

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.

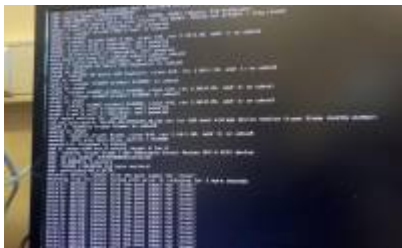
Après avoir booté sur la clé USB, on va s'identifier avec :

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

```
** OPNsense.localdomain: OPNsense 24.7 ***  
LAN (en0)      -> v4: 192.168.1.1/24  
WAN (en1)      ->  
  
HTTPS: sha256 FE 94 78 39 A1 B2 88 E5 78 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 0vnr_jv3Hf0PuPfkRVPqdg5UvKuvn7JmU•8V5gesC1bs (ECDSA)  
SSH:  SHA256 o•hxx8pLX9eeJNCqsxv0lymyHWRaJl/bMeGtq•1yhd0 (ED25519)  
SSH:  SHA256 eFS10A1XE6a/fnWzqqJ4k51PJHEessbLdoUXaCN/•Fo (RSA)  
  
elcome! 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  
other accounts. Remote login via SSH is also enabled.  
  
FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)  
login: █
```

- 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 :

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

On nous a présenter

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**





- 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

		IPv4 TCP	10.31.208.73/32	*	DMZ net	22 (SSH)	*	*	On autorise le LAN à se connecter en SSH vers la DMZ			
		IPv4 TCP	10.31.208.74/32	*	DMZ net	22 (SSH)	*	*	On autorise le LAN à se connecter en SSH vers la DMZ			
		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)			
		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)			
		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)			
		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)			

		IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	*	Notre LAN doit pouvoir accéder à Internet, faire des updates			
		IPv4 TCP	LAN net	*	*	80 (HTTP)	*	*	Notre LAN doit pouvoir accéder à Internet, faire des updates			
		IPv4 ICMP	LAN net	*	DMZ net	*	*	*	Permettre aux machines du LAN à ping celles de la DMZ			
		IPv4 ICMP	LAN net	*	BeaupNET	*	*	*	On autorise toutes les machines du LAN à ping celles du Réseau Beaupeyrat.			
		IPv4 UDP	10.31.208.67/32	*	10.31.216.67/32	67	*	*	on autorise le dhcp principal a répondre au dhcp relay			
		IPv4 UDP	10.31.208.68/32	*	10.31.216.68/32	67	*	*	on autorise le dhcp principal a répondre au dhcp relay			

2. Règles Etablies sur le réseau WAN

Automatically generated rules												
		IPv4 TCP	*	*	10.31.211.254	443 (HTTPS)	*	*				
		IPv4 ICMP	BeaupNET	*	LAN net	*	*	*	autorise le réseau Beup à ping notre réseau LAN			
		IPv4 ICMP	BeaupNET	*	DMZ net	*	*	*	autorise le réseau Beup à ping notre réseau DMZ			
		IPv4 TCP	BeaupNET	*	This Firewall	22 (SSH)	*	*	autorise le réseau Beup à se connecter en SSH sur toutes les adresses de notre panneau			
		IPv4 TCP	BeaupNET	*	LAN net	22 (SSH)	*	*	On autorise le réseau de Beaupeyrat à se connecter en SSH vers le LAN			
		IPv4 TCP	BeaupNET	*	DMZ net	22 (SSH)	*	*	On autorise le réseau de Beaupeyrat à se connecter en SSH vers le DMZ			

		IPv4 TCP	BeaupNET	*	10.31.208.1	any - 8005	*	*	On autorise notre PC à accéder à PRODMQX			
		IPv4 UDP	BeaupNET	*	DMZ net	any - 53	*	*	On autorise les machines de Beaupeyrat à joindre notre DNS qui se trouve dans la DMZ.			
		IPv4 TCP	BeaupNET	*	10.31.208.86/32	80 (HTTP)	*	*	On autorise le réseau Beaupeyrat à joindre le serveur WEB du LAN			
		IPv4 TCP	BeaupNET	*	10.31.216.86/32	80 (HTTP)	*	*	On autorise le réseau Beaupeyrat à joindre le serveur WEB de la DMZ			
		IPv4 TCP	BeaupNET	*	10.31.208.73/32	80 (HTTP)	*	*	On autorise le réseau Beup à se connecter au serveur BACKUPPC			
		IPv4 TCP	BeaupNET	*	10.31.208.74/32	80 (HTTP)	*	*	On autorise le réseau Beup à se connecter au serveur BACKUPPC			

		IPv4 UDP	BeaupNET	*	10.31.216.53/32	53 (DNS)	*	*	On autorise le réseau Beaupeyrat à joindre notre serveur DNS			
		IPv4 UDP	BeaupNET	*	10.31.216.54/32	53 (DNS)	*	*	On autorise le réseau Beaupeyrat à joindre notre serveur DNS			
		IPv4 UDP	BeaupNET	*	10.31.216.63/32	53 (DNS)	*	*	On autorise le réseau Beaupeyrat à joindre notre serveur DNS			
		IPv4 UDP	BeaupNET	*	10.31.216.64/32	53 (DNS)	*	*	On autorise le réseau Beaupeyrat à joindre notre serveur DNS			

3. Règles Etablies sur le réseau DMZ

<input type="checkbox"/>	IPv4 UDP	10.31.216.63/32	*	8.8.8.8/32	53 (DNS)	*	*	On autorise le serveur DNS de la DMZ de joindre le Serveur 8.8.8.8		
<input type="checkbox"/>	IPv4 UDP	10.31.216.53/32	*	8.8.8.8/32	53 (DNS)	*	*	On autorise le serveur DNS de la DMZ de joindre le Serveur 8.8.8.8		
<input type="checkbox"/>	IPv4 UDP	10.31.216.63/32	*	8.8.4.4/32	53 (DNS)	*	*	On autorise le serveur DNS de la DMZ de joindre le Serveur 8.8.4.4		
<input type="checkbox"/>	IPv4 UDP	10.31.216.53/32	*	8.8.4.4/32	53 (DNS)	*	*	On autorise le serveur DNS de la DMZ de joindre le Serveur 8.8.4.4		
<input type="checkbox"/>	IPv4 TCP	10.31.216.80/32	*	10.31.208.33/32	3306	*	*	On autorise le serveur WEB Public à accéder à la base de données au port 3306		
<input type="checkbox"/>	IPv4 TCP	10.31.216.80/32	*	10.31.208.33/32	3306	*	*	On autorise le serveur WEB Public à accéder à la base de données au port 3306		

<input type="checkbox"/>	IPv4 UDP	10.31.216.54/32	*	8.8.4.4/32	53 (DNS)	*	*	On autorise le serveur DNS de la DMZ de joindre le Serveur 8.8.8.8		
<input type="checkbox"/>	IPv4 UDP	10.31.216.64/32	*	8.8.4.4/32	53 (DNS)	*	*	On autorise le serveur DNS de la DMZ de joindre le Serveur 8.8.8.8		
<input type="checkbox"/>	IPv4 UDP	10.31.216.64/32	*	8.8.8.8/32	53 (DNS)	*	*	On autorise le serveur DNS de la DMZ de joindre le Serveur 8.8.4.4		
<input type="checkbox"/>	IPv4 TCP	10.31.216.80/32	*	10.31.208.34/32	3306	*	*	On autorise le serveur WEB Public à accéder à la base de données au port 3306		
<input type="checkbox"/>	IPv4 TCP	10.31.216.80/32	*	10.31.208.34/32	any-3306	*	*	On autorise le serveur WEB Public à accéder à la base de données 2 au port 3306		

<input type="checkbox"/>	IPv4 UDP	10.31.216.68/32	*	10.31.208.68/32	67	*	*	On autorise le serveur DHCP-Relay à joindre le serveur DHCP du réseau LAN		
<input type="checkbox"/>	IPv4 UDP	10.31.216.67/32	*	10.31.208.67/32	67	*	*	On autorise le serveur DHCP-Relay à joindre le serveur DHCP du réseau LAN		
<input type="checkbox"/>	IPv4 TCP	DMZ net	*	*	80 (HTTP)	*	*	Pour accéder à Internet au ports 80		
<input type="checkbox"/>	IPv4 TCP	DMZ net	*	*	443 (HTTPS)	*	*	Pour accéder à Internet au port 443		
<input type="checkbox"/>	IPv4 ICMP	DMZ net	*	LAN net	*	*	*	On autorise les ping de la dmz au lan		
<input type="checkbox"/>	IPv4 ICMP	DMZ net	*	WAN net	*	*	*	autorise les ping de la dmz au wan		

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

Last update: 2025/11/28 07:44

