Brette Morgane BTS SIO 2

2024/2025

Guide d'installation du pare-feu OPNsense



Table des matières

1.	Qu'est-ce qu'OPNsense?	2
	1.1 OPNsense qu'est-ce que c'est	3
	1.2 Quels sont les fonctions et avantages d'OPNsense?	3
2	Pré-requis et clé usb	5
	2.1 Prérequis	5
	2.2 Téléchargement de l'ISO	6
	2.3 Création clé usb bootable	6
3.	Installation	8
	3.1 Suivre les étapes :	8
	3.2 Début du processus d'installation d'OPNsense	9
3.	Assigner les interfaces	12

1.1 OPNsense qu'est-ce que c'est?

1.1 OPNsense qu'est-ce que c'est?

OPNsense est système d'exploitation basé sur FreeBSD, intégrant des fonctionnalités de sécurité avancées, et conçu pour être utilisé comme pare-feu et routeur.

1.2 Quels sont les fonctions et avantages d'OPNsense?

→pare-feu avancé

Le pare-feu de dernière génération mis en place par OPNsense est basé sur *Packet Filter*. Ce pare-feu apporte donc une gestation facile du trafic réseau.

→VPN intégré

OPNsense comprend plusieurs VPN (virtual private network) intégrés, comme IPsec (Internet Protocol security), WireGuard, et d'autres, dont la mise en place permet une connexion sécurisée, et privative, d'un utilisateur voulant se connecter à distance à un autre réseau.

→Mises à jour régulières (deux versions majeures par an)

OPNsense est un système d'exploitation qui est mis à jour régulièrement, afin de maintenir le système stable, de corriger de potentielles vulnérabilités, ou d'ajouter des nouvelles fonctionnalités. Actuellement, OPNsense a sorti sa version 25.1, mais dans ce guide d'installation nous utiliserons la version 24.7.

→Open Source

Cela signifie que le code source est accessible sans avoir la nécessité de payer, et qu'on peut l'exploiter librement.

De ce fait, OPNsense est un pare-feu qu'on peut télécharger gratuitement.

\rightarrow Interface Web intuitive

L'interface Web d'OPNsense nous permet de gérer, et configurer facilement les différentes fonctionnalités d'OPNsense.

→Extensions et plugins

Selon l'usage qu'on fait d'OPNsense, il est possible de rajouter des fonctionnalités qui nous sont nécessaires, comme un Proxy (Squid), visualiseur/analyste de trafic réseau (Ntopng).

→DHCP

OPNsense est doté d'un Dynamic Host Configuration Protocol qui va attribuer automatiquement une adresse IP aux appareils qui vont se connecter au réseau local.

\rightarrow Netflow

OPNsense comporte un Protocole de collecte de données de trafic réseau appelé Netflow.

\rightarrow Service NTP

OPNsense comporte un protocole de synchronisation réseau), servant à synchroniser de manière fiable via un réseau informatique, l'heure locale sur le pare-feu, les ordinateurs, (...).

\rightarrow Système de détection et de prévention d'intrusion (IDS/IPS)

OPNsense nous propose aussi un système de détection et de prévention d'intrusion (IDS/IPS) appelé Suricata, analysant en temps réel le trafic réseau pour identifier et bloquer les menaces.

2. Pré-requis et clé usb

2.1 Prérequis

Prérequis :

→Serveur physique à X interfaces sur lequel installé OPNsense

→ Matériel configuration RAID1¹ est souhaitable

→Clé ubs bootable de 8 Go minimum afin de télécharger, et contenir l'iso d'OPNsense

Ce tableau résume les ressources minimales, et recommandées pour la production. Toutefois, cela dépendra de l'utilisation qu'on attendra, et fera d'OPNsense.

CARACTÉRISTIQUES	MINIMUM	RECOMMANDATION
Processeur	1 GHz - 2 cœurs	1.5 GHz - Multi-coeurs
Mémoire vive (RAM)	2 Go	8 Go
Espace de stockage pour le système	Disque dur, disque SSD ou carte SD (4 Go)	120 Go en SSD

¹ Le principe du RAID1 est que les données sont dupliquées sur deux disques (miroir). De ce fait, il a pour avantage une tolérance de panne d'un disque. Mais, l'inconvénient est que la capacité est divisée par deux, et il n'y pas d'amélioration de performance notable. Alors, le RAID1 est utilisé pour les données critiques, serveurs.

2.2 Téléchargement de l'ISO

Depuis https://opnsense.org/download/télécharger l'iso « vga² »

Nous choisissons VGA, car l'installation s'depuis une clé usb bootable vers une machine physique.



Il n'y a pas besoin de modifier le système d'architecture « am64 », ainsi que le miroir de localisation « Mirror Location ».

2.3 Création clé usb bootable

→ Préparer la clé usb (au moins 8 Go + formater en FAT32)

→Graver l'iso sur la clé usb à l'aide un outil comme Rufus pour Windows 1 Brancher la clé usb

→Ouvrir Rufus³

→Sélectionner l'ISO d'OPNsense

→ Choisir le mode « écriture en Disk Image » (DD)

→Démarrer la clé usb

² Video Graphics Array, c'est une image conçue pour être utilisée sur un appareil avec un écran et un clavier physique.

³ Rufus est un logiciel permettant de créer des supports bootable (live USB) sur un périphérique externe comme une clé USB.

 \rightarrow L'insérer dans le serveur destiné à recevoir l'installation d'OPNsense

→Accéder au BIOS/UEFI et choisir USB Boot

→Démarrer la clé et suivre les instructions d'installation

OPNsense-24.7-dvd-amd64.iso.bz2

3. Installation

3.1 Suivre les étapes :

Une page d'accueil visible. Laisser le processus se poursuivre afin que l'image d'OPNsense se charge sur le serveur.

1. Boot Malti user (Enter) 2. Boot Single user 3. Escape to loader prompt 4. Reboot 5. Cons: Video Options: 6. Mernel: default/kernel (1 of 1) 7. Boot Options	00000000000000000000000000000000000000		
Autoboot in R seconds. [Space] to pause Loading kernel /boot/kernel/kernel text=Rx1013eR text=Rx801 ata=Rx196dcR=Rx469240 a	24.7 ''Thris 210 toxt=Rx45595c d	ving Tigor'' ! Lata=0×100+0×000 d	

La disposition du clavier par défaut dans OPNsense est en anglais (qwerty US) et non en français (azerty)

→rentrer le login par défaut: installer

→rentrer le mot de passe par défaut : **opnsense**

>>> Invoking s >>> Invoking s Service 'sysc >>> Invoking s Root file syst Tue Oct 22 15	start script 'openvpn' start script 'sysctl' tl' has been restarted. start script 'beep' tem: /dev/iso9660/OPNSENSE_INSTALL :25:36 UTC 2024
*** OPNsense.)	localdomain: OPNsense 24.7 ***
LAN (emØ)	-> v4: 192.168.1.1/24
HTTPS: sha256	6 45 8A 7B 30 10 5D 60 27 83 41 8C 45 F1 DB F5 6C A5 C0 87 3E 2B 48 85 1D CE 18 EE 71 DD 53 08 EF
SSH : SHA256 SSH : SHA256 SSH : SHA256	6 bQ4x0HNUh18e+PW+iksN6u0GJtSU0x1E5fRe7nsy3yw (ECDSA) 6 lefjNf2O5PVApZYju+L3YAFpphABiqo9ccaK9U0zJAg (ED25519) 6 InncN/Auq8AeqjrshXZ3b6C21LUpQRi3uh1GAuQ6HxA (RSA)
Welcome! OPNs login as 'root	sense is running in live mode from install media. Please t'to continue in live mode, or as 'installer' to start thá
installation. both accounts.	Use the default or previously-imported root password for . Remote login via SSH is also enabled.
FreeBSD/amd64	(DPNsense.localdomain) (ttyvØ)
login:	

3.2 Début du processus d'installation d'OPNsense

Il faut choisir la langue :

 \rightarrow « () French accent keys » afin d'avoir la langue française avec accent \rightarrow Clavier Azerty en appuyant sur « espace ».

keyboard мар. Other keyмaps can be chosen below. >>> Continue with fr.kbd keyмap -> Test fr.kbd keymap () Hrmenian phonetic layout () Belgian () Belgian () Belgian (accent keys) () Brazilian (accent keys) () Brazilian (accent keys) () Brazilian (accent keys) () Bulgarian (BDS) () Bulgarian (BDS) () Bulgarian (BDS) () Contral European 	Rephap Selection		
<pre>>>> Continue with fr.kbd keymap >- Test fr.kbd keymap () Armenian phonetic layout () Belgian () Belgian (accent keys) () Brazilian (accent keys) () Brazilian (accent keys) () Brazilian (without accent keys) () Bulgarian (BDS) () Bulgarian (Phonetic) () Canadian Bilingual () Central European +(<) [Press arrows, TAB or ENTER]</pre>		keyboard мap. Other keyмaps can be chosen below.	
<pre>C Armenian phonetic layout C) Belgian C) Belgian C) Belgian C) Belgian C) Belgian (accent keys) C) Brazilian (accent keys) C) Brazilian (without accent keys) C) Bulgarian (BBS) C) Bulgarian (BBS) C) Bulgarian (Phonetic) C) Canadian Bilingual C) Central European</pre>		>>> Continue with fr.kbd keymap	
<pre>() Belarusian () Belgian () Belgian (accent keys) () Brazilian (accent keys) () Brazilian (without accent keys) () Brazilian (without accent keys) () Bulgarian (BBS) () Bulgarian (Phonetic) () Canadian Bilingual () Central European</pre>		() Armenian phonetic layout	
<pre>() Belgian () Belgian (accent keys) () Brazilian (accent keys) () Brazilian (without accent keys) () Bulgarian (BDS) () Bulgarian (Phonetic) () Canadian Bilingual () Central European </pre>		() Belarusian	
<pre>() Belgian (accent keys) () Brazilian (accent keys) () Brazilian (without accent keys) () Bulgarian (BDS) () Bulgarian (Phonetic) () Canadian Bilingual () Central European</pre>		() Belgian	
<pre>() Brazilian (accent keys) () Brazilian (without accent keys) () Bulgarian (BDS) () Bulgarian (Phonetic) () Canadian Bilingual () Central European</pre>		() Belgian (accent keys)	
<pre>() Brazilian (Without accent keys) () Bulgarian (BDS) () Bulgarian (Phonetic) () Canadian Bilingual () Central European</pre>		() Brazilian (accent keys)	
C) Bulgarian (Phonetic) () Canadian Bilingual () Central European () () Cancel> [Press arrows, TAB or ENTER]		() Brazilian (without accent keys)	
() Canadian Bilingual () Central European () Central European () Cancel> [Press arrows, TAB or ENTER]		() Bulgarian (Bbo)	
Contral European ()) Central European ()) Cancel> [Press arrows, TAB or ENTER]		C) Canadian Bilingual	
L(A)		() Central European	
Cancel> [Press arrows, TAB or ENTER]			
Cancel> [Press arrows, TAB or ENTER]			
		<pre><cancel></cancel></pre>	
		LPress arrows, IHB or ENTERI	

Désormais, la langue du clavier par défaut est en français.

Maintenant, il faut choisir « Stripe⁴ », car notre serveur OPNsense est doté d'un seul disque. Ici il s'agit de choisir l'option de configuration de stockage des données qui dépend de l'architecture matériel de la machine.

→Appuyer sur « ENTREE » pour valider le « Ok », et confirmer les disques d'installation FreeBSD Installer



⁴ *Stripe* (RAID0), car serveur est doté d'un seul disque, donc impossible de faire de la redondance nécessitant plusieurs disques pour dupliquer les données. C'est un souci en ce qui concerne la tolérance aux pannes, car si le disque tombe en panne, toutes les données sont perdues, soit un risque de perte des données très élevé. *Mirroring* est le fait que chaque donnée est copiée à l'identique sur 2 disques (RAID1), offrant une meilleure tolérance aux pannes.

Appuyer juste sur « Entrée » afin de valider

FreeBSD Installer		
	ZFS Configuration	
	[*] 1a0 UMware, UMware Virtual S	
	COR < Back >	

Appuyer juste sur « Entrée » afin de valider

FreeBSD Insta	ller
	ZFS Configuration Last Chance! Are you sure you want to destroy the current contents of the following disks: da0
	CYES > < NO > [Press arrows, TAB or ENTER]

Attendre que l'installation se finisse

Installatio	n Progress	1_
Cloning current system	۲ 📃	17%]
Overall Progress	13%	

Ici possibilité de modifier le mot de passe root.

→ Choisir « Root Password » > Appuyer sur « ENTREE »



Renseigner le nouveau mot de passe

→ Sélectionner « Ok » > Appuyer sur « ENTREE »

→ Sélectionner « Complete Install » et valider.

Maintenant attendre que le serveur redémarre

The installation finished successfully. After reboot, open a web browser and navigate to https://192.168.1.1 (or the LAN IP address). The console can also be used to set a different LAN IP. Your browser may report the HTTPS certificate as untrusted and ask you to accept it. This is normal, as the default certificate will be self-signed and cannot be validated by an external root authority. Rebooting in 5 seconds. CTRL-C to abort.....

4. Assigner les interfaces

```
Rentrer le nombre 1 pour « 1) Assign interfaces<sup>5</sup> »
```

```
*** OPNsense.localdomain: OPNsense 24.7.12_4 (amd64) ***
LAN (em1)
                 ->
                   v4: 10.0.1.4/26
OPT1 (em2)
                 ->
OPT2 (em3)
                    v4: 192.168.10.100/24
WAN (em0)
HTTPS: sha256 E4 32 E8 F7 FA 93 7E 64 53 46 D9 9D 6C C3 6B 8A
               BD 53 5B 9D E8 7F B8 E4 3C 06 4D 1E AF 85 83 D9
  0) Logout
                                          7) Ping host
                                          8) Shell
  1) Assign interfaces
                                          9) pfTop
  2) Set interface IP address
                                         10) Firewall log
  3) Reset the root password
  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:
```

→Rentrer « N » pour « Do you want to configure LAGGs now »

*Sert à regroupement de plusieurs interfaces réseau pour améliorer la redondance ou la bande passante, pas utile dans notre cas (plus dans un environnement professionnel avancé) →Rentrer « N » pour « Do you want ton configure VLANs now ?

*Utile uniquement si on gère plusieurs sous-réseaux isolés sur une même carte réseau

```
0) Logout
                                           7) Ping host
  1) Assign interfaces
                                          8) Shell
                                          9) pfTop
10) Firewall log
 2) Set interface IP address
 3) Reset the root password
 4) Reset to factory defaults
                                          11) Reload all services
     Power off system
 5)
                                          12) Update from console
 6) Reboot system
                                          13) Restore a backup
Enter an option: 1
Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n
```

⁵ Cela va servir à attribuer manuellement les interfaces réseau (ex : LAN, WAN, DMZ...) aux interfaces physiques détectées sur notre système (comme em0, em1, em2, ...).

Ici sont affichées les interfaces valides, il y en a 4 au total, car OPNsense a détecté 4 interfaces réseau valides sur notre serveur physique nommés em0, em1, (...). Ces derniers correspondent par la suite à l'interface WAN, LAN, DMZ, et WIFI.

Valid interfaces	are:				
ем0 ем1	00:0c:29:b4:0c:c2 Intel(R) Legacy PRO/1000 MT 82545EM (Copper) 00:0c:29:b4:0c:cc Intel(R) Legacy PRO/1000 MT 82545EM (Copper)				
ем2 ем3	00:0c:29:b4:0c:d6 Intel(R) Legacy PRU/1000 MT 82545EM (Copper) 00:0c:29:b4:0c:e0 Intel(R) Legacy PRO/1000 MT 82545EM (Copper)				
If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.					
Enter the WAN int	terface name or 'a' for auto-detection:				

Sur certaines machines physiques il ne faut pas modifier le nom de l'interface⁶. Nous allons configurer l'interface du WAN⁷ en rentrant le nom qu'on souhaite lui attribuer, ici em0.

Enter the WAN interface name or 'a' for auto-detection: em0

Maintenant on assigne l'interface LAN en « em1 » puis les deux autres interfaces restantes, qu'on pourra nommer par la suite DMZ, et WIFI.

« This enables full Firewalling/NAT mode » signifie que OPNsense active automatiquement le NAT pour que tout ce qui vient de LAN puisse sortir via l'interface WAN, comme un routeur classique.

Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (or nothing if finished): em1 Enter the Optional interface 1 name or 'a' for auto-detection (or nothing if finished): em Invalid interface name 'em' Enter the Optional interface 1 name or 'a' for auto-detection

(or nothing if finished): em3

⁶ Les noms des interfaces sont attribués automatiquement par le noyau FreeBSD (sur lequel OPNsense est basé). Alors, si on les modifie, ou qu'on force un renommage cela peut entraîner des erreurs de détection ou d'initialisation des interfaces au démarrage.

⁷ World Area Network, la WAN est configurée en première, car elle connecte le pare-feu à Internet ou à un autre routeur, et la définir en premier permet d'accéder aux mises à jour dès l'installation, de synchroniser l'heure (NTP), (...). La WAN est également le point critique de sécurité et de connectivité. La configurer en premier garantit que tout ce qui vient d'Internet est bien identifié, analysé, ou bloqué. La configuration suit également la logique de « l'extérieur vers l'intérieur », c'est-àdire WAN (point d'entrée externe) puis LAN (réseau de confiance), (...).

Explique comment les interfaces ont été assignées →OPT1 correspond à la DMZ →OPT2 au WIFI →Ecrire « y » pour confirmer qu'on veut procéder de cette façon The interfaces will be assigned as follows:

WAN -> em0 LAN -> em1 OPT1 -> em2 OPT2 -> em3 Do you want to proceed? [y/N]:

Interfaces apparaître sous le nom qu'on leur a assigné.

*** OPNsense.localdomain: OPNsense 24.7.12_4 (amd64) *** LAN (em1) -> OPT1 (em2) -> ОРТ2 (емЗ) -> WAN (емØ) -> HTTPS: sha256 E4 32 E8 F7 FA 93 7E 64 53 46 D9 9D 6C C3 6B 8A BD 53 5B 9D E8 7F B8 E4 3C 06 4D 1E AF 85 83 D9 0) Logout 7) Ping host 1) Assign interfaces 8) Shell 9) pfTop 2) Set interface IP address Reset the root password
 Reset to factory defaults
 Power off system 10) Firewall log 11) Reload all services 12) Update from console 6) Reboot system 13) Restore a backup Enter an option: