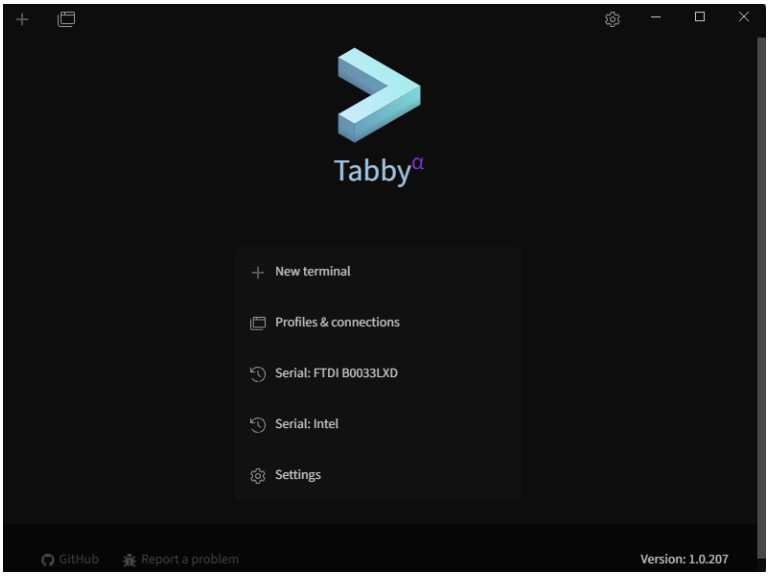
Firewall

Contents

1. Installation d'opnsense sur le Firewall Riverbed

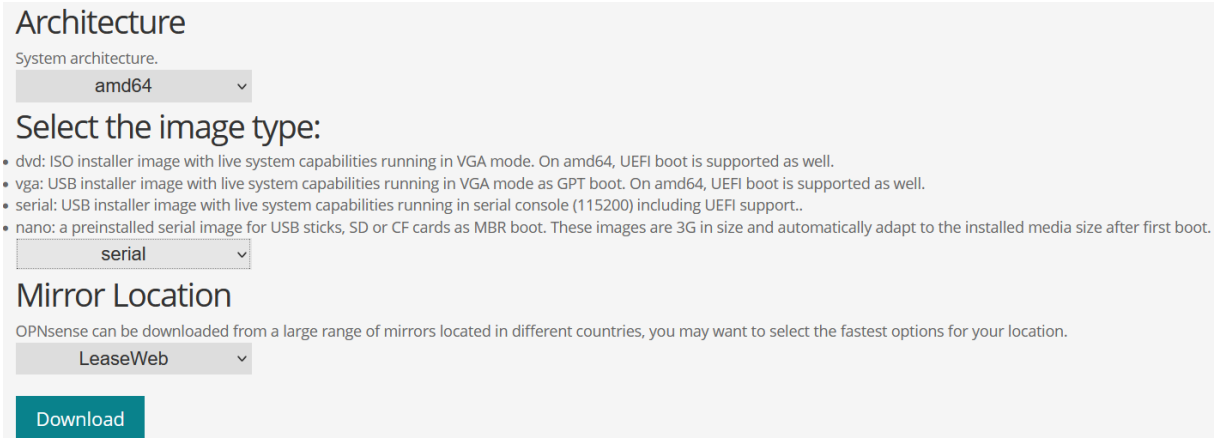
1.1 Installation de Tabby

Installer Tabby sur le PC pour se connecter au Pare-feu via le port console : https://github.com/Eugeny/tabby/releases/download/v1.0.207/tabby-1.0.207-setup-x64.exe



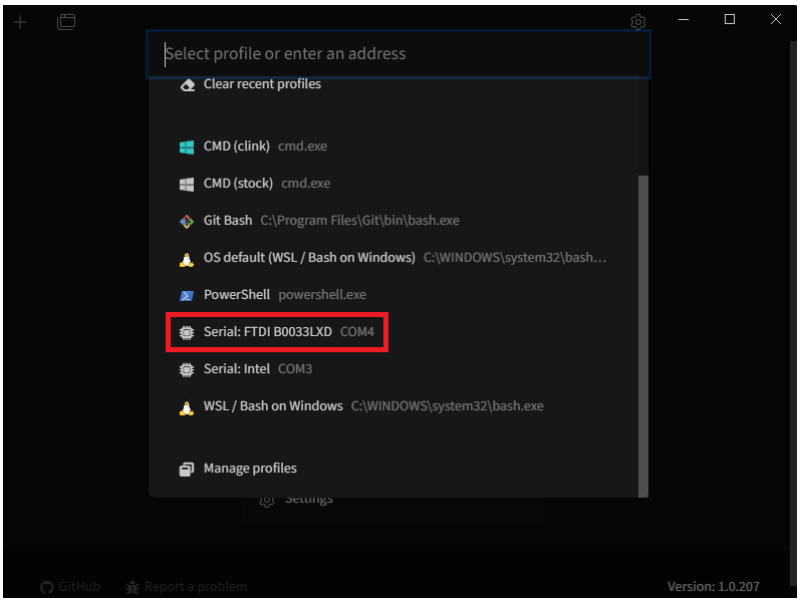
1.2 Téléchargement de l'image OPNSense

Sur le site OPNSense (https://opnsense.org/download/) j'ai télécharger l'image en serial



1.3 Se connecter au pare-feu avec Tabby

Choisir le COM 4 avec une vitesse de 9600

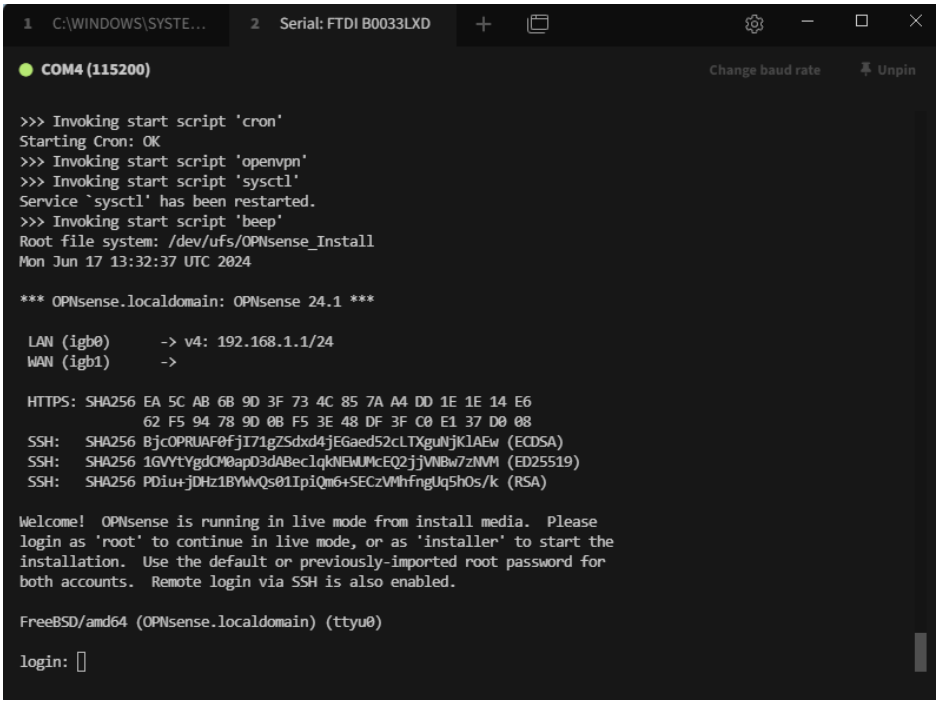


Cliquer sur F2 pour accéder au BIOS de la machine

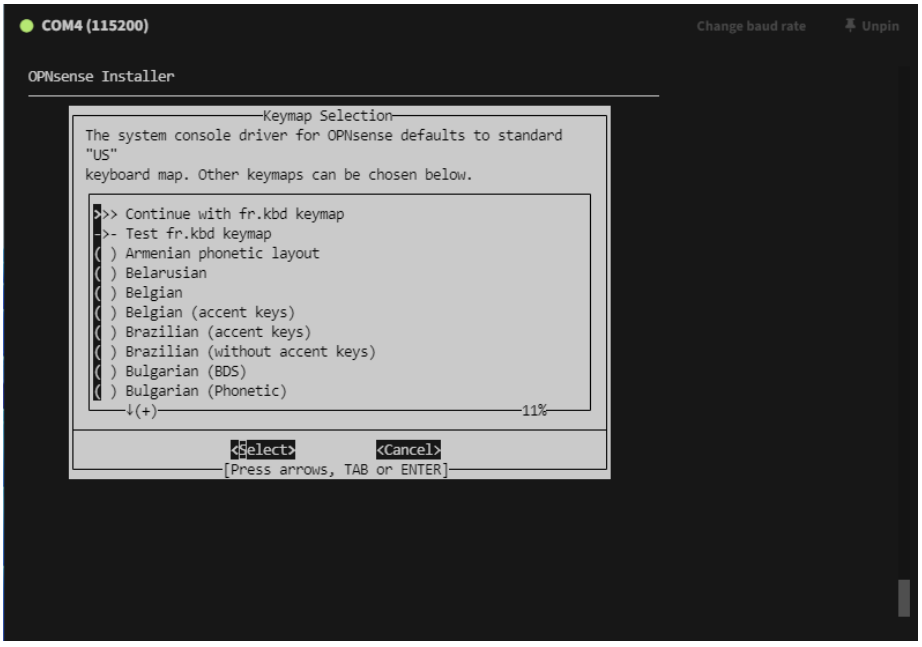
Lorsqu'on est dans le Bios de la machine on va dans l'onglet « BOOT » ensuite on met la clé USB avec l'ISO d'OPNSENSE en première option.

Ensuite on va dans « Hard Drive BBS Priorités » et on met la clé USB en première

Ensuite on enregistre et on fait un Sauvegarder et quitter et lancer en COM4 115200 au lieu de 9600. Cela devrait boot sur la l'OS de OPNSENSE et nous demander un nom d'utilisateur + mdp (Installer + opnsense)

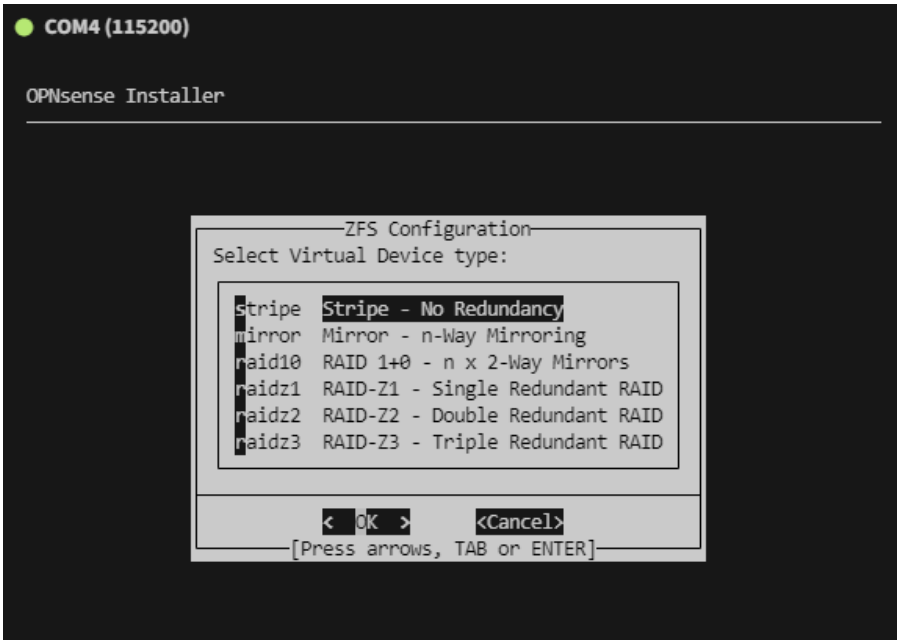


Lorsqu'on est connecté on suit le wizard d'installation. On commence par choisir le clavier AZERTY (Français) et lancer "fr.kdb keymap"



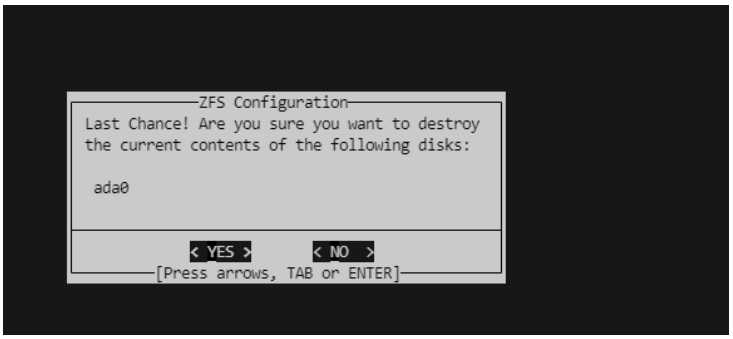
Puis on tape entrer sur « install (ZFS) »

Ensuite on choisit « no redundancy » pour la redondance

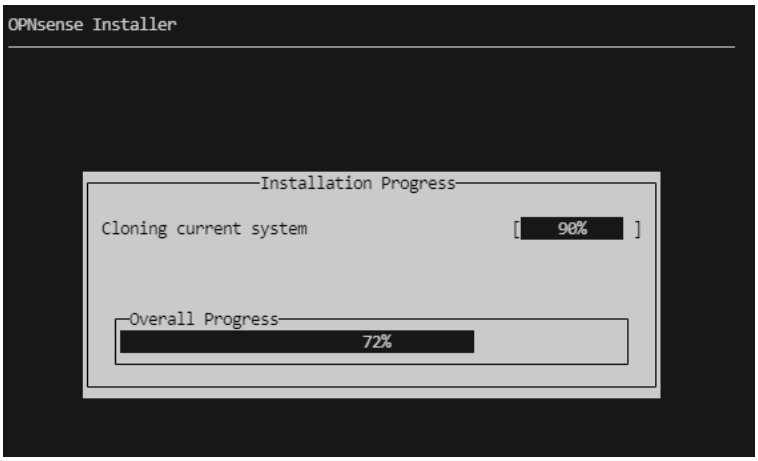


Puis on vas choisir le disque ou ont veux installer l'OS (HGST)

Et taper entrer sur « YES »

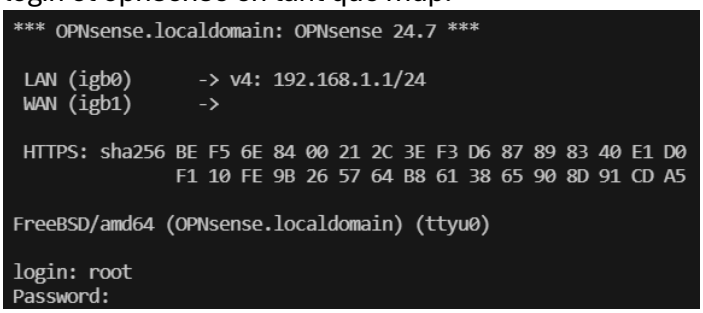


Ensuite on attend que sa s'installe.



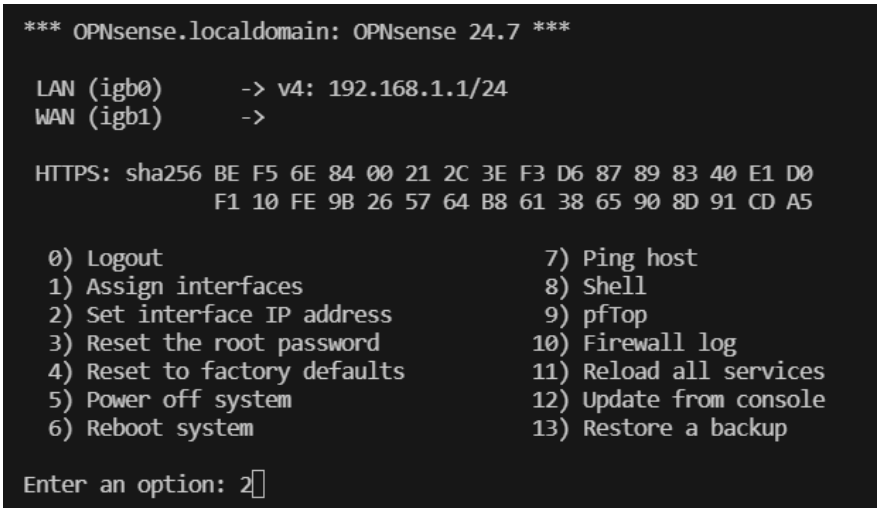
Lorsque l'OS a fini d'installer on choisis l'option de ne pas changer le password. (Complete Install)

Ensuite quand la machine a reboot on peux se connecter avec root en tant que login et opnsense en tant que mdp.



1.4 Configuration réseau du Riverbed

J'ai commencer par choisir la configuration 2 des adresse IP pour puisse mettre la LAN en 192.168.90.1 pour le client Rapsberry et en DHCP pour la WAN qui va prendre l'IP du réseau BTS SIO



On commence par la LAN

```
Available interfaces:

1 - LAN (igb0 - static, track6)
2 - WAN (igb1 - dhcp, dhcp6)

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

On configure l'IP static et le MSR

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.90.254


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
```

J'ai configuré la plage DHCP sur la LAN

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

Enter the start address of the IPv4 client address range: 192.168.90.10
Enter the end address of the IPv4 client address range: 192.168.90.20
```

Ensuite on ajoute les bons ports sur le LAN et WAN en allant sur l'Option 1 (Assign interfaces)

```
  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
```

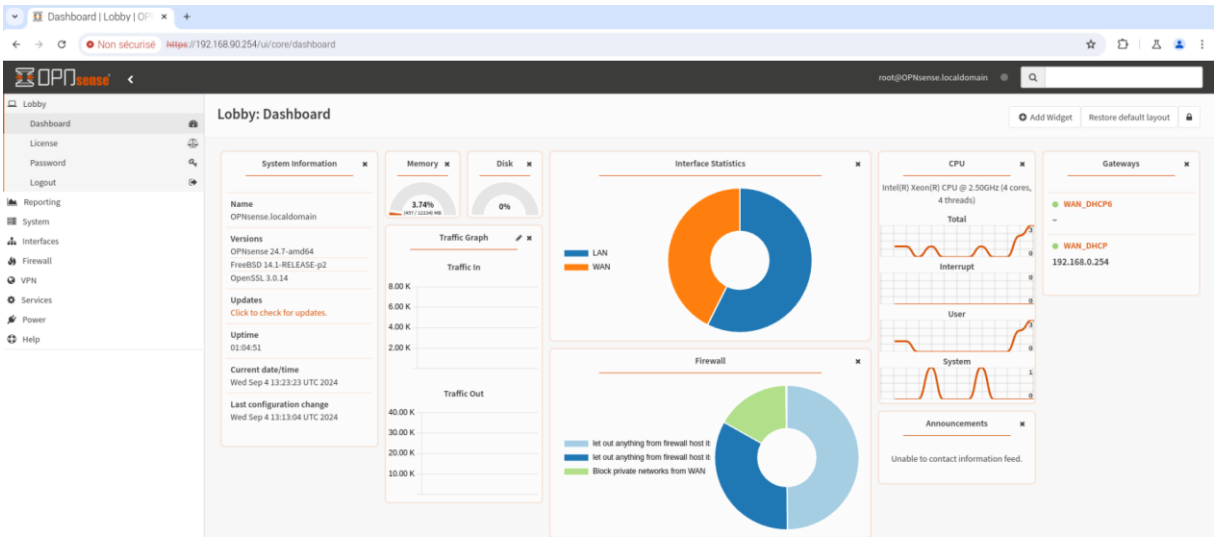
On a commencé par configurer la WAN pour avoir igb5 et LAN avec igb4

```
The interfaces will be assigned as follows:

WAN  -> igb5
LAN  -> igb4
```

1.5 Configuration via interface WEB (192.168.90.254)

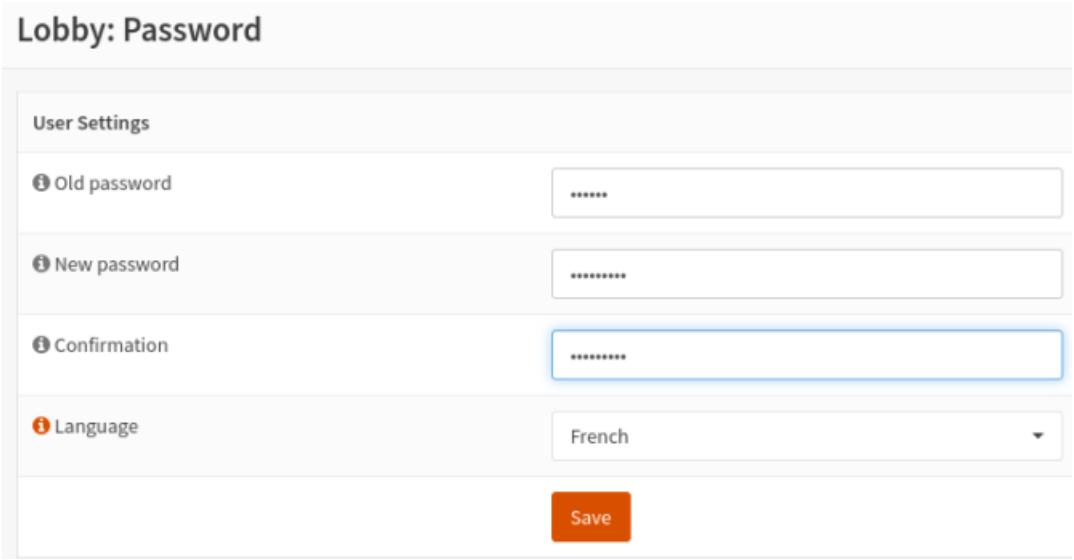
Sur le rapsberry qui est connecté avec une IP sur le sous-réseau 192.168.90.xx

Jme suis connecter sur l'interface web du pare-feu avec l'IP 192.168.90.254



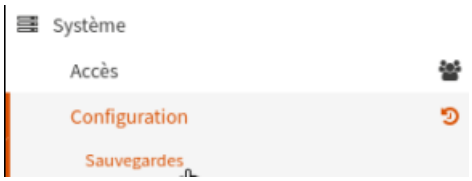
1.6 Changement du mot de passe admin du firewall/changer la langue

J'ai changé le mot de passe et la langue via l'interface WEB. Pour azerty123



1.7 Sauvegarde/restauration

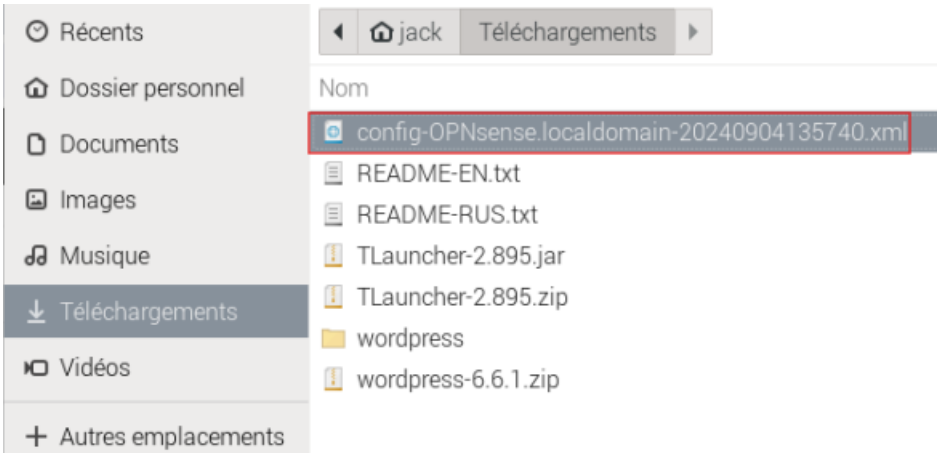
Pour configurer une sauvegarde je vais dans l'onglet « Système/Configuration/Sauvegarde »



J'ai ensuite fait une sauvegarde sur le raspberry client

Ensuite j'ai fait la restauration depuis le fichier de sauvegarde

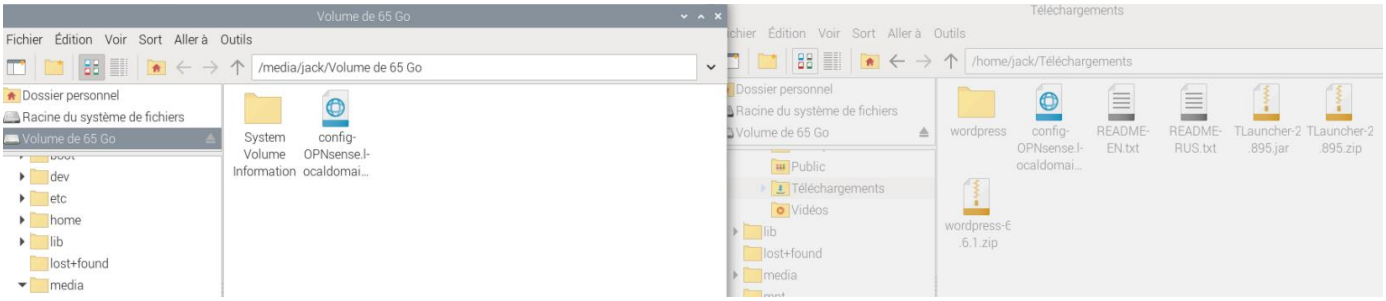
On choisi le fichier



Et cela redemarre le par-feu.

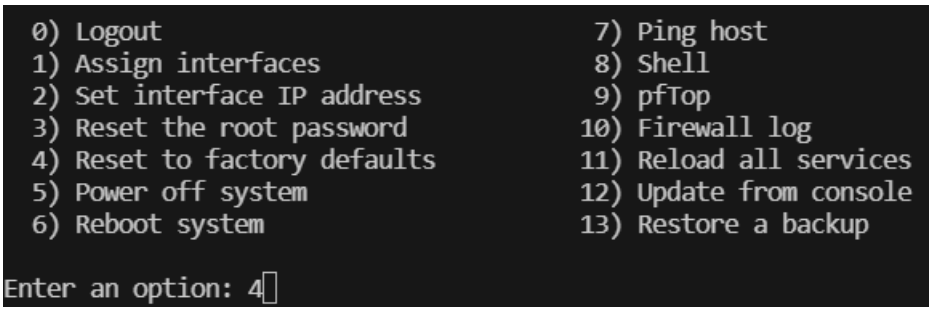
1.8 Reseter en mode usine

Je copie la sauvegarde sur une clé USB.



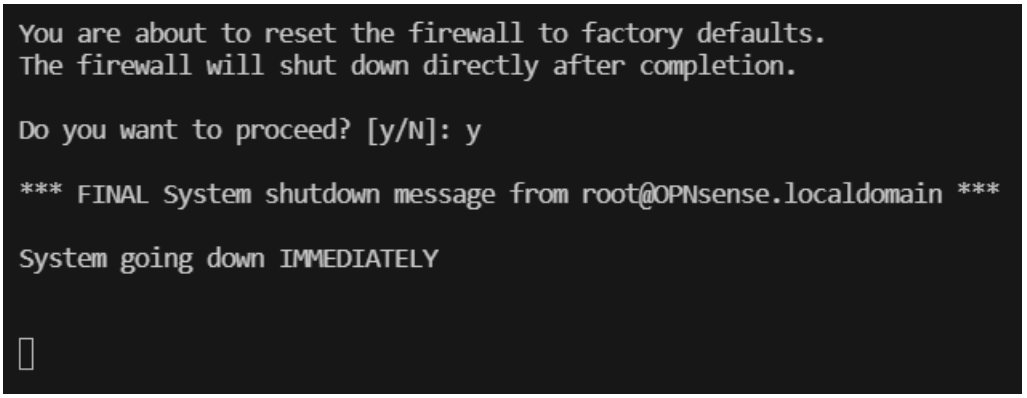
Il faut aussi créer un fichier qui se nomme config et ensuite renommer le fichier de configuration.xml en config.xml

Ensuite je reset a l'etat d'usine avec l'option 4.



Le par-feu est reset.

;lmùmmmmùm



Ensuite on branche la clé USB avec la restauration et on relance le par feu. Et lorsqu'on lance le par-feu je tape entrer pour lancer la « configuration importer » pour importer la configuration avant usine.

```
Press any key to start the configuration importer: ..

<HGST HTE725032A7E630 GSBOA3E0>    at scbus0 target 0 lun 0 (pass0,ada0)
<INTEL SSDSC2BB240G7 N2010112>     at scbus1 target 0 lun 0 (pass1,ada1)
<AHCI SGPIO Enclosure 2.00 0001>   at scbus2 target 0 lun 0 (ses0,pass2)
<SanDisk SanDisk 3.2 Gen1 DL17>    at scbus3 target 0 lun 0 (da0,pass3)
<15495061316989584408 288G>        ZFS pool (zroot)

Select device to import from (e.g. ada0) or leave blank to exit:
```

J'ai ensuite choisi la clé USB avec la commande da0

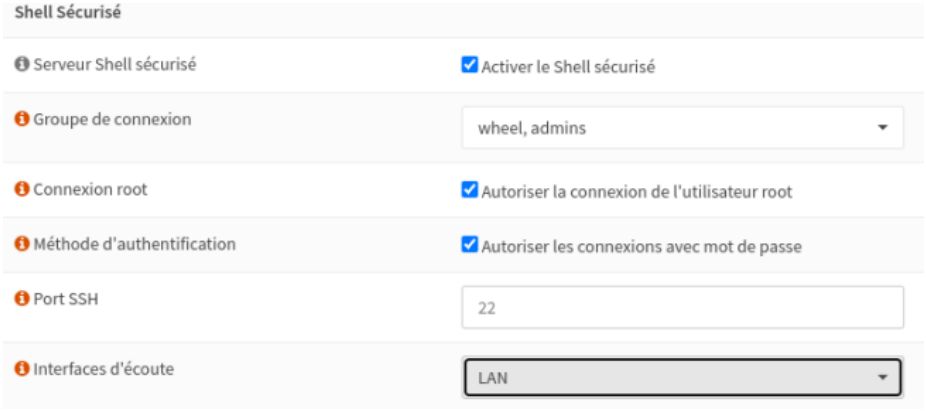
```
Starting import for partition '/dev/da0p1'.

Restoring config.xml...done.
Configuring crash dump device: /dev/ada0p3
swapon: adding /dev/ada0p3 as swap device
.ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib /usr/local/lib/compat/pkg /usr/local
/lib/compat/pkg /usr/local/lib/ipsec /usr/local/lib/perl5/5.36/mach/CORE
32-bit compatibility ldconfig path:
done.
>>> Invoking early script 'upgrade'
>>> Invoking early script 'configd'
Starting configd.
>>> Invoking early script 'templates'
Generating configuration: OK
>>> Invoking early script 'backup'
>>> Invoking backup script 'captiveportal'
>>> Invoking backup script 'dhcpleases'
>>> Invoking backup script 'duid'
>>> Invoking backup script 'netflow'
>>> Invoking backup script 'rrd'
>>> Invoking early script 'carp'
CARP event system: OK
Launching the init system...done.
Initializing.....done.
```

J'ai ensuite redémarré et la configuration est revenu

```
LAN (igb4)      -> v4: 192.168.90.254/24
WAN (igb5)      -> v4/DHCP4: 192.168.0.238/24

HTTPS: sha256 BE F5 6E 84 00 21 2C 3E F3 D6 87 89 83 40 E1 D0
              F1 10 FE 9B 26 57 64 B8 61 38 65 90 8D 91 CD A5

 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:
```

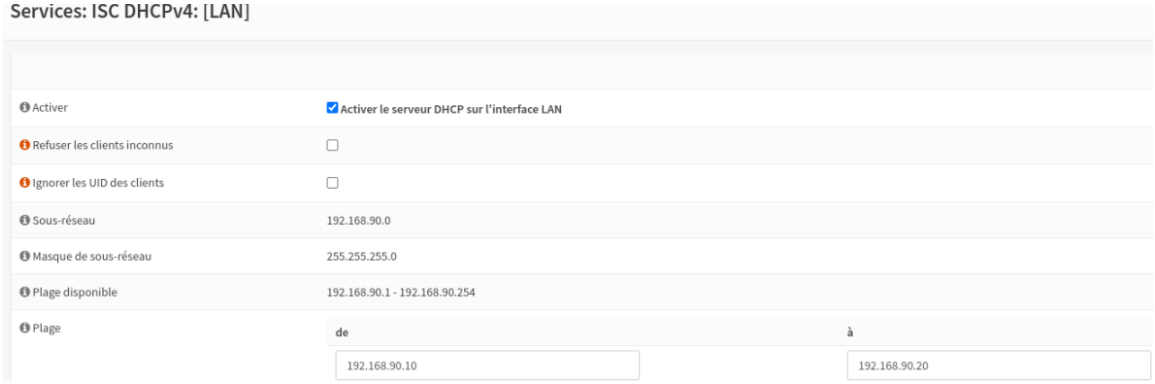
1.9 Activer le serveur SSH sur le Par-feu

On vas dans Système/Paramètres/Administration et sous « Shell sécurité » et on active les paramètres ci dessous



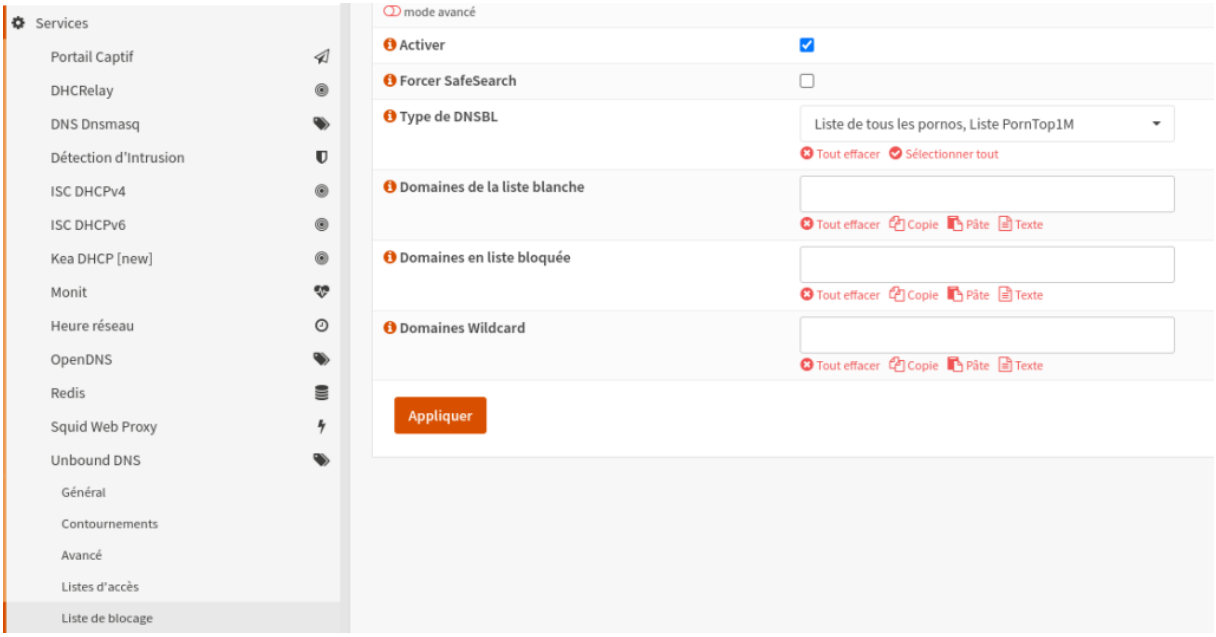
1.10 Configuration du DHCP dans la zone PRI

On est aller dans services/ISC DHCPv4/LAN et on active le serveur DHCP sur l'interface LAN et on ajoute une plage d'IP

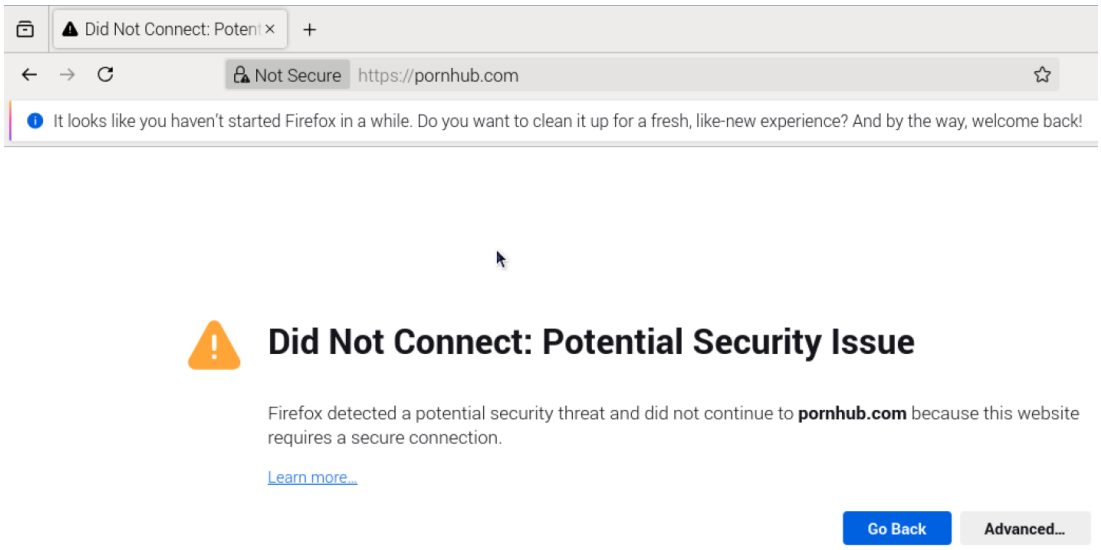


1.11 Configuration du Webfiltering et mise en place du proxy

On va dans services/OutboundDNS/Blocklist et on coche la case « Activer » et on ajoute un type de DNSBL

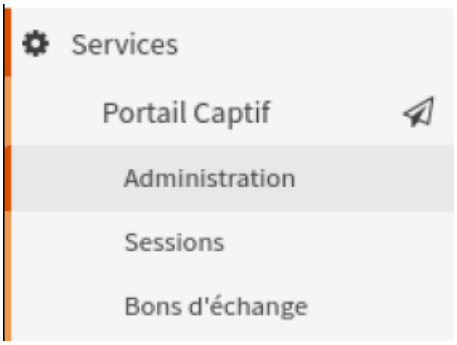


Et lorsqu'on va sur un des sites bloqués sa nous bloque.

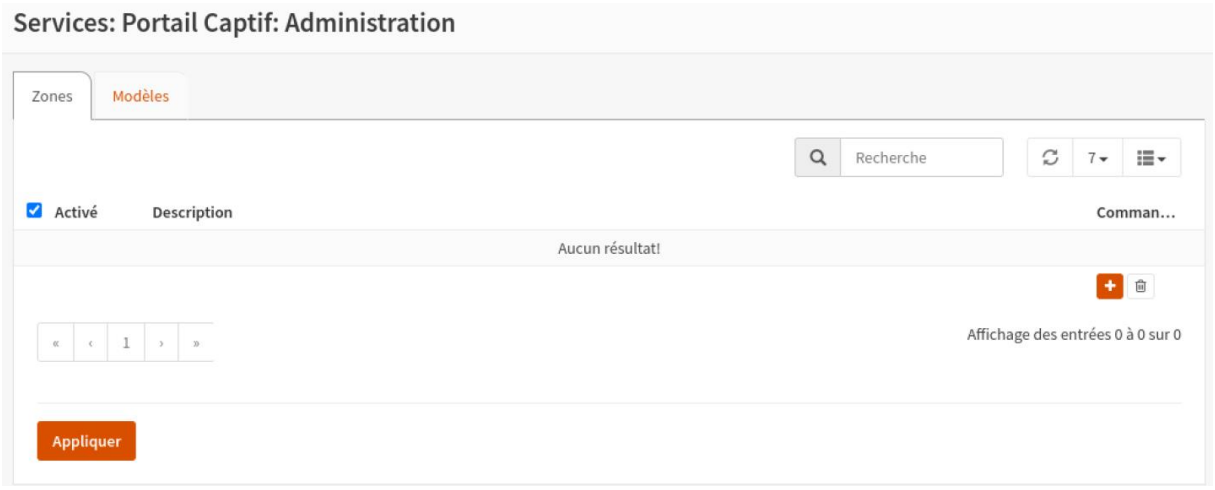


1.12 Configuration de portail d'authentification (compte local)

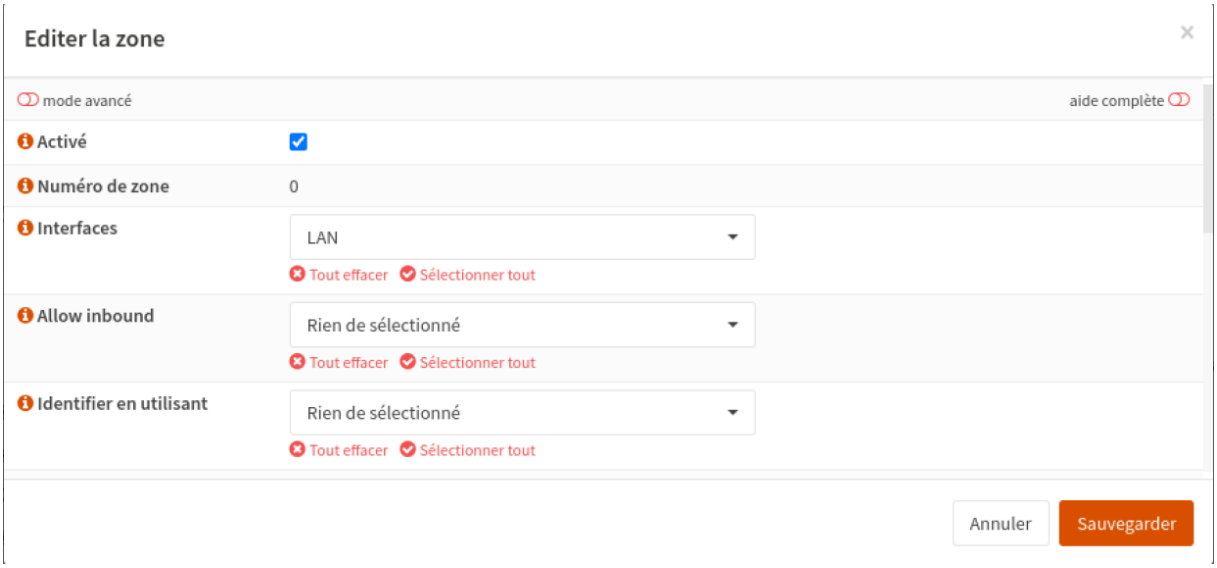
Pour configurer cela il faut aller dans /Services/Portail Captif/Administration



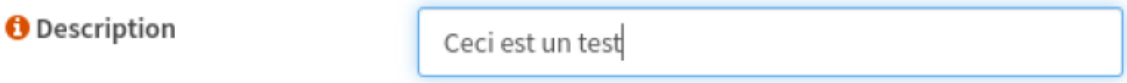
Cela nous affiche cette page :



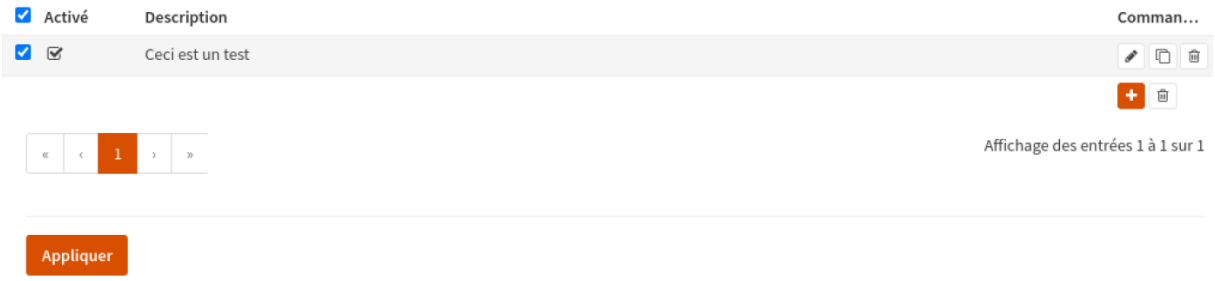
Ensuite on click sur le petit + qui nous affiche cette fenêtre



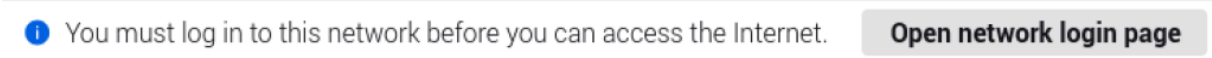
On ajoute ensuite une description toute en bas de la fenêtre et on clique sur « Appliquer »



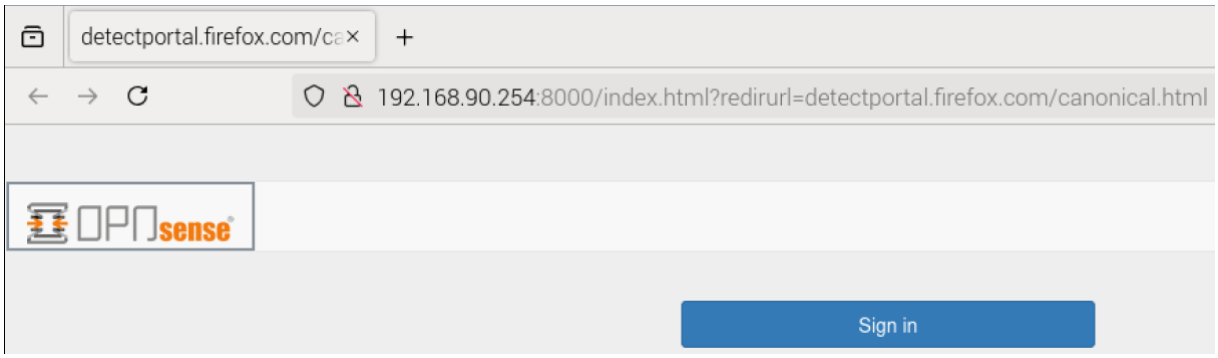
Ensuite on coche la case de « Ceci est un test » et on clique appliquer



Puis on va sur un navigateur web sur le Raspberry en 192.168.90.10 et cela nous demande de nous connecter sur une page web

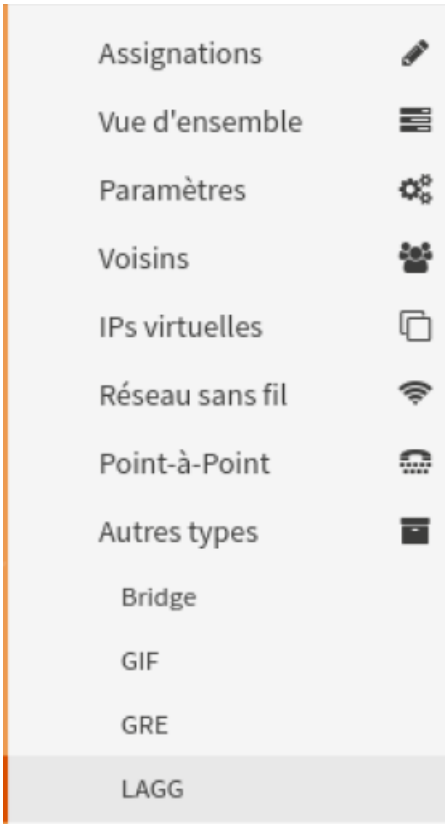


Lorsqu'on clique sur « Open network login page » et cela nous demande de se connecter avec un compte utilisateur.

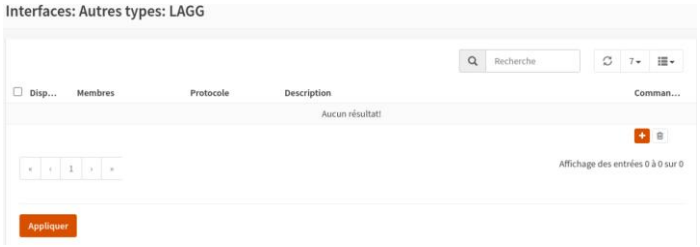


1.13 Configuration de l'agrégation de liens

Pour configurer le LAGG il faut aller dans /Interfaces/Other types/LAGG

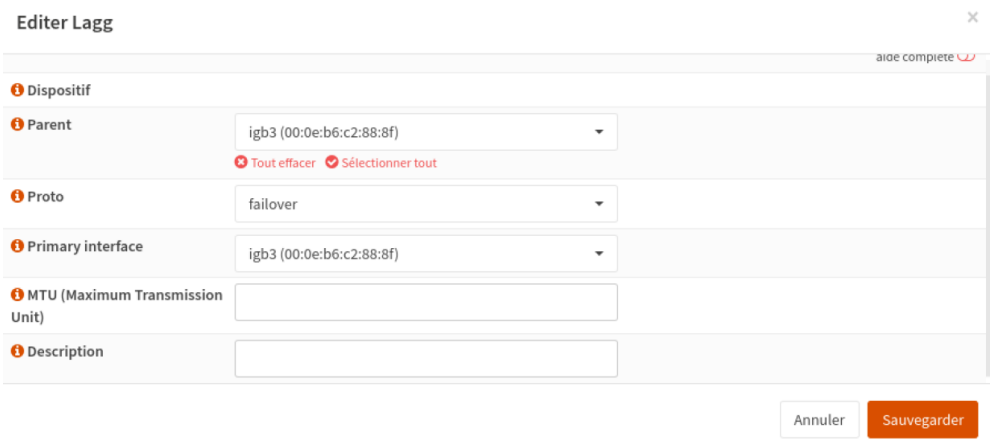


Ensuite on a une fenêtre qui s'affiche qui nous donne l'option d'ajouter un nouveau LAGG



Puis lorsqu'on clique sur le + pour ajouter une nouvelle configuration et on branche un autre câble réseau sur le port igb3 pour qu'on puisse faire une redondance (Failover).

On configure comme ci-dessous :



Ensuite « Sauvegarder » pour enregistrer la configuration