

# Mission 12: Mise en Place Et Configuration du Pare-feu OPENSENSE

OPNsense est un système d'exploitation servant de routeur et pare-feu. Tournant sur FreeBSD, il est basé sur pfSense dont il cherche à améliorer la sécurité, la fiabilité et l'optimisation du code. Il offre, en plus du filtrage et du routage, la possibilité de mettre en place de nombreux autres services. On remplace notre routeur par **OpenSense**. On utilisera une clé pour installer ce nouvel outil.

## 0.0 PREREQUIS

Un routeur x64 avec 3 interfaces réseaux à minima :

- WAN : interface de sortie
- LAN : interface pour le LAN et les services privés
- DMZ : interface pour les services publics



Il faudrait tout d'abord récupérer les adresses MAC, de toutes nos interfaces : enp2s0 ; enp4s0 ; enp5s0 .

## I) Procédure D'installation De OPNsense

### I) Installation et vérification du bon fonctionnement d'OPNsense

#### 1. Installation

Grâce à une clé bootable, nous allons installer OPNsense. Le bouton F12 menu de démarrage temporaire. Il permet de forcer le démarrage sur la clé USB, sans changer définitivement l'ordre de démarrage dans le BIOS.

Après avoir booté sur la clé USB, on va s'identifier avec :

- installer / opnsense (pour l'installer sur notre routeur)

```
** OPNsense.localdomain: OPNsense 24.7 **

LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)      ->

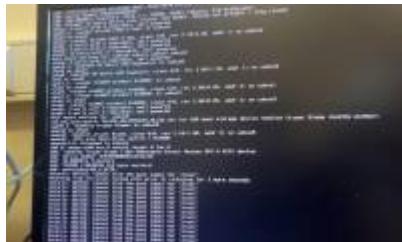
HTTPS: sha256 FE 94 7B 39 A1 B2 88 E5 7B 41 59 EF B6 61 23 41
       E8 97 A4 52 44 89 FA D1 87 95 19 AE C8 FC 81 65
SSH:   SHA256 8vnr.jv3HfOPuPfkRVPqdgsUvkUvn7JmU+BV5gesC1bs (ECDSA)
SSH:   SHA256 o+hhx8pLX9eeJNCqsvx0IyngHHRajI/bMeGtq+1yhd0 (ED25519)
SSH:   SHA256 eFS10RAXE6a/fn4zqqJ4kS1PJHEessbLdoUXnCH/+Fo (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/and64 (OPNsense.localdomain) (ttyv8)
main: #
```

- Comme langue, nous avons opté pour le français (**select fr.kbd**)

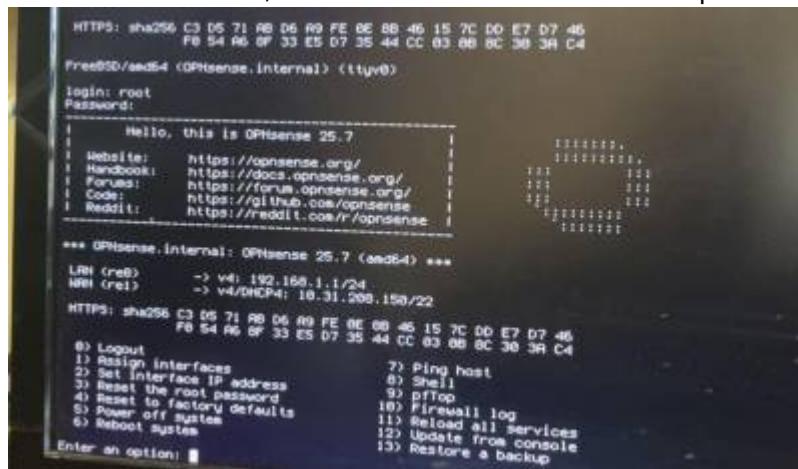
- Sélectionner ZFS (**install ZFS**)
- Sélectionner le Disque Dur sur lequel on veut installer OPNsense
- Confirmation
- Puis Procédure d'Installation



## 2. Configuration Initiale

Pendant notre Installation , nous avons changer de mot de passe : **root/mdp de Océanie** .

Quand nous allons accéder à l'interface, nous allons faire un choix des options : On choisira l'options



### Assign Interfaces

3 interfaces :

On nous a présenté

```
re0  : fc:aa:14:51:b6:1a (adresse Mac)
re1  : 9c:a2:f4:ca:0b:52
re2  : 9c:a2:f4:ca:0b:3a
```

Nous devons choisir l'interface du **WAN** , par rappor à ces adresses MAC , nous devons nous rappeler de celle l'adresse IP de sortie du Routeur puis l'attribuer . Notre cas cas,les adresses sont .

- WAN → **re0**
- LAN → **re1**
- OPT1(DMZ) → **re2**



```
F8:54 66 0F 33 E5 D7 35 44 CC 63 0B 0C 5E 5D C4

8) Logout          7) Ping host
1) Session interfaces   8) Shell
2) Set interface IP address  9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup

Enter an option: 2

Available interfaces:

1 - LAN (re1 - static, tracked)
2 - OPT1 (re2)
3 - WAN (re0 - dhcp, dhcp6)

Enter the number of the interface to configure: 3
```

- Nous refusons de configurer l'adresse IPV4 via l'interface DHCP : on met donc **n**
- Comme SUBNET (MASQUE DE SOUS RESEAU) on prend le 255.255.0.0 = 16 , notre @IPV4 de sortie est en **/16**
- On nous demande la gateway du WAN , on saisie :

**• 172.31.0.0**

- Saisir l'@IP du nom de domaine :

```
Do you want to use the gateway as the IPv4 name server, too? [Y/n] n
Enter the IPv4 name server or press <ENTER> for none:
> 8.8.8.8
```

- Nous allons sélectionner l'option 8 pour le shell et saisir la commande suivante :

**• pfctl -d # Pour désactiver le parefeu / -e pour activer le pare-feu**

## II) Accès à L'Interface Web De Configuration D'OPNsense

Pour accéder à notre Interface , nous devons taper sur notre navigateur l'@ suivante :  
**https://172.31.208.254**



### 1. Mettre la règle NAT



## III) Règles De Pare-Feu

Pour toutes nos règles de pare-feu , on aura 3 sections : **WAN** , **LAN** , **DMZ**

### 1. Règles Etablies sur le réseau LAN

Last update: 2025/11/28 sisr2-oceanie:installation\_et\_configuration\_de\_opensense https://sisr2.beaupeyrat.com/doku.php?id=sisr2-oceanie:installation\_et\_configuration\_de\_opensense  
07:44

<input type="checkbox"/>		IPv4 TCP	10.31.208.73/32	*	DMZ net	22 (SSH)	*	*	On autorise le LAN à se connecter en SSH vers la DMZ	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	10.31.208.74/32	*	DMZ net	22 (SSH)	*	*	On autorise le LAN à se connecter en SSH vers la DMZ	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	LAN net	*	10.31.216.53/32	53 (DNS)	*	*	Donner l'accès au réseau LAN d'avoir accès au Serveur DNS (qui se trouve dans la DMZ)	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	LAN net	*	10.31.216.54/32	53 (DNS)	*	*	Donner l'accès au réseau LAN d'avoir accès au Serveur DNS (qui se trouve dans la DMZ)	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	LAN net	*	10.31.216.63/32	53 (DNS)	*	*	Donner l'accès au réseau LAN d'avoir accès au Serveur DNS (qui se trouve dans la DMZ)	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	LAN net	*	10.31.216.64/32	53 (DNS)	*	*	Donner l'accès au réseau LAN d'avoir accès au Serveur DNS (qui se trouve dans la DMZ)	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	LAN net	*	443 (HTTPS)	*	*	*	Notre LAN doit pouvoir accéder à Internet, faire des updates	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	LAN net	*	80 (HTTP)	*	*	*	Notre LAN doit pouvoir accéder à Internet, faire des updates	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 ICMP	LAN net	*	DMZ net	*	*	*	Permettre aux machines du LAN à ping celles de la DMZ	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 ICMP	LAN net	*	BeupNET	*	*	*	On autorise toutes les machines du LAN à ping celles du Réseau Beaupeyrat.	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	10.31.208.67/32	*	10.31.216.67/32	67	*	*	on autorise le dhcp principal à répondre au dhcp relai	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	10.31.208.68/32	*	10.31.216.68/32	67	*	*	on autorise le dhcp principal à répondre au dhcp relai	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>

## 2. Règles Etablies sur le réseau WAN

<input type="checkbox"/>	Automatically generated rules											
<input type="checkbox"/>		IPv4 TCP	*	*	10.31.211.254	443 (HTTPS)	*	*	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>	
<input type="checkbox"/>		IPv4 ICMP	BeupNET	*	LAN net	*	*	*	autorise le réseau Beau à ping notre réseau LAN	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 ICMP	BeupNET	*	DMZ net	*	*	*	autorise le réseau Beau à ping notre réseau DMZ	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	BeupNET	*	This Firewall	22 (SSH)	*	*	autorise le réseau Beau à se connecter en SSH sur toutes les adresses de notre parefeu	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	BeupNET	*	LAN net	22 (SSH)	*	*	On autorise le réseau Beaupeyrat à se connecter en SSH vers le LAN	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	BeupNET	*	DMZ net	22 (SSH)	*	*	On autorise le réseau Beaupeyrat à se connecter en SSH vers le DMZ	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	BeupNET	*	10.31.208.1	any - 8006	*	*	On autorise notre PC à accéder à PROXIMOX	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	BeupNET	*	DMZ net	any - 53	*	*	On autorise les machines de Beaupeyrat à joindre notre DNS qui se trouve dans la DMZ.	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	BeupNET	*	10.31.208.80/32	80 (HTTP)	*	*	On autorise le réseau Beaupeyrat à joindre le serveur WEB du LAN	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	BeupNET	*	10.31.216.80/32	80 (HTTP)	*	*	On autorise le réseau Beaupeyrat à joindre le serveur WEB de la DMZ	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	BeupNET	*	10.31.208.73/32	80 (HTTP)	*	*	On autorise le réseau Beau à se connecter au serveur BACKUPPC	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 TCP	BeupNET	*	10.31.208.74/32	80 (HTTP)	*	*	On autorise le réseau Beau à se connecter au serveur BACKUPPC	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	BeupNET	*	10.31.216.53/32	53 (DNS)	*	*	On autorise le réseau Beaupeyrat à joindre notre serveur DNS	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	BeupNET	*	10.31.216.54/32	53 (DNS)	*	*	On autorise le réseau Beaupeyrat à joindre notre serveur DNS	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	BeupNET	*	10.31.216.63/32	53 (DNS)	*	*	On autorise le réseau Beaupeyrat à joindre notre serveur DNS	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>
<input type="checkbox"/>		IPv4 UDP	BeupNET	*	10.31.216.64/32	53 (DNS)	*	*	On autorise le réseau Beaupeyrat à joindre notre serveur DNS	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Details</a>

## 3. Règles Etablies sur le réseau DMZ



From:

<https://sisr2.beaupeyrat.com/> - Documentations SIO2 option SISR

Permanent link:

[https://sisr2.beaupeyrat.com/doku.php?id=sisr2-oceanie:installation\\_et\\_configuration\\_de\\_opensense](https://sisr2.beaupeyrat.com/doku.php?id=sisr2-oceanie:installation_et_configuration_de_opensense)

Last update: 2025/11/28 07:44

