[pfSense] Règles de pare-feu

Introduction

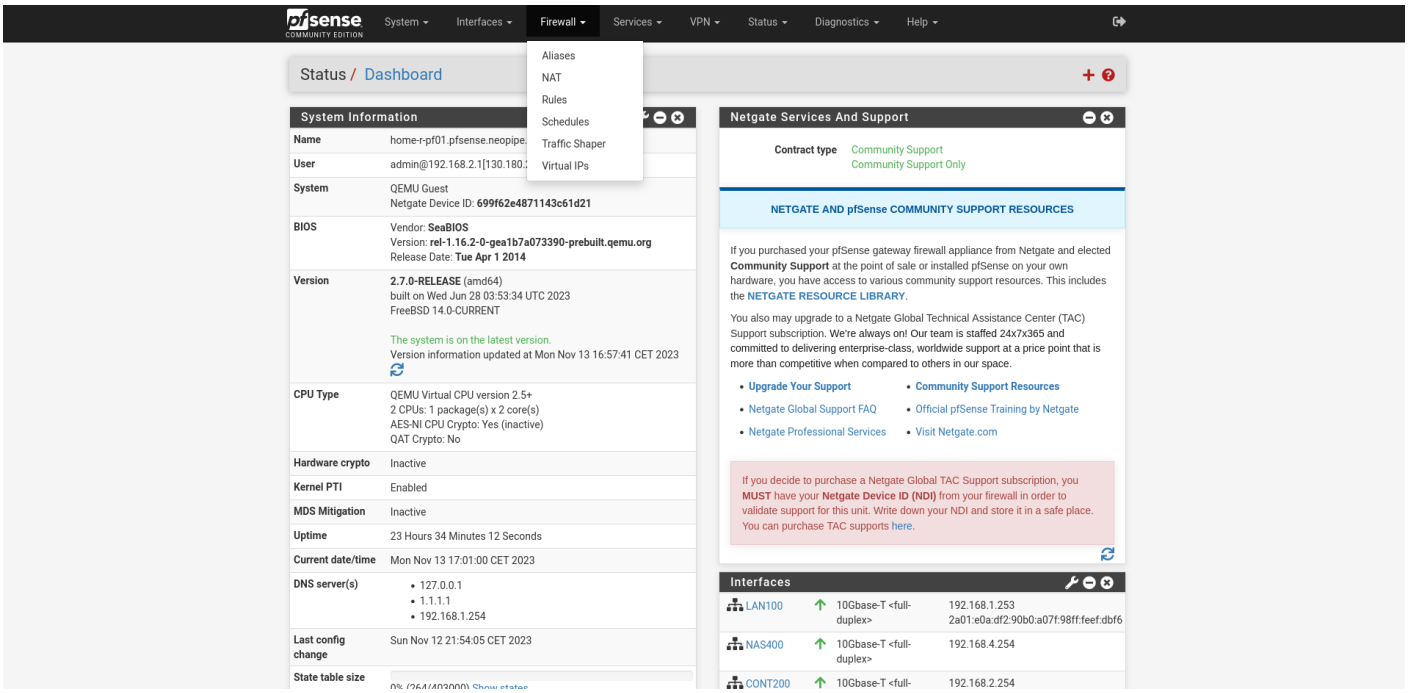
Vous pouvez configurer aisément vos propres règles de pare-feu sur pfSense depuis l'interface web.

Cependant, vous devez comprendre quelques notions primordiales pour pouvoir le faire.

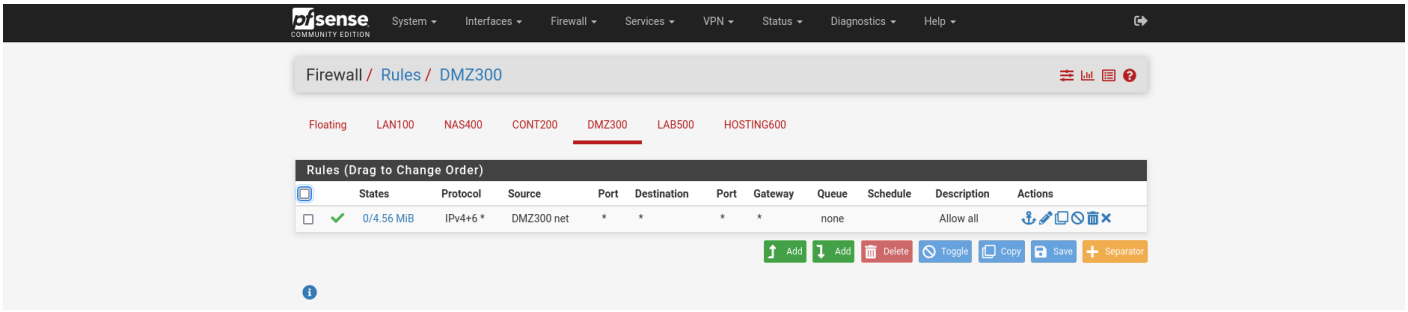
Manuel

Accéder à la table des règles

Tout d'abord, depuis l'interface web, rendez vous dans **Firewall > Rules** :



Ensuite, sélectionnez l'interface sur laquelle vous souhaitez appliquer la règle (ici DMZ300) :



Fonctionnement de la table

Pour chaque interface, vous pouvez voir apparaître les règles qui seront appliquées pour **chaque paquet** qui passe sur l'interface **dans l'ordre du haut vers le bas**.

Le paquet va donc être testé par chacune des règles :

- Dans le cas où la règle match avec le paquet, l'action définie lui sera appliquée (**PASS**, **BLOCK** ou **REJECTED**).
- Dans le cas où la règle ne match pas avec le paquet, le paquet va être testé par la règle en dessous et ainsi de suite.

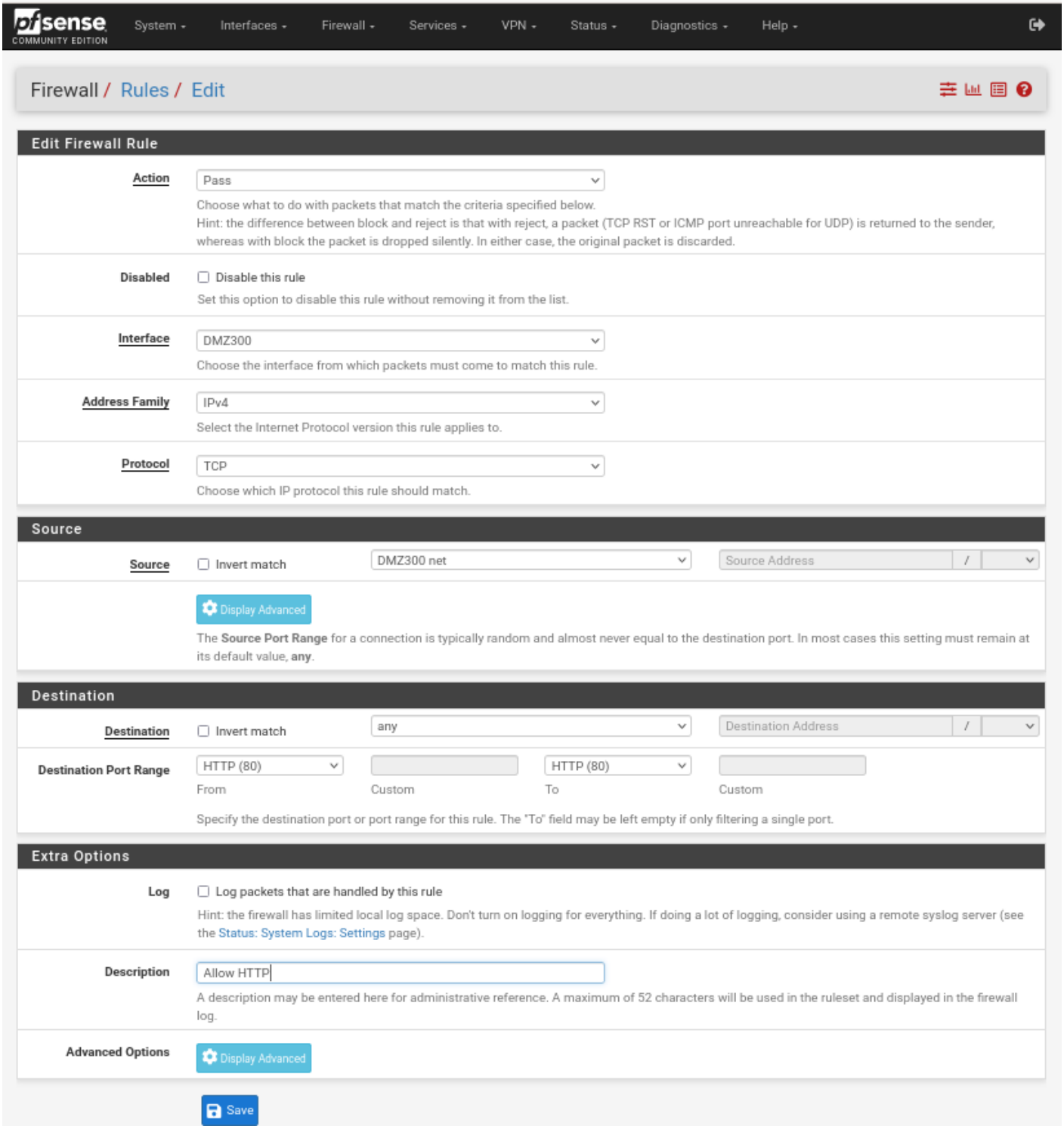
> Vous remarquerez que l'ordre des règles est capital.

Autoriser un flux

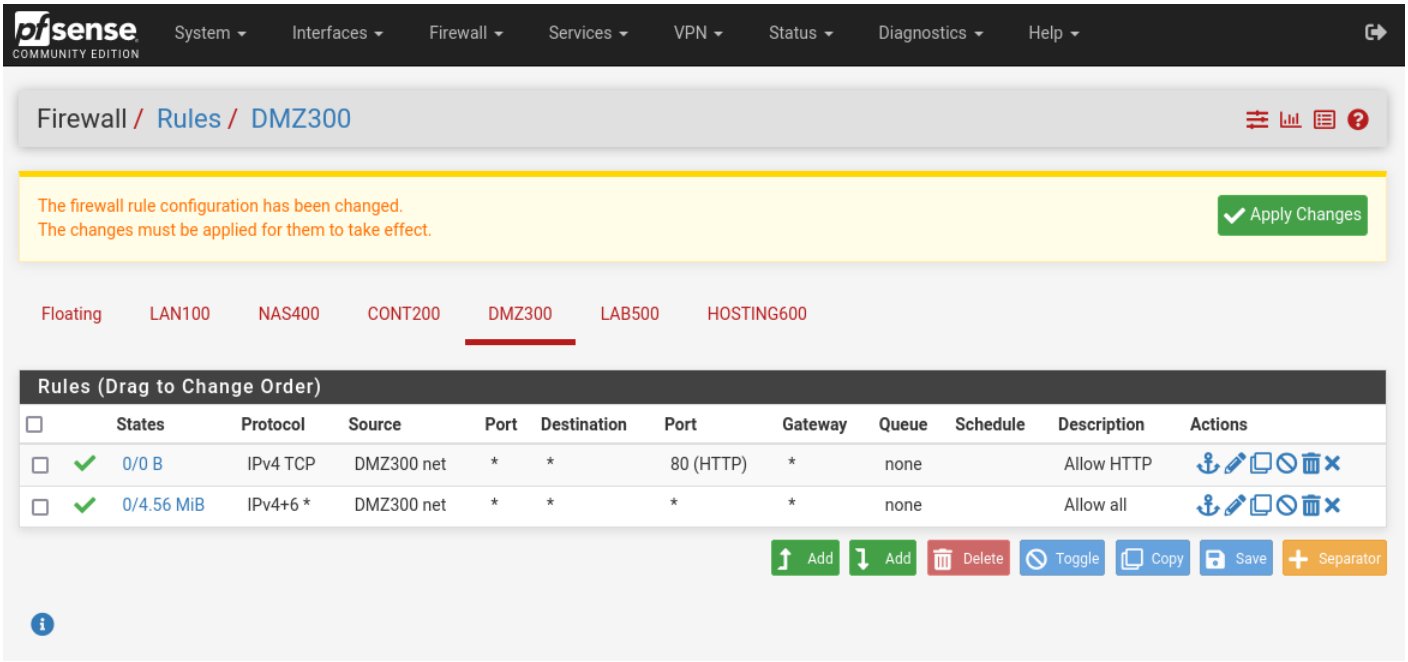
Pour l'exemple, nous allons créer une règle pour autoriser les connexions sortantes HTTP sur l'interface de la DMZ300.

Commencez par cliquer sur Add et définissez les options suivantes :

- Action : **PASS**
- Protocol : **TCP**
- Source : **DMZ300 Net**
- Destination : **any**
- Destination **Port Range : From HTTP (80) to HTTP (80)**
- Description : **Allow HTTP**



Vous pouvez appuyer sur **Save** puis **Apply Changes** pour appliquer les changements :



Bloquer un flux

Maintenant si vous souhaitez bloquer un flux, vous pouvez procéder à la même opération en modifiant simplement l'action PASS par **BLOCK**.

Revision #1
Created 13 November 2023 15:55:17 by Elieroc
Updated 13 November 2023 16:18:40 by Elieroc