01/04/2025

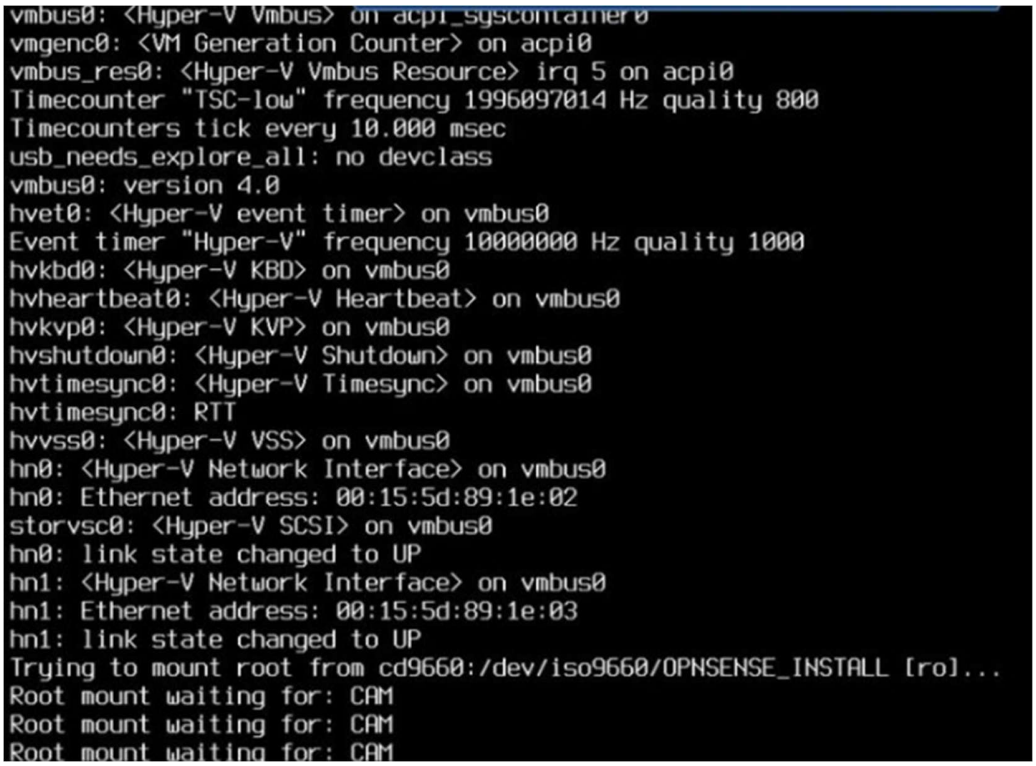
INSTALLATION D'OPNSENSE

MASSIAS Rudy
KEYCE INFORMATIQUE – BTS SIO

A. Installer le système OPNsense

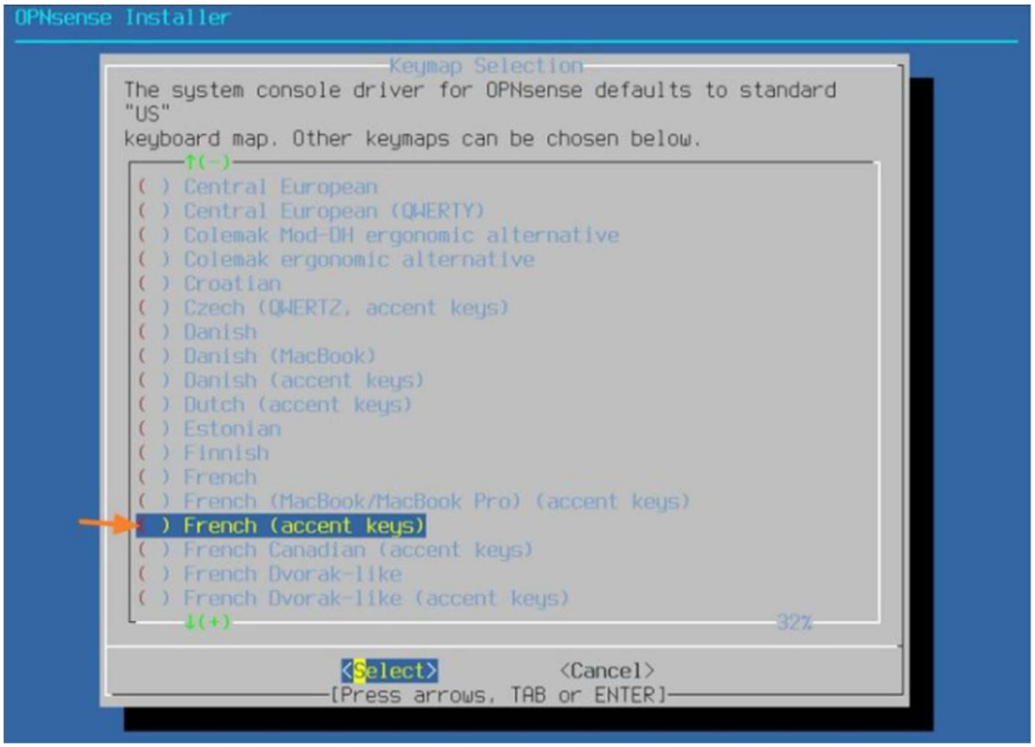
Démarrez la machine destinée à accueillir OPNsense. Vous devriez avoir une page d'accueil similaire à celle ci-dessous. Pendant quelques secondes, l'écran présenté sera visible dans la fenêtre. Laissez le processus se dérouler…

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.

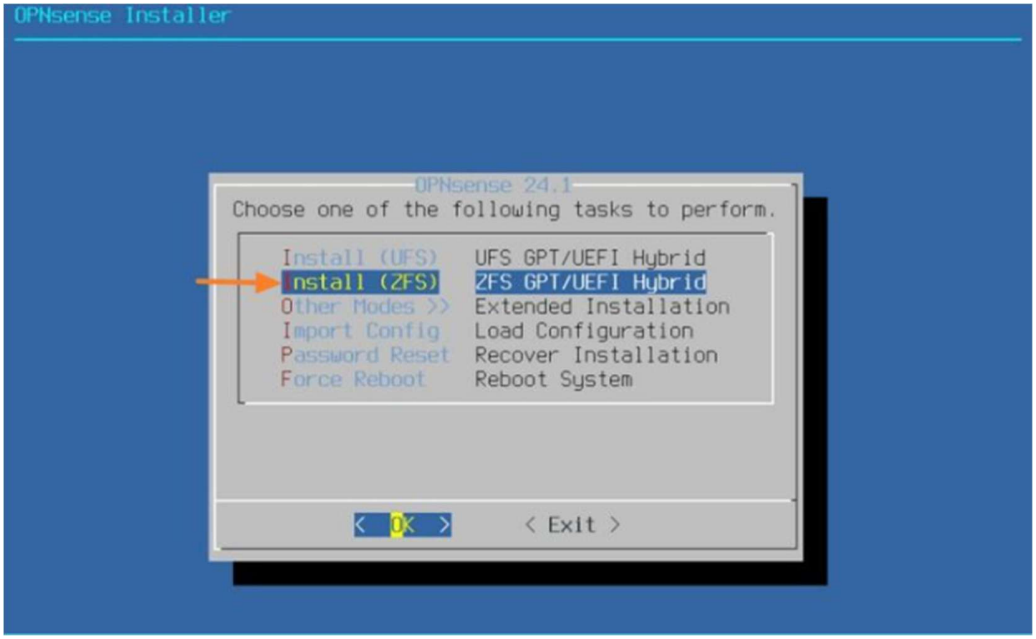


Puis, vous arrivez sur une interface similaire à celle ci-dessous. Connectez-vous à l'aide du login « installer » et du mot de passe « opnsense ». Attention, le clavier est en QWERTY pour le moment. À ce stade, nous allons commencer le processus d'installation d'OPNsense.

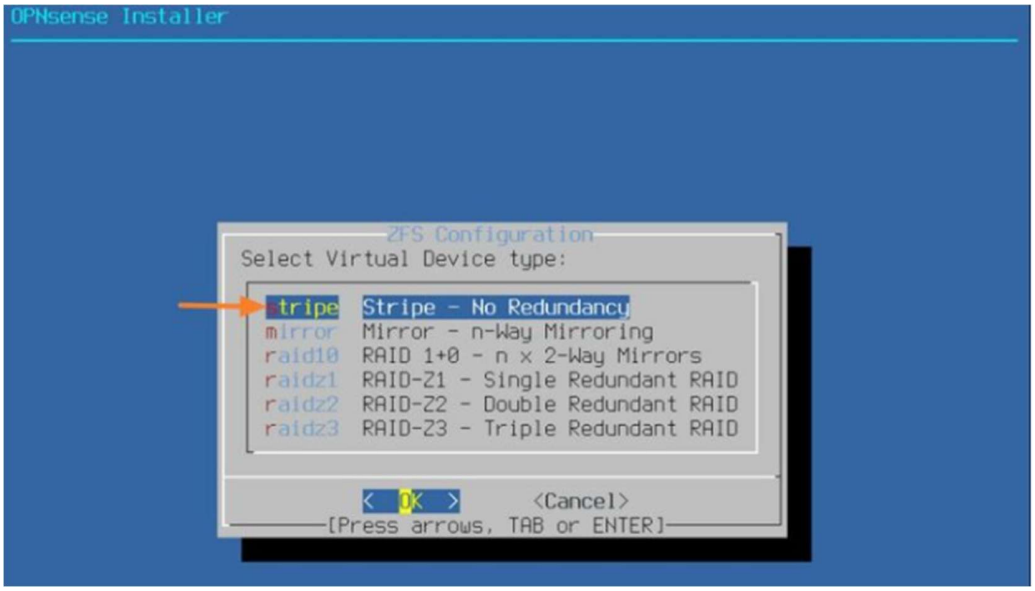
Un nouvel assistant s'affiche à l'écran. La première étape consiste à sélectionner la disposition du clavier correspondant à votre configuration. Pour un clavier AZERTY, sélectionnez l'option « French (accent keys) » dans la liste puis validez par deux fois.



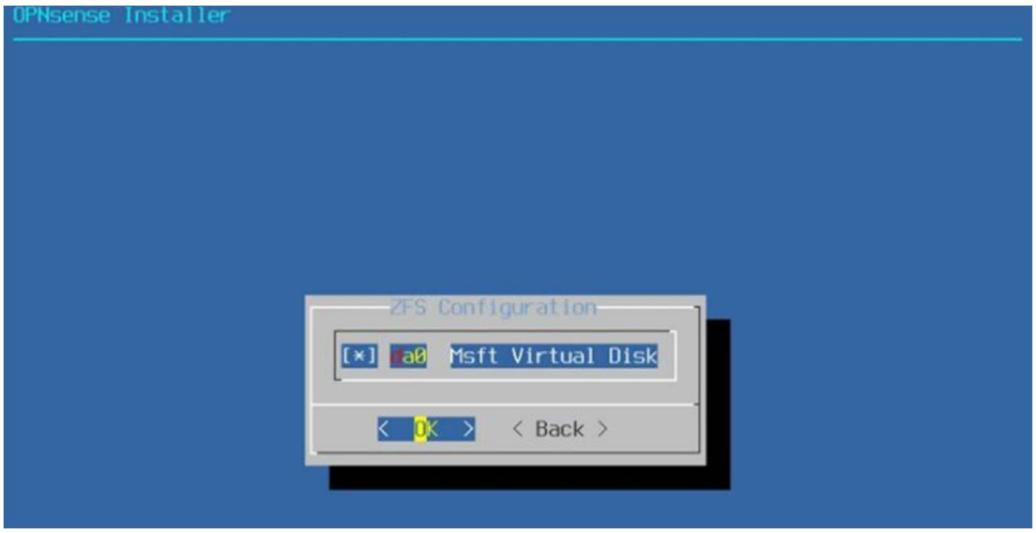
La seconde étape consiste à choisir la tâche à effectuer. Ici, nous allons effectuer une installation en utilisant le système de fichiers ZFS. Positionnez-vous sur la ligne « Install (ZFS) » et validez avec Entrée.



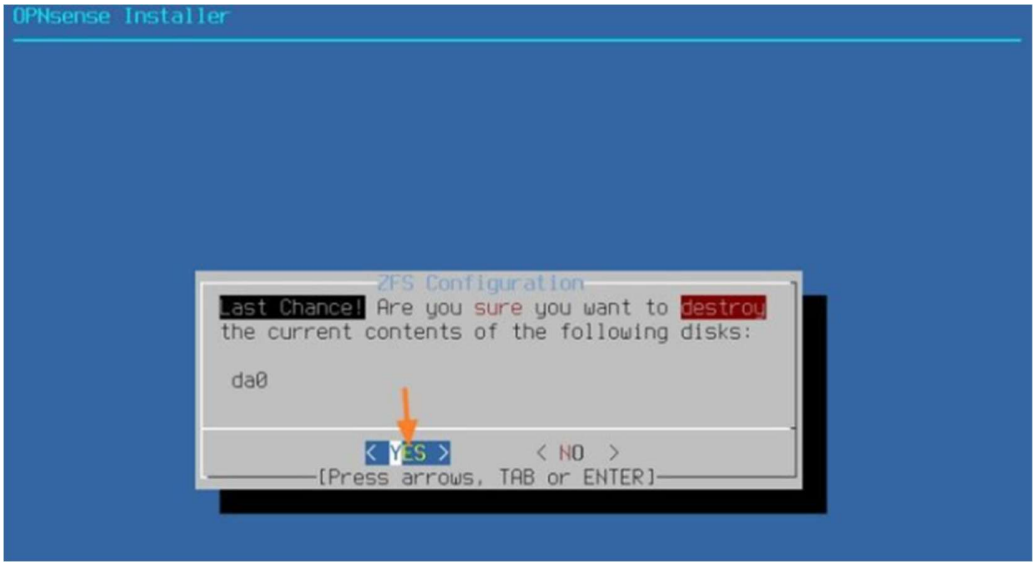
À la troisième étape, sélectionnez « stripe » puisque notre machine est équipée d'un seul disque : il n'y a pas de redondance possible pour sécuriser le stockage du pare-feu et ses données. Ceci est surtout pertinent lors de l'installation sur une machine physique pour se prémunir contre une panne matérielle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



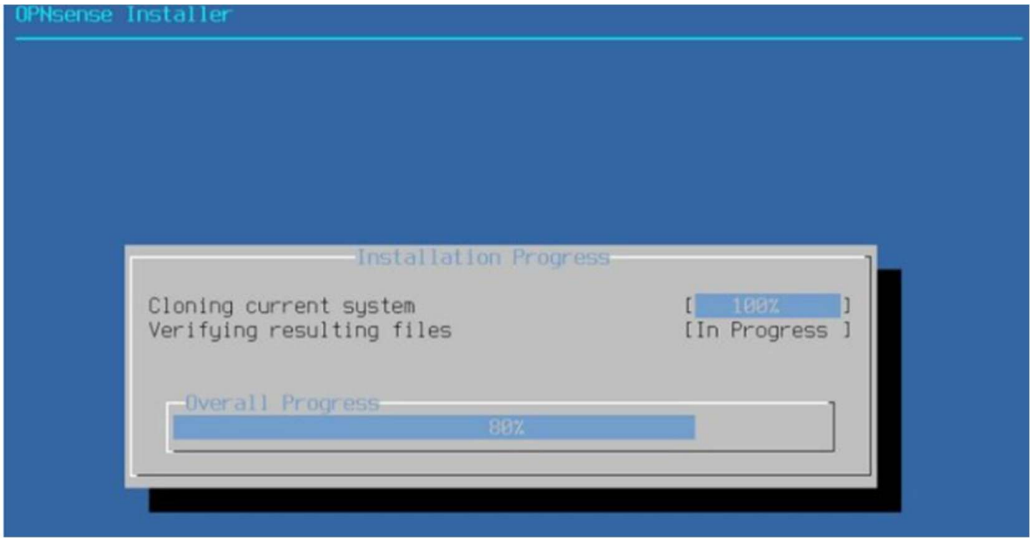
À la 4ème étape, appuyez simplement sur Entrée pour valider.



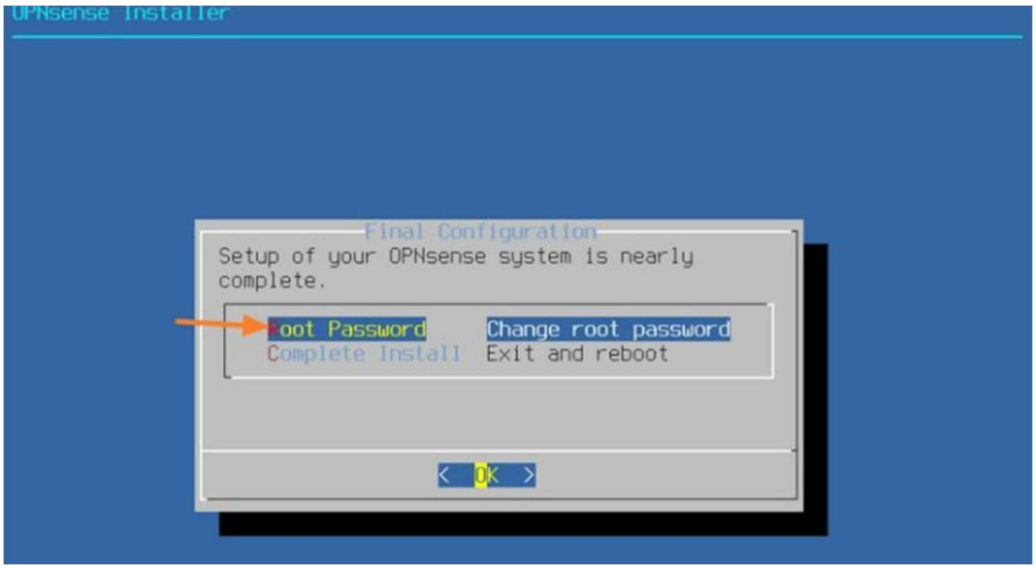
Enfin, validez en sélectionnant « YES » puis avec la touche Entrée.



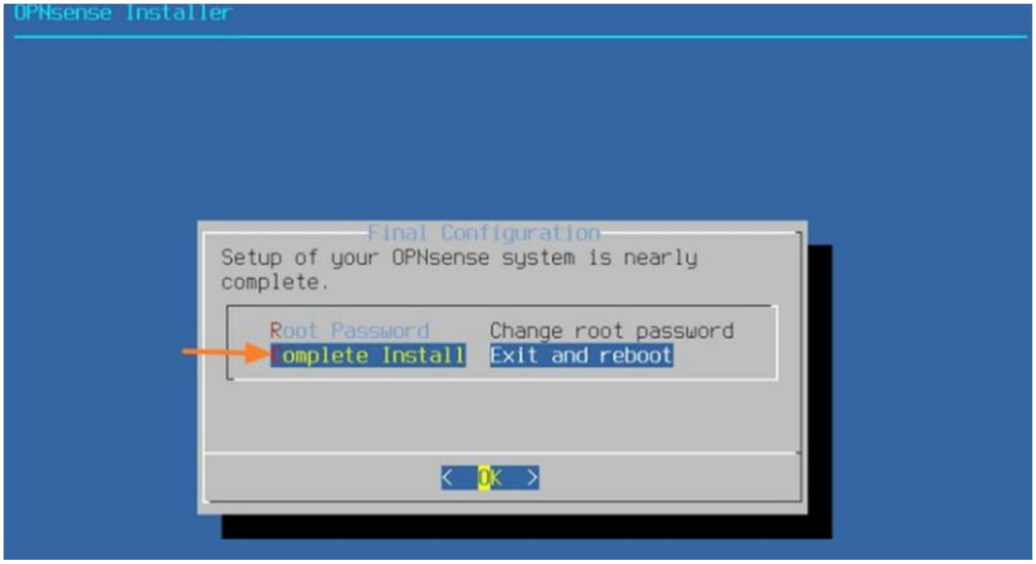
Désormais, vous devez patienter pendant l'installation d'OPNsense… Ce processus nécessite environ 5 minutes.



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 »).

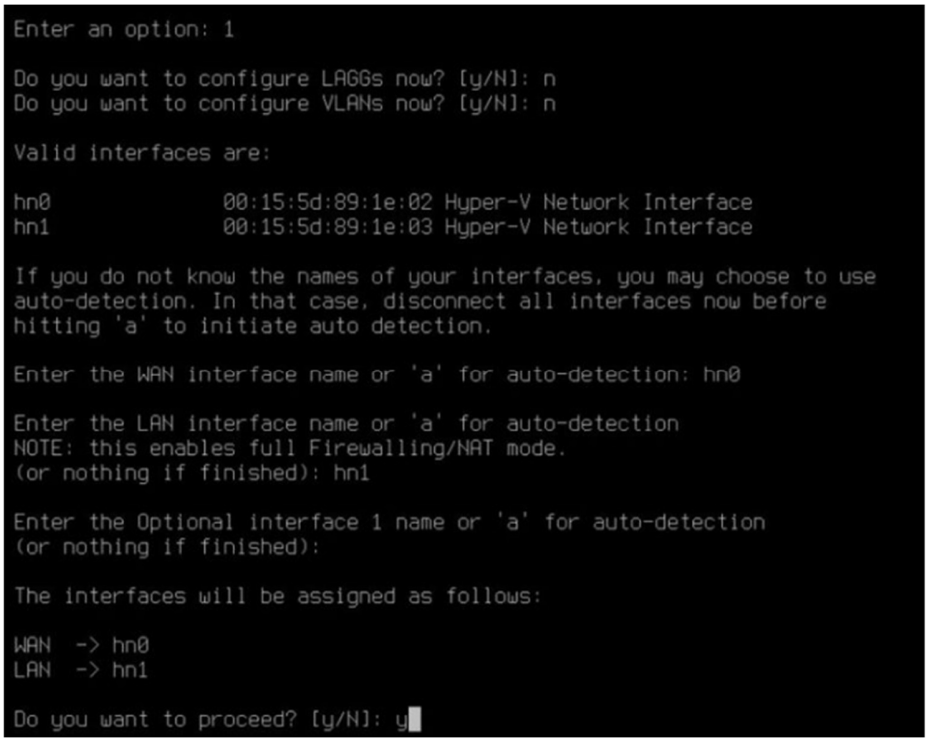
d

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.

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 :



Désormais, nous avons :

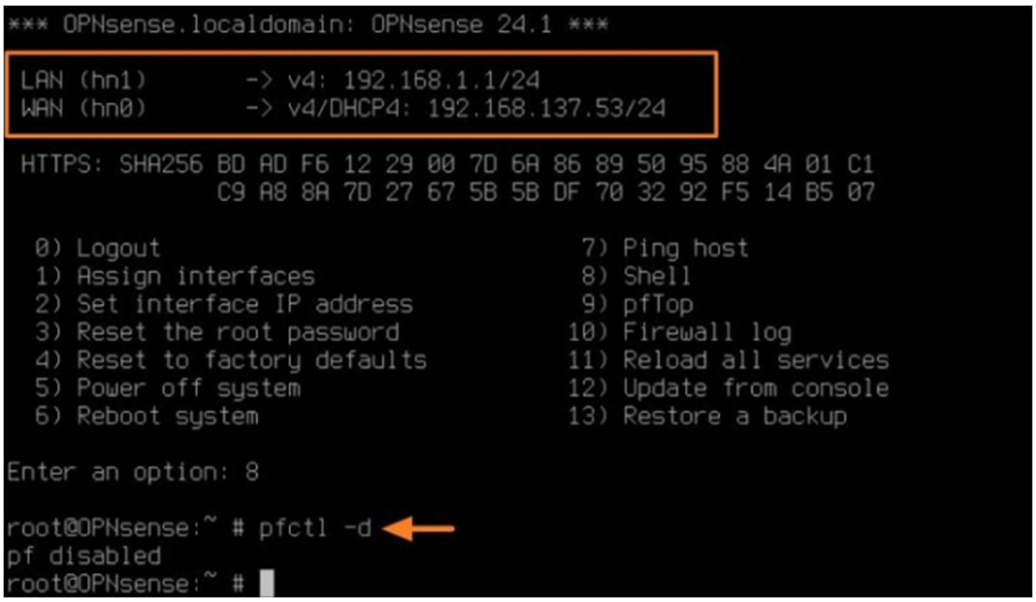
L'interface LAN associée à la carte réseau "hn1" et avec l'adresse IP par défaut d'OPNsense, à savoir 192.168.1.1/24.

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.

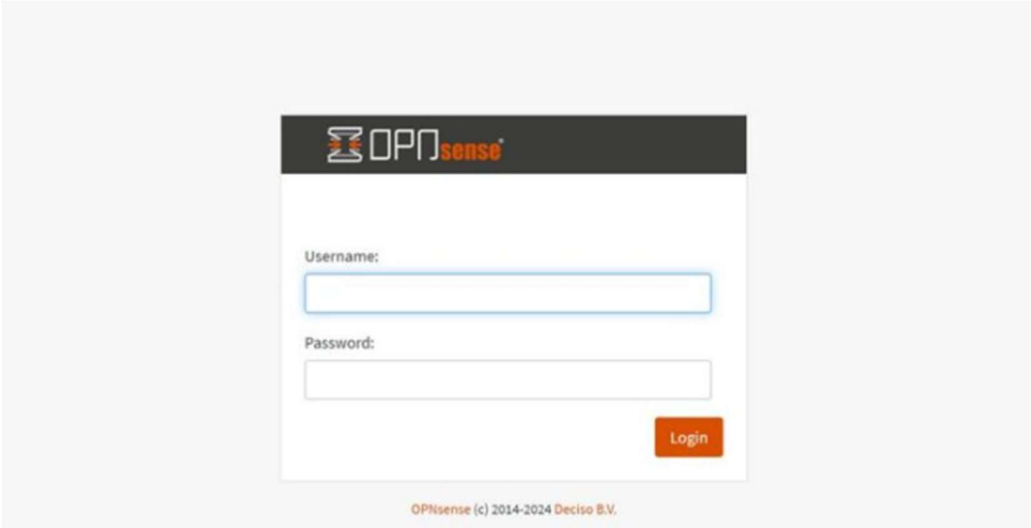
Pour cela, basculez en mode shell via l'option "8" et exécutez la commande suivante :

- pfctl -d

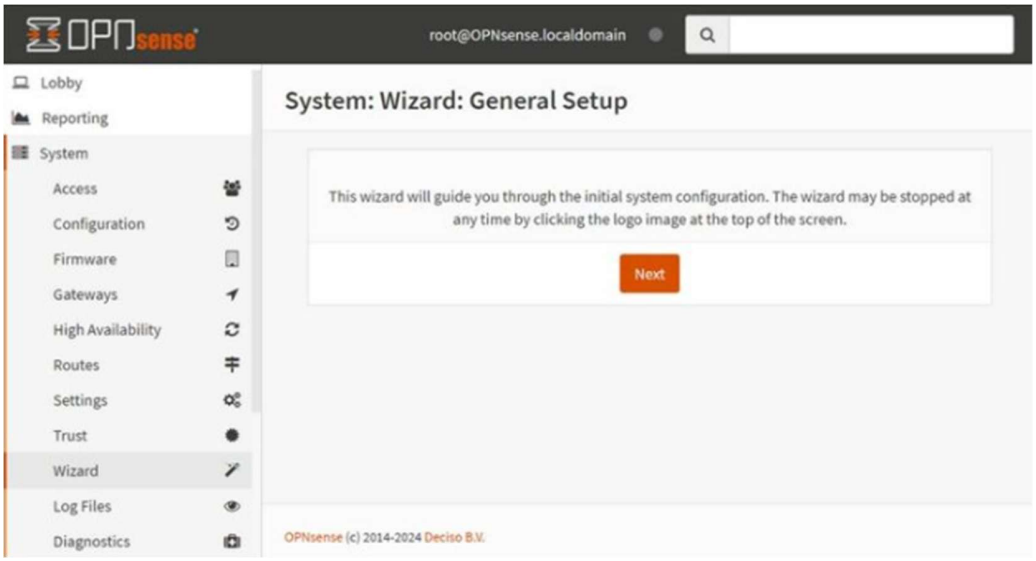


C. Accès à l'interface de gestion d'OPNsense

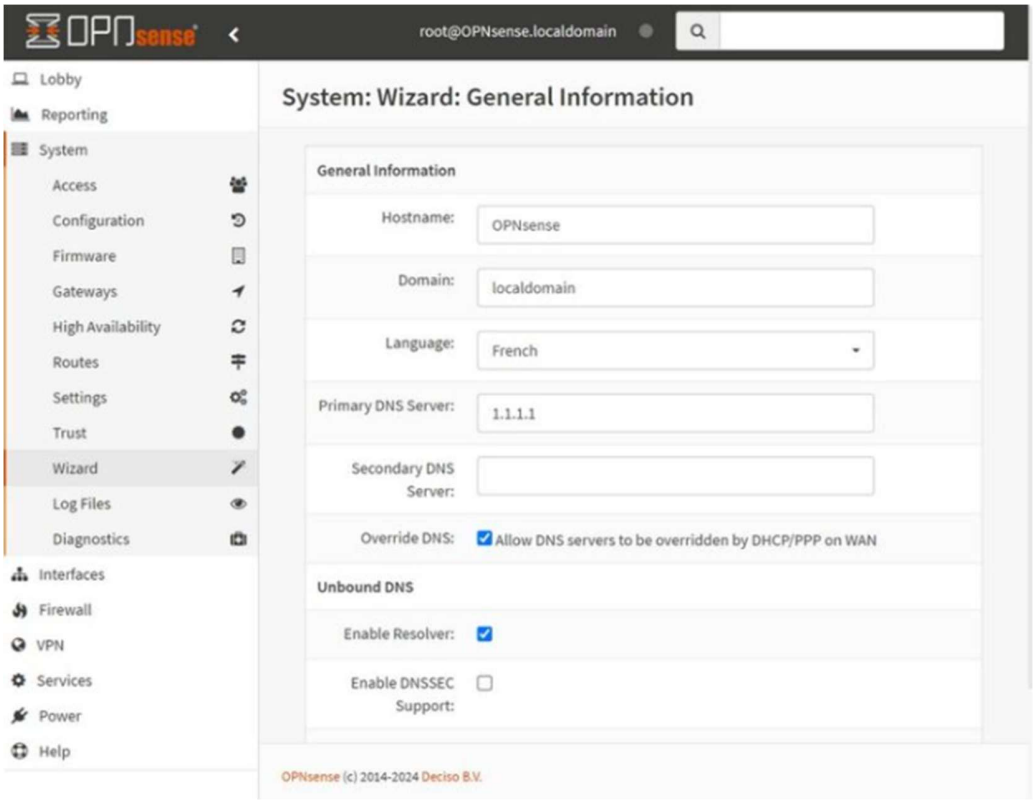
L'interface d'administration d'OPNsense est accessible en HTTPS, via l'adresse IP de l'interface LAN (ou éventuellement celle de la WAN). À partir de votre navigateur, vous arrivez sur une page de connexion. Connectez-vous avec le compte "root" et le mot de passe sélectionné précédemment.



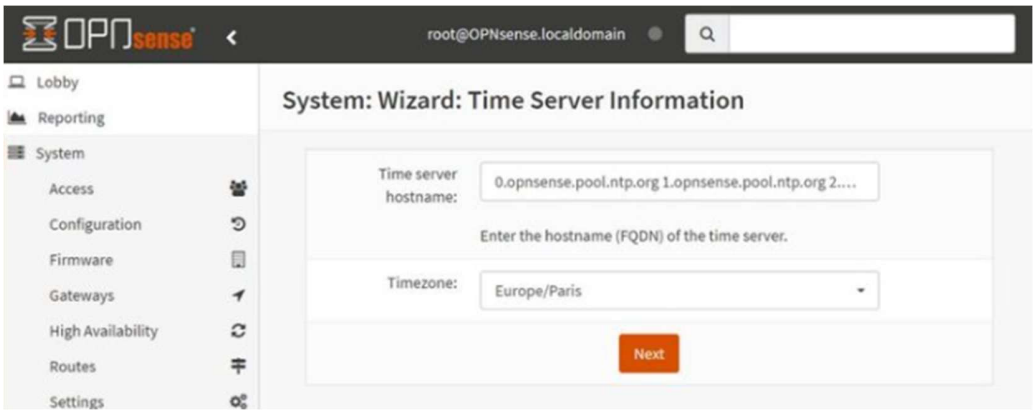
Patientez quelques secondes... Vous serez invité à suivre un assistant pour effectuer la configuration de base. Cliquez sur "Next" pour continuer.



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.

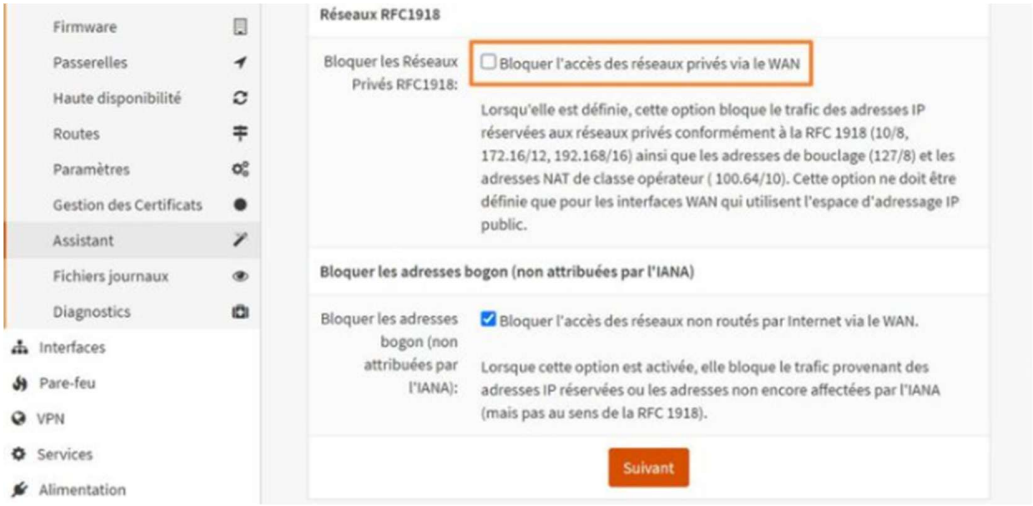


Passez à l'étape suivante. L'assistant vous offre la possibilité de définir un serveur NTP pour la synchronisation de la date et l'heure, bien qu'il y ait déjà des serveurs configurés par défaut. De plus, il est essentiel de choisir le fuseau horaire correspondant à votre emplacement géographique (sauf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

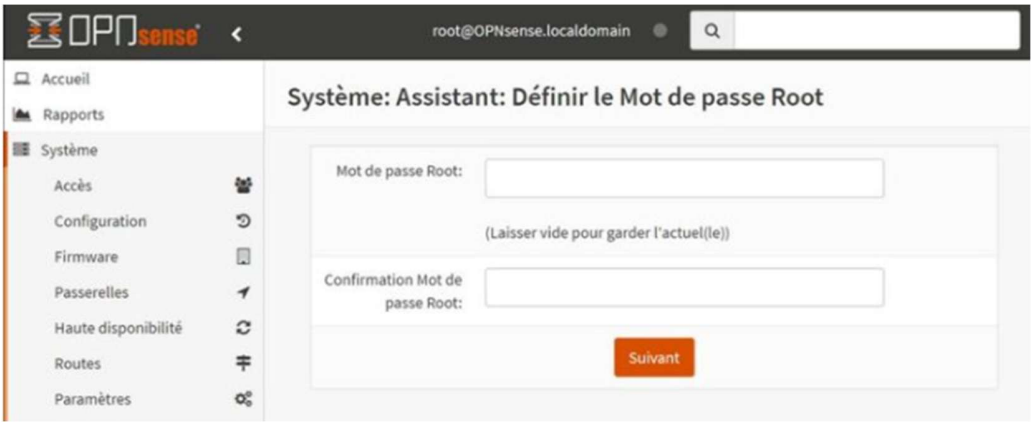


Ensuite, vient une étape importante : la configuration de l'interface WAN. Actuellement, elle est configurée en DHCP et elle va rester dans ce mode de configuration, sauf si vous souhaitez définir une adresse IP statique.

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.



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.

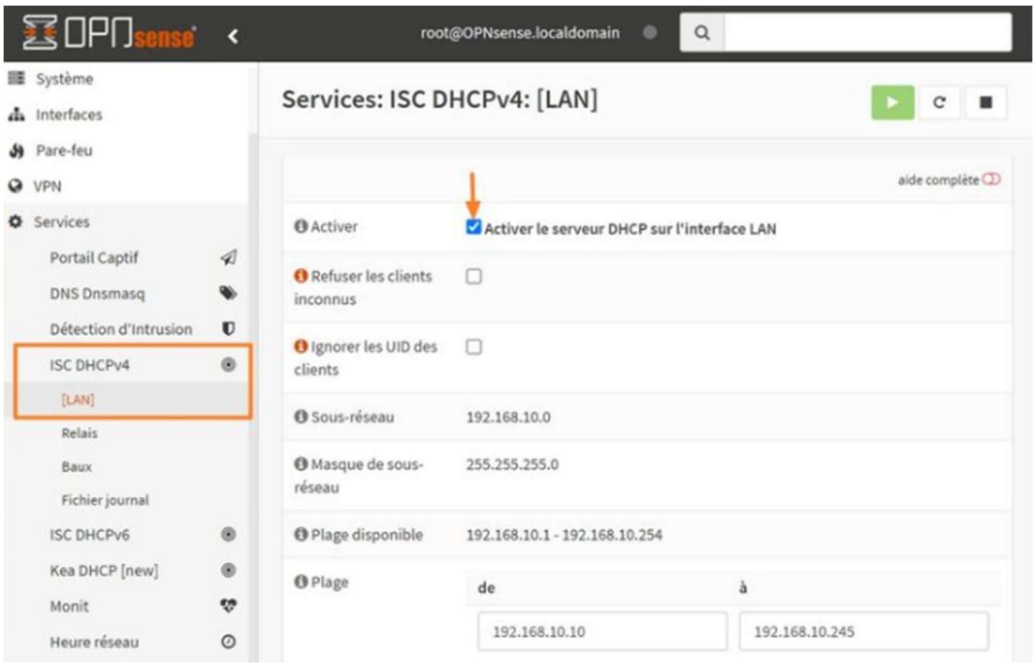
La configuration initiale est terminée

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].

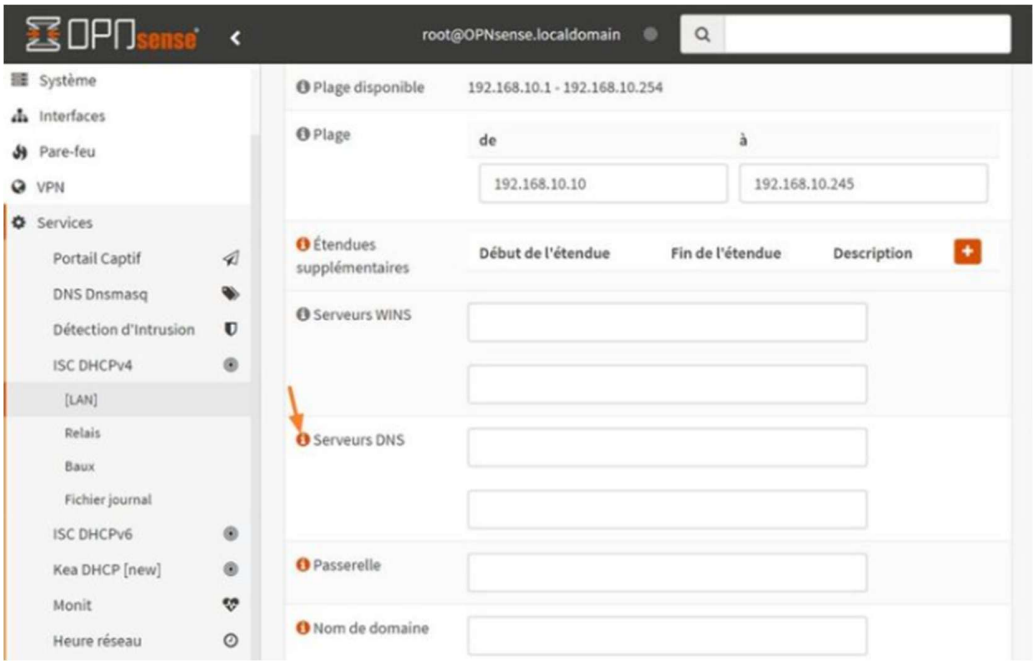
Nous pouvons constater que le DHCP est déjà activé par défaut sur le LAN ! Si ce service ne vous intéresse pas, il conviendra de le désactiver. Bien qu'il soit déjà activé et que nous voulons l'utiliser, il est important de réviser sa configuration.

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.

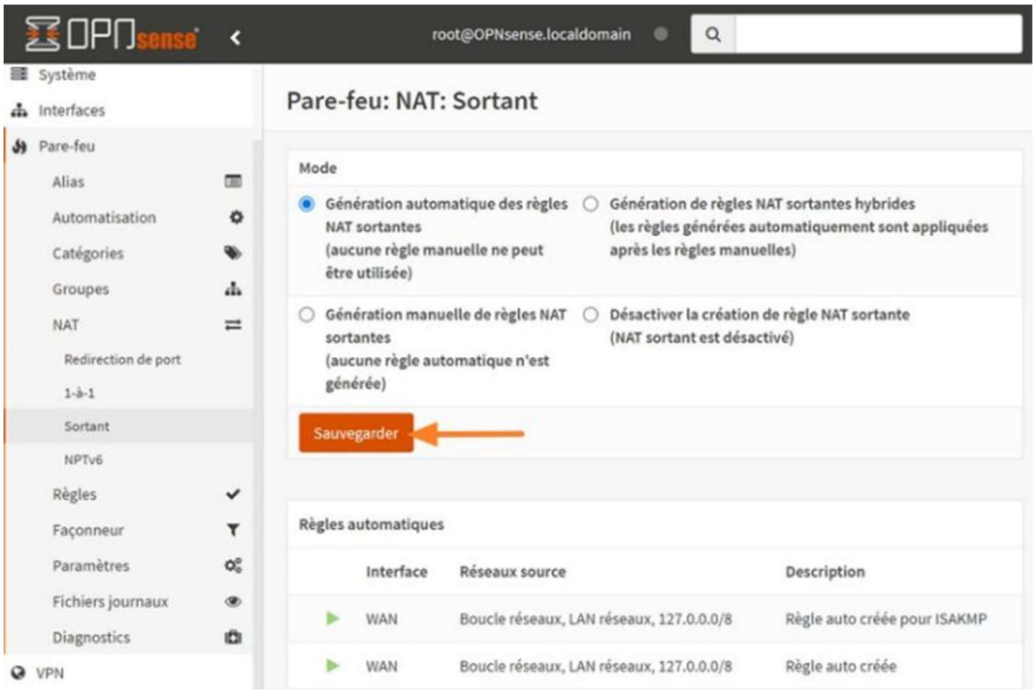
E. Configuration du NAT et des règles de firewall

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.

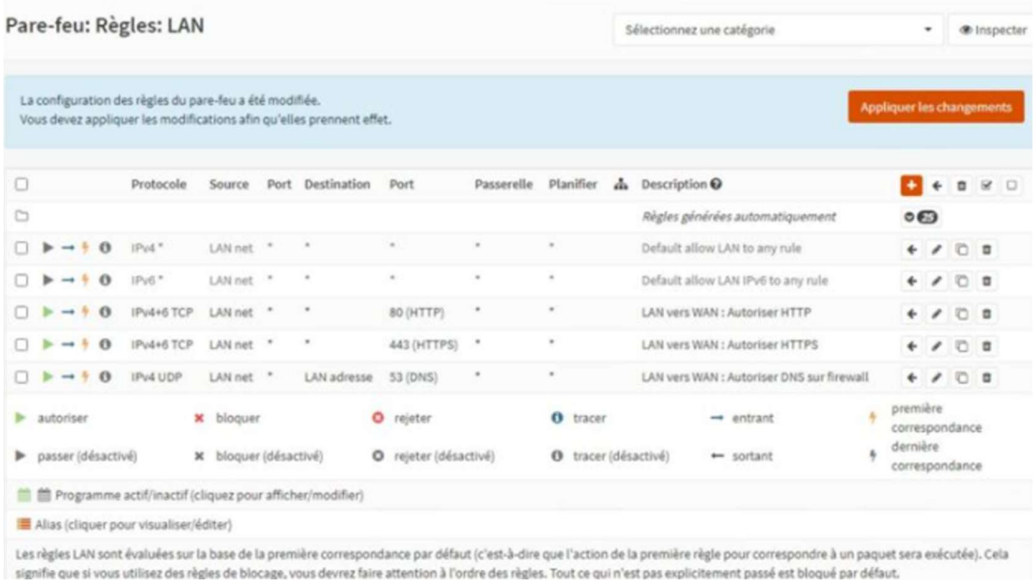
Puis, créez trois nouvelles règles pour autoriser le réseau LAN (soit "LAN net") à :

- 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/