

[pfSense] Règles de pare-feu

Introduction

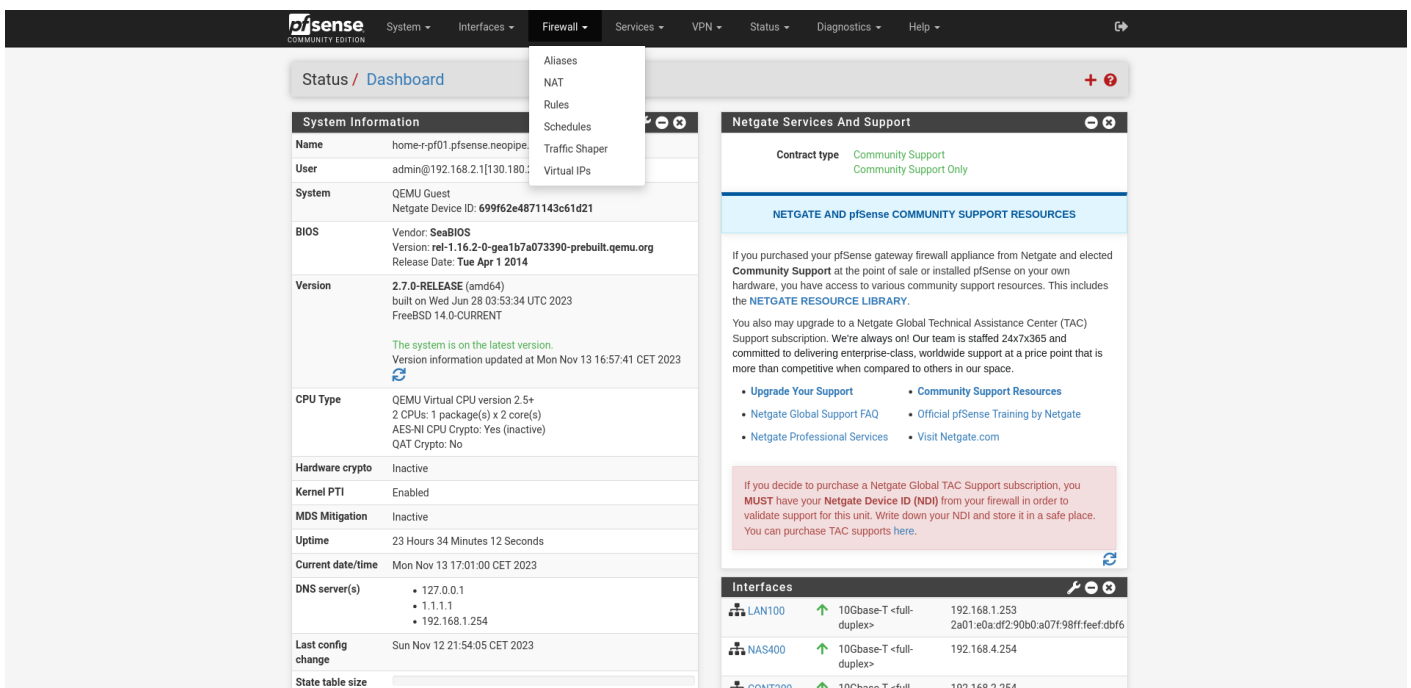
Vous pouvez configurer aisément vos propres règles de pare-feu sur pfSense depuis l'interface web.

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

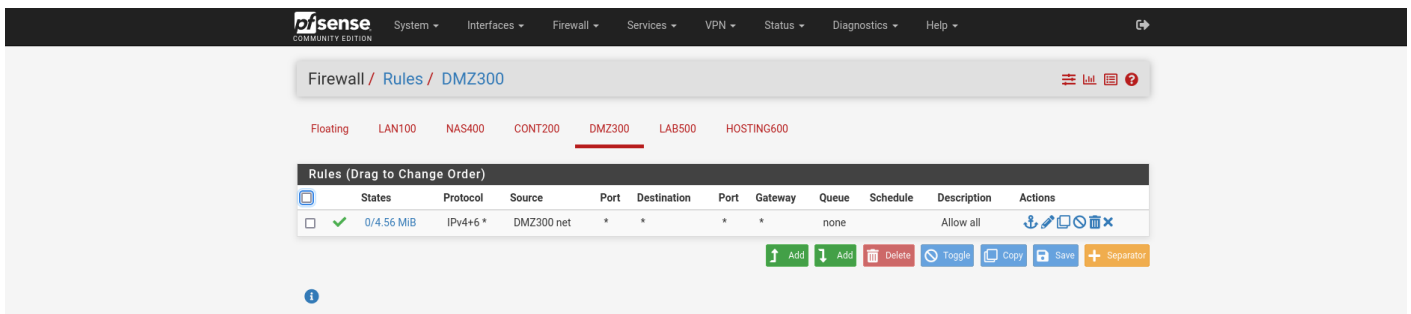
Manuel

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**



System -
Interfaces -
Firewall -
Services -
VPN -
Status -
Diagnostics -
Help -

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

DMZ300

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

☐ Invert match

DMZ300 net

Source Address
/

Display Advanced

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**.

Destination

☐ Invert match

any

Destination Address
/

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Custom

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

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Allow HTTP

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

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

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / DMZ300

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Floating LAN100 NAS400 CONT200 DMZ300 LAB500 HOSTING600

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	DMZ300 net	*	*	80 (HTTP)	*	none		Allow HTTP	Anchor Edit Copy Toggle Delete Close
<input type="checkbox"/>	✓ 0/4.56 MiB	IPv4+6 *	DMZ300 net	*	*	*	*	none		Allow all	Anchor Edit Copy Toggle Delete Close

↑ Add

↓ Add

🗑 Delete

🔄 Toggle

📄 Copy

💾 Save

+ Separator

i

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