

# Mettre en place des règles via Ipfire.

## Table des matières

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

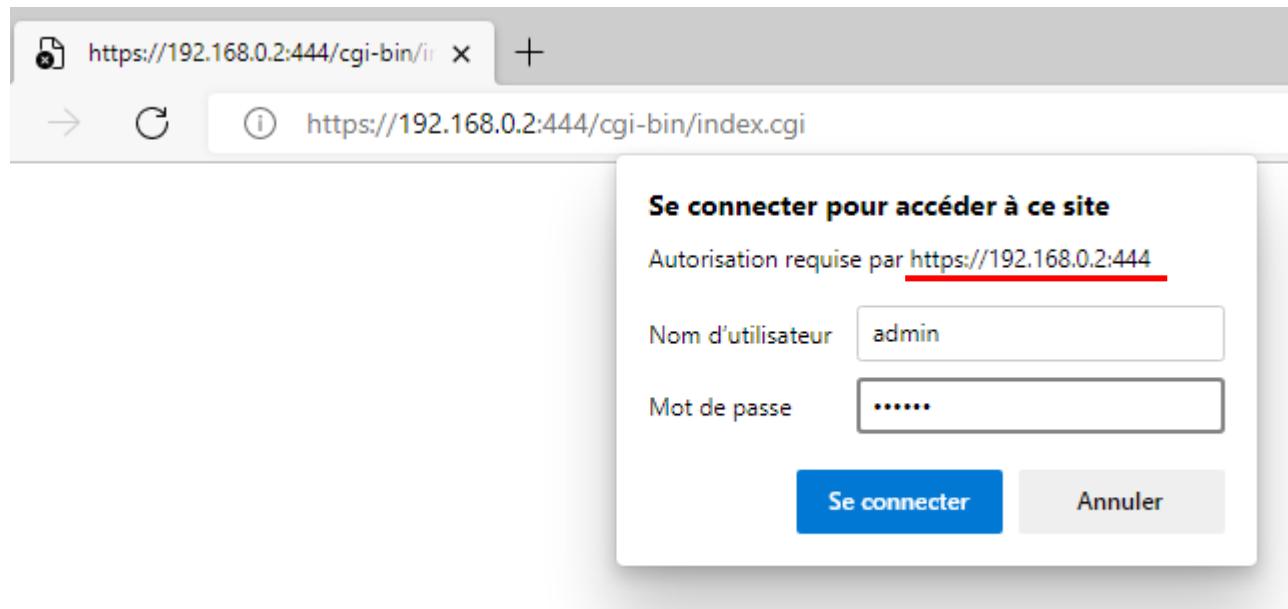
## 1. Les règles globales :

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 spécifiez 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 webconfigurateur.

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

ipfire.societea.lan - Page principale

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 ipfire.societea.lan 172.16.0.2	Connecté - (2m 59s)
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

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

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

Note

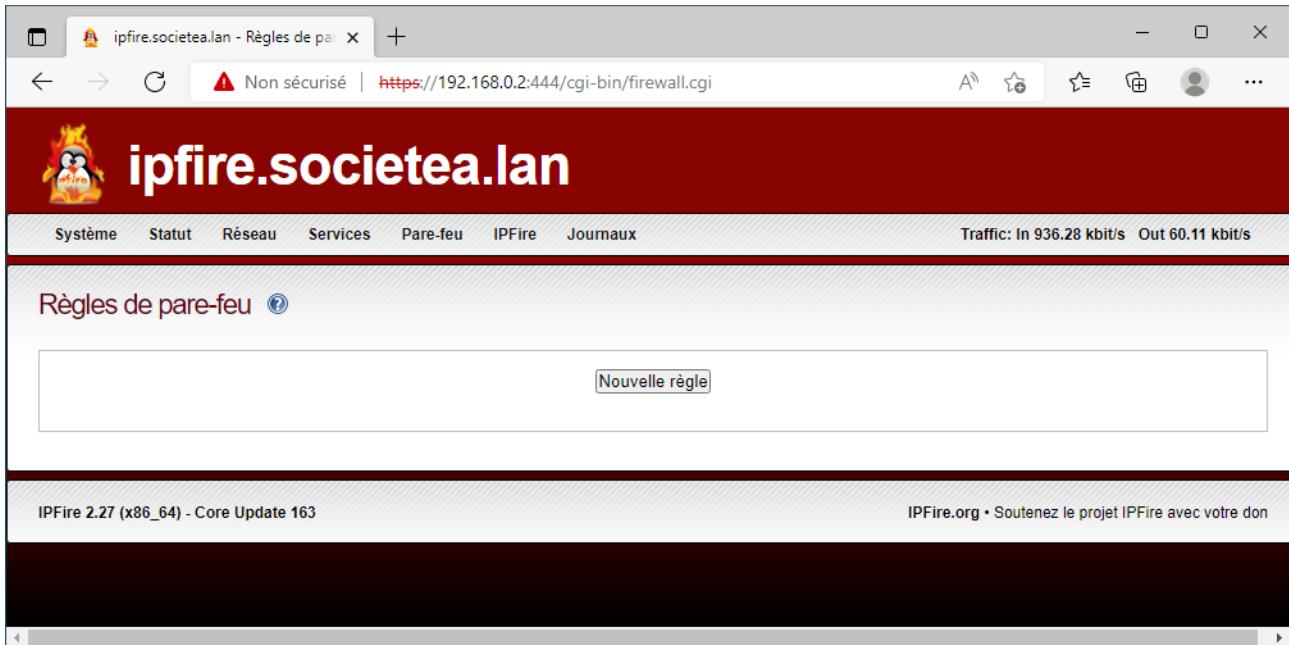
- Veuillez s'il vous plaît activer le service Fireinfo.

IPFire 2.27 (x86\_64) - Core Update 163

IPFire.org • Soutenez le projet IPFire avec votre don

https://192.168.0.2:444/cgi-bin/index.cgi

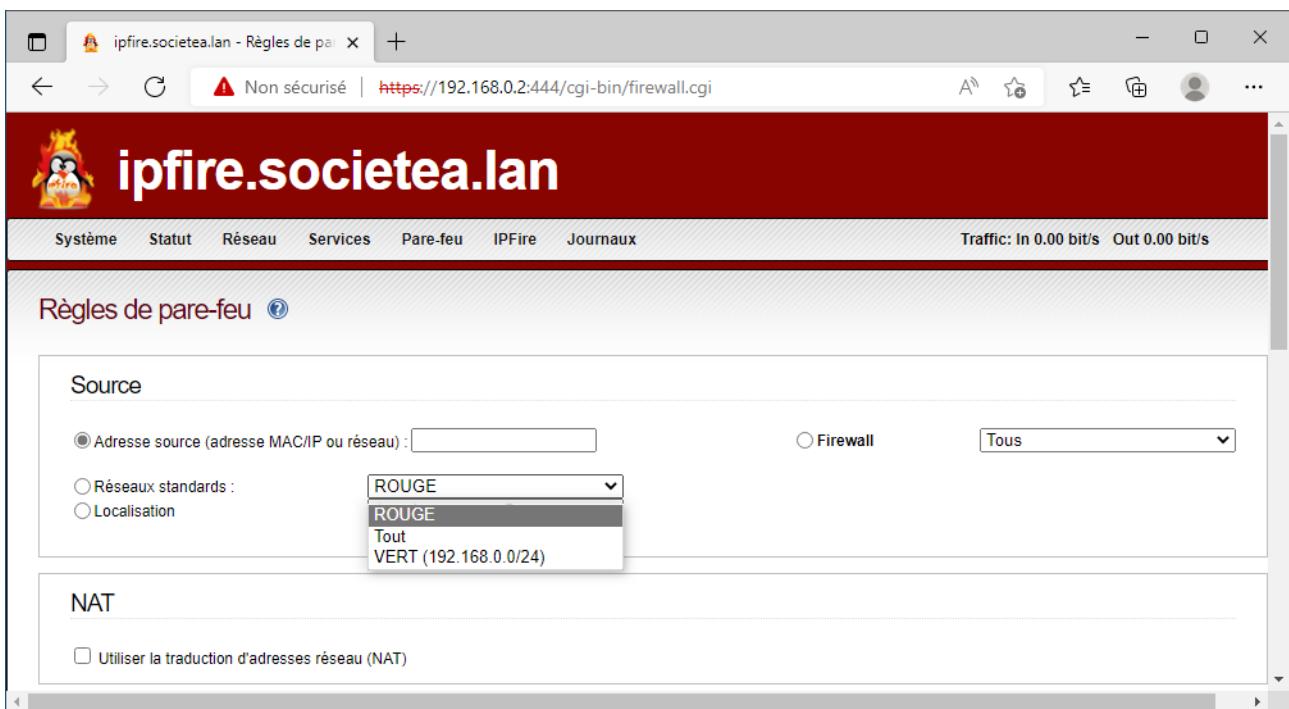
Les règles sont accessibles depuis l'onglet Pare-feu du configurateur.



The screenshot shows the IPFire web interface with the following details:

- Header:** The title bar shows "ipfire.societea.lan - Règles de pare-feu" and the URL "https://192.168.0.2:444/cgi-bin/firewall.cgi". A warning icon indicates "Non sécurisé".
- Header Bar:** The top navigation bar includes links for Système, Statut, Réseau, Services, Pare-feu (which is the active tab), IPFire, and Journaux. It also displays "Traffic: In 936.28 kbit/s Out 60.11 kbit/s".
- Content Area:** The main content is titled "Règles de pare-feu" with a "Nouvelle règle" button. Below this is a large empty table area for displaying rules.
- Footer:** The footer displays "IPFire 2.27 (x86\_64) - Core Update 163" and a link to "IPFire.org • Soutenez le projet IPFire avec votre don".

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



The screenshot shows the IPFire web interface with the following details:

- Header:** The title bar shows "ipfire.societea.lan - Règles de pare-feu" and the URL "https://192.168.0.2:444/cgi-bin/firewall.cgi". A warning icon indicates "Non sécurisé".
- Header Bar:** The top navigation bar includes links for Système, Statut, Réseau, Services, Pare-feu (active), IPFire, and Journaux. It displays "Traffic: In 0.00 bit/s Out 0.00 bit/s".
- Content Area:** The main content is titled "Règles de pare-feu" with a "Source" section. It includes fields for "Adresse source (adresse MAC/IP ou réseau)" (with a checked radio button), "Réseaux standards" (with "ROUGE" selected), "Localisation" (with "Tout" selected), and a dropdown menu showing "ROUGE" (selected), "Tout", and "VERT (192.168.0.0/24)".
- Other Sections:** Below the "Source" section is a "NAT" section with a checkbox for "Utiliser la traduction d'adresses réseau (NAT)" (unchecked).

ipfire.societea.lan - Règles de pa... +

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

**Source**

Adresse source (adresse MAC/IP ou réseau) :   Firewall

Réseaux standards :   Localisation

**NAT**

Utiliser la traduction d'adresses réseau (NAT)

**Destination**

Adresse IP de destination (adresse IP ou réseau) :   Firewall

Réseaux standards :   Localisation

**Protocole**

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

ipfire.societea.lan - Règles de pa... +

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

**Protocole**

Port source :  Port de destination :

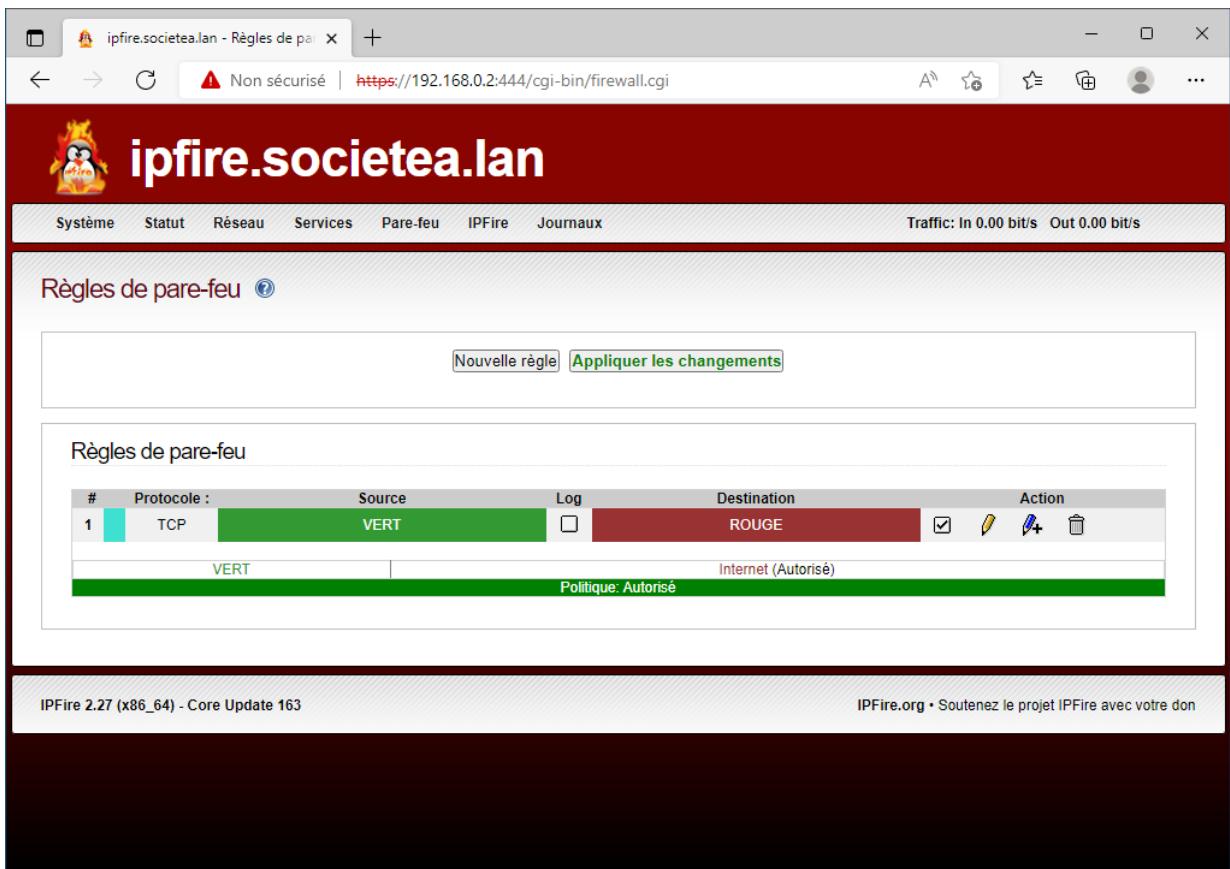
ACCEPTER  IGNORER  REFUSER

**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

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.



ipfire.societea.lan - Règles de pare-feu

Non sécurisé | https://192.168.0.2:444/cgi-bin/firewall.cgi

# ipfire.societea.lan

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

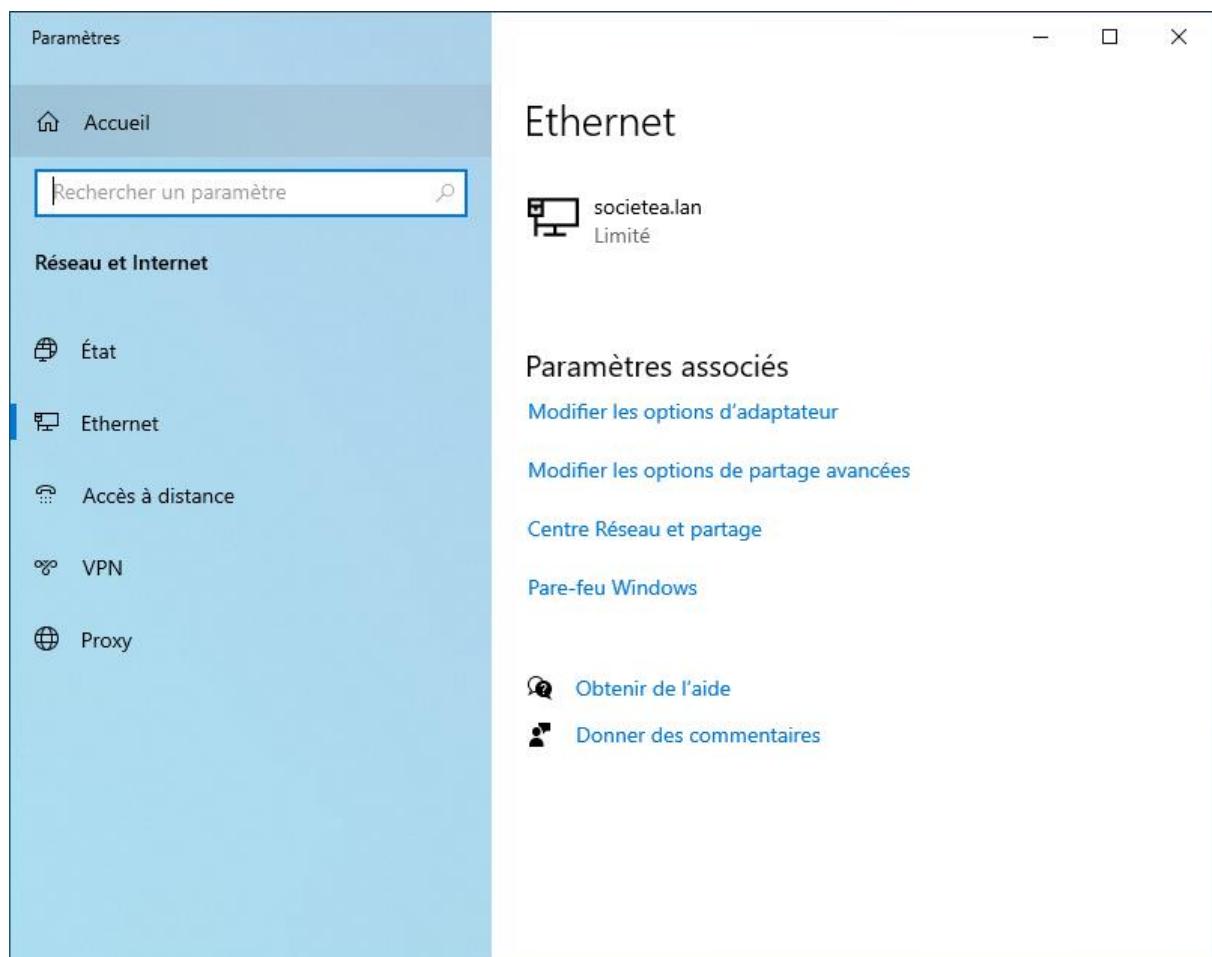
## Règles de pare-feu

Nouvelle règle Appliquer les changements

#	Protocole :	Source	Log	Destination	Action
1	TCP	VERT	<input type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>   
Politique: Autorisé Internet (Autorisé)					

IPFire 2.27 (x86\_64) - Core Update 163 IPFire.org • Soutenez le projet IPFire avec votre don

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



Paramètres

Accueil

Rechercher un paramètre

Réseau et Internet

État

Ethernet

Accès à distance

VPN

Proxy

## Ethernet

societea.lan Limité

Paramètres associés

Modifier les options d'adaptateur

Modifier les options de partage avancées

Centre Réseau et partage

Pare-feu Windows

Obtenir de l'aide

Donner des commentaires

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.



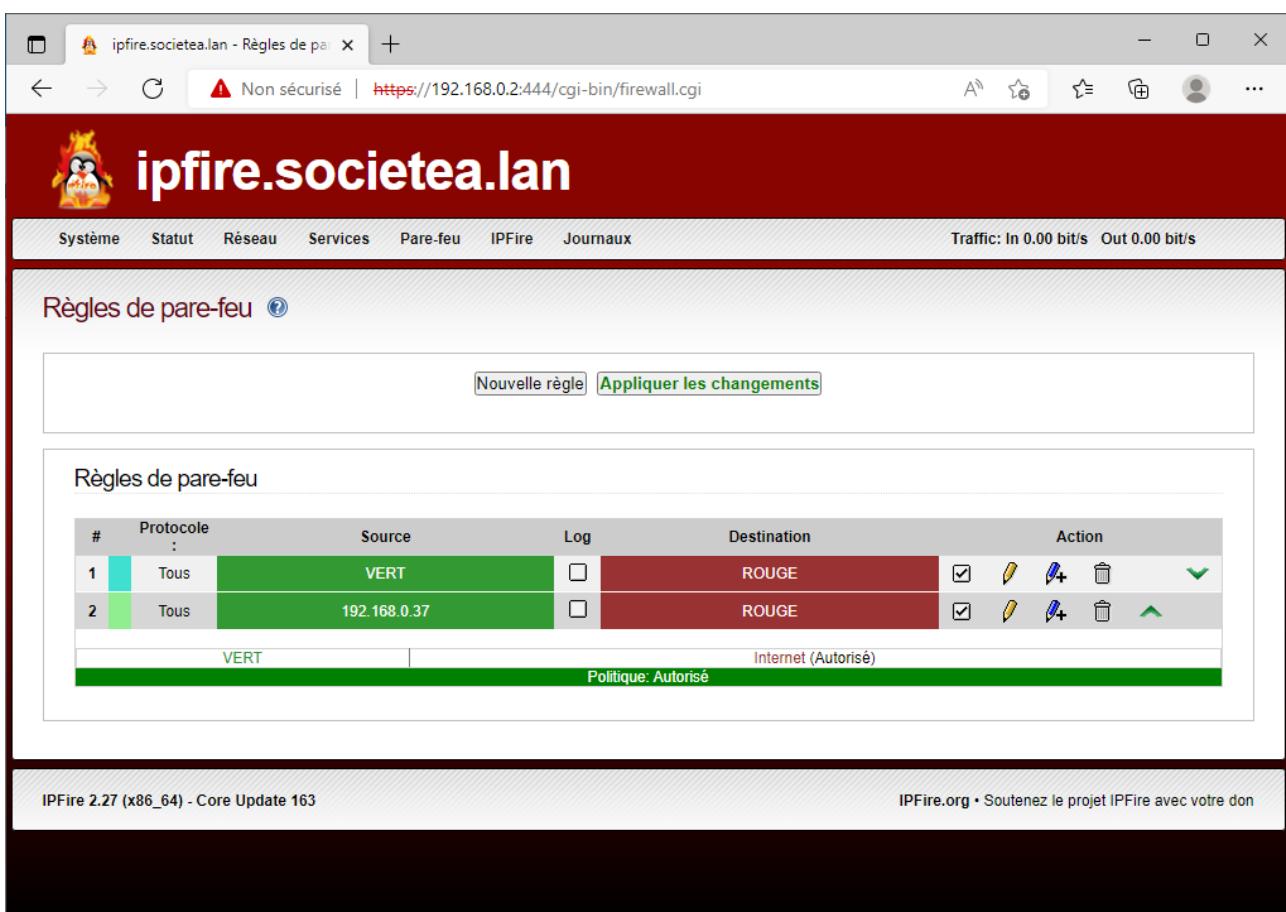
```
C:\Users\admin>ping 1.1.1.1

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.



ipfire.societea.lan - Règles de pare-feu

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

### Règles de pare-feu

Nouvelle règle Appliquer les changements

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

Vert | Internet (Autorisé)

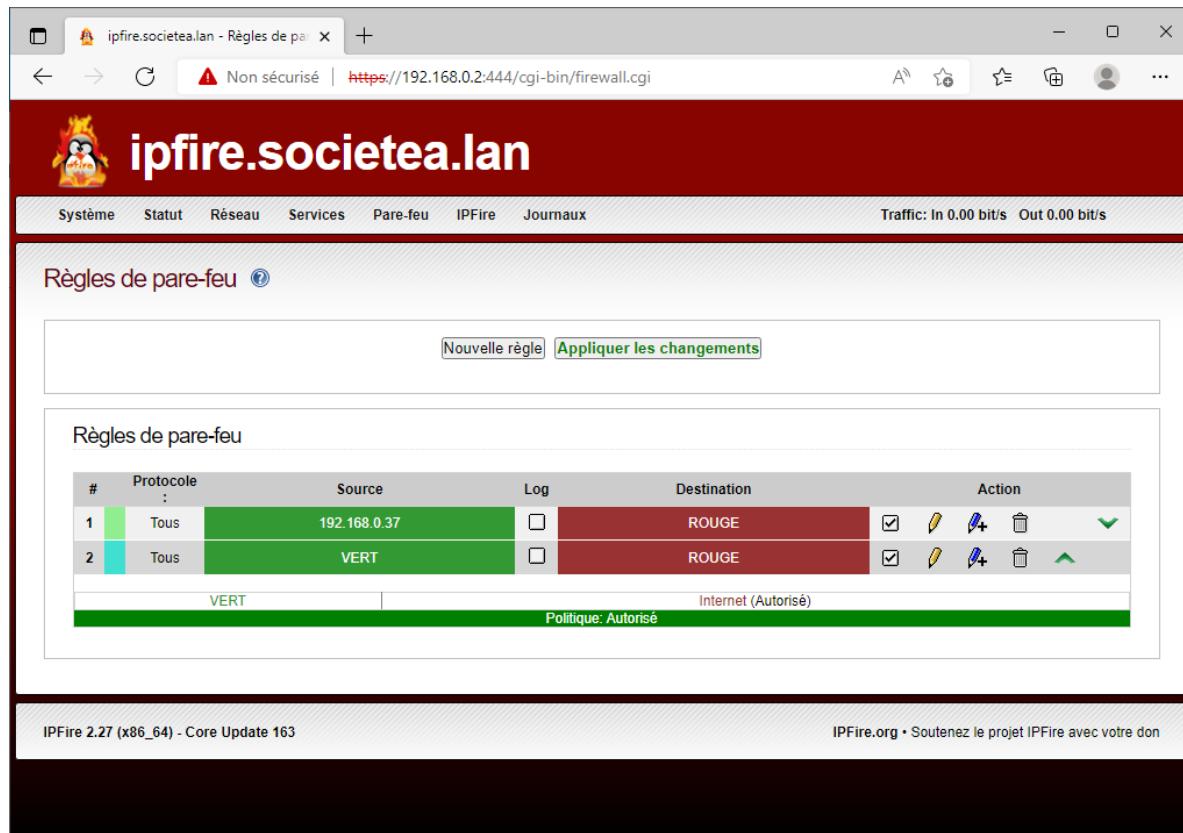
Politique: Autorisé

IPFire 2.27 (x86\_64) - Core Update 163

IPFire.org • Soutenez le projet IPFire avec votre don

La règle fine pour le client 192.168.0.37 qui vient d'être créée doit donc être placé 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.



ipfire.societea.lan - Règles de pare-feu

Non sécurisé | https://192.168.0.2:444/cgi-bin/firewall.cgi

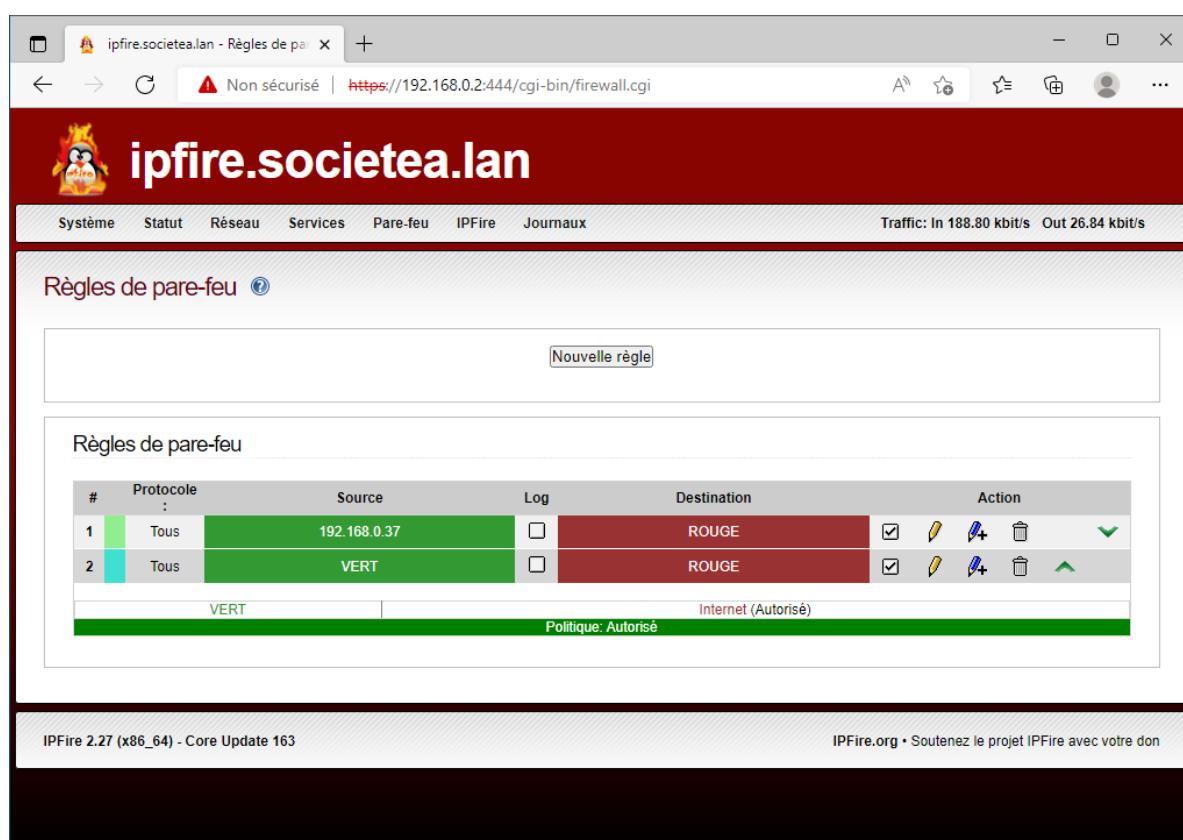
## Règles de pare-feu

#	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"/>

Politique: Autorisé

IPFire 2.27 (x86\_64) - Core Update 163

IPFire.org • Soutenez le projet IPFire avec votre don



ipfire.societea.lan - Règles de pare-feu

Non sécurisé | https://192.168.0.2:444/cgi-bin/firewall.cgi

## Règles de pare-feu

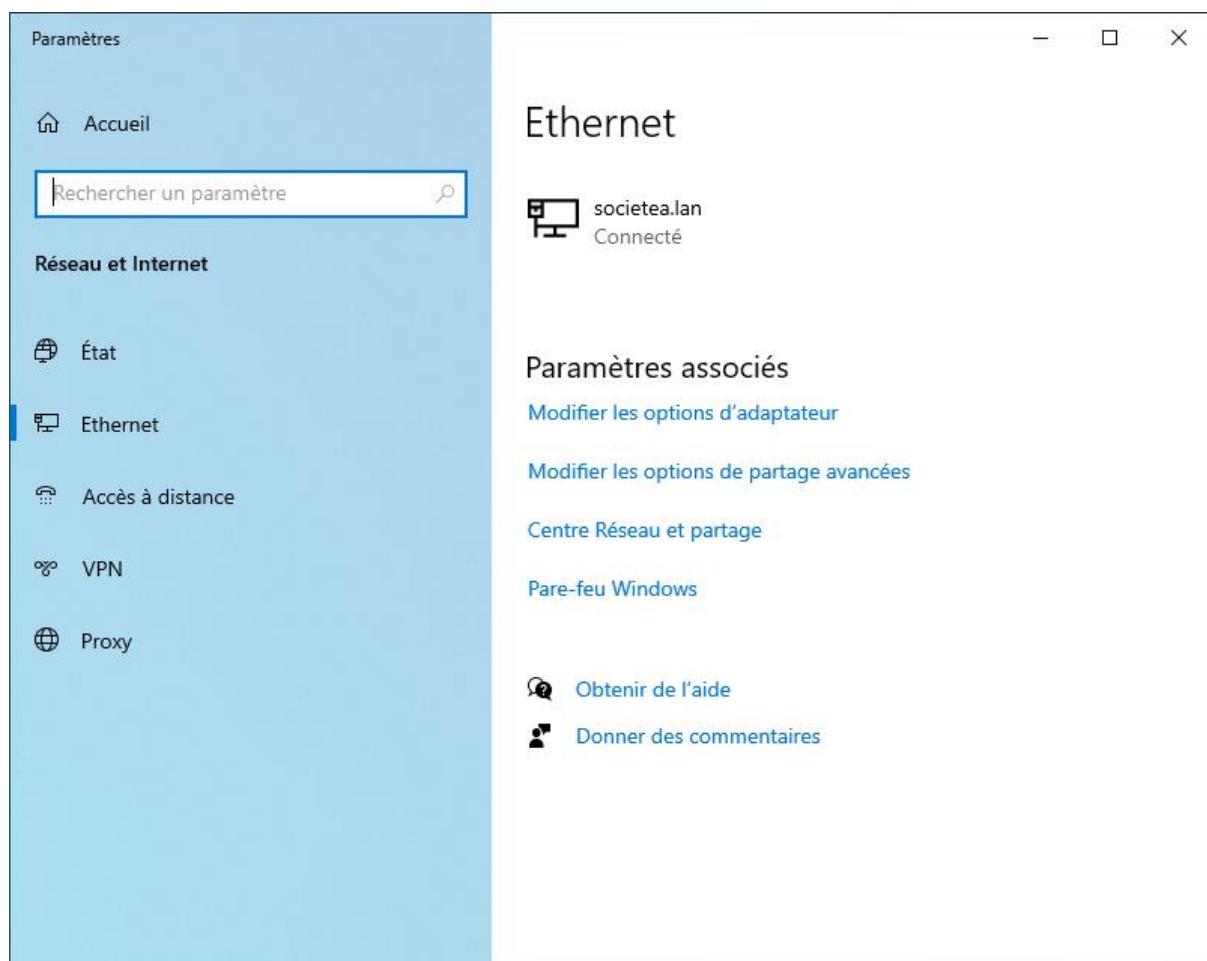
#	Protocole	Source	Log	Destination	Action
1	Tous	192.168.0.37	<input type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>
2	Tous	VERT	<input type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>

Politique: Autorisé

IPFire 2.27 (x86\_64) - Core Update 163

IPFire.org • Soutenez le projet IPFire avec votre don

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



```
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>
```