

# Mission 12 : Installation routeur/pare-feu OPNsense

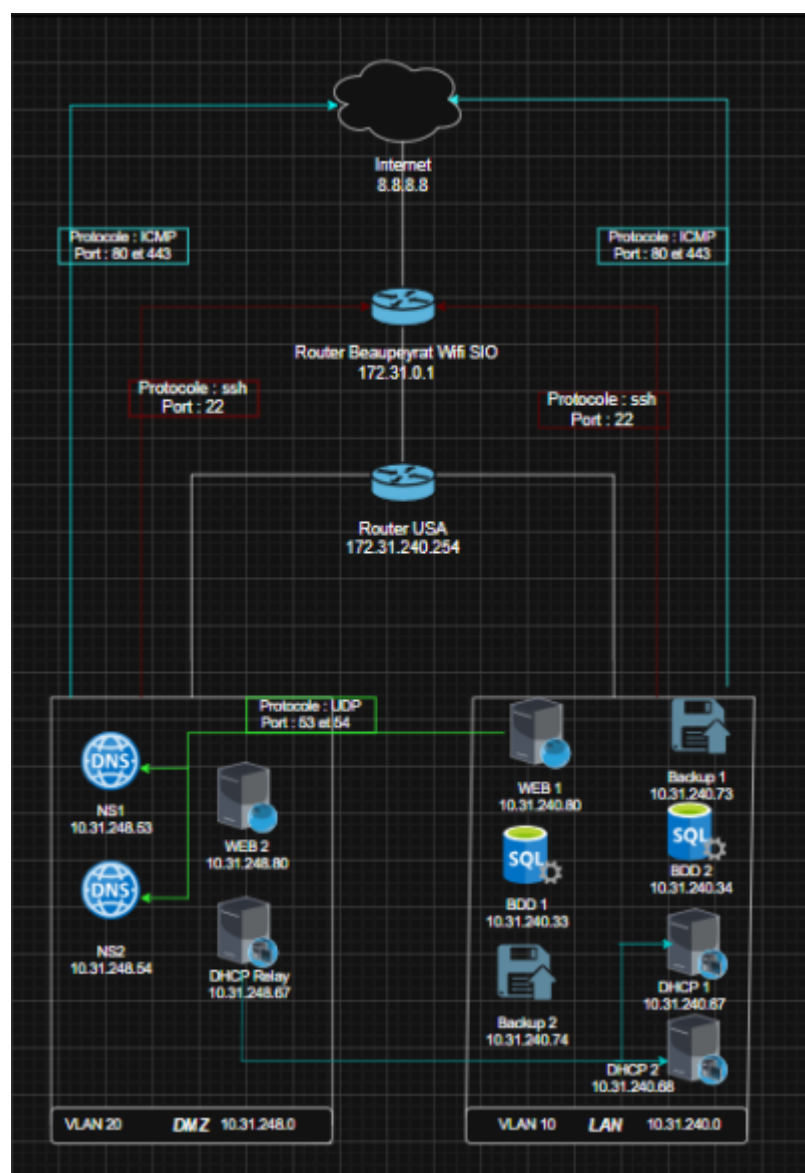
## Pré-requis

Afin de pouvoir réaliser cette mission il faut : 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

## Introduction

Nous allons installer OPNsense sur nos routeur afin de pouvoir y accéder a l'aide d'une interface graphique. Dans un même temps OPNsense nous offres une solution de pare-feu paramétrable aussi par l'interface graphique



### Avantage de la Solution OPNsense :

Cette solution est gratuite

Elle permet d'accéder a notre routeur par interfaces graphique

Possibilité de configurer des règles de pare-feu

Elle offre un tableaux de bord personnalisables avec graphiques et statistiques en temps réel

## Cahier des charges

- Installation et vérification du bon fonctionnement d'OPNsense
- Lecture de la documentation et étude des fonctionnalités d'OPNsense
- Étude des prérequis matériels
- Création et affectation des interfaces
- Accès à l'interface web de configuration d'OPNsense
- Création d'une troisième interface pour la DMZ
- Configuration de base d'OPNsense
- Mise en place du pare-feu d'OPNsense
- Grille de test et de validation du service
- Liste des problèmes rencontrés et des solutions apportées

## OPNsense

## Installation et paramétrage d'OPNsense

**Pour Commencer avant meme de faire quoi que ce soit il faut d'abord prendre en photo nos adresse MAC car c'est grace a elles que nous allons pouvoir reconnaitre nos interfaces**

**Se munir d'une clé bootable tipe Rufus ou Ventoy sur la quelle se trouve L'iso de OPNsense**

**Booter sur la clé et lancer l'installation**

**Une fois arrivé sur cette page :**

```
Last login: Fri Oct 17 05:57:48 2025

-----
|           Hello, this is OPNsense 25.7           |
|-----|-----|
| Website:   https://opnsense.org/                 |
| Handbook:  https://docs.opnsense.org/            |
| Forums:    https://forum.opnsense.org/           |
| Code:      https://github.com/opnsense           |
| Reddit:    https://reddit.com/r/opnsense         |
|-----|-----|

*** OPNsense.usa.gsb.org: OPNsense 25.7 (amd64) ***

DMZ (re2)      -> v4:
LAN (re1)      -> v4:
WAN (re0)      -> v4:

HTTPS: sha256 1A 08 E9 6B 7A AA 8E C0 FB 03 77 85 C4 0E A4 A9
          5E D3 15 29 3F 51 C0 82 BF 81 5F 2F CD 6F 73 D2
SSH:  SHA256 ANprf8QB0ddmSsQ6caSOXN3EVNVsC4vH9VvA0cL1hL0 (ECDSA)
SSH:  SHA256 2VHN7NXGUgGNDKKXVCJc1Y40Bcn1GYXxmbj1bSjW0Jk (ED25519)
SSH:  SHA256 wuMgx0bwPHgd2t5AVvRo/t0i6mDgWKouGhVugAYT2MY (RSA)

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

Enter an option:
```

**Important:**

Entré le Login Installer pour que l'installation complète se fasse

Une fois l'installation fait nous arrivons sur la page d'accueil sur laquelle on va devoir assigner nos Interfaces réseau grâce a nos adresse mac pris en photo précédemment

Les interfaces étant configuré on peut maintenant leur assigner leurs adresse IP

^

**Important:**

Il n'y a que sur l'interface WAN que l'on doit mettre en place une gateway, il n'y en a pas besoin sur toutes les autres interfaces

**Si toutes les interfaces sont bien configurer avec les bonnes adresse IP, notre routeur est accessible sur un moteur de recherche a l'adresse 10.31.243.254**



Mais ça ne suffit pas car dès que l'on va faire une modification sur l'interface graphique nous allons être déconnectés. C'est la raison pour la quelle nous devons faire



une règle qui va faire en sorte que si une connexion arrive de l'extérieur (WAN) sur le port 1234, redirige là vers la machine 10.31.243.254 sur le port 443 (HTTPS).

Cette règle la voici :

OPNsense

Reporting

System

Interfaces

Firewall

Aliases

Automation

Categories

Groups

NAT

Port Forward

One-to-One

Outbound

NPTv6

Rules

Shaper

Settings

Log Files

Diagnostics

VPN

Services

Power

Help

Firewall: NAT: Port Forward

Select category

|                          | Source        | Destination | NAT                  |       |               |             |                      |             |                   |  |
|--------------------------|---------------|-------------|----------------------|-------|---------------|-------------|----------------------|-------------|-------------------|--|
|                          | Interface     | Proto       | Address              | Ports | Address       | Ports       | IP                   | Ports       | Description       |  |
| <input type="checkbox"/> | LAN           | TCP         | *                    | *     | LAN address   | 22, 80, 443 | *                    | *           | Anti-Lockout Rule |  |
| <input type="checkbox"/> | WAN           | TCP         | *                    | *     | This Firewall | 1234        | 10.31.243.254        | 443 (HTTPS) |                   |  |
|                          | Enabled rule  |             | No redirect          |       |               |             | Linked rule          |             |                   |  |
|                          | Disabled rule |             | Disabled no redirect |       |               |             | Disabled linked rule |             |                   |  |

Alias (click to view/edit)

Ce qui fait que maintenant après chaque configuration le pare-feu ne va pas nous déconnecter

Règles WAN

Règles de pare-feu WAN

OPNsense

Reporting

System

Interfaces

Firewall

Aliases

Automation

Categories

Groups

NAT

Rules

Floating

DMZ

LAN

WAN

Shaper

Settings

Log Files

Diagnostics

VPN

Services

Power

Help

Automatically generated rules

|                          | Protocol  | Source         | Port | Destination     | Port        | Gateway | Schedule | Description                                              |  |
|--------------------------|-----------|----------------|------|-----------------|-------------|---------|----------|----------------------------------------------------------|--|
| <input type="checkbox"/> | IPv4 TCP  | *              | *    | 10.31.243.254   | 443 (HTTPS) | *       | *        |                                                          |  |
| <input type="checkbox"/> | IPv4 ICMP | 10.187.20.0/24 | *    | LAN net         | *           | *       | *        | Autorise le ping du réseau de beaup vers le LAN          |  |
| <input type="checkbox"/> | IPv4 ICMP | 10.187.20.0/24 | *    | DMZ net         | *           | *       | *        | Autorise le ping du réseau de beaup vers le DMZ          |  |
| <input type="checkbox"/> | IPv4 TCP  | 10.187.20.0/24 | *    | LAN net         | 22 (SSH)    | *       | *        | Autorise la connexion ssh du réseau de beaup vers le LAN |  |
| <input type="checkbox"/> | IPv4 TCP  | 10.187.20.0/24 | *    | 10.31.248.0/22  | 22 (SSH)    | *       | *        | Autorise la connexion ssh du réseau de beaup vers le DMZ |  |
| <input type="checkbox"/> | IPv4 TCP  | Beaupnet       | *    | 10.31.240.1/32  | 8006        | *       | *        | Autorise le réseau beaup à aller sur le proxmox          |  |
| <input type="checkbox"/> | IPv4 UDP  | Beaupnet       | *    | 10.31.248.53/32 | 53 (DNS)    | *       | *        |                                                          |  |
| <input type="checkbox"/> | IPv4 UDP  | Beaupnet       | *    | 10.31.248.54/32 | 53 (DNS)    | *       | *        |                                                          |  |
| <input type="checkbox"/> | IPv4 TCP  | Beaupnet       | *    | 10.31.240.80/32 | 80 (HTTP)   | *       | *        |                                                          |  |
| <input type="checkbox"/> | IPv4 TCP  | Beaupnet       | *    | 10.31.248.80/32 | 80 (HTTP)   | *       | *        |                                                          |  |
| <input type="checkbox"/> | IPv4 TCP  | Beaupnet       | *    | 10.31.240.80/32 | 443 (HTTPS) | *       | *        |                                                          |  |

Règles LAN

Règles de pare-feu LAN

Last login: Fri Oct 17 05:57:48 2025

OPNsense

Lobby

Reporting

System

Interfaces

Firewall

Aliases

Automation

Categories

Groups

NAT

Rules

Floating

DMZ

LAN

WAN

Shaper

Settings

Log Files

Diagnostics

VPN

Services

Power

root@OPNsense.usa.gsb.org

Search

Firewall: Rules: LAN

Select category

Inspect

|                               | Protocol  | Source          | Port     | Destination     | Port        | Gateway | Schedule | Description                                        |  |
|-------------------------------|-----------|-----------------|----------|-----------------|-------------|---------|----------|----------------------------------------------------|--|
| Automatically generated rules |           |                 |          |                 |             |         |          |                                                    |  |
|                               | IPv4 TCP  | *               | *        | *               | 443 (HTTPS) | *       | *        | Autorisé la connexion internet                     |  |
|                               | IPv4 TCP  | *               | *        | *               | 80 (HTTP)   | *       | *        | Autorisé la connexion internet                     |  |
|                               | IPv4 UDP  | *               | *        | 10.31.248.53/32 | 53 (DNS)    | *       | *        | Autorise le reseau Lan à communiquer avec le DNS   |  |
|                               | IPv4 UDP  | *               | *        | 10.31.248.54/32 | 53 (DNS)    | *       | *        | Autorise le reseau Lan à communiquer avec le DNS 2 |  |
|                               | IPv4 UDP  | 10.31.240.67/22 | *        | 10.31.248.67/22 | 67          | *       | *        | J'autorise le dhcp a communiqué avec le relay      |  |
|                               | IPv4 UDP  | 10.31.240.68/22 | *        | 10.31.248.68/22 | 67          | *       | *        | J'autorise le dhcp a communiqué avec le relay      |  |
|                               | IPv4 TCP  | 10.31.240.80/32 | 53 (DNS) | 10.31.248.53/32 | 53 (DNS)    | *       | *        |                                                    |  |
|                               | IPv4 ICMP | 10.31.240.80/32 | *        | 10.31.248.53/32 | *           | *       | *        |                                                    |  |
|                               | IPv4 TCP  | 10.31.240.73/32 | *        | DMZ net         | 22 (SSH)    | *       | *        |                                                    |  |
|                               | IPv4 ICMP | 10.31.240.73/32 | *        | DMZ net         | *           | *       | *        |                                                    |  |
|                               | IPv4 ICMP | 10.31.240.74/32 | *        | DMZ net         | *           | *       | *        |                                                    |  |
|                               | IPv4 ICMP | *               | *        | DMZ net         | *           | *       | *        | ping du LAN au DMZ                                 |  |
|                               | IPv4 UDP  | 10.31.240.33/32 | *        | 10.31.248.80/32 | 3306        | *       | *        |                                                    |  |

pass

pass (disabled)

block

block (disabled)

reject

reject (disabled)

log

log (disabled)

in

out

first match

last match

Règles DMZ

Règles de pare-feu DMZ

- Lobby
- Reporting
- System
- Interfaces
- Firewall
  - Aliases
  - Automation
  - Categories
  - Groups
  - NAT
  - Rules
  - Floating
  - DMZ
  - LAN
  - WAN
  - Shaper
  - Settings
  - Log Files
  - Diagnostics
- VPN
- Services
- Power
- Help

|                               | Protocol        | Source          | Port             | Destination     | Port              | Gateway | Schedule | Description                                     |                |
|-------------------------------|-----------------|-----------------|------------------|-----------------|-------------------|---------|----------|-------------------------------------------------|----------------|
| Automatically generated rules |                 |                 |                  |                 |                   |         |          |                                                 |                |
| <input type="checkbox"/>      | IPv4 TCP        | *               | *                | *               | 443 (HTTPS)       | *       | *        | Autorise la connexion a internet                |                |
| <input type="checkbox"/>      | IPv4 TCP        | *               | *                | *               | 80 (HTTP)         | *       | *        | Autorise la connexion a internet                |                |
| <input type="checkbox"/>      | IPv4 ICMP       | 10.31.248.53/32 | *                | 8.8.8.8/32      | *                 | *       | *        | Autorise les ping                               |                |
| <input type="checkbox"/>      | IPv4 ICMP       | 10.31.248.54/32 | *                | 8.8.8.8/32      | *                 | *       | *        | Autorise les ping                               |                |
| <input type="checkbox"/>      | IPv4 UDP        | 10.31.248.53/32 | *                | 8.8.4.4/32      | 53 (DNS)          | *       | *        | Autorise le dns vers 8.8.4.4                    |                |
| <input type="checkbox"/>      | IPv4 UDP        | 10.31.248.54/32 | *                | 8.8.4.4/32      | 53 (DNS)          | *       | *        | Autorise le dns vers 8.8.4.4                    |                |
| <input type="checkbox"/>      | IPv4 UDP        | 10.31.248.54/32 | *                | 8.8.8.8/32      | 53 (DNS)          | *       | *        | Autorise le dns vers 8.8.8.8                    |                |
| <input type="checkbox"/>      | IPv4 UDP        | 10.31.248.53/32 | *                | 8.8.8.8/32      | 53 (DNS)          | *       | *        | Autorise le dns vers 8.8.8.8                    |                |
| <input type="checkbox"/>      | IPv4 UDP        | 10.31.248.67/22 | *                | 10.31.240.67/22 | 67                | *       | *        | J'autorise la communication entre dhcp et relay |                |
| <input type="checkbox"/>      | IPv4 UDP        | 10.31.248.68/22 | *                | 10.31.240.68/22 | 67                | *       | *        | J'autorise la communication entre dhcp et relay |                |
| <input type="checkbox"/>      | IPv4 ICMP       | *               | *                | LAN net         | *                 | *       | *        |                                                 |                |
| <input type="checkbox"/>      | IPv4 ICMP       | 10.31.248.53/32 | *                | 10.31.240.80/32 | *                 | *       | *        |                                                 |                |
| <input type="checkbox"/>      | IPv4 UDP        | 10.31.248.80/32 | *                | 10.31.240.34/32 | 3306              | *       | *        |                                                 |                |
| <input type="checkbox"/>      | IPv4 UDP        | 10.31.248.80/32 | *                | 10.31.240.33/32 | 3306              | *       | *        |                                                 |                |
| <input type="checkbox"/>      | IPv4 TCP        | DMZ net         | *                | 10.31.240.73/32 | 22 (SSH)          | *       | *        |                                                 |                |
| <input type="checkbox"/>      | IPv4 TCP        | DMZ net         | *                | 10.31.240.74/32 | 22 (SSH)          | *       | *        |                                                 |                |
| <input type="checkbox"/>      | IPv4 ICMP       | *               | *                | WAN net         | *                 | *       | *        | ping du dmz au waan                             |                |
| <input type="checkbox"/>      | IPv4 ICMP       | *               | *                | LAN net         | *                 | *       | *        | ping du DMZ au LAN                              |                |
|                               | pass            |                 |                  |                 |                   |         |          |                                                 |                |
|                               | nass (disabled) |                 | block            |                 | reject            |         |          |                                                 | log            |
|                               |                 |                 | block (disabled) |                 | reject (disabled) |         |          |                                                 | log (disabled) |
|                               |                 |                 |                  |                 |                   |         |          |                                                 | in             |
|                               |                 |                 |                  |                 |                   |         |          |                                                 | out            |
|                               |                 |                 |                  |                 |                   |         |          |                                                 | first match    |
|                               |                 |                 |                  |                 |                   |         |          |                                                 | last match     |

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

Permanent link:  
[https://sisr2.beaupeyrat.com/doku.php?id=sisr2-usa:installation\\_routeur\\_pare-feu\\_opnsense](https://sisr2.beaupeyrat.com/doku.php?id=sisr2-usa:installation_routeur_pare-feu_opnsense)

Last update: 2026/03/09 13:00

