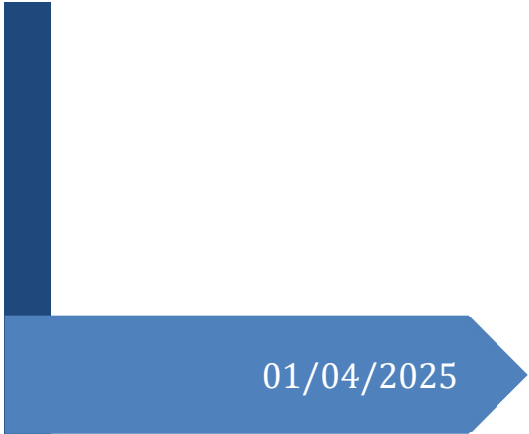
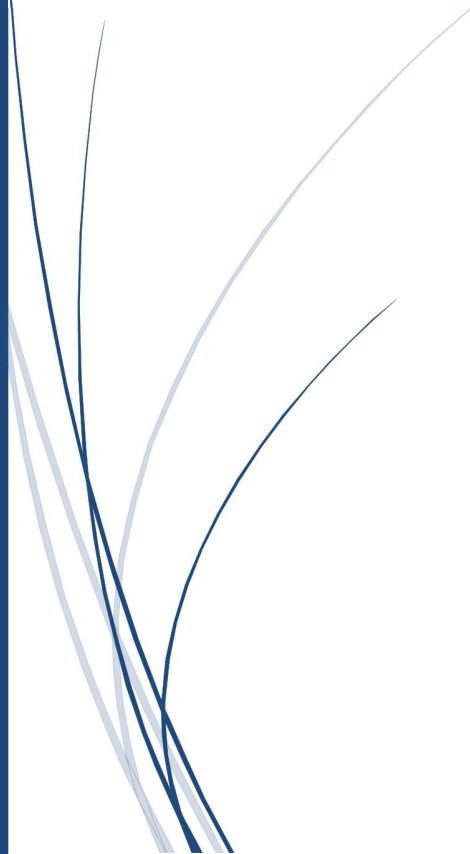


A thick dark blue vertical bar runs down the left side of the page. A medium blue arrow points to the right, overlapping the bar, with the date '01/04/2025' written inside it in white.

01/04/2025

INSTALLATION D'OPENSENSE

Several thin, curved lines in shades of blue and grey originate from the bottom left and sweep upwards and to the right, creating a sense of movement.

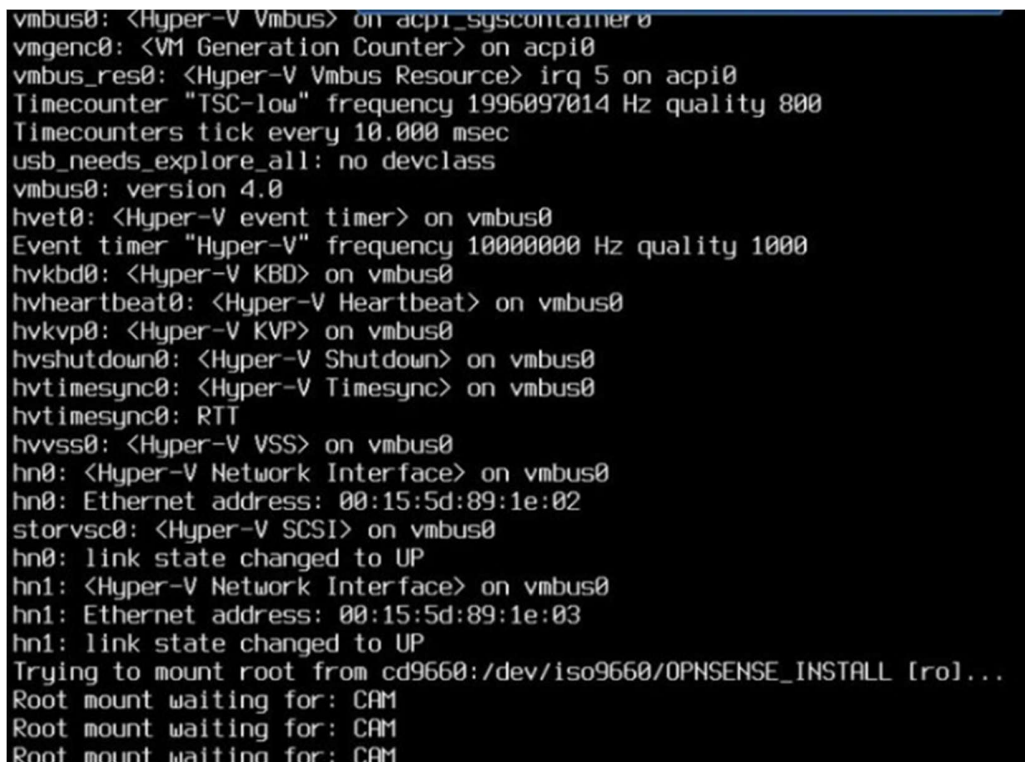
MASSIAS Rudy
KEYCE INFORMATIQUE – BTS SIO

A. Installer le système OPNsense

Démarrez la machine destinée à accueillir OPNsense. Vous devriez avoir une page d'accueil similaire à celle ci-dessous. Pendant quelques secondes, l'écran présenté sera visible dans la fenêtre. Laissez le processus se dérouler...



L'image OPNsense va être chargée sur la machine, afin que le système soit accessible en « live », c'est-à-dire qu'il est mis en mémoire de façon temporaire.



Puis, vous arrivez sur une interface similaire à celle ci-dessous. Connectez-vous à l'aide du login « installer » et du mot de passe « opnsense ». Attention, le clavier est en QWERTY pour le moment. À ce stade, nous allons commencer le processus d'installation d'OPNsense.

```
*** OPNsense.localdomain: OPNsense 24.1 ***

LAN (hn0)      -> v4: 192.168.1.1/24
WAN (hn1)      ->

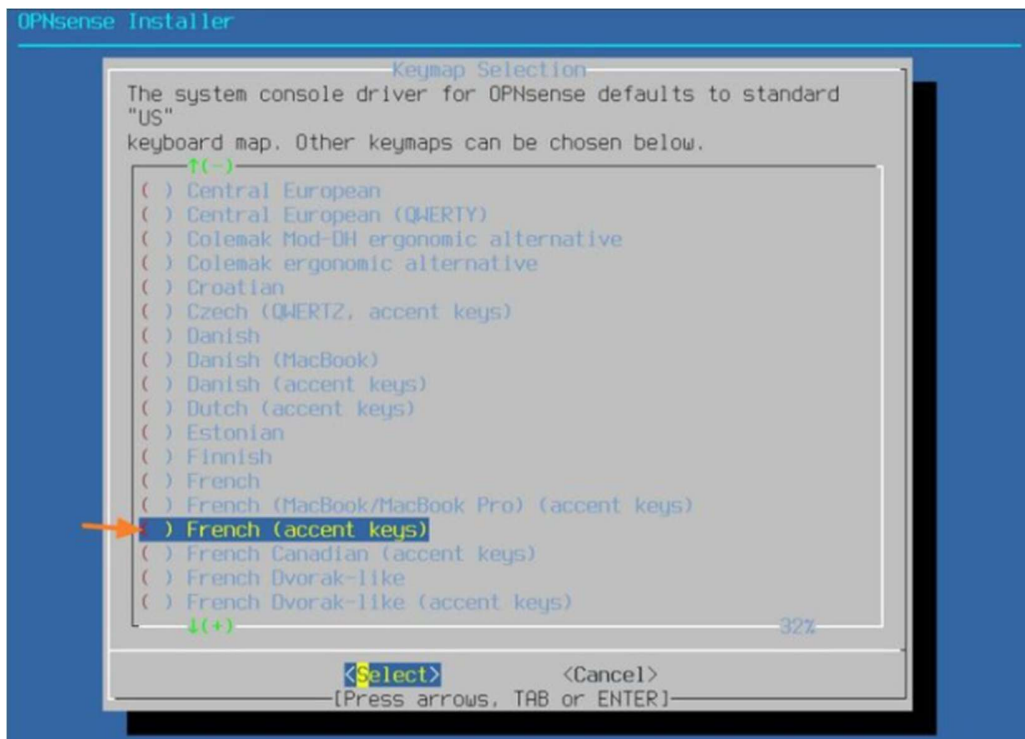
HTTPS: SHA256 FD 8E 22 31 FD 48 EB 5D 82 0D 50 A3 8C E6 BC 98
          0E 52 F6 F4 98 A6 2B FD B8 DA 6F EE 76 97 FF F7
SSH:   SHA256 9G6WH6/TF9ArZUQ6etE+CcTsPm6WCUnDIEE+wLy1Pj4 (ECDSA)
SSH:   SHA256 +cEb+hEOt/A18E38FxdxTQea1o0yTmZv20g+6V46QQ (ED25519)
SSH:   SHA256 1D+cmjkbkiUSazNYv0pArh73aH16Uc1oDSN7K1CQoEy8 (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.

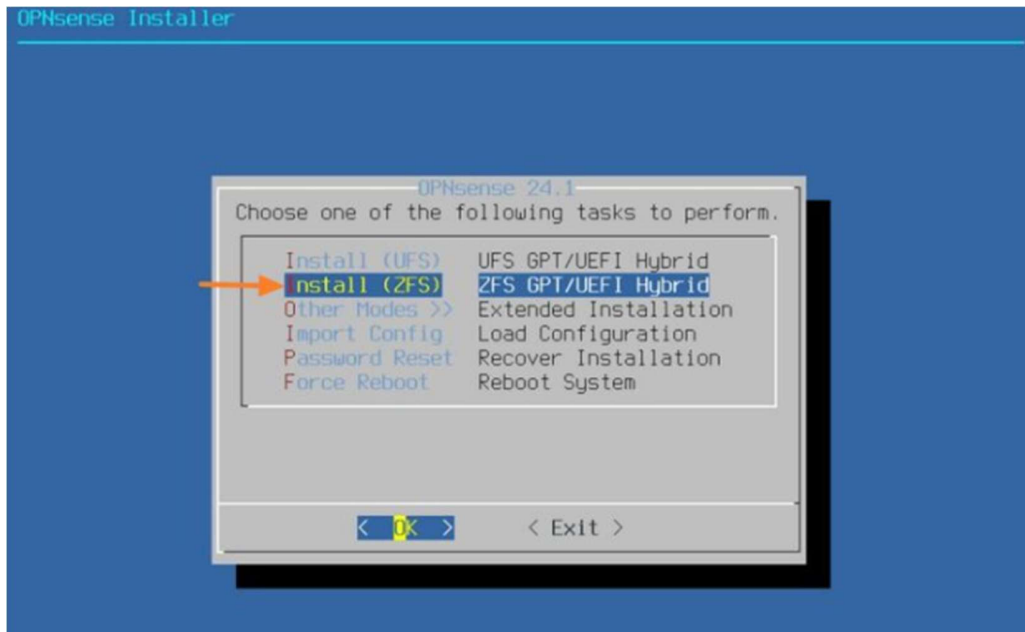
FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login: installer
```

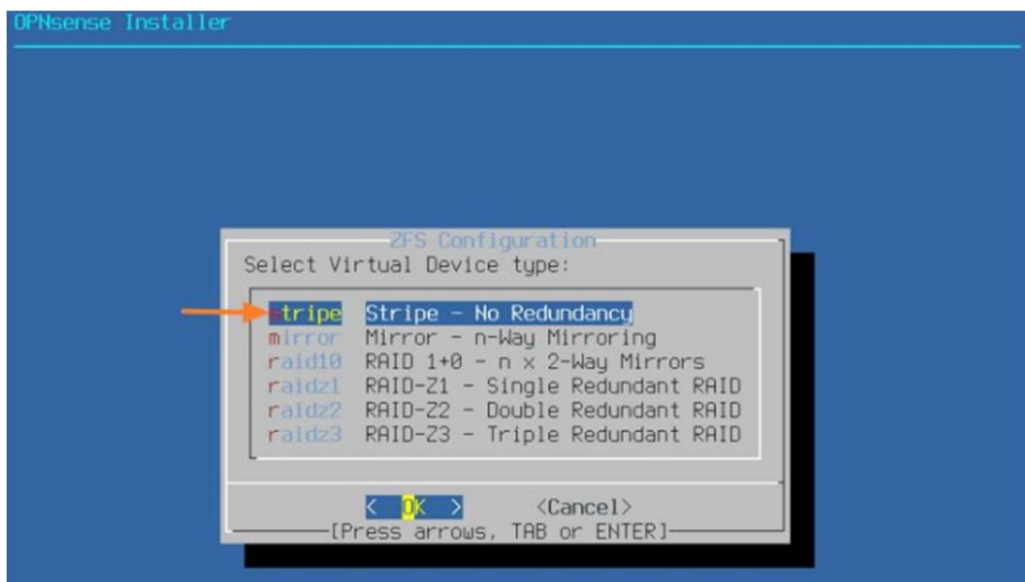
Un nouvel assistant s'affiche à l'écran. La première étape consiste à sélectionner la disposition du clavier correspondant à votre configuration. Pour un clavier AZERTY, sélectionnez l'option « French (accent keys) » dans la liste puis validez par deux fois.



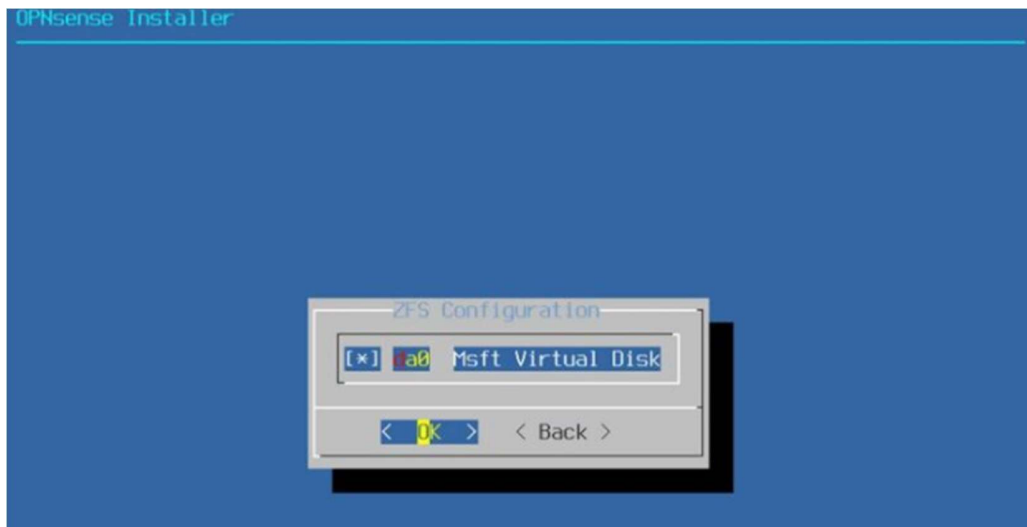
La seconde étape consiste à choisir la tâche à effectuer. Ici, nous allons effectuer une installation en utilisant le système de fichiers ZFS. Positionnez-vous sur la ligne « Install (ZFS) » et validez avec Entrée.



À la troisième étape, sélectionnez « stripe » puisque notre machine est équipée d'un seul disque : il n'y a pas de redondance possible pour sécuriser le stockage du pare-feu et ses données. Ceci est surtout pertinent lors de l'installation sur une machine physique pour se prémunir contre une panne matérielle d'un disque, via le principe du RAID.



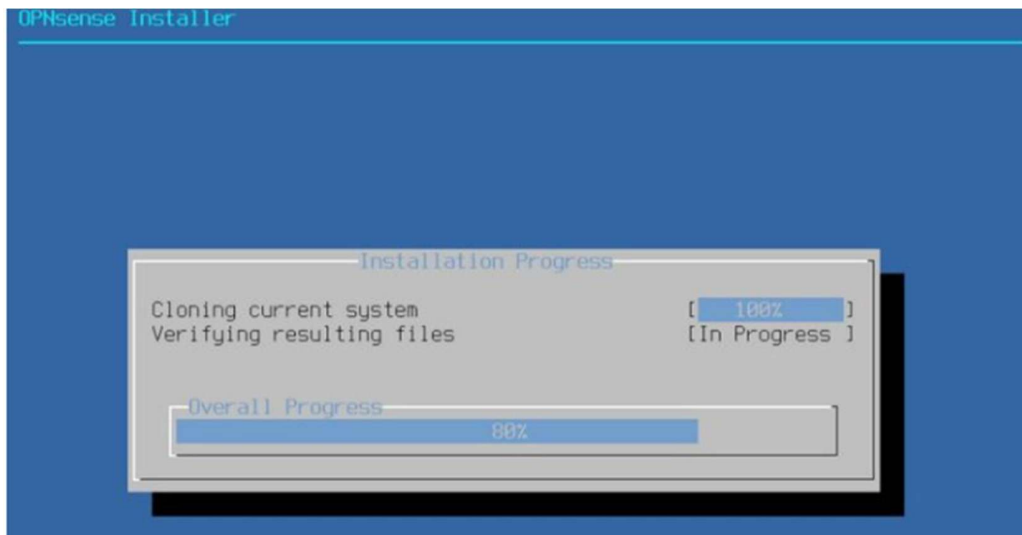
À la 4ème étape, appuyez simplement sur Entrée pour valider.



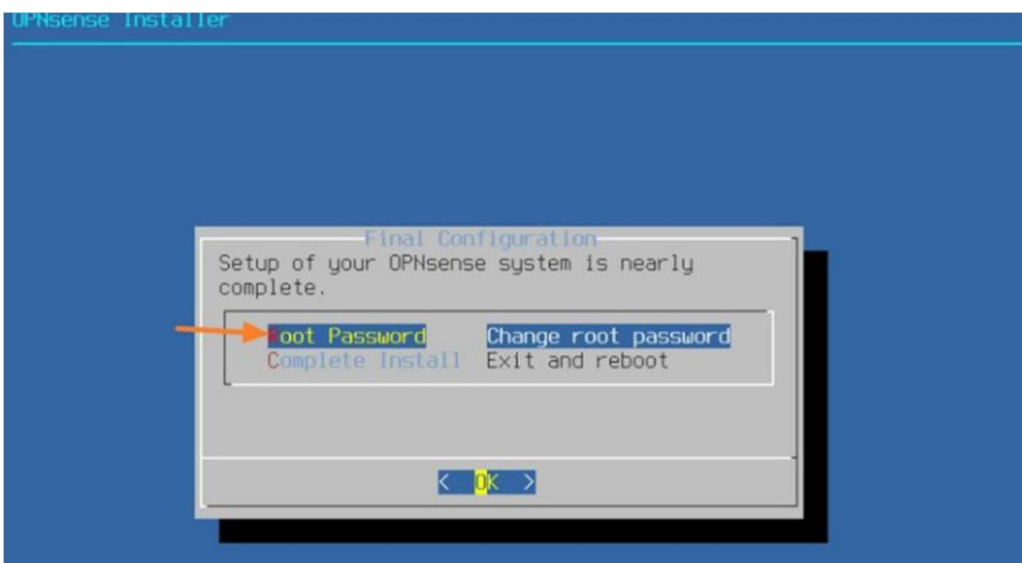
Enfin, validez en sélectionnant « YES » puis avec la touche Entrée.



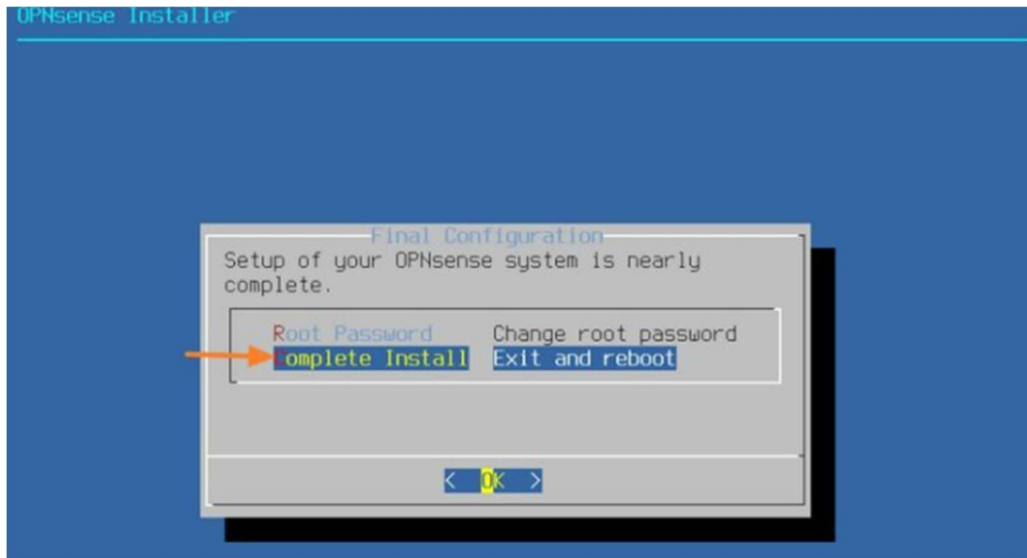
Désormais, vous devez patienter pendant l'installation d'OPNsense... Ce processus nécessite environ 5 minutes.



Une fois l'installation terminée, nous pouvons changer le mot de passe « root » avant de redémarrer. Sélectionnez « Root Password », appuyez sur Entrée et indiquez un mot de passe « root » par deux fois.



Enfin, sélectionnez « Complete Install » et appuyez sur Entrée. Profitez-en pour éjecter le disque du lecteur DVD de la VM. Dans les paramètres de la VM, vous pouvez également positionner en premier le démarrage sur le disque.



La machine virtuelle va redémarrer et charger le système OPNsense à partir du disque puisque nous venons de procéder à l'installation. Connectez-vous avec le compte « root » dans la console, et votre nouveau mot de passe (sinon le mot de passe par défaut est « opnsense »).

d

B. Associer les interfaces reseau

Vous allez arriver sur l'écran présenté ci-dessous. Faites le choix "1" et appuyez sur Entrée pour associer les cartes réseaux de la machine aux interfaces d'OPNsense.

```
*** OPNsense.localdomain: OPNsense 24.1 ***

LAN (hn0)      -> v4: 192.168.1.1/24
WAN (hn1)      ->

HTTPS: SHA256 BD AD F6 12 29 00 7D 6A 86 89 50 95 88 4A 01 C1
              C9 A8 8A 7D 27 67 5B 5B DF 70 32 92 F5 14 B5 07

0) Logout                      7) Ping host
1) Assign 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: 1
```

D'abord, l'assistant propose de configurer une agrégation de liens et des VLANs, indiquez "n" pour refuser, et à chaque fois, validez votre réponse avec Entrée. Ensuite, vous devez affecter les deux interfaces : "hn0" et "hn1" au WAN et au LAN. En principe, "hn0" correspond au WAN et l'autre interface au LAN.

Voici la marche à suivre :

```
Enter an option: 1

Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:

hn0          00:15:5d:89:1e:02 Hyper-V Network Interface
hn1          00:15:5d:89:1e:03 Hyper-V Network Interface

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 interface name or 'a' for auto-detection: hn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): hn1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> hn0
LAN  -> hn1

Do you want to proceed? [y/N]: y
```

Désormais, nous avons :

L'interface LAN associée à la carte réseau "hn1" et avec l'adresse IP par défaut d'OPNsense, à savoir 192.168.1.1/24.

L'interface WAN associée à la carte réseau "hn0" et avec une adresse IP récupérée via DHCP sur le réseau local (grâce à notre commutateur virtuel externe).

Par défaut, l'interface d'administration d'OPNsense est accessible uniquement depuis l'interface LAN, pour des raisons évidentes de sécurité. Vous devez donc vous connecter sur l'interface LAN du firewall pour effectuer l'administration. Si c'est impossible, sachez que vous pouvez administrer temporairement OPNsense depuis le WAN. Ceci implique de désactiver la fonction de firewall.

Pour cela, basculez en mode shell via l'option "8" et exécutez la commande suivante :

- pfctl -d

```
*** OPNsense.localdomain: OPNsense 24.1 ***

LAN (hn1)      -> v4: 192.168.1.1/24
WAN (hn0)      -> v4/DHCP4: 192.168.137.53/24

HTTPS: SHA256 BD AD F6 12 29 00 7D 6A 86 89 50 95 88 4A 01 C1
          C9 A8 8A 7D 27 67 5B 5B DF 70 32 92 F5 14 B5 07

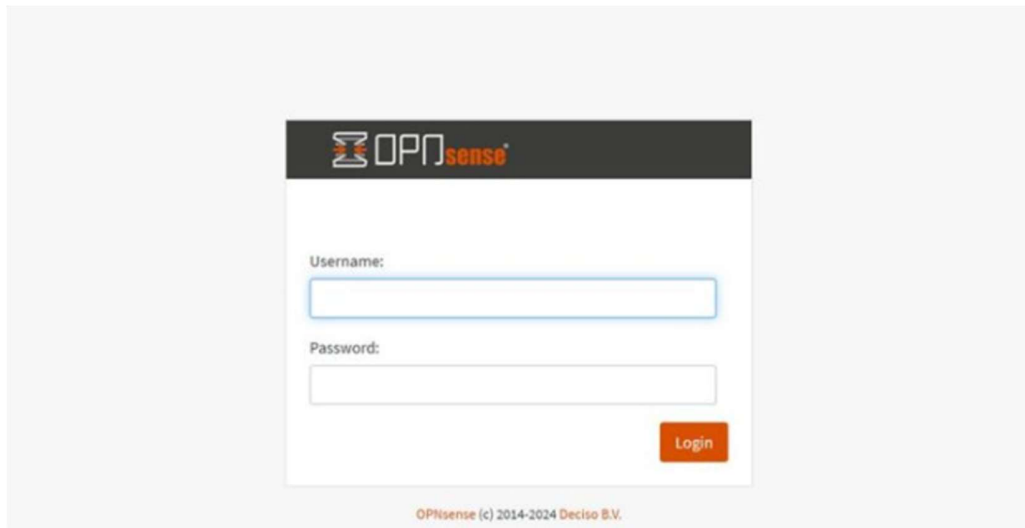
0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system  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

Enter an option: 8

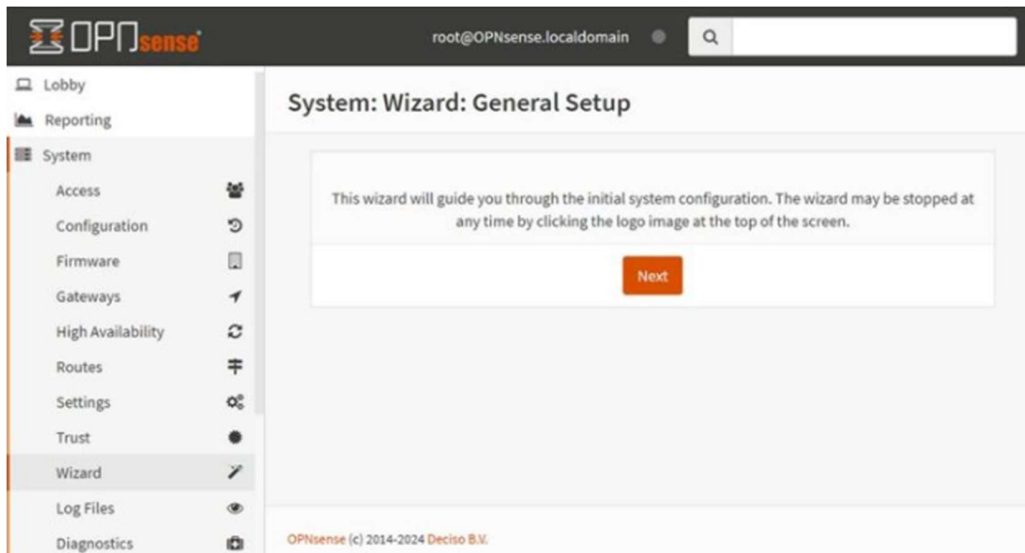
root@OPNsense:~ # pfctl -d
pf disabled
root@OPNsense:~ #
```

C. Accès à l'interface de gestion d'OPNsense

L'interface d'administration d'OPNsense est accessible en HTTPS, via l'adresse IP de l'interface LAN (ou éventuellement celle de la WAN). À partir de votre navigateur, vous arrivez sur une page de connexion. Connectez-vous avec le compte "root" et le mot de passe sélectionné précédemment.



Patientez quelques secondes... Vous serez invité à suivre un assistant pour effectuer la configuration de base. Cliquez sur "Next" pour continuer.



La première étape consiste à définir le nom d'hôte, le nom de domaine, à choisir la langue et à définir aussi le(s) serveur(s) DNS à utiliser pour la résolution de noms. Le fait de conserver l'option "Enable Resolver" permettra d'utiliser le firewall en tant que résolveur DNS, ce qui sera utile pour les machines de notre LAN virtuel.

The screenshot shows the OPNsense web interface. The left sidebar contains a menu with items: Lobby, Reporting, System (selected), Access, Configuration, Firmware, Gateways, High Availability, Routes, Settings, Trust, Wizard (active), Log Files, and Diagnostics. Below this are sections for Interfaces, Firewall, VPN, Services, Power, and Help. The main content area is titled "System: Wizard: General Information". It contains a "General Information" section with fields for Hostname (OPNsense), Domain (localdomain), Language (French), Primary DNS Server (1.1.1.1), and Secondary DNS Server. There is a checkbox for "Override DNS" which is checked, with the text "Allow DNS servers to be overridden by DHCP/PPP on WAN". Below this is an "Unbound DNS" section with checkboxes for "Enable Resolver" (checked) and "Enable DNSSEC Support" (unchecked). At the bottom, it says "OPNsense (c) 2014-2024 Deciso B.V."

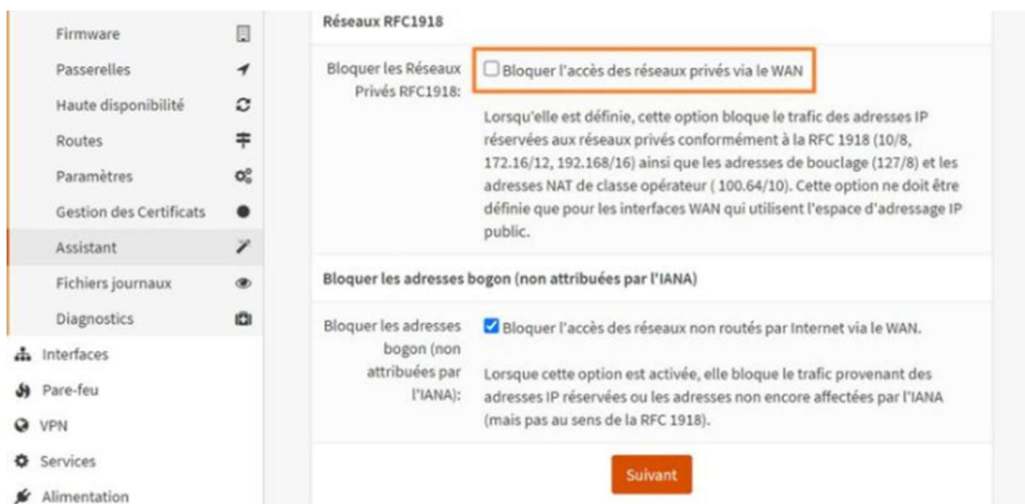
Passez à l'étape suivante. L'assistant vous offre la possibilité de définir un serveur NTP pour la synchronisation de la date et l'heure, bien qu'il y ait déjà des serveurs configurés par défaut. De plus, il est essentiel de choisir le fuseau horaire correspondant à votre emplacement géographique (sauf besoin particulier).

The screenshot shows the next step in the OPNsense wizard, titled "System: Wizard: Time Server Information". The left sidebar is the same as the previous screen. The main content area has a "Time server hostname:" field with the value "0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2....". Below this is a text prompt "Enter the hostname (FQDN) of the time server." and a "Timezone:" dropdown menu set to "Europe/Paris". At the bottom right, there is an orange "Next" button.

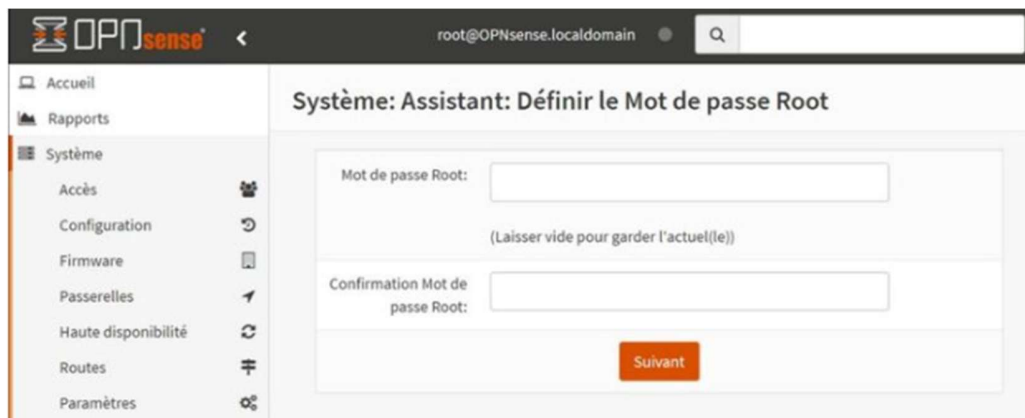
Ensuite, vient une étape importante : la configuration de l'interface WAN. Actuellement, elle est configurée en DHCP et elle va rester dans ce mode de configuration, sauf si vous souhaitez définir une adresse IP statique.



Toujours sur la page de configuration de l'interface WAN, vous devez décocher l'option "Bloquer l'accès à des réseaux privés via le WAN" si le réseau côté WAN utilise un adressage privé. Ce sera probablement le cas si vous faites un Lab, et donc cela peut vous empêcher d'accéder à Internet.



Ensuite, vous pouvez définir un mot de passe "root", mais c'est facultatif parce que nous l'avons déjà fait.



The screenshot shows the OPNsense web interface. The top header includes the OPNsense logo, a back arrow, the user 'root@OPNsense.localdomain', and a search bar. The left sidebar contains a menu with 'Accueil', 'Rapports', 'Système' (expanded), 'Accès', 'Configuration', 'Firmware', 'Passerelles', 'Haute disponibilité', 'Routes', and 'Paramètres'. The main content area is titled 'Système: Assistant: Définir le Mot de passe Root'. It contains two input fields: 'Mot de passe Root:' and 'Confirmation Mot de passe Root:'. Below the second field is a note '(Laisser vide pour garder l'actuel(le))'. An orange 'Suivant' button is at the bottom right.

Poursuivez jusqu'à la fin afin d'enclencher le rechargement de la configuration. Si vous avez besoin de continuer à prendre la main via le WAN, relancez la commande évoquée précédemment une fois ce processus terminé.



The screenshot shows the OPNsense web interface. The top header is the same as the previous screenshot. The left sidebar is also the same. The main content area is titled 'Système: Assistant: Rechargement en cours'. It contains a message box with the text: 'Un rechargement est en cours. L'assistant vous redirigera vers le tableau de bord une fois ce rechargement terminé.'

La configuration initiale est terminée



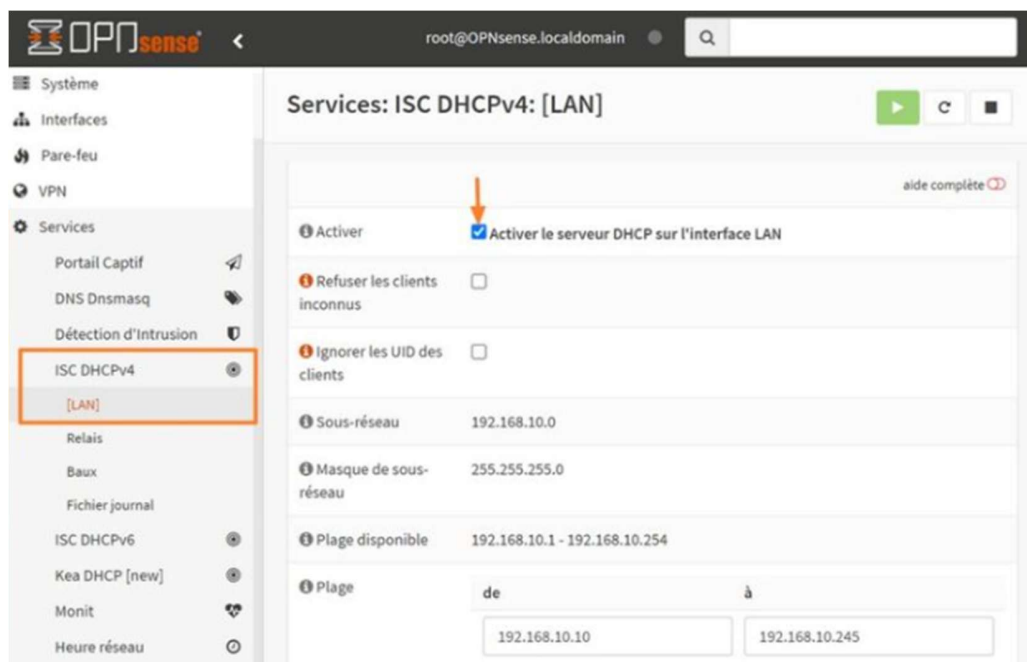
The screenshot shows the OPNsense web interface. The top header is the same. The left sidebar now includes 'Tableau de bord' (Dashboard) under the 'Accueil' section, along with 'Licence', 'Mot de passe', and 'Déconnexion'. The main content area is titled 'Configuration initiale terminée!'. It features the OPNsense logo and a message: 'Félicitations! OPNsense est maintenant configuré.' Below this, it says: 'Veuillez envisager de faire un don au projet pour nous aider à payer nos frais généraux. Consultez notre site internet pour faire un don ou acheter des services d'assistance OPNsense disponibles.' At the bottom, it says: 'Cliquer pour continuer vers le tableau de bord. Ou cliquez sur check for updates.'

D. Configuration du DHCP

Nous avons pour objectif d'utiliser le serveur DHCP d'OPNsense pour distribuer des adresses IP sur le LAN virtuel. Pour cela, nous devons accéder à cet emplacement du menu : Services > ISC DHCPv4 > [LAN].

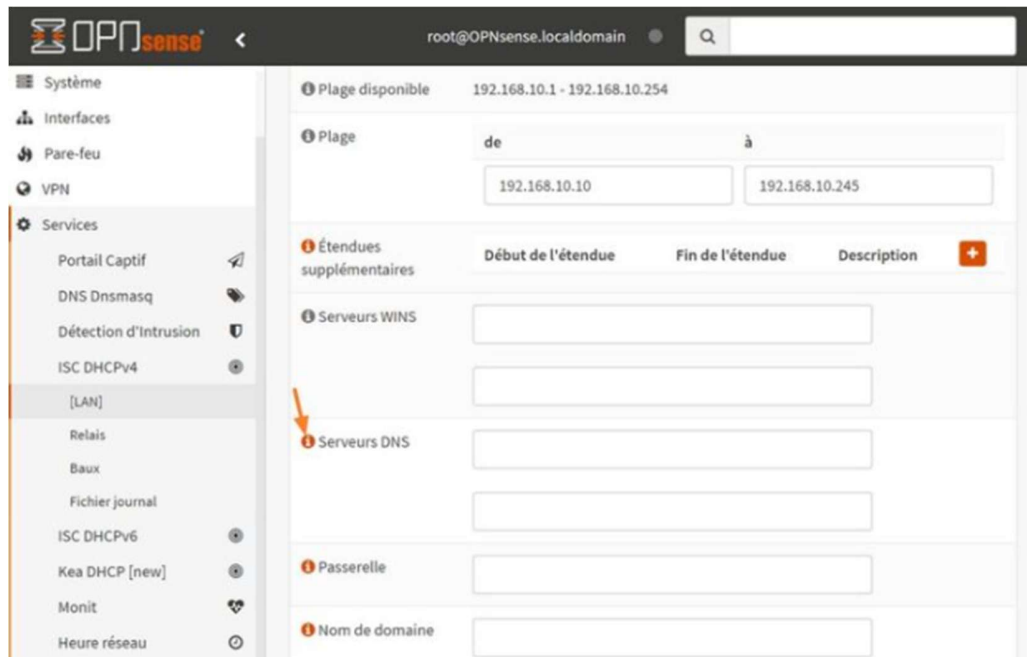
Nous pouvons constater que le DHCP est déjà activé par défaut sur le LAN ! Si ce service ne vous intéresse pas, il conviendra de le désactiver. Bien qu'il soit déjà activé et que nous voulons l'utiliser, il est important de réviser sa configuration.

Vous pouvez éventuellement modifier la plage d'adresses IP à distribuer : 192.168.10.10 à 192.168.10.245, selon les paramètres actuels.



Nous pouvons constater aussi que les champs "Serveurs DNS", "Passerelle", "Nom de domaine", etc... sont vides par défaut. En fait, il y a un héritage automatique de certaines options et des valeurs par défaut pour ces différents champs. Par exemple, pour le serveur DNS, l'adresse IP de l'interface LAN sera distribuée ce qui permettra d'utiliser le firewall OPNsense en tant que résolveur DNS.

Sauvegardez la configuration après avoir apporté des modifications, si nécessaire.



Pour tester le bon fonctionnement du serveur DHCP, vous devez connecter une machine sur le réseau LAN de votre firewall.

Cette machine doit récupérer une adresse IP à partir du serveur DHCP d'OPNsense et notre machine doit avoir accès au réseau. L'accès à Internet doit fonctionner. Attention, si vous avez désactivé la fonction de firewall pour accéder à OPNsense depuis le WAN, ceci désactive le NAT, et vous empêche donc d'accéder au Web.

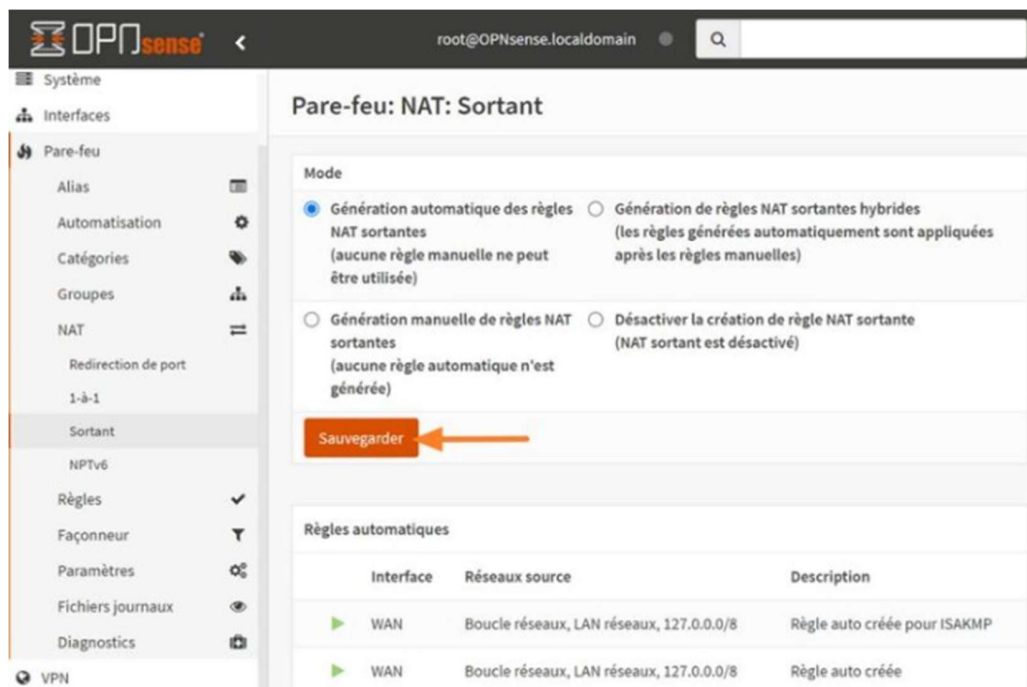
E. Configuration du NAT et des règles de firewall

La bonne nouvelle, c'est que désormais, nous pouvons accéder à l'interface d'administration d'OPNsense à partir du LAN.

<https://192.168.1.10>

Après s'être connecté à OPNsense, partons à la découverte de la configuration du NAT. Accédez à cet endroit : Pare-feu > NAT > Sortant. Ici, vous avez le choix entre la création de règles de NAT sortantes automatiques (mode par défaut) ou la création manuelle.

Choisissez le mode automatique via l'option "Génération automatique des règles NAT sortantes" et cliquez sur "Sauvegarder" (en principe, cette configuration est déjà celle active). En mode automatique, OPNsense crée lui-même une règle de NAT pour chacun de vos réseaux.



Pour le moment, tous les ordinateurs connectés au LAN virtuel "192.168.10.0/24" peuvent accéder à Internet sans restriction. Toutefois, notre objectif est de limiter l'accès vers le WAN aux seuls protocoles HTTP et HTTPS, ainsi que le DNS sur l'interface LAN du firewall.

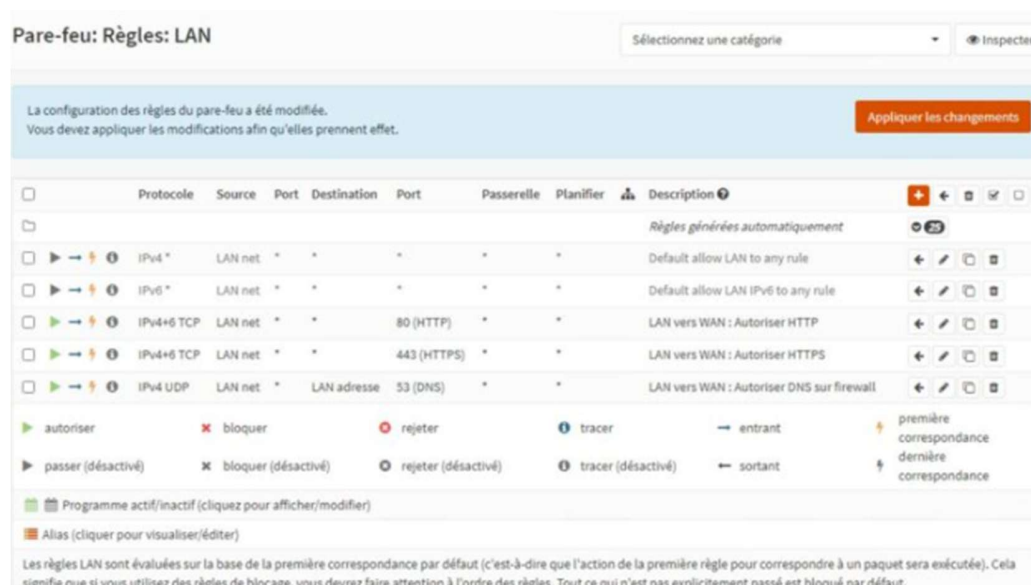
Ainsi, nous devons créer des règles de pare-feu... Parcourez le menu de cette façon : Pare-feu > Règles > LAN.

Par défaut, il y a deux règles pour autoriser tous les flux sortants du réseau LAN, en IPv4 et en IPv6. Désactivez ces deux règles en cliquant sur la flèche verte tout à gauche, au début de chaque ligne.

Puis, créez trois nouvelles règles pour autoriser le réseau LAN (soit "LAN net") à :

- accéder à toutes les destinations en HTTP.
- accéder à toutes les destinations en HTTPS.
- solliciter OPNsense sur son interface LAN (soit "LAN adresse"), via le protocole DNS (ceci implique d'utiliser le firewall comme DNS), sinon autoriser votre résolveur DNS via son adresse IP.

Ce qui donne le résultat suivant :



Il ne reste plus qu'à cliquer sur "Appliquer les changements" pour basculer en production les nouvelles règles de pare-feu. Sachez que tous les flux qui ne sont explicitement autorisés seront bloqués par défaut.

La machine du LAN peut accéder à Internet, en naviguant en HTTP et HTTPS. Tous les autres protocoles seront bloqués.

Source : <https://www.it-connect.fr/tuto-installer-et-configurer-opnsense/>