

# Installation et Configuration

## pfSense — Pare-feu & NAT



Clarac Matheo — BTS SIO 1ère année SISR

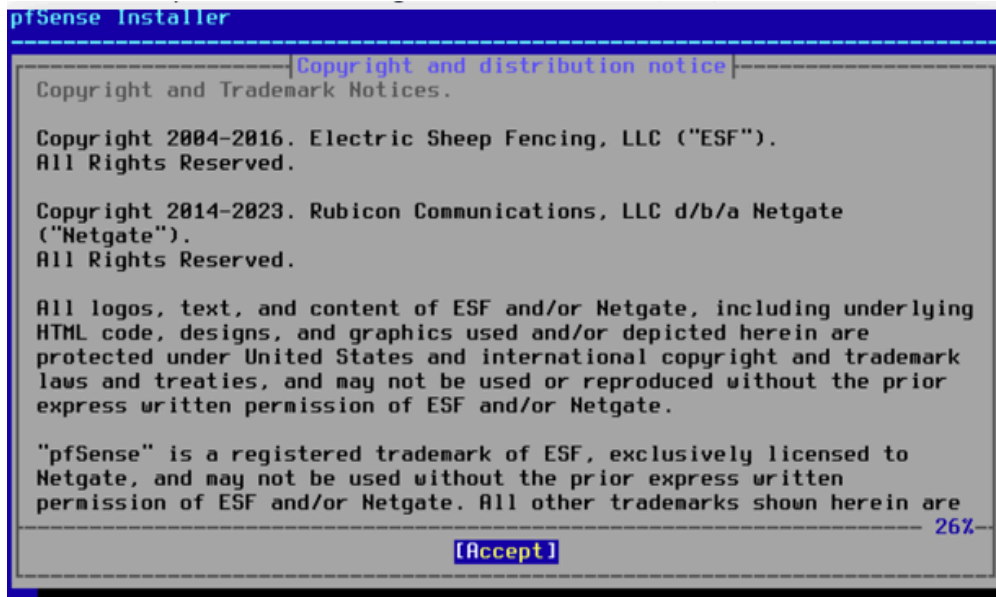
### Objectif

Installer et configurer pfSense comme pare-feu/routeur, mettre en place une architecture réseau avec une zone WAN, LAN et DMZ, puis créer des règles de pare-feu permettant l'accès au serveur web via NAT.

# 1. Installation de pfSense

pfSense est un système d'exploitation basé sur FreeBSD, utilisé comme pare-feu et routeur. L'installation se fait depuis une image ISO bootable.

1. Démarrer la machine sur l'ISO pfSense.
2. Accepter les termes de la licence (Copyright and distribution notice).
3. Suivre l'assistant d'installation : choix du clavier, partitionnement, installation.
4. Redémarrer après installation.



L'écran d'installation affiche l'avertissement de copyright et de distribution de pfSense. Cliquer sur [Accept] pour continuer.

# 2. Configuration des interfaces réseau

Après redémarrage, pfSense affiche l'assignation des interfaces réseau depuis la console. Les trois interfaces sont configurées comme suit :

```
WAN (wan) -> le0 -> v4/DHCP4: 192.168.147.105/24
LAN (lan) -> le1 -> v4: 192.168.10.1/24
DMZ (opt1) -> le2 -> v4: 192.168.20.1/24
```

Zone	Interface	Carte	Adresse IP
WAN	wan	le0	192.168.147.105/24 (DHCP)
LAN	lan	le1	192.168.10.1/24
DMZ (opt1)	opt1	le2	192.168.20.1/24

⚠ Le serveur web se trouve dans la DMZ à l'adresse 192.168.20.2. La DMZ isole les serveurs accessibles depuis l'extérieur du réseau LAN interne.

### 3. Règle de pare-feu — Accès au serveur web

Cette règle permet aux connexions provenant d'Internet (WAN) d'atteindre le serveur web situé en DMZ via un NAT de redirection de port (Port Forward).

#### Configuration de la règle

**Edit Firewall Rule**

<b>Action</b>	<div style="border: 1px solid #ccc; padding: 2px;">Pass</div> <p>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.</p>
<b>Disabled</b>	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
<b>Associated filter rule</b>	<p>This is associated with a NAT rule. Editing the interface, protocol, source, or destination of associated filter rules is not permitted. <a href="#">View the NAT rule</a></p>
<b>Interface</b>	<div style="border: 1px solid #ccc; padding: 2px;">WAN</div> <p>Choose the interface from which packets must come to match this rule.</p>
<b>Address Family</b>	<div style="border: 1px solid #ccc; padding: 2px;">IPv4</div> <p>Select the Internet Protocol version this rule applies to.</p>
<b>Protocol</b>	<div style="border: 1px solid #ccc; padding: 2px;">TCP</div> <p>Choose which IP protocol this rule should match.</p>

**Source**

<b>Source</b>	<input type="checkbox"/> Invert match <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;">Any</div> <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;">Source Address</div> / <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;"></div>
<div style="background-color: #007bff; color: white; padding: 5px; display: inline-block;">⚙️ Display Advanced</div>	
<p>The <b>Source Port Range</b> 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, <b>any</b>.</p>	
<b>Destination</b>	
<b>Destination</b>	<input type="checkbox"/> Invert match <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;">Address or Alias</div> <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;">192.168.20.2</div> / <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;"></div>
<b>Destination Port Range</b>	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid #ccc; padding: 2px;">HTTP (80)</div> <div style="border: 1px solid #ccc; padding: 2px; width: 50px;"></div> <div style="border: 1px solid #ccc; padding: 2px;">HTTP (80)</div> <div style="border: 1px solid #ccc; padding: 2px; width: 50px;"></div> </div> <p>From Custom To Custom</p> <p>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</p>
<b>Extra Options</b>	
<b>Log</b>	<input type="checkbox"/> 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 <a href="#">Status: System Logs: Settings</a> page).
<b>Description</b>	<div style="border: 1px solid #ccc; padding: 2px;">NAT</div> <p>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.</p>
<div style="background-color: #007bff; color: white; padding: 5px; display: inline-block;">⚙️ Display Advanced</div>	

## Détail des paramètres

Paramètre	Valeur
Action	Pass (Autoriser)
Interface	WAN
Address Family	IPv4
Protocole	TCP
Source	Any (toute source)
Destination	192.168.20.2 (serveur web DMZ)
Port destination	HTTP (80)
Description	NAT
Tracking ID	1747063536
Créée le	5/12/25 15:25:36 par NAT Port Forward

Rule Information	
Tracking ID	1747063536
Created	5/12/25 15:25:36 by NAT Port Forward

## 4. Récapitulatif des règles WAN

Le tableau ci-dessous liste l'ensemble des règles actives sur l'interface WAN de pfSense.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/2 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0/6 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	0/35 KiB	IPv4 TCP	*	*	192.168.20.2	80 (HTTP)	*	none		NAT	

État	Protocol	Source	Port	Destination	Port dest.	Description
<input checked="" type="checkbox"/> Bloqué	*	Reserved / Not assigned by IANA	*	*	*	Block bogon networks
<input checked="" type="checkbox"/> Autorisé	IPv4 TCP	*	*	*	443 (HTTPS)	—
<input checked="" type="checkbox"/> Autorisé	IPv4 TCP	*	*	192.168.20.2	80 (HTTP)	NAT

Explication des règles :

- Block bogon networks : bloque les adresses IP réservées ou non attribuées par l'IANA (protection par défaut).
- Port 443 (HTTPS) : autorise les connexions HTTPS entrantes depuis n'importe quelle source.
- Port 80 (HTTP) → 192.168.20.2 (NAT) : redirige le trafic HTTP entrant vers le serveur web en DMZ.

⚠ La règle NAT (port 80) a été créée automatiquement lors de la configuration du Port Forward dans le menu Firewall > NAT > Port Forward.