Loïc Corneloup

Installation OPNSense

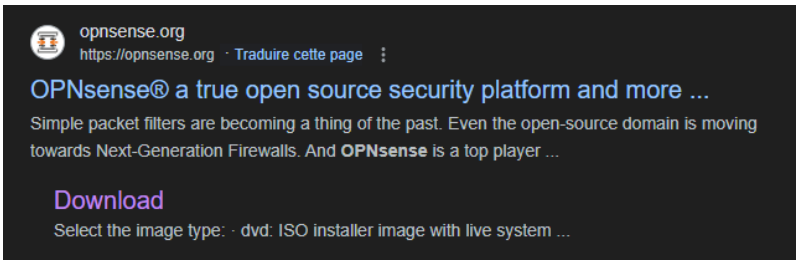
Table des matières :

Configuration Windows : 3
Installation des logiciels 3
Formatage de la clé : 5
Configuration du Pare-feu via Tabby : 6
Tabby : 6
Bios 7
Installation de l'image Opensense 11
Configuration OPNSense 18
Changement du mot de passe Admin / langue 21
MDP Admin firewall 21
Changement de la langue. 22
Sauvegarde / restauration 24
Sauvegarde 24
Restauration 26
Rester en mode usine 27
Sauvegarde 28
Rester 30
Restauration 32
Configuration du webfiltering 33
Configuration 33
Activer le SSH 36
Activer le SSH 36
Test 38

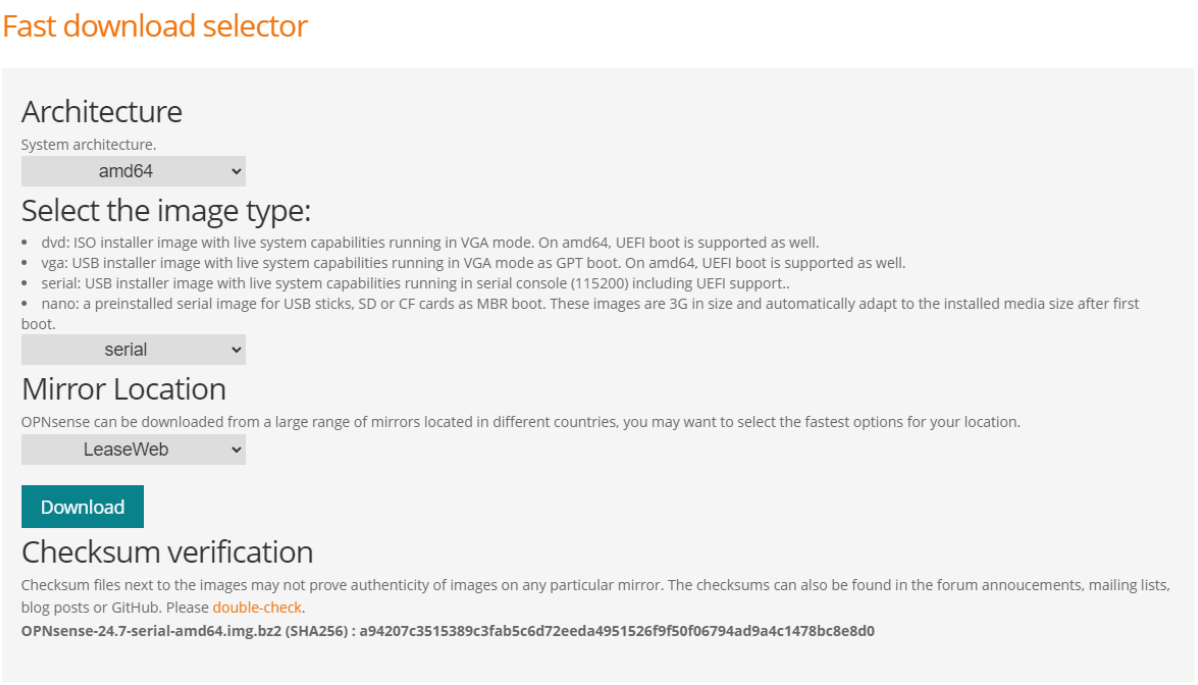
Configuration Windows :

Installation des logiciels

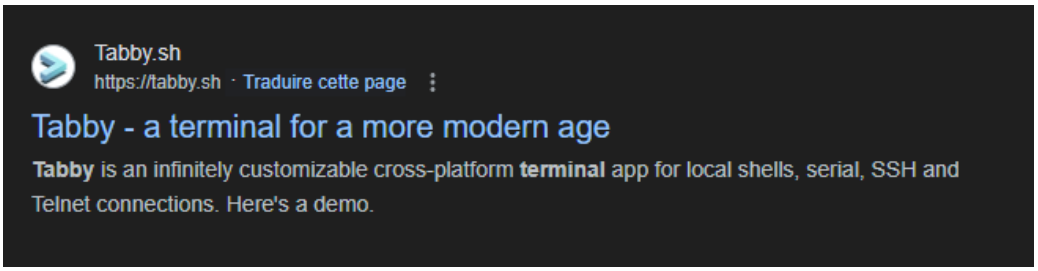
Il faut d'abord commencer par récupérer l'iso de opensense sur le site officiel (cliquer sur le lien ou il est marqué « Download » pour aller plus vite :



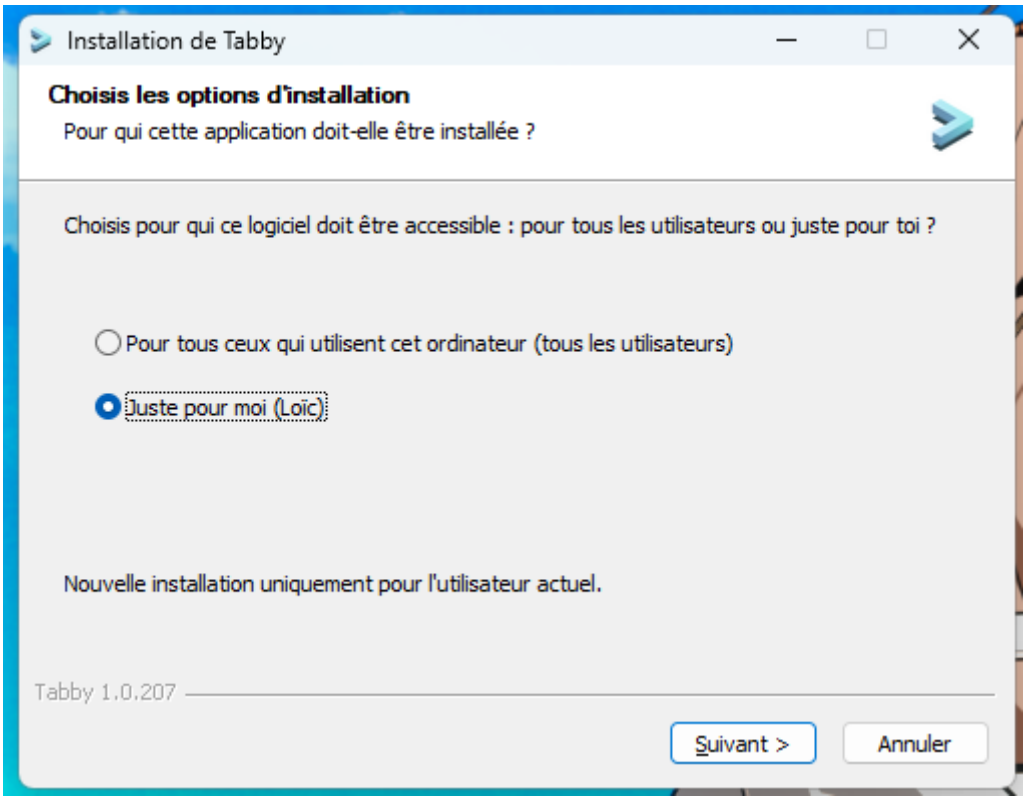
On fera attention à bien installer la version serial :



Puis on installe Tabby qui nous permettra de rentrer sur le pare-feu :

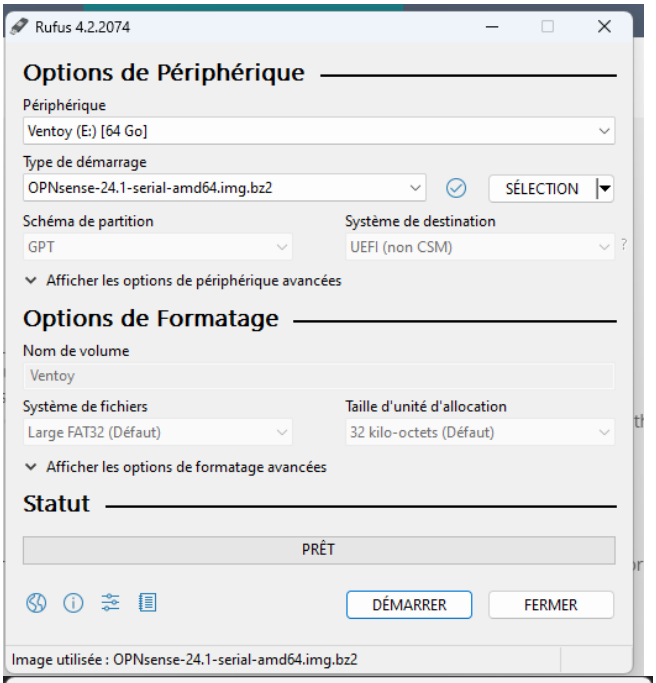


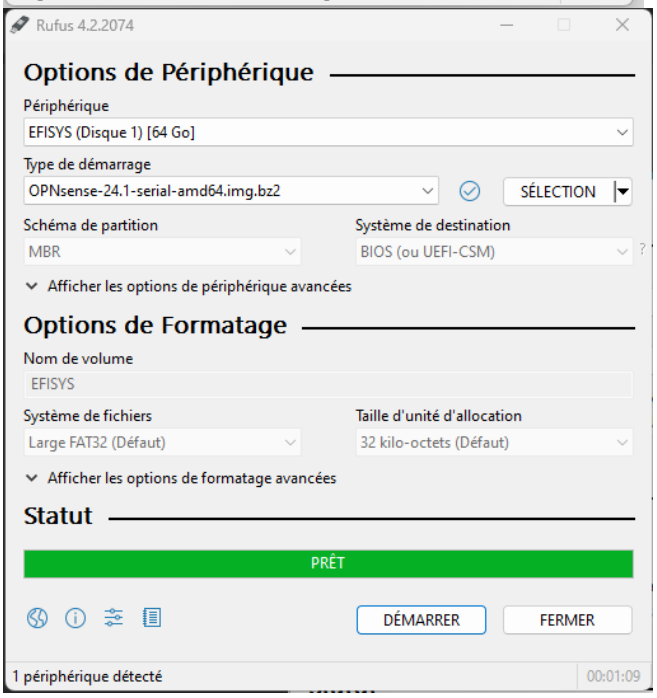
Ici on renseigne juste si le logiciel doit être installer sur tous les utilisateurs de la machine.



Formatage de la clé :

On commence par formater la clé en mettant L'iso télécharger précédemment (Le logiciel que l'on utilise ici est Rufus).

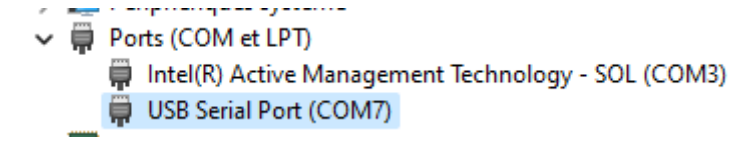


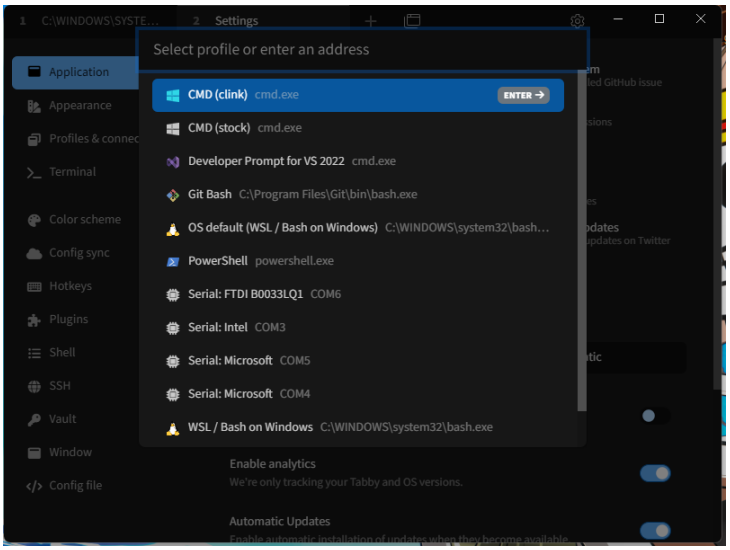


Configuration du Pare-feu via Tabby :

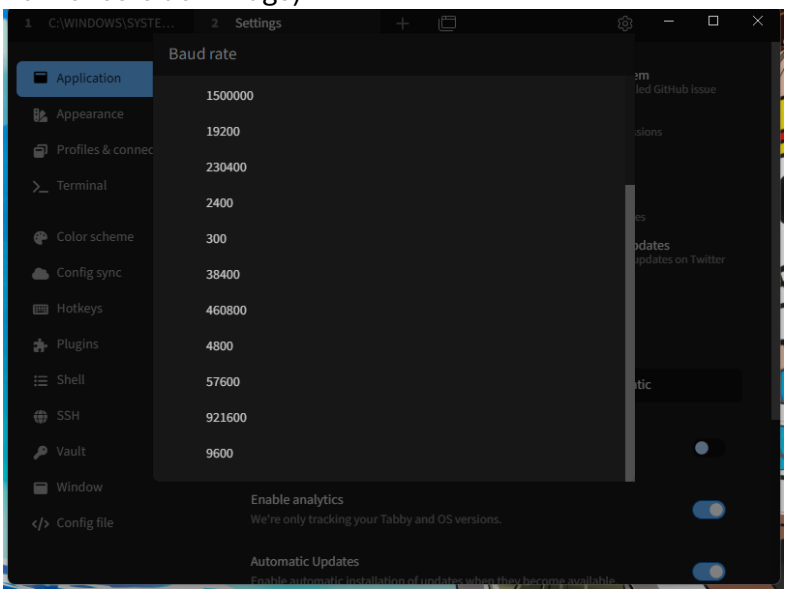
Tabby :

Sur le logiciel tabby on change de port de connexion dans "Profilés & connections", on cherchera le Serial (COM7(Pour savoir quel port utiliser on peut aller dans le gestionnaire des périphériques et aller dans la catégorie « Ports (COM et LPT) »)).





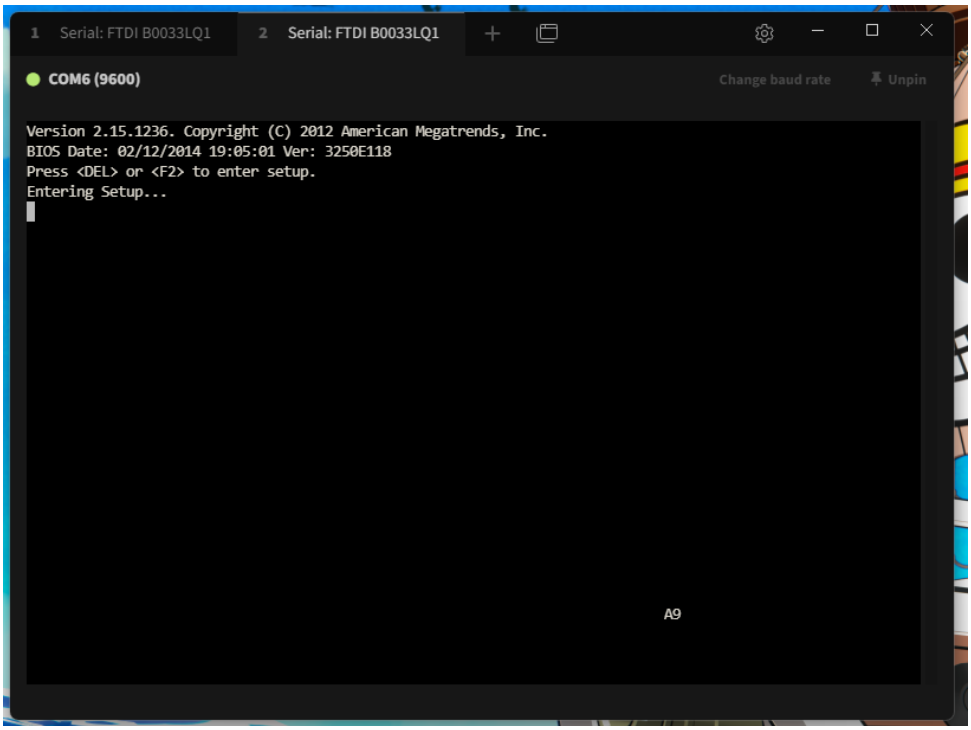
On passera la vitesse de lecture a 9600 bauds (car cela correspond à la vitesse du bios mais non le reste de l'image).



Bios

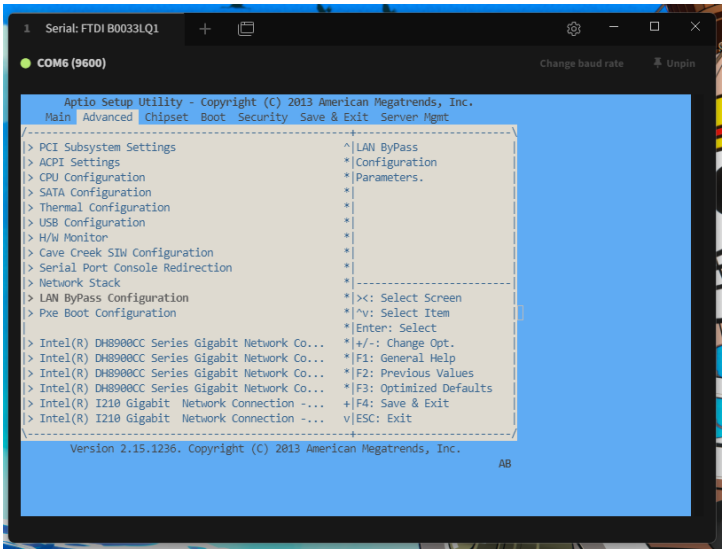
A savoir : Le BIOS est un programme indépendant, stocké dans la mémoire de la carte mère (du pare-feu), qui permet de tester et d'initialiser tous les périphériques au démarrage avant de charger le système d'exploitation

On cherchera donc à aller sur le bios, il faudra appuyer sur la console (on fait ça pour pouvoir faire un impute car si cette action n'est pas faite les touches presser ne sont pas pris en compte par le logiciel) puis sur F2 au moment du boot du pare-feu (sur l'image ci-dessous vous pouvez voir le moment ou il faut faire les actions).

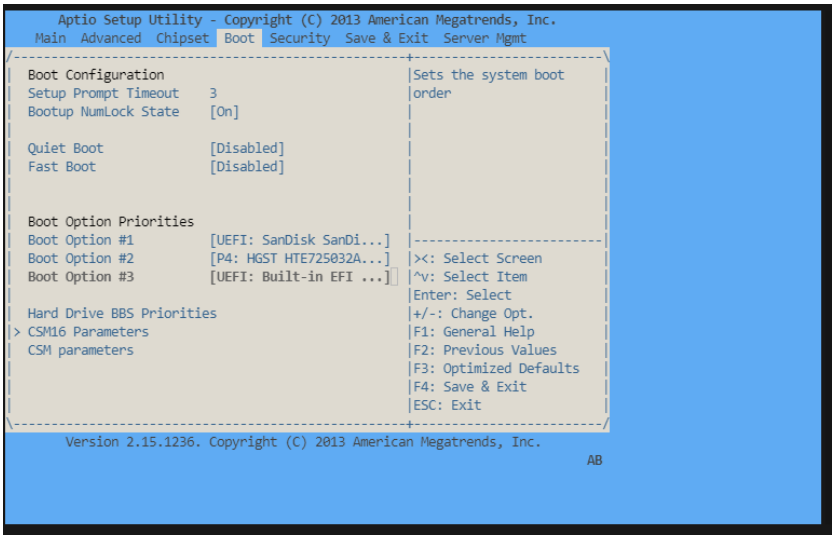


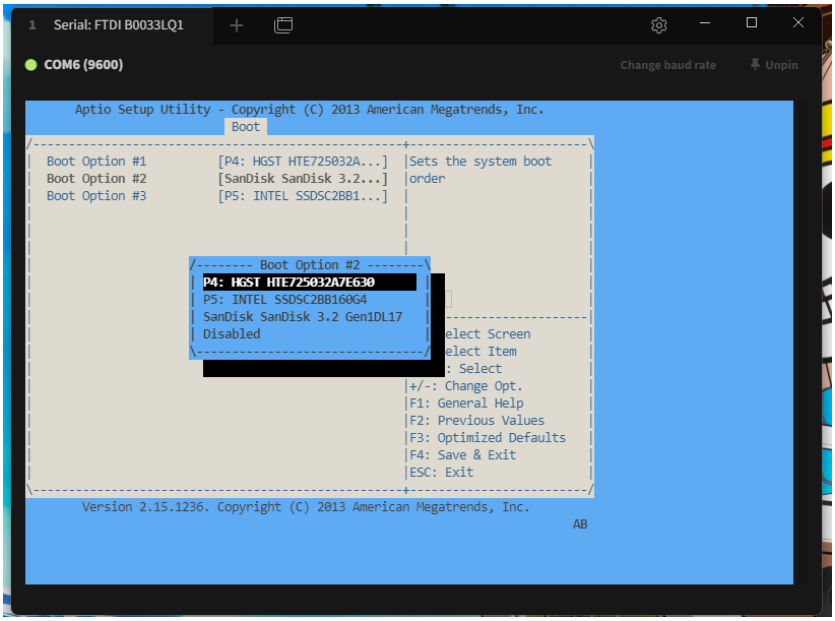
Une fois sur l'étapes précédente réussie le BIOS s'ouvre. Pour commencer dans le BIOS pour activer le LAN ByPass sur les ports. (Le LAN ByPass est une fonction qui permet de garantir la continuité du trafic réseau en reliant directement deux ports LAN en cas de défaillance de l'appareil, assurant ainsi une connexion sans interruption.)

Pour ce faire on ira dans : Advanced -> LAN ByPass Configuration-> LAN3 & LAN4, LAN5 & LAN6 ByPass et on les mettra en NO BYPASS

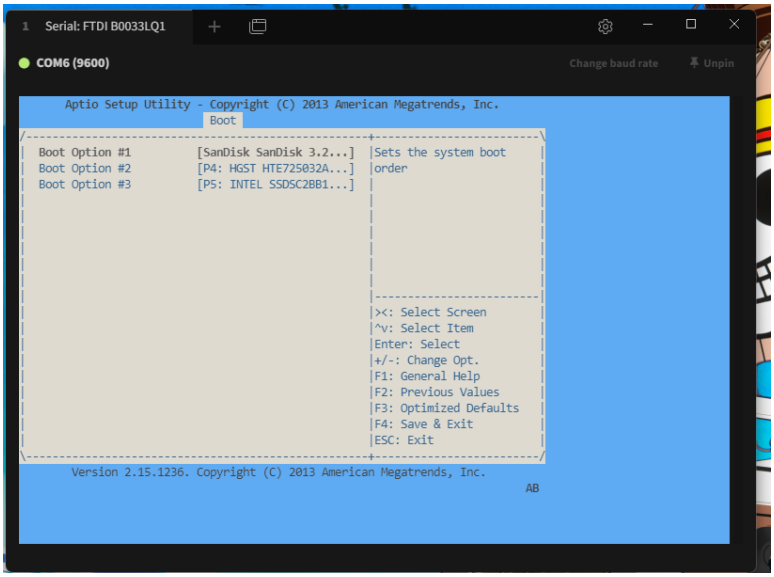


Puis on ira dans la page « Boot », on sélectionnera avec la touche « Entre » et on montera la clé USB en première position dans Boot option Priorities, ensuite on ira dans la catégorie « Hard drive BBS priorities » ou on montera la clé en première option de la même manière que l'on a fait précédemment.





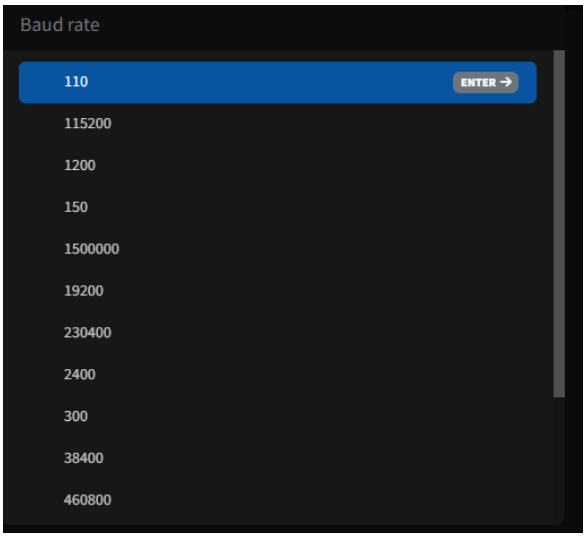
Ici on est retourné dans la catégorie « Hard drive BBS priorities » pour vérifier que la clé est bien montée.



Pour finir on ira dans la rubrique « Save & Exit », dans « save changes and Exit » et avec Entrer faite « Yes »

Installation de l'image Opensense

Après avoir configurer le BIOS et l'avoir quitté le pare-feu va redémarrer donc pendant de temps il va falloir d'abord mettre la clé avec l'ISO et ensuite passer la vitesse de lecteur a 115200bauds (le plus important est de mettre la clé car le changement de vitesse n'a rien à vois avec le redémarrage, si vous n'avez pas réussi pas de soucis coupé le pare-feu est recommencer)



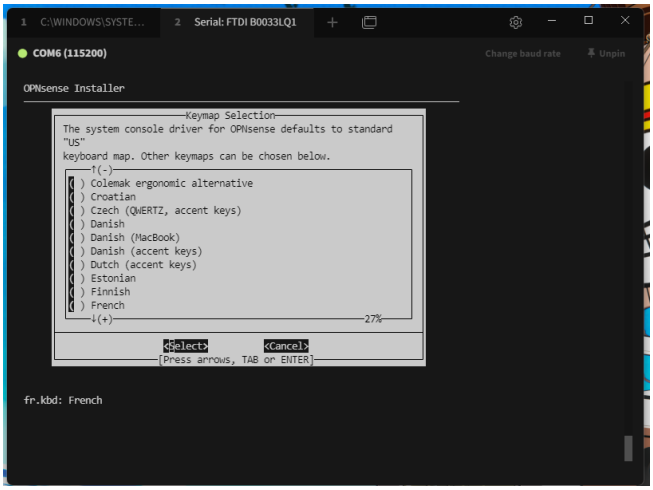
Il faudra se connecter avec c'est identifiant :

Identifiant = Installer

Mdp par défaut = opnsense

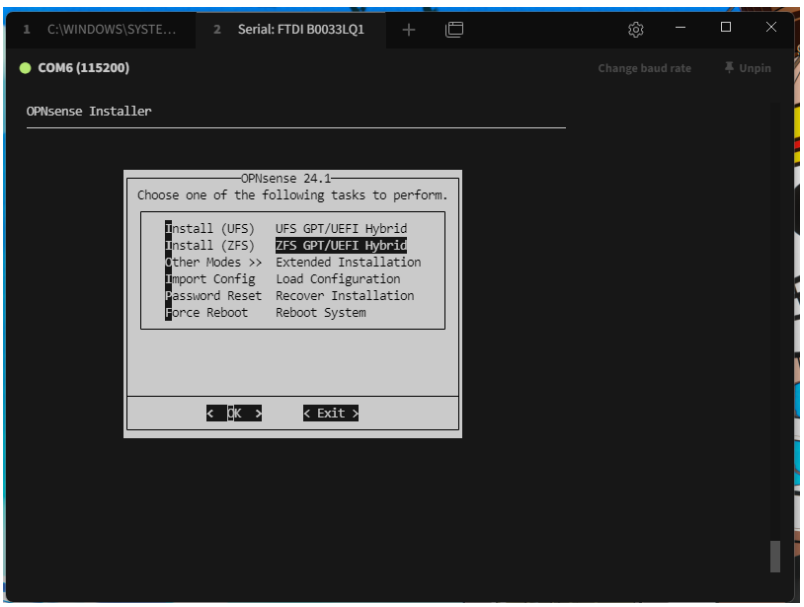
A savoir : Une fois connecter il faut savoir que comme depuis le debut la souris ne sera pas utiliser seulement les touche du clavier (ici sois on utilise le plus est le moins ou les flèches directionnel pour naviguer, la touche enter pour sélectionner mais aussi pour les touches « ok » ou « Yes » et le reste des touches pour écrire).

On arrive ensuite sur cette page ou on sélectionnera le clavier voulu donc ici « French ».



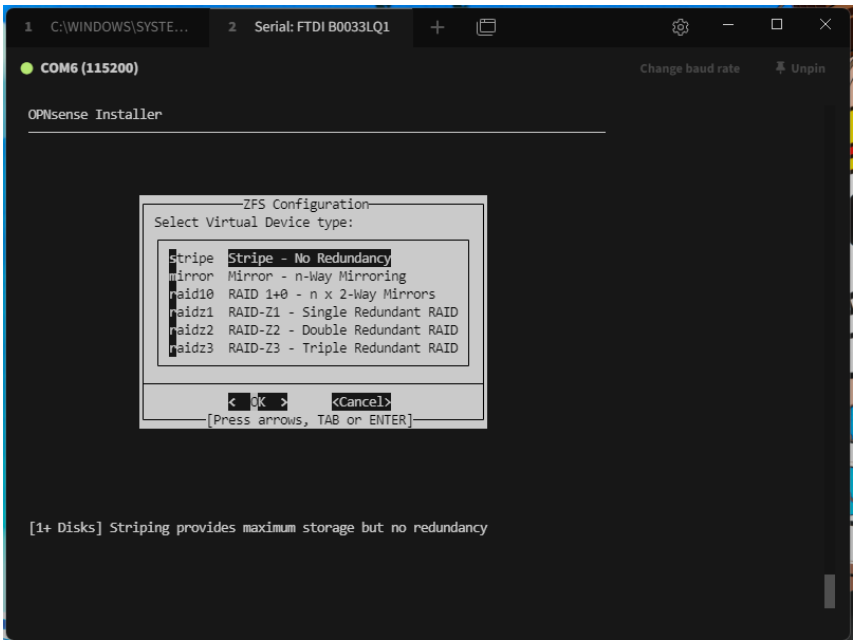
Une fois le clavier sélectionné on arrive sur cette page ou on devra sélectionner « Install (ZFS) ».

A savoir : Le ZFS (Zettabyte File System) est un système de fichiers avancé qui a été conçu pour offrir une gestion robuste, fiable et performante des données.

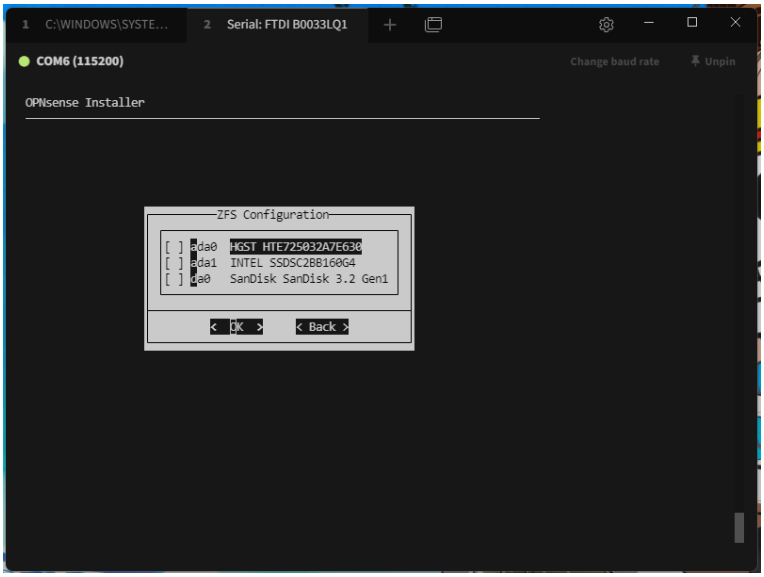


On ne sélectionne pas de mode miroir et pas de redondance.

A Savoir : pour faire un miroir il faut un deuxième disque dure car tout ce qu'est fait sur le premier et répliquer sur le second et la redondance est utile pour assurer une haute disponibilité exemple : si le disque dure principale lâche le deuxième prend le relais pour avoir un taux de disponibilité élever.

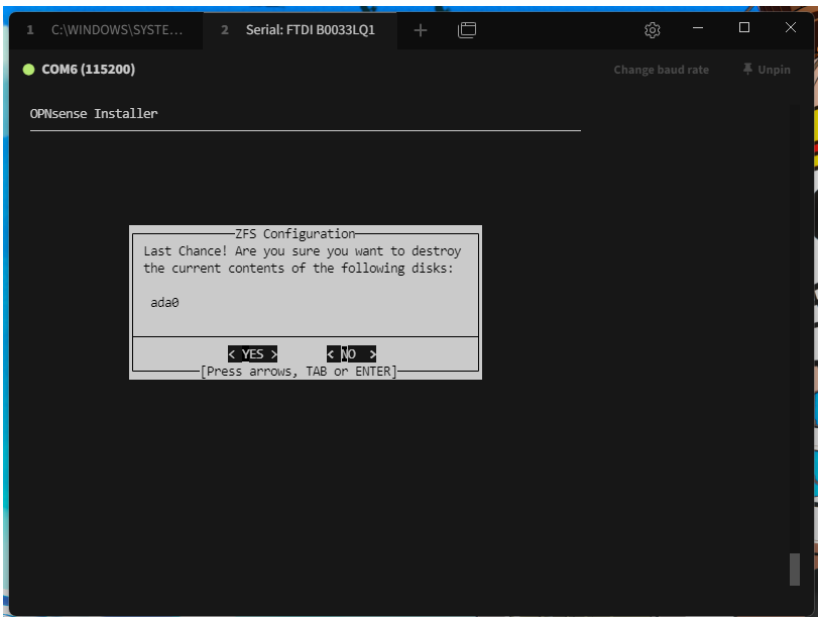


On sélectionne avec espace l'emplacement où l'on veut que la configuration soit installée (ici on veut mettre la configuration ZFS sur le disk HDD nommé « HGST HTE… »).

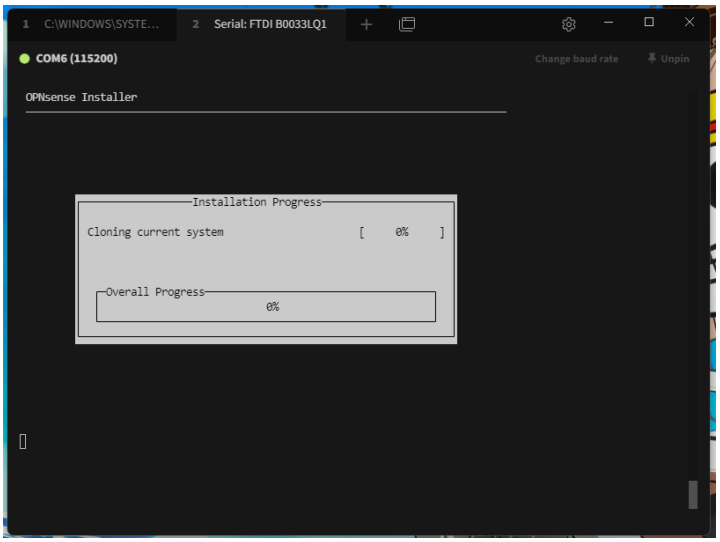


Puis descendre avec les touches directionnelles sur « ok ».

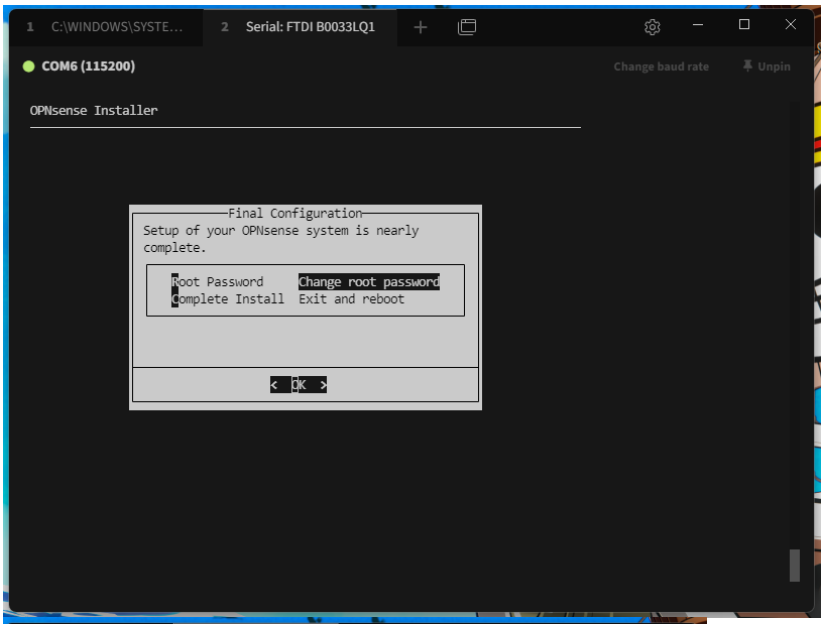
Après avoir sélectionner l'emplacement de la configuration un message pour nous prévenir que tout ce qu'il y avait sur le disk va être écrasé. Pour passer il faut appuyer sur « Entré »

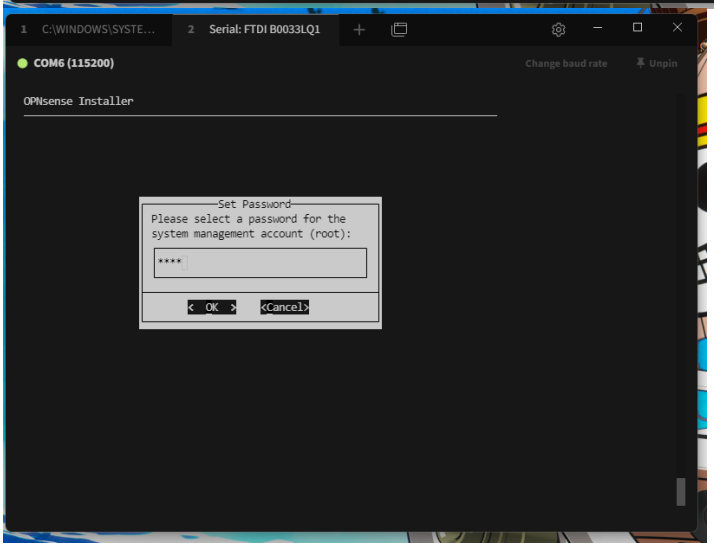


Quand la barre de chargement est à 100% on peut alors enlever la clé :

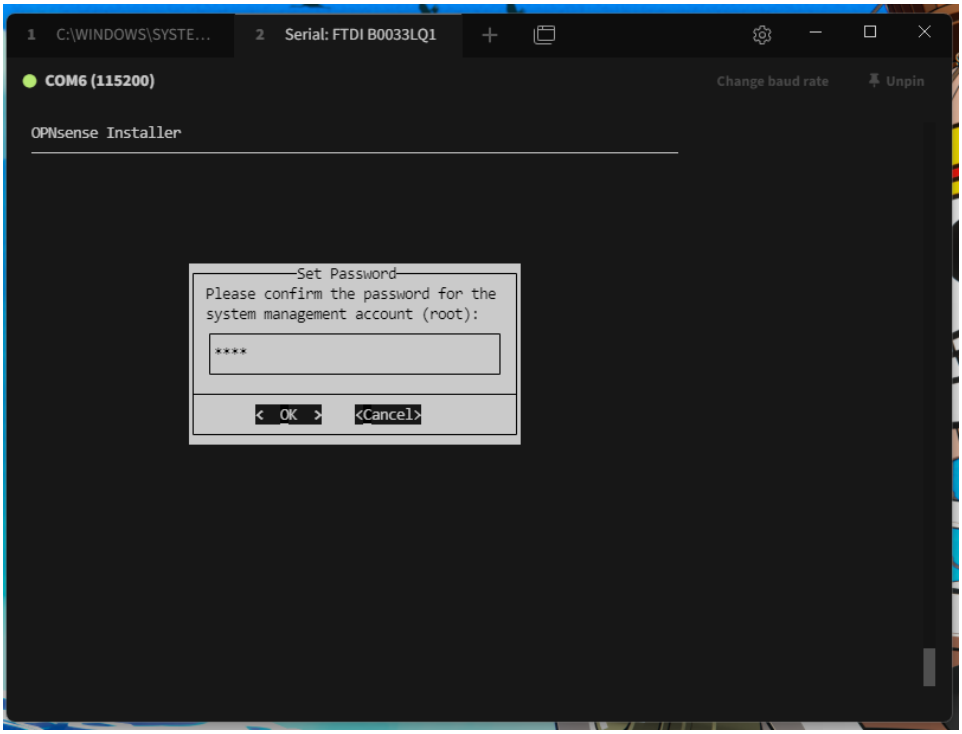


Un fois le chargement terminé on clique sur change root password (question de sécurité).

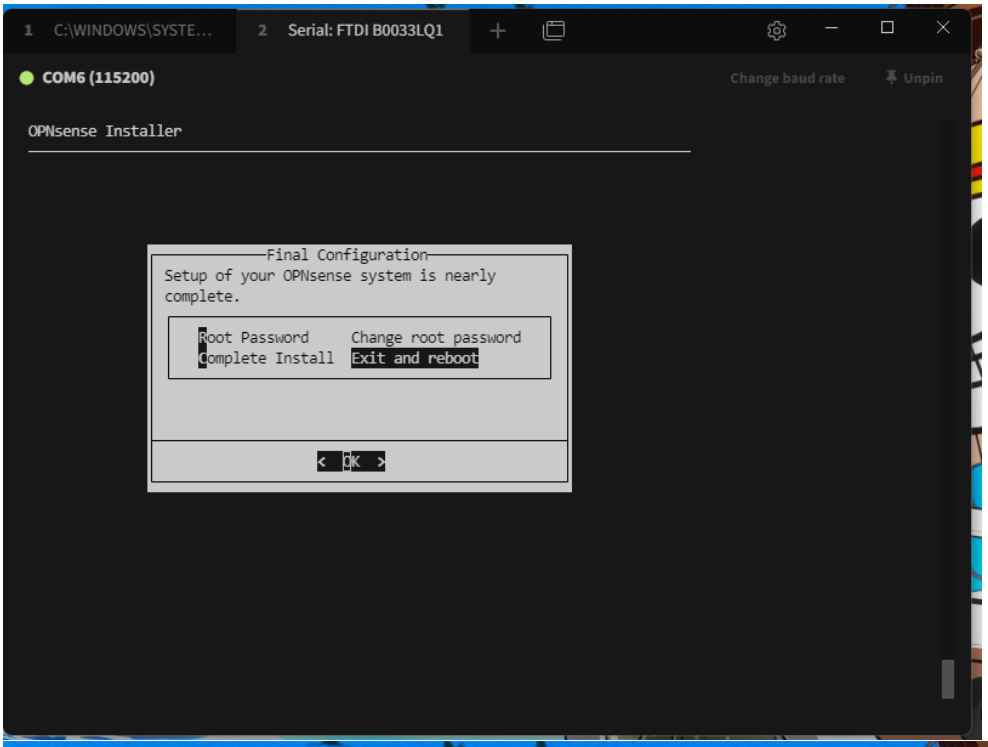


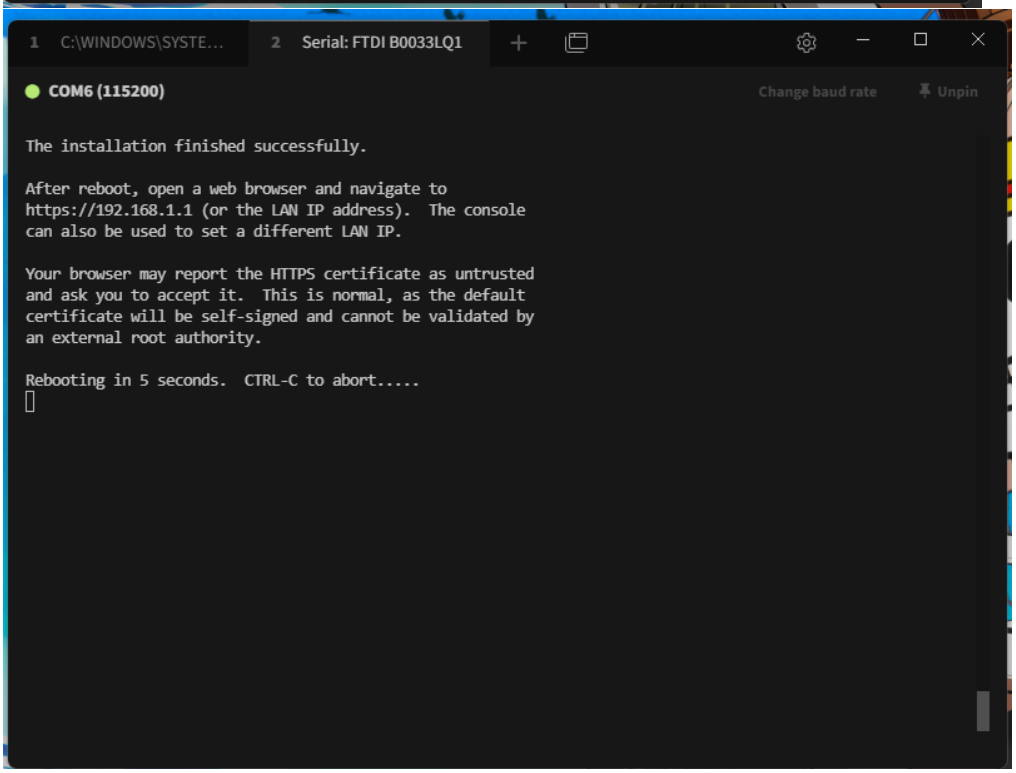


Et on confirme le MDP (en tapant le même).



Puis on sélectionne exit and reboot :





Ensuite il faudra retourner dans le bios pour mettre le HDD en priorité.

Configuration OPNSense

A savoir : pendant la configuration, il y a des propositions oui ou non en marquant [y/N] : s'il n'y a rien marqué après les points, c'est que c'est la lettre en majuscule qui est sélectionnée par défaut.

Pour commencer la configuration il faut aller dans l'option 1 pour assigner les ports.

```
*** OPNsense.localdomain: OPNsense 24.7 ***

 LAN (igb0)       -> v4: 192.168.1.1/24
 WAN (igb1)       -> v4/DHCP4: 192.168.0.239/24

 HTTPS: sha256 B6 06 75 15 27 02 48 BD 0A BD 3A 81 93 10 54 7D
               B1 CB E2 FB F8 0E D1 78 81 25 DD 8F 27 A9 36 42

  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
```

Pour les deux prochaines questions on fait « Entrée » car on ne veut pas configurer pour l'instant.

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

A la deuxième étape on nous présente les ports (sous forme d'interface) configurables, ici on nous demande quel port sera le WAN, pour configurer un port il faut marquer le numéro de port ici « igb4 » si on sait lequel correspond auquel sinon il faut brancher un équipement en RJ45 au port que le veut configurer et écrie « a »

```
Valid interfaces are:

igb0            00:0e:b6:c0:e4:5c Intel(R) I347-AT4 DH89XXCC
igb1            00:0e:b6:c0:e4:5d Intel(R) I347-AT4 DH89XXCC
igb2            00:0e:b6:c0:e4:5e Intel(R) I347-AT4 DH89XXCC
igb3            00:0e:b6:c0:e4:5f Intel(R) I347-AT4 DH89XXCC
igb4            00:0e:b6:5b:ff:f0 Intel(R) I210 (Copper)
igb5            00:0e:b6:5b:ff:f1 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: igb4
```

Ici on nous demande quel port sera sur le LAN de la même manière que précédemment dans notre cas « igb5 ».

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): igb5
```

Ici on ne met rien car on ne veut pas d'interface supplémentaire.

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

Un message nous dit quelle interface sera attribuée à quoi et si on veut procéder à l'assignation en mettant un « y ».

```
The interfaces will be assigned as follows:

WAN  -> igb4
LAN  -> igb5

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

Maintenant, on va mettre des adresses IP sur les interfaces que l'on a configurées avant.

```
*** OPNsense.localdomain: OPNsense 24.7 ***

 LAN (igb5)       -> v4: 192.168.1.1/24
 WAN (igb4)       -> v4/DHCP4: 192.168.0.242/24

 HTTPS: sha256 B6 06 75 15 27 02 48 BD 0A BD 3A 81 93 10 54 7D
               B1 CB E2 FB F8 0E D1 78 81 25 DD 8F 27 A9 36 42

  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: 2
```

Là, on nous montre les interfaces configurables. On commence par le LAN en mettant « 1 »

```
Available interfaces:

1 - LAN (igb5 - static, track6)
2 - WAN (igb4 - dhcp, dhcp6)

Enter the number of the interface to configure: 1
```

Là, on fait « entrée » car on ne veut pas mettre de DHCP sur le port LAN.

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

Maintenant on rentre l'adresse IP du port LAN, dans ce cas-là on met « 192.168.60.254 »

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.60.254
```

Là, on rentre le nombre de bits du masquer. Dans notre cas, on rentre 24 car l'adresse IP est en classe C.

```
Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Ici on fait juste « Entrée ».

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

A la prochaine étape, on écrit « n » car on ne veut mettre d'IPv6 sur le LAN via le WAN.

```
Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
```

Maintenant on appuie sur « Entrée » car on ne veut pas mettre d'IPv6 sur le LAN via DHCP6.

```
Configure IPv6 address LAN interface via DHCP6? [y/N]
```

Ici on ne veut toujours pas d'IPv6 donc « Entrée »

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

À cette étape,on va écrire un « y » car on veut mettre un DHCP sur le LAN.

```
Do you want to enable the DHCP server on LAN? [y/N] y
```

Maintenant on vient rentrer la plage d'IP que l'on veut.

```
Enter the start address of the IPv4 client address range: 192.168.60.100
Enter the end address of the IPv4 client address range: 192.168.60.200
```

Est-ce pour finir aux trois prochaines questions faites « Entrée » car on ne veut pas ces options.

```
Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N]
Do you want to generate a new self-signed web GUI certificate? [y/N]
Restore web GUI access defaults? [y/N]
```

A la fin de la configuration, on peut voir qu'une adresse IP apparaît. Elle va être utilisée pour se connecter à l'interface web de OPNSense.

```
You can now access the web GUI by opening
the following URL in your web browser:

    https://192.168.60.254
```

Changement du mot de passe Admin / langue

A savoir : changer le mot de passe Admin est super important car tout le monde peut connaître le mot de passe Admin en regardant la documentation du logiciel. On le change donc pour des questions de sécurité.

Aussi par défaut le logiciel est en anglais, donc pour pouvoir mieux s'orienter quand on ne connaît pas très bien l'anglais, il est important de changer la langue.

MDP Admin firewall

Sur le menu pour aller changer le mot de passe admin, il faut prendre l'option 3 (à écrire sur la ligne « Enter an option : »).

```
-------------------------------------------
|      Hello, this is OPNsense 24.7       |
|                                         |
| Website:      https://opnsense.org/     |
| Handbook:     https://docs.opnsense.org/|
| Forums:       https://forum.opnsense.org/|
| Code:         https://github.com/opnsense|
| Twitter:      https://twitter.com/opnsense|
-------------------------------------------

*** OPNsense.localdomain: OPNsense 24.7 ***

 LAN (igb0)       -> v4: 192.168.1.1/24
 WAN (igb1)       ->

 HTTPS: sha256 B6 06 75 15 27 02 48 BD 0A BD 3A 81 93 10 54 7D
              B1 CB E2 FB F8 0E D1 78 81 25 DD 8F 27 A9 36 42

  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: 3
```

Ici, on nous demande si on veut procéder au changement du mot de passe root, donc on met alors un « y » en minuscule pour signifier yes.

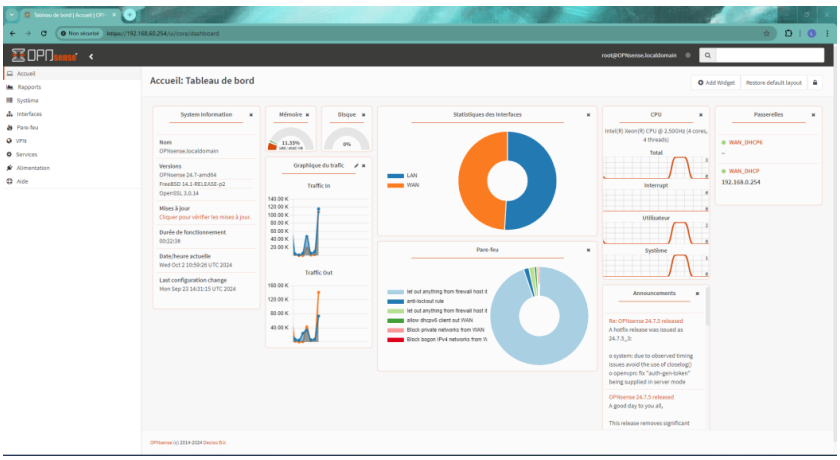
```
The root user login behaviour will be restored to its defaults.

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

Et il nous est demandé de mettre le nouveau MDP deux fois pour le confirmer.

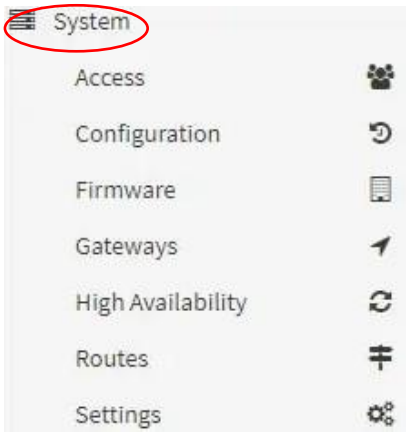
```
Type a new password:
Confirm new password:

The root user has been reset successfully.
```

Changement de la langue.

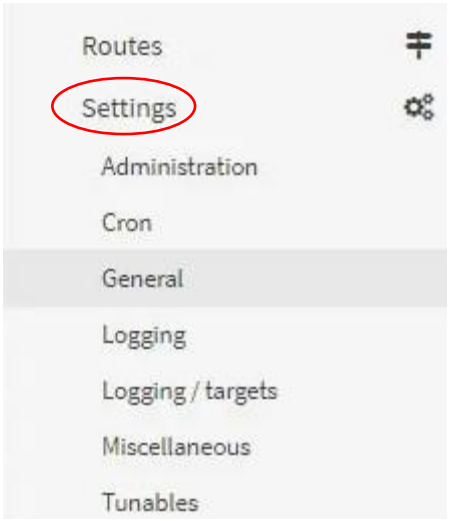
Pour changer la langue, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de l'installation) et en rentrant les identifiants de notre compte Admin.



Ensuite, à gauche, il faut aller cliquer sur la rubrique « System ».



Puis cliquer sur « Settings ».



Et aller dans la catégorie « Général ».

Puis sur le reste de l'écran, il faut aller dans la partie « Language » et mettre la langue voulue.

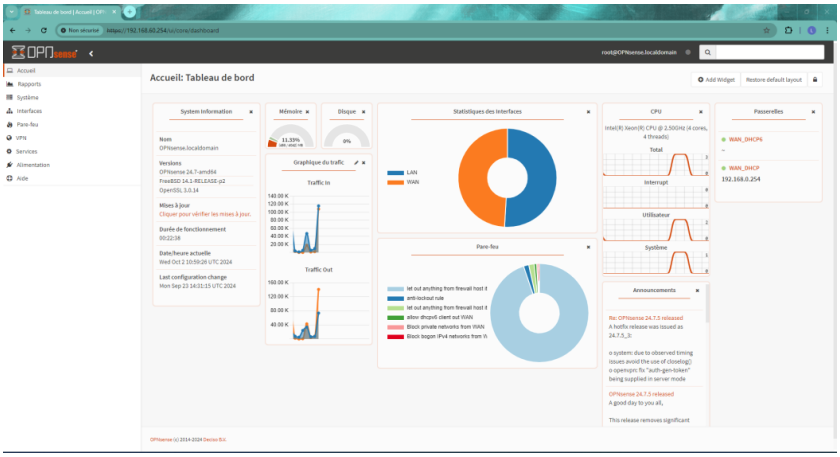
Et pour finir, il faut aller en bas de la page pour cliquer sur le bouton où il est écrit « Sauvegarder ».

Sauvegarde / restauration

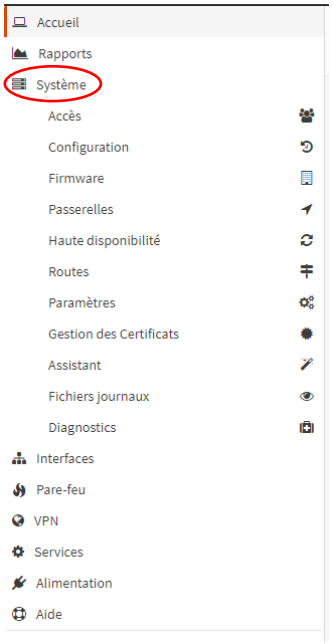
A savoir : Il est essentiel de faire des sauvegardes régulières afin de pouvoir revenir à une version antérieure en cas de mauvaise manipulation. Cela garantit que, même en cas de problème, le pare-feu restera opérationnel pour assurer la sécurité et le filtrage du réseau. Il est également important de savoir comment restaurer rapidement une sauvegarde pour gagner du temps et minimiser les interruptions de service.

Sauvegarde

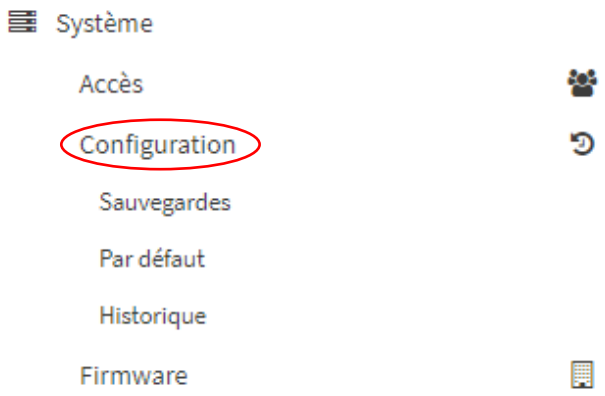
Pour faire une sauvegarde, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de l'installation) et en rentrant les identifiants de notre compte Admin.



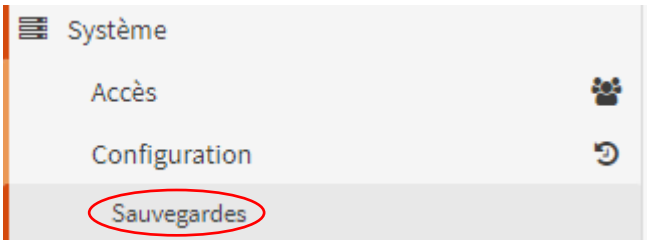
Ensuite, à gauche, il faut aller cliquer sur la rubrique « Système ».



Puis cliquer sur « Configuration ».

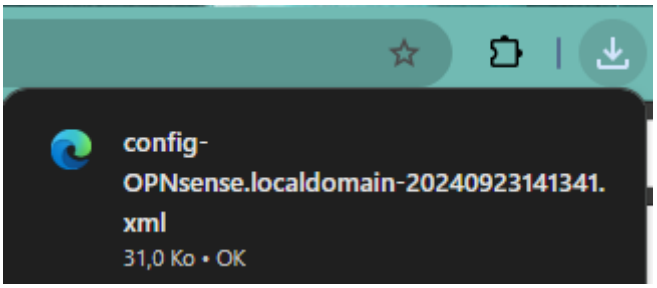


Et aller dans la catégorie « Sauvegarde ».



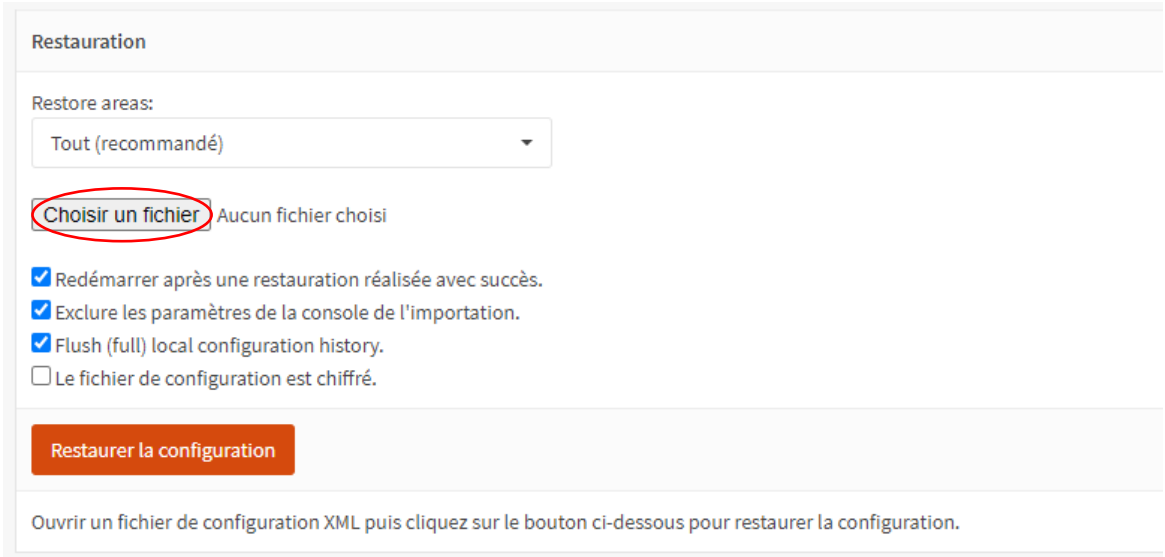
Puis sur le reste de l'écran, il faut aller dans la partie « Téléchargement » et appuyer sur « Télécharger la configuration ».

On peut voir en haut à droite que le fichier s'est bien téléchargé.

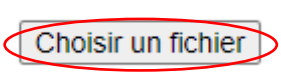


Restauration

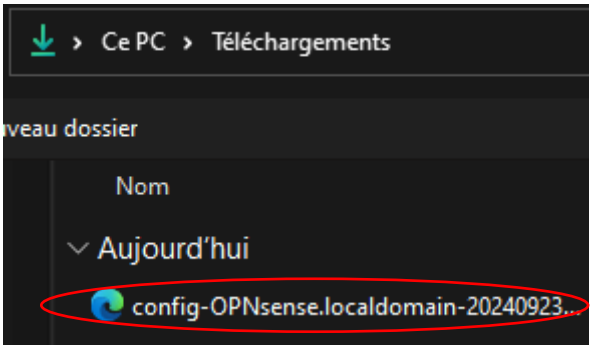
Pour faire la restauration, il faut être sur la même page que pour la sauvegarde et descendre pour aller dans la catégorie « Sauvegarde ».



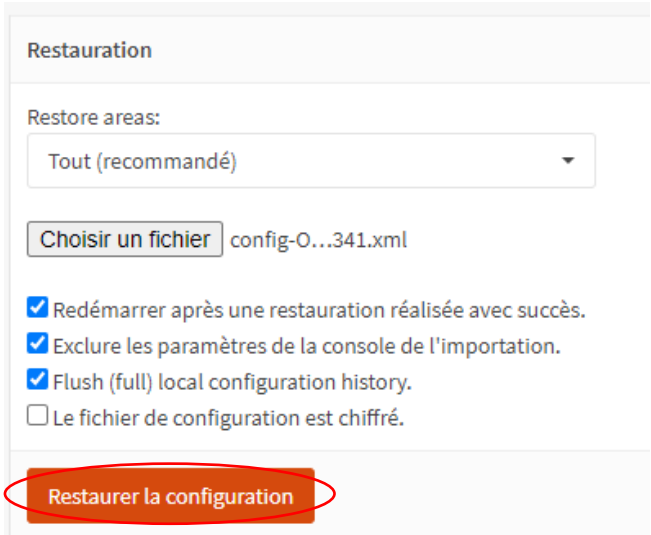
Ensuite, on va cliquer sur le bouton « choisir un fichier ».



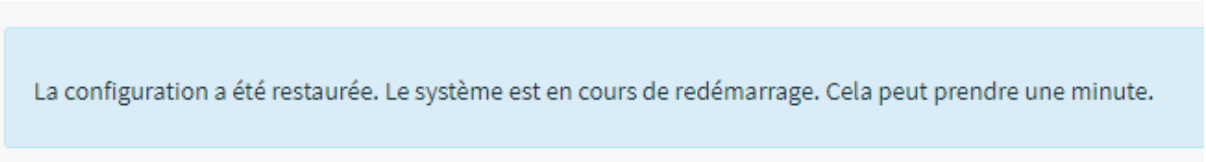
Et on sélectionne le fichier que l'on a téléchargé.



Et pour finir, il faut cliquer sur le bouton « Restaurer la configuration ».



Pour vérifier que tout s'est bien passé, tout en haut de la page, un message s'affiche.

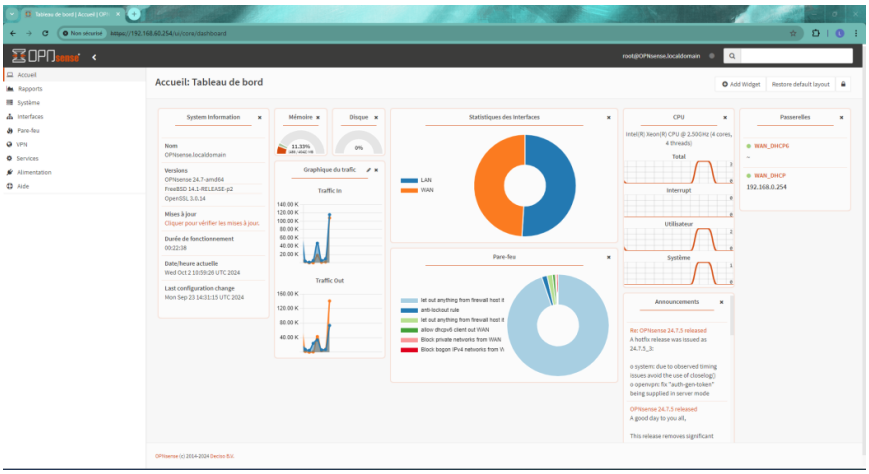


Rester en mode usine

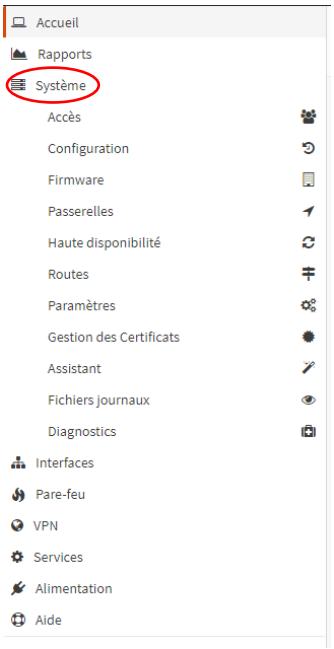
A savoir : Il est utile de rester en mode usine en cas de mauvaise configuration, en cas de panne et dysfonctionnements. Avant de faire ceci, il est important de faire une sauvegarde au préalable, ensuite rester en mode usine, puis il est possible de faire une restauration de la sauvegarde faite précédemment pour minimiser les interruptions de service.

Sauvegarde

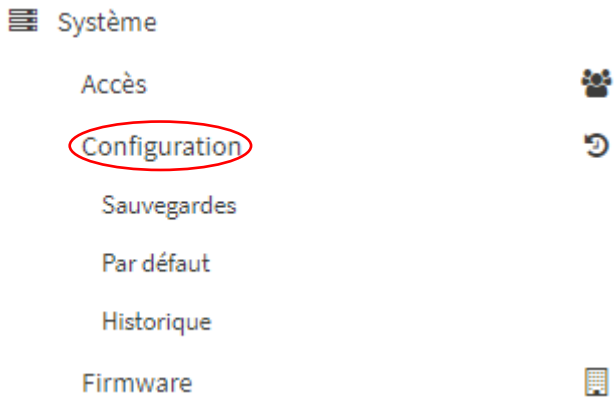
Pour faire une sauvegarde, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de l'installation) et en rentrant les identifiants de notre compte Admin.



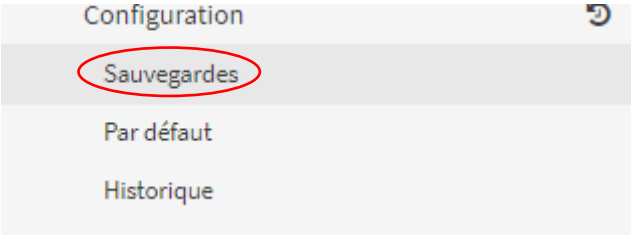
Ensuite, à gauche, il faut aller cliquer sur la rubrique « Système ».



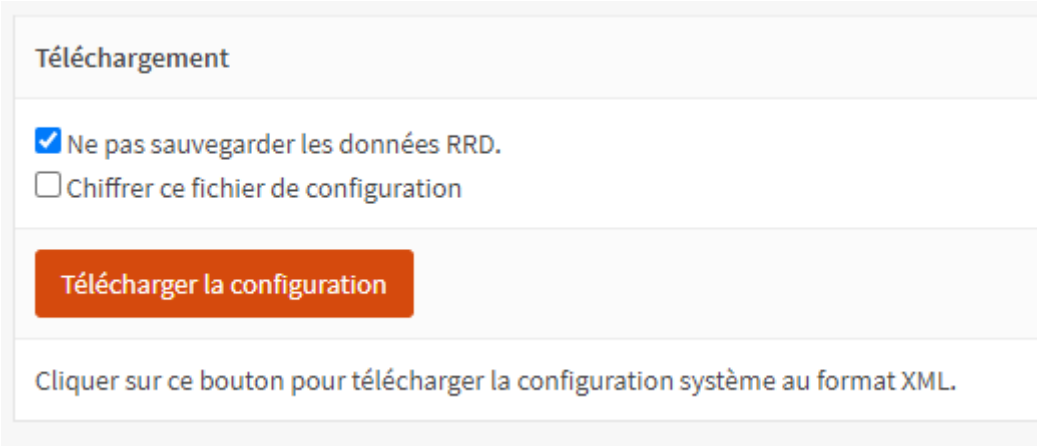
Puis cliquer sur « Configuration ».



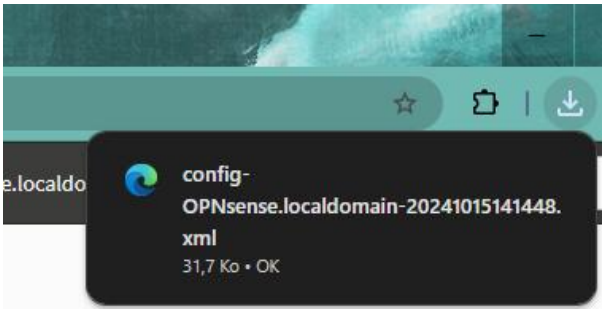
Et pour finir, dans aller dans la catégorie « Sauvegarde ».



Sur la page, il va falloir aller dans la partie « Téléchargement » et cliquer sur « Télécharger la configuration ».

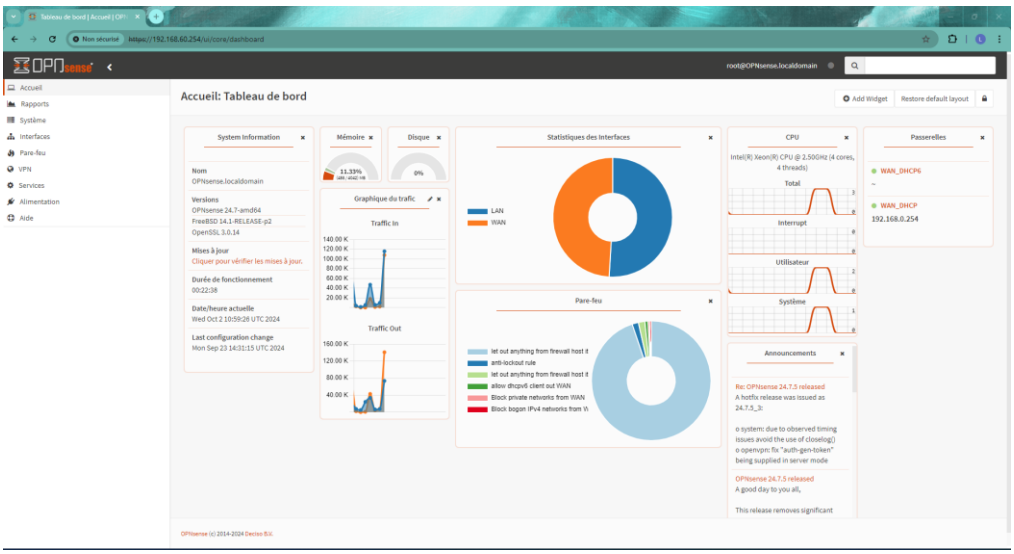


Après avoir téléchargé la configuration, un pop-up s'affiche en haut à droite montrant le téléchargement.

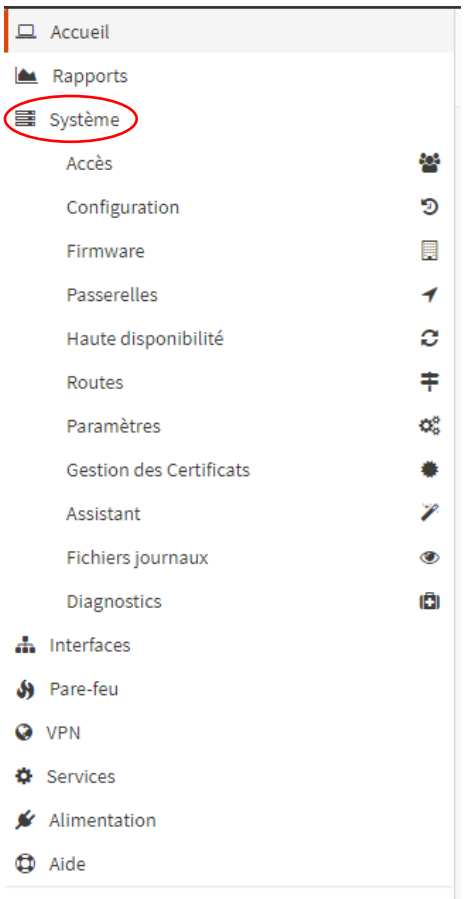


Rester

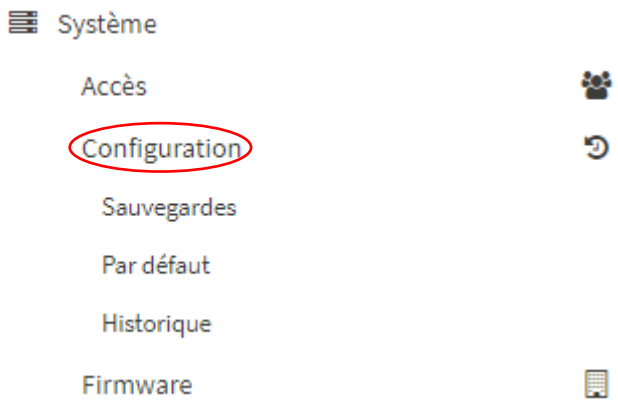
Pour passer la configuration du pare-feu en mode usine, il faut déjà aller sur la page d'accueil du pare-feu.



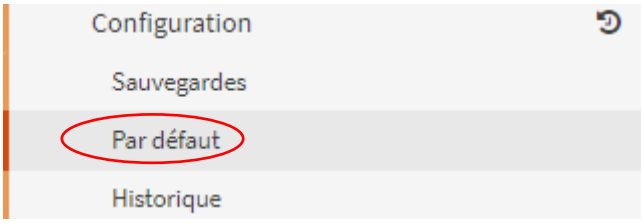
Ensuite, à gauche, il faut aller cliquer sur la rubrique « Système ».



Par la suite, il faut aller dans « Configuration ».

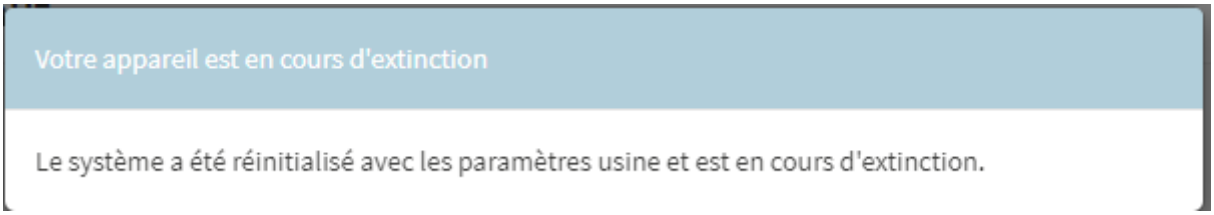


Et cliquer sur la catégorie « Par défaut ».



Sur le reste de la page, un message vient s'afficher pour prévenir de ce qui va être modifié. Et un pour pouvoir mettre la configuration par défaut, il faut cliquer sur le bouton « oui ».

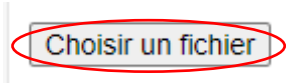
Une fois que l'on a cliqué sur le bouton, un message s'affiche pour dire que le mode usine est en cours d'application.



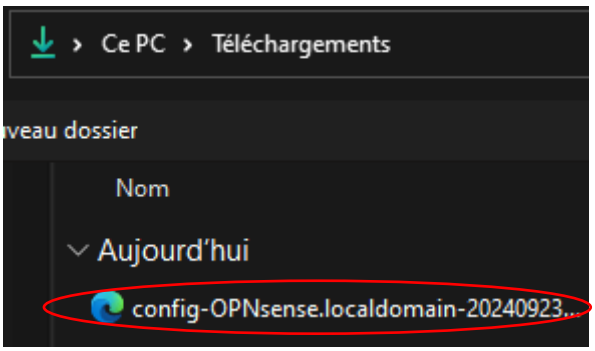
Restauration

Pour faire la restauration, il faut être sur la même page que pour la sauvegarde et descendre pour aller dans la catégorie « Sauvegarde ».

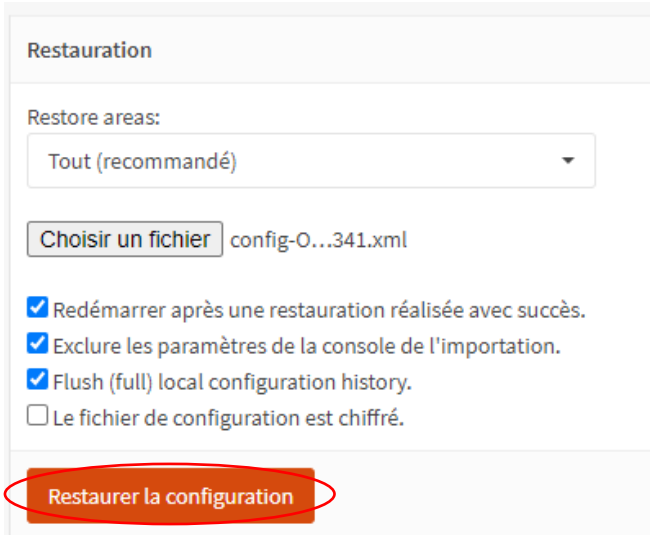
Ensuite, on va cliquer sur le bouton « choisir un fichier ».



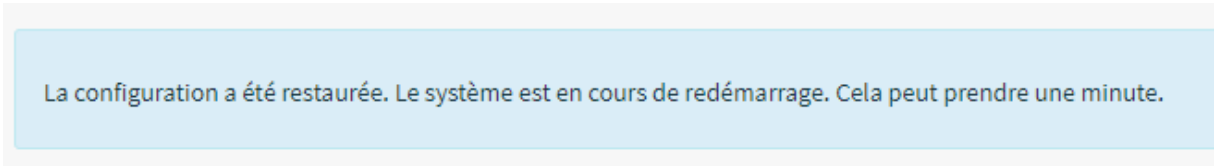
Et on sélectionne le fichier que l'on a téléchargé.



Et pour finir, il faut cliquer sur le bouton « Restaurer la configuration ».



Pour vérifier que tout s'est bien passé, tout en haut de la page, un message s'affiche.



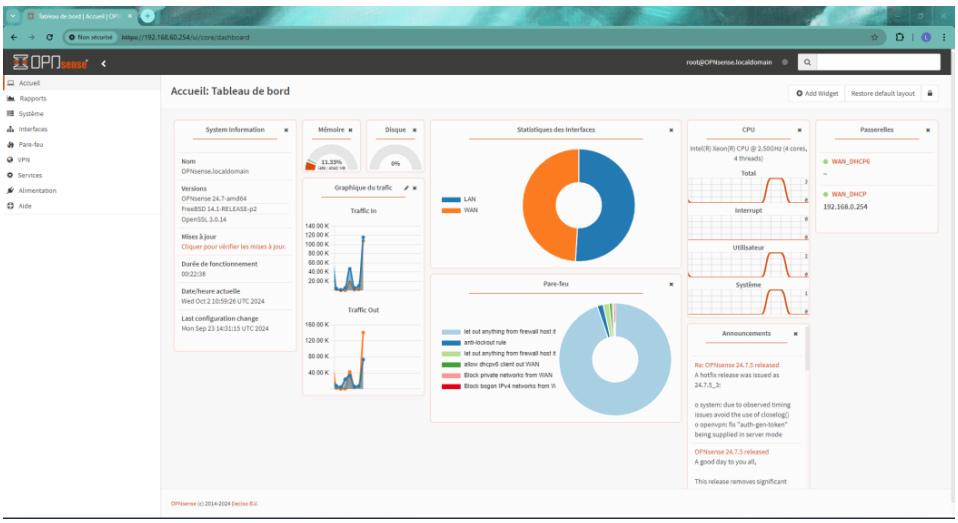
Configuration du webfiltering

A savoir : le webfiltering est utilisé car il peut bloquer l'accès à certains sites internet sur le réseau de l'entreprise.

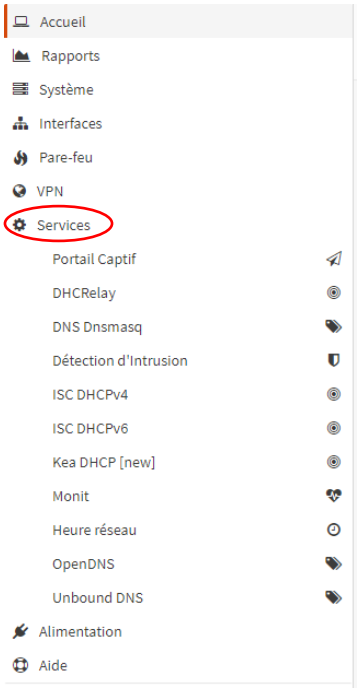
Configuration

Pour activer le service de webfilterning, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de

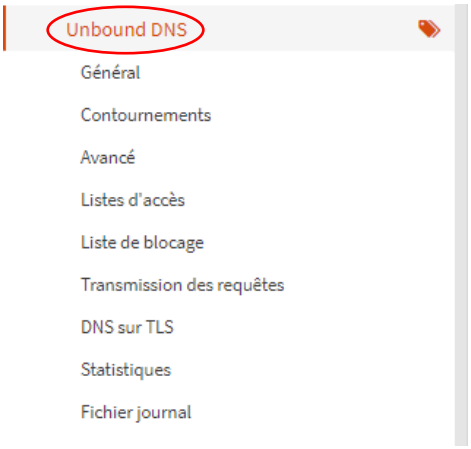
l'installation) et en rentrant les identifiants de notre compte Admin.



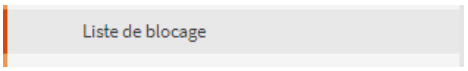
Puis sur le menu à gauche, il faut aller dans la catégorie « Services ».



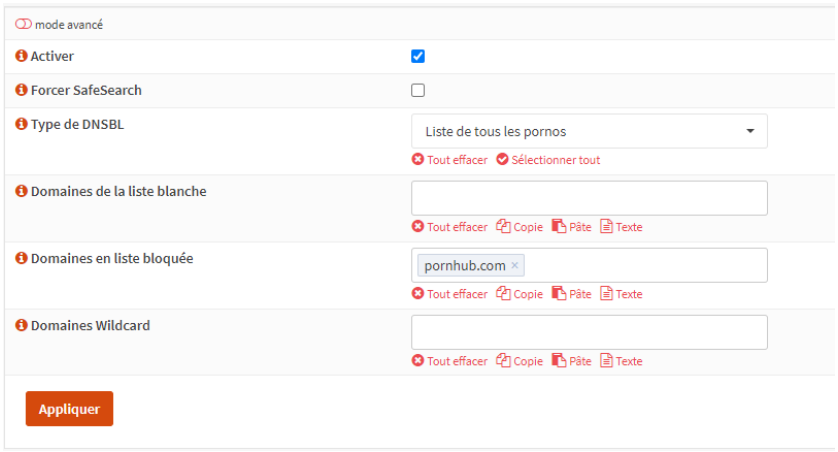
Puis cliquer sur « Unbound DNS ».



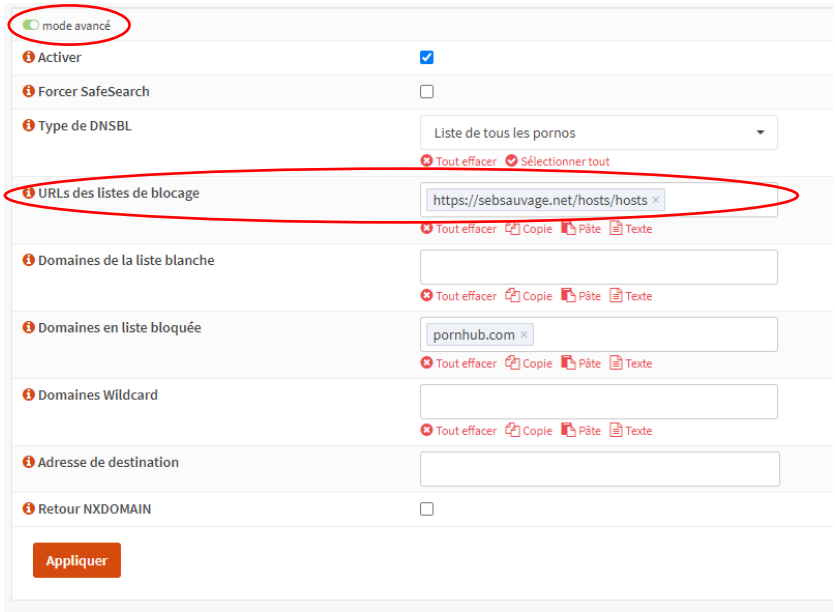
Et aller dans la catégorie « Liste de blocage ».



Une fois sur la page, on peut avoir accès à des listes de blocage déjà intégrées dans OPNSense qui se trouvent dans « Types de DNSBL » telles que des sites pornos, la cryptomonnaies et bien d'autres. Il est aussi possible de bloquer un site en particulier en rentrant l'URL dans « Domaines en liste bloquée ».



Aussi, quand on clique sur le bouton « mode avancée » il est possible d'ajouter une liste de blocage dans « URLs des listes de blocage » que l'on peut trouver sur internet comme l'URL : https://sebsauvage.net/hosts/hosts



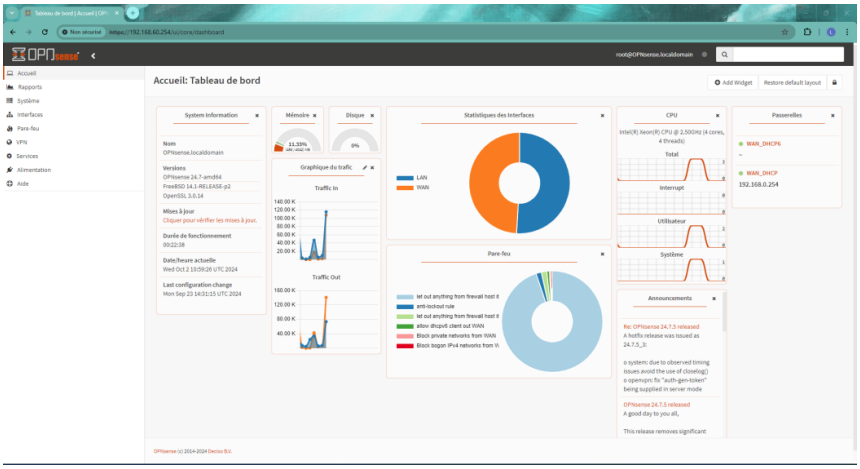
Une fois la configuration faite comme souhaité, il faut appuyer sur le bouton « Appliquer » qui se trouve en bas de la page.

Activer le SSH

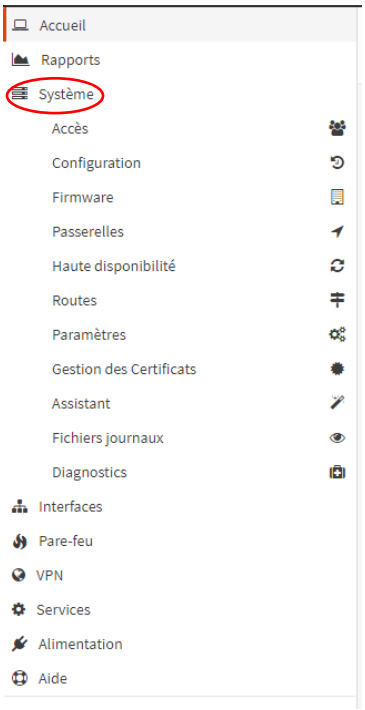
A savoir : Sur le pare-feu, il y a la possibilité d'activer le service SSH qui est utile pour prendre main sur le pare-feu à distance sans passer par le câble console et sans interface graphique.

Activer le SSH

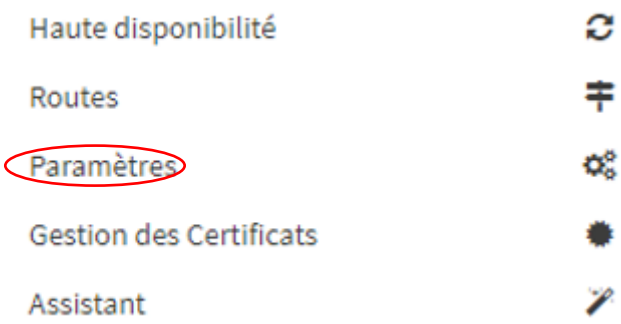
Pour activer le service SSH, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de l'installation) et en rentrant les identifiants de notre compte Admin.



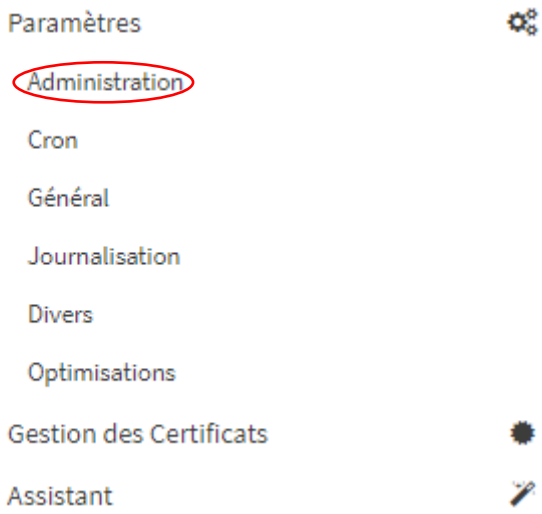
Ensuite, à gauche, il faut aller cliquer sur la rubrique « Système ».



Puis cliquer sur « Paramètres »

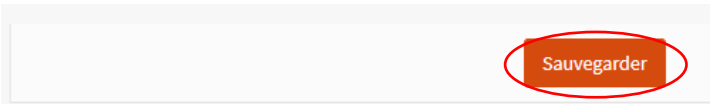


Et aller dans la catégorie « Administration ».

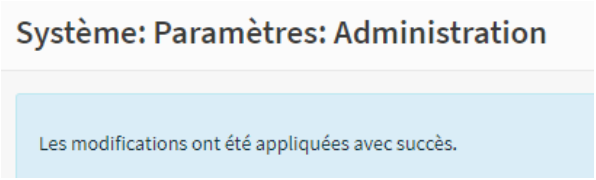


Puis sur le reste de l'écran, il faut descendre jusqu'à « Port SSH », dans le rectangle à côté il faut rentrer 22 et cocher les cases « Activer le Shell sécurisé, Autoriser la connexion de l'utilisateur root, Autoriser les connexions avec mot de passe ».

Pour finir, il faut aller tout en bas de la page pour cliquer sur le bouton « Sauvegarder »



Une fois que la sauvegarde de la configuration est bonne, un message s'affiche.



Test

Pour tester si la connexion marche bien, on vient utiliser l'invite de commande et taper la commande ssh utilisateur@IP (dans notre cas ssh root@192.168.60.254)

```
C:\Users\Loïc>ssh root@192.168.60.254
The authenticity of host '192.168.60.254 (192.168.60.254)' can't be established.
ED25519 key fingerprint is SHA256:APsIDEGW9aG/ipSHnDXZo9J/S6XkIA2giGyhG57+EPw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.60.254' (ED25519) to the list of known hosts.
(root@192.168.60.254) Password:
Last login: Wed Oct  2 10:39:24 2024
---------------------------------------------
|      Hello, this is OPNsense 24.7         |          @@@@@@@@@@@@@@@@
|                                           |        @@@@         @@@@
| Website:      https://opnsense.org/       |         @@@\\\   ///@@@
| Handbook:     https://docs.opnsense.org/  |       ))))))))   ((((((((
| Forums:       https://forum.opnsense.org/ |         @@@///   \\\@@@
| Code:         https://github.com/opnsense |        @@@@         @@@@
| Twitter:      https://twitter.com/opnsense|          @@@@@@@@@@@@@@@@
---------------------------------------------

*** OPNsense.localdomain: OPNsense 24.7 ***

 LAN (igb5)       -> v4: 192.168.60.254/24
 WAN (igb4)       -> v4/DHCP4: 192.168.0.242/24

 HTTPS: sha256 B6 06 75 15 27 02 48 BD 0A BD 3A 81 93 10 54 7D
               B1 CB E2 FB F8 0E D1 78 81 25 DD 8F 27 A9 36 42
 SSH:   SHA256 4CCdeICX+xHCcb/ONyZsCg+9D6t4n4JsDejImDWzLsI (ECDSA)
 SSH:   SHA256 APsIDEGW9aG/ipSHnDXZo9J/S6XkIA2giGyhG57+EPw (ED25519)
 SSH:   SHA256 fLKtuYrFbqiSpOPJmcaO9ib9nRPcq5MHz+AIGGuuqSI (RSA)

  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:
```