

Mise en place pare-feu avec proxy web

Table des matières

1. Activer le proxy web :.....	2
2. Gestion du filtre de contenu URL :	5
3. Création d'une règle NAT :	8
4. Gestion des utilisateurs :	9
5. Configuration du proxy sur un client :.....	10

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.

Version IPFire 2.27 - <http://192.168.1.1/wpadpac>

Note : Pour le fonctionnement correct de WPAD/PAC, d'autres modifications doivent être apportées. Veuillez consulter le [Wiki](#).

Restrictions horaires

Accès : ☐ Lun ☒ Mar ☒ Mer ☒ Jeu ☒ Ven ☒ Sam ☒ Dim De : 00 A : 24

Limites de transfert

Volume de téléchargement max. (Ko) : * 0 Volume d'envoi max. (Ko) : * 0

Contrôle téléchargements

Limite globale Green: Illimitée Limite par hôte Green: Illimitée

Filtre de type MIME Actif. ☐

Détections d'anomalies basées sur les informations des systèmes autonomes

Refuser l'accès aux destinations hébergées sur les configurations de flux rapide: ☐ Seuil: 5

Refuser l'accès aux destinations hébergées sur des réseaux annoncés de manière sélective: ☐

Méthode d'authentification

☒ Aucune ☐ Local ☐ Identd ☐ LDAP ☐ RADIUS

* Champs requis

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.

Options de pare-feu

Masquage (une seule IP pour plusieurs)

Masque réseau VERT

Masque réseau ORANGE

Journalisation du pare-feu

Supprimer les anciens paquets de synchronisation

Suppression des paquets entrants du jour

Abandon des paquets avancés par le jour

Abandon des paquets sortants par le jour

Suppression des paquets portscan du jour

Suppression des paquets entrants du journal

Suppression des paquets transférés du journal

Règles de pare-feu

Groupes de pare-feu

Options de pare-feu

Détection d'intrusion

Réseaux P2P

Blocage par localisation

Accès réseau BLEU

Tables IP

Masquage activé

Masquage activé

sur / off

sur / off

sur / off

sur / off

sur / off

sur / off

sur / off

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

Comportement du pare-feu par défaut

FORWARD

Défini le comportement du pare-feu par défaut pour les connexions à partir de réseaux locaux. Vous pouvez autoriser toutes les nouvelles connexions ou les bloquer par défaut. Les connexions entre les réseaux locaux sont également bloquées dans ce dernier mode.

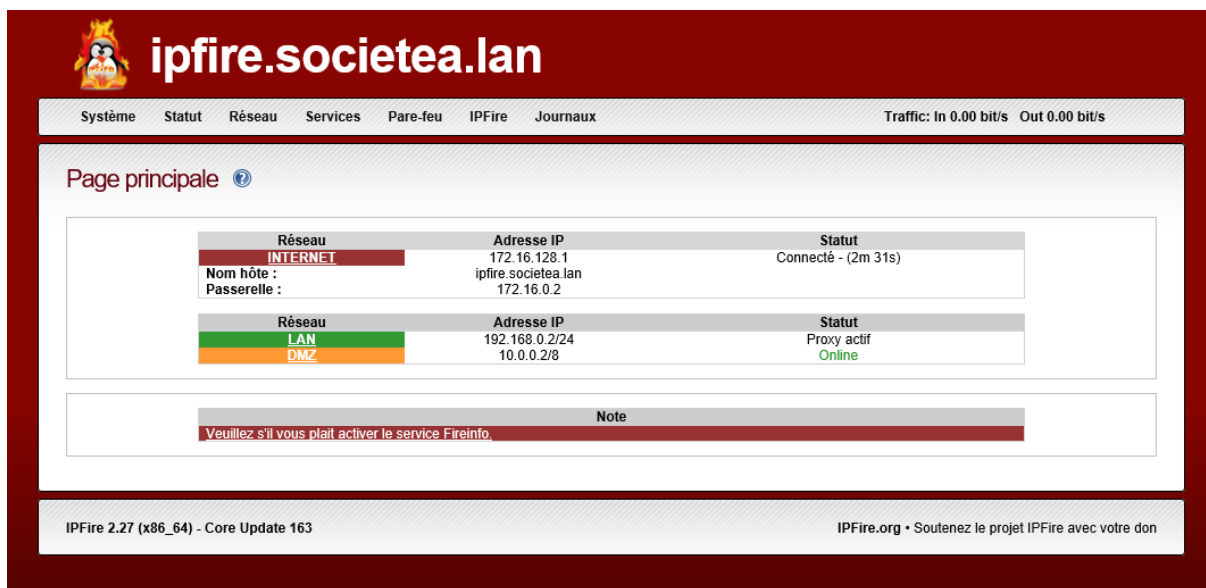
OUTGOING

Défini le comportement du pare-feu par défaut pour les connexions initiées par le pare-feu lui-même. ATTENTION, vous pouvez vous-même vous verrouiller.

IPFire 2.27 (x86_64) - Core Update 163

IPFire.org • Soutenez le projet IPFire avec votre don

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



The screenshot shows the IPFire web interface for the host ipfire.societea.lan. The top navigation bar includes links for Système, Statut, Réseau, Services, Pare-feu, IPFire, and Journaux. The main content area displays the 'Page principale' with a table of network interfaces. The 'INTERNET' interface is connected, and the 'LAN' interface has the proxy active. A note at the bottom suggests activating the Fireinfo service.

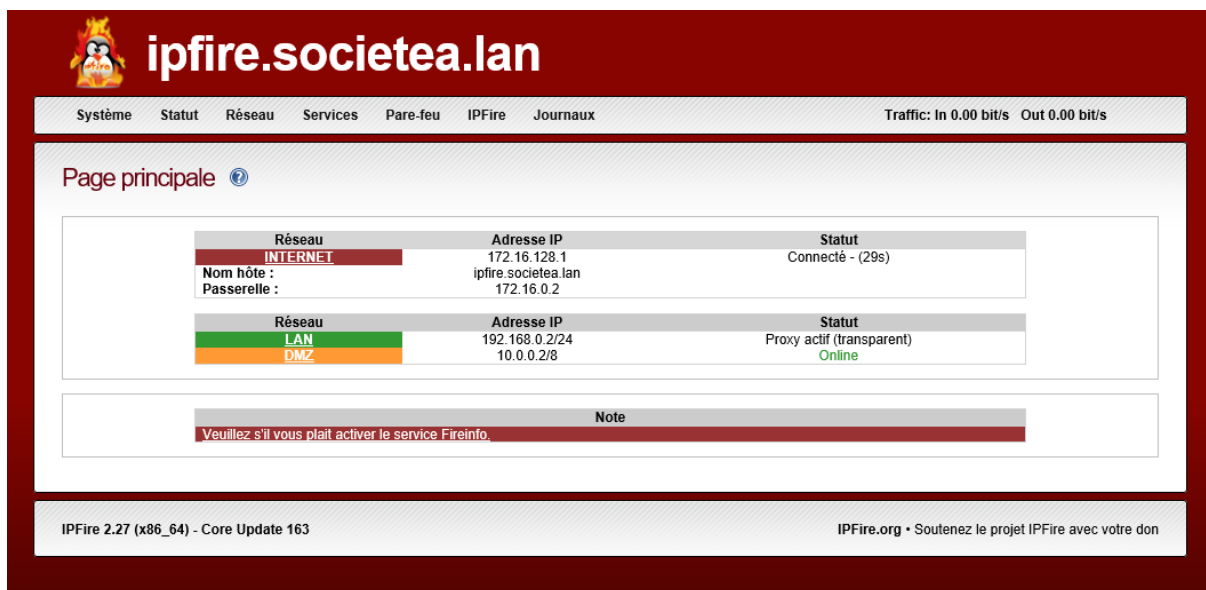
Réseau	Adresse IP	Statut
INTERNET	172.16.128.1	Connecté - (2m 31s)
Nom hôte : ipfire.societea.lan		
Passerelle : 172.16.0.2		

Réseau	Adresse IP	Statut
LAN	192.168.0.2/24	Proxy actif
DMZ	10.0.0.2/8	Online

Note: Veuillez s'il vous plaît activer le service Fireinfo.

IPFire 2.27 (x86_64) - Core Update 163 IPFire.org • Soutenez le projet IPFire avec votre don

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



This screenshot is similar to the previous one, but the 'LAN' interface status is 'Proxy actif (transparent)' instead of just 'Proxy actif'. The rest of the interface, including the navigation bar and the note about Fireinfo, remains the same.

Réseau	Adresse IP	Statut
INTERNET	172.16.128.1	Connecté - (29s)
Nom hôte : ipfire.societea.lan		
Passerelle : 172.16.0.2		

Réseau	Adresse IP	Statut
LAN	192.168.0.2/24	Proxy actif (transparent)
DMZ	10.0.0.2/8	Online

Note: Veuillez s'il vous plaît activer le service Fireinfo.

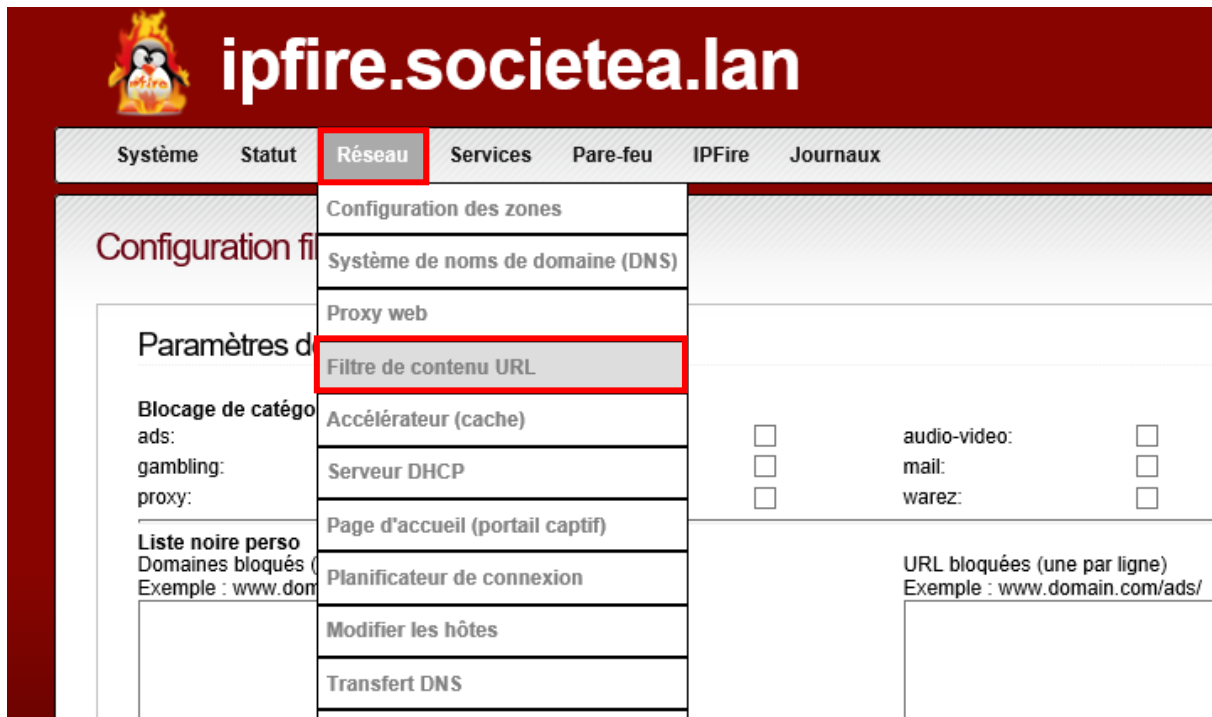
IPFire 2.27 (x86_64) - Core Update 163 IPFire.org • Soutenez le projet IPFire avec votre don

2. Gestion du filtre de contenu URL :

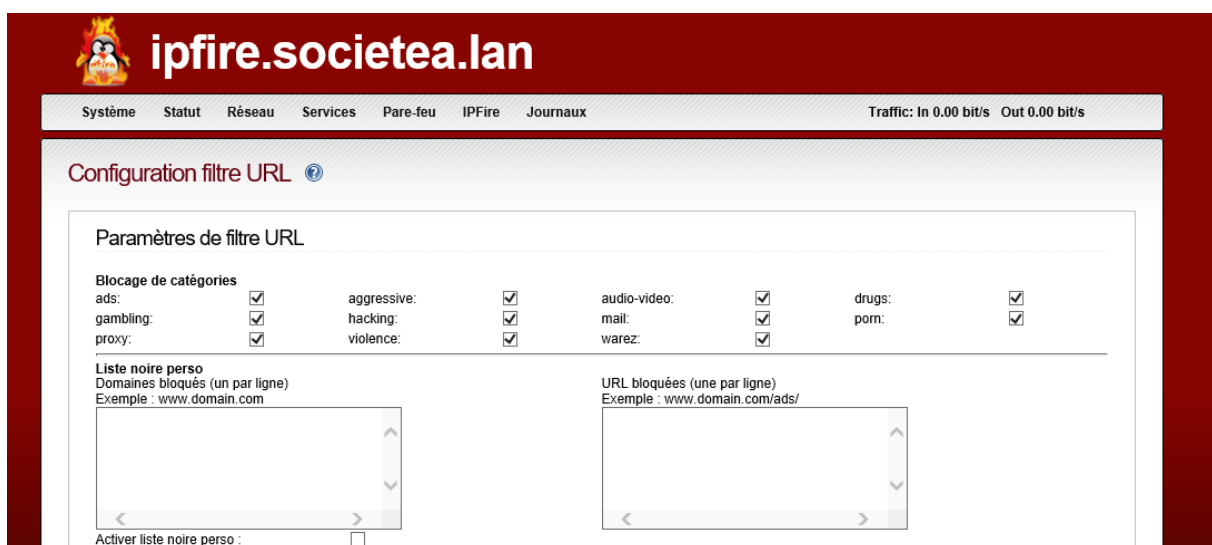
Le service proxy web va permettre de faire l'intermédiaire entre les requêtes http/https des différents clients du réseau LAN avec les serveurs web du réseau WAN.

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.

Configuration filtre URL ?

Paramètres de filtre URL

Blocage de catégories			
ads: <input checked="" type="checkbox"/>	aggressive: <input checked="" type="checkbox"/>	audio-video: <input checked="" type="checkbox"/>	drugs: <input checked="" type="checkbox"/>
gambling: <input checked="" type="checkbox"/>	hacking: <input checked="" type="checkbox"/>	mail: <input checked="" type="checkbox"/>	porn: <input checked="" type="checkbox"/>
proxy: <input checked="" type="checkbox"/>	violence: <input checked="" type="checkbox"/>	warez: <input checked="" type="checkbox"/>	

Liste noire perso
Domaines bloqués (un par ligne)
Exemple : www.domain.com
www.fnac.com

Activer liste noire perso : ☒

Liste blanche perso
Domaines autorisés (un par ligne)
Exemple : www.domain.com
www.github.com

Activer liste blanche perso : ☒

URL bloquées (une par ligne)
Exemple : www.domain.com/ads/

URLs autorisées (une par ligne)
Exemple : www.domain.com/ads/

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.

Contrôle d'accès basé sur les horaires

Fixer les contraintes horaires
Fixer les quotas utilisateur

Règlages de filtre URL

Modèle de page de redirection : legacy

Montrer catégorie page bloquée : <input type="checkbox"/>	Redirige vers cette URL : <input type="text"/>
Montrer adresse url page bloquée : <input type="checkbox"/>	Message ligne 1 : <input type="text"/>
Montrer adresse IP page bloquée : <input type="checkbox"/>	Message ligne 2 : <input type="text"/>
Utiliser "Erreur DNS" pour url bloquées : <input type="checkbox"/>	Message ligne 3 : <input type="text"/>

Paramètres avancés

Activer la liste de mots clés perso : <input type="checkbox"/>	Activer le journal : <input type="checkbox"/>
Bloquer "pubs" avec fenêtre vide : <input type="checkbox"/>	Log identifiant : <input type="checkbox"/>
Bloquer les sites atteints par leur IP : <input type="checkbox"/>	Classer les journaux par catégorie : <input type="checkbox"/>
Bloquer toutes les url non autorisées explicitement : <input type="checkbox"/>	Autoriser une liste blanche personnalisée de clients bannis : <input type="checkbox"/>

* Champs requis

Sauvegarder
Sauvegarder et redémarrer

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/download/all.tar.gz
```

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

Maintenance de filtre URL

Mise à jour de la liste noire
La nouvelle liste noire va être automatiquement compilée pour préparer les bases de données.
Le temps dépend de la taille de la liste noire et peut durer plusieurs minutes. Veuillez attendre la fin de cette tâche pour relancer le filtre URL.
Pour installer une mise à jour, uploader le fichier .tar.gz suivant :

Mise à jour automatique de la liste noire
Activer la mise à jour automatique : ☐
Fréquence de mise à jour automatique :
Choisir une source de téléchargement :
Source URL perso :

Éditeur de liste noire
Créer et éditer votre propre fichier de liste noire

Sauvegarder les paramètres du filtre URL
Inclure liste noire complète : ☐

Restaurer les paramètres du filtre URL
Pour restaurer une configuration précédemment sauvee, charger le fichier de sauvegarde .tar.gz suivant :

IPFire 2.27 (x86_64) - Core Update 163IPFire.org • Soutenez le projet IPFire avec votre don

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

Maintenance de filtre URL

Mise à jour de la liste noire
La nouvelle liste noire va être automatiquement compilée pour préparer les bases de données.
Le temps dépend de la taille de la liste noire et peut durer plusieurs minutes. Veuillez attendre la fin de cette tâche pour relancer le filtre URL.
Pour installer une mise à jour, uploader le fichier .tar.gz suivant :

Mise à jour automatique de la liste noire
Activer la mise à jour automatique : ☐
Fréquence de mise à jour automatique :
Choisir une source de téléchargement :
Source URL perso :

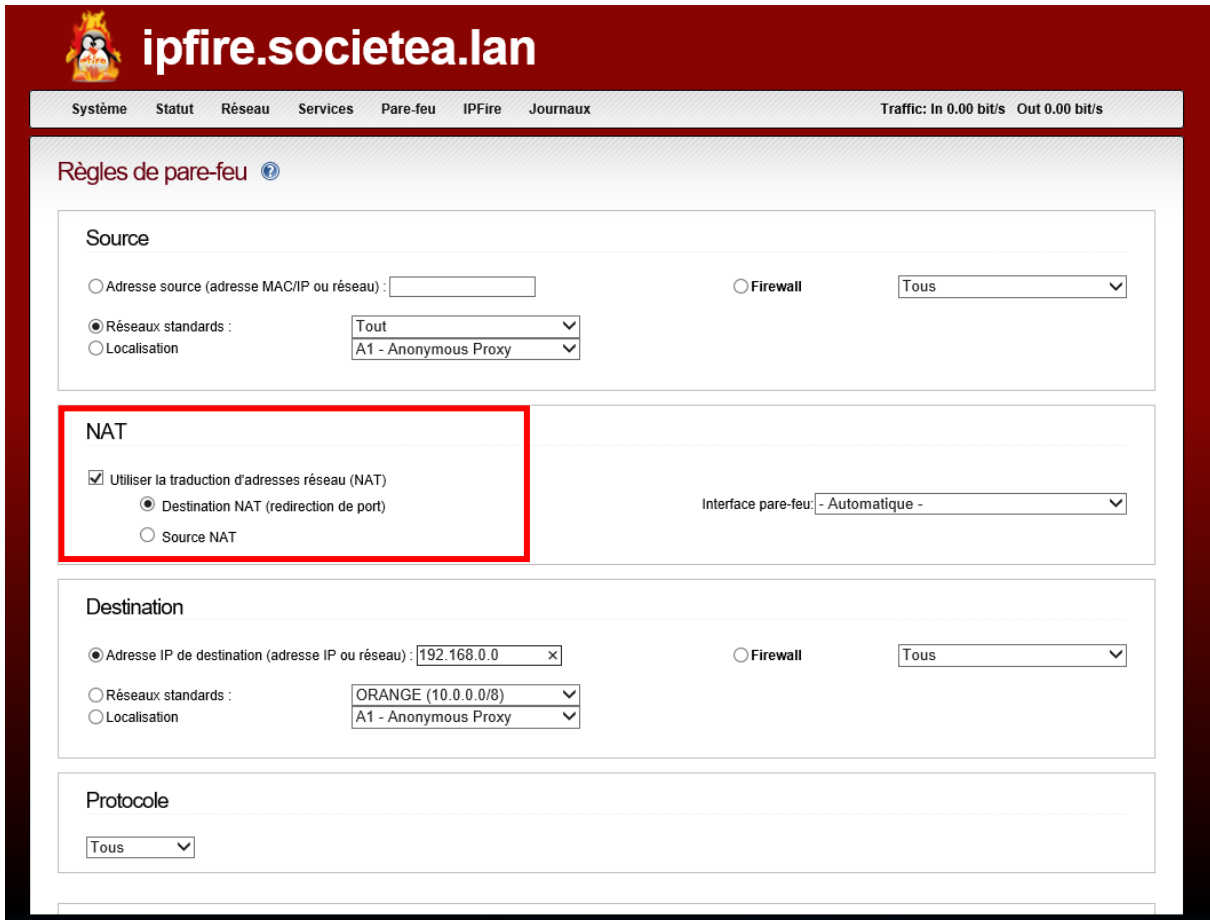
Éditeur de liste noire
Créer et éditer votre propre fichier de liste noire

Sauvegarder les paramètres du filtre URL
Inclure liste noire complète : ☐

Restaurer les paramètres du filtre URL
Pour restaurer une configuration précédemment sauvee, charger le fichier de sauvegarde .tar.gz suivant :

3. Création d'une règle NAT :

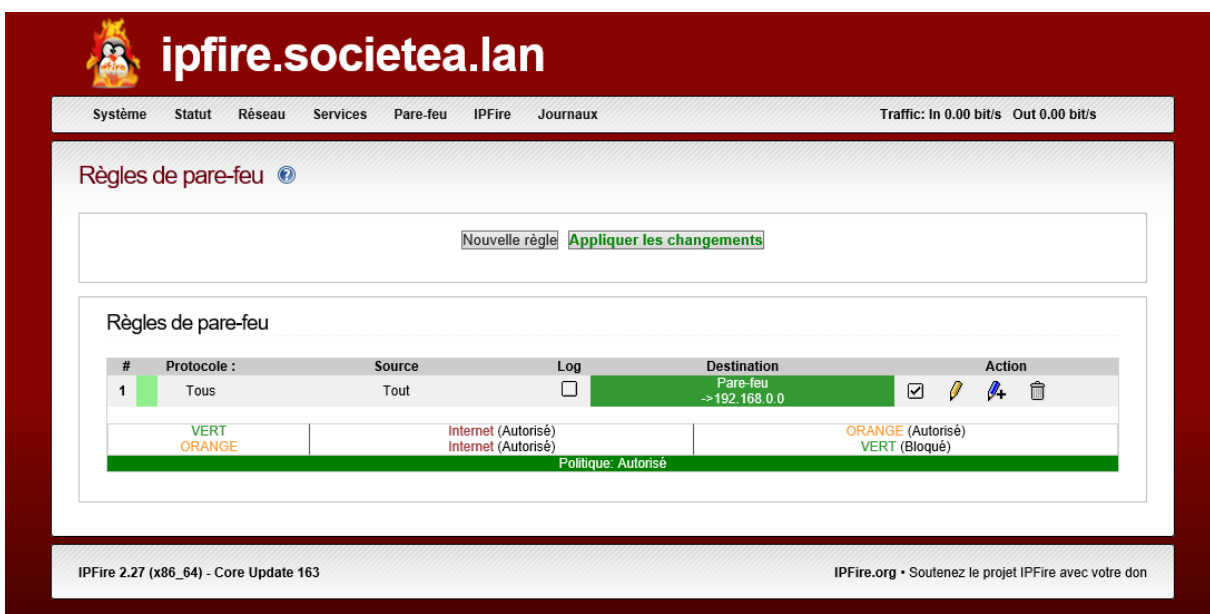
A partir du gestionnaire de règle, mettez en place une règle NAT (Network Address Translation) entre le LAN et Internet pour en autoriser le flux.



The screenshot shows the IPFire web interface with the 'Règles de pare-feu' (Firewall Rules) page. The 'NAT' section is highlighted with a red box. The configuration is as follows:

- Source:**
 - ☐ Adresse source (adresse MAC/IP ou réseau) :
 - ☒ Réseaux standards :
 - Tout
 - A1 - Anonymous Proxy
 - ☐ Localisation
- NAT:**
 - ☒ Utiliser la traduction d'adresses réseau (NAT)
 - ☒ Destination NAT (redirection de port)
 - ☐ Source NAT
 - Interface pare-feu: - Automatique -
- Destination:**
 - ☒ Adresse IP de destination (adresse IP ou réseau) : 192.168.0.0
 - ☐ Réseaux standards :
 - ORANGE (10.0.0.0/8)
 - A1 - Anonymous Proxy
 - ☐ Localisation
- Protocole:**
 - Tous

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



The screenshot shows the IPFire web interface with the 'Règles de pare-feu' (Firewall Rules) page. The first rule is highlighted in green. The configuration is as follows:

#	Protocole :	Source	Log	Destination	Action
1	Tous	Tout	<input type="checkbox"/>	Pare-feu -> 192.168.0.0	<input checked="" type="checkbox"/>
	VERT ORANGE	Internet (Autorisé) Internet (Autorisé)		ORANGE (Autorisé) VERT (Bloqué)	
Politique: Autorisé					

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.

Note : Pour le fonctionnement correct de WPAD/PAC, d'autres modifications doivent être apportées. Veuillez consulter le [Wiki](#).

Restrictions horaires
Accès : ☐ Autorisé ☒ Lun ☒ Mar ☒ Mer ☒ Jeu ☒ Ven ☒ Sam ☒ Dim De 00:00 à 24:00

Limites de transfert
Volume de téléchargement max. (Ko) : Volume d'envoi max. (Ko) :

Contrôle téléchargements
Limite globale Green: Limite par hôte Green:

Filtre de type MIME Actif: ☐

Détections d'anomalies basées sur les informations des systèmes autonomes
Refuser l'accès aux destinations hébergées sur les configurations de flux rapide: ☐ Seuil:
Refuser l'accès aux destinations hébergées sur des réseaux annoncés de manière sélective: ☐

Méthode d'authentification
☐ Aucune ☒ Local ☐ identd ☐ LDAP ☐ RADIUS

* Champs requis

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.

Méthode d'authentification
☐ Aucune ☒ Local ☐ identd ☐ LDAP ☐ RADIUS

Paramètres authentification global
Nombre de processus d'authentification : Invite du domaine d'authentification :
Cache authentification TTL (en minutes) : Domaines sans authentification (un par ligne) :
Limite d'adresses IP par utilisateur :
Cache utilisateur / IP TTL (en minutes) :
Exiger l'authentification pour un accès sans restriction des adresses sources : ☒

Authentification des utilisateurs locaux
Longueur minimale du mot de passe : Redirection par contournement pour les membres du groupe 'Etendu': ☐

* Champs requis

Créez un utilisateur autorisé à utiliser le service proxy web.

Système Statut Réseau Services Pare-feu IPFire Journaux Traffic: In 0.00 bit/s Out 0.00 bit/s

Configuration avancée du proxy web ?

Authentification des utilisateurs locaux

Gestion des utilisateurs

Nom utilisateur : Groupe :

Mot de passe : Mot de passe (confirmation) :

[Créer utilisateur](#) [Retour à la page principale](#)

Comptes utilisateurs :
Aucun compte utilisateur disponible

IPFire 2.27 (x86_64) - Core Update 163 IPFire.org • Soutenez le projet IPFire avec votre don

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

Système Statut Réseau Services Pare-feu IPFire Journaux Traffic: In 0.00 bit/s Out 0.00 bit/s

Configuration avancée du proxy web ?

Authentification des utilisateurs locaux

Gestion des utilisateurs

Nom utilisateur : Groupe :

Mot de passe : Mot de passe (confirmation) :

[Créer utilisateur](#) [Retour à la page principale](#)

Comptes utilisateurs :

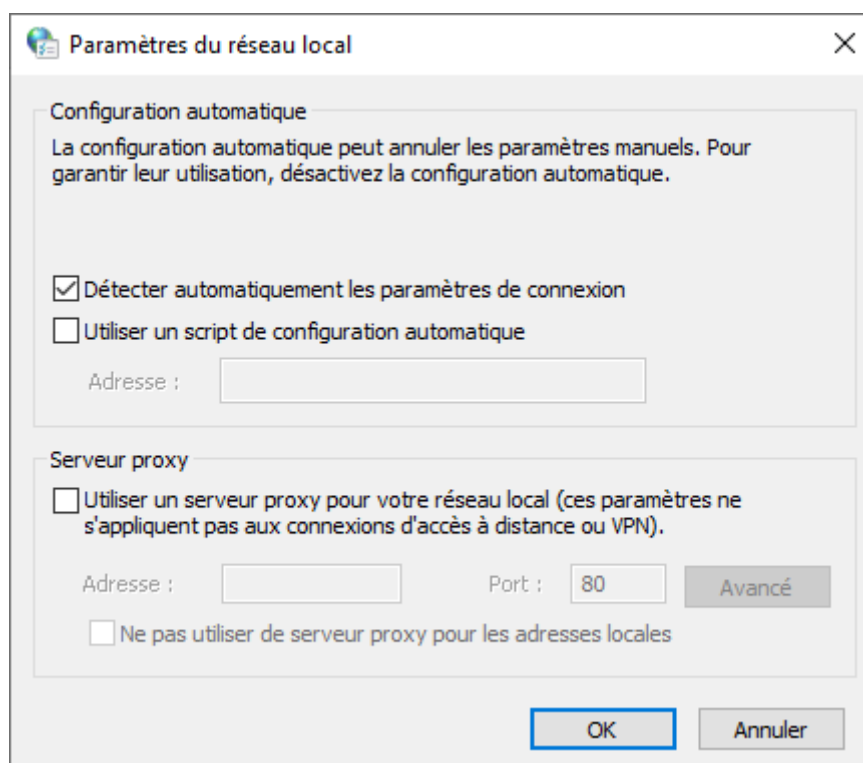
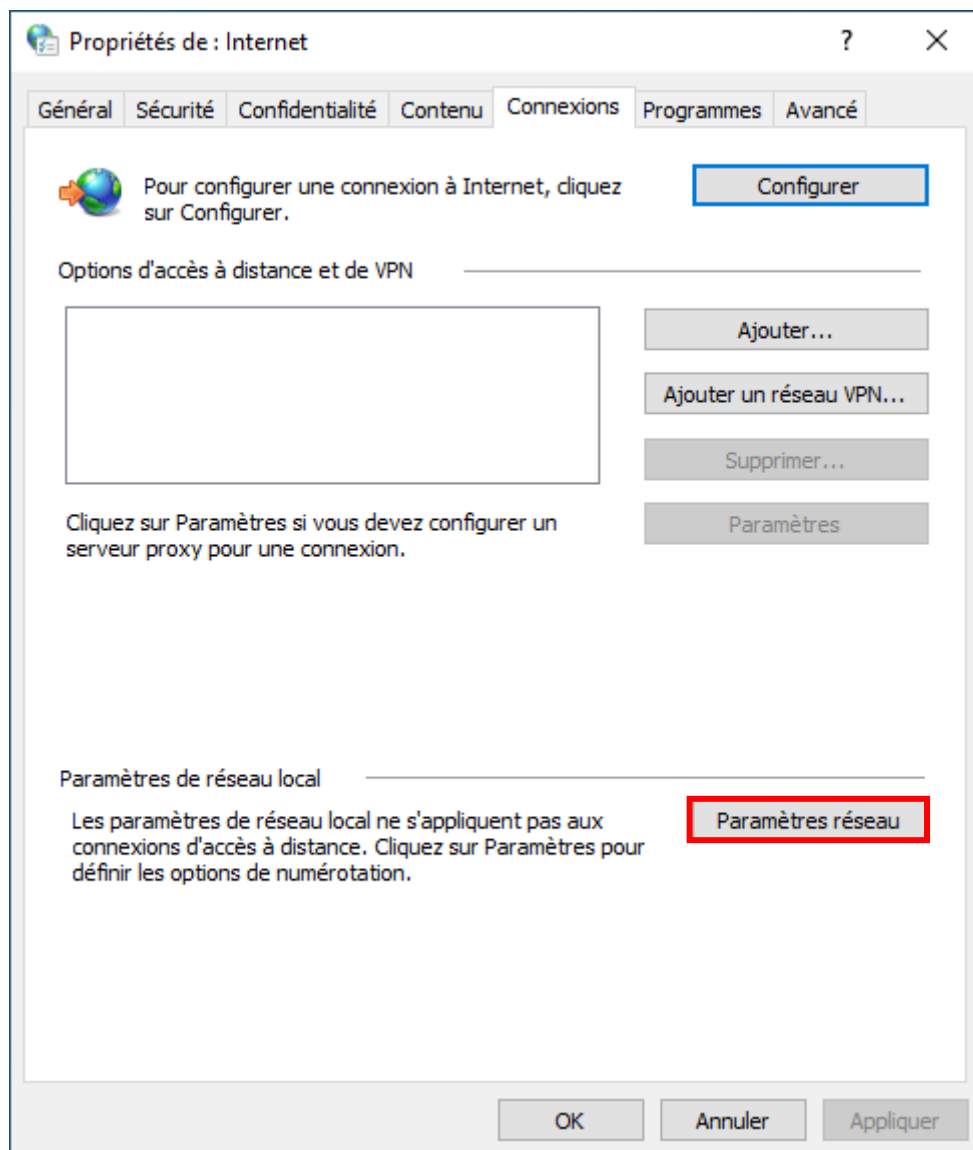
Nom utilisateur	Appartenance au groupe
userweb	Standard

Légende : [Modifier](#) [Enlever](#)

IPFire 2.27 (x86_64) - Core Update 163 IPFire.org • Soutenez le projet IPFire avec votre don

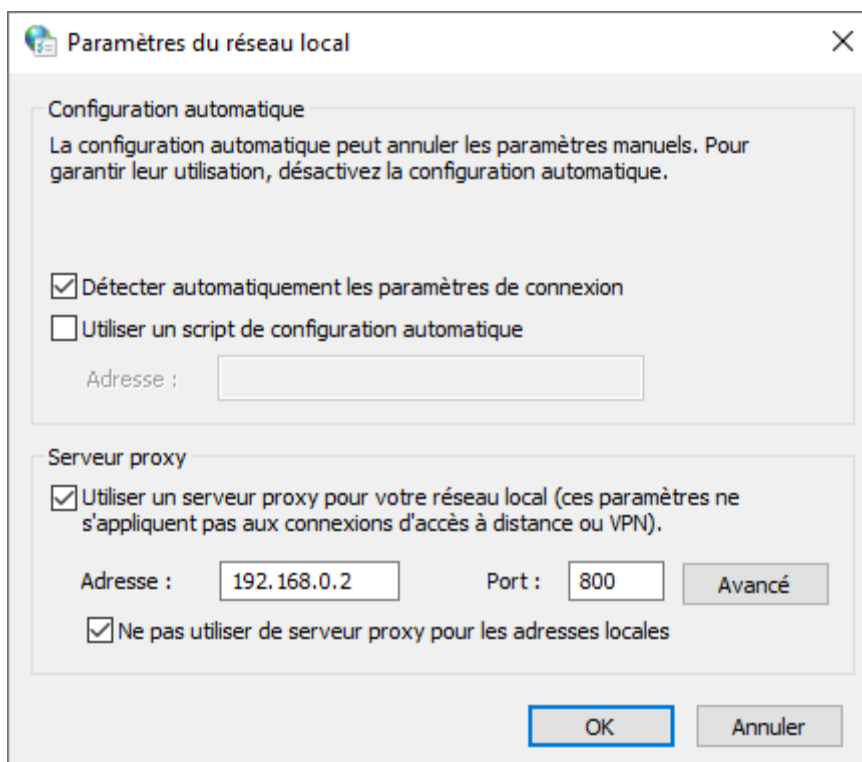
5. Configuration du proxy sur un client :

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

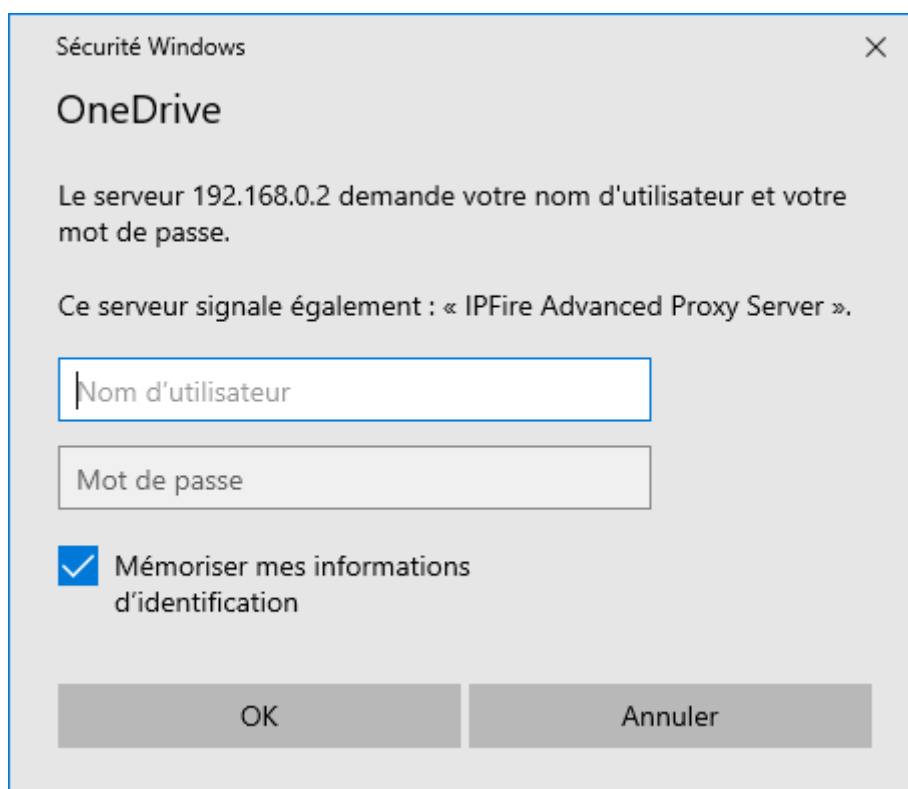


Activez l'utilisation du service proxy et spécifiez l'adresse IP du serveur ainsi que le port par défaut.

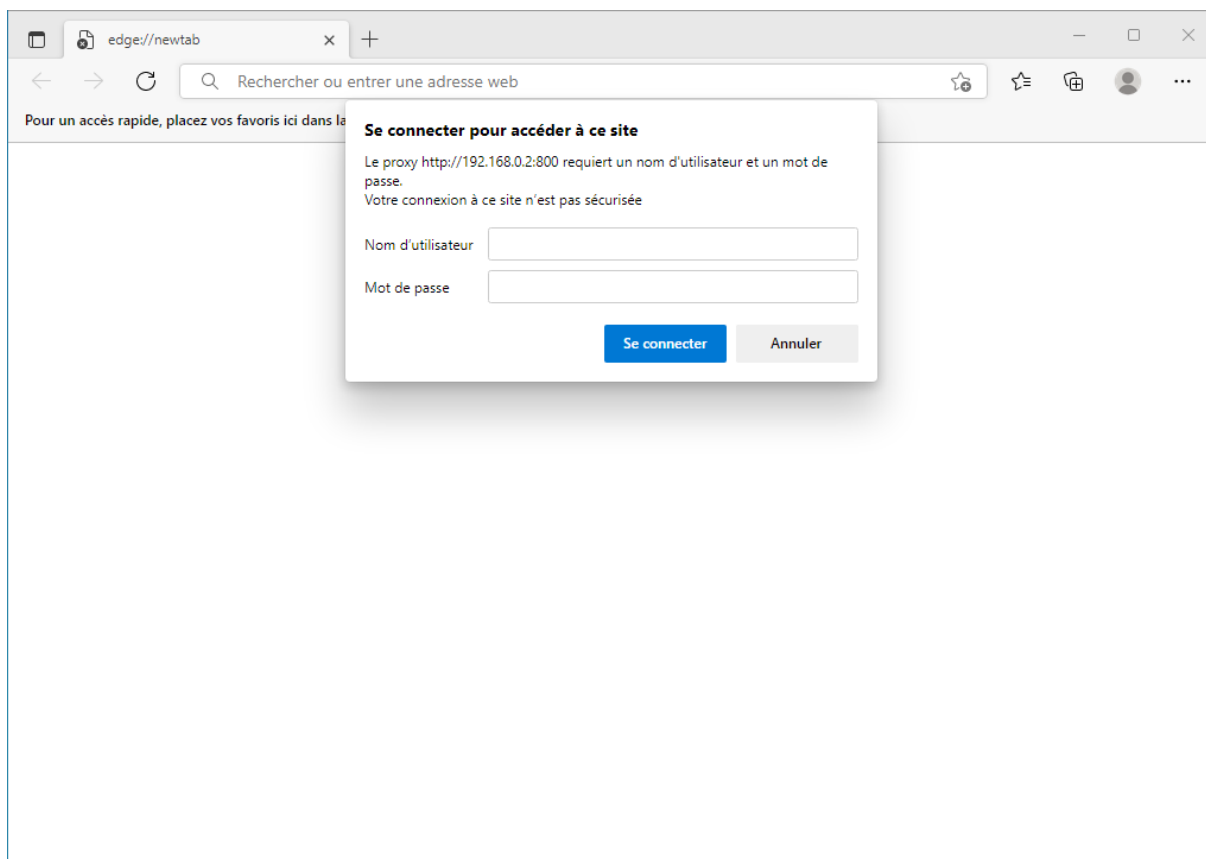
Décochez la détection automatique pour éviter les perturbations.



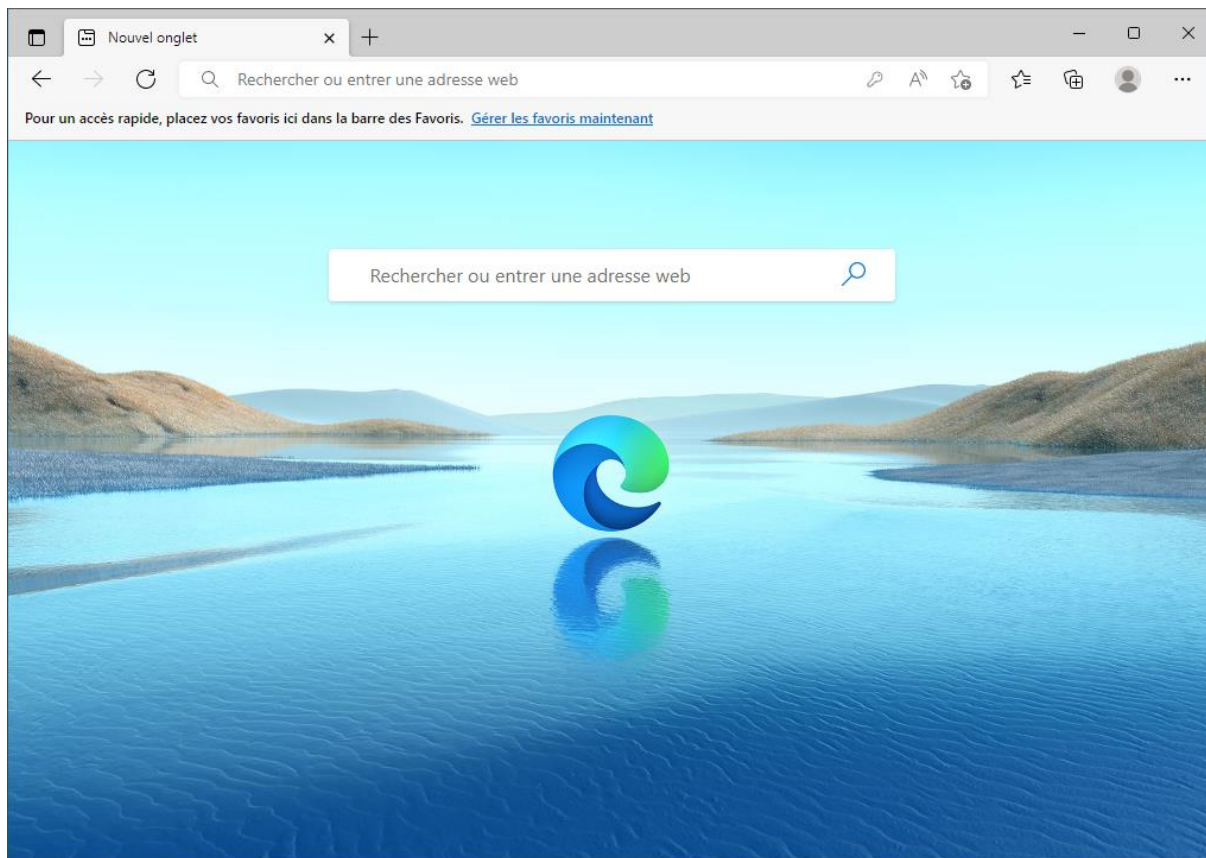
La détection d'un serveur proxy impose une demande d'authentification pour accéder à OneDrive qui se situe dans le WAN.



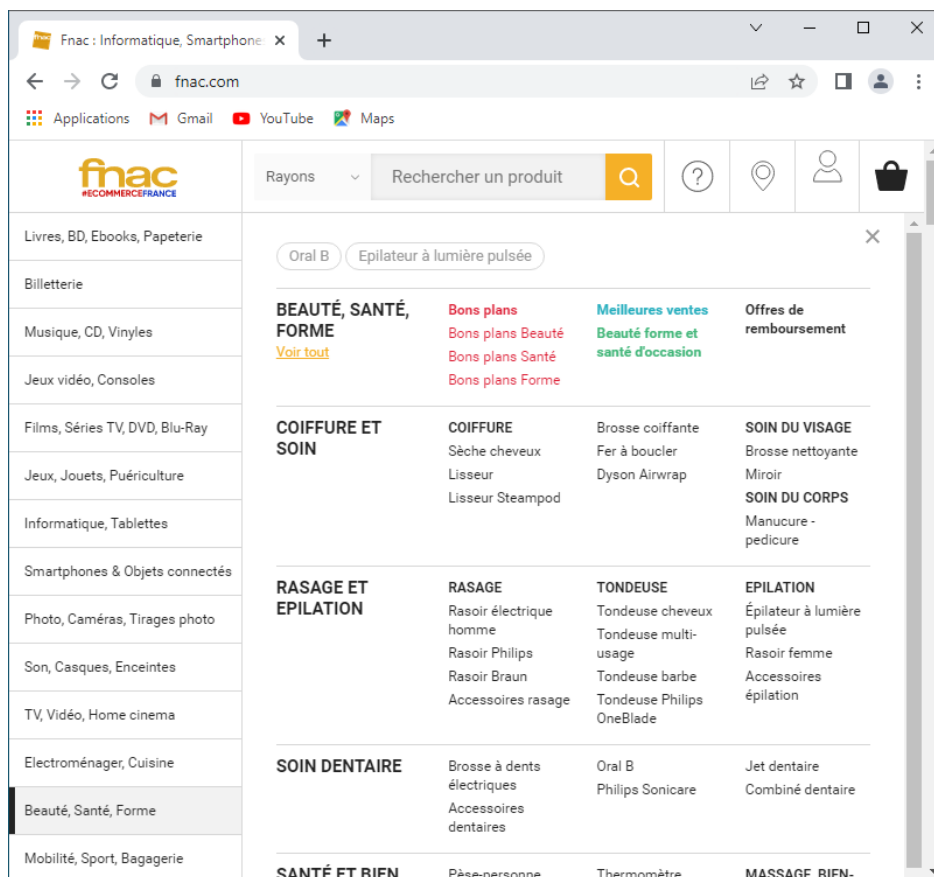
La navigation internet est soumise aux mêmes conditions et impose à l'utilisateur une authentification au serveur proxy pour continuer la navigation.



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.

