Fiche 0 : Installation, configuration, changement du mot de passe et langue (Riverbed)

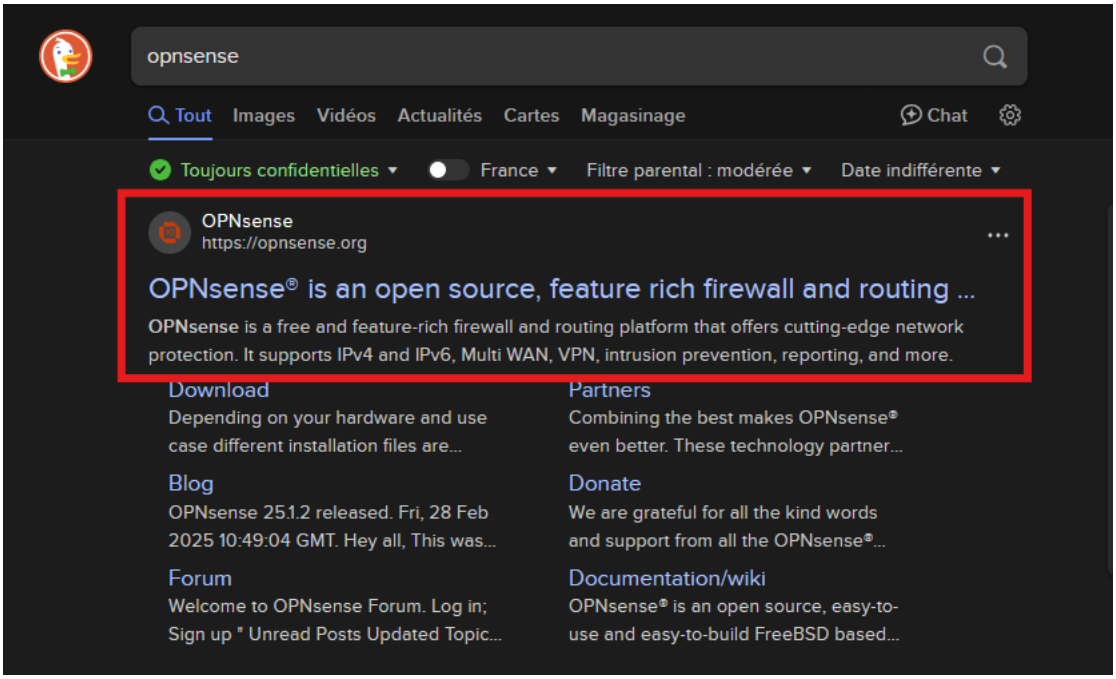
Sommaire

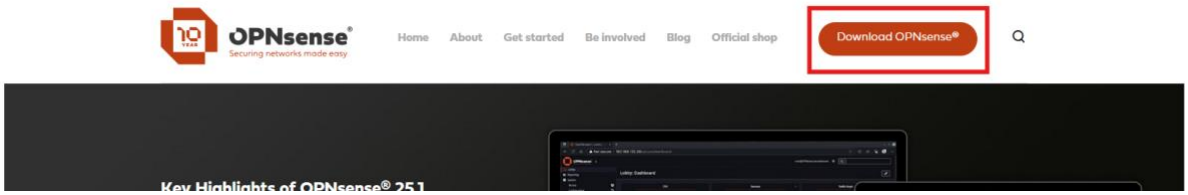
Partie 1 : Installation de OPNsense sur le Riverbed....2
1. Téléchargement de l'image ISO de OPNsense au format ISO 2
2. Création d'une clé USB avec Rufus et configuration de notre Riverbed 4
3. Installation d'OPNsense 10
Partie 2 : Post installation, configuration des interfaces, IP, mot de passe et langue 17
1. Modification du mot de passe root....17
2. Configuration des interfaces réseaux....19
3. Configuration des adresse IP....20
4. Accès à l'interface web et mise à jour du firewall 21
5. Importer et exporter la configuration....22
6. Activation du protocole SSH....23
7. Mise en place d'un web webfiltering 25

Partie 1 : Installation de OPNsense sur le Riverbed

1. Téléchargement de l'image ISO de OPNsense au format ISO

La première étape consiste à télécharger l'image au format ISO d'OPNsense afin de pouvoir l'installer dans notre Riverbed. Pour cela, il suffit de se rendre sur un moteur de recherche et de cliquer sur le site officiel d'OPNsense (opnsense.org) afin de le télécharger



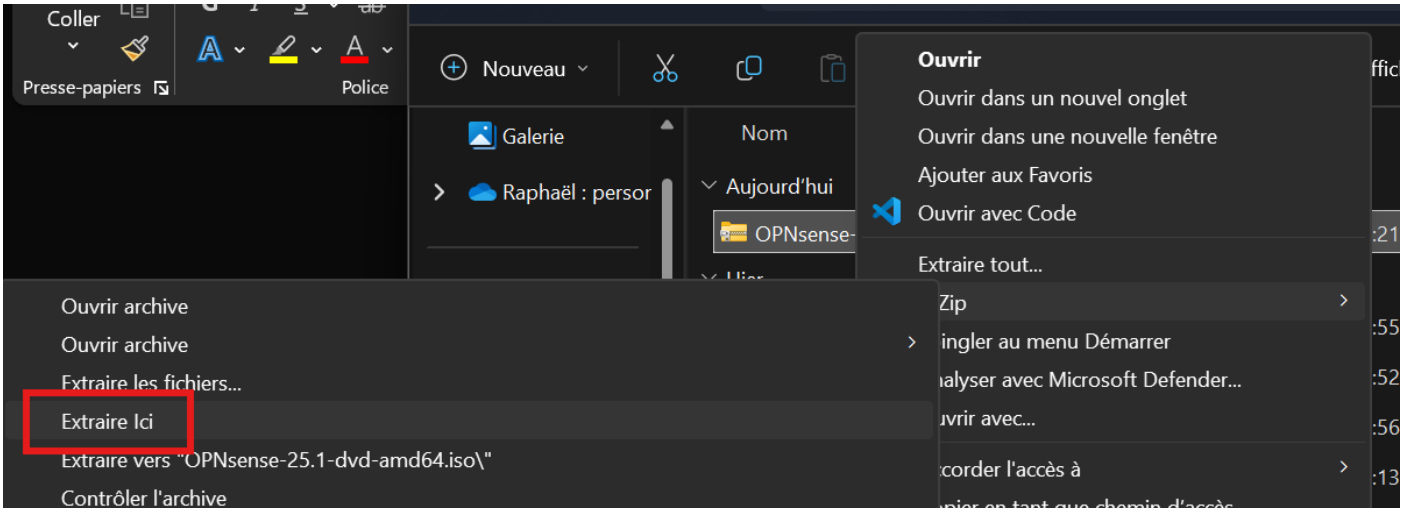


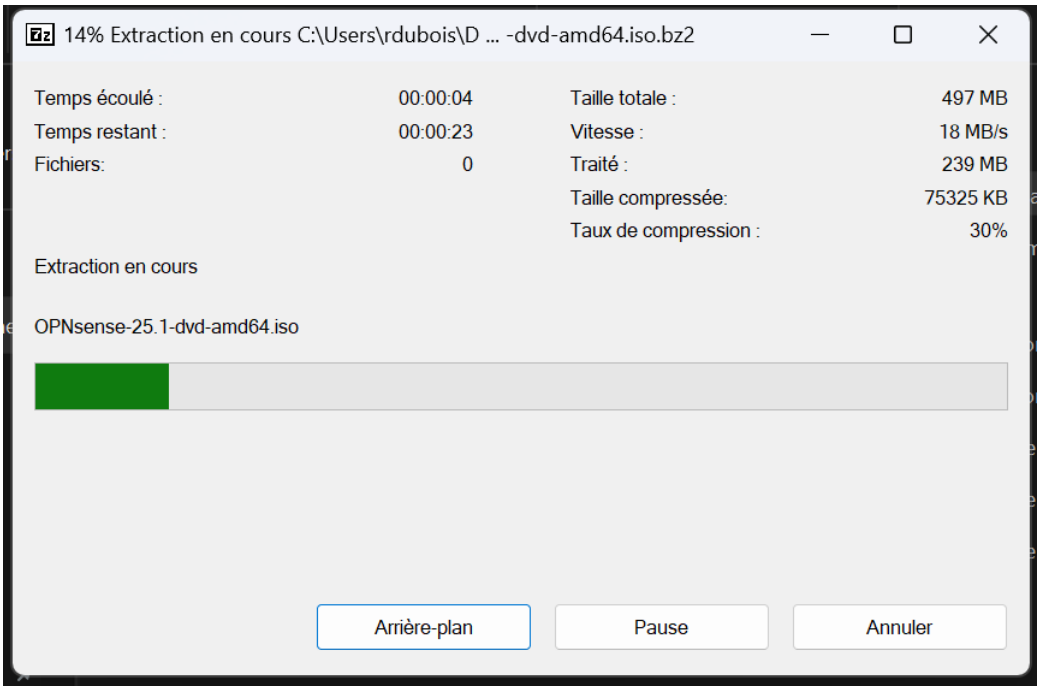
Une fois sur la page de téléchargement, il est important de sélectionner le type d'image « serial » afin d'avoir une image en .img installable via le port série avec une clé USB (les autres paramètres comme l'architecture du système et le mirror par défaut ne doivent pas être modifié sur un système Intel/AMD) :



Une fois le fichier télécharger, nous avons un fichier .iso.bz2 étant télécharger. Windows ayant des difficultés à décompresser ce type de fichiers, nous allons utiliser un logiciel libre nommé 7zip permettant de décompresser tout type de fichiers sur Windows (pour cela, il suffit de faire clic droit sur le fichier, 7zip et enfin « Extraire ici ») :







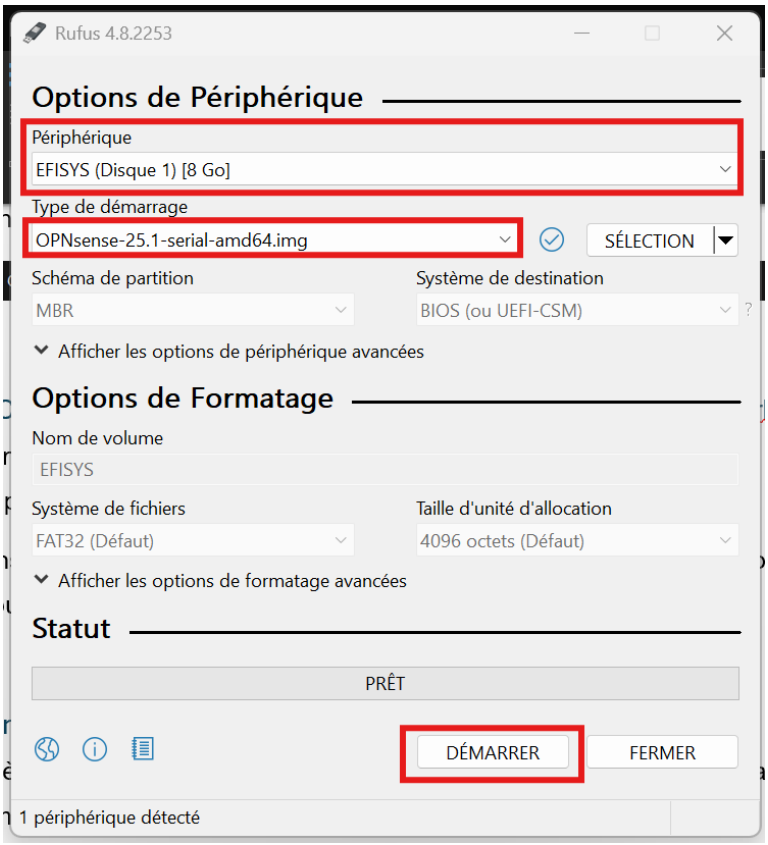
Une fois la décompression terminée, nous obtenons un fichier cette fois ci en .iso étant utilisable par notre Riverbed :



2. Création d'une clé USB avec Rufus et configuration de notre Riverbed

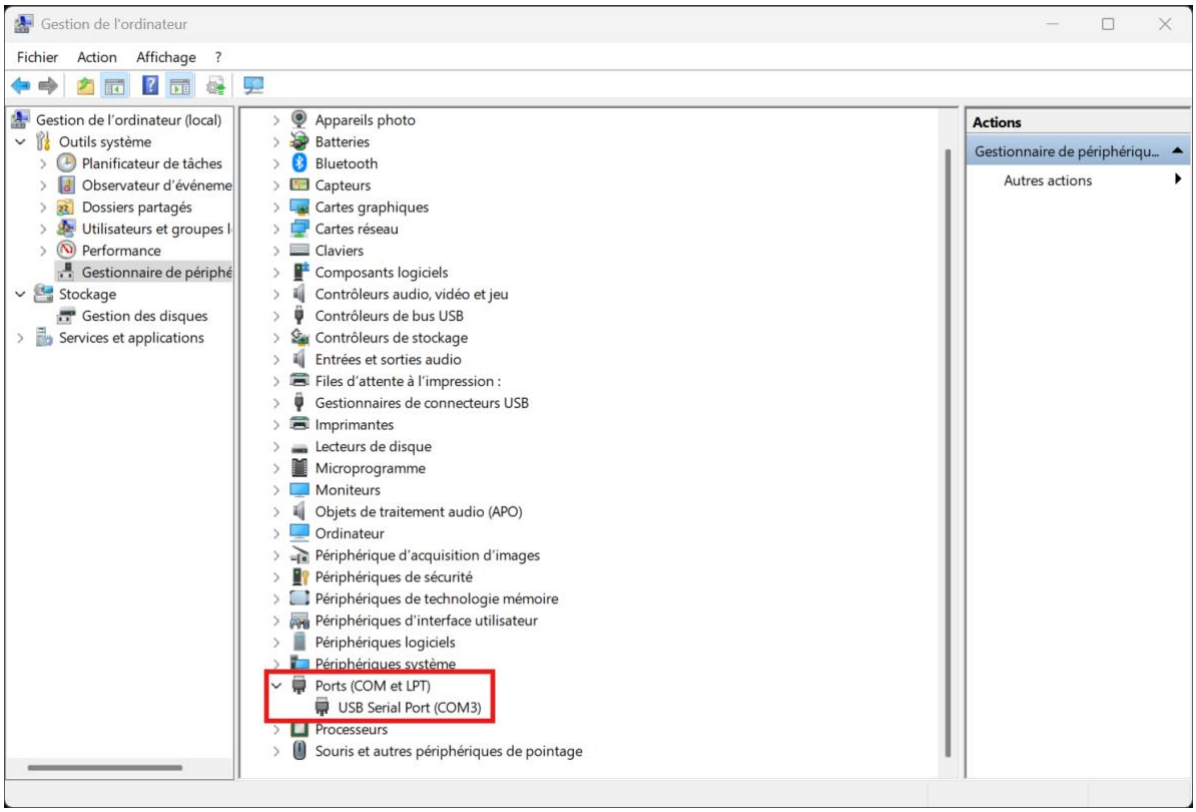
Premièrement, nous allons insérer notre clé USB et démarrer le logiciel Rufus (disponible sur le site https://rufus.ie/).

Dans ce dernier, nous allons devoir sélectionner notre clé USB, puis notre fichier .img et puis enfin cliquer sur « démarrer » pour créer notre clé bootable

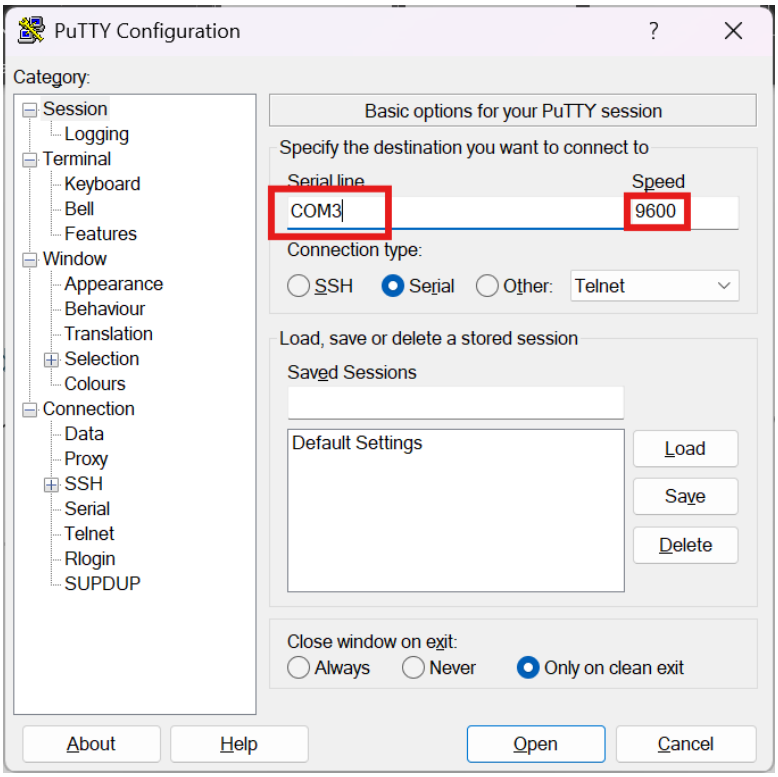


Une fois ceci fait, nous allons pouvoir l'insérer dans notre Riverbed et le démarrer.

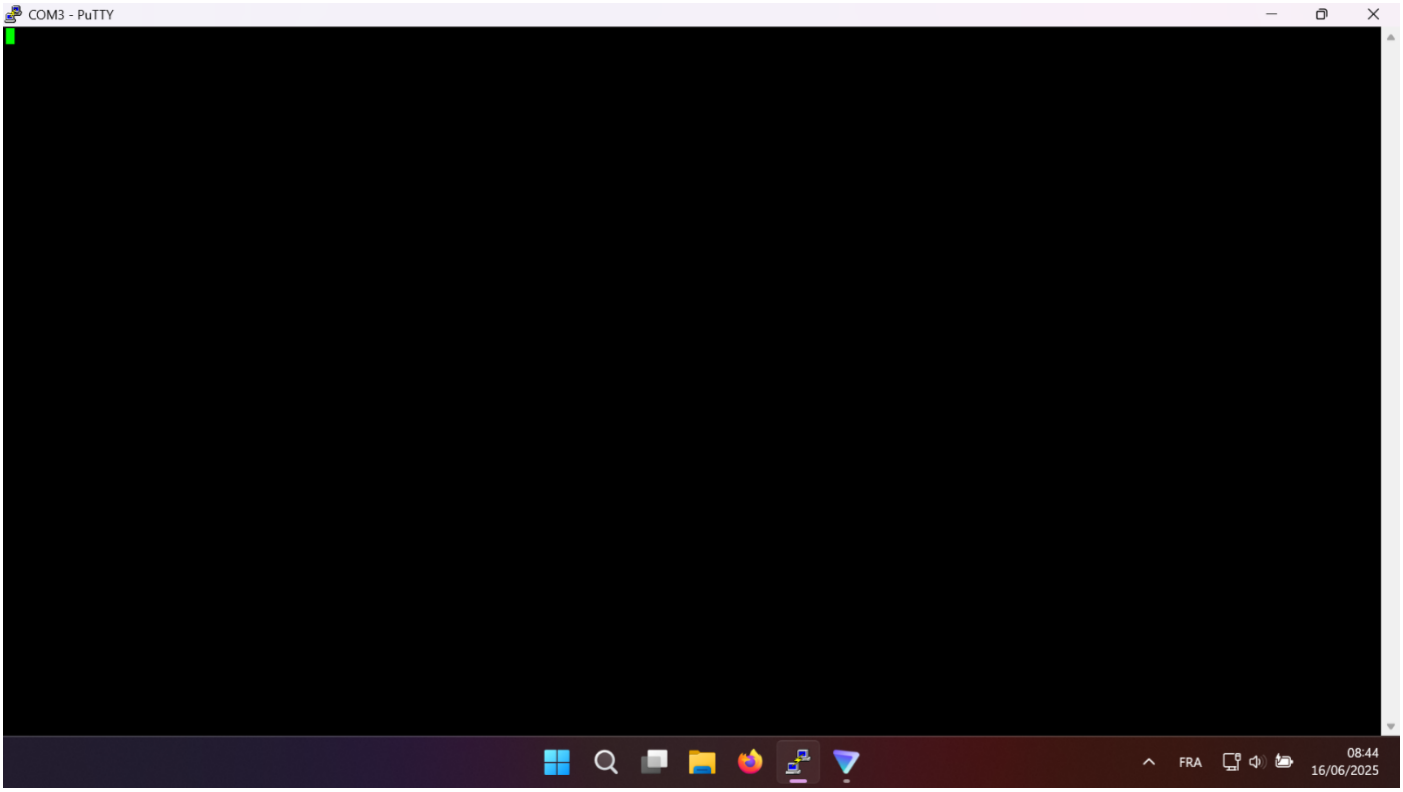
La première étape à partir de maintenant est de démarrer dans le BIOS, pour cela nous allons connecter notre câble console sur le port console du Riverbed, ainsi que le câble USB sur notre PC. Pour vérifier quel interface COM est assigné sur notre ordinateur. Pour cela il suffit d'ouvrir le gestionnaire de périphérique sur Windows et puis d'aller dans « Ports (COM et LPT)



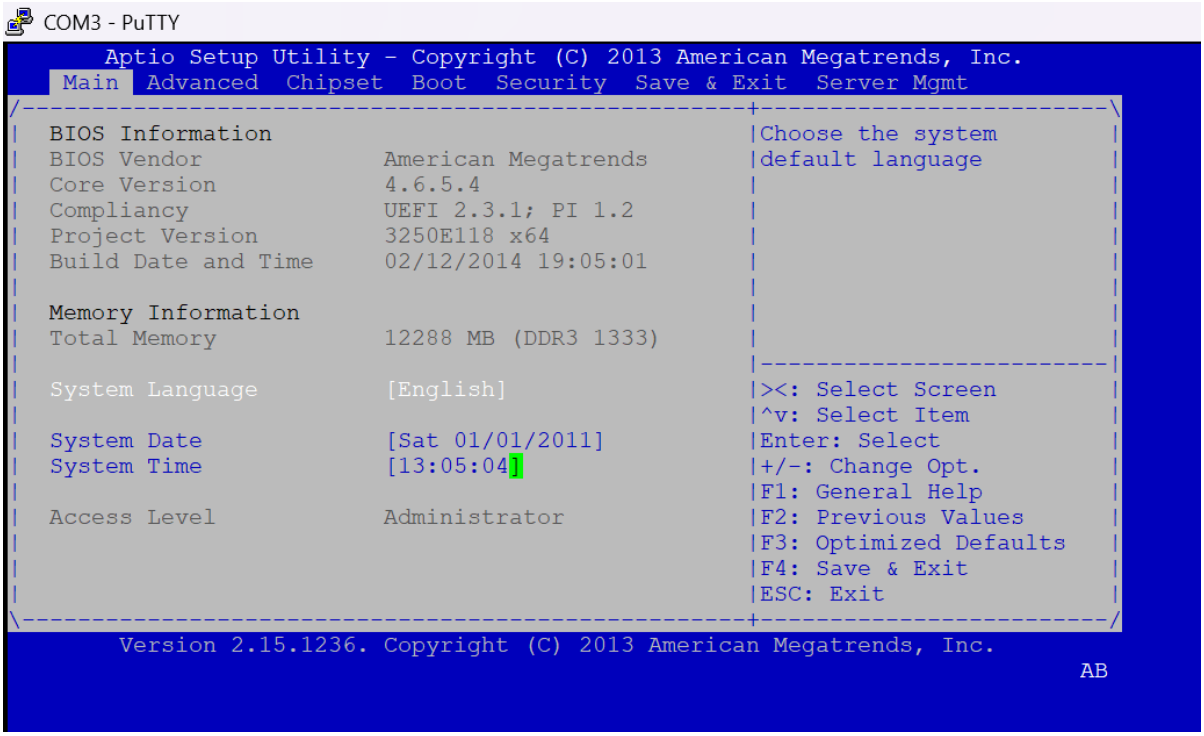
Dans notre cas on observe que le port COM est le « COM3 », on va pouvoir s'en servir pour se connecter dessus. Pour cela nous allons télécharger PuTTY (https://putty.org/) et l'installer, ce logiciel nous permet de nous connecter via le port console de notre Riverbed



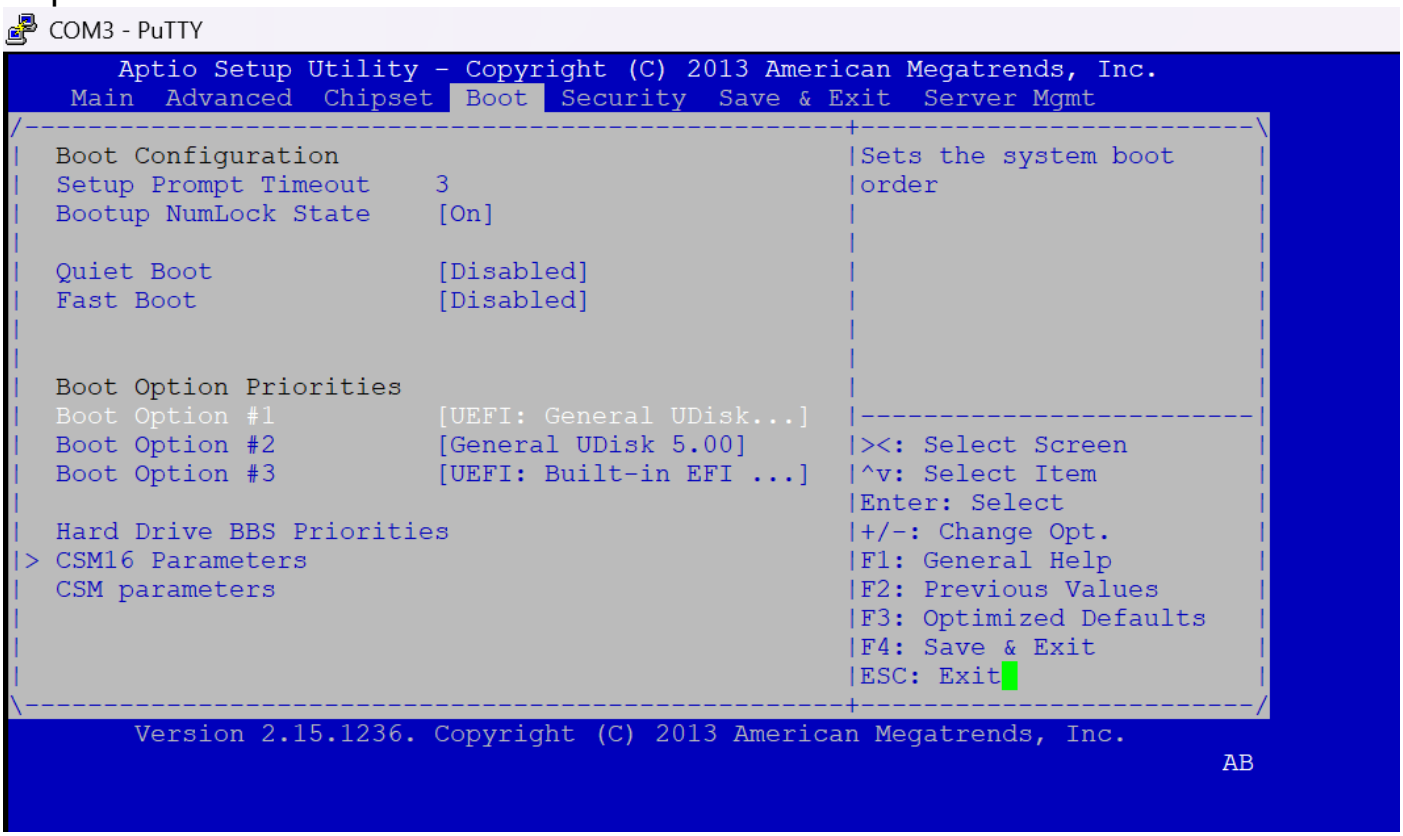
Pour le moment, pour accéder au BIOS de notre Riverbed, nous allons laisser la vitesse par défaut (9600), nous devrons la modifier plus tard afin d'accéder à OPNsense.



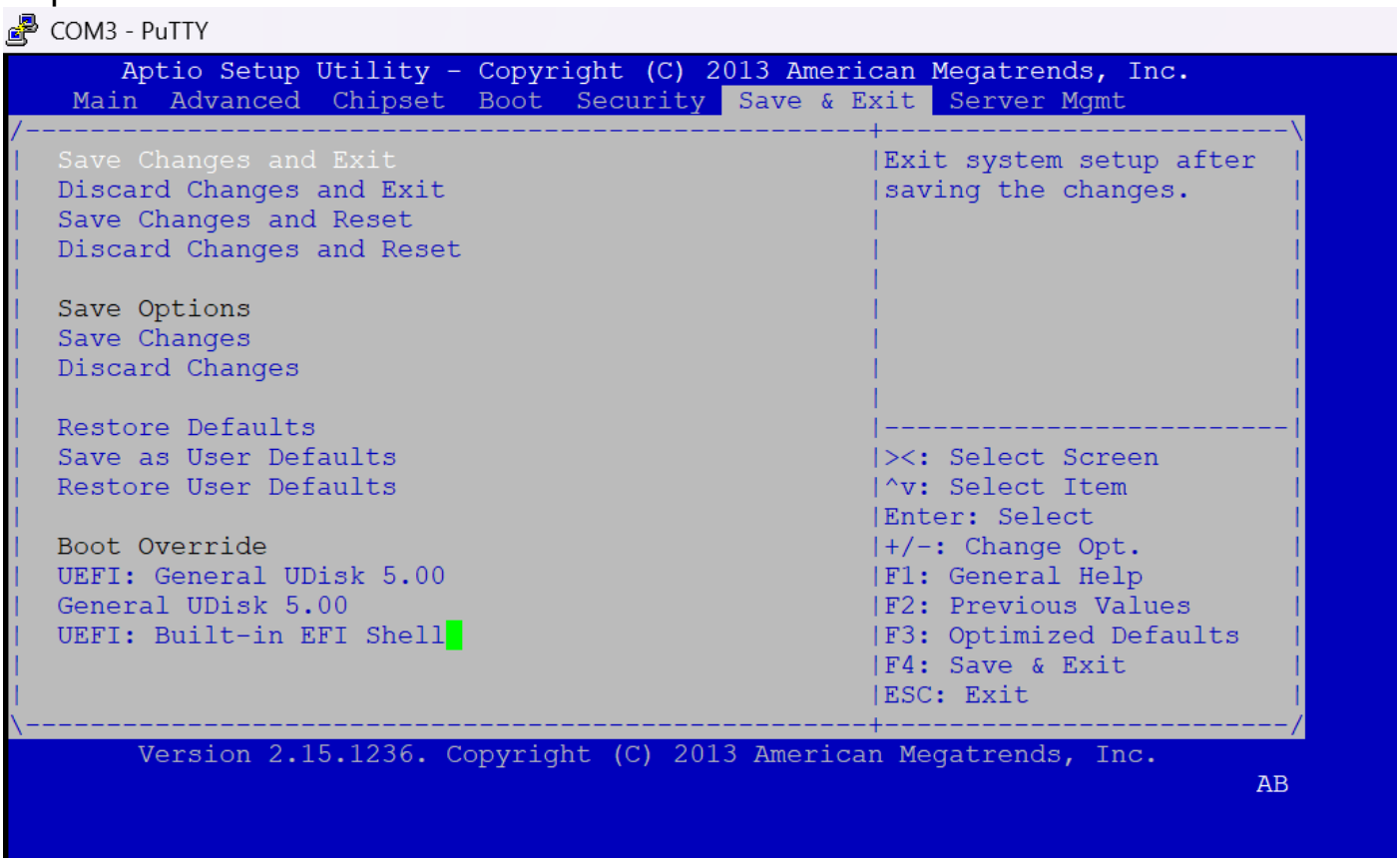
Une fois que l'on arrive sur cet écran, nous pouvons démarrer notre Riverbed. Au démarrage, nous aurons la possibilité d'appuyer sur F2 ou Del pour accéder au BIOS, ce que nous allons faire.



Une fois que nous arrivons ici, nous pouvons nous rendre dans « Boot » pour voir quel est notre périphérique de démarrage par défaut



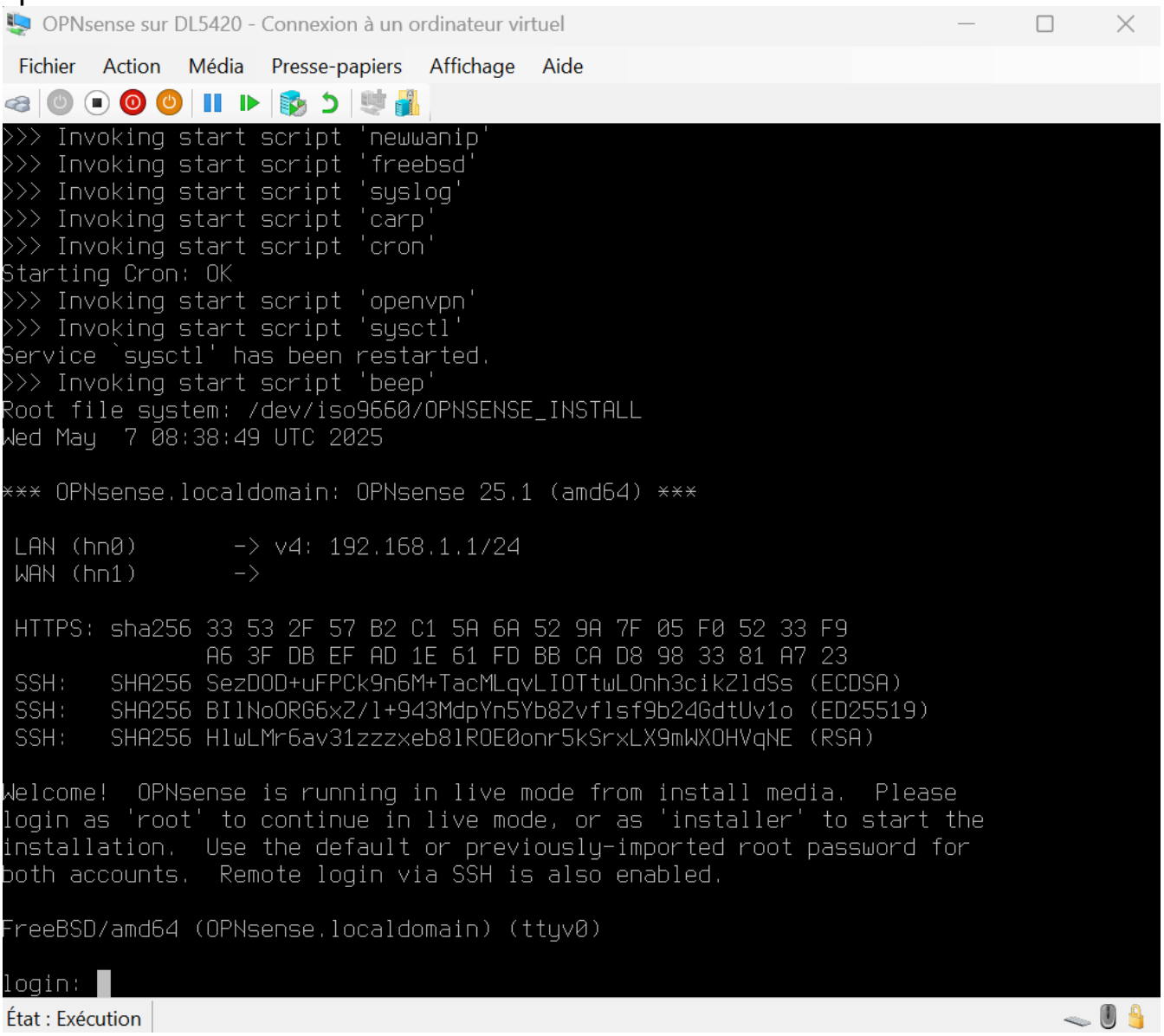
Nous remarquons que la clé USB est bien définie en « Boot Option #1 », nous pouvons allons donc appliquer les changements et redémarrer



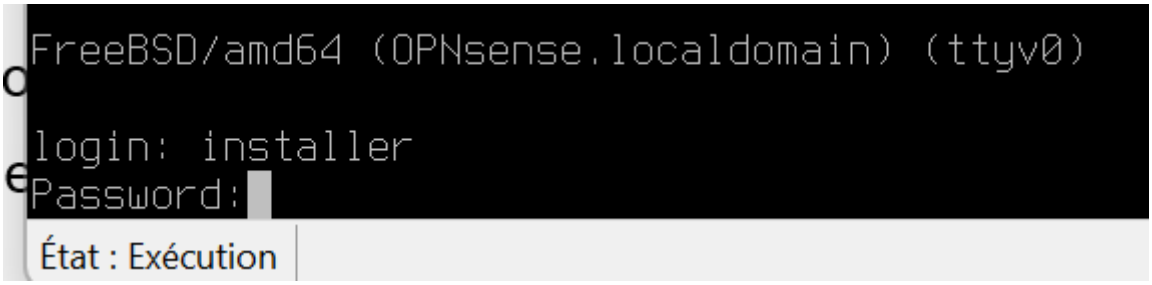
3. Installation d'OPNsense

Après cela, il suffit d'attendre quelques secondes le temps que la machine virtuelle démarre.

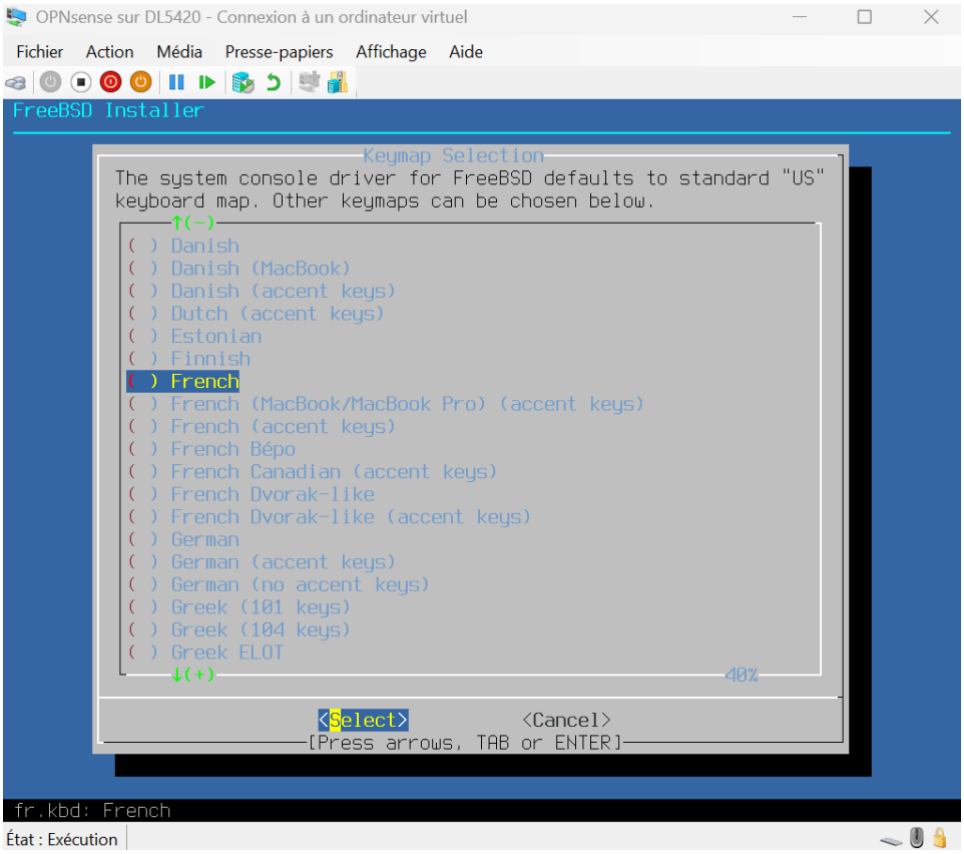
Une fois que ce dernier a démarrer, nous arrivons sur cet écran :

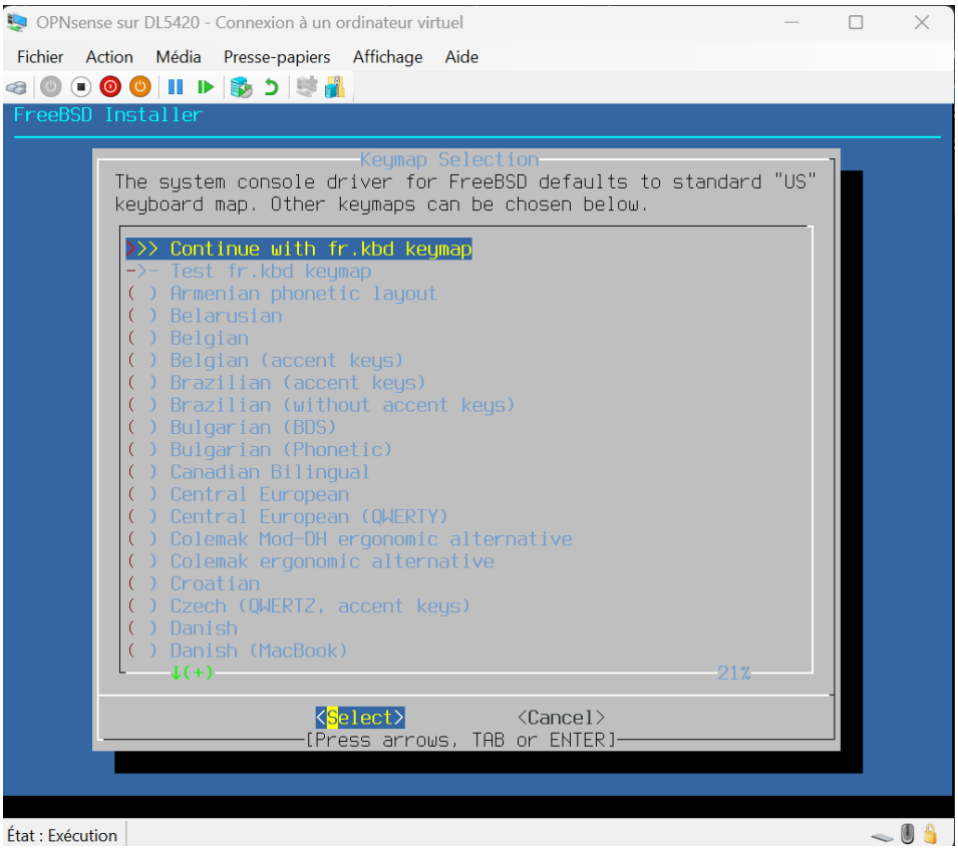


Ici, nous remarquons qu'il est indiqué que si nous souhaitons tester notre installation, nous pouvons nous connecter en tant que « root », mais que si nous souhaitons installer le système sur le disque HDD. Nous pouvons se connecter en tant que « installer ». Le mot de passe de ces comptes par défaut est « opnsense » :

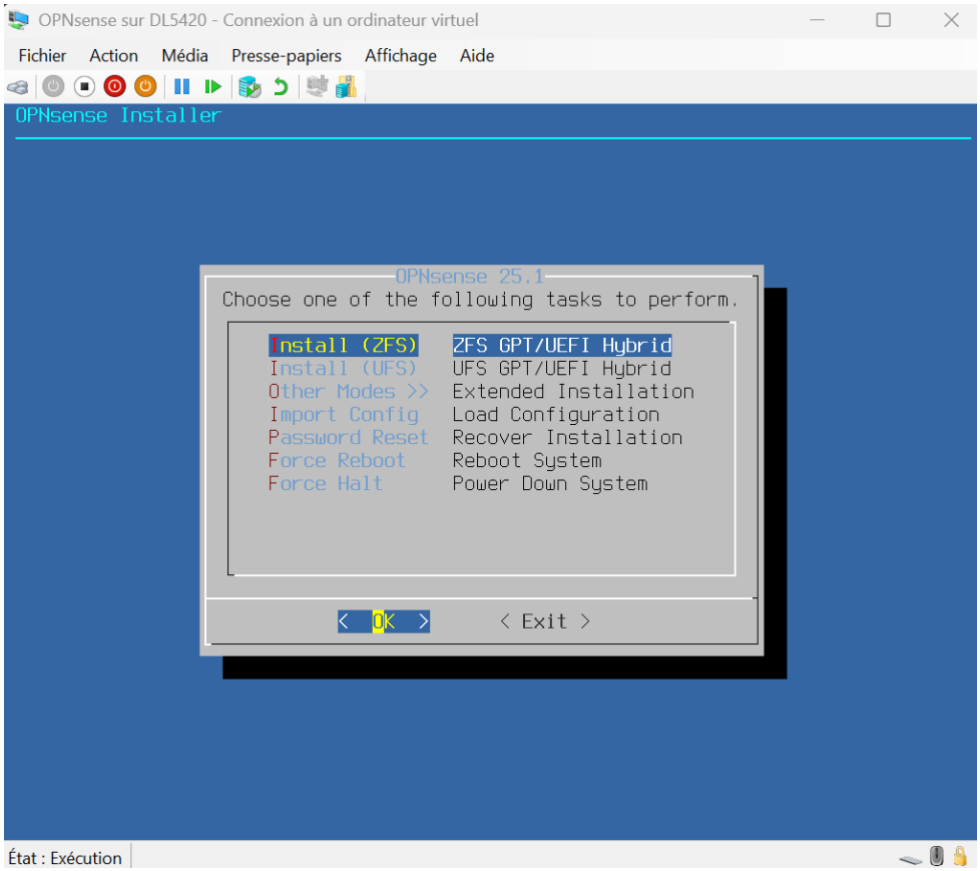


Une connecté, nous arrivons dans un menu pilotable au clavier nous demandant de choisir la disposition du clavier, dans notre cas nous allons choisir le clavier français (French) dans la liste et cliquer sur espace pour confirmer :

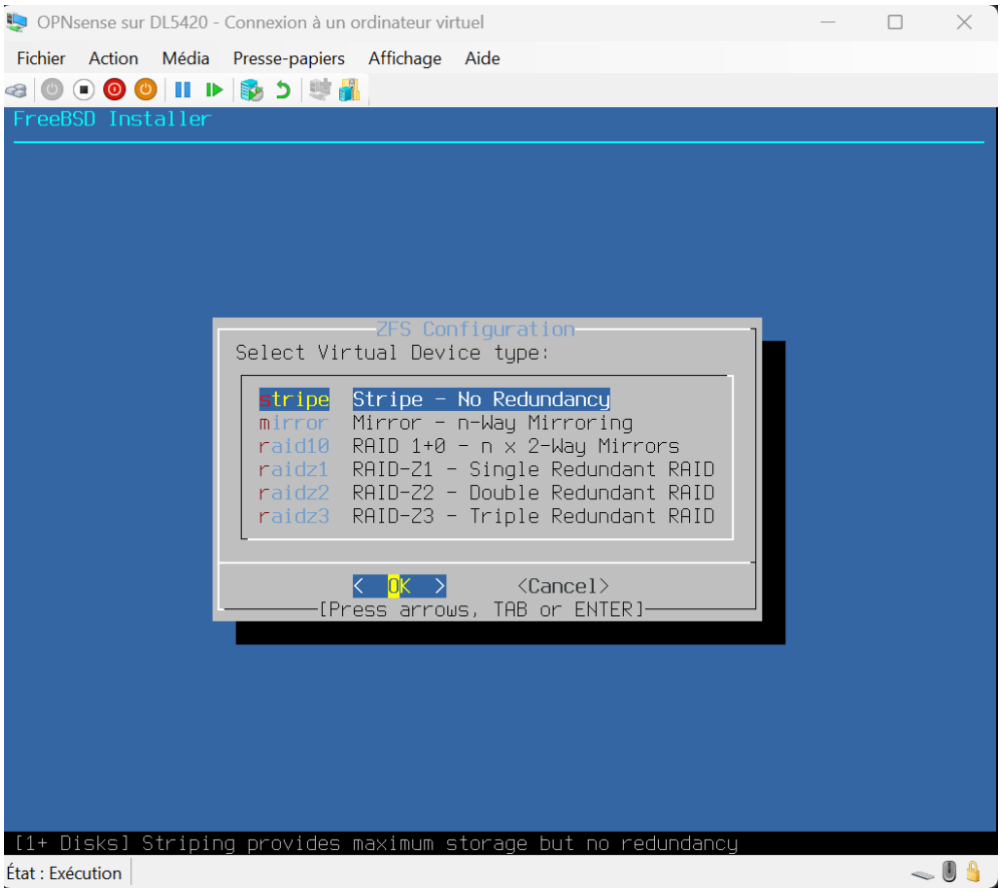




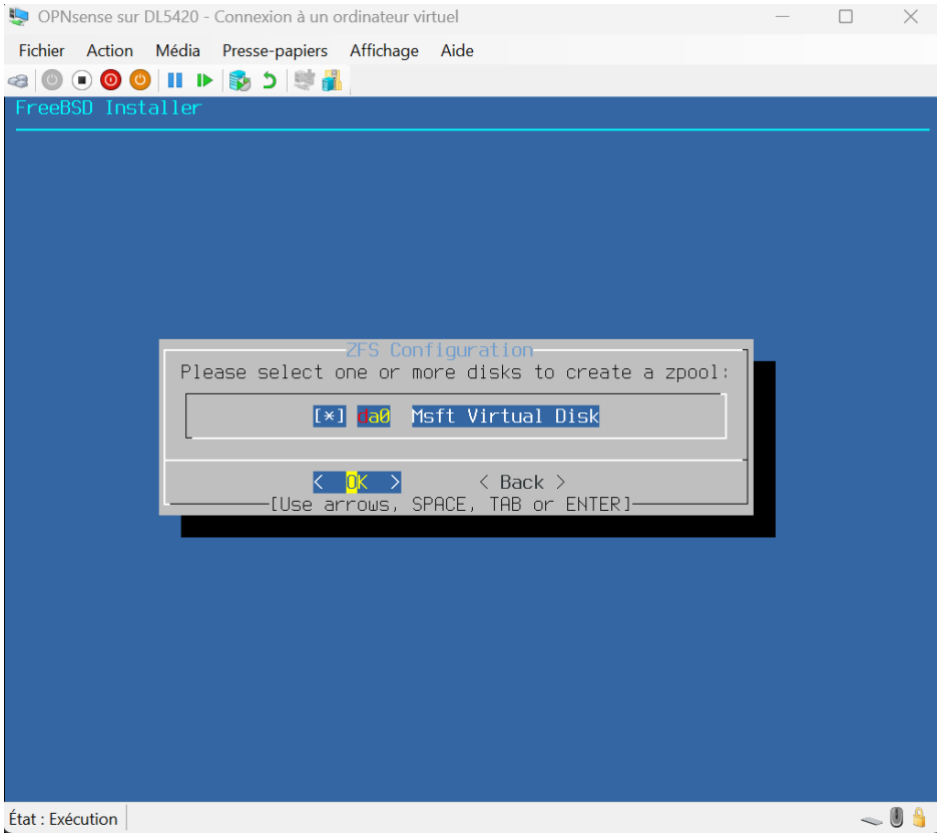
Ensuite, il suffit de sélectionner la première option pour installer OPNsense (Install ZFS)



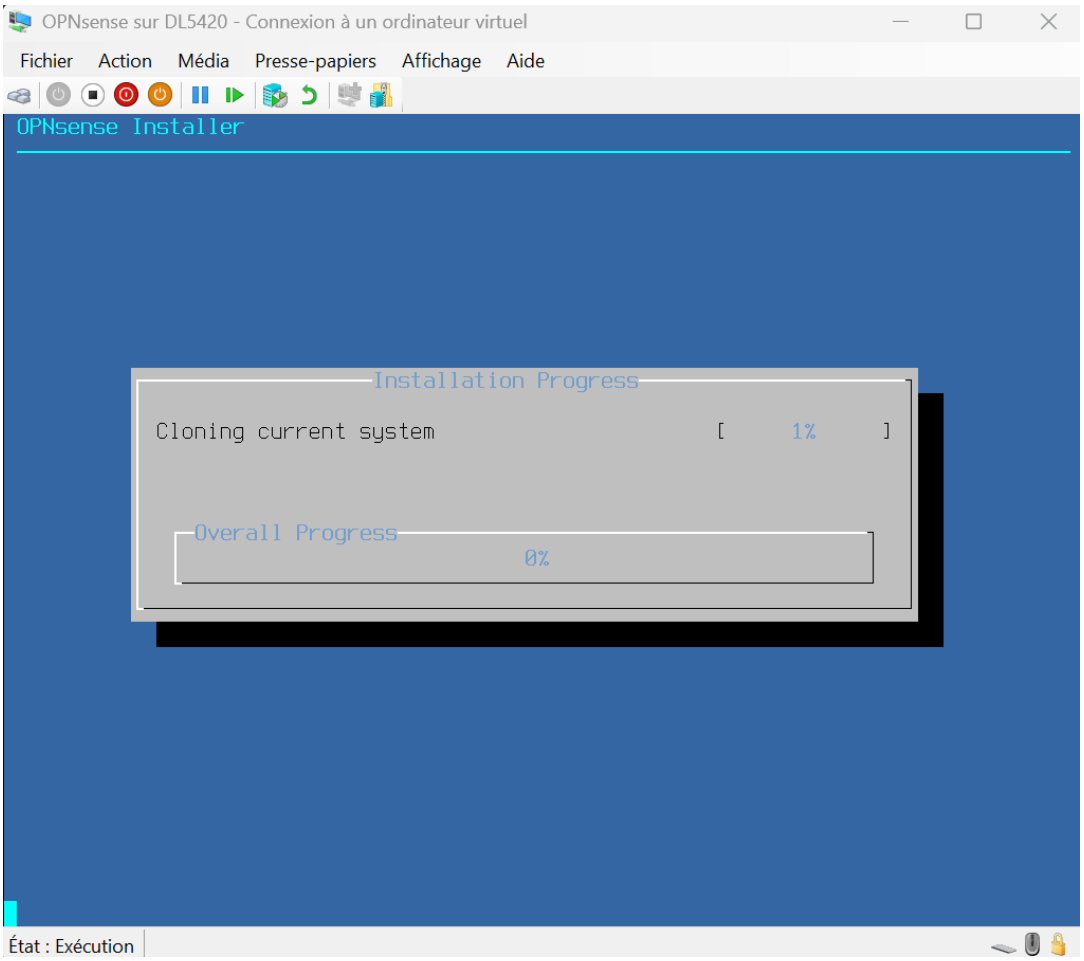
Puis nous allons avoir des options pour la redondance des données, dans notre cas nous allons sélectionner la première option (stripe) permettant de faire une installation sans redondance des données :



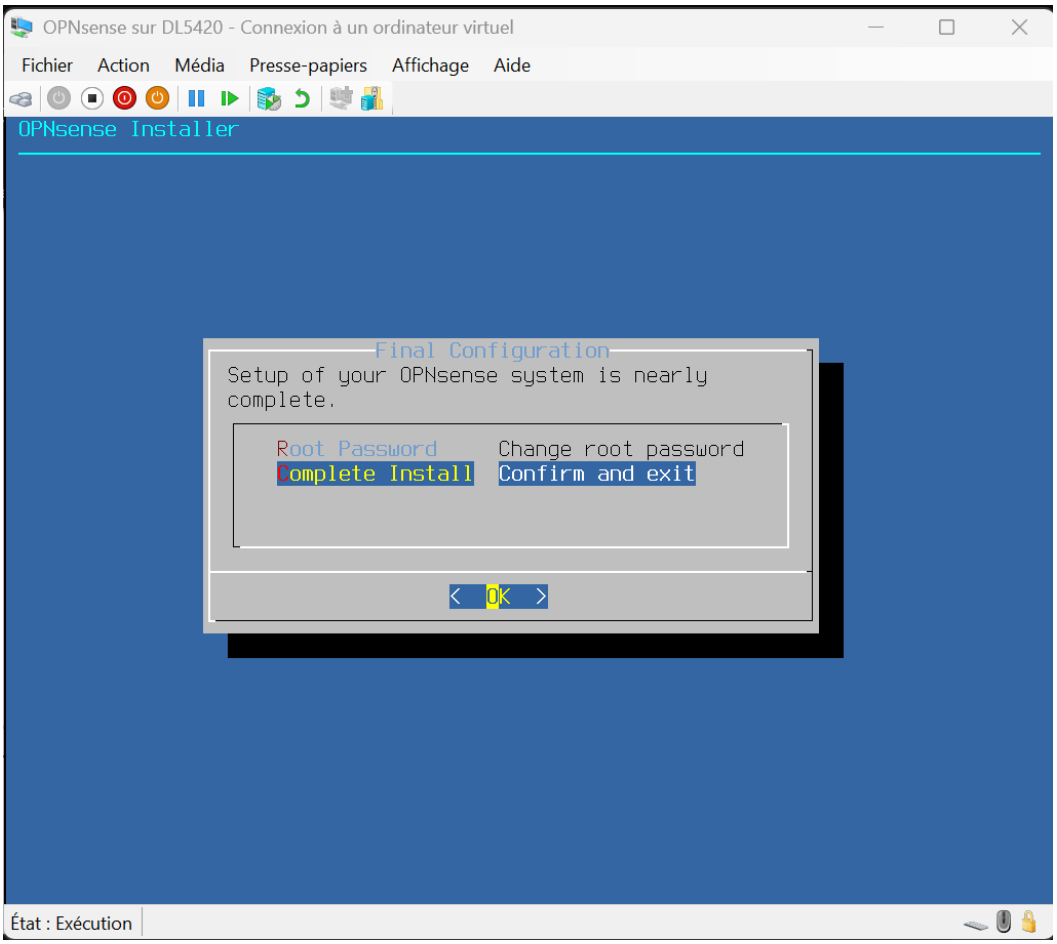
Puis enfin, nous allons sélectionner notre disque puis nous allons confirmer :



Une fois ceci fait, il suffit de patienter que l'installation se termine :



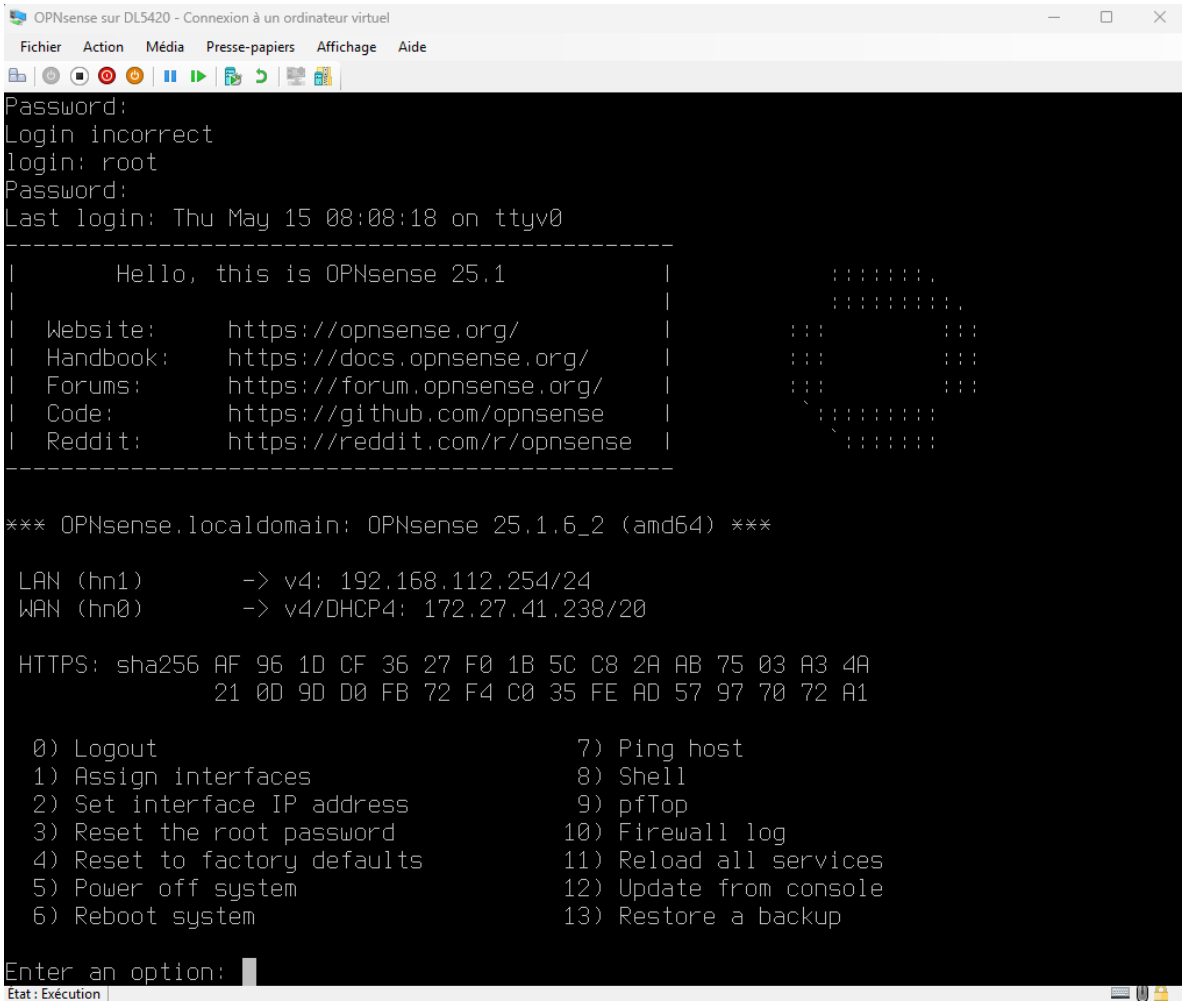
Une fois notre installation terminé, l'installateur nous propose directement de modifier le mot de passe administrateur (root), nous le feront plus tard en post installation. Une fois que nous ayons fais « complete install » nous pouvons faire « power off » pour éteindre le Riverbed OPNsense :



Partie 2 : Post installation, configuration des interfaces, IP, mot de passe et langue

1. Modification du mot de passe root

Une fois OPNsense démarré, nous pouvons nous connecter avec le login root, ainsi que le mot de passe par défaut (opnsense) :



Une fois sur cette interface, nous pouvons modifier différents aspects de notre firewall comme par exemple notre mot de passe root (étant le compte de connexion). Pour cela il suffit d'appuyer sur « 3 » pour aller dans « Reset the root password », après cela on confirme en appuyant sur « Y » puis entrée, et puis on peut enfin modifier notre mot de passe root :

```
Enter an option: 3

The root user login behaviour will be restored to its defaults.

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

Type a new password:
Confirm new password:

The root user has been reset successfully.
```

2. Configuration des interfaces réseaux

Par défaut, les interfaces WAN et LAN ne sont pas configurés correctement, pour corriger cela, il suffit de mettre la bonne interface physique (igbX) sur le côté WAN/LAN. Pour cela, dans le premier menu d'OPNsense, il suffit de se rendre dans le menu « 1 » :

```
 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
```

Igb4 et igb5 correspondant aux interfaces physiques PRI et AUX, tandis que les autres correspondent aux interfaces physiques LAN0_X et WAN0_X. Il faut donc essayer les différentes interfaces pour voir lesquels sont liés au WAN et au LAN.

Dans notre cas :

WAN/LAN	WAN	LAN
INTERFACE LOGIQUE	igb2	Igb5

INTERFACE PHYSIQUE	LAN0_1	AUX

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

Valid interfaces are:

igb0            00:0e:b6:c2:7c:b6 Intel(R) I347-AT4 DH89XXCC
igb1            00:0e:b6:c2:7c:b7 Intel(R) I347-AT4 DH89XXCC
igb2            00:0e:b6:c2:7c:b8 Intel(R) I347-AT4 DH89XXCC
igb3            00:0e:b6:c2:7c:b9 Intel(R) I347-AT4 DH89XXCC
igb4            00:0e:b6:74:62:68 Intel(R) I210 (Copper)
igb5            00:0e:b6:74:62:69 Intel(R) I210 (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 interface name or 'a' for auto-detection:
```

3. Configuration des adresse IP

Cette fois ci, nous allons nous rendre dans le paramètre « 2 ».

Dans ces paramètres, nous allons pouvoir définir un plan d'adressage à la fois pour le WAN, ainsi que le LAN. Voici le plan d'adressage proposé :

WAN/LAN	WAN	LAN
ADRESSE IP	192.168.0.51	192.168.2.254
MASQUE DE SOUS RESEAU	255.255.255.0	255.255.255.0
PASSERELLE	192.168.0.254	(Même que le firewall étant donné que c'est lui le routeur)
PLAGE D'IP (SERVEUR DHCP)	-	192.168.2.1 – 192.168.2.10

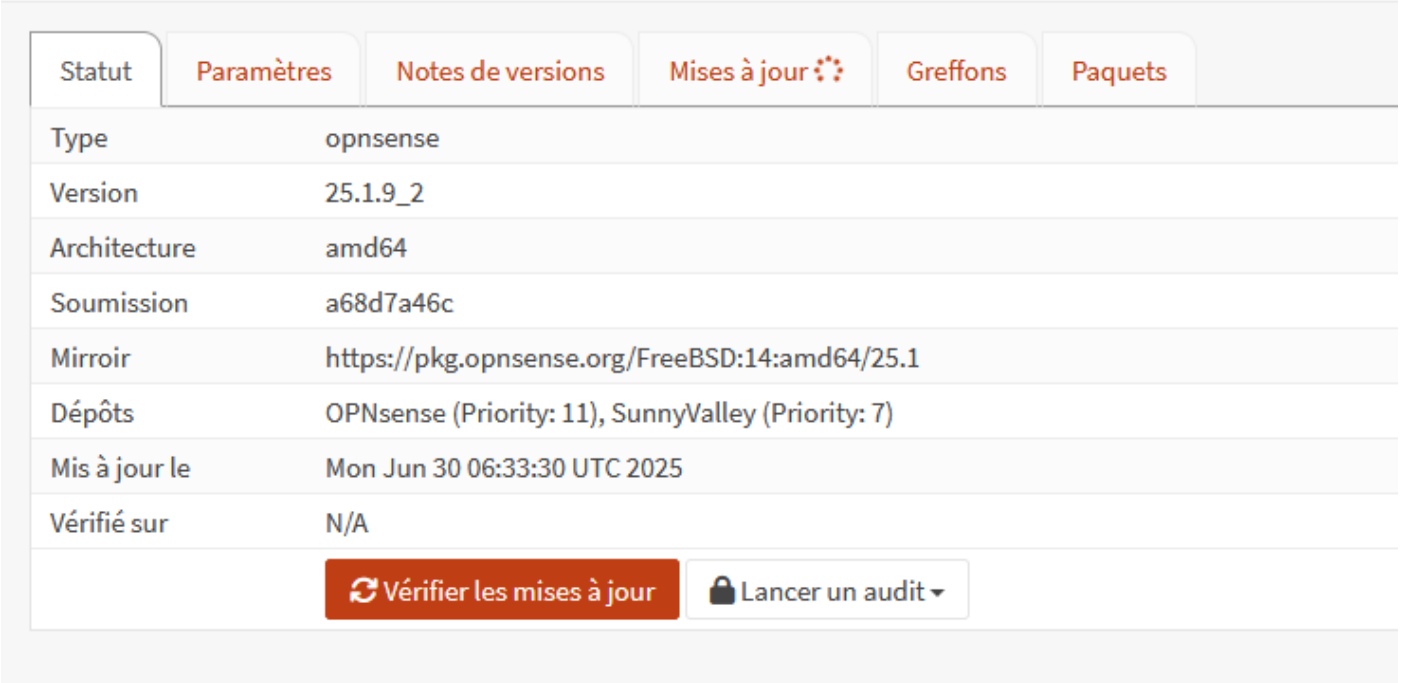
```
Enter an option: 2

Available interfaces:

1 - LAN (igb5 - static)
2 - WAN (igb2 - static)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N]

Enter the new LAN IPv4 address. Press <ENTER> for none:
>
```

4. Accès à l'interface web et mise à jour du firewall

Une fois que tout est configuré, nous pouvons connecter un PC sur le LAN du firewall. Etant donné que nous avons configuré un serveur DHCP, ce dernier va automatiquement récupérer une adresse IP.

Pour accéder à l'interface web, il suffit de se rendre sur un navigateur et d'y indiquer l'IP de notre routeur : http://192.168.2.254

Une fois dedans, il suffit de se rendre dans « Système », puis « Firmware » et enfin « Mise à jour »



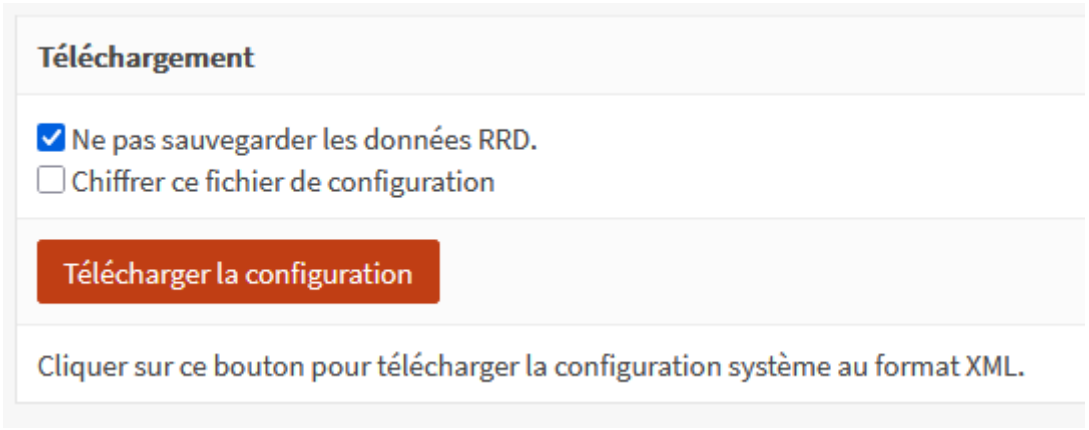
Une fois sur cet écran, il suffit de cliquer sur « Vérifier les mises à jour » et de confirmer l'installation de ces dernières

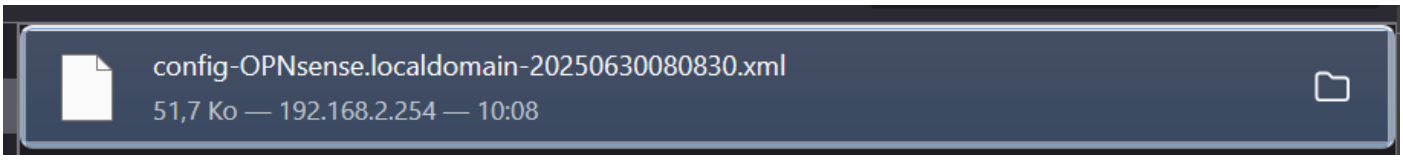


Une fois que ces dernières ont été installés, le firewall nous proposera de redémarrer, ce qui est important de faire après la mise à jour.

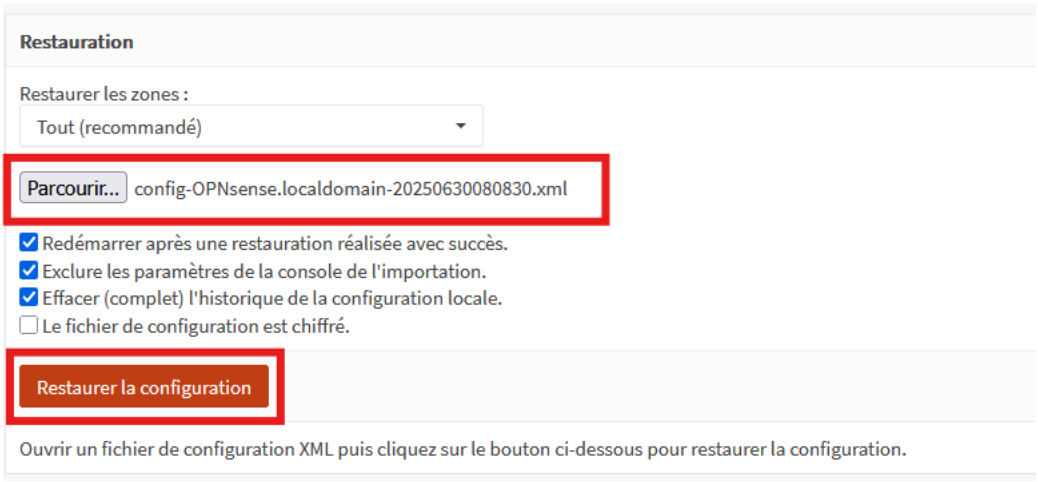
5. Importer et exporter la configuration

Pour exporter, il suffit, toujours dans l'interface graphique, de se rendre dans « Système », puis dans « Configuration » et enfin dans « Sauvegardes ». Pour exporter, il suffit de cliquer sur « Télécharger la configuration », ce qui va nous permettre d'obtenir un fichier au format XML





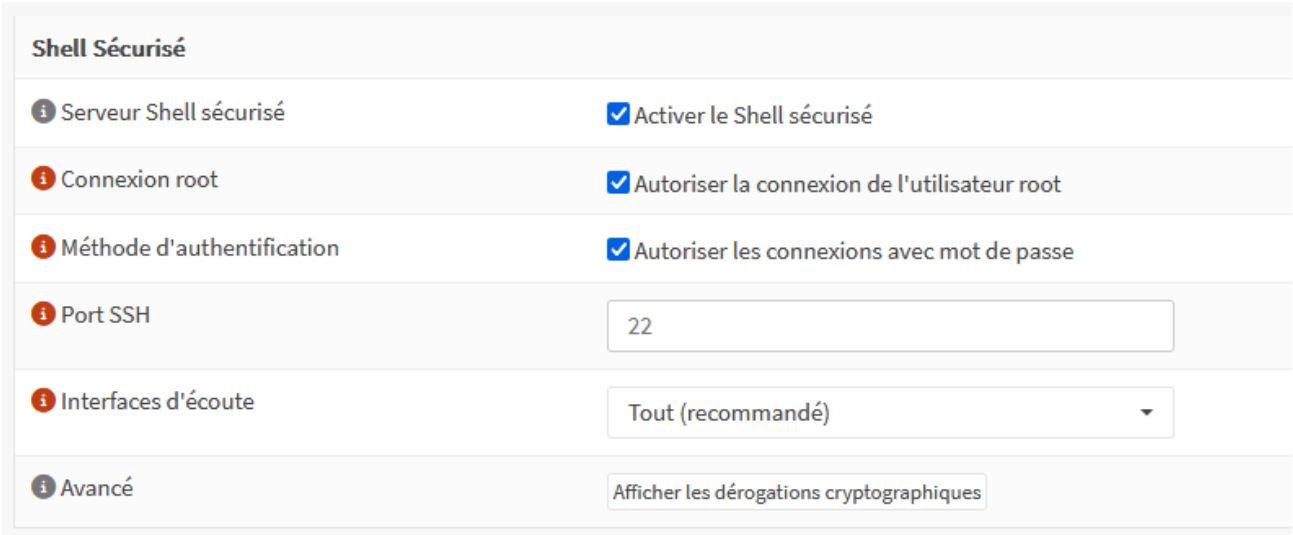
Pour restaurer cette dernière, toujours dans le même menu, il suffit de se rendre dans restauration, de sélectionner notre fichier et puis de cliquer sur restaurer en gardant les paramètres par défaut. A noté que le firewall va redémarrer après avoir restauré la configuration



6. Activation du protocole SSH

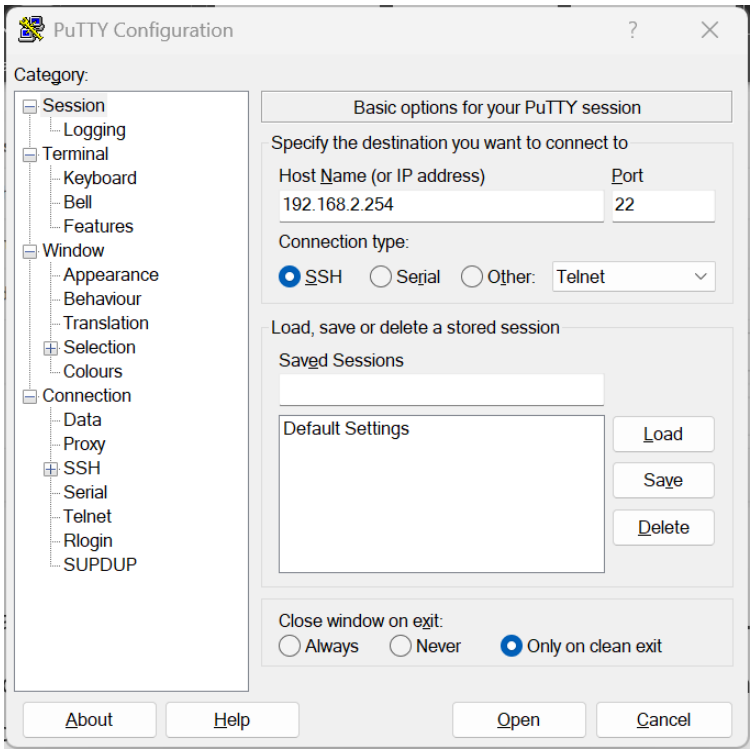
Pour activer le protocole SSH qui permet un accès depuis le réseau à la console d'administration, il suffit de se rendre dans « Système », dans « Paramètres » puis dans « Administration ».

Une fois sur cette page, nous allons nous rendre dans « Shell Sécurisé » puis nous allons cocher les cases : « Activer le Shell sécurisé », « Autoriser la connexion de l'utilisateur root » et « Autoriser les connexions avec mot de passe »

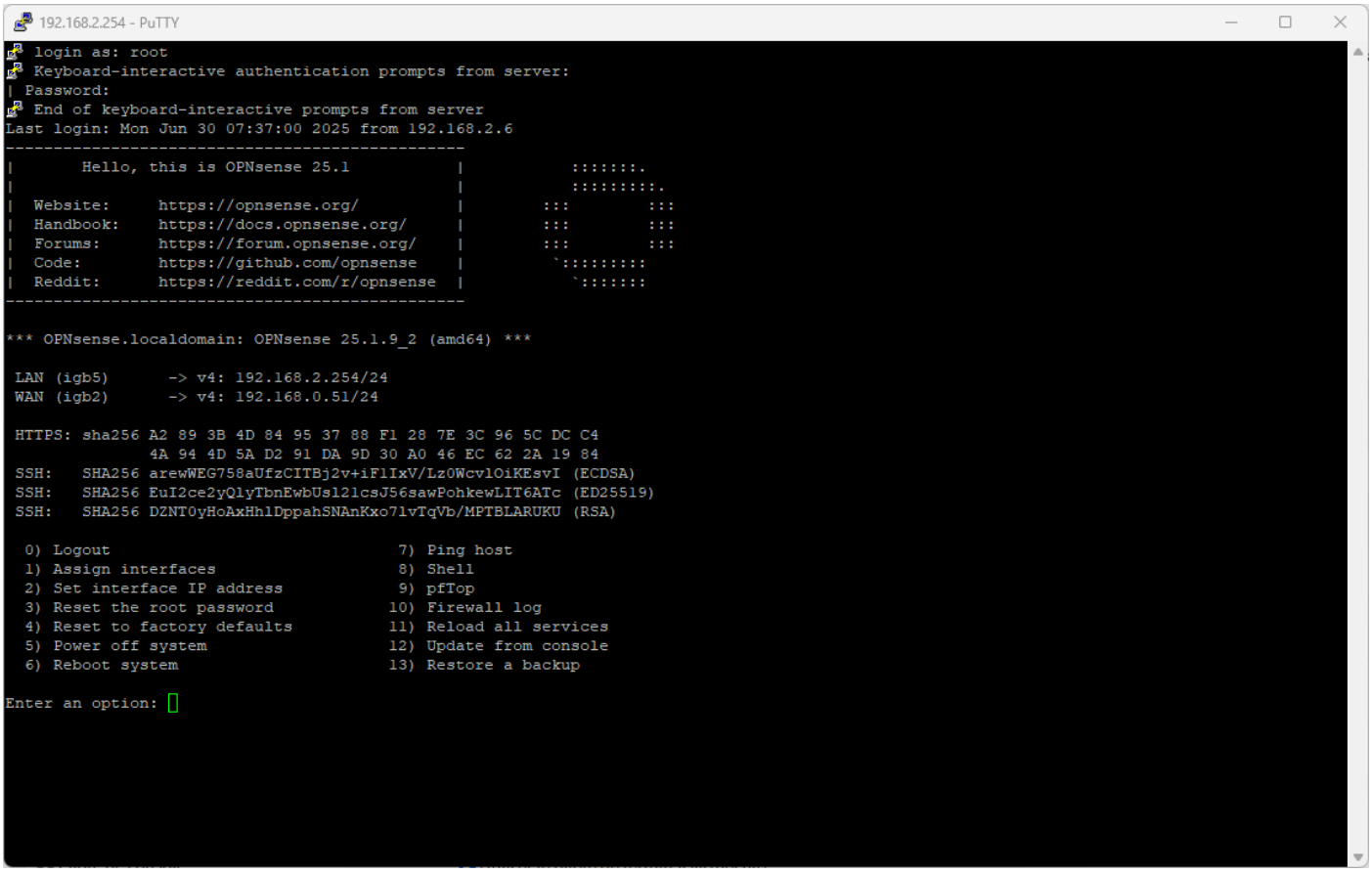


Les autres paramètres ne doivent pas être modifiés (comme le port SSH).

Pour tester notre connexion, il suffit de lancer PuTTY et de tenter une connexion avec l'adresse IP du firewall



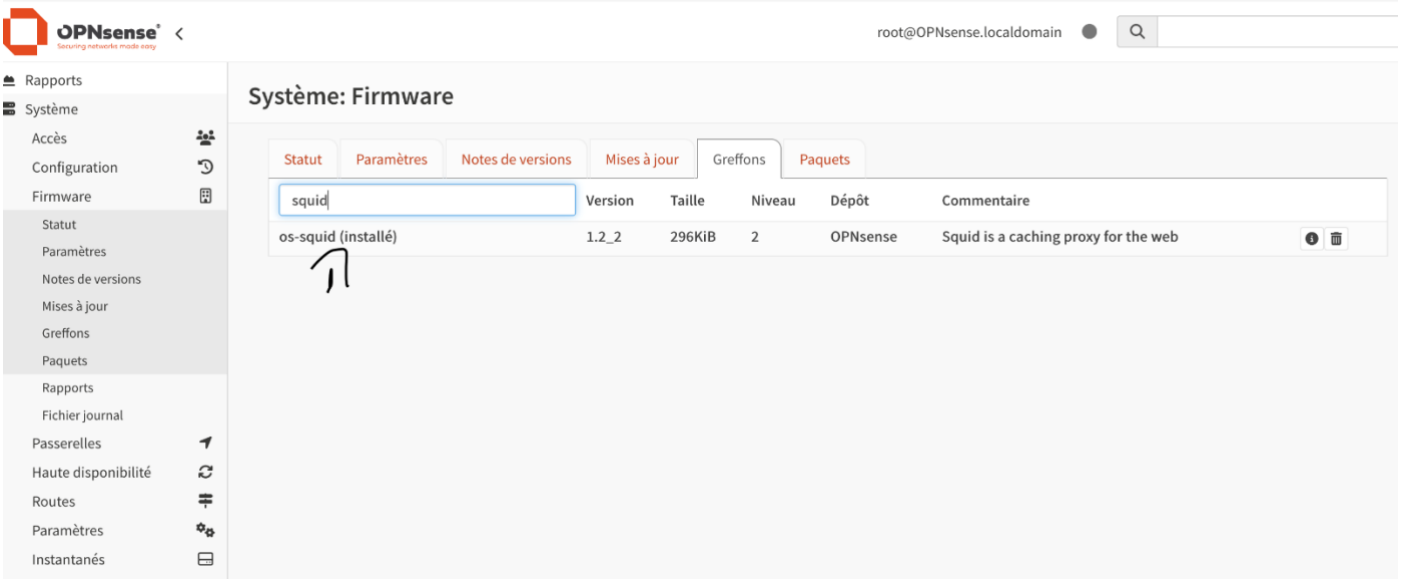
Une fois que l'on a ouvert la connexion, nous pouvons entre notre nom d'utilisateur et mot de passe afin d'accéder à la console d'administration sans connexion en port série !



7. Mise en place d'un web webfiltering

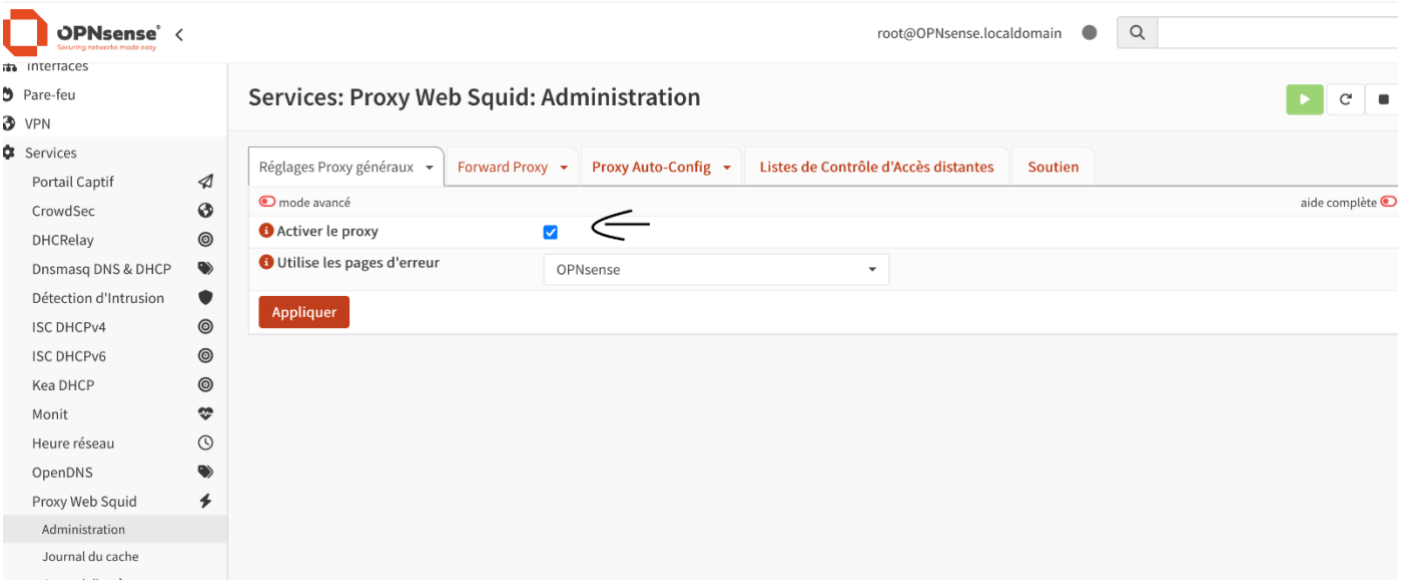
1) Installation du Paquet Squid

- Naviguez vers le menu "Système", puis sélectionnez "Firmware" et enfin "Paquets".
- Utilisez la barre de recherche pour localiser le paquet "squid".



2) Activation Générale du Service Proxy

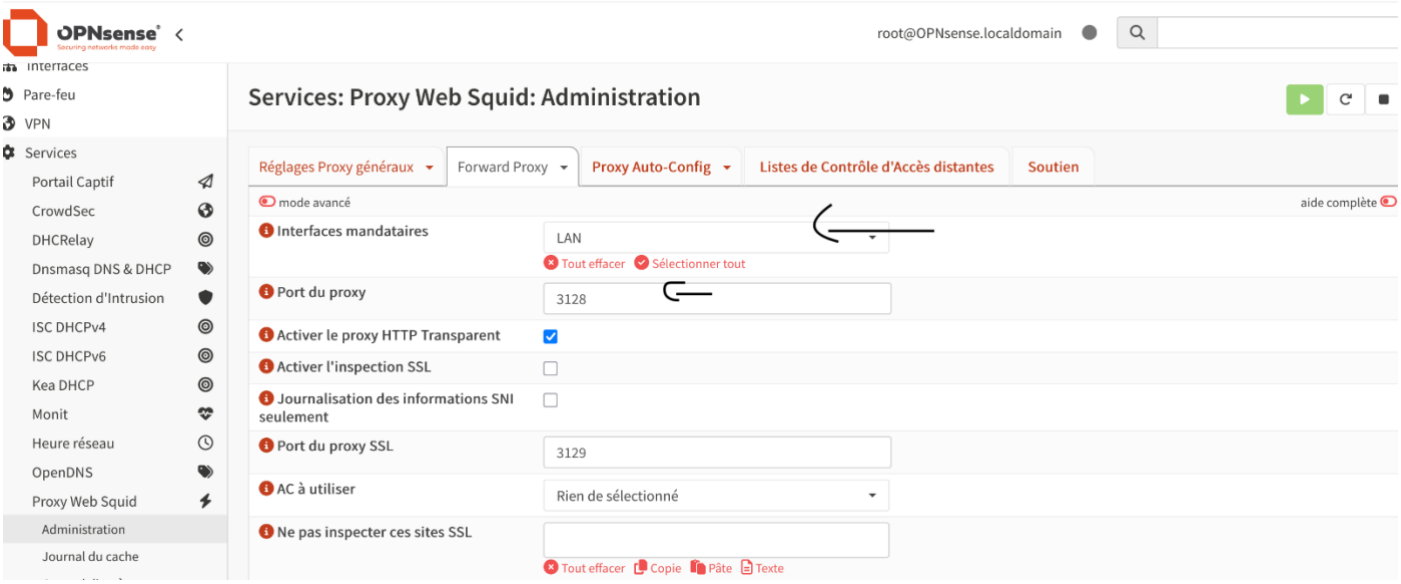
- Accédez à "Services", puis "Proxy Web Squid" et "Administration".
- J'ai coché la case "Activer le proxy".
- Cliquez sur le bouton "Appliquer" pour enregistrer cette modification.



3) Configuration des Paramètres du Proxy Forward

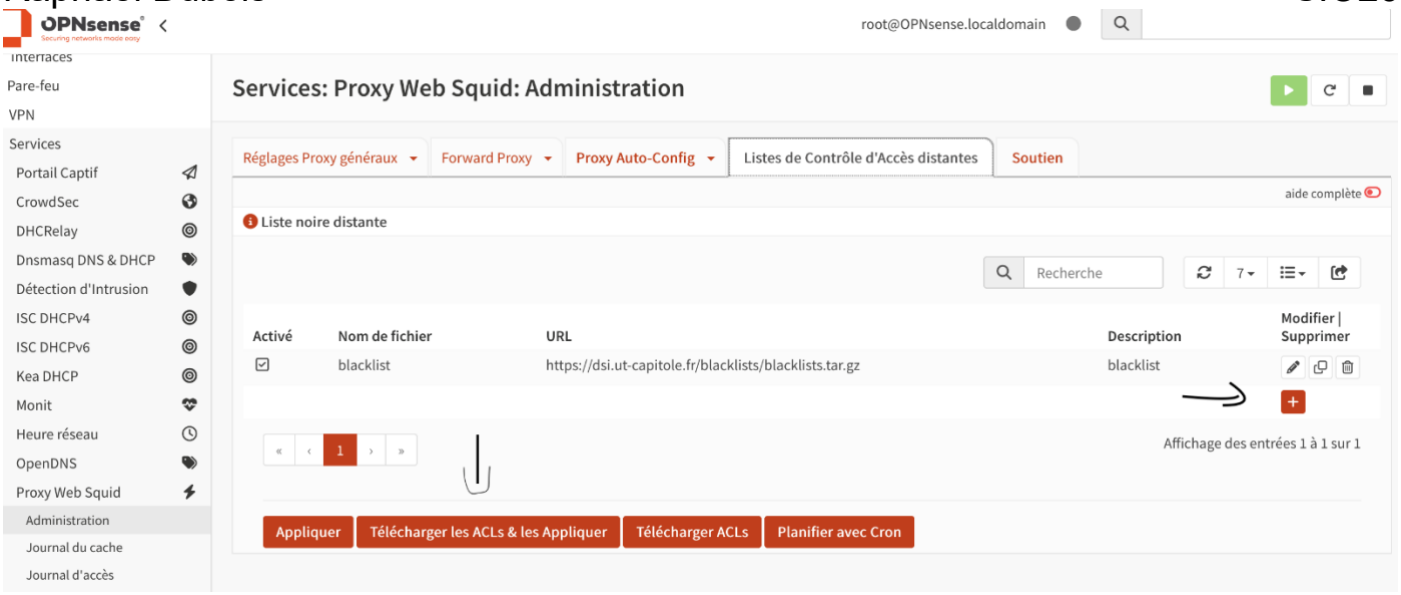
- Toujours dans "Services" > "Proxy Web Squid" > "Administration", sélectionnez l'onglet "Forward Proxy".

- Dans la section "Interfaces obligatoires", choisissez l'interface réseau à travers laquelle le proxy devra opérer, généralement "LAN".
- Le "Port du proxy HTTP" est par défaut "3128" ; il peut être modifié si nécessaire.
- Cochez la case "Activer le proxy HTTP Transparent" pour permettre une interception automatique du trafic HTTP sans configuration manuelle sur les postes clients.



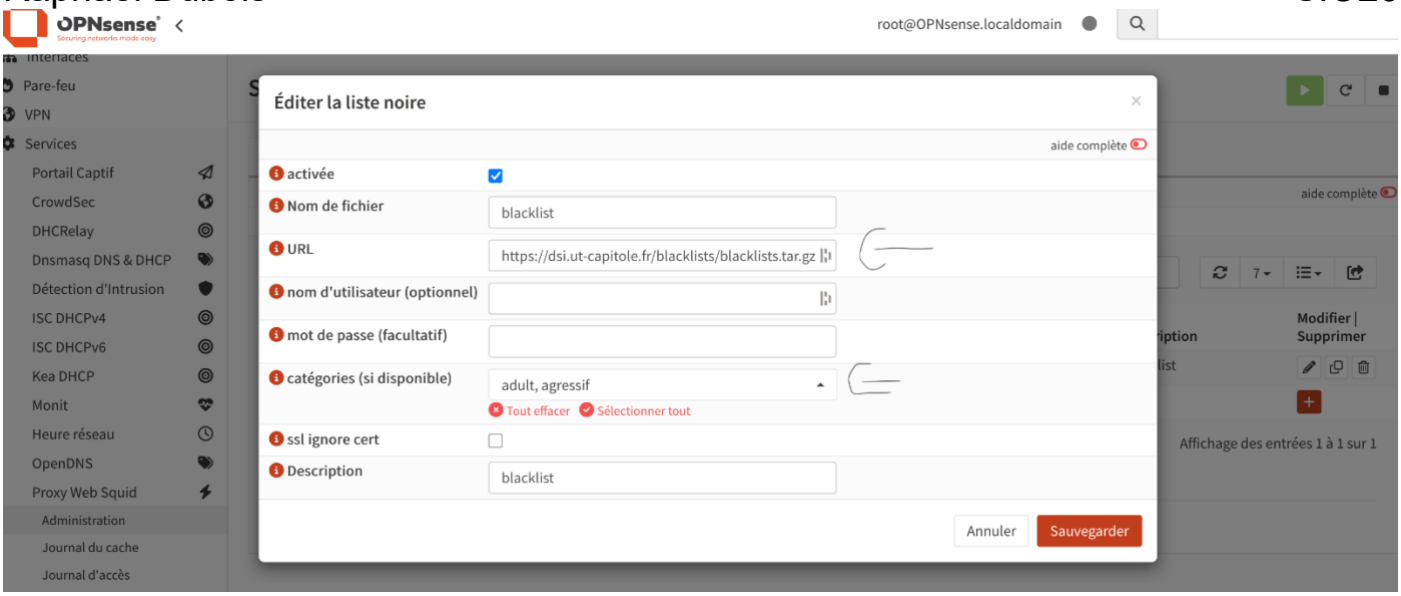
4) Initiation à l'Ajout d'une Liste de Contrôle d'Accès Distante (Blacklist)

- Dirigez-vous vers l'onglet "Listes de Contrôle d'Accès distantes" dans la section "Services" > "Proxy Web Squid" > "Administration".
- Cliquez sur l'icône "Ajouter" (représentée par un plus) pour créer une nouvelle entrée.

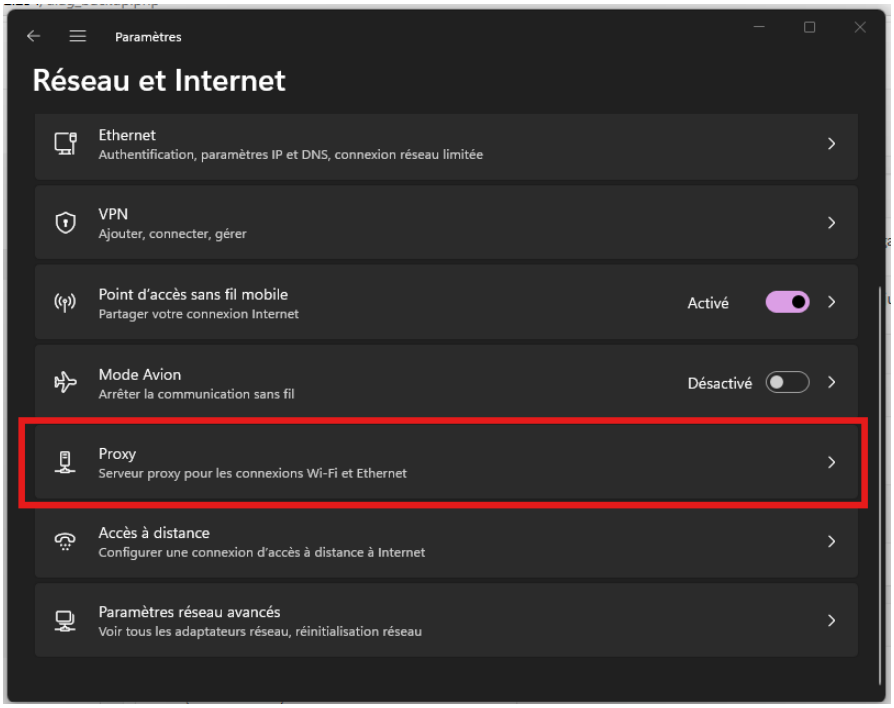


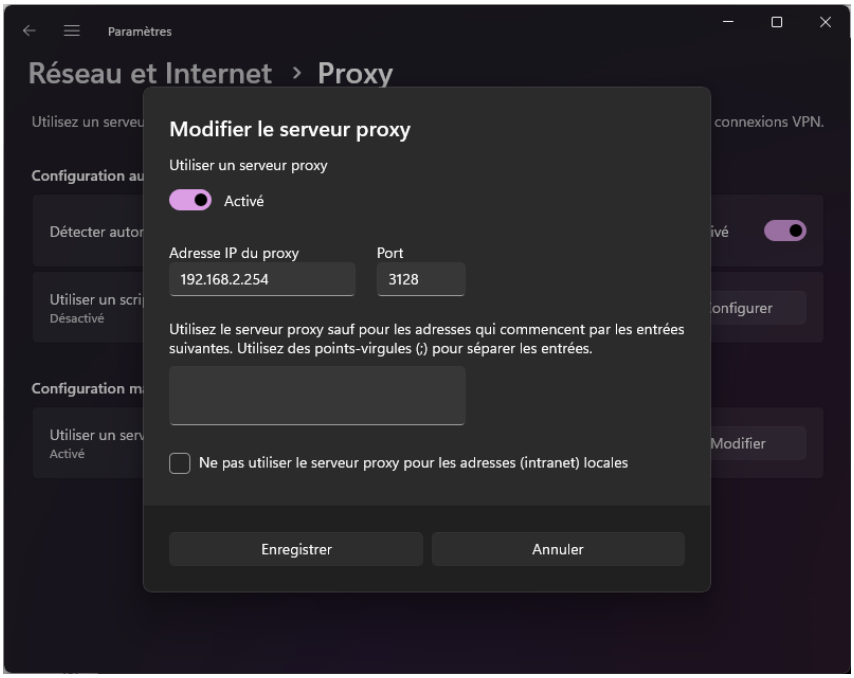
5) Détails de Configuration de la Liste Noire

- Dans la fenêtre d'édition :
  - Cochez "activée" pour activer cette liste.
  - Saisissez un "Nom de fichier" pour identifier la liste, par exemple "blacklist".
  - Indiquez l'"URL" de la liste noire distante. L'exemple donné est https://dsi.ut-capitole.fr/blacklists/blacklists.tar.gz.
  - Dans le champ "catégories (si disponible)", sélectionnez les types de contenu à bloquer (dans mon exemple, "adult").
- Cliquez sur "Sauvegarder" pour valider l'ajout de la liste.

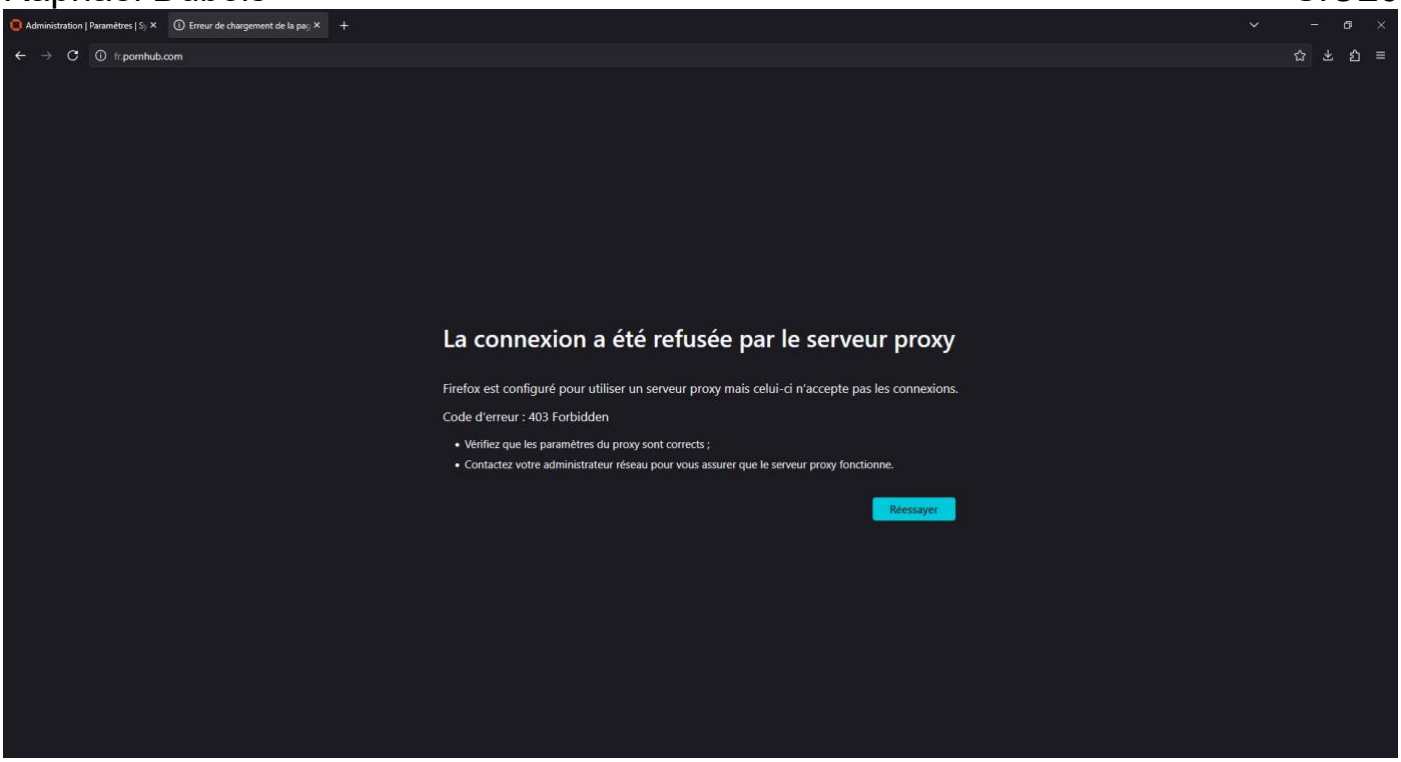


6) Configuration du proxy sur Windows :





Test blocage site adulte :


Administration | Paramètres | Sy
Erreur de chargement de la pag
fr.pornhub.com
La connexion a été refusée par le serveur proxy
Firefox est configuré pour utiliser un serveur proxy mais celui-ci n'accepte pas les connexions.
Code d'erreur : 403 Forbidden
Vérifiez que les paramètres du proxy sont corrects ;
Contactez votre administrateur réseau pour vous assurer que le serveur proxy fonctionne.
Réessayer

Concluant.