Brette Morgane BTS SIO 2 **2024/2025**

Guide d’installation du pare-feu OPNsense

Table des matières

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.

→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.

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

→ **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, (…).

→ **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 RAID1[1] 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.

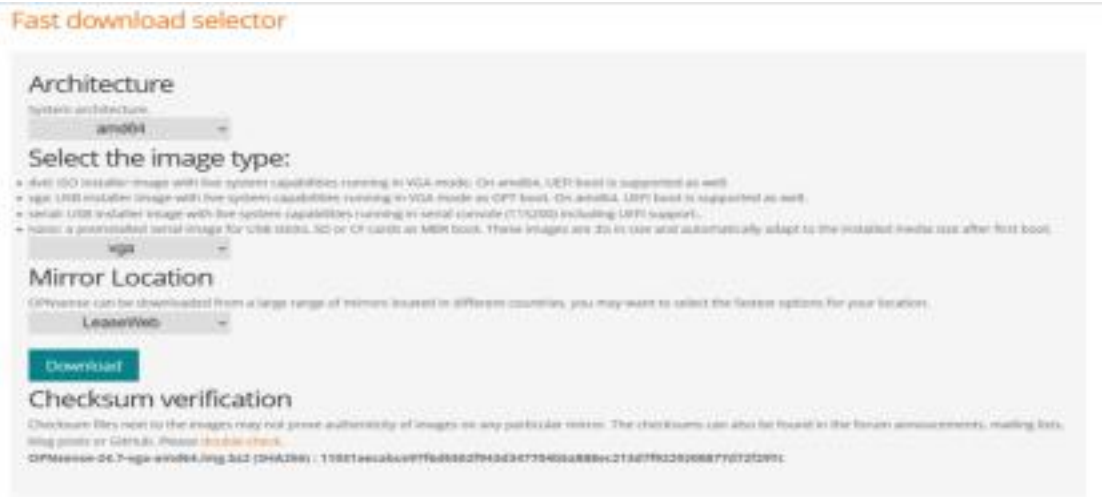
CARACTÉRISTIQUES	MINIMUM	RECOMMANDATION
Processeur	1 GHz - 2 cœurs	1.5 GHz - Multi-coeurs
Mémoire vive (RAM)	2 Go	8 Go
Espace de stockage pour le système	Disque dur, disque SSD ou carte SD (4 Go)	120 Go en SSD

[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 « vga[2] »

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 Rufus[3]

→Sélectionner l'ISO d'OPNsense

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

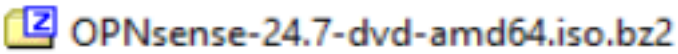
→Démarrer la clé usb

[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.

→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



3. Installation

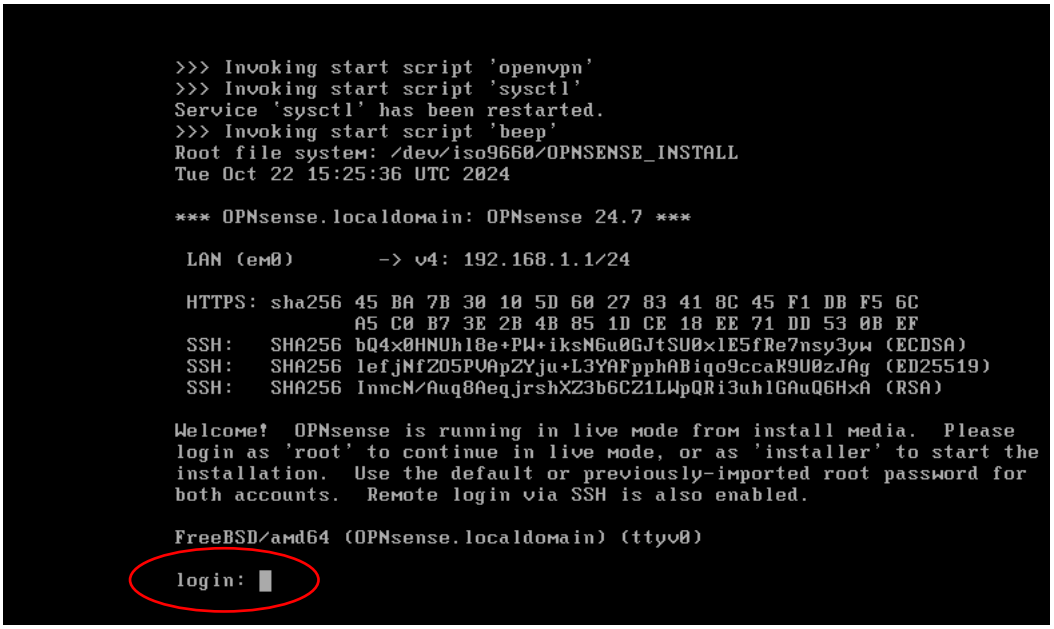
3.1 Suivre les étapes :

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

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

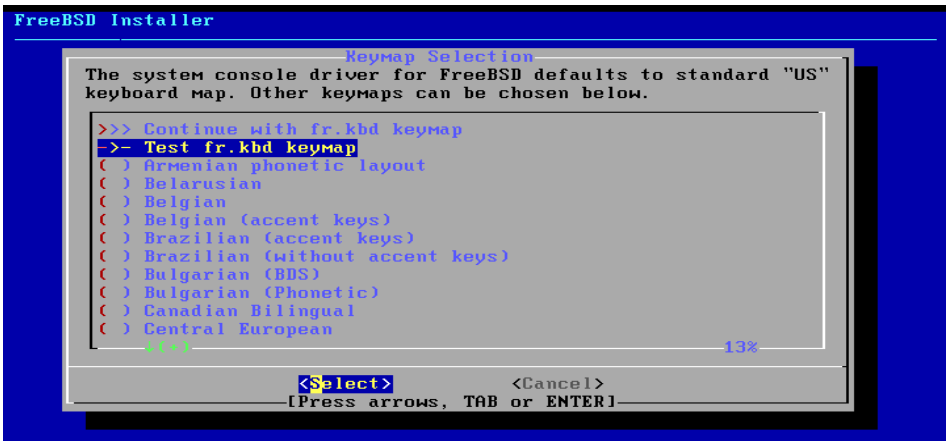
→rentrer le login par défaut: **installer**

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



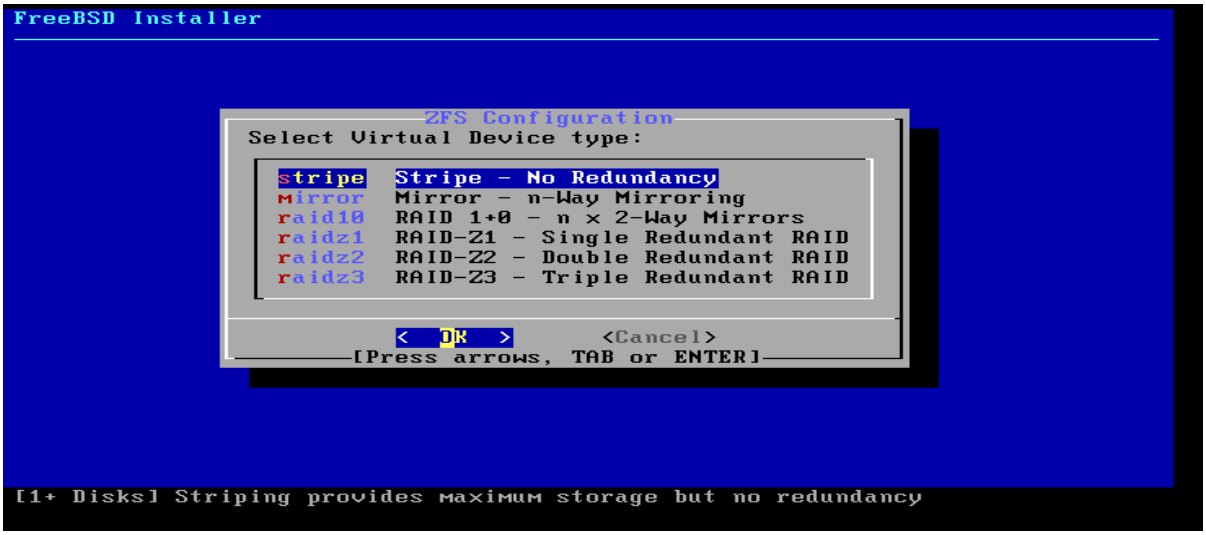
3.2 Début du processus d'installation d'OPNsense

Il faut choisir la langue :
→**« ( ) French accent keys »** afin d'avoir la langue française avec accent
→Clavier Azerty en appuyant sur « espace ».



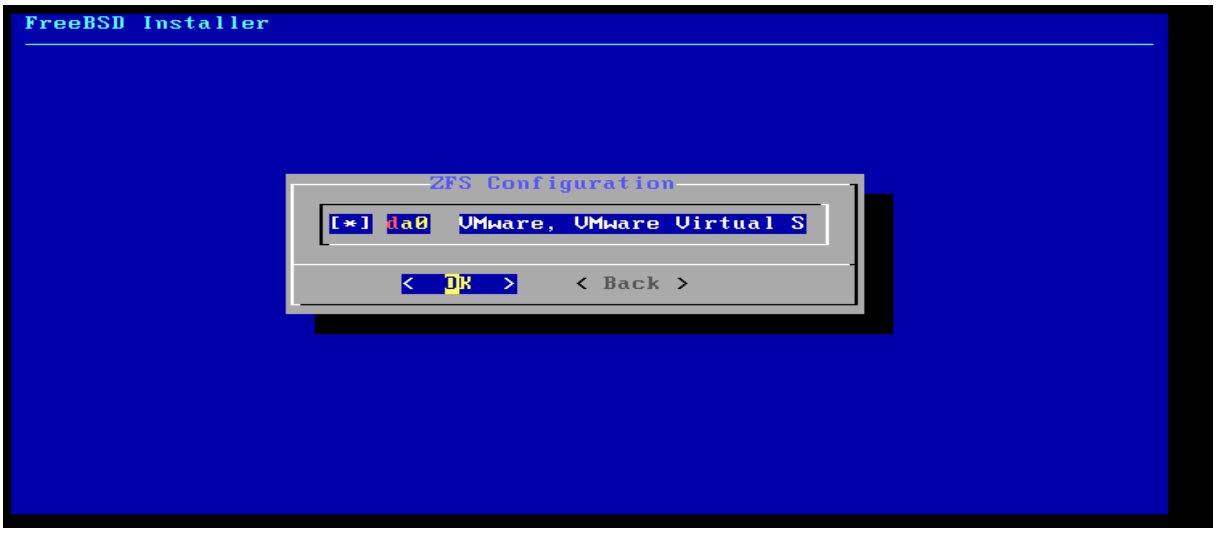
Désormais, la langue du clavier par défaut est en français.

Maintenant, il faut choisir « Stripe[4] », 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



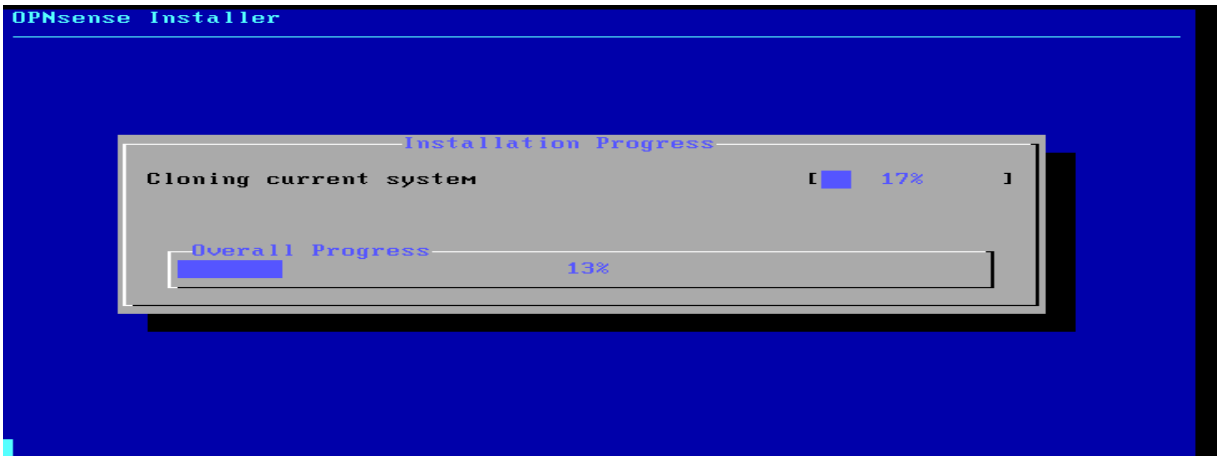
[4] *Stripe* (RAID0), car serveur est doté d'un seul disque, donc impossible de faire de la redondance nécessitant plusieurs disques pour dupliquer les données. C'est un souci en ce qui concerne la tolérance aux pannes, car si le disque tombe en panne, toutes les données sont perdues, soit un risque 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



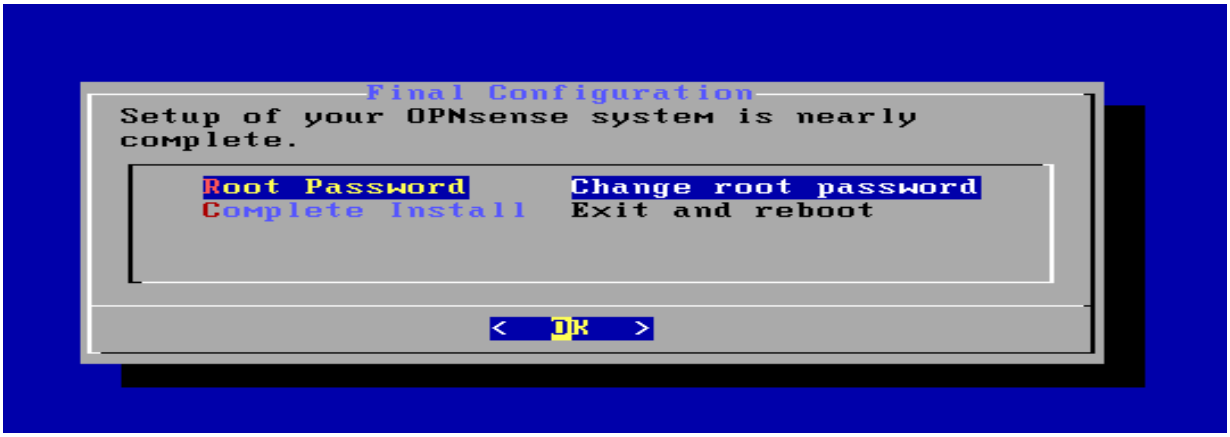
Appuyer juste sur « Entrée » afin de valider

Attendre que l'installation se finisse



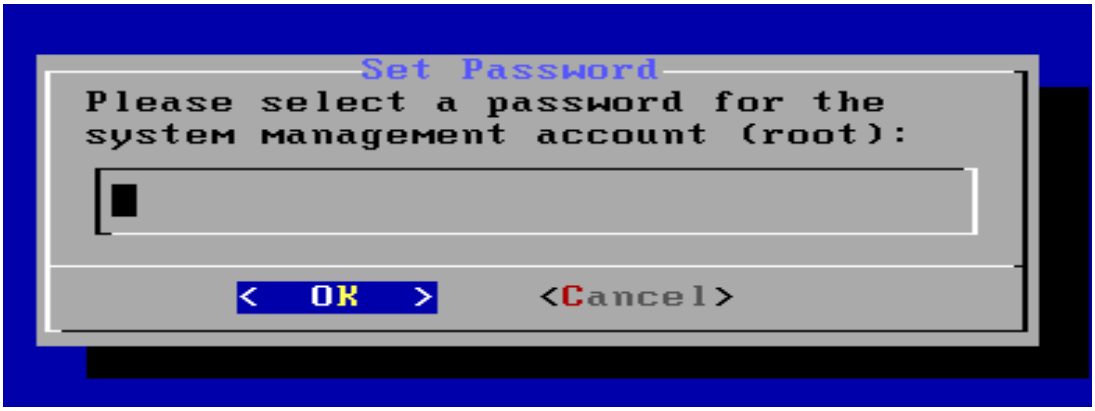
Ici possibilité de modifier le mot de passe root.

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



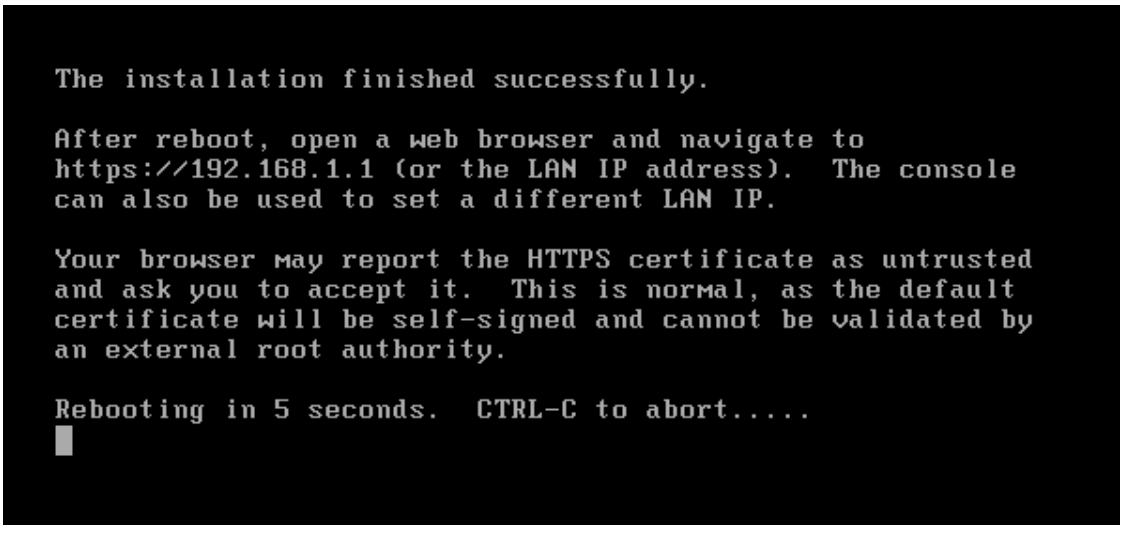
Renseigner le nouveau mot de passe

→ Sélectionner « Ok » > Appuyer sur « ENTREE »



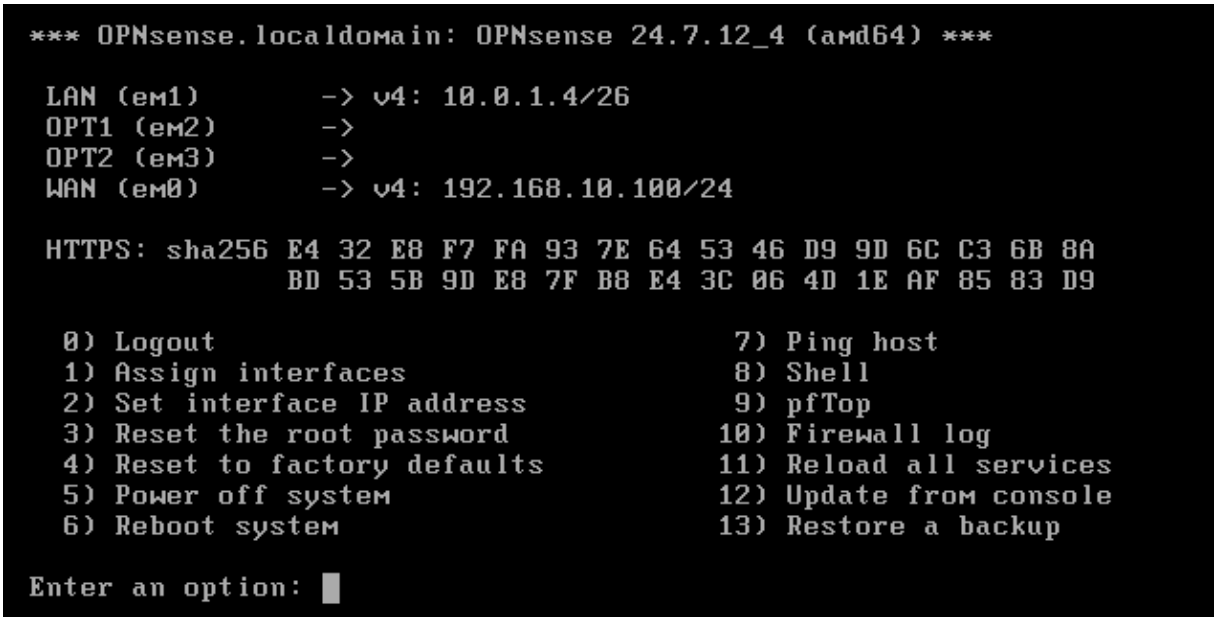
→ Sélectionner « Complete Install » et valider.

Maintenant attendre que le serveur redémarre

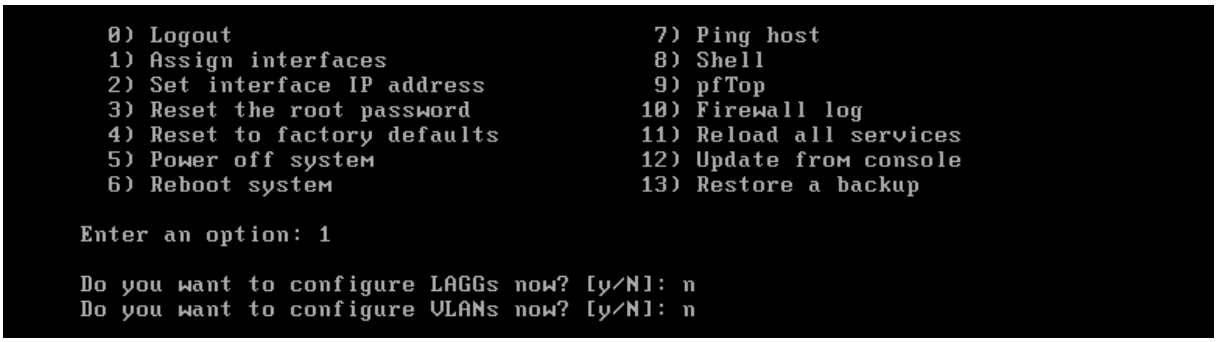


4. Assigner les interfaces

Rentrer le nombre 1 pour « 1) Assign interfaces[5] »

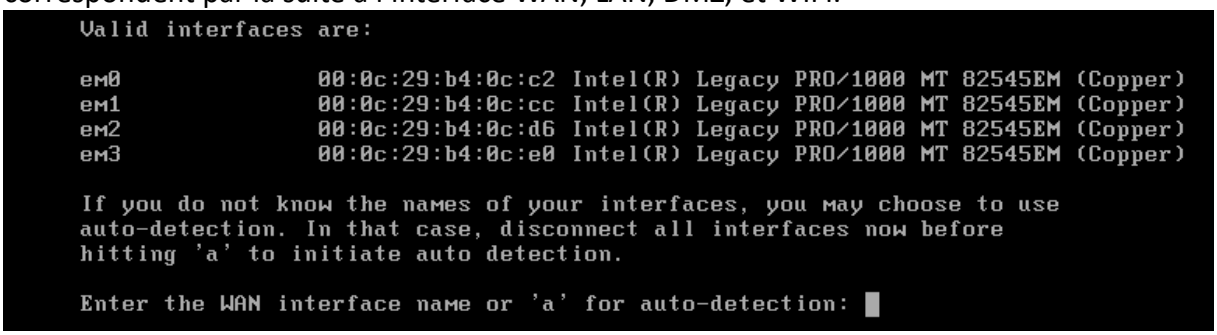


→Rentrer « N » pour « Do you want to configure LAGGs now »
*Sert à regroupement de plusieurs interfaces réseau pour améliorer la redondance ou la bande passante, pas utile dans notre cas (plus dans un environnement professionnel avancé)
→Rentrer « N » pour « Do you want ton configure VLANs now ?
*Utile uniquement si on gère plusieurs sous-réseaux isolés sur une même carte réseau

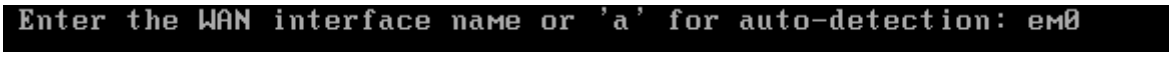


[5] Cela va servir à attribuer manuellement les interfaces réseau (ex : LAN, WAN, DMZ…) aux interfaces physiques détectées sur notre système (comme em0, em1, em2, …).

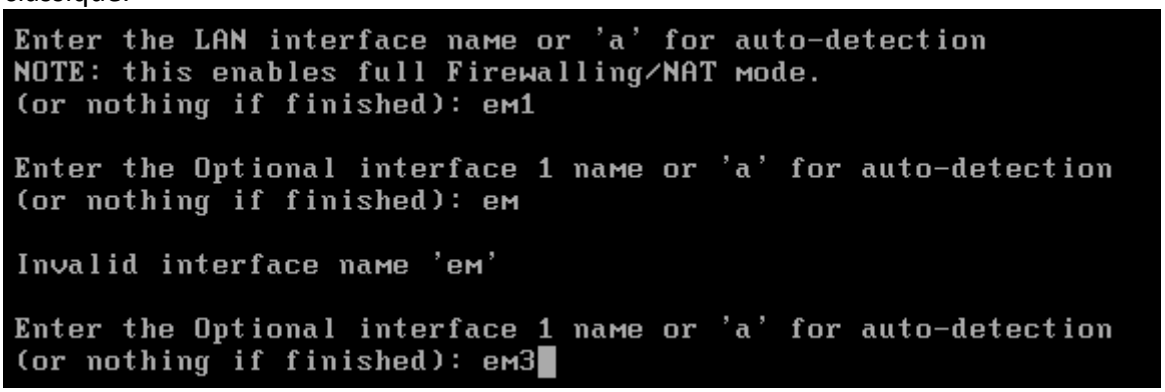
Ici sont affichées les interfaces valides, il y en a 4 au total, car OPNsense a détecté 4 interfaces réseau valides sur notre serveur physique nommés em0, em1, (…). Ces derniers correspondent par la suite à l'interface WAN, LAN, DMZ, et WIFI.



 sur certaines machines physiques il ne faut pas modifier le nom de l'interface[6].
Nous allons configurer l'interface du WAN[7] en rentrant le nom qu'on souhaite lui attribuer, ici em0.



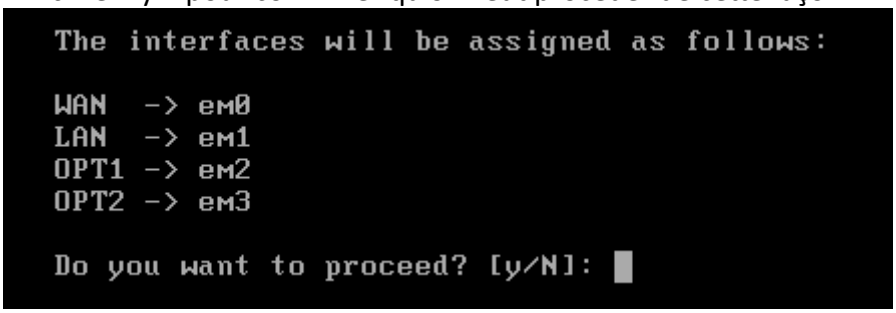
Maintenant on assigne l'interface LAN en « em1 » puis les deux autres interfaces restantes, qu'on pourra nommer par la suite DMZ, et WIFI.
« This enables full Firewalling/NAT mode » signifie que OPNsense active automatiquement le NAT pour que tout ce qui vient de LAN puisse sortir via l'interface WAN, comme un routeur classique.



[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-à-dire 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



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