

# [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.

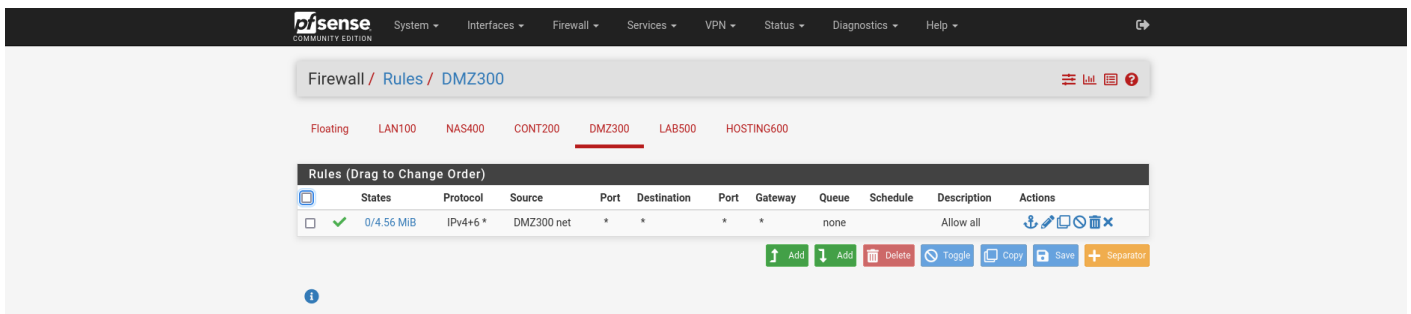
## Manuel

### Accéder à la table des règles

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

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The 'Firewall' menu is expanded, showing a dropdown with 'Aliases', 'NAT', 'Rules', 'Schedules', 'Traffic Shaper', and 'Virtual IPs'. The 'Rules' option is highlighted. The main content area is divided into two panels. The left panel, titled 'System Information', displays details about the system, including the name 'home-r-pf01.pfsense.neopipe', user 'admin@192.168.2.1[130.180.2.1]', system 'QEMU Guest', BIOS 'SeaBIOS', version '2.7.0-RELEASE (amd64)', CPU type 'QEMU Virtual CPU version 2.5+', and uptime '23 Hours 34 Minutes 12 Seconds'. The right panel, titled 'Netgate Services And Support', shows the contract type 'Community Support' and provides links to support resources. Below this, the 'Interfaces' section lists three interfaces: LAN100 (10Gbase-T <full-duplex>), NAS400 (10Gbase-T <full-duplex>), and CONT200 (10Gbase-T <full-duplex>).

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**

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Protocol** TCP 

Choose which IP protocol this rule should match.

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

 Save

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

✓ Apply Changes

DMZ300

 Add
  Add
  Delete
  Toggle
  Copy
  Save
  Separator



Updated 13 November 2023 16:18:40 by Elieroc