

# Firewall



## Contents

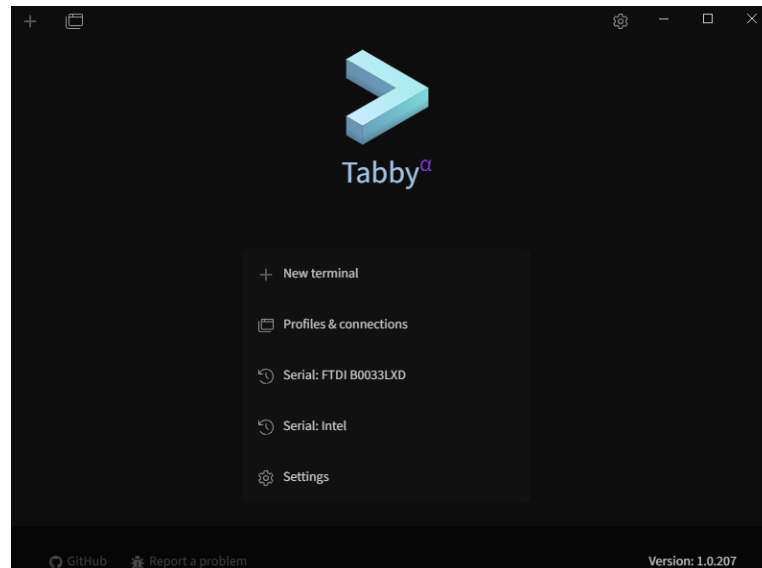
1.	Installation d'opnsense sur le Firewall Riverbed .....	2
1.1	Installation de Tabby .....	2
1.2	Téléchargement de l'image OPNSense .....	2
1.3	Se connecter au pare-feu avec Tabby .....	2
1.4	Configuration réseau du Riverbed.....	8
1.5	Configuration via interface WEB (192.168.90.254) .....	9
1.6	Changement du mot de passe admin du firewall/changer la langue .....	10
1.7	Sauvegarde/restauration.....	10
1.8	Reseter en mode usine.....	12
1.9	Activer le serveur SSH sur le Par-feu .....	14
1.10	Configuration du DHCP dans la zone PRI .....	14
1.11	Configuration du Webfiltering et mise en place du proxy.....	14
1.12	Configuration de portail d'authentification (compte local) .....	15
1.13	Configuration de l'agrégation de liens .....	17

# 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/Eugeniy/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

### Architecture

System architecture.

amd64

### Select the image type:

- dvd: ISO installer image with live system capabilities running in VGA mode. On amd64, UEFI boot is supported as well.
- vga: USB installer image with live system capabilities running in VGA mode as GPT boot. On amd64, UEFI boot is supported as well.
- serial: USB installer image with live system capabilities running in serial console (115200) including UEFI support..
- nano: a preinstalled serial image for USB sticks, SD or CF cards as MBR boot. These images are 3G in size and automatically adapt to the installed media size after first boot.

serial

### Mirror Location

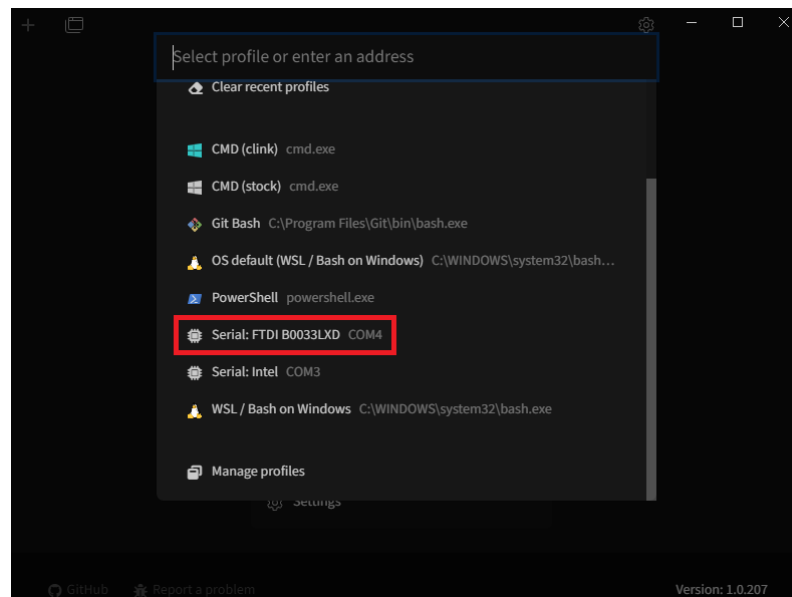
OPNsense can be downloaded from a large range of mirrors located in different countries, you may want to select the fastest options for your location.

LeaseWeb

Download

## 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)

```

1 C:\WINDOWS\SYSTE... 2 Serial: FTDI B0033LXD
COM4 (115200) Change baud rate Unpin

>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/ufs/OPNsense_Install
Mon Jun 17 13:32:37 UTC 2024

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

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

HTTPS: SHA256 EA 5C AB 6B 9D 3F 73 4C 85 7A A4 DD 1E 1E 14 E6
62 F5 94 78 9D 08 F5 3E 48 DF 3F C0 E1 37 D0 08
SSH: SHA256 BjCOPRUAF0fjI71gZ5dx4jEGaed52cLTxguNjK1AEw (ECDSA)
SSH: SHA256 1GVYtYgdCM8apD3dABec1qkNEMUMcEQ2jjVNBw7zMM (ED25519)
SSH: SHA256 PDiuzjDHZ1BYWwQs01IpiQm6+SECzVMhfngUq5hOs/k (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyu0)

login: 
```

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

```

COM4 (115200) Change baud rate Unpin

OPNsense Installer

Keymap Selection
The system console driver for OPNsense defaults to standard
"US"
keyboard map. Other keymaps can be chosen below.

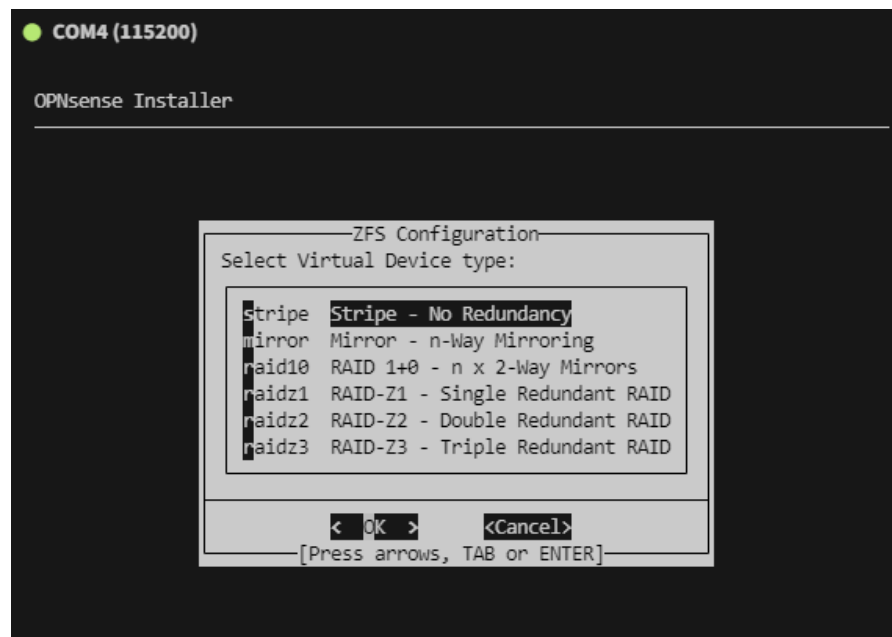
>>> Continue with fr.kbd keymap
>- Test fr.kbd keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
↓(+)-11%

[Select] [Cancel]
[Press arrows, TAB or ENTER]
```

Puis on tape entrer sur « install (ZFS) »



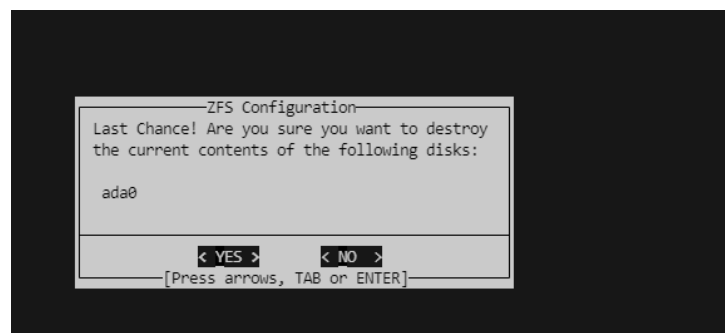
Ensuite on choisit « no redundancy » pour la redondance



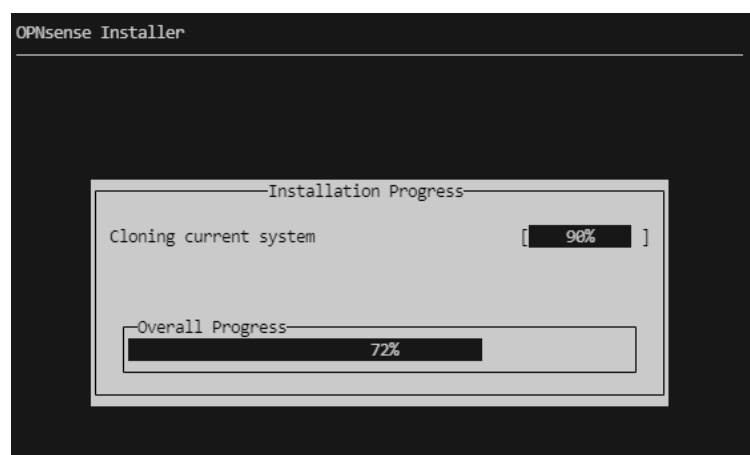
Puis on vas choisir le disque ou ont veux installer l'OS (HGST)



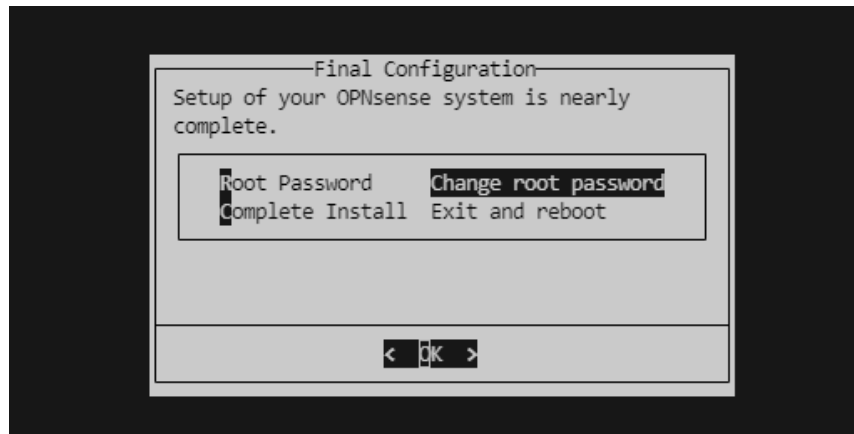
Et taper entrer sur « YES »



Ensuite on attend que sa s'installe.



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



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

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

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

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

FreeBSD/amd64 (OPNsense.localdomain) (ttyu0)
login: root
Password:
```

## 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

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

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

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: 2
```



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

Enter an option: 1
```

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

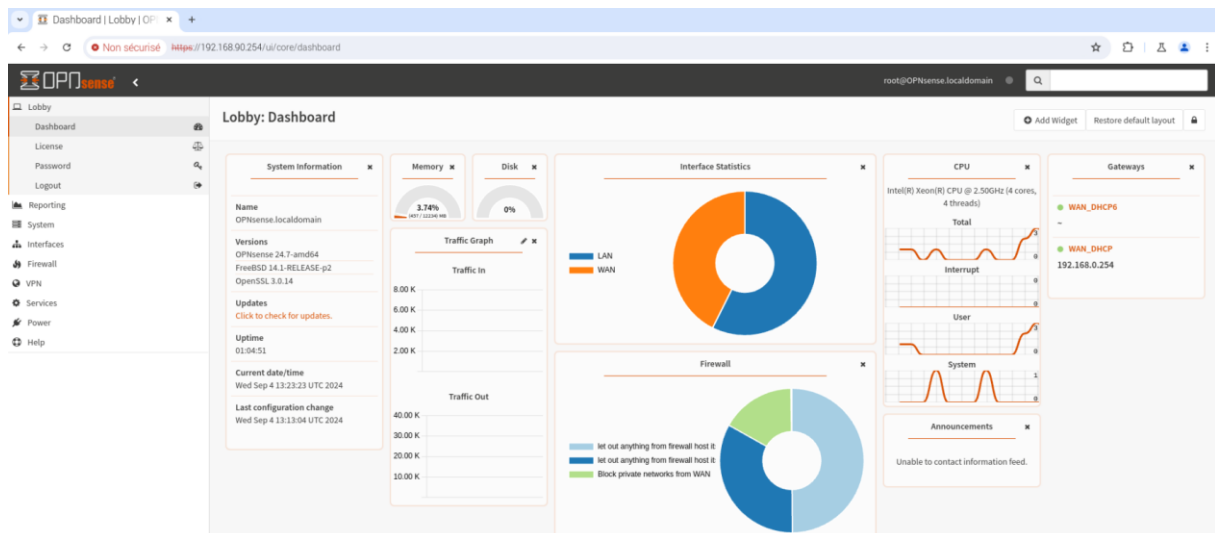
```
The interfaces will be assigned as follows:

WAN -> igb5
LAN -> igb4
```

## 1.5 Configuration via interface WEB (192.168.90.254)

Sur le raspberry 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

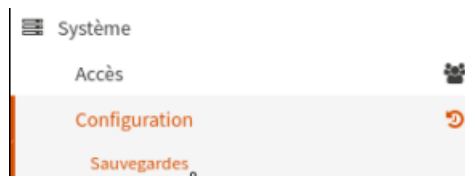
The screenshot shows the 'Lobby: Password' settings page. It includes a 'User Settings' section with the following fields:

- Old password:** A text input field with masked characters (\*\*\*\*\*).
- New password:** A text input field with masked characters (\*\*\*\*\*).
- Confirmation:** A text input field with masked characters (\*\*\*\*\*).
- Language:** A dropdown menu currently set to 'French'.

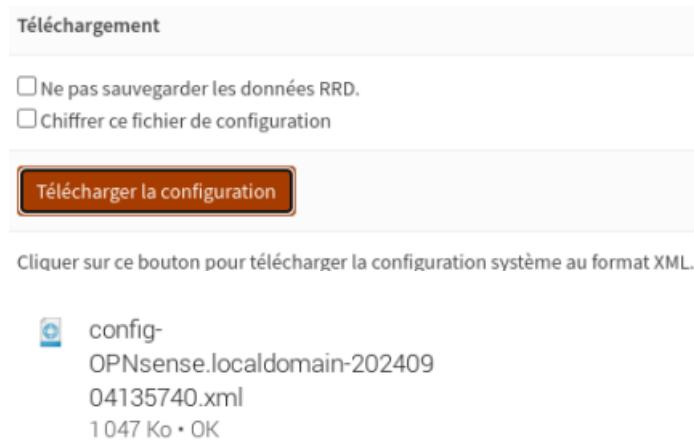
A 'Save' button is located at the bottom right of the form.

## 1.7 Sauvegarde/restauration

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



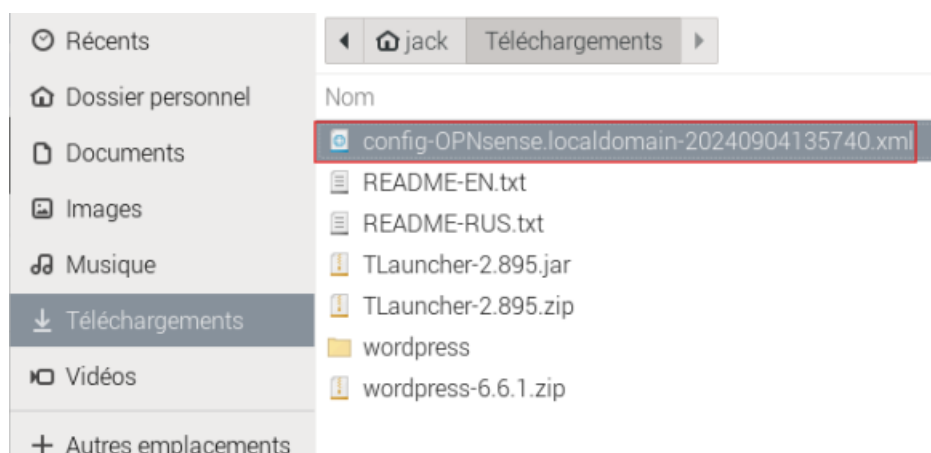
J'ai ensuite fait une sauvegarde sur le raspberry client



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



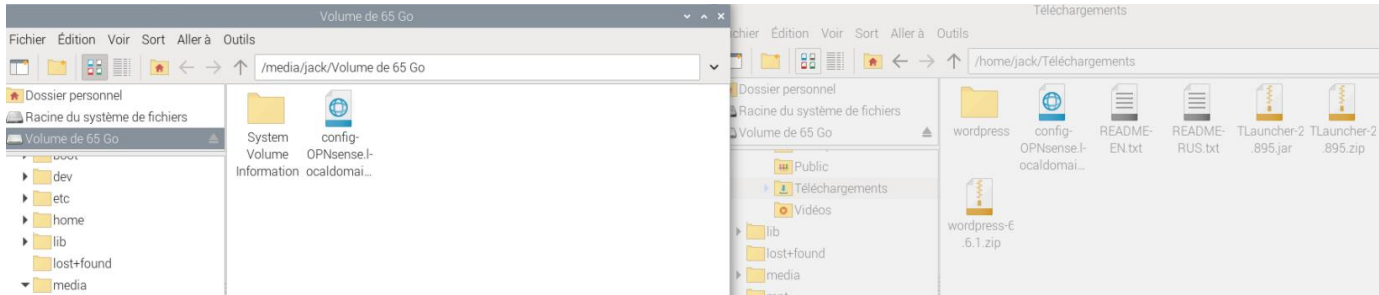
On choisi le fichier



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'état d'usine avec l'option 4.

```

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

Enter an option: 4

```

Le par-feu est reset.

;lmùmmmmùm

```

You are about to reset the firewall to factory defaults.
The firewall will shut down directly after completion.

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

*** FINAL System shutdown message from root@OPNsense.localdomain ***

System going down IMMEDIATELY


```

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 va dans Système/Paramètres/Administration et sous « Shell sécurisé » et on active les paramètres ci dessous

Shell Sécurisé

📘 Serveur Shell sécurisé	<input checked="" type="checkbox"/> Activer le Shell sécurisé
🔑 Groupe de connexion	wheel, admins
👤 Connexion root	<input checked="" type="checkbox"/> Autoriser la connexion de l'utilisateur root
🔑 Méthode d'authentification	<input checked="" type="checkbox"/> Autoriser les connexions avec mot de passe
🔑 Port SSH	22
🔑 Interfaces d'écoute	LAN

## 1.10 Configuration du DHCP dans la zone PRI

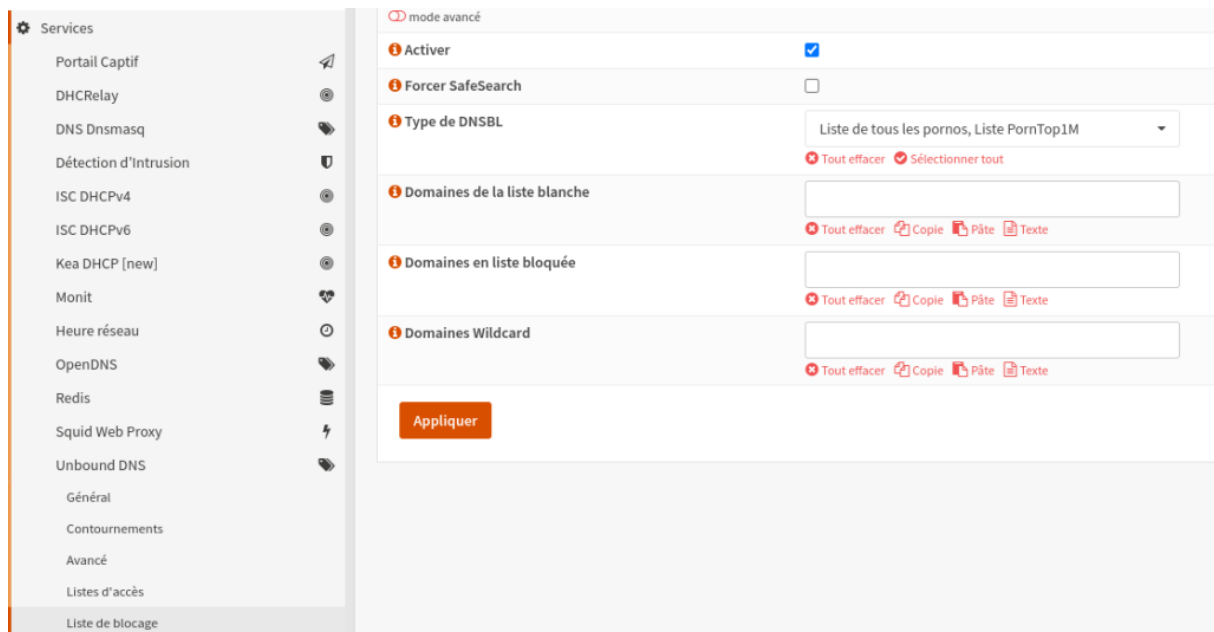
On est aller dans services/ISC DHCPv4/LAN et on active le serveur DHCP sur l'interface LAN et on ajoute une plage d'IP

Services: ISC DHCPv4: [LAN]

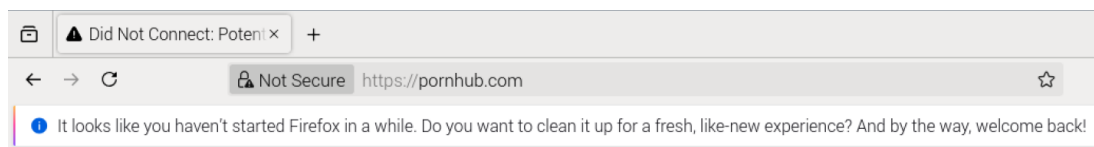
📘 Activer	<input checked="" type="checkbox"/> Activer le serveur DHCP sur l'interface LAN	
🚫 Refuser les clients inconnus	<input type="checkbox"/>	
🚫 Ignorer les UID des clients	<input type="checkbox"/>	
📘 Sous-réseau	192.168.90.0	
📘 Masque de sous-réseau	255.255.255.0	
📘 Plage disponible	192.168.90.1 - 192.168.90.254	
📘 Plage	de	à
	192.168.90.10	192.168.90.20

## 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.



## Did Not Connect: Potential Security Issue

Firefox detected a potential security threat and did not continue to **pornhub.com** because this website requires a secure connection.

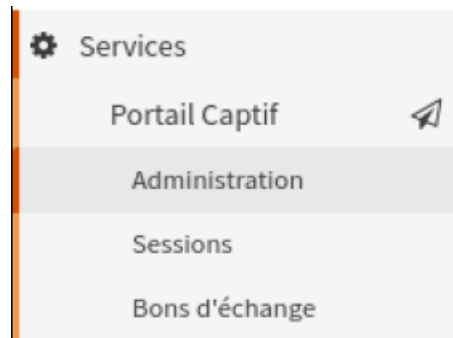
[Learn more...](#)

Go Back

Advanced...

## 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 :

Services: Portail Captif: Administration

Zones Modèles

Recherche

Aucun résultat!

« 1 »

Appliquer

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

Editer la zone

mode avancé aide complète

Activé

Numéro de zone 0

Interfaces LAN

Allow inbound Rien de sélectionné

Identifier en utilisant Rien de sélectionné

Annuler Sauvegarder




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


Description

Ceci est un test



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

<input checked="" type="checkbox"/> Activé	Description	Comman...
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Ceci est un test	  









Affichage des entrées 1 à 1 sur 1


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

 You must log in to this network before you can access the Internet.

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

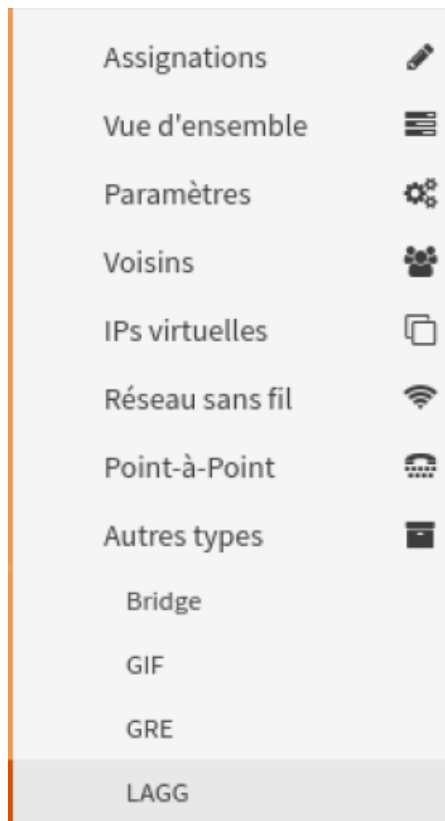
 detectportal.firefox.com/canonical.html +

     192.168.90.254:8000/index.html?redirurl=detectportal.firefox.com/canonical.html

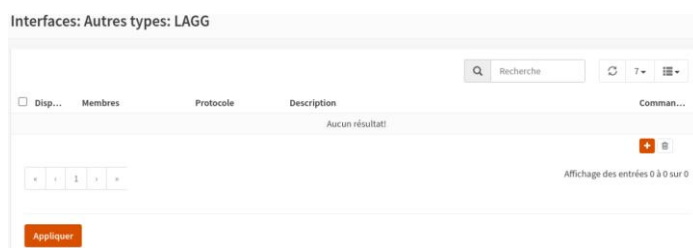


## 1.13 Configuration de l'agrégation de liens

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 :

Editer Lagg

Dispositif

Parent: igb3 (00:0e:b6:c2:88:8f)

Proto: failover

Primary interface: igb3 (00:0e:b6:c2:88:8f)

MTU (Maximum Transmission Unit):

Description:

Annuler Sauvegarder

Ensuite « Sauvegarder » pour enregistrer la configuration