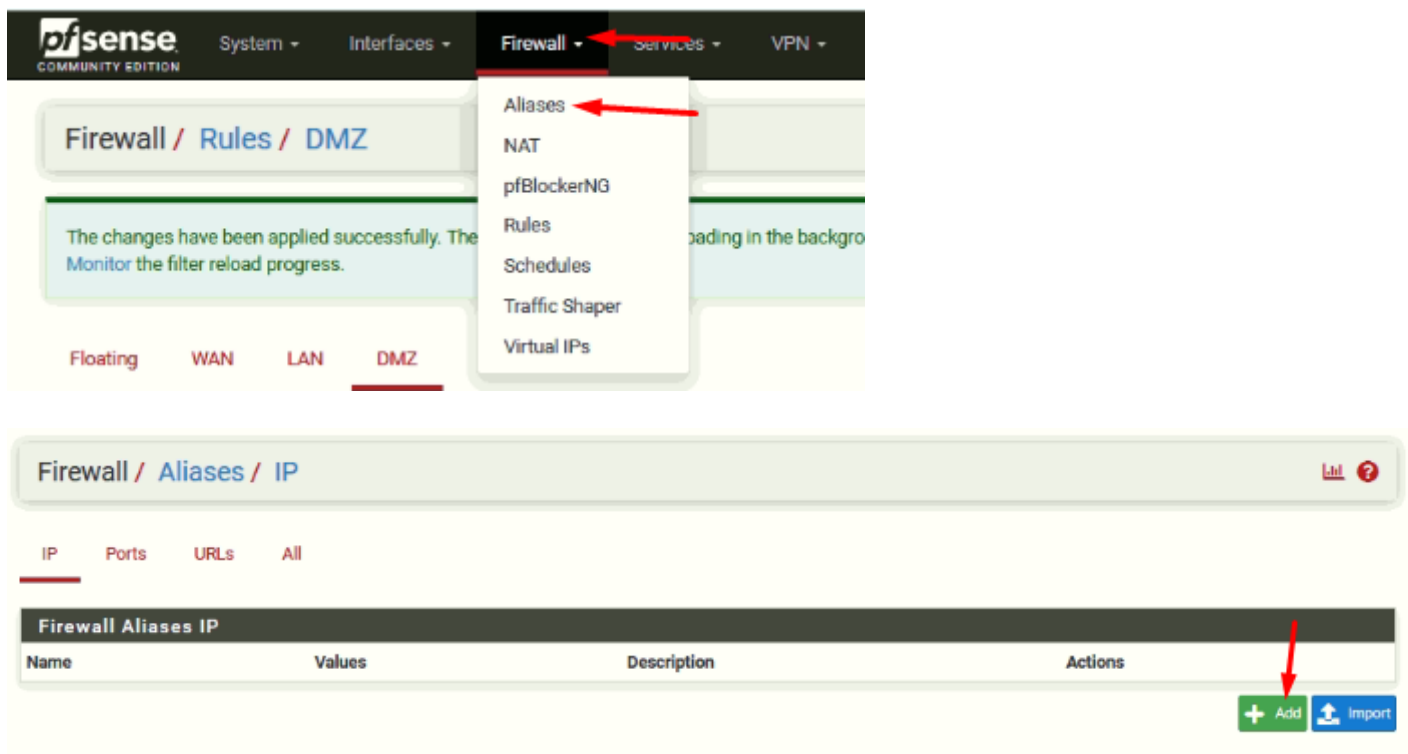


# Règles de pare-feu

Le LAN par défaut autorise tout, le WAN rejete tout et la DMZ aussi.

## Création d'alias



The image shows two screenshots of the pfSense web interface. The top screenshot shows the 'Firewall' menu with 'Aliases' selected. The bottom screenshot shows the 'Firewall / Aliases / IP' configuration page with the 'Add' button highlighted.

**Top Screenshot: Firewall Menu**

- System ▾
- Interfaces ▾
- Firewall ▾**
  - Aliases ←
  - NAT
  - pfBlockerNG
  - Rules
  - Schedules
  - Traffic Shaper
  - Virtual IPs
- Services ▾
- VPN ▾

Firewall / Rules / DMZ

The changes have been applied successfully. The Monitor the filter reload progress.

Floating WAN LAN **DMZ**

**Bottom Screenshot: Firewall / Aliases / IP**

IP Ports URLs All

**Firewall Aliases IP**

Name	Values	Description	Actions
------	--------	-------------	---------

+ Add ↑ Import

## Properties

**Name**

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

**Description**

A description may be entered here for administrative reference (not parsed).

**Type**

## Network(s)

**Hint** Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

**Network or FQDN**  /

# Règles DMZ

Pour la DMZ, on refuse l'accès au pare-feu (administration).

## Edit Firewall Rule

**Action**

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**

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

**Address Family**

Select the Internet Protocol version this rule applies to.

**Protocol**

Choose which IP protocol this rule should match.

## Source

**Source** ☐ Invert 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**.

## Destination

**Destination** ☐ Invert match   /

**Destination Port Range** (other)  (other)   
From Custom 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** BLOCK Web Interface

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

On bloque l'accès au LAN.

Floating WAN LAN **DMZ**

#### 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	*	*	This Firewall	10443	*	none	BLOCK Web Interface	   
<input type="checkbox"/>	✓	0 / 0 B	IPv4 *	*	*	*	*	none			   

 Add  Add  Delete  Save  Separator

#### Edit Firewall Rule

**Action** Block

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** DMZ

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

**Address Family** IPv4+IPv6

Select the internet Protocol version this rule applies to.

**Protocol** Any

Choose which IP protocol this rule should match.

#### Source

**Source** ☐ Invert match any Source Address /

#### Destination

**Destination** ☐ Invert match Single host or alias My\_Private\_Network














#### 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** BLOCK Access to LAN

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

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+6 *	*	*	My_Private_Network	*	*	none		BLOCK Access to LAN	    
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	*	*	This Firewall	10443	*	none		BLOCK Web Interface	    
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	*	*	*	*	*	none			    

Revision #1

Created 16 March 2021 20:13:33 by Khroners

Updated 5 July 2021 15:28:36 by Khroners