

Mettre en place des règles via Ipfire.

Table des matières

1. Les règles globales :	2
2. Les règles fines :	7

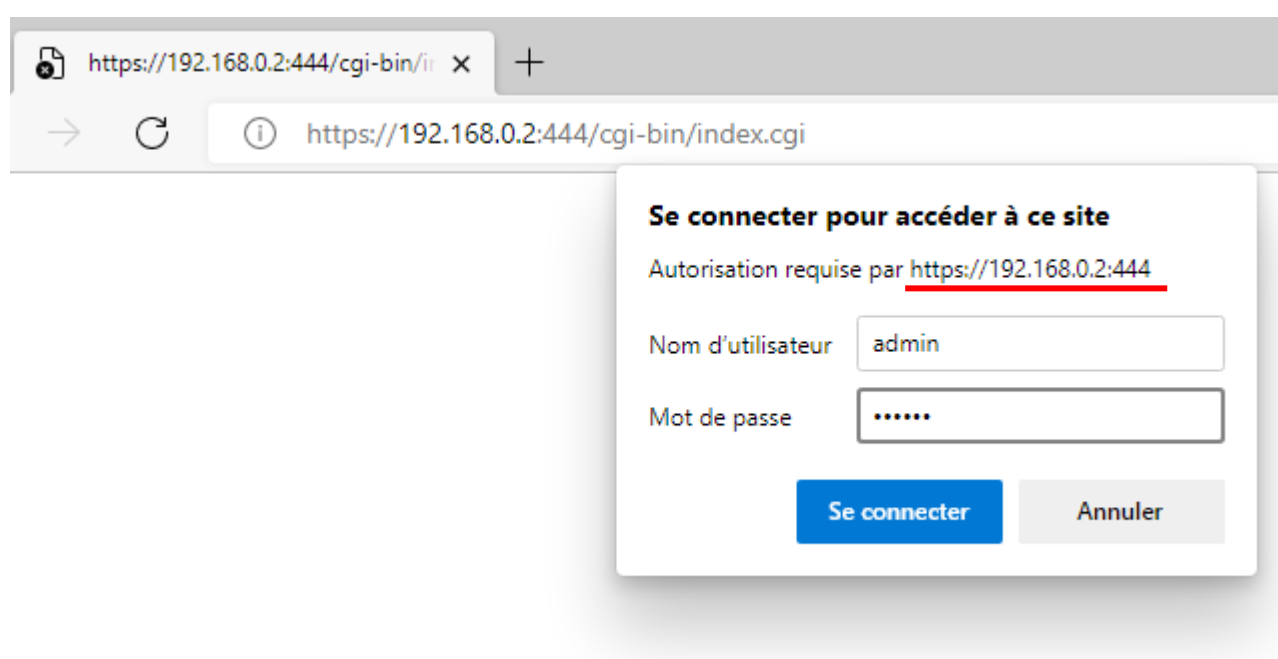
1. Les règles globales :

Comme pour le logiciel/matériel Pfsense, Ipfire permet d'établir des règles pour contrôler le flux entrant ou sortant à travers les divers réseaux.

La sémantique concernant la mise en place des règles est proche de celle de Pfsense ou les autres solutions de firewall.

Vous pouvez définir les règles en ligne de commande par le biais du terminal ou accéder au configurateur graphique par le biais d'un navigateur internet.

Vous devez spécifier l'adresse IP du pare-feu et le port 444 (par défaut) avec le protocole HTTPS dans un navigateur internet (**exemple : *https://192.168.0.2:444***).



Utilisez le compte **admin** configuré par défaut pour administrer le pare-feu depuis le webconfigurator.

Vous accéderez au tableau de bord regroupant l'ensemble des fonctionnalités que permet le système Ipfire.

ipfire.societea.lan - Page principale x +

Non sécurisé | <https://192.168.0.2:444/cgi-bin/index.cgi>

ipfire.societea.lan

Système Statut Réseau Services Pare-feu IPFire Journaux Traffic: In 2.00 Mbit/s Out 311.37 kbit/s

Page principale ?

Réseau	Adresse IP	Statut
INTERNET	172.16.128.1	Connecté - (2m 59s)
Nom hôte :	ipfire.societea.lan	
Passerelle :	172.16.0.2	
Réseau	Adresse IP	Statut
LAN	192.168.0.2/24	Proxy inactif

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

ipfire.societea.lan - Page principale x +

Non sécurisé | <https://192.168.0.2:444/cgi-bin/index.cgi>

ipfire.societea.lan

Système Statut Réseau Services Pare-feu IPFire Journaux Traffic: In 2.01 Mbit/s Out 50.13 kbit/s

Page principale ?

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

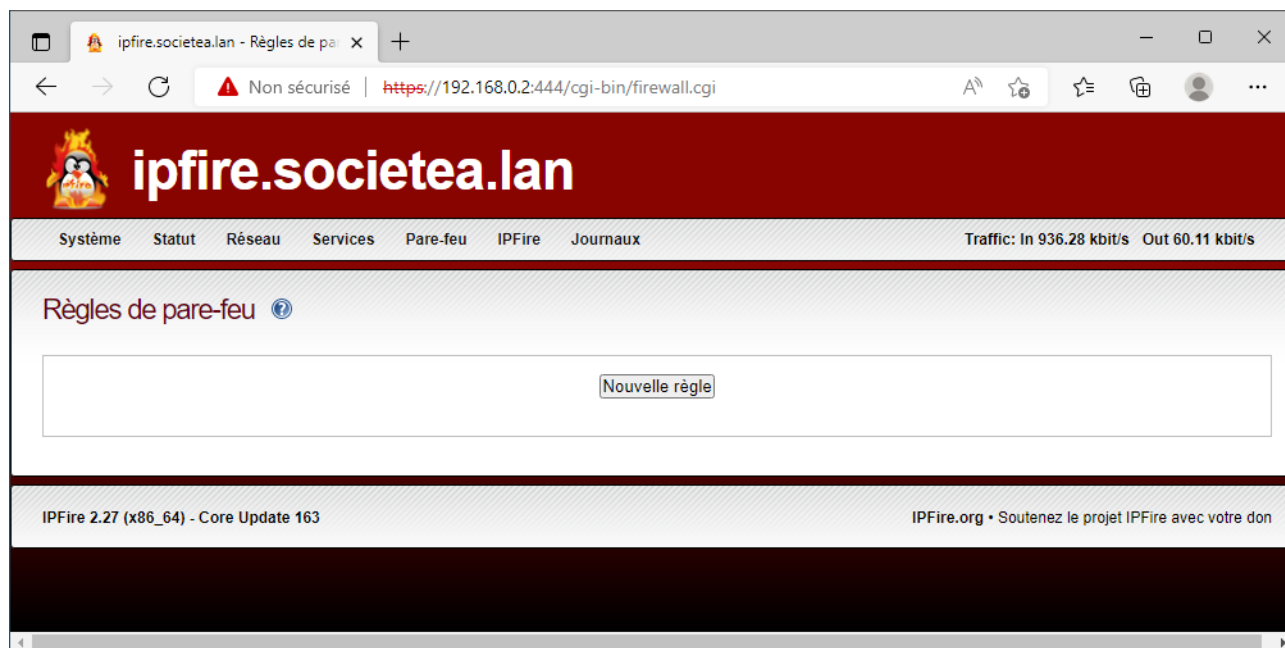
Réseau	Adresse IP	Statut
INTERNET	172.16.128.1	Connecté - (4m 2s)
Nom hôte :	ipfire.societea.lan	
Passerelle :	172.16.0.2	
Réseau	Adresse IP	Statut
LAN	192.168.0.2/24	Proxy inactif

Note

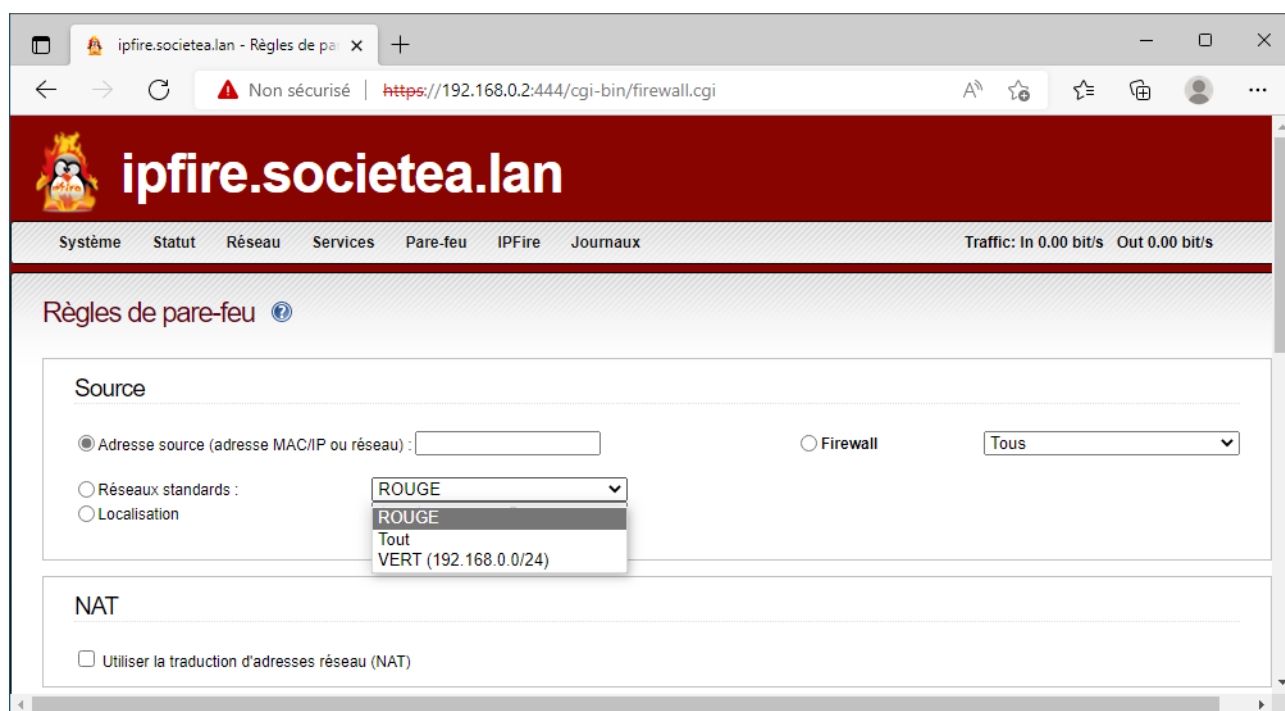
- Veuillez s'il vous plaît activer le service Fireinfo.

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

Les règles sont accessibles depuis l'onglet Pare-feu du configurateur.



Créez une nouvelle règle pour l'interface GREEN (LAN) en tant que Source.



The screenshot shows the IPFire firewall configuration interface. The browser address bar indicates the URL `https://192.168.0.2:444/cgi-bin/firewall.cgi`. The page is titled "ipfire.societea.lan - Règles de pa".

Source

- ☐ Adresse source (adresse MAC/IP ou réseau) :
- ☒ Réseaux standards :
 - VERT (192.168.0.0/24)
 - A1 - Anonymous Proxy
- ☐ Localisation

Firewall : Tous

NAT

- ☐ Utiliser la traduction d'adresses réseau (NAT)

Destination

- ☐ Adresse IP de destination (adresse IP ou réseau) :
- ☒ Réseaux standards :
 - ROUGE
 - A1 - Anonymous Proxy
- ☐ Localisation

Firewall : Tous

Protocole

A destination du réseaux RED (le WAN) afin de l'interdire (REFUSER).

The screenshot shows the IPFire firewall configuration interface. The browser address bar indicates the URL `https://192.168.0.2:444/cgi-bin/firewall.cgi`. The page is titled "ipfire.societea.lan - Règles de pa".

Protocole

- TCP

Port source : Port de destination :

☐ ACCEPTER ☐ IGNORER ☒ REFUSER

Paramètres additionnels

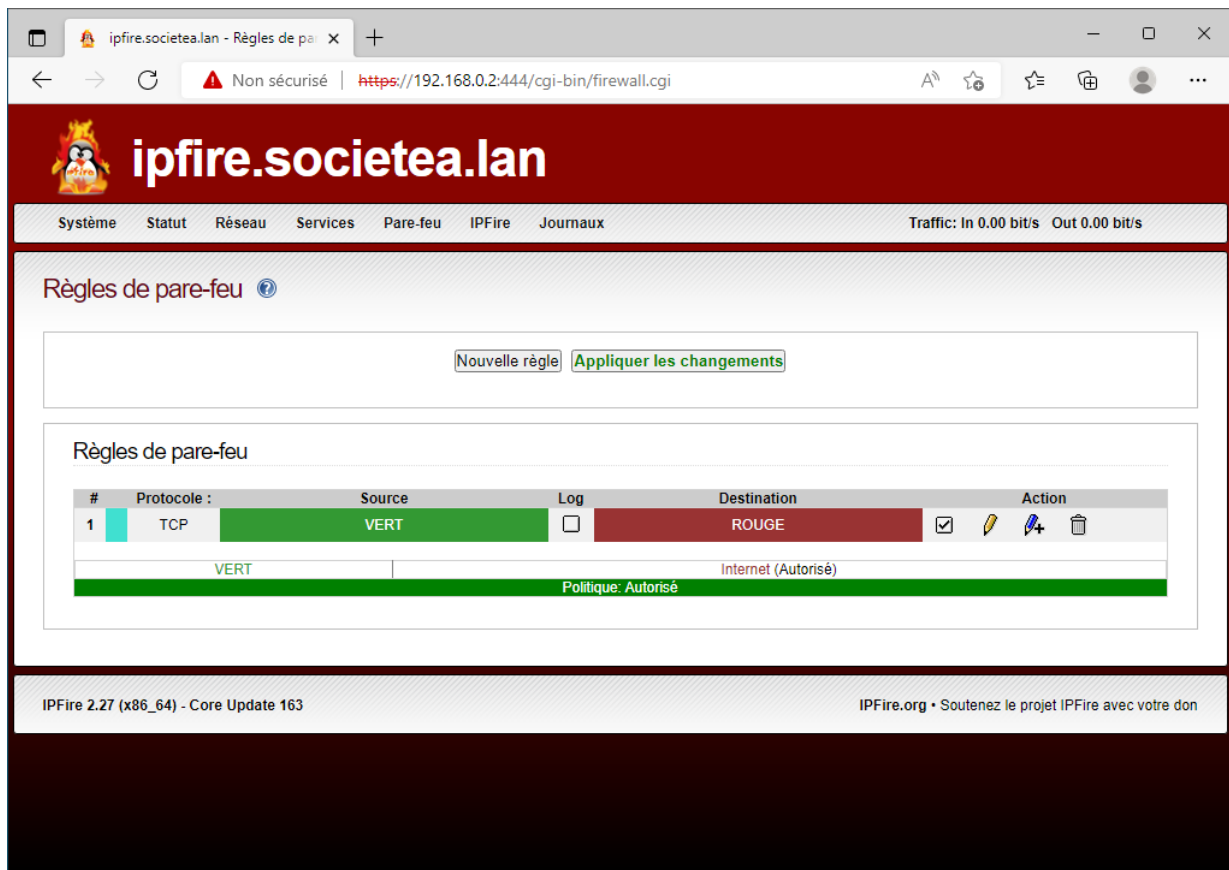
Remarque : Position de règle :

- ☐ Log de règle
- ☐ Utiliser les contraintes horaires
- ☐ Limiter les connexions simultanées par adresse IP
- ☐ Limiter le nombre des nouvelles connexions

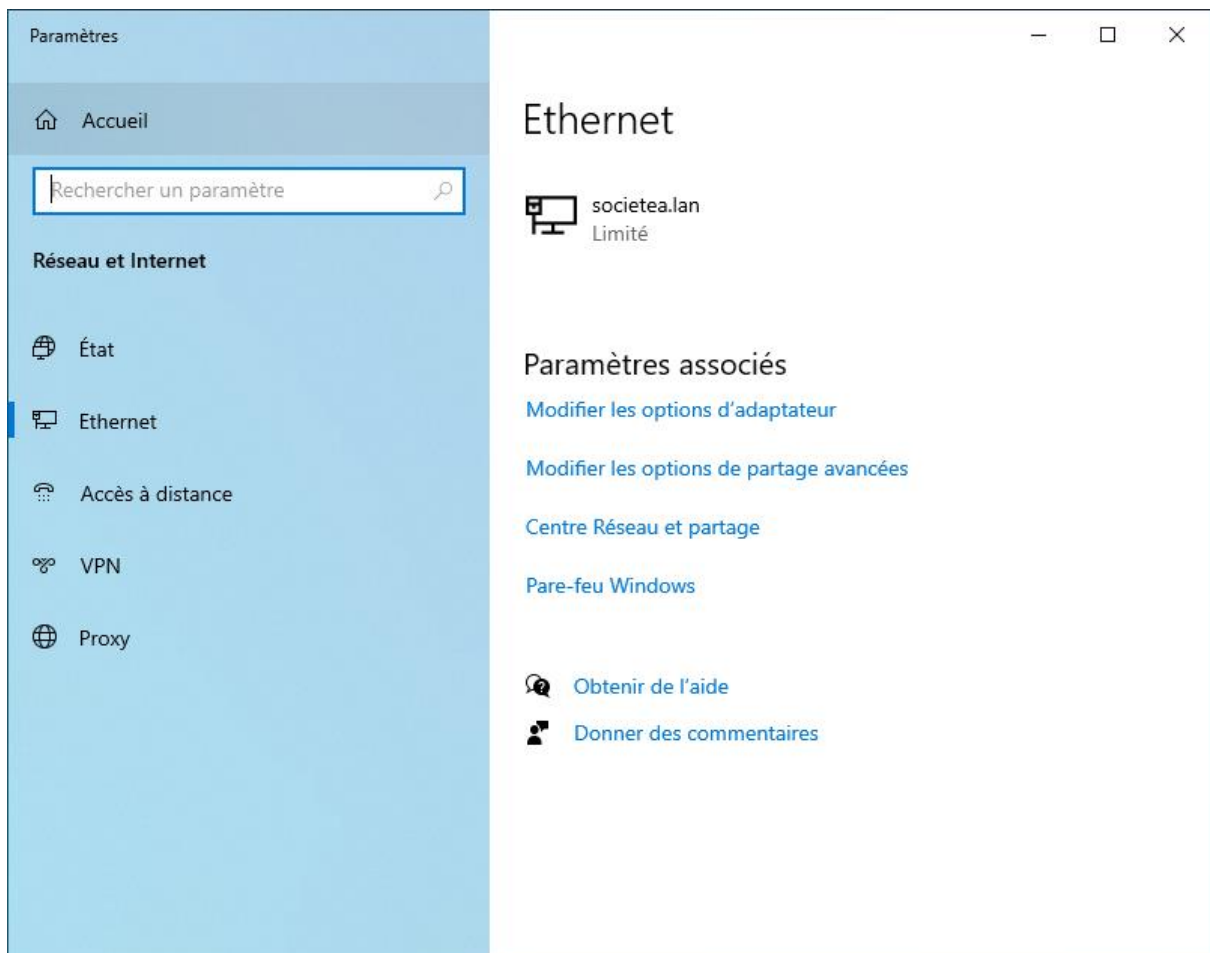
Ajouter Retour

Vous pouvez spécifier le protocole à autoriser/interdire ainsi que les ports sources et de destinations.

Choisir de refuser ou ignorer le protocole TCP par exemple, puis ajoutez la règle.



Appliquez les changements pour lire et exécuter cette nouvelle règle globale interdisant le trafic TCP à destination du réseau WAN.



Après un court instant, si la règle s'est correctement appliquée, les postes du réseau LAN ne doivent plus avoir accès à l'extérieur et donc à Internet.

```
Invite de commandes

C:\Users\admin>ping 1.1.1.1

Envoi d'une requête 'Ping' 1.1.1.1 avec 32 octets de données :
Réponse de 192.168.0.2 : Impossible de joindre le port de destination.
Réponse de 192.168.0.2 : Impossible de joindre le port de destination.
Réponse de 192.168.0.2 : Impossible de joindre le port de destination.
Réponse de 192.168.0.2 : Impossible de joindre le port de destination.

Statistiques Ping pour 1.1.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

C:\Users\admin>
```

2. Les règles fines :

Comme pour n'importe quel pare-feu, les règles sont lues de manière séquentielle par le système, l'ordre de lecture des règles est important afin qu'elles soient lues et puissent s'appliquer sans contradiction entre elles.

The screenshot shows the IPFire web interface in a browser. The address bar indicates the URL `https://192.168.0.2:444/cgi-bin/firewall.cgi`. The page title is "ipfire.societea.lan - Règles de pare-feu". The main content area is titled "Règles de pare-feu" and contains a table of firewall rules. The table has columns for #, Protocole, Source, Log, Destination, and Action. There are two rules listed: Rule 1 (blue) for 'Tous' (All) traffic from 'VERT' (Green) to 'ROUGE' (Red), and Rule 2 (green) for 'Tous' (All) traffic from '192.168.0.37' to 'ROUGE' (Red). Both rules have the 'Log' checkbox checked and the 'Action' column shows a green checkmark. Below the table, there is a summary bar showing 'VERT' and 'Internet (Autorisé)' with the policy 'Politique: Autorisé'. The footer of the interface shows 'IPFire 2.27 (x86_64) - Core Update 163' and a link to 'IPFire.org'.

#	Protocole	Source	Log	Destination	Action
1	Tous	VERT	<input checked="" type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>
2	Tous	192.168.0.37	<input checked="" type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>

VERT Internet (Autorisé)
Politique: Autorisé

La règle fine pour le client 192.168.0.37 qui vient d'être créée doit donc être placée devant la règle globale afin qu'elle soit lue et appliquée sinon le système ne la lira même pas et appliquera simplement la règle globale.

Cette règle autorise le trafic à travers le Wan pour le poste client 192.168.0.37.

The screenshot shows the IPFire web interface at <https://192.168.0.2:444/cgi-bin/firewall.cgi>. The page title is "Règles de pare-feu". At the top, there is a "Nouvelle règle" button and an "Appliquer les changements" button. Below this, the "Règles de pare-feu" table is displayed. Rule 1 is highlighted in green and is positioned at the top of the list. Rule 2 is below it. The table has columns for #, Protocole, Source, Log, Destination, and Action. Rule 1 has Source "192.168.0.37" and Destination "ROUGE". Rule 2 has Source "VERT" and Destination "ROUGE". Below the table, there is a summary bar showing "VERT" and "Internet (Autorisé)" with the policy "Politique: Autorisé". The footer shows "IPFire 2.27 (x86_64) - Core Update 163" and "IPFire.org • Soutenez le projet IPFire avec votre don".

#	Protocole	Source	Log	Destination	Action
1	Tous	192.168.0.37	<input type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>
2	Tous	VERT	<input type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>

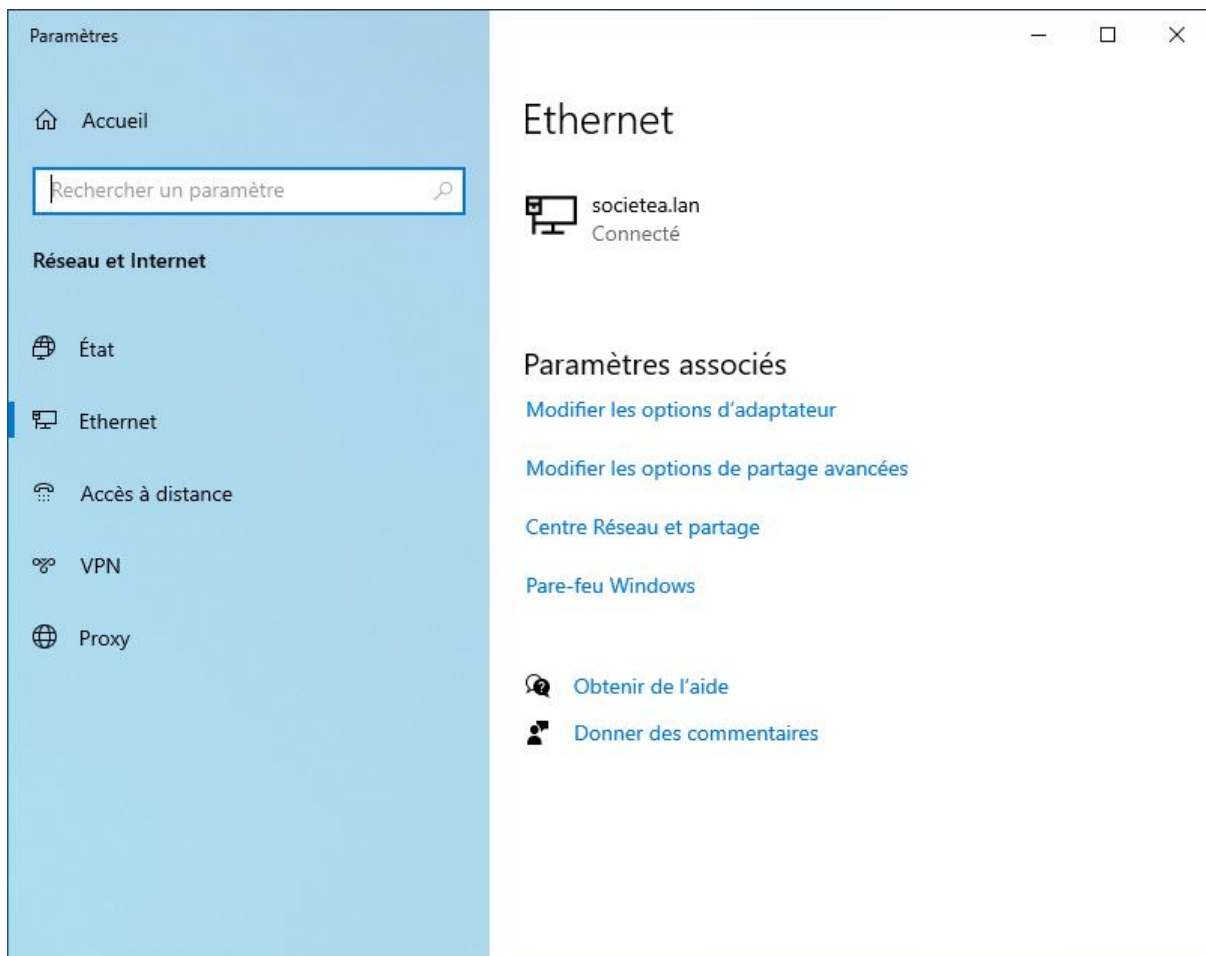
VERT Internet (Autorisé)
Politique: Autorisé

This screenshot is identical to the one above, showing the IPFire web interface with the same firewall rules. Rule 1 is at the top, followed by Rule 2. The summary bar and footer are also the same.

#	Protocole	Source	Log	Destination	Action
1	Tous	192.168.0.37	<input type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>
2	Tous	VERT	<input type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>

VERT Internet (Autorisé)
Politique: Autorisé

Après un court instant, les changements doivent s'appliquer et le poste client autorisé devrait récupérer une connexion au réseau WAN.



```
Invite de commandes

C:\Users\admin>ping 1.1.1.1

Envoi d'une requête 'Ping' 1.1.1.1 avec 32 octets de données :
Réponse de 1.1.1.1 : octets=32 temps=106 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=100 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=97 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=83 ms TTL=127

Statistiques Ping pour 1.1.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 83ms, Maximum = 106ms, Moyenne = 96ms

C:\Users\admin>
```