

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. Cration d'une rgle 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).

Système Statut Réseau Services Pare-feu IPFire Journaux

Configuration avancée

Proxy web avancé

Paramètres communs

Actif sur Green:

Transparent sur Green:

Filtre URL

Actif

Proxy montant

Adresse proxy transparente

Adresse ip du client

Nom d'utilisateur transparent

Aucune connexion directe sur la transmission

Configuration des zones

Système de noms de domaine (DNS)

Proxy web

Filtre de contenu URL

Accélérateur (cache)

Serveur DHCP

Page d'accueil (portail captif)

Planificateur de connexion

Port proxy : * 800

Port transparent : * 3128

Nom d'hôte visible : proxy

Langage des messages erronés : fr

Construction messages erronés : IPFire

Mise à jour accélérateur

Proxy montant (hôte:port) :

Nom d'utilisateur montant :

Mot de passe montant :

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).

ipfire.societea.lan

Système Statut Réseau Services Pare-feu IPFire Journaux Traffic: In 2.09 kbit/s Out 1.72 kbit/s

Configuration avancée du proxy web

Proxy web avancé

Paramètres communs

Actif sur Green:

Transparent sur Green:

Filtre URL

Actif

Mise à jour accélérateur

Actif

Port proxy : * 800

Port transparent : * 3128

Nom d'hôte visible : proxy

Langage des messages erronés : fr

Construction messages erronés : IPFire

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.

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	A		
Autorisé	<input checked="" type="checkbox"/>	00	00	24	00						

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:

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

Méthode d'authentification

Aucune Local identd LDAP RADIUS

Action:

* 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.

ipfire.societea.lan

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

Options de pare-feu

Règles de pare-feu
Groupes de pare-feu
Options de pare-feu (au interne)

Masquage (une seule IP pour plusieurs adresses)
Masque réseau VERT
Masque réseau ORANGE
Journalisation du pare-feu
Supprimer les anciens paquets de synchronisation
Suppression des paquets entrants du journal
Abandon des paquets avancés par le journal
Abandon des paquets sortants par le journal
Tables IP

Détection d'intrusion
Réseaux P2P
Blocage par localisation
Accès réseau BLEU

Masquage activé
Masquage activé

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.

Autorisé

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.

Autorisé

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 with a red header bar containing the IPFire logo and the URL "ipfire.societea.lan". Below the header is a navigation menu with tabs: Système, Statut, Réseau, Services, Pare-feu, IPFire, and Journaux. The "Réseau" tab is selected. At the top right, traffic information is displayed: "Traffic: In 0.00 bit/s Out 0.00 bit/s". The main content area is titled "Page principale" with a question mark icon. It displays network status for two interfaces:

Réseau	Adresse IP	Statut
INTERNET	172.16.128.1 ipfire.societea.lan 172.16.0.2	Connecté - (2m 31s)
LAN	192.168.0.2/24 10.0.0.2/8	Proxy actif Online
DMZ		

A note at the bottom of the main content area reads: "Veuillez s'il vous plaît activer le service Fireinfo."

At the bottom of the page, it says "IPFire 2.27 (x86_64) - Core Update 163" and "IPFire.org • Soutenez le projet IPFire avec votre don".

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

The screenshot shows the IPFire web interface with a red header bar containing the IPFire logo and the URL "ipfire.societea.lan". Below the header is a navigation menu with tabs: Système, Statut, Réseau, Services, Pare-feu, IPFire, and Journaux. The "Réseau" tab is selected. At the top right, traffic information is displayed: "Traffic: In 0.00 bit/s Out 0.00 bit/s". The main content area is titled "Page principale" with a question mark icon. It displays network status for two interfaces:

Réseau	Adresse IP	Statut
INTERNET	172.16.128.1 ipfire.societea.lan 172.16.0.2	Connecté - (29s)
LAN	192.168.0.2/24 10.0.0.2/8	Proxy actif (transparent) Online
DMZ		

A note at the bottom of the main content area reads: "Veuillez s'il vous plaît activer le service Fireinfo."

At the bottom of the page, it says "IPFire 2.27 (x86_64) - Core Update 163" and "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.

The screenshot shows the main menu of the ipfire.societea.lan web interface. The top navigation bar includes links for Système, Statut, Réseau (which is highlighted with a red box), Services, Pare-feu, IPFire, and Journaux. On the left, there's a sidebar with sections like Configuration filtre, Paramètres de filtre, Blocage de catégories, and Liste noire perso. The 'Filtre de contenu URL' option under 'Paramètres de filtre' is also highlighted with a red box. To the right, there are several configuration fields: 'audio-video:', 'mail:', 'warez:', and 'URL bloquées (une par ligne)'. A note says 'Exemple : www.domain.com/ads/'. Below these fields is a large text input area.

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

This screenshot shows the 'Configuration filtre URL' page. At the top, it displays 'Paramètres de filtre URL'. It has a section for 'Blocage de catégories' with checkboxes for ads, gambling, proxy, hacking, violence, audio-video, mail, drugs, and porn. Below this is a 'Liste noire perso' section with a text input field containing 'www.domain.com/ads/' and a note 'Exemple : www.domain.com/ads/'. There are also two scrollable lists for 'URL bloquées (une par ligne)' and 'Domaines bloqués (un par ligne)', both currently empty. At the bottom, there's a note 'Activer liste noire perso :' followed by a checkbox.

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

Configuration filtre URL

Paramètres de filtre URL

Bloque 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

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

Activer liste noire perso :

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

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

Activer liste blanche perso :

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

Réglages de filtre URL

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

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.

The screenshot shows the 'Maintenance de filtre URL' section of the IPFire webconfigurator. It includes fields for automatic update frequency (set to monthly), download source (Shalla Secure Services), and a personal URL source input. Buttons for saving and applying changes are present. Below this is the 'Editeur de liste noire' section with a link to edit a local blacklist file. The 'Sauvegarder les paramètres du filtre URL' section contains a checkbox for saving a full list and a button to create a backup file. The 'Restaurer les paramètres du filtre URL' section allows loading a previously saved configuration. At the bottom, there's a footer for IPFire 2.27 and a donation link.

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

This screenshot is identical to the one above, but with a red box highlighting the 'Mise à jour automatique de la liste noire' section. This section contains the 'Activer la mise à jour automatique' checkbox, the 'Fréquence de mise à jour automatique' dropdown set to 'Mensuelle', the 'Choisir une source de téléchargement' dropdown set to 'Univ. Toulouse', and the 'Source URL perso' input field. The rest of the page, including the editor, save options, and restore section, remains the same.

3. Cration d'une rgle NAT :

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

The screenshot shows the 'R gles de pare-feu' (Firewall Rules) configuration page. The 'NAT' section is highlighted with a red box. In this section, the 'Utiliser la traduction d'adresses r seau (NAT)' checkbox is checked, and the 'Destination NAT (redirection de port)' radio button is selected. The 'Interface pare-feu' dropdown is set to 'Automatique'. The 'Source' and 'Destination' sections show standard network selection criteria. The 'Protocole' section has a dropdown set to 'Tous'.

Ci-dessous la rgle NAT pour le r seau local 192.168.0.0/24 (LAN) pour autoriser le trafic.

The screenshot shows the list of firewall rules. There is one rule listed:

#	Protocole :	Source	Log	Destination	Action
1	Tous	Tout	<input type="checkbox"/>	Pare-feu ->192.168.0.0	<input checked="" type="checkbox"/>

The 'Destination' field shows 'Pare-feu ->192.168.0.0'. The 'Action' column contains icons for edit, add, and delete. The 'Protocole' column is set to 'Tous'. The 'Source' column is set to 'Tout'. The 'Log' column has an unchecked checkbox. The 'Destination' column is green, indicating it's a local network rule. The 'Action' column is also green. The bottom status bar indicates 'IPFire 2.27 (x86_64) - Core Update 163' and 'IPFire.org • Soutenez le projet IPFire avec votre don'.

4. Gestion des utilisateurs :

A partir de là, le proxy web est actif et interprétera 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 LunMarMerJeuVenSamDim De A
Autorisé ✓✓✓✓✓✓✓ 00:00:00 24:00:00

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 ☐

Détectations 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

Actions
Sauvegarder Sauvegarder et recharger Sauvegarder et redémarrer Effacer le cache

* 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 authentication global
Nombre de processus d'authentification : 5 Cache authentication TTL (en minutes) : 60 Limite d'adresses IP par utilisateur : Cache utilisateur / IP TTL (en minutes) : 0 Exiger l'authentification pour un accès sans restriction des adresses sources : ☑

Invite du domaine d'authentification :
Domaines sans authentication (un par ligne) :

Authentification des utilisateurs locaux
Longueur minimale du mot de passe : 6 Redirection par contournement pour les membres du groupe 'Etendu' : ☐

Gestion des utilisateurs

Actions
Sauvegarder Sauvegarder et recharger Sauvegarder et redémarrer Effacer le cache

* Champs requis

Créez un utilisateur autorisé à utiliser le service proxy web.

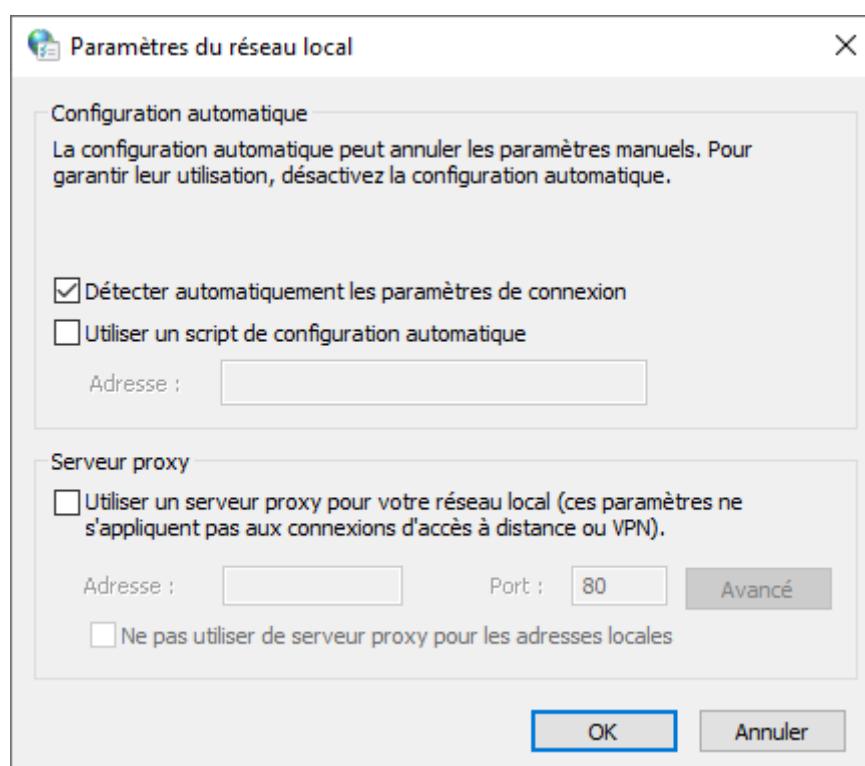
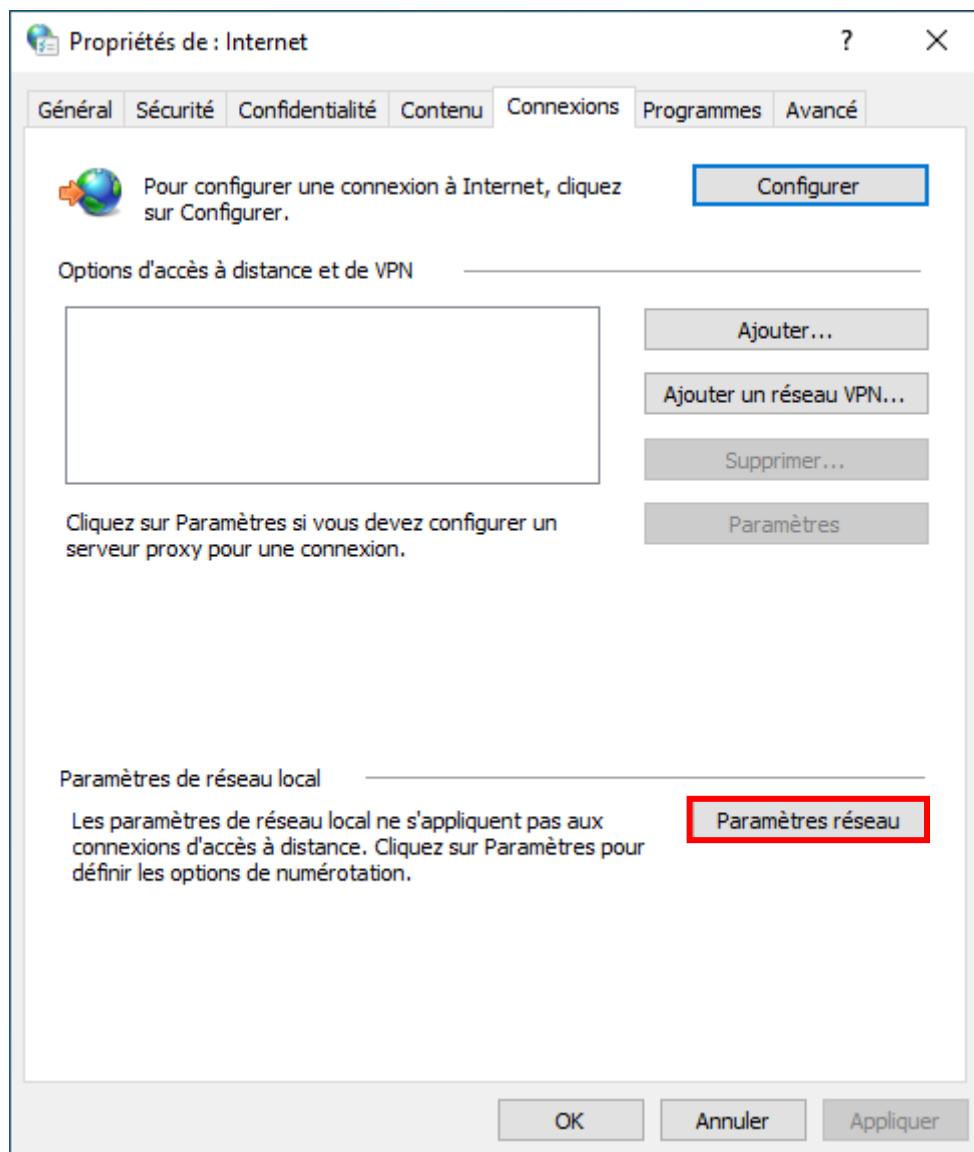
The screenshot shows the 'Advanced proxy configuration' page. In the 'User authentication' section, a new user 'userweb' is being created with a password of '*****'. The user is assigned to the 'Standard' group. Below this, a message indicates 'Aucun compte utilisateur disponible' (No user accounts available). At the bottom of the page, it says 'IPFire 2.27 (x86_64) - Core Update 163' and '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.

The screenshot shows the same 'Advanced proxy configuration' page after the user 'userweb' has been created. The 'User authentication' section now lists 'userweb' under 'Comptes utilisateurs'. The 'Appartenance au groupe' (Group membership) row for 'userweb' shows 'Standard' with edit and delete icons. A legend at the bottom explains the icons: a pencil for 'Modifier' (Edit) and a trash can for 'Enlever' (Delete). The footer information remains the same as in the previous screenshot.

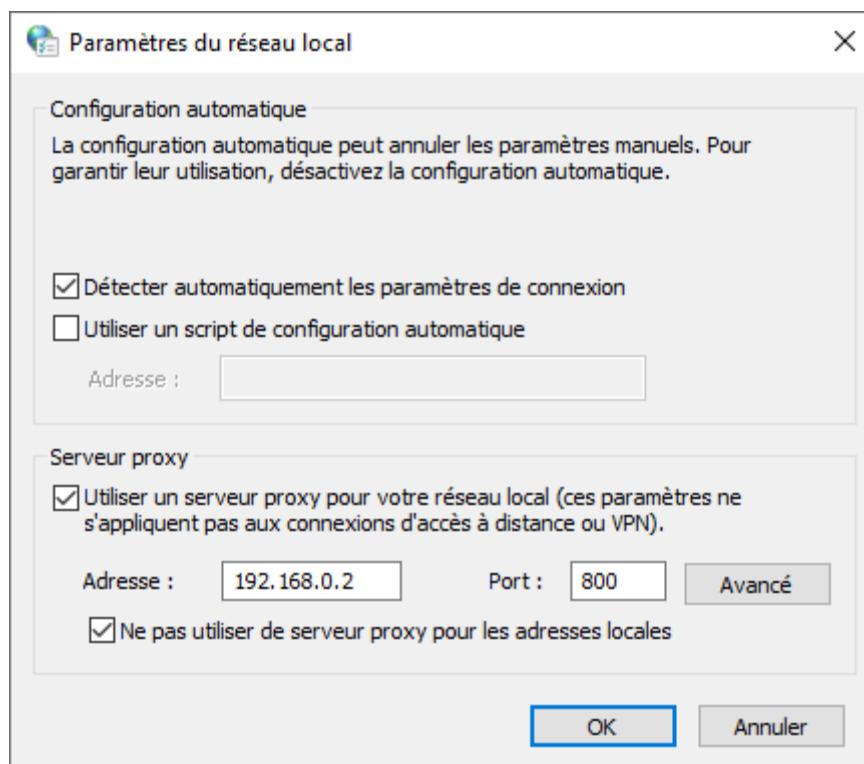
5. Configuration du proxy sur un client :

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

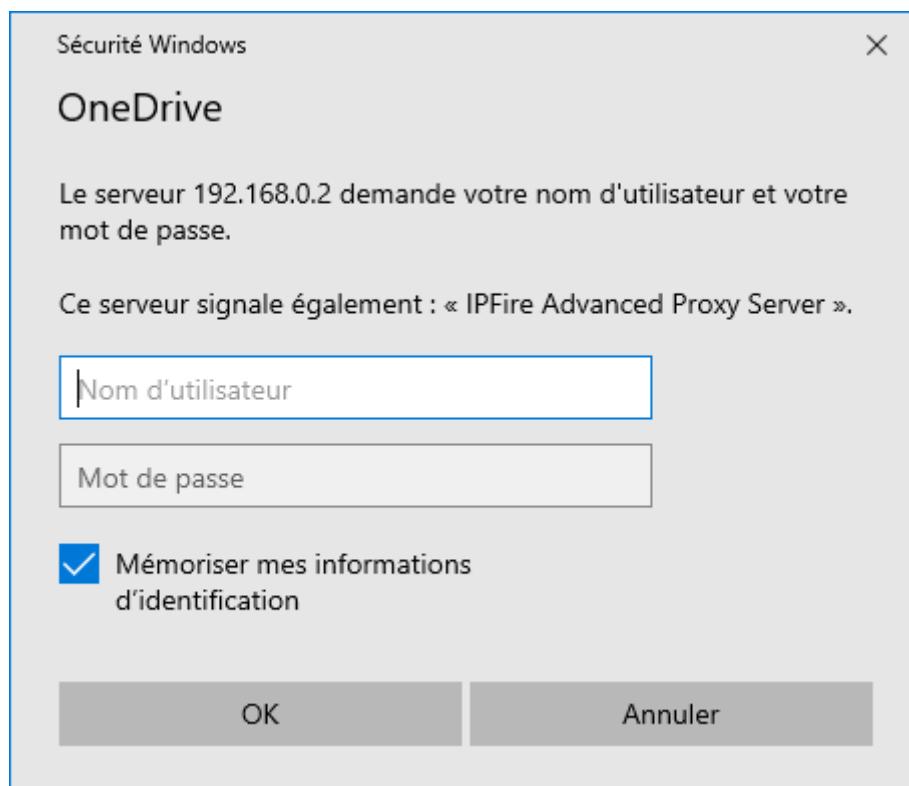


Activez l'utilisation du service proxy et spécifiez l'adresse IP du serveur ainsi que le port par défaut.

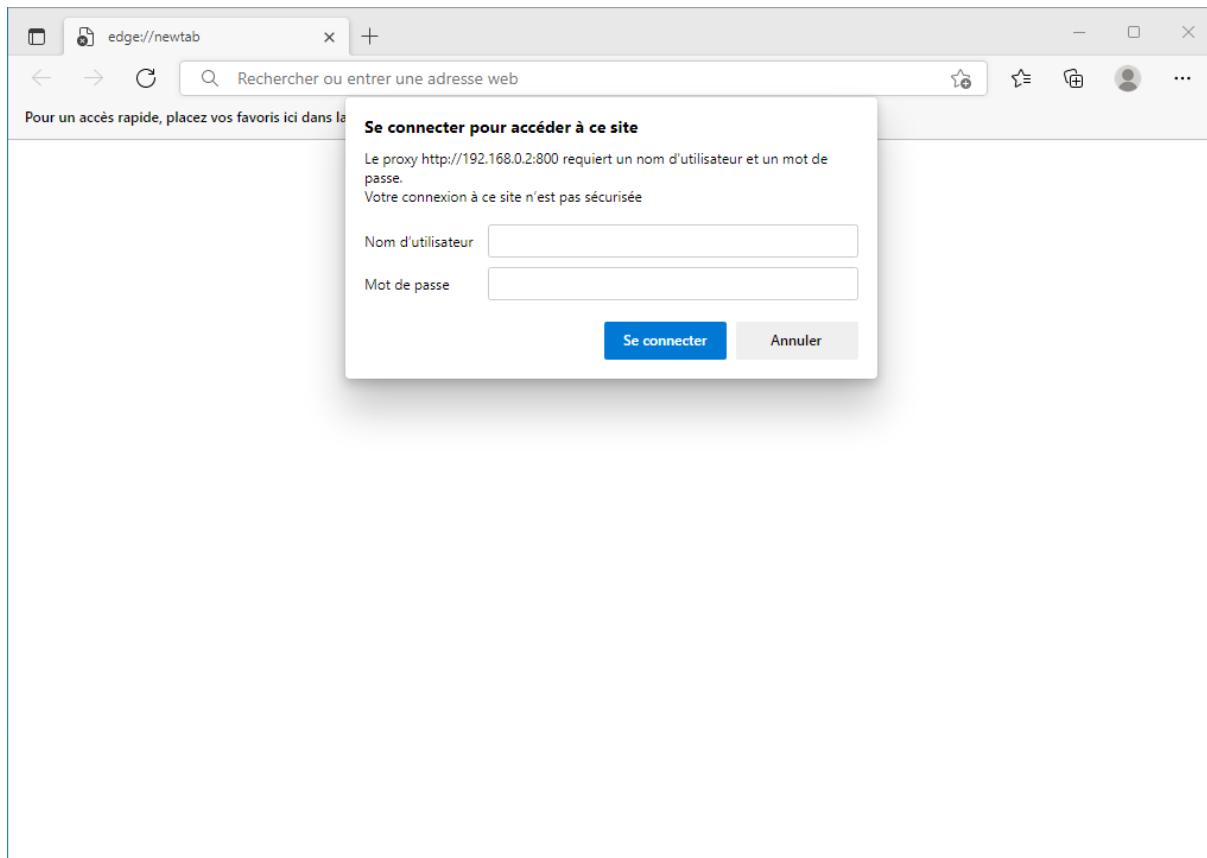
Décochez la détection automatique pour éviter les perturbations.



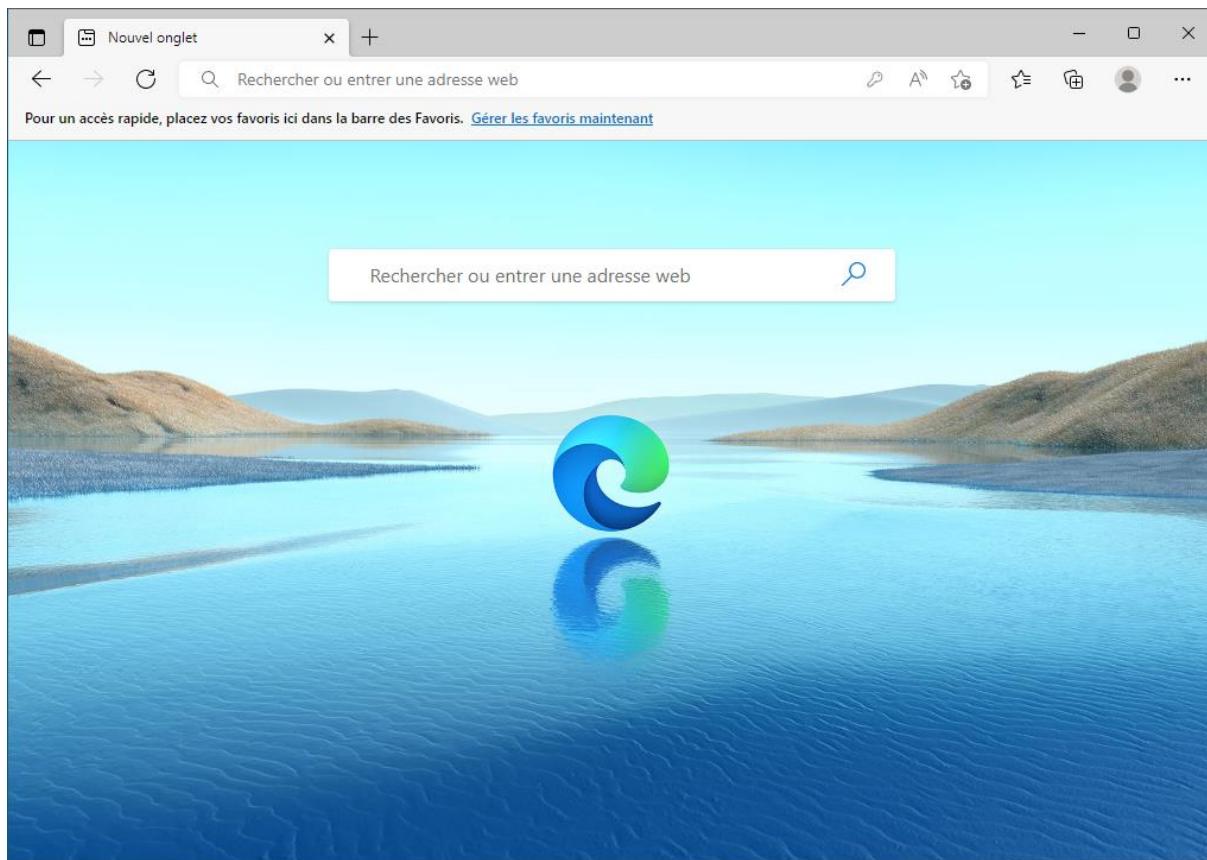
La détection d'un serveur proxy impose une demande d'authentification pour accéder à OneDrive qui se situe dans le WAN.



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.

The screenshot shows a web browser window with the URL fnac.com. The page displays the Fnac homepage with various product categories like Books, Music, Games, and Electronics. A search bar at the top right contains the text "Rechercher un produit". Below the search bar, there are several promotional sections: "BONS PLANS" (with links to Oral B and Epilator à lumière pulsée), "MEILLEURES VENTES" (with links to Oral B, Epilator à lumière pulsée, and other products), and "OFFRES DE REMBOURSEMENT". The sidebar on the left lists categories such as Livres, BD, Ebooks, Papeterie; Billetterie; Musique, CD, Vinyls; Jeux vidéo, Consoles; Films, Séries TV, DVD, Blu-Ray; Jeux, Jouets, Puériculture; Informatique, Tablettes; Smartphones & Objets connectés; Photo, Caméras, Tirages photo; Son, Casques, Enceintes; TV, Vidéo, Home cinema; Electroménager, Cuisine; Beauté, Santé, Forme; Mobilité, Sport, Bagagerie.

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

The screenshot shows a web browser window with the URL www.fnac.com. The page displays a "Ce site est inaccessible" error message. The text below the error message states: "Il se peut que la page Web à l'adresse <https://www.fnac.com/> soit temporairement inaccessible ou qu'elle ait été déplacée de façon permanente à une autre adresse Web." At the bottom of the error message, it says "ERR_TUNNEL_CONNECTION_FAILED".