Mettre en place des règles via Ipfire.

Table des matières

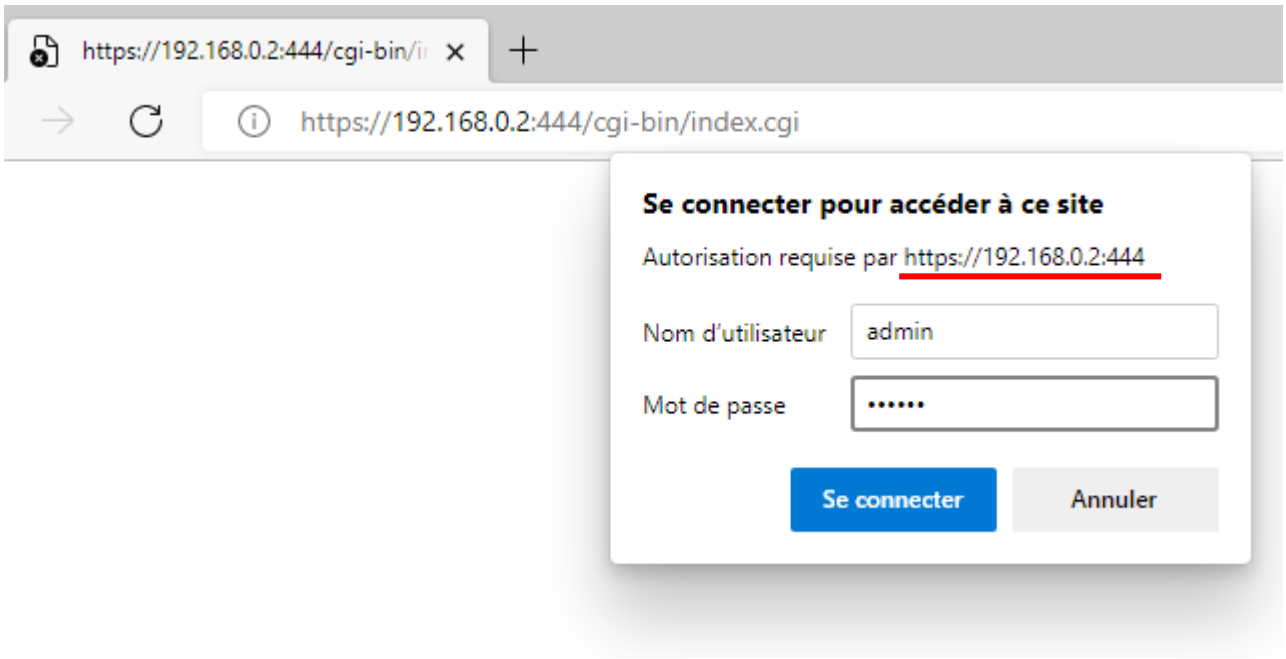
1. Les règles globales :

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.

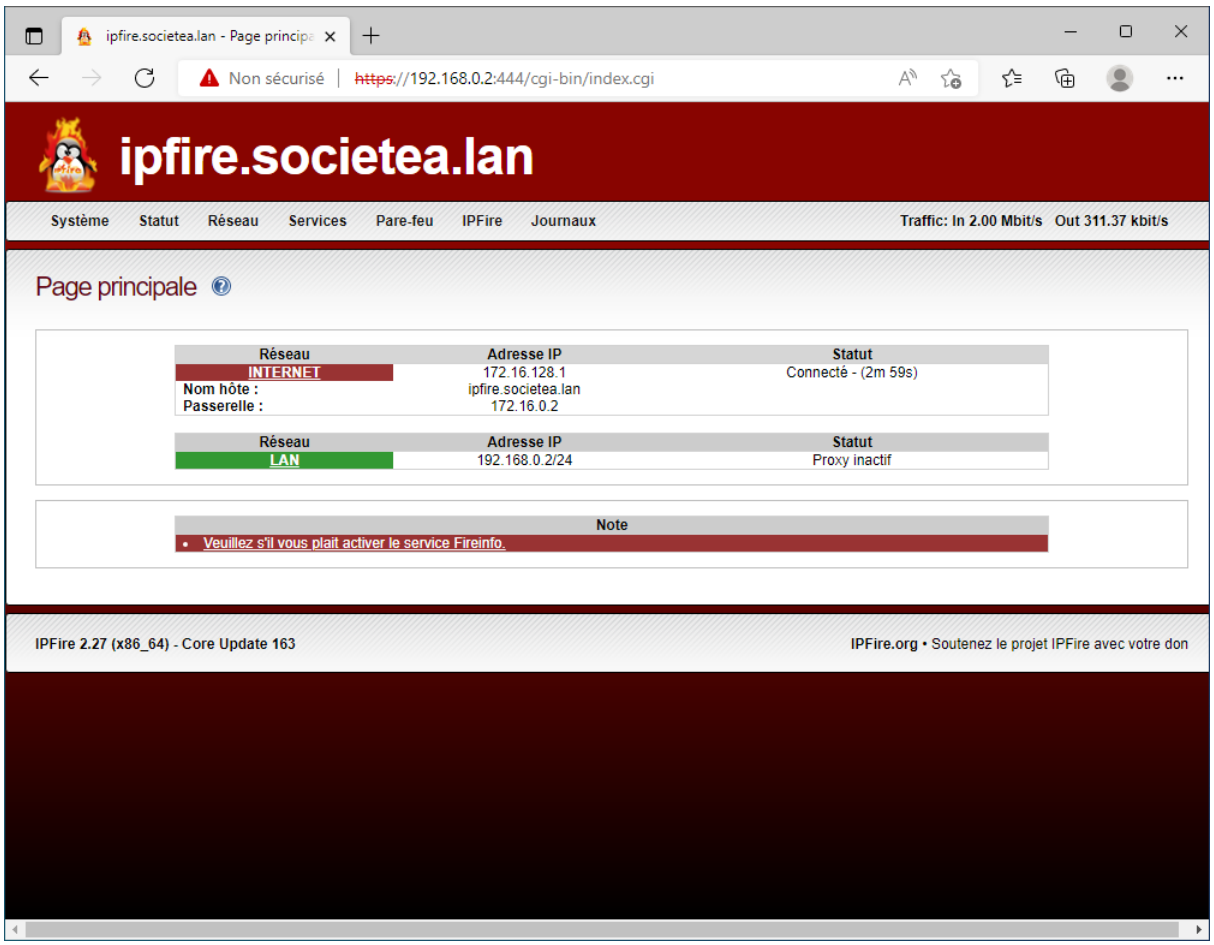
Vous pouvez définir les règles en ligne de commande par le biais du terminal ou accéder au configurateur graphique par le biais d'un navigateur internet.

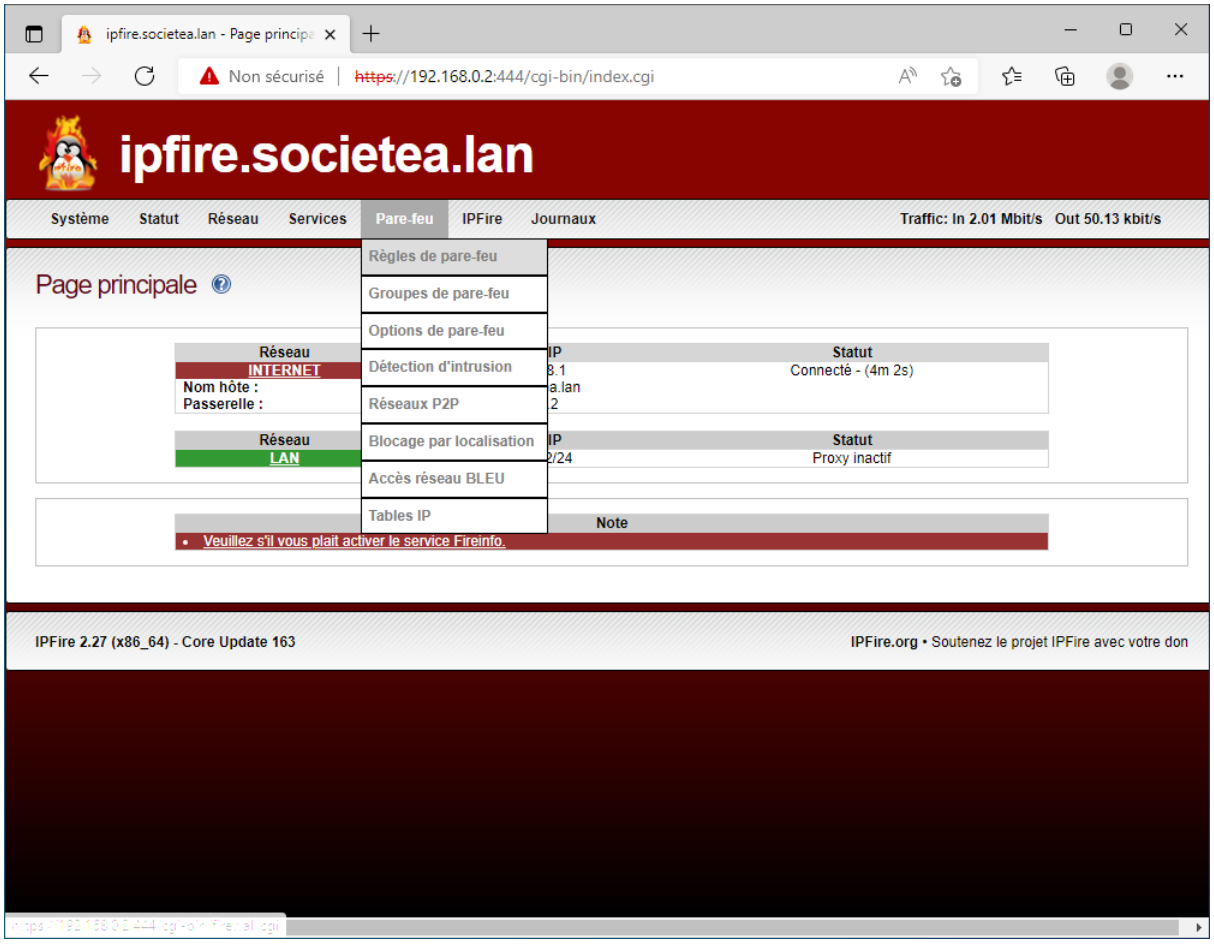
Vous devez spécifiez l'adresse IP du pare-feu et le port 444 (par défaut) avec le protocole HTTPS dans un navigateur internet (***exemple : https://192.168.0.2:444***).



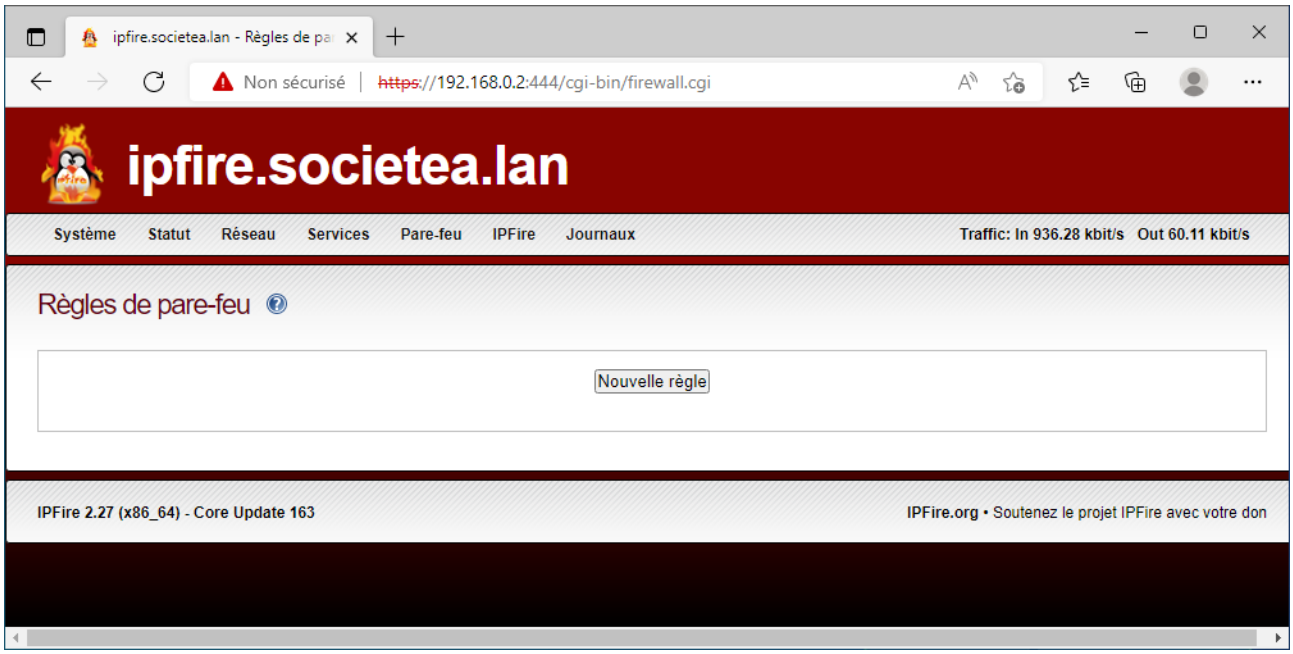
Utilisez le compte **admin** configuré par défaut pour administrer le pare-feu depuis le webconfigurator.

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

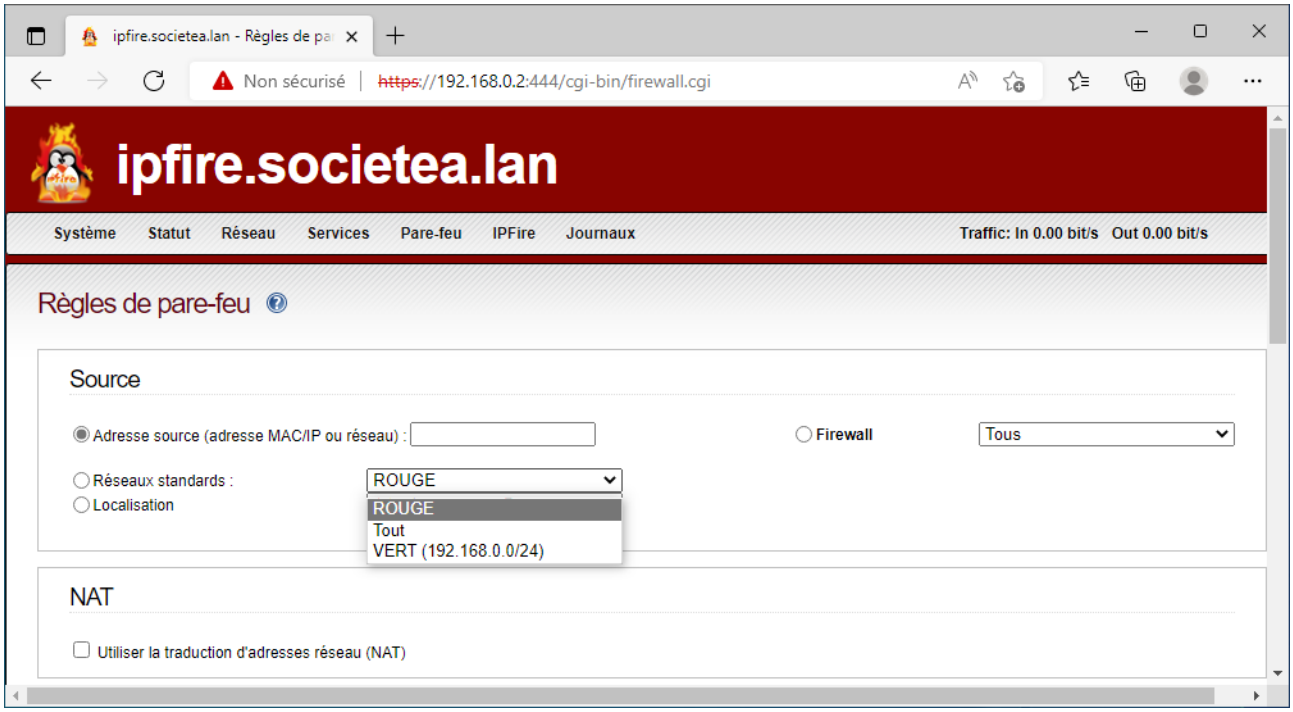

ipfire.societea.lan - Page principa
Non sécurisé | https://192.168.0.2:444/cgi-bin/index.cgi
ipfire.societea.lan
Système Statut Réseau Services Pare-feu IPFire Journaux
Traffic: In 2.00 Mbit/s Out 311.37 kbit/s
Page principale
Réseau Adresse IP Statut
INTERNET 172.16.128.1 Connecté - (2m 59s)
Nom hôte : 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 plait activer le service Fireinfo.
IPFire 2.27 (x86_64) - Core Update 163
IPFire.org • Soutenez le projet IPFire avec votre don

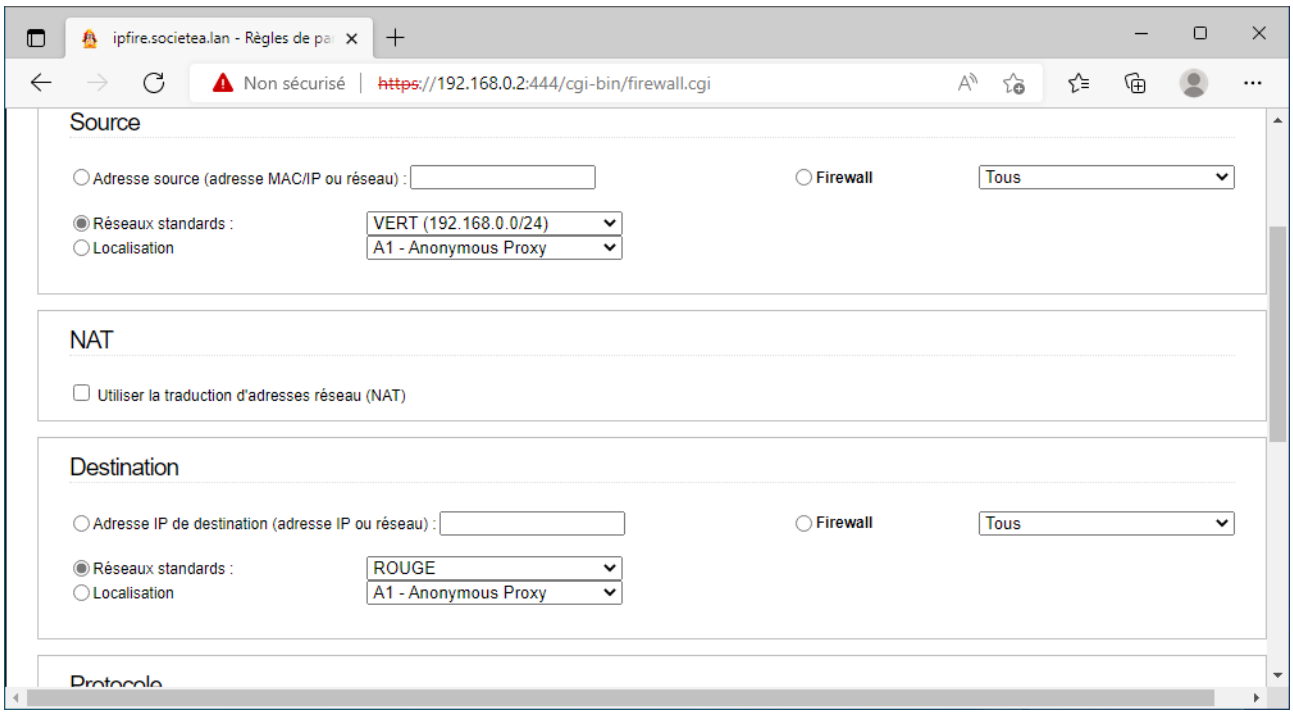

ipfire.societea.lan - Page principa
Non sécurisé | https://192.168.0.2:444/cgi-bin/index.cgi
ipfire.societea.lan
Système Statut Réseau Services Pare-feu IPFire Journaux
Traffic: In 2.01 Mbit/s Out 50.13 kbit/s
Règles de pare-feu
Groupes de pare-feu
Options de pare-feu
Détection d'intrusion
Réseaux P2P
Blocage par localisation
Accès réseau BLEU
Tables IP
Page principale
Réseau
INTERNET
Nom hôte :
Passerelle :
Réseau
LAN
Statut
Connecté - (4m 2s)
Proxy inactif
Note
Veuillez s'il vous plait 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.

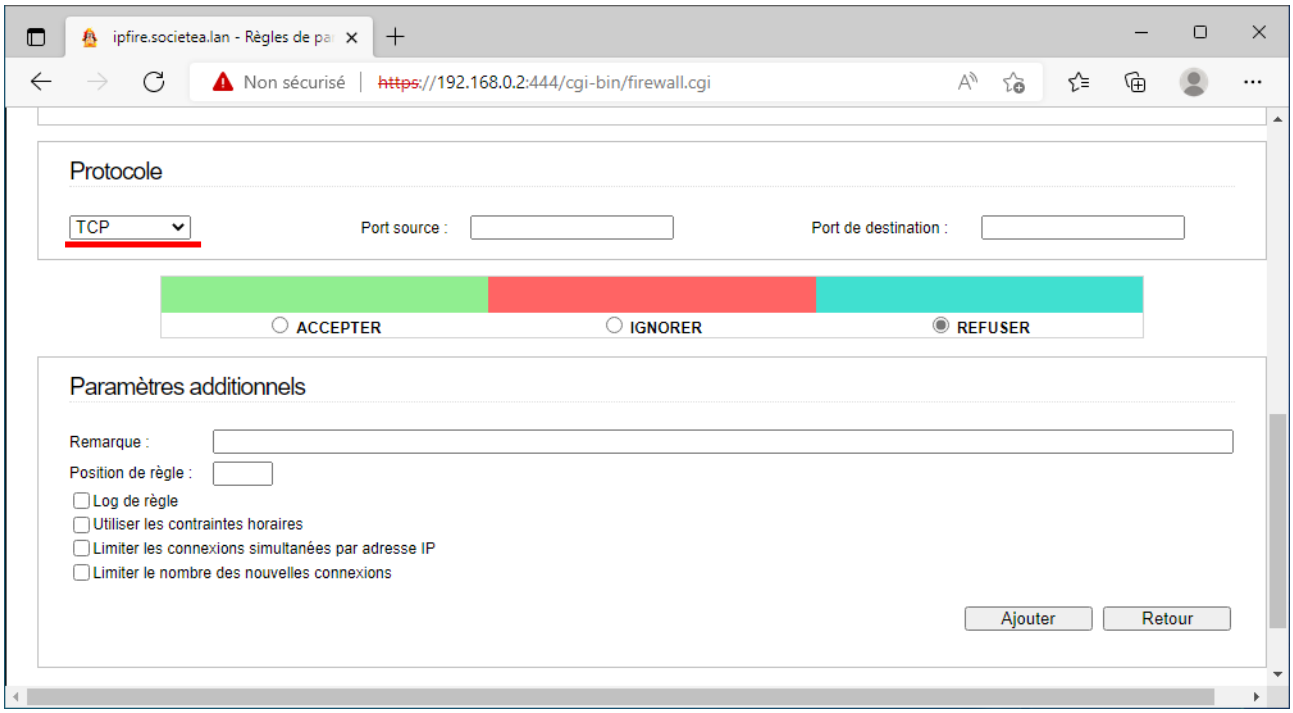


Créez une nouvelle règle pour l'interface GREEN (LAN) en tant que Source.



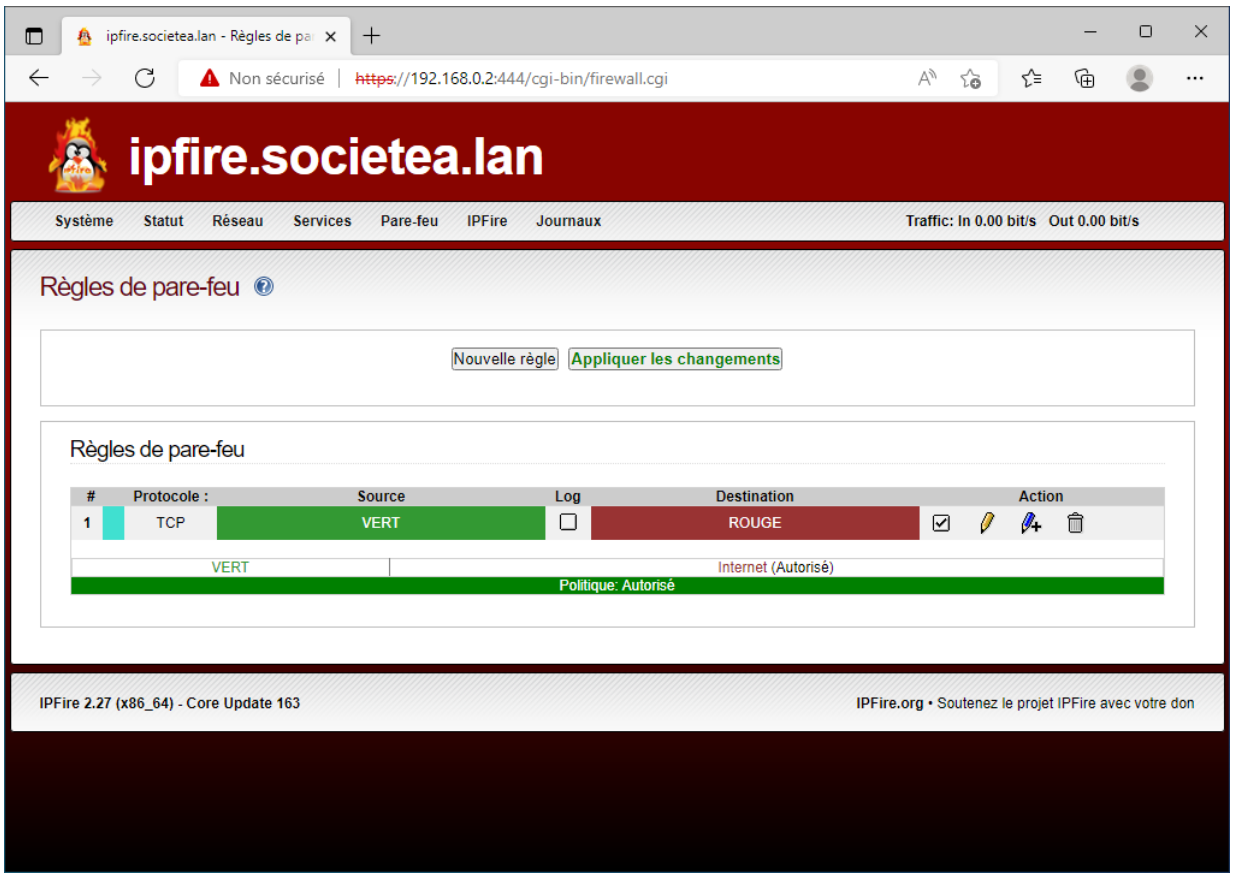


A destination du réseaux RED (le WAN) afin de l'interdire (REFUSER).

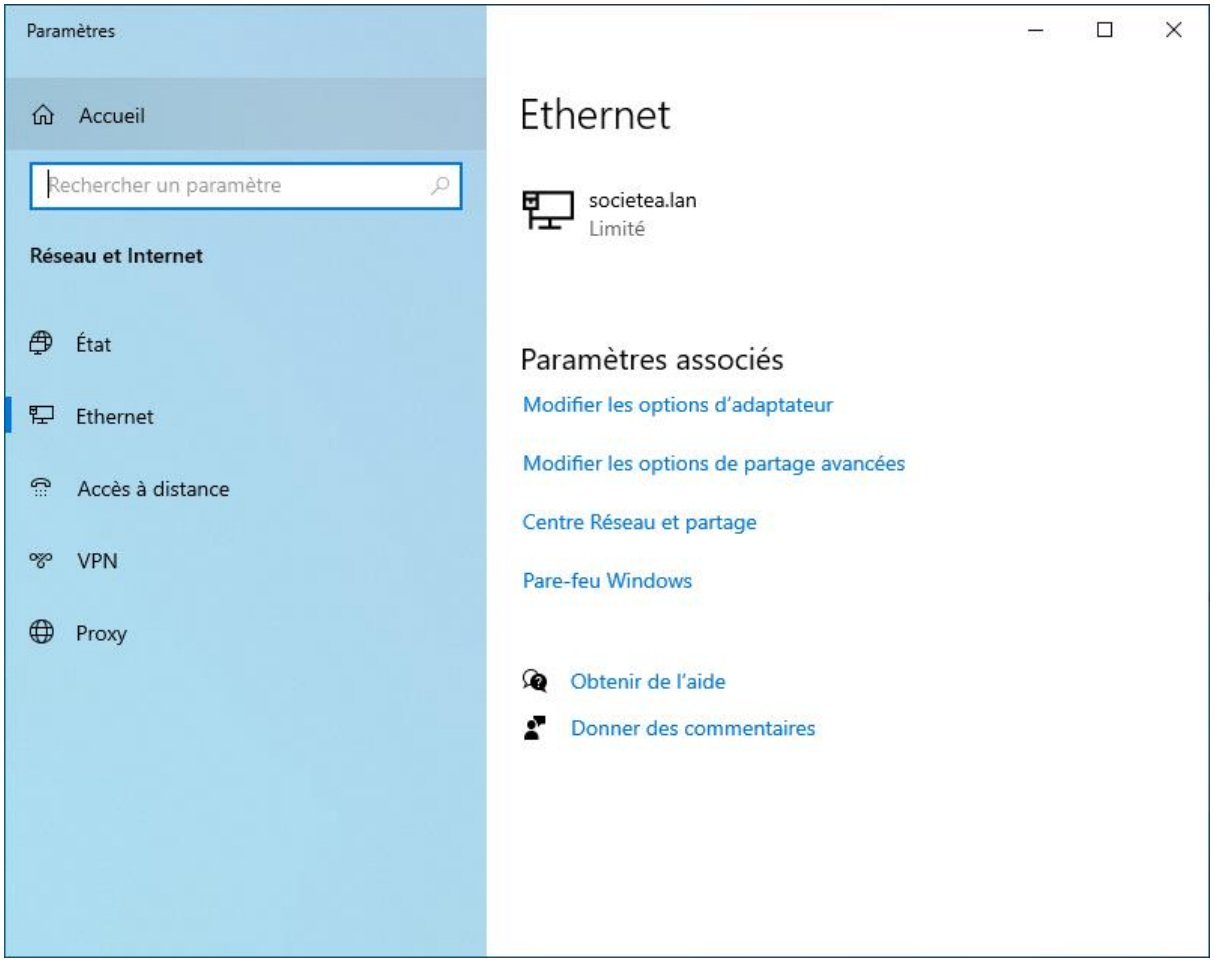


Vous pouvez spécifier le protocole à autoriser/interdire ainsi que les ports sources et de destinations.

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



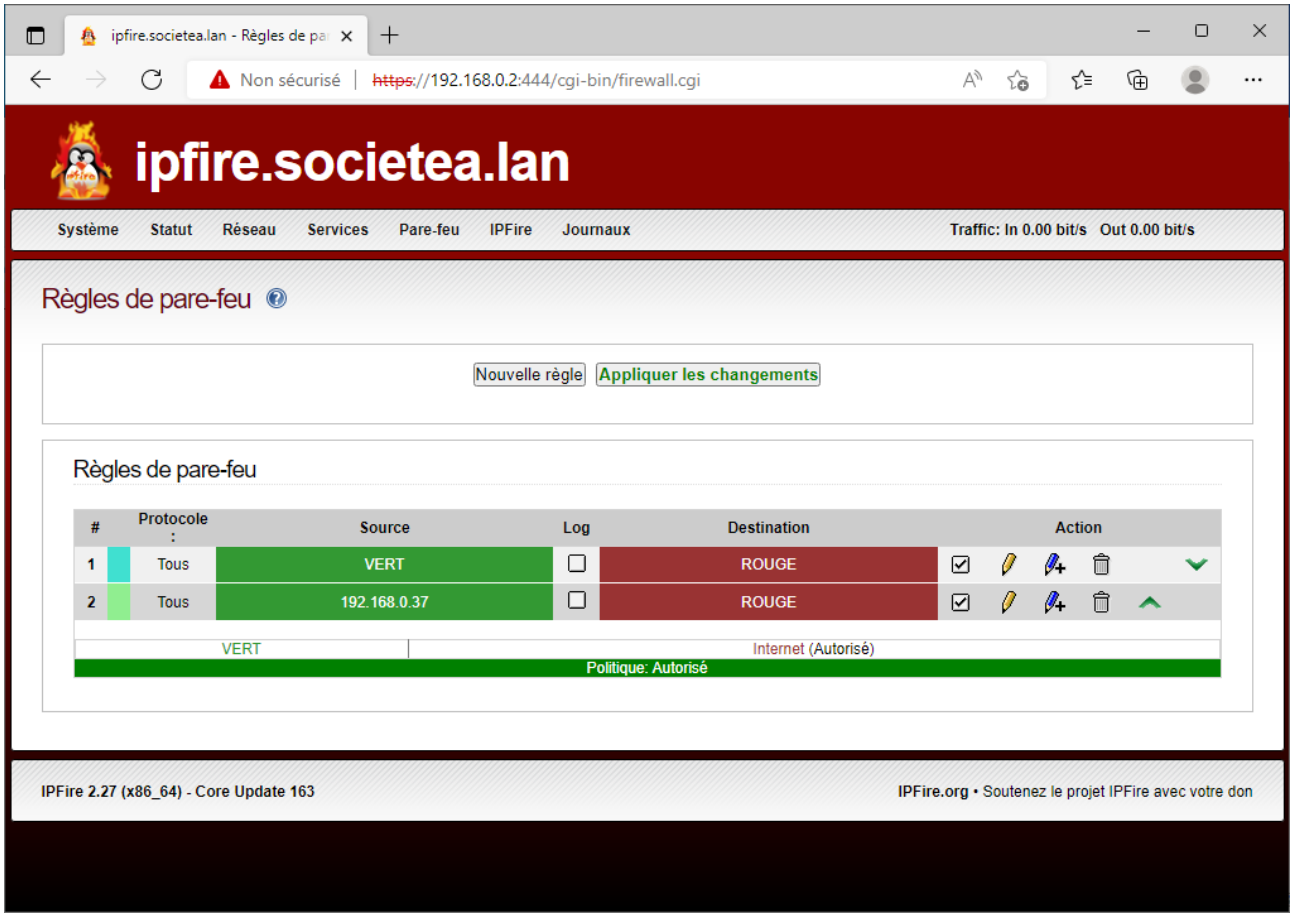
Appliquez les changements pour lire et exécuter cette nouvelle règle globale interdisant le trafic TCP à destination du réseau WAN.



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.

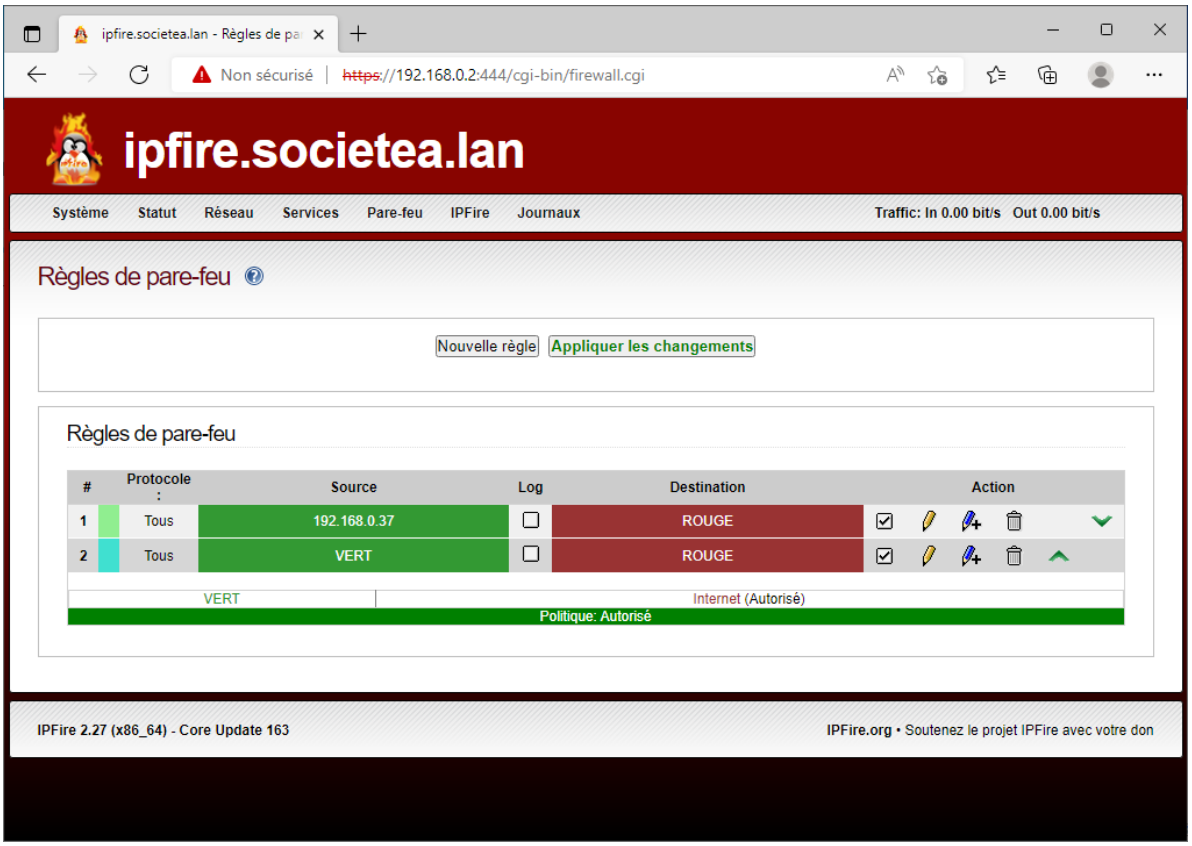
2. Les règles fines :

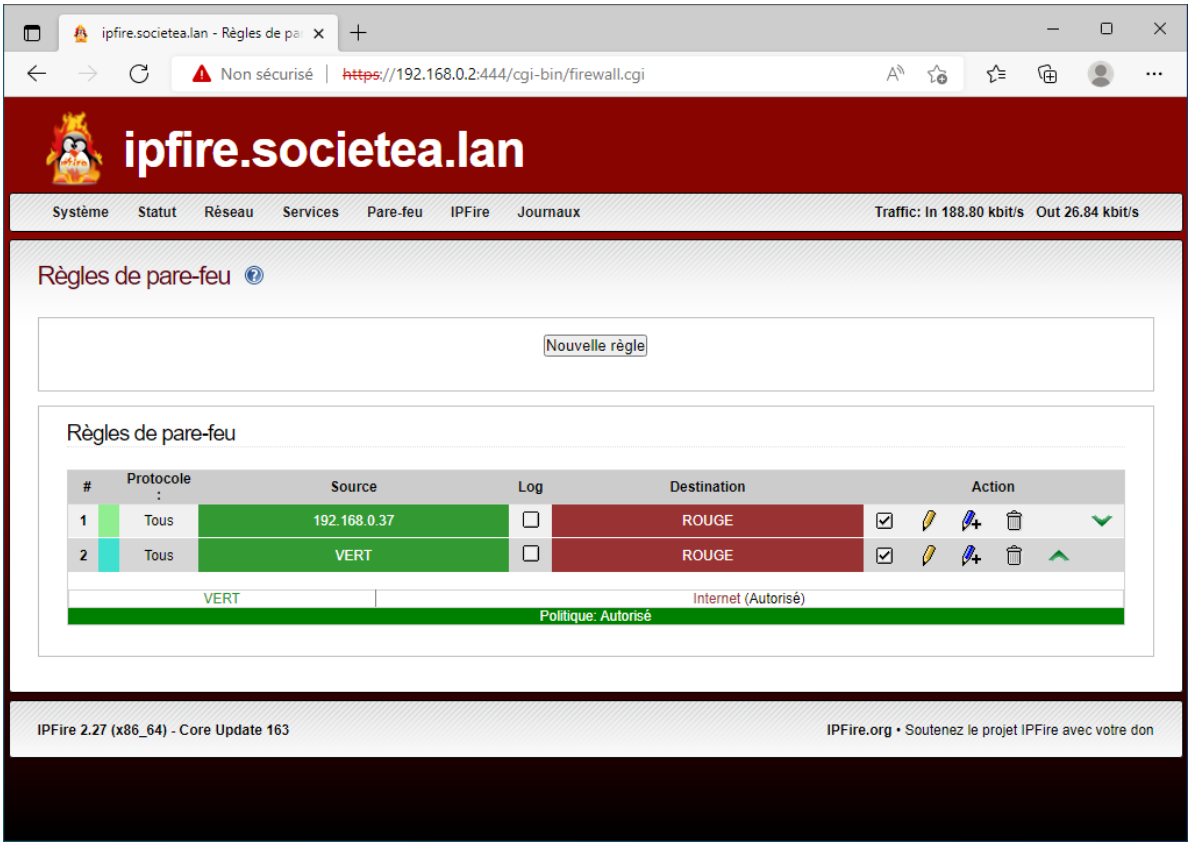
Comme pour n'importe quel pare-feu, les règles sont lues de manière séquentielle par le système, l'ordre de lecture des règles est important afin qu'elles soient lues et puissent s'appliquer sans contradiction entre elles.



La règle fine pour le client 192.168.0.37 qui vient d'être crée 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.





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