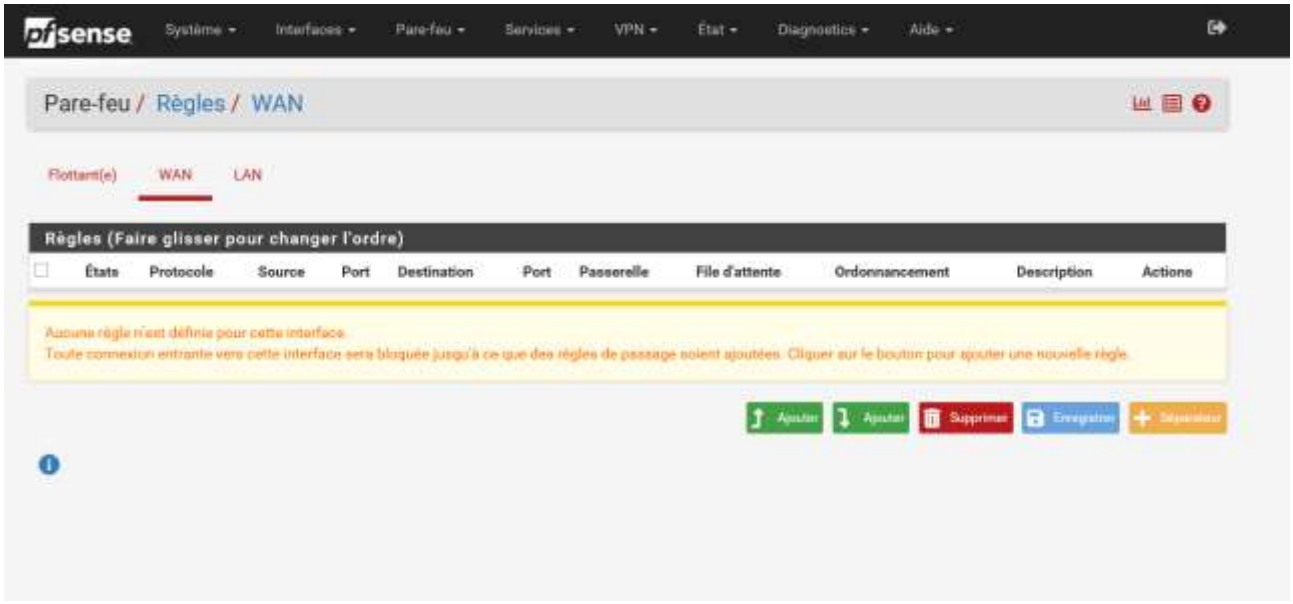
Mettre en place des règles via Pfsense.

Table des matières

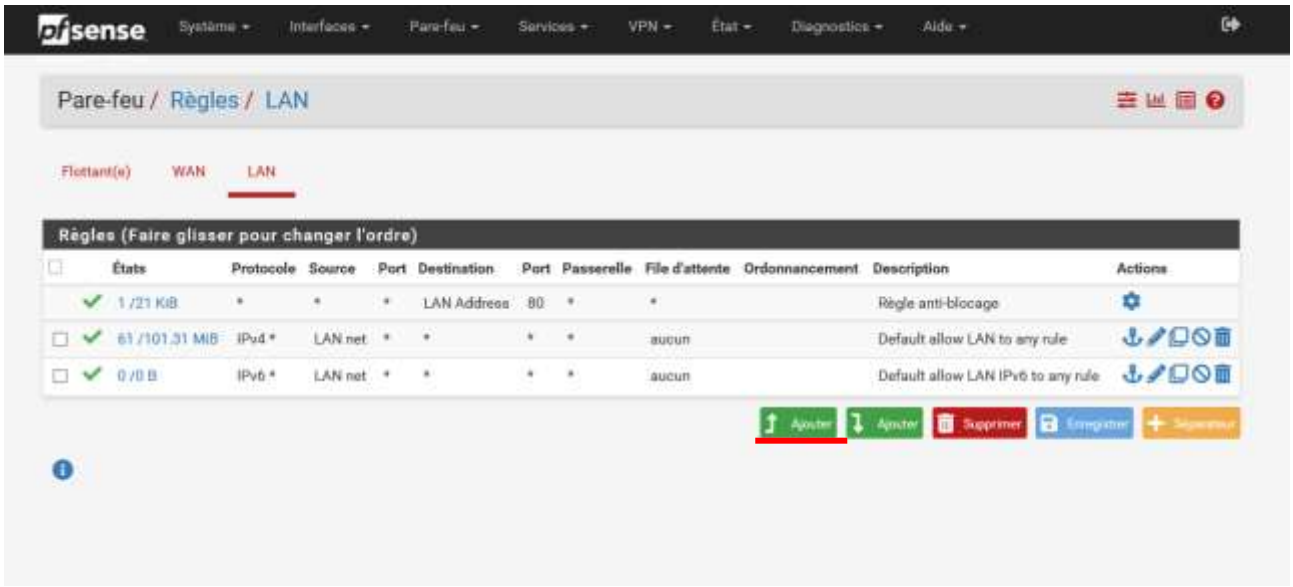
1. Les règles globales :

Vous pouvez définir les règles directement depuis le shell du système d'exploitation du pare-feu mais vous pouvez aussi le faire depuis l'interface graphique par le biais du webconfigurator que ce soit pour Pfsense ou bien Ipfire.

Nous allons mettre en place une règle générale simple qui permettra d'interdire le trafic sur les ports TCP et UDP en dehors du réseau local cela permettra d'interdire la navigation internet.



Le réseau WAN ne comporte aucune règle par défaut, nous allons configurer une nouvelle règle pour le réseau LAN qui lui comporte 3 règles par défaut.

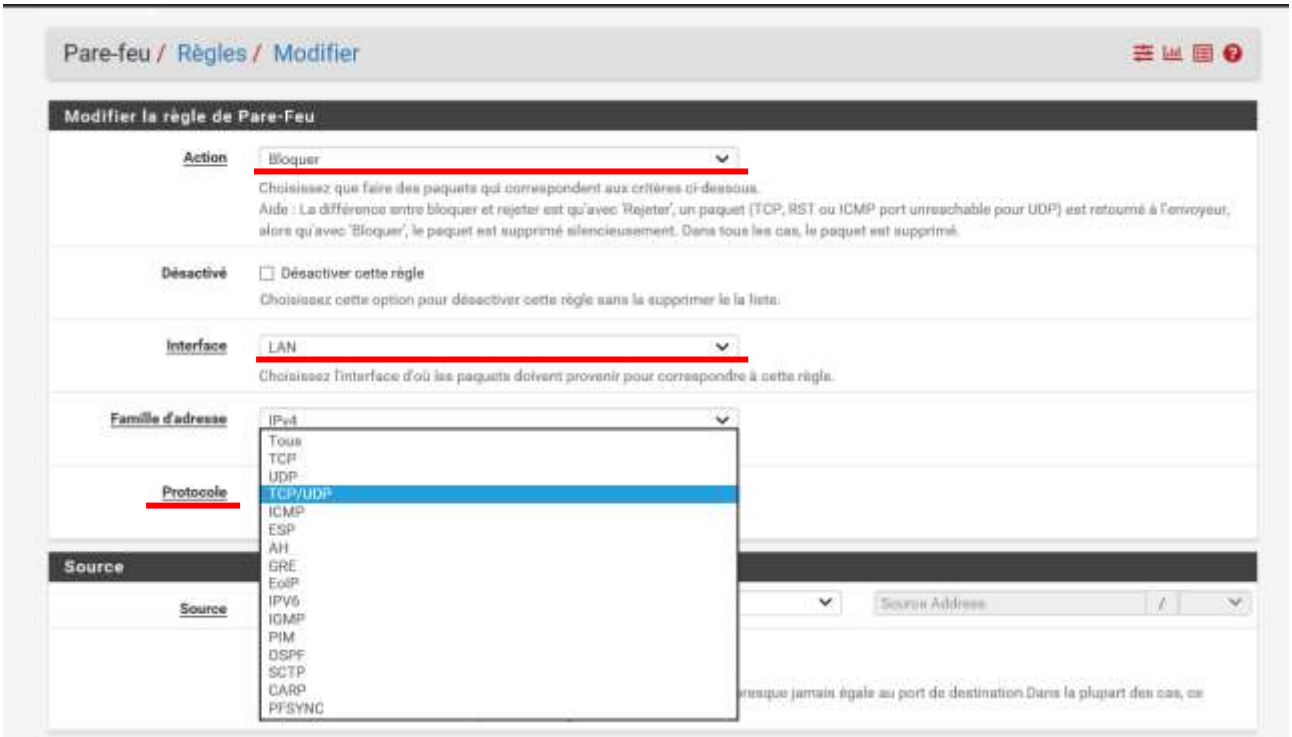


Sélectionnez le réseau pour lequel vous souhaitez mettre en place une règle en l'occurrence le **réseau local (LAN)** et faites ***Ajouter*** pour créer une nouvelle règle.

Vous devez maintenant spécifier la règle à l'aide de la sémantique habituelle des pare-feu à savoir sur Pfsense :

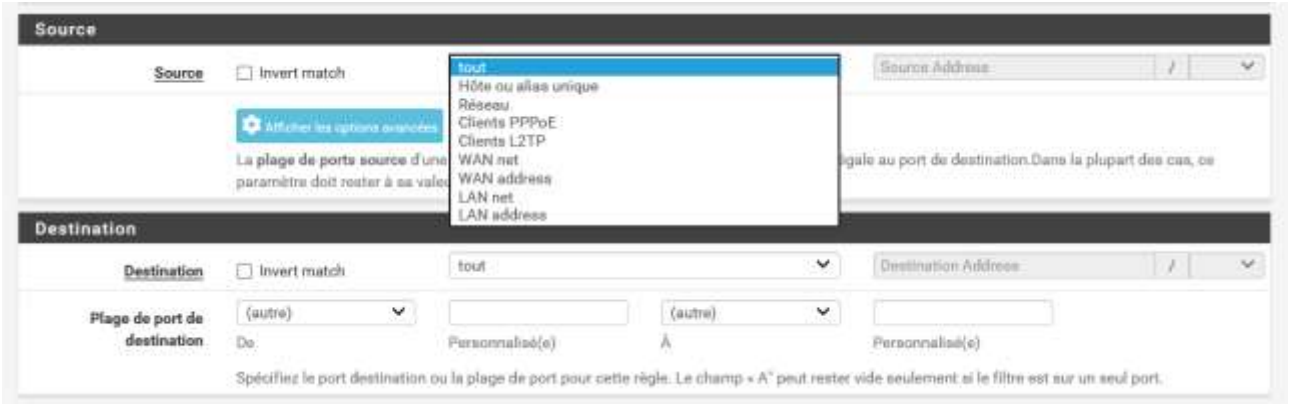
- Autoriser le trafic
- Bloquer le trafic
- Rejeter le trafic (idem que bloquer mais avec suppression discrète du paquet interdit)

Mettez en place une règle de blocage sur l'interface LAN pour les protocoles TCP et UDP par exemple.



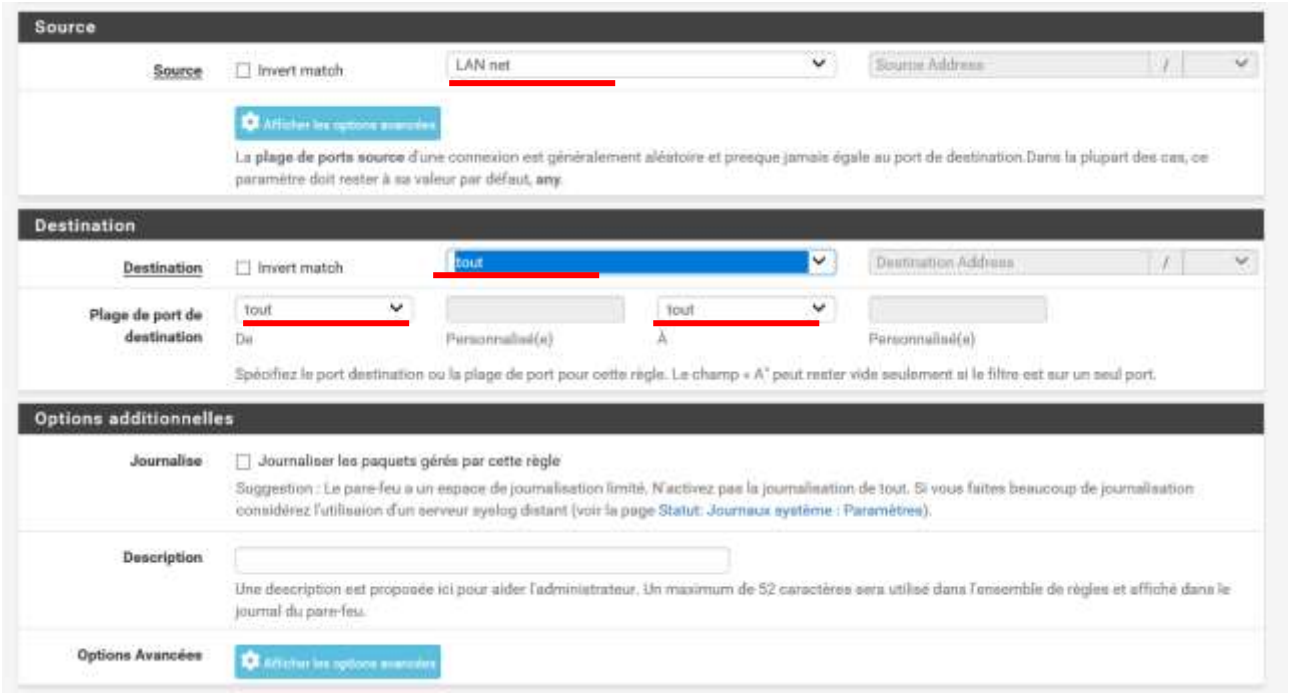
La règle suivante va permettre de bloquer toutes les connexions TCP et UDP entrantes et sortantes à partir du réseau local depuis n'importe quelles adresses IPv4 situées en dehors du réseau LAN.

Dans une deuxième partie le pare-feu vous demande de préciser les **sources** et **destinations** concernant les flux que vous souhaitez autoriser ou interdire.

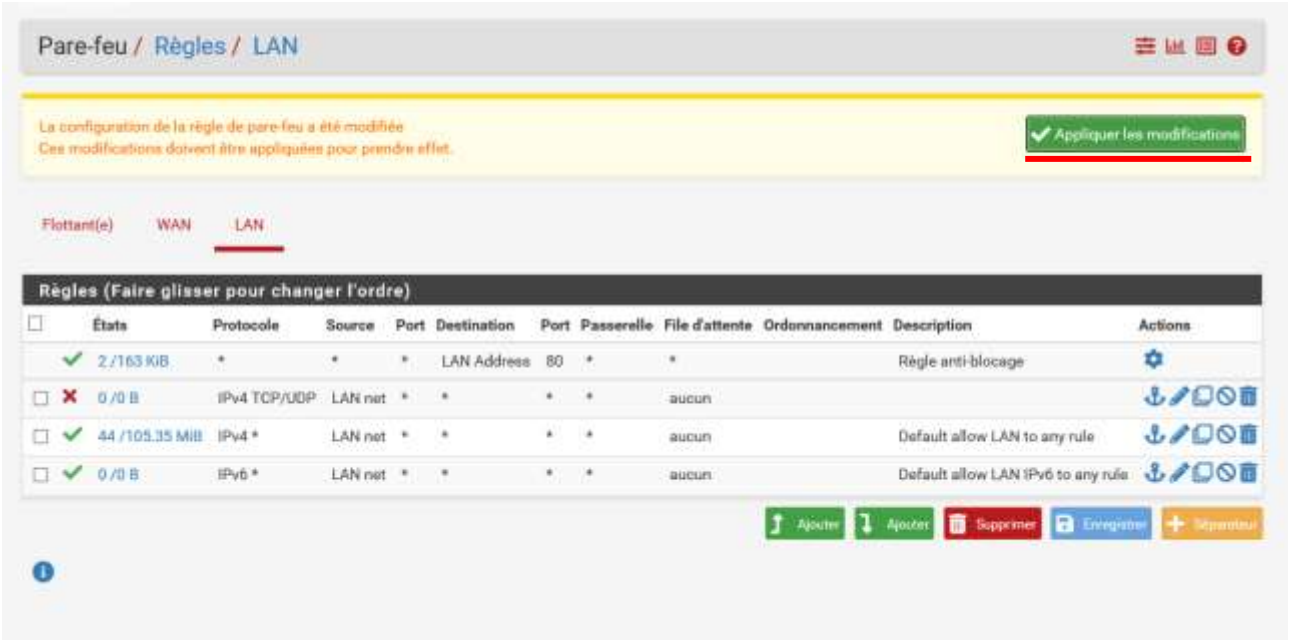


Vous pouvez spécifier des adresses réseaux ou bien aussi directement des plages de postes ou des postes en particulier, la syntaxe varie suivant le logiciel mais reste globalement similaire dans son ensemble.

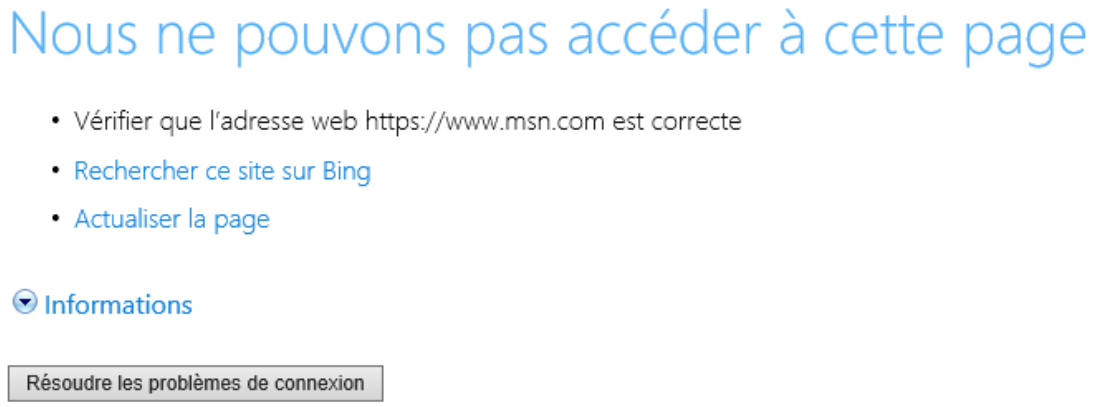
Dans l'exemple ci-dessous, l'ensemble du réseau LAN est bloqué au niveau du trafic entrant et sortant à destination de n'importe quel autre poste en dehors du réseau LAN pour les protocoles TCP et UDP.



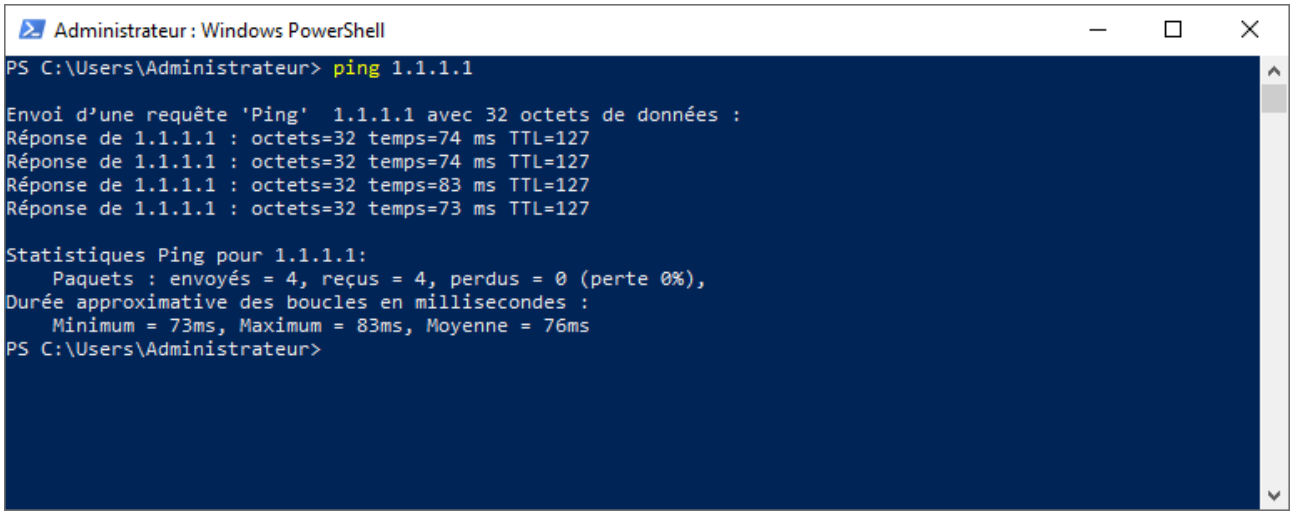
La nouvelle règle étant établie, appliquez les modifications afin que la règle soit prise en compte, parfois un certain temps est nécessaire avant la prise en compte du changement.



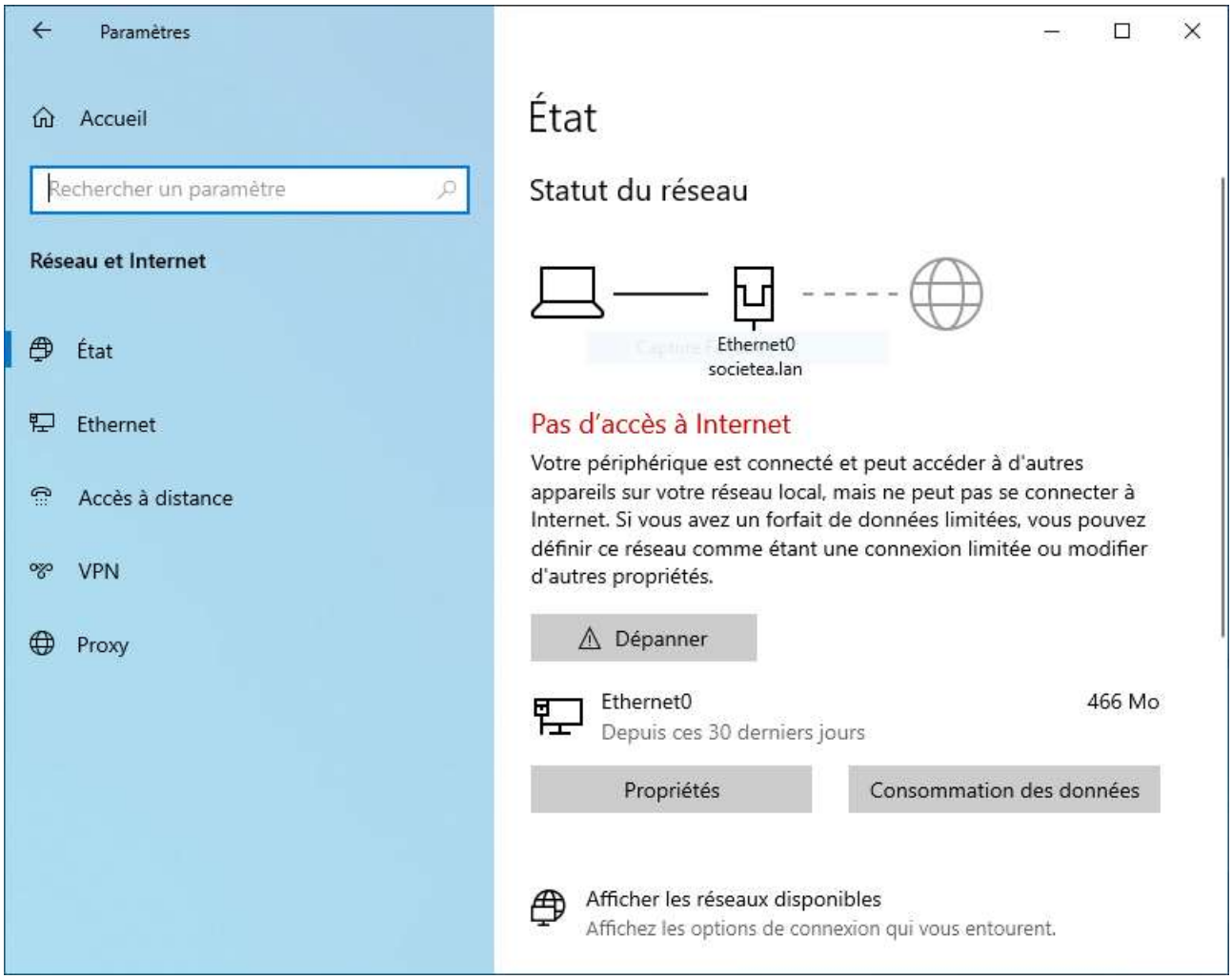
Si la règle s'exécute correctement, il devrait être impossible de lancer la navigation internet depuis le serveur ou n'importe quel autre poste du réseau LAN.



Le serveur en revanche est bien toujours connecté au réseau WAN, ce sont les protocoles TCP et UDP qui ont été bloqués.



Depuis un poste client, la connexion à Internet semble être coupée.



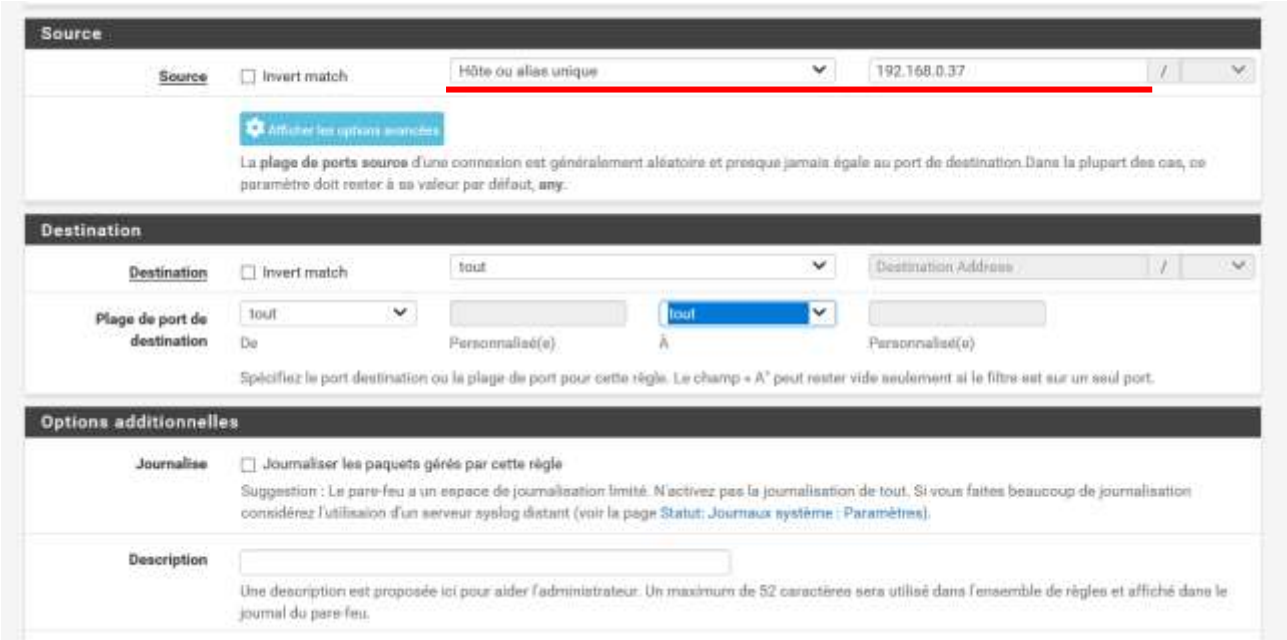
2. Les règles fines :

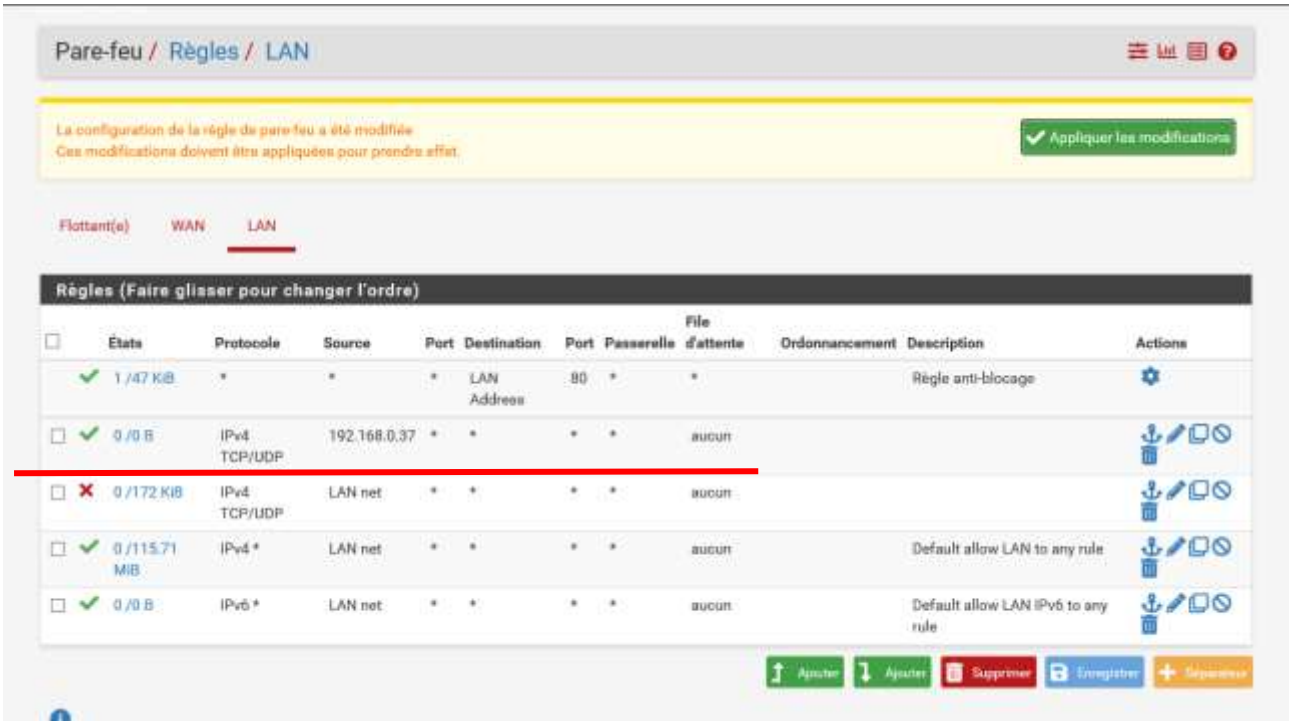
La règle de blocage de l'ensemble du flux depuis et vers le réseau local est une règle globale qui doit donc se placer vers la fin de la liste car sinon elle sera lue dès le début puis exécuter et les règles fines ne seront tout simplement pas lues et donc exécutées.

Une règle fine pourrait être par exemple d'autoriser un poste en particulier à avoir un trafic entrant et sortant en dehors du LAN, dans ce cas-là, la règle doit se placer devant les règles globales (il s'agit d'une exception aux règles globales).

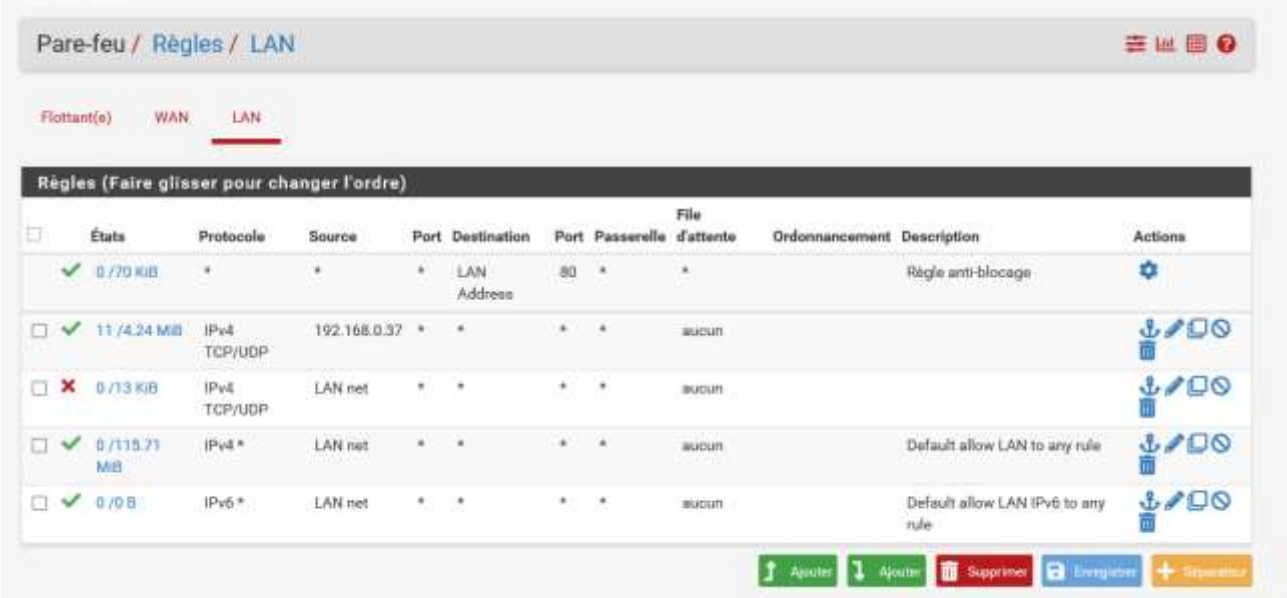
Créer une nouvelle règle autorisant un poste client à avoir un flux TCP et UDP entrant et sortant à destination de n'importe quel réseau.

Spécifiez le poste client à l'aide de son adresse IP par exemple.

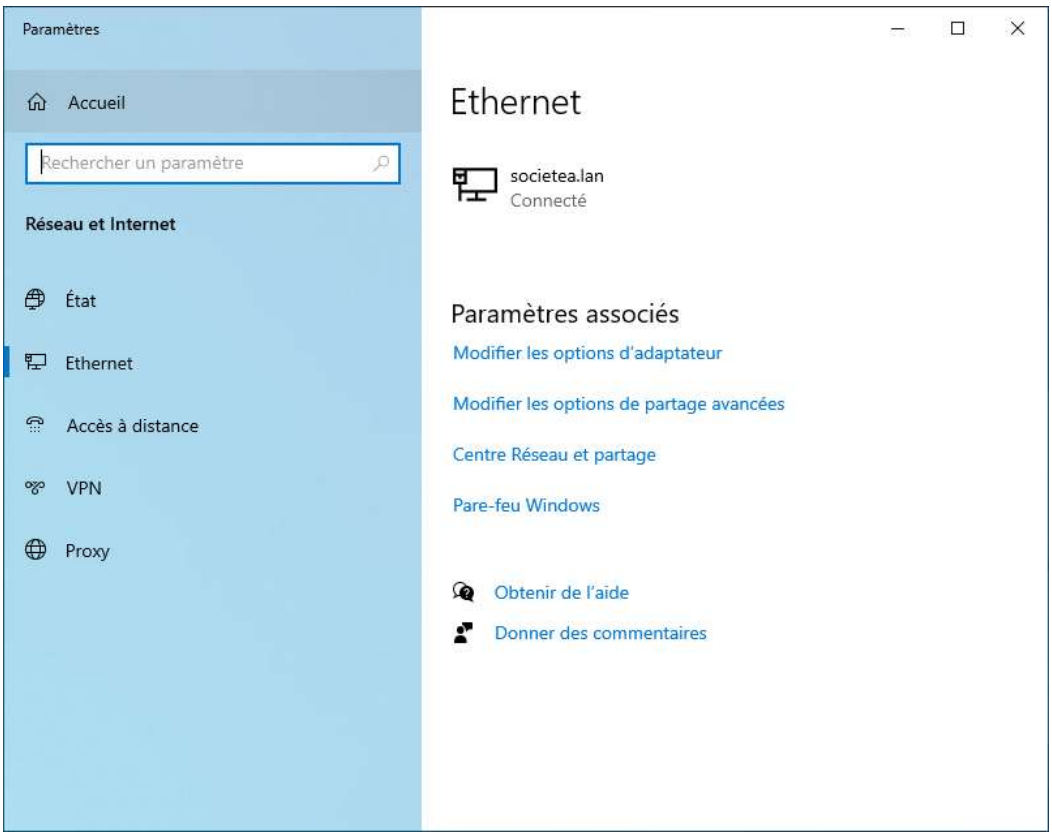


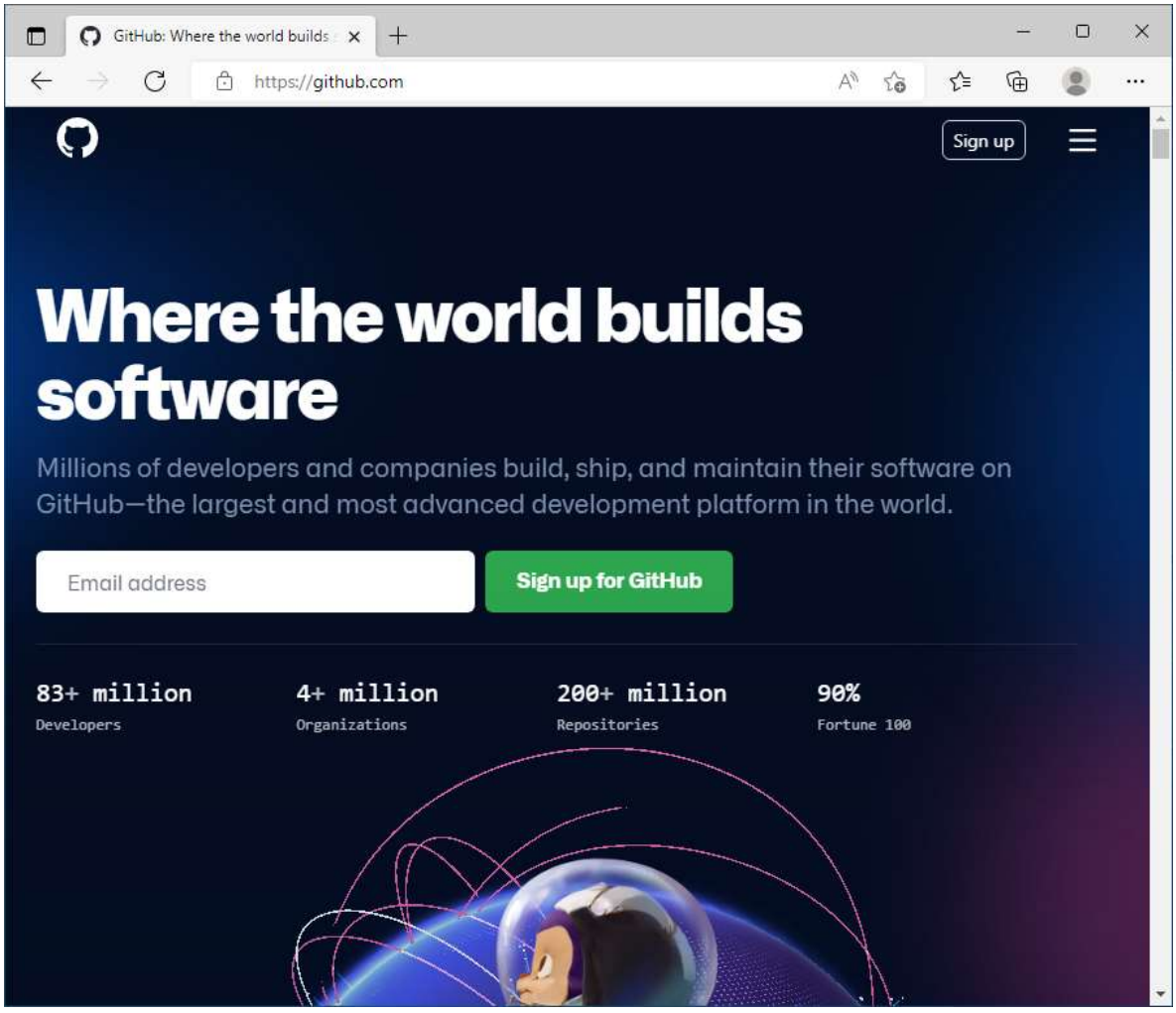


La nouvelle règle doit se trouver au-dessus de la règle globale afin d'être lue et appliquée par le pare-feu.



Après un court lap de temps, la règle devrait s'appliquée et le poste client devrait à nouveau récupérer la connexion à internet et pouvoir naviguer.


Paramètres
Accueil
Rechercher un paramètre
Réseau et Internet
État
Ethernet
Accès à distance
VPN
Proxy
Ethernet
societea.lan
Connecté
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


GitHub: Where the world builds
https://github.com
Sign up
Where the world builds software
Millions of developers and companies build, ship, and maintain their software on GitHub—the largest and most advanced development platform in the world.
Email address
Sign up for GitHub
83+ million
Developers
4+ million
Organizations
200+ million
Repositories
90%
Fortune 100

Si les clients pour lesquels vous allez mettre en place des règles spécifiques sont adressés dynamiquement, n'oubliez pas de mettre en place des réservations d'adresses IP sur le serveur DHCP sauf si les règles s'appliquent directement sur les adresses MAC des postes en question.