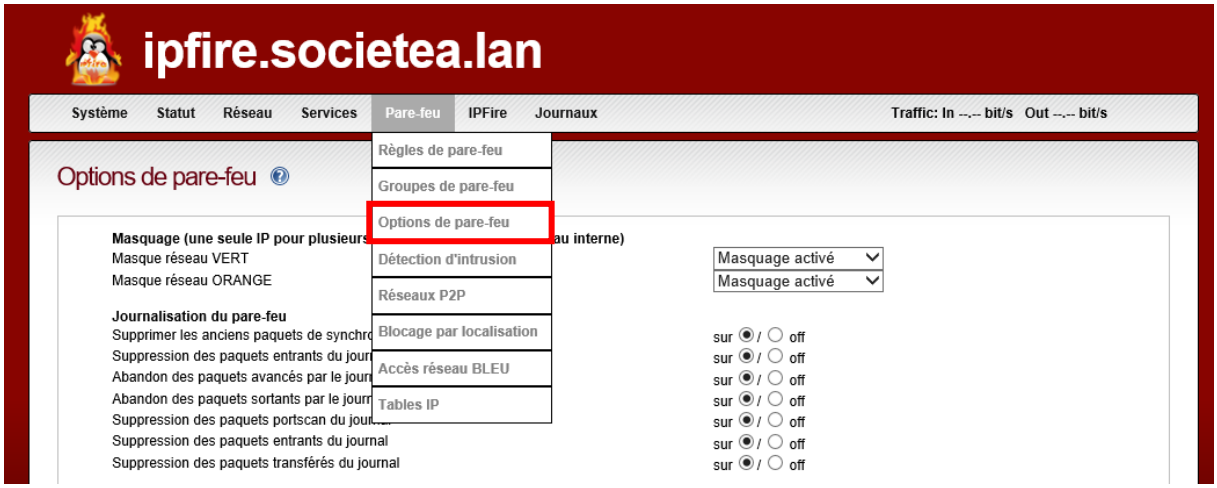
Plus bas dans ce menu, vous trouverez différents paramétrages possibles :

- Mise en place de restrictions horaires.
- Limitation des volumes de transfert par réseau et/ou hôte.
- Méthode d'authentification pour le proxy web.

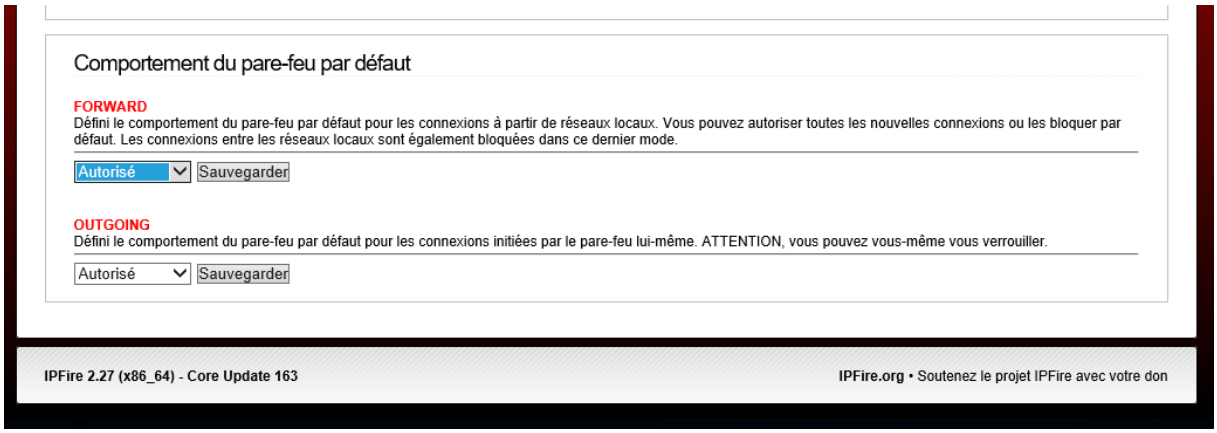


N'oubliez pas de sauvegarder les changements que vous venez d'appliquer.

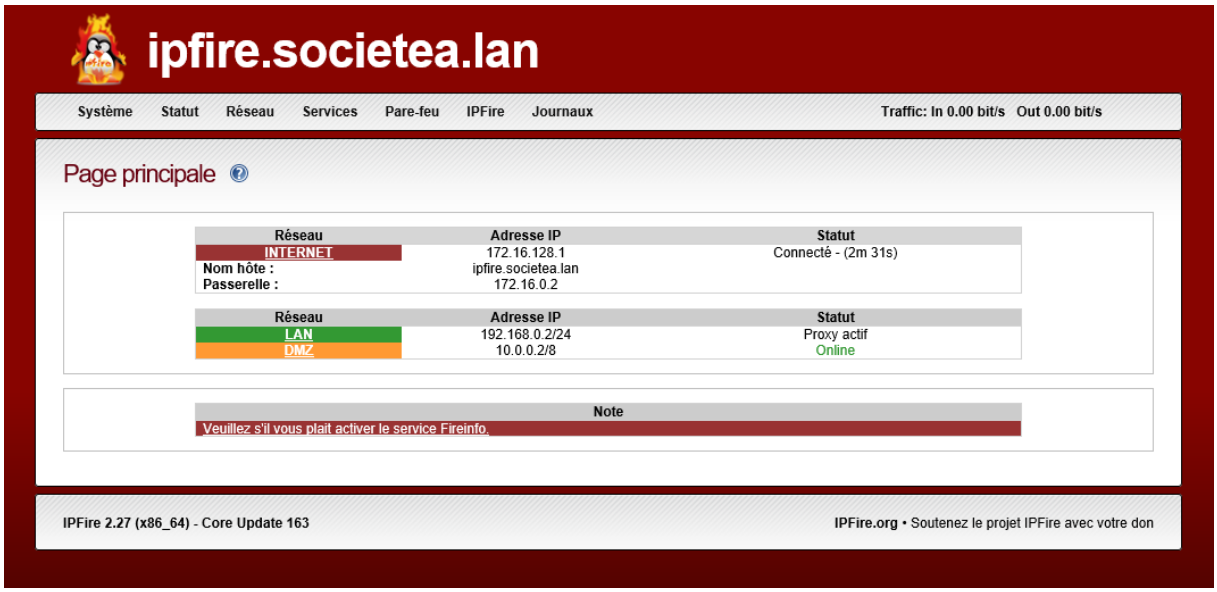
Affichez les options de pare-feu permet d'activer/désactiver différentes options pour le proxy.



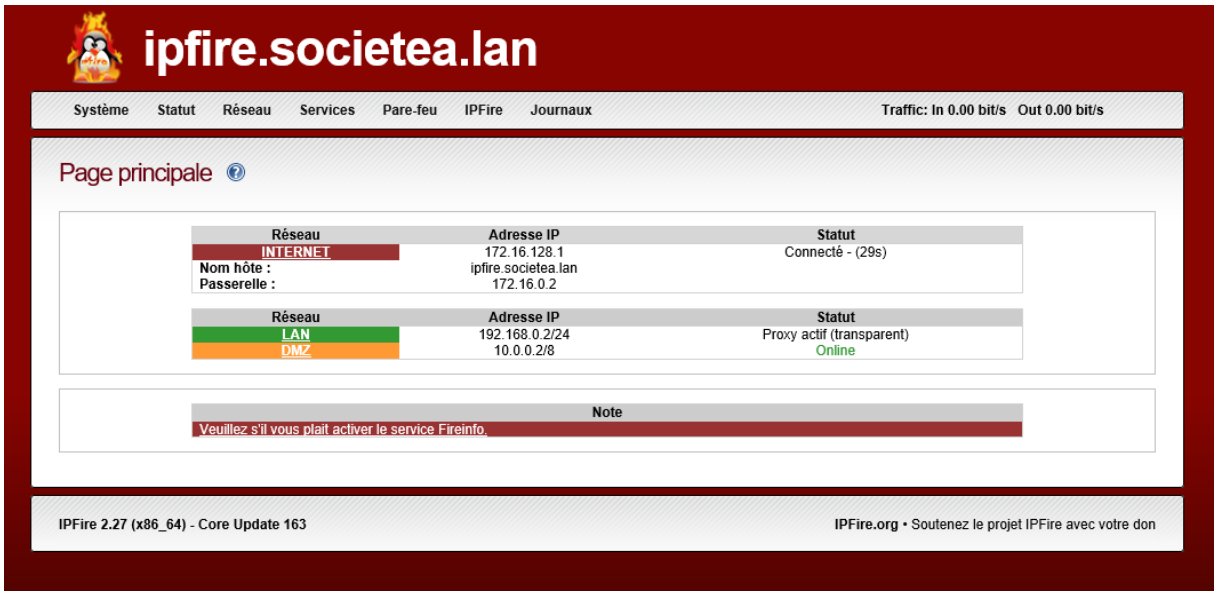
En bas du menu, vérifiez que le pare-feu autorise le flux Forward et Outgoing.



L’état actuel du pare-feu est visible directement dans l’onglet accueil du tableau de bord, ci-dessous le proxy est actif.



Ci-dessous le proxy est actif mais en mode transparent.



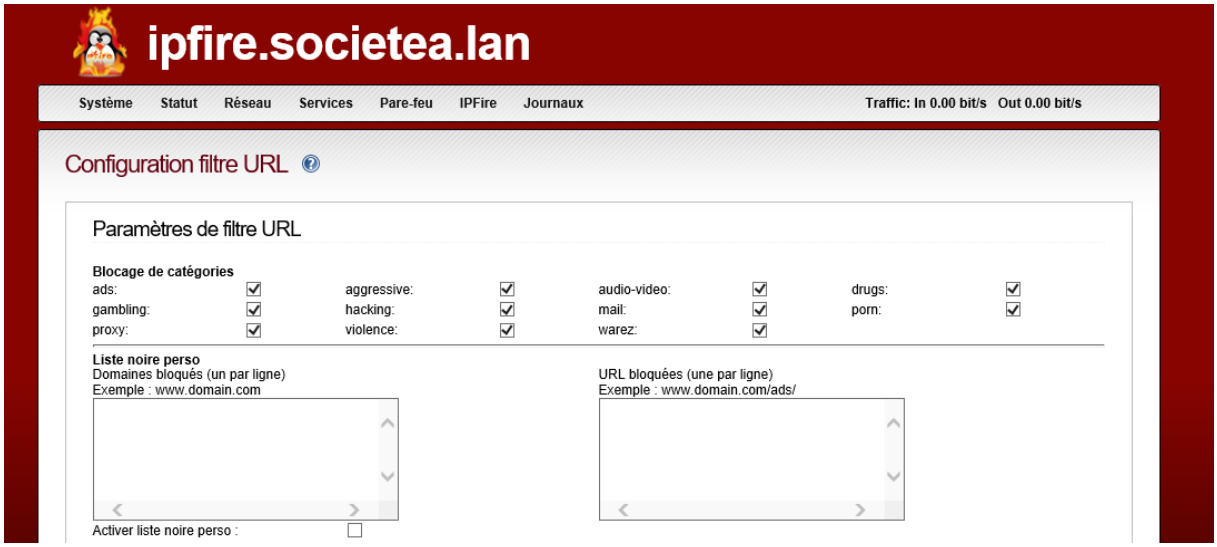
2. Gestion du filtre de contenu URL :

Le service proxy web va permettre de faire l'intermédiaire entre les requêtes http/https des différents clients du réseau LAN avec les serveurs web du réseau WAN.

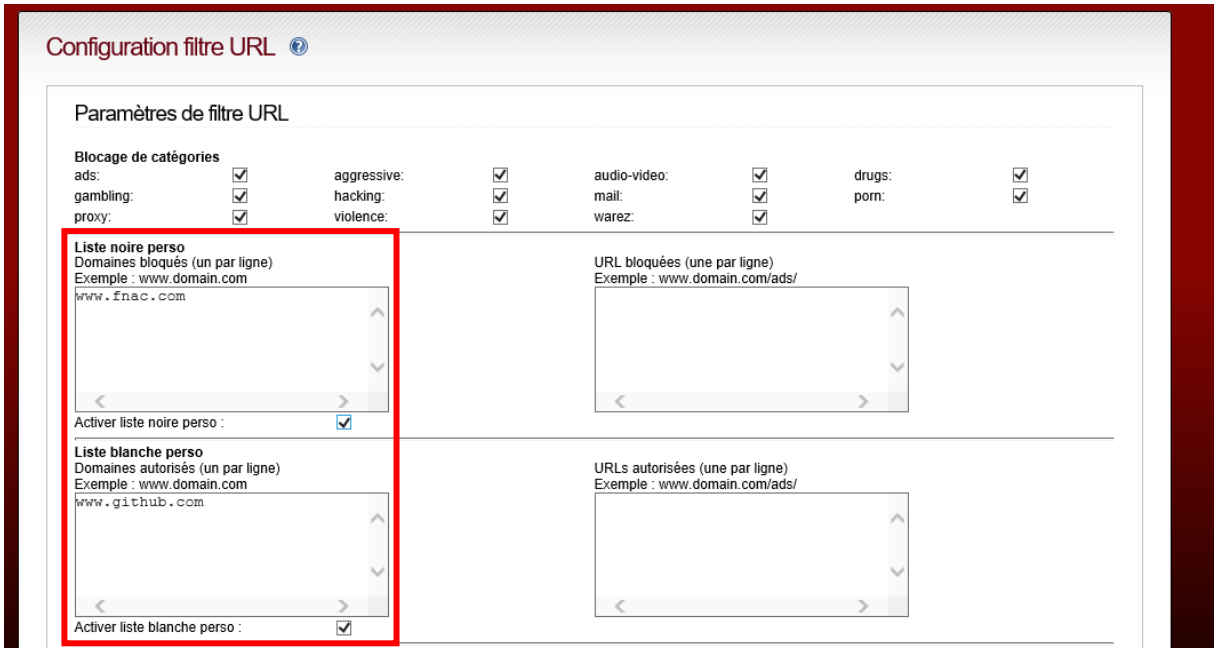
Cet intermédiaire va pouvoir filtrer les différentes requêtes http/https, ce qui vous permettra de mettre en place des restrictions au niveau de la navigation internet au sein du réseau LAN.

La gestion du filtre de contenu URL se trouve aussi dans le menu Réseau.

La première partie du menu comporte un choix de blocage prédéfini suivant différentes catégories, activez les catégories dont vous souhaitez bloquer les requêtes.



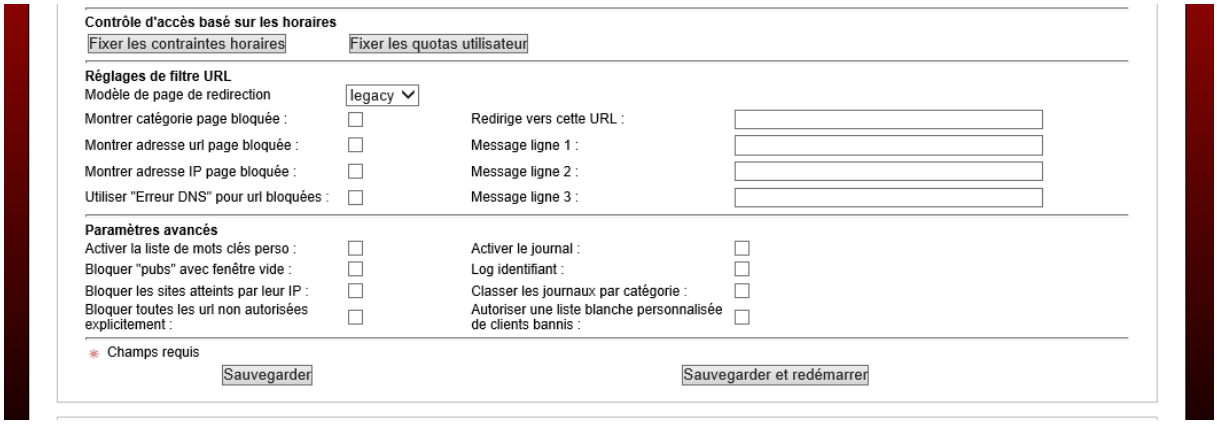
La ***liste noire perso*** permet de définir des domaines et/ou des URL à bloquer.



Dans l'exemple ci-dessus, toutes les catégories doivent être bloquées, ainsi que le domaine www.fnac.com qui est ajouté à la liste noire.

A l'inverse des listes noires, il existe une personnalisation de ***liste blanche*** par domaine et/ou URL permettant d'autoriser systématiquement la navigation des domaines/URL qui sont définis au sein de cette liste.

Vous pouvez affiner les paramètres avec des contraintes horaires et des quotas parmi les listes définies, il est aussi possible d'établir une liste personnalisée de mots clés à autoriser ou interdire.

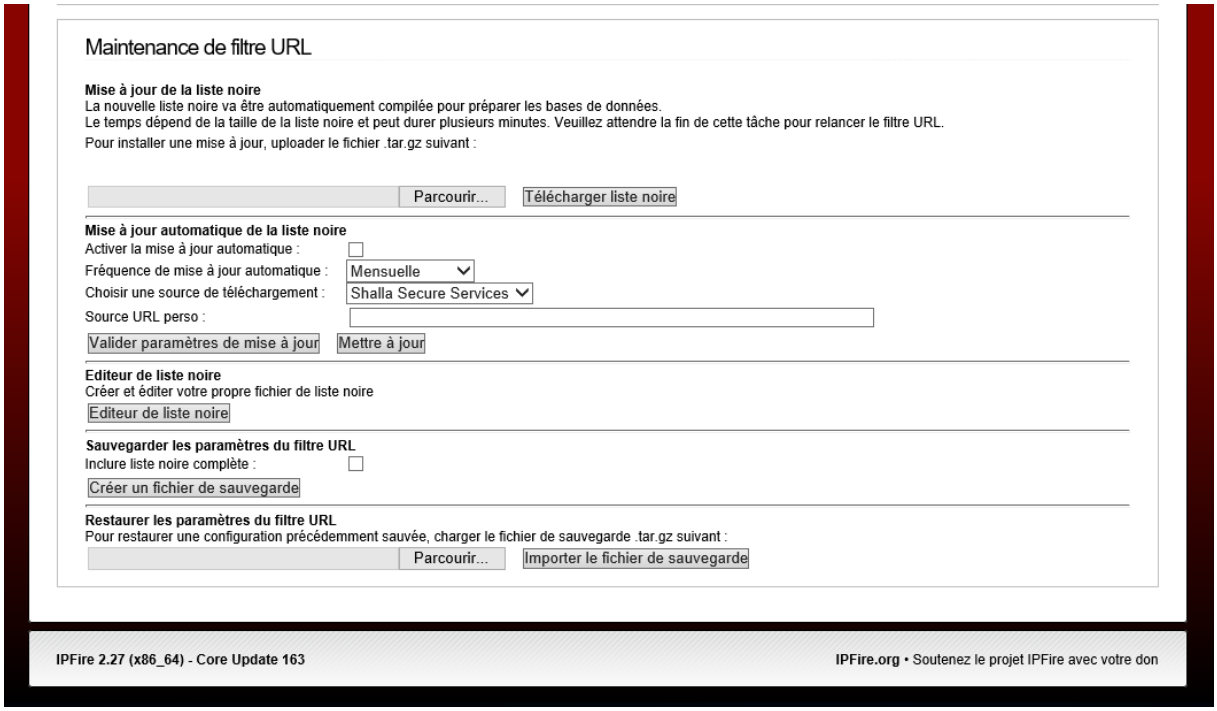


De nombreuses fondations ou universités (ou autres) établissent des listes relativement complètes de liste noire afin d'être implémenté sur les proxy web.

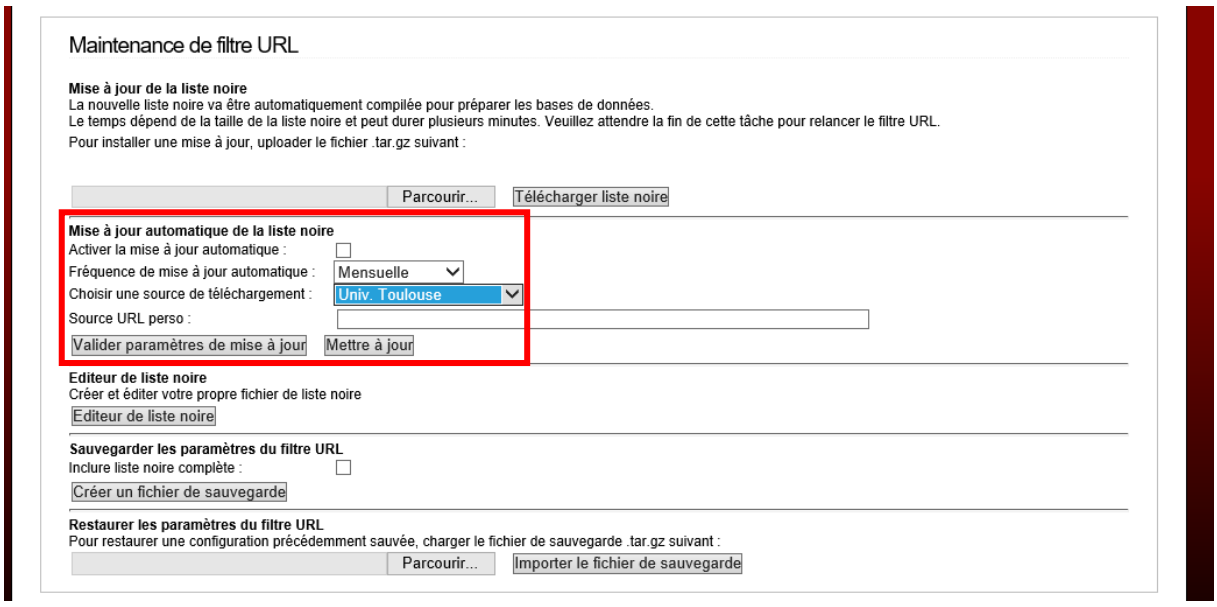
La gestion des liste noire prédéfinies se trouve dans la ***maintenance de filtre URL***, vous pouvez ajouter une archive de liste noire que vous avez préalablement téléchargé (format tar.gz).

```
[root@ipfire ~]# wget --timestamping http://dsi.ut-capitole.fr/blacklists/downlo
ad/all.tar.gz
```

Ci-dessus téléchargement d'une archive de la liste noire établie par l'université Capitole de Toulouse.

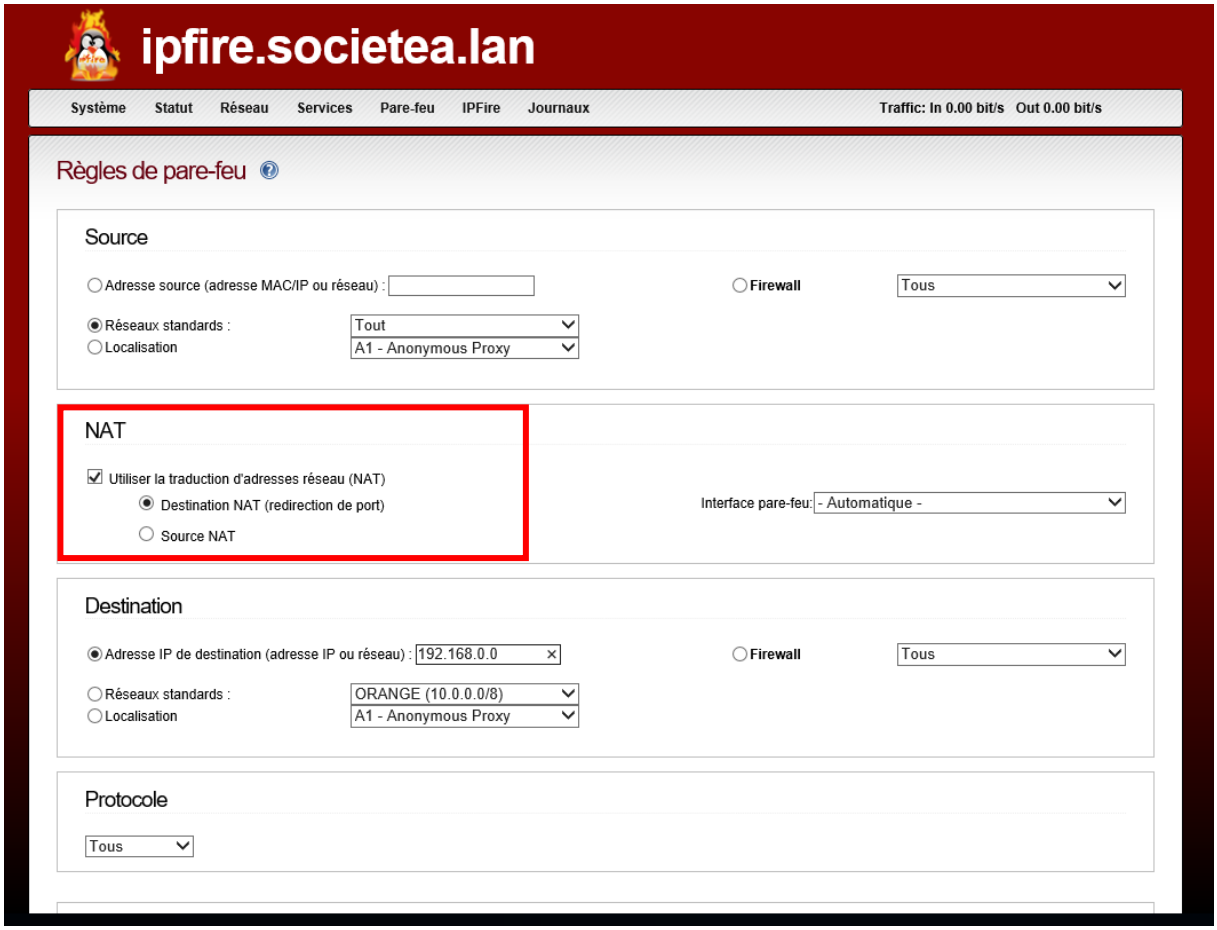


La gestion peut se faire directement par le webconfigurator qui permet de régler la fréquence ainsi que la source de la liste noire.

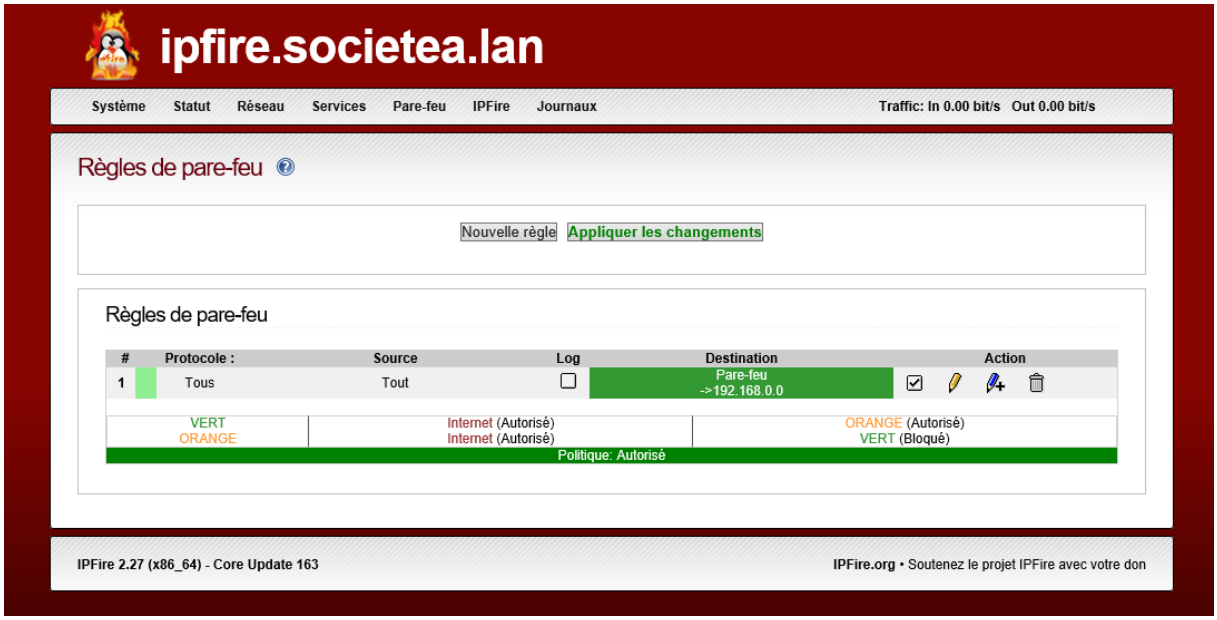


3. Création d'une règle NAT :

A partir du gestionnaire de règle, mettez en place une règle NAT (Network Address Translation) entre le LAN et Internet pour en autoriser le flux.



Ci-dessous la règle NAT pour le réseau local 192.168.0.0/24 (LAN) pour autoriser le trafic.

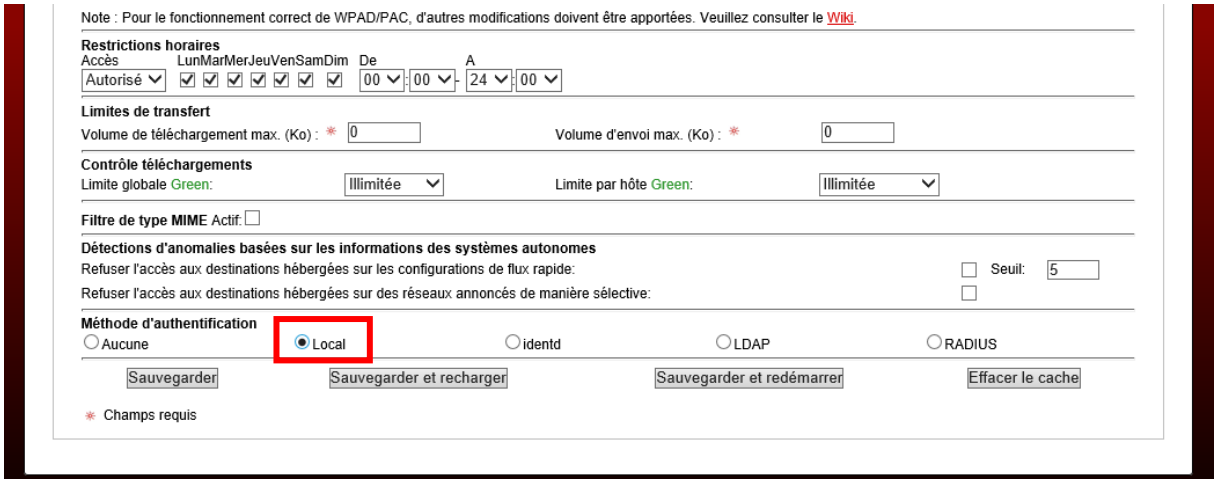


4. Gestion des utilisateurs :

A partir de là, le proxy web est actif et interprètera les requêtes http/https en fonction des listes noires et blanches.

Le proxy web a été défini sans méthode d'authentification, il est recommandé de mettre en place une méthode d'authentification permettant par exemple de contrôler les utilisateurs et leur accès au service proxy web.

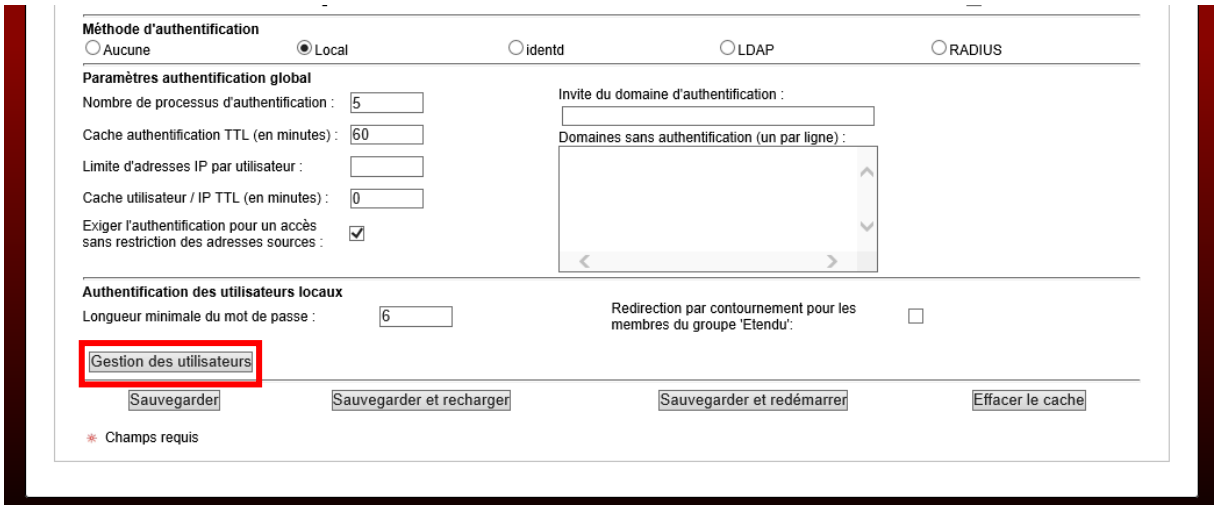
La gestion des utilisateurs est accessible depuis le menu Proxy web en bas de page.



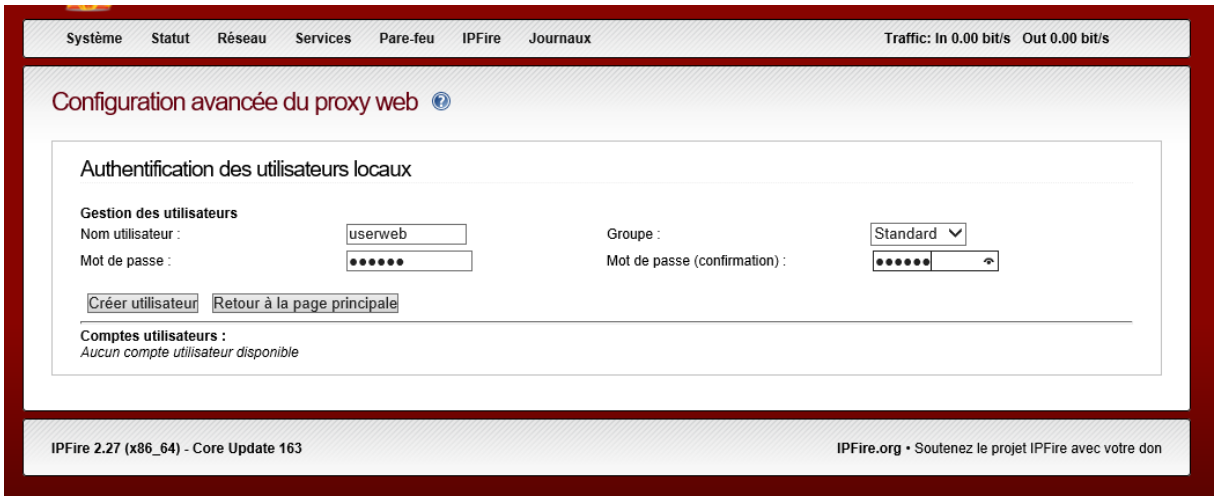
Par défaut, aucune méthode d'authentification n'est activée, vous pouvez mettre en place différentes méthodes d'authentification (annuaire LDAP, serveur RADIUS).

Mettre en place une authentification Local.

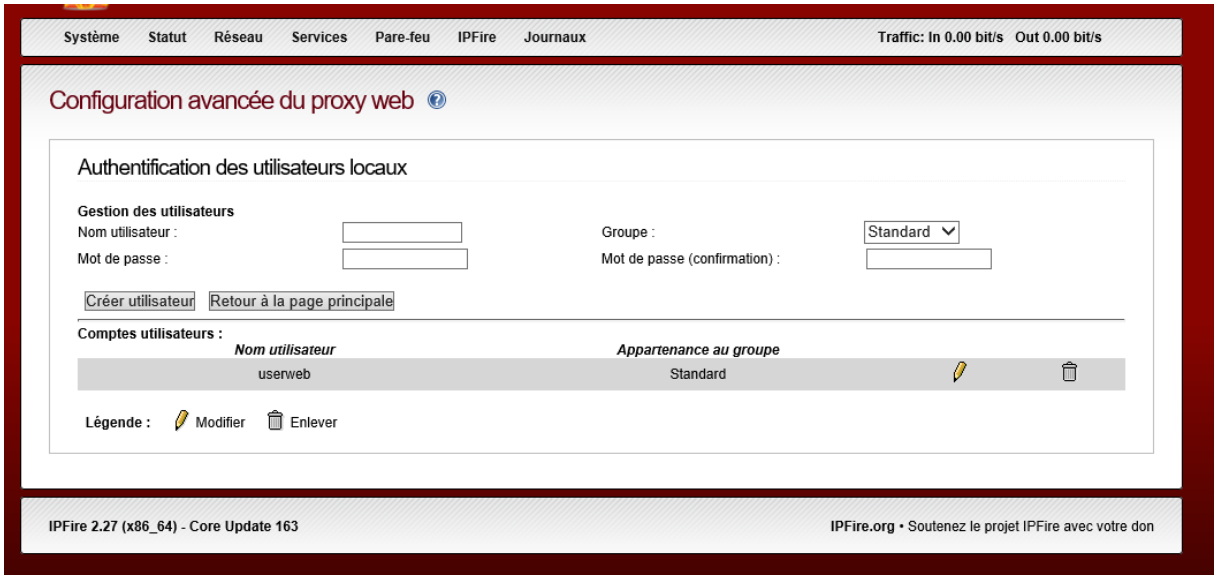
Vous pouvez maintenant gérer et créer des comptes utilisateurs pour le proxy web.



Créez un utilisateur autorisé à utiliser le service proxy web.

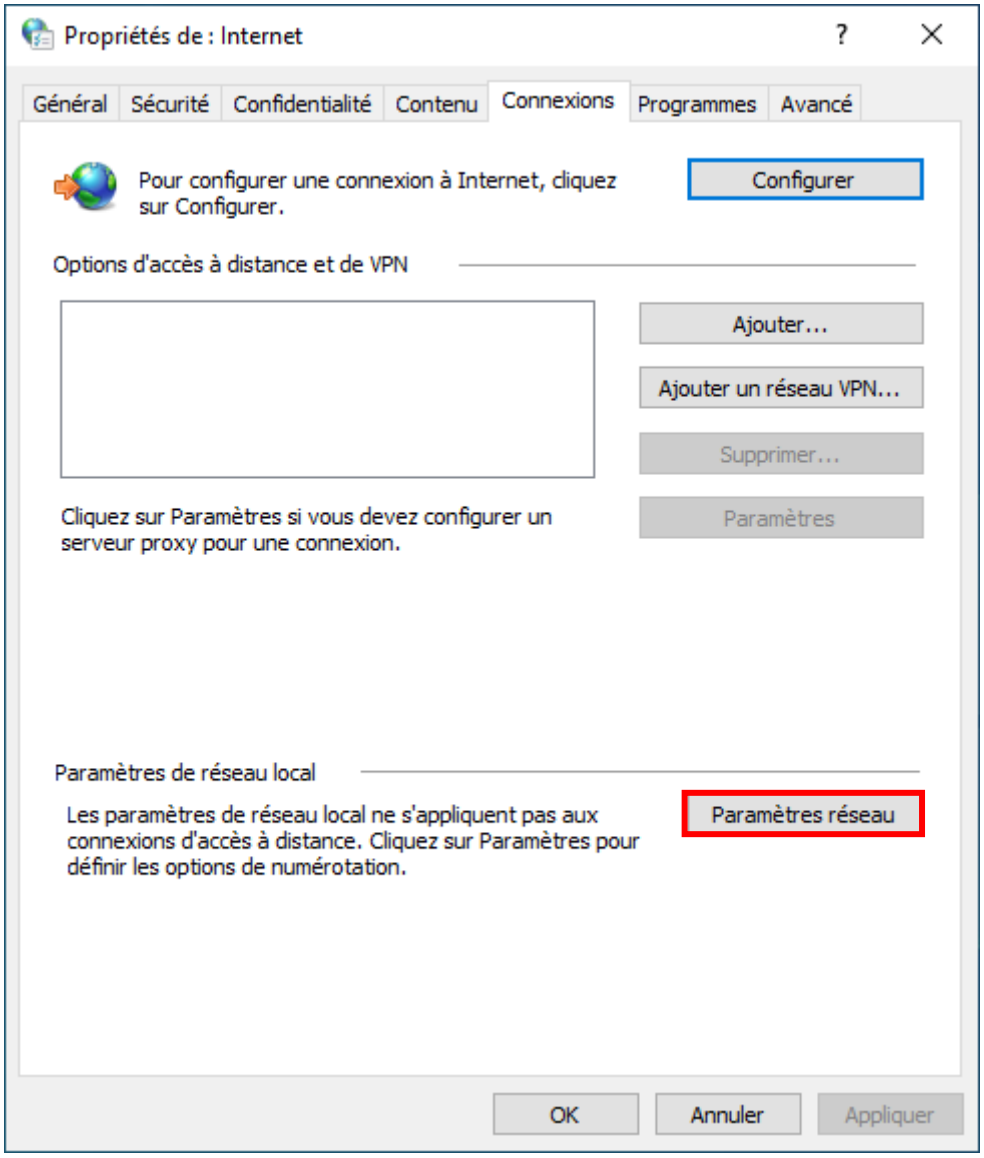


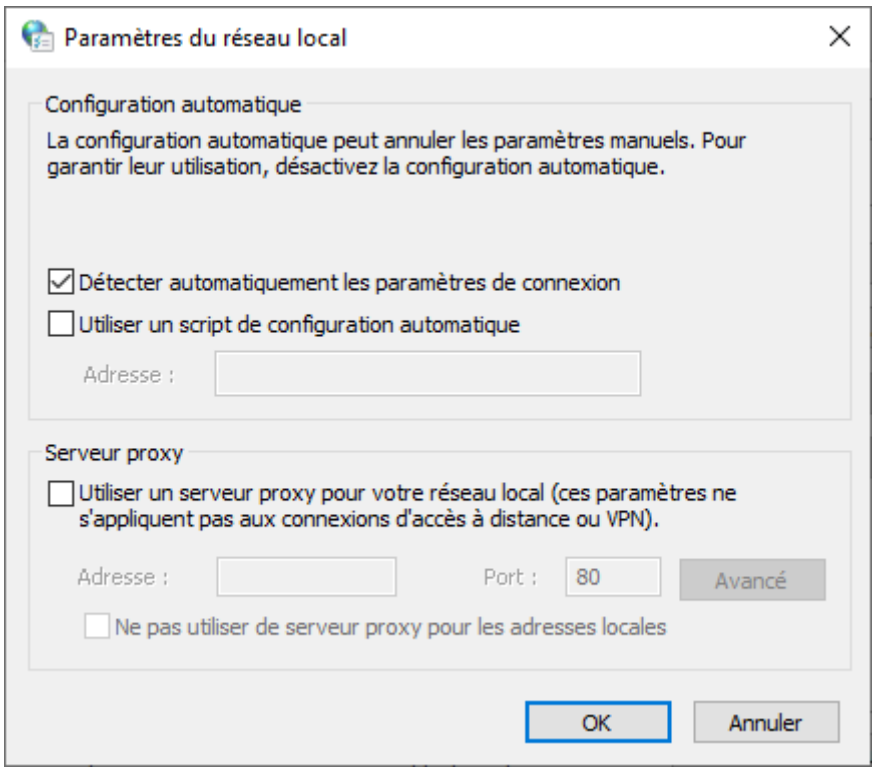
L'utilisateur créé, vous devez maintenant mettre en place le proxy par défaut sur les différents clients du parc informatique.



5. Configuration du proxy sur un client :

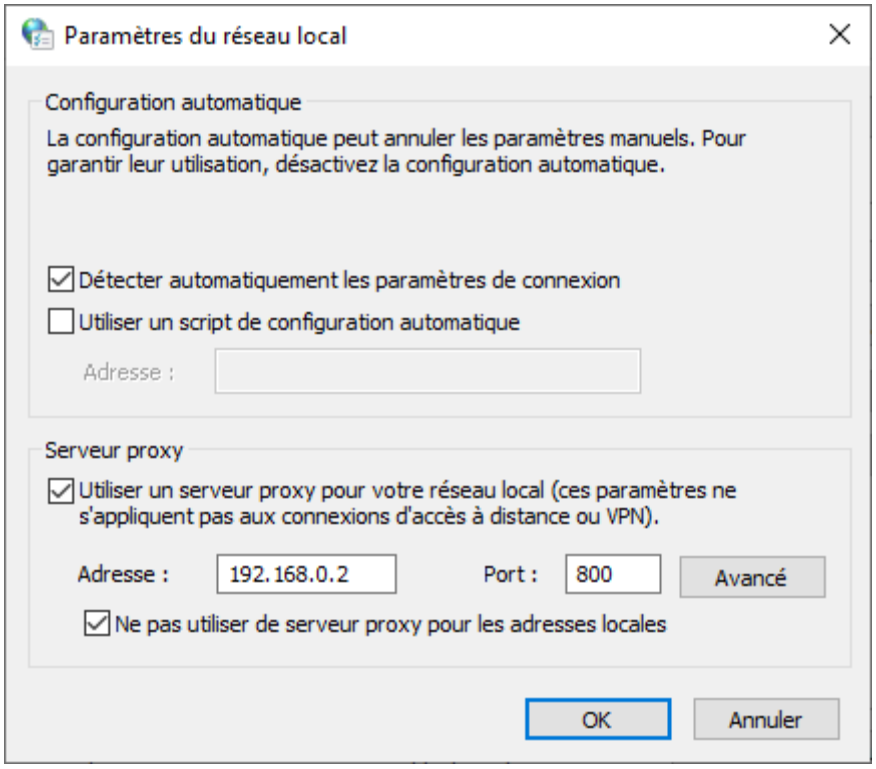
La configuration du proxy web est accessible depuis les options internet du poste client à partir de l'***onglet Connexions, option Paramètres réseau***.


Propriétés de : Internet
Général
Sécurité
Confidentialité
Contenu
Connexions
Programmes
Avancé
Pour configurer une connexion à Internet, cliquez sur Configurer.
Configurer
Options d'accès à distance et de VPN
Ajouter...
Ajouter un réseau VPN...
Supprimer...
Cliquez sur Paramètres si vous devez configurer un serveur proxy pour une connexion.
Paramètres
Paramètres de réseau local
Les paramètres de réseau local ne s'appliquent pas aux connexions d'accès à distance. Cliquez sur Paramètres pour définir les options de numérotation.
Paramètres réseau
OK
Annuler
Appliquer

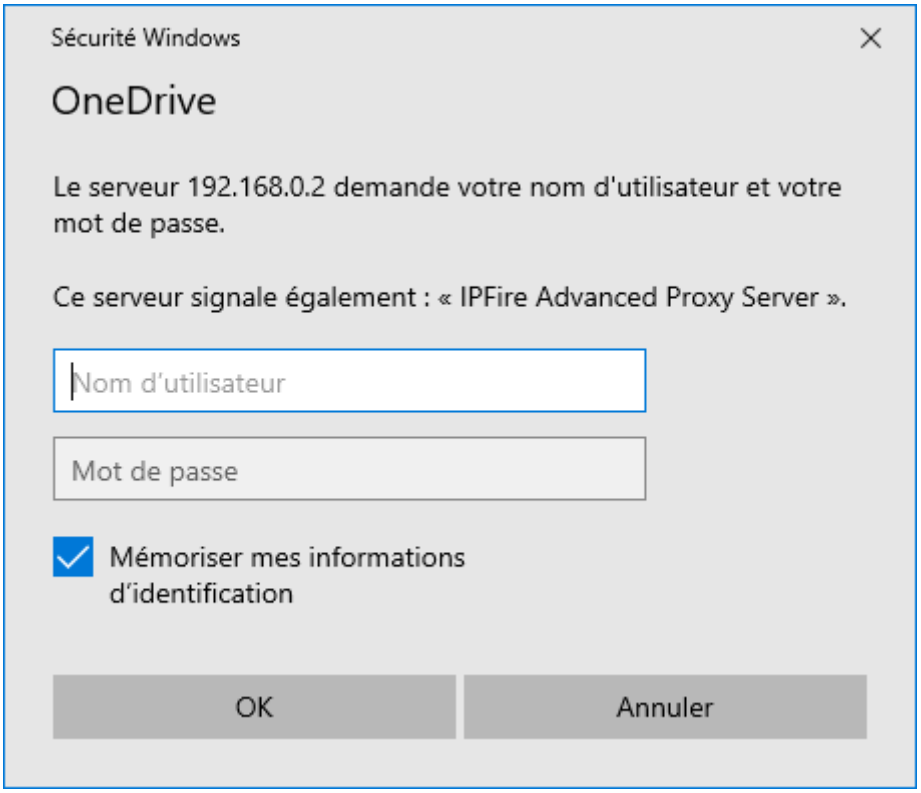

Paramètres du réseau local
Configuration automatique
La configuration automatique peut annuler les paramètres manuels. Pour garantir leur utilisation, désactivez la configuration automatique.
Détecter automatiquement les paramètres de connexion
Utiliser un script de configuration automatique
Adresse :
Serveur proxy
Utiliser un serveur proxy pour votre réseau local (ces paramètres ne s'appliquent pas aux connexions d'accès à distance ou VPN).
Adresse :
Port :
80
Avancé
Ne pas utiliser de serveur proxy pour les adresses locales
OK
Annuler

Activez l'utilisation du service proxy et spécifiez l'adresse IP du serveur ainsi que le port par défaut.

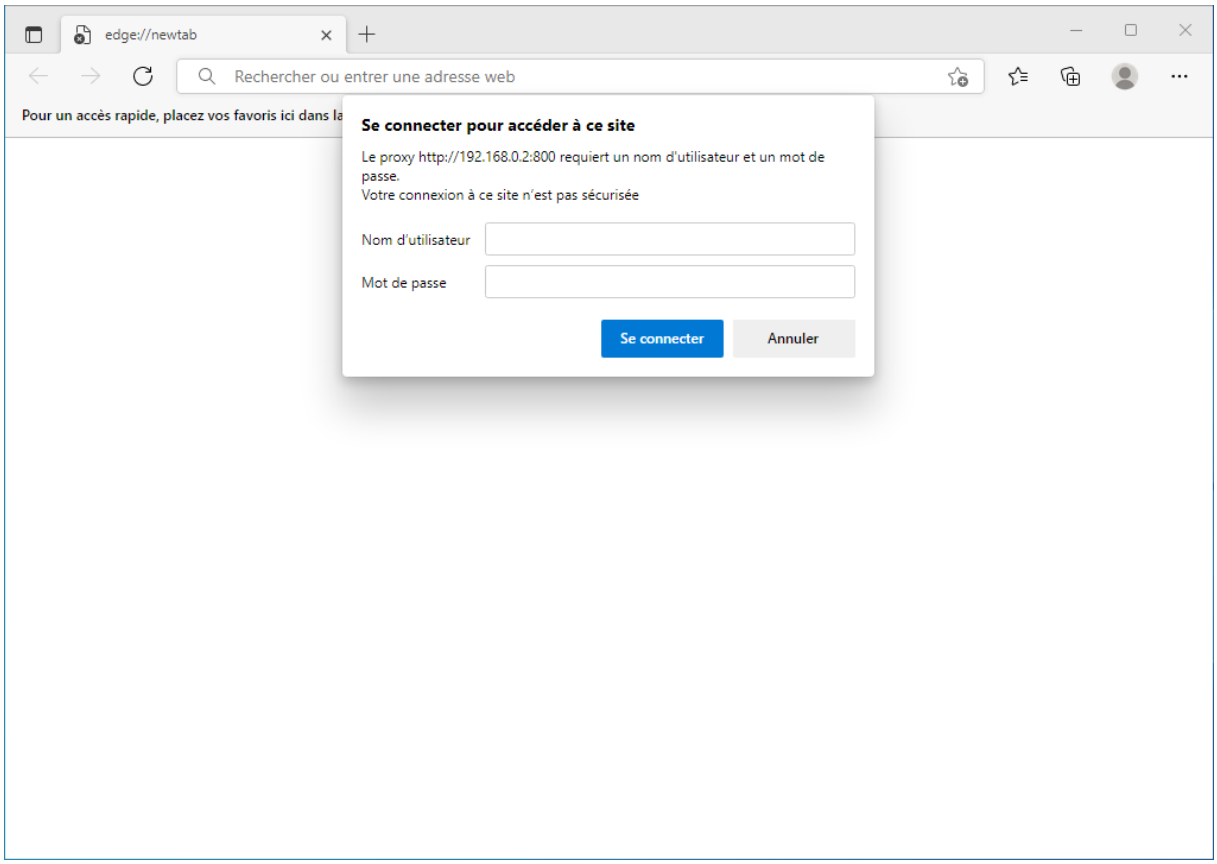
Décochez la détection automatique pour éviter les perturbations.



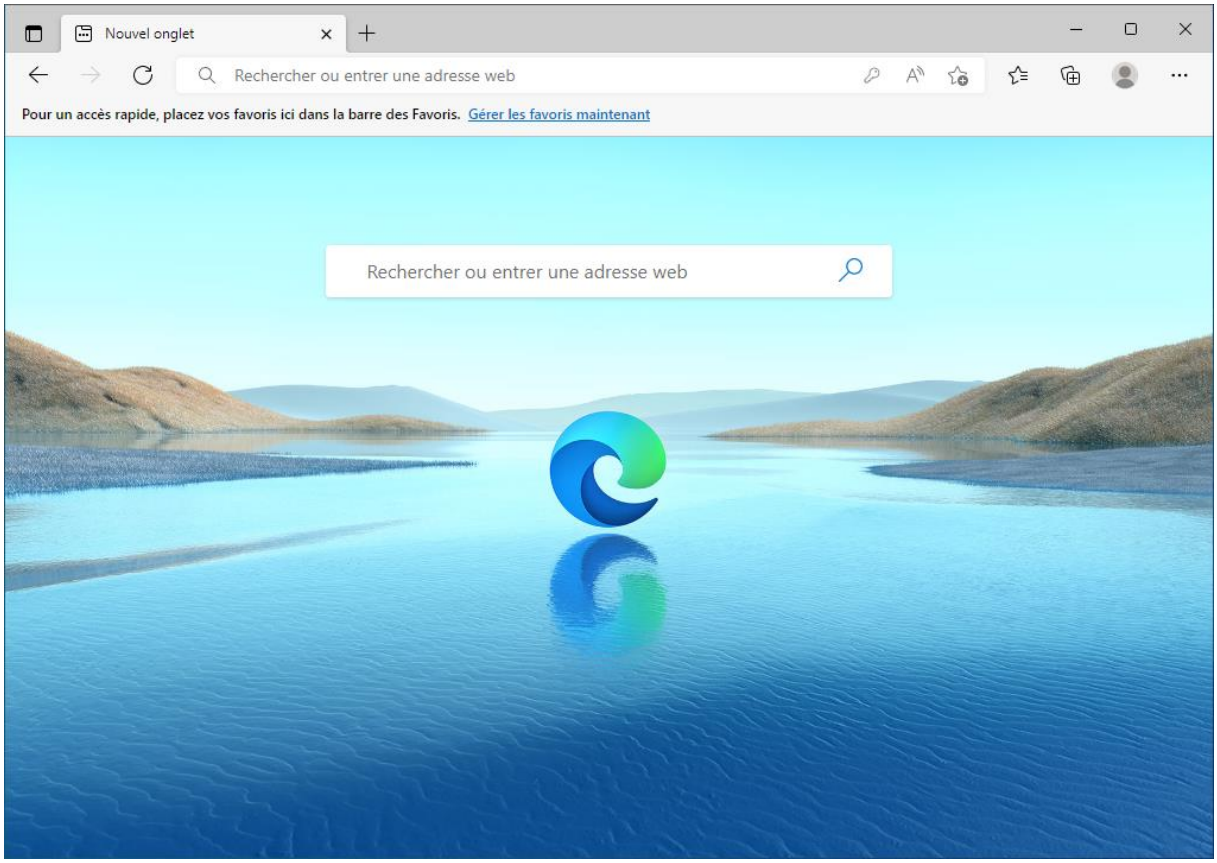
La détection d'un serveur proxy impose une demande d'authentification pour accéder à OneDrive qui se situe dans le WAN.



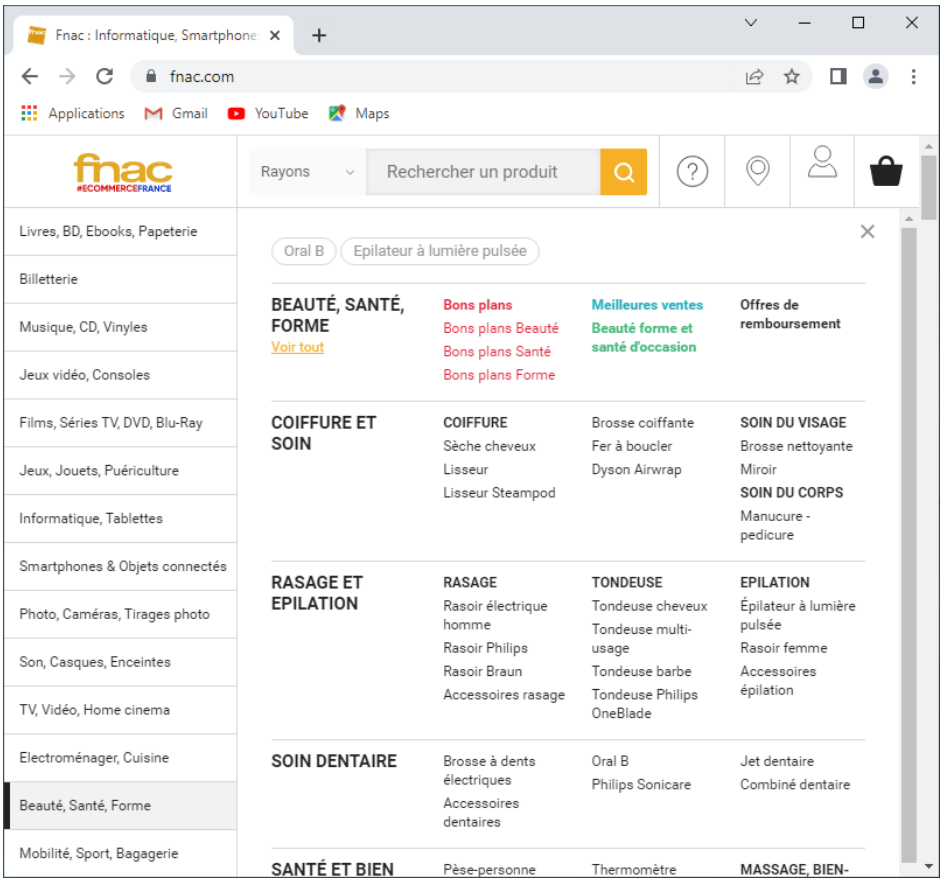
La navigation internet est soumise aux mêmes conditions et impose à l'utilisateur une authentification au serveur proxy pour continuer la navigation.



Utilisez l'utilisateur que vous avez créé sur le serveur proxy pour poursuivre la navigation.



La navigation n’est pas bloquée sur ce nom de domaine ci-dessous.



Après ajout du domaine en liste noire perso, il devient inaccessible à travers le proxy web qui le bloque.